管理：ユーザ管理とセキュリティ

SAP Sybase IQ 16.0 SP03

ドキュメント ID： DC02015-01-1603-01
改訂： 2013 年 12 月

目次

セキュリティ管理

SAP® Sybase® IQ では、ロールベースのセキュリティモデルを使用して、データベースオブジェクトへのアクセスおよび権限付き操作の実行を制御します。このモデルにより、ユーザに付与する権限を十分な詳細度で完全に制御できます。データベースでそれぞれの権限付き操作を行うには、その操作を実行するユーザに 1 つ以上のシステム権限またはオブジェクトレベル権限が割り当てられている必要があります。

*システム権限*は、承認済みデータベースタスクの実行をユーザに許可します。たとえば、ユーザに CREATE TABLE システム権限を割り当てると、そのユーザは自己所有テーブルを作成できるようになります。

*オブジェクトレベル権限*は、指定したオブジェクトに対する承認済みタスクの実行をユーザに許可します。たとえば、`TableA` に対する ALTER オブジェクトレベル権限をユーザに割り当てると、そのユーザはそのテーブルだけを変更でき、他のテーブルは変更できなくなります。

*ロール*とは、システム権限、オブジェクトレベル権限、他のロールを 1 つ以上含めることができるコンテナです。ロールをユーザに付与することは、ロールの基礎となるシステム権限とオブジェクトレベル権限をユーザに付与することに相当します。

新しいユーザはすべて、自動的に PUBLIC システムロールを付与されます。これにより、ユーザは次の操作を実行できるようになります。

- システムビューに保存されたデータを表示する。
- ほとんどのシステムストアドプロシージャを実行する。

新しく作成したユーザに対して、次の操作を実行できます。

- そのユーザにユーザ定義ロール、システムロール、システム権限、およびオブジェクトレベル権限を付与する。
- そのユーザにログインポリシーを割り当てる。デフォルトでは、ユーザはルートログインポリシーに割り当てられます。
- SQL Remote システムで使用するために、そのユーザをパブリッシャとしてまたはデータベースのリモートユーザとして設定する。

新しい、または移行された、各 SAP Sybase IQ データベースには、使い始める際に利用できる事前定義済みの一連のロールが含まれます。これらのシステムロールは、ロールベースのセキュリティを実装するための出発点として機能します。

注意： 16.0 より前のバージョンの SAP Sybase IQ を使用していた場合は、ご使用のオペレーティングシステムに対応する『移行 ガイド』の「ロールベースのセキュリティへのアップグレード」で、権限/パーミッション/グループモデルからロー

ル/権限/ユーザ拡張ロールモデルへのセキュリティモデルの変更に関する項を確認することをおすすめします。

ロールベースのセキュリティの計画と実装

ロールベースのセキュリティモデルの計画および実装には明確なワークフローが存在します。

セキュリティ階層の設計

1. ユーザによって実行されるさまざまな承認済みタスクを特定します。密接に関連するタスクをグループ化します。グループ化は、任意の組織構造 (部門、機能、など) にもとづいて行うことができます。組織階層と一致したロール階層を作成できます。各グループに名前を割り当てます。これらのグループが、作成する*ロール*に相当します。
2. 確認された承認済みタスクそれぞれの実行に必要な*システム権限*および*オブジェクトレベル権限*を確認します。
3. さまざまな承認済みタスクを実行する*ユーザ*を特定します。このユーザを、適用可能なロールまたは確認された個別のタスクに関連付けます。
4. (省略可) 作成するロールの管理者を指定します。管理者は、他のユーザに対するロールの付与と取り消しを実行できます。
5. (省略可) 作成するロールの構成部分ではないシステム権限とオブジェクトレベル権限の管理者を指定します。

セキュリティ階層の構築

1. 必要なロールを作成します。ロールを参照してください。
2. それぞれのロールにシステム権限を付与します。ロールと権限を参照してください。
3. ユーザを作成します。ユーザを参照してください。
4. 各ユーザに適用可能なロールを付与します。該当する場合は管理権限も付与します。ロールを参照してください。
5. ユーザに (ロールによってまだ間接的に付与されていない) 適用可能なオブジェクトレベル権限とシステム権限を付与します。該当する場合は管理権限も付与します。権限を参照してください。

参照：

- ロール (3 ページ)
- 権限 (33 ページ)
- ユーザ (115 ページ)

ロール

ロールは、システム権限、オブジェクトレベル権限、およびロールの包含が可能なコンテナです。ロールに対する権限の付与と取り消しは、ユーザの場合と同様です。ロールとユーザに同じ名前を使用することはできません。

ユーザ定義ロール

ユーザ定義ロールはシステム権限とオブジェクトレベル権限のカスタムコレクションであり、通常は特定のタスクまたは一連のタスクに関連する権限をグループ化するために作成されます。

ユーザ定義ロールの特徴は次のとおりです。

- ログイン権限を持たないスタンドアロンオブジェクトにすることができ、オブジェクトを所有できます。
- ロールとして動作する機能を持つデータベースユーザ (ユーザ拡張ロール) にすることができます。既存のユーザ ID にログイン権限がある場合、ユーザ拡張ロールはそのログイン権限を保持します。
- 他のオブジェクトに対する権限を付与できます。
- 他のロールの権限を付与できます。
- 名前は大文字と小文字が区別されません。

ユーザ定義ロールを付与することは、その基礎となるシステム権限とオブジェクトレベル権限をそれぞれ個別に付与することと、セマンティック上同等です。

ユーザ定義ロールをユーザ拡張ロールに変換すること、またはその逆の変換は、実行できません。

注意： 特に明記されていないかぎり、*ユーザ定義ロール*という用語は、ユーザ拡張ロールとユーザ定義ロールの両方を指します。

ユーザ定義ロールの作成

新しいユーザ定義ロールを作成します。

前提条件

MANAGE ROLES システム権限。

手順

ユーザ定義ロールにログインパスワードを設定することはできません。ユーザ定義ロールを作成するときに、ロールの管理者、およびその管理者もそのロールのメンバーにするどうかを指定することができます。管理者を指定しないと、グローバルロール管理者 (MANAGE ROLES システム権限が付与されている任意のユーザ) がそのロールのデフォルトの管理者になります。

ただし、ロールの作成時に 1 人以上のロール管理者が指定された場合、グローバルロール管理者はロールを管理できません。これは、SYS_MANAGE_ROLES_ROLE システム権限がそのロールに管理権限付きで自動的に付与されることがないためです。このため、ロールの作成時にロール管理者を定義しないか (作成後に追加)、または作成プロセス中にロール管理者のみを指定して SYS_MANAGE_ROLES_ROLE システム権限を管理権限付きで明示的に付与することを強くおすすめします。 作成プロセス。

ロールの作成後にロール管理者を追加したり削除したりできます。既存のロール名を使用して新しいロールを作成しようとすると、文が失敗します。

新しいユーザ定義ロールを作成するには、以下の文のいずれかを実行します。

作成条件	文
グローバルロール管理者のみ **ロール管理者なし**	**CREATE ROLE** *role_name*
ロールメンバーシップのないロール管理者 **グローバルロール管理者なし**	**CREATE ROLE** *role_name* **WITH ADMIN ONLY** *admin_name [,...]*
ロールメンバーシップを持つロール管理者 **グローバルロール管理者なし***	**CREATE ROLE** *role_name* **WITH ADMIN** *admin_name [,...]*
ロールメンバーシップのないロール管理者 **グローバルロール管理者あり***	**CREATE ROLE** *role_name* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE**, *admin_name [,...]*

*グローバルロール管理者にはロールのメンバーシップを付与できないので、ロール管理者にロールのメンバーシップを付与して (WITH ADMIN オプション) ロールを作成する場合は、SYS_MANAGE_ROLES_ROLE を管理者リストに含めることはできません。しかし、ロールのメンバーシップが付与されていないロール管理者を指定して (WITH ADMIN ONLY オプション) ロールを作成する場合は、これを含めることができます。

例:

次の文では、ロール管理者を指定しないロール `Sales` が作成されます。MANAGE ROLES システム権限を持つユーザが、このロールのデフォルト管理者になります。

```
CREATE ROLE Sales
```

次の文は、*Jane* と *Bob* をロール管理者として、ロールのメンバーシップは付与しないでロール `Marketing` を作成します。また、グローバルロール管理者がロールを管理することも許可します。

```
CREATE ROLE Marketing WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE, Jane,
Bob
```

参照：

- ロール管理者とグローバルロール管理者 (11 ページ)
- CREATE ROLE 文 (279 ページ)

既存のユーザをユーザ拡張ロールに変換する

ロールとして機能するように既存のユーザ ID を拡張することができます。これは、特定のユーザに割り当てられている一連のシステム権限とオブジェクトレベル権限を別のユーザに付与する必要がある場合に便利です。

前提条件

MANAGE ROLES システム権限。

手順

既存の ID にログイン権限がある場合、ユーザ拡張ロールはそのログイン権限を保持します。

ロールとして機能するようにユーザを変換するときに、そのロールの管理者を指定したり、それらの管理者もそのロールのメンバーになるかどうかを指定することができます。管理者を指定しないと、グローバルロール管理者 (MANAGE ROLES システム権限が付与されている任意のユーザ) がそのロールのデフォルトの管理者になります。

ただし、変換時に 1 人以上のロール管理者が指定された場合、グローバルロール管理者はロールを管理できません。これは、SYS_MANAGE_ROLES_ROLE システム権限がそのロールに管理権限付きで自動的に付与されることがないためです。このため、ロールの作成時にロール管理者を定義しないか (作成後に追加)、または作成プロセス中にロール管理者のみを指定して SYS_MANAGE_ROLES_ROLE システム権限を管理権限付きで明示的に付与することを強くおすすめします。 変換プロセス。

ユーザの変換後に、ロール管理者を追加および削除できます。存在しないユーザ ID を使用してユーザを変換しようとすると、文は失敗します。

既存のユーザを変換するには、次の文のいずれかを実行します。

変換条件	文
グローバルロール管理者のみ ロール管理者なし	**CREATE ROLE FOR USER** *userID*
ロールメンバーシップのないロール管理者 グローバルロール管理者なし	**CREATE ROLE FOR USER** *userID* **WITH ADMIN ONLY** *admin_name [,...]*
ロールメンバーシップを持つロール管理者 グローバルロール管理者なし*	**CREATE ROLE FOR USER** *userID* **WITH ADMIN** *admin_name [,...]*
ロールメンバーシップのないロール管理者 グローバルロール管理者*	**CREATE ROLE FOR USER** *userID* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE**, *admin_name [,...]*

*グローバルロール管理者にはロールのメンバーシップを付与できないので、ロール管理者にロールのメンバーシップを付与して (WITH ADMIN オプション) ロールを作成する場合は、SYS_MANAGE_ROLES_ROLE を管理者リストに含めることはできません。しかし、ロールのメンバーシップが付与されていないロール管理者を指定して (WITH ADMIN ONLY オプション) ロールを作成する場合は、これを含めることができます。

例:

この文は、ロールとして機能するようにユーザ `Sales1` を拡張します。ロール管理者が指定されていないため、MANAGE ROLES システム権限を持つユーザはロールを管理できます。

```
CREATE ROLE FOR USER Sales1
```

この文は、ロールとして機能するようにユーザ `Marketing1` を拡張し、ロール管理者として *Jane* および *Bob* を指定します。また、グローバルロール管理者がロールを管理することも許可します。

```
CREATE ROLE FOR USER Marketing1 WITH ADMIN ONLY
SYS_MANAGE_ROLES_ROLE, Jane, Bob
```

参照：

- ロール管理者とグローバルロール管理者 (11 ページ)
- CREATE ROLE 文 (279 ページ)

ユーザ拡張ロールからユーザへの逆変換

ユーザ拡張ロールを変換して、通常のユーザに戻すことができます。

前提条件

変換するユーザ拡張ロールに対する管理権限。

手順

ユーザ拡張ロールに付与されているログイン権限、システム権限、およびロールはすべて、ユーザに付与されます。ユーザがロールとして動作するように拡張された後で作成されたオブジェクトは、ユーザが所有者になります。ユーザ拡張ロールのメンバーはすべて、すぐに取り消されます。

常に、ログインパスワードが設定されているロール管理者またはグローバルロール管理者がロールごとに最小数 (**MIN_ROLE_ADMINS** データベースオプションで定義) 存在する必要があります。ユーザ拡張ロールを変換してユーザに戻す場合、ユーザ拡張ロールの依存ロールはすべて引き続きこの最小要件を満たす必要があります。満たさない場合、変換は失敗します。

ユーザ拡張ロールを変換してユーザに戻すには、次のどちらかの文を実行します。

変換条件	文
ロールにメンバーが まったく付与されていない。	**DROP ROLE FROM USER** *role_name*
ロールにメンバーが 付与されている。	**DROP ROLE FROM USER** *role_name* **WITH REVOKE**

ユーザまたはロールへのユーザ定義ロールの追加

ユーザまたはロール (被付与者) にユーザ定義ロールのメンバーシップを、管理権限付きまたはなしで追加します。

前提条件

付与するロールに対する管理権限。

手順

ユーザ定義ロールは、管理権限付きまたはなしで付与できます。管理権限付きで付与した場合 (WITH ADMIN オプションを使用)、ユーザは、そのロールを管理 (付与、取消、および削除) でき、さらにロールの基礎となるシステム権限とオブジェクトレベル権限をすべて使用できます。管理権限のみが付与された場合 (WITH ADMIN ONLY オプションを使用)、ユーザはロールを管理できますが、そ

の基礎となるシステム権限とオブジェクトレベル権限を使用することはできません。管理権限なしで付与された場合、ユーザはその基礎となるシステム権限とオブジェクトレベル権限を使用することはできますが、ロールを管理することはできません。

ユーザにロールのメンバーシップが付与されると、ユーザはそのロールの基礎となるすべてのシステム権限とロール、およびテーブル、ビュー、およびプロシージャに対するオブジェクトレベルパーミッションを継承します。

ロールが別のロールに付与されると、付与されるロールの全メンバーシップ (子ロール) は自動的に付与先ロール (親ロール) のメンバーになり、親ロールの基礎となるすべてのシステム権限とロール (テーブル、ビュー、およびプロシージャに対するものも含む) を継承します。親ロールの既存のメンバーは、子ロールのメンバーになったり、子ロールの基礎となるシステム権限やロールを継承したりすることはありません。

ユーザ定義ロールを被付与者に付与するには、以下の文のいずれかを実行します。

付与タイプ	文
ロールのメンバーシップとそのロールに対する完全な管理権限	**GRANT ROLE** *role_name* **TO** *grantee [,...]* **WITH ADMIN OPTION**
ロールに対する管理権限のみ管理権限のみ	**GRANT ROLE** *role_name* **TO** *grantee [,...]* **WITH ADMIN ONLY OPTION**
ロールに対する管理権限なしのロールのメンバーシップ	**GRANT ROLE** *role_name* **TO** *grantee [,...]* **WITH NO ADMIN OPTION**

例:

- User1、User2、User3 の 3 人のユーザがいます。
- Role1、Role2、Role3、Role4 の 4 つのロールがあります。
- Priv1、Priv2 の 2 つのシステム権限があります。
- Role1 には Priv1 と Role3 が付与されています。
- User2 と User3 は Role1 のメンバーです。
- Role2 には Priv2 と Role4 が付与されています。
- User3 は Role2 のメンバーです。

次の文を実行します。

```
GRANT ROLE Role1 TO User1 WITH ADMIN OPTION
```

User1 は Role1 のメンバーになります。

Role1 のメンバーとして、User1 は Priv1 および (間接的に) Role3 からすべてのシステム権限とロールを継承します。

User1 は Role1 を管理することもできます。

次の文を実行します。

```
GRANT ROLE Role2 TO Role1 WITH ADMIN OPTION
```

Role1 は Role2 のメンバーになります。

Role1 のメンバーとして、User2、User3、および User1 は (上記の付与により) Role2 から、Priv2 および (間接的に) Role4 のすべてのシステム権限とロールを継承します。

Role2 のメンバーである User3 は Role1 のメンバーにはならず、Role1 のシステム権限やロールも継承しません。

User1、User2、および User3 は Role2 を管理できます。

参照：

- GRANT ROLE 文 (297 ページ)

ユーザ定義ロールからのメンバーの削除

ロールのメンバーであるユーザまたはロールを削除します。そのユーザまたはロールは、ロールの基礎となるシステム権限またはロールを使用する権限と、そのロールを管理する権限 (付与されている場合) を失います。

前提条件

管理するロールに対する管理権限。

手順

常に、ログインパスワードが設定されているロール管理者またはグローバルロール管理者がロールごとに最小数 (**MIN_ROLE_ADMINS** データベースオプションで定義) 存在する必要があります。 メンバーがロールの管理者であり、そのメンバーの削除により最小数の要件を下回ることになる場合、削除は失敗します。
ユーザ定義ロールのメンバーシップを被付与者から削除するには、以下の文のいずれかを実行します。

取り消しタイプ	文
ロールメンバーシップおよびロールにロールに対する全管理権限	**REVOKE ROLE** *role_name* **FROM** *grantee [,...]*

取り消しタイプ	文
ロールに対する管理権限のみ 管理権限のみ	**REVOKE ADMIN OPTION FOR ROLE** *role_name* **FROM** *grantee [,...]*

参照：

- REVOKE ROLE 文 (316 ページ)

ユーザ定義ロールの削除

ユーザ定義ロールをデータベースから削除します。これは、すべての依存ロールが、有効なパスワードを持つ管理者ユーザの最小数を下回ることのない場合のみ可能です。最少値が保持されない場合、このコマンドは失敗します。

前提条件

- 削除するロールに対する管理権限。
- 削除するロールがユーザ定義ロールである場合、そのロールがオブジェクトを所有していない。

手順

ユーザ拡張ロールをユーザに戻すと、所有されているオブジェクトは削除されません。変換されたユーザが引き続きオブジェクトを所有します。

削除するロールのタイプと、ユーザに付与されているかどうかによって、DROP 文で必要になる句が異なります。

- **FROM USER** – ユーザ拡張ロールを削除する場合に必要です。
- **WITH REVOKE** – 複数のユーザとロールに付与されているロールを削除する場合に必要です。

ユーザ定義ロールを削除するには、以下の文のいずれかを実行します。

削除条件	文
ユーザ定義ロールが メンバーに付与されていない。	**DROP ROLE** *role_name*
ユーザ拡張ロールが メンバーに付与されている。	**DROP ROLE** *role_name* **WITH REVOKE**

削除条件	文
ユーザ拡張ロールが メンバーに付与されていない*。	**DROP ROLE FROM USER** *role_name*
ユーザ拡張ロールが メンバーに付与されている*。	**DROP ROLE FROM USER** *role_name* **WITH REVOKE**

*ユーザ拡張ロールは通常のユーザになります。

参照：
- DROP ROLE 文 (286 ページ)

ロール管理者とグローバルロール管理者

*ロール管理者*と*グローバルロール管理者*は、ユーザおよび他のロールに対してユーザ定義ロールを付与したり取り消したりします。必要に応じて、ロール管理者とグローバルロール管理者を追加したり削除したりできます。

1 つのロールに追加できるロール管理者の数に制限はありません。ただし、**MIN_ROLE_ADMINS** データベースオプションで最少数を指定することはできます。この最少数要件は、ロールからロール管理者またはグローバルロール管理者を取り消す場合に検証されます。ロール管理者の最少数は 1 (デフォルト) ～ 10 の間の任意の値に設定できます。

ロール管理者は、ユーザ、ユーザ拡張ロール、またはユーザ定義ロールのいずれでもかまいません。

グローバルロール管理者には、MANAGE ROLES システム権限が付与されているユーザが含まれます。グローバルロール管理者は、SYS_MANAGE_ROLES_ROLE システム権限が管理権限付きで付与されているロールを管理できます。

ロール管理者とグローバルロール管理者はいずれも、ロールの付与、取り消し、削除を行うことができ、また、ロール管理者とグローバルロール管理者をロールに追加したり、ロールから削除することもできます。ロール管理者はユーザまたはロールにでき、ロールを管理するために MANAGE ROLES システム権限は必要ありません。

ロールの作成時、またはロールの作成後にロール管理者を割り当て、そのロールのメンバーとするかどうかを指定できます。管理者を指定しない場合、デフォルトでグローバルロール管理者がそのロールの管理者になります。

ロールの作成時に 1 人以上のロール管理者が指定された場合、グローバルロール管理者はロールを管理できません。これは、SYS_MANAGE_ROLES_ROLE システム権限がそのロールに管理権限付きで自動的に付与されることがないためです。このため、ロールの作成時にロール管理者を定義しないか (作成後に追加)、また

は作成プロセス中にロール管理者のみを指定して SYS_MANAGE_ROLES_ROLE システム権限を管理権限付きで明示的に付与することを強くおすすめします。

ロールの作成時にロール管理者を指定しない場合、グローバルロール管理者 (SYS_MANAGE_ROLES_ROLE システム権限) が管理権限のみでロールに自動的に付与されます。

ロール管理者の指定なしで作成されたロールにロール管理者を後から追加すると、その追加方法に応じて、グローバルロール管理者 (SYS_MANAGE_ROLES_ROLE システム権限) が削除されたりされなかったりします。**GRANT** 文を使用した場合、SYS_MANAGE_ROLES_ROLE システム権限はロールに付与されたままになります。しかし、**CREATE OR REPLACE** 文を使用した場合は、新しいロール管理者リストに明示的に含まれていなければ SYS_MANAGE_ROLES_ROLE システム権限が削除されます。

注意： SYS_MANAGE_ROLES_ROLE システム権限をロールから削除することで、定義されているロール管理者の最小数を下回る場合は、このシステム権限を削除することはできません。

デフォルトでは、SYS_MANAGE_ROLES_ROLE システム権限は互換ロール (SYS_AUTH_*_ROLE) に付与されません。したがって、グローバルロール管理者が互換ロールを管理できるようにするには、そのロールに管理権限のみで SYS_MANAGE_ROLES_ROLE を明示的に付与する必要があります。

ロール作成時のロール管理者の追加
新しいロールを作成するときに、ロール管理者を指定します。

前提条件
MANAGE ROLES システム権限。

手順
ロールの作成時に 1 人以上のロール管理者を指定した場合、グローバルロール管理者は、明示的に指定されている場合を除いて、そのロールを管理できません。

このため、ロール管理者のリストにグローバルロール管理者を常に追加することを検討するように強くおすすめします。
作成プロセス中にロール管理者を追加するには、次のいずれかの文を実行します。

作成タイプ	文
管理権限のみ付与する。 **ロールメンバーシップは付与しない。**	**CREATE ROLE** *role_name* **WITH ADMIN ONLY** *admin_name [,...]*

作成タイプ	文
ロール管理者とグローバルロール管理者に管理権限のみ付与する。 **ロールメンバーシップは付与しない。***	**CREATE ROLE** *role_name* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE,** *admin_name [,...]*
管理権限をロールメンバーシップとともに付与する。	**CREATE ROLE** *role_name* **WITH ADMIN** *admin_name [,...]*

*グローバルロール管理者にはロールのメンバーシップを付与できないので、ロール管理者にロールのメンバーシップを付与して (WITH ADMIN オプション) ロールを作成する場合は、SYS_MANAGE_ROLES_ROLE を管理者リストに含めることはできません。

例:

Joe と Bob を Sales ロールのロール管理者にするには、次の文を実行します。

```
CREATE ROLE Sales WITH ADMIN Joe, Bob
```

WITH ADMIN 句を使用しているので、Joe と Bob は、ロールの付与と取り消し、およびこのロールの基礎となるシステム権限の使用の両方を実行できます。
WITH ADMIN ONLY 句を使用した場合は、Joe と Bob はいずれも、ロールの付与と取り消しのみを実行できます。

Joe と Bob を Sales ロールのロール管理者にして、さらにグローバルロール管理者がこのロールを管理できるようにするには、次の文を実行します。

```
CREATE ROLE Sales WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE, Joe, Bob
```

参照：

- CREATE ROLE 文 (279 ページ)

ロール作成時のグローバルロール管理者の追加
グローバルロール管理者が新しいロールを管理できるようにします。

前提条件
MANAGE ROLES システム権限。

手順
ロールの作成時に 1 人以上のロール管理者を指定した場合、グローバルロール管理者は、明示的に指定されている場合を除いて、そのロールを管理できません。

このため、ロール管理者のリストにグローバルロール管理者を常に追加することを検討するように強くおすすめします。
作成プロセス中にグローバルロール管理者を追加するには、次のいずれかの文を実行します。

作成タイプ	文
グローバルロール管理者のみ **ロール管理者なし**	**CREATE ROLE** *role_name*
ロール管理者とグローバルロール管理者の両方*	**CREATE ROLE** *role_name* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE**, *admin_name [,...]*

*グローバルロール管理者は、ロールに対する管理権限のみ (WITH ADMIN ONLY) を持つことができます。したがって、ロール作成時にロール管理者とグローバルロール管理者の両方を指定する場合は、WITH ADMIN ONLY 句のみが有効です。

例:

`Sales` ロールを作成して、グローバルロール管理者のみがそのロールを管理できるようにするには、次の文を実行します。

```
CREATE ROLE Sales
```

`Joe` と `Bob` を `Sales` ロールのロール管理者にして、管理権限のみを付与し、さらにグローバルロール管理者がこのロールを管理できるようにするには、次の文を実行します。

```
CREATE ROLE Sales WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE, Joe, Bob
```

ロール管理者の既存ロールへの追加
ロール管理者を既存ロールに追加します。1 つのロールに追加できるロール管理者の数に制限はありません。

前提条件
ロールに対する管理権限、また、ロールにグローバルロール管理者が存在する場合は MANAGE ROLES システム権限。

手順
ロール管理者を追加するには、次のどちらかの文を実行します。

付与タイプ	文
管理権限のみ付与する。	**GRANT ROLE** *role_name* **TO** *admin_name [,...]* **WITH ADMIN ONLY OPTION**
管理権限とロール メンバーシップを付与する。	**GRANT ROLE** *role_name* **TO** *admin_name [,...]* **WITH ADMIN OPTION**

例:

Mary と Bob を Sales ロールのロール管理者にするには、次の文を実行します。

```
GRANT ROLE Sales TO Mary, Bob WITH ADMIN ONLY OPTION
```

それぞれがロールを管理できますが、WITH ADMIN ONLY OPTION 句を使用しているので、そのロールの基礎となるシステム権限を使用することはできません。

Sarah を、Sales ロールを管理し、WITH ADMIN OPTION 句を使用してその基礎となるシステム権限を使用できるロール管理者にするには、次の文を実行します。

```
GRANT ROLE Sales TO Sarah WITH ADMIN OPTION
```

参照：

- GRANT ROLE 文 (297 ページ)

グローバルロール管理者の既存ロールへの追加
グローバルロール管理者を既存ロールに追加します。

前提条件
ロールに対する管理権限。

手順
グローバルロール管理者には、管理権限のみでロールを付与できます (WITH ADMIN ONLY オプション)。
グローバルロール管理者をロールに再追加するには、次の文を実行します。

```
GRANT ROLE role_name TO SYS_MANAGE_ROLES_ROLE
WITH ADMIN ONLY OPTION
```

参照：

- GRANT ROLE 文 (297 ページ)

ユーザまたはロールをグローバルロール管理者にする
ユーザまたはロールがグローバルロール管理者として操作できるようにします。

前提条件
管理権限付きで付与された MANAGE ROLES システム権限が必要です。

手順
グローバルロール管理者になるには、MANAGE ROLES システム権限が付与されている必要があります。グローバルロール管理者として操作する際は、MANAGE ROLES システム権限に対する管理権限は必要ありません。ロールに MANAGE ROLES システム権限が付与されている場合は、そのロールのすべてのメンバーがこのシステム権限と、グローバルロール管理者として操作する機能を継承します。MANAGE ROLES システム権限を付与するには、次の文を実行します。

```
GRANT MANAGE ROLES TO grantee [,...]
```

参照：
- GRANT システム権限文 (304 ページ)

ロールの既存のロール管理者の置換
現在のロール管理者を新しい管理者に置き換えます。

前提条件
ロールに対する管理権限、また、ロールにグローバルロール管理者が存在する場合は MANAGE ROLES システム権限。

手順
ロール管理者の置換には、管理者の役割を果たすユーザとロールの変更、およびロールに対するその管理権限レベルの変更が伴います。置換の範囲に応じて、2 つの方法があります。方法ごとに、ロール管理者およびグローバル管理者に対する実質的な影響が異なります。1 つ目の方法は、既存ロールの管理者を選択的に置換できます。2 つ目の方法は、既存のすべてのロール管理者を完全に置換できます。2 つ目の方法を採用する場合は、グローバルロール管理者の置換も含まれます。

1 つ目の方法は、2 つの手順によるプロセスです。新しいロール管理者を追加した後、既存の管理者をロールから削除します。常に最小数の管理者の要件を満たす必要があります。そのため、新しい管理者を追加してから既存の管理者を削除することをおすすめします。ロールにグローバルロール管理者が存在する場合、明示的に削除される場合を除いて、グローバルロール管理者は維持されます。

2 つ目の方法は 1 つの手順によるプロセスですが、より広い範囲に影響を及ぼします。ロール管理者の新しいリストを定義します。現在のロール管理者はすべて新

しいロール管理者で上書きされます。現在のロール管理者を引き続きロール管理者として使用する場合は、そのロール管理者を置換するロール管理者のリストに追加する必要があります。リストは次のように既存のすべての管理者を置換します。

- WITH ADMIN OPTION を付与された既存のロール管理者で、新しいロール管理者リストに指定されていない管理者はすべて、管理権限を持たないロールのメンバーになります。
- WITH ADMIN ONLY OPTION を付与された既存のロール管理者で、新しいロール管理者リストに指定されていない管理者はすべて、ロールのメンバーから削除されます。
- 新しいロール管理者リストで指定されている既存のロール管理者は、元の管理権限が置換権限より上位である場合は、元の管理権限を維持します。たとえば、新しいロール管理者には WITH ADMIN ONLY 権限が付与されます。`User1` は、元々 WITH ADMIN 権限を持つロールが付与されており、新しいリストで指定されているので、より上位である WITH ADMIN 権限を維持します。
- ロールにグローバルロール管理者が存在する場合、新しいロール管理者リストで明示的に指定しないかぎり、グローバルロール管理者はロールから削除されます。
- 新しいロール管理者に WITH ADMIN 権限を付与する場合、既存のグローバルロール管理者をリストに指定することはできません。既存のグローバルロール管理者には WITH ADMIN 権限を付与できないためです。既存のグローバルロール管理者はロールから削除されます。

置換管理オプションが現在のレベル以上であれば、ロール置換コマンドを発行できます。管理レベルを下げるには、まずすべてのロール管理者をロールから削除した (取り消した) 後で、もう一度ロールを付与します。

常に、ログインパスワードが設定されているロール管理者またはグローバルロール管理者がロールごとに最小数 (**MIN_ROLE_ADMINS** データベースオプションで定義) 存在する必要があります。ロール管理者の置換時に、置換管理者の数が最小数要件を満たさない場合は、置換が失敗します。

ロール管理者を置換するには、次のいずれかの文を実行します。

置換オプション	文
選択したロール管理者を置換し、管理権限のみ付与する。ロールメンバーシップは付与しない。	• **GRANT ROLE** *role_name* **TO** *admin_name [,...]* **WITH ADMIN ONLY OPTION** • **REVOKE ADMIN OPTION FOR ROLE** *role_name* **FROM** *admin_name [,...]*

置換オプション	文
選択したロール管理者を置換し、 管理権限とロールのメンバーシップを付与する。	• **GRANT ROLE** *role_name* **TO** *admin_name [,...]* **WITH ADMIN OPTION** • **REVOKE ADMIN OPTION FOR ROLE** *role_name* **FROM** *admin_name [,...]*
すべてのロール管理者を置換し、 管理権限のみ付与する。ロールメンバーシップは付与しない。 グローバルロール管理者が存在する場合は削除する。	**CREATE OR REPLACE ROLE** *role_name* **WITH ADMIN ONLY** *admin_name [,...]*
すべてのロール管理者を置換し、 管理権限とロールメンバーシップを付与する。 グローバルロール管理者が存在する場合は削除する。	**CREATE OR REPLACE ROLE** *role_name* **WITH ADMIN** *admin_name [,...]*
すべてのロール管理者を置換し、 管理権限のみ付与する。 新しいロール管理者にはグローバルロール管理者も含める。*	**CREATE OR REPLACE ROLE** *role_name* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE,** *admin_name [,...]*
すべてのロール管理者を置換し、 完全な管理権限を付与する。 ロールにグローバルロール管理者をリストアする。*	• **CREATE OR REPLACE ROLE** *role_name* **WITH ADMIN** *admin_name [,...]* • **GRANT ROLE** *role_name* **TO SYS_MANAGE_ROLES_ROLE WITH ADMIN ONLY OPTION**

*SYS_MANAGE_ROLES_ROLE は、WITH ADMIN ONLY オプションを使用してのみ、ロールに付与できます。したがって、CREATE OR REPLACE 文で WITH ADMIN ONLY オプションを指定する場合は、SYS_MANAGE_ROLES_ROLE を管理者リストで指定できます。CREATE OR REPLACE 文で WITH ADMIN オプションを指定する場合は、別途 GRANT 文で WITH ADMIN ONLY オプションを指定して、ロールに SYS_MANAGE_ROLES_ROLE を付与する必要があります。

例:

Mary と Bob は、Sales ロールの完全な管理権限を持つロール管理者です。Sales にはグローバルロール管理者が存在します。

ロール管理者の Bob を削除して、Sarah と Jeff で置換し、同じ管理権限を付与するには、次の一連の文を実行します。Bob は Sales のメンバーとして残りますが、管理権限は付与されていません。

```
GRANT ROLE sales TO Sarah, Jeff WITH ADMIN OPTION
REVOKE ADMIN OPTION FOR ROLE Sales FROM Bob
```

既存のロール管理者 (Mary と Bob) を Sarah と Jeff, に置換して完全な管理権限を付与するには、次の一連の文を実行します。グローバルロール管理者はリストで指定できない (完全な管理権限を付与できない) ので、ロール管理者を置換した後で明示的にロールに付与する必要があります。

```
CREATE OR REPLACE ROLE Sales WITH ADMIN Sarah, Jeff
GRANT ROLE sales TO SYS_MANAGE_ROLES_ROLE WITH ADMIN ONLY OPTION
```

既存のロール管理者 (Mary と Bob) を Bob と Sarah に置換して管理権限のみ付与するには、次の一連の文を実行します。グローバルロール管理者を維持するには、リストで指定する必要があります。Bob はロール管理者として残り、置換前の管理権限は新しいロール管理者のそれよりも上位なので、置換前の管理権限が維持されます。

```
CREATE OR REPLACE ROLE Sales WITH ADMIN ONLY Bob, Sarah,
SYS_MANAGE_ROLES_ROLE
```

参照：

- GRANT ROLE 文 (297 ページ)
- REVOKE ROLE 文 (316 ページ)
- CREATE ROLE 文 (279 ページ)

ロールからのロール管理者の削除

ロールからロール管理者を削除します。

前提条件

ロールに対する管理権限。

手順

常に、ログインパスワードが設定されているロール管理者またはグローバルロール管理者がロールごとに最小数 (**MIN_ROLE_ADMINS** データベースオプションで定義) 存在する必要があります。ロール管理者の削除後もこの最小数が満たされる場合に限り、ロール管理者を削除できます。

ロール管理者を削除する場合、そのユーザへのロール管理の付与が WITH ADMIN OPTION 句で行われていた場合は、ロール管理の取り消しによって、ロールを管

理する機能 (付与、取り消し、削除) のみが削除され、ロールの基礎となるシステム権限を使用する機能 (メンバーシップ) は削除されません。しかし、そのユーザへのロール管理の付与が WITH ADMIN ONLY OPTION 句で行われていた場合は、ロールにメンバーシップが関連付けられていないので、ロール管理の取り消しによって、ロール全体の取り消しと同じ効果が得られます。

ロールからロール管理者を削除するには、次のいずれかの文を実行します。

削除タイプ	文
ロール管理者は削除するが、ロールのメンバーシップは維持する。	**REVOKE ADMIN OPTION FOR ROLE** *role_name* **FROM** *admin_name [,...]*
ロール管理者をロールのメンバーシップとともに削除する。	**REVOKE ROLE** *role_name* **FROM** *admin_name [,...]*

例:

この例は、Mary と Sarah の両方が現在 Sales ロールのロール管理者であることを前提としています。Mary はロールのメンバーシップとロールの管理機能の両方を付与されています。一方、Sarah はロールの管理機能のみ付与され、メンバーシップは付与されていません。付与されている管理レベルが異なるので、Sales ロールから管理権限を取り消すために次の文を実行した場合、各管理者に対する影響は異なります。

```
REVOKE ADMIN OPTION FOR ROLE Sales FROM Mary, Sarah
```

Mary's が持つ Sales ロールの管理機能は失われますが、ロールのメンバーシップは維持されます。Sarah からは Sales ロールが完全に削除されます。

参照：

- REVOKE ROLE 文 (316 ページ)

ロールからのグローバルロール管理者の削除
ロールからグローバルロール管理者を削除します。

前提条件
ロールに対する管理権限。

手順
常に、ログインパスワードが設定されているロール管理者またはグローバルロール管理者がロールごとに最小数 (**MIN_ROLE_ADMINS** データベースオプションで定

義) 存在する必要があります。ロールのこの最小数が満たされている限り、ロールからグローバルロール管理者を削除できます。
ロールからグローバルロール管理者を削除するには、次の文を実行します。

```
REVOKE ROLE role_name
FROM SYS_MANAGE_ROLES_ROLE
```

参照：

- REVOKE ROLE 文 (316 ページ)

ロール管理者の最小数

MIN_ROLE_ADMINS データベースオプションは、残りのユーザとロールを管理するために必要なシステム権限を持つユーザとロールがいなくなるという状況が発生しないことを保証する設定値です。

この値は、ロールの総数に対してではなく、各ロールに対するロール管理者の最小数に適用され、次のときに考慮されます。

- ロールの作成または取り消し
- ユーザまたはロールの削除
- ユーザのパスワードの null への変更

注意： パスワードのないユーザまたはロールは管理者になれません。

この値を変更しようとすると、既存ロールのそれぞれに、引き続き、少なくとも新しい値で定義される数のロール管理者が存在することがシステムにより検証されます。1 つでもこの要件を満たさないロールが存在すると、この文は失敗します。同様に、ユーザを削除する場合、残りの管理者数が指定の最小値を下回れば、この文は失敗します。

注意： ロックされたアカウントは、ロールの管理者数のカウント時に考慮されません。

例 1

MIN_ROLE_ADMINS の値が 2 の場合

`Role1` には 2 人の管理者、`Role2` には 3 人の管理者がいます。

値を 1 に減らした場合、両方のロールが新しい指定ロール管理者最小数を確保していることになるため、コマンドは成功します。ただし、値を 3 に増やすと、`Role1` には、新しい最小値を満たす管理者がいないため、コマンドは失敗します。

例 2

MIN_ROLE_ADMINS の値が 4 の場合

`Role1` には 6 人の管理者、`Role2` には 4 人の管理者がいます。

Role1 からユーザを削除した場合、Role1 には最小値を満たす管理者がいるのでコマンドは成功します。ただし、Role2 からユーザを削除すると、Role2 に最小値を満たす管理者がいなくなるのでコマンドは失敗します。

参照：
- ユーザアカウントの自動ロック解除 (124 ページ)
- MIN_ROLE_ADMINS オプション (335 ページ)

ロール管理者の最小数の設定
各ロールの管理に必要なロール管理者の最小数を設定します。

前提条件
SET ANY SECURITY OPTION システム権限。

手順

ロール管理者の最小数は、1 (デフォルト) ～ 10 の範囲の任意の整数に設定できる、設定可能なデータベースオプションです。いずれかの単一ロールのロール管理者の数が最小数を満たさなくなる状況が発生するような値に最小数を変更することはできません。また、このオプションを一時的に設定することもできません。

この値は、すべてのロール全体に対してではなく、各ロールに対して適用されます。たとえば、20 個のロールが存在し、ロール管理者の最小数が 2 に設定されている場合、20 個のロール全部を管理する 2 人のロール管理者を定義する必要があるのではなく、20 個のロールのそれぞれに少なくとも 2 人ずつロール管理者を定義する必要があります。

ロール管理者の最小数を変更するには、次の文を実行します。

```
SET OPTION Public.min_role_admins = value
```

参照：
- ユーザアカウントの自動ロック解除 (124 ページ)
- MIN_ROLE_ADMINS オプション (335 ページ)

ロールを管理できない DBA ユーザ
特定の状況においては、DBA ユーザがロールを管理 (付与、取り消し、または削除) できないことがあります。

具体的には、次の場合に発生します。

- ロールのグローバルロール管理者が取り消されている。
- DBA ユーザがそのロールのロール管理者として定義されていない。

この問題を解決するには、グローバルロール管理者をそのロールに付与する (推奨) か、DBA ユーザをそのロールのロール管理者として追加します。

参照：

- GRANT ROLE 文 (297 ページ)
- ロール管理者の既存ロールへの追加 (14 ページ)
- グローバルロール管理者の既存ロールへの追加 (15 ページ)

システムロール

システムロールは、新しい各データベースに自動的に作成される組み込みのロールです。

システムロールの特徴は次のとおりです。

- 削除できません。
- その基礎となるデフォルトのシステム権限を変更することまたは取り消すことはできません。
- 他のロールやシステム権限を付与したり、取り消したりできます。
- 管理権限付き (WITH ADMIN OPTION 句または WITH ADMIN ONLY OPTION 句) で付与することはできません。
- パスワードが割り当てられていないので、付与可能なシステムロールとしてデータベースに接続することはできません。
- SYS、dbo、および rs_systabgroup ロールを除き、オブジェクトを所有しません。

dbo システムロールの付与

dbo システムロールは、多数のシステムストアドプロシージャとビューを所有しています。

前提条件

MANAGE ROLES システム権限。

手順

dbo システムロールは、デフォルトでは、SYS システムロールおよび SYS_AUTH_RESOURCE_ROLE 互換ロールの管理権限のないメンバーです。また、SYS_AUTH_DBA_ROLE 互換ロールの完全な管理権限付きのメンバーです。

dbo システムロールは、管理権限なしでのみ (WITH NO ADMIN OPTION 句で) 他のロールに付与することができます。WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は、dbo システムロールに対しては無効です。

dbo システムロールに対して、デフォルトのロールを含むシステム権限やロールを付与したり、取り消したりすることができます。
dbo システムロールを付与するには、次の文を実行します。

```
GRANT ROLE dbo TO grantee [,...]
```

参照：
- GRANT ROLE 文 (297 ページ)

diagnostics システムロールの付与

diagnostics システムロールのメンバーは、診断テーブルとビューに対する SELECT、INSERT、UPDATE、DELETE、および ALTER の各権限を継承します。

前提条件
MANAGE ROLES システム権限。

手順

diagnostics システムロールは、管理権限なしでのみ (WITH NO ADMIN OPTION 句で) 他のロールに付与することができます。WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は、diagnostics システムロールに対しては無効です。

diagnostics システムロールに対してシステム権限とロールを付与したり、取り消したりできます。
diagnostics システムロールを付与するには、次の文を実行します。

```
GRANT ROLE diagnostics TO grantee [,...]
```

参照：
- GRANT ROLE 文 (297 ページ)

PUBLIC システムロールの付与

PUBLIC システムロールは、一連のシステムテーブルに対する SELECT 権限とシステムプロシージャに対する EXECUTE 権限を持ちます。

前提条件
MANAGE ROLES システム権限。

手順

PUBLIC システムロールは、デフォルトでは、dbo システムロールと SYS システムロールの管理権限がないメンバーです。SYS ロールのメンバーとして一部のシステムテーブルとシステムビューに対する読み込みアクセスを持っているため、データベースのすべてのユーザがデータベーススキーマに関する情報を取得でき

ます。このアクセスを制限するには、SYS システムロールで PUBLIC のメンバーシップを取り消します。

新しいユーザ ID はすべて、自動的に PUBLIC システムロールのメンバーになり、このロールに特に付与されているすべての権限を継承します。PUBLIC システムロールからユーザを削除することはできますが、それによってユーザがシステムストアドプロシージャを実行できなくなる可能性があるため、この操作は実行しないことをおすすめします。

PUBLIC システムロールは、管理権限なしでのみ (WITH NO ADMIN OPTION 句で) 他のロールに付与することができます。WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は、PUBLIC システムロールに対しては無効です。

PUBLIC システムロールに対して、デフォルトのロールを含むシステム権限やロールを付与したり、取り消したりすることができます。

PUBLIC システムロールを付与するには、次の文を実行します。

```
GRANT ROLE PUBLIC TO grantee [,...]
```

参照：

- GRANT ROLE 文 (297 ページ)

rs_systabgroup システムロールの付与

rs_systabgroup システムロールは、Replication Server に必要なテーブルとシステムプロシージャを所有し、Replication Server 機能を実行するための基礎となるシステム権限をユーザに付与します。

前提条件

MANAGE ROLES システム権限。

手順

rs_systabgroup システムロールは、管理権限なしでのみ (WITH NO ADMIN OPTION 句で) 他のロールに付与することができます。WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は、rs_systabgroup システムロールに対しては無効です。

rs_systabgroup システムロールに対してシステム権限やロールを付与したり、取り消したりできます。

rs_systabgroup システムロールを付与するには、次の文を実行します。

```
GRANT ROLE rs_systabgroup TO grantee [,...]
```

参照：

- GRANT ROLE 文 (297 ページ)

SYS システムロールの付与

SYS システムロールは、データベースのシステムテーブルとシステムビューを所有します。これらのテーブルとビューには、全データベースオブジェクトと全ユーザ ID を含む、完全なデータベーススキーマの記述が含まれます。

前提条件

MANAGE ROLES システム権限。

手順

SYS システムロールには、デフォルトで、管理権限なしの dbo システムロールと PUBLIC システムロールが付与されています。しかし、dbo システムロールと PUBLIC システムロールのメンバーは、SYS システムロールに直接または間接的に付与されたシステム権限を継承しません。

SYS システムロールは、管理権限なしでのみ (WITH NO ADMIN OPTION 句で) 他のロールに付与することができます。WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は、SYS システムロールに対しては無効です。

SYS システムロールに他のシステム権限を付与したり、それらを SYS システムロールから取り消したりはできません。

SYS システムロールを付与するには、次の文を実行します。

```
GRANT ROLE SYS TO grantee [,...]
```

参照：

- GRANT ROLE 文 (297 ページ)

SYS_REPLICATION_ADMIN_ROLE の付与

SYS_RUN_REPLICATION_ADMIN_ROLE システムロールは、レプリケーションロールの付与、パブリケーション／サブスクリプション／ユーザとプロファイルの同期の管理、メッセージタイプの管理、レプリケーション関連のオプションの設定など、レプリケーションに関連する管理タスクの実行に必要です。

前提条件

MANAGE ROLES システム権限。

手順

SYS_REPLICATION_ADMIN_ROLE システムロールには、デフォルトで、管理権限なしで次のシステム権限が付与されています。

- CREATE ANY PROCEDURE

- CREATE ANY TABLE
- DROP ANY TABLE
- DROP ANY PROCEDURE
- MANAGE ANY OBJECT PRIVILEGE
- MANAGE ANY USER
- MANAGE ANY WEB SERVICE
- MANAGE REPLICATION
- MANAGE ROLES
- SERVER OPERATOR
- SELECT ANY TABLE
- SET ANY SYSTEM OPTION
- SET ANY PUBLIC OPTION
- SET ANY USER DEFINED OPTION

このデフォルトのシステム権限のセットを SYS_RUN_REPLICATION_ADMIN_ROLE システムロールから取り消すことはできませんが、SYS_RUN_REPLICATION_ADMIN_ROLE システムロールに対して追加のシステム権限やロールを付与したり取り消したりはできます。

SYS_RUN_REPLICATION_ADMIN_ROLE システムロールは、管理権限なしでのみ (WITH NO ADMIN OPTION 句で) 他のロールに付与することができます。WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は、SYS_RUN_REPLICATION_ADMIN_ROLE システムロールに対しては無効です。

SYS_REPLICATION_ADMIN_ROLE システムロールを付与するには、次の文を実行します。

```
GRANT ROLE SYS_REPLICATION_ADMIN_ROLE TO grantee [,...]
```

参照：

- GRANT ROLE 文 (297 ページ)

SYS_RUN_REPLICATION_ROLE の付与

SYS_RUN_REPLICATION_ROLE システムロールは、**dbremote** を使用したレプリケーションタスクや **dbmlsync** を使用した同期タスクの実行に必要です。SYS_RUN_REPLICATION_ROLE システムロールは、これらのユーティリティを介して接続するユーザに対してのみ有効です。

前提条件

MANAGE REPLICATION システム権限が必要です。

手順

SYS_RUN_REPLICATION_ROLE システムロールは、完全な管理権限付きの SYS_AUTH_DBA_ROLE 互換ロールのメンバーです。

次のシステム権限も、管理権限なしで付与されます。

- SELECT ANY TABLE
- SET ANY USER DEFINED OPTION
- SET ANY SYSTEM OPTION
- BACKUP DATABASE
- MONITOR

このデフォルトのシステム権限のセットを SYS_RUN_REPLICATION_ROLE システムロールから取り消すことはできませんが、SYS_RUN_REPLICATION_ROLE システムロールに追加のシステム権限やロールを付与したり取り消したりはできます。

デフォルトでは、SYS_AUTH_DBA_ROLE 互換ロールが SYS_RUN_REPLICATION_ROLE システムロールに付与され、上記の明示的に付与されるシステム権限以外の、承認済みタスク関連の他のレプリケーションを実行するための追加システム権限要件が解決されます。しかし、SYS_RUN_REPLICATION_ROLE システムロールの SYS_AUTH_DBA_ROLE 互換ロールを取り消し、他のレプリケーションタスクに必要な特定の追加システム権限またはロールを、SYS_RUN_REPLICATION_ROLE システムロールに明示的に付与することをおすすめします。

SYS_RUN_REPLICATION_ROLE システムロールは、管理権限なしでのみ (WITH NO ADMIN OPTION 句で) 他のロールに付与することができます。WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は、SYS_RUN_REPLICATION_ROLE システムロールに対しては無効です。

デフォルトでは、SYS_RUN_REPLICATION_ROLE を付与すると、基礎となるシステム権限が付与先グループのメンバーに継承されます。この継承を回避するには、このシステムロールに対してのみ WITH NO SYSTEM PRIVILEGE INHERITANCE 句を含めます。

MIN_ROLE_ADMINS データベースオプションにより、データベース内に、他のユーザに MANAGE REPLICATION システム権限を付与したり、これを取り消すことができるユーザが常に指定数は存在しているようにします。

SYS_RUN_REPLICATION_ROLE システムロールを付与するには、以下の文のいずれかを実行します。

継承タイプ	文
継承付き	**GRANT ROLE SYS_RUN_REPLICATION_ROLE TO** *grantee [,...]*
継承なし	**GRANT ROLE SYS_RUN_REPLICATION_ROLE TO** *grantee [,...]* **WITH NO SYSTEM PRIVILEGE INHERITANCE**

参照：
- GRANT ROLE 文 (297 ページ)

SYS_SPATIAL_ADMIN_ROLE システムロールの付与

SYS_SPATIAL_ADMIN_ROLE システムロールは、空間参照系と空間測定単位を作成、変更、削除、またはコメントする機能をユーザに付与します。
SYS_SPATIAL_ADMIN_ROLE は、すべての空間オブジェクトの所有者です。

前提条件
MANAGE ROLES システム権限。

手順

SYS_SPATIAL_ADMIN_ROLE システムロールには、デフォルトで、管理権限なしの MANAGE ANY SPATIAL OBJECT システム権限が付与されています。

SYS_SPATIAL_ADMIN_ROLE システムロールは、管理権限なしでのみ (WITH NO ADMIN OPTION 句で) 他のロールに付与することができます。WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は、SYS_SPATIAL_ADMIN_ROLE システムロールに対しては無効です。

SYS_SPATIAL_ADMIN_ROLE システムロールに対して、デフォルトの権限を含むシステム権限やロールを付与したり、取り消したりすることができます。

SYS_SPATIAL_ADMIN_ROLE システムロールを付与するには、次の文を実行します。

```
GRANT ROLE SYS_SPATIAL_ADMIN_ROLE TO grantee [,...]
```

参照：
- GRANT ROLE 文 (297 ページ)

システムロールの取り消し

ユーザまたはロールの持つシステムロールを取り消します。

前提条件
取り消すシステムロールに対する管理権限。

手順

システムロールを取り消すには、次の文を実行します。

```
REVOKE ROLE role_name FROM grantee [,...]
```

例:

次の文は、Mary が持つ dbo システムロールを完全に取り消します。

```
REVOKE ROLE dbo FROM Mary
```

参照：

- REVOKE ROLE 文 (316 ページ)

互換ロール

互換ロールは、権限ベースのセキュリティをサポートする 16.0 より前のバージョンの SAP Sybase IQ との下位互換性を保持するために存在します。

互換ロールの付与、取り消し、および特定の条件下での削除を行うことができます。基礎となるシステム権限を変更することはできません。ただし、互換ロールをユーザ定義ロールに移行してから、基礎となるシステム権限を変更することは可能です。互換ロールを移行すると、互換ロールの被付与者のすべてに移行したユーザ定義ロールが自動的に付与されます。

使用しているオペレーティングシステムの『移行 ガイド』で「16.0 より前のリリースからのアップグレードに関する考慮事項」>「15.x からのアップグレード後のロールベースのセキュリティ」を参照してください。

ロールが所有するビュー、プロシージャ、テーブル

ユーザではなく、ユーザ拡張ロールが所有していると、ビュー、プロシージャおよびテーブルの管理が容易になります。

オブジェクト名を修飾する必要をなくすには、テーブル、ビュー、またはストアドプロシージャへのアクセスが必要なユーザを、オブジェクトを所有するロールのメンバーにします。

たとえば、テーブル Employees をロール Personnel が所有し、Jeff はそのロールのメンバーであるとします。Jeff がテーブル Employees を参照する場合に、たとえば次のように SQL 文でテーブルの名前を指定するだけで済みます。

```
SELECT * FROM EMPLOYEES
```

しかし、Personnel のメンバーではない John がテーブル Employees を参照する場合は、次のようにテーブルの修飾名を使用する必要があります。

```
SELECT * FROM PERSONNEL.EMPLOYEES
```

注意： データベースオブジェクトの所有権は個別のユーザ ID に関連付けられるため、所有者がロールである場合、テーブルの所有権はロールのメンバーに継承されません。

システム権限は、オブジェクトを所有するロールに付与しないでください。代わりに、次のように実行します。

- 特定のシステム権限を付与して、別個のロールを作成します。
- 特定のシステム権限のメンバーシップを必要とするユーザに、該当するロールを付与します。
- 個別のロールのそれぞれを、オブジェクトを所有するロールに付与します。

これによって、各ユーザが実行するタスクを完全に制御できます。オブジェクトに関連付けられた該当するロールのメンバーシップを付与および取り消すことで、権限が必要なタスクを管理します。

たとえば、テーブル `Sales` を `Sales1` ロールが所有しているとします。ユーザ `Mary`、`Bob`、`Joe`、`Laurel`、および `Sally` に `Sales1` のメンバーシップが付与されています。`Task1_role` を作成して、特定のタスクの完了に必要なシステム権限を付与します。`Task1_role` を `Mary` と `Bob` に付与します。`Task2_role` を作成して、特定のシステム権限をこれに付与して、`Joe` と `Sally` に付与します。最後に、`Task1_role` と `Task2_role` の両方を `Sales1` に付与します。`Sales1` には両方のロールが付与されますが、`Task1_role` と `Task2_role` の基礎となるシステム権限は `Sales1` の他のメンバーに自動的には継承されません。`Mary` と `Bob` が実行できるタスクは、`Joe` と `Sally` が実行できるタスクとは異なります。`Laurel` には `Task1_role` も `Task2_role` も付与されておらず、`Sales1` にもシステム権限は直接付与されていないため、`Laurel` が `Sales` テーブルで実行可能な承認済みタスクはありません。この設定によって、各ユーザが実行できるタスクを管理および制御できます。

付与されているロールの表示

sp_displayroles ストアドプロシージャは、指定されたシステム権限、システムロール、ユーザ定義ロール、またはユーザ名に付与されたすべてのロールを返すか、またはロールの階層ツリー全体を表示します。

レポートには、ロール名、親ロール名、付与タイプ (管理権限付きまたはなし)、およびロール階層のレベルが出力されます。

自分自身のユーザ ID に対して **sp_displayroles** を実行するために必要なシステム権限はありません。他のユーザに対してこのプロシージャを実行するには、MANAGE ROLES システム権限が必要です。ロールまたはシステム権限に対してプロシージャを実行するには、指定したロールまたはシステム権限に対する管理権限が必要です。

例
次の例では、コマンドを発行したユーザに付与されているすべてのロールが返されます。

```
CALL sp_displayroles();
```

この例では、SYS_SPATIAL_ADMIN_ROLE システムロールに付与されているシステム権限のリストが返されます。

```
CALL sp_displayroles( 'SYS_SPATIAL_ADMIN_ROLE' );
```

role_name	parent_role_name	grant_type	role_level
MANAGE ANY SPATIAL OBJECT	(NULL)	NO ADMIN	1

この例では、SYS_SPATIAL_ADMIN_ROLE に付与されているシステム権限のリストが、ロール階層でその上位にあるすべてのロールも含めて返されます。

```
CALL sp_displayroles( 'SYS_SPATIAL_ADMIN_ROLE', 'expand_up');
```

role_name	parent_role_name	grant_type	role_level
SYS_AUTH_DBA_ROLE	dbo	ADMIN	-3
SYS_AUTH_SSO_ROLE	SYS_AUTH_DBA_ROLE	ADMIN	-3
MANAGE ROLES	SYS_AUTH_REMOTE_DBA_ROLE	ADMIN	-2
MANAGE ROLES	SYS_AUTH_SSO_ROLE	ADMIN	-1
MANAGE ROLES	SYS_REPLICATION_ADMIN_ROLE	NO ADMIN	-1
SYS_SPATIAL_ADMIN_ROLE	MANAGE ROLES	ADMIN	0

参照：
- sp_displayroles システムプロシージャ (355 ページ)

ユーザに付与されているロールと権限の確認

sp_has_role ストアド関数は、指定されたシステム権限またはユーザ定義ロールがプロシージャの呼び出し側に付与されているかどうかを示す整数値を返します。

この関数を実行するために必要なシステム権限は何もありません。ユーザ定義ストアドプロシージャ内でパーミッションチェックに使用された場合、ユーザがパーミッションチェックに失敗すると、この関数はエラーメッセージを表示することがあります。

- **1 –** システム権限またはユーザ定義ロールが呼び出し側ユーザに付与されていることを示します。
- **0 またはパーミッションがありません：この command/procedure を実行するためのパーミッションがありません。 –** システム権限またはユーザ定義ロールが呼び出し側ユーザに付与されていないことを示します。throw_error 引数が 1 に設定されている場合は、値 0 の代わりにエラーメッセージが返されます。
- **-1 –** 指定されたシステム権限またはユーザ定義ロールが存在しないことを示します。throw_error 引数が 1 に設定されている場合でも、エラーメッセージは表示されません。

参照：

- SP_HAS_ROLE 関数 [システム] (359 ページ)

権限

権限は、システムで承認済み操作を実行する権利をユーザに付与します。たとえば、テーブルを変更することは、変更の種類によっては権限付き操作です。

権限には、システム権限とオブジェクトレベル権限の 2 種類があります。

*システム権限*は権限付け操作を実行するための一般的な権利を付与しますが、*オブジェクトレベル権限*は特定オブジェクトでの操作の実行を制限します。たとえば、ALTER ANY TABLE システム権限がある場合は、システムの任意のテーブルを変更できます。ALTER TABLE システム権限がある場合、自分のテーブル、または ALTER オブジェクトレベル権限が付与されているテーブルのみ変更できます。オブジェクトレベル権限は、付与や取り消しは可能ですが、作成や削除はできません。

システム権限はデータベースに組み込まれ、付与や取り消しが可能ですが、作成や削除はできません。MANAGE ROLES 権限と UPGRADE ROLE 権限を除き、システム権限は変更できません。システム権限のそれぞれは、SET USER システム権限を除き、デフォルトで SYS_AUTH_SA_ROLE または SYS_AUTH_SSO_ROLE ロールのいずれかに付与されますが、両方には付与されていません。SET USER システム権限は両方のロールに付与されます。

GRANT 文および **REVOKE** 文を使用して、システム権限とオブジェクトレベル権限を付与および取り消します。

権限とパーミッション

パーミッションと権限は、ロールベースのセキュリティでは同じものを意味しません。承認済みタスクを実行するために権限を付与されているユーザでも、目的

のオブジェクトに対してその承認済みタスクの実行に必要なパーミッションを持っていない場合があります。

権限は、ユーザまたはロールに、特定の承認済みタスクを実行する権利を与えます。一方、パーミッションは、タスクが実行されるコンテキストを指します。

承認済みタスクを実行してエラーが発生した場合、表示されるエラーメッセージは通常、そのユーザにタスクを実行する権限がないということではなく、そのパーミッションがないという内容になります。権限付きタスクまたは操作を実行する前には、システムによってそのユーザに以下の実行に必要な権限があるかどうかの検証が行われます。

- 権限付き操作
- 対象オブジェクトに対する権限付き操作
- ユーザが操作を実行しようという状況における権限付き操作

ユーザにいずれかのレベルで適切な権限がない場合は、そのタスクを実行するパーミッションがないと認識されます。操作は失敗し、エラーメッセージが表示されます。

例

ユーザに、`Myconfig.ini` という名前のテキスト設定オブジェクトに対してのみ ALTER 権限が付与されています。

オブジェクト権限:ユーザが `Myconfig.ini` 以外のテキスト設定オブジェクトを変更しようとしました。ユーザに付与されているのは `Myconfig.ini` `Myconfig.ini` テキスト設定オブジェクトのみの ALTER 権限なので、このタスクは失敗します。

コンテキスト権限:ユーザが `Myconfig.ini` に対する事前フィルタを削除しようとしました。ユーザには `Myconfig.ini` に対する ALTER 権限が付与されていますが、テキスト設定オブジェクトに対する事前フィルタの削除には ALTER ANY TEXT CONFIGURATION システム権限または ALTER ANY OBJECT システム権限が必要であり、この権限はユーザに付与されていません。

システム権限

システム権限を使用すると、承認済みシステム操作へのアクセスを制御できます。サーバ上の権限付きデータベースタスクのそれぞれは、特定のシステム権限を必要とします。システム権限は、ユーザおよびロールに個別に付与できます。

システム権限をロールに付与すると、ロールのすべてのメンバーがシステム権限を継承します。ロールの新しいメンバーはすべて、基礎となるロールのシステム権限すべてを自動的に継承します。

各システム権限は、SET USER システム権限を除き、デフォルトで SYS_AUTH_SA_ROLE または SYS_AUTH_SSO_ROLE のいずれかのロールに付与

されますが、両方には付与されていません。例外として SET USER システム権限は両方のロールに付与されます。

ロールの基礎になるシステム権限を個別に付与することは、セマンティック上、ロールそのものを付与することと同じになります。システム権限は、組織の機能セキュリティ要件に合わせて、任意の組み合わせで、複数のユーザ定義システムロールに付与できます。

MANAGE ROLES 権限と UPGRADE ROLE 権限を除き、システム権限は変更できません。システム権限はロールまたはユーザへの付与またはその取り消しはできますが、削除することはできません。システム権限はオブジェクトを所有できません。

機能分野別のシステム権限
システム権限を機能分野別にまとめたリストです。

データベースのシステム権限
データベース上の承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER DATABASE システム権限
データベースを変更するのに必要です。

ALTER DATABASE システム権限によりユーザは以下のことができるようになります。

- データベースのアップグレード
- コストモデル調整の実行
- 統計情報のロード
- トランザクションログの変更 (SERVER OPERATOR システム権限も必要)
- データベースの所有権の変更 (MANAGE ANY MIRROR SERVER システム権限も必要)

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

BACKUP DATABASE システム権限
1 つ以上のアーカイブデバイスにデータベースをバックアップできます。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CHECKPOINT システム権限
データベースサーバでチェックポイントを強制実行するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP CONNECTION システム権限
任意のユーザのデータベース接続を削除するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

MANAGE PROFILING システム権限
アプリケーションプロファイリング用のサーバトレーシングを有効または無効にするために必要です。ユーザ情報の診断機能を完全利用するには、DIAGNOSTICS システムロールも必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

MONITOR システム権限
権限付き統計へのアクセス、サーバモニタ関連プロシージャの実行などのモニタリング関連タスクを実行するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

データベースオプションのシステム権限
データベースオプション設定の承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

SET ANY PUBLIC OPTION システム権限
SET ANY SECURITY OPTION システム権限または SET ANY SYSTEM OPTION システム権限が必要ない PUBLIC システムデータベースオプションを設定するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

SET ANY SECURITY OPTION システム権限
PUBLIC セキュリティデータベースオプションを設定するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

SET ANY SYSTEM OPTION システム権限
PUBLIC システムデータベースオプションを設定するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

SET ANY USER DEFINED OPTION システム権限
ユーザ定義オプションを設定するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

データ型のシステム権限
データ型に対する承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER DATATYPE システム権限
データ型を変更するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE DATATYPE システム権限
データ型を作成するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)

- すべてのシステム権限のリスト (73 ページ)

DROP DATATYPE システム権限
データ型を削除するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DB 領域のシステム権限
DB 領域上の承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY DBSPACE システム権限
DB 領域上で管理関連タスクを実行するのに必要です。

MANAGE ANY DBSPACE システム権限により、ユーザは以下のことができるようになります。

- 任意の DB 領域の CREATE 文、ALTER 文、DROP 文、または COMMENT 文を発行する
- 任意の DB 領域の CREATE オブジェクトレベル権限を付与または取り消す
- 任意の DB 領域にデータを移動する
- 任意の DB 領域に対する読み取り専用選択的リストア文を発行する
- データベース削除ファイル関数を実行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

デバッグのシステム権限
デバッグに対する承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

DEBUG ANY PROCEDURE システム権限
データベースオブジェクトの全コードをデバッグするのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

イベントのシステム権限
イベントに対する承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY EVENT システム権限
イベントを作成、変更、削除、またはトリガするのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

外部環境のシステム権限
外部環境に対する承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

CREATE EXTERNAL REFERENCE システム権限
データベースで外部参照を作成するのに必要です。

このシステム権限は、外部オブジェクトを参照するデータベースオブジェクトの作成に必要な他のシステム権限と共に必要です。

次に例を示します。

- 外部単語区切りを作成する、または外部単語区切りを使用する自己所有のテキスト設定を作成するには、CREATE TEXT CONFIGURATION システム権限と CREATE EXTERNAL REFERENCE システム権限が必要です。
- 外部プロシージャまたは外部関数を作成するには、CREATE PROCEDURE システム権限と CREATE EXTERNAL REFERENCE システム権限が必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY EXTERNAL ENVIRONMENT システム権限
外部環境を管理するのに必要です。

MANAGE ANY EXTERNAL ENVIRONMENT システム権限により、ユーザは外部環境に対する ALTER 文、COMMENT 文、 START 文、または STOP 文を発行できるようになります。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY EXTERNAL OBJECT システム権限
INSTALL 文、COMMENT ON 文、REMOVE EXTERNAL OBJECT 文の発行に必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

ファイルのシステム権限
ファイルに対する承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

READ CLIENT FILE システム権限
クライアントマシン上のファイルを読み込むのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

READ FILE システム権限
サーバマシン上のファイルを読み込むのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)

- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

WRITE CLIENT FILE システム権限
クライアントマシン上のファイルに書き込むのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

WRITE FILE システム権限
サーバマシン上のファイルに書き込むのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

インデックスのシステム権限
インデックスに対する承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY INDEX システム権限
外部インデックスを変更するのに必要です。

ALTER ANY INDEX システム権限によりユーザは以下のことができるようになります。

- 任意のユーザが所有する任意のテーブルのインデックスを変更する

- 任意のユーザが所有する任意のインデックスに対する COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY INDEX システム権限
新しいインデックスを作成するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

CREATE ANY INDEX システム権限によりユーザは以下のことができるようになります。

- 任意のユーザが所有する任意のテーブルのインデックスを作成する
- 任意のユーザが所有する任意のインデックスに対する COMMENT 文を発行する

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP ANY INDEX システム権限
任意のユーザが所有する任意のテーブルのインデックスを削除するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

LDAP システム権限
LDAP サーバ設定オブジェクトの承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY LDAP SERVER システム権限
LDAP サーバ設定オブジェクトに対する CREATE 文、ALTER 文、または DROP 文の発行に必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

マテリアライズドビューのシステム権限
マテリアライズドビューに対する承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY MATERIALIZED VIEW システム権限
任意のユーザにより所有されるマテリアライズドビューを作成するのに必要です。任意のユーザが所有するマテリアライズドビューに対する COMMENT 文を発行することもできます。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE MATERIALIZED VIEW システム権限
自己所有のマテリアライズドビューを作成するのに必要です。自己所有のマテリアライズドビューに対する COMMENT 文を発行することもできます。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY MATERIALIZED VIEW システム権限
任意のユーザが所有するマテリアライズドビューを変更するのに必要です。任意のユーザが所有するマテリアライズドビューに対する COMMENT 文を発行することもできます。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP ANY MATERIALIZED VIEW システム権限
任意のユーザが所有するマテリアライズドビューを削除するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

メッセージのシステム権限
メッセージに対する承認済みタスクの実行に関連するシステム権限です。

参照：
- すべてのシステム権限のリスト (73 ページ)

CREATE MESSAGE システム権限
メッセージを作成するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP MESSAGE システム権限
メッセージを削除するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

その他のシステム権限
その他の承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY OBJECT システム権限
任意のユーザが所有するオブジェクトを変更するのに必要です。

ALTER ANY OBJECT システム権限によりユーザは以下の文を発行できるようになります。

- ALTER TABLE
- ALTER INDEX
- ALTER JOIN INDEX
- ALTER VIEW
- ALTER MATERIALIZED VIEW
- ALTER PROCEDURE
- ALTER EVENT
- ALTER SEQUENCE
- ALTER FUNCTION
- ALTER DATATYPE
- ALTER MESSAGE
- ALTER TEXT CONFIGURATION
- ALTER TRIGGER
- ALTER STATISTICS
- さまざまなオブジェクトに対する COMMENT
- ALTER SPATIAL REFERENCE SYSTEM
- ALTER SPATIAL UNIT OF MEASURE

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY OBJECT OWNER システム権限
任意のユーザが所有するユーザテーブルの所有者を変更するために必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

注意： このシステム権限は、テーブルオブジェクトにのみ適用されます。プロシージャやマテリアライズドビューなどの他のオブジェクトの所有者を変更することはできません。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)

- すべてのシステム権限のリスト (73 ページ)

COMMENT ANY OBJECT システム権限
任意のユーザが所有する任意のオブジェクトに対してコメントを追加するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY OBJECT システム権限
任意のユーザが所有するオブジェクトを作成するのに必要です。

CREATE ANY OBJECT システム権限によりユーザは以下の文を発行できるようになります。

- さまざまなオブジェクトに対する COMMENT
- CREATE DATATYPE
- CREATE EVENT
- CREATE FUNCTION
- CREATE INDEX
- CREATE JOIN INDEX
- CREATE MATERIALIZED VIEW
- CREATE MESSAGE
- CREATE PROCEDURE
- CREATE SCHEMA
- CREATE SEQUENCE
- CREATE SPATIAL REFERENCE SYSTEM
- CREATE SPATIAL UNIT OF MEASURE
- CREATE STATISTICS
- CREATE TABLE
- CREATE TEXT CONFIGURATION
- CREATE VIEW

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP ANY OBJECT システム権限
任意のユーザが所有するオブジェクトを削除するのに必要です。

DROP ANY OBJECT システム権限によりユーザは以下の文を発行できるようになります。

- DROP DATATYPE
- DROP EVENT
- DROP FUNCTION
- DROP INDEX
- DROP JOIN INDEX
- DROP MATERIALIZED VIEW
- DROP MESSAGE
- DROP PROCEDURE
- DROP SEQUENCE
- DROP SPATIAL REFERENCE SYSTEM
- DROP SPATIAL UNIT OF MEASURE
- DROP STATISTICS
- DROP TABLE
- DROP TEXT CONFIGURATION
- DROP TRIGGER
- DROP VIEW

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY OBJECT PRIVILEGES システム権限
オブジェクトを管理するのに必要です。

MANAGE ANY OBJECT PRIVILEGES システム権限により、ユーザは次のような管理関連タスクを実行できるようになります。

- 任意のユーザにより所有されたオブジェクトに対する任意のオブジェクトレベル権限 (INSERT、UPDATE、DELETE、SELECT、ALTER、REFERENCES、または EXECUTE) を付与する
- MANAGE ANY OBJECT PRIVILEGES システム権限を持つオブジェクト所有者または別のユーザによって付与された任意のオブジェクトレベル権限を取り消す

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

REORGANIZE ANY OBJECT システム権限
任意のユーザによって所有されている該当するオブジェクトの REORGANIZE 文を発行するために必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

VALIDATE ANY OBJECT システム権限
任意のユーザが所有するシステムストア内のテーブル、マテリアライズドビュー、インデックス、またはデータベースを検証またはチェックするのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

ミラーサーバのシステム権限
ミラーサーバに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY MIRROR SERVER システム権限
高可用性サーバ管理タスクを実行するのに必要です。

MANAGE ANY MIRROR SERVER システム権限により、ユーザは以下のことができるようになります。

- ミラーサーバの CREATE 文、ALTER 文、または DROP 文を発行する
- ミラーサーバのパラメータを変更する
- ミラーサーバのオプションを設定する
- ALTER 文を実行してデータベースの所有権を変更する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

マルチプレックスのシステム権限
マルチプレックス環境で承認済みタスクを実行するにはシステム権限が必要です。

参照：
- すべてのシステム権限のリスト (73 ページ)

ACCESS SERVER LS システム権限
SERVER 論理サーバコンテキストを使用して論理サーバ接続を許可します。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)

- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

MANAGE MULTIPLEX システム権限
マルチプレックスサーバ管理に関連する管理タスクを許可します。

MANAGE MULTIPLEX システム権限によりユーザは以下のことができるようになります。

- 論理サーバポリシーに対するマルチプレックス関連の CREATE 文、ALTER 文、DROP 文、または COMMENT 文を発行する
- 論理サーバに対するマルチプレックス関連の CREATE 文、ALTER 文、DROP 文、または COMMENT 文を発行する
- 論理サーバへの DB 領域の排他割り当てを実行する
- 論理サーバの排他使用から移植済み DB 領域を解放する

注意： MANAGE MULTIPLEX システム権限はフェールオーバ設定も管理するので、手動のフェールオーバに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

プロシージャのシステム権限
プロシージャに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY PROCEDURE システム権限
任意のユーザが所有する任意のストアドプロシージャまたは関数を変更するために必要です。

ALTER ANY PROCEDURE システム権限によりユーザは以下のことができるようになります。

- 任意のユーザが所有するストアドプロシージャおよび関数を変更する

- 任意のユーザが所有するプロシージャに対する COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY PROCEDURE システム権限
任意のユーザが所有する任意のストアドプロシージャまたは関数を作成するのに必要です。

CREATE ANY PROCEDURE システム権限によりユーザは以下のことができるようになります。

- 任意のユーザが所有するストアドプロシージャおよび関数を作成する
- 任意のユーザが所有するプロシージャに対する COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE PROCEDURE システム権限
自己所有のストアドプロシージャまたは関数を作成するのに必要です。

CREATE PROCEDURE システム権限によりユーザは以下のことができるようになります。

- 自己所有のストアドプロシージャおよび関数を作成する
- 自己所有のプロシージャに対する COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP ANY PROCEDURE システム権限
任意のユーザが所有する任意のストアドプロシージャまたは関数を削除するために必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

EXECUTE ANY PROCEDURE システム権限
任意のユーザが所有する任意のストアドプロシージャまたは関数を実行するために必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

MANAGE AUDITING システム権限
sa_audit_string ストアドプロシージャを実行するために必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)

- すべてのシステム権限のリスト (73 ページ)

レプリケーションのシステム権限
承認済みレプリケーションタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE REPLICATION システム権限
レプリケーション管理タスクを実行するのに必要です。

MANAGE REPLICATION システム権限によりユーザは以下のことができるようになります。

- CREATE、ALTER、DROP、または COMMENT PUBLICATION 文を発行する
- CREATE、ALTER、DROP、または SYNCHRONIZATION SUBSCRIPTION 文を発行する
- CREATE、ALTER、DROP、または SYNCHRONIZATION USER 文を発行する
- CREATE、ALTER、DROP、または COMMENT SYNCHRONIZATION PROFILE 文を発行する
- CREATE または DROP SUBSCRIPTION 文を発行する
- CREATE REMOTE MESSAGE TYPE 文を発行する
- DROP REMOTE MESSAGE TYPE 文を発行する
- GRANT または REVOKE CONSOLIDATE 文を発行する
- GRANT または REVOKE REMOTE 文を発行する
- GRANT または REVOKE PUBLISH 文を発行する
- LOCK FEATURE 文を発行する
- START、STOP、または SYNCHRONIZE SUBSCRIPTION 文を発行する
- PASSSTHROUGH 文を発行する
- REMOTE RESET 文を発行する
- SET REMOTE OPTION 文を発行する
- START または STOP SYNCHRONIZATION SCHEMA CHANGE 文を発行する
- SYNCHRONIZE PROFILE 文を発行する
- SA_SETREMOTEUSER プロシージャを実行する
- SA_SETSUBSCRIPTION プロシージャを実行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

ロールのシステム権限
ロールに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE ROLES システム権限
新しいロールを作成し、ロールのデフォルト管理者になるために必要です。

MANAGE ROLES システム権限は、新しいユーザ定義ロールを作成できる権限ですが、この権限でロールを削除することはできません。このためには、そのロールの管理権限が必要です。

MANAGE ROLES システム権限が付与されたユーザは、ユーザ定義ロールのデフォルトのグローバルロール管理者になります。

ロール作成プロセス中、ロール管理者が指定されない場合、ロールに MANAGE ROLES システム権限 (SYS_MANAGE_ROLES_ROLE) が ADMIN ONLY OPTION 句付きで自動的に付与され、グローバルロール管理者は、このロールを管理できるようになります。作成プロセス中、1 人以上のロール管理者が指定される場合、このロールに MANAGE ROLES システム権限は付与されず、グローバルロール管理者はこのロールを管理できません。

MANAGE ROLES は、ユーザ定義ロールを管理する権限が付与される唯一のシステム権限です。

注意： ロールの管理はロールの作成時または作成後のいずれかに、ユーザに対して直接付与することもできます。ロールの管理をユーザに直接付与する場合、そのユーザにはロールを管理するための MANAGE ROLES システム権限は必要ありません。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

UPGRADE ROLE システム権限
16.0 より前の IQ データベースをアップグレードするときに導入された新しいシステム権限を管理するために必要です。

デフォルトでは、UPGRADE ROLE システム権限は SYS_AUTH_SA_ROLE ロールに付与されます (このロールが存在する場合)。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

シーケンスのシステム権限
シーケンスに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY SEQUENCE システム権限
任意のシーケンスを変更するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY SEQUENCE システム権限
任意のシーケンスを作成するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP ANY SEQUENCE システム権限
任意のシーケンスを削除するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

USE ANY SEQUENCE システム権限
任意のシーケンスを使用するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

サーバオペレータのシステム権限
承認済みサーバオペレータタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

SERVER OPERATOR システム権限
サーバオペレータタスクを実行するのに必要です。

SERVER OPERATOR システム権限によりユーザは以下のことができるようになります。

- データベースの作成
- キャッシュ管理
- データベースの削除
- データベースの開始または停止
- データベースエンジンの開始または停止
- サーバの作成、変更、または削除
- 暗号化または複合化されたデータベースの作成
- 暗号化または複合化されたファイルの作成
- データベースのトランザクションログを変更するための **ALTER** 文の発行
- 完全データベースリストアまたはカタログのみをリストアするための **RESTORE DATABASE** 文の発行

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

空間オブジェクトのシステム権限
空間オブジェクトに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY SPATIAL OBJECT システム権限
任意の空間オブジェクトを管理するのに必要です。

MANAGE ANY SPATIAL OBJECT システム権限により、ユーザは以下の文を発行できるようになります。

- 空間オブジェクトの CREATE 文、ALTER 文、または DROP 文
- 空間測定単位の CREATE 文、ALTER 文、または DROP 文
- 空間測定単位の COMMENT 文

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

統計情報のシステム権限
統計情報に対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY STATISTICS システム権限
任意のテーブルの統計に対する CREATE 文、ALTER 文、DROP 文、または UPDATE 文を発行するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

テーブルのシステム権限
テーブルに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY TABLE システム権限
任意のユーザが所有する任意のテーブルを変更するのに必要です。

ALTER DATABASE システム権限によりユーザは以下のことができるようになります。
- 任意のユーザが所有するテーブル、テーブルパーティション、またはビューに対する ALTER 文または TRUNCATE 文を発行する
- 任意のユーザが所有するテーブルに対する COMMENT 文を発行する
- 任意のユーザが所有するテーブルのカラムに対する COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY TABLE システム権限
任意のユーザが所有するテーブルを作成するのに必要です。

CREATE ANY TABLE システム権限によりユーザは以下のことができるようになります。

- 任意のユーザが所有するプロキシテーブルを含むテーブルを作成する
- 任意のユーザが所有するテーブルに対する COMMENT 文を発行する
- 任意のユーザが所有するテーブルのカラムに対する COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE PROXY TABLE システム権限
自己所有のプロキシテーブルを作成するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE TABLE システム権限
自己所有のテーブルを作成するのに必要です。

CREATE TABLE システム権限によりユーザは以下のことができるようになります。

- プロキシテーブル以外の自己所有のテーブルを作成する
- 自己所有のテーブルに対する COMMENT 文を発行する
- 自己所有のテーブルのカラムに対する COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DELETE ANY TABLE システム権限
任意のユーザが所有するテーブル、テーブルパーティション、またはビューからローを削除するために必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP ANY TABLE システム権限
任意のユーザが所有するテーブルを削除するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)

- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

INSERT ANY TABLE システム権限
任意のユーザが所有するテーブルとビューにローを挿入するために必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

LOAD ANY TABLE システム権限
-gl サーバスイッチが DBA に設定されている任意のテーブルに対して LOAD コマンドを実行するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

SELECT ANY TABLE システム権限
任意のユーザが所有するテーブル、ビュー、またはマテリアライズドビューでクエリを実行するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

TRUNCATE ANY TABLE システム権限
任意のテーブルに対して TRUNCATE コマンドを実行するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

UPDATE ANY TABLE システム権限
任意のユーザが所有するテーブルとビュー内のローを更新するために必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

テキスト設定のシステム権限
テキスト設定に対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY TEXT CONFIGURATION システム権限
任意のユーザが所有するテキスト設定を変更するのに必要です。

ALTER ANY TEXT CONFIGURATION システム権限によりユーザは以下の文を発行できるようになります。

- 任意のユーザが所有するテキスト設定に対する ALTER 文
- 任意のユーザが所有するテキスト設定に対する COMMENT 文

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY TEXT CONFIGURATION システム権限
他のユーザが所有するテキスト設定を作成するのに必要です。

CREATE ANY TEXT CONFIGURATION システム権限によりユーザは以下のことができるようになります。

- 任意のユーザが所有する設定を作成する
- 任意のユーザが所有するテキスト設定に対する COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE TEXT CONFIGURATION システム権限
自己所有のテキスト設定を作成するのに必要です。

CREATE TEXT CONFIGURATION システム権限によりユーザは以下のことができるようになります。

- 自己所有のテキスト設定を作成する
- 自己所有のテキスト設定の COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP ANY TEXT CONFIGURATION システム権限
任意のユーザが所有するテキスト設定を削除するのに必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

トリガのシステム権限
トリガに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY TRIGGER システム権限
トリガを変更するのに必要です。また、テーブルに対する ALTER 権限があれば、そのテーブルに対する COMMENT 文を発行できます。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY TRIGGER システム権限
トリガの作成に必要です。また、テーブルに対する ALTER 権限があれば、そのテーブルに対する COMMENT 文を発行できます。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

ユーザとログイン管理のシステム権限
ユーザとログインポリシーに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

CHANGE PASSWORD システム権限
自身のパスワード以外のパスワードの管理をユーザに許可します。

このシステム権限では、管理対象のパスワードを、特定のユーザリスト、特定のロールリストが付与されているユーザ、または既存データベースユーザのパスワードに限定できます。 このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- パスワード (96 ページ)
- GRANT CHANGE PASSWORD 文 (289 ページ)
- REVOKE CHANGE PASSWORD 文 (309 ページ)
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY LOGIN POLICY システム権限
ログインポリシーを管理するのに必要です。

MANAGE ANY LOGIN POLICY システム権限により、ユーザは以下の文を発行できるようになります。

- ログインポリシーの CREATE 文、ALTER 文、または DROP 文
- ログインポリシーの COMMENT 文

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)

- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY USER システム権限
ユーザを管理するのに必要です。

MANAGE ANY USER システム権限により、ユーザは以下のことができるようになります。

- データベースユーザの CREATE 文、ALTER 文、または DROP 文を発行する (初期パスワードの割り当てを含む)
- ユーザの認証メカニズムを定義する (Kerberos、統合ログイン)
- 外部ログインの CREATE 文または DROP 文を発行する
- 任意のユーザに対して次回ログイン時にパスワード変更を強制する
- 任意のユーザにログインポリシーを割り当てる
- 任意のユーザのログインポリシーをリセットする
- ユーザ、統合ログイン、または Kerberos ログインの COMMENT 文を発行する

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

SET USER システム権限
別のユーザが持つ特定のロールとシステム権限を一時的に使用 (同一化) することをユーザに許可します。

注意： SET USER システム権限は 2 語で、SETUSER 文は 1 語です。

SET USER システム権限を付与するときに、同一化の範囲を次のいずれかとして定義することができます。

- データベース内の任意のユーザ
- 指定したユーザのリスト内の (*target_users_list*) 任意のユーザ
- 1 つまたは複数の指定したロール (*target_roles_list*) のメンバーである任意のユーザ

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- 同一化 (104 ページ)
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

ビューのシステム権限
ビューに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

ALTER ANY VIEW システム権限
任意のユーザが所有するビューの変更に必要です。

ALTER ANY VIEW システム権限は、ユーザに以下の実行を許可します。

- 任意のユーザが所有するビューの変更
- 任意のユーザが所有するビューに対する COMMENT 文の発行

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE ANY VIEW システム権限
任意のユーザが所有するビューの作成に必要です。

CREATE ANY VIEW システム権限は、ユーザに以下の実行を許可します。

- 任意のユーザが所有するビューの作成
- 任意のユーザが所有するビューに対する COMMENT 文の発行

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

CREATE VIEW システム権限
自己所有のビューの作成に必要です。

CREATE VIEW システム権限は、ユーザに以下の実行を許可します。

- 自己所有のビューの作成
- 自己所有のビューに対する COMMENT 文の発行

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

DROP ANY VIEW システム権限
任意のユーザが所有するビューの削除に必要です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

Web サービスのシステム権限
Web サービスに対する承認済みタスクの実行に関連するシステム権限。

参照：
- すべてのシステム権限のリスト (73 ページ)

MANAGE ANY WEB SERVICE システム権限
Web サービス関連のタスクの管理に必要です。

MANAGE ANY WEB SERVICE システム権限により、ユーザは以下の文を発行できるようになります。

- Web サービスに対する CREATE 文、ALTER 文、または DROP 文
- Web サービスに対する COMMENT 文

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。

参照：
- GRANT システム権限文 (304 ページ)
- REVOKE システム権限文 (321 ページ)
- すべてのシステム権限のリスト (73 ページ)

すべてのシステム権限のリスト
すべてのシステム権限のリスト

システム権限は、ユーザが承認済みのデータベースタスクを実行する権限を制御します。

参照：
- ACCESS SERVER LS システム権限 (53 ページ)
- ALTER ANY INDEX システム権限 (44 ページ)
- ALTER ANY MATERIALIZED VIEW システム権限 (47 ページ)
- ALTER ANY OBJECT システム権限 (48 ページ)
- ALTER ANY OBJECT OWNER システム権限 (49 ページ)
- ALTER ANY PROCEDURE システム権限 (54 ページ)
- ALTER ANY SEQUENCE システム権限 (59 ページ)
- ALTER ANY TABLE システム権限 (62 ページ)
- ALTER ANY TEXT CONFIGURATION システム権限 (66 ページ)
- ALTER ANY TRIGGER システム権限 (68 ページ)
- ALTER ANY VIEW システム権限 (71 ページ)
- ALTER DATABASE システム権限 (35 ページ)

