IBM i 2024

IBM i コンテンツ (2024年7月版)

ハッキング未遂・情報漏洩・情報改ざんを、牽制・早期発見! IBM i の監査ジャーナルを使ってみよう

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

ハッキング未遂・情報漏洩・情報改ざんを、牽制・早期発見!
IBM i の監査ジャーナルを使ってみよう

セキュリティー監査は、システムのセキュリティーが適切に行われていることを確認する作業で、定期的に行うことが推奨されています。具体的なチェック項目としては、システム値、ユーザープロフィールとパスワード、オブジェクトの権限設定等があります。まず適切なセキュリティー設定がなされた上で、その設定が正しく行われているか、セキュリティーを破ろうとした形跡がないか、を確認するために、監査ジャーナルを使うことができます。

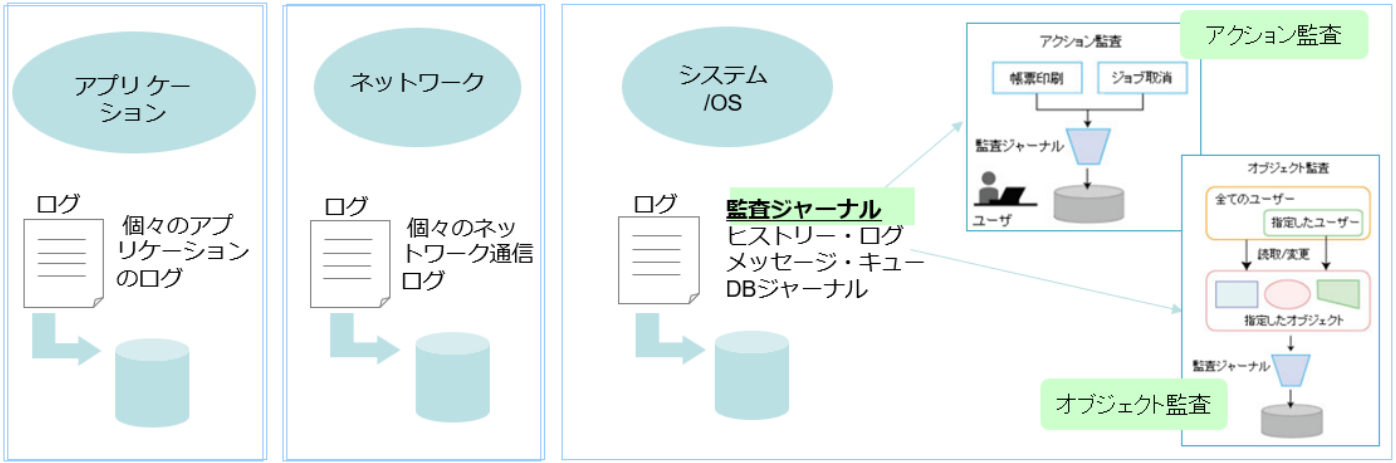
　システム基盤の管理のツールとして、監査ジャーナルを有効活用してください。

目次

1. IBM i 標準の監査ログ機能

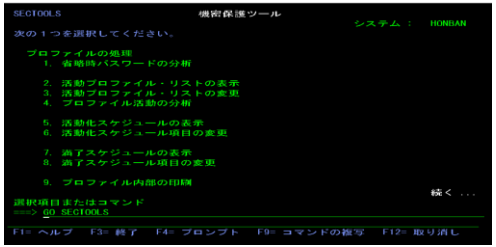
✓ IBM iは、OS標準機能で、詳細なロギングが可能
- アプリケーション/ネットワークレベルのロギング
- システム/OSレベルのロギング
  監査ジャーナル、システムヒストリー・ログ、メッセージ・キュー、DBジャーナル

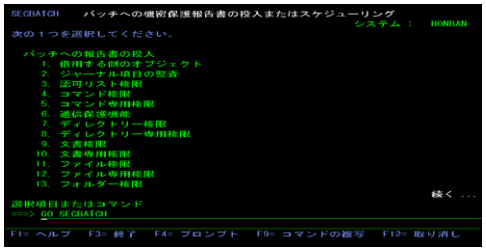
✓ 監査ジャーナル＝「アクション監査」と「オブジェクト監査」の2種類の監査
- 「アクション監査」：オブジェクトの作成や削除、変更、ジョブの取り消し、帳票印刷などユーザーの行為のログを取得
- 「オブジェクト監査」は、指定したオブジェクトにユーザーが読取、変更などのアクセスを行った際のログを取得



解説1：

・監査ジャーナルは「セキュリティー監査」のためのツールの1つです。
「セキュリティー監査」の範囲は監査ジャーナルで実現できるものよりも少し広く、監査ジャーナルだけでセキュリティー監査が完結するわけではありません。監査ジャーナル以外にもIBM i標準でセキュリティー監査を行うツールが幾つか提供されており、GO SECTOOLSやGO SECBATCHメニューから使用することができます。





・<ご注意> 監査ジャーナルは、セキュリティーが設定が適切であることを確認するもので、適切なセキュリティー設定が行われていることが前提です。
すなわち、まずシステムで適切なセキュリティー設定、権限設定を行ったうえで、その設定が守られているか、漏れがないかをチェックするためのものです。「とりあえずアクセスログを全部とっておきたい」という目的で監査ジャーナルを使用すると、取得されるログのサイズが膨大になり、システムのパフォーマンスにも影響するので、お勧めできません。

・監査ジャーナルは、指定した条件でアクセスログを取得します。
監査ジャーナルでは、全ユーザーが予め設定した条件に合う行動をとった場合に、そのイベントがジャーナル項目として順次記録されます。レシーバーは1時点ではシステムに一つです。

解説2：

・監査ジャーナルで取得可能な主な情報は下記になります。

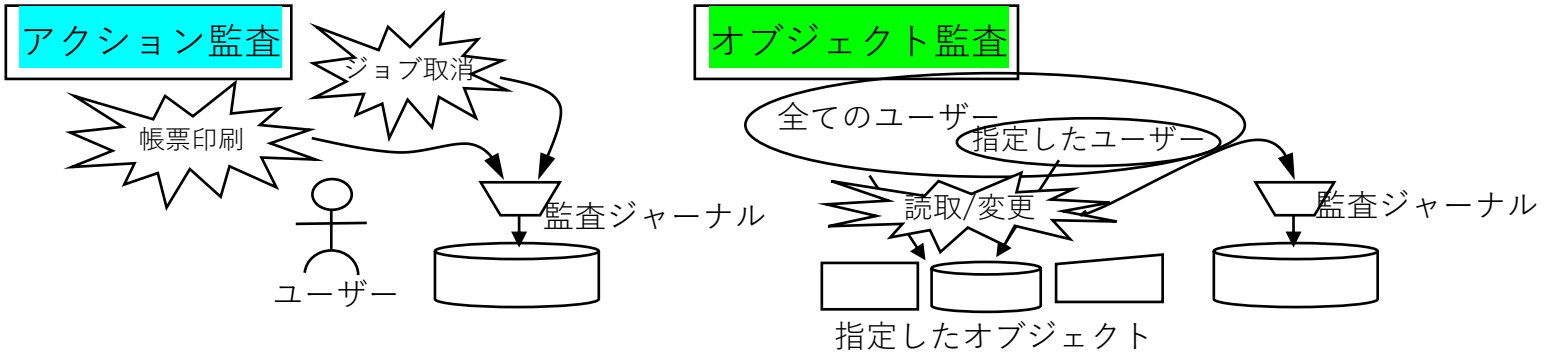
サイン・オンの失敗、拒否されたオブジェクト・アクセス
実行したコマンド
オブジェクトの作成・削除
ジョブの開始／保留／停止／取り消し／変更／終了
オブジェクトの移動、名前の変更
システム配布登録簿の変更　光ディスク・ディレクトリーの作成、削除
借用権限でのオブジェクト・アクセス
プログラム保全性エラー（システムＡＰＩ使用違反など）
スプール・ファイルの印刷、直接印刷、リモート印刷装置への送信・保管、復元
ユーザー・プロフィールの変更
システム値の変更
サービス・ツールの使用
スプール・ファイルの作成、コピー、送信
システム応答リスト、電源のオン／オフスケジュール

2. 監査ジャーナル … アクション監査とオブジェクト監査

（1）概要

✓ アクション監査（処置監査）
-ユーザーの行為を記録
-全ユーザー共通の設定＋ ユーザー個別の追加設定が可能

✓ オブジェクト監査
-オブジェクトを指定して、全ユーザーまたは指定ユーザーからのアクセスを記録
-記録されるアクセスは変更のみ/読取+変更 のどちらかを指定
-全オブジェクトを指定した設定はできない



