IBM i 2026

IBM i コンテンツ (2026年1月版)

IBM i セキュリティー戦略
ランサムウェアと脅威への対策

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 セキュリティー戦略
ランサムウェアと脅威への対策

IBM i は、企業の基幹システムを支える堅牢なプラットフォームとして長年利用されてきました。しかし、近年のサイバー攻撃の進化により、IBM i も常に備えをするべきです。特にランサムウェアは、世界中の企業に深刻な影響を与えており、IBM i 環境にも留意が必要です。
現時点では、IBM i 上で直接動作するランサムウェアは確認されていません。しかし、IBM i は最新テクノロジーを実装した OS として、多くのオープンテクノロジー規格のインターフェースを備えており、ネットワーク上の感染した PC を経由して攻撃を受ける可能性があります。感染経路は、メール添付ファイルの開封、Web ブラウザのインジェクション、偽装されたパッチやアップデートのダウンロード、さらにはソーシャルエンジニアリングなど多岐にわたります。
この資料では、IBM i におけるランサムウェアの脅威を理解し、効果的な防御策と監視方法を説明いたします。

目次

1. ランサムウェアの脅威と進化
2. IBM i でランサムウェア対策
3. IBM i でランサムウェアや不正アクセスを検知
4. その他のウィルスやマルウェアについて
5. 今後のステップ
6. IBM i セキュリティーチェックリスト
7. まとめ

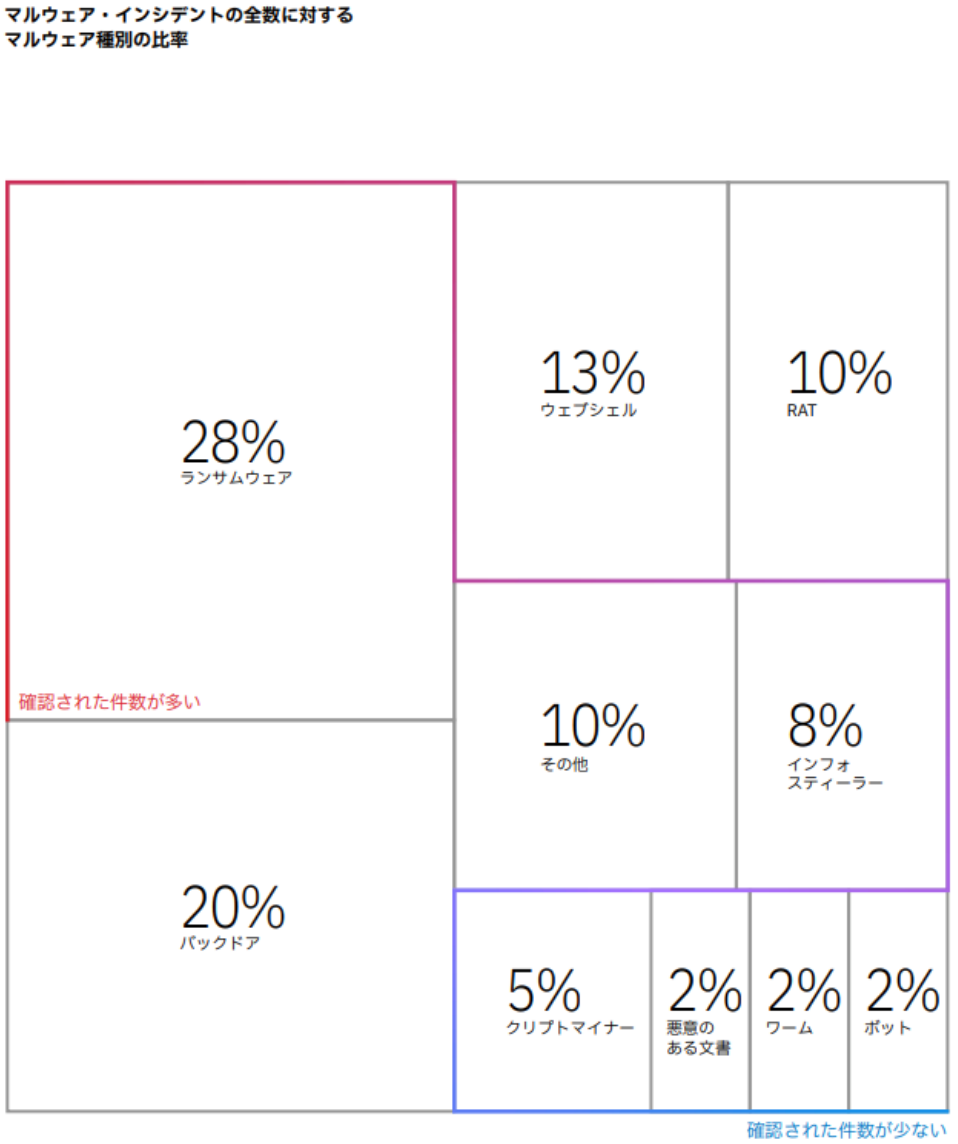
1. ランサムウェアの脅威と進化

1) ランサムウェアの現状

- ランサムウェアは、企業・公共機関・医療機関など幅広い業種を標的にしており、業務停止、金銭的損失、ブランド毀損攻撃成功時の影響が甚大と言われています。
- 攻撃者は、単なる暗号化だけでなく、データ窃取や公開を組み合わせた複合的な脅迫を行うため、被害者は法的・規制上のリスクも負う可能性があります。
- 特に重要インフラや製造業は、停止による社会的影響が大きく、攻撃対象になりやすいです。

