iEVO2024 分科会

「これだけは知っておきたい！IBM iのセキュリティ ～最低限のリスク対策とランサムウェア対応について」

2024年11月6日

日本アイ・ビー・エム株式会社
IBM Power Tech Sales

「これだけは知っておきたい！IBM i のセキュリティ ~最低限のリスク対策とランサムウェア対応について」

アジェンダ

1. どんな攻撃が増えているか？
2. どうしてIBM i は堅牢なのか？
3. IBM iのバージョンアップ・リリースアップでどんな機能が使えるの？
4. 最低限必要な対策は？

昨今のシステム攻撃の種類とは？

2024年 脅威トレンドのハイライト

正規アカウントを狙う攻撃活動が世界的に増加

71% の増加

初期侵入経路に正規アカウントを悪用するインシデントが71%増加。全体の30%を占め、フィッシングと並びトップの初期侵入経路に

23%

認証情報の窃取が確認されたインシデントの割合。昨年の11%から2倍以上に増加

ランサムウェアグループが情報窃取の手口に移行する動き

11.5% の減少

X-Forceが対応した企業・組織環境におけるランサムウェア感染インシデントの件数は11.5%減少。継続した対策が奏功

266% の増加

情報窃取マルウェアを使用するインシデントが266%増加。ランサムウェアを用いていたグループが手口を移行しているケースも

AIにまつわる脅威は”まだ”本格化していない

80万 以上の投稿

ダークウェブ・フォーラムにおいてもAIやGPTが話題に。一方、AIに対する攻撃手法やツールは成熟段階には至っていない

50% のシェア

過去の攻撃の歴史を踏まえると、特定の生成AI技術が50%以上のシェアを獲得する、もしくは3つ以下のテクノロジーに統合されるタイミングで、生成AIに対する攻撃が本格化すると予測

攻撃により組織に生じた影響

32%

データ窃取と漏洩が影響の第1位

- 2022年の19%から13%の増加
- 情報窃取マルウェアや正規ツールの悪用によるデータの持ち出しの増加が要因

24%

脅迫が引き続き高い割合を占める

- 2022年の1位から2位に後退も割合は3%増加
- ランサムウェアを使用しない、機密情報の窃取とそれを用いた脅迫への移行の動きも
- 日本ではテクニカル・サポート詐欺被害も断続的に発生