解説：

・監査ジャーナルで記録されるセキュリティー・イベントには、大きく分けて、ユーザーの「行為」を記録するのと、特定のオブジェクトへ「アクセス」を記録するものがあります。
前者を「アクション監査」、後者を 「オブジェクト監査」と呼びます。 システムの権限設定で「特殊権限」と「特定権限」があるのと同じ考え方です。

・アクション監査はシステム全体に対して設定することも、個々のユーザーに対して設定することも可能です。

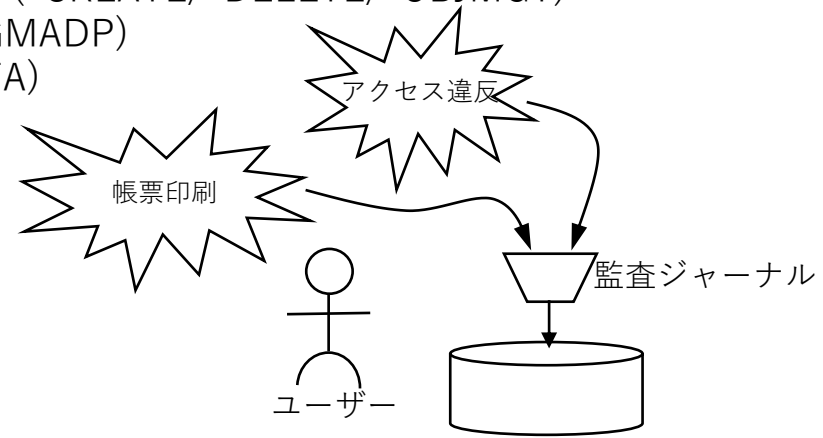
・オブジェクト監査は、監査対象となるオブジェクトに対して属性を設定することで開始されます。
オブジェクト毎に、あらゆるユーザーからのアクセスを記録するのか、特定のユーザーからのアクセスだけを記録するのかを設定できます。オブジェクト監査では、オブジェクトが変更された場合だけ記録することができます。さらに、オブジェクトが読取られただけでもログを記録することができます。
変更/読取ともさらに細かいサブタイプが定義されており、記録される内容は多岐に渡ります。

2. 監査ジャーナル …アクション監査とオブジェクト監査

（2）アクション監査・・全ユーザー共通のアクション監査

- ✓ システム値 QAUDLVL に監査する行為を指定
- ✓ 全ユーザーに対して行う場合は、システム値QAUDCTLに*AUDLVLを指定することで開始される

【例】
・権限のない操作を実行（サインオン失敗、オブジェクトのアクセス違反等）(*AUTFAIL)
・ジョブの開始/終了、他のジョブの保留、解放、停止、続行、変更 (*JOBDTA)
・オブジェクトの作成/削除/移動/名前変更 (*CREATE/*DELETE/*OBJMGT)
・借用権限を使用したプログラム実行 (*PGMADP)
・スプールファイルの印刷/送信 (*SPLFDTA)
・オブジェクトの保管/復元 (*SAVRST) 等



解説：

・アクション監査はシステム全体で全ユーザーに対して行うことも、個別のユーザーを指定して行うことも可能です。（両者の組合わせも可能）全ユーザーに対して行う場合はシステム値QAUDCTLに*AUDLVLを指定することで開始されます。
ユーザーのどのような行為を記録するかは、システム値QAUDLVLに指定します。
QAUDLVLには最大16の値を指定でき、17以上指定したい場合はシステム値QAUDLVL2に設定します。

・典型的には、まず、最低次の項目を設定することをご検討ください。

*AUTFAIL
与えられた特殊権限/特定権限を越えてなにかをしようとしたすべてのアクセス違反がログされます。
権限がないために失敗したサインオン、権限、ジョブの実行等
装置から入力された不正なパスワードまたはユーザー ID等

*JOBDTA
ユーザーによるジョブの開始/停止およびジョブに対する操作が記録されます。
保留、解放、停止、続行、変更、切断、終了、異常終了 等

*PGMFAIL
システムＡＰＩ等を使って与えられた権限を越えて実行しようとした行為が記録されます。
ブロックされた命令のログ、妥当性検査値の障害のログ、ドメイン違反 等

その他の重要な設定値として、*CREATE *DELETE *SECURITY *SAVRST 等があります。

2. 監査ジャーナル …アクション監査とオブジェクト監査

（3）アクション監査 … ユーザー個別のアクション監査

✓ ユーザープロフィールに対して監査レベル（AUDLVL）属性を指定
-ユーザーに対する監査レベルは、ユーザー監査変更(CHGUSRAUD)コマンドを使
- *CMD以外はシステム値 QAUDLVLと共通

✓ 共通のアクション監査と両方の設定が有効
-一般ユーザー → 共通アクション監査、
*SECOFRや*ALLOBJを持つユーザー → 追加で個別アクション監査等の使い分け
-ユーザープロフィールを設定し、システム値 QAUDCTLに*AUDLVL, QAUDLVLに
*NONEとすることで特定のユーザーのみを監査することも可能

解説：

・アクション監査はユーザープロフィールごとに行うことも可能です。ユーザープロフィールは「監査レベル」属性を持っており、監査するアクションをユーザープロフィールに指定すれば、システム値QAUDCTLが*AUDLVLになっていれば該当の行為が記録されます。ユーザーごとのアクション監査とシステム全体のアクション監査は重複して設定可能です（両方が有効）

・*ALLOBJ特殊権限を持つユーザーの行動には特に注意が必要なので、一般のユーザーはシステム全体で設定に従い、*ALLOBJや*SECOFRクラスのユーザーのみをユーザー個別の監査対象行為を追加して運用する、という使い方が想定されています。

・ユーザープロフィールに設定できる監査対象行為は、システム値QAUDLVLに指定できるもののサブセットに、*CMDを加えたものです。*CMDはユーザープロフィールにのみ設定可能な値で、ユーザーが実行したコマンド文字列を記録することができます。

2. 監査ジャーナル …アクション監査とオブジェクト監査

（4）オブジェクト監査

✓ **オブジェクトを指定して、ユーザーからのアクセスを記録**

-全ユーザーまたは指定したユーザー

-記録するアクセスの設定は2種類

読取り+変更 （*ALL）

変更のみ（*CHANGE）

（記録されるアクセスは多種類）

✓ **全ユーザーに対するオブジェクト監査**

-システム値 QAUDCTLに*OBJAUD指定

-さらに、監査するオブジェクトにOBJAUDパラメータ指定

*CHANGEまたは*ALL

コマンド

CHGOBJAUD（QSYS.LIB）

CHDAUD（その他IFS）

2. 監査ジャーナル …アクション監査とオブジェクト監査

（4）オブジェクト監査

✓ **ユーザー個別のオブジェクト監査**

-システム値 QAUDCTLに*OBJAUD指定

-さらに、監査するオブジェクトにOBJAUDパラメータ *USRPRF 指定

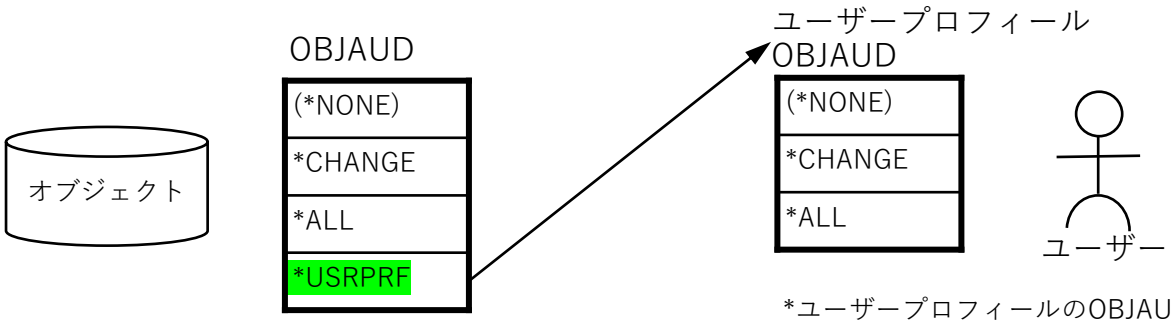
CHGOBJAUD

-ユーザープロフィールのOBJAUDパラメータを設定

*CHANGEまたは*ALL

コマンド

CHGUSRAUD



*ユーザープロフィールのOBJAUD値はオブジェクトの
OBJAUDが*USRPRFになっていない限り参照されません

解説：

・オブジェクト監査はシステム値QAUDCTLに*OBJAUDを指定することで開始され、個々のオブジェクトに対して監査属性を設定することで開始され、監査属性は*CHANGEまたは*ALLに設定されたオブジェクトに対するアクセスが記録されます。*CHANGEが指定されたオブジェクトは変更操作のみ、*ALLが指定されたオブジェクトは*CHANGEの際に記録されるアクセスを含む全アクセスが記録されます。*CHANGEでも*ALLでもアクセスには複数のサブタイプが定義されており、多様な情報が記録されます。