2) ランサムウェアの攻撃について

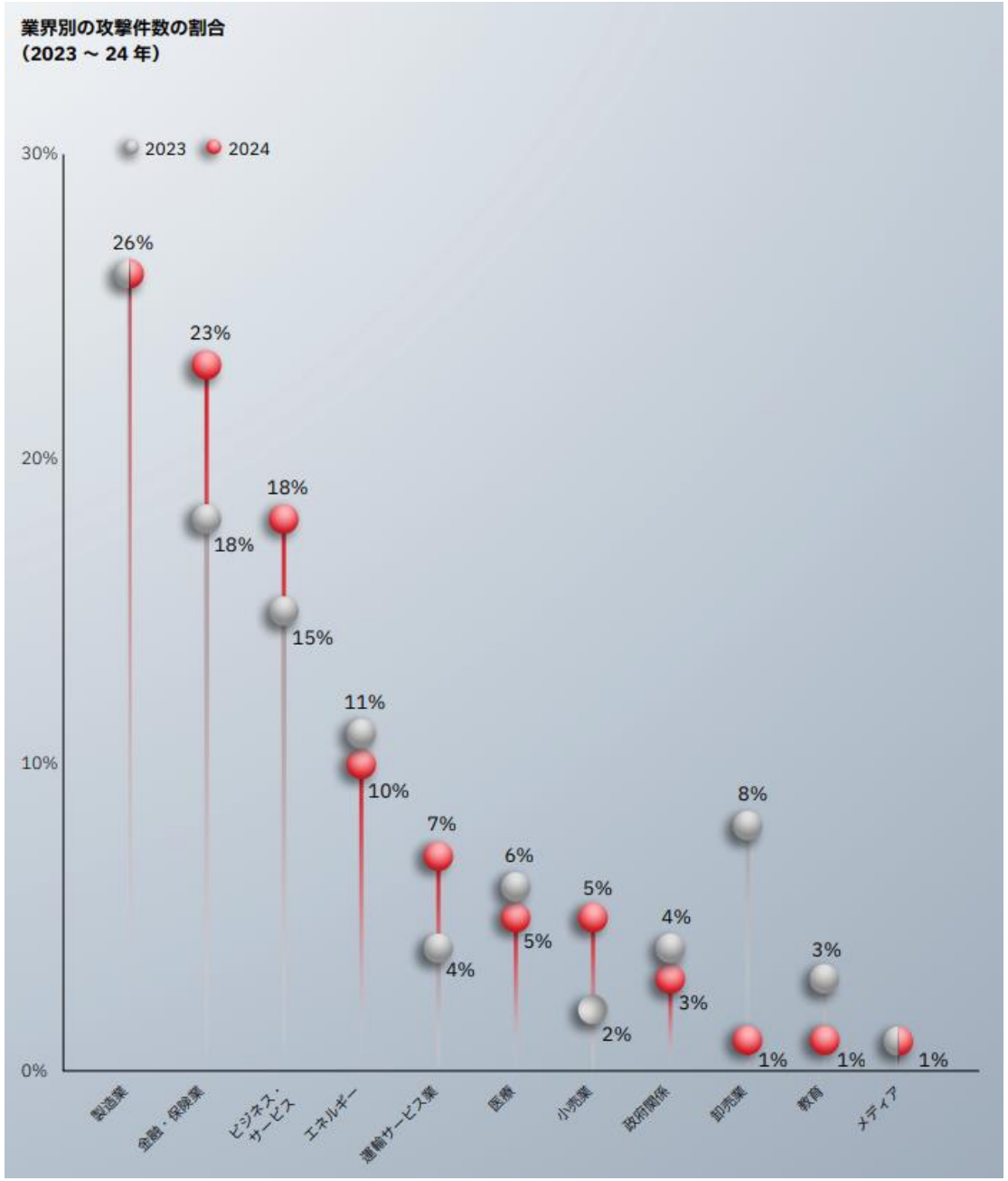
- IBM X-Force Threat Intelligence Indexによると、ランサムウェアは依然として最も多い攻撃タイプの一つとして報告されています。
- 攻撃件数は前年比で増加しており、Ransomware-as-a-Service (RaaS) により技術力のない攻撃者でも攻撃可能になったことが要因です。



1. ランサムウェアの脅威と進化

3) 業界別攻撃傾向

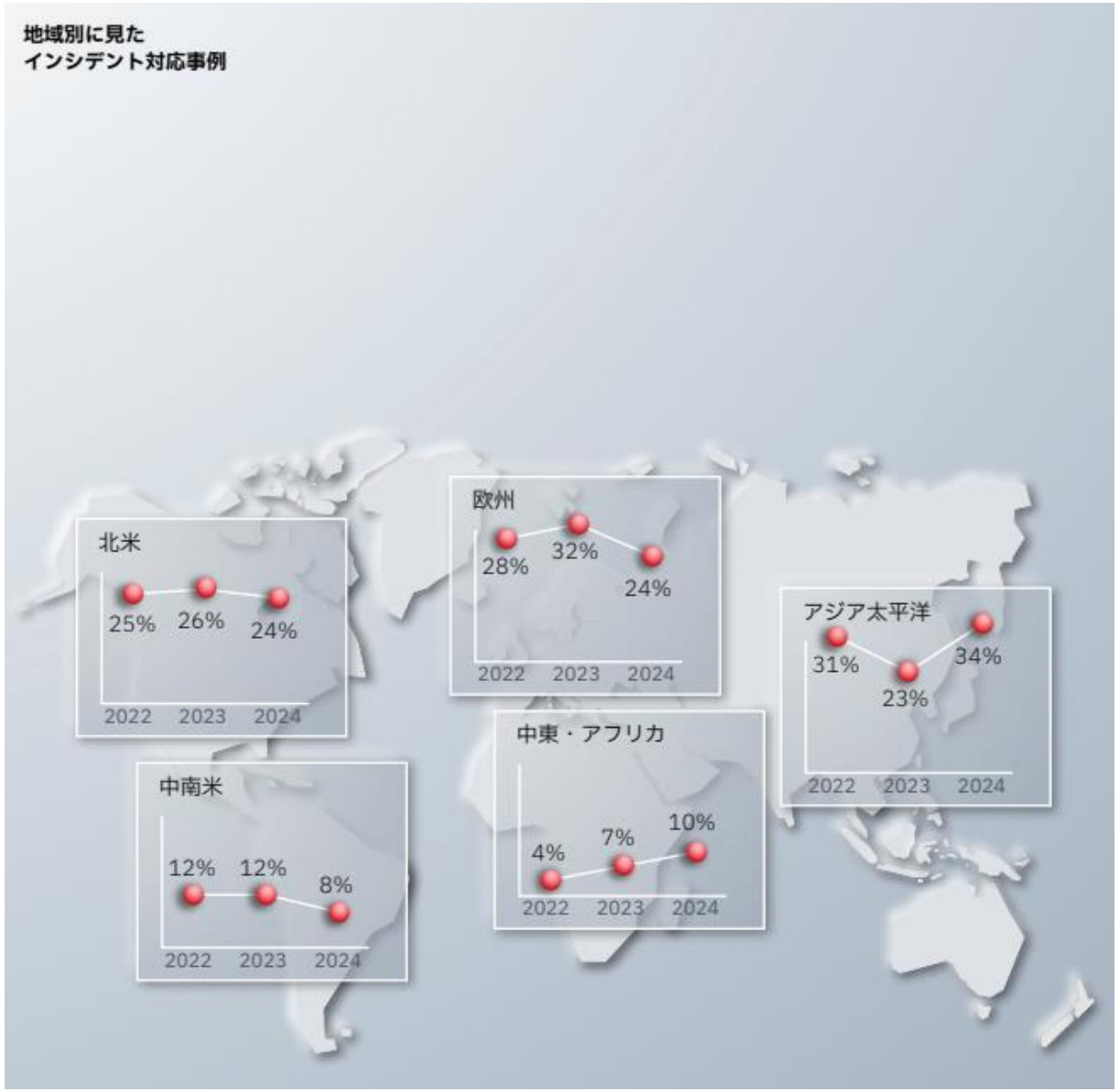
- 製造業は、2023年から引き続き最多の標的となり、インシデントの 26% を占めています。
- 重要インフラ組織に対する攻撃のうち 38% では、正規のツールが使われており、サーバーへのアクセスは 12% のインシデントで目的とされていました。
- 高価値の資産が関わる、事業として依存度が高い、財政的・地政学的に利用しやすいなどの業界を重点的に狙われています。