- ALTER DATATYPE システム権限 (39 ページ)
- BACKUP DATABASE システム権限 (36 ページ)
- CHANGE PASSWORD システム権限 (69 ページ)
- CHECKPOINT システム権限 (36 ページ)
- COMMENT ANY OBJECT システム権限 (50 ページ)
- CREATE ANY INDEX システム権限 (45 ページ)
- CREATE ANY MATERIALIZED VIEW システム権限 (46 ページ)
- CREATE ANY OBJECT システム権限 (50 ページ)
- CREATE ANY PROCEDURE システム権限 (55 ページ)
- CREATE ANY SEQUENCE システム権限 (59 ページ)
- CREATE ANY TABLE システム権限 (63 ページ)
- CREATE ANY TEXT CONFIGURATION システム権限 (67 ページ)
- CREATE ANY TRIGGER システム権限 (68 ページ)
- CREATE ANY VIEW システム権限 (71 ページ)
- CREATE DATATYPE システム権限 (39 ページ)
- CREATE EXTERNAL REFERENCE システム権限 (42 ページ)
- CREATE MATERIALIZED VIEW システム権限 (47 ページ)
- CREATE MESSAGE システム権限 (48 ページ)
- CREATE PROCEDURE システム権限 (55 ページ)
- CREATE PROXY TABLE システム権限 (63 ページ)
- CREATE TABLE システム権限 (64 ページ)
- CREATE TEXT CONFIGURATION システム権限 (67 ページ)
- CREATE VIEW システム権限 (72 ページ)
- DEBUG ANY PROCEDURE システム権限 (41 ページ)
- DELETE ANY TABLE システム権限 (64 ページ)
- DROP ANY INDEX システム権限 (45 ページ)
- DROP ANY MATERIALIZED VIEW システム権限 (47 ページ)
- DROP ANY OBJECT システム権限 (51 ページ)
- DROP ANY PROCEDURE システム権限 (56 ページ)
- DROP ANY SEQUENCE システム権限 (60 ページ)
- DROP ANY TABLE システム権限 (64 ページ)
- DROP ANY TEXT CONFIGURATION システム権限 (68 ページ)
- DROP ANY VIEW システム権限 (72 ページ)
- DROP CONNECTION システム権限 (36 ページ)
- DROP DATATYPE システム権限 (40 ページ)

- DROP MESSAGE システム権限 (48 ページ)
- EXECUTE ANY PROCEDURE システム権限 (56 ページ)
- LOAD ANY TABLE システム権限 (65 ページ)
- INSERT ANY TABLE システム権限 (65 ページ)
- MANAGE ANY DBSPACE システム権限 (40 ページ)
- MANAGE ANY EVENT システム権限 (41 ページ)
- MANAGE ANY EXTERNAL ENVIRONMENT システム権限 (42 ページ)
- MANAGE ANY EXTERNAL OBJECT システム権限 (43 ページ)
- MANAGE ANY LDAP SERVER システム権限 (46 ページ)
- MANAGE ANY LOGIN POLICY システム権限 (69 ページ)
- MANAGE ANY MIRROR SERVER システム権限 (53 ページ)
- MANAGE ANY OBJECT PRIVILEGES システム権限 (51 ページ)
- MANAGE ANY SPATIAL OBJECT システム権限 (61 ページ)
- MANAGE ANY STATISTICS システム権限 (62 ページ)
- MANAGE ANY USER システム権限 (70 ページ)
- MANAGE ANY WEB SERVICE システム権限 (73 ページ)
- MANAGE AUDITING システム権限 (56 ページ)
- MANAGE MULTIPLEX システム権限 (54 ページ)
- MANAGE PROFILING システム権限 (37 ページ)
- MANAGE REPLICATION システム権限 (57 ページ)
- MANAGE ROLES システム権限 (58 ページ)
- MONITOR システム権限 (37 ページ)
- READ CLIENT FILE システム権限 (43 ページ)
- READ FILE システム権限 (43 ページ)
- REORGANIZE ANY OBJECT システム権限 (52 ページ)
- SELECT ANY TABLE システム権限 (65 ページ)
- SERVER OPERATOR システム権限 (60 ページ)
- SET ANY PUBLIC OPTION システム権限 (38 ページ)
- SET ANY SECURITY OPTION システム権限 (38 ページ)
- SET ANY SYSTEM OPTION システム権限 (38 ページ)
- SET ANY USER DEFINED OPTION システム権限 (39 ページ)
- SET USER システム権限 (70 ページ)
- TRUNCATE ANY TABLE システム権限 (66 ページ)
- UPDATE ANY TABLE システム権限 (66 ページ)
- UPGRADE ROLE システム権限 (59 ページ)

- USE ANY SEQUENCE システム権限 (60 ページ)
- VALIDATE ANY OBJECT システム権限 (52 ページ)
- WRITE CLIENT FILE システム権限 (44 ページ)
- WRITE FILE システム権限 (44 ページ)

システム権限のユーザへの付与
特定のシステム権限を管理権限付きまたはなしで特定のユーザに付与できます。

前提条件
付与するシステム権限に対する管理権限。

手順

警告！ システム権限を付与する構文は、CHANGE PASSWORD と SET USER を除くすべてのシステム権限で同一です。

このシステム権限は、WITH ADMIN OPTION 句、WITH NO ADMIN OPTION 句、または WITH ADMIN ONLY OPTION 句を使用して付与します。句を指定しない場合、デフォルトは WITH NO ADMIN OPTION です。
システム権限をユーザに付与するには、次のいずれかの文を実行します。

管理オプション	文
完全な管理権限付きで付与する。	**GRANT** *system_privilege* **TO** *grantee [,...]* **WITH ADMIN OPTION**
管理権限のみ付与する。	**GRANT** *system_privilege* **TO** *grantee [,...]* **WITH ADMIN ONLY OPTION**
管理権限なしで付与する。	**GRANT** *system_privilege* **TO** *grantee [,...]* **WITH NO ADMIN OPTION**

参照：
- GRANT システム権限文 (304 ページ)
- GRANT CHANGE PASSWORD 文 (289 ページ)
- GRANT SET USER 文 (302 ページ)

ユーザが持つシステム権限の取り消し

特定のユーザが持つ、特定のシステム権限およびシステム権限を管理する権限を取り消します。

前提条件

取り消すシステム権限に対する管理権限。

手順

警告！ システム権限を取り消す構文は、CHANGE PASSWORD と SET USER を除くすべてのシステム権限に適用されます。

ユーザのシステム権限を取り消すには、次のどちらかの文を実行します。

管理オプション	文
管理権限のみ	**REVOKE ADMIN OPTION FOR** *system_privilege* **FROM** *grantee [,...]*
システム権限を取り消して、さらに管理権限が付与されている場合はそれも取り消す。	**REVOKE** *system_privilege* **FROM** *grantee [,...]*

例:

`Mary` と `Joe` に当初 BACKUP DATABASE システム権限が管理権限付きで付与されていたという前提で、`Mary's` の管理権限を取り消してシステム権限のみにして、システム権限を使用する機能のみ残すには、次の文を実行します。

```
REVOKE ADMIN OPTION FOR BACKUP DATABASE FROM Mary
```

`Joe` の持つシステム権限自体とすべての管理権限を取り消すには、次の文を実行します。

```
REVOKE BACKUP DATABASE FROM Joe
```

参照：

- REVOKE システム権限文 (321 ページ)
- REVOKE CHANGE PASSWORD 文 (309 ページ)
- REVOKE SET USER 文 (319 ページ)

ユーザおよび権限が付与されるシステムオブジェクト

現在のデータベースのユーザとその権限に関する情報は、データベースシステムテーブルに格納され、システムビューからアクセスできます。

システムテーブルの大半は、SYS ユーザ ID が所有します。SYS ユーザ ID はログインに使用できません。

DBA にはデータベースの他のすべてのテーブルと同様に、すべてのシステムテーブルに対する SELECT アクセス権があります。一部のテーブルに対する他のユーザのアクセスは制限されています。たとえば、データベースのユーザの権限、および各ユーザ ID のパスワードが含まれる SYS.SYSUSERPERM テーブルには、DBA のみがアクセスできます。しかし、SYS.SYSUSERPERMS は、パスワードを除く SYS.SYSUSERPERM 内のすべての情報が含まれるビューで、デフォルトではすべてのユーザにこのビューに対する SELECT アクセス権が割り当てられます。新しいデータベースで、SYS と PUBLIC のシステムロール、および DBA ユーザに自動的に設定される権限とロールメンバーシップはすべて、自由に変更できます。

システムテーブル内のユーザ ID、ロールおよび権限に関する情報

ユーザ ID、ロール、および権限に関する情報が含まれるシステムテーブルです。

テーブルとビューはすべて SYS ロールが所有し、修飾名は SYS.ISYSUSERPERM、SYS.ISYSTABLEPERM などになります。これらにテーブルに対して適切な SELECT クエリを実行すると、データベースに含まれるユーザ ID および権限のすべてに関する情報が生成されます。

テーブル	デフォルト	内容
ISYSUSERPERM	SELECT ANY TABLE システム権限	各ユーザ ID のデータベースレベルの権限とパスワード
ISYSTABLEPERM	PUBLIC	GRANT コマンドによって付与されるテーブルに対するすべての権限
ISYSCOLPERM	PUBLIC	GRANT コマンドで UPDATE 権限が付与されるすべてのカラム
ISYSPROCPERM	PUBLIC	ローごとに特定のプロシージャの使用権限が付与された個別のユーザを記載

システムビュー内のユーザ ID、ロールおよび権限に関する情報

ユーザ ID、ロール、および権限に関する情報が含まれるシステムビューです。

このリスト以外にも、データベースの各オブジェクトに関する情報が含まれるテーブルとビューがあります。

ビュー	デフォルト	内容
SYSUSERAUTH (旧式)	SELECT ANY TABLE システム権限	ユーザメンバーを除く SYSUSERPERM (旧式) 内の全情報
SYSUSERPERMS (旧式)	PUBLIC	パスワードを除く SYSUSERPERM (旧式) 内の全情報
SYSUSERLIST (旧式)	PUBLIC	パスワードを除く SYSUSERAUTH (旧式) 内の全情報
SYSTABAUTH	PUBLIC	SYSTABLEPERM の情報を読みやすくしたもの
SYSCOLAUTH	PUBLIC	SYSCOLPERM の情報を読みやすくしたもの
SYSPROCAUTH	PUBLIC	SYSPROCPERM の情報を読みやすくしたもの

システム権限をシステムロールにマッピングするストアドプロシージャ

sp_sys_priv_role_info ストアドプロシージャは、各システム権限ロールをシステムロールにマッピングするレポートを生成します。

システム権限ごとに個別のローが生成されます。このプロシージャを実行するために必要なシステム権限はありません。

オブジェクトレベル権限

データベースのオブジェクトレベル権限をユーザに付与したり、ユーザからオブジェクトレベル権限を取り消したりできます。

データベースオブジェクトの所有権限

データベースオブジェクトの所有権には、そのオブジェクトに対するアクションを実行する権限が付随しています。

データベースオブジェクトの作成者は、必ずしもその所有者である必要はありません。作成プロセスで、別のユーザを所有者として指定することができます。所有者を指定しない場合は、作成者が所有者になります。

テーブルの*所有者*は、たとえば、テーブル構造の変更、他のデータベースユーザへのテーブル内の情報の更新権限の付与などを実行できます。

注意： テーブルの所有者は、十分な権限がある場合、またはコマンドラインや構成ファイルで **-gl all** スイッチを指定してサーバが起動された場合にデータをロードできます。**LOAD TABLE** コマンドを発行するには、所有権または CREATE ANY OBJECT システム権限だけでは不十分です。テーブルに対する INSERT 権限も必要です。

ALTER ANY OBJECT システム権限を持つユーザは (所有者にかかわりなく)、CREATE ANY OBJECT システム権限などを使用して作成されたすべてのデータベースオブジェクトを変更できます。CREATE ANY OBJECT システム権限を持つユーザは、データベースオブジェクトを作成して他のユーザを所有者にすることができます。

データベース権限の継承

データベース権限は、ユーザに直接付与することも、ロールメンバーシップを利用して継承することもできます。

権限名	データベースオブジェクトのサポート対象	許可される操作
ALL	テーブル、ビュー、マテリアライズドビュー	テーブル、ビューおよびマテリアライズドビューに関連するすべてのタスクの実行。
ALTER	テーブル	テーブルの構造の変更。
CREATE	DB 領域	DB 領域でのオブジェクトの作成。必要となる追加の権限は、作成されるオブジェクトによって異なる。たとえば、テーブルを作成するには、CREATE TABLE、CREATE ANY TABLE、または CREATE ANT OBJECT のいずれかが必要。
DELETE	テーブル、ビュー	テーブルまたはビューのローの削除。
EXECUTE	プロシージャ、ユーザ定義関数	プロシージャまたはユーザ定義関数の実行。
INSERT	テーブル、ビュー	テーブルまたはビューへのローの挿入。
LOAD	テーブル	**-gl** データベースオプションが NONE 以外に設定されている場合に、テーブルをロードする。
REFERENCES	テーブル	テーブルに対するインデックスを作成し、テーブルを参照する外部キーを作成する。
SELECT	テーブル、ビュー	テーブルまたはビューの情報の確認。
TRUNCATE	テーブル、マテリアライズドビュー	テーブルまたはマテリアライズドビューのトランケート。
UPDATE	テーブル、ビュー	テーブルまたはビューのローを更新する。
USAGE	シーケンスジェネレータ	シーケンス内の現在の値または次の値の評価。

マルチプレックスでは、書き込みサーバが所有するテーブルに対するテーブル変更は、その書き込みサーバのみが実行できます。

オブジェクトレベル権限の付与と取り消し

権限の組み合わせをユーザに付与したり、取り消すことで、データベースオブジェクトに対するユーザのアクセスを定義できます。

テーブルに対する ALTER 権限の付与

テーブルの構造を変更する権限を付与します。この権限は、ビューには適用されません。

前提条件

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- WITH GRANT OPTION 句によるテーブルに対する ALTER オブジェクト権限
- テーブルを所有している。

手順

ALTER 権限を付与するには、次のように入力します。

```
GRANT ALTER
  ON table_name
  TO userID [,...]
```

参照：

- GRANT オブジェクトレベル権限文 (295 ページ)
- オブジェクトレベル権限の管理権の付与 (85 ページ)

テーブルとビューに対する DELETE 権限の付与

指定されたテーブルまたはビューのすべてのデータを削除する権限を付与します。

前提条件

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- WITH GRANT OPTION 句によるテーブルに対する DELETE オブジェクト権限
- テーブルを所有している。

手順

DELETE 権限を付与するには、次のように入力します。

```
GRANT DELETE
  ON table_name
  TO userID [,...]
```

参照：
- GRANT オブジェクトレベル権限文 (295 ページ)
- オブジェクトレベル権限の管理権の付与 (85 ページ)

テーブルとビューに対する INSERT 権限の付与
テーブルまたはビューにデータを挿入する権限を付与します。

前提条件

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- WITH GRANT OPTION 句によるテーブルに対する INSERT オブジェクト権限
- テーブルを所有している。

手順
INSERT 権限を付与するには、次のように入力します。

```
GRANT INSERT
  ON table_name
  TO userID [,...]
```

参照：
- GRANT オブジェクトレベル権限文 (295 ページ)
- オブジェクトレベル権限の管理権の付与 (85 ページ)

テーブルに対する LOAD 権限の付与
指定したテーブルをロードする権限を付与します。

前提条件
次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- WITH GRANT OPTION 句によるテーブルに対する LOAD オブジェクト権限
- テーブルを所有している。

手順
LOAD 権限を付与するには、次のように入力します。

```
GRANT LOAD
  ON table_name
  TO userID [,...]
```

参照：
- GRANT オブジェクトレベル権限文 (295 ページ)

- オブジェクトレベル権限の管理権の付与 (85 ページ)

テーブルに対する REFERENCES 権限の付与
テーブルのインデックスと外部キーに対する権限を付与します。この権限は、ビューには適用されません。この権限は、テーブル内のカラムのセットに限定することができます。

前提条件

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- WITH GRANT OPTION 句によるテーブルに対する REFERENCES オブジェクト権限
- テーブルを所有している。

手順
REFERENCES 権限を付与するには、次のように入力します。

```
GRANT REFERENCES column_name
  ON table_name
  TO userID [,...]
```

例:

次の文は、ユーザ `Joe` に、`sales_table` という名前のテーブルのカラム `Col_1` と `Col_2` に対する REFERENCES 権限を付与します。

```
GRANT REFERENCES Col_1, Col_2 ON sales_table
TO Joe
```

参照：
- GRANT オブジェクトレベル権限文 (295 ページ)
- オブジェクトレベル権限の管理権の付与 (85 ページ)

テーブルとビューに対する SELECT 権限の付与
テーブルまたはビューのデータを選択する権限を付与します。変更する権限は付与しません。この権限は、テーブル内のカラムのセットに限定することができます。

前提条件

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- WITH GRANT OPTION 句によるテーブルに対する SELECT オブジェクト権限

- テーブルを所有している。

手順
SELECT 権限を付与するには、次のように入力します。

```
GRANT SELECT column_name
  ON table_name
  TO userID [,...]
```

例:

次の文は、ユーザ Joe に、sales_table という名前のテーブルのカラム Col_1 と Col_2 に対する SELECT 権限を付与します。

```
GRANT SELECT Col_1, Col_2 ON sales_table
TO Joe
```

参照：
- GRANT オブジェクトレベル権限文 (295 ページ)
- オブジェクトレベル権限の管理権の付与 (85 ページ)

テーブルに対する TRUNCATE 権限の付与
指定したテーブルをトランケートする権限を付与します。

前提条件
次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- WITH GRANT OPTION 句によるテーブルに対する TRUNCATE オブジェクト権限
- テーブルを所有している。

手順
TRUNCATE 権限を付与するには、次のように入力します。

```
GRANT TRUNCATE
  ON table_name
  TO userID [,...]
```

参照：
- GRANT オブジェクトレベル権限文 (295 ページ)
- オブジェクトレベル権限の管理権の付与 (85 ページ)

テーブルとビューに対する UPDATE 権限の付与
テーブルまたはビューのデータを変更する権限を付与します。この権限は、テーブル内のカラムのセットに限定することができます。

前提条件

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- WITH GRANT OPTION 句によるテーブルに対する UPDATE オブジェクト権限
- テーブルを所有している。

手順
UPDATE 権限を付与するには、次のように入力します。

```
GRANT UPDATE column_name
  ON table_name
  TO userID [,...]
```

例:

次の文は、ユーザ `Joe` に、`sales_table` という名前のテーブルのカラム `Col_1` と `Col_2` に対する UPDATE 権限を付与します。

```
GRANT UPDATE Col_1, Col_2 ON sales_table
TO Joe
```

参照：

- GRANT オブジェクトレベル権限文 (295 ページ)
- オブジェクトレベル権限の管理権の付与 (85 ページ)

オブジェクトレベル権限の管理権の付与
他のユーザへの個別のオブジェクト権限の譲渡を許可する権限をユーザに付与します。

前提条件

次の条件を 1 つ以上満たしている必要があります。

- テーブルを作成している。
- ADMIN OPTION によるテーブルに対する権限。
- LOAD と TRUNCATE のオブジェクト権限。
- MANAGE ANY OBJECT PRIVILEGE システム権限。WITH GRANT OPTION 句を使用して LOAD または TRUNCATE オブジェクト権限が付与されている場合、被付与者はそのオブジェクト権限を他のユーザに付与できますが、元の

GRANT 文で指定されたテーブルに限定されます。この場合は、被付与者に MANAGE ANY OBJECT PRIVILEGE システム権限は必要ありません。

手順

1. データベースに接続します。
2. 権限を他のユーザに付与する権利を付与するには、次のように入力します。

```
GRANT Object_privilege _name
  ON table_name
  TO userID [,...]
  WITH GRANT OPTION
```

例:

次の文は、Mary にテーブル Sales で削除を実行する権限を付与します。

```
GRANT DELETE ON Sales TO Mary
```

次の文は、Joe にテーブル Sales での削除実行と他のユーザへの DELETE 権限の付与の両方の権利を付与します。

```
GRANT DELETE ON Sales TO Joe
WITH GRANT OPTION
```

参照：

- GRANT オブジェクトレベル権限文 (295 ページ)
- オブジェクトレベル権限の管理権の付与 (85 ページ)

DB 領域に対する CREATE 権限の付与

指定された DB 領域にデータベースオブジェクトを作成する権限を付与します。

前提条件

MANAGE ANY DBSPACE システム権限が必要です。

手順

CREATE 権限を付与するには、次のように入力します。

```
GRANT CREATE
  ON dbspace_name
  TO userID [,...]
```

参照：

- GRANT CREATE 文 (293 ページ)

関数とプロシージャに対する EXECUTE 権限の付与
プロシージャまたはユーザ定義関数を実行する権限を付与します。

前提条件
次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- そのプロシージャを所有している。

手順
EXECUTE 権限を付与するには、次のように入力します。

```
GRANT EXECUTE
  ON procedure_name
  TO userID [,...]
```

参照：
- GRANT EXECUTE 文 (294 ページ)

シーケンスジェネレータに対する USAGE 権限の付与
シーケンス内の現在値および次の値を評価する権限を付与します。

前提条件
次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限
- そのシーケンスジェネレータを所有している。

手順
USAGE 権限を付与するには、次のように入力します。

```
GRANT USAGE
  ON sequence_name
  TO userID [,...]
```

参照：
- GRANT USAGE ON SEQUENCE 文 (308 ページ)

オブジェクトレベル権限の取り消し
特定のオブジェクトレベル権限を使用する機能または他のユーザに権限を付与する機能をユーザから削除します。

前提条件
付与者は、次の条件の少なくとも 1 つを満たす必要があります。

- 取り消す権限の付与者である
- MANAGE ANY OBJECT PRIVILEGE システム権限を持っている

手順

WITH GRANT OPTION 句を使用して権限を付与されたユーザの権限を取り消す場合、そのユーザがその権限を付与したすべてのユーザもその権限が取り消されます。たとえば、User1 に WITH GRANT OPTION 句を使用して SELECT 権限を付与し、User1 がその SELECT 権限を User2 に付与したとします。User1 の SELECT 権限を取り消した場合、User2 もその権限が取り消されます。

REVOKE コマンドは、オブジェクトレベル権限そのものに適用され、その権限に付与されている管理権には適用されません。したがって、管理権のみを取り消して、オブジェクトレベル権限をそのまま残すということはできません。オブジェクトレベル権限に対するユーザの管理権のみを正しく取り消すには、まずオブジェクトレベル権限を取り消して、次にその権限を WITH GRANT OPTION 句を使用しないで再付与する必要があります。

1. オブジェクトレベル権限およびその管理権限を取り消すには、次の文を実行します。

```
REVOKE object_privilege_name
  ON table_name
  FROM userID [,...]
```

2. (省略可) 次に、管理権限なしでオブジェクトレベル権限を再付与するには、次の文を実行します。

```
GRANT object_privilege_name
  ON table_name
  TO userID [,...]
```

例:

この例では、Joe に、Sales テーブルに対する削除を実行する権限と他のユーザにそのテーブルに対する DELETE オブジェクトレベル権限を付与する権限の両方が付与されているものとします。

次の文は、テーブル Sales に対するすべての DELETE オブジェクトレベル権限を取り消します。これには、文字通りすべての管理権限も含まれます。

```
REVOKE DELETE ON Sales FROM Joe
```

次の文は、管理権限なしでオブジェクトレベル権限だけを再付与します。

```
GRANT DELETE ON Sales TO Joe
```

参照：

- REVOKE オブジェクトレベル権限文 (314 ページ)

- REVOKE CREATE 文 (312 ページ)
- REVOKE EXECUTE 文 (313 ページ)
- REVOKE USAGE ON SEQUENCE 文 (325 ページ)

DB 領域のテーブルオブジェクトの管理に必要な権限

必要な権限は、実行するタスクによって異なります。

DB 領域に新しいテーブルを作成するには、その DB 領域に対する CREATE オブジェクトレベル権限が必要です。既存のテーブルまたはカラムを DB 領域に移動するには、MANAGE ANY DBSPACE システム権限または移動先の DB 領域に対する CREATE オブジェクトレベル権限が必要です。

DB 領域の要件のほかに、個別のタスクのシステム権限も必要です。たとえば、テーブルを作成するには CREATE TABLE または CREATE ANY TABLE システム権限が必要で、そのテーブルを変更するには ALTER ANY TABLE システム権限が必要となります。

たとえば、DB 領域 `test1` に自分が所有者となる `table1` を作成するには、`test1` に対する CREATE オブジェクレベル権限のほかに、CREATE TABLE システム権限も必要です。その後、`table1` を DB 領域 `test1` から DB 領域 `test2` に移動する場合は、MANAGE ANY DBSPACE システム権限または `test2` (移動先の DB 領域) に対する CREATE オブジェクトレベル権限が必要です。

必要な権限は、ユーザまたはロールに付与したり、取り消したりできます。ロールのメンバーはすべて、ロールから権限を継承します。

デフォルトでは、IQ_SYSTEM_MAIN、IQ_SYSTEM_TEMP、および SYSTEM に対する CREATE オブジェクトレベル権限は PUBLIC に付与されます。

権限を制御するコマンドラインオプション

データベースサーバの起動コマンド **start_iq** には、一部のデータベースおよびサーバ機能権限レベルを設定するオプションが含まれます。

データベースの起動および停止に関連するスイッチ

-gd オプションを使用すると、実行中のサーバ上でデータベースを起動または停止できるユーザを、すでに接続しているデータベースに対して一定のレベルの権限が付与されたユーザに制限することができます。

- **DBA** – (デフォルト値) SERVER OPERATOR システム権限を持つユーザのみが追加のデータベースを起動できます。
- **ALL** – (**start_iq** および `default.cfg` のデフォルト) すべてのユーザがデータベースの起動と停止を実行できます。この設定は、DBA が **START DATABASE** コマンドを発行する必要がないことを意味します。ただし、ユーザがデータベー

スを起動した後、そのデータベースにアクセスする権限がユーザに付与される必要があります。

- **NONE** – 実行中のサーバ上で Interactive SQL からデータベースを起動または停止できるユーザはいません。

注意： サーバを起動したときに **-gd ALL** が設定されていない場合、SERVER OPERATOR システム権限が付与されたユーザのみがそのサーバ上で追加のデータベースを起動できます。つまり、サーバと同時に起動されていないデータベース、またはサーバ起動後に SERVER OPERATOR システム権限を持つユーザによって起動されていないデータベースには、ユーザは接続できません。ただし、SERVER OPERATOR システム権限がないユーザもデータベースを停止することはできます。このため、運用データベースではこの設定を DBA に変更することをおすすめします。

データベースの作成と削除に関連するスイッチ

-gu オプションは、データベースを作成または削除できるユーザを、接続先のデータベースの一定のレベルの権限を持つユーザに制限します。

- **DBA** – SERVER OPERATOR システム権限を持つユーザのみがデータベースの作成および削除を実行できます。
- **ALL** (デフォルト) – すべてのユーザがデータベースの作成および削除を実行できます。
- **NONE** – ユーザはデータベースの作成や削除を実行できません。
- **UTILITY_DB** – `utility_db` データベースに接続できるユーザのみがデータベースの作成および削除を実行できます。

サーバ停止に関連するスイッチ

-gk オプションは、**dbstop** ユーティリティまたは **STOP ENGINE** コマンドを使用してサーバを停止できるユーザを制限します。

- **DBA** (デフォルト) – SERVER OPERATOR システム権限を持つユーザのみがサーバを停止できます。
- **ALL** – すべてのユーザがサーバを停止できます。
- **NONE** – ユーザは、**dbstop** ユーティリティまたは **STOP ENGINE** コマンドを使用してサーバを停止できません。

データベースのロードとアンロードに関連するスイッチ

-gl オプションは、**LOAD TABLE** を使用してデータをロードできるユーザを、データベースに対する一定の権限を持つユーザに制限します。

- **DBA** – LOAD ANY TABLE、ALTER ANY TABLE、または ALTER ANY OBJECT システム権限を持つすべてのユーザがデータをロードできます。

- **ALL** (**start_iq** と `default.cfg` のデフォルト) – すべてのユーザがデータをロードできます。
- **NONE** – データのロードはできません。

参照：
- -gl iqsrv16 サーバオプション (341 ページ)
- -gu iqsrv16 データベースサーバオプション (341 ページ)
- -gk iqsrv16 データベースサーバオプション (340 ページ)

プロシージャを実行する権限の取り消し
特定のプロシージャを実行または呼び出す権限を取り消します。

前提条件
取り消し者は、次のいずれかの条件を満たす必要があります。
- 取り消す権限の付与者である。
- MANAGE ANY OBJECT PRIVILEGE システム権限を持っている。

手順
特定のプロシージャを実行する EXECUTE 権限を取り消すには、次の文を実行します。

```
REVOKE EXECUTE ON procedure_name
FROM grantee [,...]
```

参照：
- REVOKE EXECUTE 文 (313 ページ)

付与されているオブジェクトレベル権限を表示するストアドプロシージャ
sp_objectpermission ストアドプロシージャを実行すると、指定されたロールまたはユーザ名に付与されているオブジェクト権限、または指定されたオブジェクトまたは DB 領域に対して付与されているオブジェクト権限のレポートが生成されます。

レポートには、権限の付与者と被付与者のユーザ ID、オブジェクトの名前と所有者、付与されている権限、および被付与者がその権限を他のユーザに付与できるかどうかが出力されます。

自分自身のユーザ ID に対してこのプロシージャを実行するために必要なシステム権限はありません。他のユーザまたは DB 領域に対して **sp_objectpermission** を実行するには、それぞれ MANAGE ANY OBJECT PRIVILEGE 権限または MANAGE ANY DBSPACE 権限が必要です。

参照：

- sp_objectpermission システムプロシージャ (418 ページ)

システムプロシージャ権限

権限付きシステムプロシージャが動作できるセキュリティモデルは 2 つあります。各モデルでは、異なる方法でシステムプロシージャを実行できます。

注意： 次の情報は、SAP Sybase IQ の権限付きシステムプロシージャのみに適用されます。ユーザ定義のストアドプロシージャには適用されません。

最初のモデルは、SYSTEM PROCEDURE DEFINER モデルと呼ばれます。このモデルでは、権限付きシステムプロシージャがその所有者 (通常、dbo) の権限で実行されます。2 番目のモデルは、SYSTEM PROCEDURE INVOKER モデルと呼ばれます。このモデルでは、権限付きシステムプロシージャがその実行者の権限で実行されます。

SYSTEM PROCEDURE DEFINER モデルを使用して権限付きシステムプロシージャを実行するには、そのプロシージャに対する明示的な EXECUTE オブジェクトレベル権限を付与します。そのシステムプロシージャの基本となる承認済みタスクの実行に必要なシステム権限は、所有者 (システムプロシージャ definer) から自動的に継承されます。

SYSTEM PROCEDURE INVOKER モデルを使用した権限付きシステムプロシージャについては、PUBLIC ロールに EXECUTE オブジェクトレベル権限が付与されます。デフォルトで、ユーザはいずれも PUBLIC ロールのメンバーであるため、すべてのユーザが EXECUTE 権限を自動的に継承します。しかし、PUBLIC ロールはそのシステムプロシージャの所有者ではなく、またシステム権限は何も付与されていないため、基礎となる承認済みタスクの実行に必要なシステム権限をユーザに直接または間接的に付与する必要があります。

デフォルトでは、バージョン 16.0 以降で作成されたデータベースでは、SYSTEM PROCEDURE INVOKER モデルを使用して、すべての権限付きシステムプロシージャが実行されます。16.0 より前のバージョンで作成され、16.0 以降にアップグレードされたデータベースは、SYSTEM PROCEDURE DEFINER モデルと SYSTEM PROCEDURE INVOKER モデルの両方の組み合わせを使用して、権限付きシステムプロシージャを実行します。この結合モデルでは、16.0 より前の権限付きシステムプロシージャはすべて、SYSTEM PROCEDURE DEFINER モデルを使用して実行され、16.0 (または以降のいずれかのリリース) で導入された権限付きシステムプロシージャは、SYSTEM PROCEDURE INVOKER モデルを使用して実行されます。デフォルトのセキュリティモデルは、データベースの作成時、アップグレード時、またはそれ以降に随時、上書きすることができます。ただし、カスタムのストアドプロシージャおよびアプリケーションの機能が失われることがあるため、これはおすすめしません。

権限付きシステムプロシージャを実行する機能の付与

権限付きシステムプロシージャを実行する機能を付与する際に使用するプロセスは、そのシステムプロシージャが実行されるセキュリティモデルによって異なります。

SYSTEM PROCEDURE DEFINER モデルを使用する権限付きシステムプロシージャの場合は、そのシステムプロシージャに対する EXECUTE オブジェクトレベル権限をユーザに付与します。

```
GRANT EXECUTE ON sys_procedure_name
    TO grantee [,...]
```

SYSTEM PROCEDURE INVOKER モデルを使用する権限付きシステムプロシージャの場合は、そのシステムプロシージャで必要な基礎となるシステム権限をユーザに付与します。 **sp_proc_priv()** を使用して、システムプロシージャの実行に必要なシステム権限を指定します。

```
GRANT system_privilege_name
    TO grantee [,...]
```

参照：

- GRANT EXECUTE 文 (294 ページ)

権限付きシステムプロシージャを実行する機能の取り消し

権限付きシステムプロシージャを実行する機能を取り消す際に使用するプロセスは、そのシステムプロシージャが実行されるセキュリティモデルによって異なります。

SYSTEM PROCEDURE DEFINER モデルを使用する権限付きシステムプロシージャの場合は、そのシステムプロシージャに対する EXECUTE オブジェクトレベル権限をユーザから取り消します。

```
REVOKE EXECUTE ON sys_procedure_name
    FROM grantee [,...]
```

SYSTEM PROCEDURE INVOKER モデルを使用する権限付きシステムプロシージャの場合は、ユーザが持つそのシステムプロシージャで必要な基礎となるシステム権限を取り消します。

```
REVOKE system_privilege_name
    FROM grantee [,...]
```

参照：

- REVOKE EXECUTE 文 (313 ページ)

データベースが使用するセキュリティモデルの特定

データベースが使用できるセキュリティモデルは 2 つあります。

データベースが使用しているセキュリティモデルを特定するには、次の文を実行します。

```
select IF ((HEXTOINT(substring(db_property('Capabilities'),
1,length(db_property('Capabilities'))-20)) & 8) = 8)
THEN 1
ELSE 0
END IF
```

1 は、データベースが SYSTEM PROCEDURE INVOKER モデルを使用していることを示します。0 は、データベースが複合モデルを使用していることを示します。

複合モデルでは、16.0 より前の権限付きシステムプロシージャのみが SYSTEM PROCEDURE DEFINER を使用して実行されます。これらのシステムプロシージャを特定するには、16.0 より前の権限付きシステムプロシージャのリストを参照してください。

新しい、またはアップグレードされた 16.0 以降のデータベースを、SYSTEM PROCEDURE DEFINER モデルを使用してすべてのシステムプロシージャを実行するように設定することはできません。

16.0 より前の権限付きシステムプロシージャ

16.0 より前の権限付きシステムプロシージャのリストです。

複合セキュリティモデルを使用する権限付きシステムプロシージャ

これらの権限付きシステムプロシージャの場合、SYSTEM PROCEDURE DEFINER を使用するようにデータベースが設定されていると、実行するプロシージャに対する EXECUTE オブジェクトレベル権限のみが必要になります。データベースが SYSTEM PROCEDURE INVOKER を使用するように設定されている場合は、各プロシージャで必要とされる個別のシステム権限も必要です。各システムプロシージャの実行に必要なシステム権限については、『リファレンス：ビルディングブロック、テーブル、およびプロシージャ ガイド』を参照してください。

• sa_audit_string • sa_checkpoint_execute • sa_disable_auditing_type • sa_disk_free_space • sa_enable_auditing_type • sa_external_library_unload • sa_flush_cache • sa_list_external_library • sa_server_option • sa_procedure_profile • sa_procedure_profile_summary • sa_table_page_usage • sa_validate • sp_iq_reset_identity • sp_iqaddlogin • sp_iqbackupdetails • sp_iqbackupsummary • sp_iqcardinality_analysis • sp_iqcheckdb • sp_iqcheckoptions • sp_iqclient_lookup • sp_iqcolumn • sp_iqcolumnuse • sp_iqconnection • sp_iqconstraint • sp_iqcontext • sp_iqconstraint • sp_iqcontext • sp_iqcursorinfo • sp_iqdatatype • sp_iqdbsize	• sp_iqdbspace • sp_iqdbspaceinfo • sp_iqdbspaceobjectinfo • sp_iqdbstatistics • sp_iqdroplogin • sp_iqemptyfile • sp_iqestdbspaces • sp_iqestspace • sp_iqevent • sp_iqfile • sp_iqhelp • sp_iqindex • sp_iqindex_alt • sp_iqindexadvice • sp_iqindexfragmentation • sp_iqindexinfo • sp_iqindexmetadata • sp_iqindexsize • sp_iqindexuse • sp_iqlmconfig • sp_iqlocks • sp_iqmodifyadmin • sp_iqmodifylogin • sp_iqmpxcheckdqpconfig • sp_iqmpxdumptlvlog • sp_iqmpxfilestatus • sp_iqmpxincconnpoolinfo • sp_iqmpxincheartbeatinfo • sp_iqcopyloginpolicy • sp_iqmpxincconnpoolinfo • sp_iqmpxincheartbeatinfo	• sp_iqmpxinfo • sp_iqmpxversioninfo • sp_iqobjectinfo • sp_iqpkeys • sp_iqprocedure • sp_iqprocparm • sp_iqrebuildindex • sp_iqrename • sp_iqrestoreaction • sp_iqrowdensity • sp_iqsetcompression • sp_iqsharedtempdistrib • sp_iqshowcompression • sp_iqshowpsexe • sp_iqspaceinfo • sp_iqspaceused • sp_iqstatistics • sp_iqstatus • sp_iqsysmon • sp_iqtable • sp_iqtablesize • sp_iqtableuse • sp_iqtransaction • sp_iqunusedcolumn • sp_iqunusedindex • sp_iqunusedtable • sp_iqversionuse • sp_iqview • sp_iqwho • sp_iqworkmon

呼び出し側の権限を使用する権限付きシステムプロシージャ
これらの 16.0 より前の権限付きシステムプロシージャは、セキュリティモデルの設定に関係なく、そのプロシージャの所有者ではなくそのプロシージャを実行するユーザの権限で実行されます。したがって、システムプロシージャに対する EXECUTE オブジェクトレベル権限 (デフォルトでは PUBLIC ロールのメンバーシップによって付与) のほかに、そのシステムプロシージャに必要な追加のシステ

ム権限が付与されている必要があります。各システムプロシージャの実行に必要なシステム権限については、『リファレンス：ビルディングブロック、テーブル、およびプロシージャ ガイド』を参照してください。

- sa_describe_shapefile
- sa_get_user_status
- sa_locks
- sa_performance_diagnostics
- sa_report_deadlocks
- sa_text_index_stats

パスワード

他のユーザのパスワードを管理する機能をユーザに付与できます。パスワード変更の実行に 1 人または 2 人のユーザが必要となるようにパスワード管理を設定できます。

データベースでのパスワード

バージョン 15.0 時点の SAP Sybase IQ では、パスワードのハッシュ処理に SHA256 が使用されます。パスワードは、UTF-8 で格納されます。

作成または変更したパスワードは、UTF-8 に変換されてからハッシュされ、データベースに保存されます。データベースをアンロードし、別の文字セットを使用するデータベースに再ロードした場合でも、既存のパスワードは機能します。サーバがクライアントの文字セットを UTF-8 に変換できない場合、パスワードには 7 ビット ASCII 文字を使用することをおすすめします。それ以外の文字を使用すると、パスワードが機能しないことがあります。

CHANGE PASSWORD システム権限のユーザへの付与

他のユーザのパスワードの管理をユーザに許可します。

前提条件

- CHANGE PASSWORD システム権限が管理権限付きで付与されている必要があります。
- 指定される各ターゲットユーザ (target_users_list) は、ログインパスワードが設定されている既存のユーザまたはユーザ拡張ロールです。
- 指定された各ターゲットロール (target_roles_list) は、既存のユーザ拡張ロールまたはユーザ定義ロールである必要があります。

手順

データベース内のすべてのユーザ (ANY)、特定のユーザのみ (*target_users_list*)、または特定のロールのメンバー (ANY WITH ROLES *target_roles_list*) のパスワードを

変更する機能をユーザに付与できます。CHANGE PASSWORD システム権限に対する管理権限は、ANY 句を使用する場合のみ付与できます。

句を指定しない場合のデフォルトは ANY、WITH NO ADMIN OPTION です。

CHANGE PASSWORD システム権限を再付与する場合、付与の効果は累積されます。たとえば、`User1` に対して、`User2` と `User3` に限定してこの権限を付与し、さらに `Role1` に限定してこの権限を再付与した場合、`User1` は `User2`、`User3`、および `Role1` の任意のメンバーのパスワードを管理できます。

CHANGE PASSWORD システム権限をユーザに付与する際、ユーザの元の権限が付与される権限よりも上位である場合、元の上位の権限が維持されます。たとえば、この権限を ANY 句を使用して付与した後、*target_users_list* 句を使用して再付与した場合、ANY 句で付与された権限が維持されます。

CHANGE PASSWORD システム権限を付与するには、次のいずれかの文を実行します。

付与タイプ	文
任意のデータベースユーザに完全な管理権限付きで付与する。	**GRANT CHANGE PASSWORD** (**ANY**) **TO** *user_ID* **WITH ADMIN OPTION**
任意のデータベースユーザに管理権限のみ付与する。	**GRANT CHANGE PASSWORD** (**ANY**) **TO** *user_ID* **WITH ADMIN ONLY OPTION**
任意のデータベースユーザに管理権限なしで付与する。	**GRANT CHANGE PASSWORD** (**ANY**) **TO** *user_ID* **WITH NO ADMIN OPTION**
指定したユーザに管理権限なしで付与する。	**GRANT CHANGE PASSWORD** (*target_users_list*) **TO** *user_ID* **WITH NO ADMIN OPTION**

付与タイプ	文
指定したロールの任意のメンバーに管理権限なしで付与する。	**GRANT CHANGE PASSWORD** (**ANY WITH ROLES** *target_roles_list*) **TO** *user_ID* **WITH NO ADMIN OPTION**
指定したユーザまたは指定したロールの任意のメンバーに管理権限なしで付与する。	**GRANT CHANGE PASSWORD** (*target_users_list*), (**ANY WITH ROLES** *target_roles_list*) **TO** *user_ID* **WITH NO ADMIN OPTION**

例:

次の文は、任意のデータベースユーザのパスワードを変更する機能を Sam に付与します。

```
GRANT CHANGE PASSWORD (ANY) TO Sam
or
GRANT CHANGE PASSWORD TO Sam
```

次の文は、Jane、*Joe*、および Laurel のみのパスワードを変更する機能を Sally と Bob に付与します。

```
GRANT CHANGE PASSWORD (Jane, Joe, Laurel) TO Sally, Bob
```

次の文は、Sales1 ロールの任意のメンバーのパスワードを変更する機能を Mary に付与します。

```
GRANT CHANGE PASSWORD (ANY WITH ROLES Sales1) TO Mary
```

次の文は、Joe、Sue、または Sales2 ロールの任意のメンバーのパスワードを変更する機能を Sarah に付与します。

```
GRANT CHANGE PASSWORD (Joe, Sue), (ANY WITH ROLES Sales2) TO Sarah
```

次の文は、Marketing1 ロールまたは Marketing2 ロールの任意のメンバーのパスワードを変更する機能を Joan に付与します。

```
GRANT CHANGE PASSWORD (ANY WITH ROLES Marketing1, Marketing2) TO Joan
```

参照：

- GRANT CHANGE PASSWORD 文 (289 ページ)

ユーザが持つ CHANGE PASSWORD システム権限の取り消し

ユーザが持つ、パスワード管理機能およびシステム権限の管理機能を取り消します。

前提条件

CHANGE PASSWORD システム権限が管理権限付きで付与されている必要があります。

手順

CHANGE PASSWORD システム権限は、異なる句を使用して、特定のユーザに複数回付与することができます。たとえば、`User1` に CHANGE PASSWORD システム権限を ANY 句を使用して付与した後で、*target_users_list* 句を使用して再付与します。複数回付与されている場合、それを取り消すには、**GRANT** 文に指定した同じ形式の句を使用する必要があります。

上の例の場合、ANY 句を使用して `User1` からシステム権限を取り消しても、*target_users_list* 句で付与された権限は有効なままです。最終的に、`User1` の機能は、*target_users_list* で指定されているユーザのパスワードを管理することに制限されます。一方、*target_users_list* 句を使用して `User1` からシステム権限を取り消すと、ANY 句で付与された権限は有効なままです。この場合、最終的に、`User1` はデータベース内の任意のユーザのパスワードを管理する機能を維持できます。

CHANGE PASSWORD システム権限を取り消すには、次のいずれかの文を実行します。

取り消しタイプ	説明
システム権限に対する管理権限のみ取り消す。	**REVOKE ADMIN OPTION FOR CHANGE PASSWORD** (**ANY**) **FROM** *user_ID [,...]*
任意のデータベースユーザのパスワードを管理するシステム権限およびその管理権限を取り消す。	**REVOKE CHANGE PASSWORD** **FROM** *user_ID [,...]*
指定したロールのパスワードを管理するシステム権限を取り消す。	**REVOKE CHANGE PASSWORD** (*target_users_list*) **FROM** *user_ID [,...]*

取り消しタイプ	説明
指定したロールのパスワードを管理するシステム権限を取り消す。	**REVOKE CHANGE PASSWORD** (**ANY WITH ROLES** *target_roles_list*) **FROM** *user_ID [,...]*

例:

次の文はどちらも、任意のデータベースユーザのパスワードを変更する Sam の機能を取り消します。

```
REVOKE CHANGE PASSWORD (ANY) FROM Sam
or
GRANT CHANGE PASSWORD TO Sam
```

ANY 句と WITH ADMIN OPTION 句を使用して CHANGE PASSWORD システム権限が Frank に付与されていることを前提として、次の文は、Frank に付与されているシステム権限の管理機能のみを取り消します。データベース内の任意のユーザのパスワードを変更する機能は維持されます。

```
REVOKE ADMIN OPTION FOR CHANGE PASSWORD (ANY) FROM Frank
```

次の文は、Sally と Bob が持つ、Jane、Joe、および Laurel のみのパスワードを変更する機能を取り消します。

```
REVOKE CHANGE PASSWORD (Jane, Joe, Laurel) FROM Sally, Bob
```

次の文は、Mary が持つ Sales1 ロールの任意のメンバーのパスワードを変更する機能を取り消します。

```
REVOKE CHANGE PASSWORD (ANY WITH ROLES Sales1) FROM Mary
```

次の文は、Sarah が持つ、Joe、Sue、または Sales2 ロールの任意のメンバーのパスワードを変更する機能を取り消します。

```
REVOKE CHANGE PASSWORD (Joe, Sue), (ANY WITH ROLES Sales2) FROM Sarah
```

次の文は、Joan が持つ Marketing1 ロールまたは Marketing2 ロールの任意のメンバーのパスワードを変更する機能を取り消します。

```
REVOKE CHANGE PASSWORD (ANY WITH ROLES Marketing1, Markeing2) FROM
Joan
```

参照：

- REVOKE CHANGE PASSWORD 文 (309 ページ)

パスワードの変更: 単一制御

単一のユーザで別のユーザのパスワードを管理できます。

前提条件

- CHANGE PASSWORD システム権限。
- 管理するユーザにターゲットユーザのパスワードを変更する権限が付与されている。

手順

コマンドプロンプトで次のコマンドを入力します。

```
ALTER USER userID
IDENTIFIED BY password
```

参照：

- ユーザ ID とパスワードの大文字と小文字の区別 (118 ページ)
- ALTER USER 文 (263 ページ)

二重制御パスワード管理オプション

二重制御パスワードオプションでは、ターゲットユーザのパスワードの変更に 2 人の管理ユーザが必要です。これにより、ターゲットユーザのパスワードを 1 人のユーザが知る (または制御する) ことがないようにします。

新しいパスワードの各パートを生成するのに、2 人の管理ユーザが必要とされます。ターゲットユーザの新しいパスワードはこれらの 2 つのパートで構成されます。同じユーザが、両方のパスワードパートを生成することはできません。同じユーザが両方のパスワードパートを定義しようとすると、サーバによりエラーメッセージが表示され、2 つ目のパスワードパートは設定されません。

最初のパスワードパートが指定され、2 つ目のパートはまだ指定されていないところでサーバが再起動しても、最初のパスワードパートは保持されます。2 つ目のパスワードパートが別のユーザによって指定されると、二重パスワード変更プロセスが完了します。その後、ターゲットユーザは組み合わせたパスワードパートを使用してログインできます。

開始後は、ユーザに CHANGE PASSWORD システム権限と、ターゲットユーザのパスワードを管理する権限がある場合、パスワードとして "NULL" を指定することによって、ターゲットユーザの二重パスワードの生成をキャンセルできます。

パスワードパートを設定する各管理ユーザは、ターゲットユーザに新しいパスワードパートと、それが最初のパートであるか、2 つ目のパートであるかを知らせる必要があります。パスワードを使用するには、ターゲットユーザは、最初の

パート、次に 2 つ目のパートという順序で二重パスワードを入力します。各パートに最大 127 文字という制限があります。

二重パスワードの変更プロセスが完了したときにターゲットユーザがログインしていない場合は、そのままログインするだけです。二重パスワードが受け入れられると、ユーザはただちにパスワードを変更するように求められます。これが、パスワードセキュリティの最終段階になります。二重パスワード変更プロセスが完了したときにユーザがログインしている場合、ユーザは **ALTER USER** 文または **GRANT CONNECT** 文、あるいは **sp_password** システムプロシージャまたは **sp_iqpassword** システムプロシージャを使用してパスワードを変更できます。現在のパスワードを要求されたら、現在のセッションで最初に入力したパスワードではなく、新しい二重パスワードを入力します。

パスワード変更二重パスワードオプションはログインポリシーで有効化されます。

参照：

- ユーザ ID とパスワードの大文字と小文字の区別 (118 ページ)
- ALTER USER 文 (263 ページ)
- GRANT CONNECT 文 (291 ページ)
- sp_iqpassword プロシージャ (416 ページ)

パスワード変更の二重制御の有効化

ユーザのパスワードを変更する際に、2 人の管理ユーザからの入力を必要とします。

前提条件

MANAGE ANY LOGIN POLICY OPTION システム権限。

手順

パスワード管理の二重制御は、ログインポリシーの設定オプションです。デフォルトでは、無効 (OFF) です。

このオプションを有効にするには、次の文を実行します。

```
ALTER LOGIN POLICY policy-name
CHANGE_PASSWORD_DUAL_CONTROL=ON
```

参照：

- ALTER LOGIN POLICY 文 (252 ページ)
- CREATE LOGIN POLICY 文 (271 ページ)

パスワードの変更: 二重制御

別のユーザのパスワードの管理に 2 ユーザが必要です。

前提条件

- CHANGE PASSWORD システム権限。
- 管理するユーザにターゲットユーザのパスワードを変更する権限が付与されている。
- CHANGE_PASSWORD_DUAL_CONTROL オプションが管理ユーザのログインポリシーで有効になっている。

手順

1. コマンドプロンプトで、最初の管理ユーザが次のコマンドを入力します。
   ```
   ALTER USER userID
   IDENTIFIED FIRST BY password_part1
   ```
2. コマンドプロンプトで、2 番目の管理ユーザが次のコマンドを入力します。
   ```
   ALTER USER userID
   IDENTIFIED LAST BY password_part1
   ```

例

ログインポリシー `Sales1` の **CHANGE_PASSWORD_DUAL_CONTROL** オプションが有効になっており、`User3` に `Sales1` が割り当てられていて、`User1` と `User2` には `User3` のパスワードを変更するために必要な権限が付与されていると想定して、次の文で `User3` の 2 つのパスワード部分を *NewPassPart1* と *NewPassPart2* に設定します。

User1 は次のコマンドを入力します。

```
ALTER USER user3 IDENTIFIED FIRST BY NewPassPart1
```

User2 は次のコマンドを入力します。

```
ALTER USER user3 IDENTIFIED LAST BY NewPassPart2
```

参照：

- ユーザ ID とパスワードの大文字と小文字の区別 (118 ページ)
- ALTER USER 文 (263 ページ)

同一化

ユーザは、タスクの開始の実行に必要な最小の権限をすでに持っている場合に、一時的に別のユーザの特定のロールとシステム権限を使用して (同一化して) 操作を実行できます。

User1 が主要タスクの実行を担当していますが、手が空いていないとします。User2 は、そのタスクの実行のための十分な権限を持ち、さらに User1 が使用できない追加権限も持っています。User2 がそのタスクを実行した場合、そのタスクは User1 が実行した場合と異なる形で完了する可能性があります。これを回避するために、User2 は一時的に User1 に固有のロールとシステム権限を使用して (同一化して) そのタスクを実行します。

同一化を行うには、最初に SET USER システム権限をユーザに付与してから、SETUSER 文を発行して同一化を開始します。

注意： SET USER システム権限は 2 語で、SETUSER 文は 1 語です。

SET USER システム権限を付与するときに、同一化の範囲を次のいずれかとして定義することができます。

- データベース内の任意のユーザ
- 指定したユーザのリスト内の (*target_users_list*) 任意のユーザ
- 1 つまたは複数の指定したロール (*target_roles_list*) のメンバーである任意のユーザ

別のユーザに同一化するには、同一化するユーザ (被付与者) は、少なくとも、同一化されるユーザ (ターゲット) と同じかそれ以上の管理権限を持つすべてのロールおよびシステム権限が付与されている必要があります。これは、*最小限の*基準と呼ばれます。同一化するユーザは、それ以外のロール、システム権限、またはより上位の管理権限を持っていてもかまいませんが、それ以下であることはできません。*最小限の*基準に違反する結果にならないかぎり、ユーザが別のユーザに同一化している間に、同一化実行者または同一化対象者に対してロールおよび権限の付与または取り消しを行うことができます。付与または取り消しによってこの基準に違反する結果になる場合は、エラーメッセージが表示され、文は失敗します。

たとえば、User1 が正常に User2 に同一化しているとします。User1 に新しいロールを付与しますが、User2 には付与しません。この付与によって User1 が User2 に同一化するための基準に違反する結果にはならない (User1 は引き続き、少なくとも User2 に付与されているものと同じロールと権限を持つ) ため、この付与は成功します。しかし、User1 ではなく User2 に新しいロールを付与した場

合は、User2 が User1 よりも多くのロールを付与されることになるため、この付与文は失敗します。

別のユーザに同一化すると、自分のユーザ ID ではなく、同一化の対象のユーザのユーザ ID が監査ログに表示されます。ただし、同一化 (SETUSER コマンドの発行) も監査ログに記録されるため、タスクを実行したのが被付与者ユーザなのかターゲットユーザなのかは判別できます。

マルチプレックス設定では、コーディネータ上に存在する接続で同一化がアクティブになっていて、最小限の基準に違反するロールおよび権限の付与または取り消しが試行された場合に、アクティブな同一化が含まれている接続は終了します。接続が終了すると同一化も終了し、最小限の基準の違反は問題ではなくなるため、**GRANT** 文または **REVOKE** 文は正常に実行されます。

同一化の要件

特定の一連の基準 (*最小限の*要件とも呼ばれる) が満たされている場合にのみ、ユーザは別のユーザに正常に同一化することができます。

正常な同一化のための基準は次の 4 つです。

1. 同一化実行者にターゲットユーザを同一化する権限が付与されている。
2. 同一化実行者は、少なくともターゲットユーザに付与されているすべてのロールとシステム権限を持っている。
3. 同一化実行者に、同等以上の管理権限付きで上述のロールとシステム権限が付与されている。

   注意： 管理権限の基準を満たすという目的においては、WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は同様の管理権限を付与するものとみなされます。また、両者は、WITH NO ADMIN OPTION 句より上位の管理権限を付与するものとみなされます。たとえば、User1 には WITH ADMIN OPTION 句を指定して Role1 が付与され、User2 には WITH ADMIN ONLY 句を指定して Role1 が付与され、User3 には WITH NO ADMIN OPTION 句を指定して Role1 が付与されているとします。この場合、User1 と User2 には、同様の管理権限を持つ Role1 が付与されているとみなされます。また、User1 と User2 には、User3 より上位の管理権限を持つ Role1 が付与されているとみなされます。
4. ターゲットユーザに拡張をサポートするシステム権限が付与されている場合、そのシステム権限を同一化実行者に付与する際に使用する句が、ターゲットユーザに付与する際に使用した句のスーパーセットである必要があります。拡張をサポートするのは SET USER システム権限と CHANGE PASSWORD システム権限のみです。
   - ANY 句は、*target_roles_list* 句と *target_users_list* 句のスーパーセットとみなされます。ターゲットユーザに ANY 句を使用して SET USER システム権限

が付与されている場合、同一化実行者にも ANY 句を使用して付与されている必要があります。

- ターゲットユーザに *target_roles_list* 句と *target_users_list* 句の両方を使用して SET USER システム権限が付与されている場合、同一化実行者にもその 2 つの句を使用してシステム権限が付与されている必要があり、さらにそれぞれの句のターゲットリストは、その句を使用してターゲットユーザに付与された内容と同等またはそのスーパーセットである必要があります。たとえば、同一化実行者とターゲットユーザのどちらも、ターゲットリストにそれぞれ `User1` と `User2`、および `Role1` と `Role2` が含まれる場合、各句のターゲットリストで付与される内容は同等とみなされます。一方、同一化実行者に対してターゲットリストで付与される内容にそれぞれ `User1` と `User2` および `Role1` と `Role2` が含まれ、ターゲットユーザに対してターゲットリストで付与される内容に `User1` と `Role2` のみが含まれる場合、同一化実行者に対してターゲットリストで付与される内容はターゲットユーザのスーパーセットであるとみなされます。
- ターゲットユーザに 1 つのターゲットリスト句を使用して SET USER システム権限が付与されている場合、同一化実行者のターゲットリストは、ターゲットユーザのリストと同等またはそのスーパーセットである必要があります。たとえば、同一化実行者とターゲットユーザの両方の *target_user_list* に `User1` と `User2` が含まれる場合 (同等) または同一化実行者のリストに `User1` と `User2`、ターゲットユーザのリストに `User2` がそれぞれ含まれる場合です。`User1` と `User2` (同一化実行者のリスト) は `User2` (ターゲットユーザのリスト) のスーパーセットです。
- 定義により、ユーザは常に自分自身を同一化できます。したがって、ターゲットユーザに同一化実行者を同一化する権限が付与されている場合、これは同一化実行者の基準要件である同等またはスーパーセットであることに違反しません。たとえば、`User3` が同一化実行者、`User4` がターゲットユーザであり、`User3` の *target_user_list* には、`User4` と `User5` が含まれています。`User4` の *target_user_list* には、`User3` と `User5` が含まれています。このターゲットリストから同一化実行者を削除した場合、`User3` のターゲットリストは基準要件を満たします。

シナリオ 1

基準 2 と基準 3 が満たされていると仮定して、次のシナリオを検討します。

- *User1*、*User2*、*User3*、*User4*、および *User5* の 5 人のユーザが存在するとします。
- *Role1* と *Role2* の 2 つのロールがあります。
- *User1* には、ANY 句を使用して SET USER システム権限が付与されています。

- *User2* には、*User1* および *User4* の *target_users_list* 句を使用して SET USER システム権限が付与されています。
- *User3* には、*User1*、*User2*、*User4*、および *User5* の *target_users_list* 句と、*Role1* および *Role2* の ANY WITH ROLES *target_roles_list* 句を使用して SET USER システム権限が付与されています。
- *User4* には、ANY 句および *Role1* の *target_roles_list* 句を使用して SET USER システム権限が付与されています。
- *User5* には、*User4* の *target_users_list* 句と、*Role1* の ANY WITH ROLES *target_roles_list* 句を使用して、SET USER システム権限が付与されています。

User1 と *User4* は、それぞれ ANY 句を使用して SET USER システム権限が付与されているため、*User2*、*User3*、および *User5* に正常に同一化することができます (基準 4)。

User1 と *User4* は、それぞれ ANY 付与があるため、相互に同一化できます (基準 4)。

User2、*User3*、および *User5* は、ANY 付与がないため、*User1* または *User4* に同一化できません (基準 4)。

User2 は、次の理由により *User3* または *User5* に同一化できません。

- *User2* には、これらのユーザに同一化する権限が付与されていない (基準 1)。
- SET USER システム権限が、*target_roles_list* 句を指定して *User2* に付与されていない (基準 4)。

User3 は、次の理由により正常に *User2* に同一化できます。

- *User3* には、*target_users_list* 句を指定して *User2* に同一化する権限が付与されている (基準 1)。
- *User3* の *target_users_list* 句は、*User2* のスーパーセットである (基準 4)。*User3* には *target_role_list* 句による付与がありますが、User2 には同じ付与がないため、この付与は *User2* への同一化の要件を満たすために必要なものではありません。

User3 は、次の理由により正常に *User5* に同一化できます。

- *User3* には、*target_users_list* 句を指定して *User5* に同一化する権限が付与されている (基準 1)。
- *User3* の *target_users_list* 句リストは、*User5* のスーパーセットである (基準 4)。
- *User3* と *User5* の *target_roles_list* 句リストが同等である (基準 4)。

User5 は、次の理由により他のユーザに同一化できません。

- *User1* と *User4* に ANY 付与がある (基準 4)。
- *User2* と *User3* に、*User5* に付与されたもののサブセットではない *target_users_list* 句による付与がある (基準 4)。
- *User3* に、サブセットではない *target_roles_list* 句による付与がある (基準 4)。

シナリオ 2
基準 1 と基準 4 が満たされていると仮定して、次を検討します。

- *User6* と *User7* の 2 人のユーザがいるとします。
- *Role4* と *Role5* の 2 つのロールがあります。
- *User6* には、WITH ADMIN OPTION 句を含む *Role4*、WITH ADMIN ONLY OPTION 句を含む *Role5*、および WITH ADMIN OPTION 句を含む MANAGE ANY USER システム権限が付与されています。
- *User7* には、WITH ADMIN OPTION 句を含む *Role4* と WITH NO ADMIN OPTION 句を含む *Role5* が付与されています。

User6 は、次の理由により正常に *User7* に同一化できます。

- *User6* と *User7* にはいずれも *Role4* と *Role5* が付与されている。*User6* に追加の権限 (MANAGE ANY USER システム権限) が付与されていることは問題にならない (基準 2)。
- *User6* には、*User7* と同等の管理権限を含む *Role4* が付与されている。*User6* には、*User7* より上の管理権限を含む *Role5* が付与されている (基準 3)。

User7 は、次の理由により *User6* に同一化できません。

- *User7* には *Role4* と *Role5* が付与されているが、MANAGE ANY USER システム権限が付与されていない (基準 2)。
- *User7* には、*User6* より下位の管理権限を含む *Role5* が付与されている (基準 3)。

シナリオ 3
次を検討します。

- *User8*、 *User9*、および *User10* の 3 人のユーザがいるとします。
- *Role5* と *Role6* の 2 つのロールがあります。
- *User8* には、WITH ADMIN OPTION 句を含む *Role5* と WITH ADMIN OPTION 句を含む MANAGE ANY USER システム権限が付与されています。
- *User9* および *User10* には、WITH NO ADMIN OPTION 句を含む *Role5* が付与されています。
- *User8* には、*target_users_list* 句を含み、*User9* と *User10* に同一化するための SET USER システム権限が付与されています。

- *User9*には、*target_users_list*句を含み、*User10*に同一化するためのSET USERシステム権限が付与されています。

*User8*は、次の理由により正常に*User9*に同一化できます。

- *User8*には、*target_users_list*句を指定して*User9*に同一化する権限が付与されている (基準 1)。
- *User8*の*target_users_list*句リストは、*User9*のスーパーセットである (基準 4)。
- *User8*と*User9*はともに*Role5*を付与され、*User8*には*User9*より上のこのロールに対する管理権限が付与されている (基準 2 および 3)。

*User8*は、次の理由により正常に*User10*に同一化できます。

- *User8*には、*User10*に同一化するための権限が付与されている (基準 1)。
- *User10*にはSET USERシステム権限が付与されていないので、要件 4 が適用されない
- *User8*と*User10*はともに*Role5*を付与され、このロールに対して同じ管理権限を持つ (基準 2 および 3)。

*User9*は、次の理由により*User8*に同一化できません。

- *User9*には、*User8*に同一化するための権限が付与されていない (基準 1)。
- *User8*と*User9*にはともに*Role5*が付与されているが、*User9*に付与されたこのロールへの管理権限は、*User8*に付与された権限より下位である (基準 3)。

基準の検証は、SET USERシステム権限が付与されるときではなく、SETUSER文の実行時に行われます。SETUSER文の発行時にいずれかの基準をユーザが満たしていないと、「パーミッションがありません」というメッセージが表示され、同一化は開始されません。

SET USERシステム権限のユーザへの付与

データベースの別のユーザに同一化することを特定のユーザに許可します。このシステム権限は、管理権限付きまたはなしで付与できます。

前提条件

- SET USERシステム権限が管理権限付きで付与されている必要があります。
- 指定される各ターゲットユーザ (target_users_list) は、ログインパスワードが設定されている既存のユーザまたはユーザ拡張ロールです。
- 指定された各ターゲットロール (target_roles_list) は、既存のユーザ拡張ロールまたはユーザ定義ロールである必要があります。

手順

データベース内のすべてのユーザ (ANY)、特定のユーザのみ (*target_users_list*)、または特定のロールのメンバー (ANY WITH ROLES *target_roles_list*) に同一化する権

限をユーザに付与できます。SET USER システム権限に対する管理権限は、ANY 句を使用する場合のみ付与できます。

句を指定しない場合は、ANY がデフォルトです。

SET USER システム権限をユーザに再付与する場合、付与の効果は累積されます。

ANY 句を使用するときに管理句を指定しない場合は、WITH NO ADMIN OPTION がデフォルトです。

target_users_list 句または *target_roles_list* 句を指定する場合は、WITH NO ADMIN OPTION が唯一有効な管理句です。

SET USER システム権限を付与するには、次のいずれかの文を実行します。

付与タイプ	文
任意のデータベースユーザを同一化するシステム権限を 完全な管理権限付きで付与する。	**GRANT SET USER** (**ANY**) TO *user_ID [,...]* **WITH ADMIN OPTION**
任意のデータベースユーザを同一化するシステム権限を 管理権限のみで付与する。	**GRANT SET USER** (**ANY**) TO *user_ID [,...]* **WITH ADMIN ONLY OPTION**
任意のデータベースユーザを同一化するシステム権限を 管理権限なしで付与する。	**GRANT SET USER** (**ANY**) TO *user_ID [,...]* **WITH NO ADMIN OPTION**
指定したユーザを 同一化するシステム権限を付与する。	**GRANT SET USER** (*target_users_list*) TO *user_ID [,...]*
指定したロールの任意のメンバーを 同一化するシステム権限を付与する。	**GRANT SET USER** (**ANY WITH ROLES** *target_roles_list*) TO *user_ID [,...]*

付与タイプ	文
指定したユーザと指定したロールのメンバーを同一化するシステム権限を付与する。	**GRANT SET USER** (*target_users_list*), (**ANY WITH ROLES** *target_roles_list*) TO *user_ID [,...]*

例:

次の文はどちらも、任意のデータベースユーザを同一化する機能を *Sam* に付与します。

```
GRANT SET USER (ANY) TO Sam
or
GRANT SET USER TO Sam
```

次の文は、*Mary*、*Joe*、または *Sue* のみを同一化する機能を *Bob* と *Jeff* に付与します。

```
GRANT SET USER (Mary, Joe, Sue) TO Bob, Jeff
```

次の文は、*Sales1* ロールの任意のメンバーを同一化する機能を *Mary* に付与します。

```
GRANT SET USER (ANY WITH ROLES Sales1) TO Mary
```

次の文は、*Joe* または *Sue*、または *Sales2* ロールの任意のメンバーを同一化する機能を *Sarah* に付与します。

```
GRANT SET USER (Joe, Sue), (ANY WITH ROLES Sales2) TO Sarah
```

次の文は、*Marketing1* ロールまたは *Marketing2* ロールの任意のメンバーを同一化する機能を *Joan* に付与します。

```
GRANT SET USER (ANY WITH ROLES Marketing1, Marketing2) TO Joan
```

参照：

- GRANT SET USER 文 (302 ページ)

別のユーザへの同一化の開始

別のユーザとまったく同じロールとシステム権限を使用 (同一化) することをユーザに許可します。同一化の効果は、同一化を終了するか、現在のセッションが終了するまで持続します。

前提条件
同一化実行者とターゲットユーザが同一化のすべての要件を満たしている必要があります。「同一化の要件について」を参照してください。

手順

最小限の条件の検証は、SET USER システム権限が付与されるときではなく、SETUSER コマンドの実行時に行われます。SETUSER コマンドを実行すると、同一化するユーザが最小限の条件のいずれかを満たしていない場合、「パーミッションがありません」というメッセージが表示され、同一化は開始されません。ただし、その後の SETUSER の実行時に最低限の条件がすべて満たされると、同一化が開始されます。

SETUSER 文を発行して同一化が開始すると、手動でその同一化を終了するか、別のユーザへの同一化を開始するか、または現在のセッションが終了するまで、同一化の効果は持続します。同一化の最低限の条件に違反する結果にならないかぎり、ユーザが別のユーザに同一化している間に、同一化実行者または同一化対象者に対してロール、権限、およびそれらに関連する管理権限の付与または取り消しを行うことができます。付与または取り消しによってこの基準に違反する結果になる場合は、エラーメッセージが表示され、文は失敗します。必要なタスクを実行したらすぐに同一化を終了することをおすすめします。

コマンドプロンプトで次のコマンドを入力します。

```
SETUSER userID
```

参照：
- SETUSER 文 (328 ページ)
- 同一化の要件 (105 ページ)

ユーザの現在の同一化ステータスの検証

正常に開始された同一化は、手動で終了するか、セッションの終了時まで有効になります。

現在の同一化ステータスを検証するには、SETUSER コマンドが発行されたマシン上で次のコマンドを実行します。

```
SELECT CURRENT USER
```

このコマンドは、現在ログイン中のユーザとしてマシンが認識しているユーザ名を返します。これがそのマシンで予期されるユーザである場合、そのマシン上で

同一化はアクティブではありません。予期されないユーザ名が表示された場合、マシン上で現在同一化されているユーザであることを示します。

例
Joe がログインしている接続で、次のコマンドを実行します。

```
> select current user
> go
current user
------------------------------------------------------------------
------------------------------------------------------------
Joe

(1 row affected)

>setuser mary
>go
>select current user
> go
current user
------------------------------------------------------------------
------------------------------------------------------------
Mary
```

別のユーザへの同一化の終了

マシンで行われている別のユーザの同一化を終了します。別のユーザへの同一化を開始したら、その効果は、同一化を終了するか、現在のセッションが終了するまで持続します。

前提条件
SETUSER コマンドは、このコマンドが開始された接続と同じ接続から発行する必要があります。

手順
コマンドプロンプトで次のコマンドを入力します。

```
SETUSER
```

参照：
- SETUSER 文 (328 ページ)

ユーザが持つ SET USER システム権限の取り消し

ユーザが持つ、他のユーザを同一化する機能および SET USER システム権限を管理する機能を取り消します。

前提条件
SET USER システム権限が管理権限付きで付与されている必要があります。

手順

SET USER システム権限は、異なる句を使用して、特定のユーザに複数回付与することができます。たとえば、`User1` に SET USER システム権限を ANY 句を使用して付与した後で、target_users_list 句を使用して再付与します。複数回付与されている場合、それを取り消すには、GRANT に指定した同じ形式の句を使用する必要があります。ANY 句を使用して `User1` からシステム権限を取り消しても、*target_users_list* 句で付与された権限は有効なままです。最終的に、User1 の機能は *target_users_list* で指定されているユーザを同一化することに制限されます。一方、*target_users_list* 句を使用して `User1` からシステム権限を取り消すと、ANY 句で付与された権限は有効なままです。この場合、最終的に、`User1` はデータベース内の任意のユーザを同一化する機能を維持できます。

注意： 上の例では、User1 は同一化が正常終了するための条件をすべて満たしているものとします。

SET USER システム権限を取り消すには、次のいずれかの文を実行します。

取り消しタイプ	説明
システム権限に対する管理権限のみ取り消す。	**REVOKE ADMIN OPTION FOR SET USER** (**ANY**) **FROM** *user_ID [,...]*
任意のデータベースユーザを同一化するシステム権限およびその管理権限を取り消す。	**REVOKE SET USER** FROM**FROM** *user_ID [,...]*
指定した同一化するシステム権限を取り消す。	**REVOKE SET USER** (*target_users_list*) **FROM** *user_ID [,...]*
指定したロールを同一化するシステム権限を取り消す。	**REVOKE SET USER** (**ANY WITH ROLES** *target_roles_list*) **FROM** *user_ID [,...]*

例:

次の文は、*Sam* の持つ任意のデータベースユーザを同一化する機能を取り消します。

```
REVOKE SET USER (ANY) FROM Sam
or
REVOKE SET USER FROM Sam
```

次の文は、*Frank* の持つ SET USER システム権限に対する管理権限のみを取り消します。*Frank* は引き続きデータベース内の任意のユーザを同一化できます。

```
REVOKE ADMIN OPTION FOR SET USER (ANY) FROM Frank
```

次の文は、*Bob* と *Jeff* の持つ *Mary*、*Joe*、または *Sue* のみを同一化する機能を取り消します。

```
REVOKE SET USER (Mary, Joe, Sue) FROM Bob, Jeff
```

次の文は、*Mary* の持つ *Sales1* ロールの任意のメンバーを同一化する機能を 取り消します。

```
REVOKE SET USER (ANY WITH ROLES Sales1) FROM Mary
```

次の文は、*Sarah* の持つ *Joe* または *Sue*、または *Sales2* ロールの任意のメンバーを同一化する機能を取り消します。

```
REVOKE SET USER (Joe, Sue), (ANY WITH ROLES Sales2) FROM Sarah
```

次の文は、*Joan* の持つ *Marketing1* ロールまたは *Marketing2* ロールの任意のメンバーを同一化する機能を取り消します。

```
REVOKE SET USER (ANY WITH ROLES Marketing1, Markeing2) FROM Joan
```

参照：

- REVOKE SET USER 文 (319 ページ)

ユーザ

ユーザ管理には、ユーザ ID の作成と削除、およびパスワードの管理が含まれます。

DBA ユーザ

DBA ユーザは、新しい SAP Sybase IQ データベースの作成時に作成されるデフォルトユーザです。

DBA ユーザの初期パスワードは "sql" に設定されます。データベース作成時にデフォルトのユーザ名またはパスワードを上書きするには、DBA USER 句または DBA PASSWORD 句を指定して **CREATE DATABASE** 文を使用します。

注意： データベースの作成時にデフォルトのパスワードを上書きしない場合、できるだけ早くパスワードを変更することを強くおすすめします。

デフォルトでは、DBA ユーザに SYS_AUTH_DBA_ROLE ロールの管理権限が自動的に付与され、次に SYS_AUTH_SA_ROLE ロールと SYS_AUTH_SSO_ROLE ロールが付与されます。これらのロールの組み合わせによって DBA ユーザにデータ

ベース内のすべてのシステム権限およびオブジェクトレベル権限が付与されます。これらの権限により、DBA はデータベース上のあらゆるアクティビティ、テーブルの作成、テーブル構造の変更、新しいユーザ ID の作成、ユーザからの権限の取り消しなどを実行できるようになります。

データベースのセキュリティとアカウンタビリティを確保するには、最初のユーザ ID として "dba"などの汎用名を使用しないようにします。実際のユーザのログイン名と強力なパスワードを使用してください。

SYS_AUTH_DBA_ROLE ロールが付与されたユーザ
特定の状況においては、SYS_AUTH_DBA_ROLE ロールの基礎となるロールは削除可能であり、SYS_AUTH_SA_ROLE ロールと SYS_AUTH_SSO_ROLE ロールの基礎となるシステム権限は取り消し可能です。ただし、SAP Sybase IQ のマニュアルでは、DBA ユーザがデータベース管理者であり、基礎となるロールとシステム権限はすべてデフォルトで付与されたものが保持されると想定しています。

アクティブな DBA ユーザのパスワードの紛失を防ぐために、1 つ以上の追加の DBA アカウントを (ランダム生成されるユーザ名とパスワードで) 作成し、このクレデンシャルを厳重に保管しておきます。アクティブな DBA パスワードが紛失された場合、追加のクレデンシャルのいずれかを使用してその DBA アカウントにログインし、元のアカウントパスワードをリセットします。

新しいユーザの追加
DBA は新しいユーザをデータベースに追加できます。新しいユーザには、承認済みタスクをデータベース上で実行するための権限が付与されます。DBA の責任を他のユーザ ID に分散することはできますが、SYS_AUTH_DBA_ROLE ロールによるデータベース全体の管理は DBA の責任です。

DBA はデータベースオブジェクトを作成して、他のユーザ ID にこれらのオブジェクトの所有権を割り当てることができます。

大文字と小文字を区別するデータベースでの DBA ユーザ ID
ユーザ ID とパスワードはデータベースオブジェクトです。

DBA パスワードの変更
DBA ユーザのすべてのデータベースに対するデフォルトのパスワードは、`sql` です。データベースに対する不正なアクセスを防ぐために、このパスワードを変更します。

前提条件

CHANGE PASSWORD システム権限。

ヒント： **dbisql** を使用している場合は、付与された権限をコマンドファイルに保管し、権限の変更、再実行、再作成時に必要に応じて参照できるようにしてください。

手順

ユーザパスワードを変更するには、次のように実行します。

```
ALTER USER userID
IDENTIFIED BY password
```

参照：

- ユーザ ID とパスワードの大文字と小文字の区別 (118 ページ)
- ALTER USER 文 (263 ページ)

スーパユーザ

スーパーユーザは、あらゆるシステム権限を行使し、あらゆるロールを管理することができます。つまり、システム内であらゆる権限付き操作を実行できます。ロールベースのセキュリティでは、データベースの管理にスーパーユーザを必要としません。そのため、DBA ユーザがスーパーユーザでないことがあります。

デフォルトでは、DBA ユーザは任意のシステム権限を行使できますが、ユーザ定義ロールのすべてを管理できるとはかぎらないため、真のスーパーユーザとは見なされません。SAP Sybase IQ では、新しいデータベースまたは移行されたデータベースでのスーパーユーザの自動作成は行われません。

スーパユーザを作成するには、ユーザを作成して SYS_AUTH_DBA_ROLE 互換ロールを付与します。

注意： SYS_AUTH_DBA_ROLE を移行した場合は、SYS_AUTH_DBA_ROLE の基礎となるデフォルトのシステム権限 のすべてを管理権限付きで手動で付与して、スーパユーザを作成する必要があります。

スーパーユーザを作成した後は、スーパーユーザステータスを保持するために、すべての新しいユーザ拡張ロールおよびユーザ定義ロールを管理権限付きでスーパーユーザに付与する必要があります。

DBA ユーザがスーパユーザとして操作できるようにするには、すべての新しいユーザ拡張ロールおよびユーザ定義ロールを管理権限付きで DBA ユーザに付与する必要があります。

管理権限は、ロール管理者またはグローバルロール管理者の形式で付与できます。

パスワードのセキュリティの強化

パスワードは、データベースのセキュリティシステムの重要な部分です。パスワードのセキュリティを強化するには、いくつかのオプションがあります。

- **ログインポリシーの実装** – パスワードの変更頻度を制御し、アカウントがロックされるまでに実行可能なログイン試行回数を指定するか、パスワードの有効期限切れを強制します。「ログインポリシー」を参照してください。
- **パスワードの最小長の実装** – デフォルトでは、パスワードは任意の長さで指定できます。セキュリティを強化するために、すべての新しいパスワードに必要な最小長を設定して、短い (したがって、推測しやすい) パスワードを禁止することができます。推奨される最小長は 6 です。「MIN_PASSWORD_LENGTH」を参照してください。
- **パスワードルールの実装** – パスワードにおける特定の種類の文字の要求、パスワードの再使用の禁止、パスワードの有効期限の適用などを含む詳細なパスワードルールを実装します。ルールの検証は、新しいユーザ ID の作成時、またはパスワードの変更時に行われます。「VERIFY_PASSWORD_FUNCTION」を参照してください。

参照：

- ログインポリシー (125 ページ)
- VERIFY_PASSWORD_FUNCTION オプション (337 ページ)
- MIN_PASSWORD_LENGTH オプション (340 ページ)

データベースでのパスワード

バージョン 15.0 時点の SAP Sybase IQ では、パスワードのハッシュ処理に SHA256 が使用されます。パスワードは、UTF-8 で格納されます。

作成または変更したパスワードは、UTF-8 に変換されてからハッシュされ、データベースに保存されます。データベースをアンロードし、別の文字セットを使用するデータベースに再ロードした場合でも、既存のパスワードは機能します。サーバがクライアントの文字セットを UTF-8 に変換できない場合、パスワードには 7 ビット ASCII 文字を使用することをおすすめします。それ以外の文字を使用すると、パスワードが機能しないことがあります。

ユーザ ID とパスワードの大文字と小文字の区別

パスワードの大文字と小文字の区別は、他の識別子とは異なります。

SAP Sybase IQ と SAP Sybase SQL Anywhere® では、データベース自体の大文字小文字の区別の設定にかかわりなく、新しく作成されたデータベース内のパスワードではすべて大文字と小文字が区別されます。デフォルトのユーザ ID は DBA です。このユーザのパスワードは小文字の *sql* です。

既存のデータベースを再構築する場合、SAP Sybase IQ および SQL Anywhere でのパスワードの大文字と小文字の区別は、次のように決まります。

- 元々大文字小文字の区別がないデータベースで入力されたデータベースの場合は、パスワードの大文字小文字の区別は元通り無視されます。
- 元々大文字小文字の区別があるデータベースに入力されたパスワードでは、大文字のみのパスワードと大文字小文字が混在しているパスワードの大文字小文字の区別が維持されます。すべて小文字で入力されていたパスワードには、大文字小文字の区別が適用されません。
- 既存のパスワードでも新しいパスワードでも、変更されると大文字と小文字の区別が有効になります。

SAP Adaptive Server® Enterprise では、ユーザ ID とパスワードの大文字と小文字の区別は、サーバの大文字と小文字の区別に従います。

新規ユーザの作成

新しいユーザ ID を作成します。

前提条件

MANAGE ANY USER システム権限。

手順

新しいユーザを作成するには、次のように実行します。

```
CREATE USER userID
IDENTIFIED BY password
```

例:

次の文は、ユーザ ID `Joe`、パスワード `welcome` のユーザをデータベースに追加します。

```
CREATE USER Joe
IDENTIFIED BY welcome
```

参照：

- CREATE USER 文 (282 ページ)

ユーザの削除

データベースからユーザ ID を削除します。

前提条件

- MANAGE ANY USER システム権限が必要。

- 削除するユーザは、データベースオブジェクトを所有していないこと。また、現在データベースに接続していないこと。

手順
削除するユーザに外部ログインが定義されている場合、プロセスの一部としてその外部ログインが削除されます。ただし、リモートサーバ上に関連オブジェクトが存在しても、それらは削除されません。
ユーザを削除するには、次の文を実行します。

```
DROP USER userID
```

注意：
- ユーザを削除すると、このユーザが付与したパーミッションもすべて削除されます。
- 削除するユーザがデータベースにオブジェクトを所有している場合、次のエラーメッセージが表示され、コマンドは失敗します。

```
Cannot drop a user that owns tables in runtime system
SQLCODE=-128, ODBC 3  State="42000"
    Line 1, column 1
```

例:

次の文は、データベースからユーザ ID Joe を削除します。

```
DROP USER Joe
```

参照：
- DROP USER 文 (288 ページ)

ユーザパスワードの変更

別のユーザのパスワードを変更します。

前提条件
CHANGE PASSWORD システム権限が必要です。

手順

パスワードルール (**MIN_PASSWORD_LENGTH** オプション) を設定して、割り当てられた新規パスワードがルールに従っていることを確認します (**VERIFY_PASSWORD_FUNCTION** オプション)。たとえば、パスワードに数字 1 つを含めること、ユーザ ID と同じにはできないことなどを指定できます。

ユーザパスワードを変更するには、次のように実行します。

```
ALTER USER user_ID
IDENTIFIED BY password
```

例:

次の文は、新しいパスワード `P&ssW0rd` をユーザ `M_Smith` に割り当てます。

```
ALTER USER M_Smith IDENTIFIED BY P&ssW0rd
```

参照：

- ユーザ ID とパスワードの大文字と小文字の区別 (118 ページ)
- ALTER USER 文 (263 ページ)
- VERIFY_PASSWORD_FUNCTION オプション (337 ページ)
- MIN_PASSWORD_LENGTH オプション (340 ページ)

ユーザ拡張ロールからユーザへの逆変換

ユーザ拡張ロールを変換して、通常のユーザに戻すことができます。

前提条件

変換するユーザ拡張ロールに対する管理権限。

手順

ユーザ拡張ロールに付与されているログイン権限、システム権限、およびロールはすべて、ユーザに付与されます。ユーザがロールとして動作するように拡張された後で作成されたオブジェクトは、ユーザが所有者になります。ユーザ拡張ロールのメンバーはすべて、すぐに取り消されます。

常に、ログインパスワードが設定されているロール管理者またはグローバルロール管理者がロールごとに最小数 (**MIN_ROLE_ADMINS** データベースオプションで定義) 存在する必要があります。ユーザ拡張ロールを変換してユーザに戻す場合、ユーザ拡張ロールの依存ロールはすべて引き続きこの最小要件を満たす必要があります。満たさない場合、変換は失敗します。

ユーザ拡張ロールを変換してユーザに戻すには、次のどちらかの文を実行します。

変換条件	文
ロールにメンバーが まったく付与されていない。	**DROP ROLE FROM USER** *role_name*
ロールにメンバーが 付与されている。	**DROP ROLE FROM USER** *role_name* **WITH REVOKE**

参照：

- DROP ROLE 文 (286 ページ)

ユーザアカウントの永続的なロック

特定のユーザアカウントを永続的にロックするには、lockedオプションをONに設定したログインポリシーをアカウントに割り当てる必要があります。無効にされたユーザアカウントは、SAP Sybase IQ サーバに接続できません。

前提条件

- ログインポリシーを作成または変更するには、MANAGE ANY LOGIN POLICY システム権限が必要。
- ユーザにログインポリシーを割り当てるには、MANAGE ANY USER システム権限が必要。

手順

1. LOCKED オプションを ON に設定して、ログインポリシーを作成します。
2. **ALTER USER** コマンドを実行して、無効にするユーザアカウントにログインポリシーを割り当てます。

   注意： ユーザにログインポリシーを割り当てる際に、同一の **ALTER USER** コマンド内で複数のユーザ名を指定することはできません。

例:

次のコマンドは、`LOCKED` オプションを ON に設定して `lp_locked_users` という名前の新規ログインポリシーを作成します。

```
CREATE LOGIN POLICY lp_locked_users locked=ON
```

次のコマンドは、`lp_locked_users` ログインポリシーをユーザ `John` と `Mary` に割り当てます。これによって、`John` と `Mary` はログインできなくなります。

```
ALTER USER john LOGIN POLICY lp_locked_users
ALTER USER Mary LOGIN POLICY lp_locked_users
```

参照：

- ユーザアカウントの自動ロック解除 (124 ページ)
- ALTER USER 文 (263 ページ)
- CREATE LOGIN POLICY 文 (271 ページ)

ユーザアカウントのロック解除

ユーザアカウントのロックを解除します。

前提条件
MANAGE ANY USER システム権限が必要です。

手順
次のいずれかを行います。

アカウントロックの理由	タスク
locked オプションが ON に設定されたログインポリシーを割り当てたためにユーザアカウントがロックされている	locked オプションが OFF に設定されたログインポリシーをユーザに割り当てなおす。
MAX_FAILED_LOGIN_ATTEMPTS または MAX_DAYS_SINCE_LOGIN の指定を超えたためにユーザアカウントがロックされている	RESET LOGIN POLICY オプションを指定して **ALTER USER** 文を発行する。ログインポリシーを強制的にリセットすると、ユーザのログインの設定がログインポリシーの元の値に戻ります。通常はこれで、ログイン失敗回数の超過または最終ログイン後の最大日数の超過によって暗黙的に設定されたすべてのロックが解除されます。 **注意：** 特定のユーザに割り当てられたログインポリシーの値をリセットしても、同じログインポリシーが割り当てられている全ユーザの値がリセットされることはありません。

例

ログインポリシー `lp` で、LOCKED オプションが OFF に設定されているとします。この場合に次の例を使用すると、`John` に現在割り当てられているログインポリシーが、ログインポリシー `lp` に置き換えられます。

```
ALTER USER john LOGIN POLICY lp
```

MAX_FAILED_LOGIN_ATTEMPTS または MAX_DAYS_SINCE_LOGIN の指定を超えたために `John's` のアカウントがロックされているとします。この場合に次の例を使用すると、`John` に現在割り当てられているログインポリシーの値のリセットが強制的に実行されます。

```
ALTER USER john RESET LOGIN POLICY
```

参照：
- ユーザアカウントの自動ロック解除 (124 ページ)
- ALTER LOGIN POLICY 文 (252 ページ)
- ALTER USER 文 (263 ページ)

ユーザアカウントの自動ロック解除

MANAGE ANY USER システム権限を持つすべての管理ユーザがログイン試行に失敗したためにデータベースからロックアウトされた場合、データベースサービスの一部またはすべてがロックダウンすることがあります。

ユーザアカウントは、ログインポリシーで定義されたログイン失敗の最大試行回数制限 (MAX_FAILED_LOGIN_ATTEMPTS) を超過すると、自動的にロックされます。いったんロックされると、そのアカウントは、MANAGE ANY USER システム権限が付与されたユーザによってマニュアルでロック解除する必要があります。ただし、MANAGE ANY USER システム権限を持つすべてのユーザがログイン試行失敗によってロックアウトされると、データベースサービスの一部またはすべてがロックダウンする可能性があります。