・オブジェクトの監査値は、CHGOBJAUDおよびCHGAUDコマンドを使って設定しますが、ライブラリーやディレクトリーを指定してその下のオブジェクトをすべて同じ属性に設定することも可能です。

・オブジェクトの監査値に*CHANGEや*ALLを指定した場合は全てのユーザーからのアクセスが記録されますが、*USRPRF と指定することもでき、その場合アクセスしてきたユーザープロフィールのオブジェクト監査値が参照され、これにしたがってアクセスが記録されるかどうかが決まります。ユーザープロフィールにはオブジェクト監査値として*CHANGEまたは*ALLを指定することができます。

・ユーザープロフィールにはアクション監査値（処置監査値）とオブジェクト監査値の両方を指定することができます。

3. 監査ジャーナルを使ってみよう(設定方法)

(1) 概要

- ✓ セキュリティー・ポリシーの決定
  - ➢ アクション監査、オブジェクト監査、ユーザー監査
- ✓ 準備（作成・設定）
  - ➢ 監査ジャーナル、ジャーナル・レシーバーの作成
  - ➢ システム値、ユーザー・プロファイル、オブジェクト
- ✓ ３つの監査タイプを構成
  - ➢ システム全体の監査
    - アクション監査
    - オブジェクト・アクセス監査
  - ➢ 特定のオブジェクトを対象にした監査
  - ➢ 特定のユーザーを対象にした監査
    - 追加のアクションの監査
    - 選択したオブジェクトの監査

解説：

IBM iでセキュリティー監査を行うためには、監査ジャーナルを利用します。監査を実施するための準備の手順は、次の通りです

・セキュリティー・ポリシーの決定　＜当資料では、この部分の作業は省略しています。＞

監査を実施するにあたりセキュリティー・ポリシーに従って、次の監査する範囲を決定します。

アクション・イベント
全てのサーバーのユーザーのセキュリティーに関するイベントの記録の決定
追加に特定ユーザーの監査をするかどうか決定
サーバー上の特定オブジェクトの監査を実施するかどうか決定
全てのユーザーか特定ユーザー用にオブジェクト監査をするかどうか

・ジャーナル・レシーバー、ジャーナルの準備

監査ジャーナル、ジャーナル・レシーバーの作成

監査を実施するためには、監査ジャーナル用のジャーナル、ジャーナル・レシーバーを作成する要があります。システムは、自動で、ジャーナル、ジャーナル・レシーバーを作成しません。
作成するジャーナルは、QSYS/QAUDJRNです。

ジャーナル・レシーバーの作成

QSYS以外のライブラリーに作成します。

ジャーナルの作成

・システム値

監査関連のシステム値の設定

（２）監査ジャーナルの設定をしてみよう

✓ 下記は、設定例です。最初に、セキュティ・ポリシーの決定が必要ですが、ここでは省略しています。監査ジャーナルの設定は、自社に合わせてカスタマイズしてください。

１．監査用のジャーナル・レシーバー、ジャーナルの作成

①監査用ジャーナル・レシーバー、ジャーナル保管用のライブラリーを作成

（例）CRTLIB LIB(JRNRCV) TEXT(' 監査ジャーナル・レシーバー用 ')

②監査用ジャーナル・レシーバーの作成

（例）CRTJRNRCV JRNRCV(JRNRCV/AUDRCV0001) TEXT(' 監査用レシーバー ‘)

③監査用ジャーナルを作成（QSYS/QAUDJRNを作成）

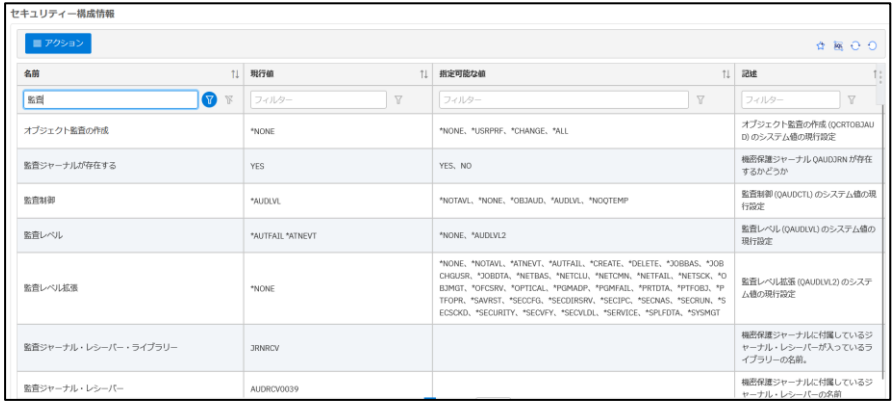
（例）CRTJRN JRN(QSYS/QAUDJRN) JRNRCV(JRNRCV/AUDRCV0001)

解説：

・作成したジャーナル環境は、下記のコマンドで確認できます。
WRKJRNA JRN(QSYS/QAUDJRN)

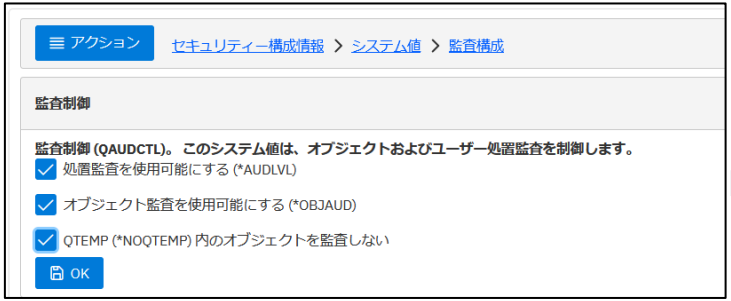
```
                        ジャーナル属性の処理

ジャーナル . . . . . :   QAUDJRN          ライブラリー . . . . :   QSYS

接続されたレシーバー . . :   AUDRCV0001       ライブラリー . . . . :   JRNRCV

テキスト . . . . . :   *BLANK

ASP . . . . . :   1                ジャーナル処理されたオブジェクト:
メッセージ待ち行列 . :   QSYSOPR             現行 . . . . . :         1
  ライブラリー . . . :     *LIBL             最大 . . . . . :    250000
レシーバーの管理 . . :   *SYSTEM           回復カウント . . . . :   *SYSDFT
レシーバーの削除 . . :   *NO               レシーバーサイズオプション . :   *RMVINTENT
ジャーナル・キャッシュ . . . :   *NO                                  *MAXOPT2
遅延の管理 . . . . . :   10
遅延の削除 . . . . . :   10
ジャーナル・タイプ . :   *LOCAL
ジャーナル状態 . . . :   *ACTIVE
項目データの最小化 . :   *NONE
```

・あるいは、Navigator for iでも確認できます。　名前のところに「監査」と入力すると監査の関連情報が表示されます。
セキュリティーのアイコンで、セキュリティー構成情報を選択

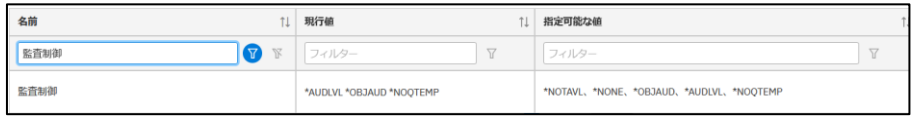


2．システム値QAUDCTLを変更し、監査ジャーナルを開始する

✓ QAUDCTL を*NONE以外にすると、監査が開始されます。
ここでは、QAUDCTLに、 *AUDLVL *OBJAUD *NOQTEMP を指定します。



IBM Navigator for iで左図のように全てチェックして、[OK]をクリックします。



QAUDCTLの値	動　作　内　容
*NONE	監査は実行されません。
*OBJAUD オブジェクト監査	CHGOBJAUD コマンドを使用して監査用に選択されたオブジェクトの監査が実行されます。 CHGOBJAUDでは、*NONE, *USRPRF, *CHANGE, *ALLのいずれかが指定できます。
*AUDLVL アクション監査	QAUDLVL システム値および CHGUSRAUD コマンドまたは AUDLVL キーワードによって制御される変更内容の監査が実行されます。（次ページのQAUDLVL指定時の監査内容を参照してください。）
*NOQTEMP	QTEMP 中のほとんどのオブジェクトの監査は行われません。 *NOQTEMPは， *OBJAUD または *AUDLVL のいずれかと一緒に指定しなければなりません。 *NOQTEMP単独で指定することはできません。

