IBM i 2024

IBM i コンテンツ (2024年8月版)

IBM i のセキュリティー機能を正しく設定して、より安全に利用しよう

日本アイ・ビー・エム株式会社
テクノロジー事業本部
IBM Powerテクニカルセールス

IBM i のセキュリティー機能を正しく設定して、より安全に利用しよう

IBM i は、業界で最もセキュアなシステムの 1 つと考えられています。設計の当初からセキュリティーがシステムの中核部分に組み込まれているためです。
ただし、より安全に使用するには、IBM iの基本的なセキュリティー機能を正しく理解して、設定していることが前提になります。
　当資料では、IBM iプラットフォームで使用することができる固有のセキュリティー機能と基本用語について解説します。
セキュリティ機能を正しく理解して、より安全に、IBM i を利用・活用しましょう。

目次

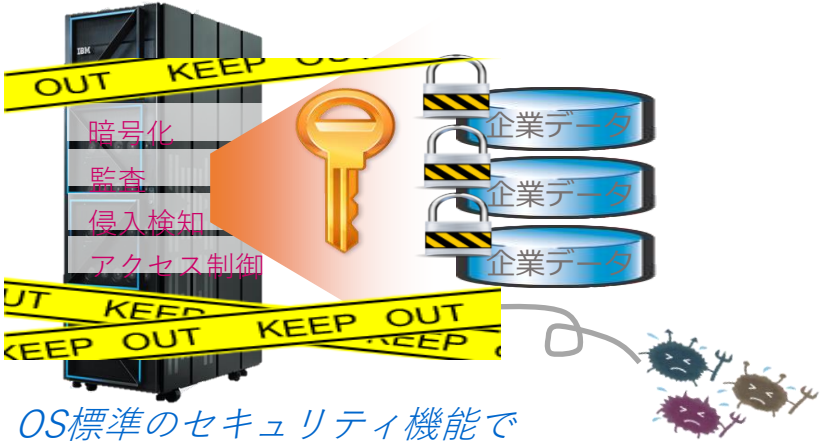
1. IBM i の堅牢なセキュリティー設計

- ✓ IBM iは、OSの標準のセキュリティー機能で、堅牢なセキュリティーを維持できる設計
- ✓ IBM iとx86サーバーでのセキュティーの違いを図示すると下記のようになる

設計に埋め込まれたセキュリティ

IBM i

堅牢なシステムでデータを死守し、即時分析に活かす



OS標準のセキュリティ機能で
データ漏洩リスクを極小化

- ◆ デザインレベルで統合化された
  セキュリティ・フレームワーク
- ◆ エンタープライズ・レベルのセキュリティ機能

x 86サーバー

多数の脆弱なプラットフォームにデータをコピー

外部からの攻撃者　*悪意を持った内部犯行者*

高まるデータ漏洩の危険性
不必要なデータ移動で高まるコスト

- ◆ 複数のベンダーから多くのツールを導入でも穴がある
- ◆ 最小限のセキュリティ認定
- ◆ 無数のウィルス被害

解説：

・IBM iは、認証、権限の付与、保全性、機密性、および監査の目的に関連する一連の豊富なセキュリティー機能およびサービスを提供します。

・ただし、組織における企業のセキュリティー・ポリシーの実装に責任を持つシステム部門は、IBM iで利用できるセキュリティー機能を把握している必要があります。

・当資料ではIBM iのセキュティー機能における基本を、IBM i7.5では必須になった、アクセス制御の観点から解説していきます。

2. IBM i セキュリティー・レベル

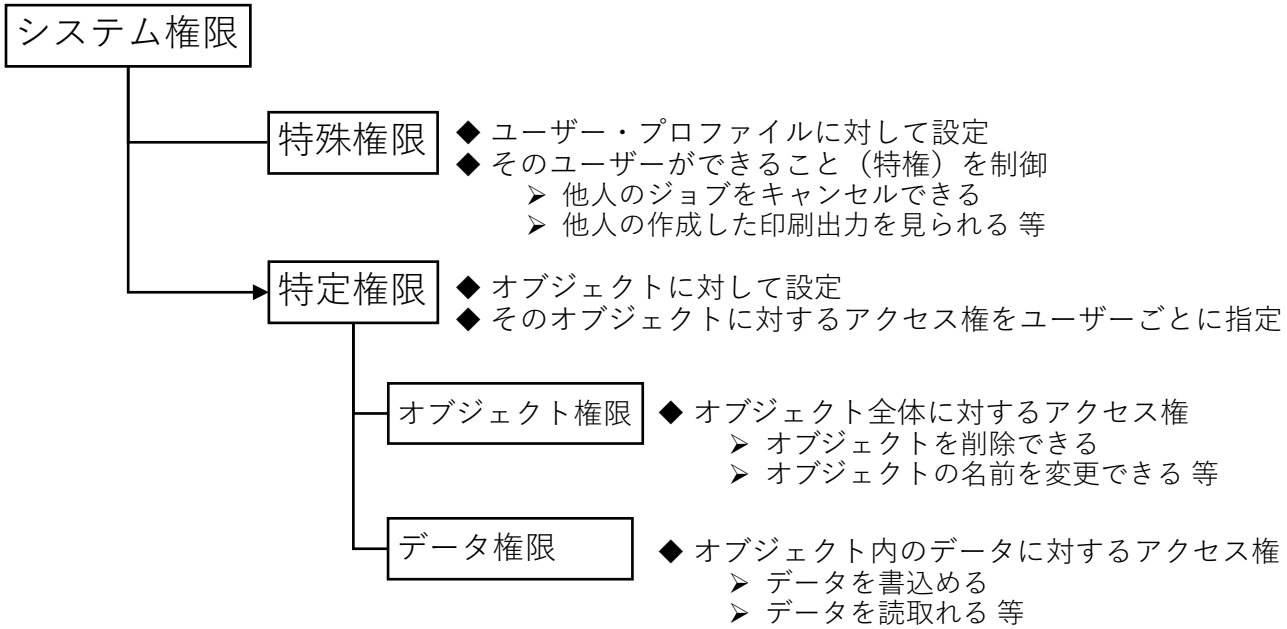
- ✓ **システム全体の機密保護レベル設定は、QSECURITYという システム値で決定される**
- ✓ **IBM i 7.5 では、システム値 QSECURITY をセキュリティー・レベル10 / 20 に設定することは不可。セキュリティティーレベルを40以上に設定することが必須**