このシナリオを回避するには、次のログインポリシーオプションを使用します。

- **ROOT_AUTO_LOCK_TIME –** MANAGE ANY USER システム権限を持つユーザの自動ロック解除時間を定義します。ルートログインポリシーで root_auto_lock_time を小さな値に設定できます (例: 15 分)。サーバには数時間という上限が設定されています。
- **AUTO_UNLOCK_TIME –** 他のすべてのユーザの自動ロック解除時間を定義します。ルートログインポリシーをはじめとした任意のログインポリシーで AUTO_UNLOCK_TIME を UNLIMITED (デフォルト値) に設定します。

これら値の設定には、MANAGE ANY LOGIN POLICY システム権限が必要です。

ユーザに付与されたパーミッションにもとづいて、これらのログインポリシーオプションのいずれかがロック解除の際に検証されます。自動ロック解除は、ログイン試行の失敗によってロックされたアカウントにのみ適用され、他の理由によってロックされたアカウントには適用されません。ユーザのロックステータスはログイン時に検証され、そのユーザが指定された自動ロック解除時間と同じかこれを超えている場合、そのユーザはログインを許可され、FAILED_LOGIN_ATTEMPTS カウンタがゼロにリセットされます。

参照：
- ロール管理者の最小数 (21 ページ)
- ユーザアカウントのロック解除 (123 ページ)
- ユーザアカウントの永続的なロック (122 ページ)
- ALTER LOGIN POLICY 文 (252 ページ)

- ALTER USER 文 (263 ページ)

ログインポリシー

*ログインポリシー*は、SAP Sybase IQ でユーザ接続の確立時に適用されるルールを定義します。各ログインポリシーは、ログインポリシーオプションと呼ばれるオプションのセットに関連付けられています。

いずれかのマルチプレックスサーバログイン管理コマンドを実行すると、そのコマンドはマルチプレックス内のすべてのサーバに自動的に伝達されます。最高のパフォーマンスを実現するには、これらのコマンドまたは DDL をコーディネータで実行します。

ルートログインポリシーの変更

ルートログインポリシーのオプション値は変更できますが、ポリシーの削除はできません。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順
新しいデータベースはそれぞれ、ルートポリシーと呼ばれるデフォルトのログインポリシーで作成されます。ログインポリシーを指定しないでユーザアカウントを作成した場合、そのユーザはルートログインポリシーに属します。
ルートログインポリシーのオプションを変更するには、以下を実行します。

```
ALTER LOGIN POLICY ROOT {login_policy_options}
```

参照：
- ALTER LOGIN POLICY 文 (252 ページ)
- ログインポリシーオプション (273 ページ)
- マルチプレックスログインポリシーの設定 (259 ページ)
- LDAP ログインポリシーオプション (258 ページ)

新しいログインポリシーの作成

ログインポリシーの作成時に明示的に設定されなかったオプションは、その値をルートログインポリシーから継承します。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順
ログインポリシー名はユニークである必要があります。追加するログインポリシー名が既存の場合には、エラーメッセージが表示されます。
新しいログインポリシーを作成するには、以下を実行します。

```
CREATE LOGIN POLICY policy_name {login_policy_options}
```

例:

次の文では、Test1 ログインポリシーが作成され、PASSWORD_LIVE_TIME オプションが 60 日に設定されます。

```
CREATE LOGIN POLICY Test1
password_life_time=60
```

参照：
- CREATE LOGIN POLICY 文 (271 ページ)
- ログインポリシーオプション (273 ページ)
- マルチプレックスログインポリシーの設定 (259 ページ)
- LDAP ログインポリシーオプション (258 ページ)

既存のログインポリシーの変更

既存のログインポリシー内でオプションを変更します。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順
既存のログインポリシーのオプションを変更するには、以下を実行します。

```
ALTER LOGIN POLICY policy-name {login_policy_options}
```

例:

次の文は、Test1 ログインポリシーの LOCKED オプションと MAX_CONNECTIONS オプションを変更します。

```
ALTER LOGIN POLICY Test1
locked=on
max_connections=5
```

参照：
- ALTER LOGIN POLICY 文 (252 ページ)
- ログインポリシーオプション (273 ページ)
- マルチプレックスログインポリシーの設定 (259 ページ)
- LDAP ログインポリシーオプション (258 ページ)

ログインポリシーの削除

ルートログインポリシーやユーザに現在割り当てられているログインポリシーを削除することはできません。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順

1. 削除するログインポリシーが現在割り当てられているユーザがいないことを確認します。
2. 以下を実行します。

```
DROP LOGIN POLICY policy_name
```

参照：

- DROP LOGIN POLICY 文 (285 ページ)

新規ユーザ作成時のログインポリシーの割り当て

ユーザアカウントの作成時にログインポリシーを割り当てない場合、このアカウントはルートログインポリシーに割り当てられます。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順
新規ユーザの作成時にルートログインポリシー以外のログインポリシーを割り当てます。1 人のユーザに同時に割り当てることができるログインポリシーは 1 つのみです。
以下を実行します。

```
CREATE USER userID
[ IDENTIFIED BY password ]
[ LOGIN POLICY policy-name ]
```

注意： ユーザにログインポリシーを割り当てる際に、同一の **CREATE USER** コマンド内で複数のユーザ ID を指定することはできません。

例:

次の文では、パスワードが `welcome` の `Joe` というユーザが作成され、ログインポリシー `Test2` が割り当てられます。

```
CREATE USER Joe
IDENTIFIED BY welcome
LOGIN POLICY Test2
```

参照：

- CREATE USER 文 (282 ページ)

ログインポリシーの既存ユーザへの割り当て

既存の SAP Sybase IQ ユーザにログインポリシーを割り当てます。

前提条件

MANAGE ANY LOGIN POLICY システム権限。

手順

1. 以下を実行します。
   ```
   ALTER USER userID
   LOGIN POLICY policy_name
   ```
2. 新しいログインポリシーを適用するには、ユーザにいったんログアウトしてからログインしなおすように求めます。

参照：

- ALTER USER 文 (263 ページ)

ユーザ接続数

ユーザ接続数を管理するにはいくつかの方法があります。

次の実行が可能です。

- 単一ユーザのアクティブなログイン数の制限 - MAX_CONNECTIONS ログインポリシーオプションが設定されたログインポリシーをユーザに割り当てます。
- ユーザアカウントのロック:
  - 明示的 – LOCKED オプションが ON に設定されたログインポリシーをユーザに割り当てます。
  - 暗黙的 – MAX_FAILED_LOGIN_ATTEMPTS オプションが設定されたログインポリシーをユーザに割り当てます。ユーザのログイン試行回数が設定値を超えると、そのユーザアカウントはロックされます。
- パスワード有効期限条件の設定 - PASSWORD_EXPIRY_ON_NEXT_LOGIN ログインポリシーオプションが設定されたログインポリシーをユーザに割り当てま

す。また、FORCE PASSWORD CHANGE 句が含まれる **CREATE USER** 文または **ALTER USER** 文を実行することもできます。

ユーザへのログインポリシーの割り当て、またはパスワード変更の強制には、MANAGE ANY USER システム権限が必要です。ログインポリシーの作成や変更には、MANAGE ANY LOGIN POLICY システム権限が必要です。

ログイン要求失敗後の接続の阻止

ログイン試行失敗の最大回数を超えると、ユーザは接続できなくなります。

前提条件

- ログインポリシーを作成または変更するには、MANAGE ANY LOGIN POLICY システム権限。
- ユーザにログインポリシーを割り当てるには、MANAGE ANY USER システム権限。

手順

ユーザが指定されたログイン試行回数以内に有効なログインクレデンシャルを入力できないと、アカウントが自動的にロックされるように、システムを設定できます。ロックされると、その後、有効なクレデンシャルが入力されてもユーザは接続できません。手動でロック解除されるまで、そのアカウントはロックされた状態になります。MAX_FAILED_LOGIN_ATTEMPTS ログインポリシーオプションは、ユーザアカウントがロックされるまでの連続試行失敗回数を制御します。この値は、ルートログインポリシーを含めて新規または既存のログインポリシーに設定して、そのログインポリシーが割り当てられたすべてのユーザに適用できます。

1. MAX_FAILED_LOGIN_ATTEMPTS オプションを設定するには、新規ログインポリシーを作成するか、既存のポリシーを変更します。
2. MAX_FAILED_LOGIN_ATTEMPTS オプションの値を定義します。
3. 必要に応じて、ログインポリシーを該当するユーザに割り当てます。

例

この例は、`lp` という名前で新規ログインポリシーを作成します。このポリシーでは試行が 5 回失敗した後にユーザアカウントを自動的にロックします。

```
CREATE LOGIN POLICY lp max_failed_login_attempts=5
```

この例は、5 回の試行失敗後にユーザアカウントを自動的にロックする `exist_lp` という名前の既存のログインポリシーを変更します。

```
ALTER LOGIN POLICY lp max_failed_login_attempts=5
```

この例では、ログインポリシー lp をユーザ John に割り当てます。John に lp ログインポリシーが割り当てられた後は、連続して 5 回無効なクレデンシャルが入力されるとログインできなくなります。

```
ALTER USER John LOGIN POLICY lp
```

参照：

- ALTER LOGIN POLICY 文 (252 ページ)
- ALTER USER 文 (263 ページ)
- CREATE LOGIN POLICY 文 (271 ページ)
- ログインポリシーオプション (254 ページ)
- LDAP ログインポリシーオプション (258 ページ)
- マルチプレックスログインポリシーの設定 (259 ページ)

DBA リカバリアカウントの作成

運用システム用の DBA リカバリアカウントを作成します。DBA リカバリアカウントは、元の DBA アカウントパスワードを紛失した場合に備えたバックアップです。

1. ランダムに生成されたユーザ名とパスワードを使用した 1 つ以上の追加 DBA アカウントを作成します。
2. クレデンシャルを安全な場所に保管します。

参照：

- CREATE USER 文 (282 ページ)

DBA リカバリアカウントでのログイン

DBA リカバリアカウントを使用してログインし、元の DBA アカウントパスワードをリセットします。

1. 安全な場所から DBA リカバリアカウントのユーザ名とパスワードを取得します。
2. リカバリアカウントを使用してログインします。
3. 元の DBA アカウントのパスワードをリセットします。
4. DBA リカバリアカウントのクレデンシャルを安全な場所に戻します。

ストアドプロシージャを使用した接続の管理

ユーザ接続を管理するストアドプロシージャは複数存在します。

次の表に、各 SAP Sybase IQ ログイン管理機能を実行するプロシージャを示します。

ストアドプロシージャ	目的	必要なシステム権限
sa_get_user_status	既存のユーザすべての現在のステータスを取得する。	既存のユーザすべての現在のステータスを取得するための MANAGE ANY USER システム権限。MANAGE ANY USER システム権限を持たないユーザは、自身の現在のステータスのみ取得できる。
sp_expireallpass-words	すべてのパスワードをただちに有効期限切れにする。	MANAGE ANY USER システム権限
sp_iqaddlogin	次回ログイン時に、ユーザの追加、ユーザパスワードの定義、ログインポリシーとパスワードの有効期限の指定を行う。	MANAGE ANY USER システム権限
sp_iqcopyloginpolicy	既存のログインポリシーをコピーして、新しいログインポリシーを作成する。	MANAGE ANY LOGIN POLICY システム権限
sp_iqdroplogin	指定されたユーザを削除する。	MANAGE ANY USER システム権限
sp_iqmodifylogin	指定されたユーザにログインポリシーを割り当てる。	MANAGE ANY USER システム権限
sp_iqmodifyadmin	指定されたログインポリシーのオプションを所定の値に設定する。	MANAGE ANY LOGIN POLICY システム権限
sp_iqpassword	自身または別のユーザのパスワードを変更する。	すべてのユーザは **sp_iqpassword** を実行して、各自のパスワードを変更できる。別のユーザのパスワードを変更するには、CHANGE PASSWORD システム権限が必要。

参照：

- sp_expireallpasswords システムプロシージャ (359 ページ)
- sp_iqcopyloginpolicy プロシージャ (371 ページ)
- sp_iqdroplogin プロシージャ (382 ページ)
- sp_iqmodifyadmin プロシージャ (388 ページ)
- sp_iqmodifylogin プロシージャ (389 ページ)
- sp_iqpassword プロシージャ (416 ページ)
- sp_iqaddlogin プロシージャ (362 ページ)
- sa_get_user_status システムプロシージャ (353 ページ)

接続が使用するリソースの管理

ユーザとロールのセットを作成すると、データベースに対するパーミッションを管理できます。またデータベースのセキュリティと管理によって、個々のユーザが使用できるリソースを制限することもできます。

たとえば、他のデータベースユーザの低速化が発生しないようにするため、単一の接続による大量の使用可能メモリや CPU の占有を防止することができます。

ユーザリソースを制御するデータベースオプション

リソースを制御するデータベースオプションは、*リソースガバナ*と呼ばれます。**SET OPTION** 文を使用して、データベースオプションを設定します。

- **CURSOR_WINDOW_ROWS –** バッファするカーソルローの数を定義します。
- **MAX_CARTESIAN_RESULT –** 直積ジョインを含むクエリの結果ローの数を制限します。
- **MAX_IQ_THREADS_PER_CONNECTION –** IQ の操作に使用される各接続で使用可能な処理スレッド数を設定します。
- **TEMP_CACHE_MEMORY_MB –** SAP Sybase IQ テンポラリストアのキャッシュサイズを設定します (テンポラリキャッシュサイズの設定には、サーバオプション **-iqtc** の使用をおすすめします)。
- **QUERY_TEMP_SPACE_LIMIT –** 1 つのクエリで使用できるテンポラリ DB 領域の量を制限します。
- **QUERY_ROWS_RETURNED_LIMIT –** クエリオプティマイザに対してリソース消費量が過剰なクエリを拒否するように指定します。オプティマイザの見積もりで、クエリの結果セットがこのオプションの値を超えると判断された場合、オプティマイザはクエリを拒否し、エラーメッセージを返します。

次のデータベースオプションは、エンジンに影響を与えますが、SAP Sybase IQ に対してはそれほど影響を及ぼしません。

- **JAVA_HEAP_SIZE** – 1 接続あたりの、Java アプリケーションに割り当てられるメモリの最大サイズ (バイト単位) を設定します。
- **MAX_CURSOR_COUNT** – 1 つの接続におけるカーソルの数を制限します。
- **MAX_STATEMENT_COUNT** – 1 つの接続で作成される文の数を制限します。

データベースオプションの設定は、ロール構造内では継承されません。

参照：
- SET OPTION 文 (326 ページ)

ビューとプロシージャによるセキュリティ

ビューとストアドプロシージャを使用することで、企業のニーズに応じて権限を調整できます。

高度なセキュリティを必要とするデータベースでは、テーブルに権限を直接定義することには限界があります。ユーザに付与されるテーブルに対する権利は、テーブル全体に適用されます。テーブルごとではなく、より精密に権限を割り当てることが必要な場合があります。次に例を示します。

- 従業員テーブルに保管された個人情報または機密情報へのアクセスを、テーブルの他の部分にアクセスする必要があるユーザには付与しないでおく必要がある。
- セールスコールの詳細が記述されたテーブルに対する権限を営業担当者に付与する一方で、営業担当者に許可するのは各自のコールに対する更新権限のみにする。

ビューを使用したセキュリティの調整

ビューを使用して、テーブルの一部分のみへのアクセスをユーザに付与します。

ローまたはカラムを単位にして部分を定義することができます。たとえば、特定のユーザグループに `Employees` テーブルの `Salary` カラムの参照を許可しないこと、または各自が作成したテーブルのローのみがユーザに表示されるようにすることが必要な場合があります。

例 1
販売管理者は、自分の部署の従業員に関するデータベースの情報にアクセスする必要があります。しかし、この管理者が他部署の従業員のデータにアクセスする理由はありません。

Sales Manager のユーザ ID を作成し、必要な情報が提供されるビューを作成して、適切な権限を Sales Manager のユーザ ID に付与します。

1. MANAGE ANY USER システム権限を持つユーザとして、**GRANT** 文を使用して新しいユーザ ID を作成します。SQL キーワードであるため、DBA は引用符で囲みます。

```
CONNECT "DBA"
IDENTIFIED by sql;
GRANT CONNECT
TO SalesManager
IDENTIFIED BY sales
```

2. 営業部の従業員だけを参照するビューを次のように定義します。テーブルの所有者が明確に識別できるように、テーブルを "DBA".Employees と指定し、SalesManager ユーザ ID がこのビューを使用できるようにします。このようにしないと、SalesManager がビューを使用するときに、このユーザ ID が認識しないテーブルを **SELECT** 文が参照することになります。

```
CREATE VIEW emp_sales AS
SELECT EmployeeID, GivenName, Surname
FROM "DBA".Employees
WHERE DepartmentID = 200
```

3. SalesManager にビューを表示する権限を付与します。テーブルに対する権限の付与と同じコマンドを使用して、ビューに対する権限を付与します。

```
GRANT SELECT
ON emp_sales
TO SalesManager
```

例 2

この例は、販売管理者が注文の概要を表示できるビューを作成します。このビューは、複数のテーブルからの情報を必要とします。

1. ビューを作成します。

```
CREATE VIEW order_summary AS
SELECT OrderDate, Region, SalesRepresentative
FROM "GROUPO".SalesOrders
    KEY JOIN "GROUPO".Customers
```

2. SalesManager に、このビューを調べる権限を付与します。

```
GRANT SELECT
ON order_summary
TO SalesManager
```

3. プロセスが正常に機能したかどうかを確認するため、SalesManager のユーザ ID に接続して、作成したビューを表示します。

```
CONNECT SalesManager IDENTIFIED BY sales ;
SELECT * FROM "GROUPO".emp_sales ;
SELECT * FROM "GROUPO".order_summary ;
```

SalesManager には、元のテーブルを参照する権限は付与されていません。したがって、次のコマンドを使用すると、権限エラーが発生します。

```
SELECT * FROM "DBA".Employees ;
SELECT * FROM "DBA".SalesOrders;
```

これらの例は、ビューを使用して SELECT 権限を調整する方法を示しています。同様の方法で、ビューに対する INSERT、DELETE、および UPDATE 権限も付与できます。

ビューの使用におけるガイドライン

ビュー作成に使用する **SELECT** 文にも、ビューの挿入、削除、更新の機能にも、一定の制限があります。

SELECT 文に対する制限

ORDER BY 句を **SELECT** クエリで使用することはできません。リレーショナルテーブルでは、ローやカラムの並び順には意味がありませんが、ORDER BY 句を使用すると、ビューのローの順序が規定されるからです。GROUP BY 句、サブクエリ、ジョインは、ビューの定義で使用できます。

スカラー値サブクエリは、最上位レベルの **SELECT** リスト内でのみサポートされます (ビュー、派生テーブル、サブクエリではサポートされません)。最上位レベルの **SELECT** の FROM 句で使用するビューまたは派生テーブルが単純なため、最上位レベルの **SELECT** にフラット化できる場合もあります。結果として、前述のルールが実際に適用されるのは、サブクエリ、フラット化されていないビュー、およびフラット化されていない派生テーブルに対してのみです。次に例を示します。

```
CREATE VIEW test_view AS SELECT testkey,(SELECT COUNT(*) FROM
tagtests WHERE tagtests.testkey = testtrd.testkey ) FROM
testtrd
```

```
SELECT * FROM test_view
Msg 21, Level 14, State 0:
SQL Anywhere Error -1005004: Subqueries are allowed only as arguments
of
comparisons, IN, and EXISTS,
-- (opt_Select.cxx 2101)
```

ビューを作成するには、必要とする正確な結果が必要なフォーマットで得られるまで **SELECT** クエリを編集します。思いどおりの **SELECT** クエリが完成したら、そのクエリの先頭に次のフレーズを追加してビューを作成します。次に例を示します。

```
CREATE VIEW viewname AS
```

ビューの挿入と削除に関するガイドライン

ビューに関連付けられている **SELECT** 文によっては、そのビューに対する **UPDATE**、**INSERT**、**DELETE** 文を実行できないことがあります。

以下を含むビューでは更新、挿入、または削除を行うことができません。

- **COUNT(*)** などの集合関数

- **SELECT** 文の GROUP BY 句
- **UNION** 操作

これらの場合には、**UPDATE**、**INSERT**、または **DELETE** コマンドから基本となるテーブルに対する操作を処理できないためです。

警告！ dbo ユーザ ID はシステムオブジェクトを所有するため、dbo ユーザ ID が所有するビューを削除しないでください。このようなビューを削除したり、テーブルに変更したりすると、予期しない問題が発生する可能性があります。

プロシージャを使用したセキュリティの調整

プロシージャは、ユーザが実行できるアクションを制限します。

ユーザには、プロシージャが機能するテーブルに対する権限がない場合でも、プロシージャの EXECUTE 権限を付与できます。

デフォルトでは、プロシージャはそのプロシージャの所有者の権限によって実行されます。テーブルを更新するプロシージャの場合、プロシージャ所有者がそのテーブルに対する UPDATE 権限を持っていれば、プロシージャを実行できます。プロシージャの所有者は、CREATE/ALTER PROCEDURE 文で SQL SECURITY INVOKER を指定して、プロシージャを実行するユーザの権限を使用してプロシージャが実行されるように制限できます。

タスクベースセキュリティの制限の設定

元になるテーブルに対するすべてのアクセスを禁止し、特定のストアドプロシージャを実行する権限またはロールをユーザに付与します。この方法では、データベース変更の制御方法が厳密に定義されます。

SAP Sybase IQ システムプロシージャを使用して、特定の権限を持つユーザに、特定のタスクの管理を許可するには次のようにします。

1. 実行対象の承認済みタスクの各セットにロールを作成し、そのロールに該当するシステム権限を付与します。
2. これらのロールのそれぞれに、1 つの共通ロールを付与します。
3. 該当するロールに、承認済みタスクを実行するための IQ プロシージャに対する EXECUTE 権限を付与します。
4. 承認済みタスクが付与される新規ユーザの作成時に、承認済みタスクのそれぞれに作成されたロールをそのユーザに付与します。

関連ストアドプロシージャの実行権限のユーザへの付与

ストアドプロシージャの実行に必要なシステム権限をユーザに付与します。ほとんどの権限はロールメンバーシップを介して継承されるため、ユーザはシステム権限および IQ プロシージャの実行権限をロールから継承できます。

前提条件

MANAGE ANY USER または EXECUTE ANY PROCEDURE システム権限が必要です。

手順

ユーザ `user1` に MANAGE ANY USER システム権限、およびユーザ管理に関連するプロシージャの実行権限を付与するには、次のようにします。

1. ロール `USER_ADMIN_GRP` を作成します。

   ```
   CREATE ROLE USER_ADMIN_GRP
   ```

2. MANAGE ANY USER システム権限を `USER_ADMIN_GRP` ロールに付与します。

   ```
   GRANT MANAGE ANY USER TO USER_ADMIN_GRP
   ```

3. SAP Sybase IQ のユーザ管理用ストアドプロシージャの EXECUTE 権限を `USER_ADMIN_GRP` に付与します。

   ```
   GRANT EXECUTE on sp_iqaddlogin
   to USER_ADMIN_GRP
   GRANT EXECUTE on sp_iqcopyloginpolicy
   to USER_ADMIN_GRP
   GRANT EXECUTE on sp_iqdroplogin
   to USER_ADMIN_GRP
   GRANT EXECUTE on sp_iqmodifyadmin
   to USER_ADMIN_GRP
   GRANT EXECUTE on sp_iqmodifylogin
   to USER_ADMIN_GRP
   ```

4. `USER_ADMIN_GRP` ロールを `user1` に付与します。 `user1` は、`USER_ADMIN_GRP` ロールメンバーシップを介して、MANAGE ANY USER システム権限と割り当てられた IQ プロシージャの実行能力を継承します。

   ```
   GRANT ROLE USER_ADMIN_GRP TO user1
   ```

ロールアクセスの関連ストアドプロシージャ

さまざまな関連ストアドプロシージャの権限を付与するロールを作成することができます。

ロール名	付与されるシステム権限	ストアドプロシージャ
OPERATOR_GRP	BACKUP DATABASE DROP CONNECTION CHECKPOINT MONITOR ACCESS SERVER LS	sp_iqbackupdetails sp_iqbackupsummary sp_iqconnection sp_iqsysmon
SPACEADMIN_GRP	MANAGE ANY DBSPACE ACCESS SERVER LS	sp_iqdbspace sp_iqdbspaceinfo sp_iqdbspaceobjectinfo sp_iqemptyfile sp_iqestdbspaces sp_iqfile sp_iqobjectinfo sp_iqspaceused

参照：

- sp_iqbackupdetails プロシージャ (363 ページ)
- sp_iqbackupsummary プロシージャ (365 ページ)
- sp_iqconnection プロシージャ (367 ページ)
- sp_iqdbspace プロシージャ (371 ページ)
- sp_iqdbspaceinfo プロシージャ (375 ページ)
- sp_iqdbspaceobjectinfo プロシージャ (378 ページ)
- sp_iqemptyfile プロシージャ (383 ページ)
- sp_iqestdbspaces プロシージャ (384 ページ)
- sp_iqfile プロシージャ (385 ページ)
- sp_iqobjectinfo プロシージャ (390 ページ)
- sp_iqspaceused プロシージャ (393 ページ)
- sp_iqsysmon プロシージャ (395 ページ)

データの機密性

クライアントと SAP Sybase IQ サーバ間、または SAP Sybase IQ クライアントとデータベースサーバ間の通信は、トランスポートレイヤセキュリティ (TLS) を使用して保護できます。

SAP Sybase IQ では、データベースまたはカラムを暗号化できます。

Kerberos 認証、およびカラムの暗号化のサポートは、別途ライセンスが必要な SAP Sybase IQ Advanced Security オプションに含まれています。

参照：

- SAP Sybase IQ でのカラムの暗号化 (204 ページ)
- SAP Sybase IQ での FIPS サポート (203 ページ)

データベースの暗号化と復号化

データベースの暗号化を使用して、データベース内のデータを第三者が解読しにくくすることができます。データベースを安全に管理するために、単純暗号化または強力な暗号化のいずれかを選択できます。

注意： データベースが暗号化されている場合、WinZip などのツールでデータベースを圧縮しても、元のデータベースファイルよりも大幅に小さくはなりません。

単純暗号化と強力な暗号化

単純暗号化
単純暗号化は、難読化と同じです。これにより第三者は、ディスクユーティリティを使用してファイルを表示し、データベースのデータを解読することが困難になります。単純暗号化では、データベースの暗号化のためのキーは不要です。

強力な暗号化
強力なデータベース暗号化方式では、キー (パスワード) がないとデータベースの操作やアクセスを行うことができません。アルゴリズムは、データベースやトランザクションログファイルに含まれる情報をエンコードして解読できないようにしています。

SAP Sybase IQ では、データベース管理者が、次の 4 種類の強力な暗号化のテクノロジを管理します。

- 強力な暗号化のステータス
- 暗号化キー
- 暗号化キーの保護

- 暗号化アルゴリズム

サポートされている強力な暗号化アルゴリズム
SAP Sybase IQ の強力な暗号化を実装するために使用するアルゴリズムは AES です。これは、米国商務省標準技術局 (NIST：National Institute of Standards and Technology) によってブロック暗号のための新しい次世代標準暗号化方式 (AES：Advanced Encryption Standard) として選択されたブロック暗号化アルゴリズムです。

AES_FIPS (128 ビット) または AES256_FIPS (256 ビット) タイプを使用することで、別の FIPS 認定の AES モジュールを指定して強力な暗号化を実装することもできます。-fips オプションを指定してデータベースサーバを起動した場合、AES、AES256、AES_FIPS、または AES256_FIPS の強力な暗号方式で暗号化されたデータベースを実行できますが、単純暗号化方式で暗号化されたデータベースは実行できません。暗号化されていないデータベースはサーバで開始できます。

AES_FIPS または AES256_FIPS で暗号化したデータベースを実行するために使用するコンピュータには、SAP Sybase IQ セキュリティオプションをインストールしてください。

FIPS 認定の暗号化は、すべてのプラットフォームで使用できるわけではありません。サポートされるプラットフォームのリストについては、http://www.sybase.com/detail?id=1061806 を参照してください。

注意： 別途ライセンスが必要な必須コンポーネント

FIPS 認定の暗号化には別のライセンスが必要です。強力な暗号化テクノロジはすべて、輸出規制対象品目です。

データベースの暗号化方式

- **暗号化されたデータベースを作成するには –** 次を使用できます。
  - 初期化ユーティリティ (iqinit) と、強力な暗号化を有効にするための各種オプションの組み合わせ。
    iqinit ユーティリティの -ep オプションと -ek オプションを使用すると、強力な暗号化が適用されたデータベースが作成され、プロンプトボックスまたはコマンドラインで暗号化キーを指定できます。iqinit の -ea オプションは、暗号化アルゴリズムを AES または AES256 (FIPS 認定モジュールの場合は AES_FIPS または AES256_FIPS) に設定します。
  - CREATE DATABASE 文。
- **既存のデータベースを暗号化するには –** 既存のデータベースでは、強力な暗号化のオンとオフを簡単に切り替えることはできませんが、次のいずれかを使用して、強力な暗号化を実装できます。

- 既存のデータベースを再構築 (アンロード／リロード) して、そのときに暗号化ステータスを変更します。データベースを再構築して、既存のデータベースに含まれるすべてのデータとスキーマをアンロードできます。新しいデータベースを作成して (ここで強力な暗号化のステータスを含めたさまざまな設定を変更できます)、データを新しいデータベースに再ロードします。強力に暗号化されたデータベースをアンロードするにはキーが必要です。データベースを再構築 (アンロード／リロード) するには、次の方式のいずれかを使用します。
  - アンロードユーティリティ (dbunload)

    アンロードユーティリティ (dbunload) と、新規データベースを強力な暗号化で作成するためのオプション。-an オプションは、新規データベースを作成します。強力な暗号化と暗号化キーをプロンプトボックスまたはコマンドラインで指定するには、-ep オプションまたは -ek オプションを使用します。-ea オプションは、暗号化アルゴリズムを AES または AES256 (FIPS 認定モジュールの場合は AES_FIPS または AES256_FIPS) に設定します。
  - UNLOAD 文と RELOAD 文
  - [データベースアンロードウィザード]。
- CREATE ENCRYPTED DATABASE 文または CREATE ENCRYPTED FILE を使用できます。

- **テーブル、カラム、およびマテリアライズドビューを暗号化するには** – Column and table encryption を参照してください。

参照：

- カラムとテーブルの暗号化 (146 ページ)

CREATE ENCRYPTED DATABASE 文と CREATE ENCRYPTED FILE 文の比較

既存のデータベースを暗号化する場合は CREATE ENCRYPTED DATABASE 文を使用します。CREATE ENCRYPTED FILE 文は、リカバリが必要なデータベースを暗号化する場合にのみ使用します。

この文の実行時には、暗号化しているデータベースには接続できません。

CREATE ENCRYPTED FILE 文と CREATE ENCRYPTED DATABASE 文には次の違いがあります。

- CREATE ENCRYPTED FILE 文はデータベース関連ファイル (トランザクションログ、トランザクションログミラー、DB 領域) ごとに実行する必要がありますが、CREATE ENCRYPTED DATABASE 文では、データベース関連ファイルがすべて自動的に暗号化されます。

- CREATE ENCRYPTED DATABASE 文はリカバリが必要なデータベースには使用できませんが、CREATE ENCRYPTED FILE 文は使用できます。
- CREATE ENCRYPTED DATABASE 文は、プロシージャ、トリガ、またはバッチ内では使用できません。CREATE ENCRYPTED FILE 文は使用できます。
- CREATE ENCRYPTED DATABASE 文では単純暗号化アルゴリズムがサポートされていますが、CREATE ENCRYPTED FILE 文ではこのアルゴリズムはサポートされていません。

暗号化されたデータベースの作成 (SQL の場合)

データベースは、CREATE DATABASE 文で ENCRYPTED 句を使用して作成している間に暗号化できます。

前提条件

デフォルトでは、SERVER OPERATOR システム権限が必要です。-gu データベースサーバオプションを使用すると、必要な権限を変更できます。

手順

このタスクは、既存のデータベースの暗号化とは異なります。既存のデータベースを暗号化するには、CREATE ENCRYPTED DATABASE 文を使用してください。

警告！ 警告

データベースに強力な暗号化を適用した場合、暗号化キーのコピーを必ず安全な場所に保管してください。暗号化キーがわからなくなった場合は、Sybase 製品の保守契約を結んでいるサポートセンタに依頼してもデータにはアクセスできません。アクセスできなくなったデータベースは、廃棄して、新しくデータベースを作成する必要があります。

1. Interactive SQL で、既存のデータベースに接続します。
2. ENCRYPTED 句、KEY オプション、ALGORITHM オプションを含む CREATE DATABASE 文を実行します。

暗号化されているデータベースが作成されます。

暗号化されたデータベースの作成 (iqinit ユーティリティの場合)

iqinit ユーティリティを使用して、暗号化されたデータベースを作成できます。

前提条件

この作業を実行するための前提条件はありません。

手順

警告！ 警告

データベースに強力な暗号化を適用した場合、暗号化キーのコピーを必ず安全な場所に保管してください。暗号化キーがわからなくなった場合は、Sybase 製品の保守契約を結んでいるサポートセンタに依頼してもデータにはアクセスできません。アクセスできなくなったデータベースは、廃棄して、新しくデータベースを作成する必要があります。

iqinit ユーティリティを実行してデータベースを作成します。

- 単純暗号化でデータベースを暗号化するには、-ea simple オプションを含めます。
- 強力な暗号化でデータベースを作成するには、-ek または -ep オプションを含めて、暗号化キーを指定します。

暗号化されているデータベースが作成されます。

次のステップ

データベースの起動時または作成時に、暗号化キーを指定する必要があります。

既存のデータベースを使用して、暗号化されたデータベースを作成 (SQL の場合)

データベースの暗号化されたコピーを、CREATE ENCRYPTED DATABASE 文を使用して作成することもできます。この文では、ファイルのコピーを作成 (この場合は、暗号化形式で) します。元のデータベースファイルは上書きしません。

前提条件

デフォルトでは、CREATE ENCRYPTED DATABASE 文を実行するには SERVER OPERATOR システム権限が必要です。-gu データベースサーバオプションを使用すると、必要な権限を変更できます。

暗号化しようとしているデータベースは実行中でないことが必要です。

手順

警告！ 警告

データベースに強力な暗号化を適用した場合、暗号化キーのコピーを必ず安全な場所に保管してください。暗号化キーがわからなくなった場合は、Sybase 製品の保守契約を結んでいるサポートセンタに依頼してもデータにはアクセスできません。アクセスできなくなったデータベースは、廃棄して、新しくデータベースを作成する必要があります。

1. Interactive SQL で、暗号化しているデータベース以外の既存のデータベースに接続します。
2. CREATE ENCRYPTED DATABASE 文を使用してデータベースを暗号化します。

CREATE ENCRYPTED DATABASE 文を実行すると、ファイルが暗号化 (上書き) されるのではなく、ファイルのコピーが暗号化形式で作成されます。データベースに関連付けられたトランザクションログ、トランザクションログミラー、または DB 領域がある場合は、これらのファイルの暗号化されたコピーも作成されます。

データベースの復号化 (SQL の場合)

CREATE DECRYPTED DATABASE 文を使用して、データベースを復号化することができます。この文では、ファイルのコピーを作成 (復号化形式で) します。元のデータベースファイルは上書きしません。

前提条件

デフォルトでは、CREATE DECRYPTED TABLE DATABASE 文を実行するには SERVER OPERATOR システム権限が必要です。-gu データベースサーバオプションを使用すると、必要な権限を変更できます。

暗号化しようとしているデータベースは実行中でないことが必要です。

手順

リカバリが必要なデータベースがあり、テクニカルサポートに送信するために復号化する場合は、CREATE DECRYPTED FILE 文を使用します。トランザクションログ、トランザクションログミラー、DB 領域ファイルなどのデータベース関連ファイルもすべてこの文を使用して復号化します。

1. Interactive SQL で、復号化するデータベース以外のデータベースに接続します。
2. CREATE DECRYPTED DATABASE 文を実行します。

CREATE DECRYPTED DATABASE 文を実行すると、ファイルが復号化 (上書き) されるのではなく、ファイルのコピーが復号化形式で作成されます。データベースに関連付けられたトランザクションログ、トランザクションログミラー、または DB 領域がある場合は、これらのファイルの復号化されたコピーも作成されます。

暗号化キー

暗号化キーには簡単に推測できない値を選択することをおすすめします。キーの長さは任意ですが、短いと推測されやすいため、一般的には長い方が適しています。また、数字、文字、特殊文字を組み合わせると、キーは推測されにくくなります。

暗号化キーでは常に大文字と小文字が区別されます。また、前後のスペースや、セミコロンを含めることはできません。

データベースを起動するたびに、キーを指定してください。キーを忘れた場合はデータベースにまったくアクセスできなくなります。

暗号化キーの入力に、コマンドプロンプト (デフォルト) またはプロンプトボックスのいずれかを選択できます。プロンプトボックスでのキー入力を選択すると、キーが表示されないため、さらにセキュリティが強化されます。クライアントでは、データベースを起動するたびにキーを指定してください。データベース管理者がデータベースを起動する場合は、クライアントでキーを使用する必要はありません。

警告！ 警告

データベースに強力な暗号化を適用した場合、暗号化キーのコピーを必ず安全な場所に保管してください。暗号化キーがわからなくなった場合は、Sybase 製品の保守契約を結んでいるサポートセンタに依頼してもデータにはアクセスできません。アクセスできなくなったデータベースは、廃棄して、新しくデータベースを作成する必要があります。

データベースの暗号化キーの変更

CREATE ENCRYPTED DATABASE 文を使用して、暗号化されたデータベースや、テーブル暗号化が有効になっているデータベースの暗号化キーを変更することができます。暗号化キーを変更しても、既存のファイルは上書きされませんが、新しいキーで暗号化されたファイルのコピーが作成されます。

前提条件

デフォルトでは、CREATE ENCRYPTED DATABASE 文を実行するには SERVER OPERATOR システム権限が必要です。-gu データベースサーバオプションを使用すると、必要な権限を変更できます。

手順

CREATE ENCRYPTED DATABASE 文を使用して、暗号化されたデータベースの暗号化キーを変更します。

暗号化キーが変更されます。

セキュリティとパフォーマンスの問題

データベースが暗号化されている場合、SAP Sybase IQ のパフォーマンスが低下します。パフォーマンスの影響は、ディスクとのページの読み取りや書き込みの頻度によって異なります。また、サーバが使用するキャッシュサイズを適切に設定することによって影響を最小限にできます。

キャッシュの初期サイズを増やすには、サーバの起動時に -c オプションで指定します。キャッシュの動的なサイズ変更がサポートされているオペレーティングシステムでは、使用されるキャッシュサイズが、使用可能なメモリの容量によって

制限される場合があります。そのため、キャッシュサイズを増加するには、使用可能なメモリを増加します。

カラムとテーブルの暗号化

データベースの一部だけを暗号化する場合は、カラムまたはテーブルを暗号化することを選択できます。

カラムの暗号化は、任意のテーブル内の任意のカラムに対していつでも実行できます。テーブルの暗号化を行うには、データベースでテーブルの暗号化が有効になっている必要があります。テーブルの暗号化は、データベースの作成 (初期化) 時に有効にします。

- **テーブルを暗号化するには** – 次を使用できます。
  - 初期化ユーティリティ (iqinit)。
  - CREATE DATABASE 文。
  - ALTER DATABASE 文。
  - CREATE ENCRYPTED TABLE DATABASE 文。
- **カラムを暗号化するには** – ENCRYPT 関数。
- **マテリアライズドビューを暗号化するには** – ALTER MATERIALIZED VIEW 文。

カラムの暗号化

データベースのカラムを暗号化するには、ENCRYPT 関数を使用します。ENCRYPT 関数は、同じ AES の強力な暗号化アルゴリズムを使用します。このアルゴリズムはデータベースの暗号化用に使用され、その関数に渡される値を暗号化します。

暗号化されたデータは、DECRYPT 関数で復号化できます。このとき、ENCRYPT 関数で指定したキーと同じキーを使用する必要があります。これらの関数はともに LONG BINARY 値を返します。異なるデータ型を使用する必要がある場合は、CAST 関数を使用して、その値を必要なデータ型に変換できます。

ENCRYPT 関数と DECRYPT 関数も、未加工の暗号化をサポートしています。データベースサーバ内のデータを、エクスポートしてサーバ外で復号化できるフォーマットに暗号化できます。

データベースユーザが復号化された形式のデータにアクセスする必要があっても、暗号化キーにはアクセスできないようにする必要がある場合は、DECRYPT 関数を使用するビューを作成できます。これにより、ユーザは暗号化キーを知らなくても、復号化されたデータにアクセスできるようになります。テーブルを使用したビューまたはストアドプロシージャを作成する場合は、ALTER VIEW 文や ALTER PROCEDURES 文の SET HIDDEN パラメータを使用して、ユーザがビュー定義やプロシージャ定義を参照することによって暗号化キーにアクセスできないようにすることができます。

カラムの暗号化の例
次の例では、user_info というテーブルのパスワードを格納するカラムを暗号化するトリガを使用します。user_info テーブルは、次のように定義されています。

```
CREATE TABLE user_info (
   employee_ID INTEGER NOT NULL PRIMARY KEY,
   user_name CHAR(80),
   user_pwd CHAR(80) );
```

新しいユーザが追加されたとき、または既存のユーザのパスワードが更新されたときに、2 つのトリガが user_pwd カラムの値を暗号化するためにデータベースに追加されます。

- encrypt_new_user_pwd トリガは、新しいローが user_info テーブルに追加されるたびに実行されます。

  ```
  CREATE TRIGGER encrypt_new_user_pwd
  BEFORE INSERT
  ON user_info
  REFERENCING NEW AS new_pwd
  FOR EACH ROW
  BEGIN
      SET new_pwd.user_pwd=ENCRYPT(new_pwd.user_pwd, '8U3dkA');
  END;
  ```

- encrypt_updated_pwd トリガは、user_info テーブルの user_pwd カラムが更新されるたびに実行されます。

  ```
  CREATE TRIGGER encrypt_updated_pwd
  BEFORE UPDATE OF user_pwd
  ON user_info
  REFERENCING NEW AS new_pwd
  FOR EACH ROW
  BEGIN
      SET new_pwd.user_pwd=ENCRYPT(new_pwd.user_pwd, '8U3dkA');
  END;
  ```

データベースに新しいユーザを追加する場合

```
INSERT INTO user_info
VALUES ( '1', 'd_williamson', 'abc123');
```

SELECT 文を発行して user_info テーブルの情報を表示する場合、user_pwd カラムの値はバイナリデータ (パスワードの暗号化された形式) であり、INSERT 文で指定された値 abc123 ではありません。

このユーザのパスワードを変更した場合は、encrypt_updated_pwd トリガが起動され、新しいパスワードが暗号化形式で user_pwd カラムに表示されます。

```
UPDATE user_info
SET user_pwd='xyz'
WHERE employee_ID='1';
```

元のパスワードは、次の SQL 文を発行して検索できます。この文はデータを復号化するために DECRYPT 関数と暗号化キーを使用し、値を LONG BINARY から CHAR 型に変換するために CAST 関数を使用しています。

```
SELECT CAST (
   DECRYPT( user_pwd, '8U3dkA' )
   AS CHAR(100))
   FROM user_info
   WHERE employee_ID = '1';
```

未加工の暗号化

未加工の暗号化を使用すると、データベースサーバ内のデータを、エクスポートしてデータベースサーバ外で復号化できるフォーマットに暗号化できます。このような暗号化は、**未加工**フォーマットと呼ばれます。未加工フォーマットでデータを暗号化するには、暗号化キーと初期化ベクトルを指定する必要があります。また、必要に応じて埋め込みフォーマットも指定します。データを復号化するには、同じパラメータ値を指定する必要があります。

また、DECRYPT 関数を使用して、データベースサーバ内のデータを復号化することもできます。

未加工の暗号化は、次の場合に便利です。

- **データベースユーザがデータにアクセスできないようにする場合** – 未加工の暗号化を使用して、データベース管理者さえもアクセスさせない機密データを暗号化し、データベースサーバを使用しないでクライアントアプリケーションでデータを復号化することができます。未加工の暗号化は、データの暗号化と復号化をデータベースサーバのみが実行する必要がある場合はおすすめできません。
- **TLS 暗号化を使用できない場合** – 未加工の暗号化は、TLS 暗号化の代わりに使用できます。TLS 暗号化とは異なり、未加工の暗号化では、リプレイや中間者攻撃を防止できません。また、データベースサーバも認証できません。

例

データベースの SensitiveData テーブルにある binary_data カラムから、データベースを使用しないクライアントにデータを送信する必要があります。機密データであるため、次の SQL 文を使用して、データを未加工フォーマットに暗号化します。

```
SELECT ENCRYPT( binary_data, 'TheEncryptionKey','AES(FORMAT=RAW)',
'ThisIsTheIV' )FROM SensitiveData;
```

暗号化データを、内容を復号化できるアプリケーションとともにクライアントにコピーします。また、アプリケーションで使用する暗号化キー (TheEncryptionKey) と初期化ベクトル (ThisIsTheIV) もクライアントに提供します。クライアントはアプリケーションを使用してデータを復号化し、表示します。

テーブル暗号化

テーブル暗号化によって、データベース全体の暗号化がもたらすようなパフォーマンスの低下を招くことなく、機密データが含まれるテーブルやマテリアライズドビューを暗号化することができます。テーブルの暗号化が有効な場合、暗号化されたテーブルのテーブルページ、関連するインデックスページ、テンポラリファイルのページが暗号化されます。暗号化されたテーブルのトランザクションを含むトランザクションログのページも暗号化されます。

データベース内のテーブルを暗号化するためには、テーブル暗号化を有効にしておく必要があります。テーブル暗号化の有効化は、データベースを初期化するときに行います。テーブル暗号化が有効になっているかどうかを確認するには、次のように DB_PROPERTY 関数を使用して EncryptionScope データベースプロパティの値を取得します。

```
SELECT DB_PROPERTY( 'EncryptionScope' );
```

TABLE が返された場合は、テーブル暗号化が有効になっています。

テーブル暗号化で暗号化アルゴリズムが有効であるかどうかを確認するには、次のように DB_PROPERTY 関数を使用して Encryption データベースプロパティの値を取得します。

```
SELECT DB_PROPERTY( 'Encryption' );
```

テーブル暗号化がパフォーマンスに及ぼす影響

暗号化されたテーブルでは、各テーブルページがディスクへの書き込みと同時に暗号化され、ディスクから読み取るときに復号化されます。このプロセスはアプリケーションには影響しません。ただし、暗号化されたテーブルの読み込みや書き込みにおいてパフォーマンスが多少低下することがあります。既存のテーブルを暗号化または復号化する場合、テーブルのサイズによっては時間がかかることがあります。

暗号化されたテーブル内のカラムに対するインデックスのインデックスページ、暗号化されたテーブルのトランザクションを含むトランザクションログのページ、データベースのテンポラリファイルのすべてのページも暗号化されます。その他のデータベースとトランザクションログページは暗号化されません。

暗号化されたテーブルに圧縮されたカラムが含まれている場合があります。その場合、データは圧縮されてから暗号化されます。

テーブルの暗号化は必要記憶域には影響しません。

テーブル暗号化が有効であるデータベースの起動

テーブル暗号化が有効であるデータベースを起動する方法は、暗号化されたデータベースを起動する場合と同じです。たとえば、-ek オプションを指定してデータベースを起動する場合は、キーを指定する必要があります。-ep オプションを指定してデータベースを起動すると、キーの入力を要求されます。

データベース内のテーブル暗号化の有効化 (SQL の場合)

CREATE DATABASE 文を使用して、テーブル暗号化が有効なデータベースを作成するか、CREATE ENCRYPTED TABLE DATABASE 文を使用して、既存のデータベースでテーブル暗号化を有効にします。

前提条件

デフォルトでは、CREATE DATABASE 文と CREATE ENCRYPTED TABLE DATABASE 文を実行するには SERVER OPERATOR システム権限が必要です。-gu データベースサーバオプションを使用すると、必要な権限を変更できます。

手順

テーブル暗号化は、データベースの作成時に有効にして設定する必要があります。データベースでテーブル暗号化が有効でない場合、または、データベースの暗号化が有効になっている場合は、CREATE ENCRYPTED TABLE DATABASE 文を使用すると、テーブル暗号化が有効なデータベースのコピーが作成されます。また、元のデータベースファイルは上書きされません。

テーブル暗号化が有効なデータベースを作成するか、既存のデータベースでテーブル暗号化を有効にします。

オプション	アクション
テーブル暗号化が有効なデータベースを作成する	CREATE DATABASE 文を使用してデータベースを作成します。このとき、キーと暗号化アルゴリズムを指定します。
既存のデータベースでテーブル暗号化を有効にする	CREATE ENCRYPTED TABLE DATABASE でデータベースのコピーを作成し、キーを指定します。

テーブル暗号化は有効です。

次のステップ

CREATE TABLE 文を使用するか、暗号化する既存のテーブルを ALTER TABLE 文で変更して、暗号化されたテーブルを作成します。テーブルを暗号化するときは、テーブル暗号化を有効にするときに指定したキー、アルゴリズム、またはその両方を使用します。

データベース内のテーブル暗号化の有効化 (iqinit ユーティリティの場合)
データベースの作成中にコマンドラインを使用して、テーブル暗号化を有効にすることができます。

前提条件

テーブル暗号化は、データベースの作成時に有効にして設定する必要があります。データベースでテーブル暗号化が有効になっていない場合、またはデータベース暗号化が有効な場合は、テーブル暗号化を有効にしてデータベースを再作成する必要があります。

手順
iqinit で -et オプションと -ek オプションを指定し、キーと暗号化アルゴリズムも指定して、データベースを作成します。

テーブル暗号化は有効です。

テーブルの暗号化
暗号化されたテーブルを CREATE TABLE 文で作成するか、既存のテーブルを ALTER TABLE 文で暗号化することができます。

前提条件

CREATE TABLE 文を使用するには、次のシステム権限のいずれかが必要です。

CREATE TABLE
CREATE ANY TABLE
CREATE ANY OBJECT

ALTER TABLE 文を作成するには、変更するテーブルの所有者であるか、次のいずれかの権限を持っている必要があります。

そのテーブルに対する ALTER 権限
ALTER ANY TABLE
ALTER ANY OBJECT

データベース内のテーブルを暗号化するためには、そのデータベースでテーブル暗号化が有効になっている必要があります。

手順

テーブルを暗号化するときは、データベースの作成時に指定した暗号化のアルゴリズムとキーが使用されます。

暗号化が有効なテーブルを作成するか、既存のテーブルを暗号化することができます。

オプション	アクション
暗号化が有効なテーブルを作成する	CREATE TABLE 文の ENCRYPTED 句を使用してテーブルを作成します。
既存のテーブルを暗号化する	ALTER TABLE 文の ENCRYPTED 句を使用してテーブルを暗号化します。

テーブルが暗号化されます。

IPv6 のサポート

SAP Sybase IQ は、インターネットプロトコルバージョン 6 (IPv6) をサポートしています。これにはインターネット上でパケットをルーティングするためのアドレス情報と制御情報が含まれています。

IPv6 は、2^{128} 個のユニークな IP アドレスをサポートし、従来の IPv4 でサポートされていたアドレス数から大幅に増加しています。SAP Sybase IQ は、IPv4 と IPv6 の両方のアドレスをサポートし、クライアントまたはサーバ上で任意に IP アドレスを指定できます。

ODBC クラスでは、リモートデータアクセスでの IPv6 アドレスの使用をサポートします。JDBC クラスでは、リモートデータアクセスでの IPv6 アドレスの使用をサポートしていません。

トランスポートレイヤセキュリティの設定

次の手順には、トランスポートレイヤセキュリティの設定に必要なタスクの概要が記載されています。

1. デジタル証明書を取得します。
   ID ファイルと証明書ファイルが必要です。サーバ ID ファイルにはサーバのプライベートキーが含まれているので、データベースサーバにセキュリティ保護された状態で格納する必要があります。サーバ証明書ファイルはクライアントに配布します。
   証明書は、証明書認証局から購入するか、証明書作成ユーティリティ (createcert) を使用して作成することができます。SAP Sybase IQ には、証明書を作成する機能もあり、特に開発やテストのときに便利です。
2. SAP Sybase IQ クライアント／サーバアプリケーション用のトランスポートレイヤセキュリティを設定する場合は、次の手順に従います。
   - **トランスポートレイヤセキュリティを指定して SAP Sybase IQ データベースサーバを起動する** – -ec データベースサーバオプションを使用して、セキュリティのタイプ、サーバ ID ファイル名、サーバのプライベートキーを保護するパスワードを指定します。

共有メモリを経由した暗号化されていない接続も許可する場合は、-es オプションを指定します。

TDS では TLS プロトコルを使用しません。暗号化されていない接続が TDS プロトコルを使用できないようにするには、tcpip オプションの -x tcpip(TDS=NO) を指定します。

- **トランスポートレイヤセキュリティを使用するようにクライアントアプリケーションを設定する** – Encryption 接続パラメータ [ENC] を使用して、信頼できる証明書のパスとファイル名を指定します。

3. SAP Sybase IQ Web サービス用のトランスポートレイヤセキュリティを設定する場合は、次の手順に従います。
   - **トランスポートレイヤセキュリティを指定して SAP Sybase IQ データベースサーバを起動する** – -xs データベースサーバオプションを使用して、セキュリティのタイプ、サーバ ID ファイル名、サーバのプライベートキーを保護するパスワードを指定します。
   - **ブラウザまたは他の Web クライアントが証明書を信頼するように設定する** – SAP Sybase IQ Web サービスを暗号化します。
4. SAP Sybase IQ Multiplex データベースサーバを設定する場合は、次の手順に従います。

   INC および MIPC 接続で、-ec サーバオプションの内容から使用する TLS 接続パラメータが決定されます。
   TRUSTED_CERTIFICATES_FILE オプションを適切な証明書認証局に設定します。

デジタル証明書

トランスポートレイヤセキュリティを設定するには、デジタル証明書が必要です。証明書は、証明書認証局から入手するか、証明書作成ユーティリティ (createcert) を使用して作成することができます。

証明書作成ユーティリティ
証明書作成ユーティリティ (createcert) で、RSA を使用して X.509 証明書ファイルを生成できます。

証明書ビューアユーティリティ
証明書ビューアユーティリティ viewcert で、RSA を使用して X.509 証明書を読み込むことができます。

サーバ認証に使用する証明書
サーバ認証に使用する証明書ファイルは、同じ手順で作成できます。どちらの場合も、ID ファイルと証明書ファイルを作成します。

サーバ認証の場合は、サーバ ID ファイルとクライアントに配布する証明書ファイルを作成します。

証明書設定
証明書には、自己署名されたものと、民間またはエンタープライズ認証局によって署名されたものがあります。

- **自己署名証明書** – 自己署名されたサーバ証明書は、単純な設定で使用します。
- **エンタープライズルート証明書** – エンタープライズルート証明書を使用すると、サーバ証明書に署名できるため、複数のサーバが配備されている環境でのデータの整合性と拡張性が向上します。

  サーバ証明書の署名に使用するプライベートキーは、安全な中央のロケーションに保存できます。
  サーバ認証では、クライアントを再設定しなくても、データベースサーバを追加できます。
- **民間認証局** – エンタープライズルート証明書の代わりに、サードパーティの認証局を使用できます。民間認証局は、プライベートキーを保存するための専用の設備を備えており、高品質なサーバ証明書を作成します。

自己署名ルート証明書
自己署名ルート証明書は、1 つのデータベースサーバを使用する単純な設定に使用できます。

注意： ヒント

サーバ ID ファイルが複数必要な場合は、エンタープライズレベルの証明書チェーンまたは民間認証局を使用します。認証局にはルートプライベートキーを格納する専用の設備があり、拡張性と証明書の高度な整合性を提供します。

- **証明書** – サーバ認証証明書の場合、自己署名証明書はクライアントに配布されます。自己署名証明書は、識別情報、サーバのパブリックキー、自己署名されたデジタル署名を含む電子文書です。
- **ID ファイル** – サーバ認証証明書の場合、ID ファイルはセキュリティ保護された状態でデータベースサーバに格納されます。ID ファイルは、自己署名証明書 (クライアントに配布) と、対応するプライベートキーを組み合わせたものです。プライベートキーがあると、データベースサーバは、初期ハンドシェイクでクライアントから送信されたメッセージを復号化できます。

証明書チェーン

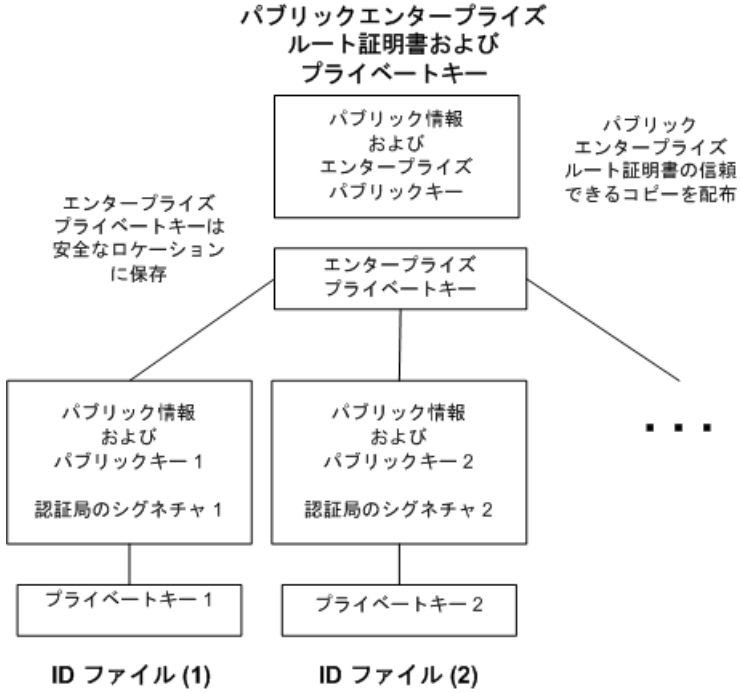
複数の ID ファイルが必要な場合は、自己署名証明書の代わりに証明書チェーンを使用することで、セキュリティと拡張性を高めることができます。証明書チェーンでは、ID の署名に認証局またはエンタープライズルート証明書が必要です。

証明書チェーンを使用する利点

証明書チェーンには、次の利点があります。

- **拡張性** – サーバ認証の場合、エンタープライズルート証明書または認証局によって署名されたすべての証明書を信頼するようにクライアントを設定できます。新しいデータベースサーバを追加する場合、クライアントに新しい証明書のコピーは不要です。
- **セキュリティ** – エンタープライズルート証明書のプライベートキーは、ID ファイルにはありません。ルート証明書のプライベートキーを高セキュリティのロケーションに保存したり、専用の設備を備えている認証局を使用することで、サーバ認証の整合性が保護されます。

次の図は、エンタープライズルート証明書の基本アーキテクチャを示しています。



マルチサーバ環境での証明書の使用

マルチサーバ環境で使用する証明書を作成するには、次の手順に従います。

- パブリックエンタープライズルート証明書およびエンタープライズプライベートキーを生成します。
  エンタープライズプライベートキーは安全なロケーションに保存します。専用の設備の方が安全です。
  サーバ認証の場合は、パブリックエンタープライズルート証明書をクライアントに配布します。
- エンタープライズルート証明書を使用して、ID に署名します。
  パブリックエンタープライズルート証明書とエンタープライズプライベートキーを使用して、各 ID に署名します。サーバ認証の場合は、ID ファイルをサーバ用に使用します。

サードパーティの認証局を使用して、サーバ証明書に署名することもできます。民間認証局は、プライベートキーを保存するための専用の設備を備えており、高品質なサーバ証明書を作成します。

エンタープライズルート証明書
エンタープライズルート証明書を使用すると、複数のサーバが配備されている環境での、データの整合性と拡張性が向上します。

信頼できる証明書を作成するために使用されるプライベートキーは、専用の設備に保存できます。
サーバ認証では、クライアントを再設定しなくてもサーバを追加できます。

エンタープライズルート証明書を設定するには、エンタープライズルート証明書と、ID の署名に使用するエンタープライズプライベートキーを作成します。

署名付き ID ファイル
エンタープライズルート証明書を使用して、サーバの ID ファイルに署名できます。

サーバ認証の場合、各サーバ用に ID ファイルを生成します。これらの証明書はエンタープライズルート証明書によって署名されるため、createcert -s オプションを使用します。

グローバル署名証明書
民間認証局とは、高品質の証明書の作成と、これらの証明書を使用した証明書要求への署名を事業としている組織です。

グローバル署名証明書には、次の利点があります。

- 会社内での通信の場合、共通して信頼するものとして、外部の認可された認証局を使用すると、システムのセキュリティの信頼性が高まります。認証局は、署名を行ったすべての証明書の識別情報が正確であることを保証する必要があります。

- 認証局は、証明書を生成するための管理された環境と高度な方法を提供します。
- ルート証明書のプライベートキーは、秘密にしておきます。企業内ではこの重要情報を格納するのに適した場所がない可能性がありますが、認証局では専用の設備を設計して管理できます。

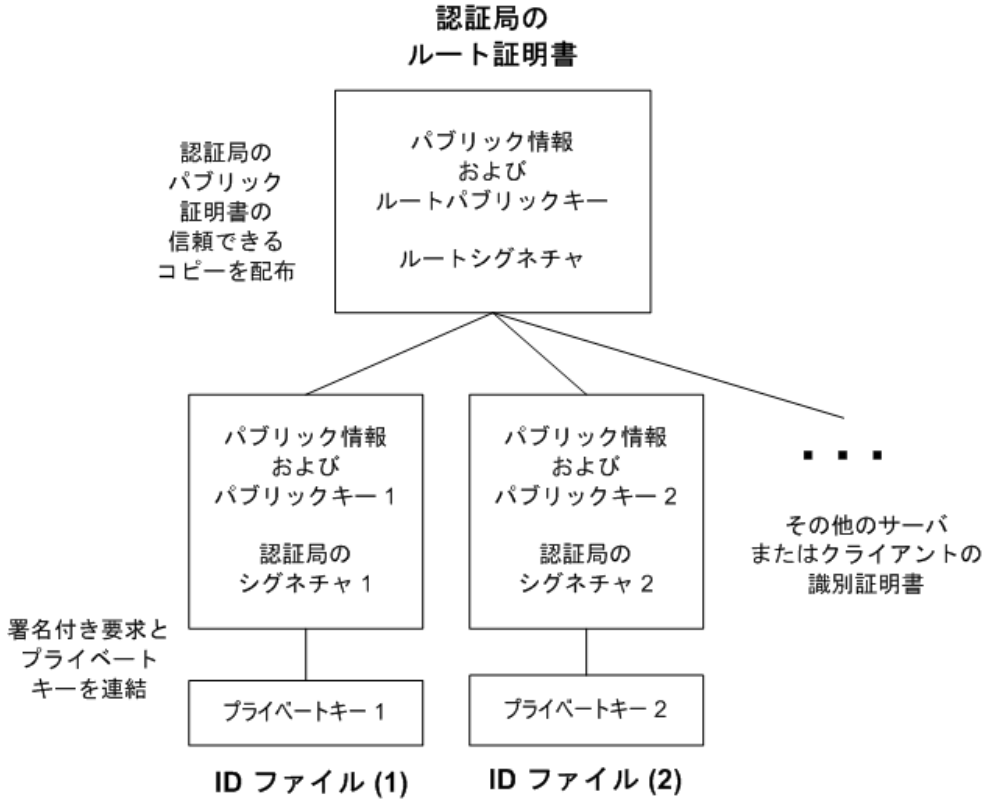
グローバル署名証明書の設定
グローバル署名 ID ファイルを設定するには、次の手順に従います。

- -r オプションを指定した createcert ユーティリティを使用して証明書を要求します。
- 認証局を使用して各要求に署名します。署名付き要求と対応するプライベートキーを組み合わせて、サーバの ID ファイルを作成できます。

注意： エンタープライズルート証明書にグローバル署名できる場合があります。これは、認証局が、他の証明書に署名できる証明書を生成する場合のみ適用されます。

グローバル署名 ID ファイル

グローバル署名証明書を直接、サーバの ID ファイルとして使用できます。次の図は、複数の ID ファイルの設定を示します。



iqsrv16 コマンドラインで、サーバ ID ファイルと、プライベートキーのパスワードを参照します。

認証局の証明書に対するクライアントの信頼設定

サーバ認証の場合は、サーバにアクセスするクライアントがチェーン内のルート証明書を信頼することを確認する必要があります。グローバル署名証明書の場合、ルート証明書は証明書認証局の証明書です。

注意： グローバル署名証明書を使用する場合、各クライアントはフィールド値を確認して、同じ認証局が他のクライアント用に署名した証明書を信用することを避けなければなりません。

ユーティリティデータベースサーバのセキュリティ

SAP Sybase IQ には、物理的実体が存在せずデータを含めることができない「*ユーティリティデータベース*」と呼ばれる幻データベースが組み込まれています。

ユーティリティデータベースは、任意の SAP Sybase IQ サーバで実行できます。SAP Control Center の場合、ユーティリティデータベースのサーバはユーティリティサーバと呼ばれます。

ユーティリティデータベースは、限られた機能に特化されています。これを使用すると、物理データベースに接続せずに **CREATE DATABASE** や **DROP DATABASE** などのデータベースファイル操作文を実行することができます。

また、ユーティリティデータベースからは、データベースプロパティと接続プロパティも取得できます。これらのプロパティは、ユーティリティデータベースに接続しているときに作成するデータベースに適用されます。

設定作業の 1 つとして、ユーティリティデータベースとそのサーバのセキュリティの設定があります。次の選択を行う必要があります。

- ユーティリティデータベースへの接続が可能なユーザ
- ファイル管理文の実行が可能なユーザ

接続時のユーティリティデータベース名の定義

ユーティリティデータベースにはデータベースファイルが関連付けられていないため、このデータベースの起動時にデータベースファイルを指定することはできません。接続時にデータベース名を指定する必要があります。

ユーティリティデータベースへの接続時に、データベース名として `utility_db` を指定します。

次に例を示します。

```
dbisqlc -c "uid=dba;pwd=sql;eng=myserver;dbn=utility_db"
```

注意： ユーティリティデータベースに接続して Windows のローパーティションを使用する IQ データベースを作成する場合は、IQ PATH の構文に違いがあります。たとえば、デバイス I の Windows ローパーティションを指定する場合、ユーティリティデータベースでは "¥¥.¥I:" と指定します。他の IQ データベースでは、円記号を二重にする必要があります。つまり、この同じデバイスを「¥¥¥¥.¥¥I:」と指定します。円記号は、IQ データベースではエスケープ文字として扱われるのに対し、ユーティリティデータベースでは通常の文字として扱われます。

ユーティリティデータベースのパスワードの定義

ユーティリティデータベースにユーザ ID DBA を定義します。

1. テキストエディタを使用して、ファイル util_db.ini を開きます。このファイルは、サーバ実行プログラムのディレクトリに格納されています。

   このディレクトリはサーバ上にあるので、このファイルへのアクセスは制御できます。つまり、どのユーザがパスワードにアクセスできるかも制御できます。
2. 次の行を見つけて、「password」を使用するパスワードに置き換えます。

   ```
   [UTILITY_DB]
   PWD=password
   ```

   util_db.ini ファイルはテキストエディタを使用して簡単に読み取ることができるため、utility_db セキュリティレベルの使用はデータベースサーバをホストするコンピュータの物理的なセキュリティに依存します。

ファイル管理文を実行するためのパーミッション

別のレベルのセキュリティを使用してデータベースの作成と削除を制御することによって、データベースのセキュリティが強化されます。**-gu** データベースサーバコマンドラインオプションは、ファイル管理文の実行可能ユーザを制御します。

ファイル管理文の使用には、all、none、DBA、および utility_db の 4 レベルのパーミッションが存在します。utility_db レベルでは、ユーティリティデータベースに接続可能なユーザのみが、ファイル管理文を使用できます。

表 1 : ロール管理のパーミッション

-gu スイッチの値	効果	適用対象
all	誰でもファイル管理文を実行できる	ユーティリティデータベースを含む任意のデータベース
none	誰もファイル管理文を実行できない	ユーティリティデータベースを含む任意のデータベース
DBA	SERVER OPERATOR システム権限を持つユーザのみがファイル管理文を実行できる	ユーティリティデータベースを含む任意のデータベース
utility_db	ユーティリティデータベースに接続できるユーザのみがファイル管理文を実行できる	ユーティリティデータベースのみ

例
Sun、HP、Linux、および Windows の各プラットフォームで、ユーティリティデータベースのパスワードを認識しているユーザのみに、ユーティリティデータベースへの接続とデータベースの作成または削除を許可するには、コマンドラインから次のコマンドでサーバを起動します。

```
start_iq -n testsrv -gu utility_db
```

AIX で、ユーティリティデータベースのパスワードを認識しているユーザのみに、ユーティリティデータベースへの接続とデータベースの作成または削除を許可するには、コマンドラインから次のコマンドでサーバを起動します。

```
start_iq -n testsrv -gu utility_db -iqmt 256
```

インストール時に、ユーティリティデータベースのパスワードが `IQ&Mine49` に設定されているとします。この場合に次のコマンドを使用すると、Interactive SQL ユーティリティがクライアントアプリケーションとして起動され、`testsrv` という名前のサーバに接続し、ユーティリティデータベースがロードされ、ユーザを接続します。

```
dbisql -c "uid=DBA;pwd=IQ&Mine49;dbn=utility_db;eng=testsrv"
```

この文を実行すると、ユーティリティデータベースに正常に接続され、データベースの作成と削除が可能になります。

注意： データベース名、ユーザ ID、およびパスワードでは、大文字と小文字が区別されます。必ず、**dbisql** コマンドと `util_db.ini` ファイルで大文字と小文字が一致するように指定してください。

データのセキュリティ

データベースには機密情報や個人情報などが含まれている場合があるので、データベースや格納されるデータのセキュリティを考慮した設計になっていることが重要です。

システムセキュリティ機能

システムセキュリティ機能がデータベースサーバ上で稼働しているデータベースにアクセスできないようにすることができます。

機能が保護されている (アクセス不可にされている) 場合は、クライアントアプリケーション、データベース定義ストアドプロシージャ、トリガ、イベントで機能を使用できなくなります。セキュリティ機能の設定は、選択されたデータベースサーバで稼働中のすべてのデータベースに適用されます。セキュリティ機能は、ウィルスなどの不明な組み込み論理が含まれる可能性のあるデータベースを起動

する必要がある場合、または、サードパーティベンダがホストしているデータベースサーバまたはデータベースをロックダウンする場合に便利です。**-sf** データベースサーバオプションを使用すると、データベースサーバで稼働中のデータベースに対して保護する機能を指定できます。

セキュリティ機能キー
システムセキュリティ機能キーは、データベースサーバの作成時に **-sk** データベースサーバオプションを指定して作成します。データベースサーバが稼働中になった後は、**sa_server_option** システムプロシージャを使用して、機能を保護するか、保護解除するかを変更します。

システムセキュリティ機能キーを作成した後は、カスタマイズセキュリティ機能キーを作成できます。このキーは特定のユーザに割り当てられ、管理者がそのキーで保護した機能のみにユーザのアクセスを制限します。

カスタマイズセキュリティ機能キーは、select システムプロシージャを使用して管理します。

セキュリティ機能キーの作成

ユーザが使用できるデータベース機能を制御するには、セキュリティ機能データベースサーバオプション (-sf) を使用して、データベースサーバでユーザがアクセスできない機能を指定します。-sk データベースサーバオプションでシステムセキュリティ機能キーを作成し、sp_create_secure_feature_key システムプロシージャでカスタマイズセキュリティ機能キーを作成します。

前提条件

SERVER OPERATOR システム権限が必要です。また、manage_keys 機能にアクセスできることが必要です。

手順

セキュリティ機能の設定は、データベースサーバで稼働中のすべてのデータベースに適用されます。

セキュリティ保護オプション (-sf) で、次のような機能を使用できるかどうかを指定できます。

サーバ側のバックアップ
外部ストアドプロシージャ
リモートデータアクセス
Web サービス

-sk オプションで、データベースサーバのセキュリティ機能へのアクセスを管理するシステムセキュリティ機能キーを指定します。データベースサーバが稼働中になった後、セキュリティ機能のリストを変更するには、sa_server_option システム

プロシージャを使用します。データベースサーバが稼働中になった後、カスタマイズセキュリティ機能キーを変更するには、sp_alter_secure_feature_key システムプロシージャを使用します。

1. コマンドプロンプトで、-sf および -sk オプションを使用してデータベースサーバを起動します。

   たとえば、次のコマンドで、データベーサーバを起動して、すべての機能を保護します。このコマンドには、接続のセキュリティ機能へのアクセスを許可するために後で使用できるキーも含まれます。

   ```
   iqsrv16 -n secure_server -sf all -sk someSystemKey c:¥mydemo.db
   ```

2. データベースサーバに接続します。

   ```
   dbisql -c
   "UID=DBA;PWD=sql;Host=myhost;Server=secure_server;DBN=mydemo"
   ```

3. sp_use_secure_feature_key システムプロシージャを呼び出して、接続のセキュリティ機能キーを指定します。この場合、セキュリティ機能キーは、-sk オプションで指定したものと同じです。

   ```
   CALL sp_use_secure_feature_key ( 'system' , 'someSystemKey' );
   ```

4. sa_server_option システムプロシージャを使用して、システムセキュリティ機能キーのセキュリティ機能を変更します。

   例：

   ```
   CALL sa_server_option( 'SecureFeatures', '-remote_data_access' );
   ```

5. 特定のユーザのカスタマイズセキュリティ機能キーを作成します。

   たとえば、Bob のカスタマイズセキュリティ機能キーを作成して、電子メールの送信を許可します。

   ```
   CALL sp_create_secure_feature_key ( 'bobsKey' , 'anotherAuthKey' ,
   'sa_send_email' );
   ```

   データベースにログインした後、Bob が電子メールを送信するには、次のコマンドを実行する必要があります。

   ```
   CALL sp_use_secure_feature_key ( 'bobsKey' , 'anotherAuthKey' );
   ```

   データベースサーバ secure_server で稼働中のデータベースのユーザは、remote_data_access 機能を除き、すべてのセキュリティ機能にアクセスできません。ただし、ユーザ Bob は、sa_send_email にもアクセスできます。

現在、データベースサーバには、システムセキュリティ機能だけでなく、特定のユーザに割り当てられたカスタマイズセキュリティ機能もあります。

参照：

- -sk iqsrv16 データベースサーバオプション (343 ページ)
- -sf iqsrv16 データベースサーバオプション (344 ページ)

- sp_alter_secure_feature_key システムプロシージャ (422 ページ)
- sp_create_secure_feature_key システムプロシージャ (355 ページ)
- sp_drop_secure_feature_key システムプロシージャ (424 ページ)
- sp_list_secure_feature_key システムプロシージャ (424 ページ)
- sp_use_secure_feature_key システムプロシージャ (425 ページ)

外部認証

SAP Sybase IQ は、LDAP と Kerberos の各外部認証方式をサポートしています。

SAP Sybase IQ での LDAP ユーザ認証

SAP Sybase IQ は、幅広く使用されている国際規格である Lightweight Directory Access Protocol (LDAP) をベースとする既存の全社的ディレクトリアクセスフレームワークに統合することができます。

SAP Sybase IQ と LDAP ユーザ認証の統合により以下がサポートされます。

- 検索された識別名 (DN) を使用した認証
- 高可用性を確保するためのセカンダリ LDAP サーバへのフェイルオーバー
- 以前エラーが発生したサーバへの自動フェイルバック
- OpenLDAP サードパーティライブラリとの統合
- LDAP サーバとの安全な通信
- 頻繁な短時間接続に有効な設計
- 複数のドメインと複数の LDAP サーバへの拡張性

LDAP ユーザ認証のライセンス要件

Advanced Security オプション (IQ_SECURITY) は、環境を不正アクセスから保護します。SAP Sybase IQ で LDAP ユーザ認証を使用可能にするにはこのオプションが必要です。

LDAP サーバ設定オブジェクトについて

SAP Sybase IQ は、LDAP サーバと呼ばれる設定オブジェクトを使用して、LDAP ユーザ認証を実行できるようにします。

その名前と異なり、LDAP サーバは、実際のサーバではなく、SAP Sybase IQ サーバに存在する設定オブジェクトです。その唯一の機能は、LDAP ユーザ認証を実行できるように、物理 LDAP サーバへの接続を提供することです。LDAP サーバ設定オブジェクトの設定は、LDAP ユーザ認証の式の SAP Sybase IQ 側にのみ適用されます。LDAP サーバ設定オブジェクトの設定が物理 LDAP サーバに書き込まれることは絶対にありません。

注意： このマニュアルでは、わかりやすくするために、LDAP サーバ設定オブジェクトは SAP Sybase IQ の内部設定オブジェクトを指します。LDAP サーバは外部エンティティを指します。

LDAP ユーザ認証を使用した場合のフェイルオーバー機能

フェイルオーバー機能は、プライマリ LDAP サーバ設定オブジェクトとセカンダリ LDAP サーバ設定オブジェクトを作成することでサポートできます。

各 LDAP サーバ設定オブジェクトは 1 つの LDAP サーバに接続し、プライマリサーバまたはセカンダリサーバとして指定できます。指定プライマリ LDAP サーバ設定オブジェクトが LDAP サーバに接続できない場合、指定セカンダリ LDAP サーバ設定オブジェクトがユーザ認証に使用されます。SQL 文を使用して、フェイルオーバーおよびフェイルバックを手動で管理できます。また、SAP Sybase IQ で変更が適切であることが検出されれば、自動的に実行されます。

ログインポリシーでプライマリとセカンダリの LDAP サーバ設定オブジェクトを定義します。フェイルオーバーを発生させるには、プライマリとセカンダリの LDAP サーバ設定オブジェクトを定義する必要があります。プライマリ LDAP サーバ設定オブジェクトのみログインポリシーに定義している場合、フェイルオーバーは行われません。セカンダリ LDAP サーバ設定オブジェクトがプライマリ LDAP サーバ設定オブジェクトなしで定義されている場合、セカンダリ LDAP サーバ設定オブジェクトはプライマリ LDAP サーバ設定オブジェクトとして動作し、フェイルオーバーは発生しません。

セカンダリ LDAP サーバ設定オブジェクトを指定する際、LDAP サーバ設定オブジェクトが正しいフェイルオーバー LDAP サーバに接続するように設定する必要があります。フェイルオーバー時、セカンダリ LDAP サーバ設定オブジェクトがセカンダリ LDAP サーバに接続できない場合、SAP Sybase IQ の LDAP ユーザ認証は機能しなくなります。

LDAP ユーザ認証の有効化

SAP Sybase IQ で LDAP ユーザ認証を設定します。設定が完了したら、ユーザが LDAP ユーザ認証を使用してログオンできることを確認します。

1. ログイン方法としての LDAP ユーザ認証の設定

   LDAP ユーザ認証を有効にするには、値 LDAPUA を LOGIN_MODE データベースオプションに追加する必要があります。
2. LDAP サーバ設定オブジェクトの作成

   新しい LDAP サーバ設定オブジェクトを作成して、LDAP ユーザ認証を実行できるようにします。
3. LDAP サーバ設定オブジェクトの検証

   新規または既存の LDAP サーバ設定オブジェクトの属性を検証します。
4. LDAP ユーザ認証ログインポリシーオプションの管理

LDAP ユーザ認証固有のログインポリシーオプションは複数あります。これらのオプションは、LDAP ユーザ認証を使用するユーザに割り当てるログインポリシー (ルートを含む) で定義する必要があります。

5. LDAP サーバ設定オブジェクトの現在のステータスの表示

   sa_get_ldapserver_status ストアドプロシージャを実行して、LDAP サーバ設定オブジェクトの現在のステータスに関するレポートを生成します。

ログイン方法としての LDAP ユーザ認証の設定

LDAP ユーザ認証を有効にするには、値 `LDAPUA` を LOGIN_MODE データベースオプションに追加する必要があります。

前提条件

SET ANY SECURITY OPTION システム権限が必要です。

手順

設定後、LDAP ユーザ認証がただちに使用可能になります。
LDAPUA 値を LOGIN_MODE オプションに追加するには、次を実行します。

```
SET OPTION PUBLIC.login_mode = LDAPUA
```

LDAP サーバ設定オブジェクトの作成

新しい LDAP サーバ設定オブジェクトを作成して、LDAP ユーザ認証を実行できるようにします。

前提条件

MANAGE ANY LDAP SERVER システム権限が必要です。

手順

LDAP サーバ設定オブジェクトは、SAP Sybase IQ と物理 LDAP サーバの間の接続を提供します。複数の LDAP サーバを、特にフェイルオーバーのために、使用する場合、LDAP サーバごとに個別の LDAP サーバ設定オブジェクトを設定します。LDAP サーバ設定オブジェクトのパラメータは、`ISYSLDAPSERVER` (システムビュー SYSLDAPSERVER) システムテーブルに格納されます。作成時に自動的に LDAP サーバへの接続を有効にするには、WITH ACTIVATE 句を使用します。

1. 新しい LDAP サーバ設定オブジェクトに定義する適用可能な SEARCH DN 属性の値を指定します。

表 2 : SEARCH DN 属性

属性	有効な値
URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
ACCESS ACCOUNT	外部 LDAP サーバに接続するユーザの識別名。
IDENTIFIED BY	ACCESS ACCOUNT に指定されている識別名に関連付けられたパスワード。
IDENTIFIED BY ENCRYPTED	ACCESS ACCOUNT に指定されている識別名に関連付けられた、暗号化されたパスワード。

2. 新しい LDAP サーバ設定オブジェクトの適用可能な LDAPUA サーバ属性の値を指定します。

表 3 : LDAPUA 属性

属性	有効な値
SEARCH DN	SEARCH DN 属性 (ステップ 1 参照) から定義されるすべての属性。
AUTHENTICATION URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
CONNECTION TIMEOUT	SAP Sybase IQ と外部 LDAP サーバの間の DN 検索と認証の両方に適用される接続タイムアウト値を指定する。ミリ秒単位で指定し、デフォルト値は 10 秒。
CONNECTION RETRIES	DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続の再試行回数を指定する。有効な値の範囲は 1 ～ 60 で、デフォルト値は 3。

属性	有効な値
TLS	DN 検索と認証の両方に使用する LDAP サーバへの接続に、TLS とセキュア LDAP プロトコルのいずれを使用するかを定義する。有効な設定は ON および OFF (デフォルト)。 **注意：** 「セキュア LDAP の有効化」と「TLS 接続の信頼関係の設定」を参照。

3. **CREATE LDAP SERVER** コマンドに適用可能な属性と句を指定して実行します。次に例を示します。

```
CREATE LDAP SERVER secure_primary
SEARCH DN
     URL 'ldaps://my_LDAPserver:636/dc=MyCompany,dc=com??sub?cn=*'
     ACCESS ACCOUNT 'cn=myadmin, cn=Users, dc=mycompany, dc=com'
     IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldaps://my_LDAPserver:636/'
CONNECTION TIMEOUT 3000
CONNECTION RETRIES 3
TLS OFF
WITH ACTIVATE
```

LDAP サーバ設定オブジェクトの検証

新規または既存の LDAP サーバ設定オブジェクトの属性を検証します。

前提条件

MANAGE ANY LDAP SERVER システム権限が必要です。

手順

管理者が新しい LDAP サーバ設定オブジェクトを設定する際または SAP Sybase IQ と LDAP サーバの間の接続の問題を診断する際は、**VALIDATE LDAP SERVER** コマンドが役に立ちます。VALIDATE LDAP SERVER 文によって確立された接続は一時的であり、文の実行が終了する際に閉じられます。

LDAP サーバにそのユーザが存在することを検証するには、**CHECK** 句を使用します。userID および比較する *user-dn-string* を指定します。

1. 検証する LDAP サーバ設定オブジェクトの SEARCH DN 属性を指定します。

表 4 : SEARCH DN 属性

属性	有効な値
URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
ACCESS ACCOUNT	外部 LDAP サーバに接続するユーザの識別名。
IDENTIFIED BY	ACCESS ACCOUNT に指定されている識別名に関連付けられたパスワード。
IDENTIFIED BY ENCRYPTED	ACCESS ACCOUNT に指定されている識別名に関連付けられた、暗号化されたパスワード。

2. 検証する LDAP サーバ設定オブジェクトの LDAPUA 属性を指定します。

表 5 : LDAPUA 属性

属性	有効な値
SEARCH DN	SEARCH DN 属性 (ステップ 1 参照) から定義されるすべての属性。
AUTHENTICATION URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
CONNECTION TIMEOUT	SAP Sybase IQ と外部 LDAP サーバの間の DN 検索と認証の両方に適用される接続タイムアウト値を指定する。ミリ秒単位で指定し、デフォルト値は 10 秒。
CONNECTION RETRIES	DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続の再試行回数を指定する。有効な値の範囲は 1 ～ 60 で、デフォルト値は 3。
TLS	DN 検索と認証の両方に使用する LDAP サーバへの接続に、TLS とセキュア LDAP プロトコルのいずれを使用するかを定義する。有効な設定は ON および OFF (デフォルト)。 **注意：** 「セキュア LDAP の有効化」と「TLS 接続の信頼関係の設定」を参照。

3. 適用可能な属性を指定して **VALIDATE LDAP SERVER** コマンドを実行します。

たとえば、apps_primary という名前の LDAP サーバ設定オブジェクトが次のように作成され、SET OPTION PUBLIC.login_mode が 'Standard,LDAPUA' に設定されているとします。

```
CREATE LDAP SERVER apps_primary
SEARCH DN
    URL 'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=myadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
WITH ACTIVATE
```

次の文は、userID の myusername が存在することを、オプションの CHECK 句を使用して LDAP サーバ設定オブジェクト apps_primary 上の予想されるユーザの識別名 (引用符で囲まれている) と比較することによって検証します。

```
VALIDATE LDAP SERVER apps_primary
CHECK myusername 'cn=myusername,cn=Users,dc=mycompany,dc=com'
```

LDAP ユーザ認証ログインポリシーオプションの管理

LDAP ユーザ認証固有のログインポリシーオプションは複数あります。これらのオプションは、LDAP ユーザ認証を使用するユーザに割り当てるログインポリシー (ルートを含む) で定義する必要があります。

LDAP サーバデータベースオブジェクト固有のオプションは、ログインポリシーを最初に作成するときに定義するか、ルートログインポリシーを含む既存のポリシーに追加できます。

ログインポリシーオプションの定義には、MANAGE ANY LOGIN POLICY システム権限が必要です。

参照：

- LDAP サーバ設定オブジェクトの現在のステータスの表示 (174 ページ)

ルートログインポリシーの変更

ルートログインポリシーのオプション値は変更できますが、ポリシーの削除はできません。

前提条件

MANAGE ANY LOGIN POLICY システム権限。

手順
新しいデータベースはそれぞれ、ルートポリシーと呼ばれるデフォルトのログインポリシーで作成されます。ログインポリシーを指定しないでユーザアカウントを作成した場合、そのユーザはルートログインポリシーに属します。
ルートログインポリシーのオプションを変更するには、以下を実行します。

```
ALTER LOGIN POLICY ROOT {login_policy_options}
```

参照：
- 既存のログインポリシーの変更 (172 ページ)
- 新しいログインポリシーの作成 (172 ページ)
- ログインポリシーの既存ユーザへの割り当て (173 ページ)

既存のログインポリシーの変更
既存のログインポリシー内でオプションを変更します。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順
既存のログインポリシーのオプションを変更するには、以下を実行します。

```
ALTER LOGIN POLICY policy-name {login_policy_options}
```

例:

次の文は、`Test1` ログインポリシーの LOCKED オプションと MAX_CONNECTIONS オプションを変更します。

```
ALTER LOGIN POLICY Test1
locked=on
max_connections=5
```

参照：
- ルートログインポリシーの変更 (171 ページ)
- 新しいログインポリシーの作成 (172 ページ)
- ログインポリシーの既存ユーザへの割り当て (173 ページ)

新しいログインポリシーの作成
ログインポリシーの作成時に明示的に設定されなかったオプションは、その値をルートログインポリシーから継承します。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順
ログインポリシー名はユニークである必要があります。追加するログインポリシー名が既存の場合には、エラーメッセージが表示されます。
新しいログインポリシーを作成するには、以下を実行します。

```
CREATE LOGIN POLICY policy_name {login_policy_options}
```

例:

次の文では、Test1 ログインポリシーが作成され、PASSWORD_LIVE_TIME オプションが 60 日に設定されます。

```
CREATE LOGIN POLICY Test1
password_life_time=60
```

参照：
- ルートログインポリシーの変更 (171 ページ)
- 既存のログインポリシーの変更 (172 ページ)
- ログインポリシーの既存ユーザへの割り当て (173 ページ)

ログインポリシーの既存ユーザへの割り当て
既存の SAP Sybase IQ ユーザにログインポリシーを割り当てます。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順

1. 以下を実行します。

   ```
   ALTER USER userID
   LOGIN POLICY policy_name
   ```

2. 新しいログインポリシーを適用するには、ユーザにいったんログアウトしてからログインしなおすように求めます。

参照：
- ルートログインポリシーの変更 (171 ページ)
- 既存のログインポリシーの変更 (172 ページ)
- 新しいログインポリシーの作成 (172 ページ)

LDAP サーバ設定オブジェクトの現在のステータスの表示

sa_get_ldapserver_status ストアドプロシージャを実行して、LDAP サーバ設定オブジェクトの現在のステータスに関するレポートを生成します。