解説：

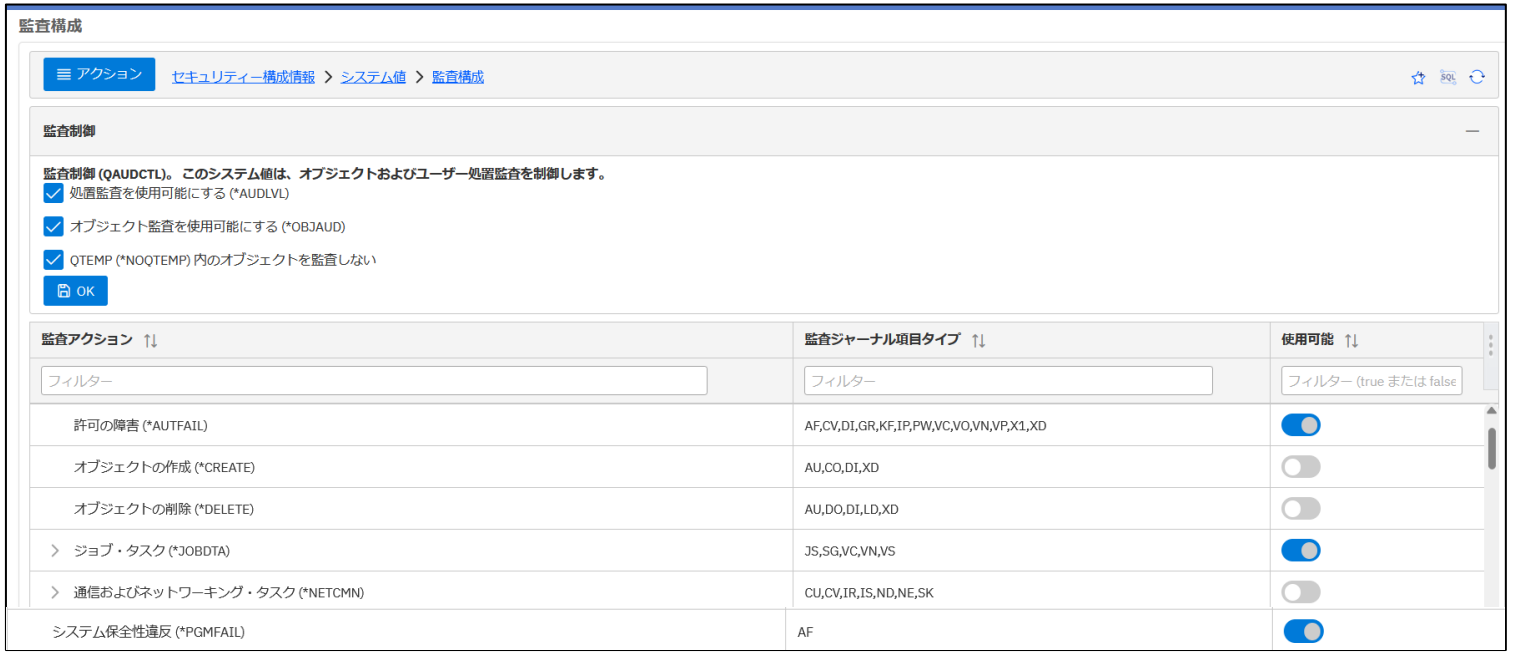
・QAUDCTLの推奨値：下記の３つを指定
- ✓ オブジェクト監査が定義されたオブジェクトに関するアクティビティをログに記録する(*OBJAUD)
- ✓ QAUDLVLシステム値に指定されたイベントをログに記録する(*AUDLVL)。
- ✓ QTEMP内のオブジェクトを監査しない(*NOQTEMP)。

・オブジェクト監査（*OBJAUD）
- ✓ CHGOBJAUDコマンドで明示的に指定したオブジェクトの監査のみ実施
- ✓ *CHANGEはそのオブジェクトに対しての変更作業のみ、*ALLは読取、書き込みを含むすべての動作が監査されます。

・アクション監査 (*AUDLVL)
- ✓ 基本的にQAUDLVLに指定された監査内容が、監査されますが、加えてユーザー・プロファイルに対して設定された項目が監査されます。例えば、QAUDLVLに*DELETEの指定があり、ユーザー監査項目（CHGUSRAUT, AUDLVLキーワード）に*CHANGEがあった場合このユーザーの削除と変更の両方の動作が監査されます。しかし、一般ユーザーは削除動作のみとなります。

3．システム値QAUDLVLを変更します。
- ✓ **どんなセキュリティー関連イベントをログとして記録するかを決定します。**
- ✓ ここでは、QAUDLVLに、　*AUTFAIL　*JOBDTA　*PGMFAIL
  を指定します。(それぞれの内容についてはP9の解説を参照)

Navigator for iで下図のように、右端の使用可能フィルターをONに選択します。



解説：

・QAUDLVL システム値が有効になるためには、QAUDCTL システム値に *AUDLVL があることが前提です。
・QAUDLVL2システム値は、17 個以上の監査値が必要な場合に、QAUDLVLに*AUDLVL2を指定し、QAUDLVL2には、17個を越えた指定をすることができます。
・下記に、主要なシステム値(QAUDLVL)を解説します。

QAUDLVL の値	動　作　内　容
*AUTFAIL	システムにサインオンしようとして失敗した試行、および オブジェクトにアクセスして失敗した試行がログに記録されます。 ユーザーがシステムで 許可されていない機能を実行しようとしていないかを モニターできます。
*CMD	システムは、ユーザーが実行する コマンド文字列をログに記録します。 LOG(*NO) および ALWRTVSRC(*NO) を指定して作成された CL プログラムからコマンドを実行する場合は、コマンド名とライブラリー名だけがログに記録されます。*CMD を使用して、特定のユーザー（機密保護担当者など）のアクションを記録することができます。
*CREATE	ライブラリー QTEMP に作成されたオブジェクトは監査されません。作成された次のオブジェクトが監査されます。 ➢ 新規作成されたオブジェクト ➢ 既存のオブジェクトの置き換えのために作成されたオブジェクト
*DELETE	システム上のオブジェクトの削除がすべて監査されます。
*JOBDTA	ジョブに影響する次の処置が監査されます。 ➢ ジョブ開始および停止データ ➢ 保留，解放，停止，続行，変更，切断，終了，異常終了，
*OBJMGT	次の総称オブジェクト・タスクが監査されます。 ➢ オブジェクトの移動 ➢ オブジェクトの名前変更

QAUDLVL の値	動　作　内　容
*PGMFAIL	次のプログラム障害が監査されます。 ➢ ブロックされた命令 ➢ 妥当性検査値の障害 ➢ 定義域違反
*PRTDTA	次の印刷機能が監査されます。 ➢ スプール・ファイルの印刷 ➢ パラメーター SPOOL(*NO) での印刷
*SAVRST	次の保管および復元情報が監査されます。 ➢ 所有者のユーザー・プロファイルを借用するプログラムが復元される時点 ➢ ユーザー名が入っているジョブ記述が復元される時点 ➢ 復元されるオブジェクトについて所有権および権限情報が変更される時点 ➢ ユーザー・プロファイルの権限が復元される時点 ➢ システム状態プログラムが復元される時点 ➢ システム・コマンドが復元される時点 ➢ オブジェクトが復元される時点
*SECURITY	次のものを含めて，すべての機密保護関連機能が監査されます。 ➢ オブジェクト権に対する変更 ➢ ユーザー・プロファイルの作成，変更，削除，および復元操作 ➢ オブジェクト所有権に対する変更 ➢ 所有者のプロファイルを借用することになるプログラムに対する変更 (CHGPGM) ➢ システム値とネットワーク属性に対する変更 ➢ サブシステムの経路指定に対する変更 ➢ QSECOFR パスワードが DST からの出荷時の値にリセットされる時点 ➢ 保守ツール機密保護担当者のユーザー ID のパスワードを省略時の値にする要求時 ➢ オブジェクトの監査属性に対する変更