QSECURITYシステム値	解説
10 セキュリティ機能オフ	システムにサインオン時、パスワードが必要ありません。ユーザーは、すべてのシステム資源をアクセスすることができます。現在は使用不可
20 パスワードによる機密保護のみ	システムにサインオン時、ID/パスワードを必要とします。全てのユーザーが、すべてのシステム資源をアクセスすることができます。
30 パスワードとオブジェクトによる機密保護	システムにサインオン時、ID/パスワードを必要とします。ユーザー毎に、資源保護機能が働き、ユーザーの持つアクセス権限に応じて操作が制限されます。
40 パスワード、オブジェクト、およびオペレーティング・システムの保全性	レベル30の機能が有効になります。 さらにシステム保全性機能が働き、サポートされていないインターフェースを介してオブジェクトにアクセスしようとした場合には、プログラムは正常に実行されません。**現在の一般的な利用環境においてはレベル40以上を推奨。現在の出荷時デフォルトは40になります。**
50 パスワード、オブジェクト、および拡張オペレーティング・システム保全性	レベル40の機能が有効になります。 さらに、サポートされているインターフェースに対して、サポートされていないパラメーター値を渡そうとしたり、あるいはサポートされていないインターフェースを介してオブジェクトにアクセスしようとした場合には、プログラムは正常に実行されません。US国防総省のC2セキュリティ機能要件を満たすシステム保全性が提供されます。

解説：

・ IBM i 7.5 では、システム値 QSECURITY をセキュリティー・レベル10 / 20 に設定することはできません。
ただし、OSリリースアップでは、現行のセキュリティー・レベル20・30の設定は、IBM i 7.5に移行しても維持されます。

・IBM i 7.5で、出荷時のデフォルトのQSECURITYの値は40になります。
このセキュリティ・レベルでは、ユーザー毎に、オブジェクトに対するアクセス権の設定が必要になります。



3. 特殊権限とユーザー・クラス

（1）概要

- ✓ IBM i ではユーザーID（ユーザー・プロフィール）と、重要なシステムの特定機能を実行するための特殊権限という機能を持つ

- ✓ 特殊権限は、システムの特定操作を実行するために必要となる権限
  - ➢ バックアップの実行、他のジョブの制御、システムオブジェクトへのアクセス、印刷制御等がある
  - ➢ 設定値は、*ALLOBJ、*AUDIT、*IOSYSCFG、*JOBCTL、*SAVSYS、*SECADM、*SERVICE、*SPLCTLになる

- ✓ 特殊権限のセットをユーザープロフィールに対して付与する際に、システムがデフォルトで提供するユーザー・クラスを指定する事で容易に設定が可能
  - ➢ ユーザー・クラスには、下記の5つ
    *SECOFR（システム管理担当者）、*SECADM (機密保護担当者)
    *PGMR (プログラマー)、*SYSOPR（ システムオペレーター)と
    *USER (一般ユーザー)

3. 特殊権限とユーザー・クラスとは

（2）特殊権限の詳細

- ✓ ユーザーにいくつかの特殊権限を指定することが可能
- ✓ ユーザー・プロファイルの作成時に、ユーザー・クラスに基づく特殊権限を選択

特殊権限	説明
***ALLOBJ**	*ALLOBJ特殊権限をもつユーザーは、オブジェクトがそのユーザーに対して権限を与えているかどうかに関わらず、**システム上の全てのオブジェクトにアクセス可能となる。**また、他のユーザーに対しオブジェクトの操作権限を付与することができる。但し他の特殊権限を必要な操作は実行できない。
***AUDIT**	機密保護監査の設定を変更可能。*ALLOBJ, *SECADM, *AUDITを持つユーザーは他のユーザーに*AUDIT権限を付与可能。
***IOSYSCFG**	入出力装置の構成の作成、変更を実行する事ができる。
***JOBCTL**	ジョブの実行属性、ジョブ待ち行列、スプール出力待ち行列等の制御を行なう事が可能。サブシステムの停止、起動も可能。
***SAVSYS**	システム上の全てのオブジェクトに対し、保管・復元、記憶域（ディスク上）からの開放が可能
***SECADM**	*SECADM特殊権限を持つユーザーは全てのユーザープロフィールの作成・変更・削除が可能。*SECADMおよび*ALLOBJを持つユーザーは他のユーザーに*SECADM権限を付与する事が可能。
***SERVICE**	システムサービスツール(SST)を開始するための権限
***SPLCTL**	他のユーザーが作成したものも含め、スプールファイル（印刷データ）の制御を実行可能。