ステータス情報には、LDAP サーバ設定オブジェクトの名前、オブジェクト識別子、現在の状態、および最終状態変更日時が含まれます。設定が適切で正常に動作している LDAP サーバ設定オブジェクトの状態は READY または ACTIVE です。

このストアドプロシージャを実行するために必要なシステム権限はありません。

参照：

- LDAP ユーザ認証ログインポリシーオプションの管理 (171 ページ)

SAP Sybase IQ による LDAP サーバ設定オブジェクトの管理

管理には、LDAP サーバ設定オブジェクトの作成、変更、および LDAP ユーザ認証を利用しやすくするためのオプションの保守が含まれます。

ログイン方法としての LDAP ユーザ認証の設定

LDAP ユーザ認証を有効にするには、値 `LDAPUA` を LOGIN_MODE データベースオプションに追加する必要があります。

前提条件

SET ANY SECURITY OPTION システム権限が必要です。

手順

設定後、LDAP ユーザ認証がただちに使用可能になります。
LDAPUA 値を LOGIN_MODE オプションに追加するには、次を実行します。

```
SET OPTION PUBLIC.login_mode = LDAPUA
```

参照：

- LOGIN_MODE オプション (334 ページ)

LDAP ユーザ認証のみを使用する環境での標準認証の許可

LDAP ユーザ認証のみをサポートする環境で、標準認証を使用する認証を、選択したユーザに許可します。

LDAP ユーザ認証が SAP Sybase IQ データベースへのアクセスを許可する唯一の認証方法である場合、次の場合にどのユーザもログオンできないシナリオになる可能性があります。

- LDAP ユーザ認証が有効なログインポリシーが存在しない場合

- LDAP 認証が有効なログインポリシーにユーザが割り当てられていない場合
- LDAP ユーザ認証を使用するログインポリシーに割り当てられているすべてのユーザアカウントがロックされている場合

このシナリオは回避できない可能性があります。ただし、選択した数のユーザに対して、標準認証による SAP Sybase IQ データベースへのログインを許可する方法があります。この方法は、LOGIN_MODE 設定によりすべてのユーザがデータベースに接続できない場合の一時的な解決方法として用意されたものです。

標準認証によるアクセスを選択したユーザに許可する際、少なくとも 1 人のそのようなユーザが SET ANY SECURITY OPTION システム権限または MANAGE ANY LOGIN POLICY システム権限を持つことを保証して、それらのユーザが永続的に問題を解決できるようにします。LDAP ユーザ認証を使用してどのユーザもログインできない問題を永続的に解決するには、その根本原因に応じて、これらの 2 つのシステム権限の一方または両方が必要になります。最大 5 個のユーザ ID を、セミコロンで区切り二重引用符で囲んで指定できます。

標準認証によるアクセスは、ロックダウン問題が発生してから許可します。前もって設定する必要はありません。事前に設定しておく必要はありません。選択したユーザに対して、標準認証によるログインを許可するには、**–al** *user-id-list* コマンドラインスイッチを指定して **start_iq** ユーティリティを実行します。許可されたユーザは、クレデンシャルの入力を要求するプロンプトで、標準認証のユーザ名とパスワードを入力します。

サーバレベルまたはデータベースレベルのいずれかで **-al** スイッチを指定します。サーバレベルで指定した場合、**-al** スイッチは、次回のサーバの再起動時まで有効な状態で保持されます。データベースレベルで指定した場合、**-al** スイッチは、次にデータベースを停止して再起動するまで有効な状態で保持されます。
標準認証を許可するには、次のどちらかのコマンドを実行します。

レベル	文
サーバ	**start_iq -al** *"user1,user2,user3" server_name.cfg database-name.db*
データベース	**start_iq** *servername.cfg database_name.db* **-al** *"user1,user2,user3"*

例:

次の例では、login_mode が「LDAPUA」に設定されていることを前提としています。次のコマンドは、標準認証による `server1` 上の `database1` への認証を `Alice`、`Bob`、および `Carol` の各ユーザに許可します。

```
start_iq –al  "alice;bob;carol" server1.cfg database1.db
```

参照：

- -al iqsrv16 サーバオプション (336 ページ)

- -al iqsrv16 データベースオプション (337 ページ)

TLS 接続の信頼関係の設定

ユーザ認証のための外部 LDAP サーバへのトランスポートレイヤセキュリティ (TLS) 接続に使用する信頼関係が含まれるファイルのロケーションと名前を定義します。

前提条件

SET ANY SECURITY OPTION システム権限が必要です。

手順

SAP Sybase IQ は、LDAP ユーザ認証時に LDAP サーバに対するクライアントとして動作し、TLS 証明書に署名した認証局 (CA) の名前が格納されているファイルにアクセスする必要があります。CA へのパスとファイル名は、パブリックレベルでのみ設定できる TRUSTED_CERTIFICATES_FILE データベースセキュリティオプションに格納されます。デフォルトでは、このオプションは NULL (無効) に設定されていますが、これは信頼できる CA が存在しないのでアウトバウンド接続を開始できないことを意味します。この値は設定すると、すぐに有効になります。

サーバ証明書に署名した信頼できる CA のリストは、Windows 環境内のローカルの C: ドライブの ロケーションで、そのマシンに存在するすべての SAP Sybase アプリケーション間で共有できます。

TRUSTED_CERTIFICATES_FILE データベースセキュリティオプションを設定するには、次の文を実行します。

```
SET OPTION PUBLIC.TRUSTED_CERTIFICATES_FILE = 'path/filename'
```

例

次の例では、¥trusted.txt という名前のファイルで、信頼できる証明書ファイルへのパスを C:¥sybase¥shared に設定します。

```
SET OPTION PUBLIC.TRUSTED_CERTIFICATES_FILE = 'C:¥sybase¥shared
¥trusted.txt'
```

参照：

- TRUSTED_CERTIFICATES_FILE オプション (336 ページ)

LDAP サーバ設定オブジェクトの作成

新しい LDAP サーバ設定オブジェクトを作成して、LDAP ユーザ認証を実行できるようにします。

前提条件

MANAGE ANY LDAP SERVER システム権限が必要です。

手順

LDAP サーバ設定オブジェクトは、SAP Sybase IQ と物理 LDAP サーバの間の接続を提供します。複数の LDAP サーバを、特にフェイルオーバーのために、使用する場合、LDAP サーバごとに個別の LDAP サーバ設定オブジェクトを設定します。LDAP サーバ設定オブジェクトのパラメータは、`ISYSLDAPSERVER` (システムビュー SYSLDAPSERVER) システムテーブルに格納されます。作成時に自動的に LDAP サーバへの接続を有効にするには、WITH ACTIVATE 句を使用します。

1. 新しい LDAP サーバ設定オブジェクトに定義する適用可能な SEARCH DN 属性の値を指定します。

表 6 : SEARCH DN 属性

属性	有効な値
URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
ACCESS ACCOUNT	外部 LDAP サーバに接続するユーザの識別名。
IDENTIFIED BY	ACCESS ACCOUNT に指定されている識別名に関連付けられたパスワード。
IDENTIFIED BY ENCRYPTED	ACCESS ACCOUNT に指定されている識別名に関連付けられた、暗号化されたパスワード。

2. 新しい LDAP サーバ設定オブジェクトの適用可能な LDAPUA サーバ属性の値を指定します。

表 7 : LDAPUA 属性

属性	有効な値
SEARCH DN	SEARCH DN 属性 (ステップ 1 参照) から定義されるすべての属性。
AUTHENTI-CATION URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。

属性	有効な値
CONNECTION TIMEOUT	SAP Sybase IQ と外部 LDAP サーバの間の DN 検索と認証の両方に適用される接続タイムアウト値を指定する。ミリ秒単位で指定し、デフォルト値は 10 秒。
CONNECTION RETRIES	DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続の再試行回数を指定する。有効な値の範囲は 1 ～ 60 で、デフォルト値は 3。
TLS	DN 検索と認証の両方に使用する LDAP サーバへの接続に、TLS とセキュア LDAP プロトコルのいずれを使用するかを定義する。有効な設定は ON および OFF (デフォルト)。 **注意：** 「セキュア LDAP の有効化」と「TLS 接続の信頼関係の設定」を参照。

3. **CREATE LDAP SERVER** コマンドに適用可能な属性と句を指定して実行します。次に例を示します。

```
CREATE LDAP SERVER secure_primary
SEARCH DN
     URL 'ldaps://my_LDAPserver:636/dc=MyCompany,dc=com??sub?cn=*'
     ACCESS ACCOUNT 'cn=myadmin, cn=Users, dc=mycompany, dc=com'
     IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldaps://my_LDAPserver:636/'
CONNECTION TIMEOUT 3000
CONNECTION RETRIES 3
TLS OFF
WITH ACTIVATE
```

参照：

- LDAP サーバ設定オブジェクト URL の構文とパラメータ (187 ページ)
- セキュア LDAP の有効化 (186 ページ)
- CREATE LDAP SERVER 文 (267 ページ)
- LDAP サーバ設定オブジェクトの属性の編集 (181 ページ)
- TLS 接続の信頼関係の設定 (176 ページ)

LDAP サーバ設定オブジェクトの検証

新規または既存の LDAP サーバ設定オブジェクトの属性を検証します。

前提条件

MANAGE ANY LDAP SERVER システム権限が必要です。

手順

管理者が新しい LDAP サーバ設定オブジェクトを設定する際または SAP Sybase IQ と LDAP サーバの間の接続の問題を診断する際は、**VALIDATE LDAP SERVER** コマン

ドが役に立ちます。VALIDATE LDAP SERVER 文によって確立された接続は一時的であり、文の実行が終了する際に閉じられます。

LDAP サーバにそのユーザが存在することを検証するには、**CHECK** 句を使用します。userID および比較する *user-dn-string* を指定します。

1. 検証する LDAP サーバ設定オブジェクトの SEARCH DN 属性を指定します。

表 8 : SEARCH DN 属性

属性	有効な値
URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
ACCESS ACCOUNT	外部 LDAP サーバに接続するユーザの識別名。
IDENTIFIED BY	ACCESS ACCOUNT に指定されている識別名に関連付けられたパスワード。
IDENTIFIED BY ENCRYPTED	ACCESS ACCOUNT に指定されている識別名に関連付けられた、暗号化されたパスワード。

2. 検証する LDAP サーバ設定オブジェクトの LDAPUA 属性を指定します。

表 9 : LDAPUA 属性

属性	有効な値
SEARCH DN	SEARCH DN 属性 (ステップ 1 参照) から定義されるすべての属性。
AUTHENTI-CATION URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
CONNEC-TION TIME-OUT	SAP Sybase IQ と外部 LDAP サーバの間の DN 検索と認証の両方に適用される接続タイムアウト値を指定する。ミリ秒単位で指定し、デフォルト値は 10 秒。

属性	有効な値
CONNECTION RETRIES	DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続の再試行回数を指定する。有効な値の範囲は 1 ～ 60 で、デフォルト値は 3。
TLS	DN 検索と認証の両方に使用する LDAP サーバへの接続に、TLS とセキュア LDAP プロトコルのいずれを使用するかを定義する。有効な設定は ON および OFF (デフォルト)。 **注意：** 「セキュア LDAP の有効化」と「TLS 接続の信頼関係の設定」を参照。

3. 適用可能な属性を指定して **VALIDATE LDAP SERVER** コマンドを実行します。

たとえば、apps_primary という名前の LDAP サーバ設定オブジェクトが次のように作成され、SET OPTION PUBLIC.login_mode が 'Standard,LDAPUA' に設定されているとします。

```
CREATE LDAP SERVER apps_primary
SEARCH DN
    URL 'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=myadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
WITH ACTIVATE
```

次の文は、userID の myusername が存在することを、オプションの CHECK 句を使用して LDAP サーバ設定オブジェクト apps_primary 上の予想されるユーザの識別名 (引用符で囲まれている) と比較することによって検証します。

```
VALIDATE LDAP SERVER apps_primary
CHECK myusername 'cn=myusername,cn=Users,dc=mycompany,dc=com'
```

参照：

- セキュア LDAP の有効化 (186 ページ)
- LDAP サーバ設定オブジェクト URL の構文とパラメータ (187 ページ)
- VALIDATE LDAP SERVER 文 (331 ページ)
- LDAP サーバ設定オブジェクトの属性の編集 (181 ページ)
- TLS 接続の信頼関係の設定 (176 ページ)

LDAP サーバ設定オブジェクトのアクティブ化

接続状態を READY に設定することによって、LDAP サーバ設定オブジェクトをアクティブにします。これにより、LDAP ユーザ認証が有効になります。

前提条件

MANAGE ANY LDAP SERVER システム権限が必要です。

手順

LDAP サーバ設定オブジェクトの属性値は `ISYSLDAPSERVER` システムテーブルから読み込まれ、LDAP サーバへの新しい接続および SAP Sybase IQ サーバに着信する認証要求に適用されます。ユーザの認証が正常終了すると、LDAP サーバへの接続状態は ACTIVE に変化します。

LDAP サーバ設定オブジェクトをアクティブにするには、次の文を実行します。

```
ALTER LDAP SERVER LDAP_server_name
WITH ACTIVATE
```

参照：

- ALTER LDAP SERVER 文 (249 ページ)
- LDAP サーバ設定オブジェクトのステータス (185 ページ)

LDAP サーバ設定オブジェクトの属性の編集

LDAP サーバに既存の属性を変更します。属性に対するすべての変更は、次回以降の接続に適用されます。変更が適用されたときにすでに開かれていた接続には、変更がすぐに反映されることはありません。

前提条件

MANAGE ANY LDAP SERVER システム権限が必要です。

手順

1. 変更する既存の SEARCH DN 属性を指定します。

表 10 : SEARCH DN 属性

属性	有効な値
URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
ACCESS ACCOUNT	外部 LDAP サーバに接続するユーザの識別名。
IDENTIFIED BY	ACCESS ACCOUNT に指定されている識別名に関連付けられたパスワード。
IDENTIFIED BY ENCRYPTED	ACCESS ACCOUNT に指定されている識別名に関連付けられた、暗号化されたパスワード。

2. 変更する既存の LDAPUA 属性を指定します。

表 11 : LDAPUA 属性

属性	有効な値
SEARCH DN	SEARCH DN 属性 (ステップ 1 参照) から定義されるすべての属性。
AUTHENTI-CATION URL	ホスト (名前または IP アドレスで指定)、ポート番号、および指定されたユーザ ID の DN をルックアップするために実行する検索を指定するか、NULL を入力する。 **注意：** サポートされている構文については、「LDAP サーバ設定オブジェクト URL の構文とパラメータ」を参照。
CONNEC-TION TIME-OUT	SAP Sybase IQ と外部 LDAP サーバの間の DN 検索と認証の両方に適用される接続タイムアウト値を指定する。ミリ秒単位で指定し、デフォルト値は 10 秒。
CONNEC-TION RE-TRIES	DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続の再試行回数を指定する。有効な値の範囲は 1 ～ 60 で、デフォルト値は 3。

属性	有効な値
TLS	DN 検索と認証の両方に使用する LDAP サーバへの接続に、TLS とセキュア LDAP プロトコルのいずれを使用するかを定義する。有効な設定は ON および OFF (デフォルト)。 **注意：** 「セキュア LDAP の有効化」と「TLS 接続の信頼関係の設定」を参照。

3. 使用するサーバ句を指定します。

句	説明
WITH SUSPEND	LDAP サーバをメンテナンスモードにする。
WITH ACTIVATE	LDAP サーバを READY 状態にして、LDAP 認証を有効にする。
WITH REFRESH	LDAP ユーザ認証を再初期化する。

4. **ALTER LDAP SERVER** コマンドに適用可能なパラメータと句を指定して実行します。次に例を示します。

```
ALTER LDAP SERVER apps_primary
AUTHENTICATION URL 'ldap://my_LDAPserver:1066/'
CONNECTION RETRIES 10
WITH ACTIVATE
```

参照：
- LDAP サーバ設定オブジェクト URL の構文とパラメータ (187 ページ)
- セキュア LDAP の有効化 (186 ページ)
- ALTER LDAP SERVER 文 (249 ページ)
- TLS 接続の信頼関係の設定 (176 ページ)
- LDAP サーバ設定オブジェクトの検証 (178 ページ)

LDAP サーバ設定オブジェクトの更新

LDAP サーバを再初期化します。LDAP サーバの接続状態が ACTIVE または READY のどちらでもない場合、このコマンドは失敗します。

前提条件
MANAGE ANY LDAP SERVER システム権限が必要です。

手順
LDAP サーバを更新すると、この LDAP サーバへの接続はすべて閉じられ、LDAP サーバ上のオプション値が `ISYSLDAPSERVER` システムテーブルから再度読み込まれます。読み込まれた値は、LDAP サーバへのすべての新しい接続および SAP

Sybase IQ サーバに着信するすべてのユーザ認証要求に適用されます。REFRESH コマンドを実行しても、LDAP サーバの接続状態およびクライアントから SAP Sybase IQ サーバへの既存の接続は、どちらも変更されません。

次回のユーザ認証時にすべての変更が使用されることを保証するには、TRUSTED_CERTIFICATES_FILE データベースオプションを変更した後か、または TRUSTED_CERTIFICATES_FILE データベースオプションで指定されているファイルの内容を変更した後に、LDAP サーバを更新することをおすすめします。

LDAP サーバを更新するには、次の文を実行します。

```
ALTER LDAP SERVER LDAP_server_name
WITH REFRESH
```

参照：

- ALTER LDAP SERVER 文 (249 ページ)
- LDAP サーバ設定オブジェクトのステータス (185 ページ)

LDAP サーバ設定オブジェクトの中断

LDAP サーバをメンテナンスモードにします。LDAP サーバへのすべての接続が閉じられ、LDAP ユーザ認証を使用できなくなります。

前提条件

MANAGE ANY LDAP SERVER システム権限が必要です。

手順

LDAP サーバを中断するには、次の文を実行します。

```
ALTER LDAP SERVER LDAP_server_name
WITH SUSPEND
```

参照：

- ALTER LDAP SERVER 文 (249 ページ)
- LDAP サーバ設定オブジェクトのステータス (185 ページ)

LDAP サーバ設定オブジェクトの削除

READY 状態または ACTIVE 状態のどちらでもない LDAP サーバ設定オブジェクトを削除します。

前提条件

MANAGE ANY LDAP SERVER システム権限が必要です。

手順

READY 状態または ACTIVE 状態のどちらかの LDAP サーバ設定オブジェクトに対して DROP 文を発行すると、失敗します。また、削除する LDAP サーバ設定オブジェクトを参照するログインポリシーが存在する場合も、DROP 文は失敗します。削除する前に、すべてのログインポリシーから LDAP サーバ設定オブジェクトへの参照が削除されることを保証するには、WITH DROP ALL REFERENCES 句を使用します。サーバ状態チェックを無効にして、現在の状態に関係なくデータベースオブジェクトをメンテナンスモードにするには、LDAP サーバ設定オブジェクトを削除する際に WITH SUSPEND 句を使用します。

LDAP サーバ設定オブジェクトを削除すると、`ISYSLDAPSERVER` システムテーブルから指定されたオブジェクトが削除されます。
LDAP サーバ設定オブジェクトを削除するには、適用可能な句を使用して、次のコマンドを実行します。

```
DROP LDAP SERVER LDAP_Server_name
WITH SUSPEND
WITH DROP ALL REFERENCES
```

例:

次の例では、`ldapserver1` という名前の LDAP サーバ設定オブジェクトをその現在の状態に関係なく削除し、すべてのログインポリシー内の `ldapserver1` への参照を削除します。

```
DROP LDAP SERVER ldapserver1
WITH DROP ALL REFERENCES
WITH SUSPEND
```

次の **DROP LDAP SERVER** コマンドは、`ldapserver2` という名前の LDAP サーバ設定オブジェクトがいずれかのログインポリシーで参照されている場合に失敗します。これは、WITH DROP ALL REFERENCES 句が指定されていないからです。

```
DROP LDAP SERVER ldapserver1
WITH SUSPEND
```

参照：

- DROP LDAP SERVER 文 (284 ページ)
- LDAP サーバ設定オブジェクトのステータス (185 ページ)

LDAP サーバ設定オブジェクトのステータス

LDAP サーバ設定オブジェクトの可能なステータスのリスト。

LDAP サーバ設定オブジェクトのステータスは、書き込み可能データベースの `ISYSLDAPSERVER` システムテーブル内に永続的に保持され、LDAP ユーザ認証の可視性を管理者に提供します。LDAP サーバ設定オブジェクトが再起動された場

合は、シャットダウン時の状態が保持されます。これにより、LDAP サーバ設定オブジェクトの保持は、再起動時の全体にわたって有効になります。読み取り専用のデータベースの場合、ステータスの変化は永続的には保持されません。メモリのみに保持されるので、データベースがシャットダウンされると情報が失われます。接続状態は、読み取り専用のデータベースの値を使用して起動時に設定され、一時的な状態変化はメモリ内で行われ、LDAP ユーザ認証を提供します。

LDAP サーバ設定オブジェクトで発生する可能性があるステータスは次のとおりです。

- **RESET** – LDAP サーバ設定オブジェクトの 1 つ以上の属性が、前回の有効化時以降に入力または変更されています。
- **READY** – LDAP サーバ設定オブジェクトの接続準備が整っています。
- **ACTIVE** – LDAP サーバ設定オブジェクトが 1 回以上、LDAP ユーザ認証に成功しています。
- **FAILED** – LDAP サーバ設定オブジェクトへの接続に問題が発生しています。
- **SUSPENDED** – LDAP サーバ設定オブジェクトはメンテナンスモードで、LDAP ユーザ認証に使用できません。

セキュア LDAP の有効化

セキュア LDAP は、TLS 証明書による認証を使用して、なりすましから保護します。

TLS 証明書を使用すると、サーバの自己申告が正しいことの証明付きで LDAP サーバにクライアントが接続できます。

LDAP サーバ設定オブジェクトでセキュア LDAP を有効にするには、次の 2 つの形式のいずれかを使用します。

- **ldaps://** – LDAP サーバ設定オブジェクトで、SEARCH DN URL 属性または AUTHENTICATION URL 属性を定義する際は、ldaps:// を使用し、TLS 属性を OFF に設定します。
- **TLS パラメータ** – LDAP サーバ設定オブジェクトで、SEARCH DN URL 属性を定義する際は、ldap:// を使用し、TLS 属性を ON に設定します。

注意： Active Directory (AD)、Tivoli、SunONE Oracle DS、および OpenLDAP の現在のバージョンは両方のオプションをサポートしています。以前のバージョンでは 1 つのオプションしかサポートしていない場合があります。全バージョンとの互換性を確保するため、SAP Sybase IQ では両方のオプションがサポートされています。

LDAP サーバ設定オブジェクト URL の構文とパラメータ

URL は、ホスト (ユーザまたは IP アドレスによる)、ポート番号、および LDAP サーバに対するセキュアな識別名 (DN) ルックアップの実行時に行われる検索を特定します。

LDAP サーバに対するセキュアな接続の実行方法に応じて、URL の構文は 2 つの形式のうちのいずれかを使用します。URL の基礎となるパラメータはどちらの形式でも同じです。

- **ldaps:// –** LDAP サーバ設定オブジェクトで、SEARCH DN URL 属性または AUTHENTICATION URL 属性を定義する際は、ldaps:// を使用し、TLS 属性を OFF に設定します。

```
ldapurl::=ldaps://host:[port]/[node]?[attributes]? [base | one |
sub]? [filter]
```

- **TLS パラメータ –** LDAP サーバ設定オブジェクトで、SEARCH DN URL 属性を定義する際は、ldap:// を使用し、TLS 属性を ON に設定します。

```
ldapurl::=ldap://host:[port]/[node]?[attributes]? [base | one |
sub]? [filter]
```

パラメータ	説明
host	LDAP サーバのホスト名。
port	LDAP サーバのポート番号。
node	検索を開始するオブジェクト階層のノード。
attributes	結果セットに返される属性リスト。各 LDAP サーバは、LDAP サーバで使用されるスキーマに応じてさまざまな属性をサポートできる。ただし、各 LDAP サーバでは、最初の属性のみ使用され、この属性がユーザの識別名 (DN) を返す。
base | one | sub	検索条件を修飾する。 base – ベースノードの検索を指定する。 one – ノードと 1 つのサブレベルの検索を指定する。 sub – ノードと全サブレベルの検索を指定する。
filter	データベースユーザの識別名 (DN) の検索に使用する属性を指定する。フィルタは、"uid=*," のように単純にも、"(uid=*)(ou=group)" など複合的にもできる。フィルタ内の属性は、LDAP サーバのスキーマによって異なる。DN の検索時は、LDAP ユーザ認証により各ワイルドカード文字 (*) がデータベースユーザ ID に置換される。

当初、URL は LDAP サーバ設定オブジェクトの作成時にサーバ属性の 1 つとして定義され、いつでも変更可能です。これらのパラメータにデフォルト値はありません。LDAP サーバ設定オブジェクトの作成または変更には、MANAGE ANY LDAP SERVER システム権限が必要です。

注意： Active Directory (AD)、Tivoli、SunONE Oracle DS、および OpenLDAP の現在のバージョンは両方のオプションをサポートしています。以前のバージョンでは 1 つのオプションしかサポートしていない場合があります。全バージョンとの互換性を確保するため、SAP Sybase IQ では両方のオプションがサポートされています。

LDAP ユーザ認証ログインポリシーオプションの管理

LDAP ユーザ認証固有のログインポリシーオプションは複数あります。これらのオプションは、LDAP ユーザ認証を使用するユーザに割り当てるログインポリシー (ルートを含む) で定義する必要があります。

LDAP サーバデータベースオブジェクト固有のオプションは、ログインポリシーを最初に作成するときに定義するか、ルートログインポリシーを含む既存のポリシーに追加できます。

ログインポリシーオプションの定義には、MANAGE ANY LOGIN POLICY システム権限が必要です。

ルートログインポリシーの変更

ルートログインポリシーのオプション値は変更できますが、ポリシーの削除はできません。

前提条件

MANAGE ANY LOGIN POLICY システム権限。

手順

新しいデータベースはそれぞれ、ルートポリシーと呼ばれるデフォルトのログインポリシーで作成されます。ログインポリシーを指定しないでユーザアカウントを作成した場合、そのユーザはルートログインポリシーに属します。
ルートログインポリシーのオプションを変更するには、以下を実行します。

```
ALTER LOGIN POLICY ROOT {login_policy_options}
```

参照：

- 既存のログインポリシーの変更 (189 ページ)
- 新しいログインポリシーの作成 (189 ページ)
- ログインポリシーの既存ユーザへの割り当て (190 ページ)
- LDAP ユーザ認証ログインポリシーオプションの管理 (188 ページ)

- ALTER LOGIN POLICY 文 (252 ページ)

既存のログインポリシーの変更
既存のログインポリシー内でオプションを変更します。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順
既存のログインポリシーのオプションを変更するには、以下を実行します。

```
ALTER LOGIN POLICY policy-name {login_policy_options}
```

例:

次の文は、`Test1` ログインポリシーの LOCKED オプションと MAX_CONNECTIONS オプションを変更します。

```
ALTER LOGIN POLICY Test1
locked=on
max_connections=5
```

参照：
- ルートログインポリシーの変更 (188 ページ)
- 新しいログインポリシーの作成 (189 ページ)
- ログインポリシーの既存ユーザへの割り当て (190 ページ)
- LDAP ユーザ認証ログインポリシーオプションの管理 (188 ページ)
- ALTER LOGIN POLICY 文 (252 ページ)

新しいログインポリシーの作成
ログインポリシーの作成時に明示的に設定されなかったオプションは、その値をルートログインポリシーから継承します。

前提条件
MANAGE ANY LOGIN POLICY システム権限。

手順
ログインポリシー名はユニークである必要があります。追加するログインポリシー名が既存の場合には、エラーメッセージが表示されます。
新しいログインポリシーを作成するには、以下を実行します。

```
CREATE LOGIN POLICY policy_name {login_policy_options}
```

例:

次の文では、Test1 ログインポリシーが作成され、PASSWORD_LIVE_TIME オプションが 60 日に設定されます。

```
CREATE LOGIN POLICY Test1
password_life_time=60
```

参照：

- ルートログインポリシーの変更 (188 ページ)
- 既存のログインポリシーの変更 (189 ページ)
- ログインポリシーの既存ユーザへの割り当て (190 ページ)
- LDAP ユーザ認証ログインポリシーオプションの管理 (188 ページ)
- CREATE LOGIN POLICY 文 (271 ページ)

ログインポリシーの既存ユーザへの割り当て

既存の SAP Sybase IQ ユーザにログインポリシーを割り当てます。

前提条件

MANAGE ANY LOGIN POLICY システム権限。

手順

1. 以下を実行します。

   ```
   ALTER USER userID
   LOGIN POLICY policy_name
   ```

2. 新しいログインポリシーを適用するには、ユーザにいったんログアウトしてからログインしなおすように求めます。

参照：

- ルートログインポリシーの変更 (188 ページ)
- 既存のログインポリシーの変更 (189 ページ)
- 新しいログインポリシーの作成 (189 ページ)
- ALTER USER 文 (263 ページ)

LDAP ユーザ認証を使用する場合のユーザとパスワードの管理

LDAP ユーザ認証を使用して SAP Sybase IQ にログインするには、各ユーザが、外部 LDAP サーバ上にアクティブなユーザ ID とパスワード、さらに SAP Sybase IQ サーバ上にアクティブなユーザ ID を持っている必要があります。

SAP Sybase IQ で新しいユーザを作成する場合、必須ではありませんが、最初に LDAP ユーザ認証によるログインが行われるまで新しいユーザアカウントが保護

なしの状態にならないようにするため、パスワードを指定することをおすすめします。

新しいユーザが初めてログオンする際または既存ユーザがパスワード変更後に初めてログインする際、SAP Sybase IQ データベース内のパスワードは、外部 LDAP サーバで定義されている対応するユーザパスワードで自動的に上書きされます。したがって、LDAP ユーザ認証を使用するユーザが SAP Sybase IQ のパスワードに対して実行する必要がある保守作業はすべて、SAP Sybase IQ サーバ上ではなく、常に外部 LDAP サーバ上で実行する必要があります。

このパスワードの自動同期の結果として、標準認証の使用を許可されたユーザ (パスワードは SAP Sybase IQ データベースに定義) は、標準認証を使用してログオンを試行する際に、LDAP サーバクレデンシャルの使用を続行する必要があります。

ユーザの現在のステータス情報の表示

sa_get_user_status ストアドプロシージャを実行して、ユーザの現在のステータスに関するレポートを生成します。

レポートには、接続および失敗したログインに関する情報、さらにユーザがロックアウトされているかどうか、ロックされている場合はその理由が出力されます。ユーザが LDAP ユーザ認証で認証されている場合は、ユーザの識別名およびその識別名が見つかった日時も出力されます。

このストアドプロシージャを実行するには、MANAGE ANY USER システム権限が必要です。MANAGE ANY USER システム権限を持たないユーザは、MANAGE ANY USER システム権限を付与されているユーザが所有するカバープロシージャを作成して実行することによって、ユーザ情報を取得できます。

参照：

- sa_get_user_status システムプロシージャ (353 ページ)

LDAP サーバ設定オブジェクトの現在のステータスの表示

sa_get_ldapserver_status ストアドプロシージャを実行して、LDAP サーバ設定オブジェクトの現在のステータスに関するレポートを生成します。

ステータス情報には、LDAP サーバ設定オブジェクトの名前、オブジェクト識別子、現在の状態、および最終状態変更日時が含まれます。設定が適切で正常に動作している LDAP サーバ設定オブジェクトの状態は READY または ACTIVE です。

このストアドプロシージャを実行するために必要なシステム権限はありません。

参照：

- sa_get_ldapserver_status システムプロシージャ (352 ページ)

Kerberos 認証

Kerberos ログイン機能を使用すると、データベース接続、オペレーティングシステム、ネットワークのログインを、単一のユーザ ID とパスワードで管理できます。Kerberos ログインの使用は、ユーザにとって便利であると同時に、1 つのセキュリティシステムでデータベースとネットワークのセキュリティを維持できます。次のような利点があります。

- ユーザはデータベースに接続するときにユーザ ID やパスワードを入力しなくてよい
- 複数のユーザを 1 つのデータベースユーザ ID にマッピングできる
- Kerberos へのログインに使用する名前とパスワードはデータベースユーザの ID とパスワードと一致している必要がない

Kerberos は、秘密鍵暗号を使用して強力な認証と暗号化を実現するネットワーク認証プロトコルです。Kerberos にログインしているユーザは、ユーザ ID やパスワードを指定しなくてもデータベースに接続できます。

認証に Kerberos を使用できます。認証を Kerberos に委任するには、次の処理を行います。

- Kerberos ログインを使用するようにサーバとデータベースを設定する。
- コンピュータまたはネットワークにログインするユーザ ID と、データベースユーザの間にマッピングを作成する。

警告！ 警告

Kerberos ログインを単一のセキュリティソリューションとして使用する場合に検討する必要があるセキュリティ上の重要事項があります。

Kerberos ソフトウェアは SAP Sybase IQ に含まれません。このソフトウェアは別途入手してください。Kerberos ソフトウェアには次のコンポーネントが含まれます。

- **Kerberos ライブラリ** – Kerberos クライアントまたは GSS (Generic Security Services)-API ランタイムライブラリと呼ばれています。Kerberos ライブラリは、明確に定義されている GSS-API を実装したもので、Kerberos を使用するクライアントコンピュータおよびサーバコンピュータでそれぞれ必要です。KDC として Active Directory を使用する場合は、サードパーティ製 Kerberos クライアントライブラリの代わりに、組み込みの Windows SSPI インタフェースを使用できます。

SSPI は、SAP Sybase IQ クライアントのみが Kerberos 接続パラメータで使用できます。SAP Sybase IQ データベースサーバは SSPI を使用できません。サポートされる SSPI 以外の Kerberos クライアントを使用する必要があります。

- **Kerberos キー配布センター (KDC) サーバ –** KDC はユーザおよびサーバの保管場所として機能します。また、ユーザやサーバの ID を検証します。KDC は、通常、アプリケーションやユーザログインに使用しないサーバコンピュータにインストールされます。

SAP Sybase IQ は、DBLib クライアント、ODBC クライアント、OLE DB クライアント、ADO.NET クライアント、Sybase Open Client、jConnect クライアントからの Kerberos 認証をサポートします。Kerberos 認証は SAP Sybase IQ トランスポートレイヤセキュリティ暗号化と組み合わせて使用できますが、SAP Sybase IQ はネットワーク通信での Kerberos 暗号化をサポートしていません。

Windows では、Kerberos を Windows ドメインとドメインアカウントに使用します。Active Directory Windows Domain Controllers は Kerberos KDC を実装します。この環境で認証を行うには、データベースサーバコンピュータにサードパーティ製 Kerberos クライアントまたはランタイムが必要ですが、Windows クライアントコンピュータはサードパーティ製 Kerberos クライアントまたはランタイムの代わりに組み込み Windows SSPI インタフェースを使用できます。

Kerberos クライアント

Kerberos 認証がサーバプラットフォームで利用できます。テスト済みの Kerberos クライアントのリストについては、http://www.sybase.com/detail?id=1061807 を参照してください。

サポートされている Kerberos クライアントが使用する keytab ファイルと GSS-API ファイルのデフォルトの名前とロケーションのリストを次の表に示します。

注意： SSPI は、SAP Sybase IQ クライアントのみが Kerberos 接続パラメータで使用できます。SAP Sybase IQ データベースサーバは SSPI を使用できません。サポートされる SSPI 以外の Kerberos クライアントを使用する必要があります。

Kerberos クライアント	デフォルト keytab ファイル	GSS-API ライブラリファイル名	説明
Windows MIT Kerberos クライアント	`C:¥WINDOWS¥krb5kt`	`gssapi32.dll` または `gssapi64.dll`	KRB5_KTNAME 環境変数を設定してからデータベースサーバを起動することで、別の keytab ファイルを指定できます。

Kerberos クライアント	デフォルト keytab ファイル	GSS-API ライブラリファイル名	説明
Windows CyberSafe Kerberos クライアント	C:¥Program Files¥Cyber-Safe¥ v5srvtab	gssapi32.dll または gssapi64.dll	CSFC5KTNAME 環境変数を設定してからデータベースサーバを起動することで、別の keytab ファイルを指定できます。
UNIX MIT Kerberos クライアント	/etc/ krb5.keytab	libgssapi_ krb5.so [1]	KRB5_KTNAME 環境変数を設定してからデータベースサーバを起動することで、別の keytab ファイルを指定できます。
UNIX CyberSafe Kerberos クライアント	/krb5/ v5srvtab	libgss.so [1]	CSFC5KTNAME 環境変数を設定してからデータベースサーバを起動することで、別の keytab ファイルを指定できます。
UNIX Heimdal Kerberos クライアント	/etc/ krb5.keytab	libgssapi.so.1 [1]	

[1] ファイル名はオペレーティングシステムと Kerberos クライアントバージョンによって異なります。

SAP Sybase IQ で使用するための Kerberos システムの設定

SAP Sybase IQ で使用するように Kerberos 認証を設定することができます。

前提条件

Kerberos 認証を使用してコンピュータにログインする必要があります。

手順

Kerberos は、秘密鍵暗号を使用して強力な認証と暗号化を実現するネットワーク認証プロトコルです。

1. 必要に応じて、Kerberos クライアントソフトウェア (GSS-API ランタイムライブラリを含む) をクライアントとサーバの両方にインストールし、設定を行います。

Active Directory Key Distribution Center (KDC) を使用する Windows クライアントコンピュータでは、SSPI を使用でき、Kerberos クライアントをインストールする必要はありません。

2. 必要に応じて、Kerberos KDC でユーザごとに Kerberos プリンシパルを作成します。

   Kerberos プリンシパルとは Kerberos ユーザ ID であり、形式は *user*/*instance*@*REALM* です。/*instance* はオプションです。すでに Kerberos を使用している場合は、プリンシパルがすでに存在しているので、ユーザごとに Kerberos プリンシパルを作成する必要はありません。

   プリンシパルの大文字と小文字は区別されるため、正しく指定する必要があります。大文字と小文字の違いしかない複数のプリンシパルのマッピングはサポートされていません (たとえば、jjordan@MYREALM.COM と JJordan@MYREALM.COM の両方にマッピングすることはできません)。

3. Kerberos プリンシパルを SAP Sybase IQ データベースサーバの KDC に作成します。

   データベースサーバ用のデフォルトの Kerberos プリンシパルの形式は *server-name*@*REALM* です。*server-name* は SAP Sybase IQ データベースサーバ名です。別のサーバプリンシパルを使用する場合は、-kp サーバオプションを使用します。プリンシパルは大文字と小文字が区別されます。*server-name* には、マルチバイト文字、/、¥、または @ を含めることはできません。

   サーバでは KDC 認証に keytab ファイルが使用されるので、KDC 内にサーバサービスプリンシパルを作成する必要があります。keytab ファイルは保護および暗号化されます。

4. セキュリティに十分注意しながら、プリンシパル *server-name*@*REALM* 用の keytab ファイルを KDC から抽出し、SAP Sybase IQ データベースサーバを実行中のコンピュータにコピーします。keytab ファイルのデフォルトロケーションは、Kerberos クライアントとプラットフォームによって異なります。keytab ファイルのパーミッションは、SAP Sybase IQ サーバが読み取ることができ、不正なユーザに読み取りパーミッションがないよう設定する必要があります。

Kerberos システムが認証され、SAP Sybase IQ で使用するように設定されます。

次のステップ

Kerberos を使用するように、SAP Sybase IQ データベースサーバとデータベースを設定します。

Kerberos を使用するための SAP Sybase IQ データベースの設定

Kerberos ログインを使用するように SAP Sybase IQ データベースを設定できます。

前提条件

SET ANY PUBLIC OPTION システム権限と MANAGE ANY USER システム権限が必要です。

Kerberos の設定について、SAP Sybase IQ で使用できるように設定を済ませている必要があります。

手順

Kerberos ログイン機能を使用すると、データベース接続、オペレーティングシステム、ネットワークのログインを、単一のユーザ ID とパスワードで管理できます。

1. SAP Sybase IQ データベースサーバを -krb または -kr オプションを使用して起動し、Kerberos 認証を有効にします。また、-kl オプションを使用して GSS-API ライブラリのロケーションを指定し、Kerberos を有効にすることもできます。
2. パブリックオプションまたは一時的なパブリックオプション login_mode を Kerberos を含む値に変更します。データベースオプションはそれらが見つかったデータベースにのみ適用されるので、複数のデータベースが同じデータベースサーバにロードされ実行されていても、データベースごとに異なる Kerberos ログイン設定を持たせることができます。次に例を示します。

   ```
   SET OPTION PUBLIC.login_mode = 'Kerberos,Standard';
   ```

   警告！ 警告

   login_mode データベースオプションを Kerberos に設定すると、接続できるのは、Kerberos ログインマッピングを付与されているユーザだけに制限されます。SYS_AUTH_DBA_ROLE システムロールを持つユーザでないかぎり、ユーザ ID とパスワードを使用して接続しようとすると、エラーが発生します。
3. クライアントユーザのデータベースユーザ ID を作成します。既存のデータベースユーザに適切な権限があれば、そのデータベースユーザ ID を Kerberos ログインに使用できます。次に例を示します。

   ```
   CREATE USER "kerberos-user"
   IDENTIFIED BY abc123;
   ```
4. GRANT KERBEROS LOGIN TO 文を実行して、クライアントの Kerberos プリンシパルから既存のデータベースユーザ ID へのマッピングを作成します。次に例を示します。

```
GRANT KERBEROS LOGIN TO "pchin@MYREALM.COM"
AS USER "kerberos-user";
```

使用されている Kerberos プリンシパルにマッピングがない場合に接続するには、Guest データベースユーザ ID が存在することと、パスワードがあることを確認します。

5. クライアントユーザが Kerberos プリンシパルを使用してログオン済みである (有効な Kerberos TGT：Ticket Granting Ticket がある) こと、およびクライアントの Kerberos チケットの期限が切れていないことを確認します。ドメインアカウントにログインしている Windows ユーザは、TGT をすでに持っており、プリンシパルに必要なパーミッションがあれば、サーバに認証されます。

   チケット付与権限付きチケットはユーザパスワードを使用して暗号化された Kerberos チケットで、ユーザ ID の検証に Ticket Granting Service が使用します。

6. KERBEROS 接続パラメータ (通常は KERBEROS=YES、ただし KERBEROS=SSPI または KERBEROS=*GSS-API-library-file* も使用可) を指定して、クライアントから接続します。ユーザ ID またはパスワードの接続パラメータが指定された場合は、無視されます。次に例を示します。

   ```
   dbisql -c "KERBEROS=YES;Server=my_server_princ"
   ```

SAP Sybase IQ データベースが Kerberos 認証を使用するように設定されます。

次のステップ

Kerberos 認証を使用してクライアントから接続することができます。または、Kerberos ログインマッピングを作成することもできます。

Sybase Open Client または jConnect アプリケーションからの接続

Sybase Open Client または jConnect アプリケーションから接続するには、次の手順に従います。

- Kerberos 認証を設定します。
- Kerberos を使用するように SAP Sybase IQ を設定します。
- Adaptive Server Enterprise での Kerberos 認証と同様に、Sybase Open Client または jConnect を設定します。サーバ名は SAP Sybase IQ サーバ名である必要があります。名前の大文字と小文字は区別されます。Sybase Open Client または jConnect から代替サーバ名を使用して接続することはできません。

Windows で Kerberos ログインに SSPI を使用する

Windows ドメインでは、クライアントコンピュータに Kerberos クライアントをインストールしなくても、Windows ベースのコンピュータで SSPI を使用できます。Windows ドメインアカウントには、関連付けられた Kerberos プリンシパルがあらかじめ用意されています。

前提条件

Kerberos の設定について、SAP Sybase IQ で使用できるように設定を済ませている必要があります。SAP Sybase IQ のデータベースサーバとデータベースについて、Kerberos を使用できるように設定を済ませている必要があります。

手順

SSPI は、SAP Sybase IQ クライアントのみが Kerberos 接続パラメータで使用できます。SAP Sybase IQ データベースサーバは SSPI を使用できません。サポートされる SSPI 以外の Kerberos クライアントを使用する必要があります。

クライアントコンピュータからデータベースに接続します。次に例を示します。

```
dbisql -c "KERBEROS=SSPI;Server=my_server_princ"
```

接続文字列に Kerberos=SSPI と指定されている場合、Kerberos ログインが試行されます。

次の SQL 文を使用した接続も成功します。ただし、接続が成功するためには、データベースサーバ上のデフォルトデータベースの Kerberos ログインマッピングと一致するユーザプロファイル名を使用してユーザがすでにログオンしていることが必要です。

```
CONNECT USING 'KERBEROS=SSPI';
```

Windows で Kerberos 認証に SSPI を使用できます。

トラブルシューティング：Kerberos 接続

Kerberos 認証を有効にしようとしたり、使おうとしたりしたときに予期しないエラーが発生した場合は、データベースサーバとクライアントで追加の診断メッセージを有効にすることをおすすめします。

データベースサーバの起動時に -z オプションを指定します。または、すでに実行中のサーバのデータベースサーバメッセージログに追加の診断メッセージを表示するには `CALL sa_server_option( 'DebuggingInformation', 'ON' )` を使用します。LogFile 接続パラメータを使用すると、指定したファイルにクライアント診断メッセージが書き込まれます。

LogFile 接続パラメータを使用する代わりに、-z パラメータを使用して Ping ユーティリティ (dbping) を実行することができます。-z パラメータにより診断メッセージが表示され、接続の問題の原因を特定するのに役立ちます。

データベースサーバの起動に関する問題

現象	一般的な解決策
「Kerberos GSS-API ライブラリをロードできません。」メッセージ	• Kerberos クライアントが、GSS-API ライブラリも含めて、データベースサーバコンピュータにインストールされていることを確認します。 • ロードしようとしたライブラリ名が、データベースサーバの -z 出力にリストされます。ライブラリ名が正しいことを確認します。必要に応じて、-kl オプションを使用して正しいライブラリ名を指定します。 • フォルダと、サポートしているライブラリが、ライブラリパス (Windows では %PATH%) にリストされていることを確認します。 • GSS-API ライブラリにエントリポイントがないことがデータベースサーバの -z 出力に示されていた場合、そのライブラリはサポートされている Kerberos Version 5 GSS-API ライブラリではありません。
「サーバ名 "*server-name*" の Kerberos クレデンシャルを取得できません。」メッセージ	• *server-name*@*REALM* のプリンシパルが KDC にあることを確認します。プリンシパルは大文字と小文字が区別されるので、データベースサーバ名とプリンシパル名のユーザ部分の大文字と小文字が一致していることを確認します。 • SAP Sybase IQ サーバ名がプリンシパルのプライマリ/ユーザ部分になっていることを確認します。 • サーバのプリンシパルが keytab ファイルに抽出されていること、およびその keytab ファイルが Kerberos クライアントに対して適切なロケーションにあることを確認します。 • データベースサーバコンピュータ上の Kerberos クライアントの領域がサーバプリンシパルの領域と異なっている場合は、-kr オプションを使用してサーバプリンシパルの領域を指定します。
「Kerberos ログインが失敗しました。」クライアントエラー	• データベースサーバの診断メッセージを確認します。サーバが使用する keytab ファイルに関する問題のなかには、クライアントが認証しようとするまで検出されないものがあります。

Kerberos クライアント接続のトラブルシューティング

クライアントが Kerberos 認証を使用して接続しようとしてエラーが発生した場合について、次の表に示します。

現象	一般的な解決策
「Kerberos ログインはサポートされていません。」エラーが発生し、LogFile にメッセージ「Kerberos GSS-API ライブラリのロードに失敗しました」が出力されている。	• Kerberos クライアントが、GSS-API ライブラリも含めて、クライアントコンピュータにインストールされていることを確認します。 • LogFile で指定されたファイルに、ロードしようとしたライブラリがリストされています。ライブラリ名が正しいことを確認し、必要に応じて Kerberos 接続パラメータを使用して正しいライブラリ名を指定します。 • サポートしているライブラリがあるディレクトリがライブラリパス (Windows では %PATH%) にリストされていることを確認します。 • GSS-API ライブラリにエントリポイントがないことが LogFile 出力に示されていた場合、そのライブラリはサポートされている Kerberos Version 5 GSS-API ライブラリではありません。
「Kerberos ログインはサポートされていません。」エラー	• データベースサーバに対して -krb、-kl、-kr の各サーバオプションが 1 つ以上指定されており、Kerberos ログインが有効になっていることを確認します。 • Kerberos がクライアントとサーバの両プラットフォーム上の SAP Sybase IQ でサポートされていることを確認します。
「Kerberos ログインが失敗しました。」エラー	• ユーザが Kerberos にログイン済みであること、およびそのユーザに期限が切れていない有効なチケット付与権限付きチケットがあることを確認します。 • クライアントコンピュータとサーバコンピュータとの間で、時刻のずれが 5 分未満であることを確認します。
「ログインモード 'Kerberos' は、login_mode 設定で許可されていません。」エラー	• Kerberos ログインが許可されるには、login_mode オプションのパブリックまたは一時的なパブリックのデータベースオプションの設定に値 Kerberos が含まれている必要があります。

現象	一般的な解決策
"ログイン ID '*client-Kerberos-principal* はどのデータベースユーザ ID にもマップされていません。"	• Kerberos プリンシパルが GRANT KERBEROS LOGIN 文を使用してデータベースユーザ ID にマッピングされている必要があります。GRANT KERBEROS LOGIN 文には、領域を含む完全なクライアントプリンシパルが指定されている必要があります。また、インスタンスまたは領域しか違わないプリンシパルも別のプリンシパルとして扱われます。 • また、明示的にマッピングされていない有効な Kerberos プリンシパルを接続可能にするには、GRANT CONNECT を使用して、ゲストデータベースユーザ ID とパスワードを作成します。

セキュリティについての考慮事項：セキュリティを強化するための一時的なパブリックオプション

与えられたデータベースに対して login_mode オプションの値を設定し、SET OPTION 文を使用した標準、統合化、Kerberos、LDAPUA の各ログインの組み合わせを永続的に許可すると、指定されたタイプのログインがそのデータベースに対して有効になります。たとえば、次の文は標準ログインと統合化ログインを永続的に許可します。

```
SET OPTION PUBLIC.login_mode = 'Standard,Integrated';
```

データベースを停止して再起動した場合でも、このオプションの値は変わらず、統合化ログインは有効のままです。

SET TEMPORARY OPTION を使用して login_mode オプションを設定した場合、統合化ログインによるユーザアクセスは可能ですが、データベースがシャットダウンされるまでの間に限られます。次の文は、オプションの値を一時的に変更します。

```
SET TEMPORARY OPTION PUBLIC.login_mode = 'Standard,Integrated';
```

永久オプション値が Standard の場合、データベースは停止時にその値に戻ります。

一時的なパブリックオプションを設定すると、データベースのセキュリティを強化できます。統合化、Kerberos、または LDAPUA のログインをデータベースに追加すると、データベースを実行しているオペレーティングシステムのセキュリティがそのデータベースで利用されます。データベースを別のコンピュータにコピーすると、データベースへのアクセスは SAP Sybase IQ のセキュリティモデルに戻ります。

セキュリティについての考慮事項：コピーされたデータベースファイル

データベースファイルがコピー可能な場合、統合化ログインと Kerberos ログインに一時的なパブリック login_mode オプションを使用してください。ファイルをコピーした場合、統合化ログインと Kerberos ログインはデフォルトでサポートされません。

データベースに機密情報が含まれる場合、データベースファイルが保存されているコンピュータを不正アクセスから保護する必要があります。保護しなかった場合、データベースファイルがコピーされ、別のコンピュータからデータに不正にアクセスされる可能性があります。データベースのセキュリティを強化するには、次の処理を行います。

- パスワードを複雑にして、推測しにくくします。
- PUBLIC.login_mode データベースオプションを Standard に設定します。統合化ログインまたは Kerberos ログインを有効にする場合は、一時的なパブリックオプションのみがサーバの起動ごとに変更されるようにします。これにより、データベースがコピーされたとしても、可能になるのは標準ログインだけになります。
- AES 暗号化アルゴリズムを使用して、データベースファイルを強力に暗号化します。暗号化キーは複雑にして、推測しにくくします。

Kerberos のためのライセンス要件

Advanced Security オプション (IQ_SECURITY) は、環境を不正アクセスから保護します。SAP Sybase IQ で Kerberos ユーザ認証を使用するにはこのオプションが必要です。

SAP Sybase IQ の Advanced Security オプション

SAP® Sybase® IQ Advanced Security オプションでは、カラムの暗号化、FIPS (連邦情報処理規格) 認定のネットワーク暗号化技術と、データベース接続、オペレーティングシステムログイン、ネットワークログインに対する LDAP 認証および Kerberos 認証がサポートされています。Advanced Security オプションは、SAP Sybase IQ の個別にライセンス供与されるオプションです。

SAP Sybase IQ での FIPS サポート

SAP Sybase IQ では、FIPS 認定の暗号化技術がサポートされています。FIPS は、LinuxAMD64 Server、Solaris Sparc Server、Solaris AMD64 Server、LinuxAMD32 Client、および Windows32 Client でサポートされています。

SAP Sybase IQ での FIPS サポートによる主な影響は、暗号化に非決定性を持たせることです。この動作がデフォルトになっています。非決定的アルゴリズムでは、入力値が同じでも毎回異なる出力値が得られます。したがって、文字列を暗号化するキーを使用する場合、暗号化された文字列は毎回異なります。ただしこのアルゴリズムの場合、キーを使用して非決定的結果を復号化することも可能です。この機能により、暗号化アルゴリズムの解析はさらに難しくなり、暗号化はさらに安全になります。

FIPS 認定の暗号化は、すべてのプラットフォームで使用できるわけではありません。サポートされているプラットフォームのリストについては、

SAP Sybase IQ には、RSA と FIPS の両方のセキュリティが組み込まれています。RSA の暗号化では個別のライブラリは必要ありませんが、FIPS では次のオプションライブラリが必要です。

- dbfips16.dll、libeay32.dll、msvcr90.dll、ssleay32.dll (32 ビット Windows)
- dbfips16.dll、libeay32.dll、msvcr100.dll、ssleay32.dll (64 ビット Windows)
- libssl.so および libcrypto.so (Linux)

いずれのセキュリティモデルにも証明書が必要です。`rsaserver` 証明書の名前は、`rsaserver.id` です。

FIPS 認定の暗号化テクノロジ

FIPS 認定のセキュリティアルゴリズムを使用すると、データベースファイルを暗号化したり、データベースクライアント／サーバ通信、Web サービスにおける通信を暗号化できます。

連邦情報処理規格 (FIPS) 140-2 では、セキュリティアルゴリズムの要件を指定しています。FIPS 140-2 は、米国商務省標準技術局 (NIST：National Institute of Standards and Technology) およびカナダ通信安全保障局 (CSE：Canadian Communications Security Establishment) を通じて、米国政府とカナダ政府から付与されます。

FIPS の強制

必要に応じて、FIPS オプションを使用して、クライアントまたはサーバでの FIPS 認定暗号化の使用を強制できます。FIPS オプションをオンに設定すると、セキュリティ保護された通信はすべて FIPS 認定である必要があります。ユーザが非 FIPS の RSA 暗号化を使用しようとした場合、その RSA は自動的に FIPS 認定 RSA にアップグレードされます。FIPS オプションは、FIPS 認定暗号化を強制的に使用するクライアントまたはサーバで設定できます。SAP Sybase IQ サーバには、-fips コマンドラインオプションがあります。クライアントには fips オプションがあり、暗号化接続パラメータを使用して設定できます。

SAP Sybase IQ でのカラムの暗号化

SAP Sybase IQ では、ユーザ暗号化カラムがサポートされています。

SAP Sybase IQ データベースファイルの強力な暗号化では、128 ビットのアルゴリズムと、セキュリティキーを使用します。データは判読不能で、キーがなければ事実上解読できません。サポートされるアルゴリズムは、FIPS-197 (Federal Information Processing Standard for the Advanced Encryption Standard) に準拠しています。

SAP Sybase IQ では、**AES_ENCRYPT** 関数、**AES_DECRYPT** 関数、および **LOAD TABLE ENCRYPTED** 句によってユーザ暗号化カラムをサポートしています。これらの関数をアプリケーションから呼び出すことで、カラムデータを明示的に暗号化および復号化できます。暗号化キーと復号化キーの管理は、アプリケーションで行います。

カラムの暗号化に影響を与えるデータベースオプションがあります。

参照：

- カラムの暗号化に対するデータベースオプション (236 ページ)

カラムの暗号化のためのライセンス要件

SAP Sybase IQ でユーザ暗号化カラムを使用するには Advanced Security オプション (IQ_SECURITY) が必要です。

暗号化に関する用語の定義

格納されているデータの暗号化について説明する場合に使用する用語の定義は、次のとおりです。

- プレーンテキスト - 判読可能な元の形式のデータです。プレーンテキストは文字データに限定されず、データを元の表現方法で記述するために使用されます。
- 暗号化テキスト - プレーンテキスト形式の情報の内容を保持する、判読不能な形式のデータです。
- 暗号化 - プレーンテキストから暗号化テキストへの可逆性のある変換のことです。「暗号文化」とも呼ばれます。
- 復号化 - 暗号化テキストからプレーンテキストへの逆変換のことです。「暗号解除」とも呼ばれます。
- キー - データの暗号化または復号化に使用する数値です。対称キー暗号化方式では、暗号化と復号化の両方に同じキーを使用します。非対称キー暗号化方式では、暗号化と復号化にそれぞれ異なる (ただし数学的に関連した) キーを使用します。SAP Sybase IQ インタフェースは文字列をキーとして受け入れます。
- Rijndael – 「ラインダール」と読みます。さまざまなキーサイズとブロックサイズをサポートする暗号化アルゴリズムです。このアルゴリズムは、単純なバイト全体の操作を使用するように設計されているため、ソフトウェアで比較的簡単に実装できます。
- AES - Advanced Encryption Standard の略です。慎重に扱う必要があるが機密ではない電子データの保護用に FIP が承認した暗号化アルゴリズムです。AES は、ブロックサイズとキー長を制限した Rijndael アルゴリズムを採用しています。AES は、SAP Sybase IQ がサポートするアルゴリズムです。

暗号化カラムのデータ型

暗号化カラムでサポートされるデータ型と、これらのデータ型の処理は、次のとおりです。

サポートされるデータ型

AES_ENCRYPT 関数の最初のパラメータには、次のサポートされるデータ型のいずれかを指定する必要があります。

CHAR	NUMERIC

VARCHAR	FLOAT
TINYINT	REAL
SMALLINT	DOUBLE
INTEGER	DECIMAL
BIGINT	DATE
BIT	TIME
BINARY	DATETIME
VARBINARY	TIMESTAMP
UNSIGNED INT	SMALLDATETIME
UNSIGNED BIGINT	

LOB データ型は、現時点では SAP Sybase IQ のカラム暗号化でサポートされていません。

データ型の保持

SAP Sybase IQ では、**AES_DECRYPT** 関数が、データ型をパラメータとして受け取るか、**CAST** 関数の中に含まれていれば、データを復号化したときにプレーンテキストの元のデータ型の保持が保証されます。

SAP Sybase IQ は、**CAST** 関数のターゲットのデータ型と、元の暗号化されたデータのデータ型を比較します。この 2 つのデータ型が一致しない場合は、元のデータ型とターゲットのデータ型に関する詳細情報と一緒に -1001064 エラーが返されます。

たとえば、暗号化された VARCHAR(1) 値に対し、次の復号化文が有効であるとします。

```
SELECT AES_DECRYPT ( thecolumn, 'theKey',
VARCHAR(1) ) FROM thetable
```

データを、次の文を使用して復号化しようとしたとします。

```
SELECT AES_DECRYPT ( thecolumn, 'theKey',
SMALLINT ) FROM thetable
```

この場合、次のエラーが返されます。

```
Decryption error: Incorrect CAST type smallint(5,0)
for decrypt data of type varchar(1,0).
```

このようなデータ型のチェックは、**CAST** またはデータ型パラメータが指定された場合にのみ実行されます。そうでない場合、クエリは暗号化テキストをバイナリデータとして返します。

次の文のように、リテラル定数に対して **AES_ENCRYPT** 関数を使用したとします。

```
INSERT INTO t (cipherCol) VALUES (AES_ENCRYPT (1, 'key'))
```

1 のデータ型はあいまいになります。1 のデータ型は、TINYINT、SMALLINT、INTEGER、UNSIGNED INT、BIGINT、UNSIGNED BIGINT、およびその他のデータ型になる可能性があります。

あいまいさの問題を解決するには、次のように **CAST** 関数を明示的に使用する必要があります。

```
INSERT INTO t (cipherCol)
VALUES ( AES_ENCRYPT (CAST (1 AS UNSIGNED INTEGER), 'key'))
```

データを暗号化するときに **CAST** 関数を使用してデータ型を明示的に変換しておけば、データを復号化するときに **CAST** 関数を使用することで問題の発生を防止できます。

暗号化対象のデータがカラムのデータの場合、または暗号化されたデータが **LOAD TABLE** によって挿入された場合は、あいまいさは発生しません。

暗号化テキストに対する異なるデータ型の影響

さまざまなデータ型の同一の暗号化テキストを生成するには、**AES_ENCRYPT** の入力を同じデータ型にキャストすることで同一の暗号化テキストを生成します。

AES_ENCRYPT 関数によって生成される暗号化テキストは、入力値とキーが同じであっても、データ型が異なれば違ったものになります。したがって、2 つの暗号化テキストカラムに、2 つの異なるデータ型を持つ暗号化した値が保持されている場合、それらのカラムをジョインして同じ結果が返されるとは限りません。

たとえば、次の行を実行したとします。

```
CREATE TABLE tablea(c1 int, c2 smallint);
INSERT INTO tablea VALUES (100,100);
```

値 AES_ENCRYPT(c1, 'key') は AES_ENCRYPT(c2,'key') と異なり、値 AES_ENCRYPT(c1,'key') は AES_ENCRYPT(100,'key') と異なります。

この問題を解決するには、**AES_ENCRYPT** の入力を同じデータ型にキャストします。たとえば、次のサンプルコードの結果は同じになります。

```
AES_ENCRYPT(c1, 'key');
```

```
AES_ENCRYPT(CAST(c2 AS INT), 'key');
```

```
AES_ENCRYPT(CAST(100 AS INT), 'key');
```

参照：

- AES_ENCRYPT 関数 [文字列] (208 ページ)

AES_ENCRYPT 関数 [文字列]

指定された暗号化キーを使用して、指定された値を暗号化し、VARBINARY または LONG VARBINARY を返します。

構文

```
AES_ENCRYPT( string-expression, key )
```

パラメータ

string-expression – 暗号化されるデータ。**AES_ENCRYPT** にはバイナリ値を渡すこともできます。データベースで大文字と小文字が区別されない場合でも、このパラメータでは大文字と小文字が区別されます。

key – *string-expression* の暗号化に使用される暗号化キー。元の値を取得するには、値を復号化するときにも同じキーを使用します。データベースで大文字と小文字が区別されない場合でも、このパラメータでは大文字と小文字が区別されます。

ほとんどのパスワードの場合と同様に、キーの値には推測されにくい値を選択します。キーの値には、少なくとも 16 文字の長さを持ち、大文字と小文字を含み、数字、特殊文字を使用したものを選びます。このキーは、データを復号化するときに常に必要です。

警告！ キーをなくさないでください。キーのコピーを安全な場所に保管してください。キーを失うと、暗号化したデータにまったくアクセスできなくなります。データを修復する方法もありません。

使用法

AES_ENCRYPT は、入力値の *string-expression* より最大で 31 バイト長い VARBINARY 値を返します。この関数によって返される値は暗号化テキストであり、判読できません。**AES_DECRYPT** 関数を使用して、**AES_ENCRYPT** 関数で暗号化された *string-expression* を復号化できます。*string-expression* を正常に復号化するには、データの暗号化に使用されたのと同じ暗号化キーとアルゴリズムを使用する必要があります。正しくない暗号化キーを指定した場合は、エラーが生成されます。

暗号化した値をテーブルに格納する場合は、カラムのデータ型を VARBINARY または VARCHAR にし、長さを 32 バイト以上にして、データに対して文字セット変換が実行されないようにします (文字セット変換が実行されるとデータを復号化できなくなります)。VARBINARY カラムまたは VARCHAR カラムの長さが 32 バイトより短いと、**AES_DECRYPT** 関数はエラーを返します。

AES_ENCRYPT 関数の結果のデータ型は LONG BINARY になる可能性があります。**SELECT INTO** 文で **AES_ENCRYPT** を使用する場合は、非構造化データ分析オプションのライセンスを所有しているか、**CAST** を使用して **AES_ENCRYPT** を正しいデータ型とサイズに設定する必要があります。

標準と互換性

- SQL — ISO/ANSI SQL 文法のベンダ拡張。
- Sybase – Adaptive Server では、サポートされていません。

参照：

- AES_DECRYPT 関数 [文字列] (211 ページ)
- 暗号化と復号化の例 (238 ページ)
- LOAD TABLE ENCRYPTED 句 (212 ページ)
- 暗号化テキストに対する異なるデータ型の影響 (207 ページ)
- 暗号化カラムのデータ型 (205 ページ)

REPLACE 関数 [文字列]

検出されたすべての部分文字列を、別の部分文字列に置換します。

構文

```
REPLACE ( original-string, search-string, replace-string )
```

パラメータ

いずれかの引数が NULL であれば、関数から NULL が返されます。

パラメータ	説明
original-string	検索される文字列。この文字列の長さに制限はない。
search-string	検索して *replace-string* に置き換えられる文字列。この文字列は 255 バイトに制限されている。*search-string* が空の文字列の場合は、元の文字列がそのまま返される。
replace-string	置換文字列。*search-string* を置き換える。任意の長さの文字列を指定できる。*replace-string* が空の文字列の場合は、検索されたすべての *search-string* が削除される。

戻り値

LONG VARCHAR

LONG NVARCHAR

注意： 結果データ型は LONG VARCHAR です。**SELECT INTO** 文で **REPLACE** を使用する場合は、非構造化データ分析オプションのライセンスを所有しているか、**CAST** を使用して **REPLACE** を正しいデータ型とサイズに設定する必要があります。

備考

REPLACE 関数の結果データ型は、LONG VARCHAR です。**SELECT INTO** 文で **REPLACE** を使用する場合は、非構造化データ分析オプションのライセンスを所有しているか、**CAST** を使用して **REPLACE** を正しいデータ型とサイズに設定する必要があります。

この問題には、次の 2 つの対処方法があります。

- ローカルテンポラリテーブルを宣言し、**INSERT** を実行します。

```
DECLARE local temporary table #mytable
  (name_column char(10)) on commit preserve rows;
INSERT INTO #mytable SELECT REPLACE(name,'0','1')   FROM
dummy_table01;
```

- **CAST** を使用します。

```
SELECT CAST(replace(name, '0', '1') AS Char(10)) into #mytable
from dummy_table01;
```

replace-string が *search-string* よりも長く、置換後のカラムの長さをコントロールする必要がある場合は、**CAST** 関数を使用してください。次に例を示します。

```
CREATE TABLE aa(a CHAR(5));
INSERT INTO aa VALUES('CCCCC');
COMMIT;
SELECT a, CAST(REPLACE(a,'C','ZZ') AS CHAR(5)) FROM aa;
```

標準と互換性

- SQL - ISO/ANSI SQL 文法のベンダ拡張。
- Sybase - Adaptive Server Enterprise 互換。

例

次の文は、値 "xx.def.xx.ghi" を返します。

```
SELECT REPLACE( 'abc.def.abc.ghi', 'abc', 'xx' ) FROM iq_dummy
```

次の文は、**ALTER PROCEDURE** 文を含む結果セットを生成します。この文を実行すると、名前が変更されたテーブルを参照するストアドプロシージャが修復されます (テーブル名を一意にすることをおすすめします)。

```
SELECT REPLACE(
  replace(proc_defn,'OldTableName','NewTableName'),
  'create procedure',
  'alter procedure')
FROM SYS.SYSPROCEDURE
WHERE proc_defn LIKE '%OldTableName%'
```

次の例では、カンマ以外の区切り文字を **LIST** 関数に使用します。

```
SELECT REPLACE( list( table_id ), ',', '--')
FROM  SYS.ISYSTAB
WHERE table_id <= 5
```

AES_DECRYPT 関数 [文字列]

指定されたキーを使用して文字列を復号化します。デフォルトでは、VARBINARY、LONG BINARY、または元のプレーンテキストのデータ型が返されます。

構文

AES_DECRYPT(*string-expression*, *key* [, *data-type*])

パラメータ

string-expression – 復号化される文字列。この関数にはバイナリ値を渡すこともできます。大文字と小文字を区別しないデータベースであっても、パラメータの大文字と小文字は区別されます。

key – *string-expression* の復号化に必要な暗号化キーです。暗号化された元の値を取得するには、このキーは、*string-expression* の暗号化に使用されたのと同じ暗号化キーである必要があります。データベースで大文字と小文字が区別されない場合でも、このパラメータでは大文字と小文字が区別されます。

警告！ キーをなくさないでください。キーのコピーを安全な場所に保管してください。キーを失うと、暗号化したデータにまったくアクセスできなくなります。データを修復する方法もありません。

data-type – このオプションパラメータでは、復号化する *string-expression* のデータ型を指定します。これは、元のプレーンテキストと同じデータ型である必要があります。

AES_ENCRYPT 関数を使用してデータを挿入する際に **CAST** 文を使用していない場合は、VARCHAR を *data-type* として渡すことにより、**AES_DECRYPT** を使用して同じデータを表示することができます。*data-type* を **AES_DECRYPT** に渡さない場合は、VARBINARY データ型が返されます。

使用法

AES_DECRYPT 関数を使用して、**AES_ENCRYPT** 関数で暗号化された *string-expression* を復号化できます。データ型の指定がない場合、この関数は、入力文字列と同じバイト数の VARBINARY 値または LONG VARBINARY 値を返します。それ以外の場合は、指定したデータ型が返されます。

string-expression を正常に復号化するには、データの暗号化に使用されたのと同じ暗号化キーを使用する必要があります。暗号化キーが正しくない場合は、エラーが返されます。

例

`user_info` テーブルからユーザのパスワードを復号化します。

```
SELECT AES_DECRYPT(user_pwd, '8U3dkA', CHAR(100))
FROM user_info;
```

標準と互換性

- SQL — ISO/ANSI SQL 文法のベンダ拡張。
- Sybase – Adaptive Server では、サポートされていません。

参照：

- AES_ENCRYPT 関数 [文字列] (208 ページ)
- 暗号化と復号化の例 (238 ページ)
- LOAD TABLE ENCRYPTED 句 (212 ページ)
- 暗号化カラムのデータ型 (205 ページ)

LOAD TABLE ENCRYPTED 句

LOAD TABLE 文では、column-spec キーワード **ENCRYPTED** がサポートされています。

column-specs は、**LOAD TABLE** 文のカラム名の後ろに、次の順序で指定する必要があります。

- *format-specs*
- *null-specs*
- *encrypted-specs*

構文

ENCRYPTED(*data-type* '*key-string*' [, '*algorithm-string*'])

パラメータ

- **data-type – AES_ENCRYPT** 関数への入力として使用する、入力ファイルフィールドの変換先のデータ型。*data-type* は、**AES_DECRYPT** 関数の出力のデータ型と同じデータ型である必要があります。
- **key-string –** データの暗号化に使用する暗号化キー。このキーは、文字列リテラルにする必要があります。元の値を取得するには、値を復号化するときに同じキーを使用します。データベースで大文字と小文字が区別されない場合でも、このパラメータでは大文字と小文字が区別されます。

ほとんどのパスワードの場合と同様に、キーの値には推測されにくい値を選択します。キーの値には、少なくとも 16 文字の長さを持ち、大文字と小文字を含み、数字、特殊文字を使用したものを選びます。このキーは、データを復号化するときに常に必要です。

警告！ キーをなくさないでください。キーのコピーを安全な場所に保管してください。キーを失うと、暗号化したデータにまったくアクセスできなくなります。データを修復する方法もありません。

- **algorithm-string –** データの暗号化に使用するアルゴリズム。このパラメータはオプションですが、データの暗号化と復号化は同じアルゴリズムを使用して行う必要があります。現時点では、サポートされているアルゴリズムは AES のみなので、これがデフォルトで使用されます。AES は、NIST (National Institute of Standards and Technology) がブロック暗号化の新しい AES (Advanced Encryption Standard) として選択したブロック暗号化アルゴリズムです。

使用法

ENCRYPTED のカラムの指定では、カラムにロードされるデータの暗号化に使用する暗号化キーと、必要に応じてアルゴリズムを指定できます。このロード先のカラムのデータ型は VARBINARY である必要があります。他のデータ型を指定するとエラーが返されます。

例

```
LOAD TABLE table_name
(
plaintext_column_name,
a_ciphertext_column_name
NULL('nil')
ENCRYPTED(varchar(6),'tHefiRstkEy') ,
another_encrypted_column
ENCRYPTED(bigint,'thEseconDkeY','AES')
)
FROM '/path/to/the/input/file'
FORMAT ascii
DELIMITED BY ';'
ROW DELIMITED BY '¥0xa'
QUOTES OFF
ESCAPES OFF
```

ここで、**LOAD TABLE** 文の入力ファイルのフォーマットは、次のとおりです。

```
a;b;c;
d;e;f;
g;h;i;
```

参照：

- AES_ENCRYPT 関数 [文字列] (208 ページ)
- AES_DECRYPT 関数 [文字列] (211 ページ)

- 暗号化と復号化の例 (238 ページ)
- 暗号化カラムのデータ型 (205 ページ)

LOAD TABLE 文

外部ファイルからデータベーステーブルにデータをインポートします。

クイックリンク：

「パラメータ」 (215 ページ)

「例」 (228 ページ)

「使用法」 (230 ページ)

「標準」 (234 ページ)

「パーミッション」 (234 ページ)

構文

```
[ INTO ] TABLE [ owner.]table-name
   ... ( load-specification [, …] )
   ...  { FROM | USING [ CLIENT ] FILE }
   { 'filename-string' | filename-variable } [, …]
   ... [ CHECK CONSTRAINTS { ON | OFF } ]
   ... [ DEFAULTS { ON | OFF } ]
   ... [ QUOTES OFF ]
   ... ESCAPES OFF
   ... [ FORMAT { ascii | binary | bcp } ]
   ... [ DELIMITED BY 'string' ]
   ... [ STRIP { OFF | RTRIM } ]
   ... [ WITH CHECKPOINT { ON | OFF } ]
   ... [ BYTE ORDER { NATIVE | HIGH | LOW } ]
   ... [ LIMIT number-of-rows ]
   ... [ NOTIFY number-of-rows ]
   ... [ ON FILE ERROR { ROLLBACK | FINISH | CONTINUE } ]
   ... [ PREVIEW { ON | OFF } ]
   ... [ ROW DELIMITED BY 'delimiter-string' ]
   ... [ SKIP number-of-rows ]
   ... [ HEADER SKIP number [ HEADER DELIMITED BY 'string' ] ]
   ... [ WORD SKIP number ]
   ... [ ON PARTIAL INPUT ROW { ROLLBACK | CONTINUE } ]
   ... [ IGNORE CONSTRAINT constraint-type [, …] ]
   ... [ MESSAGE LOG 'string' ROW LOG 'string' [ ONLY LOG log-what
[, …] ]
   ... [ LOG DELIMITED BY 'string' ]

load-specification – (back to Syntax)
   { column-name [ column-spec ]
      | FILLER ( filler-type ) }

column-spec – (back to load-specification)
   { ASCII ( input-width )
   | BINARY [ WITH NULL BYTE ]
```

```
    | PREFIX { 1 | 2 | 4 }
    | 'delimiter-string'
    | DATE ( input-date-format )
    | DATETIME ( input-datetime-format )
    | ENCRYPTED ( data-type 'key-string' [, 'algorithm-string' ] )
    | DEFAULT default-value }
    [ NULL ( { BLANKS | ZEROS | 'literal', …} ) ]

filler-type – (back to load-specification)
    { input-width
    | PREFIX { 1 | 2 | 4 }
    | 'delimiter-string'
    }

constraint-type – (back to Syntax)
    { CHECK integer
    | UNIQUE integer
    | NULL integer
    | FOREIGN KEYinteger
    | DATA VALUE integer
    | ALL integer
    }

log-what – (back to Syntax)
    { CHECK
    | ALL
    | NULL
    | UNIQUE
    | DATA VALUE
    | FOREIGN KEY
    | WORD
    }
```

パラメータ

（先頭に戻る） (214 ページ)

- **FROM –** データのロード元のファイルを 1 つ以上指定します。複数のファイルを指定する場合は、各 `filename-string` をカンマで区切ります。*filename-string* は、文字列としてサーバに渡されます。このため、文字列は他の SQL 文字列と同じフォーマット要件に従います。

  Windows のディレクトリパスを示すには、円記号 (¥) を 2 つの円記号で表します。したがって、ファイル `c:¥temp¥input.dat` から `Employees` テーブルにデータをロードする文は、次のようになります。

  ```
  LOAD TABLE Employees
  FROM 'c:¥¥temp¥¥input.dat' ...
  ```

  パス名は、クライアントアプリケーションではなくデータベースサーバを基準にした相対パスを指定します。別のコンピュータのデータベースサーバ上で文を実行している場合、ディレクトリ名で参照されるのは、クライアントマシンのディレクトリではなく、そのサーバマシンのディレクトリです。マルチプ

レックスデータベースをロードする場合、すべてのファイル名に絶対パス (完全修飾パス) を使用します。相対パス名は使用しないでください。

リソースの制約があるため、SAP Sybase IQ ではすべてのデータがロードされる保証はありません。リソースの割り付けに失敗した場合、そのロードトランザクション全体がロールバックされます。ファイルは 1 つずつ読み込まれ、FROM 句で指定された順に処理されます。SKIP または LIMIT の値は、ロードの開始時に適用され、各ファイルには適用されません。

LOAD TABLE FROM 句は今後廃止されますが、サーバ上に存在するファイルの指定に使用できます。次に、クライアントコンピュータ上の a.inp ファイルからデータをロードする例を示します。

```
LOAD TABLE t1(c1,c2,filler(30))
USING CLIENT FILE 'c:¥¥client-data¥¥a.inp'
QUOTES OFF ESCAPES OFF
IGNORE CONSTRAINT UNIQUE 0, NULL 0
MESSAGE LOG 'c:¥¥client-data¥¥m.log'
ROW LOG 'c:¥¥client-data¥¥r.log'
ONLY LOG UNIQUE
```

- **USING –** USING FILE は、サーバから 1 つまたは複数のファイルをロードします。この句は、FROM *filename* 句を指定する場合と同義です。USING CLIENT FILE は、クライアントから 1 つまたは複数のファイルのバルクロードを行います。クライアント側のファイルの文字セットは、サーバ照合と同じである必要があります。SAP Sybase IQ はファイルリスト内のファイルを逐次処理します。各ファイルは処理時に読み込みモードでロックされ、その後で、ロックが解除されます。クライアント側のバルクロードでは、余分なディスク領域、メモリ、ネットワークモニタリングデーモン要件などの管理作業にかかるオーバヘッドは発生しません。ただし、ファイルごとの単一スレッド処理が強制的に実行されます。

  ラージオブジェクトのバルクロードを行う場合は、USING CLIENT FILE 句をプライマリファイルとセカンダリファイルの両方に適用します。

  LOAD TABLE 文では、gzip 形式でのみ、圧縮されたクライアントファイルとサーバファイルをロードできます。拡張子 ".gz" または ".gzip" のファイルはすべて圧縮ファイルとみなされます。 圧縮ファイルのロード時に、名前付きパイプまたはセカンダリファイルはサポートされません。同一の **LOAD TABLE** 文で圧縮ファイルと圧縮解除ファイルを指定することができます。1 回のロードでは、各圧縮ファイルが 1 スレッドで処理されます。

  クライアント側ロード中に、IGNORE CONSTRAINT ログファイルがクライアントホスト上で作成されます。ログファイルの作成中にエラーが発生すると、操作がロールバックします。

クライアント側バルクロードは、Command Sequence プロトコルを使用する Interactive SQL クライアントと ODBC/JDBC クライアントによってサポートされています。TDS プロトコルを使用するクライアントではサポートされていません。ネットワーク上のデータセキュリティを確保するには、トランスポートレイヤセキュリティを使用します。クライアント側バルクロードを使用できるユーザを制御するには、セキュア機能 (-sf) サーバ起動スイッチ、**ALLOW_READ_CLIENT_FILE** データベースオプション、READCLIENTFILE アクセス制御を使用します。

- **CHECK CONSTRAINTS –** 検査制約を評価します。ユーザはこれを無視することも、ログに記録することもできます。CHECK CONSTRAINTS はデフォルトで ON に設定されます。

  CHECK CONSTRAINTS OFF に設定すると、SAP Sybase IQ はすべての検査制約違反を無視します。これは、たとえばデータベースの再構築時などに便利です。テーブルにユーザ定義関数を呼び出す検査制約があり、その関数がまだ作成されていない場合、このオプションを OFF に設定しなければ再構築が失敗します。

  このオプションは、次のオプションに対して相互に排他的です。これらのオプションのいずれかが同じロードに指定されていると、エラーが発生します。

  - IGNORE CONSTRAINT ALL
  - IGNORE CONSTRAINT CHECK
  - LOG ALL
  - LOG CHECK

- **DEFAULTS –** カラムのデフォルト値を使用します。このオプションはデフォルトで ON です。DEFAULTS オプションが OFF の場合は、カラムリストに存在しないカラムに NULL が割り当てられます。

  DEFAULTS オプションの設定は、AUTOINCREMENT を含むすべてのカラムの DEFAULT 値に適用されます。

- **QUOTES –** 入力文字列が引用符文字で囲まれることを指定します。QUOTES はオプションのパラメータで、デフォルトでは ON です。引用符文字はアポストロフィ (一重引用符) または二重引用符のいずれかです。文字列内で初めて出現した場合、これらの文字はその文字列の引用符文字列として処理されます。文字列データは、対応する引用符文字で終わっている必要があります。

  QUOTES ON の場合、カラムデリミタ文字またはローデリミタ文字をカラム値の一部とすることができます。開始と終端の引用符文字は、値の一部とはみなされず、ロードされるデータ値から取り除かれます。

QUOTES ON が指定されている値に引用符文字を含めるには、2 つの引用符を使用します。たとえば、次の行では 3 番目のカラムの値に一重引用符文字が含まれています。

```
'123 High Street, Anytown', '(715)398-2354',''''
```

STRIP を ON (デフォルト) に指定すると、後続ブランクを削除してから値が挿入されます。後続ブランクが削除されるのは、引用符で囲まれていない文字列だけです。引用符で囲まれた文字列では、後続ブランクが保持されます。先行ブランクまたは TAB 文字は、この設定が ON の場合にのみ削除されます。

データ抽出機能には、引用符を処理するオプション (**TEMP_EXTRACT_QUOTES**、**TEMP_EXTRACT_QUOTES_ALL**、および **TEMP_EXTRACT_QUOTE**) があります。IQ メインストアテーブルにロードされるデータを抽出する場合に、デフォルトの ASCII 抽出で文字列フィールドにカラムデリミタまたはローデリミタが含まれているときは、抽出に **TEMP_EXTRACT_BINARY** オプションを使用し、**LOAD TABLE** に FORMAT binary オプションと QUOTES OFF オプションを使用します。

制限事項：

- QUOTES ON は、カラムデリミタがある ASCII フィールドにのみ適用されます。
- QUOTES ON の場合、カラムデリミタまたはローターミネータの最初の文字に一重引用符および二重引用符は使用できません。
- QUOTES ON では、指定のファイルの単一スレッド処理が強制的に実行されます。
- QUOTES オプションは、その設定に関係なく、セカンダリファイルからのバイナリラージオブジェクト (BLOB) データまたはキャラクタラージオブジェクト (CLOB) データのロードに適用されません。開始引用符または終了引用符は、CLOB データの一部としてロードされます。引用符で囲まれている 2 つの連続した引用符は、QUOTES ON オプションを使用すると 2 つの連続した引用符としてロードされます。
- Adaptive Server BCP は、QUOTES オプションをサポートしていません。フィールドデータはすべて、QUOTES OFF 設定の場合と同様にコピーされます。QUOTES ON は SAP Sybase IQ **LOAD TABLE** 文のデフォルト設定であるため、BCP 出力から SAP Sybase IQ テーブルに ASE データをインポートする場合は QUOTES OFF を指定する必要があります。

例外:

- **LOAD TABLE** で、引用符で囲まれたフィールドの終了引用符文字の後に空白でない文字がある場合、次のエラーがレポートされてロード操作はロールバックされます。

```
Non-SPACE text found after ending quote character for
an enclosed field.
SQLSTATE: QTA14    SQLCODE: -1005014L
```

- QUOTES ON で、カラムデリミタの最初の文字として一重引用符または二重引用符が指定された場合、次のエラーがレポートされてロード操作は失敗します。

```
Single or double quote mark cannot be the 1st character
of column delimiter or row terminator with QUOTES option
ON.
SQLSTATE: QCA90    SQLCODE: -1013090L
```

- **ESCAPES –** ESCAPES が ON (デフォルト) の場合に、入力フィールドの *column-spec* 定義を省略すると、データベースサーバは円記号に続く文字を特殊文字として認識、解釈します。改行文字は ¥n という組み合わせとして、他の文字はタブ文字の ¥x09 のような 16 進の ASCII コードとしてデータに含めることができます。連続した 2 つの円記号 (¥¥) は 1 つの円記号として解釈されます。SAP Sybase IQ では、ESCAPES を OFF に設定する必要があります。

- **FORMAT –** SAP Sybase IQ は ASCII とバイナリの入力フィールドをサポートします。フォーマットは通常、上記の *column-spec* で定義します。カラムに対してこの定義を省略した場合、SAP Sybase IQ はデフォルトとしてこのオプションで定義したフォーマットを使用します。入力行は、ascii (デフォルト) フィールドまたは **binary** フィールドを持ち、1 行あたり 1 ローで構成され、カラムデリミタ文字で値が区切られているものとみなされます。

  SAP Sybase IQ は、**LOAD TABLE** コマンドへの入力として BCP 文字ファイルのデータも受け入れます。

  - **LOAD TABLE FORMAT BCP** 文を使用して SAP Sybase IQ テーブルにロードされる BCP データファイルは、-c オプションを使用して、プラットフォームを問わないファイルフォーマットでエクスポート (BCP OUT) する必要があります。
  - FORMAT BCP の場合、**LOAD TABLE** 文のデフォルトのカラムデリミタは <tab> で、デフォルトのローターミネータは <newline> です。
  - FORMAT BCP では、ローの最後のカラムはカラムデリミタではなくローターミネータで終了します。カラムデリミタがローターミネータの前にある場合、データの一部として扱われます。
  - ロード指定で最後のカラムではないカラムのデータは、カラムデリミタだけを使用して区切ります。最後のカラムではないカラムで、ローターミネータがカラムデリミタの前にある場合、そのローターミネータはカラムデータの一部として扱われます。
  - カラムデリミタは DELIMITED BY 句で指定できます。FORMAT BCP の場合、デリミタの長さは 10 文字以下である必要があります。デリミタの長さが 10 を超える場合はエラーが返されます。

- FORMAT BCP では、ロード指定にカラム名、NULL、ENCRYPTED のみを含めることができます。ロード指定にこれ以外のオプションが指定された場合は、エラーが返されます。
  たとえば、次の **LOAD TABLE** ロード指定は有効です。

```
LOAD TABLE x( c1, c2 null(blanks), c3 )
FROM 'bcp_file.bcp'
FORMAT BCP
...
```

```
LOAD TABLE x( c1 encrypted(bigint,'KEY-ONE','aes'), c2, c3 )
FROM 'bcp_file.bcp'
FORMAT BCP
...
```

- **DELIMITED BY –** *column-spec* 定義でカラムデリミタを省略した場合は、デフォルトのカラムデリミタ文字であるカンマが使用されます。1 文字の ASCII 文字、または 16 進の文字表現を入力することにより、別のカラムデリミタを指定できます。DELIMITED BY 句は次のようになります。

```
... DELIMITED BY '¥x09' ...
```

  デリミタとして改行文字を使用する場合は、特殊文字の組み合わせである '¥n' またはその ASCII 値である '¥x0a' を指定できます。column-spec の *delimiter-string* には最大 4 文字まで指定できますが、DELIMITED BY 句では 1 文字しか指定できません。

- **STRIP –** 引用符で囲まれていない値を挿入する前に、その値の後続ブランクを削除するかどうかを指定します。**LOAD TABLE** コマンドでは、次の STRIP キーワードを指定できます。
  - **STRIP OFF –** 後続ブランクを削除しません。
  - **STRIP RTRIM –** 後続ブランクを削除します。
  - **STRIP ON –** 非推奨。STRIP RTRIM を使用してください。

  STRIP を ON (デフォルト) に指定すると、SAP Sybase IQ は後続ブランクを削除してから値を挿入します。これは VARCHAR データの場合にのみ有効です。STRIP OFF では後続ブランクは保持されます。

  後続ブランクが削除されるのは、引用符で囲まれていない文字列だけです。引用符で囲まれた文字列では、後続ブランクが保持されます。ブランクを区別する必要がない場合は、後続スペースをすべて削除する代わりに、FILLER オプションを使用して、削除するバイト数をより詳細に指定できます。SAP Sybase IQ では、STRIP OFF はさらに効率的で、後続ブランクの処理は ANSI 規格に準拠します (CHAR データでは、常にブランクが埋め込まれます。したがって、この STRIP オプションが有効なのは、VARCHAR データの場合だけです)。