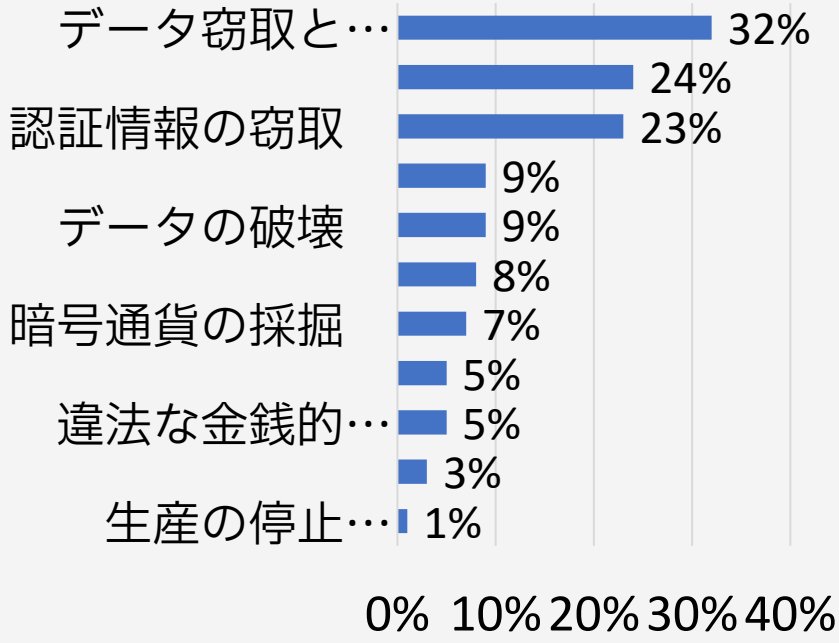
23%

認証情報の窃取が急増

- 攻撃者は正規認証情報を用いた不正ログインの手口に注目
- 機密情報と共に認証情報も狙われている

2023年 攻撃により組織に生じた影響の内訳

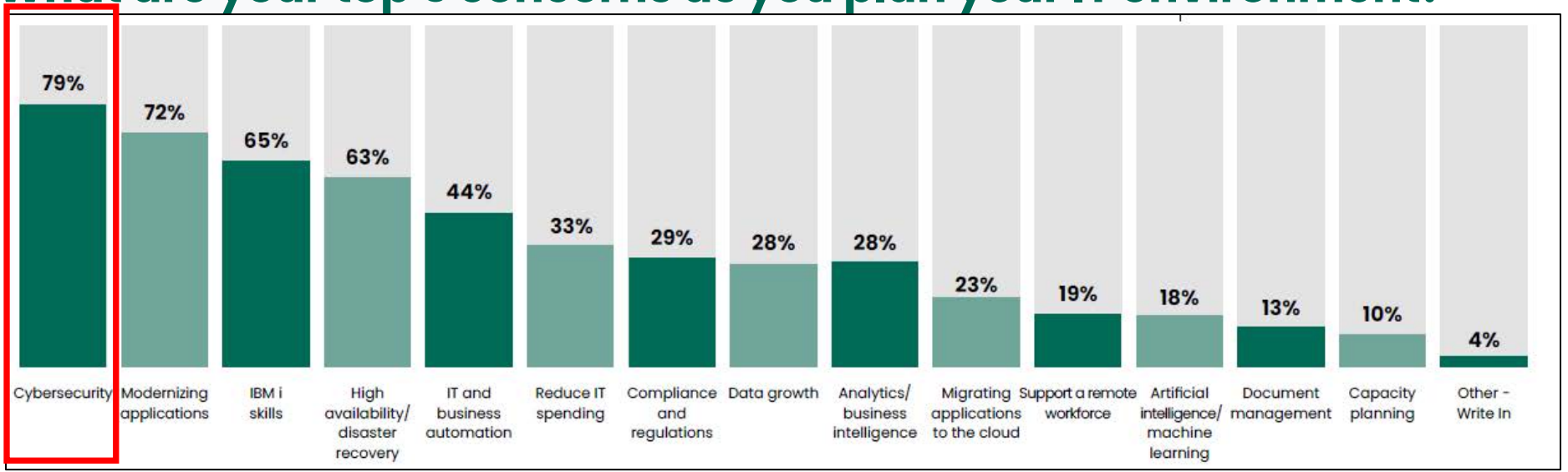
Source: IBM X-Force



IT に関する懸念事項 (世界中ののIBM iユーザ調査)
By FORTRA

https://www.fortra.com/resources/guides/ibm-i-marketplace-survey-results

What are your top 5 concerns as you plan your IT environment?