解説：

・システム・セキュリティー・レベルにより、デフォルトの特殊権限をユーザー・クラスごとに決定します。特殊権限はまた、セキュリティー・レベルの変更時にユーザー・プロファイルから追加および除去されます。

3. 特殊権限とユーザー・クラスとは

（3）ユーザー・クラスと特殊権限の関係

✓ デフォルトの特殊権限が、ユーザー・クラスごとに決定される

特殊権限	説明	ユーザー・クラス				
		*USER ユーザー	*SYSOPR オペレータ	*PGMR プログラマー	*SECADM 機密保護担当	*SECOFR システム管理者
*ALLOBJ	システム上すべてのオブジェクトに対する権限	(10,20)	(10,20)	(10,20)	(10,20)	○
*AUDIT	監査機能を実行を制御する権限					○
*IOSYSCFG	システム入出力構成を変更できる権限					○
*JOBCTL	ジョブ待ち行列上にあるジョブのすべての操作を行うのに必要な権限		○	(10,20)	(10,20)	○
*SAVSYS	システムの保管、復元、および記憶域解放を行える権限	(10,20)	○	(10,20)	(10,20)	○
*SECADM	機密保護管理者権限				○	○
*SERVICE	保守機能を実行可能					○
*SPLCTL	すべてのスプール関連機能を実行可能					○
*NONE	認可される特殊権限なし	○		○		○

凡例：○:全QSECURITY値で有効、10,20 : QSECURITY値が10,20において有効

4. 特定権限とは

（1）概要

- ✓ IBM i 上の全オブジェクトは、そのオブジェクトがアクセスされた際の権限をオブジェクト毎に定義可能
- ✓ 特定権限は下記の 3 種類ある

➢ オブジェクト権限

オブジェクトの属性変更や削除など、オブジェクト全体に対する操作権限

オブジェクト名の変更、ライブラリーの移動、オブジェクトの保管・復元、所有者の変更等

➢ データ権限

データベースファイルなどオブジェクトに含まれるレコードの読み取りや変更操作に関する

権限：データの読み取り、追加、変更（更新）、削除等

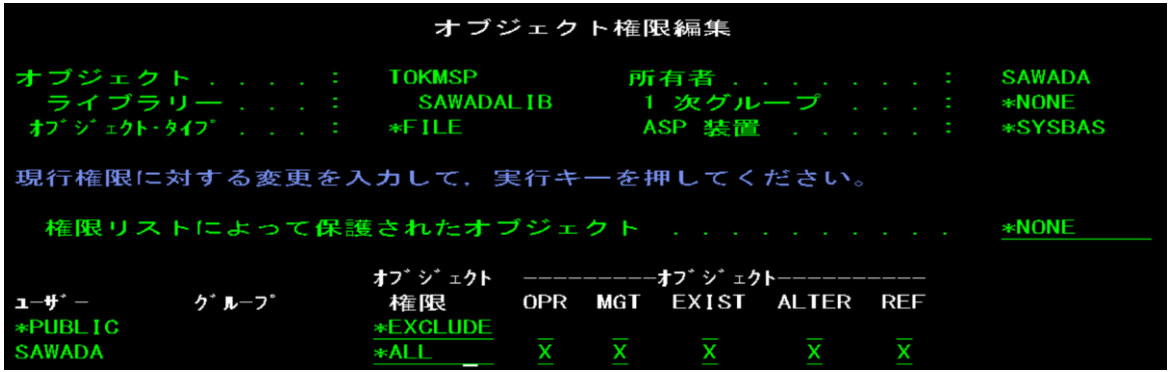
➢ フィールド権限

データベースファイルなどに含まれる個々のフィールド（カラム）に対して実行可能な操作を行う為の権限：フィールド（カラム）に対するデータの読み取り、変更、追加等

解説：

・ユーザー・プロファイルが *ALLOBJ 特殊権限を持っていると、 オブジェクト権限は無意味になります。
・出力待ち行列を保護しようと、どのように努力しても、
*SPLCTL 特殊権限を持つユーザーは、システム上の任意のスプール・ファイルを見ることができます。
*JOBCTL 特殊権限を持つユーザーは、システム操作に影響を与え、ジョブを宛先変更することができます。
*SERVICE 特殊権限を持つユーザーは、オペレーティング・システムを介さなくても、 保守ツールを使用してデータにアクセスすることができます。

・オブジェクト権限編集 (EDTOBJAUT) コマンドを使用して、ライブラリーおよびライブラリー内のオブジェクトの特定権限を指定できます。



4. 特定権限とは

（2）特定権限の詳細：オブジェクト権限（1/3）

- ✓ オブジェクト権限は、特定のオブジェクトに関する許可をユーザーに与え、そのオブジェクトに対してユーザーは何ができるかを指定
  - ➢ オブジェクト権限は、あらかじめ、*USE、*CHANGE、*ALL、および *EXCLUDE といったいくつかのシステム定義の権限が定義されている。 これらの権限はファイル、プログラム、およびライブラリーの保護に適用される。