STRIP オプションは、可変長の非バイナリデータにのみ適用され、ASCII 固定幅の挿入には適用されません。たとえば、次のようなスキーマがあるとします。

```
CREATE TABLE t( c1 VARCHAR(3) );
LOAD TABLE t( c1 ',' ) ........ STRIP RTRIM    // trailing blanks
trimmed

LOAD TABLE t( c1 ',' ) ........ STRIP OFF      // trailing blanks
not trimmed

LOAD TABLE t( c1 ASCII(3) ) ... STRIP RTRIM    // trailing blanks
not trimmed
LOAD TABLE t( c1 ASCII(3) ) ... STRIP OFF      // trailing blanks
trimmed

LOAD TABLE t( c1 BINARY ) ..... STRIP RTRIM    // trailing blanks
trimmed
LOAD TABLE t( c1 BINARY ) ..... STRIP OFF      // trailing blanks
trimmed
```

バイナリデータの後続ブランクは常に削除されます。

- **WITH CHECKPOINT** – SAP Sybase IQ がチェックポイントを実行するかどうかを決定します。このオプションは、SAP Sybase IQ データベースの SQL Anywhere テーブルをロードする場合にのみ役立ちます。

  デフォルト設定は OFF です。この句を ON に設定すると、文が正常に完了し、ロギングされた後にチェックポイントが発行されます。接続がコミットを実行してから次のチェックポイントを実行するまでにサーバに障害が発生した場合、リカバリを正常に完了するには、テーブルのロードに使用されたデータファイルが存在する必要があります。しかし、WITH CHECKPOINT ON を指定した後にリカバリが必要になった場合は、リカバリ時にデータファイルは必要ありません。

  データベースが破損したため、バックアップを使用して現在のログファイルを適用する必要がある場合は、この句の指定内容にかかわりなく、データファイルが必要となります。

  警告！ データベースオプション CONVERSION_ERROR を OFF に設定すると、エラーがレポートされることなく不良データがテーブルにロードされることがあります。WITH CHECKPOINT ON を指定しない場合、データベースのリカバリが必要となったときには、CONVERSION_ERROR が ON (デフォルト値) であれば、リカバリが失敗することがあります。CONVERSION_ERROR を OFF に設定し、WITH CHECKPOINT ON が指定されていないときは、テーブルをロードしないことをおすすめします。

  詳細については、「CONVERSION_ERROR オプション [TSQL]」を参照してください。

- **BYTE ORDER –** 読み込み時のバイトの順序を指定します。このオプションはすべてのバイナリ入力フィールドに適用されます。何も定義されなければ、このオプションは無視されます。SAP Sybase IQ は通常、それ自体が稼働しているコンピュータのネイティブフォーマットでバイナリデータを読み込みます (デフォルトは NATIVE です)。次のように指定することもできます。
  - HIGH: マルチバイトの値が上位バイト優先である場合に指定します (Sun、IBM AIX、HP などのビッグエンディアンプラットフォーム用)。
  - LOW: マルチバイトの値が下位バイト優先である場合に指定します (Windows などのリトルエンディアンプラットフォーム用)。
- **LIMIT –** テーブルに挿入するローの最大数を指定します。デフォルトは 0 で無制限を意味します。ロー数の最大値は 2^{31} - 1 (2147483647) です。
- **NOTIFY –** 指定した個数のローがテーブルに正常に挿入されるたびに、メッセージが通知されるように指定します。デフォルトは 0 (通知の出力なし) です。このオプションの値は、NOTIFY_MODULUS データベースオプションの値を上書きします。
- **ON FILE ERROR –** 入力ファイルが存在しないか、またはファイルを読み込むパーミッションが不適切であるために、ファイルを開くことができない場合の SAP Sybase IQ の動作を指定します。次のいずれかを指定できます。
  - **ROLLBACK –** トランザクション全体をアボートします (デフォルト)。
  - **FINISH –** すでに完了している挿入処理を完了して、ロード処理を終了します。
  - **CONTINUE –** エラーを返しますが、該当するファイルのみをスキップしてロード処理を継続します。

  ON FILE ERROR 句は 1 つしか使用できません。
- **PREVIEW –** 各カラムの開始位置、名前、データ型など、ロード先テーブルへの入力のレイアウト情報を表示します。SAP Sybase IQ はロード処理の開始時にこの情報を表示します。ログファイルにログを書き込んでいる場合は、この情報もログに書き込みます。
- **ROW DELIMITED BY delimiter-string –** 入力レコードの末尾を指定する文字列を最大 4 バイト長で指定します。このオプションが使用できるのは、ロー内の全フィールドが次のいずれかである場合に限られます。
  - カラムターミネータで区切られている場合
  - DATE または DATETIME の *column-spec* オプションでデータが定義されている場合
  - ASCII 固定長フィールド

並列ロードを確実に行うためには、常に ROW DELIMITED BY を使用します。LOAD 指定でこの句を省略すると、SAP Sybase IQ はロードを並列実行ではなく逐次実行します。

入力フィールドにバイナリデータが格納されている場合は、このオプションは使用できません。このオプションを指定すると、ローターミネータにより、不足したフィールドが NULL に設定されます。すべてのローに同じローデリミタがあり、すべてのカラムデリミタと区別する必要があります。ローデリミタ文字列およびフィールドデリミタ文字列に、互いの初期サブセットを指定することはできません。たとえば、フィールドデリミタとして "*" を、ローデリミタとして "*#" を指定することはできませんが、フィールドデリミタとして "#" を、ローデリミタとして "*#" を指定することはできます。

ローにデリミタがない場合は、SAP Sybase IQ はエラーを返し、ロードトランザクション全体をロールバックします。唯一の例外はファイルの最終レコードです。この場合、そのローがロールバックされて、警告メッセージが返されます。Windows では通常、ローデリミタは改行文字とそれに続く復帰文字によって指定されます。このオプションまたは FILLER では、これらの文字を、上記で説明されている *delimiter-string* として指定しなければならない場合があります。

- **SKIP –** このロードで入力テーブルの開始時にスキップするローの数を定義します。スキップするローの最大数は 2^{31} - 1 (2147483647) です。デフォルトは 0 です。SKIP は、スキップするローを読み込むときに単一スレッドモードで動作します。
- **HEADER SKIP…HEADER DELIMITED BY – LOAD TABLE** でスキップする、ヘッダローを含むデータファイルの先頭行数を指定します。指定した数のローがスキップされるまで、すべての **LOAD TABLE** カラム指定と他のロードオプションは無視されます。
  - スキップする行数には、0 以上の数を指定する必要があります。
  - 行は、HEADER DELIMITED BY 句で指定した 1 ～ 4 文字のデリミタ文字列で区切られます。デフォルトの HEADER DELIMITED BY 文字列は、'¥n' 文字です。
  - HEADER DELIMITED BY 文字列の最大長は 4 文字です。文字列の長さが 5 文字以上または 1 未満の場合は、エラーが返されます。
  - ゼロ以外の HEADER SKIP 値を指定すると、HEADER DELIMITED BY デリミタを含むすべてのデータが、HEADER SKIP 句で指定した数のデリミタが検出されるまで無視されます。
  - 指定されている数のローがスキップされるまで、すべての **LOAD TABLE** カラム指定と他のロードオプションは無視されます。指定されている数のロー

がスキップされると、**LOAD TABLE** カラム指定と他のロードオプションが残りのデータに適用されます。
  - "ヘッダ" バイトは、データの開始位置でのみ無視されます。USING 句で複数のファイルが指定されていると、後続のファイルに同様のローが含まれている場合でも、HEADER SKIP は、指定されている数のヘッダローがスキップされるまで、最初のファイルの最初のローから始まるデータだけを無視します。**LOAD TABLE** は、実際のデータの解析を開始すると、ヘッダを検索しません。
  - HEADER SKIP で指定されている数のローをスキップする前に、**LOAD TABLE** がすべての入力データを処理しても、エラーはレポートされません。

- **WORD SKIP –** ワードインデックスの作成時に、指定された制限よりも長いデータが検出されてもロードを続行できます。

  ワードが許可されている最大サイズを超えたためにローがロードされない場合、警告メッセージが `.iqmsg` ファイルに書き込まれます。WORD サイズ制限の違反は、オプションで MESSAGE LOG ファイルに記録され、拒否されたローは、ROW LOG ファイルに記録されます。これらのファイルは **LOAD TABLE** 文で指定されます。

  - このオプションが指定されていない場合、**LOAD TABLE** は、指定された制限を超えた最初のワードでエラーをレポートしてロールバックします。
  - *number* は、「最大許容単語長を超える単語はサポートされません。」のエラーを無視する回数を指定します。
  - 0 (ゼロ) は制限がないことを意味します。

- **ON PARTIAL INPUT ROW –** ロード中に部分入力ローがあった場合のアクションを指定します。次のいずれかを指定できます。

  - CONTINUE は、警告を発行し、ロード操作を続行します。これはデフォルトです。
  - ROLLBACK は、ロード操作全体をアボートし、エラーをレポートします。

    ```
    Partial input record skipped at EOF.
    SQLSTATE: QDC32    SQLSTATE: -1000232L
    ```

- **IGNORE CONSTRAINT –** ロード中に発生した CHECK、UNIQUE、NULL、DATA VALUE、または FOREIGN KEY 整合性制約違反を無視するかどうか、また、違反をいくつ無視してからロールバックを開始するかを決める違反の最大数を指定します。*constrainttype* の指定に応じて、次のような動作となります。

  - **CHECK limit –** *limit* に 0 を指定すると、CHECK 制約違反は無制限に無視されます。CHECK が指定されなければ、最初に CHECK 制約違反が発生した時点で **LOAD** 文がロールバックされます。*limit* が 0 でなければ、CHECK 制約違反が *limit* + 1 回発生した時点でロードがロールバックされます。

- **UNIQUE *limit* –** *limit* に 0 を指定すると、UNIQUE 制約違反は無制限に無視されます。*limit* が 0 でなければ、UNIQUE 制約違反が *limit* + 1 回発生した時点でロードがロールバックされます。
- **NULL *limit* –** *limit* に 0 を指定すると、NULL 制約違反は無制限に無視されます。*limit* が 0 でなければ、NULL 制約違反が *limit* + 1 回発生した時点でロードがロールバックされます。
- **FOREIGN KEY *limit* –** *limit* に 0 を指定すると、FOREIGN KEY 制約違反は無制限に無視されます。*limit* が 0 でなければ、FOREIGN KEY 制約違反が *limit* + 1 回発生した時点でロードがロールバックされます。
- **DATA VALUE *limit* –** データベースオプションに CONVERSION_ERROR = ON を指定すると、エラーがレポートされて文がロールバックされます。*limit* に 0 を指定した場合、DATA VALUE 制約違反 (データ型変換エラー) は無制限に無視されます。*limit* が 0 でなければ、DATA VALUE 制約違反が *limit* + 1 回発生した時点でロードがロールバックされます。
- **ALL *limit* –** データベースオプションに `CONVERSION_ERROR = ON` が指定された場合、エラーがレポートされて文がロールバックされます。*limit* に 0 を指定した場合、すべての整合性制約違反は無制限に無視されます。*limit* が 0 以外の場合は、UNIQUE、NULL、DATA VALUE、FOREIGN KEY の整合性制約違反を無視した数の累計が *limit* の値を超えた時点で、ロードはロールバックされます。たとえば、次の IGNORE CONSTRAINT オプションを指定したとします。

  ```
  IGNORE CONSTRAINT NULL 50, UNIQUE 100, ALL 200
  ```

  この場合、整合性制約違反の合計数は 200 を超えることができません。同時に、NULL 制約違反は 50、UNIQUE 制約違反は 100 を超えてはなりません。これらのいずれかの制限を超えた時点で、LOAD TABLE 文はロールバックされます。

  注意： 1 つのローに、整合性制約違反が複数ある場合もあります。それぞれの整合性制約違反が、当該の種類の違反としてカウントされ、件数が制限に近づきます。

  無視された整合性制約違反をロギングする場合は、IGNORE CONSTRAINT オプションの limit を 0 以外の値に設定します。ロギングする違反の数が多すぎると、ロードのパフォーマンスに影響します。

IGNORE CONSTRAINT 句に CHECK、UNIQUE、NULL、または FOREIGN KEY を指定しない場合、これらのいずれかのタイプの整合性制約違反が最初に起きた時点でロードがロールバックします。

IGNORE CONSTRAINT 句で DATA VALUE が指定されていない場合は、このタイプの整合性制約違反が最初に見つかった時点で、ロードはロールバックされ

ます。ただし、データベースオプション CONVERSION_ERROR = OFF が設定されている場合は除きます。CONVERSION_ERROR = OFF が指定されていると、すべての DATA VALUE 制約違反に警告がレポートされ、ロードが継続されます。

ロードが完了すると、整合性制約違反に関する情報メッセージが .iqmsg ファイルに記録されます。このメッセージには、ロード中に発生した整合性制約違反の数と、スキップされたローの数が含まれます。

- **MESSAGE LOG –** 整合性制約違反に関する情報を記録するログファイルの名前と、ログに記録する違反のタイプを指定します。ロードの開始と完了を示すタイムスタンプは、MESSAGE LOG ファイルと ROW LOG ファイルの両方に記録されます。MESSAGE LOG と ROW LOG は両方とも指定する必要があります。指定がないと、整合性違反についての情報はログ記録されません。
  - ONLY LOG 句を指定しなかった場合は、整合性制約違反に関する情報はログに記録されません。ロードの開始と完了を示すタイムスタンプのみが記録されます。
  - ONLY LOG 句に指定されたすべてのタイプの整合性制約の違反についての情報、また、キーワード WORD が指定されている場合はすべてのワードインデックス長制限の違反についての情報がログに記録されます。
  - 制約違反がログに記録される場合、整合性制約違反が発生するたびに、MESSAGE LOG ファイルに必ず 1 行の情報が生成されます。

    MESSAGE LOG ファイルのローの数 (レポートされたエラーの数) が、IGNORE CONSTRAINT オプションの制限を超えることがあります。並行して動作する複数のスレッドによってロードが実行されるためです。制約違反の数が指定された制限を超えたことを、複数のスレッドがレポートする場合もあります。
  - 制約違反がログに記録される場合、特定のローに関する情報は、(そのローで整合性制約違反がいくつ発生しようと) ROW LOG ファイルに必ず 1 行で記録されます。

    MESSAGE LOG ファイルに記録された個々のエラーの数と、ROW LOG ファイルに記録されたローの数が一致しない場合があります。両者のロー数の差異は MESSAGE LOG の項で説明した、ロードの並行処理によるものです。
  - MESSAGE LOG ファイルと ROW LOG ファイルには、ローパーティションや名前付きパイプは使用できません。
  - MESSAGE LOG ファイルまたは ROW LOG ファイルがすでに存在する場合、新しい情報がそのファイルに追加されます。
  - MESSAGE LOG ファイルまたは ROW LOG ファイルに無効なファイル名を指定すると、エラーが発生します。

- MESSAGE LOG ファイルと ROW LOG ファイルに同じファイル名を指定すると、エラーが発生します。

IGNORE CONSTRAINT オプションと MESSAGE LOG オプションをさまざまに組み合わせて指定すると、さまざまなロギングアクションが実行されます。

表 12 : LOAD TABLE のロギングアクション

IGNORE CONSTRAINT の指定の有無	MESSAGE LOG の指定の有無	アクション
あり	あり	無視されたすべての整合性制約違反が、ロールバックが発生するまでのユーザ指定の limit も含めて記録される。
なし	あり	ロールバックが発生する前の最初の整合性制約違反が記録される。
あり	なし	何もロギングされない。
なし	なし	何もロギングされない。最初の整合性制約違反でロールバックが実行される。

ヒント： 無視された整合性制約違反を記録する場合は、IGNORE CONSTRAINT オプションの limit を 0 以外の値に設定します。1 つのローに複数の整合性制約違反がある場合、MESSAGE LOG ファイルには、各違反がそれぞれ別個のローとして記録されます。ロギングする違反の数が多すぎると、ロードのパフォーマンスに影響します。

- **LOG DELIMITED BY –** ROW LOG ファイルのデータ値を区切るセパレータを指定します。デフォルトのセパレータはカンマです。

  SAP Sybase IQ では、FORMAT BCP が **LOAD TABLE** 句として指定された場合でも、エラーメッセージを返さなくなりました。また、次の状態が確認され、対応するエラーメッセージが返されます。

  - 指定されたロード形式が ASCII、BINARY、または BCP のいずれでもない場合、SAP Sybase IQ はメッセージ「`LOAD` のフォーマットとしてサポートされているのは `ASCII`、`BCP` および `BINARY` のみです。」を返します。
  - **LOAD TABLE** のカラム指定にカラム名、NULL、または ENCRYPTED 以外のものが含まれている場合、SAP Sybase IQ はエラーメッセージ「`LOAD ... FORMAT BCP` のロードの指定は無効です。」を返します。
  - FORMAT BCP ロードのカラムデリミタまたはローターミネータのサイズが 10 文字を超えた場合、SAP Sybase IQ はメッセージ「デリミタ `'%2'` の長さは `1` から `%3` 文字にする必要があります。」を返します (ここで、%3 には 10 が入ります)。

FORMAT BCP と FORMAT ASCII で発生する可能性があるエラーまたは警告の状態に対応するメッセージは、どちらのフォーマットでも同じです。

- 指定されるロードデフォルト値が AUTOINCREMENT、IDENTITY、または GLOBAL AUTOINCREMENT の場合、SAP Sybase IQ はエラー「デフォルト値 %2 は LOAD のデフォルト値として使用できません。%1」を返します。
- **LOAD TABLE** 指定に、指定されたファイルからロードする必要があるカラムが含まれていない場合、SAP Sybase IQ がエラー「LOAD 文には入力ファイルからロードされるカラムを少なくとも 1 つ含める必要があります。」をレポートし、**LOAD TABLE** 文がロールバックします。
- ロード時に TEXT インデックスがあるテキストドキュメントで単語の数が最大数を超えると、SAP Sybase IQ から次のエラーが返されます。「テキストドキュメントが語数の最大値を超えています。サポートされているドキュメント当たりの最大語数は 4294967295 です。」

例

（先頭に戻る） (214 ページ)

- **例 1 –** 1 つのファイルのデータを Windows システム上の Products テーブルにロードします。タブは、Description カラムと Color カラムの後に続くカラムデリミタとして使用されます。

```
LOAD TABLE Products
( ID ASCII(6),
FILLER(1),
Name   ASCII(15),
FILLER(1),
Description   '¥x09',
Size   ASCII(2),
FILLER(1),
Color   '¥x09',
Quantity   PREFIX 2,
UnitPrice   PREFIX 2,
FILLER(2) )
FROM 'C:¥¥mydata¥¥source1.dmp'
QUOTES OFF
ESCAPES OFF
BYTE ORDER LOW
NOTIFY 1000
```

- **例 2 –** クライアントコンピュータにあるファイル a.inp からデータをロードします。

```
LOAD TABLE t1(c1,c2,filler(30))
USING CLIENT FILE 'c:¥¥client-data¥¥a.inp'
QUOTES OFF ESCAPES OFF
IGNORE CONSTRAINT UNIQUE 0, NULL 0
```

```
MESSAGE LOG 'c:¥¥client-data¥¥m.log'
ROW LOG 'c:¥¥client-data¥¥r.log'ONLY LOG UNIQUE
```

- **例 3 –** 2 つのファイルからのデータを UNIX システム上の `product_new` テーブル (NULL 値使用可) にロードします。タブ文字がデフォルトカラムデリミタで、改行文字がローデリミタです。

```
LOAD TABLE product_new
( id,
name,
description,
size,
color   '¥x09'   NULL( 'null', 'none', 'na' ),
quantity   PREFIX 2,
unit_price   PREFIX 2 )
FROM '/s1/mydata/source2.dump',
'/s1/mydata/source3.dump'
QUOTES OFF
ESCAPES OFF
FORMAT ascii
DELIMITED BY '¥x09'
ON FILE ERROR CONTINUE
ROW DELIMITED BY '¥n'
```

- **例 4 –** ワード長の制限違反を 10 回は無視し、11 回目に新しいエラーを表示してロードをロールバックします。

```
load table PTAB1(
       ck1          ','  null ('NULL') ,
       ck3fk2c2     ','  null ('NULL') ,
       ck4          ','  null ('NULL') ,
       ck5          ','  null ('NULL') ,
       ck6c1        ','  null ('NULL') ,
       ck6c2        ','  null ('NULL') ,
       rid          ','  null ('NULL')  )
FROM 'ri_index_selfRI.inp'
       row delimited by '¥n'
       LIMIT 14   SKIP 10
       IGNORE CONSTRAINT UNIQUE 2, FOREIGN KEY 8
       word skip 10 quotes off escapes off strip
       off
```

- **例 5 – FORMAT BCP** ロードオプションを使用して、テーブル `t1` を **BCP** 文字ファイル `bcp_file.bcp` からテーブルにロードします。

```
LOAD TABLE t1 (c1, c2, c3)
FROM 'bcp_file.bcp'
FORMAT BCP
...
```

- **例 6 – DEFAULT** ロードオプションを使用して、デフォルト値 12345 を `c1` にロードして、`c2` および `c3` をデータとともに `LoadConst04.dat` ファイルからロードします。

```
LOAD TABLE t1 (c1 DEFAULT '12345 ', c2, c3, filler(1))
FROM 'LoadConst04.dat'
STRIP OFF
QUOTES OFF
ESCAPES OFF
DELIMITED BY ',';
```

- **例 7 – FORMAT BCP** ロードオプションを使用して、c1 および c2 をデータとともにファイル bcp_file.bcp からロードし、c3 を値 10 に設定します。

```
LOAD TABLE t1 (c1, c2, c3 DEFAULT '10')
FROM 'bcp_file.bcp'
FORMAT BCP
QUOTES OFF
ESCAPES OFF;
```

- **例 8 –** 次のコードフラグメントは、データファイルの先頭のヘッダローを 1 行無視します。ヘッダローは「&&」で区切られています。

```
LOAD TABLE
...HEADER SKIP 1 HEADER DELIMITED by '&&'
```

- **例 9 –** 次のコードフラグメントは、データファイルの先頭のヘッダローを 2 行無視します。ヘッダ行のそれぞれは、「¥n」によって区切られています。

```
LOAD TABLE
...HEADER SKIP 2
```

- **例 10 –** ファイルを RLV 対応テーブルにロードします。

  FORMAT BCP ロードオプションを使用して、**BCP** 文字ファイル bcp_file.bcp から RLV 対応テーブル rvt1 にデータをロードします。

```
LOAD TABLE rvt1 (c1, c2, c3)
FROM 'bcp_file.bcp'
FORMAT BCP
...
```

使用法

（先頭に戻る） (214 ページ)

LOAD TABLE 文を使用すると、ASCII またはバイナリデータのファイルからデータベーステーブルに大量の挿入を効率よく行うことができます。

LOAD TABLE では、整合性制約違反が発生し、違反に関する情報を記録する場合のロードの動作を制御することもできます。

LOAD TABLE はテンポラリテーブルに対して使用できますが、テンポラリテーブルを **ON COMMIT PRESERVE ROWS** で宣言している必要があります。宣言されていないと、次回の **COMMIT** 時にロードしたローが削除されます。

LOAD TABLE は、ラージオブジェクト (LOB) データのロードをサポートしています。

SAP Sybase IQ は、ASCII データとバイナリデータの両方からのロードをサポートし、また、固定長と可変長の両方のフォーマットをサポートしています。これらのフォーマットのすべてを処理するには、*load-specification* を指定して、ソースファイルの各「カラム」またはフィールドからロードされるデータの種類を SAP Sybase IQ に指示する必要があります。*column-spec* を使用すると、次のフォーマットを定義できます。

- 固定長バイトの ASCII。*input-width* 値は、各レコードの入力フィールドの固定幅のバイト数を示す整数値です。
- 入力の長さの指定に PREFIX のバイト数 (1、2、または 4) を使用するバイナリフィールドと非バイナリフィールド。
  PREFIX 句に関連する部分は、次の 2 つです。
  - Prefix 値 - 常にバイナリ値。
  - 関連付けられるデータバイト - 常に文字フォーマット。バイナリフォーマットは使用されません。

  `TEMP_EXTRACT_BINARY` オプションを ON に設定し、抽出機能を使用してデータがアンロードされる場合は、バイナリデータのロード時に **BINARY WITH NULL BYTE** パラメータを各カラムに使用する必要があります。
- セパレータで区切られた可変長文字列。ターミネータを 16 進の ASCII 文字として指定できます。*delimiter-string* には、4 文字までの任意の文字列を使用できます。これには任意に組み合わせた印刷可能文字、および印刷されない文字を表す任意の 8 ビットの 16 進 ASCII コードなどが含まれます。たとえば、次のように指定します。
  - ターミネータとなるタブを表す '¥x09'。
  - null ターミネータ '¥x00' ("C" の文字列と同様に表示されないターミネータ)。
  - ターミネータとなる改行文字の '¥x0a'。特殊文字の組み合わせである '¥n' を使用して改行を表すこともできます。

  注意： デリミタ文字列の長さには 1 ～ 4 文字を指定できますが、**DELIMITED BY** 句には 1 文字しか指定できません。**BCP** では、10 文字までのデリミタが使用できます。
- ASCII 文字としての DATE または DATETIME 文字列。SAP Sybase IQ でサポートされる日付または日付時刻データ型に対応するフォーマットのいずれかを使用して、文字列の *input-date-format* または *input-datetime-format* を定義する必要があります。日付値には **DATE** を、日付／時刻、および時刻の値には **DATETIME** を使用します。

表 13 : 日付と時刻のフォーマット

オプション	意味
yyyy または YYYY yy または YY	年を表す。デフォルトは現在の年。
mm または MM	月を表す。5 月には「05」というように、必要に応じて必ず先行 0 またはブランクを使用する。DATE 値には月を含める必要がある。たとえば、**DATE** 値として「1998」と入力すると、エラーになる。「03」と入力した場合、SAP Sybase IQ はデフォルトの年と日付を適用して、「1998-03-01」に変換する。
dd または DD jjj または JJJ	日付を表す。デフォルトの日付は 01。1 桁の日付は、日付の先頭に 0 を付ける。たとえば、最初の日は「01」となる。J または j は年のユリウス日付 (1 ～ 366) を示す。
hh HH	時間を示す。時間は 24 時間表記に基づく。1 桁の時刻は、その前に 0 または空白を付ける。たとえば、午前 1 時は「01」となる。「00」は有効な値で、午前 0 時 (深夜) を表す。
nn	分を示す。1 桁の分は、分の前に 0 を付ける。たとえば、8 分は「08」となる。
ss[.ssssss]	秒数とコンマ以下の秒数を示す。
aa	午前または午後を示す。
pp	必要な場合にのみ、午後を示す (このオプションはバージョン 12.0 より前の SAP Sybase IQ とは互換性がない。以前は「pp」と「aa」は同義であった)。
hh	SAP Sybase IQ は、分と秒をゼロとみなす。たとえば、入力した **DATETIME** 値が「03」の場合、SAP Sybase IQ では、「03:00:00.0000」に変換される。
hh:nn または hh:mm	SAP Sybase IQ は秒をゼロとみなす。たとえば、入力した時刻値が「03:25」の場合、SAP Sybase IQ では「03:25:00.0000」に変換される。

表 14 : DATE と DATETIME フォーマットのオプションの例

入力データ	フォーマット仕様
12/31/98	DATE ('MM/DD/YY')
19981231	DATE ('YYYYMMDD')
123198140150	DATETIME ('MMDDYYhhnnss')
14:01:50 12-31-98	DATETIME ('hh:nn:ss MM-DD-YY')
18:27:53	DATETIME ('hh:nn:ss')

入力データ	フォーマット仕様
12/31/98 02:01:50AM	DATETIME ('MM/DD/YY hh:nn:ssaa')

SAP Sybase IQ には、一般的な日付、時刻および日付時刻フォーマット用のロードの最適化が装備されています。ロードするデータがこれらのフォーマットのいずれかに当てはまる場合は、正しいフォーマットを使用することによってロード時間を大幅に削減できます。

date/time フィールドを ASCII 固定幅フィールド (上記参照) として指定し、FILLER(1) オプションを使用してカラムデリミタをスキップすることもできます。

column-spec の NULL の部分は、テーブルのカラムにデータをロードするときに、特定の入力値を NULL として処理する方法を示します。NULL として処理される文字には、BLANKS、ZEROS、または定義したその他のリテラルのリストなどがあります。NULL 値を指定するか、またはソースファイルから NULL 値を読み込む場合は、ロード先カラムに NULL を格納できる必要があります。

ZEROS は次のように解釈されます。入力データ (ASCII の場合は変換前) がすべてバイナリのゼロ (文字のゼロではない) の場合にかぎり、セルは NULL に設定されます。

- 入力データが文字のゼロの場合は、次のようになります。
  1. NULL (ZEROS) を指定しても、セルに NULL がセットされることはない。
  2. NULL ('0') を指定すると、セルに NULL がセットされる。
- 入力データがバイナリのゼロ (全ビットがクリア) の場合は、次のようになります。
  1. NULL (ZEROS) を指定すると、セルに NULL がセットされる。
  2. NULL ('0') を指定しても、セルに NULL がセットされることはない。

たとえば、**LOAD** 文に `col1 date('yymmdd') null(zeros)` が含まれ、日付が 000000 であると、000000 を `DATE`(4) に変換できないことを示すエラーが表示されます。データが 000000 である場合に、**LOAD TABLE** で NULL 値が `col1` に挿入されるようにするには、NULL 句を `null('000000')` のように記述するか、データを同等のバイナリのゼロに修正して NULL(ZEROS) を使用します。

`VARCHAR` セルの長さがゼロで、セルが NULL 以外の場合は、長さゼロのセルが作成されます。その他のデータ型については、セルの長さがゼロの場合、SAP Sybase IQ によって NULL が挿入されます。これは ANSI 準拠の動作です。ANSI 以外で長さゼロのの文字データを処理するには、**NON_ANSI_NULL_VARCHAR** データベースオプションを設定します。

DEFAULT オプションを使用して、デフォルトのロードカラム値を指定します。カラムにテーブルスキーマで定義されたデフォルト値がない場合でも、デフォルト

値をカラムにロードできるようになります。この機能によって、ロード時の柔軟性が向上します。

- **LOAD TABLE** 文で指定されたデフォルト値を使用するには、**LOAD TABLE DEFAULTS** オプションを ON にする必要があります。**DEFAULTS** オプションが OFF の場合、指定されたロードデフォルト値は使用されず、代わりに NULL 値がカラムに挿入されます。
- **LOAD TABLE** コマンドには、**LOAD TABLE** コマンドで指定されたファイルからロードする必要があるカラムが 1 つ以上含まれている必要があります。そうしないと、エラーが報告され、ロードは実行されません。
- 指定されたデフォルトのロード値は、カラムのサポート対象のデフォルト値、およびデフォルト値の制約と一致している必要があります。**LOAD TABLE DEFAULT** オプションでは、デフォルトのロード値として **AUTOINCREMENT**、**IDENTITY**、および **GLOBAL AUTOINCREMENT** はサポートされません。
- **LOAD TABLE DEFAULT** *default-value* は、データベースと同じ文字セットである必要があります。
- **LOAD TABLE DEFAULT** 句で指定されたロードデフォルト値では、デフォルト値の暗号化はサポートされていません。
- 指定されたロードデフォルト値の評価によって発生した制約性違反は、テーブルに挿入されたローごとにカウントされます。

load-specification のもう 1 つの重要部分は、**FILLER** オプションです。このオプションを指定すると、ソース入力ファイル内の指定したフィールドをスキップします。たとえば、ローの末尾の文字や入力ファイルのフィールド全体を、テーブルに追加する必要がない場合があります。**FILLER** では、*column-spec* 定義と同様に、ASCII 固定長バイト、セパレータで区切った可変長文字列、PREFIX バイトを使用するバイナリフィールドを指定できます。

標準

（先頭に戻る） (214 ページ)

- SQL - ISO/ANSI SQL 文法のベンダ拡張。
- SAP Sybase Database 製品 - なし。

パーミッション

（先頭に戻る） (214 ページ)

LOAD TABLE 文の実行に必要なパーミッションは、データベースサーバの **-gl** コマンドラインオプションに応じて次のように異なります。

- **-gl ALL** – テーブルの所有者であるか、テーブルに対する ALTER または LOAD パーミッションが付与されているか、ALTER ANY TABLE、LOAD ANY

TALBE、または ALTER ANY OBJECT システム権限が付与されている必要があります。

- **-gl DBA –** ALTER ANY TABLE、LOAD ANY TABLE、または ALTER ANY OBJECT システム権限が必要です。
- **-gl NONE – LOAD TABLE** 文の実行は許可されません。

-gl コマンドラインオプションの詳細については、ユーティリティガイド > 「start_iq データベースサーバ起動ユーティリティ」 > 「start_iq サーバオプション」を参照してください。

また、**LOAD TABLE** はテーブルに対する書き込みロックが必要です。

暗号化テキストでの文字列の比較

データの大文字と小文字が区別されない場合、または ISO_BINENG 以外の照合を使用している場合は、文字列の比較を実行するために暗号化テキストカラムを復号化する必要があります。

文字列の比較を実行する場合、多くの照合において等価な文字列と同一の文字列の違いは重要です。これは、**CREATE DATABASE** の **CASE** オプションに依存します。**CASE RESPECT** に設定され、ISO_BINENG 照合を使用するデータベースは、SAP Sybase IQ でのデフォルトであり、等価性と同一性の問題は同様に解決されます。

同一の文字列は常に等価ですが、等価な文字列は必ずしも同一ではありません。文字列が同じバイト値を使用して表現される場合のみ、文字列は同一です。データの大文字と小文字が区別されない場合、または複数の文字が等しいものとして処理される必要がある照合を使用する場合、等価性と同一性の違いは重要です。ISO1LATIN1 はこのような照合の例です。

たとえば、大文字と小文字が区別されないデータベース内の文字列「ABC」と文字列「abc」は、同一ではありませんが等価です。大文字と小文字が区別されるデータベースの場合、これらは同一でも等価でもありません。

Sybase 暗号化関数によって作成される暗号化テキストは、等価性ではなく同一性を保持します。つまり、"ABC" と "abc" の暗号化テキストは決して等価ではありません。

照合または **CASE** の設定でこのような比較が許可されていない場合に暗号化テキストで等価性の比較を実行するには、アプリケーションでそのカラム内の値を、等価な値がなく、したがって同一の値もない、何らかの標準の形式に変更する必要があります。たとえば、**CASE IGNORE** と ISO_BINENG 照合を使用してデータベースを作成し、アプリケーションで入力値をカラムに挿入する前にその入力値すべてに UCASE を適用すれば、等価な値はすべて同一にもなります。

カラムの暗号化に対するデータベースオプション

カラムの暗号化と復号化に影響する SAP Sybase IQ データベースオプションの設定があります。ほとんどのカラム暗号化処理で、デフォルトの設定は最適な設定ではありません。

暗号化テキストの予期しないトランケートの防止

暗号化関数による暗号化テキストの出力 (またはその他の文字やバイナリ文字列) が予期せずにトランケートされないようにするには、STRING_RTRUNCATION データベースオプションを設定します。

```
SET OPTION STRING_RTRUNCATION = 'ON'
```

STRING_RTRUNCATION を ON (デフォルト) に設定すると、ロード、挿入、更新、または **SELECT INTO** の操作で文字列がトランケートされるたびにエンジンでエラーが発生します。これは ISO/ANSI SQL の動作であり、推奨される方法です。

明示的なトランケートが必要な場合は、**LEFT**、**SUBSTRING**、**CAST** などの文字列式を使用します。

STRING_RTRUNCATION を OFF に設定すると、文字列の暗黙的なトランケートが実行されます。

また、**AES_DECRYPT** 関数も、入力された暗号化テキストのデータ長の有効性をチェックするだけでなく、テキスト出力もチェックして、復号化した後のデータ長と指定されたキーの適正さの両方を検証します データ型の引数を指定したた場合は、データ型もチェックされます。

暗号化テキストの整合性の維持

ASE_BINARY_DISPLAY を設定することで、暗号化テキストの整合性を維持します。

```
SET OPTION ASE_BINARY_DISPLAY = 'OFF'
```

ASE_BINARY_DISPLAY を OFF (デフォルト) に設定すると、バイナリデータはローバイナリ形式のまま変更されません。

ASE_BINARY_DISPLAY を ON に設定すると、バイナリデータは 16 進数文字列の表示表現に変換されます。このオプションは、エンドユーザに対してデータを表示する必要がある場合や、データを別の外部システムにエクスポートする必要がある (転送中にローバイナリが変更される可能性がある) 場合にのみ、一時的に ON に設定します。

暗号化テキストの誤用の防止

CONVERSION_MODE を設定することで、実質的に意味のない操作となる暗号化データの暗黙のデータ型変換を防止します。

CONVERSION_MODE データベースオプションは、さまざまな操作で、バイナリデータ型 (BINARY、VARBINARY、および LONG BINARY) と他の非バイナリデータ型 (BIT、TINYINT、SMALLINT、INT、UNSIGNED INT、BIGINT、UNSIGNED BIGINT、CHAR、VARCHAR、および LONG VARCHAR) 間の暗黙的な変換を制限します。

```
SET TEMPORARY OPTION CONVERSION_MODE = 1
```

CONVERSION_MODE を 1 に設定すると、**INSERT** コマンド、**UPDATE** コマンド、およびクエリ内でのバイナリデータ型から他の非バイナリデータ型への暗黙的な変換が制限されます。バイナリ変換制限モードは、**LOAD TABLE** デフォルト値および **CHECK** 制約にも適用されます。

CONVERSION_MODE オプションのデフォルト値 0 では、12.7 より前のバージョンの SAP Sybase IQ でのバイナリデータ型の暗黙的な変換動作が維持されます。

CONVERSION_MODE オプション

さまざまな操作で、バイナリデータ型 (BINARY、VARBINARY、および LONG BINARY) と他の非バイナリデータ型 (BIT、TINYINT、SMALLINT、INT、UNSIGNED INT、BIGINT、UNSIGNED BIGINT、CHAR、VARCHAR および LONG VARCHAR) 間の暗黙的な変換を制限します。

指定できる値
0, 1

デフォルト値
0

スコープ
オプションは、データベース (PUBLIC) レベルまたは ユーザレベルで設定できます。データベースレベルで設定した場合、値は新しいユーザのデフォルト値になりますが、既存のユーザには影響を与えません。ユーザレベルで設定した場合は、そのユーザの PUBLIC 値 のみが上書きされます。自分のオプションを設定する場合は、システム権限は必要ありません。自分以外のユーザのオプションをデータベースレベルまたはユーザレベルで設定する場合は、システム権限が必要です。

このオプションを設定するには、SET ANY PUBLIC OPTION システム権限が必要です。個々の接続または PUBLIC ロールに一時的に設定できます。すぐに有効になります。

備考
デフォルト値 0 は、12.7 より前のバージョンの暗黙の変換動作を保持します。**CONVERSION_MODE** を 1 に設定すると、**INSERT**、**UPDATE**、およびクエリ内でのバイナリデータ型から他の非バイナリデータ型への暗黙的な変換が制限されます。バイナリ変換制限モードは、**LOAD TABLE** のデフォルト値と CHECK 制約にも適用されます。**CONVERSION_MODE 1** を設定することで、実質的に意味のない操作となる暗号化データの暗黙のデータ型変換を防止できます。

SAP Sybase IQ Advanced Security オプションの暗号化カラム機能を使用するには、そのためのライセンスを取得している必要があります。

暗黙的な変換の制限
CONVERSION_MODE オプションのバイナリ変換制限モード値が 1 (**CONVERSION_MODE** = 1) の場合、次の操作の暗黙的な変換が制限されます。

- CHECK 制約またはデフォルト値を指定した **LOAD TABLE**
- **INSERT...SELECT**、**INSERT...VALUE**、**INSERT...LOCATION**
- 特定の種類の **UPDATE**
- 更新可能カーソルを介する、特定の種類の **INSERT** と **UPDATE**
- 通常、クエリのすべての側面

暗号化と復号化の例

コメント付きの SQL で記述した、**AES_ENCRYPT** 関数と **AES_DECRYPT** 関数の使用例を示します。

```
--   This example of aes_encrypt and aes_decrypt function use is
presented in three parts:
--
-- Part I: Preliminary description of target tables and users as DDL
-- Part II: Example schema changes motivated by introduction of
encryption
-- Part III: Use of views and stored procedures to protect encryption
keys
--


--   Part I: Define target tables and users

--   Assume two classes of user, represented here by the instances
--   PrivUser and NonPrivUser, assigned to groups reflecting
differing
--   privileges.

--   The initial state reflects the schema prior to the introduction
--   of encryption.

--   Set up the starting context: There are two tables with a common
key.
```

```
--   Some columns contain sensitive data, the remaining columns do
not.
--   The usual join column for these tables is sensitiveA.
--   There is a key and a unique index.

    grant connect to PrivUser identified by 'verytrusted' ;
    grant connect to NonPrivUser identified by 'lesstrusted' ;

    grant connect to high_privileges_group ;
    create role high_privileges_group ;
    grant role high_privileges_group to PrivUser ;

    grant connect to low_privileges_group ;
    create role low_privileges_group ;
    grant role low_privileges_group to NonPrivUser ;

    create table DBA.first_table
                    (sensitiveA char(16) primary key
                    ,sensitiveB numeric(10,0)
                    ,publicC    varchar(255)
                    ,publicD    date
                    )  ;


--   There is an implicit unique HG (HighGroup) index enforcing the
primary key.

    create table second_table
                    (sensitiveA char(16)
                    ,publicP integer
                    ,publicQ tinyint
                    ,publicR varchar(64)
                    )  ;

    create hg index second_A_HG on second_table ( sensitiveA ) ;

--   TRUSTED users can see the sensitive columns.

    grant select ( sensitiveA, sensitiveB, publicC, publicD )
        on DBA.first_table to PrivUser ;
    grant select ( sensitiveA, publicP, publicQ, publicR )
        on DBA.second_table to PrivUser ;

--   Non-TRUSTED users in existing schema need to see sensitiveA to
be
--   able to do joins, even though they should not see sensitiveB.

    grant select ( sensitiveA, publicC, publicD )
        on DBA.first_table to NonPrivUser ;
    grant select ( sensitiveA, publicP, publicQ, publicR )
        on DBA.second_table to NonPrivUser ;

--   Non-TRUSTED users can execute queries such as

    select I.publicC, 3*II.publicQ+1
    from DBA.first_table I, DBA.second_table II
```

```
    where I.sensitiveA = II.sensitiveA and I.publicD IN
( '2006-01-11' ) ;

--   and

    select count(*)
    from DBA.first_table I, DBA.second_table II
    where I.sensitiveA = II.sensitiveA and SUBSTR(I.sensitiveA,4,3)
    BETWEEN '345' AND '456' ;

--   But only TRUSTED users can execute the query

    select I.sensitiveB, 3*II.publicQ+1
    from DBA.first_table I, DBA.second_table II
    where I.sensitiveA = II.sensitiveA and I.publicD IN
( '2006-01-11' ) ;


--   Part II: Change the schema in preparation for encryption
--
--    The DBA introduces encryption as follows:
--
--    For applicable tables, the DBA changes the schema, adjusts
access
--    permissions, and updates existing data. The encryption
--    keys used are hidden in a subsequent step.


--   DataLength comparison for length of varbinary encryption result
--   (units are Bytes):
--
--    PlainText CipherText    Corresponding Numeric Precisions
--
--            0       16
--      1 -  16       32      numeric(1,0)   - numeric(20,0)
--     17 -  32       48      numeric(21,0)  - numeric(52,0)
--     33 -  48       64      numeric(53,0)  - numeric(84,0)
--     49 -  64       80      numeric(85,0)  - numeric(116,0)
--     65 -  80       96      numeric(117,0) - numeric(128,0)
--     81 -  96      112
--     97 - 112      128
--    113 - 128      144
--    129 - 144      160
--    145 - 160      176
--    161 - 176      192
--    177 - 192      208
--    193 - 208      224
--    209 - 224      240

--   The integer data types tinyint, small int, integer, and bigint
--   are varbinary(32) ciphertext.

--   The exact relationship is
--   DATALENGTH(ciphertext) =
--   (((DATALENGTH(plaintext)+ 15) / 16) + 1) * 16
```

```
--   For the first table, the DBA chooses to preserve both the
plaintext and
--   ciphertext forms. This is not typical and should only be done if
the
--   database files are also encrypted.

--   Take away NonPrivUser's access to column sensitiveA and transfer
--   access to the ciphertext version.

--   Put a unique index on the ciphertext column. The ciphertext
--   itself is indexed.

--   NonPrivUser can select the ciphertext and use it.

--   PrivUser can still select either form (without paying decrypt
costs).

    revoke select ( sensitiveA ) on DBA.first_table from
NonPrivUser ;
    alter table DBA.first_table add encryptedA varbinary(32) ;
    grant select ( encryptedA ) on DBA.first_table to PrivUser ;
    grant select ( encryptedA ) on DBA.first_table to NonPrivUser ;
    create unique hg index first_A_unique on first_table
( encryptedA ) ;
    update DBA.first_table
        set encryptedA = aes_encrypt(sensitiveA, 'seCr3t')
        where encryptedA is null ;
    commit

--   Now change column sensitiveB.

    alter table DBA.first_table add encryptedB varbinary(32) ;
    grant select ( encryptedB ) on DBA.first_table to PrivUser ;
    create unique hg index first_B_unique on first_table
( encryptedB ) ;
    update DBA.first_table
        set encryptedB = aes_encrypt(sensitiveB,
        'givethiskeytonoone') where encryptedB is null ;
    commit

--   For the second table, the DBA chooses to keep only the
ciphertext.
--   This is more typical and encrypting the database files is not
required.

    revoke select ( sensitiveA ) on DBA.second_table from
NonPrivUser ;
    revoke select ( sensitiveA ) on DBA.second_table from PrivUser ;
    alter table DBA.second_table add encryptedA varbinary(32) ;
    grant select ( encryptedA ) on DBA.second_table to PrivUser ;
    grant select ( encryptedA ) on DBA.second_table to NonPrivUser ;
    create unique hg index second_A_unique on second_table
( encryptedA ) ;
    update DBA.second_table
        set encryptedA = aes_encrypt(sensitiveA, 'seCr3t')
        where encryptedA is null ;
```

```
    commit
    alter table DBA.second_table drop sensitiveA ;

--   The following types of queries are permitted at this point,
before
--   changes are made for key protection:

--   Non-TRUSTED users can equi-join on ciphertext; they can also
select
--   the binary, but have no way to interpret it.

    select I.publicC, 3*II.publicQ+1
    from DBA.first_table I, DBA.second_table II
    where I.encryptedA = II.encryptedA and I.publicD IN
( '2006-01-11' ) ;

--   Ciphertext-only access rules out general predicates and
expressions.
--   The following query does not return meaningful results.
--
--   NOTE: These four predicates can be used on the varbinary
containing
--   ciphertext:
--      = (equality)
--      <> (inequality)
--      IS NULL
--      IS NOT NULL

    select count(*)
    from DBA.first_table I, DBA.second_table II
    where I.encryptedA = II.encryptedA and SUBSTR(I.encryptedA,4,3)
        BETWEEN '345' AND '456' ;

--   The TRUSTED user still has access to the plaintext columns that
--   were retained. Therefore, this user does not need to call
--   aes_decrypt and does not need the key.

    select count(*)
    from DBA.first_table I, DBA.second_table II
    where I.encryptedA = II.encryptedA and SUBSTR(I.sensitiveA,4,3)
        BETWEEN '345' AND '456' ;


--   Part III: Protect the encryption keys

--   This section illustrates how to grant access to the plaintext,
but
--   still protect the keys.

--   For the first table, the DBA elected to retain the plaintext
columns.
--   Therefore, the following view has the same capabilities as the
trusted
--   user above.
--   Assume group_member is being used for additional access control.
```

```
--   NOTE: In this example, NonPrivUser still has access to the
ciphertext
--   encrypted in the base table.

    create view DBA.a_first_view (sensitiveA, publicC, publicD)
        as
            select
            IF group_member('high_privileges_group',user_name()) = 1
                 THEN sensitiveA
                 ELSE NULL
              ENDIF,
              publicC,
              publicD
            from first_table ;

    grant select on DBA.a_first_view to PrivUser ;
    grant select on DBA.a_first_view to NonPrivUser ;

--   For the second table, the DBA did not keep the plaintext.
--   Therefore, aes_decrypt calls must be used in the view.
--   IMPORTANT: Hide the view definition with ALTER VIEW, so that no
one
--   can discover the key.

    create view DBA.a_second_view
(sensitiveA,publicP,publicQ,publicR)
        as
            select
            IF group_member('high_privileges_group',user_name()) = 1
                 THEN aes_decrypt(encryptedA,'seCr3t', char(16))
                 ELSE NULL
              ENDIF,
              publicP,
              publicQ,
              publicR
            from second_table ;

    alter view DBA.a_second_view set hidden ;
    grant select on DBA.a_second_view to PrivUser ;
    grant select on DBA.a_second_view to NonPrivUser ;

--   Likewise, the key used for loading can be protected in a stored
     procedure.
--   By hiding the procedure (just as the view is hidden), no-one can
see
--   the keys.

    create procedure load_first_proc(@inputFileName varchar(255),
                        @colDelim varchar(4) default '$',
                        @rowDelim varchar(4) default '¥n')
        begin
            execute immediate with quotes
                'load table DBA.second_table
                (encryptedA encrypted(char(16),' ||
              '''' || 'seCr3t' || '''' || '),publicP,publicQ,publicR)
```

```
' ||
                ' from ' || '''' || @inputFileName || '''' ||
                ' delimited by ' || '''' || @colDelim || '''' ||
                ' row delimited by ' || '''' || @rowDelim || '''' ||
                ' quotes off escapes off' ;
        end
    ;

    alter procedure DBA.load_first_proc set hidden ;

--   Call the load procedure using the following syntax:

    call load_first_proc('/dev/null', '$', '¥n') ;

--   Below is a comparison of several techniques for protecting the
--   encryption keys by using user-defined functions (UDFs), other
views,
--   or both. The first and the last alternatives offer maximum
performance.

--   The second_table is secured as defined earlier.


--   Alternative 1:
--   This baseline approach relies on restricting access to the
entire view.

     create view

DBA.second_baseline_view(sensitiveA,publicP,publicQ,publicR)
        as
            select
            IF group_member('high_privileges_group',user_name()) = 1
                 THEN aes_decrypt(encryptedA,'seCr3t', char(16))
                 ELSE NULL
              ENDIF,
              publicP,
              publicQ,
              publicR
            from DBA.second_table ;

     alter view DBA.second_baseline_view set hidden ;
     grant select on DBA.second_baseline_view to NonPrivUser ;
     grant select on DBA.second_baseline_view to PrivUser ;


--   Alternative 2:
--     Place the encryption function invocation within a user-defined
--   function (UDF).
--    Hide the definition of the UDF. Restrict the UDF permissions.
--    Use the UDF in a view that handles the remainder of the security
--      and business logic.
--    Note: The view itself does not need to be hidden.

     create function DBA.second_decrypt_function(IN datum
```

```
varbinary(32))
            RETURNS char(16) DETERMINISTIC
            BEGIN
                RETURN aes_decrypt(datum,'seCr3t', char(16));
            END  ;

     grant execute on DBA.second_decrypt_function to PrivUser ;
     alter function DBA.second_decrypt_function set hidden ;

     create view

DBA.second_decrypt_view(sensitiveA,publicP,publicQ,publicR)
        as
                select
               IF group_member('high_privileges_group',user_name())
= 1
                     THEN second_decrypt_function(encryptedA)
                     ELSE NULL
                  ENDIF,
                  publicP,
                 publicQ,
                 publicR
                from DBA.second_table ;

     grant select on DBA.second_decrypt_view to NonPrivUser ;
     grant select on DBA.second_decrypt_view to PrivUser ;

--  Alternative 3:
--    Sequester only the key selection in a user-defined function.
--    This function could be extended to support selection of any
--  number of keys.
--    This UDF is also hidden and has restricted execute privileges.
--    Note: Any view that uses this UDF therefore does not compromise
-- the key values.

     create function DBA.second_key_function()
              RETURNS varchar(32) DETERMINISTIC
              BEGIN
                return 'seCr3t' ;
              END

     grant execute on DBA.second_key_function to PrivUser ;
     alter function DBA.second_key_function set hidden ;

     create view
DBA.second_key_view(sensitiveA,publicP,publicQ,publicR)
                as
                    select
                      IF
group_member('high_privileges_group',user_name()) = 1
                         THEN
aes_decrypt(encryptedA,second_key_function(),
                         char(16))
                         ELSE NULL
                      ENDIF,
                      publicP,
```

```
                      publicQ,
                      publicR
                    from DBA.second_table ;

     grant select on DBA.second_key_view to NonPrivUser ;
     grant select on DBA.second_key_view to PrivUser ;


--  Alternative 4:
--    The recommended alternative is to separate the security logic
--   from the business logic by dividing the concerns into two views.
--    Only the security logic view needs to be hidden.
--   Note: The performance of this approach is similar to that of the
first
-- alternative.

     create view

DBA.second_SecurityLogic_view(sensitiveA,publicP,publicQ,publicR)
            as
                select
               IF group_member('high_privileges_group',user_name())
= 1
                     THEN aes_decrypt(encryptedA,'seCr3t', char(16))
                     ELSE NULL
                  ENDIF,
                  publicP,
                  publicQ,
                  publicR
                from DBA.second_table ;

     alter view DBA.second_SecurityLogic_view set hidden ;

     create view

DBA.second_BusinessLogic_view(sensitiveA,publicP,publicQ,publicR)
            as
                select
                  sensitiveA,
                  publicP,
                  publicQ,
                  publicR
                from DBA.second_SecurityLogic_view ;

     grant select on DBA.second_BusinessLogic_view to NonPrivUser ;
     grant select on DBA.second_BusinessLogic_view to PrivUser ;

-- End of encryption example
```

参照：

- AES_ENCRYPT 関数 [文字列] (208 ページ)
- AES_DECRYPT 関数 [文字列] (211 ページ)
- LOAD TABLE ENCRYPTED 句 (212 ページ)

SAP Sybase IQ での Kerberos 認証サポート

SAP Sybase IQ では Kerberos 認証がサポートされています。これは、1 つのユーザ ID とパスワードでオペレーティングシステムおよびネットワークへのログインとデータベース接続の両方を管理できるログイン機能です。

Kerberos クレデンシャルを使用することで、ユーザ ID やパスワードを指定せずにデータベースに接続できます。

Kerberos 認証は、別途ライセンスが必要な SAP Sybase IQ Advanced Security オプションの一部です。

Kerberos のためのライセンス要件

Advanced Security オプション (IQ_SECURITY) は、環境を不正アクセスから保護します。SAP Sybase IQ で Kerberos ユーザ認証を使用するにはこのオプションが必要です。

SAP Sybase IQ での LDAP ユーザ認証サポート

SAP Sybase IQ は、幅広く使用されている国際規格である Lightweight Directory Access Protocol (LDAP) をベースとする既存の全社的ディレクトリアクセスフレームワークに統合することができます。

LDAP ユーザ認証のライセンス要件

Advanced Security オプション (IQ_SECURITY) は、環境を不正アクセスから保護します。SAP Sybase IQ で LDAP ユーザ認証を使用可能にするにはこのオプションが必要です。

付録： SQL リファレンス

このマニュアルで使用されている SQL 文、データベースオプション、関数、およびシステムプロシージャについての参考資料。

SQL 文

Interactive SQL 文は、データベースをカスタマイズおよび変更します。

ALTER LDAP SERVER 文

LDAP サーバ設定オブジェクトへの変更は以降の接続に適用されます。変更が適用されたときにすでに開始していた接続に対しては、変更がすぐに反映されることはありません。

クイックリンク：

「パラメータ」 (249 ページ)

「例」 (251 ページ)

「使用法」 (251 ページ)

「標準」 (251 ページ)

「パーミッション」 (251 ページ)

構文

```
ALTER LDAP SERVER ldapua-server-name
    { ldapua-server-attribs
    | [ WITH ( SUSPEND | ACTIVATE | REFRESH ) ] }

ldapua-server-attribs – （構文に戻る）
    SEARCH DN
        URL { 'URL_string' | NULL }
        | ACCESS ACCOUNT { 'DN_string' | NULL }
        | IDENTIFIED BY ( 'password' | NULL }
        | IDENTIFIED BY ENCRYPTED { encrypted-password | NULL }
    | AUTHENTICATION URL { 'URL_string' | NULL }
    | CONNECTION TIMEOUT timeout_value
    | CONNECTION RETRIES retry_value
    | TLS { ON | OFF }
```

パラメータ

（先頭に戻る） (249 ページ)

- **URL –** 指定されたユーザ ID のホスト (名前または IP アドレスで指定)、ポート番号、および DN ルックアップで実行される検索を指定します。この値は、ISYSLDAPSERVER システムテーブルに格納される前に、LDAP URL 構文が正しいかどうかが検証されます。この文字列の最大サイズは 1024 バイトです。
- **ACCESS ACCOUNT –** SAP Sybase IQ 内のユーザではなく、SAP Sybase IQ が使用するために LDAP サーバで作成されたユーザ。このユーザの識別名 (DN) は、LDAP サーバへの接続に使用されます。このユーザは、SEARCH DN URL で指定された場所でユーザ ID によって DN を検索するためのパーミッションを、LDAP サーバ内に保持しています。この文字列の最大サイズは 1024 バイトです。
- **IDENTIFIED BY –** ACCESS ACCOUNT ユーザに関連付けられたパスワードを指定します。このパスワードは、対称暗号化を使用してディスクに保存されます。パスワードを解除して何も設定しない場合は、値 NULL を指定します。クリアテキストのパスワードの最大サイズは 255 バイトです。
- **IDENTIFIED BY ENCRYPTED –** ACCESS ACCOUNT に指定されている識別名に関連付けられた暗号化形式のパスワードを設定します。バイナリ値は暗号化されたパスワードであるため、ディスクにそのまま保存されます。パスワードを解除して何も設定しない場合は、値 NULL を指定します。バイナリの最大サイズは 289 バイトです。暗号化キーは有効な varbinary 値である必要があります。.暗号化キーは、引用符で囲まないでください。
- **AUTHENTICATION URL –** ユーザの認証に使用する LDAP サーバのホスト (名前または IP アドレスで指定) とポート番号を指定します。これは、URL_string として定義された値で、ISYSLDAPSERVER に格納される前に、LDAP URL 構文が正しいかどうかが検証されます。事前の DN 検索によって得られたユーザの DN とユーザパスワードによって、新しい接続が認証 URL にバインドされます。LDAP サーバへの正常な接続は、接続ユーザの ID の証明とみなされます。この文字列の最大サイズは 1024 バイトです。
- **CONNECTION TIMEOUT –** DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続のタイムアウトを指定します。この値はミリ秒で指定します。デフォルト値は 10 秒です。
- **CONNECTION RETRIES –** DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続の再試行回数を指定します。有効な値の範囲は 1 〜 60 で、デフォルト値は 3 です。
- **TLS –** DN 検索と認証の両方に使用する LDAP サーバへの接続に、TLS とセキュア LDAP プロトコルのいずれを使用するかを定義します。ON に設定すると、TLS プロトコルが使用され、URL は "ldap://" で始まります。OFF に設定すると (または指定しないと)、セキュア LDAP プロトコルが使用され、URL は

“ldaps://” で始まります。TLS プロトコルを使用する場合は、LDAP サーバによって使用される証明書に署名する認証局 (CA) の証明書が含まれているファイル名を使用して、データベースセキュリティオプション TRUSTED_CERTIFICATES_FILE を指定します。

- **WITH ACTIVATE –** LDAP サーバ設定オブジェクトを有効にして、作成時にすぐに使用できるようにします。これによって、1 つの文で LDAP ユーザ認証の定義と有効化を行うことができます。WITH ACTIVATE を使用すると、LDAP サーバ設定オブジェクトのステータスは READY に変わります。

例

（先頭に戻る） (249 ページ)

- **例 1 –** `apps_primary` という名前の LDAP サーバ設定オブジェクトを中断します。

```
ALTER LDAP SERVER apps_primary SUSPEND
```

- **例 2 –** `apps_primary` という名前の LDAP サーバ設定オブジェクトがホスト `fairfax` 上の別の URL を認証に使用するように変更し、ポート番号を `1066` に設定し、接続試行回数を `10` に設定して、最後に LDAP サーバ設定オブジェクトを有効化します。

```
ALTER LDAP SERVER apps_primary
AUTHENTICATION URL 'ldap://my_LDAPserver:1066/'
CONNECTION RETRIES 10
WITH ACTIVATE
```

使用法

（先頭に戻る） (249 ページ)

属性の LDAP サーバ設定オブジェクト値のリセットに加えて、**ALTER LDAP SERVER** 文により、管理者はサーバのステータスと動作を手動で調整できます。これは、LDAP サーバ設定オブジェクトをメンテナンスモードにしたり、メンテナンスモードからサービスモードに戻すことによって行います。

標準

（先頭に戻る） (249 ページ)

ANSI SQL – 準拠レベル： Transact-SQL® 拡張。

パーミッション

（先頭に戻る） (249 ページ)

MANAGE ANY LDAP SERVER システム権限が必要です。

ALTER LOGIN POLICY 文

既存のログインポリシーを変更、または論理サーバアクセスを設定します。

クイックリンク：

「パラメータ」 (253 ページ)

「例」 (253 ページ)

「使用法」 (253 ページ)

「パーミッション」 (254 ページ)

構文

構文 1

```
ALTER LOGIN POLICY policy-name
    { { ADD | DROP | SET } LOGICAL SERVER ls-assignment-list
    [ LOGICAL SERVER ls-override-list ])

ls-assignment-list - (back to Syntax 1)
    { { ls-name, ...}
    | ALL
    | COORDINATOR
    | SERVER
    | NONE
    | DEFAULT }

ls-override-list - (back to Syntax 1)
    { ls-name, ...}

ls-name - (back to ls-assignment-list) or (back to ls-override-list)
    { OPEN | user-defined-ls-name }
```

構文 2

```
ALTER LOGIN POLICY policy-name policy-option

policy-option - (back to Syntax 2)
    policy-option-name = policy-option-value

policy-option-name - (back to policy-option)
   AUTO_UNLOCK_TIME
    | CHANGE_PASSWORD_DUAL_CONTROL
    | DEFAULT_LOGICAL_SERVER
    | LOCKED
    | MAX_CONNECTIONS
    | MAX_DAYS_SINCE_LOGIN
    | MAX_FAILED_LOGIN_ATTEMPTS
    | MAX_NON_DBA_CONNECTIONS
    | PASSWORD_EXPIRY_ON_NEXT_LOGIN
    | PASSWORD_GRACE_TIME
    | PASSWORD_LIFE_TIME
```

```
    | ROOT_AUTO_UNLOCK_TIME
    | LDAP_PRIMARY_SERVER
    | LDAP_SECONDARY_SERVER
    | LDAP_AUTO_FAILBACK_PERIOD
    | LDAP_FAILOVER_TO_STD
    | LDAP_REFRESH_DN

policy-option-value - (back to policy-option)
    { UNLIMITED | DEFAULT | value }
```

パラメータ

（先頭に戻る） (252 ページ)

- **policy-name –** ログインポリシーの名前。ルートを指定してルートログインポリシーを修正します。
- **policy-option-name –** ポリシーオプションの名前。各オプションの詳細については、「ログインポリシーオプション」と「LDAP ログインポリシーオプション」を参照してください。
- **policy-option-value –** ログインポリシーオプションに割り当てられる値。UNLIMITED を指定すると、制限は使用されません。DEFAULT を指定すると、デフォルトの制限が使用されます。各オプションでサポートされている値については、「ログインポリシーオプション」と「LDAP ログインポリシーオプション」を参照してください。.

適用対象

シンプレックスとマルチプレックス。

例

（先頭に戻る） (252 ページ)

- **例 1 –** 「論理サーバへのアクセス許可設定」と「マルチプレックスログインポリシーの設定」を参照してください。
- **例 2 –** `Test1` ログインポリシーで password_life_time 値を `UNLIMITED` に設定し、max_failed_login_attempts 値を `5` に設定します。

```
ALTER LOGIN POLICY Test1
password_life_time=UNLIMITED
max_failed_login_attempts=5;
```

使用法

（先頭に戻る） (252 ページ)

ポリシーオプションを指定しない場合は、ルートログインポリシーからこのログインポリシーの値が取得されます。新しいポリシーは、

MAX_NON_DBA_CONNECTIONS および ROOT_AUTO_UNLOCK_TIME ポリシーオプションを継承しません。

新しいデータベースのすべてに、ルートログインポリシーが含まれています。ルートログインポリシーの値を変更することはできますが、ポリシーは削除できません。

パーミッション

（先頭に戻る） (252 ページ)

MANAGE ANY LOGIN POLICY システム権限が必要です。

ログインポリシーオプション

ルートログインポリシーとユーザ定義ログインポリシーで使用可能なオプションを次に示します。

オプション	説明
AUTO_UNLOCK_TIME	MANAGE ANY USER システム権限が付与されていないアカウントがロックされてから自動的にロック解除されるまでの時間。このオプションは、ルートログインポリシーを含む任意のログインポリシーで定義できる。 • **値** – 0 ～ UNLIMITED • **デフォルト** – UNLIMITED • **適用対象** – MANAGE ANY USER システム権限が付与されていないすべてのユーザ。
CHANGE_PASSWORD_DUAL_CONTROL	別のユーザのパスワードを変更するために、CHANGE PASSWORD システム権限が付与されている 2 人のユーザからの入力を要求する。 • **値** – ON、OFF • **デフォルト** – OFF • **適用対象** – すべてのユーザ。

オプション	説明

DEFAULT_LOGICAL_SERVER	接続文字列で論理サーバが指定されていない場合、ユーザはユーザのログインポリシーで指定されている DEFAULT_LOGICAL_SERVER オプションに接続する。
	• **値** –
	  • 既存のユーザ定義論理サーバの名前。
	  • ALL – すべての論理サーバへのアクセスを許可する。
	  • AUTO – ルートログインポリシーのデフォルト論理サーバの値。
	  • COORDINATOR – 現在のコーディネータノード。
	  • NONE – あらゆるマルチプレックスサーバへのアクセスを拒否する。
	  • OPEN – 単独またはユーザ定義論理サーバの名前とともに使用する。どのユーザ定義論理サーバのメンバーでもないすべてのマルチプレックスノードへのアクセスを許可する。
	  • SERVER – SERVER 論理サーバのセマンティックに従って、すべてのマルチプレックスノードへのアクセスを許可する。
	• **デフォルト** – AUTO
	• **適用対象** – すべてのユーザ。MANAGE MULTIPLEX システム権限が必要。

LOCKED	ON に設定すると、ユーザは新しい接続を確立できない。この設定は一時的にログインポリシーユーザへのアクセスを拒否する。このオプションは、論理サーバに設定されたログインポリシーの上書きはできない。 • **値** – ON、OFF • **デフォルト** – OFF • **適用対象** – MANAGE ANY USER システム権限を持つユーザを除くすべてのユーザ。

オプション	説明
MAX_CONNECTIONS	1 ユーザに許可される最大同時接続数。このオプションは、論理サーバごとの設定を指定できる。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – SERVER OPERATOR または DROP CONNECTION システム権限を持つユーザを除くすべてのユーザ。
MAX_DAYS_SINCE_LOGIN	同一ユーザによる連続する 2 回のログインの間で許容される最大経過日数。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – MANAGE ANY USER システム権限を持つユーザを除くすべてのユーザ。
MAX_FAILED_LOGIN_ATTEMPTS	前回のユーザアカウントへのログイン成功以降、アカウントがロックされるまでのログイン失敗の最大回数。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – すべてのユーザ。
MAX_NON_DBA_CONNECTIONS	SERVER OPERATOR または DROP CONNECTION システム権限を持たないユーザが確立できる同時接続の最大数。このオプションは、ルートログインポリシーでのみサポートされる。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – SERVER OPERATOR または DROP CONNECTION システム権限を持つユーザを除くすべてのユーザ。

オプション	説明
PASSWORD_EXPIRY_ON_NEXT_LOGIN	ON に設定すると、次回のログイン時にユーザのパスワードの有効期限が切れる。 • **値** – ON、OFF • **デフォルト** – OFF • **適用対象** – すべてのユーザ。 **注意：** この機能は現在、SAP Control Center へのログイン時に実装されなくなっています。ユーザは、パスワードの変更を要求されません。ただし、SAP Control Center 外から (たとえば Interactive SQL を使用して) SAP Sybase IQ にログインする際には要求されます。
PASSWORD_GRACE_TIME	パスワードの有効期限が切れるまでの日数 (ログインが可能だが、デフォルトの post_login プロシージャによって警告が発行される期間)。 • **値** – 0 ～ 2147483647 • **デフォルト** – 0 • **適用対象** – すべてのユーザ。
PASSWORD_LIFE_TIME	パスワードの変更が必要となるまでの最大日数。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – すべてのユーザ。
ROOT_AUTO_UNLOCK_TIME	MANAGE ANY USER システム権限が付与されているアカウントがロックされてから自動的にロック解除されるまでの時間。このオプションは、ルートログインポリシーでのみ定義できる。 • **値** – 0 ～ UNLIMITED • **デフォルト** – 15 • **適用対象** – MANAGE ANY USER システム権限が付与されているすべてのユーザ。

LDAP ログインポリシーオプション

LDAP ユーザ認証で使用可能なログインポリシーオプションを示します。

オプション	説明
LDAP_PRIMARY_SERVER	プライマリ LDAP サーバの名前を指定する。 • **値** – 該当なし • **デフォルト** – なし • **適用対象** – すべてのユーザ。
LDAP_SECONDARY_SERVER	セカンダリ LDAP サーバの名前を指定する。 • **値** – 該当なし • **デフォルト** – なし • **適用対象** – すべてのユーザ。
LDAP_AUTO_FAIL-BACK_PERIOD	プライマリサーバへの自動フェールバックが試行されるまでの時間 (分単位) を指定する。 • **値** – 0 ～ 2147483647 • **デフォルト** – 15 分 • **適用対象** – すべてのユーザ。
LDAP_FAILOVER_TO_STD	システムリソース、ネットワークの停止、接続のタイムアウト、または同様のシステム障害が原因で LDAP サーバによる認証に失敗した場合に、標準認証による認証を許可する。ただし、LDAP サーバから返された実際の認証の失敗を標準認証にフェールバックすることは許可しない。 • **値** – ON、OFF • **デフォルト** – ON • **適用対象** – すべてのユーザ。

オプション	説明
LDAP_REFRESH_DN	ISYSLOGINPOLICYOPTION システムテーブル内の ldap_refresh_dn の値を協定世界時 (UTC) の現在時刻で更新する。 ISYSLOGINPOLICYOPTION の ldap_refresh_dn の値が ISYSUSER の user_dn の値より新しい場合、LDAP によるユーザ認証のたびに新しいユーザ DN の検索が行われる。その場合、新しいユーザ DN で user_dn の値が更新され、現在時刻で user_dn_changed_at の値が再更新される。 • **値** – NOW • **ROOT ポリシーの初期値** – NULL • **ユーザ定義ログインポリシーの初期値** – 現在時刻を UTC で格納 • **適用対象** – すべてのユーザ。

マルチプレックスログインポリシーの設定

マルチプレックスサーバのログインポリシーを設定します。

例

この例では、論理サーバのログインポリシー設定が上書きされ、論理サーバ ls1 の最大接続数が増加します。

```
ALTER LOGIN POLICY lp1 max_connections=20 LOGICAL SERVER ls1;
```

使用法

マルチプレックスにのみ適用されます。

任意のマルチプレックスサーバ上で実行するログイン管理コマンドは、マルチプレックス内のすべてのサーバに自動的に伝達されます。最高のパフォーマンスを実現するには、これらのコマンドまたは DDL をコーディネータで実行します。

論理サーバレベルで上書きすると、特定のログインポリシーオプションが、論理サーバごとに設定が異なることになります。
SYS.ISYSIQLSLOGINPOLICYOPTION には、論理サーバ上書きのためのログインポリシーオプション値が格納されています。ISYSIQLSLOGINPOLICYOPTION には、ログインポリシーオプションの論理サーバの上書きのそれぞれに対応するローが存在します。

論理サーバへのアクセス許可設定
論理サーバアクセスを設定します。

例 1

ルートログインポリシーが論理サーバの ls4 と ls5 へのアクセスを許可し、ログインポリシー lp1 が論理サーバの割り当てなしで存在するとします。次の文は、ログインポリシー lp1 に、論理サーバ ls4 と ls5 へのアクセス許可も実質的に割り当てます。

論理サーバ ls1 をログインポリシー lp1 に割り当てます。

```
ALTER LOGIN POLICY lp1 ADD LOGICAL SERVER ls1
```

例 2

次の文は、ログインポリシー lp1 から論理サーバの ls2 と ls3 へのアクセスを許可します。

```
ALTER LOGIN POLICY lp1 ADD LOGICAL SERVER ls2, ls3
```

例 3

ログインポリシー lp1 を変更して、ls3 と ls4 にのみにアクセスを許可します。

```
ALTER LOGIN POLICY lp1 ADD LOGICAL SERVER ls4

ALTER LOGIN POLICY lp1 DROP LOGICAL SERVER ls1, ls2
```

または

```
ALTER LOGIN POLICY lp1 SET LOGICAL SERVER ls3, ls4
```

例 4

ログインポリシー lp1 を変更して、すべての論理サーバへのアクセスを拒否します。

```
ALTER LOGIN POLICY lp1 SET LOGICAL SERVER NONE
```

例 5

ログインポリシー lp1 の現在の論理サーバ割り当てを削除し、ルートログインポリシーの論理サーバ割り当てを継承できるようにします。

```
ALTER LOGIN POLICY lp1 SET LOGICAL SERVER DEFAULT
```

使用法
ADD 句、DROP 句、または SET 句を使用すると、次のようにログインポリシーの論理サーバ割り当てを設定できます。

- **ADD –** 新しい論理サーバ割り当てをログインポリシーに追加します。
- **DROP –** ログインポリシーから既存の論理サーバ割り当てを削除します。
- **SET –** 特定のログインポリシーのすべての論理サーバ割り当てを新しい一連の論理サーバに置き換えます。

ADD 句、DROP 句、または SET 句のいずれか 1 つのみを使用します。SERVER、NONE、DEFAULT は、SET 句でのみ使用します。個別の論理サーバ名は、ls-assignment list または ls-override list ごとに 1 回のみ指定します。

次の場合には、エラーが返されます。

- ADD 句で指定された論理サーバが、すでにログインポリシーに割り当てられている場合。
- DROP 句で指定された論理サーバが、ログインポリシーに現在割り当てられていない場合。
- 論理サーバ割り当ての変更により、割り当てられている論理サーバ間でメンバーシップの重複が発生する場合。

SYS.ISYSIQLOGINPOLICYLSINFO には、論理サーバ割り当ての情報が格納されています。ISYSIQLOGINPOLICYLSINFO には、ログインポリシーオプションの論理サーバの上書きのそれぞれに対応するローが存在します。

ALTER ROLE 文

互換ロールをユーザ定義システムロールに移行してから、その互換ロールを自動的に削除します。

注意： ALTER ROLE 文を使用して SYS_AUTH_SA_ROLE または SYS_AUTH_SSO_ROLE を移行することはできません。これらのロールは、SYS_AUTH_DBA_ROLE が移行されると、自動的に移行されます。

クイックリンク：

「パラメータ」 (262 ページ)

「例」 (262 ページ)

「使用法」 (263 ページ)

「標準」 (263 ページ)

「パーミッション」 (263 ページ)

構文

構文 1 – SYS_AUTH_DBA_ROLE を移行する場合

```
ALTER ROLE predefined_sys_role_name
   MIGRATE TO new_role_name [, new_sa_role_name, new_sso_role_name]
```

構文 2 – 他のすべての互換ロールを移行する場合

```
ALTER ROLE predefined_sys_role_name
   MIGRATE TO new_role_name
```

パラメータ

（先頭に戻る） (261 ページ)

- **predefined_sys_role_name –** データベースにまだ存在する (まだ削除されていない) 互換ロールの名前。
- **new_role_name –** 新しいロールの名前として、プレフィクス SYS_ で始まる名前またはサフィクス _ROLE で終わる名前は使用できません。
- **new_sa_role_name –** SYS_AUTH_DBA_ROLE を移行する場合のみ指定する必要があります。SYS_AUTH_SA_ROLE の基礎となるシステム権限を移行する新しいロールはデータベースに既存であってはいけません。また、新しいロールの名前として、プレフィクス SYS_ で始まる名前またはサフィクス _ROLE で終わる名前は使用できません。
- **new_sso_role_name –** SYS_AUTH_DBA_ROLE を移行する場合のみ指定する必要があります。SYS_AUTH_SSO_ROLE の基礎となるシステム権限を移行する新しいロールはデータベースに既存であってはいけません。また、新しいロールの名前として、プレフィクス SYS_ で始まる名前またはサフィクス _ROLE で終わる名前は使用できません。

例

（先頭に戻る） (261 ページ)

- **例 1 –** SYS_AUTH_DBA_ROLE を新しいロール `Custom_DBA`、`Custom_SA`、および `Custom_SSO` にそれぞれ移行します。さらに自動的に、SYS_AUTH_DBA_ROLE に付与されているすべてのユーザ、基礎となるシステム権限、およびロールを適用可能な新しいロールに移行します。最後に、SYS_AUTH_DBA_ROLE、SYS_AUTH_SA_ROLE、および SYS_AUTH_SSO_ROLE を削除します。

  ```
  ALTER ROLE SYS_AUTH_DBA_ROLE
  MIGRATE TO Custom_DBA, Custom_SA, Custom_SSO
  ```

- **例 2 –** SYS_AUTH_OPERATOR_ROLE ロールを新しいロール `Operator_role` に移行します。さらに自動的に、SYS_AUTH_OPERATOR_ROLE に付与されているすべてのユーザ、基礎となるシステム権限、およびロールを新しいロールに移行し、SYS_AUTH_OPERATOR_ROLE を削除します。

```
ALTER ROLE SYS_AUTH_OPERATOR_ROLE
MIGRATE TO Operator_role
```

使用法

（先頭に戻る） (261 ページ)

移行プロセス中は、次の処理が実行されます。

- 新しいユーザ定義ロールが作成されます。
- 移行中の事前定義済みのロールに現在付与されているすべてのシステム権限が、自動的に新しいユーザ定義ロールに付与されます。
- 移行中の事前定義済みのロールに現在付与されているすべてのユーザとロールが、自動的に新しいユーザ定義ロールに付与されます。
- 互換ロールは削除されます。

移行プロセス中はロール管理者が指定されないので、グローバルロール管理者のみが新しいロールを管理できます。CREATE ROLE 文を使用して、適切な管理権限を持つロール管理者をロールに追加します。

標準

（先頭に戻る） (261 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (261 ページ)

MANAGE ROLES システム権限が管理権限付きで付与されている必要があります。

ALTER USER 文

ユーザ設定を変更します。

クイックリンク：

「パラメータ」 (264 ページ)

「例」 (265 ページ)

「使用法」 (265 ページ)

「標準」 (267 ページ)

「パーミッション」 (267 ページ)

構文

構文 1 - データベースユーザの定義を変更します

```
ALTER USER user-name
    | [ IDENTIFIED BY password ]
    | [ LOGIN POLICY policy-name ]
    | [ FORCE PASSWORD CHANGE { ON | OFF } ]
```

構文 2 - LDAP ユーザの識別名 (DN) をリフレッシュします

```
ALTER USER user-name
    REFRESH DN
```

構文 3 - ユーザのログインポリシーの元の値へ復元します

```
ALTER USER user-name
    RESET LOGIN POLICY
```

構文 4 – ユーザのログインポリシーで CHANGE_PASSWORD_DUAL_CONTROL が有効になっている場合の、ユーザパスワードを変更します

```
ALTER USER user-name
    IDENTIFIED [ FIRST | LAST ] BY password_part
```

パラメータ

（先頭に戻る） (263 ページ)

- **user-name –** ユーザの名前。
- **IDENTIFIED BY –** ユーザのパスワード。ユーザのログインポリシーで CHANGE_PASSWORD_DUAL_CONTROL オプションが有効になっている場合、この句はサポートされません (ERROR)。
- **IDENTIFIED[FIRST | LAST] BY –** ターゲットユーザのログインポリシーで CHANGE_PASSWORD_DUAL_CONTROL オプションが有効になっている場合に必須の句。FIRST | LAST キーワードで、定義する二重パスワードの部分を指定します。
- **policy-name –** ユーザを割り当てるログインポリシーの名前。ログインポリシーを指定しないと、変更は行われません。LOGIN POLICY 句が指定されていない場合、変更は行われません。
- **FORCE PASSWORD CHANGE –** ログイン時にユーザが新しいパスワードを指定する必要があるかどうかを制御します。この設定は、ユーザのログインポリシーの PASSWORD_EXPIRY_ON_NEXT_LOGIN オプションの設定を上書きします。

  注意： この機能は現在、SAP Control Center へのログイン時に実装されなくなっています。ユーザは、パスワードの変更を要求されません。ただし、SAP Control Center 外から (たとえば Interactive SQL を使用して) SAP Sybase IQ にログインする際には要求されます。

- **RESET LOGIN POLICY –** ユーザのログインの設定をログインポリシー内の元の値に戻します。通常は、これによって、ユーザのログイン失敗回数が最大値を超えたか、前回のログイン以降に経過した日数が最大値を超えたために暗黙的に設定されたロックがすべてクリアされます。ログインポリシーをリセットすると、MAX_FAILED_LOGIN_ATTEMPTS や MAX_DAYS_SINCE_LOGIN などのログインポリシーオプションの上限を超えたためにロックされていたアカウントに、ユーザがアクセスできるようになります。
- **REFRESH DN –** LDAP 認証時に使用される、ユーザの保存済みの DN およびタイムスタンプをクリアします。

例

（先頭に戻る） (263 ページ)

- **例 1 –** ユーザ `SQLTester` を変更します。パスワードは、`welcome` に設定されます。`SQLTester` ユーザは `Test1` ログインポリシーに割り当てられ、パスワードの有効期限は次回ログイン時に切れません。

```
ALTER USER SQLTester
IDENTIFIED BY welcome
LOGIN POLICY Test1
FORCE PASSWORD CHANGE OFF
```

- **例 2 –** LDAP 認証で使用される、ユーザ `Mary` の識別名 (DN) およびタイムスタンプをクリアします。

```
ALTER USER Mary REFRESH DN
```

- **例 3 –** user3 のパスワードを PassPart1PassPart2 に設定します。ここでは、`user1` と `user2` が CHANGE PASSWORD システム権限を持っており、`user3` のログインポリシーで change_password_dual_control オプションが有効になっている (ON) ことを前提にしています。

  user1 は次のように入力します。

```
ALTER USER user3 IDENTIFIED FIRST BY PassPart1
```

  user2 は次のように入力します。

```
ALTER USER user3 IDENTIFIED LAST BY PassPart2
```

  設定後に、user3 はパスワード `PassPart1PassPart2` を入力してログオンします。

使用法

（先頭に戻る） (263 ページ)

ユーザ ID とパスワードで禁止されていることは次のとおりです。

- 最初の文字をスペース、一重引用符または二重引用符にする
- 最後の文字をスペースにする
- セミコロンを含める

パスワードは 255 文字を超えることはできません。

PASSWORD_EXPIRY_ON_NEXT_LOGIN 値を ON に設定すると、このログインポリシーに割り当てられたすべてのユーザのパスワードは、次回ログイン時にすぐに期限切れになります。次回ログイン時にユーザにパスワードの変更を強制するには、**ALTER USER** 句と **LOGIN POLICY** 句を使用します。

二重パスワード変更プロセス中に CHANGE_PASSWORD_DUAL CONTROL ログインポリシーオプションを無効 (OFF) にした場合は、次のようになります。

- ターゲットユーザは、すでに定義されている単一パスワード部分を使用してログインできなくなります。単一パスワード制御構文を使用して **ALTER USER** コマンドを再発行する必要があります。
- 二重パスワード変更プロセスが完了した後、ターゲットユーザがログインする前に、このオプションを無効にしても、ターゲットユーザには何の影響もありません。ターゲットユーザは、両方のパスワード部分を使用してログインする必要があります。

二重パスワード変更プロセスの実行時にユーザがすでにログインしている場合は、新しいパスワードの両方の部分が設定されるまで、現在のセッションでユーザが自分のパスワードを変更することはできません。二重パスワード変更プロセスが完了すると、ターゲットユーザは **GRANT CONNECT**、**ALTER USER**、**sp_password**、または **sp_iqpassword** を使用して、ログアウトしてからでなくてもパスワードを変更できます。現在のパスワードの入力を要求されたら、現在のセッションで最初に入力したパスワードではなく、新しい二重制御パスワードを使用します。

二重パスワード変更プロセスでどちらかのパスワード部分を設定している間は、**GRANT CONNECT** 文はサポートされません。ただし、二重パスワード変更プロセスが完了すると、ターゲットユーザは **GRANT CONNECT** 文、**ALTER USER**、**sp_password**、または **sp_iqpassword** を使用して、ログアウトしてからでなくても自分のパスワードを変更できます。

CHANGE PASSWORD システム権限を持つユーザがパスワードの両方の部分を正常に指定すると同時に、ターゲットユーザのパスワードの有効期限が自動的に切れます。これによって、ターゲットユーザは次回ログイン時にパスワードの変更を強制されます。

ユーザパスワードのハッシュに使用される暗号化アルゴリズムは、FIPS 認定の暗号化サポートです。

- この DLL は **dbfips10.dll** と呼ばれます。
- HASH 関数ではアルゴリズム **SHA1_FIPS** および **SHA256_FIPS** を使用できます。

- **-fips** サーバオプションを指定したときに FIPS 認定でないアルゴリズムを HASH 関数に指定すると、データベースサーバでは **SHA1** の代わりに **SHA1_FIPS** が、**SHA256** の代わりに **SHA256_FIPS** が使用されます。また、**MD5** を使用した場合はエラーが返されます (**MD5** は FIPS 認定のアルゴリズムではありません)。
- **-fips** オプションを指定した場合は、データベースサーバではパスワードハッシュ処理に SHA256_FIPS が使用されます。

標準

（先頭に戻る） (263 ページ)

- SQL - ISO/ANSI SQL 文法のベンダ拡張。
- SAP Sybase Database 製品 - Adaptive Server ではサポートされていません。

パーミッション

（先頭に戻る） (263 ページ)

- 自分のパスワードを変更する場合は、権限は不要です。
- 任意のユーザのパスワードを変更する場合は、CHANGE PASSWORD システム権限が必要です。
- **LOGIN POLICY** 句、**FORCE PASSWORD CHANGE** 句、**RESET LOGIN POLICY** 句、または **REFRESH DN** 句を使用する場合は、MANAGE ANY USER システム権限が必要です。

CREATE LDAP SERVER 文

LDAP ユーザ認証用の新しい LDAP サーバ設定オブジェクトを作成します。LDAP サーバ設定オブジェクトの作成中に定義されたパラメータは、ISYSLDAPSERVER (システムビュー SYSLDAPSERVER) システムテーブルに格納されます。

クイックリンク：

「パラメータ」 (268 ページ)

「例」 (269 ページ)

「標準」 (271 ページ)

「パーミッション」 (271 ページ)

構文

```
CREATE LDAP SERVER ldapua-server-name
    [ ldapua-server-attribs ]
    [ WITH ACTIVATE ]
```

```
ldapua-server-attribs
    SEARCH DN
        URL { 'URL_string' | NULL }
        | ACCESS ACCOUNT { 'DN_string' | NULL }
        | IDENTIFIED BY ( 'password' | NULL }
        | IDENTIFIED BY ENCRYPTED { encrypted-password | NULL }
    | AUTHENTICATION URL { 'URL_string' | NULL }
    | CONNECTION TIMEOUT timeout_value
    | CONNECTION RETRIES retry_value
    | TLS { ON | OFF }
```

パラメータ

（先頭に戻る） (267 ページ)

- **URL –** 指定されたユーザ ID のホスト (名前または IP アドレスで指定)、ポート番号、および DN ルックアップで実行される検索を指定します。この値は、ISYSLDAPSERVER システムテーブルに格納される前に、LDAP URL 構文が正しいかどうかが検証されます。この文字列の最大サイズは 1024 バイトです。
- **ACCESS ACCOUNT –** SAP Sybase IQ 内のユーザではなく、SAP Sybase IQ が使用するために LDAP サーバで作成されたユーザ。このユーザの識別名 (DN) は、LDAP サーバへの接続に使用されます。このユーザは、SEARCH DN URL で指定された場所でユーザ ID によって DN を検索するためのパーミッションを、LDAP サーバ内に保持しています。この文字列の最大サイズは 1024 バイトです。
- **IDENTIFIED BY –** ACCESS ACCOUNT ユーザに関連付けられたパスワードを指定します。このパスワードは、対称暗号化を使用してディスクに保存されます。パスワードを解除して何も設定しない場合は、値 NULL を指定します。クリアテキストのパスワードの最大サイズは 255 バイトです。
- **IDENTIFIED BY ENCRYPTED –** ACCESS ACCOUNT に指定されている識別名に関連付けられた暗号化形式のパスワードを設定します。バイナリ値は暗号化されたパスワードであるため、ディスクにそのまま保存されます。パスワードを解除して何も設定しない場合は、値 NULL を指定します。バイナリの最大サイズは 289 バイトです。暗号化キーは有効な varbinary 値である必要があります。.暗号化キーは、引用符で囲まないでください。
- **AUTHENTICATION URL –** ユーザの認証に使用する LDAP サーバのホスト (名前または IP アドレスで指定) とポート番号を指定します。これは、URL_string として定義された値で、ISYSLDAPSERVER に格納される前に、LDAP URL 構文が正しいかどうかが検証されます。事前の DN 検索によって得られたユーザの DN とユーザパスワードによって、新しい接続が認証 URL にバインドされま

す。LDAP サーバへの正常な接続は、接続ユーザの ID の証明とみなされます。この文字列の最大サイズは 1024 バイトです。

- **CONNECTION TIMEOUT –** DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続のタイムアウトを指定します。この値はミリ秒で指定します。デフォルト値は 10 秒です。
- **CONNECTION RETRIES –** DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続の再試行回数を指定します。有効な値の範囲は 1 ～ 60 で、デフォルト値は 3 です。
- **TLS –** DN 検索と認証の両方に使用する LDAP サーバへの接続に、TLS とセキュア LDAP プロトコルのいずれを使用するかを定義します。ON に設定すると、TLS プロトコルが使用され、URL は "ldap://" で始まります。OFF に設定すると (または指定しないと)、セキュア LDAP プロトコルが使用され、URL は “ldaps://” で始まります。TLS プロトコルを使用する場合は、LDAP サーバによって使用される証明書に署名する認証局 (CA) の証明書が含まれているファイル名を使用して、データベースセキュリティオプション TRUSTED_CERTIFICATES_FILE を指定します。
- **WITH ACTIVATE –** LDAP サーバ設定オブジェクトを有効にして、作成時にすぐに使用できるようにします。これによって、1 つの文で LDAP ユーザ認証の定義と有効化を行うことができます。WITH ACTIVATE を使用すると、LDAP サーバ設定オブジェクトのステータスは READY に変わります。

例

（先頭に戻る） (267 ページ)

- **例 1 –** 検索パラメータ、認証 URL を設定し、タイムアウトを 3 秒に設定し、ユーザの認証を開始できるようにサーバを有効化します。TLS プロトコルまたは SECURE LDAP プロトコルを使用しないで LDAP サーバに接続します。

```
SET OPTION PUBLIC.login_mode = ‘Standard,LDAPUA’
CREATE LDAP SERVER apps_primary
SEARCH DN
    URL 'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
WITH ACTIVATE
```

- **例 2 –** 例 1 と同じ検索パラメータを使用しますが、"ldaps" を指定することにより、ホスト my_LDAPserver、ポート 636 の LDAP サーバとのセキュア LDAP 接続が確立されるようにします。このポートにはセキュア LDAP プロトコルを使用している LDAP クライアントだけが接続できます。データベースセキュリ

ティオプション TRUSTED_CERTIFICATE_FILE は、"ldaps://my_LDAPserver:636" の LDAP サーバで使用される証明書に署名した認証局 (CA) の証明書が含まれるファイル名を使用して設定されている必要があります。LDAP サーバとのハンドシェイクの際に、LDAP サーバから提示された証明書が SAP Sybase IQ サーバ (LDAP クライアント) によってチェックされ、ファイル内にリストされているいずれかの証明書によって署名されているかどうか確認されます。これで、そのサーバが、自身が示しているサーバであるというクライアントからの信頼が構築されます。ACCESS ACCOUNT パラメータと IDENTIFIED BY パラメータは、そのクライアントが、自身が示しているクライアントであるという LDAP サーバからの信頼を構築します。

注意： TLS プロトコルではなくセキュア LDAP を使用する場合、TLS パラメータを OFF に設定する必要があります。

```
SET OPTION PUBLIC.login_mode = 'Standard,LDAPUA'
SET OPTION PUBLIC.trusted_certificates_file = '/mycompany/shared/
trusted.txt'
CREATE LDAP SERVER secure_primary
SEARCH DN
    URL  'ldaps://my_LDPAserver:636/dc=MyCompany,dc=com??sub?
cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldaps://my_LDAPserver:636/'
CONNECTION TIMEOUT 3000
TLS OFF
WITH ACTIVATE
```

- **例 3 –** ポート 389 で TLS プロトコルを構築します。また、データベースセキュリティオプション TRUSTED_CERTIFICATE_FILE はファイル名を指定して設定する必要があり、例 2 と同じセキュリティタイプを提供します。この例では、LDAP サーバベンダのサポート対象を拡大するため、TLS プロトコルは ON にします。

注意： SAP Sybase IQ サーバでセキュア LDAP または TLS を設定する方法を決定する際、使用するすべての LDAP サーバの要件を確認します。

```
SET OPTION PUBLIC.login_mode = 'Standard,LDAPUA'
SET OPTION PUBLIC.trusted_certificates_file = '/mycompany/shared/
trusted.txt'
CREATE LDAP SERVER tls_primary
SEARCH DN
    URL  'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
TLS ON
WITH ACTIVATE
```

標準

（先頭に戻る） (267 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (267 ページ)

MANAGE ANY LDAP SERVER システム権限が必要です。

CREATE LOGIN POLICY 文

ログインポリシーをデータベースに作成します。

クイックリンク：

「パラメータ」 (272 ページ)

「例」 (272 ページ)

「使用法」 (272 ページ)

「パーミッション」 (272 ページ)

構文

```
CREATE LOGIN POLICY policy-name policy-option

policy-option – （構文に戻る）
    policy-option-name = policy-option-value

policy-option-name – (back to policy-option)
  AUTO_UNLOCK_TIME
    | CHANGE_PASSWORD_DUAL_CONTROL
    | DEFAULT_LOGICAL_SERVER
    | LOCKED
    | MAX_CONNECTIONS
    | MAX_DAYS_SINCE_LOGIN
    | MAX_FAILED_LOGIN_ATTEMPTS
    | MAX_NON_DBA_CONNECTIONS
    | PASSWORD_EXPIRY_ON_NEXT_LOGIN
    | PASSWORD_GRACE_TIME
    | PASSWORD_LIFE_TIME
    | ROOT_AUTO_UNLOCK_TIME
    | LDAP_PRIMARY_SERVER
    | LDAP_SECONDARY_SERVER
    | LDAP_AUTO_FAILBACK_PERIOD
    | LDAP_FAILOVER_TO_STD
    | LDAP_REFRESH_DN

policy-option-value – (back to policy-option)
   { UNLIMITED | DEFAULT | value }
```

パラメータ

（先頭に戻る） (271 ページ)

- **policy-name –** ログインポリシーの名前。ルートを指定してルートログインポリシーを修正します。
- **policy-option-name –** ポリシーオプションの名前。各オプションの詳細については、「ログインポリシーオプション」と「LDAP ログインポリシーオプション」を参照してください。
- **policy-option-value –** ログインポリシーオプションに割り当てられる値。UNLIMITED を指定すると、制限は使用されません。DEFAULT を指定すると、デフォルトの制限が使用されます。各オプションでサポートされている値については、「ログインポリシーオプション」と「LDAP ログインポリシーオプション」を参照してください。.