1. ランサムウェアの脅威と進化

4) 地域別攻撃傾向

- 2024 年に攻撃件数が最多だったのはアジア太平洋 （APAC）地域で、調査対象となった全インシデントの 34% を占めています。
- APAC 諸国の中で攻撃が最も多かったのは日本で、調査対象の全インシデントの 66% に達してます。



2. IBM i でランサムウェア対策

2025年8月時点でIBM i 上で直接実行されるランサムウェアは確認されていません。
しかし、ネットワーク上で感染した PC によって IBM i が影響を受ける可能性はあります。

IBM i は PC 向けのファイルサーバーとして機能し、あらゆる種類のバイナリーデータを保持できます。つまり、IBM i は感染ファイルを保存することはありますが、そのファイルが IBM i 上で直接実行され、システム自体が感染する可能性は極めて低いといえます。

感染ファイルがシステムに入り込む経路は複数存在します。ネットワーク共有だけでなく、FTP、SCP、リムーバブルメディアなども含まれます。これらのファイルは、同じ経路やローカルで稼働する Web サービスを介して PC に再び共有される可能性があります。

IBM i で一番狙われやすい機能はファイル共有機能です。
そのため、NetServer (SMB) や NFS の設定を適切に管理する方法を中心にIBM i のセキュリティー設定方法をご紹介していきます。

2. IBM i でランサムウェア対策

1) NetServer (SMB) 共有の制御

- ゲストアクセスを無効化
  - IBM i プロファイルがないユーザーがNetServer機能を利用する際、ゲストユーザーとして既存のIBM i ユーザープロファイルにマッピングされる。ユーザーが高い権限を持っている場合は攻撃リスクが高いため、無効化を推奨
  - 必要な場合は、ゲストユーザーの権限を最小限（理想は読み取り専用）に設定
  - 設定方法：
    - Navigator for i でダッシュボードのバーからネットワーク→TCPIPサーバーを選択
    - IBM i ネットサーバーを選択してプロパティーを選択

2. IBM i でランサムウェア対策

1) NetServer (SMB) 共有の制御 – 続き
   - 設定方法(続き)：
     - セキュリティータブから次回開始の展開を選択
     - 設定されているゲストユーザーIDが設定されている場合は空欄にする
     - NetServerを再起動して変更を反映(先ほどのページでサーバーの開始、停止が可能)

2. IBM i でランサムウェア対策

1) NetServer (SMB) 共有の制御 – 続き

- 不要な共有を削除
  - IBM Navigator for iで共有の一覧を確認し、不要なものを停止
  - IFSのルート（/）は絶対に共有せずに必要なフォルダのみ共有し、露出範囲を最小化
  - 設定方法：
    - Navigator for i でダッシュボードのバーからファイルシステム→ファイル共有を選択
    - 共有一覧から不要な共有を右クリックして選択、共有停止を選択