QAUDLVL の値	動　作　内　容
*SERVICE	監査されるすべてのサービス・コマンドおよび API 呼び出しのリストについては，　機密保護解説書の資料を参照してください。
*SPLFDTA	次のスプール・ファイル機能が監査されます。 ➢ スプール・ファイルの作成 ➢ スプール・ファイルの削除 ➢ スプール・ファイルの表示 ➢ スプール・ファイルのコピー ➢ スプール・ファイルからのデータの取り出し (QSPGETSP) ➢ スプール・ファイルの保留 ➢ スプール・ファイルの解放 ➢ スプール・ファイル属性変更 (CHGSPLFA コマンド)
*SYSMGT	監査対象ユーザーによる次のシステム管理タスクが監査されます。 ➢ 階層ファイル・システム登録 ➢ 操作援助機能に対する変更 ➢ システム応答リストに対する変更 ➢ DRDA リレーショナル・データベース・ディレクトリーに対する変更 ➢ ネットワーク・ファイル操作
*PGMADP	プログラム所有者からの権限の借用が監査されます。
*OPTICAL	光ディスク機能が監査されます。
*NETCMN	ネットワーク通信の監査：IP 規則処置　と　セキュア・ソケット接続

4. テスト用のユーザープロファイルと物理ファイルを作成して、監査ジャーナルのテスト

✓ 実際にテストユーザーID、物理ファイルを作って、監査ジャーナルへ監査を記録

事前準備

①テスト用のユーザーIDを作成
（例）CRTUSRPRF USRPRF(AUDTEST) PASSWORD()

②ユーザー監査の処理
CHGUSRAUDコマンドで、下記の設定にする
OBJAUT(*ALL)・・オブジェクト操作全て監査記録
AUDLVL(*CMD)・・CLコマンド文字列を監査記録
（例）CHGUSRAUD USRPRF(AUDTEST) OBJAUD(*ALL) AUDLVL(*CMD)

③オブジェクト監査の処理
既存の得意先マスター（TOKMSP)と品目マスター（HINMSP)を下記のように設定します。
-CHGOBJAUDで下記の設定にする　OBJAUD(*USRPRF)

（例）CHGOBJAUD OBJ(SAWADALIB/TOKMSP) OBJTYPE(*FILE) OBJAUD(*USRPRF)
CHGOBJAUD OBJ(SAWADALIB/HINMSP) OBJTYPE(*FILE) OBJAUD(*USRPRF)

-共通権限を、TOKMSPは*EXCLUDE にして、HINMSPは*ALLにする
（例) EDTOBJAUT OBJ(SAWADALIB/ファイル名) OBJTYPE(*FILE)で、
*PUBLICの権限を上記に設定

解説：

・ユーザー監査の処理

- ユーザー監査変更(CHGUSRAUD)コマンド：特定ユーザーのオブジェクト監査、アクション監査を指定

コマンド形式

CHGUSRAUD USRPRF(ユーザー・プロファイル)
OBJAUD(オブジェクト監査値)
AUDLVL(ユーザー処置の監査)・・システム値 QAUDLVL および QAUDLVL2 は,
このパラメーターと一緒に使用されます

・オブジェクト監査の処理

-オブジェクトに対する監査をセットアップまたは変更

コマンド形式

CHGOBJAUD OBJ(オブジェクト)
OBJAUD(オブジェクト監査値)

オブジェクト監査値 (OBJAUD): オブジェクトと関連付けるオブジェクト監査値を指定します。
下記の4つの設定値があります。

*NONE :このオブジェクトを使用しても、変更しても、監査項目は機密保護ジャーナルに送られません。

*USRPRF : このアクセスに対して監査レコードを送るかどうかを決定するために、このオブジェクトをアクセスしている
ユーザーのユーザー・プ　ロファイルが使用されます。特定のユーザーに対して監査をオンにするためには、
CHGUSRAUDコマンドのOBJAUDキーワードが使用されます。

*CHANGE :すべてのユーザーによるこのオブジェクトへのすべての変更アクセスが記録されます。

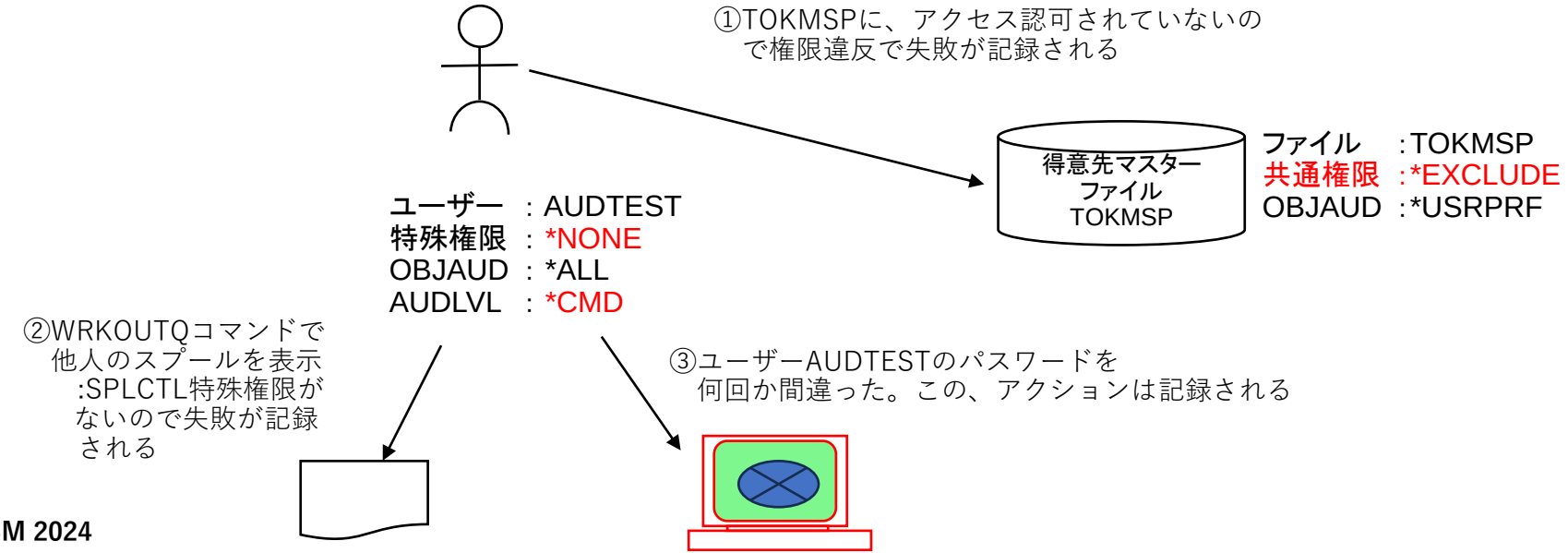
*ALL: すべてのユーザーによるこのオブジェクトへのすべての変更または読み取りアクセスが記録されます。

5．テスト用のユーザープロファイルと物理ファイルを作成して、監査ジャーナルのテスト

✓ 次に、テストユーザーIDでログインして、先ほど作成したファイルなどを触って、監査ジャーナルに記録

テスト実施

下記の①から③を実行します。



解説：

①TOKMSPへのアクセスの失敗・・・アクセス権限違反（拒否）が記録される

（例） DSPFD FILE(SAWADALIB/TOKMSP)コマンドで下記のエラーが出る。

「ライブラリーSAWADALIBのファイルTOKMSPは認可されていない。

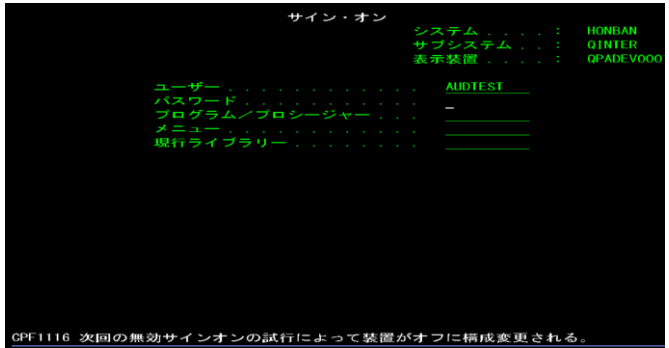
SAWADALIBのTOKMSPとして指定されたファイルを表示することができない」

②WRKOUTQで他社のスプールの表示の失敗・・アクセス権限違反（拒否）が記録される

（例）

③パスワードの間違い(右図例)

が記録されます。

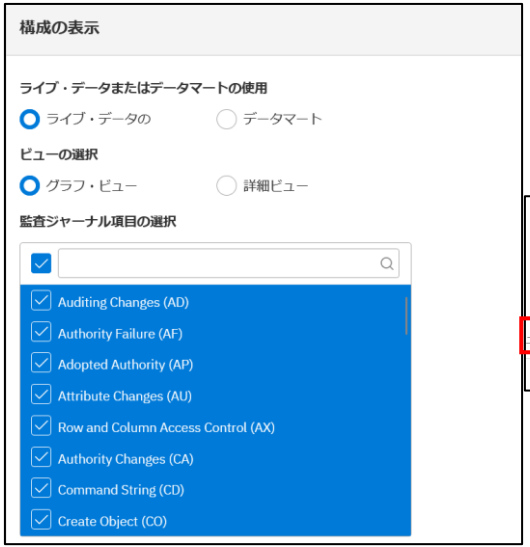


4. 監査ジャーナルを使ってみよう(分析方法)