なぜIBM i はセキュリティーの脆弱性が少ないのか？

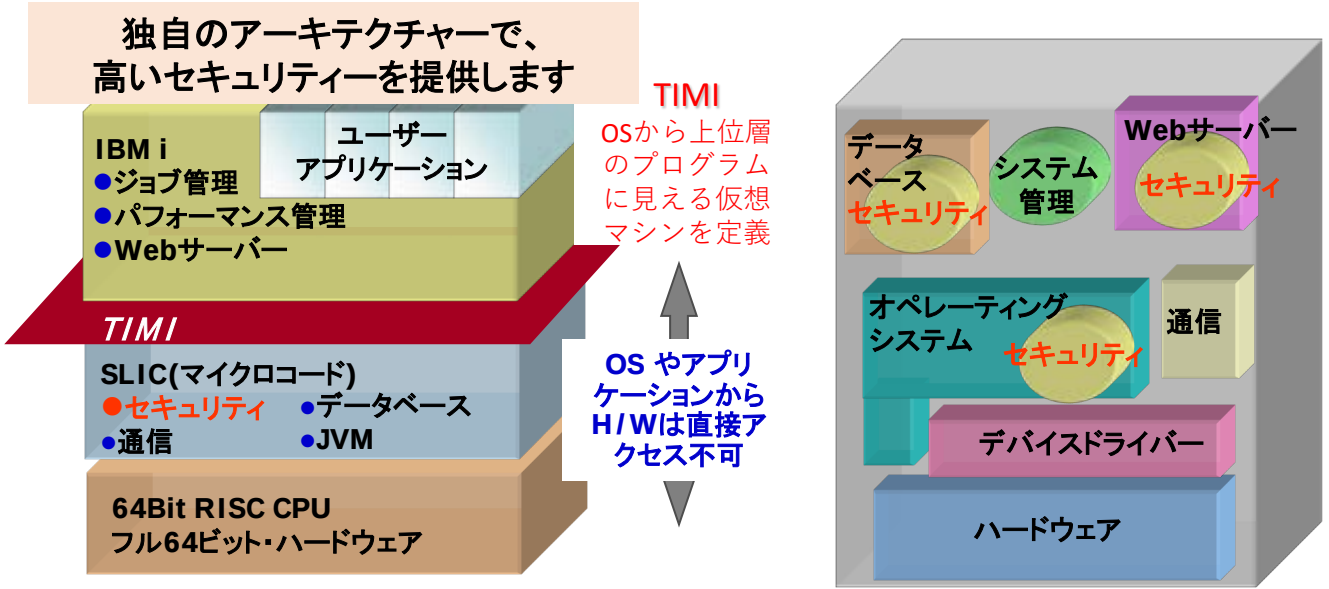
セキュリティーの堅牢性

IBM i

先進機能をOSに統合
オブジェクト指向デザイン
カーネルの仕様は非公開
OSより上位層のプログラムは、メモリーやレジスターなどH/Wを直接操作不可能

Windows

各種機能が統一されたデザインではない(データベース、機密保護、バックアップなど
ウイルス感染/データ改竄されやすい
1つのソフトのバージョンが変わるとシステム全体の稼動の保証はなし



実際に、IBM i は、競合するオペレーティングシステムと比較して、セキュリティ上の脆弱性が桁違いに少ない

セキュリティー脆弱性統計

OS	Windows Sever 2016	Windows Sever 2019	IBM i
統計期間	2016年～	2019年～	2015年～
報告件数	3503	2995	27
スコア8以上	794	698	4

https://www.cvedetails.com/ より製品毎に集計（2024年7月1日現在）

- ✓ 確かに、IBM i は、最も安全なプラットフォームであると言われている(実際にその通りではある)
- ✓ IBM i は、新バージョン・リリース、セキュリティ機能を拡張し続けている
- ✓ 絶え間なく進化するセキュリティの脅威が存在する昨今では、適切にIBM iのセキュリティ機能を使っていく必要がある

IBM iの最新リリースで使える最新機能とは？

IBM i は時代の要請に対応できる様々なセキュリティ機能を拡張し続けています

パスワード (IBM i 7.5) ・より強力な暗号化方式（SHA2-512）で暗号化
・パスワードがパスワード規則に適合するかどうかをAPIで確認

権限変更(IBM i 7.5) ・デフォルト の「*PUBLIC」権限の値を「*USE」に変更

権限収集 - トレース (IBM i 7.3-)
各IDのアクセス状況をトレース・報告

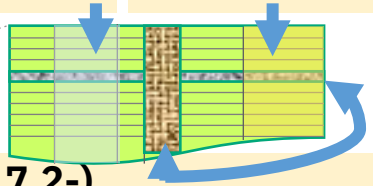
権限収集 – オブジェクト (IBM i 7.4) オブジェクトへのアクセスを精査し、必要な最低限の権限を報告

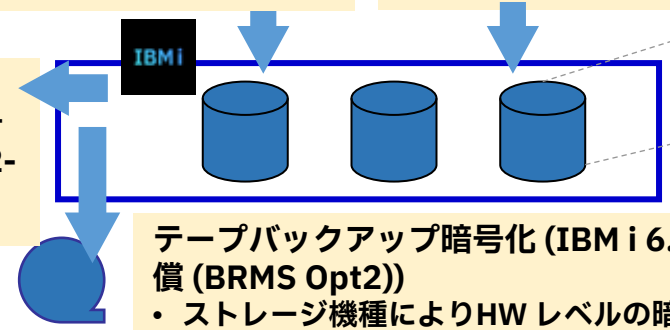
カラム暗号化 (IBM i 7.1-)
- フィールド・プロシジャーによる実装

監査用追加カラム (IBM i 7.3-) OSが自動でデータ付与

侵入検知 （IBM i 6.1-）
ID･PWの連続間違いなど
- GUI にてポリシー設定
- 異常時リアルタイム発報

ASP 暗号化 （IBM i 7.1- 有償）
- ディスク空間全体の暗号化





クラウドバックアップ暗号化 (IBM i 7.2- 有償)