2. IBM i でランサムウェア対策

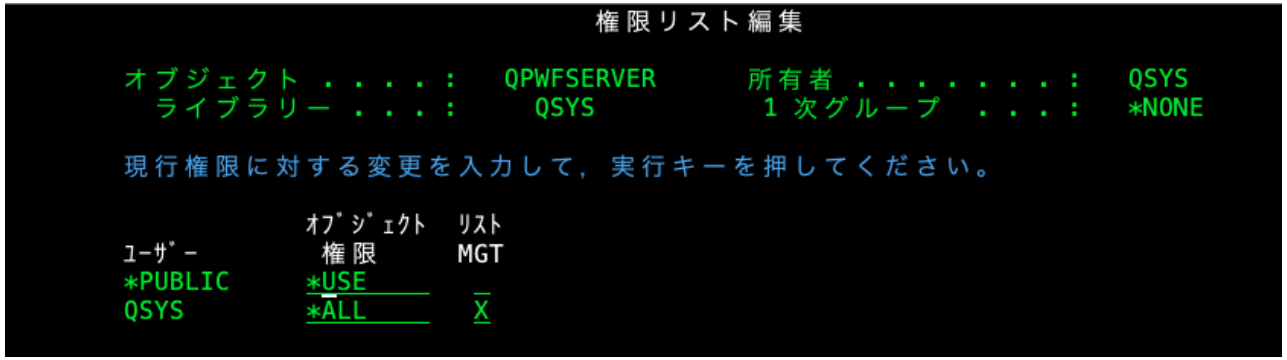
1) NetServer (SMB) 共有の制御 – 続き

- 共有を読み取り専用に設定
  - 必要な共有は読み取り専用に設定し、書き込みを防止
  - 例：請求書PDFの参照のみなら書き込み不要
  - 設定方法：
    - Navigator for i でダッシュボードのバーからファイルシステム→ファイル共有を選択(前スライドと同じ)
    - 共有一覧から設定する共有を右クリックして選択→プロパティーを選択
    - アクセスを「読み取り/書き込み」から「読み取り専用に変更」

2. IBM i でランサムウェア対策

1) NetServer (SMB) 共有の制御 – 続き

- /QSYS.LIBの保護
  - NetServerを使用してQSYS.LIBの共有が必要な場合は、下記の手順でアクセスの制御を行なってください。
- 権限リストにあるQPWFSERVERを使ってNetServer経由の/QSYS.LIBアクセスを制限に加えて、NetServer全体や共有単位で権限リストを設定してください。
- 設定手順
  - 権限リストによるアクセス制御
    - 下記コマンドで権限リスト(QPWFSERVER)の初期設定を変更
      - EDTAUTL AUTL(QPWFSERVER)
      - *PUBLICを*EXCLUDEに変更(一般ユーザーがリモートクライアントから QSYS.LIB にアクセスできなくなる)
        - 初期状態では *PUBLIC に USE 権限 が付与
        - 権限一覧：USE（参照）、CHANGE（更新）、EXCLUDE（アクセス禁止）



2. IBM i でランサムウェア対策

1) NetServer (SMB) 共有の制御 – 続き

- 設定手順(続き)
  - 下記コマンドを使用してアクセスを許可するユーザーの追加
    - ADDAUTLE AUTL(QPWFSERVER) USER(USR名) AUT(*USE)
  - 下記コマンドを使用して設定したユーザーのリストを確認可能
    - EDTAUTL AUTL(QPWFSERVER)
    - 今回はTEST1を*USE権限で追加

2. IBM i でランサムウェア対策

1) NetServer (SMB) 共有の制御 – 続き

- 設定手順(続き)
  - NetServer全体や共有単位で権限リストを設定
    - Navigator for i でダッシュボードのバーからファイルシステム→ファイル共有を選択
    - 公開しているライブラリーを選択して許可を選択(今回はライブラリー名：IMAOを選択)

2. IBM i でランサムウェア対策

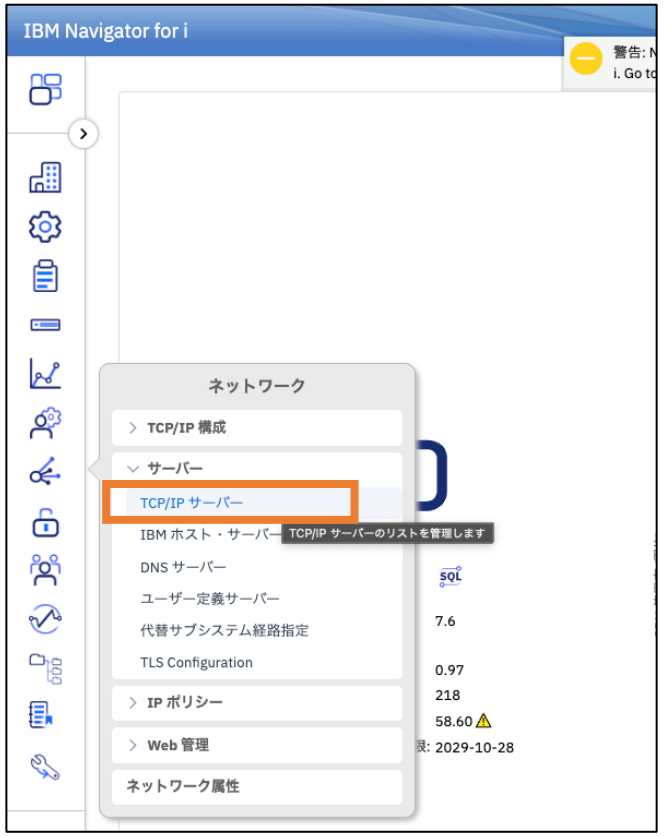
1) NetServer (SMB) 共有の制御 – 続き

- 設定手順(続き)
  - プロパティー画面で下記の項目を制御可能
    - アクセスや暗号化の必要性、権限リストで制御

2. IBM i でランサムウェア対策

2) NFS（Network File System）エクスポートの制御

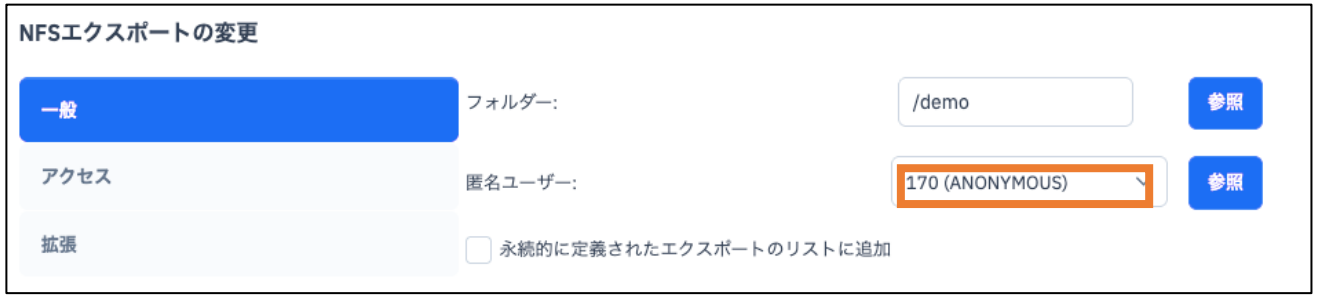
- 匿名アクセス（QNFSANON）を無効化（ANON=-1設定）
- 設定手順
  - Navigator for i でダッシュボードのバーからネットワーク→TCPIPサーバーを選択
  - NFSを選択してエクスポートを選択