	オブジェクト権限			
	***USE権限**	***CHANGE権限**	***ALL権限**	***EXCLUDE権限**
許可されている ファイル操作	ファイル中の情報の表示	ファイル中のレコードの表示、変更、および削除	ファイルの作成および削除。 ファイル中のレコードの追加、変更、および削除。 他人がファイルを使用する権限。	許可なし
許可されている プログラム操作	プログラムの実行	プログラムの記述の変更	プログラムの作成、変更、および削除。他人がプログラムを使用する権限。	許可なし
許容されている ライブラリー操作	ライブラリー内のオブジェクトの場合、 権限によって許可されている、特定のオブジェクトに対するすべての操作。 • ライブラリーの場合、記述情報の表示。	ライブラリー内のオブジェクトの場合、 権限によって許可されている、特定のオブジェクトに対するすべての操作。 • ライブラリーへの新規オブジェクトの追加。 • ライブラリー記述の変更。	変更権限によって許可されるすべての処理。 • ライブラリーの削除。 • ライブラリーに対する権限を他のユーザーに付与。	許可なし

解説：

・オブジェクト権限は、特定のオブジェクトに関する許可をユーザーに与え、そのオブジェクトに対して
ユーザーは何ができるかを指定できます。 具体的で詳細なユーザー権限 (たとえば、レコードの追加や変更)
を介して、オブジェクト資源を制限できます。 システム資源を使用して、*ALL、*CHANGE、*USE、
*EXCLUDE といった、特定のシステム定義の権限のサブセットへのアクセスをユーザーに与えることが
できます。

・システム定義にないユーザー定義の権限設定も可能です。その場合は、オブジェクト権限に[USER DEF]
と表示されます。

・下記のマニュアルの 「システム定義の権限」を参照
https://www.ibm.com/docs/ja/i/7.5?topic=authority-system-defined-authorities

・統合ファイルシステムのオブジェクト権限について
ルート、QOpenSys、およびユーザー定義のファイル・システムは、IBM i、PC、および UNIX** の オブジェクト管理とセキュリティーの両方の機能を組み合わせて提供します。 IBM i セッション (WRKAUT および CHGAUT) から 統合ファイル・システム・コマンドを使用すると、 すべての通常 IBM i オブジェクト権限を設定することができます。

（例）下記は、WRKAUT OBJ(‘/home/SAWADA‘)　コマンド

4. 特定権限とは

（3）特定権限の詳細：オブジェクト権限 (2/3)

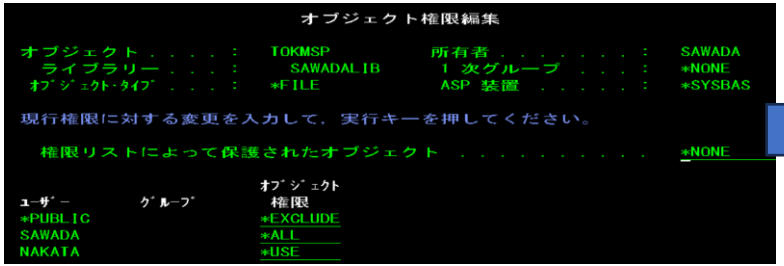
- ✓ オブジェクト権限は、特定のオブジェクトに関する許可をユーザーに与え、そのオブジェクトに対してユーザーは何ができるかを指定する。 先ほどのシステム定義を使うと下記のサブセットが設定され、データベースの場合は、データ権限も設定される。

オブジェクト権限		
オブジェクト操作権	***OBJOPR**	オブジェクト記述の参照、データ権限で定義したオブジェクトを使用する権限
オブジェクト管理権	***OBJMGT**	オブジェクトの移動、名前の変更、セキュリティの指定
オブジェクト存在権	***OBJEXIST**	オブジェクトの保管、復元、削除、所有者の変更
オブジェクト変更権	***OBJALTER**	データベース・メンバーの追加、消去、初期化、再編成の実行。データベース属性の変更（トリガーの追加、削除）、SQLパッケージ属性の変更
オブジェクト参照権	***OBJREF**	データベースの参照制約の設定
権限リスト管理	***AUTLMGT**	権限リストへのユーザーの追加、権限の追加、削除
データ権限		
読み取り	***READ**	オブジェクトの内容の表示（データベースレコードの読み取り許可）
追加	***ADD**	オブジェクトに項目を追加（データベースレコードを追加、待ち行列への追加）
更新	***UPD**	オブジェクトの内容の変更（データベースレコードの更新）
削除	***DLT**	オブジェクトから項目を削除（データベースレコードの削除、待ち行列からの削除）
実行	***EXECUTE**	プログラム、サービス・プログラムまたはSQLパッケージの実行

解説：

・オブジェクト権限の編集コマンド(EDTOBJAUT)の例
：SAWADALIB　ライブラリーのTOKMSP(物理ファイル）の場合

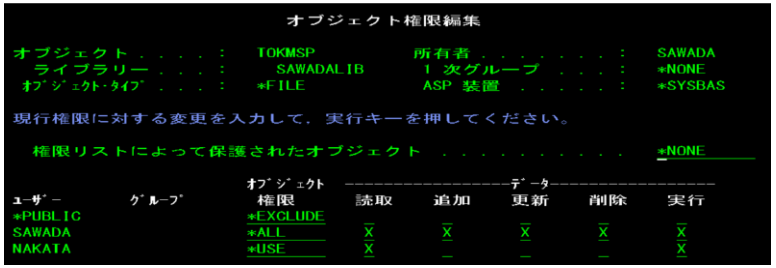
➢ EDTOBJAUT OBJ(SAWADALIB/TOKMSP)
OBJTYPE(*FILE) コマンド



F11
キー

➢ オブジェクト権限の詳細が表示される

➢ さらにF11キーを押すと
データ権限の詳細が表示される



・オブジェクト権限のサブセットについてはSQLコマンドで設定することも可能です。
https://www.ibm.com/docs/ja/i/7.5?topic=security-object-authority

