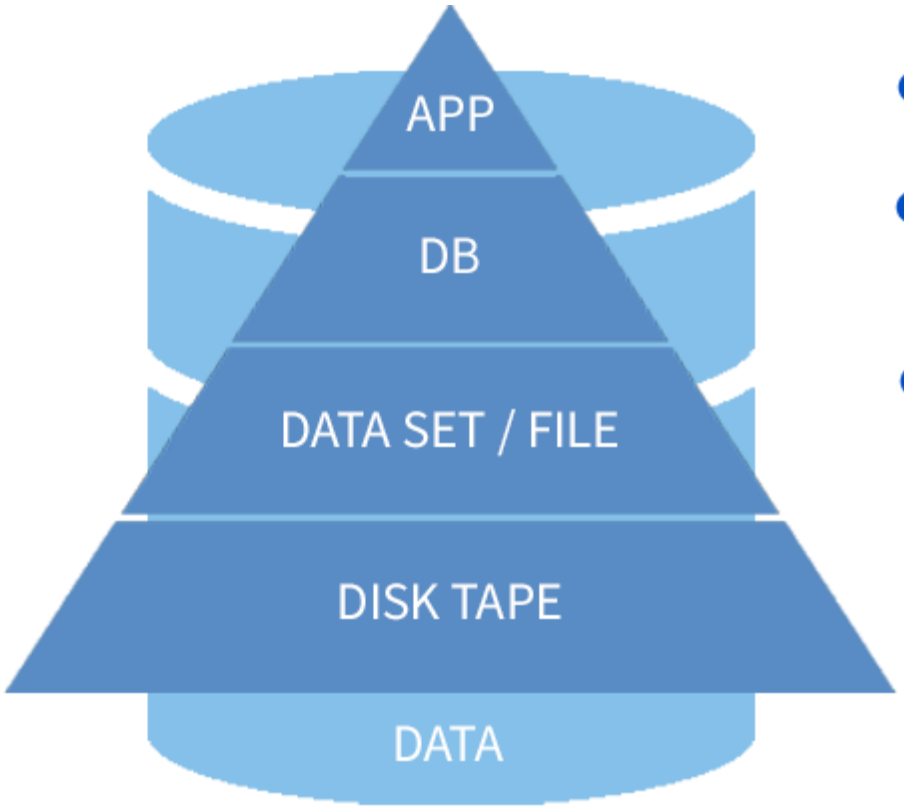
IBM Power（IBM i）のセキュリティ対策

IBM Power（IBM i）で堅牢なセキュリティを構築するためのポイントと対策についてご紹介します。

INDEX

JBCC

セキュリティ対策で守るべきものとは・・・



- アプリケーション（APP）
  超機密データ
- データベース（DB）
  機密性の高い使用中、
  もしくは転送中および保管中のデータ
- ファイル/データセット
  転送中および保存中のデータの
  アクセス制御に関連付けられた機密データ
- ディスクおよびテープ全体
  暗号化等によりデータを物理的に
  保管中のデータを保護

堅牢なセキュリティを構築するための3つのポイント

1. 「セキュリティ・ポリシー（個人情報の取り扱いポリシー）」を策定する

遵守するべき社内ルールを取り決める

2. セキュリティに強いコンピューター・システムを選択する

強固なセキュリティ機能を持つコンピューター機器、ソフトウェアを選択する

IBM Power（IBM i）は、高いセキュリティ、
堅牢なシステムを構築するために必要な様々な機能やアーキテクチャーを標準機能で提供します

3. セキュリティ・ポリシーを正しく運用する

誰が、いつ、どこから、どのデータに、どのような操作をしたか、把握できることが重要

・セキュリティに「100%安全」ということはありえない
・何か起こった時にそれに対処できる準備をしておくことが重要

セキュリティポリシーが正しく運用されているかを日々確認することが重要

・遵守状況の定期的な調査
・サーバーのアクセス･ログの定期的な確認

IBM Power（IBM i）を使用して、適切なシステム設定 + 適切な運用管理を行うことで、
堅牢なシステムを構築することができます

適切なシステム設定をすべき項目

QSECURITY・システム値 *SEC・ユーザープロフィール 特殊権限・ユーザープロフィール制限機能・オブジェクト特定権限
権限リスト・借用権限・監査ジャーナル・5250端末関連の設定・FTP・TELNET・ Netサーバー・SQL・JDBC・ODBCアクセス

IBM i セキュリティ対策のポイント

IBM Power（ IBM i)の高度なセキュリティ機能も、正しく設定・運用しないと十分に活用ができない！
近年では特に内部不正防止の視点での対策が重要！

~~IBM i はセキュリティが強固なシステム~~
セキュリティを強固にすることができるシステム

設定・運用対象ポイント
A ユーザープロファイル管理
B システム値設定
C 外部アクセス制御
D 通信の暗号化
E 最新テクノロジーの活用
F 監査ジャーナル（履歴証左）