適用対象

シンプレックスとマルチプレックス。

例

（先頭に戻る） (271 ページ)

- **例 1 –** `Test1` ログインポリシーを作成します。このログインポリシーでは、パスワードは無期限で、アカウントがロックされるまでに許容されるユーザパスワードの入力回数が最大 5 回に設定されています。

```
CREATE LOGIN POLICY Test1
password_life_time=UNLIMITED
max_failed_login_attempts=5;
```

使用法

（先頭に戻る） (271 ページ)

ポリシーオプションを指定しない場合は、ルートログインポリシーからこのログインポリシーの値が取得されます。新しいポリシーは、MAX_NON_DBA_CONNECTIONS および ROOT_AUTO_UNLOCK_TIME ポリシーオプションを継承しません。

パーミッション

（先頭に戻る） (271 ページ)

MANAGE ANY LOGIN POLICY システム権限が必要です。

次のシステム権限は、記載されているログインポリシーオプションを上書きできます。

例外システム権限	ログインポリシーオプション
SERVER OPERATOR システム権限または DROP CONNECTION システム権限	MAX_NON_DBA_CONNS MAX_CONNECTIONS
MANAGE ANY USER システム権限	LOCKED MAX_DAYS_SINCE_LOGIN

ログインポリシーオプション

ルートログインポリシーとユーザ定義ログインポリシーで使用可能なオプションを次に示します。

オプション	説明
AUTO_UNLOCK_TIME	MANAGE ANY USER システム権限が付与されていないアカウントがロックされてから自動的にロック解除されるまでの時間。このオプションは、ルートログインポリシーを含む任意のログインポリシーで定義できる。 • **値** – 0 ～ UNLIMITED • **デフォルト** – UNLIMITED • **適用対象** – MANAGE ANY USER システム権限が付与されていないすべてのユーザ。
CHANGE_PASSWORD_DUAL_CONTROL	別のユーザのパスワードを変更するために、CHANGE PASSWORD システム権限が付与されている 2 人のユーザからの入力を要求する。 • **値** – ON、OFF • **デフォルト** – OFF • **適用対象** – すべてのユーザ。

オプション	説明

DEFAULT_LOGICAL_SERVER	接続文字列で論理サーバが指定されていない場合、ユーザはユーザのログインポリシーで指定されている DEFAULT_LOGICAL_SERVER オプションに接続する。
	• **値** –
	  • 既存のユーザ定義論理サーバの名前。
	  • ALL – すべての論理サーバへのアクセスを許可する。
	  • AUTO – ルートログインポリシーのデフォルト論理サーバの値。
	  • COORDINATOR – 現在のコーディネータノード。
	  • NONE – あらゆるマルチプレックスサーバへのアクセスを拒否する。
	  • OPEN – 単独またはユーザ定義論理サーバの名前とともに使用する。どのユーザ定義論理サーバのメンバーでもないすべてのマルチプレックスノードへのアクセスを許可する。
	  • SERVER – SERVER 論理サーバのセマンティックに従って、すべてのマルチプレックスノードへのアクセスを許可する。
	• **デフォルト** – AUTO
	• **適用対象** – すべてのユーザ。MANAGE MULTIPLEX システム権限が必要。

LOCKED	ON に設定すると、ユーザは新しい接続を確立できない。この設定は一時的にログインポリシーユーザへのアクセスを拒否する。このオプションは、論理サーバに設定されたログインポリシーの上書きはできない。 • **値** – ON、OFF • **デフォルト** – OFF • **適用対象** – MANAGE ANY USER システム権限を持つユーザを除くすべてのユーザ。

オプション	説明
MAX_CONNECTIONS	1 ユーザに許可される最大同時接続数。このオプションは、論理サーバごとの設定を指定できる。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – SERVER OPERATOR または DROP CONNECTION システム権限を持つユーザを除くすべてのユーザ。
MAX_DAYS_SINCE_LOGIN	同一ユーザによる連続する 2 回のログインの間で許容される最大経過日数。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – MANAGE ANY USER システム権限を持つユーザを除くすべてのユーザ。
MAX_FAILED_LOGIN_ATTEMPTS	前回のユーザアカウントへのログイン成功以降、アカウントがロックされるまでのログイン失敗の最大回数。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – すべてのユーザ。
MAX_NON_DBA_CONNECTIONS	SERVER OPERATOR または DROP CONNECTION システム権限を持たないユーザが確立できる同時接続の最大数。このオプションは、ルートログインポリシーでのみサポートされる。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – SERVER OPERATOR または DROP CONNECTION システム権限を持つユーザを除くすべてのユーザ。

オプション	説明
PASSWORD_EXPIRY_ON_NEXT_LOGIN	ON に設定すると、次回のログイン時にユーザのパスワードの有効期限が切れる。 • **値** – ON、OFF • **デフォルト** – OFF • **適用対象** – すべてのユーザ。 **注意：** この機能は現在、SAP Control Center へのログイン時に実装されなくなっています。ユーザは、パスワードの変更を要求されません。ただし、SAP Control Center 外から (たとえば Interactive SQL を使用して) SAP Sybase IQ にログインする際には要求されます。
PASSWORD_GRACE_TIME	パスワードの有効期限が切れるまでの日数 (ログインが可能だが、デフォルトの post_login プロシージャによって警告が発行される期間)。 • **値** – 0 ～ 2147483647 • **デフォルト** – 0 • **適用対象** – すべてのユーザ。
PASSWORD_LIFE_TIME	パスワードの変更が必要となるまでの最大日数。 • **値** – 0 ～ 2147483647 • **デフォルト** – UNLIMITED • **適用対象** – すべてのユーザ。
ROOT_AUTO_UNLOCK_TIME	MANAGE ANY USER システム権限が付与されているアカウントがロックされてから自動的にロック解除されるまでの時間。このオプションは、ルートログインポリシーでのみ定義できる。 • **値** – 0 ～ UNLIMITED • **デフォルト** – 15 • **適用対象** – MANAGE ANY USER システム権限が付与されているすべてのユーザ。

LDAP ログインポリシーオプション

LDAP ユーザ認証で使用可能なログインポリシーオプションを示します。

オプション	説明
LDAP_PRIMARY_SERV-ER	プライマリ LDAP サーバの名前を指定する。 • **値** – 該当なし • **デフォルト** – なし • **適用対象** – すべてのユーザ。
LDAP_SECONDARY_SERVER	セカンダリ LDAP サーバの名前を指定する。 • **値** – 該当なし • **デフォルト** – なし • **適用対象** – すべてのユーザ。
LDAP_AUTO_FAIL-BACK_PERIOD	プライマリサーバへの自動フェールバックが試行されるまでの時間 (分単位) を指定する。 • **値** – 0 〜 2147483647 • **デフォルト** – 15 分 • **適用対象** – すべてのユーザ。
LDAP_FAILOVER_TO_STD	システムリソース、ネットワークの停止、接続のタイムアウト、または同様のシステム障害が原因で LDAP サーバによる認証に失敗した場合に、標準認証による認証を許可する。ただし、LDAP サーバから返された実際の認証の失敗を標準認証にフェールバックすることは許可しない。 • **値** – ON、OFF • **デフォルト** – ON • **適用対象** – すべてのユーザ。

オプション	説明
LDAP_REFRESH_DN	ISYSLOGINPOLICYOPTION システムテーブル内の ldap_refresh_dn の値を協定世界時 (UTC) の現在時刻で更新する。 ISYSLOGINPOLICYOPTION の ldap_refresh_dn の値が ISYSUSER の user_dn の値より新しい場合、LDAP によるユーザ認証のたびに新しいユーザ DN の検索が行われる。その場合、新しいユーザ DN で user_dn の値が更新され、現在時刻で user_dn_changed_at の値が再更新される。 • **値** – NOW • **ROOT ポリシーの初期値** – NULL • **ユーザ定義ログインポリシーの初期値** – 現在時刻を UTC で格納 • **適用対象** – すべてのユーザ。

マルチプレックスログインポリシーの設定

マルチプレックスサーバのログインポリシーを設定します。

例

この例では、論理サーバのログインポリシー設定が上書きされ、論理サーバ ls1 の最大接続数が増加します。

```
ALTER LOGIN POLICY lp1 max_connections=20 LOGICAL SERVER ls1;
```

使用法

マルチプレックスにのみ適用されます。

任意のマルチプレックスサーバ上で実行するログイン管理コマンドは、マルチプレックス内のすべてのサーバに自動的に伝達されます。最高のパフォーマンスを実現するには、これらのコマンドまたは DDL をコーディネータで実行します。

論理サーバレベルで上書きすると、特定のログインポリシーオプションが、論理サーバごとに設定が異なることになります。
SYS.ISYSIQLSLOGINPOLICYOPTION には、論理サーバ上書きのためのログインポリシーオプション値が格納されています。ISYSIQLSLOGINPOLICYOPTION には、ログインポリシーオプションの論理サーバの上書きのそれぞれに対応するローが存在します。

CREATE ROLE 文

新しいロールを作成したり、既存ユーザをロールとして使用できるように拡張したり、任意のロールのロール管理者を管理したりできます。

クイックリンク：

「パラメータ」 (279 ページ)

「例」 (280 ページ)

「使用法」 (281 ページ)

「標準」 (281 ページ)

「パーミッション」 (281 ページ)

構文

```
CREATE [ OR REPLACE ] ROLE { role_name | FOR USER userID }
   [ WITH ADMIN [ ONLY ] admin_name [...,], [ SYS_MANAGE_ROLES_ROLE ]
```

パラメータ

（先頭に戻る） (279 ページ)

- **role_name –** OR REPLACE 句を使用する場合を除き、*role_name* をデータベースに既存の名前にはできません。
- **OR REPLACE –** *role_name* はデータベースにすでに存在している必要があります。*role_name* がまだ存在していない場合、新しいユーザ定義ロールが作成されます。現在のすべての管理者が、以下のように *admin_name [..]* 句に指定されている管理者で置換されます。
  - WITH ADMIN OPTION を付与され、新しいロール管理者リストに指定されていない既存のロール管理者はすべて、ロールに対する管理権限を持たないロールのメンバーになります。
  - WITH ADMIN ONLY OPTION を付与され、新しいロール管理者リストに指定されていない既存のロール管理者はすべて、ロールのメンバーから削除されます。

  OR REPLACE 句を使用する際、新しいロール管理者リストに含まれている既存のロール管理者は、元の管理権限が置換権限より上位である場合、元の管理権限を保持します。たとえば、ユーザ A が、そのロールに対する WITH ADMIN 権限を付与されている既存のロール管理者であるとします。新しいロール管理者には WITH ADMIN ONLY 権限が付与されます。ユーザ A がこのリストに含まれている場合、ユーザ A は上位である WITH ADMIN 権限を保持します。

- **FOR USER –** OR REPLACE なしで FOR USER 句を使用する場合、*userID* は、ロールとして現在機能できない既存ユーザの名前である必要があります。
- **admin_name –** ロールの管理者として指定するユーザのリスト。
- **WITH ADMIN –** 指定の各 *admin_name* に、そのロールと、その基礎となるすべてのシステム権限に対する管理権限が付与されます。
  SYS_MANAGE_ROLES_ROLE がリストに含まれている場合は、WITH ADMIN 句は無効になります。
- **WITH ADMIN ONLY –** 指定の各 *admin_name* に、基礎となるシステム権限ではなく、そのロールに対する管理権限が付与されます。
- **SYS_MANAGE_ROLES_ROLE –** グローバルロール管理者がロールを管理できるようにします。WITH ADMIN ONLY 句とともに指定できます。

例

（先頭に戻る） (279 ページ)

- **例 1 –** ロール `Sales` を作成します。グローバルロール管理者のみがロールを管理できます。

```
CREATE ROLE Sales
```

- **例 2 –** 既存ユーザ `Jane` をロールとして機能できるように拡張します。

```
CREATE OR REPLACE ROLE FOR USER Jane
```

- **例 3 –** `Mary` と `Jeff` をロールの管理権限を持つロール管理者として、ロール `Finance` を作成します。グローバルロール管理者はこのロールを管理できません。

```
CREATE ROLE Finance
WITH ADMIN Mary, Jeff
```

- **例 3 –** `Mary` と `Jeff` をロール管理者として、ロール `Marketing` を作成します。グローバルロール管理者もこのロールを管理できます。

```
CREATE ROLE Finance
WITH ADMIN ONLY Mary, Jeff, SYS_MANAGE_ROLES_ROLE
```

- **例 4 –** `Finance` は `Harry` と `Susan` が管理権限を持つロール管理者である既存のロールです。`Susan` は管理者のままにして、`Harry` は置換し、グローバルロール管理者を追加します。新しいロール管理者は、管理権限のみを保有します。

  次の文は、`Susan` を管理者として保持しますが、`Susan` はもともと付与されていた管理権限の方が高いためにロールに対する管理権限を保持します。
  `Harry` は管理権限のみの `Bob` と `Sarah` に置換され、グローバル管理者が追加

されています。Harry は引き続きロールメンバーではありますが、管理権限は失います。

```
CREATE OR REPLACE ROLE Finance
WITH ADMIN ONLY Susan, Bob, Sarah, SYS_MANAGE_ROLE_ROLE
```

使用法

（先頭に戻る） (279 ページ)

ロール管理者 (*admin_name*) を指定し、グローバルロール管理者 (SYS_MANAGE_ROLES_ROLE) を含めない場合、グローバルロール管理者は新しいロールを管理できなくなります。したがって、作成時にはロール管理者を指定しないことをおすすめします。後で、OR REPLACE 句を使用して追加するようにしてください。

ADMIN 句を指定しない場合、デフォルトの WITH ADMIN ONLY 句が使用され、デフォルトの管理者はグローバルロール管理者 (SYS_MANAGE_ROLES_ROLE) になります。

ロール管理者を置換する際、ロールにグローバルロール管理者がいれば、新しいロール管理者リストにその管理者を含める必要があります。このようにしないと、ロールから削除されます。

ただし、WITH ADMIN 句を使用してロール管理者を付与する場合、この句はグローバルロール管理者に対しては無効なので、**GRANT ROLE** 文を使用して、グローバルロール管理者 (SYS_MANAGE_RILES_ROLE) をロールに追加しなおす必要があります。この付与に失敗すると、グローバルロール管理者はロールを管理できなくなります。

標準

（先頭に戻る） (279 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (279 ページ)

- 新しいロールを作成する場合 – MANAGE ROLES システム権限が必要です。
- OR REPLACE 句を使用する場合 – 置換するロールに対する管理権限とともに MANAGE ROLES システム権限が必要です。

CREATE USER 文

ユーザを作成します。

クイックリンク：

「パラメータ」 (282 ページ)

「例」 (283 ページ)

「使用法」 (283 ページ)

「標準」 (283 ページ)

「パーミッション」 (284 ページ)

構文

```
CREATE USER   user-name   [ IDENTIFIED BY password ]
[ LOGIN POLICY policy-name ]
[ FORCE PASSWORD CHANGE { ON | OFF } ]
```

パラメータ

（先頭に戻る） (282 ページ)

- **user-name –** ユーザの名前。
- **IDENTIFIED BY –** ユーザのパスワード。
- **policy-name –** ユーザを割り当てるログインポリシーの名前。ログインポリシーを指定しないと、変更は行われません。
- **FORCE PASSWORD CHANGE –** ログイン時にユーザが新しいパスワードを指定する必要があるかどうかを制御します。この設定は、ユーザのログインポリシーの PASSWORD_EXPIRY_ON_NEXT_LOGIN オプションの設定を上書きします。

  注意： この機能は現在、SAP Control Center へのログイン時に実装されなくなっています。ユーザは、パスワードの変更を要求されません。ただし、SAP Control Center 外から (たとえば Interactive SQL を使用して) SAP Sybase IQ にログインする際には要求されます。
- **password –** ユーザにパスワードを指定する必要はありません。パスワードのないユーザは、データベースに接続できません。これは、ロールを作成して、そのロールユーザ ID を使用したユーザをデータベースに接続させないようにする場合に便利です。ユーザ ID には、有効な識別子を使用します。ユーザ ID とパスワードで禁止されていることは次のとおりです。

- 最初の文字をスペース、一重引用符または二重引用符にする
- 最後の文字をスペースにする
- セミコロンを含める

パスワードには有効な識別子、または一重引用符で囲まれた文字列 (最大 255 文字) を指定できます。パスワードでは大文字と小文字を区別します。パスワードには 7 ビット ASCII 文字で使用してください。それ以外の文字を使用すると、データベースサーバがクライアントの文字セットを UTF-8 に変換できない場合に、パスワードが正しく機能しないことがあります。

VERIFY_PASSWORD_FUNCTION オプションを使用して、パスワードルール (パスワードには 1 つ以上の数字が含まれている必要があるなど) を実装する関数を指定できます。パスワード検証関数を使用する場合は、**GRANT CONNECT** 文に複数のユーザ ID とパスワードを指定することはできません。

ユーザパスワードのハッシュに使用される暗号化アルゴリズムは、FIPS 認定の暗号化サポートです。

- DLL は、dbfips10.dll という名前です。
- HASH 関数では、アルゴリズム SHA1_FIPS と SHA256_FIPS を使用できます。
- -fips サーバオプションを指定したときに FIPS 認定でないアルゴリズムを HASH 関数に指定すると、データベースサーバでは SHA1 の代わりに SHA1_FIPS が、SHA256 の代わりに SHA256_FIPS が使用されます。また、MD5 を使用した場合はエラーが返されます (MD5 は FIPS 認定のアルゴリズムではありません)。
- -fips オプションを指定した場合は、パスワードハッシュ処理に SHA256_FIPS が使用されます。

例

（先頭に戻る） (282 ページ)

- **例 1 –** `SQLTester` という名前のユーザを作成し、パスワードを welcome に設定します。`SQLTester` ユーザは `Test1` ログインポリシーに割り当てられ、パスワードは次回ログイン時に有効期限切れになります。

```
CREATE USER SQLTester IDENTIFIED BY welcome
LOGIN POLICY Test1
FORCE PASSWORD CHANGE ON;
```

標準

（先頭に戻る） (282 ページ)

- SQL - ISO/ANSI SQL 文法のベンダ拡張。
- SAP Sybase Database 製品 - Adaptive Server ではサポートされていません。

パーミッション

（先頭に戻る） (282 ページ)

MANAGE ANY USER システム権限が必要です。

DROP LDAP SERVER 文

指定された LDAP サーバ設定オブジェクトが READY または ACTIVE 状態ではないことを検証した後に、SYSLDAPSERVER システムビューから削除します。

クイックリンク：

「パラメータ」 (284 ページ)

「例」 (284 ページ)

「使用法」 (285 ページ)

「標準」 (285 ページ)

「パーミッション」 (285 ページ)

構文

```
DROP LDAP SERVER ldapua-server-name
    [ WITH DROP ALL REFERENCES ] [ WITH SUSPEND ]
```

パラメータ

（先頭に戻る） (284 ページ)

- **WITH DROP ALL REFERENCES –** ログインポリシーに参照がある LDAP サーバ設定オブジェクトをサービスから削除します。
- **WITH SUSPEND –** READY 状態または ACTIVE 状態の LDAP サーバ設定オブジェクトでも削除を可能にします。

例

（先頭に戻る） (284 ページ)

- **例 1 –** LDAP サーバ設定オブジェクトへの参照がすべてのログインポリシーから削除されている場合、次の 2 つのコマンドセットは同じになります。WITH DROP ALL REFERENCES パラメータと WITH SUSPEND パラメータを使用する

と、**ALTER LDAP SERVER** 文の後に **DROP LDAP SERVER** 文を実行する必要がなくなります。

```
DROP LDAP SERVER ldapserver1 WITH DROP ALL REFERENCES WITH SUSPEND
```

この文は次の文と同義です。

```
ALTER LDAP SERVER ldapserver1 WITH SUSPEND DROP LDAP SERVER
ldapserver1 WITH DROP ALL REFERENCES
```

使用法

（先頭に戻る） (284 ページ)

READY 状態または ACTIVE 状態の LDAP サーバ設定オブジェクトに対して **DROP LDAP SERVER** 文を発行すると、失敗します。これにより、アクティブな LDAP サーバ設定オブジェクトが偶発的に削除されないようにできます。また、LDAP サーバ設定オブジェクトを参照するログインポリシーが存在する場合も、**DROP LDAP SERVER** 文は失敗します。

標準

（先頭に戻る） (284 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (284 ページ)

MANAGE ANY LDAP SERVER システム権限が必要です。

DROP LOGIN POLICY 文

ログインポリシーをデータベースから削除します。

クイックリンク：

「例」 (285 ページ)

「使用法」 (286 ページ)

「パーミッション」 (286 ページ)

構文

DROP LOGIN POLICY *policy-name*

例

（先頭に戻る） (285 ページ)

- **例 1 –** `Test11` ログインポリシーを作成してから削除します。

```
CREATE LOGIN POLICY Test11;
DROP LOGIN POLICY Test11 ;
```

使用法

（先頭に戻る） (285 ページ)

DROP LOGIN POLICY 文は、ユーザに割り当てられたポリシーを削除しようとすると失敗します。**ALTER USER** 文を使用してユーザのポリシー割り当てを変更するか、**DROP USER** を使用してユーザを削除できます。

パーミッション

（先頭に戻る） (285 ページ)

MANAGE ANY LOGIN POLICY システム権限が必要です。

DROP ROLE 文

データベースからユーザ定義ロールを削除したり、ユーザ拡張ロールを通常のユーザに変換したりします。

クイックリンク：

「パラメータ」 (286 ページ)

「例」 (287 ページ)

「使用法」 (287 ページ)

「標準」 (287 ページ)

「パーミッション」 (288 ページ)

構文

```
DROP ROLE [ FROM USER ] role_name
    [ WITH REVOKE ]
```

パラメータ

（先頭に戻る） (286 ページ)

- **role_name –** データベースに既存のロールの名前である必要があります。
- **FROM USER –** データベースから削除するのではなく、ユーザ拡張ロールを通常のユーザに戻す際に必要です。*role_name* は、データベースに存在している必要があります。

このユーザは、ユーザ拡張ロールに付与されていたログイン権限、システム権限、およびロールをそのまま保持し、ユーザ拡張ロールが所有していたオブジェクトの所有者になります。ユーザ拡張に付与されていたユーザはただちに取り消されます。

- **WITH REVOKE** – ユーザがロールの基礎となるシステム権限を付与されたスタンドアロンロールまたはユーザ拡張ロールを削除するときに必要です。WITH ADMIN OPTION 句と　WITH NO ADMIN OPTION　句のどちらかを使用して付与できます。

例

（先頭に戻る） (286 ページ)

- **例 1** – 他のユーザまたはロールには付与されていない `Joe` という名前のユーザ拡張ロールを通常のユーザに戻します。

```
DROP ROLE FROM USER Joe
```

- **例 2** – 他のユーザまたはロールには付与されていない `Jack` という名前のユーザ拡張ロールをデータベースから削除します。

```
DROP ROLE Jack
```

- **例 3** – 他のユーザまたはロールに付与されている `Sam` という名前のユーザ拡張ロールを通常のロールに戻します。

```
DROP ROLE FROM USER Sam
WITH REVOKE
```

- **例 4** – 他のユーザまたはロールに付与されている `Sales2` という名前のスタンドアロンロールをデータベースから削除します。

```
DROP ROLE Sales2
WITH REVOKE
```

使用法

（先頭に戻る） (286 ページ)

ユーザ定義ロールは、残される依存ロールのすべてが、有効なパスワードを持つ管理ユーザの最少数を満たしていれば、データベースから削除することも、通常のユーザに戻すこともできます。

標準

（先頭に戻る） (286 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (286 ページ)

- 削除するロールに対する管理権限が必要です。
- 削除するロールがオブジェクトを所有している場合、DROP 文の実行時に、オブジェクトがセッションおよびユーザで使用されていてはいけません。

DROP USER 文

ユーザを削除します。

クイックリンク：

「パラメータ」 (288 ページ)

「例」 (288 ページ)

「標準」 (288 ページ)

「パーミッション」 (288 ページ)

構文

```
DROP USER user-name
```

パラメータ

（先頭に戻る） (288 ページ)

- **user-name –** 削除するユーザの名前。

例

（先頭に戻る） (288 ページ)

- **例 1 –** データベースからユーザ `SQLTester` を削除します。

```
DROP USER SQLTester
```

標準

（先頭に戻る） (288 ページ)

- SQL – ISO/ANSI SQL 準拠。
- SAP Sybase Database 製品 - Adaptive Server ではサポートされていません。

パーミッション

（先頭に戻る） (288 ページ)

MANAGE ANY USER システム権限が必要です。

注意： ユーザを削除すると、このユーザが所有しているオブジェクトとこのユーザが付与した権限がすべて削除されます。

GRANT CHANGE PASSWORD 文

ユーザが、他のユーザのパスワードを管理し、CHANGE PASSWORD システム権限を管理できるようにします。

クイックリンク：

「パラメータ」 (289 ページ)

「例」 (290 ページ)

「使用法」 (290 ページ)

「標準」 (291 ページ)

「パーミッション」 (291 ページ)

構文

```
GRANT CHANGE PASSWORD ( target_user_list | ANY | ANY WITH ROLES
target_role_list  )
   TO userID [,...]
   [ WITH ADMIN [ONLY] OPTION | WITH NO ADMIN OPTION]
```

パラメータ

（先頭に戻る） (289 ページ)

- **target_user_list –** 被付与者が同一化の対象とする可能性のあるユーザ。このリストは、ログインパスワードを持つ既存のユーザまたはユーザ拡張ロールで構成される必要があります。リスト内の userID はカンマで区切ります。
- **ANY –** ログインパスワードを持つすべてのデータベースユーザが、各被付与者のパスワードを管理する潜在的ターゲットユーザになります。
- **ANY WITH ROLES *target_role_list* –** 各被付与者のターゲットロールのリスト。いずれかのターゲットロールを付与されたユーザは、各被付与者の潜在的ターゲットユーザになります。*target_role_list* は既存のロールで構成される必要があり、前述のロールを付与されたユーザはログインパスワードを持つデータベースユーザで構成される必要があります。複数の userID を指定する場合は、カンマで区切ります。
- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

- **WITH ADMIN OPTION –** (ANY 句でのみ有効) ユーザは、パスワードを管理でき、別のユーザに CHANGE PASSWORD システム権限を付与することもできます。
- **WITH ADMIN ONLY OPTION –** (ANY 句でのみ有効) ユーザは、別のユーザに CHANGE PASSWORD システム権限を付与できますが、他のユーザのパスワードを管理することはできません。
- **WITH NO ADMIN OPTION –** ユーザはパスワードを管理できますが、別のユーザに CHANGE PASSWORD システム権限を付与することはできません。

例

（先頭に戻る） (289 ページ)

- **例 1 –** `Sally` と `Laurel` に、`Bob`、`Sam`、および `Peter` のパスワードを管理する権限を付与します。

```
GRANT CHANGE PASSWORD (Bob, Sam, Peter) TO (Sally, Laurel)
```

- **例 2 –** データベース内の任意のユーザに CHANGE PASSWORD システム権限を付与する権限を `Mary` に付与します。ただし、システム権限は WITH ADMIN ONLY OPTION 句付きで付与されるので、`Mary` は、別のユーザのパスワードを管理できません。

```
GRANT CHANGE PASSWORD (ANY) TO Mary WITH ADMIN ONLY OPTION
```

- **例 3 –** `Steve` と `Joe` に、`Role1` または `Role2` のメンバーのパスワードを管理する権限を付与します。

```
GRANT CHANGE PASSWORD (ANY WITH ROLES Role1, Role2) TO Steve, Joe
```

使用法

（先頭に戻る） (289 ページ)

データベース内の任意のユーザ (ANY) または特定のユーザのみ (*target_users_list*) または特定のロールのメンバー (ANY WITH ROLES *target_roles_list*) のパスワードを管理する機能をユーザに付与できます。CHANGE PASSWORD システム権限に対する管理権限は、ANY 句を使用する場合のみ付与できます。

句を指定しない場合、ANY がデフォルトで使用されます。GRANT 文で管理句の指定がない場合、WITH NO ADMIN OPTION 句が使用されます。

デフォルトでは、CHANGE PASSWORD システム権限は、SYS_AUTH_SA_ROLE 互換ロールには WITH NO ADMIN OPTION 句付きで、SYS_AUTH_SSO_ROLE 互換ロールには ADMIN ONLY OPTION 句付きで付与されます (互換ロールが存在する場合)。

標準

（先頭に戻る） (289 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (289 ページ)

- CHANGE PASSWORD システム権限が管理権限付きで付与されている必要があります。
- 指定される各ターゲットユーザ (target_users_list) は、ログインパスワードが設定されている既存のユーザまたはユーザ拡張ロールです。
- 指定された各ターゲットロール (target_roles_list) は、既存のユーザ拡張ロールまたはユーザ定義ロールである必要があります。

GRANT CONNECT 文

ユーザに CONNECT 権限を付与します。

クイックリンク：

「パラメータ」 (291 ページ)

「例」 (291 ページ)

「使用法」 (292 ページ)

「標準」 (293 ページ)

「パーミッション」 (293 ページ)

構文

```
GRANT  CONNECT
    TO  userID [,...]
    IDENTIFIED  BY  password [,...]
```

パラメータ

（先頭に戻る） (291 ページ)

- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

例

（先頭に戻る） (291 ページ)

- **例 1 –** データベースに Laurel と Hardy という名前の 2 人の新規ユーザを作成します。

```
GRANT CONNECT TO Laurel, Hardy
IDENTIFIED BY Stan, Ollie
```

- **例 2 –** ユーザ Jane をパスワードなしで作成します。

```
GRANT CONNECT TO Jane
```

- **例 3 –** Bob のパスワードを newpassword に変更します。

```
GRANT CONNECT TO Bob IDENTIFIED BY newpassword
```

使用法

（先頭に戻る） (291 ページ)

GRANT CONNECT は新規ユーザの作成に使用できます。また、すべてのユーザが自分のパスワードの変更にも使用できます。

ヒント： ユーザを作成するには、**GRANT CONNECT** 文ではなく、**CREATE USER** 文を使用してください。

新しいユーザを追加するときに既存のユーザのユーザ ID を誤って入力すると、その既存ユーザのパスワードを変更することになります。これは正常な動作とみなされるため、警告は発生しません。

sp_addlogin と **sp_adduser** のストアドプロシージャもユーザの追加に使用できます。これらのプロシージャでは、既存のユーザ ID を追加しようとするとエラーが表示されます。

注意： ユーザ ID の追加と削除を行うには、**GRANT** 文や **REVOKE** 文ではなくシステムプロシージャを使用してください。

パスワードのないユーザは、データベースに接続できません。これは、ロールユーザ ID への接続をすべて拒否する場合のグループ作成に便利です。パスワードなしでユーザを作成するには、IDENTIFIED BY 句を含めません。

パスワードを指定する際には、有効な識別子である必要があります。パスワードの最大文字長は 255 バイトです。データベースオプション **VERIFY_PASSWORD_FUNCTION** に空の文字列以外が設定されている場合、**GRANT CONNECT TO** 文はそのオプションの値で識別される関数を呼び出します。その関数が NULL を返す場合は、パスワードがルールに従っていることを示します。VERIFY_PASSWORD_FUNCTION オプションが設定されている場合、**GRANT CONNECT** 文には *userid* と *password* をそれぞれ 1 つだけ指定できます。

データベースユーザ ID 名およびパスワードとして無効なものは次のとおりです。

- 空白文字または一重引用符や二重引用符で始まる
- 最後の文字をスペースにする
- セミコロンを含める

標準

（先頭に戻る） (291 ページ)

- SQL – その他の構文は、ISO/ANSI SQL 文法のベンダ拡張です。
- SAP Sybase Database 製品 - セキュリティモデルは Adaptive Server と SAP Sybase IQ では異なるため、他の構文も異なります。

パーミッション

（先頭に戻る） (291 ページ)

- 新しいユーザを作成する場合は、MANAGE ANY USER システム権限が必要です。
- すべてのユーザが自分のパスワードを変更できます。
- 別のユーザのパスワードを変更する場合は、CHANGE PASSWORD システム権限が必要です。

注意： 別のユーザのパスワードを変更する場合は、そのユーザがデータベースに接続していないことが必要です。

参照：

- CREATE USER 文 (282 ページ)

GRANT CREATE 文

指定の DB 領域に対する CREATE 権限を指定のユーザおよびロールに付与します。

クイックリンク：

「パラメータ」 (294 ページ)

「例」 (294 ページ)

「標準」 (294 ページ)

「パーミッション」 (294 ページ)

構文

```
GRANT CREATE
   ON dbspace_name
   TO userID [,...]
```

パラメータ

（先頭に戻る） (293 ページ)

- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

例

（先頭に戻る） (293 ページ)

- **例 1 –** ユーザ `Lawrence` と `Swift` に DB 領域 *DspHist* に対する `CREATE` 権限を付与します。

```
GRANT CREATE ON DspHist
TO LAWRENCE, SWIFT
```

- **例 2 –** ユーザ `Fiona` と `Ciaran` に DB 領域 `DspHist` に対する `CREATE` 権限を付与します。

```
GRANT CREATE ON DspHist TO Fiona, Ciaran
```

標準

（先頭に戻る） (293 ページ)

- SQL – その他の構文は、ISO/ANSI SQL 文法のベンダ拡張です。
- SAP Sybase Database 製品 - セキュリティモデルは Adaptive Server と SAP Sybase IQ では異なるため、他の構文も異なります。

パーミッション

（先頭に戻る） (293 ページ)

MANAGE ANY DBSPACE システム権限が必要です。

GRANT EXECUTE 文

プロシージャまたはユーザ定義関数に対する EXECUTE 権限を付与します。

クイックリンク：

「パラメータ」 (295 ページ)

「標準」 (295 ページ)

「パーミッション」 (295 ページ)

構文

```
GRANT EXECUTE
  ON [ owner.] {procedure-name | user-defined-function-name }
  TO userID [,...]
```

パラメータ

（先頭に戻る） (294 ページ)

- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

標準

（先頭に戻る） (294 ページ)

- SQL – 構文は永続的ストアドモジュール機能です。
- SAP Sybase Database 製品 - セキュリティモデルは Adaptive Server と SAP Sybase IQ では異なるため、他の構文も異なります。

パーミッション

（先頭に戻る） (294 ページ)

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限。
- そのプロシージャを所有している。

GRANT オブジェクトレベル権限文

個々のテーブルまたはビューに対するデータベースオブジェクトレベル権限をユーザまたはロールに付与します。

クイックリンク：

「パラメータ」 (296 ページ)

「使用法」 (297 ページ)

「標準」 (297 ページ)

「パーミッション」 (297 ページ)

構文

```
GRANT object-level-privilege [, …]
   ON [ owner.]object-name
   TO userID [,...]
   [ WITH GRANT OPTION ]
```

```
object-level-privilege
    ALL [ PRIVILEGES ]
    | ALTER
    | DELETE
    | INSERT
    | LOAD
    | REFERENCE [ ( column-name [, …] ) ]
    | SELECT [ ( column-name [, …] ) ]
    | TRUNCATE
    | UPDATE [ ( column-name, …) ] }
```

パラメータ

（先頭に戻る） (295 ページ)

- **userID –** 既存ユーザまたは不変ロールの名前になります。リストは、ログインパスワードを持つ既存ユーザで構成する必要があります。リスト内の userID はカンマで区切ります。
- **ALL –** すべての権限をユーザに付与します。
- **ALTER –** ユーザが **ALTER TABLE** 文を使用してテーブルを変更できます。この権限は、ビューには使用できません。
- **DELETE –** ユーザがテーブルまたはビューからローを削除できます。
- **INSERT –** ユーザが指定のテーブルまたはビューにローを挿入できます。
- **LOAD –** ユーザが指定のテーブルまたはビューにデータをロードできます。
- **REFERENCES –** ユーザが、指定したテーブルのインデックス、および、指定したテーブルを参照する外部キーを作成できます。カラム名を指定した場合は、ユーザは指定したカラムだけを参照できます。カラムの REFERENCES 権限は、ビューに対しては付与できません。テーブルに対してのみ付与できます。
- **SELECT –** ユーザがビューまたはテーブルの情報を参照できます。カラム名を指定すると、ユーザは指定したカラムだけを参照できます。カラムの SELECT パーミッションは、ビューに対しては付与できません。テーブルに対してのみ付与できます。.
- **TRUNCATE –** ユーザが指定のテーブルまたはビューをトランケートできます。
- **UPDATE –** ユーザがビューまたはテーブルのローを更新できます。カラム名を指定すると、ユーザは指定したカラムだけを更新できます。カラムの UPDATE 権限は、ビューに対しては付与できません。テーブルに対してのみ付与できま

す。テーブルを更新するには、ユーザはそのテーブルに対する SELECT 権限と UPDATE 権限の両方を保有している必要があります。

- **WITH GRANT OPTION** – 指定したユーザ ID に、同じ権限を他のユーザ ID に付与する権限も与えます。

使用法

（先頭に戻る） (295 ページ)

テーブル権限をリストすることも、ALL を指定して一度にすべての権限を付与することもできます。

標準

（先頭に戻る） (295 ページ)

- SQL - 構文は初級レベル機能です。
- SAP Sybase Database 製品 - 構文は Adaptive Server でサポートされています。

パーミッション

（先頭に戻る） (295 ページ)

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限。
- そのテーブルに対して WITH GRANT OPTION 句を指定してオブジェクト権限が付与されている。
- テーブルを所有している。

GRANT ROLE 文

ユーザまたは他のロールに、管理権限付きまたはなしでロールを付与します。

クイックリンク：

「パラメータ」 (299 ページ)

「例」 (299 ページ)

「使用法」 (300 ページ)

「標準」 (301 ページ)

「パーミッション」 (301 ページ)

構文

```
GRANT ROLE role_name [, …]
    TO grantee [, …]
```

```
    [ {WITH NO ADMIN | WITH ADMIN [ ONLY ] } OPTION ]
    [ WITH NO SYSTEM PRIVILEGE INHERITANCE ]

role_name
    dbo†††
    | diagnostics†††
    | PUBLIC†††
    | rs_systabgroup†††
    | SA_DEBUG†††
    | SYS†††
    | SYS_AUTH_SA_ROLE
    | SYS_AUTH_SSO_ROLE
    | SYS_AUTH_DBA_ROLE††
    | SYS_AUTH_RESOURCE_ROLE†
    | SYS_AUTH_BACKUP_ROLE†
    | SYS_AUTH_VALIDATE_ROLE†
    | SYS_AUTH_WRITEFILE_ROLE
    | SYS_AUTH_WRITEFILECLIENT_ROLE
    | SYS_AUTH_READFILE_ROLE
    | SYS_AUTH_READFILECLIENT_ROLE
    | SYS_AUTH_PROFILE_ROLE
    | SYS_AUTH_USER_ADMIN_ROLE
    | SYS_AUTH_SPACE_ADMIN_ROLE
    | SYS_AUTH_MULTIPLEX_ADMIN_ROLE
    | SYS_AUTH_OPERATOR_ROLE
    | SYS_AUTH_PERMS_ADMIN_ROLE
    | SYS_REPLICATE_ADMIN_ROLE†††
    | SYS_RUN_REPLICATE_ROLE†††
    | SYS_SPATIAL_ADMIN_ROLE†††
    | user-defined role name
```

- 選択互換ロールを他のロールに付与する際は WITH NO SYSTEM PRIVILEGE INHERITANCE 句を使用できます。この句は、ロールのメンバーによる互換ロールの基礎となるシステム権限の自動継承を禁止します。ユーザ拡張ロールに付与した場合は、WITH NO SYSTEM PRIVILEGE INHERITANCE 句はそのロールのメンバーにのみ適用されます。ロールとして機能するユーザは、この句に関係なく、基礎となるシステム権限を自動的に継承します。
- WITH NO ADMIN OPTION WITH NO SYSTEM PRIVILEGE INHERITANCE 句と WITH NO SYSTEM PRIVILEGE INHERITANCE 句はセマンティック上同じです。
- †SYS_AUTH_BACKUP_ROLE ロール、SYS_AUTH_RESOURCE_ROLE ロール、または SYS_AUTH_VALIDATE_ROLE ロールを付与する際に、WITH NO SYSTEM PRIVILEGE INHERITANCE 句と組み合わせて WITH ADMIN OPTION 句または WITH ADMIN ONLY 句を指定することはできません。
- ††SYS_AUTH_DBA_ROLE ロールまたは SYS_RUN_REPLICATION_ROLE ロールを付与する際に、WITH ADMIN OPTION 句は、WITH NO SYSTEM PRIVILEGE INHERITANCE 句と組み合わせてのみ指定できます。
- †††WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句はシステムロールではサポートされません。

パラメータ

（先頭に戻る） (297 ページ)

- **role_name –** データベースにすでに存在している必要があります。複数のロール名を指定するときはカンマで区切ります。
- **grantee –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。
- **WITH NO ADMIN OPTION –** 各 *grantee* は、各 *role_name* の基礎となるシステム権限を付与されますが、*role_name* を別のユーザに付与することはできません。
- **WITH ADMIN ONLY OPTION –** 各 *userID* に各 *role_name* に対する管理権限は付与されますが、*role_name* の基礎となるシステム権限は付与されません。
- **WITH ADMIN OPTION –** 各 userID は、各 *role_name* の基礎となるシステム権限を付与され、加えて、*role_name* を別のユーザに付与する権限も付与されます。
- **WITH NO SYSTEM PRIVILEGE INHERITANCE –** 付与元ロールの基礎となるシステム権限は、付与先ロールのメンバーに継承されません。ただし、付与先ロールがユーザ拡張ロールである場合、その拡張ユーザには基礎となるシステム権限が付与されます。

例

（先頭に戻る） (297 ページ)

- **例 1 –** `Sales_Role` を `Sally` に管理権限付きで付与します。つまり、このユーザはこのロールにより付与される承認済みタスクを実行できるほか、他のユーザーに `Sales_Role` を付与したり、このロールを取り消したりできます。

```
GRANT ROLE Sales_Role TO Sally WITH ADMIN OPTION
```

- **例 2 –** 互換ロール SYS_AUTH_PROFILE_ROLE をロール `Sales_Admin` に管理権限なしで付与します。`Sales_Admin` はスタンドアロンロールであり、`Mary` と `Peter` にはすでに `Sales_Admin` が付与されています。SYS_AUTH_PROFILE_ROLE は継承可能な互換ロールなので、`Mary` と `Peter` には `Sales_Role` の基礎となるシステム権限が付与されています。このロールには管理権限が付いていないので、ロールの付与と取り消しはできません。

```
GRANT ROLE SYS_AUTH_PROFILE_ROLE TO Sales_Role WITH NO ADMIN
OPTION
```

- **例 3 –** 互換ロール SYS_AUTH_BACKUP_ROLE を管理権限なしで `Tom` に付与します。`Tom` は、`Betty` と Laurel に付与されているユーザ拡張ロールです。

SYS_AUTH_BACKUP_ROLE は継承不可の互換ロールなので、このロールの基礎となるシステム権限は Betty と Laurel に付与されません。ただし、Tom は拡張ユーザなので、Tom には基礎となるシステム権限が直接付与されます。

```
GRANT ROLE SYS_AUTH_BACKUP_ROLE TO Tom
WITH NO SYSTEM PRIVILEGE INHERITANCE
```

使用法

（先頭に戻る） (297 ページ)

WITH ADMIN OPTION 句または WITH ADMIN ONLY OPTION 句を使用することによって、被付与者にロールの付与または取り消しは許可されますが、ロールの削除は許可されません。

GRANT 文で管理句の指定がない場合、デフォルトでは、各互換ロールは次のデフォルト管理権限付きで付与されます。

WITH ADMIN OPTION	WITH ADMIN ONLY OPTION	WITH NO ADMIN OPTION
SYS_AUTH_SA_ROLE SYS_AUTH_SSO_ROLE	SYS_AUTH_DBA_ROLE	SYS_AUTH_RESOURCE_ROLE SYS_AUTH_BACKUP_ROLE SYS_AUTH_VALIDATE_ROLE SYS_AUTH_WRITEFILE_ROLE SYS_AUTH_WRITEFILECLIENT_ROLE SYS_AUTH_READFILE_ROLE SYS_AUTH_READFILECLIENT_ROLE SYS_AUTH_PROFILE_ROLE SYS_AUTH_USER_ADMIN_ROLE SYS_AUTH_SPACE_ADMIN_ROLE SYS_AUTH_MULTIPLEX_ADMIN_ROLE SYS_AUTH_OPERATOR_ROLE SA_DEBUG SYS_RUN_REPLICATION_ROLE

SYS_AUTH_PERMS_ADMIN_ROLE ロールは、次のデフォルト管理権限付きで次の基礎となるロールを付与します。

WITH ADMIN OPTION	WITH NO ADMIN OPTION
SYS_AUTH_BACKUP_ROLE	MANAGE ROLES
SYS_AUTH_OPERATOR_ROLE	MANAGE ANY OBJECT PRIVILEGE
SYS_AUTH_USER_ADMIN_ROLE	CHANGE PASSWORD
SYS_AUTH_SPACE_ADMIN_ROLE	
SYS_AUTH_MULTIPLEX_ADMIN_ROLE	
SYS_AUTH_RESOURCE_ROLE	
SYS_AUTH_VALIDATE_ROLE	
SYS_AUTH_PROFILE_ROLE	
SYS_AUTH_WRITEFILE_ROLE	
SYS_AUTH_WRITEFILECLIENT_ROLE	
SYS_AUTH_READFILE_ROLE	
SYS_AUTH_READFILECLIENT_ROLE	

標準

（先頭に戻る） (297 ページ)

- SQL – その他の構文は、ISO/ANSI SQL 文法のベンダ拡張です。
- SAP Sybase Database 製品 - 構文は Adaptive Server でサポートされています。

パーミッション

（先頭に戻る） (297 ページ)

- 以下のシステムロールを付与するには、MANAGE ROLES システム権限が必要です。
  - dbo
  - diagnostics
  - PUBLIC
  - rs_systabgroup
  - SA_DEBUG SYS
  - SYS
  - SYS_REPLICATION_ADMIN_ROLE
  - SYS_RUN_REPLICATION_ROLE
  - SYS_SPATIAL_ADMIN_ROLE
- 以下のロールを付与するには、そのロールに対する管理権限が必要です。
  - SYS_AUTH_SA_ROLE

- SYS_AUTH_SSO_ROLE
- SYS_AUTH_DBA_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_AUTH_VALIDATE_ROLE
- SYS_AUTH_WRITEFILE_ROLE
- SYS_AUTH_WRITEFILECLIENT_ROLE
- SYS_AUTH_READFILE_ROLE
- SYS_AUTH_READFILECLIENT_ROLE
- SYS_AUTH_PROFILE_ROLE
- SYS_AUTH_USER_ADMIN_ROLE
- SYS_AUTH_SPACE_ADMIN_ROLE
- SYS_AUTH_MULTIPLEX_ADMIN_ROLE
- SYS_AUTH_OPERATOR_ROLE
- SYS_AUTH_PERMS_ADMIN_ROLE
- <ユーザ定義ロール名>

GRANT SET USER 文

別のユーザに同一化できる権限と、SET USER システム権限を管理する権限を付与します。

クイックリンク：

「パラメータ」 (302 ページ)

「例」 (303 ページ)

「使用法」 (304 ページ)

「標準」 (304 ページ)

「パーミッション」 (304 ページ)

構文

```
GRANT SET USER ( target_users_list
       | ANY
       | ANY WITH ROLES target_roles_list )
  TO userID [,...]
  [ WITH ADMIN [ ONLY ] OPTION | WITH NO ADMIN OPTION ]
```

パラメータ

（先頭に戻る） (302 ページ)

- **target_users_list –** ログインパスワードを持つ既存のユーザで構成される必要があり、被付与者ユーザによる同一化の対象ではなくなった可能性のあるター

ゲットユーザの潜在的リストです。リスト内のユーザ ID はカンマで区切ります。

- **ANY –** 各被付与者のターゲットユーザの潜在的リストは、ログインパスワードを持つすべてのデータベースユーザで構成されます。
- **ANY WITH ROLES *target_roles_list* –** *target_role_list* は既存のロールで構成される必要があります。各被付与者のターゲットユーザの潜在的リストは、*target_role_list* 内のロールのサブセットが付与されているログインパスワードを持つデータベースユーザで構成される必要があります。リスト内のロールはカンマで区切ります。
- **userID –** 各 *userID* は、既存のユーザまたは不変ロールの名前になります。リストは、ログインパスワードを持つ既存ユーザで構成される必要があります。リスト内の userID はカンマで区切ります。
- **WITH ADMIN OPTION –** (ANY 句を指定する場合のみ有効) ユーザは SETUSER コマンドを発行して別のユーザに同一化することも、SET USER システム権限を別のユーザに付与することもできます。
- **WITH ADMIN ONLY OPTION –** (ANY 句を指定する場合のみ有効) ユーザは SETUSER システム権限を別のユーザに付与することはできますが、SETUSER コマンドを発行して別のユーザに同一化することはできません。
- **WITH NO ADMIN OPTION –** ユーザは SETUSER コマンドを発行して別のユーザに同一化することはできますが、SET USER システム権限を別のユーザに付与することはできません。

例

（先頭に戻る） (302 ページ)

- **例 1 –** `Bob`、`Sam`、および `Peter` に同一化できる権限を `Sally` と `Laurel` に付与します。

```
GRANT SET USER (Bob, Sam, Peter) TO (Sally, Laurel)
```

- **例 2 –** データベース内の任意のユーザに SET USER システム権限を付与する権限を `Mary` に付与します。ただし、このシステム権限は WITH ADMIN ONLY OPTION 句付きで付与されるので、`Mary` は、他のユーザに同一化することはできません。

```
GRANT SET USER (ANY) TO Mary WITH ADMIN ONLY OPTION
```

- **例 3 –** `Role1` または `Role2` に同一化できる権限を `Steve` と `Joe` に付与します。

```
GRANT SET USER (ANY WITH ROLES Role1, Role2) TO Steve, Joe
```

使用法

（先頭に戻る） (302 ページ)

データベース内の任意のユーザ (ANY) または特定のユーザのみ (*target_users_list*) または特定のロールのメンバー (ANY WITH ROLES *target_roles_list*) に同一化する権限を、ユーザに付与できます。SET USER システム権限に対する管理権限は、ANY 句を使用する場合のみ付与できます。

句を指定しない場合、ANY がデフォルトで使用されます。GRANT 文で管理句の指定がない場合、WITH NO ADMIN OPTION 句が使用されます。

SET USER システム権限をユーザに再付与する場合、付与の効果は累積されます。

デフォルトでは、SET USER システム権限は SYS_AUTH_SSO_ROLE 互換ロールに (存在していれば) WITH NO ADMIN OPTION 句付きで付与されます。

SET USER システム権限の付与のみが、別のユーザへの同一化権限を付与します。別のユーザへの同一化に必要とされる*最低*条件の検証は、**SETUSER** 文が発行されるまで発生しません。

標準

（先頭に戻る） (302 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (302 ページ)

- SET USER システム権限が管理権限付きで付与されている必要があります。
- 指定される各ターゲットユーザ (target_users_list) は、ログインパスワードが設定されている既存のユーザまたはユーザ拡張ロールです。
- 指定された各ターゲットロール (target_roles_list) は、既存のユーザ拡張ロールまたはユーザ定義ロールである必要があります。

GRANT システム権限文

特定のシステム権限を管理権限付きまたはなしでユーザまたはロールに付与します。

クイックリンク：

「パラメータ」 (305 ページ)

「例」 (305 ページ)

「使用法」 (305 ページ)

「標準」 (306 ページ)

「パーミッション」 (306 ページ)

構文

```
GRANT system_privilege_name [, …]
   TO userID [, …]
   [ { WITH NO ADMIN | WITH ADMIN [ ONLY ] } OPTION ]
```

パラメータ

（先頭に戻る） (304 ページ)

- **system_privilege_name –** 既存のシステム権限の名前になります。
- **userID –** 既存ユーザまたは不変ロールの名前になります。リストは、ログインパスワードを持つ既存ユーザで構成する必要があります。複数の userID はカンマで区切ります。
- **WITH NO ADMIN OPTION –** ユーザはシステム権限を管理できますが、別のユーザにシステム権限を付与することはできません。
- **WITH ADMIN ONLY OPTION –** WITH ADMIN ONLY OPTION 句が使用される場合、各 *userID* には、*system_privilege* そのものではなく各 *system_privilege* に対する管理権限が付与されます。
- **WITH ADMIN OPTION –** *userID* のそれぞれに、*system_privilege* の基礎となるシステム権限に加え、それぞれの *system_privilege* に対する管理権限も付与されます。

例

（先頭に戻る） (304 ページ)

- **例 1 –** `Joe` に DROP CONNECTION システム権限を管理権限付きで付与します。

```
GRANT DROP CONNECTION TO Joe WITH ADMIN OPTION
```

- **例 2 –** `Sally` に CHECKPOINT システム権限を管理権限なしで付与します。

```
GRANT CHECKPOINT TO Sally WITH NO ADMIN OPTION
```

- **例 3 –** `Jane` に MONITOR システム権限を管理権限のみで付与します。

```
GRANT MONITOR TO Jane WITH ADMIN ONLY OPTION
```

使用法

（先頭に戻る） (304 ページ)

GRANT 文で管理句の指定がない場合、デフォルトでは WITH NO ADMIN OPTION 句が使用されます。

標準

（先頭に戻る） (304 ページ)

- SQL – その他の構文は、ISO/ANSI SQL 文法のベンダ拡張です。
- SAP Sybase Database 製品 - 構文は Adaptive Server でサポートされています。

パーミッション

（先頭に戻る） (304 ページ)

付与するシステム権限に対する管理権限が必要です。

すべてのシステム権限のリスト

すべてのシステム権限のリスト。

システム権限は、ユーザが承認済みのデータベースタスクを実行する権限を制御します。

次に、使用可能なシステム権限のリストを示します。

- ACCESS SERVER LS
- ALTER ANY INDEX
- ALTER ANY MATERIALIZED VIEW
- ALTER ANY OBJECT
- ALTER ANY OBJECT OWNER
- ALTER ANY PROCEDURE
- ALTER ANY SEQUENCE
- ALTER ANY TABLE
- ALTER ANY TEXT CONFIGURATION
- ALTER ANY TRIGGER
- ALTER ANY VIEW
- ALTER DATABASE
- ALTER DATATYPE
- BACKUP DATABASE
- CHANGE PASSWORD
- CHECKPOINT
- COMMENT ANY OBJECT
- CREATE ANY INDEX
- CREATE ANY MATERIALIZED VIEW
- CREATE ANY OBJECT

- CREATE ANY PROCEDURE
- CREATE ANY SEQUENCE
- CREATE ANY TABLE
- CREATE ANY TEXT CONFIGURATION
- CREATE ANY TRIGGER
- CREATE ANY VIEW
- CREATE DATATYPE
- CREATE EXTERNAL REFERENCE
- CREATE MATERIALIZED VIEW
- CREATE MESSAGE
- CREATE PROCEDURE
- CREATE PROXY TABLE
- CREATE TABLE
- CREATE TEXT CONFIGURATION
- CREATE VIEW
- DEBUG ANY PROCEDURE
- DELETE ANY TABLE
- DROP ANY INDEX
- DROP ANY MATERIALIZED VIEW
- DROP ANY OBJECT
- DROP ANY PROCEDURE
- DROP ANY SEQUENCE
- DROP ANY TABLE
- DROP ANY TEXT CONFIGURATION
- DROP ANY VIEW
- DROP CONNECTION
- DROP DATATYPE
- DROP MESSAGE
- EXECUTE ANY PROCEDURE
- LOAD ANY TABLE
- INSERT ANY TABLE
- MANAGE ANY DBSPACE
- MANAGE ANY EVENT
- MANAGE ANY EXTERNAL ENVIRONMENT
- MANAGE ANY EXTERNAL OBJECT
- MANAGE ANY LDAP SERVER
- MANAGE ANY LOGIN POLICY
- MANAGE ANY MIRROR SERVER
- MANAGE ANY OBJECT PRIVILEGES

- MANAGE ANY SPATIAL OBJECT
- MANAGE ANY STATISTICS
- MANAGE ANY USER
- MANAGE ANY WEB SERVICE
- MANAGE AUDITING
- MANAGE MULTIPLEX
- MANAGE PROFILING
- MANAGE REPLICATION
- MANAGE ROLES
- MONITOR
- READ CLIENT FILE
- READ FILE
- REORGANIZE ANY OBJECT
- SELECT ANY TABLE
- SERVER OPERATOR
- SET ANY PUBLIC OPTION
- SET ANY SECURITY OPTION
- SET ANY SYSTEM OPTION
- SET ANY USER DEFINED OPTION
- SET USER (管理権限のみで付与)
- TRUNCATE ANY TABLE
- UPDATE ANY TABLE
- UPGRADE ROLE
- USE ANY SEQUENCE
- VALIDATE ANY OBJECT
- WRITE CLIENT FILE
- WRITE FILE

GRANT USAGE ON SEQUENCE 文

指定されたシーケンスに対する USAGE システム権限をユーザまたはロールに付与します。

クイックリンク：

「パラメータ」 (309 ページ)

「標準」 (309 ページ)

「パーミッション」 (309 ページ)

構文

```
GRANT USAGE ON SEQUENCE sequence-name
   TO userID [,...]
```

パラメータ

（先頭に戻る） (308 ページ)

- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

標準

（先頭に戻る） (308 ページ)

- SQL – 構文は永続的ストアドモジュール機能です。
- SAP Sybase Database 製品 - セキュリティモデルは Adaptive Server と SAP Sybase IQ では異なるため、他の構文も異なります。

パーミッション

（先頭に戻る） (308 ページ)

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限。
- そのシーケンスを所有している。

REVOKE CHANGE PASSWORD 文

パスワードおよびシステム権限を管理する権限をユーザから削除します。

クイックリンク：

「パラメータ」 (310 ページ)

「例」 (310 ページ)

「使用法」 (310 ページ)

「標準」 (311 ページ)

「パーミッション」 (311 ページ)

構文

```
REVOKE [ ADMIN OPTION FOR ] CHANGE PASSWORD
   [(target_user_list
      | ANY
      | ANY WITH ROLES target_role_list )]
   FROM userID [,...]
```

パラメータ

（先頭に戻る） (309 ページ)

- **target_user_list –** 被付与者が同一化の対象とする可能性のあるユーザ。このリストは、ログインパスワードを持つ既存のユーザまたはユーザ拡張ロールで構成される必要があります。リスト内の userID はカンマで区切ります。
- **ANY –** ログインパスワードを持つすべてのデータベースユーザが、各被付与者のパスワードを管理する潜在的ターゲットユーザになります。
- **ANY WITH ROLES *target_role_list* –** 各被付与者のターゲットロールのリスト。いずれかのターゲットロールを付与されたユーザは、各被付与者の潜在的ターゲットユーザになります。*target_role_list* は既存のロールで構成される必要があり、前述のロールを付与されたユーザはログインパスワードを持つデータベースユーザで構成される必要があります。複数の userID を指定する場合は、カンマで区切ります。
- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

例

（先頭に戻る） (309 ページ)

- **例 1 –** `Joe` が `Sally` または `Bob` のパスワードを管理できる権限を削除します。

```
REVOKE CHANGE PASSWORD (Sally, Bob) FROM Joe
```

- **例 2 –** CHANGE PASSWORD システム権限が WITH ADMIN OPTION 句付きで `Sam` に付与されていた場合、この例では、`Sam` から、別のユーザに CHANGE PASSWORD システム権限を付与できる権限は削除されますが、元の **GRANT CHANGE PASSWORD** 文で指定されているユーザのパスワードの管理権限は `Sam` に残ります。ただし、CHANGE PASSWORD システム権限が WITH ADMIN ONLY OPTION 句付きで `Sam` に付与されていた場合、この例では、`Sam` からシステム権限のすべてのパーミッションが削除されます。

```
REVOKE ADMIN OPTION FOR CHANGE PASSWORD FROM Sam
```

使用法

（先頭に戻る） (309 ページ)

CHANGE PASSWORD システム権限が最初にどのように付与されているかによって、ADMIN OPTION FOR 句付きで CHANGE PASSWORD システム権限を取り消した場合、異なる結果になります。CHANGE PASSWORD システム権限が WITH ADMIN OPTION 句付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めると、CHANGE PASSWORD システム権限を管理する権限 (つま

り、システム権限を別のユーザに付与できる権限) のみが取り消されます。他のユーザのパスワードを実際に管理する権限は残ります。ただし、CHANGE PASSWORD システム権限が WITH ADMIN ONLY OPTION 付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めることは、CHANGE PASSWORD システム権限全体を取り消すこととセマンティック上同じになります。最後に、CHANGE PASSWORD システム権限が WITH NO ADMIN OPTION 句付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めても、元々管理権限が付与されていないので、何も取り消されません。

付与されているユーザとロールの任意の組み合わせから CHANGE PASSWORD システム権限を取り消すことができます。

標準

（先頭に戻る） (309 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (309 ページ)

CHANGE PASSWORD システム権限が管理権限付きで付与されている必要があります。

REVOKE CONNECT 文

ユーザをデータベースから削除します。

クイックリンク：

「パラメータ」 (311 ページ)

「使用法」 (312 ページ)

「標準」 (312 ページ)

「パーミッション」 (312 ページ)

構文

```
REVOKE CONNECT
    FROM userID [,...]
```

パラメータ

（先頭に戻る） (311 ページ)

- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

使用法

（先頭に戻る） (311 ページ)

ユーザ ID を追加および削除するには、**GRANT** 文または **REVOKE** 文ではなく、システムプロシージャまたは CREATE USER 文および DROP USER 文を使用します。

ユーザがテーブルなどのデータベースオブジェクトを所有している場合、そのユーザの接続権限を取り消すことはできません。**REVOKE** 文、または **sp_droplogin** ストアドプロシージャあるいは **sp_iqdroplogin** ストアドプロシージャでこれを行おうとすると、「ランタイムシステムでは、テーブルを所有しているユーザを削除することはできません。」のようなエラーが返されます。

標準

（先頭に戻る） (311 ページ)

ANSI SQL – 準拠レベル: Transact-SQL 拡張。

パーミッション

（先頭に戻る） (311 ページ)

MANAGE ANY USER システム権限が必要です。

注意： 別のユーザの **CONNECT** パーミッションまたはテーブルパーミッションを取り消すと、そのユーザはそのデータベースに接続できなくなります。

REVOKE CREATE 文

指定されたユーザ ID から、指定された DB 領域に対する CREATE 権限を削除します。

クイックリンク：

「パラメータ」 (313 ページ)

「例」 (313 ページ)

「標準」 (313 ページ)

「パーミッション」 (313 ページ)

構文

```
REVOKE  CREATE ON dbspace-name
    FROM userID [,...]
```

パラメータ

（先頭に戻る） (312 ページ)

- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

例

（先頭に戻る） (312 ページ)

- **例 1 –** ユーザ `Smith` から DB 領域 `DspHist` に対する CREATE 権限を取り消します。

```
REVOKE CREATE ON DspHist FROM Smith
```

- **例 2 –** データベースからユーザ ID `fionat` の DB 領域 `DspHist` に対する CREATE 権限を取り消します。

```
REVOKE CREATE ON DspHist FROM fionat
```

標準

（先頭に戻る） (312 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (312 ページ)

MANAGE ANY DBSPACE システム権限が必要です。

REVOKE EXECUTE 文

GRANT 文を使用して付与された EXECUTE パーミッションを削除します。

クイックリンク：

「パラメータ」 (314 ページ)

「標準」 (314 ページ)

「パーミッション」 (314 ページ)

構文

```
REVOKE  EXECUTE ON [ owner.]procedure-name
    FROM userID [,...]
```

パラメータ

（先頭に戻る） (313 ページ)

- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

標準

（先頭に戻る） (313 ページ)

- SQL – 構文は永続的ストアドモジュール機能です。
- SAP Sybase Database 製品 - 構文は Adaptive Server でサポートされています。ユーザ管理とセキュリティモデルは、Adaptive Server と SAP Sybase IQ では異なります。

パーミッション

（先頭に戻る） (313 ページ)

次のいずれかが必要です。

- プロシージャを所有している
- MANAGE ANY OBJECT PRIVILEGE システム権限が付与されている

REVOKE オブジェクトレベル権限文

GRANT 文を使用して付与されたオブジェクトレベル権限を削除します。

クイックリンク：

「パラメータ」 (315 ページ)

「例」 (315 ページ)

「標準」 (316 ページ)

「パーミッション」 (316 ページ)

構文

```
REVOKE { object-level-privilege [,...]
    [ owner.]table-name
   FROM userID [,...]

object-level-privilege
    ALL [ PRIVILEGES ]
    | ALTER
    | DELETE
    | INSERT
    | LOAD
```

```
   | REFERENCE [ ( column-name [, …] ) ]
   | SELECT [ ( column-name [, …] ) ]
   | TRUNCATE
   | UPDATE [ ( column-name, …) ] }
```

パラメータ

（先頭に戻る） (314 ページ)

- **userID –** 既存ユーザまたは不変ロールの名前になります。リストは、ログインパスワードを持つ既存ユーザで構成される必要があります。リスト内の userID はカンマで区切ります。
- **ALL –** すべての権限をユーザに付与します。
- **ALTER –** ユーザが **ALTER TABLE** 文を使用してテーブルを変更できます。この権限は、ビューには使用できません。
- **DELETE –** ユーザがテーブルまたはビューからローを削除できます。
- **INSERT –** ユーザが指定のテーブルまたはビューにローを挿入できます。
- **LOAD –** ユーザが指定のテーブルまたはビューにデータをロードできます。
- **REFERENCES –** ユーザが、指定したテーブルのインデックス、および、指定したテーブルを参照する外部キーを作成できます。カラム名を指定した場合は、ユーザは指定したカラムだけを参照できます。カラムの REFERENCES 権限は、ビューに対しては付与できません。テーブルに対してのみ付与できます。
- **SELECT –** ユーザがビューまたはテーブルの情報を参照できます。カラム名を指定すると、ユーザは指定したカラムだけを参照できます。カラムの SELECT パーミッションは、ビューに対しては付与できません。テーブルに対してのみ付与できます。.
- **TRUNCATE –** ユーザが指定のテーブルまたはビューをトランケートできます。
- **UPDATE –** ユーザがビューまたはテーブルのローを更新できます。カラム名を指定すると、ユーザは指定したカラムだけを更新できます。カラムの UPDATE 権限は、ビューに対しては付与できません。テーブルに対してのみ付与できます。テーブルを更新するには、ユーザはそのテーブルに対する SELECT 権限と UPDATE 権限の両方を保有している必要があります。

例

（先頭に戻る） (314 ページ)

- **例 1 –** ユーザ `Dave` が `Employees` テーブルに挿入できないようにします。

```
REVOKE INSERT ON Employees FROM Dave
```

- **例 2 –** ユーザ `Dave` が `Employees` テーブルを更新できないようにします。

```
REVOKE UPDATE ON Employees FROM Dave
```

標準

（先頭に戻る） (314 ページ)

- SQL - 構文は初級レベル機能です。
- SAP Sybase Database 製品 - 構文は Adaptive Server でサポートされています。

パーミッション

（先頭に戻る） (314 ページ)

次のいずれかが必要です。

- テーブルを所有している
- GRANT OPTION 句付きで MANAGE ANY OBJECT PRIVILEGE システム権限が付与されている

REVOKE ROLE 文

ロールのユーザメンバーシップ、またはロールを管理する権限を削除します。

クイックリンク：

「パラメータ」 (317 ページ)

「例」 (317 ページ)

「標準」 (318 ページ)

「パーミッション」 (318 ページ)

構文

```
REVOKE [ ADMIN OPTION FOR ] ROLE  role_name  [,...]
    FROM  grantee [,...]

role_name
    dbo†††
    | diagnostics†††
    | PUBLIC†††
    | rs_systabgroup†††
    | SA_DEBUG†††
    | SYS†††
    | SYS_AUTH_SA_ROLE
    | SYS_AUTH_SSO_ROLE
    | SYS_AUTH_DBA_ROLE
    | SYS_AUTH_RESOURCE_ROLE
```

```
    | SYS_AUTH_BACKUP_ROLE
    | SYS_AUTH_VALIDATE_ROLE
    | SYS_AUTH_WRITEFILE_ROLE
    | SYS_AUTH_WRITEFILECLIENT_ROLE
    | SYS_AUTH_READFILE_ROLE
    | SYS_AUTH_READFILECLIENT_ROLE
    | SYS_AUTH_PROFILE_ROLE
    | SYS_AUTH_USER_ADMIN_ROLE
    | SYS_AUTH_SPACE_ADMIN_ROLE
    | SYS_AUTH_MULTIPLEX_ADMIN_ROLE
    | SYS_AUTH_OPERATOR_ROLE
    | SYS_AUTH_PERMS_ADMIN_ROLE
    | SYS_REPLICATE_ADMIN_ROLE†††
    | SYS_RUN_REPLICATE_ROLE†††
    | SYS_SPATIAL_ADMIN_ROLE†††
    | user-defined role name
```

†††ADMIN OPTION FOR 句はシステムロールに対してはサポートされていません。

パラメータ

（先頭に戻る） (316 ページ)

- **role_name –** データベースにすでに存在している必要があります。複数のロール名を指定するときはカンマで区切ります。
- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。
- **ADMIN OPTION FOR –** 各 *userID* に、指定の *role_name* に対する管理権限が付与されている必要があります。

  注意： そのロールが元々 WITH ADMIN ONLY OPTION 句で付与されていない限り、この句では、ロールのメンバーシップではなく、ロールの管理権限のみを取り消します。WITH ADMIN ONLY OPTION 句付きで付与されているロールに対しては、ADMIN OPTION FOR 句は、ロール内のメンバーシップを全部取り消すこととセマンティック上同じなので、この句は省略可能です。

例

（先頭に戻る） (316 ページ)

- **例 1 –** ユーザ定義 (スタンドアロン) ロール `Role1` を `User1` から取り消します。

  ```
  REVOKE ROLE Role1 FROM User1
  ```

  このコマンドを実行した後、`User1` には、`Role1` に付与されているシステム権限を使用して承認済みタスクを実行する権限がなくなります。
- **例 2 –** `User1` から、互換ロール SYS_AUTH_WRITEFILE_ROLE を管理する権限を取り消します。

```
REVOKE ADMIN OPTION FOR ROLE SYS_AUTH_WRITEFILE_ROLE FROM User1
```

SYS_AUTH_WRITEFILE_ROLE によって付与されている認証済みタスクを実行する権限は User1 に残ります。

標準

（先頭に戻る） (316 ページ)

- SQL – その他の構文は、ISO/ANSI SQL 文法のベンダ拡張です。
- SAP Sybase Database 製品 - 構文は Adaptive Server でサポートされています。

パーミッション

（先頭に戻る） (316 ページ)

以下のロールを取り消すには MANAGE ROLES システム権限が必要です。

- diagnostics
- dbo
- PUBLIC
- rs_systabgroup
- SA_DEBUG
- SYS
- SYS_RUN_REPLICATE_ROLE
- SYS_SPATIAL_ADMIN_ROLE

以下のロールを取り消すには、そのロールに対する管理権限が必要です。

- SYS_AUTH_SA_ROLE
- SYS_AUTH_SSO_ROLE
- SYS_AUTH_DBA_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_AUTH_VALIDATE_ROLE
- SYS_AUTH_WRITEFILE_ROLE
- SYS_AUTH_WRITEFILECLIENT_ROLE
- SYS_AUTH_READFILE_ROLE
- SYS_AUTH_READFILECLIENT_ROLE
- SYS_AUTH_PROFILE_ROLE
- SYS_AUTH_USER_ADMIN_ROLE
- SYS_AUTH_SPACE_ADMIN_ROLE
- SYS_AUTH_MULTIPLEX_ADMIN_ROLE
- SYS_AUTH_OPERATOR_ROLE

- SYS_AUTH_PERMS_ADMIN_ROLE
- <ユーザ定義ロール名>

REVOKE SET USER 文

別のユーザに同一化できる権限と、SET USER システム権限を管理する権限を削除します。

クイックリンク：

「パラメータ」 (319 ページ)

「例」 (320 ページ)

「使用法」 (320 ページ)

「標準」 (320 ページ)

「パーミッション」 (320 ページ)

構文

```
REVOKE [ ADMIN OPTION FOR ] SETUSER
   (target_user_list
      | ANY
      | ANY WITH ROLES target_role_list ])
 FROM userID [,...]
```

パラメータ

（先頭に戻る） (319 ページ)

- **target_user_list –** ログインパスワードを持つ既存のユーザで構成される必要があり、被付与者ユーザによる同一化の対象ではなくなった可能性のあるターゲットユーザの潜在的リストです。リスト内のユーザ ID はカンマで区切ります。
- **ANY –** 各被付与者のターゲットユーザの潜在的リストは、ログインパスワードを持つすべてのデータベースユーザで構成されます。
- **ANY WITH ROLES *target_role_list* –** *target_role_list* は既存のロールで構成される必要があります。各被付与者のターゲットユーザの潜在的リストは、*target_role_list* 内のロールのサブセットが付与されているログインパスワードを持つデータベースユーザで構成される必要があります。リスト内のロールはカンマで区切ります。
- **userID –** 各 *userID* は、既存のユーザまたは不変ロールの名前になります。リストは、ログインパスワードを持つ既存ユーザで構成される必要があります。リスト内の userID はカンマで区切ります。

例

（先頭に戻る） (319 ページ)

- **例 1 –** Bob が Sally または Bob に同一化できないようにします。

```
REVOKE SET USER (Sally, Bob) FROM Bob
```

- **例 2 –** SET USER システム権限が WITH ADMIN OPTION 句付きで Sam に付与されていた場合、この例により、Sam から、別のユーザに SET USER システム権限を付与できる権限は削除されますが、指定されているユーザへの同一化権限は Sam に残ります。ただし、SET USER システム権限が WITH ADMIN ONLY OPTION 句付きで Sam に付与されていた場合、この例により、Sam からシステム権限のすべてのパーミッションが削除されます。

```
REVOKE ADMIN OPTION FOR SET USER FROM Sam
```

使用法

（先頭に戻る） (319 ページ)

SET USER システム権限が最初にどのように付与されているかによって、ADMIN OPTION FOR 句付きで SET USER システム権限を取り消した場合、異なる結果になります。SET USER システム権限が WITH ADMIN OPTION 句付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めると、SET USER システム権限を管理する権限 (つまり、システム権限を別のユーザに付与できる権限) のみが取り消されます。別のユーザーに実際に同一化する権限は残ります。ただし、SET USER システム権限が WITH ADMIN ONLY OPTION 付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めることは、SET USER システム権限全体を取り消すこととセマンティック上同じになります。最後に、SET USER システム権限が WITH NO ADMIN OPTION 句付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めても、元々管理システム権限が付与されていないので、何も取り消されません。

標準

（先頭に戻る） (319 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (319 ページ)

SET USER システム権限が管理権限付きで付与されている必要があります。

REVOKE システム権限文

特定のユーザから特定のシステム権限を削除し、権限を管理する権限も削除します。

クイックリンク：

「パラメータ」 (321 ページ)

「例」 (321 ページ)

「使用法」 (322 ページ)

「標準」 (322 ページ)

「パーミッション」 (322 ページ)

構文

```
REVOKE [ ADMIN OPTION FOR ] system_privilege_name [,...]
   FROM userID [,...]
```

パラメータ

（先頭に戻る） (321 ページ)

- **system_privilege_name –** 既存のシステム権限になります。
- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。
- **ADMIN OPTION FOR –** 各 *system_privilege* が、管理権限付きで指定の各 *userID* に現在付与されている必要があります。

  注意： この句では、システム権限の管理権限のみが取り消され、システム権限そのものは残ります。ただし、システム権限が WITH ADMIN ONLY OPTION 句付きで付与されていた場合は、ADMIN OPTION FOR 句により、システム権限が完全に取り消されます。このシナリオでは、管理権限を取り消すために ADMIN OPTION FOR 句の使用は必須ではありません。

例

（先頭に戻る） (321 ページ)

- **例 1 –** ユーザ `Jim` の BACKUP DATABASE システム権限を取り消します。

  ```
  REVOKE BACKUP DATABASE FROM Jim
  ```

- **例 2 –** BACKUP DATABASE システム権限がユーザ `Jim` に WITH ADMIN OPTION 句付きで付与されている場合、この例により、ユーザ `Jim` から、BACKUP

DATABASE システム権限を管理する権限が取り消されます。システム権限で承認されているタスクを実行する権限は残ります。ただし、BACKUP DATABASE システム権限が WITH ADMIN ONLY OPTION 句付きで Jim に付与されていた場合、この例では、ユーザ Jim からシステム権限のすべてのパーミッションが削除されます。

```
REVOKE ADMIN OPTION FOR BACKUP DATABASE FROM Jim
```

使用法

（先頭に戻る） (321 ページ)

システム権限が最初にどのように付与されているかによって、ADMIN OPTION FOR 句付きでシステム権限を取り消した場合、異なる結果になります。システム権限が WITH ADMIN OPTION 句付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めると、システム権限を管理する権限 (つまり、システム権限を別のユーザに付与できる権限) のみが取り消されます。システム権限を実際に使用する権限は残ります。ただし、システム権限が WITH ADMIN ONLY OPTION 付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めることは、システム権限全体を取り消すこととセマンティック上同じになります。最後に、システム権限が WITH NO ADMIN OPTION 句付きで付与されている場合、ADMIN OPTION FOR 句を REVOKE 文に含めても、元々管理システム権限が付与されていないので、何も取り消されません。

標準

（先頭に戻る） (321 ページ)

- SQL – その他の構文は、ISO/ANSI SQL 文法のベンダ拡張です。
- SAP Sybase Database 製品 - 構文は Adaptive Server でサポートされていません。

パーミッション

（先頭に戻る） (321 ページ)

取り消すシステム権限に対する管理権限が必要です。

すべてのシステム権限のリスト

すべてのシステム権限のリスト。

システム権限は、ユーザが承認済みのデータベースタスクを実行する権限を制御します。

次に、使用可能なシステム権限のリストを示します。

- ACCESS SERVER LS

- ALTER ANY INDEX
- ALTER ANY MATERIALIZED VIEW
- ALTER ANY OBJECT
- ALTER ANY OBJECT OWNER
- ALTER ANY PROCEDURE
- ALTER ANY SEQUENCE
- ALTER ANY TABLE
- ALTER ANY TEXT CONFIGURATION
- ALTER ANY TRIGGER
- ALTER ANY VIEW
- ALTER DATABASE
- ALTER DATATYPE
- BACKUP DATABASE
- CHANGE PASSWORD
- CHECKPOINT
- COMMENT ANY OBJECT
- CREATE ANY INDEX
- CREATE ANY MATERIALIZED VIEW
- CREATE ANY OBJECT
- CREATE ANY PROCEDURE
- CREATE ANY SEQUENCE
- CREATE ANY TABLE
- CREATE ANY TEXT CONFIGURATION
- CREATE ANY TRIGGER
- CREATE ANY VIEW
- CREATE DATATYPE
- CREATE EXTERNAL REFERENCE
- CREATE MATERIALIZED VIEW
- CREATE MESSAGE
- CREATE PROCEDURE
- CREATE PROXY TABLE
- CREATE TABLE
- CREATE TEXT CONFIGURATION
- CREATE VIEW
- DEBUG ANY PROCEDURE
- DELETE ANY TABLE
- DROP ANY INDEX
- DROP ANY MATERIALIZED VIEW
- DROP ANY OBJECT

- DROP ANY PROCEDURE
- DROP ANY SEQUENCE
- DROP ANY TABLE
- DROP ANY TEXT CONFIGURATION
- DROP ANY VIEW
- DROP CONNECTION
- DROP DATATYPE
- DROP MESSAGE
- EXECUTE ANY PROCEDURE
- LOAD ANY TABLE
- INSERT ANY TABLE
- MANAGE ANY DBSPACE
- MANAGE ANY EVENT
- MANAGE ANY EXTERNAL ENVIRONMENT
- MANAGE ANY EXTERNAL OBJECT
- MANAGE ANY LDAP SERVER
- MANAGE ANY LOGIN POLICY
- MANAGE ANY MIRROR SERVER
- MANAGE ANY OBJECT PRIVILEGES
- MANAGE ANY SPATIAL OBJECT
- MANAGE ANY STATISTICS
- MANAGE ANY USER
- MANAGE ANY WEB SERVICE
- MANAGE AUDITING
- MANAGE MULTIPLEX
- MANAGE PROFILING
- MANAGE REPLICATION
- MANAGE ROLES
- MONITOR
- READ CLIENT FILE
- READ FILE
- REORGANIZE ANY OBJECT
- SELECT ANY TABLE
- SERVER OPERATOR
- SET ANY PUBLIC OPTION
- SET ANY SECURITY OPTION
- SET ANY SYSTEM OPTION
- SET ANY USER DEFINED OPTION
- SET USER (管理権限のみで付与)

- TRUNCATE ANY TABLE
- UPDATE ANY TABLE
- UPGRADE ROLE
- USE ANY SEQUENCE
- VALIDATE ANY OBJECT
- WRITE CLIENT FILE
- WRITE FILE

REVOKE USAGE ON SEQUENCE 文

指定されたシーケンスに対する USAGE 権限を削除します。

クイックリンク：

「パラメータ」 (325 ページ)

「標準」 (325 ページ)

「パーミッション」 (325 ページ)

構文

```
REVOKE  USAGE ON SEQUENCE  sequence-name
    FROM  userID [,...]
```

パラメータ

（先頭に戻る） (325 ページ)

- **userID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。複数の userID はカンマで区切ります。

標準

（先頭に戻る） (325 ページ)

- SQL – 構文は永続的ストアドモジュール機能です。
- SAP Sybase Database 製品 - セキュリティモデルは Adaptive Server と SAP Sybase IQ では異なるため、他の構文も異なります。

パーミッション

（先頭に戻る） (325 ページ)

次のいずれかが必要です。

- MANAGE ANY OBJECT PRIVILEGE システム権限。
- そのシーケンスを所有している。

SET OPTION 文

データベースの動作および Transact-SQL との互換性に影響を及ぼすオプションを変更します。オプションの値を設定すると、すべてのユーザまたは個別のユーザの動作を一時的または永続的なスコープで変更できます。

クイックリンク：

「パラメータ」 (326 ページ)

「例」 (327 ページ)

「使用法」 (327 ページ)

「標準」 (328 ページ)

「パーミッション」 (328 ページ)

構文

```
SET [ EXISTING ] [ TEMPORARY ] OPTION
   … [ userid. | PUBLIC.]option-name = [ option-value ]
```

パラメータ

（先頭に戻る） (326 ページ)

- **option-value –** ホスト変数 (インジケータ使用可)、文字列、識別子、または数値。文字列に設定する場合、*option-value* の最大長は 127 バイトです。

  option-value を省略すると、指定されたオプション設定がデータベースから削除されます。これがユーザ個人のオプション設定の場合は、値は PUBLIC 設定に戻ります。