2. IBM i でランサムウェア対策

2) NFS（Network File System）エクスポートの制御 – 続き

- 設定手順(続き)
  - エクスポートされているディレクトリーから対象のディレクトリを選択して変更を選択
    - ここでルート（/）や/QSYS.LIBのエクスポートがされている場合は削除して、必要なフォルダのみ共有し、露出範囲を最小化する。
  - 匿名ユーザーの部分をANONYMOUSに選択
    - デフォルトではユーザー名：QNFSANONが設定されていて匿名アクセスが有効
    - 匿名アクセスが有効の場合、認証なしでファイルにアクセス可能になる
    - リンクを参考にして事前にユーザー：ANONYMOUSを作成しておく必要があります
  - NetServerを再起動して変更を反映



2. IBM i でランサムウェア対策

2) NFS（Network File System）エクスポートの制御 – 続き

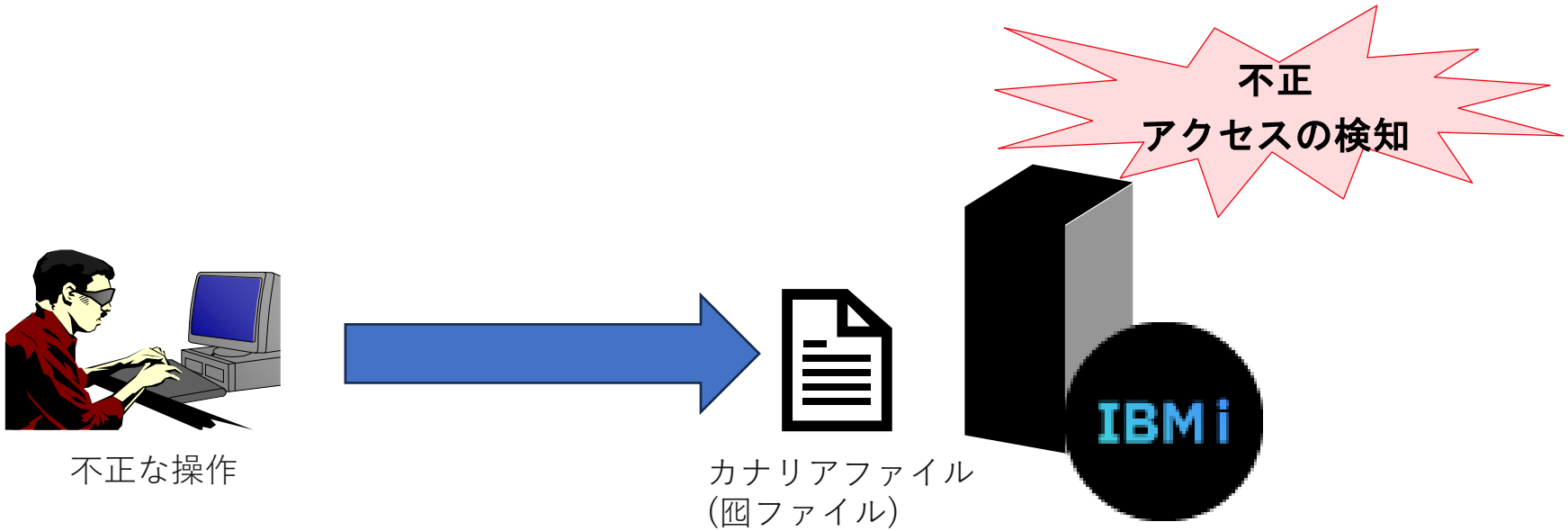
- NFSエクスポートを読み取り専用に設定
- 設定手順
  - P15、p16と同様にエクスポートされているディレクトリーから対象のディレクトリを選択して変更を選択
  - アクセスから既存のアクセス権限を編集を選択
  - オプションでアクセスを読み取り専用に変更

3. IBM i でランサムウェアや不正アクセスを検知

IBM i 環境でランサムウェアや情報漏洩を早期で検知する方法としてカナリアファイル+監査ジャーナルを使用した方法をご紹介します。

カナリアファイル： 囮ファイルとしてランサムウェアや不正アクセスを早期に検知するために使われるファイル

監査ジャーナル：システムのセキュリティー監査専用のジャーナルで、ユーザー操作やシステムイベントを記録するための仕組み　詳細については[こちら]



3. IBM i でランサムウェアや不正アクセスを検知

設定手順

- カナリアファイルの作成
  - 作成例
    - 攻撃者が興味を持ちそうな名前（例：HR、Payroll、Projects）
    - よく狙われる拡張子を使用（例：.docx、.xlsx、.pdf、.zip、.jpgなど）
    - ファイルサイズはゼロバイト不可。数KB以上で実データ風
  - 今回は下記のファイル名：HR_Payroll .xlsxを作成

	A	B	C	D	E	F
1	EmployeeID	Name	Department	Salary	Bonus	BankAccount
2	1001	Michael Jones	HR	550000	5000	XXXX-XXXX-1234
3	1002	Sarah Smith	Finance	620000	7000	XXXX-XXXX-5678
4	1003	David Brown	IT	580000	6000	XXXX-XXXX-9101
5	1004	Emily Davis	Marketing	530000	4500	XXXX-XXXX-1121
6	1005	James Wilson	Sales	600000	6500	XXXX-XXXX-3141
7	1006	Linda Taylor	Finance	640000	7200	XXXX-XXXX-5161
8	1007	Robert Miller	HR	560000	4800	XXXX-XXXX-7181
9	1008	Patricia Anderson	IT	590000	6100	XXXX-XXXX-9202
10	1009	Christopher Thomas	Operations	570000	5000	XXXX-XXXX-1222
11	1010	Barbara Jackson	Legal	650000	7500	XXXX-XXXX-3242
12						
13						