- ✓ IBM Navigator for iの機能拡張により、簡単に監査ジャーナルに記録されたデータを簡単に検索することが可能

①IBM Navigator for i にログインして、
セキュリティー→監査ジャーナル項目 を選択します

②ライブ・データで、ビューの選択をグラフ・ビューにします。監査ジャーナルの項目を全て選択します。
ユーザー名に、[AUDTEST]を入力します。
[OK]をクリック。



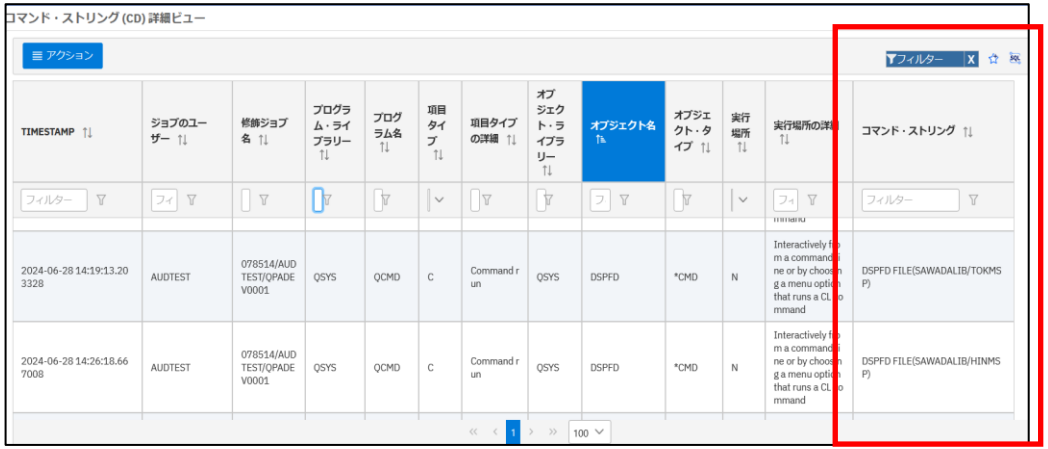
解説： **下記は、ジャーナル項目のタイプ一覧（アクション監査/オブジェクト監査）です。2桁の英文字で、全ての監査項目を示しています。**

AD 監査変更	ML オフィス・サービス・メール処置	SE 変更済みサブシステム経路指定項目
AF 権限障害	NA 変更済みネットワーク属性	SF スプール・ファイルに対する処置
AP 借用権限の獲得	ND APPN ディレクトリー探索フィルター違反	SG 非同期シグナル
AU 属性変更	NE APPN エンドポイント・フィルター違反	SK セキュア・ソケット接続
CA 権限変更	OM オブジェクト移動またはオブジェクト名変更	SM システム管理変更
CD コマンド・ストリング監査	OR オブジェクト復元	SO サーバー・セキュリティー・ユーザー情報処置
CO オブジェクト作成	OW オブジェクト所有権の変更	ST 保守ツールの使用
CP 変更、作成、または保管されるユーザー・プロファイル	O1 (光ディスク・アクセス) 単一ファイルまたはディレクトリー	SV 変更済みシステム値
CQ *CRQD オブジェクトの変更	O2 (光ディスク・アクセス) 二重ファイルまたはディレクトリー	VA アクセス制御リストの変更
CU クラスター操作	O3 (光ディスク・アクセス) ボリューム	VC 接続の開始または終了
CV 接続検証	PA 借用権限に変更済みのプログラム	VF サーバー・ファイルのクローズ
CY 暗号構成	PG オブジェクトの1 次グループの変更	VL 超過した会計限度
DI ディレクトリー・サーバー	PO 印刷出力	VN ネットワークのログオン、ログオフ
DO オブジェクト削除	PS プロファイル・スワップ	VO 妥当性検査リスト処置
DS DST 機密パスワード再設定	PW パスワードが無効	VP ネットワーク・パスワード・エラー
EV システム環境変数	RA 復元時権限変更	VR ネットワーク資源アクセス
GR 汎用レコード	RJ ユーザー・プロファイルが指定されているジョブ記 述の復元	VS サーバー・セッションの開始または終了
GS ソケット記述子が別のジョブに与えられた	RO 回復時オブジェクト所有者変更	VU ネットワーク・プロファイルの変更
IM 侵入モニター	RP 借用権限プログラム復元	VV サービス状況の変更
IP プロセス間通信	RQ *CRQD オブジェクトの復元	X0 ネットワーク認証
IR IP 規則アクション	RU ユーザー・プロファイル権限の復元	YC アクセスされたDLO オブジェクト(変更)
IS インターネット・セキュリティー管理	RZ 復元中の1 次グループの変更	YR アクセスされたDLO オブジェクト(読み取り)
JD ジョブ記述のユーザー・パラメーターへの変更	SD システム配布ディレクトリーに変更	ZC アクセスされたオブジェクト(変更)
JS ジョブに影響を与える処置		ZM SOM アクセス方式
KF キー・リング・ファイル		ZR アクセスされたオブジェクト(読み取り)
LD リンク、非リンク、またはディレクトリー項目の探索		

4. 監査ジャーナルを使ってみよう(分析方法)

③先ほどのテストを実施すると下記のような
グラフが表示されます。
・CDはコマンドの記録
・JSはジョブ変更の記録
・AFは、権限障害
・ZRは、オブジェクト読み取り

④例えば、グラフのCD(コマンドの記録）をクリックします。
ユーザー:AUDTESTに、AUDLVL(*CMD)を付与したので、テストで実行した様々なCLコマンドが、
監査ジャーナルに記録されています。



4. 監査ジャーナルを使ってみよう(分析方法)

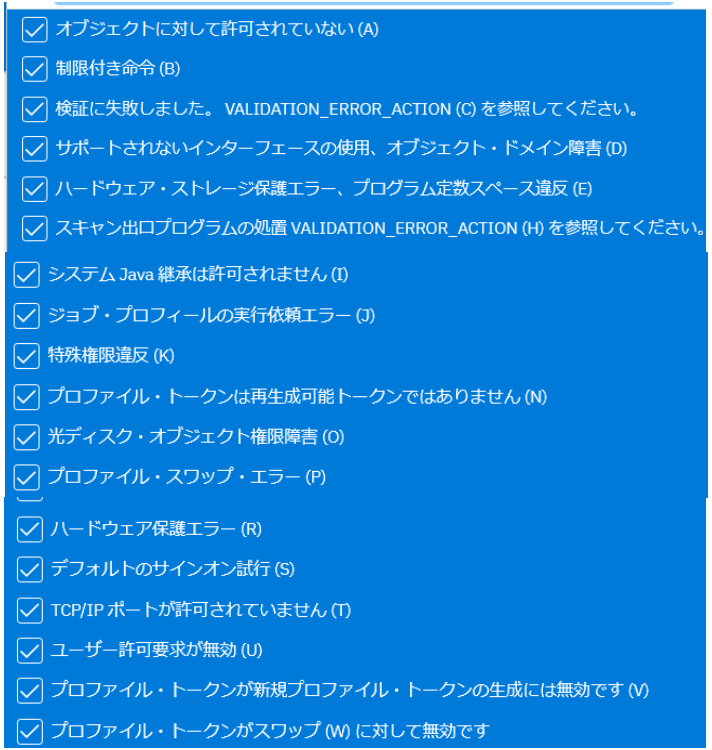
⑤グラフのAF（権限障害）をクリックします。

・上２つは、ユーザーAUDTESTが、TOKMSPファイルへのアクセス権の無いので権限エラーがでています。
・下の１つは、スプールファイルのアクセス権のないQPRINTのファイルにアクセスしたので権限エラーになっています。

TIMESTAMP	ジョブのユーザー	修飾ジョブ名	プログラム・ライブラリー	プログラム名	オブジェクト・ライブラリー	オブジェクト名	オブジェクト・タイプ	違反タイプ	違反タイプの詳細	ユーザー・
フィルター								A, B, C, D, E, H, I, J, K, N, O, P, R, S, T, U, V, W, X, Y, Z	フィルター	フィルター
2024-06-28 14:18:09.190048	AUDTEST	078514/AUDTEST/QPADEV0001	QSYS	QCMD	SAWADALIB	TOKMSP	*FILE	A	Not authorized to object	AUDTEST
2024-06-28 14:19:13.204192	AUDTEST	078514/AUDTEST/QPADEV0001	QSYS	QCMD	SAWADALIB	TOKMSP	*FILE	A	Not authorized to object	AUDTEST
2024-06-28 14:29:32.941936	AUDTEST	078514/AUDTEST/QPADEV0001	QSYS	QCMD	QGPL	QPRINT	*OUTQ	A	Not authorized to object	AUDTEST