  注意： 整数値の指定が可能なデータベースオプションの場合、SAP Sybase IQ によって *option-value* の小数設定がすべて整数値にトランケートされます。たとえば、3.8 という値は 3 にトランケートされます。

- **EXISTING –** そのオプションに PUBLIC のユーザ ID 設定がすでに存在している場合を除き、個別のユーザ ID に対するオプション値は設定できません。

- **TEMPORARY –** 変更の有効期間を変更します。TEMPORARY 句がない場合、オプションの変更は永続的です。**SET OPTION** を使用して明示的に変更されるまで、変更されません。

  個別のユーザ ID を使用して TEMPORARY 句が適用された場合、そのユーザがデータベースにログインしている間だけ、新しいオプション値が有効になります。

PUBLIC ユーザ ID とともに TEMPORARY 句が使用された場合、データベースの実行中はその変更が継続されます。データベースが停止されると、PUBLIC ユーザ ID の TEMPORARY オプションは永続値に戻ります。

TEMPORARY オプションが削除されると、オプション設定は永続的な設定に戻ります。

例

（先頭に戻る） (326 ページ)

- **例 1 –** DATE_FORMAT オプションを設定します。

```
SET OPTION public.date_format = 'Mmm dd yyyy'
```

- **例 2 –** WAIT_FOR_COMMIT オプションを ON に設定します。

```
SET OPTION wait_for_commit = 'on'
```

- **例 3 –** embedded SQL の例を示します。

```
EXEC SQL SET OPTION :user.:option_name = :value;
EXEC SQL SET TEMPORARY OPTION Date_format = 'mm/dd/yyyy';
```

使用法

（先頭に戻る） (326 ページ)

オプションのクラスは次のとおりです。

- 一般的なデータベースオプション
- Transact-SQL 互換性データベースオプション

ユーザ ID または PUBLIC ユーザ ID を指定することで、個別ユーザ、*userid* で示されるロール、PUBLIC ユーザ ID (全ユーザがメンバーであるロール) のいずれに対してオプションが設定されるかが決まります。オプションがロール ID に適用される場合、ロールのメンバーによるオプション設定の継承は行われません。その変更はロール ID のみに適用されます。ロールが指定されない場合、そのオプション変更は現在ログオン中で **SET OPTION** 文を発行したユーザ ID に適用されます。たとえば、次の文では、オプション変更が PUBLIC ユーザ ID に適用されます。

```
SET OPTION Public.login_mode = standard
```

Embedded SQL では、データベースオプションが設定できるのは、一時的にすぎません。

PUBLIC ユーザ ID のオプション値を変更すると、独自の値を設定していないすべてのユーザにそのオプション値が設定されます。そのオプションに PUBLIC ユーザ ID 設定がすでに存在している場合を除き、個別のユーザ ID に対するオプション値は設定できません。

オプションの値を永続に設定するのではなく、PUBLIC ユーザ ID に対するオプションを一時的に設定すると、セキュリティが向上します。たとえば、**LOGIN_MODE** オプションが有効な場合、データベースは、そのデータベースを実行しているシステムのログインセキュリティに依存します。このオプションを一時的に有効にすると、Windows ドメインのセキュリティに依存しているデータベースは、データベースが停止し、ローカルマシンにコピーされた場合でも、セキュリティが損なわれることはありません。この場合、一時的に有効化された **LOGIN_MODE** は、永続値、つまり統合化ログインが許可されない Standard などに戻ります。

警告！ カーソルからローをフェッチしている際のオプション設定の変更は、予期しない動作を招く可能性があるためサポートされていません。たとえば、カーソルからのフェッチ中に DATE_FORMAT 設定を変更すると、結果セットで返されるローの日付フォーマットが統一されないことになります。ローをフェッチしている間にオプション設定を変更しないでください。

標準

（先頭に戻る） (326 ページ)

- SQL - ISO/ANSI SQL 文法のベンダ拡張。
- SAP Sybase Database 製品 - Adaptive Server ではサポートされていません。SAP Sybase IQ では、**SET** 文の使用時に一部の Adaptive Server オプションをサポートしています。

パーミッション

（先頭に戻る） (326 ページ)

各自のオプションを設定する際に特に要求されるシステム権限はありません。

別のユーザのデータベースオプションを設定するには、SET ANY PUBLIC OPTION システム権限が必要です。

PUBLIC ユーザ ID の SYSTEM オプションを設定するには、SET ANY SYSTEM OPTION システム権限が必要です。

PUBLIC ユーザ ID の SECURITY オプションを設定するには、SET ANY SECURITY OPTION システム権限が必要です。

SETUSER 文

ユーザは、タスクの開始の実行に必要な最小の権限をすでに持っている場合に、一時的に別のユーザのロールとシステム権限を使用して (同一化とも呼ばれる) 操作を実行できます。

注意： SET USER システム権限は 2 語で、SETUSER 文は 1 語です。

クイックリンク：

「パラメータ」 (329 ページ)

「使用法」 (329 ページ)

「標準」 (329 ページ)

「パーミッション」 (329 ページ)

構文

```
SETUSER userID
```

パラメータ

（先頭に戻る） (328 ページ)

- **UserID –** ログインパスワードを持つ既存のユーザまたはロールの名前になります。

使用法

（先頭に戻る） (328 ページ)

最小限の基準の検証は、SET USER システム権限が付与されるときではなく、SETUSER 文が実行されるときに行われます。

正常な同一化を終了するには、ユーザ ID を指定しないで SETUSER 文を発行します。

標準

（先頭に戻る） (328 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (328 ページ)

以下が必要です。

- 同一化実行者にターゲットユーザを同一化する権限が付与されている。
- 同一化実行者は、少なくともターゲットユーザに付与されているすべてのロールとシステム権限を持っている。
- 同一化実行者に、同等以上の管理権限付きで上述のロールとシステム権限が付与されている。

注意： 管理権限の基準を満たすという目的においては、WITH ADMIN OPTION 句と WITH ADMIN ONLY OPTION 句は同様の管理権限を付与するものとみなさ

れます。また、両者は、WITH NO ADMIN OPTION 句より上位の管理権限を付与するものとみなされます。たとえば、User1 には WITH ADMIN OPTION 句を指定して Role1 が付与され、User2 には WITH ADMIN ONLY 句を指定して Role1 が付与され、User3 には WITH NO ADMIN OPTION 句を指定して Role1 が付与されているとします。この場合、User1 と User2 には、同様の管理権限を持つ Role1 が付与されているとみなされます。また、User1 と User2 には、User3 より上位の管理権限を持つ Role1 が付与されているとみなされます。

- ターゲットユーザに拡張をサポートするシステム権限が付与されている場合、そのシステム権限を同一化実行者に付与する際に使用する句が、ターゲットユーザに付与する際に使用した句のスーパーセットである必要があります。拡張をサポートするのは SET USER システム権限と CHANGE PASSWORD システム権限のみです。
  - ANY 句は、*target_roles_list* 句と *target_users_list* 句のスーパーセットとみなされます。ターゲットユーザに ANY 句を使用して SET USER システム権限が付与されている場合、同一化実行者にも ANY 句を使用して付与されている必要があります。
  - ターゲットユーザに *target_roles_list* 句と *target_users_list* 句の両方を使用して SET USER システム権限が付与されている場合、同一化実行者にもその 2 つの句を使用してシステム権限が付与されている必要があり、さらにそれぞれの句のターゲットリストは、その句を使用してターゲットユーザに付与された内容と同等またはそのスーパーセットである必要があります。たとえば、同一化実行者とターゲットユーザのどちらも、ターゲットリストにそれぞれ User1 と User2、および Role1 と Role2 が含まれる場合、各句のターゲットリストで付与される内容は同等とみなされます。一方、同一化実行者に対してターゲットリストで付与される内容にそれぞれ User1 と User2 および Role1 と Role2 が含まれ、ターゲットユーザに対してターゲットリストで付与される内容に User1 と Role2 のみが含まれる場合、同一化実行者に対してターゲットリストで付与される内容はターゲットユーザのスーパーセットであるとみなされます。
  - ターゲットユーザに 1 つのターゲットリスト句を使用して SET USER システム権限が付与されている場合、同一化実行者のターゲットリストは、ターゲットユーザのリストと同等またはそのスーパーセットである必要があります。たとえば、同一化実行者とターゲットユーザの両方の *target_user_list* に User1 と User2 が含まれる場合 (同等) または同一化実行者のリストに User1 と User2、ターゲットユーザのリストに User2 がそれぞれ含まれる場合です。User1 と User2 (同一化実行者のリスト) は User2 (ターゲットユーザのリスト) のスーパーセットです。
  - 定義により、ユーザは常に自分自身を同一化できます。したがって、ターゲットユーザに同一化実行者を同一化する権限が付与されている場合、こ

れは同一化実行者の基準要件である同等またはスーパーセットであることに違反しません。たとえば、User3 が同一化実行者、User4 がターゲットユーザであり、User3 の *target_user_list* には、User4 と User5 が含まれています。User4 の *target_user_list* には、User3 と User5 が含まれています。このターゲットリストから同一化実行者を削除した場合、User3 のターゲットリストは基準要件を満たします。

VALIDATE LDAP SERVER 文

既存の LDAP サーバ設定オブジェクトの設定に対する変更を適用前に検証します。

クイックリンク：

「パラメータ」 (331 ページ)

「例」 (333 ページ)

「使用法」 (333 ページ)

「標準」 (334 ページ)

「パーミッション」 (334 ページ)

構文

```
VALIDATE LDAP SERVER [ ldapua-server-name | ldapua-server-attribs ]
    [ CHECK userid [ user-dn-string ] ]

ldapua-server-attribs
    SEARCH DN
                URL { 'URL_string' | NULL }
                | ACCESS ACCOUNT { 'DN_string' | NULL }
                | IDENTIFIED BY ( 'password' | NULL }
                | IDENTIFIED BY ENCRYPTED { encrypted-password | NULL }

    | AUTHENTICATION URL { 'URL_string' | NULL }
    | CONNECTION TIMEOUT timeout_value
    | CONNECTION RETRIES retry_value
    | TLS { ON | OFF }
```

パラメータ

（先頭に戻る） (331 ページ)

- **ldapua-server-name –** LDAP サーバ設定オブジェクトを指定します。
- **URL –** ホスト（名前または IP アドレスで指定)、ポート番号、指定のユーザ ID の DN ルックアップで実行される検索を指定します。この値は、LDAP URL 構文が正しいかどうかがの検証後に、ISYSLDAPSERVER システムテーブルに格納されます。この文字列の最大サイズは 1024 バイトです。

- **ACCESS ACCOUNT –** SAP Sybase IQ 内のユーザではなく、SAP Sybase IQ が使用するために LDAP サーバで作成されたユーザ。このユーザの識別名 (DN) は、LDAP サーバへの接続に使用されます。このユーザは、SEARCH DN URL で指定された場所でユーザ ID によって DN を検索するためのパーミッションを、LDAP サーバ内に保持しています。この文字列の最大サイズは 1024 バイトです。
- **IDENTIFIED BY –** ACCESS ACCOUNT ユーザに関連付けられたパスワードを指定します。このパスワードは、対称暗号化を使用してディスクに保存されます。パスワードを解除して何も設定しない場合は、値 NULL を指定します。クリアテキストのパスワードの最大サイズは 255 バイトです。
- **IDENTIFIED BY ENCRYPTED –** ACCESS ACCOUNT 識別名に関連付けられるパスワードを暗号化形式で設定します。バイナリ値は暗号化されたパスワードであるため、ディスクにそのまま保存されます。パスワードを解除して何も設定しない場合は、値 NULL を指定します。バイナリの最大サイズは 289 バイトです。
- **AUTHENTICATION URL –** ユーザの認証に使用する LDAP サーバのホスト (名前または IP アドレスで指定) とポート番号を指定します。これは、<URL_string> として定義された値で、LDAP URL 構文が正しいかどうかの検証後に `ISYSLDAPSERVER` システムテーブルに格納されます。事前の DN 検索によって得られたユーザの DN とユーザパスワードによって、新しい接続が認証 URL にバインドされます。LDAP サーバへの正常な接続は、接続ユーザの ID の証明とみなされます。この文字列の最大サイズは 1024 バイトです。
- **CONNECTION TIMEOUT –** DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続のタイムアウトを指定します。この値はミリ秒で指定します。デフォルト値は 10 秒です。
- **CONNECTION RETRIES –** DN 検索と認証の両方に使用する SAP Sybase IQ から LDAP サーバへの接続の再試行回数を指定します。有効値の範囲は 1 ～ 60 で、デフォルト値は 3 です。
- **TLS –** DN 検索と認証の両方に使用する LDAP サーバへの接続に、TLS とセキュア LDAP プロトコルのいずれを使用するかを定義します。ON に設定すると、TLS プロトコルが使用され、URL は "ldap://" で始まります。OFF に設定すると (または指定なしにすると)、セキュア LDAP プロトコルが使用され、URL は “ldaps://” で始まります。TLS プロトコルを使用する場合は、LDAP サーバで使用される証明書に署名した認証局 (CA) の証明書が含まれているファイル名を使用して、データベースセキュリティオプション TRUSTED_CERTIFICATES_FILE を指定します。

- **CHECK userID –** LDAP サーバで存在が検証される userID。
- **user-dn-string –** 検証を目的としてユーザの DN 値をユーザ ID と比較します。

例

（先頭に戻る） (331 ページ)

- **例 1 –** apps_primary LDAP サーバ設定オブジェクトが次のように作成されているとします。

```
SET OPTION PUBLIC.login_mode = 'Standard,LDAPUA'
CREATE LDAP SERVER apps_primary
SEARCH DN
    URL 'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
WITH ACTIVATE
```

  次の文は、userID の `myusername` が存在することを、オプションの CHECK 句を使用し、`apps_primary` LDAP サーバ設定オブジェクトで予測されるユーザの識別名 (引用符で囲まれている) と比較することによって検証します。

```
VALIDATE LDAP SERVER apps_primary
CHECK myusername 'cn=myusername,cn=Users,dc=mycompany,dc=com'
```

- **例 2 –** 検索属性が含まれている場合、LDAP サーバ設定オブジェクトの名前が **VALIDATE LDAP SERVER** 文で定義されている必要はありません。

```
VALIDATE LDAP SERVER
SEARCH DN
   URL  'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
CHECK myusername 'cn=myusername,cn=Users,dc=mycompany,dc=com'
```

使用法

（先頭に戻る） (331 ページ)

この文は、管理者が LDAP ユーザ認証が使用されるように新しいサーバを設定する場合、および LDAP サーバ設定オブジェクトと外部 LDAP サーバ間の問題を診断する場合に便利です。**VALIDATE LDAP SERVER** 文による接続はすべて一時的で、この文の終了により切断されます。

名前で LDAP サーバ設定オブジェクトを検証する際は、以前の **CREATE LDAP SERVER** 文と **ALTER LDAP SERVER** 文の定義が使用されます。また、*ldapua-server-*

attributes が LDAP サーバ設定オブジェクト名の代わりに指定された場合、指定の属性が検証されます。*ldapua-server-attributes* が指定された場合、構文エラーを識別するために URL が解析され、構文エラーが検出されると、文の処理が停止します。

LDAP サーバ設定オブジェクト名か、正常に解析された *ldapua-server-attributes* セットのいずれかを使用して、外部 LDAP サーバへの接続が試行されます。パラメータ ACCESS ACCOUNT とパスワードが指定されている場合、この値が SEARCH DN URL への接続確立に使用されます。構成は SEARCH DN URL、ACCESS ACCOUNT、および ACCESS ACCOUNT のパスワードになります。

オプションの CHECK 句を使用すると、外部 LDAP サーバ上のユーザの存在の検証に検索内の userID が使用されます。指定ユーザの予想される DN 値が既知の場合はこの値を指定でき、この値が検索結果と比較され、成功または失敗が判断されます。

標準

（先頭に戻る） (331 ページ)

ANSI SQL – 準拠レベル： Transact-SQL 拡張。

パーミッション

（先頭に戻る） (331 ページ)

MANAGE ANY LDAP SERVER システム権限が必要です。

データベースオプション

データベースオプションは、データベースの動作をカスタマイズおよび変更します。

LOGIN_MODE オプション

データベースの統合化ログインの使用を制御します。

指定できる値

- Standard – デフォルト設定。統合化ログインは使用できません。統合化ログインを使用して接続しようとすると、エラーが発生します。
- Mixed – 統合化ログインと標準ログインの両方を使用できます。
- Integrated – データベースへのログインはすべて、統合化ログインを使用して実行する必要があります。

- Kerberos – データベースへのログインはすべて、Kerberos ログインを使用して実行する必要があります。
- LDPAUA – データベースへのログインはすべて、LDAP ログインを使用して実行する必要があります。

注意： Mixed は、「Standard,Integrated」と同じになります。

デフォルト値
Standard

スコープ
オプションは、データベース (PUBLIC) レベルでのみ設定できます。

このオプションを設定するには、SET ANY SECURITY OPTION システム権限が必要です。すぐに有効になります。

備考
値では大文字と小文字が区別されません。

警告！

- 混合環境で **LOGIN_MODE** を 1 つのモード (Integrated のみ、LDAPUA のみなど) に制限すると、対応するログインマッピングが付与されたユーザのみに接続が制限されます。その他の方法を使用して接続しようとすると、エラーが発生します。唯一の例外は、完全な管理権 (SYS_AUTH_DBA_ROLE または SYS_AUTH_SSO_ROLE) が付与されたユーザです。
- **LOGIN_MODE** を LDAPUA のみに制限すると、LDAPUA が許可されるユーザポリシーまたはログインポリシーが存在しない場合に、接続可能なユーザが存在しない設定が発生する可能性があります。この状況から復旧するには、**start_iq** ユーティリティでコマンドラインスイッチ **-al** *user-id-list* を指定してください。

MIN_ROLE_ADMINS オプション

すべてのロールについて、必要な管理者の最小数を設定します。

指定可能な値
1 – 10

デフォルト
1

スコープ
オプションは、データベース (PUBLIC) レベルでのみ設定できます。

このオプションを設定するには、SET ANY SECURITY OPTION システム権限が必要です。すぐに有効になります。

備考
このオプションは、すべてのロールについて、必要な管理者の最小数を設定します。この値は、ロール全体に対するロール管理者の最小数ではなく、各ロールに対するロール管理者の最小数に適用されます。この値は、ロールまたはユーザを削除する際に、残りのユーザとロールの管理に十分なシステム権限を持つユーザとロールがいなくなるというシナリオが発生しないことを保証します。

TRUSTED_CERTIFICATES_FILE オプション

LDAP ユーザ認証による送信トランスポートレイヤセキュリティ (TLS) 接続、INC 接続、および MIPC 接続のための信頼関係を指定します。

指定可能な値
サーバ証明書に署名する信頼された認証局のリストを含む TXT ファイルの場所を示す有効なネットワークパス。

デフォルト
NULL。信頼された認証局がないため送信 TLS 接続を開始できないことを意味します。

スコープ
オプションは、データベース (PUBLIC) レベルでのみ設定できます。

このオプションを設定するには、SET ANY SECURITY OPTION システム権限が必要です。すぐに有効になります。

備考
このオプションは、信頼された認証局のリストの場所を示すパスを指定します。リストは、TXT ファイルに保管する必要があります。このファイルは、Windows 環境内でそのマシン上のすべての SAP Sybase アプリケーションによって使用されるローカルドライブ上の場所で共有できます。

-al iqsrv16 サーバオプション

標準認証を使用して、特定数のユーザのみに LDAPUA の LOGIN_MODE を拡張します。

構文

```
-al "user1;user2;user3" server_name.cfg database-name.db
```

備考

- 最大 5 つのユーザ ID をセミコロンで区切って指定できます。各ユーザ ID は二重引用符で囲みます。
- サーバレベルでの実行時には、**-al** スイッチはサーバの次回の再起動時まで有効です。

-al iqsrv16 データベースオプション

標準認証を使用して、特定数のユーザのみに LDAPUA の LOGIN_MODE を拡張します。

構文

```
-al "user1;user2;user3" server_name.cfg database_name.db
```

備考

- 最大 5 つのユーザ ID をセミコロンで区切って指定できます。各ユーザ ID は二重引用符で囲みます。
- データベースレベルでの実行時には、データベースの次回の停止/起動時まで有効です。

VERIFY_PASSWORD_FUNCTION オプション

パスワードルールの実装に使用できる、ユーザ指定の認証の関数を指定します。

指定できる値
文字列

デフォルト
" (空の文字列)。(パスワードが設定されている場合、関数は呼び出されません)

スコープ
オプションは、データベース (PUBLIC) レベルまたは ユーザレベルで設定できます。データベースレベルで設定した場合、値は新しいユーザのデフォルト値になりますが、既存のユーザには影響を与えません。ユーザレベルで設定した場合は、そのユーザの PUBLIC 値 のみが上書きされます。自分のオプションを設定する場合は、システム権限は必要ありません。自分以外のユーザのオプションをデータベースレベルまたはユーザレベルで設定する場合は、システム権限が必要です。

このオプションを設定するには、SET ANY SECURITY OPTION システム権限が必要です。個々の接続または PUBLIC ロールに一時的に設定できます。すぐに有効になります。

備考

VERIFY_PASSWORD_FUNCTION オプションの値が有効な文字列に設定されている場合、**GRANT CONNECT TO** *userid* **IDENTIFIED BY** *password* 文によってオプション値で指定された関数が呼び出されます。

ユーザが関数を上書きするのを防ぐために、オプション値は、*owner.function_name* の形式で指定する必要があります。

関数は、次の 2 つのパラメータを取ります。

- *user_name* VARCHAR(128)
- *new_pwd* VARCHAR(255)

戻り値のデータ型は、VARCHAR(255) です。

VERIFY_PASSWORD_FUNCTION が設定されている場合、**GRANT CONNECT** 文で複数のユーザ ID とパスワードを指定することはできません。

例

次のサンプルコードは、テーブルと関数を定義し、いくつかのログインポリシーオプションを設定します。同時に、パスワードにおける特定の種類の文字の要求、パスワードの再使用の禁止、パスワードの有効期限の適用などを含む詳細なパスワード規則も実装します。ユーザ ID の作成時、またはパスワードの変更時には、verify_password_function オプションを使用してデータベースサーバによってこの関数が呼び出されます。アプリケーションでは post_login_procedure オプションによって指定されるプロシージャが呼び出され、有効期限前にパスワードの変更が必要であることを通知することができます。

```
-- only DBA should have privileges on this table
CREATE TABLE DBA.t_pwd_history(
        pk          INT         DEFAULT AUTOINCREMENT PRIMARY KEY,
        user_name   CHAR(128),  -- the user whose password is set
        pwd_hash    CHAR(32) ); -- hash of password value to detect
                                -- duplicate passwords

-- called whenever a non-NULL password is set
-- to verify the password conforms to password rules
CREATE FUNCTION DBA.f_verify_pwd( uid     VARCHAR(128),
                                  new_pwd VARCHAR(255) )
RETURNS VARCHAR(255)
BEGIN
    -- enforce password rules
    -- enforce minimum length (can also be done with
    -- min_password_length option)
    IF length( new_pwd ) < 6 THEN
        RETURN 'password must be at least 6 characters long';
    END IF;

    -- number of lowercase characters IN new_pwd
    SELECT count(*) INTO num_lower_chars
```

```
        FROM pwd_chars WHERE CAST( c AS BINARY ) BETWEEN 'a' AND 'z';

    -- enforce rules based on characters contained in new_pwd
    IF ( SELECT count(*) FROM pwd_chars WHERE c BETWEEN '0' AND '9' )
            < 1 THEN
        RETURN 'password must contain at least one numeric digit';
    ELSEIF length( pwd_alpha_only ) < 2 THEN
        RETURN 'password must contain at least two letters';
    ELSEIF num_lower_chars = 0
           OR length( pwd_alpha_only ) - num_lower_chars = 0 THEN
        RETURN 'password must contain both upper- and lowercase
characters';
    END IF;

    -- not the same as any user name
    -- (this could be modified to check against a disallowed words
table)
    IF EXISTS( SELECT * FROM SYS.SYSUSER
                    WHERE lower( user_name ) IN
( lower( pwd_alpha_only ),
                                              lower( new_pwd ) ) ) THEN
        RETURN 'password or only alphabetic characters in password '
||
               'must not match any user name';
    END IF;

    -- not the same as any previous password for this user
    IF EXISTS( SELECT * FROM t_pwd_history
                    WHERE user_name = uid
                   AND pwd_hash = hash( uid || new_pwd, 'md5' ) ) THEN
        RETURN 'previous passwords cannot be reused';
    END IF;

    -- save the new password
    INSERT INTO t_pwd_history( user_name, pwd_hash )
        VALUES( uid, hash( uid || new_pwd, 'md5' ) );

    RETURN( NULL );
END;

ALTER FUNCTION DBA.f_verify_pwd SET HIDDEN;
GRANT EXECUTE ON DBA.f_verify_pwd TO PUBLIC;
SET OPTION PUBLIC.verify_password_function = 'DBA.f_verify_pwd';


-- All passwords expire in 180 days. Expired passwords can be changed
-- by the user using the NewPassword connection parameter.
ALTER LOGIN POLICY DEFAULT password_life_time = 180;

-- If an application calls the procedure specified by the
-- post_login_procedure option, then the procedure can be used to
-- warn the user that their password is about to expire. In
particular,
-- Interactive SQL calls the post_login_procedure.
ALTER LOGIN POLICY DEFAULT password_grace_time = 30;
```

オプションをオフにするには、空の文字列を指定します。

```
SET OPTION PUBLIC.VERIFY_PASSWORD_FUNCTION = ''
```

MIN_PASSWORD_LENGTH オプション

データベースの新しいパスワードの長さの最小値を設定します。

指定できる値
0 以上の整数

値はバイト単位です。シングルバイト文字セットの場合、これは文字数と同じになります。

デフォルト値
3 文字

スコープ
オプションは、データベース (PUBLIC) レベルでのみ設定できます。

このオプションを設定するには、SET ANY SECURITY OPTION システム権限が必要です。すぐに有効になります。

備考
このオプションを使用すると、すべての新しいパスワードの長さに最小値が設定され、セキュリティが強化されます。既存のパスワードには影響しません。

例
新しいパスワードの最小長を 6 バイトに設定します。

```
SET OPTION PUBLIC.MIN_PASSWORD_LENGTH = 6
```

-gk iqsrv16 データベースサーバオプション

データベースサーバの停止に必要な権限を設定します。

構文

```
iqsrv16 -gk { DBA | all | none } ...
```

指定可能な値

- **DBA –** SERVER OPERATOR システム権限を持つユーザのみがデータベースサーバを停止できます。これはネットワークサーバのデフォルトです。
- **all –** データベースサーバを停止するのに権限が必要ありません。
- **none –** データベースサーバを停止できません。

適用対象
すべてのオペレーティングシステムとデータベースサーバ。

備考
-gd データベースサーバオプションは、dbstop ユーティリティに適用されるほか、次の文にも適用されます。

- ALTER DATABASE *dbname* FORCE START 文
- STOP DATABASE 文

-gl iqsrv16 サーバオプション

LOAD TABLE を使用してデータをロードするためのパーミッションを設定します。

構文
-gl level

備考
LOAD TABLE 文はデータベースサーバマシンからファイルを読み取ります。このような文を使用したファイルシステムアクセスを制御するために、**-gl** コマンドラインスイッチを使用して、このような文の使用に必要なデータベースパーミッションレベルを調整できます。*level* は次のいずれかです。

- DBA - LOAD ANY TABLE システム権限、ALTER ANY TABLE システム権限、または ALTER ANY OBJECT システム権限を持つユーザのみがデータをロードできます。
- ALL - すべてのユーザがデータをロードできます。
- NONE - データのロードはできません。

オプションには大文字の構文も小文字の構文も使用できます。

デフォルト設定は、**start_iq** を使用して起動されたサーバの場合は **all** で、その他の場合は **dba** です。以前のバージョンとの一貫性を維持するために、すべてのシステムで **all** 値を使用してください。`iqdemo.cfg` および `default.cfg` 設定ファイルでは、**all** 設定が使用されています。

-gu iqsrv16 データベースサーバオプション

データベースファイル管理文 (データベースの作成や削除などの文) の実行に必要な権限を設定します。

構文

```
iqsrv16 -gu { all | none | DBA | utility_db } ...
```

指定可能な値

-gu オプション	効果	適用対象
all	*このオプションは推奨されなくなりました。*すべてのユーザがファイル管理文を実行できます。	ユーティリティデータベースを含むすべてのデータベース
none	ファイル管理文の実行は許可されません。	ユーティリティデータベースを含むすべてのデータベース
DBA	SERVER OPERATOR システム権限を持つユーザのみがファイル管理文を実行できます。	ユーティリティデータベースを含むすべてのデータベース
utility_db	ユーティリティデータベースに接続できるユーザのみがファイル管理文を実行できます。	ユーティリティデータベースのみ

デフォルト
DBA

適用対象
すべてのオペレーティングシステムとデータベースサーバ。

備考
次のデータベースファイル管理文を実行できるユーザが制限を受けます。

- ALTER DATABASE dbfile ALTER TRANSACTION LOG
- CREATE DATABASE 文
- CREATE DECRYPTED DATABASE 文
- CREATE DECRYPTED FILE 文
- CREATE ENCRYPTED DATABASE 文
- CREATE ENCRYPTED FILE 文
- DROP DATABASE 文
- RESTORE DATABASE 文

utility_db を指定した場合、これらの文はユーティリティデータベースからのみ実行できます。DBA を指定した場合、これらの文は SERVER OPERATOR システム権限を持つユーザのみ実行できます。none を指定した場合は、どのユーザもこれらの文を実行できません。

例

ファイル管理文の使用を防ぐため、-gu オプションの none 権限レベルを使用してデータベースサーバを起動します。次のコマンドは、データベースサーバを起動し、TestSrv という名前を付けます。このコマンドによって mytestdb.db データベースがロードされますが、どのユーザも、そのサーバを使用してデータベースを作成または削除したり、他のファイル管理文を実行したりすることはできません。これは、ユーザのリソース作成権の有無や、ユーティリティデータベースをロードして接続できるかどうかには関係ありません。

```
iqsrv16 -n TestSrv -gu none c:¥mytestdb.db
```

ユーティリティデータベースのパスワードを知っているユーザだけにファイル管理文の実行を許可するには、次のコマンドを実行してサーバを起動します。

```
iqsrv16 -n TestSrv -su secret -gu utility_db
```

次のコマンドは、Interactive SQL をクライアントアプリケーションとして起動し、TestSrv という名前のサーバに接続し、ユーティリティデータベースをロードして、ユーザを接続させます。

```
dbisql -c
"UID=DBA;PWD=secret;DBN=utility_db;Host=host1;Server=TestSrv"
```

上記のコマンドが正常に実行されると、ユーザがユーティリティデータベースに接続し、ファイル管理文を実行できます。

-sk iqsrv16 データベースサーバオプション

データベースサーバに対して保護されている機能へのアクセスを許可にするの使用できる、システムセキュリティ機能キーを指定します。

構文

```
iqsrv16 -sk key ...
```

適用対象

すべてのオペレーティングシステムとデータベースサーバ。

備考

-sf オプションを使用してデータベースサーバの機能を保護するときに、sk オプションを含めることもできます。このオプションで指定したキーを sp_use_secure_feature_key システムプロシージャで使用すると、接続に対して保護されている機能へのアクセスを許可できます。この場合、sa_server_option システムプロシージャを使用して、データベースサーバ上で実行されているすべてのデータベースを保護する機能または機能セットに変更を加えることもできます。

キーは、6 文字以上の空でない文字列にする必要があり、二重引用符、制御文字 (0x20 未満のすべての文字)、またはバックスラッシュを含めることはできません。データベースごとのセキュリティ機能キーは 1000 個に制限されています。

sp_use_secure_feature_key システムプロシージャの authorization_key パラメータの値として、-sk で指定した値以外の値を設定した場合、エラーにはならず、-sf で指定した機能が接続に対して引き続き保護されます。

-sf を指定しないで -sk を指定した場合は、デフォルトのセキュリティ機能のみが有効になりますが、データベースサーバの実行中にシステムセキュリティ機能キーを使用してセキュリティ機能の設定を変更することができます。

例

次のコマンドは、バックアップ機能を保護した状態で、secure_server という名前のデータベースサーバを起動します。後で、-sk オプションで指定したキーを使用し、特定の接続に対してそれらの機能へのアクセスを許可できます。

```
iqsrv16 -n secure_server -sf backup -sk j978kls12
```

secure_server データベースサーバで実行中のデータベースへの接続に対して、-sk で指定した値を authorization_key パラメータに設定すると、secure_server データベースサーバで保護されている機能のバックアップや変更をその接続で実行できるようになります。

```
CALL sp_use_secure_feature_key ( 'MyKey' , 'j978kls12' );
```

その後、次のコマンドを実行すると、secure_server で実行中のデータベースに対してすべての機能を保護できます。

```
CALL sa_server_option( 'SecureFeatures', 'all' );
```

-sf iqsrv16 データベースサーバオプション

現在のデータベースサーバで実行中のデータベースで使用できる機能にユーザがアクセスできるかどうかを制御します。セキュアな機能 (セキュリティで保護された機能) には適切な権限を持つユーザのみがアクセスできます。一方で、セキュアでない機能 (セキュリティで保護されない機能) にはすべてのユーザがアクセスできます。

構文

```
iqsrv16 -sf feature-list ...
```

```
feature-list :
feature-name | feature-set [ ,feature-name | feature-set ] ...
```

機能セット	含まれている機能 (機能セットは太字)
none	manage_features、manage_keys および disk_sandbox 以外の機能はすべてセキュリティで保護されません。
manage_server	processor_affinity
manage_security	manage_features manage_keys manage_disk_sandbox
server_security	disk_sandbox trace_system_event

機能セット	含まれている機能 (機能セットは太字)
all	**client –** read_client_file write_client_file **remote –** remote_data_access send_udp send_email web_service_client **local –** • **local_call –** cmdshell external_procedure java • **local_db –** backup restore database dbspace • **local_env –** getenv • **local_io –** create_trace_file read_file write_file directory sp_list_directory sp_create_directory sp_copy_directory sp_move_directory sp_delete_directory sp_copy_file sp_move_file

機能セット	含まれている機能 (機能セットは太字)
	sp_delete_file • **local_log –** request_log console_log webclient_log

パラメータ

- **none –** どの機能もセキュリティで保護されないことを指定します。
- **manage_server –** ユーザは、すべてのデータベースサーバ関連機能にアクセスできなくなります。この機能セットには、次の機能が含まれています。
  - **processor_affinity –** ユーザは、データベースサーバのプロセッサのアフィニティ (使用する論理プロセッサの数) を変更できなくなります。
- **manage_security –** ユーザは、データベースサーバのセキュリティの管理を許可する機能にアクセスできなくなります。デフォルトでは、これらの機能はセキュリティで保護されています。
  - **manage_features –** ユーザは、データベースサーバ上でセキュリティで保護できる機能のリストを変更できなくなります。
  - **manage_keys –** セキュリティ機能キーの作成、変更、削除、またはリストができなくなります。

    manage_keys 機能にアクセスできるものの manage_features 機能にアクセスできないユーザは、そのユーザに割り当てられているよりも多くのセキュリティ機能を持つキーを定義することができなくなります。
  - **manage_disk_sandbox –** ユーザは、sa_server_option システムプロシージャまたは sa_db_option システムプロシージャを使用してディスクサンドボックス設定を一時的に変更することができなくなります。すべてのデータベースまたはユーザに対して manage_disk_sandbox セキュリティ機能をオフにすることはできません。sp_use_secure_feature_key システムプロシージャを使用して個々の接続に対してオフにすることのみ可能です。
- **server_security –** ユーザは、セキュリティ設定を一時的にバイパスできる機能にアクセスできなくなります。デフォルトでは、これらの機能はセキュリティで保護されています。
  - **disk_sandbox –** ユーザは、メインデータベースファイルがあるディレクトリ以外の場所でデータベースファイルの読み込み／書き込み操作を実行できなくなります。

- **trace_system_event –** ユーザは、ユーザ定義のトレースイベントを作成できなくなります。

- **all –** ユーザは以下のグループにアクセスできなくなります。
  - **client –** ユーザは、クライアント関連入出力へのアクセスを許可するすべての機能にアクセスできなくなります。この機能は、クライアントコンピューティング環境へのアクセスを制御します。この機能セットには、次の機能が含まれています。
    - **read_client_file –** クライアントファイルの読み込みを可能にする文が使用できなくなります。たとえば、READ_CLIENT_FILE 関数や LOAD TABLE 文がこれに該当します。
    - **write_client_file –** クライアントファイルへの書き込みを可能にする文が使用できなくなります。たとえば、UNLOAD 文や WRITE_CLIENT_FILE 関数がこれに該当します。
  - **remote –** リモートアクセスまたはリモートプロセスとの通信を許可するすべての機能にアクセスできなくなります。この機能セットには、次の機能が含まれています。
    - **remote_data_access –** プロキシテーブルなどのリモートデータアクセスサービスがすべて使用できなくなります。
    - **send_udp –** sa_send_udp システムプロシージャを使用して指定したアドレスに UDP パケットを送信する機能が使用できなくなります。
    - **send_email –** xp_sendmail などの電子メールシステムプロシージャが使用できなくなります。
    - **web_service_client –** Web サービスクライアントのストアドプロシージャコール (HTTP 要求を発行するストアドプロシージャ) が使用できなくなります。
  - **local –** ユーザは、すべてのローカル関連機能にアクセスできなくなります。この機能は、サーバコンピューティング環境へのアクセスを制御します。この機能セットには、`local_call`、`local_db`、`local_io`、`local_log` の各機能サブセットが含まれています。
    - **local_call –** ユーザは、データベースサーバの直接的な一部ではなく、データベースサーバによって制御されていないコードについて、その実行機能を提供するすべての機能にアクセスできなくなります。この機能セットには、次の機能が含まれています。
      - **cmdshell –** xp_cmdshell プロシージャが使用できなくなります。
      - **external_procedure –** 外部ストアドプロシージャが使用できなくなります。この設定によってデータベースサーバに組み込まれている xp_* システムプロシージャ (xp_cmdshell や xp_readfile など) が使用で

きなくなることはありません。これらのシステムプロシージャには、個別の機能制御オプションがあります。
  - **external_procedure_v3 –** ユーザ定義関数を参照してください。
  - **java –** Java プロシージャなどの Java 関連機能が使用できなくなります。
- **local_db –** ユーザは、すべてのデータベースファイル関連機能にアクセスできなくなります。この機能セットには、次の機能が含まれています。
  - **backup –** BACKUP 文と、BACKUP 文を使用したサーバ側バックアップの実行機能が使用できなくなります。dbbackup ユーティリティによるクライアント側バックアップは引き続き実行できます。
  - **restore –** RESTORE DATABASE 文が使用できなくなります。
  - **database –** CREATE DATABASE 文、ALTER DATABASE 文、DROP DATABASE 文、CREATE ENCRYPTED FILE 文、CREATE DECRYPTED FILE 文、CREATE ENCRYPTED DATABASE 文、CREATE DECRYPTED DATABASE 文が使用できなくなります。
  - **dbspace –** CREATE DBSPACE 文、ALTER DBSPACE 文、DROP DBSPACE 文が使用できなくなります。
- **local_env –** ユーザは、すべての環境変数関連機能にアクセスできなくなります。この機能セットには、次の機能が含まれています。
  - **getenv –** ユーザは、どの環境変数の値の読み込みもできなくなります。
- **local_io –** ユーザは、ファイルとその内容への直接アクセスを許可するすべての機能にアクセスできなくなります。この機能セットには、次の機能が含まれています。
  - **create_trace_file –** イベントトレースターゲットを作成する文が使用できなくなります。
  - **read_file –** ローカルファイルの読み込みを可能にする文が使用できなくなります。たとえば、xp_read_file システムプロシージャ、LOAD TABLE 文、OPENSTRING(FILE ...) の使用がこれに該当します。代替名の load_table や xp_read_file は廃止されました。
  - **write_file –** ローカルファイルへの書き込みを可能にする文が使用できなくなります。たとえば、UNLOAD 文や xp_write_file システムプロシージャがこれに該当します。代替名の unload_table や xp_write_file は廃止されました。
  - **delete_file –** ローカルファイルの削除を可能にするすべての文が使用できなくなります。たとえば、この機能をセキュリティで保護する

ことで、-x オプションや -xo オプションを指定した場合に dbbackup ユーティリティの実行が失敗します。

- **directory –** ディレクトリクラスプロキシテーブルが使用できなくなります。remote_data_access が無効の場合、この機能は無効になります。
- **sp_list_directory –** sp_list_directory システムプロシージャが使用できなくなります。
- **sp_create_directory –** sp_create_directory システムプロシージャが使用できなくなります。
- **sp_copy_directory –** sp_copy_directory システムプロシージャが使用できなくなります。
- **sp_move_directory –** sp_move_directory システムプロシージャが使用できなくなります。
- **sp_delete_directory –** sp_delete_directory システムプロシージャが使用できなくなります。
- **sp_copy_file –** sp_copy_file システムプロシージャが使用できなくなります。
- **sp_move_file –** sp_move_file システムプロシージャが使用できなくなります。
- **sp_delete_file –** sp_delete_file システムプロシージャが使用できなくなります。

- **local_log –** ユーザは、結果としてディスク上のファイルにデータを直接作成したり書き込んだりするすべてのロギング機能にアクセスできなくなります。この機能セットには、次の機能が含まれています。

  - **request_log –** 要求ログのファイル名を変更する機能と、その最大サイズまたは最大ファイル数を増やす機能が使用できなくなります。データベースサーバの起動コマンドには、要求ログファイルとそのファイルの最大サイズを指定できます。ただし、それらをデータベースサーバの起動後に変更することはできません。要求ログの機能が無効になっていても、要求ロギングのオンとオフを切り替えたり、要求ログファイルの最大ファイルサイズや最大ファイル数を減らしたりすることは引き続き可能です。
  - **console_log –** sa_server_option システムプロシージャの ConsoleLogFile オプションを使用してデータベースサーバメッセージログのファイル名を変更する機能が使用できなくなります。また、この機能をセキュリティで保護すると、sa_server_option システムプロシージャの ConsoleLogMaxSize オプションを使用してログファイルの最大サイズを増やす機能が使用できなくなります。データベースサーバの起動時には、サーバログファイルとそのサイズを指定できます。
  - **webclient_log –** sa_server_option システムプロシージャの WebClientLogFile オプションを使用して Web サービスクライアントロ

グのファイル名を変更する機能が使用できなくなります。データベースサーバの起動時に Web サービスクライアントログファイルを指定できます。

適用対象
すべてのオペレーティングシステムとデータベースサーバ。

備考
データベースサーバの所有者はこのオプションを使用して、データベースサーバで実行中のデータベースで使用できる機能にユーザがアクセスできるかどうかを制御できます。また、データベースサーバの所有者は、-sk オプションを使用してシステムセキュリティ機能キーを作成し、-sf オプションで指定された機能にユーザがアクセスできないようにすることができます。

システムのセキュリティ機能キーを指定しないでデータベースを起動した場合は、デフォルトのセキュリティ機能がセキュリティで保護され、データベースサーバやそのサーバで実行中のすべてのデータベースについてセキュリティ機能の設定を変更できなくなります。後でシステムのセキュリティ機能キーを作成することはできません。データベースサーバをシャットダウンし、再起動時にシステムのセキュリティ機能キーを指定する必要があります。

feature-list は、データベースサーバで保護する機能名または機能セットをカンマで区切って示したリストです。機能をセキュリティで保護すると、管理者以外のすべてのデータベースユーザがアクセスできなくなります。機能セットを指定すると、そのセットに含まれているすべての機能が保護されます。機能セット内の機能の全部ではなく一部を保護する場合は、個別の機能名を指定します。

注意： 機能セットの部分機能のうち、デフォルトで保護されている機能について、コマンドラインから保護を解除することはできません。たとえば、次のコマンドは動作しません。

```
-sf manage_security, -manage_keys
```

機能を保護する (アクセスできなくする) ことを指定するには *feature-name* を使用し、機能の保護を解除する (すべてのデータベースユーザがアクセスできるようにする) ことを指定するには *–feature-name* または *feature-name–* を使用します。たとえば、次のコマンドは、DB 領域機能にのみすべてのユーザがアクセスできることを指定します。

```
iqsrv16 -n secure_server -sf all,-dbspace
```

例

次のコマンドは、要求ログへのアクセスを許可し、すべてのリモートデータアクセス機能を保護した状態で、secure_server という名前のデータベースサーバを起動します。-sk オプションで指定したキーを、後で sp_use_secure_feature_key シス

テムプロシージャで使用することで、現在の接続のすべてのユーザがそれらの機能にアクセスできるようになります。

```
iqsrv16 -n secure_server -sf remote,-request_log -sk j978kls12
```

secure_server データベースサーバで実行中のデータベースに接続しているユーザが、sp_use_secure_feature_key システムプロシージャを使用して、-sk で指定された値と同じ値を authorization_key パラメータに設定した場合は、その接続からリモートデータアクセス機能にアクセスできます。

```
CALL sp_use_secure_feature_key ( 'MyKey' , 'j978kls12' );
```

次のコマンドは、ローカルデータベース機能を除くすべての機能を保護します。

```
iqsrv16 -n secure_server -sf all,-local_db
```

プロシージャと関数

システム情報を取得するには、SAP Sybase IQ データベースでシステム提供のストアド関数とストアドプロシージャを使用します。

sa_get_ldapserver_status システムプロシージャ

LDAP サーバ設定オブジェクトの現在のステータスを確認します。

構文
sa_get_ldapserver_status()

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。

備考

カラム名	データ型	説明
ldsrv_id	UNSIGNED BIGINT	LDAP サーバ設定オブジェクトのユニークな識別子。プライマリキーであり、ログインポリシーから LDAP サーバを参照する際に使用する。
ldsrv_name	CHAR(128)	LDAP サーバ設定オブジェクトに割り当てられている名前。

カラム名	データ型	説明
ldsrv_state	CHAR(9)	LDAP サーバの読み込み専用状態。 1 – RESET 2 – READY 3 – ACTIVE 4 – FAILED 5 – SUSPENDED 数値がシステムテーブルに格納され、対応するテキスト値がシステムビューに表示される。
ldsrv_last_state_change	TIMESTAMP	最終状態変更発生時刻を示す。LDAP サーバのローカルのタイムゾーンに関係なく、この値は協定世界時 (UTC) で格納される。

SYSLDAPSERVER のカラムの値は、チェックポイントが発生してメモリの内容がディスク上のカタログに書き込まれる前に確認します。カタログのカラム ldsrv_state と ldsrv_last_state_change の更新は、LDAP ディレクトリサーバの障害による接続の切断など、LDAP サーバオブジェクトの状態が変化するイベントが発生したために実行される LDAP サーバオブジェクトに対するチェックポイントの実行中に非同期に実行されます。LDAP サーバオブジェクトの状態には、LDAP ディレクトリサーバの状態が反映されます。

sa_get_user_status システムプロシージャ

ユーザの現在のステータスを特定できます。

構文

```
sa_get_user_status( )
```

結果セット

カラム名	データ型	説明
user_id	UNSIGNED INTEGER	ユーザを識別するユニークな番号。
user_name	CHAR(128)	ユーザの名前。
connections	INTEGER	このユーザによる現在の接続数。
failed_logins	UNSIGNED INTEGER	ユーザがログインしようとして失敗した回数。

カラム名	データ型	説明
last_login_time	TIMESTAMP	ユーザが最後にログインした現地時刻。
locked	TINYINT	ユーザアカウントがロックされているかどうかを示すインジケータ。
reason_locked	LONG VARCHAR	アカウントがロックされた理由。
user_dn	CHAR(1024)	LDAP サーバに接続しているユーザ ID の識別名 (DN)。
user_dn_cached_at	TIMESTAMP	DN が保存されたローカル時刻。
password_change_state	BIT	二重パスワードの変更が進行中であるかどうかを示す値 (0 = いいえ、1 = はい)デフォルトは 0 です。
password_change_first_user	UNSIGNED INTEGER	二重パスワードの最初の部分を設定したユーザの user_id で、それ以外の場合は NULL。
password_change_second_user	UNSIGNED INTEGER	二重パスワードの 2 番目の部分を設定したユーザの user_id で、それ以外の場合は NULL。
user_dn	CHAR(1024)	ユーザの識別名を設定します。
user_dn_cached_at	TIMESTAMP	識別名が見つかった日付と時刻。

備考
このプロシージャは、ユーザの現在のステータスを示す結果セットを返します。基本的なユーザ情報に加えて、ユーザがロックアウトされているかどうかを示すカラムや、ロックアウトの理由が格納されたカラムが含まれています。ポリシーによるロック、パスワードの有効期限超過、失敗試行回数の超過を理由として、ユーザをロックアウトできます。

LDAP ユーザ認証を使用してユーザを認証した場合、出力にユーザの識別名と、識別名が見つかった日付と時刻が含まれます。

権限
自分自身についての情報を表示できます。権限は必要ありません。他のユーザの情報を表示する場合は、MANAGE ANY USER システム権限が必要です。

関連する動作
なし。

例

次の例は、sa_get_user_status システムプロシージャを使用して、データベースユーザのステータスを返します。

```
CALL sa_get_user_status;
```

sp_create_secure_feature_key システムプロシージャ

新しいセキュリティ機能キーを作成します。

構文

```
sp_create_secure_feature_key （
    name,
    auth_key,
    features ）
```

パラメータ

- **name –** 新しいセキュリティ機能キーの VARCHAR (128) 名。この引数は、NULL または空白文字列にできません。
- **auth_key –** セキュリティ機能キーの CHAR (128) 認証キー。認証キーは、6 文字以上の空でない文字列にする必要があります。
- **features –** 新しいキーで有効にできるセキュリティ機能のカンマ区切りのリスト (LONG VARCHAR)。機能の前に "-" を指定すると、このセキュリティ機能キーを設定してもその機能は再び有効にはならないことを意味します。

権限

そのシステムプロシージャに対する EXECUTE 権限が必要です。また、データベースサーバ所有者であり、その接続に対する manage_keys 機能が有効である必要があります。

備考

このプロシージャでは、どのユーザにも設定可能な新しいセキュリティ機能が作成されます。システムセキュリティ機能キーは、-sk データベースサーバオプションを使用して作成されます。

sp_displayroles システムプロシージャ

ユーザ定義のロールまたはユーザに付与されているすべてのロールを表示するか、またはロールの階層ツリー全体を表示します。

構文

```
sp_displayroles (
   [ user_role_name ],
   [ display_mode ],
   [ grant_type ] )
```

パラメータ

- **user_role_name –** 有効な値は次のとおりです。
  - 有効なシステム権限名またはシステム権限ロール名
  - 有効なユーザ定義ロール名
  - 有効なユーザ名

  デフォルトでは、引数が指定されない場合、現在のログインユーザが使用されます。
- **display_mode –** 有効な値は次のとおりです。
  - **EXPAND_UP –** 入力されたロールまたはシステム権限が付与されているすべてのロールを表示します。これは、親レベルのロール階層ツリーです。
  - **EXPAND_DOWN –** 入力されたロールまたはユーザに付与されているすべてのロールまたはシステム権限を表示します。これは、子レベルのロール階層ツリーです。

  引数が指定されない場合 (デフォルト)、直接付与されたロールまたはシステム権限のみが表示されます。
- **grant_type –** 有効な値は次のとおりです。
  - **ALL –** 付与されているすべてのロールまたはシステム権限を表示します。
  - **NO_ADMIN –** WITH NO ADMIN OPTION 句または WITH ADMIN OPTION 句を使用して付与されているすべてのロールまたはシステム権限を表示します。
  - **ADMIN –** WITH ADMIN OPTION 句または WITH ADMIN ONLY OPTION 句を使用して付与されているすべてのロールまたはシステム権限を表示します。

  引数を指定しないと、[ALL] が使用されます。

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。 他のユーザに対してこのプロシージャを実行する場合は、MANAGE ROLES システム権限が必要です。ロールまたはシステム権限に対して実行する場合は、そのロールの管理者であるか、システム権限に対する管理権限が必要です。

備考

カラム名	データ型	説明
role_name	char(128)	ロール/システム権限の名前をリストする。

カラム名	データ型	説明
parent_role_name	char(128)	親のロール名をリストする。
grant_type	char(10)	付与タイプをリストする。
role_level	smallint	Expand_down モードの場合、1 は直接付与されたロールを示し、2 は 1 つ下の階層を示し、以下同様。 Expand_up モードの場合、0 は指定されたロールが付与されているロールを示し、-1 は 1 つ上の階層を示し、以下同様。

名前としてシステム権限名が指定された場合、結果には、システム権限ロール名ではなくシステム権限名が表示されます。

モードとして Expand_down が指定された場合、レベル 1 の parent_role_name は NULL (直接付与されたロール) です。モードが指定されない場合 (デフォルト)、直接付与されたロールのみ表示されるので、role_level は 1、parent_role_name は NULL です。

名前としてユーザ名、モードとして expand_up が指定された場合、ユーザは任意のロール階層の最上位レベルに存在するので、結果は返されません。同様に、名前として不変のシステム権限名、モードとして Expand_down が指定された場合、不変のシステム権限は任意のロール階層の最下位レベルに存在するので、結果は返されません。

デフォルトモードの場合、parent_role_name カラムは NULL、role_level は 1 です。

例

次の例では、次の GRANT 文が実行されているとします。

```
GRANT SERVER OPERATOR TO r4;
GRANT BACKUP DATABASE TO r3 WITH ADMIN OPTION;
GRANT DROP CONNECTION TO r3 WITH ADMIN ONLY OPTION;
GRANT MONITOR TO r2;GRANT CHECKPOINT TO r1;
GRANT ROLE r2 TO r1 WITH ADMIN OPTION;
GRANT ROLE r3 TO r2 WITH NO ADMIN OPTION;
GRANT ROLE r4 TO r3 WITH ADMIN ONLY OPTION;
GRANT ROLE r1 TO user1;
GRANT ROLE r1 TO r7;
GRANT ROLE r7 TO user2 WITH ADMIN OPTION;
GRANT BACKUP DATABASE TO user2 WITH ADMIN ONLY OPTION;
```

`sp_displayroles( 'user2', 'expand_down', 'ALL' )` を実行すると、次のような内容が出力されます。

role_name	parent_role_name	grant_type	role_level
r7	NULL	ADMIN	1
PUBLIC	NULL	NO ADMIN	1
BACKUP DATABASE	NULL	ADMIN ONLY	1
dbo	PUBLIC	NO ADMIN	2
r1	r7	NO ADMIN	2
r2	r1	ADMIN	3
CHECKPOINT	r1	NO ADMIN	3
r3	r2	NO ADMIN	4
MONITOR	r2	NO ADMIN	4
r4	r3	ADMIN ONLY	5
BACKUP DATABASE	r3	ADMIN	5
DROP CONNECTION	r3	ADMIN ONLY	5

`sp_displayroles( 'user2', 'expand_down', 'NO_ADMIN' )`を実行すると、次のような内容が出力されます。

role_name	parent_role_name	grant_type	role_level
r7	NULL	ADMIN	1
PUBLIC	NULL	NO ADMIN	1
dbo	PUBLIC	NO ADMIN	2
r1	r7	NO ADMIN	2
r2	r1	ADMIN	3
CHECKPOINT	r1	NO ADMIN	3
r3	r2	NO ADMIN	4
MONITOR	r2	NO ADMIN	4
BACKUP DATABASE	r3	ADMIN	5

`sp_displayroles( 'r3', 'expand_up', 'NO_ADMIN' )`を実行すると、次のような内容が出力されます。

role_name	parent_role_name	grant_type	role_level
r1	r7	NO ADMIN	-2
r2	r1	ADMIN	-1
r3	r2	NO ADMIN	0

`sp_displayroles( 'r1', 'NO_ADMIN', 'expand_up')` を実行すると、次のような内容が出力されます。

role_name	parent_role_name	grant_type	role_level
r1	r7	NO ADMIN	0

sp_expireallpasswords システムプロシージャ

すべてのパスワードをただちに有効期限切れにします。

構文 1

```
call sp_expireallpasswords
```

構文 2

```
sp_expireallpasswords
```

権限

そのシステムプロシージャに対する EXECUTE 権限に加え、次のものが必要です。
MANAGE ANY USER システム権限。

SP_HAS_ROLE 関数 [システム]

指定されたシステム権限またはユーザ定義ロールが呼び出し側ユーザに付与されているかどうかを示す整数値を返します。ユーザ定義ストアドプロシージャ内で権限チェックに使用された場合、ユーザが権限チェックに失敗すると、**SP_HAS_ROLE** はエラーメッセージを返します。

構文

dbo.sp_has_role(*[rolename], [grant_type], [throw_error]*)

パラメータ

パラメータ	説明
rolename	システム権限またはユーザ定義ロールの名前。

パラメータ	説明
grant_type	有効な値は ADMIN と NO ADMIN。NULL が指定されるか、または何も指定されない場合、NO ADMIN がデフォルトで使用される。
throw_error	有効な値： • [1] – システム権限またはユーザ定義ロールが呼び出し側ユーザに付与されていない場合、指定されたエラーメッセージを表示する。 • [0] – (デフォルト) 指定されたシステム権限またはユーザ定義ロールが呼び出し側ユーザに付与されていない場合、エラーメッセージを表示しない。

戻り値

値	説明
1	システム権限またはユーザ定義ロールは呼び出し側ユーザに付与されている。
0 またはパーミッションがありません：このコマンド／プロシージャを実行するためのパーミッションがありません。	システム権限またはユーザ定義ロールは呼び出し側ユーザに付与されていない。throw_error 引数が 1 に設定されている場合は、値 0 の代わりにエラーメッセージが返される。
-1	指定されたシステム権限またはユーザ定義ロールが存在しない。throw_error 引数が 1 に設定されている場合でも、エラーメッセージは表示されない。

備考

grant_type 引数の値が ADMIN である場合、この関数は、呼び出し側ユーザがシステム権限の管理権限を持っているかどうかをチェックします。grant_type 引数の値が NO ADMIN である場合、この関数は、呼び出し側ユーザがシステム権限またはロールを使用する権限を持っているかどうかをチェックします。

grant_type 引数が指定されていない場合、デフォルトで NO ADMIN が使用され、出力は、指定されたシステム権限またはユーザ定義ロールが直接的または間接的に呼び出し側ユーザに付与されているかどうかのみを示します。

rolename と grant_type の両方の引数が NULL で、throw_error 引数が 1 である場合、エラーメッセージが表示されます。この処理は、呼び出し側ユーザの

特定のシステム権限の存在をチェックした後ではなく、カタログテーブルから特定の値を読み込んだ後にエラーメッセージを表示するようなストアドプロシージャの場合に役に立つ可能性があります。

注意： 引数 rolename と grant_type が NULL、throw_error が 1 に設定されている場合、またはこれら 3 つの引数がすべて NULL に設定されている場合は、パーミッションがないというエラーメッセージが返されます。

例
次のシナリオを検討します。

- u1 は、WITH NO ADMIN OPTION 句を使用して CREATE ANY PROCEDURE システム権限が付与されている。
- u1 は、CREATE ANY TABLE システム権限を付与されていない。
- u1 は、WITH ADMIN ONLY OPTION 句を使用してユーザ定義ロール Role_A が付与されている。
- Role_B は存在するが、u1 には付与されていない。
- ロール Role_C は存在しない。

このシナリオにもとづいて、次の各コマンドを実行します。

- `sp_has_role 'create any procedure'`

  値 1 を返します。これは、u1 に CREATE ANY PROCEDURE システム権限が付与されていることを示します。
- `sp_has_role 'create any table'`

  値 0 を返します。これは、u1 に CREATE ANY TABLE システム権限が付与されていないことを示します。throw_error 引数は指定されていないので、エラーメッセージは返されません。
- `sp_has_role 'create any procedure','admin',1`

  「Permission denied」エラーメッセージを返します (throw_error=1)。u1 に CREATE ANY PROCEDURE システム権限は付与されていますが、それに対する管理権限は u1 には付与されていません。
- `sp_has_role 'Role_A'`

  値 1 を返します。これは、u1 にロール Role_A が付与されていることを示します。
- `sp_has_role 'Role_A','admin',1`

  値 1 を返します。これは、u1 にロール Role_A が管理権限付きで付与されていることを示します。
- `sp_has_role 'Role_B'`

値 0 を返します。これは、u1 にロール ROLE_B が付与されていないことを示します。throw_error 引数は指定されていないので、エラーメッセージは返されません。

- `sp_has_role 'Role_C'`

  値 -1 を返します。これは、ロール ROLE_C が存在しないことを示します。
- `sp_has_role 'Role_C',NULL,1`

  値 -1 を返します。これは、ロール ROLE_C が存在しないことを示します。

sp_iqaddlogin プロシージャ

新しい SAP Sybase IQ ユーザアカウントを指定のログインポリシーに追加します。

構文 1

```
call sp_iqaddlogin ('username_in', 'pwd' [,
'password_expiry_on_next_login'] [, 'policy_name'] )
```

構文 2

```
sp_iqaddlogin 'username_in', 'pwd' [, 'password_expiry_on_next_login']
[, 'policy_name']
```

構文 3

```
sp_iqaddlogin  username_in, pwd [, password_expiry_on_next_login] [,
policy_name]
```

パラメータ

- **username_in –** ユーザのログイン名。ログイン名は識別子の規則に従う必要があります。
- **pwd –** ユーザのパスワード。パスワードは、パスワード規則に準拠する必要があります。つまり、有効な識別子である必要があります。
- **password_expiry_on_next_login –** (オプション) ユーザのログインが作成されたらすぐに、ユーザのパスワードを失効させるかどうかを指定します。デフォルトの設定は OFF です (パスワードに有効期限はありません)。
- **policy_name –** (オプション) 指定のログインポリシーの下にユーザを作成します。指定しないと、ルートログインポリシーの下にユーザが作成されます。

sp_iqaddlogin を使って作成し、1 日で有効期限が切れるように設定した *username_in/pwd* は、翌日は終日有効であり、翌々日に無効になります。つまり、ログインを今日作成し、 *n* 日で有効期限が切れるように設定した場合、日付が *(n +1)* 日目になると使用できなくなります。

権限
そのシステムプロシージャに対する EXECUTE 権限に加え、次のものが必要です。
MANAGE ANY USER システム権限

備考
新しい SAP Sybase IQ ユーザアカウントを追加し、ログインポリシーをユーザに割り当てて、ユーザを ISYSUSER システムテーブルに追加します。ユーザがすでにそのデータベースのユーザ ID を持っているが、`ISYSUSER` 内に登録されていない場合 (**GRANT CONNECT** 文または SAP Control Center によってユーザ ID が追加された場合など) は、**sp_iqaddlogin** によってユーザがテーブルに追加されます。

SAP Sybase IQ では、プロシージャを呼び出すときにログインポリシー名を指定しないと、ユーザがルートログインポリシーに割り当てられます。

注意： ログインポリシーに対する最大ログイン数が無制限の場合、そのログインポリシーに属するユーザが持つことができる接続は無制限になります。

最初のユーザログインでは、パスワードの変更が強制され、ログインポリシーが新しく作成されたユーザに割り当てられます。新しいユーザの作成には **CREATE USER** が使用されますが、下位互換性保持のため、**sp_iqaddlogin** も引き続きサポートされます。

例
この呼び出しでは、パスワード `irk324` を持つユーザ `rose` が `expired_password` というログインポリシーに追加されます。この例では、expired_password ログインポリシーがすでに存在しているものとします。

```
call sp_iqaddlogin('rose', 'irk324', 'ON', 'expired_password')
```

```
sp_iqaddlogin 'rose','irk324', 'ON', 'expired_password'
```

sp_iqbackupdetails プロシージャ

特定のバックアップに含まれるすべての dbfile を表示します。

構文
sp_iqbackupdetails *backup_id*

パラメータ
- **backup_id –** バックアップ操作のトランザクション識別子を指定します。

注意： 次のクエリを実行すると、`SYSIQBACKUPHISTORY` テーブルから backup_id 値を取得できます。

```
select * from sysiqbackuphistory
```

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。

備考
sp_iqbackupdetails は、次の値を返します。

表 15 : sp_iqbackupdetails のカラム

カラム名	説明
backup_id	バックアップトランザクションの識別子。
backup_time	バックアップの時間。
backup_type	バックアップの種類："Full"、"Incremental since incremental"、または "Incremental since full"。
selective_type	バックアップのサブタイプ ("All inclusive"、"All RW files in RW dbspaces"、"Set of RO dbspace/file")。
depends_on_id	バックアップが依存する以前のバックアップの識別子。
dbspace_id	バックアップされる DB 領域の識別子。
dbspace_name	SYSIQBACKUPHISTORYDETAIL からの DB 領域の名前。DB 領域名が、指定の dbspace_id の SYSDBSPACE の DB 領域名と一致する場合。それ以外の場合は "null"。
dbspace_rwstatus	"ReadWrite" または "Read Only"。
dbspace_createid	DB 領域作成トランザクション識別子。
dbspace_alterid	Alter DBSPACE 読み込み／書き込みモードトランザクション識別子。
dbspace_online	ステータス "Online" または "Offline"。
dbspace_size	バックアップ時の DB 領域のサイズ (キロバイト)。
dbspace_backup_size	DB 領域でのバックアップ時のデータのサイズ (キロバイト)。
dbfile_id	バックアップされる dbfile の識別子。
dbfile_name	バックアップ操作後に名前が変更されなかった場合は、論理ファイル名。変更された場合は "null"。
dbfile_rwstatus	"ReadWrite" または "Read Only"。

カラム名	説明
dbfile_createid	dbfile 作成トランザクション識別子。
dbfile_alterid	Alter DBSPACE alter FILE 読み込み／書き込みモードトランザクション識別子。
dbfile_size in MB	dbfile のサイズ (メガバイト)。
dbfile_backup_size	dbfile バックアップのサイズ (キロバイト)。
dbfile_path	指定された dbspace_id および dbfile_id の SYSDBFILE の物理ファイルパス ("file_name") と一致する場合は、SYSBACKUPDETAIL からの dbfile パス。それ以外の場合は "null"。

例

sp_iqbackupdetails の出力例を次に示します。

```
backup_id   backup_time             backup_type   selective_type   d
epends_on_id
      883   2008-09-23 13:58:49.0   Full          All
inclusive                0

dbspace_id   dbspace_name   dbspace_rwstatus   dbspace_createid
         0   system         ReadWrite                         0

dbspace_alterid   dbspace_online dbspace_size dbspace_backup_size
dbfile_id
              0              0        2884              2884        0

dbfile_name dbfile_rwstatus dbfile_createid dbfile_alterid
dbfile_size
     system       ReadWrite               0              0      2884

dbfile_backup_size dbfile_path
             2884  C:¥¥Documents and Settings¥¥All Users¥¥SybaseIQ¥
¥demo¥¥iqdemo.db
```

sp_iqbackupsummary プロシージャ

実行されたバックアップ操作の概要を示します。

構文

sp_iqbackupsummary [*timestamp or backup_id*]

パラメータ

- **timestamp または backup_id** – バックアップ操作をレポートする間隔を指定します。タイムスタンプまたはバックアップ ID を指定した場合、指定した時間に等しいか、それより大きい backup_time を持つレコードのみが返されます。タ

イムスタンプを指定しない場合、ISYSIQBACKUPHISTORY のすべてのバックアップレコードが返されます。

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。

備考

表 16 : sp_iqbackupsummary のカラム

カラム名	説明
backup_id	バックアップトランザクションの識別子
backup_time	バックアップの時間
backup_type	バックアップの種類："Full"、"Incremental since incremental"、または "Incremental since full"。
selective_type	バックアップのサブタイプ ("All Inclusive"、"All RW files in RW dbspaces"、"Set of RO dbspace/file")。
virtual_type	仮想バックアップの種類："Non-virtual"、"Decoupled"、または "Encapsulated"。
depends_on_id	バックアップが依存するバックアップの識別子
creator	バックアップの作成者
backup_size	バックアップのサイズ (キロバイト)
user_comment	ユーザコメント
backup_command	発行された backup 文 (コメントなし)

例
sp_iqbackupsummary の出力例を次に示します。

```
backup_id   backup_time             backup_type   selective_type   v
irtual_type
      883   2008-09-23 13:58:49.0   Full          All inclusive    Non
virtual

depends_on_id   creator   backup_size   user_comment   backup_command
            0   DBA              10864                backup database to
                                                          'c:¥¥¥¥temp
¥¥¥¥b1'
```

sp_iqconnection プロシージャ

接続およびバージョンについての情報を表示します。この情報には、テンポラリ DB 領域を使用しているユーザ、バージョンを有効にしているユーザ、各接続が SAP Sybase IQ 内で行っている作業、接続ステータス、データベースバージョンステータスなどが含まれます。

構文

```
sp_iqconnection [ connhandle ]
```

適用対象

シンプレックスとマルチプレックス。

権限

そのシステムプロシージャに対する EXECUTE 権限が必要です。 さらに、次のいずれかが必要です。 システム権限：

- DROP CONNECTION
- MONITOR
- SERVER OPERATOR

備考

connhandle は、`Number` 接続プロパティに等しい、接続の ID 番号です。 **connection_property** システム関数は、次のように接続 ID を返します。

```
SELECT connection_property ( 'Number' )
```

有効な *connhandle* の入力パラメータで呼び出されると、**sp_iqconnection** はその接続に対応する 1 つのローのみを返します。

sp_iqconnection は、有効な各接続に対して 1 つのローを返します。ConnHandle、Name、Userid、LastReqTime、ReqType、CommLink、NodeAddr、LastIdle の各カラムは、Number、Name、Userid、LastReqTime、ReqType、CommLink、NodeAddr、LastIdle の各接続プロパティにそれぞれ対応しており、システム関数 **sa_conn_info** と同じ値を返します。追加のカラムは、SAP Sybase IQ エンジンの SAP Sybase IQ 側から接続データを返します。ローは、ConnCreateTime の順で並べられます。

MPXServerName カラムには、次の表に示すようにノード間通信 (INC) に関連する情報が格納されています。

実行されているサーバ	MPXServerName カラムの内容
シンプレックスサーバ	NULL (すべての接続がローカル／ユーザ接続)。
マルチプレックスコーディネータ	• ローカル／ユーザ接続の場合は NULL。 • 各 INC 接続 (オンデマンド接続または専用ハートビート接続のいずれか) のセカンダリノードのサーバ名 (接続元) の値を含む。
マルチプレックスセカンダリ	• ローカル／ユーザ接続の場合は NULL。 • コーディネータのサーバ名 (接続元) の値を含む。

Java アプリケーションでは、TDS クライアントから SAP Sybase IQ 固有の接続プロパティを RemotePWD フィールドで指定します。次の例は、IQ 固有の接続パラメータの指定方法を示します。**myconnection** は IQ 接続名です。

```
p.put("RemotePWD",",,CON=myconnection");
```

カラム名	説明
ConnHandle	接続の ID 番号。
ConnectionName	パラメータで指定される接続名。
Userid	接続のユーザ ID。
LastReqTime	指定された接続に対する直前の要求が開始された時刻。
ReqType	最後の要求のタイプを示す文字列。
IQCmdType	SAP Sybase IQ 側で現在実行されているコマンド (存在する場合)。コマンドの種類には、エンジンの実装レベルで定義されたコマンドが反映される。これらのコマンドは、トランザクションコマンド、IQ ストア内のデータを対象とした DDL および DML コマンド、内部 IQ カーソルコマンド、特殊な制御コマンド (**OPEN** と **CLOSE**、**BACKUP DATABASE**、**RESTORE DATABASE** など) で構成される。
LastIQCmdTime	この接続の SAP Sybase IQ エンジンの IQ 側で最後の IQ コマンドが開始または完了した時刻。
IQCursors	この接続の IQ ストアでオープンしているカーソルの数。

カラム名	説明
LowestIQCursorState	IQ カーソルの状態 (存在する場合)。接続に複数のカーソルがある場合、すべてのカーソルの中で最小のカーソル状態、つまり完了までの時間が最も長いものが表示される。カーソル状態は内部の SAP Sybase IQ 実装の詳細を反映するもので、将来的に変更される可能性がある。このバージョンのカーソル状態は、NONE、INITIALIZED、PARSED、DESCRIBED、COSTED、PREPARED、EXECUTED、FETCHING、END_OF_DATA、CLOSED、および COMPLETED。名前からもわかるように、カーソル状態は操作の最後に変更される。たとえば、状態 PREPARED は、カーソルが実行中であることを示す。
IQthreads	現在、接続に割り当てられている SAP Sybase IQ スレッドの数。割り当て済みのスレッドでも、アイドルである可能性がある。このカラムから、どの接続がリソースを最も多く使用しているかを判断できる。
TxnID	接続の現在のトランザクションのトランザクション ID。この ID は、BeginTxn、CmtTxn、および PostCmtTxn メッセージによって `.iqmsg` ファイルに表示されるトランザクション ID、また、データベースが開かれたときにログ記録される Txn ID Seq と同じである。
ConnCreateTime	接続が作成された時刻。
TempTableSpaceKB	この接続が IQ テンポラリテーブルに格納されているデータに使用している IQ テンポラリストアの領域 (KB 単位)。
TempWorkSpaceKB	この接続が、ソート、ハッシュ、テンポラリビットマップなどの作業領域として使用している IQ テンポラリストアの領域 (KB 単位)。ビットマップや、SAP Sybase IQ テンポラリテーブルのインデックスの一部分であるその他のオブジェクトによって使用されている領域は、TempTableSpaceKB に反映される。
IQConnID	`.iqmsg` ファイル内のすべてのメッセージの一部として含まれている 10 桁の接続 ID。これは、サーバセッション内でユニークな、単純増加する整数である。
satoiq_count	SAP Sybase IQ エンジンの SQL Anywhere 側から IQ 側への超過の数の表示に使用される内部カウンタ。これは、接続のアクティビティを確認するのに役立つ場合がある。結果セットはローのバッファに返され、satoiq_count や iqtosa_count がローごとに 1 回増分することはない。
iqtosa_count	SAP Sybase IQ エンジンの IQ 側から SQL Anywhere 側への超過の数の表示に使用される内部カウンタ。これは、接続のアクティビティを確認するのに役立つ場合がある。

カラム名	説明
CommLink	接続用の通信リンク。これは、SAP Sybase IQ がサポートするネットワークプロトコルのいずれかで、同一マシン接続の場合は「local」になる。
NodeAddr	クライアント／サーバ接続のクライアント側に対応するノード。
LastIdle	要求間のチックの数。
MPXServerName	INC 接続の場合、varchar(128) 値には、INC 接続を開始したマルチプレックスサーバの名前が含まれる。INC 接続でない場合は NULL になる。
LSName	接続の論理サーバ名。論理サーバのコンテキストが未知または適用不可の場合、NULL となる。
INCConnName	ユーザ接続の基礎となる INC 接続の名前。このカラムのデータ型は varchar(255)。**sp_iqconnection** でサスペンドされたユーザ接続の INC 接続名が表示される場合、そのユーザ接続にはサスペンドされた関連 INC 接続も存在する。
INCConnSuspended	このカラムの値 "Y"は、ユーザ接続の基礎となる INC 接続がサスペンド状態であることを示す。値 "N" は、接続がサスペンドされていないことを示す。

例

sp_iqconnection

```
ConnHandle      Name    Userid                 LastReqTime   ReqType
=== ================== ======  ==========================   =======
 1  'SQL_DBC_100525210' 'DBA'   '2011-03-28  09:29:24.466'  'OPEN'


           IQCmdType    LastIQCmdTime      IQCursors  LowestIQCursorState
====================    ==============     =========  ===================
'IQUTILITYOPENCURSOR'  2011-03-28 09:29:24.0       0             'NONE'


IQthreads   TxnID          ConnCreateTime TempTableSpaceKB TempWorkSpaceKB
=========  =======  =====================  =============== ===============
        0  3352568  2011-03-28 09:29:20.0                0           0


IQconnID satoiq_count iqtosa_count CommLink NodeAdd LastIdle MPXServerName
======== ============ ============ ======== ======= ======== ============
      34           43           2  'local'      ''      244  (NULL)

LSName      INCConnName                  INCConnSuspended
==========  ===================          ================
Finance_LS  'IQ_MPX_SERVER_P54'          'Y'
```

sp_iqcopyloginpolicy プロシージャ

既存のログインポリシーをコピーして、新しいログインポリシーを作成します。

構文 1

```
call sp_iqcopyloginpolicy ('existing-policy-name', 'new-policy-name' )
```

構文 2

```
sp_iqcopyloginpolicy 'existing-policy-name', 'new-policy-name'
```

パラメータ

- **existing-policy-name –** コピーするログインポリシー。
- **new-policy-name –** 作成する新しいログインポリシーの名前 (CHAR(128))。

権限
そのシステムプロシージャに対する EXECUTE 権限に加え、次のものが必要です。 MANAGE ANY LOGIN POLICY システム権限。

例
root という既存のログインポリシーからログインポリシーオプション値をコピーして、*lockeduser* という名前の新しいログインポリシーを作成します。

```
call sp_iqcopyloginpolicy ('root','lockeduser')
```

sp_iqdbspace プロシージャ

各 SAP Sybase IQ DB 領域についての詳細情報を表示します。

構文

```
sp_iqdbspace [ dbspace-name ]
```

適用対象
シンプレックスとマルチプレックス。

権限
MANAGE ANY DBSPACE システム権限。そのシステムプロシージャに対する EXECUTE 権限に加え、次のものが必要です。

備考
sp_iqdbspace の情報は、データを移動する必要があるかどうかの判断に、また移動されたデータについては旧バージョンの割り付けが解除されているかどうかの判定に使用されます。

カラム名	説明
DBSpaceName	**CREATE DBSPACE** 文で指定された DB 領域の名前。**CREATE DATABASE...CASE IGNORE** または **CASE RESPECT** の指定に関係なく、DB 領域名は常に大文字と小文字が区別されない。
DBSpaceType	DB 領域のタイプ (MAIN、SHARED_TEMP、TEMPORARY、RLV、または CACHE)。
Writable	T (書き込み可能) または F (書き込み不可)。
Online	T (オンライン) または F (オフライン)。
Usage	DB 領域のすべてのファイルで現在使用されている DB 領域の割合。
TotalSize	DB 領域のすべてのファイルの合計サイズ。単位は、B (バイト)、K (キロバイト)、M (メガバイト)、G (ギガバイト)、T (テラバイト)、または P (ペタバイト)。
Reserve	DB 領域のすべてのファイルに追加できる予約領域の合計。
NumFiles	DB 領域内のファイルの数。
NumRWFiles	DB 領域内の読み込み／書き込みファイルの数。
Stripingon	F (オフ)。
StripeSize	ディスクストライピングの有効化時は、常に 1。
BlkTypes	ユーザデータと内部システム構造が使用している領域。
OkToDrop	DB 領域を削除できる場合は "Y"、それ以外の場合は "N"。

BlkTypes カラムのブロックタイプ識別子の値は、次のとおりです。

識別子	ブロックタイプ
A	アクティブなバージョン
B	バックアップ構造
C	チェックポイントログ
D	データベースの識別情報
F	フリーリスト
G	グローバルフリーリストマネージャ
H	フリーリストのヘッダブロック

識別子	ブロックタイプ
I	インデックスアドバイスの格納
M	マルチプレックス CM*
O	旧バージョン
R	RLV フリーリストマネージャ
T	テーブルの使用
U	インデックスの使用
N	カラムの使用
X	チェックポイントでの削除

*マルチプレックスコミット ID ブロック (実際は 128 ブロック) は、シンプレックスデータベースで使用されていない場合でも、すべての IQ データベースに存在します。

例
DB 領域に関する情報を表示します。

```
sp_iqdbspace;
```

注意： 出力内容をわかりやすくするため、次の例は `iqdemo` データベース内のオブジェクトを示しています。`iqdemo` には `iq_main` というサンプルのユーザ DB 領域が含まれていますが、この領域はユーザ独自のデータベースには存在しない場合があります。

DBSpaceName	DBSpaceType	Writable
IQ_MAIN	MAIN	T
IQ__ SYSTEM_ MAIN	MAIN	T
IQ_SYSTEM_ TEMP	TEMPORARY	T
myDas	CACHE	T

(続き) Online	Usage	DBSpaceName
T	55	IQ_MAIN
T	21	IQ__ SYSTEM_ MAIN

(続き) Online	Usage	DBSpaceName
T	1	IQ_SYSTEM_ TEMP
T	1	myDas

(続き) Reserve	NumFiles	NumRWFiles
200M	1	1
50M	1	1
50M	1	1
0B	5	5

(続き) DBSpaceName	Stripingon	Stripe Size
IQ_MAIN	T	1K
IQ__ SYSTEM_ MAIN	F	8K
IQ_SYSTEM_ TEMP	F	8K
myDas	T	1K

(続き) Blk Types	OkTo Drop
1H, 5169A, 190	N
1H, 7648F, 32D, 128M	N
1H, 64F, 32A	N
5, 192FH	Y

sp_iqdbspaceinfo プロシージャ

指定のテーブルで使用される各オブジェクトおよびサブオブジェクトのサイズを表示します。RLV DB 領域はサポートされていません。

構文

```
sp_iqdbspaceinfo [ dbspace-name ] [ , owner_name ] [ ,
object_name ] [ , object-type  ]
```

パラメータ

すべてのパラメータがオプションであり、どのパラメータも他のパラメータの値に依存することなく指定できます。

- **dbspace_name –** 指定した場合、**sp_iqdbspaceinfo** は、指定の DB 領域内のコンポーネントを持つ各テーブルを 1 行ごとに表示します。指定しない場合、このプロシージャはデータベース内のすべての DB 領域の情報を表示します。
- **owner_name –** オブジェクトの所有者。指定した場合、**sp_iqdbspaceinfo** は、指定の所有者のテーブルのみの出力を表示します。指定しない場合、**sp_iqdbspaceinfo** は、データベース内のすべてのユーザのテーブルに関する情報を表示します。
- **object_name –** テーブルの名前。指定しない場合、**sp_iqdbspaceinfo** は、データベース内のすべてのテーブルに関する情報を表示します。
- **object_type –** 有効な **table** オブジェクト。

sp_iqdbspaceinfo ストアドプロシージャでは、*dbspace_name*、*object_name*、および *owner_name* の解釈に、ワイルドカード文字がサポートされています。これは、**LIKE** 句がクエリ内のパターンを照合するのと同じ方法で、指定のパターンと一致するすべての DB 領域の情報を表示します。

適用対象

シンプレックスとマルチプレックス。

権限

そのシステムプロシージャに対する EXECUTE 権限が必要です。 さらに、次のいずれかが必要です。 システム権限：

- BACKUP DATABASE
- SERVER OPERATOR
- MANAGE ANY DBSPACE

備考

RLV DB 領域を指定した場合、このプロシージャは結果を返しません。

sp_iqdbspaceinfo は、各 DB 領域に存在するオブジェクトによって使用される領域量を DBA に示します。DBA はこの情報を使用して、DB 領域を削除する前に移動

する必要のあるオブジェクトを判断できます。サブオブジェクトカラムには、整数の量でレポートされるサイズが表示されます。各値の後ろには、サフィックス B、K、M、G、T、または P が付き、これらはそれぞれバイト、キロバイト、メガバイト、ギガバイト、テラバイト、およびペタバイトを表します。

テーブルの場合、**sp_iqdbspaceinfo** は、すべてのサブオブジェクトのサイジング情報を表示します (サフィックス B、K、M、G、T、または P を持つ整数の量を使用します)。この情報は、*dbspace_name*、*object_name*、および *owner_name* でソートされます。

表 17 : sp_iqdbspaceinfo のカラム

カラム名	説明
dbspace_name	DB 領域の名前。
object_type	オブジェクトのタイプ (**table** または **joinindex** のみ)。
owner	オブジェクトの所有者の名前。
object_name	DB 領域にあるオブジェクトの名前。
object_id	オブジェクトのグローバルオブジェクト ID。
id	オブジェクトのテーブル ID。
columns	指定の DB 領域のカラム記憶領域のサイズ。
indexes	指定の DB 領域のインデックス記憶領域のサイズ。システムで生成されたインデックス (一意性制約の HG インデックス、FP インデックスなど) は使用できない。
metadata	指定の DB 領域のメタデータオブジェクトの記憶領域サイズ。
primary_key	指定の DB 領域のプライマリキー関連オブジェクトの記憶領域サイズ。
unique_constraint	指定の DB 領域の一意性制約関連オブジェクトの記憶領域サイズ。
foreign_key	指定の DB 領域の外部キー関連オブジェクトの記憶領域サイズ。
dbspace_online	DB 領域がオンライン (**Y**) か、オフライン (**N**) かを示す。

-r スイッチ (読み込み専用) で起動したサーバに対して sp_iqdbspaceinfo を実行すると、「`Msg 13768, Level 14, State 0: SQL Anywhere Error -757: Modifications not permitted for read-only database`」というエラーが表示されます。これは予期された動作です。`sp_iqdbspace`、`sp_iqfile`、`sp_iqdbspaceobjectinfo`、`sp_iqobjectinfo` などの他のストアドプロシージャでは、このエラーは発生しません。

例

注意： 出力内容をわかりやすくするため、次の例は iqdemo データベース内のオブジェクトを示しています。iqdemo には iq_main というサンプルのユーザ DB 領域が含まれていますが、この領域はユーザ独自のデータベースには存在しない場合があります。

データベース内のすべての DB 領域のすべてのテーブルにあるすべてのオブジェクトおよびサブオブジェクトのサイズを表示します。

```
sp_iqdbspaceinfo
```

```
dbspace_name    object_type  owner   object_name     object_id  id
  columns
iq_main        table       DBA     emp1            3689     741   96K
iq_main        table       DBA     iq_dummy        3686     740   24K
iq_main        table       DBA     sale            3698     742   96K
iq_main         table        GROUPO  Contacts          3538     732
   288K
iq_main         table        GROUPO  Customers         3515     731
   240K
iq_main        table       GROUPO  Departments     3632     738   72K
iq_main         table        GROUPO  Employees         3641     739
   408K
iq_main         table        GROUPO  FinancialCodes    3612     736
   72K
iq_main        table       GROUPO  FinancialData    3621     737   96K
iq_main         table        GROUPO  Products
 3593     735   272K
iq_main         table        GROUPO  SalesOrderItems   3580     734
   120K
iq_main         table        GROUPO  SalesOrders       3565     733
   144K

indexes  metadata  primary_key  unique_constraint  foreign_key  dbsp
ace_online
0B       1.37M     0B           0B                 0B           Y
0B       464K      0B           0B                 0B           Y
0B       1.22M     0B           0B                 0B           Y
0B       5.45M     24K          0B                 48K          Y
48K      4.63M     24K          0B                 0B           Y
0B       1.78M     24K          0B                 48K          Y
0B       8.03M     24K          0B                 48K          Y
0B       1.53M     24K          0B                 0B           Y
0B       2.19M     24K          0B                 48K          Y
192K     4.67M     24K          0B                 0B           Y
0B       2.7M      24K          0B                 104K         Y
0B       3.35M     24K          0B                 144K         Y
```

データベース内の指定 DB 領域に指定ユーザが所有する、すべてのオブジェクトおよびサブオブジェクトのサイズを表示します。

```
sp_iqdbspaceinfo iq_main,GROUPO
```

```
dbspace_name    object_type  owner   object_name     object_id  id
  columns
iq_main         table        GROUPO  Contacts          3538     732
   288K
iq_main         table        GROUPO  Customers         3515     731
   240K
iq_main        table       GROUPO  Departments      3632    738   72K
iq_main         table        GROUPO  Employees         3641     739
   408K
iq_main         table        GROUPO  FinancialCodes    3612     736
   72K
iq_main        table       GROUPO  FinancialData    3621    737   96K
iq_main         table        GROUPO  Products          3593     735
   272K
iq_main         table        GROUPO  SalesOrderItems   3580     734
   120K
iq_main         table        GROUPO  SalesOrders       3565     733
   144K

indexes  metadata  primary_key  unique_constraint  foreign_key  dbsp
ace_online
0B       5.45M     24K          0B                 48K          Y
48K      4.63M     24K          0B                 0B           Y
0B       1.78M     24K          0B                 48K          Y
0B       8.03M     24K          0B                 48K          Y
0B       1.53M     24K          0B                 0B           Y
0B       2.19M     24K          0B                 48K          Y
192K     4.67M     24K          0B                 0B           Y
0B       2.7M      24K          0B                 104K         Y
0B       3.35M     24K          0B                 144K         Y
```

データベース内の指定 DB 領域に指定ユーザが所有する、指定のオブジェクトとそのサブオブジェクトのサイズを表示します。

```
sp_iqdbspaceinfo iq_main,GROUPO,Departments
```

```
dbspace_name    object_type  owner   object_name     object_id  id
  columns
iq_main        table       GROUPO  Departments      3632    738   72K

indexes  metadata  primary_key  unique_constraint  foreign_key  dbsp
ace_online
0B       1.78M     24K          0B                 48K          Y
```

sp_iqdbspaceobjectinfo プロシージャ

指定の DB 領域のテーブルタイプのオブジェクトとそのサブオブジェクト (カラム、インデックス、メタデータ、プライマリキー、一意性制約、外部キー、およびパーティション) をリストします。RLV DB 領域はサポートされていません。

構文

sp_iqdbspaceobjectinfo [*dbspace-name*] [, *owner_name*] [, *object_name*] [, *object-type*]