テープバックアップ暗号化 (IBM i 6.1- 有償 (BRMS Opt2))
- ストレージ機種によりHW レベルの暗号化も可能

RCAC (IBM i 7.2-)
- Row & Column Access Control レコード単位 または項目単位で制御
- 行（Row）アクセスに認証
- 列（Column）をマスク

POWER9、Power10による暗号化パフォーマンス向上
Power10によるメインメモリ暗号化

ハッキング・マルウェア・ランサムウェアに強いIBM i + IBM Power
ハード (IBM Power) + SW (IBM i) 統合設計 / IBM i オブジェクト指向テクノロジー / 水平・垂直マイクロコードテクノロジー

IBM i で最低限必要な対策とは？

IBM i のセキュリティの維持と向上のために、下記の5つの方策を提言します。

1. IBM i を最新の状態に保つ
   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する

2. IBM i のユーザーの権限を最小権限にする
   まずは、IBM i 7.3及び7.4で導入された権限の収集機能を使用し、現行業務に必要な最低限の権限を調査し、ユーザー毎に、オブジェクトレベルの権限認可する

3. データ回復の準備とテストを実施
   完全に分離、およびセグメント化されたバックアップ方法で、文書化された計画をして、計画的に復元のテストする

4. NetServerを介したネットワークへのIFS（IBM iファイルシステム）の露出を減らす
   可能な限り最低レベルの権限に設定されていることを確認
   理想的には、変更を防ぐために読み取り専用にする

5. 監査ジャーナルを設定し、セキュリティ・ログを監視

1. IBM i を最新の状態に保つ

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する

ソフトウェア保守契約のあるOSを利用する

- ✓ 可能な限り最新リリースのOSにする（セキュリティ機能は拡張されて強化されている）
- ✓ 既知の脆弱性については必ずPTFがあるので、定期的に適用する

予防保守の重要性

- ✓ IBMに報告される問題の4 分の3 は既知のものであり、予防保守が正しく行われていれば避けることができるはずのものである→計画外のダウンタイム削減
- ✓ 定期的に予防保守PTF適用すれば、計画も立てやすく、一回あたりの適用時間も少なくて済む
- ✓ 安定した環境でも3 から4 か月ごとに、累積PTF パッケージの適用をお勧め

2. IBM i のユーザー権限を最小にする

まずは、IBM i 7.3及び7.4で導入された権限の収集機能を使用し、現行業務に
必要な最低限の権限を調査し、ユーザー毎にオブジェクトレベルの権限認可する

- ✓ 自社のセキュリティ・ポリシーに、業務レベルのアクセス権限を規定する
- ✓ IBM i 7.3の権限収集機能を使用して、現行業務のユーザーのアクセスに基づいて、
  必要なアクセス許可を決定します
  IBM i 7.4では、オブジェクトによる権限収集が可能なので、オブジェクトレベルの権限認可
  がさらに容易になっている
- ✓ 特殊権限が、多くのユーザーに割り当てられると、リスクになる
- ✓ ID/パスワード情報を厳格に管理(特にパスワードは、定期更新する)
  （多要素認証も適切に導入する）