3. IBM i でランサムウェアや不正アクセスを検知

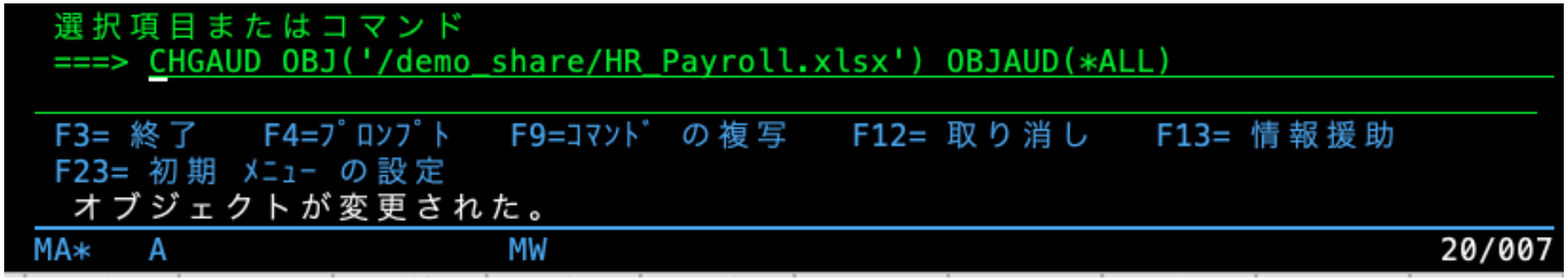
設定手順

- カナリアファイルの配置
  - 配置する場所については下記のポイントを参考に配置
    - ネットワーク経由でアクセス可能な場所
    - 重要なデータやディレクトリが存在する場所
  - 今回はネットサーバーでファイル共有を行なっている/demo_share配下に設置
    - Navigator for i でダッシュボードのバーからファイルシステム→統合ファイルシステムを選択
    - 配置するフォルダを右クリックしてアップロード先を選択
    - 使用するフォルダを選択してUploadを選択

3. IBM i でランサムウェアや不正アクセスを検知

設定手順

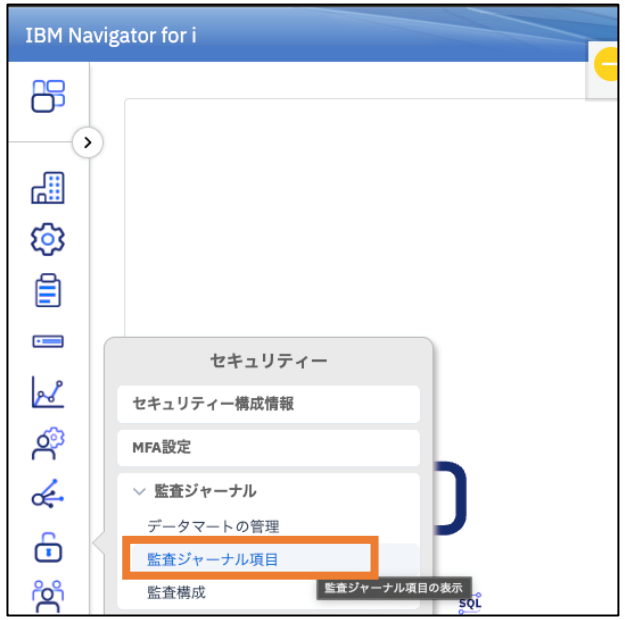
- 監査設定
  - ここからは監査ジャーナルの初期設定が完了していることを前提に進めます。
    - 初期設定の方法はこちらのP17「監査ジャーナルの設定をしてみよう」を参考にしてください。
  - 下記コマンドを使用してオブジェクトの監査を指定します。
    - CHGAUD OBJ('/demo_share/HR_Payroll.xlsx') OBJAUD(*ALL)
  - 今回は読み取り・書き込み・名前の変更を検知
    (暗号化検知のみの場合は*CHANGEにして書き込み、名前変更を検知します)