解説：

・AF(権限障害）には、下記のような様々な「違反タイプ」があります。

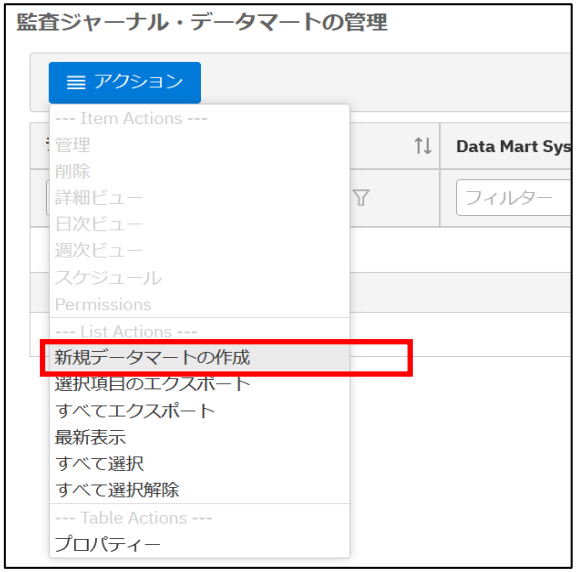


5．監査ジャーナルのデータマート機能を使ってみよう

- ✓ IBM i 7.5 TR4 の機能拡張により、監査ジャーナルに記録された大量のデータを簡単に迅速に分析できるように、データマート機能が提供
- ✓ データマート機能を使用すると、関心あるタイプの監査ジャーナルのデータを高速に検索可能

①IBM Navigator for i にログインして、セキュリティー→「データマートの管理」を選択します。

②「アクション」→「新規データマートの作成」を選択します。



5．監査ジャーナルのデータマート機能を使ってみよう

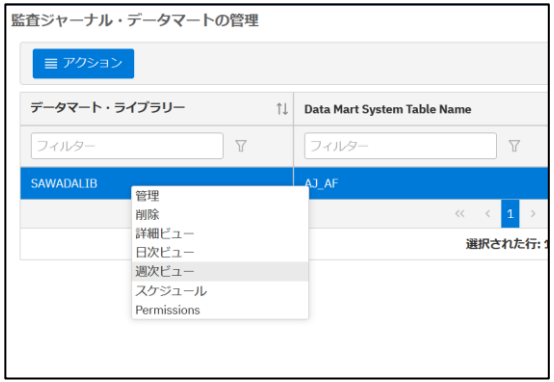
③関心のある監査タイプ毎にデータ マートを作成できます。

・データ マートを作成するライブラリ（どのライブラリーでもOKです）
・ジャーナルエントリー・タイプ（ジャーナル項目を１つ選択します）
・時間範囲を選択

（例）下記は、現行の監査ジャーナルから、権限エラー（AF)のみを抽出して、
データマート作成しています。(自動でAJ_AFという名称のデータベースが作成されます)

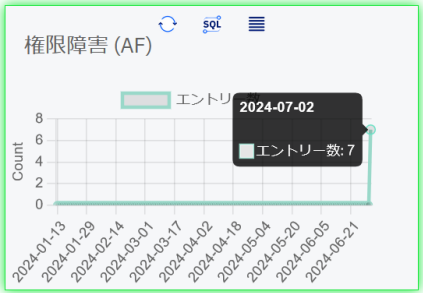
5．監査ジャーナルのデータマート機能を使ってみよう

④「アクション」→「週次ビュー」を選択
・週次のエラーの状況確認

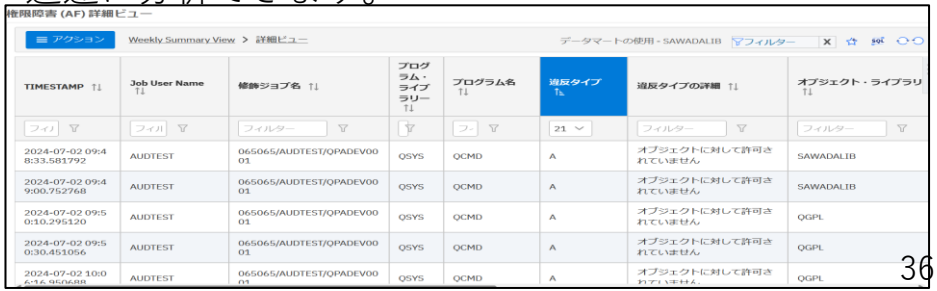


⑤下記で、そのままOKを選択

⑥グラフで、週次のエラーを傾向分析できます。
7/2に、7件のエラー確認しました。
・7/2のポイントをクリックします。



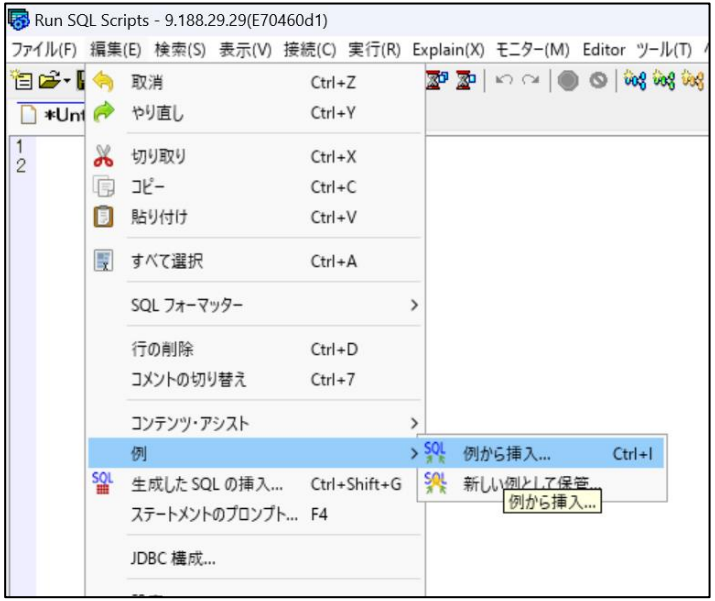
⑦下記のように権限エラーの詳細が確認できます。
このように監査ジャーナルのデータを項目毎に抽出して、迅速に分析できます。