3．データ回復の準備とテストを実施する

完全に分離、およびセグメント化されたバックアップ方法で、文書化された計画をして、計画的に復元のテストする

システム管理　サーバーのバックアップ
https://www.ibm.com/docs/ja/ssw_ibm_i_75/pdf/rzaiupdf.pdf

✓　いつ、どの範囲を対象として保管するか

ライセンス内部コード	**毎四半期** 主にPTF適用時、リリース・アップ時等に変更されます。
QSYS内のIBM i オブジェクト	**毎四半期** 主にPTF適用時、リリース・アップ時等に変更されます。
ユーザー・プロファイル 専用認可	**毎日** 定期的に変更されます。
構成オブジェクト	**毎日** 定期的に変更されます。
IBM提供のディレクトリー	**毎四半期** 主にPTF適用時、リリース・アップ時等に変更されます。
IBM i のオプショナル・ライブラリー QHLPSYS、QUSRTOOL	**毎四半期** 主にPTF適用時、リリース・アップ時等に変更されます。
ライセンス・プログラム・ライブラリー QRPG、QCBL、Qxxxx	**毎四半期** ライセンス・プログラムの更新時に変更されます。
ユーザー・データを含むIBMライブラリー QGPL、QUSRSYS、QS36F、#LIBRARY	**毎日** 定期的に変更されます。
ユーザー・ライブラリー LIBA、LIBB、LIBC、LIBD、etc.	**毎日** 定期的に変更されます。
文書およびフォルダー	**毎日** 定期的に変更されます。 (使用時)
配布オブジェクト	**毎日** 定期的に変更されます。 (使用時)
ディレクトリー内のユーザー・オブジェクト	**毎日** 定期的に変更されます。

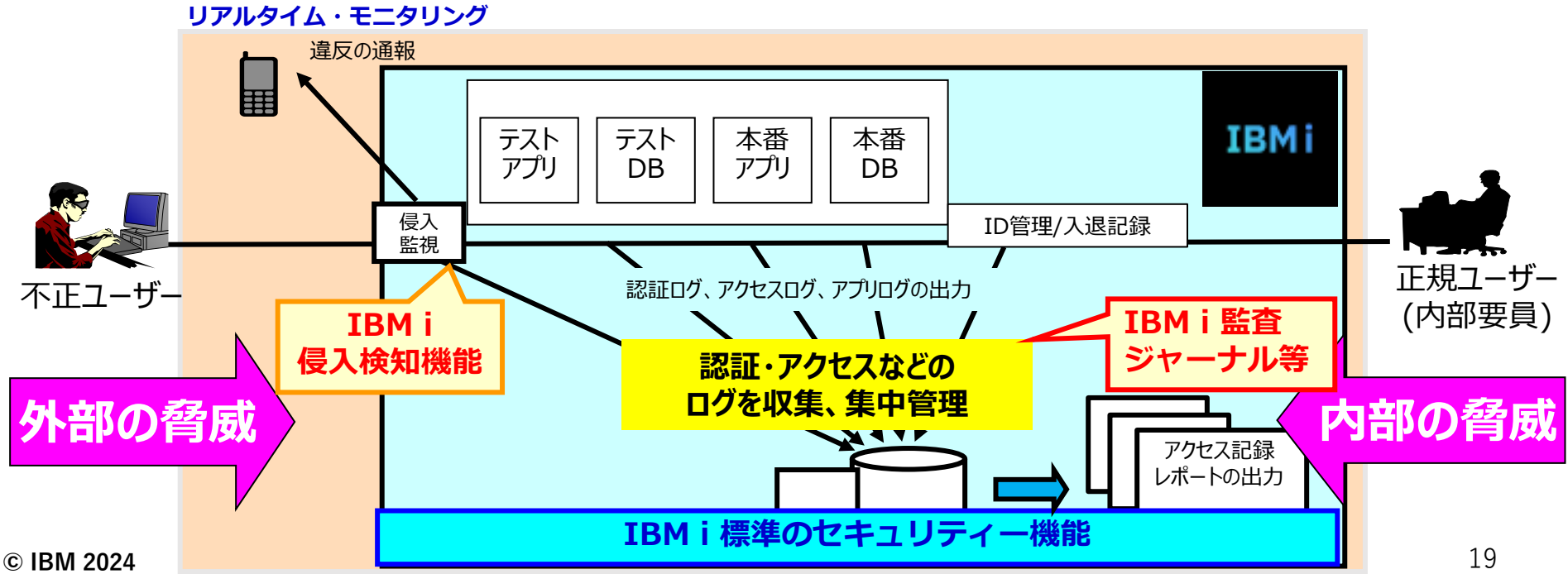
4. NetServerを介したネットワークへのIFS（IBM iファイルシステム）の露出を減らす

IBM i をファイルサーバーとしてWindowsやクライアントから利用する場合、IBM iの共用フォルダーが悪意あるプログラムの温床・媒介となる可能性があります
一般的なセキュリティの観点も併せて下記のようなマルウェア、ウィルス等への対策も鑑みた推奨設定