パラメータ
すべてのパラメータがオプションであり、どのパラメータも他のパラメータの値とは関係なく指定できます。

- **dbspace-name –** 指定した場合、**sp_iqdbspaceobjectinfo** は、指定の DB 領域についてのみ出力を表示する。指定しない場合、データベース内のすべての DB 領域の情報を表示します。
- **owner-name –** オブジェクトの所有者。指定した場合、**sp_iqdbspaceobjectinfo** は、指定の所有者のテーブルのみの出力を表示します。指定しない場合、**sp_iqdbspaceobjectinfo** は、データベース内のすべてのユーザのテーブルの情報を表示する。
- **object-name –** テーブルの名前。指定しない場合、**sp_iqdbspaceobjectinfo** は、データベース内のすべてのテーブルの情報を表示します。
- **object-type – table** オブジェクトの有効なオブジェクトタイプ。

sp_iqdbspaceobjectinfo ストアドプロシージャでは、*dbspace_name*、*object_name*、および *owner_name* の解釈に、ワイルドカード文字がサポートされています。これは、**LIKE** 句がクエリ内のパターンを照合するのと同じ方法で、指定のパターンと一致するすべての DB 領域の情報を表示します。

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。

備考
RLV DB 領域を指定した場合、このプロシージャは結果を返しません。

テーブルの場合、**sp_iqdbspaceobjectinfo** は、関連するすべてのサブオブジェクトの要約情報を dbspace_name および owner and object_name でソートして表示します。

sp_iqdbspaceobjectinfo は、入力パラメータ値に基づいて次の情報を表示します。

表 18 : sp_iqdbspaceobjectinfo のカラム

カラム名	説明
dbspace_name	DB 領域の名前。
dbspace_id	DB 領域の識別子。
object_type	テーブル。
owner	オブジェクトの所有者の名前。
object_name	DB 領域にあるテーブルオブジェクトの名前。

カラム名	説明
object_id	オブジェクトのグローバルオブジェクト ID。
id	オブジェクトのテーブル ID。
columns	指定の DB 領域にあるテーブルカラムの数。カラム、またはいずれかのカラムパーティションが DB 領域にある場合、その DB 領域に存在しているものとして数えられる。結果は n/N フォームで表示される (テーブルの合計 N 個のカラムのうち n 個が指定された DB 領域に存在)。
indexes	指定の DB 領域にあるテーブルのユーザ定義インデックスの数。n/N フォームで表示される (テーブル上の合計 N 個のインデックスのうち n 個が指定された DB 領域に存在)。一意性制約の場合、FP インデックスや HG インデックスなどのシステム作成のインデックスは含まない。
metadata	サブオブジェクトのメタデータ情報もこの DB 領域にあるかどうかを示すブールフィールド (Y/N)。
primary_key	テーブルのプライマリキー (存在する場合) がこの DB 領域にあるかどうかを示すブールフィールド (1/0)。
unique_constraint	指定の DB 領域にあるテーブルの一意性制約の数。n/N フォームで表示される (テーブル上の合計 N 個の一意性制約のうち n 個が指定された DB 領域に存在)。
foreign_key	指定の DB 領域にあるテーブルの外部キーの数。n/N フォームで表示される (テーブル上の合計 N 個の外部キーのうち n 個が指定された DB 領域に存在)。
partitions	指定の DB 領域にあるテーブルのパーティションの数。n/N フォームで表示される (テーブルの合計 N 個のパーティションのうち n 個が指定された DB 領域に存在)。

例

出力内容をわかりやすくするため、次の例は `iqdemo` データベース内のオブジェクトを示しています。`iqdemo` には `iq_main` というサンプルのユーザ DB 領域が含まれていますが、この領域はユーザ独自のデータベースには存在しない場合があります。

データベース内の特定の DB 領域に関する情報を表示します。

```
sp_iqdbspaceobjectinfo iq_main
```

```
dbspace_name  dbspace_id object_type  owner   object_name  object_id  id  columns
```

```
iq_main       16387      table        DBA     emp1           3689
   741  4/4
iq_main       16387      table        DBA     iq_dummy       3686
   740  1/1
iq_main       16387      table        DBA     sale           3698
   742  4/4
iq_main       16387      table        GROUPO  Contacts       3538
   732  12/12
iq_main       16387      table        GROUPO  Customers      3515
   731  10/10
iq_main       16387      table        GROUPO  Departments    3632
   738  3/3
iq_main       16387      table        GROUPO  Employees      3641
   739  21/21
iq_main       16387      table        GROUPO  FinancialCodes 3612
   736  3/3
iq_main       16387      table        GROUPO  FinancialData  3621
   737  4/4
iq_main       16387      table        GROUPO  Products       3593
   735  8/8
iq_main       16387      table        GROUPO  SalesOrderItems3580
   734  5/5
iq_main       16387      table        GROUPO  SalesOrders    3565
   733  6/6

indexes  metadata  primary_key  unique_constraint  foreign_key  part
itions
0/0      Y                   0  0/0                0/0          0/0
0/0      Y                   0  0/0                0/0          0/0
0/0      Y                   0  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
1/1      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
0/0      Y                   1  0/0                1/1          0/0
0/0      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
4/4      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                2/2          0/0
0/0      Y                   1  0/0                3/3          0/0
```

データベース内で指定した DB 領域の指定ユーザが所有するオブジェクトに関する情報を表示します。

```
sp_iqdbspaceobjectinfo iq_main,GROUPO
```

```
dbspace_name  dbspace_id object_type  owner   object_name    object_
id  id  columns
iq_main       16387      table        GROUPO  Contacts       3538
     732 2/12
iq_main       16387      table        GROUPO  Customers      3515
     731 10/10
iq_main       16387      table        GROUPO  Departments    3632
     738 3/3
iq_main       16387      table        GROUPO  Employees      3641
     739 21/21
iq_main       16387      table        GROUPO  FinancialCodes 3612
```

```
     736 3/3
iq_main       16387      table        GROUPO  FinancialData  3621
     737 4/4
iq_main       16387      table        GROUPO  Products       3593
     735 8/8
iq_main       16387      table        GROUPO  SalesOrderItems3580
     734 5/5
iq_main       16387      table        GROUPO  SalesOrders    3565
     733 6/6

indexes  metadata  primary_key  unique_constraint  foreign_key  part
itions
0/0      Y                   1  0/0                1/1          0/0
1/1      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
0/0      Y                   1  0/0                1/1          0/0
0/0      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
4/4      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                2/2          0/0
0/0      Y                   1  0/0                3/3          0/0
```

次の例では、コマンドで dbspace_x 上のすべてのテーブルを dbspace_y に移動します。

```
SELECT 'ALTER TABLE ' || owner || '.' ||
object_name || ' MOVE TO dbspace_y;'
FROM sp_iqdbspaceobjectinfo()
WHERE object_type = 'table' AND
dbspace_name = 'dbspace_x';
```

次の **ALTER TABLE** コマンドはその結果です。

```
ALTER TABLE DBA.dt1 MOVE TO dbspace_y;
ALTER TABLE DBA.dt2 MOVE TO dbspace_y;
ALTER TABLE DBA.dt3 MOVE TO dbspace_y;
```

sp_iqdroplogin プロシージャ

SAP Sybase IQ のユーザアカウントを削除します。

構文 1

call sp_iqdroplogin （‘*userid*’）

構文 2

sp_iqdroplogin ‘*userid*’

構文 3

sp_iqdroplogin *userid*

構文 4

```
sp_iqdroplogin （'userid'）
```

パラメータ

- **userid –** 削除するユーザの ID。

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。

備考
sp_iqdroplogin は、指定されたユーザを削除します。

例
次のコマンドはすべて、ユーザ `rose` を削除します。

```
sp_iqdroplogin 'rose'
```

```
sp_iqdroplogin rose
```

```
call sp_iqdroplogin ('rose')
```

sp_iqemptyfile プロシージャ

dbfile を空にし、dbfile 内のオブジェクトを、同じ DB 領域にある別の使用可能な読み込み／書き込み dbfile に移動します。RLV DB 領域にあるファイルには使用できません。

構文

```
sp_iqemptyfile （ logical-file--name ）
```

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。 さらに、次のいずれかが必要です。システム権限:

- BACKUP DATABASE
- SERVER OPERATOR
- ALTER DATABASE

さらに、次のシステム権限のいずれかを所有している必要があります。

- INSERT ANY TABLE
- UPDATE ANY TABLE
- DELETE ANY TABLE
- ALTER ANY TABLE

- LOAD ANY TABLE
- TRUNCATE ANY TABLE
- ALTER ANY OBJECT

備考
sp_iqemptyfile は、dbfile を空にします。**sp_iqemptyfile** プロシージャを実行するには、DB 領域を読み込み専用にしておく必要があります。このプロシージャは、ファイル内のオブジェクトを、同じ DB 領域にある別の使用可能な読み込み／書き込み dbfile に移動します。使用可能な他の読み込み／書き込み dbfile がない場合は、SAP Sybase IQ からエラーメッセージが表示されます。

注意：マルチプレックス環境では、コーディネータで **sp_iqemptyfile** のみを実行できます。プロシージャを正常に完了するには、1 つの読み込み／書き込み DB 領域が使用可能である必要があります。

dbfile が RLV DB 領域にある場合は、次のエラーメッセージが表示されます。

```
Cannot empty files in an rlv store dbspace.
```

例
dbfile **dbfile1** を空にします。

```
sp_iqemptyfile 'dbfile1'
```

sp_iqestdbspaces プロシージャ

指定した合計インデックスサイズに必要な DB 領域の数とサイズを見積もります。

構文

```
sp_iqestdbspaces ( db_size_in_bytes, iq_page_size,
min_#_of_bytes, max_#_of_bytes )
```

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。 さらに、次のいずれかが必要です。 システム権限:

- MANAGE ANY DBSPACE
- ALTER DATABASE

備考
sp_iqestdbspaces は、データのユニーク性に応じて、いくつかの推奨をレポートします。

推奨	説明
min	データの差が少ない場合は、**min** で推奨されているサイズの DB 領域セグメントだけを作成することもできます。これらの推奨は、最小限の差を持つデータを最大限に圧縮した場合のものです。
avg	データの差が平均的であれば、**min** で推奨されているとおりに DB 領域セグメントを作成し、**avg** で推奨されているサイズで追加のセグメントを作成します。
max	データの差が大きい (ユニークな値が多い) 場合は、**min**、**avg**、**max** で推奨されているとおりに DB 領域セグメントを作成します。
spare	データ内のユニークな値の数がわからない場合は、**min**、**avg**、**max**、**spare** で推奨されているとおりに DB 領域セグメントを作成します。データをロードした後で、使用していないセグメントはいつでも削除できますが、作成するセグメントが少なすぎると時間がかかります。

データベースサイズ、IQ ページサイズ、DB 領域セグメントあたりのバイト数の範囲に基づいて、DB 領域セグメントの数とサイズに関する情報を表示します。このプロシージャでは、指定された IQ ページサイズのデフォルトブロックサイズでデータベースが作成されていることを前提として計算します。それ以外の場合、正しい推定値は返されません。

表 19 : sp_iqestdbspaces のパラメータ

名前	データ型	説明
db_size_in_bytes	decimal(16)	データベースのサイズ (バイト)。
iq_page_size	smallint	データベースの IQ セグメント用に定義されているページサイズ。2 の累乗で、範囲は 65536 ～ 524288、デフォルトは 131072 です。
min_#_of_bytes	int	dbspace セグメントあたりの最小バイト数。デフォルトは 20,000,000 (20MB) です。
max_#_of_bytes	int	DB 領域セグメントあたりの最大バイト数。デフォルトは 2,146,304,000 (2.146GB) です。

sp_iqfile プロシージャ

DB 領域の各 dbfile についての詳細情報を表示します。

構文

```
sp_iqfile [ dbspace-name ]
```

適用対象
シンプレックスとマルチプレックス。

権限
MANAGE ANY DBSPACE システム権限。そのシステムプロシージャに対する EXECUTE 権限に加え、次のものが必要です。

備考
sp_iqfile は、DB 領域の各 dbfile のデータの使用率、プロパティ、タイプを表示します。この情報を使用して、データの移動が必要かどうかを判断できます。また、移動されたデータに関しては、旧バージョンの割り付けが解除されているかどうかを確認できます。

カラム名	説明
DBSpaceName	**CREATE DBSPACE** 文で指定された DB 領域の名前。**CREATE DATABASE...CASE IGNORE** または **CASE RESPECT** の指定に関係なく、DB 領域名は常に大文字と小文字が区別されない。
DBFileName	論理ファイル名。
Path	物理ファイルまたはローパーティションの場所。
SegmentType	DB 領域のタイプ (`MAIN`、`TEMPORARY`、`RLV`、または `CACHE`)。
RWMode	DB 領域のモード。常に、読み書き (RW)。
Online	T (オンライン) または F (オフライン)。
Usage	DB 領域のこのファイルで現在使用されている DB 領域の割合。マルチプレックス設定のセカンダリノードに対して実行した場合は、NA がこのカラムに表示される。
DBFileSize	ファイルまたはローパーティションの現在のサイズ。ローパーティションでは、このサイズ値は物理サイズよりも小さくなる場合がある。
Reserve	DB 領域のこのファイルに追加できる予約領域。
StripeSize	ディスクストライピングの有効化時は、常に 1。
BlkTypes	ユーザデータと内部システム構造が使用している領域。
FirstBlk	ファイルに割り当てられている最初の IQ ブロック番号。
LastBlk	ファイルに割り当てられている最後の IQ ブロック番号。
OkToDrop	ファイルを削除できる場合は "Y"、それ以外の場合は "N"。

識別子	ブロックタイプ
A	アクティブなバージョン
B	バックアップ構造
C	チェックポイントログ
D	データベースの識別情報
F	フリーリスト
G	グローバルフリーリストマネージャ
H	フリーリストのヘッダブロック
I	インデックスアドバイスの格納
M	マルチプレックス CM*
O	旧バージョン
R	RLV フリーリストマネージャ
T	テーブルの使用
U	インデックスの使用
N	カラムの使用
X	チェックポイントでの削除

*マルチプレックスコミット ID ブロック (実際は 128 ブロック) は、シンプレックスデータベースで使用されていない場合でも、すべての IQ データベースに存在します。

例
DB 領域のファイルに関する情報を表示します。

```
sp_iqfile;
```

```
sp_iqfile;
DBSpaceName,DBFileName,Path,SegmentType,RWMode,Online,
Usage,DBFileSize,Reserve,StripeSize,BlkTypes,FirstBlk,
LastBlk,OkToDrop

'IQ_SYSTEM_MAIN','IQ_SYSTEM_MAIN','/sun1-c1/users/smith/mpx/m/
mpx_db.iq','MAIN','RW','T','21','
2.92G','0B','1K','1H,76768F,32D,19A,185O,128M,34B,32C'
,1,384000,'N'

'mpx_main1','mpx_main1','/sun1-c1/users/smith/mpx/m/
mpx_main1.iq','MAIN','RW','T','1'
```

```
,'100M','0B','1K','1H',1045440,1058239,'N'

'IQ_SHARED_TEMP','sharedfile1_bcp','/sun1-c1/users/smith/mpx/m/
f1','SHARED_TEMP','RO','T','0',
'50M','0B','1K','1H',1,6400,'N'

'IQ_SHARED_TEMP','sharedfile2_bcp','/sun1-c1/users/smith/mpx/m/
f2','SHARED_TEMP','RO','T','0',
'50M','0B','1K','1H',1045440,1051839,'N'

'myDAS', 'ssd_dev_1', '/dev/raw/ssd_dev_1', 'CACHE', 'RW', 'T', '2',
'20M', '0B', '1K', '1H', '64F', '1', '5120', 'N'
'myDAS', 'ssd_dev_2', '/dev/raw/ssd_dev_2', 'CACHE', 'RW', 'T', '1',
'20M', '0B', '1K', '1H', '32F', '522208', '527327', 'N'
'myDAS', 'ssd_dev_3', '/dev/raw/ssd_dev_3', 'CACHE', 'RW', 'T', '1',
'20M', '0B', '1K', '1H', '32F', '1044416', '1049535', 'N'
'myDAS', 'ssd_dev_4', '/dev/raw/ssd_dev_4', 'CACHE', 'RW', 'T', '1',
'20M', '0B', '1K', '1H', '32F', '1566624', '1571743', 'N'
'myDAS', 'ssd_dev_5', '/dev/raw/ssd_dev_5', 'CACHE', 'RW', 'T', '1',
'20M', '0B', '1K', '1H', '32F', '2088832', '2093951', 'N'

'IQ_SYSTEM_TEMP','IQ_SYSTEM_TEMP','/sun1-c1/users/smithmpx/m/
mpx_db.iqtmp','TEMPORARY','RW',
'T','1','2.92G','0B','1K','1H,64F,33A',1,384000,'N'
```

sp_iqmodifyadmin プロシージャ

指定したログインポリシーのオプションを所定の値に設定します。ログインポリシーを指定しないと、オプションがルートポリシーに設定されます。マルチプレックスでは、**sp_iqmodifyadmin** は、マルチプレックスサーバ名であるオプションのパラメータを指定します。

構文 1

```
call sp_iqmodifyadmin （'policy_option_name', 'value_in' ,
['login_policy_name'] )
```

構文 2

```
sp_iqmodifyadmin 'policy_option_name',
'value_in' ,'login_policy_name '
```

構文 3

```
sp_iqmodifyadmin  policy_option_name, value_in, login_policy_name
```

構文 4

```
sp_iqmodifyadmin 'policy_option_name',
'value_in' ,'login_policy_name ' ,'server_name '
```

パラメータ

- **policy_option_name –** 変更するログインポリシーオプション。
- **value_in –** ログインポリシーオプションの新しい値。
- **login_policy_name –** ログインポリシーオプションが変更されるポリシー。

権限
そのシステムプロシージャに対する EXECUTE 権限に加え、次のものが必要です。 MANAGE ANY LOGIN POLICY システム権限。

例
lockeduser という名前のポリシーで、ログインオプション `locked` を ON に設定します。

```
call sp_iqmodifyadmin ('locked','on','lockeduser')
```

`Writer1` という名前のマルチプレックスサーバ上の *lockeduser* というポリシーで、ログインオプション `locked` を ON に設定します。

```
call sp_iqmodifyadmin ('locked','on','lockeduser','Writer1')
```

sp_iqmodifylogin プロシージャ

ユーザをログインポリシーに割り当てます。

構文 1

```
call sp_iqmodifylogin ('userid' [, 'login_policy_name'])
```

構文 2

```
sp_iqmodifylogin 'userid', ['login_policy_name']
```

パラメータ

- **userid –** 変更するアカウントの名前を保持する変数。
- **login_policy_name –** (オプション) ユーザを割り当てるログインポリシーの名前を指定します。ログインポリシー名を指定しないと、ユーザがルートログインポリシーに割り当てられます。

権限
そのシステムプロシージャに対する EXECUTE 権限に加え、次のものが必要です。 MANAGE ANY USER システム権限。

例
ユーザ `joe` を `expired_password` というログインポリシーに割り当てます。

```
sp_iqmodifylogin 'joe', 'expired_password'
```

ユーザ joe をルートログインポリシーに割り当てます。

```
call sp_iqmodifylogin ('joe')
```

sp_iqobjectinfo プロシージャ

データベースのオブジェクトおよびサブオブジェクトのパーティションと DB 領域の割り当てを返します。

構文

sp_iqobjectinfo [*owner_name*] [, *object_name*] [, *object-type*]

パラメータ

- **owner_name –** オブジェクトの所有者。指定した場合、**sp_iqobjectinfo** は、指定の所有者のテーブルのみの出力を表示します。指定しない場合、**sp_iqobjectinfo** は、データベース内のすべてのユーザのテーブルに関する情報を表示します。
- **object_name –** テーブルの名前。指定しない場合、**sp_iqobjectinfo** は、データベース内のすべてのテーブルに関する情報を表示します。
- **object-type –** 有効な **table** オブジェクトタイプ。

  オブジェクトタイプが table の場合は、引用符で囲んでください。

すべてのパラメータがオプションであり、どのパラメータも他のパラメータの値とは関係なく指定できます。

権限

そのシステムプロシージャに対する EXECUTE 権限が必要です。

備考

入力パラメータは **sp_iqobjectinfo** とともに使用します。**sp_iqobjectinfo** の結果にクエリを実行でき、クエリの **WHERE** 句で述部を使用する代わりに、入力パラメータを使用することで、クエリのパフォーマンスが向上します。たとえば、クエリ A は次のように記述します。

```
SELECT COUNT(*) FROM sp_iqobjectinfo()
WHERE owner = 'DBA'
AND object_name = 'tab_case510'
AND object_type = 'table'
AND sub_object_name is NULL
AND dbspace_name = 'iqmain7'
AND partition_name = 'P1'
```

クエリ B は、クエリ A を記述し直して、**sp_iqobjectinfo** 入力パラメータを使用できるようにしたものです。

```
SELECT COUNT(*) FROM sp_iqobjectinfo('DBA','tab_case510','table')
WHERE sub_object_name is NULL
AND dbspace_name = 'iqmain7'
AND PARTITION_NAME = 'P1'
```

クエリ B は、クエリ A よりも短時間で結果を返します。入力パラメータが **sp_iqobjectinfo** に渡されると、プロシージャはシステムテーブル内の少数のレコードを比較してジョインします。つまり、クエリ A に比べ作業が少なくなります。クエリ B では、述部はプロシージャ自体に適用され、プロシージャで返される結果セットが小さくなります。そのため、クエリで適用される述部の数が少なくなります。

sp_iqobjectinfo ストアドプロシージャでは、*owner_name*、*object_name*、および *object_type* の解釈に、ワイルドカード文字がサポートされています。これは、**LIKE** 句がクエリ内のパターンを照合するのと同じ方法で、指定のパターンと一致するすべての DB 領域の情報を表示します。

特定のまたはすべてのデータベースオブジェクト (テーブルタイプ) とそのサブオブジェクトの、すべてのパーティションと DB 領域割り当てを返します。サブオブジェクトは、カラム、インデックス、プライマリキー、一意性制約、および外部キーです。

表 20 : sp_iqobjectinfo のカラム

カラム名	説明
owner	オブジェクトの所有者の名前。
object_name	DB 領域にあるオブジェクト (テーブルタイプ) の名前。
sub_object_name	DB 領域に存在するオブジェクトの名前。
object_type	オブジェクトのタイプ (カラム、インデックス、プライマリキー、一意性制約、外部キー、パーティション、テーブル)。
object_id	オブジェクトのグローバルオブジェクト ID。
id	オブジェクトのテーブル ID。
dbspace_name	オブジェクトが存在する DB 領域の名前。文字列 "[multiple]" は、分割されたオブジェクトの特別なメタローに表示される。出力内の [multiple] ローは、その後ろにテーブルまたはカラムを記述する複数のローが続くことを示す。
partition_name	指定のオブジェクトのパーティションの名前。

例

注意： 出力内容をわかりやすくするため、次の例は `iqdemo` データベース内のオブジェクトを示しています。`iqdemo` には `iq_main` というサンプルのユーザ DB

領域が含まれていますが、この領域はユーザ独自のデータベースには存在しない場合があります。

指定のユーザが所有する特定のデータベースオブジェクトおよびサブオブジェクトのパーティションおよび DB 領域割り当てに関する情報を表示します。

```
sp_iqobjectinfo GROUPO,Departments
```

```
owner   object_name  sub_object_name                object_type  obj
ect_id  id
GROUPO  Departments  (NULL)                          table         3
632     738
GROUPO  Departments  DepartmentID                    column        3
633     738
GROUPO  Departments  DepartmentName                  column        3
634     738
GROUPO  Departments  DepartmentHeadID                column        3
635     738
GROUPO  Departments  DepartmentsKey                  primary
key   83       738
GROUPO  Departments  FK_DepartmentHeadID_EmployeeID  foreign
key   92       738

dbspace_name     partition_name
iq_main          (NULL)
iq_main          (NULL)
iq_main          (NULL)
iq_main          (NULL)
iq_main          (NULL)
iq_main          (NULL)
```

object-type **table** で、指定のユーザが所有する特定のデータベースオブジェクトおよびサブオブジェクトのパーティションおよび DB 領域割り当てに関する情報を表示します。

```
sp_iqobjectinfo DBA,sale,'table'
```

```
owner  object_name  sub_object_name  object_type  object_id  id
DBA    sale         (NULL)           table        3698       742
DBA    sale         prod_id          column       3699       742
DBA    sale         month_num        column       3700       742
DBA    sale         rep_id           column       3701       742
DBA    sale         sales            column       3702       742

dbspace_name      partition_name
iq_main           (NULL)
iq_main           (NULL)
iq_main           (NULL)
iq_main           (NULL)
iq_main           (NULL)
```

sp_iqspaceused プロシージャ

空き領域と IQ ストア、IQ テンポラリストア、RLV ストア、および IQ グローバルと IQ ローカルの共有テンポラリストアの使用領域に関する情報を表示します。

構文

```
sp_iqspaceused(out mainKB            unsigned bigint,
               out mainKBUsed        unsigned bigint,
               out tempKB            unsigned bigint,
               out tempKBUsed        unsigned bigint,
               out shTempTotalKB     unsigned bigint,
               out shTempTotalKBUsed unsigned bigint,
               out shTempLocalKB     unsigned bigint,
               out shTempLocalKBUsed unsigned bigint,
               out rlvLogKB          unsigned bigint,
               out rlvLogKBUsed      unsigned bigint)
```

適用対象
シンプレックスとマルチプレックス。

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。 さらに、次のいずれかが必要です。 システム権限：

- ALTER DATABASE
- MANAGE ANY DBSPACE
- MONITOR

備考
sp_iqspaceused は、unsigned bigint の out パラメータとしていくつかの値を返します。このシステムストアドプロシージャをユーザ定義のストアドプロシージャから呼び出すと、メイン、テンポラリ、および RLV ストアの領域の使用量を確認できます。

sp_iqspaceused は、**sp_iqstatus** によって提供された情報のサブセットを返しますが、計算に使用する SQL 変数内の情報をユーザが返すこともできます。

マルチプレックスデータベースで実行すると、このプロシージャは、プロシージャを実行しているサーバに適用されます。また、IQ_SHARED_TEMP で使用される領域も返します。

カラム名	説明
mainKB	IQ メインストアの領域の合計 (KB 単位)。

カラム名	説明
mainKBUsed	データベースが使用している IQ メインストアの領域 (KB 単位)。セカンダリマルチプレックスノードは '(Null)' を返す。
tempKB	IQ テンポラリストアの領域の合計 (KB 単位)。
tempKBUsed	データベースが使用している IQ テンポラリストアの領域の合計 (KB 単位)。
shTempTotalKB	IQ グローバル共有テンポラリストアの領域の合計 (KB 単位)。
shTempLocalKB	IQ ローカル共有テンポラリストアの領域の合計 (KB 単位)。
shTempLocalKBUsed	データベースが使用している IQ ローカル共有テンポラリストアの領域 (KB 単位)。
rlvLogKB	RLV ストアの領域の合計 (KB 単位)。
rlvLogKBUsed	データベースが使用している RLV ストアの領域 (KB 単位)。

例

sp_iqspaceused には 7 つの出力パラメータが必要です。7 つの出力パラメータを宣言してから **sp_iqspaceused** を呼び出す、ユーザ定義ストアドプロシージャ **myspace** を作成します。

```
  create or replace procedure dbo.myspace()
begin
     declare mt unsigned bigint;
     declare mu unsigned bigint;
     declare tt unsigned bigint;
     declare tu unsigned bigint;
     declare gt unsigned bigint;
     declare gu unsigned bigint;
     declare lt unsigned bigint;
     declare lu unsigned bigint;
     declare tt_t unsigned bigint;
     declare mt_t unsigned bigint;
     declare gt_t unsigned bigint;
     declare lt_t unsigned bigint;
     call sp_iqspaceused(mt,mu,tt,tu,gt,gu,lt,lu);
     if (tt = 0) then
        set tt_t = 0;
     else
        set tt_t = tu*100/tt;
     end if;
     if (mt = 0) then
        set mt_t = 0;
     else
        set mt_t = mu*100/mt;
     end if;
```

```
     if (gt = 0) then
        set gt_t = 0;
     else
        set gt_t = gu*100/gt;
     end if;
     if (lt = 0) then
        set lt_t = 0;
     else
        set lt_t = lu*100/lt;
     end if;
  select cast(mt/1024 as unsigned bigint) as mainMB,
         cast(mu/1024 as unsigned bigint) as mainusedMB, mt_t as
mainPerCent,
         cast(tt/1024 as unsigned bigint) as tempMB,
         cast(tu/1024 as unsigned bigint) as tempusedMB, tt_t as
tempPerCent,
         cast(gt/1024 as unsigned bigint) as shTempTotalKB,
        cast(gu/1024 as unsigned bigint) as shTempTotalKBUsed, gt_t
as globalshtempPerCent,
         cast(lt/1024 as unsigned bigint) as shTempLocalMB,
        cast(lu/1024 as unsigned bigint) as shTempLocalKBUsed, lt_t
as localshtempPerCent;
end
```

sp_iqspaceused の出力を表示するには、**myspace** を実行します。

```
myspace
```

sp_iqsysmon プロシージャ

SAP Sybase IQ の複数のコンポーネントをモニタします。モニタ対象には、バッファキャッシュ、メモリ、スレッド、ロック、入出力機能、および CPU 使用率の管理などが含まれます。

バッチモードでの構文

```
sp_iqsysmon start_monitor
sp_iqsysmon stop_monitor [, 'section(s)' ]
or
sp_iqsysmon 'time-period' [, 'section(s)' ]
```

ファイルモードでの構文

```
sp_iqsysmon start_monitor, 'filemode' [, 'monitor-options' ]
sp_iqsysmon stop_monitor
```

バッチモードでのパラメータ

- **start_monitor –** モニタリングを開始します。
- **stop_monitor –** モニタリングを停止し、レポートを表示します。
- **time-period –** モニタリングの期間 (HH:MM:SS 形式で指定)。
- **section(s) – sp_iqsysmon** によって表示される 1 つ以上のセクションの省略形。

省略形の完全なリストについては、「備考 (0　ページ)」の項を参照してください。

複数のセクションを指定する場合は、セクションの省略形をスペースで区切り、そのリストを一重引用符または二重引用符で囲みます。デフォルトでは、すべてのセクションを表示します。

IQ メインストアに関連するセクションの場合、セクションの省略形に 'm' または 't' のプレフィクスを付けることによって、それぞれメインストアまたはテンポラリストアを指定できます。プレフィクスを使用しない場合、両方のストアがモニタされます。たとえば、'mbufman' を指定した場合、IQ メインストアバッファマネージャのみがモニタされる。'mbufman tbufman' または 'bufman' を指定した場合、メインストアとテンポラリストアの両方のバッファマネージャがモニタされる。

注意： SAP Sybase IQ コンポーネントのディスク I/O およびロックマネージャは、現在 **sp_iqsysmon** ではサポートされていません。

ファイルモードでのパラメータ

- **start_monitor –** モニタリングを開始します。
- **stop_monitor –** モニタリングを停止し、残りの出力をログファイルに書き込みます。
- **filemode –** ファイルモードで **sp_iqsysmon** を実行することを指定します。ファイルモードでは、モニタリング期間中一定の時間間隔でサンプリングした統計情報が示されます。デフォルトでは、*dbname.connid-iqmon* という名前のログファイルに出力が書き込まれます。出力ファイルのサフィックスを変更するには、**file_suffix** オプションを使用します。**file_suffix** オプションの説明については、「*monitor_options* パラメータ」を参照してください。
- **monitor_options –** monitor _options 文字列には 1 つ以上のオプションを含めることができます。
  - **-interval seconds –** レポート間隔を秒単位で指定します。モニタ統計のサンプリング情報が、一定の時間間隔でログファイルに出力されます。-interval オプションを指定しない場合のデフォルトの間隔は 60 秒です。最小レポート間隔は 2 秒です。このオプションで指定した間隔が無効であるか、2 秒未満である場合、2 秒間隔に設定されます。

    最初の表示では、サーバの起動からのカウンタが示されます。それ以降の表示では、前の表示との差が示されます。通常は、パフォーマンスに問題がある期間 (クエリ実行時や特定の時間帯) に 60 秒のデフォルト間隔でモニタを実行すると、有意な結果を得ることができます。間隔が短すぎると、意味のある結果を取得できないことがあります。ジョブ時間に見合った間隔を指定する必要があります。通常は 60 秒で十分です。

- **-file_suffix suffix –** `dbname.connid-suffix` という名前のモニタリング出力ファイルを作成します。-file_suffix オプションを指定しないと、サフィックスはデフォルトで `iqmon` に設定されます。-file_suffix オプションを指定した場合で、サフィックスを指定しないか、サフィックスとしてブランクの文字列を指定したときは、サフィックスは使用されません。
- **-append または -truncate –** 前者は既存の出力ファイルへの追加、後者は既存の出力ファイルのトランケートを **sp_iqsysmon** に指示します。デフォルトは、トランケートです。両方のオプションを指定した場合、文字列内の後ろのほうで指定されたオプションが優先されます。
- **-section section(s) –** モニタログファイルに書き込む 1 つ以上のセクションの省略形を指定します。

  省略形の完全なリストについては、「備考 (0　ページ)」の項を参照してください。

  デフォルトでは、すべてのセクションが書き込まれます。ファイルモードのセクションリストで指定する省略形は、バッチモードで使用する省略形と同じです。複数のセクションを指定する場合、セクションの省略形をスペースで区切る必要があります。

  セクションなしで -section オプションを指定した場合、どのセクションもモニタされません。無効なセクション省略形は無視され、IQ メッセージファイルに警告が書き込まれます。

権限
そのシステムプロシージャに対する EXECUTE 権限に加え、次のものが必要です。 MONITOR システム権限。

備考

レポート対象のレポートセクションまたは IQ コンポーネント	入力する省略形
バッファ割り付け	(メイン) – mbufalloc (テンポラリ) – tbufalloc
バッファマネージャ	(メイン) – mbufman (テンポラリ) – tbufman
バッファプール	(メイン) – mbufpool (テンポラリ) – tbufpool
カタログの統計	catalog

レポート対象のレポートセクションまたは IQ コンポーネント	入力する省略形
CPU の使用率	cpu
フリーリスト管理	(メイン) – mfreelist (テンポラリ) – tfreelist
メモリ管理	memory
プリフェッチ管理	(メイン) – mprefetch (テンポラリ) – tprefetch
IQ RLV インメモリストアの統計	rlv
LMA (Large Memory Allocator) の統計	lma
サーバコンテキスト統計	server
スレッド管理	threads
トランザクション管理	txn

sp_iqsysmon ストアドプロシージャは、SAP Sybase IQ の複数のコンポーネントをモニタします。モニタ対象には、バッファキャッシュ、メモリ、スレッド、ロック、入出力機能、および CPU 使用率の管理などが含まれます。

sp_iqsysmon プロシージャは、次の 2 つのモニタリングモードをサポートします。

- **バッチモード – sp_iqsysmon** は、モニタを開始してから停止するまでの期間、または *time-period* パラメータで指定した期間にモニタ統計情報を収集します。モニタリング期間の経過後、**sp_iqsysmon** は集約した統計情報のリストを表示します。

  バッチモードの **sp_iqsysmon** は、SAP Adaptive Server® Enterprise プロシージャ **sp_sysmon** と同様のものです。
- **ファイルモード – sp_iqsysmon** はモニタを開始してから停止するまで、一定の時間間隔でサンプリングした統計情報をログファイルに書き込みます。

  ファイルモードの最初の記録では、サーバの起動からのカウンタが示されます。それ以降の記録では、前の表示との差が示されます。

  ファイルモードの **sp_iqsysmon** は、**IQ UTILITIES** コマンド **START MONITOR** および **STOP MONITOR** インタフェースに似ています。

バッチモードでの構文例
例 1：

バッチモードでモニタを開始し、メインストアおよびテンポラリストアのすべてのセクションを表示します。

```
sp_iqsysmon start_monitor
sp_iqsysmon stop_monitor
```

例 2：

バッチモードでモニタを開始し、メインストアのバッファマネージャとバッファプールの統計情報を表示します。

```
sp_iqsysmon start_monitor
sp_iqsysmon stop_monitor 'mbufman mbufpool'
```

例 3：

10 分後にモニタ情報を出力します。

```
sp_iqsysmon '00:10:00'
```

例 4：

5 分後に、**sp_iqsysmon** レポートのメモリマネージャのセクションのみを出力します。

```
sp_iqsysmon '00:05:00', memory
```

例 5：

モニタを開始した後、2 つのプロシージャと 1 つのクエリを実行し、モニタを停止して、レポートのバッファマネージャのセクションのみを出力します。

```
sp_iqsysmon start_monitor
     go
     execute proc1
     go
     execute proc2
     go
     select sum(total_sales) from titles
     go
     sp_iqsysmon stop_monitor, bufman
     go
```

例 6：

2 分後に、レポートのメインバッファマネージャおよびメインバッファプールのセクションのみを出力します。

```
sp_iqsysmon '00:02:00', 'mbufman mbufpool'
```

例 7：

1 分後に、レポートの RLV セクションのみを出力します。

```
sp_iqsysmon '01:00:00','rlv'
```

例 8：

5 分後に、レポートの LMA セクションのみを出力します。

```
sp_iqsysmon '00:00:05', 'lma'
```

例 9：

バッチモードでモニタを 10 秒間実行し、10 秒間の経過後に集約した統計情報を表示します。

```
sp_iqsysmon '00:00:10', 'mbufpool memory'
```

ファイルモードでの構文例
例 1：

モニタを開始してから停止するまで、2 秒ごとに情報をトランケートし、ログファイルに書き込みます。

```
sp_iqsysmon start_monitor, 'filemode', '-interval 2'
     .
     .
     .
     sp_iqsysmon stop_monitor
```

例 2：

dbname.connid-testmon という名前の ASCII ファイルに、メインバッファマネージャおよびメモリマネージャのセクションの出力のみを追加します。データベース iqdemo の場合は、ファイル iqdemo.2-testmon に結果を書き込みます。

```
sp_iqsysmon start_monitor, 'filemode',
     '-file_suffix testmon -append -section mbufman memory'
     .
     .
     .
     sp_iqsysmon stop_monitor
```

例 3：

レポートの RLV セクションおよび LMA セクションのみを出力します。

```
sp_iqsysmon start_monitor,'filemode','-section rlv lma'
     sp_iqsysmon stop_monitor
```

例 4：

ファイルモードでモニタを開始し、メインバッファプールとメモリマネージャの統計情報を 5 秒間隔でログファイルに書き込みます。

```
sp_iqsysmon start_monitor, ‘filemode’, '-interval 5 -section
mbufpool memory'
sp_iqsysmon stop_monitor
```

sp_iqsysmon プロシージャ例

sp_iqsysmon 出力例です。

例 1：

20 分後にバッファ割り付け (メインおよびテンポラリ) の出力を表示します。

```
sp_iqsysmon '00:20:00', 'mbufalloc tbufalloc'

================================
Buffer Allocator (Main)"
================================

STATS-NAME                    VALUE
NActiveCommands                   2
BufAllocMaxBufs                2275( 81.6% )
BufAllocAvailBufs              2115( 93.0% )
BufAllocReserved                160( 7.0% )
BufAllocAvailPF                 750( 33.0% )
BufAllocSlots                   100
BufAllocNPinUsers                 0
BufAllocNPFUsers                  2
BufAllocNPostedUsrs               0
BufAllocNUnpostUsrs               0
BufAllocPinQuota                  0
BufAllocNPostEst                  0
BufAllocNUnPostEst                0
BufAllocMutexLocks                0
BufAllocMutexWaits                0( 0.0% )

STATS-NAME                    VALUE
NActiveCommands                   2
BufAllocMaxBufs                2275( 81.6% )
BufAllocAvailBufs              2115( 93.0% )
BufAllocReserved                160( 7.0% )
BufAllocAvailPF                 750( 33.0% )
BufAllocSlots                   100
BufAllocNPinUsers                 0
BufAllocNPFUsers                  2
BufAllocNPostedUsrs               0
BufAllocNUnpostUsrs               0
BufAllocPinQuota                  0
BufAllocNPostEst                  0
BufAllocNUnPostEst                0
BufAllocMutexLocks                0
BufAllocMutexWaits                0( 0.0% )


STATS-NAME                  TOTAL  UNKNWN    HASH        CSORT     ROW
ROWCOL      FP  GARRAY      LOB   BTREE      BM      BV   STORE     TEST
NumClients                    2       0       0           0       2
0       0       0       0       0       0       0       0       0
PinUserQuota                  0       0       0           0       0
0       0       0       0       0       0       0       0       0
```

```
PrefetchUserQuota            160       0       0           0     160
0       0       0       0       0       0       0       0       0
PinUserRegisters               2       2       0           0       0
0       0       0       0       0       0       0       0       0
PfUserRegisters             4697       0       0           0     382
2621     377     182       0       2       0       0       0       0

ClientCountOfPinners           0       1       3           6      10
33      66     100     333     666    1000    3333    6666   10000
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Hash                           0       0       0           0       0
0       0       0       0       0       0       0       0       0
Sort                           0       0       0           0       0
0       0       0       0       0       0       0       0       0
Row                            2       0       0           0       0
0       0       0       0       0       0       0       0       0
RowColumn                      0       0       0           0       0
0       0       0       0       0       0       0       0       0
FP                             0       0       0           0       0
0       0       0       0       0       0       0       0       0
Garray                         0       0       0           0       0
0       0       0       0       0       0       0       0       0
LOB                            0       0       0           0       0
0       0       0       0       0       0       0       0       0
BTree                          0       0       0           0       0
0       0       0       0       0       0       0       0       0
BM                             0       0       0           0       0
0       0       0       0       0       0       0       0       0
BV                             0       0       0           0       0
0       0       0       0       0       0       0       0       0
Store                          0       0       0           0       0
0       0       0       0       0       0       0       0       0
Test                           0       0       0           0       0
0       0       0       0       0       0       0       0       0
DBCC                           0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Run                            0       0       0           0       0
0       0       0       0       0       0       0       0       0
QCPRun                         0       0       0           0       0
0       0       0       0       0       0       0       0       0
TextDoc                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
VDO                            0       0       0           0       0
0       0       0       0       0       0       0       0       0
Load                        Pass       2       0           0       0
0       0       0       0       0       0       0       0       0
```

```
STATS-NAME (cont'd)           DBCC  BLKMAP  IQUTIL
NumClients                    0       0       0           0       0
0       0       0       0       0
PinUserQuota                  0       0       0           0       0
0       0       0       0       0
PrefetchUserQuota             0       0       0           0       0
0       0       0       0       0
PinUserRegisters              0       0       0           0       0
0       0       0       0       0
PfUserRegisters               0       0       0           0       0
0       0       0    1133       0

ClientCountOfPinners         33333   66666  100000   4294967295
Unknown                          0       0       0           0
Hash                             0       0       0           0
Sort                             0       0       0           0
Row                              0       0       0           0
RowColumn                        0       0       0           0
FP                               0       0       0           0
Garray                           0       0       0           0
LOB                              0       0       0           0
BTree                            0       0       0           0
BM                               0       0       0           0
BV                               0       0       0           0
Store                            0       0       0           0
Test                             0       0       0           0
DBCC                             0       0       0           0
Unknown                          0       0       0           0
Unknown                          0       0       0           0
Run                              0       0       0           0
QCPRun                           0       0       0           0
TextDoc                          0       0       0           0
Unknown                          0       0       0           0
Unknown                          0       0       0           0
VDO                              0       0       0           0
Load                         0       0       0           0       0       0


================================
Buffer Allocator (Temporary)
================================

STATS-NAME                   VALUE
NActiveCommands                  2
BufAllocMaxBufs               2275( 81.6% )
BufAllocAvailBufs             2263( 99.5% )
BufAllocReserved                12( 0.5% )
BufAllocAvailPF                908( 39.9% )
BufAllocSlots                  100
BufAllocNPinUsers                2
BufAllocNPFUsers                 2
BufAllocNPostedUsrs              0
BufAllocNUnpostUsrs              0
BufAllocPinQuota               175
BufAllocNPostEst                 2
BufAllocNUnPostEst               2
```

```
BufAllocMutexLocks                0
BufAllocMutexWaits                0( 0.0% )

STATS-NAME                    TOTAL  UNKNWN    HASH        CSORT     ROW
ROWCOL      FP  GARRAY      LOB   BTREE      BM      BV   STORE     TEST
NumClients                      4       0       0           4       0
0       0       0       0       0       0       0       0       0       0
PinUserQuota                   10       0       0          10       0
0       0       0       0       0       0       0       0       0       0
PrefetchUserQuota               2       0       0           2       0
0       0       0       0       0       0       0       0       0       0
PinUserRegisters              668       0     300         247
0       0       0       0       0       0       0       0       0       0
PfUserRegisters               675       0       0         295       0
0       0       0       0       0       0       0       1       0

ClientCountOfPinners            0       1       3           6      10
33      66     100     333     666    1000    3333    6666   10000
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Hash                            0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Sort                            2       0       1           0       1
0       0       0       0       0       0       0       0       0       0
Row                             0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
RowColumn                       0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
FP                              0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Garray                          0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
LOB                             0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
BTree                           0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
BM                              0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
BV                              0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Store                           0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Test                            0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
DBCC                            0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Run                             0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
QCPRun                          `       0       0           0       0
0       0       0       0       0       0       0       0       0       0
TextDoc                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
```

```
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0
VDO                           0       0       0           0       0
0       0       0       0       0       0       0       0       0
Load                        Pass       2       0           0       0
0       0       0       0       0       0       0       0       0

STATS-NAME (cont'd)           DBCC   BLKMAP   IQUTIL
NumClients                    0       0       0           0       0
0       0       0       0       0
PinUserQuota                  0       0       0           0       0
0       0       0       0       0
PrefetchUserQuota             0       0       0           0       0
0       0       0       0       0
PinUserRegisters              0       0       0         110       2
0       0       0       0       9
PfUserRegisters               0       0       0         378       0
0       0       1       0       0

ClientCountOfPinners        33333   66666  100000   4294967295
Unknown                         0       0       0           0
Hash                            0       0       0           0
Sort                            0       0       0           0
Row                             0       0       0           0
RowColumn                       0       0       0           0
FP                              0       0       0           0
Garray                          0       0       0           0
LOB                             0       0       0           0
BTree                           0       0       0           0
BM                              0       0       0           0
BV                              0       0       0           0
Store                           0       0       0           0
Test                            0       0       0           0
DBCC                            0       0       0           0
Unknown                         0       0       0           0
Unknown                         0       0       0           0
Run                             0       0       0           0
QCPRun                          0       0       0           0
TextDoc                         0       0       0           0
Unknown                         0       0       0           0
Unknown                         0       0       0           0
VDO                             0       0       0           0
Load                          0       0       0           0       0
0
```

例 2：

20 分後にバッファマネージャ (メインおよびテンポラリ) の出力を表示します。

```
sp_iqsysmon '00:20:00', 'mbufman tbufman'


==============================
Buffer Manager (Main)
```

```
==============================

STATS-NAME                    TOTAL    NONE  TXTPOS  TXTDOC  CMPACT
BTREEV  BTREEF      BV     VDO   DBEXT    DBID    SORT   STORE  GARRAY
Finds                      80137       0       0       0       0    9046
3307       0   20829        0        0        0        0     275
Hits                       80090       0       0       0       0    9015
3291       0   20829        0        0        0        0     275
Hit%                        99.9       0       0       0       0    99.7
99.5       0     100        0        0        0        0     100
FalseMiss                  26469       0       0       0       0
63      40        0    1097        0        0        0        0        0
UnOwnRR                       48       0       0       0       0     31
16       0        1        0        0        0        0        0
Cloned                             0       0       0       0       0
0        0        0        0        0        0        0        0        0
Creates                     1557       0       0       0       0     60
179      0      256        0        0        0        0       58
Destroys                       546       0       0       0       0
12      21        0        6        0        0        0        0       29
Dirties                     7554       0       0       0       0   1578
585       0        0        0        0        0        0        0
RealDirties                    2254       0       0       0       0
117     180        0      542        0        0        0        0       58
PrefetchReqs                     80       0       0       0       0
0        0        0       74        0        0        0        0        0
PrefetchNotInMem                  1       0       0       0       0
0        0        0        1        0        0        0        0        0
PrefetchInMem                  1466       0       0       0       0
0        0        0     1466        0        0        0        0        0
Reads                         48       0       0       0       0     31
16       0        1        0        0        0        0        0
PReadBlks                      114       0       0       0       0
80      32        0        2        0        0        0        0        0
PReadKB                           0       0       0       0       0
0        0        0        0        0        0        0        0        0
ReReads                           0       0       0       0       0
0        0        0        0        0        0        0        0        0
Writes                      2002       0       0       0       0    104
163      0      538        0        0        0        0       29
PWriteBlks                  6506       0       0       0       0    210
326      0     1115        0        0        0        0       58
PWriteKB                          0       0       0       0       0
0        0        0        0        0        0        0        0        0
GrabbedDirty                      0       0       0       0       0
0        0        0        0        0        0        0        0        0
ReadRemoteRpc                     0       0       0       0       0
0        0        0        0        0        0        0        0        0
ReadRemotePhyIO                   0       0       0       0       0
0        0        0        0        0        0        0        0        0

STATS-NAME (cont'd)         BARRAY  BLKMAP    HASH    CKPT      BM
TEST    CMID   RIDCA      LOB  LVCRID    FILE  RIDMAP   RVLOG
Finds                       2681    8329       0       0   35670
0        0        0        0        0        0        0        0
Hits                        2681    8329       0       0   35670
```

```
0       0       0       0       0       0       0       0
Hit%                        100     100       0       0     100
0       0       0       0       0       0       0       0
FalseMiss                    84    8329       0       0   16856
0       0       0       0       0       0       0       0
UnOwnRR                       0       0       0       0       0
0       0       0       0       0       0       0       0
Cloned                        0       0       0       0       0
0       0       0       0       0       0       0       0
Creates                     108     358       0       0     538
0       0       0       0       0       0       0       0
Destroys                      0     126       0       0      59
0       0       0       0       0       0       0       0
Dirties                     512     235       0       0    4644
0       0       0       0       0       0       0       0
RealDirties                 128     593       0       0     636
0       0       0       0       0       0       0       0
PrefetchReqs                  6       0       0       0       0
0       0       0       0       0       0       0       0
PrefetchNotInMem              0       0       0       0       0
0       0       0       0       0       0       0       0
PrefetchInMem                 0       0       0       0       0
0       0       0       0       0       0       0       0
Reads                       0       0       0       0       0       0
0       0       0       0       0       0       0
PReadBlks                     0       0       0       0       0
0       0       0       0       0       0       0       0
PReadKB                       0       0       0       0       0
0       0       0       0       0       0       0       0
ReReads                       0       0       0       0       0
0       0       0       0       0       0       0       0
Writes                      128     466       0       0     574
0       0       0       0       0       0       0       0
PWriteBlks                  239    3728       0       0     830
0       0       0       0       0       0       0       0
PWriteKB                      0       0       0       0       0
0       0       0       0       0       0       0       0
GrabbedDirty                  0       0       0       0       0
0       0       0       0       0       0       0       0
ReadRemoteRpc                 0       0       0       0       0
0       0       0       0       0       0       0       0
ReadRemotePhyIO               0       0       0       0       0
0       0       0       0       0       0       0

STATS-NAME                  VALUE
BusyWaits                      98
LRUNumLocks                401784
LRUNumSpinsWoTO                0      0%
LRUNumSpinLoops             4315
LRUNumTimeOuts              4315  -1.10%
BmapHTNumLocks                 0
BmapHTNumWaits                 0      0%
CacheTeamTimesWoken          182
CacheTeamNumAsleep            10
BmapHTMaxEntries            4096
BmapHTNEntries                27
```

```
BmapHTNInserts                31954
BmapHTNCollisn                  203
BmapHTNFinds                  51419
BmapHTNHits                   19576
BmapHTNHits1                  19550
BmapHTNHits2                     26
BmapHTNClears                 31933
BmapHTNLChain                     1
BmapHTNRehash                     0
BlockmapMutexsNLocks              0
BlockmapMutexsNWaits              0
BlockmapUID                    3659
BlockmapUIDnallocs             3652
BlockmapRegEver               31851
BlockmapRegisters             31844
BufHTNBuckets                  4608
BufHTNEntries                  1208
BufHTNw2orMore                  158
BufHTMaxBucketSize               19
BufHTNFoiledOps                   0
IONumLocks                        0
IONumWaits                        0      0%

==============================
Buffer Manager (Temporary)
==============================

STATS-NAME                    TOTAL    NONE  TXTPOS  TXTDOC  CMPACT
BTREEV  BTREEF      BV     VDO   DBEXT    DBID    SORT   STORE  GARRAY
Finds                        31656       0       0       0       0
0       0       0       0       0       0    1022       0       0
Hits                         31655       0       0       0       0
0       0       0       0       0       0    1022       0       0
Hit%                           100       0       0       0       0
0       0       0       0       0       0     100       0       0
FalseMiss                    23898       0       0       0       0
0       0       0       0       0       0       0       0       0
UnOwnRR                          0       0       0       0       0
0       0       0       0       0       0       0       0       0
Cloned                           0       0       0       0       0
0       0       0       0       0       0       0       0       0
Creates                       5682       0       0       0       0
0       0       0       0       0       0    1048     716       0
Destroys                      5670       0       0       0       0
0       0       0       0       0       0     821      17       0
Dirties                       6702       0       0       0       0
0       0       0       0       0       0     379       0       0
RealDirties                   5692       0       0       0       0
0       0       0       0       0       0    1048     716       0
PrefetchReqs                     1       0       0       0       0
0       0       0       0       0       0       0       0       0
PrefetchNotInMem                 1       0       0       0       0
0       0       0       0       0       0       0       0       0
PrefetchInMem                  446       0       0       0       0
0       0       0       0       0       0     446       0       0
Reads                            2       0       0       0       0       0
```

```
0       0       0       0       0       0       0       0
PReadBlks                   4096       0       0       0       0
0       0       0       0       0       0       0       0       0
PReadKB                        0       0       0       0       0
0       0       0       0       0       0       0       0       0
ReReads                        2       0       0       0       0
0       0       0       0       0       0       0       0       0
Writes                        10       0       0       0       0
0       0       0       0       0       0       0       0       0
PWriteBlks                    80       0       0       0       0
0       0       0       0       0       0       0       0       0
PWriteKB                       0       0       0       0       0
0       0       0       0       0       0       0       0       0
GrabbedDirty                   0       0       0       0       0
0       0       0       0       0       0       0       0       0
ReadRemoteRpc                  0       0       0       0       0
0       0       0       0       0       0       0       0       0
ReadRemotePhyIO                0       0       0       0       0
0       0       0       0       0       0       0       0       0

STATS-NAME (cont'd)        BARRAY  BLKMAP    HASH    CKPT      BM
TEST    CMID    RIDCA      LOB  LVCRID    FILE  RIDMAP   RVLOG
Finds                          0    8569     124       0   21939
0       0       0       0       0       2       0       0
Hits                           0    8569     124       0   21939
0       0       0       0       0       1       0       0
Hit%                           0     100     100       0     100
0       0       0       0       0      50       0       0
FalseMiss                      0    8569       0       0   15328
0       0       0       0       0       1       0       0
UnOwnRR                        0       0       0       0       0
0       0       0       0       0       0       0       0
Cloned                         0       0       0       0       0
0       0       0       0       0       0       0       0
Creates                        0    1440     777       0    1041
0       0       0       0       0       0     660       0
Destroys                       0    1434     777       0     123
0       0       0       0       0       0     660       0
Dirties                        0       0       0       0    6323
0       0       0       0       0       0       0       0
RealDirties                    0    1440     777       0    1051
0       0       0       0       0       0     660       0
PrefetchReqs                   0       0       0       0       0
0       0       0       0       0       1       0       0
PrefetchNotInMem               0       0       0       0       0
0       0       0       0       0       1       0       0
PrefetchInMem                  0       0       0       0       0
0       0       0       0       0       0       0       0
Reads                       0       0       0       0       0       0
0       0       0       0       2       0       0
PReadBlks                      0       0       0       0       0
0       0       0       0       0    4096       0       0
PReadKB                        0       0       0       0       0
0       0       0       0       0       0       0       0
ReReads                        0       0       0       0       0
0       0       0       0       0       2       0       0
```

```
Writes                          0       0       0       0      10
0       0       0       0       0       0       0       0
PWriteBlks                      0       0       0       0      80
0       0       0       0       0       0       0       0
PWriteKB                        0       0       0       0       0
0       0       0       0       0       0       0       0
GrabbedDirty                    0       0       0       0       0
0       0       0       0       0       0       0       0
ReadRemoteRpc                   0       0       0       0       0
0       0       0       0       0       0       0       0
ReadRemotePhyIO                 0       0       0       0       0
0       0       0       0       0       0       0       0

STATS-NAME                   VALUE
BusyWaits                        0
LRUNumLocks                 136253
LRUNumSpinsWoTO                  0      0%
LRUNumSpinLoops               2780
LRUNumTimeOuts                2780  -0.02%
BmapHTNumLocks                   0
BmapHTNumWaits                   0      0%
CacheTeamTimesWoken              1
CacheTeamNumAsleep              10
BmapHTMaxEntries              4096
BmapHTNEntries                  17
BmapHTNInserts                2334
BmapHTNCollisn                   0
BmapHTNFinds                   183
BmapHTNHits                      0
BmapHTNHits1                     0
BmapHTNHits2                     0
BmapHTNClears                 2327
BmapHTNLChain                    0
BmapHTNRehash                    0
BlockmapMutexsNLocks             0
BlockmapMutexsNWaits             0
BlockmapUID                   2380
BlockmapUIDnallocs            2335
BlockmapRegEver               2344
BlockmapRegisters             2334
BufHTNBuckets                 4608
BufHTNEntries                   24
BufHTNw2orMore                   0
BufHTMaxBucketSize               3
BufHTNFoiledOps                  0
IONumLocks                       0
IONumWaits                       0      0%
```

例 3：

20 分後にバッファプール (メインおよびテンポラリ) の出力を表示します。

```
sp_iqsysmon '00:20:00', 'mbufpool tbufpool'

==============================
Buffer Pool (Main)
```

```
==============================

STATS-NAME                    TOTAL    NONE  TXTPOS  TXTDOC  CMPACT
BTREEV  BTREEF      BV     VDO   DBEXT    DBID    SORT   STORE  GARRAY
MovedToMRU                  68731       0       0       0       0    9094
2767       0   21083        0        0        0        0     303
MovedToWash                      0       0       0       0       0       0
0       0       0       0       0       0       0       0       0       0
RemovedFromLRU              67564       0       0       0       0
9020    2597       0   20830        0       0       0       0     274
RemovedFromWash             11457       0       0       0       0
1559     356       0    2189        0       0       0       0      68
RemovedInScanMode               0       0       0       0       0
0       0       0       0       0       0       0       0       0
MovedToPSList                   0       0       0       0       0
0       0       0       0       0       0       0       0       0
RemovedFromPSList               0       0       0       0       0
0       0       0       0       0       0       0       0       0

STATS-NAME (cont'd)        BARRAY  BLKMAP    HASH    CKPT      BM
TEST    CMID   RIDCA     LOB  LVCRID    FILE  RIDMAP   RVLOG
MovedToMRU                  2169    8561       0       0   24754
0       0       0       0       0       0       0       0
MovedToWash                     0       0       0       0       0
0       0       0       0       0       0       0       0
RemovedFromLRU              2065    8330       0       0   24448
0       0       0       0       0       0       0       0
RemovedFromWash              233    1437       0       0    5615
0       0       0       0       0       0       0       0
RemovedInScanMode               0       0       0       0       0
0       0       0       0       0       0       0       0
MovedToPSList                   0       0       0       0       0
0       0       0       0       0       0       0       0
RemovedFromPSList               0       0       0       0       0
0       0       0       0       0       0       0       0

STATS-NAME                   VALUE
Pages                         2787
InUse                         1208 ( 43.3% )
Dirty                           11 ( 0.4% )
Pinned                          19 ( 0.7% )
Flushes                          0
FlushedBufferCount               0
GetPageFrame                  1605
GetPageFrameFailure              0
GotEmptyFrame                 1605
Washed                           0
TimesSweepersWoken               0
PriorityWashed                   0
NPrioritySweepersWoken           0
washTeamSize                    10
WashMaxSize                    455 ( 16.3% )
washNBuffers                   455 ( 16.3% )
washNDirtyBuffers                0 ( 0.0% )
washSignalThreshold             46 ( 1.7% )
washNActiveSweepers              0
```

```
NPriorityWashBuffers             0
NActivePrioritySweepers          0
washIntensity                    0
FlushAndEmpties                  0
EmptiedBufferCount               0
EmptiedSkippedCount              0
EmptiedWriteCount                0
EmptiedErrorCount                0
nAffinityTotal                   0 ( 0.0% )
nAffinityArea                    0 ( 0.0% )

==============================
Buffer Pool (Temporary)
==============================

STATS-NAME                    TOTAL    NONE  TXTPOS  TXTDOC  CMPACT
BTREEV  BTREEF      BV     VDO   DBEXT    DBID    SORT   STORE  GARRAY
MovedToMRU                  30514       0       0       0       0
0       0       0       0       0       0    1218     696       0
MovedToWash                   258       0       0       0       0
0       0       0       0       0       0       0     256       0
RemovedFromLRU              30506       0       0       0       0
0       0       0       0       0       0    1218     694       0
RemovedFromWash             30503       0       0       0       0
0       0       0       0       0       0    1218     694       0
RemovedInScanMode               0       0       0       0       0
0       0       0       0       0       0       0       0       0
MovedToPSList                   0       0       0       0       0
0       0       0       0       0       0       0       0       0
RemovedFromPSList               0       0       0       0       0
0       0       0       0       0       0       0       0       0

STATS-NAME (cont'd)         BARRAY  BLKMAP    HASH    CKPT      BM
TEST    CMID   RIDCA     LOB  LVCRID    FILE  RIDMAP   RVLOG
MovedToMRU                      0    8575     124       0   19898
0       0       0       0       0       3       0       0
MovedToWash                     0       0       0       0       0
0       0       0       0       0       2       0       0
RemovedFromLRU                  0    8569     124       0   19898
0       0       0       0       0       3       0       0
RemovedFromWash                 0    8569     124       0   19898
0       0       0       0       0       0       0       0
RemovedInScanMode               0       0       0       0       0
0       0       0       0       0       0       0       0
MovedToPSList                   0       0       0       0       0
0       0       0       0       0       0       0       0
RemovedFromPSList               0       0       0       0       0
0       0       0       0       0       0       0       0

STATS-NAME                  VALUE
Pages                        2787
InUse                          24 ( 0.9% )
Dirty                          17 ( 0.6% )
Pinned                          4 ( 0.1% )
Flushes                         0
FlushedBufferCount              0
```

```
GetPageFrame                   5684
GetPageFrameFailure               0
GotEmptyFrame                  5684
Washed                            0
TimesSweepersWoken                0
PriorityWashed                    0
NPrioritySweepersWoken            0
washTeamSize                     10
WashMaxSize                     455 ( 16.3% )
washNBuffers                     20 ( 0.7% )
washNDirtyBuffers                13 ( 0.5% )
washSignalThreshold              46 ( 1.7% )
washNActiveSweepers               0
NPriorityWashBuffers              0
NActivePrioritySweepers           0
washIntensity                     0
FlushAndEmpties                   0
EmptiedBufferCount                0
EmptiedSkippedCount               0
EmptiedWriteCount                 0
EmptiedErrorCount                 0
nAffinityTotal                    0 ( 0.0% )
nAffinityArea                     0 ( 0.0% )
```

例 4：

20 分後にプリフェッチマネージャ (メインおよびテンポラリ) の出力を表示します。

```
sp_iqsysmon '00:20:00', 'mprefetch tprefetch'

==============================
Prefetch Manager (Main)
==============================

STATS-NAME                   VALUE
PFMgrNThreads                   10
PFMgrNSubmitted                 81
PFMgrNDropped                    0
PFMgrNValid                      0
PFMgrNRead                       1
PFMgrNReading                    0
PFMgrCondVar              Locks  0  Lock-Waits 0 ( 0.0% )  Signals 0
Broadcasts  2  Waits  2

==============================
Prefetch Manager (Temporary)
==============================

STATS-NAME                   VALUE
PFMgrNThreads                   10
PFMgrNSubmitted                  1
PFMgrNDropped                    0
PFMgrNValid                      0
PFMgrNRead                       1
PFMgrNReading                    0
```

```
PFMgrCondVar              Locks  0  Lock-Waits 0 ( 0.0% )  Signals 0
Broadcasts  2  Waits  2
```

例 5：

20 分後に IQ ストアフリーリスト (メインおよびテンポラリ) の出力を表示します。

```
sp_iqsysmon '00:20:00', 'mfreelist tfreelist'

==============================
IQ Store (Main) Free List
==============================

STATS-NAME                   VALUE
FLBitCount                   74036
FLIsOutOfSpace                 NO
FLMutexLocks                    0
FLMutexWaits                    0 ( 0.0% )

==============================
IQ Store (Temporary) Free List
==============================

STATS-NAME                   VALUE
FLBitCount                    4784
FLIsOutOfSpace                 NO
FLMutexLocks                    0
FLMutexWaits                    0 ( 0.0% )
```

例 6：

20 分後にメモリマネージャ、スレッドマネージャ、CPU 使用率、トランザクションマネージャの出力を表示します。

```
sp_iqsysmon '00:20:00', 'memory threads cpu txn'

==============================
Memory Manager
==============================

STATS-NAME                      VALUE
MemAllocated                 67599536  ( 66015 KB )
MemAllocatedMax             160044816 ( 156293 KB )
MemAllocatedEver           1009672456 ( 986008 KB )
MemNAllocated                   77309
MemNAllocatedEver              914028
MemNTimesLocked                     0
MemNTimesWaited                     0      ( 0.0 %)

==============================
Thread Manager
==============================

STATS-NAME                      VALUE
ThrNumOfCpus                        4
ThreadLimit                        99
```

```
ThrNumThreads                          98      ( 99.0 %)
ThrReserved                            15      ( 15.2 %)
ThrNumFree                             55      ( 55.6 %)
NumThrUsed                             44      ( 44.4 %)
UsedPerActiveCmd                       22
ThrNTeamsInUse                          5
ThrMaxTeams                             7
NumTeamsAlloc                         238
TeamThrAlloc                          421
SingleThrAlloc                        492
ThrMutexLocks                           0
ThrMutexWaits                           0       ( 0.0 %)

==============================
CPU time statistics
==============================

STATS-NAME                          VALUE
Elapsed Seconds                     59.65     ( 25.0 %)
CPU User Seconds                    37.79     ( 15.8 %)
CPU Sys Seconds                      1.89      ( 0.8 %)
CPU Total Seconds                   39.68     ( 16.6 %)

==============================
Transaction Manager
==============================

STATS-NAME                          VALUE
TxnMgrNPending                          0
TxnMgrNBlocked                          2
TxnMgrNWaiting                          0
TxnMgrPCcondvar                  Locks     0      Lock-Wait 0 ( 0.0 %)
Signals 0  Broadcasts 2 Waits 2
TxnMgrTxnIDseq                        407
TxnMgrtxncblock                   Locks     0       Lock-Wait 0 ( 0.0 %)
TxnMgrVersionID                         0
TxnMgrOAVI                              0
TxnMgrVersionLock                Locks     0      Lock-Wait 0 ( 0.0 %)
Signals 0  Broadcasts 0 Waits 0
```

例 7：

20 分後にサーバコンテキストおよびカタログ統計の出力を表示します。

```
sp_iqsysmon '00:20:00', 'context catalog'

==============================
Context Server statistics
==============================

STATS-NAME                       VALUE
StCntxNumConns                       1
StCntxNResource                     16
StCntxNOrigResource                 18
StCntxNWaiting                       0
StCntxNWaited                        0
```

```
StCntxNAdmitted              1116
StCntxLock                  Locks  0 Lock-Waits  0 ( 0.0 %)
StCntxCondVar               Locks  0 Lock-Waits  0 ( 0.0 %)

==============================
Catalog, DB Log, and Repository statistics
==============================

STATS-NAME                  VALUE
CatalogLock             RdLocks  0   RdWaits  0 ( 0.0 %)  RdTryFails
0  WrLocks  30037  WrWaits  0 ( 0.0 %)  WrTryFail 0
DbLogMLock                  Locks  0 Lock-Waits  0 ( 0.0 %)
DbLogSLock                  Locks  0 Lock-Waits  0 ( 0.0 %)
RepositoryNList                0
RepositoryLock            Locks  1  SpinsWoTO  0 ( 0.0 %)     Spins
0  TimeOuts     0 ( 0.0 %)
```

例 8：

20 分後に、IQ RLV インメモリストアおよび LMA (Large Memory Allocator) の統計の出力を表示します。

```
sp_iqsysmon '00:20:00', 'rlv lma'

==============================
IQ In-Memory Store
==============================

STATS-NAME               VALUE
RLV Memory Limit       2048 MB
RLV Memory Used           0 MB
RLV Chunks Used              0

==============================
Large Memory Allocator
==============================

STATS-NAME               VALUE
Large Memory Space     2048 MB
Large Memory Max Fle    512 MB
Large Memory Num Fle         0
Large Memory Flexibl       0.5
Large Memory Flexibl      0 MB
Large Memory Inflexi       0.9
Large Memory Inflexi      0 MB
Large Memory Anti-St       0.5
Large Memory Num Con         0
```

sp_iqpassword プロシージャ

ユーザのパスワードを変更します。

構文 1

```
call sp_iqpassword ('caller_password', 'new_password' [, 'user_name'])
```

構文 2

```
sp_iqpassword 'caller_password', 'new_password' [, 'user_ name']
```

パラメータ

- **caller_password –** 自分のパスワード。自分のパスワードを変更する場合は、古い方のパスワードを指定します。CHANGE PASSWORD システム権限を持つユーザが別のユーザのパスワードを変更する場合は、caller_password には変更を実行するユーザのパスワードを指定する。
- **new_password –** ユーザまたは *loginname* の新しいパスワード。
- **user_name –** CHANGE PASSWORD システム権限を持つ別のユーザによってパスワードが変更されるユーザのログイン名。自分のパスワードを変更する場合は user_name を指定しない。

権限

そのシステムプロシージャに対する EXECUTE 権限が必要です。 各自のパスワードを設定する際に要求される追加のシステム権限はありません。他のユーザのパスワードを変更する場合は、CHANGE PASSWORD システム権限が必要です。

備考

ユーザパスワードは識別子です。すべてのユーザが **sp_iqpassword** を使用して自分のパスワードを変更できます。既存のユーザのパスワードを変更するには、CHANGE PASSWORD システム権限が必要です。

識別子の最大長は、128 バイトです。識別子は、次のいずれかの条件に当てはまる場合、二重引用符または角カッコで囲む必要があります。

- 識別子にスペースが含まれている。
- 識別子の先頭文字がアルファベット文字ではない (以下を参照)。
- 識別子に予約語が含まれている。
- 識別子にアルファベット文字と数字以外の文字が含まれている。
  アルファベット文字 に含まれるのは、アルファベット、アンダースコア文字 (_)、アットマーク (@)、シャープ記号 (#)、ドル記号 ($) です。データベースの照合順によって、どの文字をアルファベットまたは数字として扱うかが決まります。

例

ログインしたユーザのパスワードを irk103 から exP984 に変更します。

```
sp_iqpassword 'irk103', 'exP984'
```

ログインしたユーザが、`joe` に対する CHANGE PASSWORD システム権限を持っている場合に、ユーザ `joe` のパスワードを `eprr45` から `pdi032` に変更します。

```
call sp_iqpassword ('eprr45', 'pdi932', 'joe')
```

sp_objectpermission システムプロシージャ

指定されたロールまたはユーザ名に付与されているオブジェクト権限または指定されたオブジェクトまたは DB 領域に対して付与されているオブジェクト権限のレポートを生成します。

構文

sp_objectpermission ([*object_name*], [*object_owner*], [*object_type*])

パラメータ

- **object_name –** オブジェクト、DB 領域、ユーザ、またはロールの名前。指定しない場合、現在のユーザのオブジェクト権限がレポートされる。デフォルト値は NULL。
- **object_owner –** 指定されたオブジェクト名のオブジェクト所有者の名前。指定されたオブジェクト所有者が所有する指定されたオブジェクトのオブジェクト権限が表示される。別のユーザまたはロールが所有するオブジェクトのオブジェクト権限を取得するには、このパラメータを指定する必要がある。デフォルト値は NULL。
- **object_type –** 有効な値：
  - TABLE*
  - VIEW
  - MATERIALIZED VIEW
  - SEQUENCE
  - PROCEDURE
  - FUNCTION
  - DBSPACE
  - USER

  注意： * カラムレベルのオブジェクト権限も表示される。

  値が指定されていない場合、すべてのオブジェクトタイプの権限が返される。デフォルト値は NULL。

権限

そのシステムプロシージャに対する EXECUTE 権限が必要です。。どのユーザも **sp_objectpermission** を実行して、自分自身に付与されているすべてのオブジェクト権限を取得することができます。また、オブジェクト所有者もこのプロシージャを実行して、自分の所有するオブジェクトのオブジェクト権限を取得することができます。次のオブジェクト権限を取得するには、追加のシステム権限が必要です。

- **他のユーザに付与されたオブジェクト権限や他のユーザが所有するオブジェクトに対して付与されたオブジェクト権限** – MANAGE ANY OBJECT PRIVILEGE システム権限も必要です。
- **ロールが所有するオブジェクトに対して付与されたオブジェクト権限やロールに付与されたオブジェクト権限** – MANAGE ANY OBJECT PRIVILEGE システム権限を持っているか、そのロールのロール管理者であることも必要です。
- **DB 領域のオブジェクト権限** – MANAGE ANY DBSPACE システム権限が必要です。

備考

カラム名	データ型	説明
grantor	char(128)	付与者のユーザ ID。
grantee	char(128)	被付与者のユーザ ID。
object_name	char(128)	オブジェクトの名前。
owner	char(128)	オブジェクト所有者の名前。
object_type	char(20)	オブジェクトのタイプ。
column_name	char(128)	カラム名。
permission	char(20)	権限の名前。
grantable	char(1)	権限が付与可能かどうか。

すべての引数が任意で、次のレポートを生成することができます。

- 入力がオブジェクト (テーブル、ビュー、プロシージャ、関数、シーケンスなど) の場合、このプロシージャは、そのオブジェクトに対するさまざまなオブジェクト権限を持つすべてのロールとユーザのリストを表示します。
- 入力がロールまたはユーザの場合、このプロシージャは、ロールまたは入力に付与されているすべてのオブジェクト権限のリストを表示します。**sp_objectpermission** を実行してユーザまたはロールのオブジェクト権限を表示する場合、ロールの付与によって継承されたオブジェクト権限も表示されます。
- 入力が DB 領域名の場合、このプロシージャは、指定された DB 領域に対する CREATE 権限を持つすべてのユーザまたはロールのリストを表示します。
- デフォルトでは、オブジェクトタイプは NULL であり、指定されたオブジェクト名に一致する既存のすべてのオブジェクトタイプに対するオブジェクト権限が表示されます。

例

次の GRANT 文が実行されているとします。

```
GRANT SERVER OPERATOR TO r4;
GRANT BACKUP DATABASE TO r3 WITH ADMIN OPTION;
GRANT DROP CONNECTION TO r3 WITH ADMIN ONLY OPTION;
GRANT MONITOR TO r2;GRANT CHECKPOINT TO r1;
GRANT ROLE r2 TO r1 WITH ADMIN OPTION;
GRANT ROLE r3 TO r2 WITH NO ADMIN OPTION;
GRANT ROLE r4 TO r3 WITH ADMIN ONLY OPTION;
```

次のオブジェクト権限を検討します。

- `r5` はデータベース内のテーブル `test_tab` とプロシージャ `test_proc` を所有します。
- `r5` に対する管理権限を持つ `u5` が次の権限を付与します。
  - GRANT SELECT ON r5.test_tab TO r2 WITH GRANT OPTION;
  - GRANT SELECT (c1), UPDATE (c1) ON r5.test_tab TO r6 WITH GRANT OPTION;
  - GRANT EXECUTE ON r5.test_proc TO r3;
- `r6` に対する管理権限を持つ `u6` が次の権限を付与します。
  - GRANT SELECT (c1), REFERENCES (c1) ON r5.test_tab TO r3;

`sp_objectpermission( 'r1' )` を実行すると、次のような内容が出力されます。

表 21 : sp_objectpermission('r1') の出力例

grantor	grantee	object_name
u5	r2	test_tab
u6	r3	test_tab
u6	r3	test_tab
u6	r3	test_proc

(続き) owner	object_type	grantor
r5	TABLE	u5
r5	COLUMN	u6
r5	COLUMN	u6
r5	PROCEDURE	u6

(続き) grantable	column_name	privilege
Y	NULL	SELECT
N	c1	SELECT
Y	c1	REFERENCES
N	NULL	EXECUTE

`sp_objectpermission( 'test_tab', 'r5', 'table' )` を実行すると、次のような内容が出力されます。

表 22 : sp_objectpermission('test_tab', 'r5', 'table') の出力例

grantor	grantee	object_name
u5	r2	test_tab
u5	r6	test_tab
u5	r6	test_tab
u6	r3	test_tab
u6	r3	test_tab

(続き) owner	object_type	grantor
r5	TABLE	u5
r5	COLUMN	u5
r5	COLUMN	u5
r5	COLUMN	u6
r5	COLUMN	u6

(続き) column_name	privilege	grantable
NULL	SELECT	Y
c1	SELECT	Y

(続き) column_name	privilege	grantable
c1	UPDATE	Y
c1	SELECT	N
c1	REFERENCES	N

sp_sys_priv_role_info システム権限

システム権限を対応するシステムロールとマッピングするレポートを生成します。システム権限ごとに 1 つのローが返されます。

構文

sp_sys_priv_role_info()

権限

そのシステムプロシージャに対する EXECUTE 権限が必要です。

備考

カラム名	データ型	説明
sys_priv_name	char(128)	システム権限の名前。
sys_priv_role_name	char(128)	システム権限に対応するロール名。
sys_priv_id	unsigned int	システム権限の ID。

sp_alter_secure_feature_key システムプロシージャ

認証キー、機能リスト、またはその両方を変更して、以前に定義されたセキュリティ機能キーを変更します。

構文

```
sp_alter_secure_feature_key （
    name,
    auth_key,
    features ）
```

パラメータ

- **name –** 変更するセキュリティ機能キーの VARCHAR (128) 名。指定した名前のキーが既存である必要があります。

- **auth_key –** セキュリティ機能キーの CHAR (128) 認証キー。認証キーは、6 文字以上の空でない文字列か、または既存の認証キーが変更されないことを示す NULL である必要があります。
- **features –** キーで有効にできるセキュリティ機能のカンマ区切りのリスト (LONG VARCHAR)。feature_list には、既存の feature_list リストが変更されないことを示す NULL を指定できます。

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。また、データベースサーバ所有者であり、その接続に対する manage_keys 機能が有効である必要があります。

備考
このプロシージャを使用すると、既存のセキュリティ機能キーの認証キーまたは機能リストを変更できます。

sp_create_secure_feature_key システムプロシージャ

新しいセキュリティ機能キーを作成します。

構文

```
sp_create_secure_feature_key （
    name,
    auth_key,
    features ）
```

パラメータ

- **name –** 新しいセキュリティ機能キーの VARCHAR (128) 名。この引数は、NULL または空白文字列にできません。
- **auth_key –** セキュリティ機能キーの CHAR (128) 認証キー。認証キーは、6 文字以上の空でない文字列にする必要があります。
- **features –** 新しいキーで有効にできるセキュリティ機能のカンマ区切りのリスト (LONG VARCHAR)。機能の前に "-" を指定すると、このセキュリティ機能キーを設定してもその機能は再び有効にはならないことを意味します。

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。また、データベースサーバ所有者であり、その接続に対する manage_keys 機能が有効である必要があります。

備考
このプロシージャでは、どのユーザにも設定可能な新しいセキュリティ機能が作成されます。システムセキュリティ機能キーは、-sk データベースサーバオプションを使用して作成されます。

sp_drop_secure_feature_key システムプロシージャ

セキュリティ機能キーを削除します。

構文

```
sp_drop_secure_feature_key （ name ）
```

パラメータ

- **name –** 削除するセキュリティ機能キーの VARCHAR (128) 名。

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。また、データベースサーバ所有者であり、その接続に対する manage_keys 機能が有効である必要があります。

備考
指定したキーが存在しない場合は、エラーが返されます。指定したキーが存在する場合、それがセキュリティ機能とセキュリティ機能キーの管理が可能な最後のセキュリティ機能キーでないかぎり、削除されます。たとえば、システムセキュリティ機能キーは、manage_features と manage_keys の両方のセキュリティ機能が有効な別のキーが存在しないかぎり、削除できません。

sp_list_secure_feature_key システムプロシージャ

ディレクトリの内容に関する情報を返します。

構文

```
sp_list_secure_feature_keys （ ）
```

権限
そのシステムプロシージャに対する EXECUTE 権限が必要です。また、データベースサーバ所有者であり、その接続に対する manage_keys 機能が有効である必要があります。

備考

カラム名	データ型	説明
name	VARCHAR(128)	セキュリティ機能キーの名前。
features	LONG VARCHAR	セキュリティ機能キーによって有効化されるセキュリティ機能。

このプロシージャは、既存のセキュリティ機能キーの名前と、各キーによって有効にできるセキュリティ機能のセットを返します。

ユーザが manage_features と manage_keys のセキュリティ機能を有効にしている場合、このプロシージャはすべてのセキュリティ機能キーのリストを返します。

ユーザが manage_keys セキュリティ機能のみを有効にしている場合、このプロシージャは、現在のユーザが有効にしている機能と同じ機能またはそのサブセットを有効にするキーを返します。

sp_use_secure_feature_key システムプロシージャ

既存のセキュリティ機能キーを有効にします。

構文

```
sp_use_secure_feature_key ( name, sfkey)
```

パラメータ

- **name –** 有効にするセキュリティ機能キーの VARCHAR (128) 名。
- **sfkey –** 有効にするセキュリティ機能キーの CHAR (128) 認証キー。認証キーは 6 文字以上である必要があります。

権限

そのシステムプロシージャに対する EXECUTE 権限が必要です。

備考

このプロシージャは、指定されたセキュリティ機能キーで有効になるセキュリティ機能を有効にします。

付録：起動パラメータと接続パラメータ

start_iq ユーティリティの起動オプションと接続パラメータの参考資料です。

-ec iqsrv16 データベースサーバオプション

トランスポートレイヤセキュリティまたは暗号化を使用して、すべてのクライアントとの間で転送されるすべての Command Sequence 通信プロトコルパケット (DBLib、ODBC、OLE DB) を暗号化します。TDS パケットは暗号化されません。

構文

```
iqsrv16 -ec encryption-options ...
```

```
encryption-options :
```

```
{ NONE |
   SIMPLE |
   TLS ( [ FIPS={ Y | N }; ]
   IDENTITY=server-identity-filename;
   IDENTITY_PASSWORD=password ) }, ...
```

指定可能な値

- **NONE –** 暗号化されない接続を受け入れます。
- **SIMPLE –** 単純暗号化された接続を受け入れます。このタイプの暗号化は、すべてのプラットフォームで、また以前のバージョンのデータベースサーバとクライアントでサポートされます。単純暗号化では、サーバ認証、RSA 暗号化、またはその他のトランスポートレイヤセキュリティ機能は提供されません。
- **TLS –** RSA 暗号化で暗号化された接続を受け入れます。TLS パラメータは次の引数を受け取ります。
  - **FIPS –** FIPS 認定の RSA 暗号化の場合は、`FIPS=Y` を指定します。RSA FIPS 認定の暗号化は別の認定ライブラリを使用しますが、9.0.2 以降で RSA を指定しているクライアントと互換性があります。

    FIPS 認定コンポーネントがサポートされているプラットフォームのリストについては、http://www.sybase.com/detail?id=1061806 を参照してください。

    アルゴリズムは、証明書を作成するときに使用される暗号化と一致する必要があります。

- ***server-identity-filename* –** サーバ ID 証明書のパスとファイル名を指定します。FIPS 認定の RSA 暗号化を使用している場合は、RSA アルゴリズムを使用して証明書を生成する必要があります。
- ***password* –** サーバのプライベートキーのパスワードを指定します。このパスワードは、サーバ証明書を作成するときに指定します。

適用対象
NONE と SIMPLE は、すべてのサーバとオペレーティングシステムに適用されます。

TLS は、すべてのサーバとオペレーティングシステムに適用されます。

FIPS 認定の暗号化サポートの詳細については、http://www.sybase.com/detail?id=1061806 を参照してください。

備考
このオプションは、トランスポートレイヤセキュリティを使用してクライアントアプリケーションとデータベースサーバ間の通信パケットを安全化する場合に使用します。

-ec オプションを指定すると、データベースサーバは指定された暗号化タイプによって暗号化される接続のみ受け入れます。カンマ区切りリストで、少なくとも 1 つのサポートされているパラメータを指定してください。TDS プロトコルを介した接続は、jConnect を使用する Java アプリケーションを含みますが、-ec オプションの使用に関係なく常に受け入れられ、暗号化されることはありません。この TDS プロトコルオプションを NO に設定すると、これらの暗号化されていない TDS 接続は禁止されます。

デフォルトでは、通信パケットは暗号化されないため、セキュリティに潜在的なリスクがあります。ネットワークパケットのセキュリティが心配な場合は、-ec オプションを使用します。暗号化がパフォーマンスに及ぼす影響はごくわずかです。

データベースサーバが単純暗号化を受け入れ、暗号化されない接続を受け入れない場合、暗号化を使用しない TDS 接続以外の接続では、単純暗号化が使用されます。

`-ec SIMPLE` を指定してデータベースサーバを起動すると、データベースサーバは単純暗号化を使用した接続だけを受け入れます。TLS 接続 (RSA 暗号化、RSA FIPS 認定暗号化) は失敗し、暗号化を要求しない接続では単純暗号化が使用されます。

データベースサーバで TCP/IP 上の暗号化された接続を受け入れ、さらに共有メモリを介してローカルコンピュータのデータベースへも接続できるようにする場合は、データベースサーバの起動時に -ec オプションとともに -es オプションを指定できます。

dbrsa16.dll ファイルには、暗号化と復号化に使用される RSA コードが含まれています。dbfips16.dll ファイルには、FIPS 認定の RSA アルゴリズムのコードが含まれています。データベースサーバに接続するときに、適切なファイルが見つからなかったり、エラーが発生したりすると、データベースサーバメッセージウィンドウにメッセージが表示されます。指定されたタイプの暗号化を開始できない場合、サーバは起動しません。

クライアントとサーバで暗号化の設定が一致していることが必要です。設定が異なっていると、次の場合を除き、接続は失敗します。

- データベースサーバに対して -ec SIMPLE を指定し、-ec NONE を指定しなかった場合、暗号化を要求しない接続は許可され、自動的に単純暗号化が使用されます。
- データベースサーバ側で RSA を指定し、クライアント側で FIPS 認定の暗号化を指定している場合、またはその逆の場合には、接続は成功します。この場合、Encryption 接続プロパティはデータベースサーバ側で指定された値を返します。

注意： 強力な暗号化テクノロジはすべて、輸出規制対象品目です。

例

次の例は、暗号化されない接続と単純暗号化を使用する接続を許可します。

```
iqsrv16 -ec NONE,SIMPLE -x tcpip c:¥mydemo.db
```

次の例は、RSA サーバ証明書 rsaserver.id を使用するデータベースサーバを起動します。

```
iqsrv16 -ec TLS(IDENTITY=rsaserver.id;IDENTITY_PASSWORD=test) -x
tcpip c:¥mydemo.db
```

次の例は、FIPS 認定の RSA サーバ証明書 rsaserver.id を使用するデータベースサーバを起動します。

```
iqsrv16 -ec TLS(FIPS=Y;IDENTITY=rsaserver.id;IDENTITY_PASSWORD=test)
-x tcpip c:¥mydemo.db
```

-es iqsrv16 データベースサーバオプション

共有メモリを経由した暗号化されていない接続を許可します。

構文

```
iqsrv16 -ec encryption-options -es ...
```

適用対象
すべてのサーバとオペレーティングシステム。

備考
このオプションは、-ec オプションとともに指定された場合のみ有効です。-es オプションは、共有メモリを経由した、暗号化されていない接続を許可するようにデータベースサーバに指定します。TCP/IP を介した接続では、-ec オプションで指定された暗号化タイプを使用する必要があります。このオプションは、リモートクライアントからのデータベースアクセスには暗号化された接続を使用し、パフォーマンス上の理由から、ローカルコンピュータからのデータベースアクセスには暗号化されていない接続を使用できるようにしたい場合に便利です。

例

次の例は、単純暗号化を使用する接続と、共有メモリを経由した暗号化されない接続を許可します。

```
iqsrv16 -ec SIMPLE -es -x tcpip c:¥mydemo.db
```

TDS 通信パラメータ

サーバが TDS 接続を許可するかどうかを制御します。

使用法
TCP/IP、NamedPipes (サーバ側のみ)

値
YES, NO

デフォルト値
YES

説明
データベースサーバへの TDS 接続を許可しないようにするには、TDS を NO に設定します。サーバに対して暗号化された接続だけが行われるように保証するには、これらのポートオプションを使用して TDS 接続を禁止することが唯一の方法です。

例
次のコマンドは、TCP/IP プロトコルを使用するデータベースサーバを起動しますが、Open Client または jConnect アプリケーションからの接続を許可しません。

```
start_iq -x tcpip(TDS=NO) ...
```

索引

G

H

I

K

L

M

R

S

T

U

V

W

あ

い

お

か

す

せ

た

て

と

な

は

ひ

ふ

ま

め

も

ゆ

ら

り

ろ