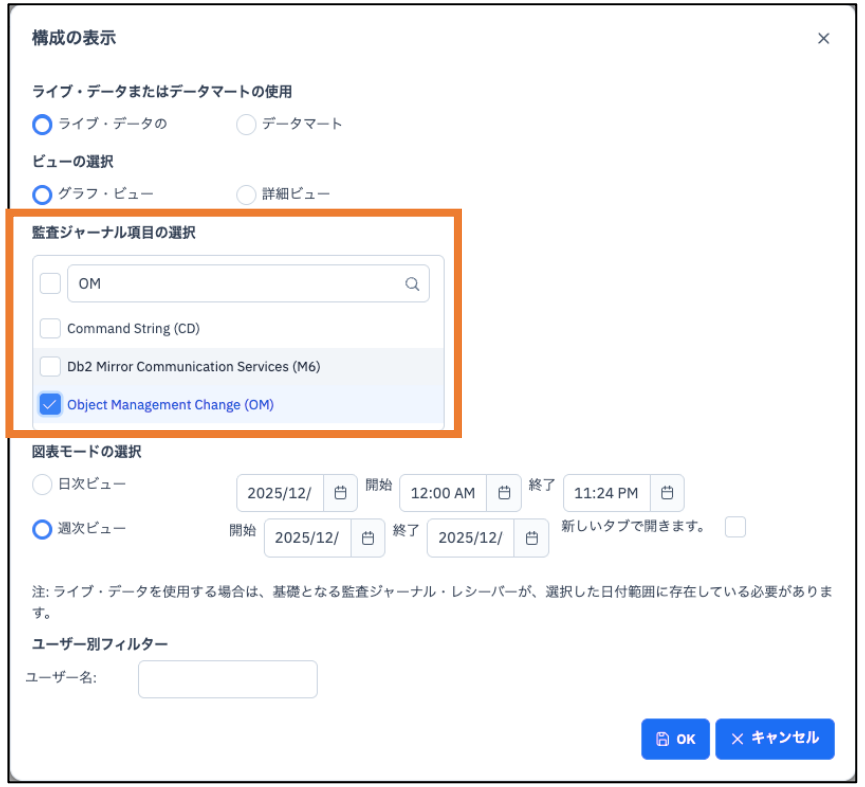


3. IBM i でランサムウェアや不正アクセスを検知

実際に動かしてみる

- オブジェクトの名前変更を行う
  - /demo_share配下のHR_Payroll .xlsxのファイル名を変更
- 監査ジャーナルに記録されたデータを確認
  - Navigator for i でダッシュボードのバーからセキュリティー→監査ジャーナル項目を選択
  - 今回はファイル名を変更したのでOM(オブジェクト管理変更)を指定して確認
  - 他にも検知イベントとして下記の項目を指定することを推奨
    - ZR：読み取り
    - ZC：書き込み





3. IBM i でランサムウェアや不正アクセスを検知

実際に動かしてみる

- 監査ジャーナルに記録されたデータを確認する
  - 下記のようにオブジェクト管理の詳細ビューからオブジェクト名が変更されている履歴が確認可能

3. IBM i でランサムウェアや不正アクセスを検知

誤検知について

- 情報漏えい検知は誤検知が多い
  - 誤操作でファイルを開く社員や大量コピーを行うことでアラートが発生することはあります。
  - ただし、内部脅威や早期検知には有効です。

- 誤検知を減らす方法
  - 暗号化検知のみの設定を行う。
  - CHGAUDで*CHANGE監査を設定（書き込み・名前変更のみ検知）する。
  - 書き込みや名前変更は通常操作で発生しにくいため、誤検知が減少します。
  - ファイル名は「aa～」「zz～」で始めるとランサムウェアが最初に処理しやすく、早期検知可能です。
  - ファイル内容はランダム文字列や「このファイルはランサムウェア検知用」などの注意文でも可能です。

検知後の対策

- 攻撃元PCを即座にネットワークから切断
- ログを確認し、影響範囲を特定
- 社内ポリシーに従い、データ復旧・侵害対応を実施
- 必要に応じてパートナー様に支援依頼

4. その他のウィルスやマルウェアについて

- ランサムウェア以外の脅威
  - IBM i はモダンな OS であり、オープンソースや Web アプリ（PHP など）を実行可能です。Linux向けWebShellやスクリプト型マルウェアがIBM i環境で攻撃手段として成立します。
  - 参考文献：https://community.ibm.com/community/user/blogs/alejandro-lazzaro/2025/10/13/malware-and-ibm-i

- アンチウイルス対応について
  - IBM i OS 自体にはウイルススキャンエンジンやシグネチャデータベースは含まれません。
  - IBM およびサードパーティからアンチウイルス・アンチマルウェア製品が提供されてます。
  - IBM提供の PowerSC には ClamAV エンジンが含まれ、FreshClam による定期更新や IFS スキャンが可能です。

- セキュリティー評価の実施
  - IT 標準では外部組織による年次セキュリティー評価が推奨されております。

紹介したランサムウェア対策に加えて、次ページに紹介する今後のステップを行うことを推奨します。

5. 今後のステップ

IBM i のセキュリティー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経由でのIFS共有は必要最小限にとどめ、ユーザープロファイルの権限を最小限にする
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、セキュリティー・ログを監視

5. 今後のステップ

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（セキュリティー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

5. 今後のステップ

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ー・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
→つまり、現状の実行時権限の可視化を行い、オブジェクトへの付与権限の最適化（最小化）が可能

✓ 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）

5. 今後のステップ

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(システム管理ドキュメント：サーバーのバックアップについて)

✓ 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。

5. 今後のステップ

4) NetServer経由でのIFS共有は必要最小限にとどめ、ユーザープロファイルの権限を最小限にする

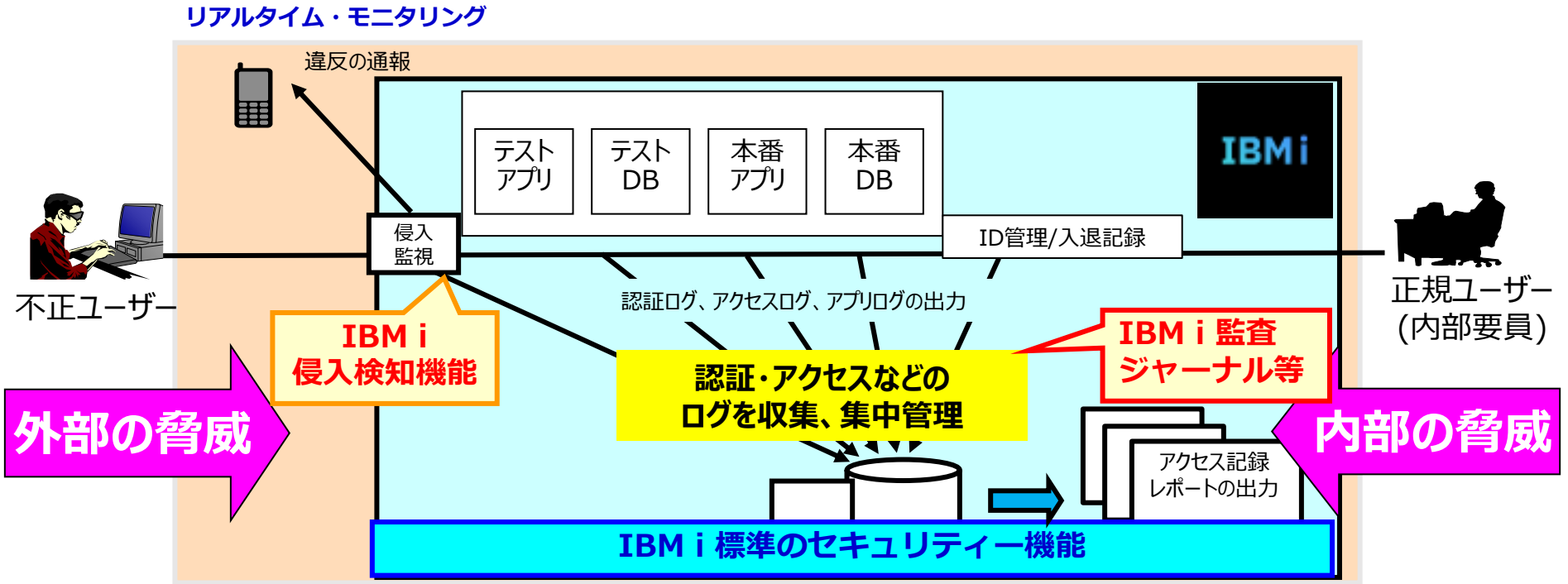
IBM i をファイルサーバーとしてWindowsやクライアントから利用する場合、IBM iの共用フォルダーが悪意あるプログラムの温床・媒介となる可能性があります
一般的なセキュリティーの観点も併せて下記のようなマルウェア、ウィルス等への対策も鑑みた推奨設定