1. **IFSルート（/）とQOpenSysのアクセス権を *PUBLIC RWXから * PUBLIC * RXに変更する**
2. **ライブラリー、IFSフォルダの不要な書き込み権限を削除する（ファイルの暗号化防止のため）**
3. **ライブラリー、IFSフォルダの不要な読み取り権限を削除する（データの漏えい防止）**
4. **NetServerやNFSエクスポートではゲスト/匿名のネットワークアクセスを無効にする、不要なネットワーク共有/エクスポートを削除する、ファイルは読み取り専用を基本とし必要なものに限定して変更・削除権限を付与する**
5. **公開するディレクトリとファイルの数を極力減らす。IFSルート（/）は絶対にシェア/エクスポートしない**
6. **QPWFSERVER権限リストを使用して、NetServerなどからの /QSYS.LIB配下 へのアクセスをブロックする**
7. **アクセス許可はできるだけ少ない人数に制限する**

5. 監査ジャーナルを設定し、セキュリティ・ログを監視

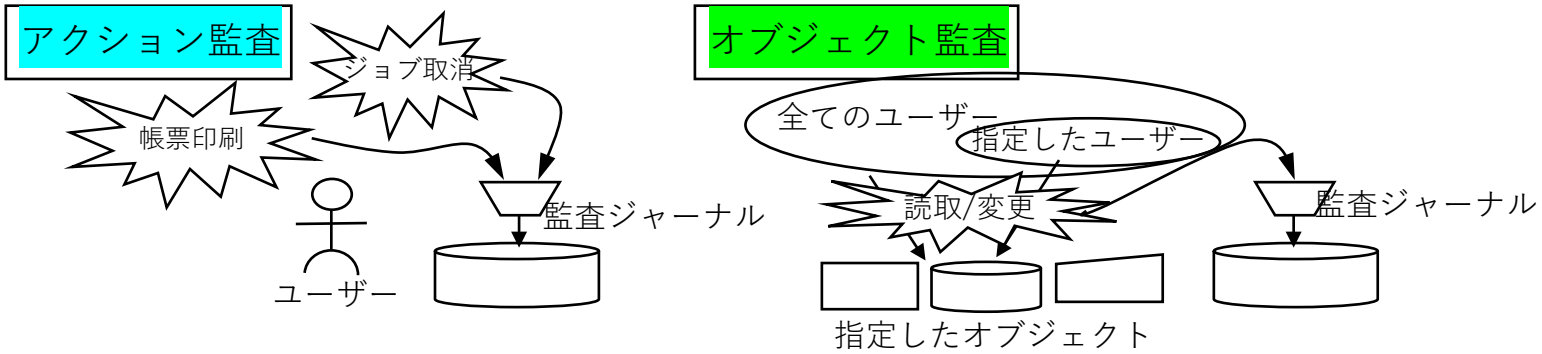
- ✓ IBM i では 外部及び、内部からの脅威に対応して、下記の機能が実装されています
  - ➢ 内部からの脅威：ユーザーID管理/入退記録管理/オブジェクトのアクセス管理と監査機能 【内部不正の防止】
  - ➢ 外部からの脅威：侵入検知機能 【外部からの攻撃の早期の検知が被害を最小にする】



監査ジャーナル … アクション監査とオブジェクト監査

- ✓ 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



監査ジャーナル機能は、Navigaror for iで設定・管理できる

- ✓ **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**

①Navigator 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

②セキュリティ・イベントの記録が
下図のように、表示できます

IBM i の侵入検知機能を使おう

- ✓ IBM i では、侵入検知機能はOS標準機能　（IBM i 6.1以降）
- ✓ TCP/IP ネットワークを介して侵入する疑わしい侵入イベントを監査する侵入検知ポリシーを作成できる
  - ➢ 侵入モニター(IM)レコードが、監査ジャーナルとしてログされる
- ✓ 侵入の防止ではなく、疑わしい侵入活動を監査する機能
- ✓ リアルタイム通知が可能
  - ➢ IMレコードに加えてe-mail,MSGQに送信