4. 特定権限とは

（3）特定権限の詳細：オブジェクト権限 (3/3)

- ✓ データベース・ファイルに対してフィールド権限がサポートされる。 サポートされている権限は、管理、変更、参照、読取、追加、および更新。
- ✓ これらの権限だけが、SQL ステートメントの GRANT および REVOKE によって管理可能。 オブジェクト権限表示 (DSPOBJAUT) コマンドおよびオブジェクト権限編集 (EDTOBJAUT) コマンドによって、 これらの権限を表示のみ可能。 EDTOBJAUT コマンドを使っても、フィールド権限は表示できるだけで、編集することは不可
- ✓ ACSのスキーマ機能を使って、権限を編集可能

フィールド権限		
管理	*MGT	データベースフィールド（カラム）に対するセキュリティの指定
更新	*ALTER	データベースフィールド（カラム）属性の変更
参照	*REF	データベースフィールド（カラム）に参照制約を指定
読み取り	*READ	データベースフィールド（カラム）の内容を読み取る
追加	*ADD	データベースフィールド（カラム）にデータを追加する
更新	*UPDATE	データベースフィールド（カラム）の内容を変更する

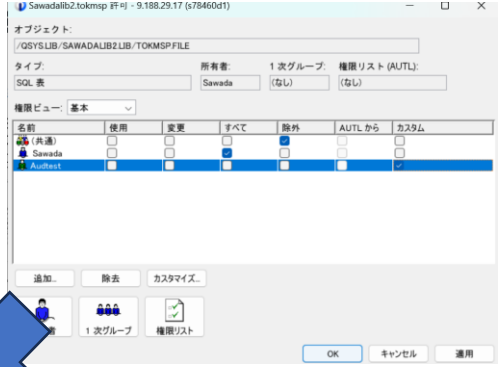
解説：

・フィールド権限のマニュアルは下記.
https://www.ibm.com/docs/ja/i/7.5?topic=accessed-field-authorities

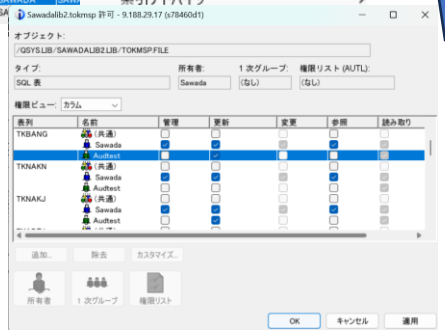
・フィールド権限は、ACSのスキーマ機能で、設定できます。
(例;SAWADALIB2ライブラリーのTOKMSP(物理ファイル）にユーザー:AUDTESTが、
フィールド:TKBANG(得意先番号）とTKNAKJ(得意先名）のみ更新できる設定

➢ ACSのスキーマを立ち上げ、表のTOKMSP
を選択し、「許可」をクリック

➢ 「権限ビュー：基本AUDTESTのユーザーでを選択。



➢ 「権限ビュー：カラムで
AUDTESTのユーザーでカラムごとに
必要権限を選択できる。



4. 特定権限とは

（4）特定権限の設定例

- ✓ 各オブジェクト（LIB、PF、LF、PGM、MENU、DSPFなどの単位）に対しての操作権限は、ユーザー、もしくは、グループ、一般ユーザー(*PUBLIC)に対して、権限グループもしくは個別の権限を設定する
- ✓ 個別のオブジェクトに権限を設定する代わりに、権限リストを作成しオブジェクトに割り振ることも可能
- ✓ また、オブジェクトの所有者、（下記のユーザー１)はこのオブジェクトに対する全権限を持つ

ユーザープロフィール	グループプロフィール	オブジェクト権限	オブジェクト権限					データ権限				
			OPR	MGT	存在	変更	REF	読取	追加	更新	削除	実行
ユーザー1		*ALL	○	○	○	○	○	○	○	○	○	○
ユーザー2		*CHANGE	○	×	×	×	×	○	○	○	○	○
	グループ1	*USE	○	×	×	×	×	○	×	×	×	○
*PUBLIC		*EXCLUDE	×	×	×	×	×	×	×	×	×	×
ユーザー3		USER DEF	ユーザーが個別にオブジェクト/データ操作権限を設定									

解説：

・オブジェクトを作成したユーザーがオブジェクトの所有者となります。

・グループプロファイルの作成のマニュアルは以下になります。
https://www.ibm.com/docs/ja/i/7.5?topic=groups-creating-group-profile

・グループプロファイルの活用について
同一アプリケーションを使用するユーザーやアプリケーション開発用のユーザーIDに関しては、
グループプロフィールを活用する事ができます。グループプロフィールを作成し、これに必要な
セキュリティ設定を行い、実際に使用するユーザーIDをこのグループプロフィールにメンバー追加することで、個々のユーザー毎にセキュリティ設定するよりも管理を用意にする事が可能です。

・グループプロフィールに属するユーザープロフィールでオブジェクトを作成すると、
オブジェクト作成時の所有者をグループプロフィールとして指定する事ができます。
これにより、異なるユーザープロフィールを使用するプログラマー間でも簡単に全て同じ
オブジェクト権限を使用する事が出来るようになります。