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. 今後のステップ

5) 監査ジャーナルを設定し、セキュリティー・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】



6. IBM i セキュリティーチェックリスト

- ゲストや匿名ネットワークアクセスを無効化する
- 可能な限りネットワーク共有やエクスポートを削除する
- 共有やエクスポートは可能なら読み取り専用に設定する
- 共有やエクスポートのマウントポイントを移動し、公開されるディレクトリやファイルを減らす
  - IFS のルート（/）を共有／エクスポートしないこと
- QPWFSERVER を使用して NetServer から /QSYS.LIB へのアクセスをブロックする
- 共有データへのアクセスを可能な限り少人数に制限する
  - ライブラリや IFS フォルダーの権限を変更し、書き込み権限を削除（ファイル暗号化防止）
  - ライブラリや IFS フォルダーの権限を変更し、読み取り権限を削除（データ流出防止）
  - システムセットアップ完了後、IFS のルート（/）と /QOpenSys の権限を *PUBLIC *RWX → *RX に変更
  - IBM i 7.5 以上の場合、サーバーおよび共有レベルの権限リストを追加
- データ回復の準備とテストを実施する
- 侵害を即時検知するため、 カナリアファイルやハニーポット監視システムを設定する
- PTF、パッチ、OS レベルを最新に保つ
- アンチウイルス／アンチマルウェアプログラムの導入を検討する
- 外部機関による年次セキュリティー評価を受ける

7. まとめ

IBM i は業界で最も高いセキュリティー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ーリスクに応じて、IBM i セキュリティー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ー機能の活用
  - すべてのセキュリティー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
  - セキュリティーの継続的な評価&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

IBM i 若手技術者コミュニティー
IBM i RiSING　参加者募集中！

「技術力向上と情報交換を目的とした若手エンジニアのためのコミュニティー」

4月~10月の半年間で活動

- 年3回IBM主催の全体会議(キックオフ/中間発表/最終発表)
  ＋ 各チームにおける分科会に参加
- RPGモダナイゼーション・Git/VS code活用・生成AI連携・
  Node js・パフォーマンス可視化・IBM i 学習支援　等

IBM i の業務経験が10年以内の技術者の方

2024/2025年同活動参加メンバーの継続参加も大歓迎！

参加登録

https://ibm.biz/Rising2026Reg

※　本活動は研修ではなくコミュニティー活動です。IBM i の基本操作を理解されている方、または今後積極的に学ぶ意欲のある方を前提として参加をお願いしています。

IBM i 関連情報 – 1) 情報サイト (2025/12/08 更新)

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

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

新・IBM i入門ガイド［操作・運用編］
https://www.imagazine.co.jp/01-ibm-i-jikkoukankyou-of-ibm-i-nyumon-guide-sousa-unyou/
新・IBM i入門ガイド［開発編］
https://www.imagazine.co.jp/01-development-tools-of-ibm-i-nyumon-guide-kaihatsu/
これから使う人のためのIBM i入門ガイド (旧バージョン)
https://www.imagazine.co.jp/imagazine-7071/

IBM i 製品とサポートのロードマップ
https://ibm.biz/ibmiroadmap2025

IBM i 7.6 技術資料 (英語版)
https://www.redbooks.ibm.com/abstracts/sg248588.html

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」「9105-41B」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 Power Virtual Server 情報
https://ibm.biz/pvsjapan

IBM i 関連情報 – 2) スキル関連サイト (2025/12/08 更新)

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 リスキリングカレッジ
https://ibm.biz/ibmireskill2025

IBM i RiSING - IBM i 若手技術者コミュニティー
2026年度参加者募集ページ
https://ibm.biz/Rising2026Reg
<ご参考> 2025年度ページ
https://ibm.biz/ibmirising2025

IBM TechXchange Powerユーザーコミュニティー (日本)
https://ibm.biz/ibm-power-user-community

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 i 研修サービス (ティアンドトラスト社提供)
https://www.tat.co.jp/cor/COR420P.php

IBM i 研修サービス (クレスコ・ジェイキューブ社提供)
https://www.cresco-jcube.co.jp/business/j-cube-academy

IBM i 研修サービス (ソリューション・ラボ・ジャパン社提供)
https://www.slj-net.co.jp/sustainable-solutions/rpg/

IBM i 研修サービス (ソルパック社提供)
https://www.solpac.co.jp/service/powersystems/TrainingService/

IBM i 関連情報 – 3) オンデマンド・セミナー (2025/12/08 更新)

IBM i Advantage 2025 オンデマンド・セミナー
2026年1月15日放映開始予定
https://ibm.biz/ibmiadvantage2025

IBM i World 2025 オンデマンド・セミナー
https://ibm.biz/ibmiworld2025

IBM i Advantage 2024 オンデマンド・セミナー
https://ibm.biz/ibmiadvantage2024video

IBM i World 2024 オンデマンド・セミナー
https://video.ibm.com/recorded/133917616

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