- ✓ GUIインターフェースのサポート
  - ➢ IBM Navigator for iによる設定で、監査ジャーナルを意識せずにイベント表示

侵入検知機能も、**Navigaror for iで、簡単に設定・管理**

- ✓ IBM Navigator for iのGUI を使用して、侵入検知ポリシーを構成および管理し、侵入イベントを表示できます

①IBM Navigator for iの「セキュリティ」→「侵入検知」→「ポリシーの管理」を選択

②侵入検知ポリシーを作成します。「アクション」→「NEW」を選択

③侵入検知のイベントの検知できます

まとめ～IBM i のセキュリティー維持向上のために

IBM i は業界で最も高いセキュリティ機能を備えたインフラですが、

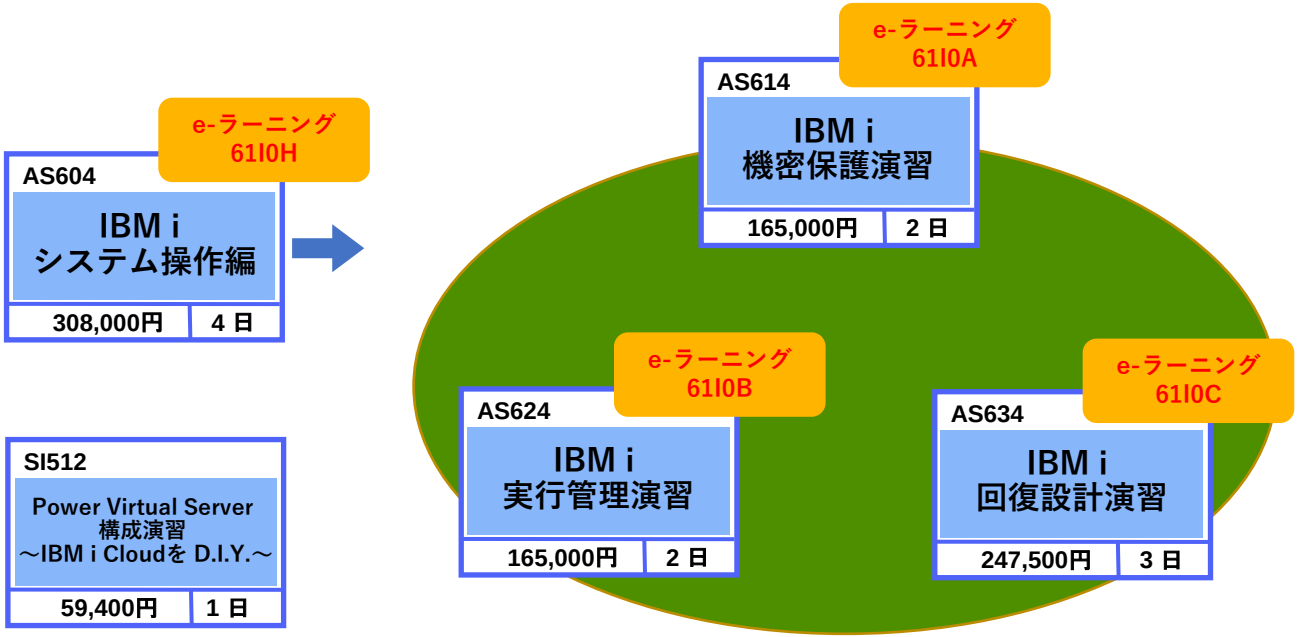
- **時代に呼応して変化するシステム利用形態やセキュリティリスクに応じて、IBM i セキュリティも継続的な見直しが必要です。**
  - -> 当資料でもご紹介した各種セキュリティ機能の活用
  - -> すべてのセキュリティ設定を有効化する必要はありません
    自社環境を前提に検討し、最もハイリスクなものから取り組んでください

- **また、以下も重要です。**
  - 最新（IBMの保守サポートがある）OS ver.を使用する、できる限り最新の PTFを適用する
  - 万一の被災に備えて、システムの完全なバックアップ＆復元の手順を策定し、復元検証も実施する
  - IBM iの重要な基幹データを、周辺サーバーに分散させない
  - セキュリティの継続的な評価&改善サイクルの実践が重要です 自社で困難な場合は、パートナー様や、IBMへ依頼してください

このあたりの必須研修とかあるのか？

IBM i – システム管理のアイラーニング様研修

現場での経験を重ねつつ、必要なコースを学習してください



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