5. 権限リストとは

（1）概要

- ✓ ユーザーが処理する必要のある、あらゆるオブジェクトへのアクセス権をユーザーごとに明示的に規定するには、大量の重複労力が必要になる

- ✓ セキュリティ要件の同じ複数のオブジェクトに対して、共通の権限リストを指定してアクセス権管理を容易にする事ができる

- ✓ 権限リストは権限の管理を単純化する。 ユーザー権限はリスト上の各オブジェクトにではなく、権限リストに定義される。 新しいオブジェクトが権限リストで保護される場合、リスト上のユーザーは オブジェクトに対する権限を獲得できる

- ✓ アクセス権限の変更（ユーザーの追加・削除、ユーザーのアクセス権の変更等）時には権限リストだけを編集すれば、権限リストを指定している全てのオブジェクトのアクセス権限を一度に変更することができる

解説：

・権限リストのマニュアルは下記になります。
https://www.ibm.com/docs/ja/i/7.5?topic=concepts-authorization-lists
https://www.ibm.com/docs/ja/i/7.5?topic=security-planning-authorization-lists

・権限リストは、システム上の専用権限の数を減少させます。 各ユーザーは 1 つのオブジェクト、つまり権限リストに対して専用権限を持ちます。 これによってリスト上のすべてのオブジェクトに対して、ユーザー権限が与えられます。 システムの専用権限の数を減らすことには、運用を楽にすること以外に以下のような利点があります。

- ユーザー・プロファイルのサイズを小さくできる。(権限はユーザープロファイルに保持される)
- システムを保管する (SAVSYS) ときや、 セキュリティー・データを保管する (SAVSECDTA) 時のパフォーマンスを改善できる。

5. 権限リストとは

（２）使用例

（例） **SAWADALIB(ライブラリー)の下のすべてのプログラム(*PGM)に対し、**
ユーザー:NAKATA は、*ALL権限、AUDTESTは、*CHANGE権限を付与する

1．権限リスト(SAWALST1）を作成　:権限リスト作成 (CRTAUTL) コマンドを使用
CRTAUTL AUTL(SAWALST1) TEXT('SAWADALIBライブラリーのプログラム権限')

2.　権限リストに対してユーザーを追加:
：　ADDAUTLEコマンドで権限リストに対してユーザープロファイル名を追加
ADDAUTLE AUTL(SAWALST1) USER(NAKATA) AUT(*ALL)
ADDAUTLE AUTL(SAWALST1) USER(AUDTEST) AUT(*CHANGE)

3.　権限リストを、アクセス権限を付与したい個々のオブジェクトに割り当て
：GRTOBJAUTコマンドでAUTLパラメーターに権限リスト名を指定
GRTOBJAUT OBJ(SAWADALIB/*ALL) OBJTYPE(*PGM) AUTL(SAWALST1)

以上で、SAWADALIB(ライブラリー）の下のすべてのプログラム（*PGM)に対し、ユーザー:NAKATAは*ALL権限、
AUDTESTは*CHANGE権限が付与されました。

解説：

・権限リストの確認方法
権限リストの表示コマンド(DSPAUTL) で、権限リストの内容を表示できます。

- DSPAUTL AUTL(SAWALST1)　　権限リストを作成したユーザーは、権限*ALLで表示されます。

```
                          権限リスト表示
オブジェクト . . . . :   SAWALST1          所有者 . . . . . . . . . :   SAWADA
  ライブラリー . . . :     QSYS            1 次グループ . . . . :   *NONE

                    オブジェクト   リスト
ユーザー              権限         MGT
*PUBLIC             *CHANGE
SAWADA              *ALL           X
AUDTEST             *CHANGE
NAKATA              *ALL
```

- 権限リストが保護を行っているオブジェクトをすべてリストするには、画面で F15 を使用します。

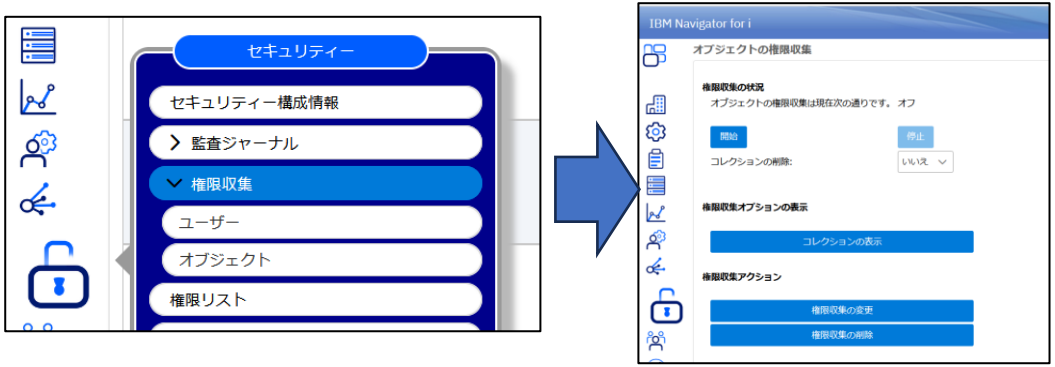
```
                      権限リスト・オブジェクトの表示
権限リスト . . . . . . . . . . . . :   SAWALST1
  ライブラリー . . . . . . . . . . :     QSYS
所有者 . . . . . . . . . . . . . . :   SAWADA
1 次グループ . . . . . . . . . . . :   *NONE

                                                    1 次
オブジェクト     ライブラリー     タイプ     所有者     グループ     テキスト
AAAAPGM          SAWADALIB       *PGM       SAWADA     *NONE        EOL/400 パッチ実習
BATCHFTP         SAWADALIB       *PGM       SAWADA     *NONE        EOL/400  FTP テスト
BCH110           SAWADALIB       *PGM       SAWADA     *NONE        EOL/400 バッチ・プ
BCH120           SAWADALIB       *PGM       SAWADA     *NONE        EOL/400 バッチ・プ
BPL010           SAWADALIB       *PGM       SAWADA     *NONE        EOL/400 バッチ実習
BPL030           SAWADALIB       *PGM       SAWADA     *NONE        EOL/400 バッチ実習
FPROC            SAWADALIB       *PGM       SAWADA     *NONE
HELLO            SAWADALIB       *PGM       SAWADA     *NONE
IPH110           SAWADALIB       *PGM       SAWADA     *NONE        EOL/400 対話型 (1
                                                                     続く ...
```