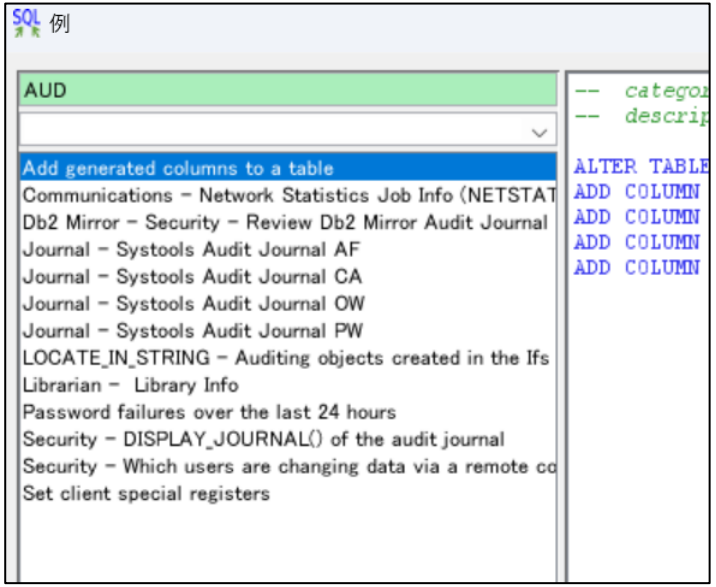
（補足）SQLサービスを使って、監査ジャーナルの分析を容易にできます。

✓ 監査ジャーナルの検索は、IBM Navigator for i以外に、SQLサービスを利用して検索できます。

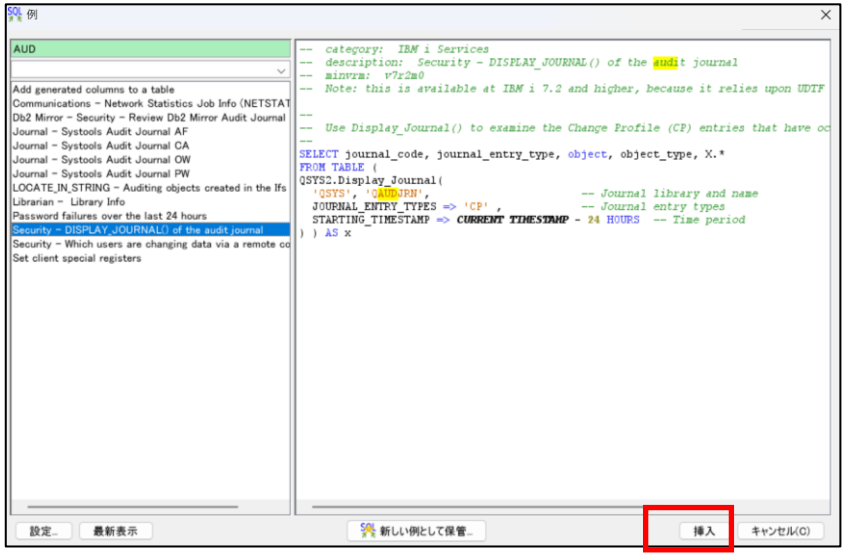
①ACSのSQLコマンドを起動します
「編集」→「例」→「例から挿入」を選択



②一番上のカラムに、「AUD」と入力すると
監査関連のSQLコマンド例が表示されます。



③下から3つ目の「*Security - DISPLAY_JOURNAL()* 」
を選択し、「挿入」を選択



④SQLコマンド欄に、サンプルが挿入されます。
これは、現時点から24時間前までの監査ジャーナルを、
を使って、特定のジャーナル項目のタイプを検索する
SQLコマンドです。

（例）デフォルトのCP（ユーザープロファイルの作成）を
PW(パスワードのエラー）に変更します。

```
1
2  -- category: IBM i Services
3  -- description: Security - DISPLAY_JOURNAL() of the audit journal
4  -- minvrm: v7r2m0
5  -- Note: this is available at IBM i 7.2 and higher, because it relies upon UDTF default & named parameter support
6
7  --
8  -- Use Display_Journal() to examine the Change Profile (CP) entries that have occurred over the last 24 hours.
9  --
10 SELECT journal_code, journal_entry_type, object, object_type, X.*
11 FROM TABLE (
12 QSYS2.Display_Journal(
13  'QSYS', 'QAUDJRN', -- Journal library and name
14  JOURNAL_ENTRY_TYPES => 'CP' , -- Journal entry types
15  STARTING_TIMESTAMP => CURRENT TIMESTAMP - 24 HOURS -- Time period
16 ) ) AS x
```

```
-- category: IBM i Services
-- description: Security - DISPLAY_JOURNAL() of the audit journal
-- minvrm: v7r2m0
-- Note: this is available at IBM i 7.2 and higher, because it relies upon UDTF default & named parameter support

--
-- Use Display_Journal() to examine the Change Profile (CP) entries that have occurred over the last 24 hours.
--
SELECT journal_code, journal_entry_type, object, object_type, X.*
FROM TABLE (
QSYS2.Display_Journal(
 'QSYS', 'QAUDJRN', -- Journal library and name
 JOURNAL_ENTRY_TYPES => 'PW' , -- Journal entry types
 STARTING_TIMESTAMP => CURRENT TIMESTAMP - 24 HOURS -- Time period
) ) AS x
```

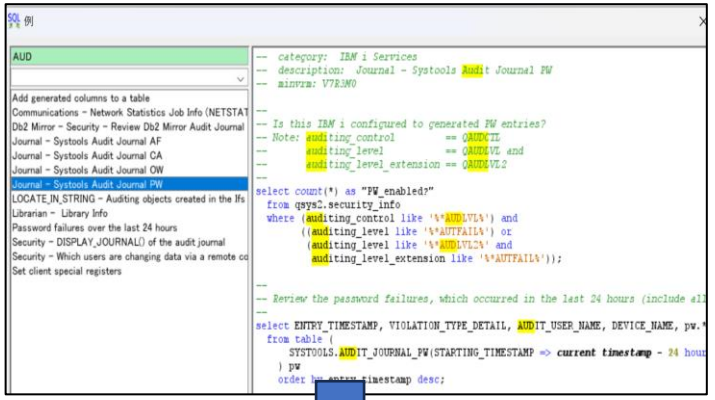
⑤下記のように過去24時間以内に、4件のパスワードエラーがあるのを確認できます。

*Untitled 1

```
-- category:  IBM i Services
-- description:  Security - DISPLAY_JOURNAL() of the audit journal
-- minvrm:  v7r2m0
-- Note: this is available at IBM i 7.2 and higher, because it relies upon UDTF default & named parameter support

--
-- Use Display_Journal() to examine the Change Profile (CP) entries that have occurred over the last 24 hours.
--
SELECT journal_code, journal_entry_type, object, object_type, X.*
FROM TABLE (
QSYS2.Display_Journal(
  'QSYS', 'QAUDJRN',                    -- Journal library and name
  JOURNAL_ENTRY_TYPES => 'PW',          -- Journal entry types
  STARTING_TIMESTAMP  => CURRENT TIMESTAMP - 24 HOURS  -- Time period
) ) AS x
```

JOURNAL_CODE	JOURNAL_ENTRY_TYPE	OBJECT	OBJECT_TYPE	ENTRY_TIMESTAMP	SEQUENCE_NUMBER
T	PW	-	-	2024-07-02 09:42:27.125120	260
T	PW	-	-	2024-07-02 10:06:45.034976	494
T	PW	-	-	2024-07-02 10:37:08.947488	1193
T	PW	-	-	2024-07-02 15:21:23.265440	6862

⑥このパスワードエラーのより詳細な分析は、先ほどの例の「*Journal - Systools Audit Journal PW*」を選択することで可能になります。




```
-- category:  IBM i Services
-- description:  Journal - Systools Audit Journal PW
-- minvrm:  V7R3M0

--
-- Is this IBM i configured to generated PW entries?
-- Note: auditing_control          == QAUDCTL
--       auditing_level            == QAUDLVL and
--       auditing_level_extension  == QAUDLVL2
--
select count(*) as "PW_enabled?"
  from qsys2.security_info
  where (auditing_control like '%*AUDLVL%') and
        ((auditing_level like '%*AUTFAIL%') or
         (auditing_level like '%*AUDLVL2%' and
          auditing_level_extension like '%*AUTFAIL%'))
```

ENTRY_TIMESTAMP	VIOLATION_TYPE_DETAIL	AUDIT_USER_NAME	DEVICE_NAME	ENTRY_TIMESTAMP
2024-07-02 15:21:23.265440	パスワードが無効です	SAWADA	-	2024-07-02 15:21:23.265440
2024-07-02 10:37:08.947488	パスワードが無効です	AUDTEST	QPADEV0001	2024-07-02 10:37:08.947488
2024-07-02 10:06:45.034976	パスワードが無効です	AUDTEST	QPADEV0001	2024-07-02 10:06:45.034976
2024-07-02 09:42:27.125120	パスワードが無効です	AUDTEST	QPADEV0001	2024-07-02 09:42:27.125120

SQL を実行すると右記のように、誰が、どの端末でパスワードエラーになったのかを確認できます。

まとめ：適切なセキュリティー設定と 監査のお勧め

- ✓ **最初に、自社のセキュリティー要件を定義してください**
- ✓ **次に、監査・ログのルールと管理プロセスを定義してください。**
- ✓ **監査ルールに従って、適切なセキュリティー設定を行います。**
- ✓ **セキュリティー・ルールが破られようとしていないか、監査ジャーナルを監視するしくみを日常の運用に組み込みます。**

＊監査ジャーナルは、大量のデータを発生します。自社のディスク容量に注意してください。過去の監査ジャーナルはテープに取得して定期的に削除してください。

6. 補足情報

1. 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

2. システムセキュリティーの計画と設定
   https://www.ibm.com/docs/ja/i/7.5?topic=security-planning-setting-up-system

3. IBM i でのセキュリティーの監査
   https://www.ibm.com/docs/ja/i/7.5?topic=reference-auditing-security-i

4. IBM i 7.5 TR4での新機能（監査ジャーナルの紹介は、P39-40）
   https://www.common.be/wp-content/uploads/2024/06/IBM-i-TR-Announcement-Guided-Tour.pdf

5. 監査ジャーナルのデータマートの作成プロシジャーのマニュアル
   https://www.ibm.com/docs/en/i/7.5?topic=services-manage-audit-journal-data-mart-procedure

6. SQLコマンドでの監査ジャーナルの分析用コマンドのマニュアル
   https://www.ibm.com/docs/en/i/7.5?topic=services-audit-journal-entry

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/