6. オブジェクトの権限収集

（1）概要

- ✓ オブジェクトの権限収集機能とは
  - ➢ 権限検査に関連したデータを収集する機能。分析するツールも付属。
  - ➢ 権限収集を使用することで、セキュリティー管理者はアプリケーションを正常に実行できるようにするためにオブジェクトに必要な最小限の権限を決定
  - ➢ IBM i 7.4 権限収集サポートにより、ユーザーがアクセスする特定のオブジェクトに関する権限情報の収集が可能になった
- ✓ 使用方法
  - ➢ すべての機能は、CLコマンドでも可能だが、「IBM Navigator for i」のセキュリティ→「権限収集」メニューから実行できる



解説：

・IBM i で使用されている業務アプリケーションには、オブジェクトに対して過剰な権限が付与されていることが多い

・従来、アプリケーション内のオブジェクトの共通権限 (*PUBLIC) は、アプリケーションの実行に必要な権限を超える権限値に設定されました。 例えば、 物理ファイル(*FILE) に対する共通権限は、アプリケーションがデータに対する *USE 権限を必要とする場合でも、*CHANGE に設定できます。

・ユーザーがアプリケーションの外部からこの特定のテーブル・オブジェクト内のデータを変更できるようになるため、このような過度の権限の設定はシステムの機密漏れを引き起こします。

・ 権限収集サポートは、アプリケーション・オブジェクトのセキュリティーをロックダウンするのに役立つツールを機密保護管理者とアプリケーション・プロバイダーに提供するように設計されています。

・収集できるオブジェクトのタイプは、QSYS ファイル・システム、root (/)、QOpenSys、
ユーザー定義ファイル・システム、文書ライブラリ・オブジェクトです。

6. オブジェクトの権限収集

（1）使用例（1 / 2）

✓ （例）SAWADALIB のFILE(HINMSP)である品目マスターのオブジェクトの権限収集をして分析する

①IBM Navigator for iでは、「権限収集の変更」で、オブジェクトを指定する。ここでは、ライブラリ「SAWADALIB」のファイル「HINMSP」を指定して[OK]をクリック

②メニューから「オブジェクト権限収集の開始」を実行

解説：

・Navigator for iが使えない場合はコマンドでも収集設定と開始を実行できます。

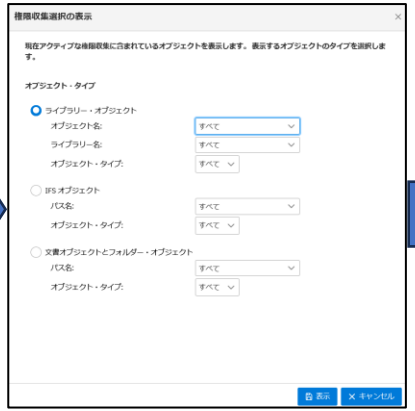
コマンド例：
収集：CHGAUTCOL OBJ('/QSYS.LIB/SAWADALIB.LIB/HINMSP.FILE') AUTCOLVAL(*OBJINF)
開始：STRAUTCOL TYPE(*OBJAUTCOL)
収集の終了：ENDAUTCOL TYPE(*OBJAUTCOL)

6. オブジェクトの権限収集

（1）使用例（2 / 2）

✓ （例）SAWADALIB のFILE(TOKMSP)である得意先マスターのオブジェクトの権限収集をして分析する

③このあと、何日か現行業務で使ってもらい、
業務に必要な権限を収集する。
Navigator for iで、権限収集を「停止」をクリック
「コレクションの表示」をクリック　　そのままで「表示」



④下記の表示で、
現行権限と必須権限とあるが、業務で必要なのは必須権限です。

ユーザー「KAWASAKI」は、現行権限は*ALLOBJであるが、
必須権限では「*READ *UPD」。
ユーザー「YAMADA」も、必須権限「*READ」でOK。
ユーザー毎に最低必要な権限に、することが推奨です。

解説：

・権限収集後に、SQLコマンドでも、権限収集データを表示できます。
　自由に項目を選択できるので、大量データの場合には、便利です。

（例）SAWADALIBライブラリーのHINMSPファイルの権限収集のデータ表示するSQLコマンド

```
SELECT * FROM QSYS2.AUTHORITY_COLLECTION_OBJECT
  WHERE SYSTEM_OBJECT_SCHEMA = 'SAWADALIB'   AND
  SYSTEM_OBJECT_TYPE = '*FILE'  AND SYSTEM_OBJECT_NAME = 'HINMSP' ;
```

*Untitled 1

```
1 SELECT * FROM QSYS2.AUTHORITY_COLLECTION_OBJECT
2   WHERE SYSTEM_OBJECT_SCHEMA = 'SAWADALIB'   AND
3   SYSTEM_OBJECT_TYPE = '*FILE'  AND SYSTEM_OBJECT_NAME = 'HINMSP' ;
```

Authorization Name AUTHORIZATION_NAME	Check Timestamp CHECK_TIMESTAMP	System Object Name SYSTEM_OBJECT_NAME	System Object Schema SYSTEM_OBJECT_SCHEMA	System Object Type SYSTEM_OBJECT_TYPE	ASP Name ASP_NAME	ASP Number ASP_NUMBER	Object Name OBJECT_NAME	Object Schema OBJECT_SCHEMA	Object Type OBJECT_TYPE	Authorization List AUTHORIZATION_LIST	Au Ch Su AU
KAWASAKI	2024-07-29 13:43:01.602319	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
KAWASAKI	2024-07-29 13:43:01.602454	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
KAWASAKI	2024-07-29 13:43:01.601704	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
KAWASAKI	2024-07-29 13:43:01.602139	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
SAWADA	2024-07-29 13:40:58.213591	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
SAWADA	2024-07-29 13:40:58.213705	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
SAWADA	2024-07-29 13:40:58.213088	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
SAWADA	2024-07-29 13:40:58.213413	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
YAMADA	2024-07-29 13:41:44.859122	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
YAMADA	2024-07-29 13:42:02.411861	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
KAWASAKI	2024-07-29 13:43:13.140898	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
SAWADA	2024-07-29 13:41:13.451007	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
KAWASAKI	2024-07-29 13:43:01.602545	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
KAWASAKI	2024-07-29 13:43:01.602418	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
SAWADA	2024-07-29 13:40:58.213793	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1
SAWADA	2024-07-29 13:40:58.213669	HINMSP	SAWADALIB	*FILE	*SYSBAS	0	HINMSP	SAWADALIB	-	-	1

まとめ：セキュリティの維持と向上のために

- ✓ **IBM i のセキュリティに必要な機能を学び、活用する**

- ✓ **IBM i を最新の状態に保ちましょう**
  OSバージョン、テクノロジー・リフレッシュ、PTFレベルをなるべく最新に！

- ✓ **IBM i のユーザーの権限を最小に**
  IBM i 7.4から導入されたオブジェクト権限の収集機能を使用し、
  必要な最低限の権限を調査しましょう。

- ✓ **データの回復のテストと準備**
  完全に分離、およびセグメント化されたバックアップと、
  計画的に復元のテストをしましょう。

7. 補足情報

1. IBM i のセキュリティー
   https://www.ibm.com/docs/ja/i/7.5?topic=security

2. IBM iセキュリティーの概要
   https://www.ibm.com/docs/ja/i/7.5?topic=reference-introduction-i-security

3. システム・セキュリティーの計画と設定
   https://www.ibm.com/docs/ja/ssw_ibm_i_75/pdf/rzamvpdf.pdf

4. 特定権限は、マニュアル上では、下記の「資源保護」の項目に詳しい記述あります。
   https://www.ibm.com/docs/ja/i/7.5?topic=concepts-resource-security

5. iMagazine 「IBM i 7.4はデータセキュリティを強化　～オブジェクトごとに権限設定が可能に」
   https://www.imagazine.co.jp/feature-ibm-i-7-4-part8/

IBM i 関連情報

IBM i ポータル・サイト
https://ibm.biz/ibmijapan

i Magazine (IBM i 専門誌。春夏秋冬の年4回発刊)
https://www.imagazine.co.jp/IBMi/

IBM i World 2023 オンデマンド・セミナー
https://ibm.biz/ibmiworld2023

IBM i World 2022 オンデマンド・セミナー
https://video.ibm.com/recorded/132423205

月イチIBM Power情報セミナー「IBM Power Salon」
https://ibm.biz/power-salon

IBM i 関連セミナー・イベント
https://ibm.biz/powerevents-j

IBM i Club (日本のIBM i ユーザー様のコミュニティー)
https://ibm.biz/ibmiclubjapan

IBM i 研修サービス (i-ラーニング社提供)
https://www.i-learning.jp/service/it/iseries.html

IBM Power Systems Virtual Server 情報
https://ibm.biz/pvsjapan

IBM i 情報サイト iWorld
https://ibm.biz/iworldweb

IBM i サポートロードマップ
https://www.ibm.com/downloads/cas/JB8AXO9V

IBM i 7.5 技術資料
https://www.ibm.com/docs/ja/i/7.5

IBM Power ソフトウェアのダウンロードサイト (ESS)
https://ibm.biz/powerdownload

Fix Central (HW・SWのFix情報提供)
https://www.ibm.com/support/fixcentral/

IBM My Notifications (IBM IDの登録 [無償] が必要)
「IBM i」「9009-41G」などPTF情報の必要な製品を選択して登録できます。
https://www.ibm.com/support/mynotifications

IBM i 各バージョンのライフサイクル
https://www.ibm.com/support/pages/release-life-cycle

IBM i 以外のSWのライフサイクル (個別検索)
https://www.ibm.com/support/pages/lifecycle/

IBM i Advantage 2024 開催決定!

12月3日(火)・4日(水)
IBM虎ノ門イノベーションスタジオ (メイン会場)
IBM大阪中之島フェスティバルタワー・ウエスト (中継)

12月24日(火)
Webセミナー + Q&Aセッション

今から**カレンダーブロック**をお願いいたします。
下記サイトに最新情報を掲載します↓

https://ibm.biz/ibm-power-user-**community**

IBM i
continuous innovation
continuous integration
Advantage 2024