内部不正防止の基本原則

	項目	内容	対策例
1	犯行を難しくする	対策を強化することで犯罪行為を難しくする（やりにくくする）	対策を強化することで犯罪行為を難しくする（やりにくくする）
2	捕まるリスクを高める	管理や監視を強化することで捕まるリスクを高める（やると見つかる）	管理や監視を強化することで捕まるリスクを高める（やると見つかる）
3	犯行の見返りを減らす	標的を隠したり、排除したり、利益を得にくくすることで犯行を防ぐ（割に合わない）	標的を隠したり、排除したり、利益を得にくくすることで犯行を防ぐ（割に合わない）
4	犯行の誘因を減らす	犯罪を行う気持ちにさせないことで犯行を抑止する（その気にさせない）	犯罪を行う気持ちにさせないことで犯行を抑止する（その気にさせない）
5	犯罪の弁明をさせない	犯行者による自らの行為の正当化理由を排除する（言い訳をさせない）	基本方針の策定、管理・運用策の策定、業務委託契約、就業規則

IBM i セキュリティ再認識①～Windos / Linux サーバーとの比較

【セキュリティーの堅牢性】

IBM Power（ IBM i ）は

◆当初から企業での商業ユースを想定したシステムデザイン

◆低コストで高いセキュリティを実現可能

● IBM i

・必須セキュリティ機能をOSに全て統合

・オブジェクト指向デザイン

・カーネルの仕様は非公開SLICに組み込まれた
セキュリティ機能で整合性のとれた
安全性の高いセキュリティを実現

・ 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 / Linux

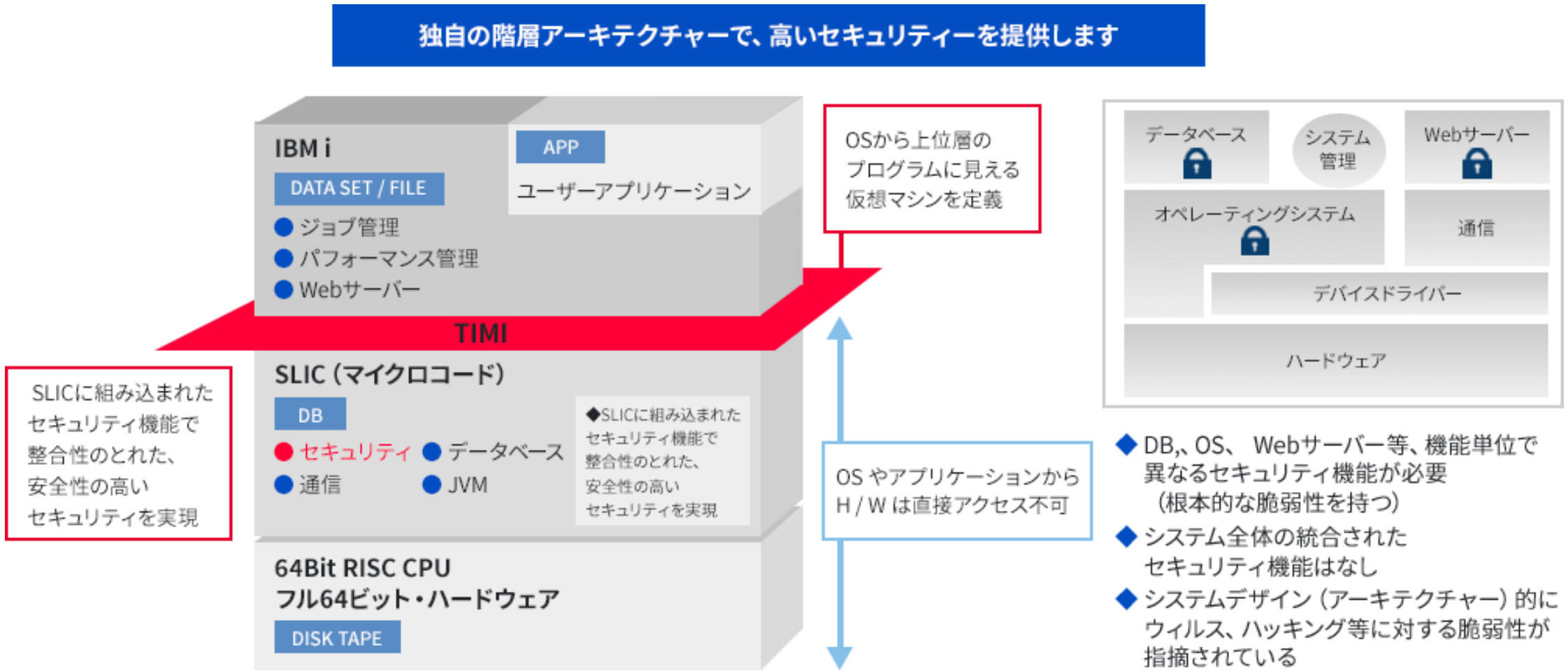
・各種機能が統一されたデザインではない
（データベース、機密保護、バックアップなど）

・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

IBM i セキュリティ再認識①～Windos / Linux サーバーとの比較

さらに最新の IBM i では情報漏えいに強いセキュリティを構築可能です。

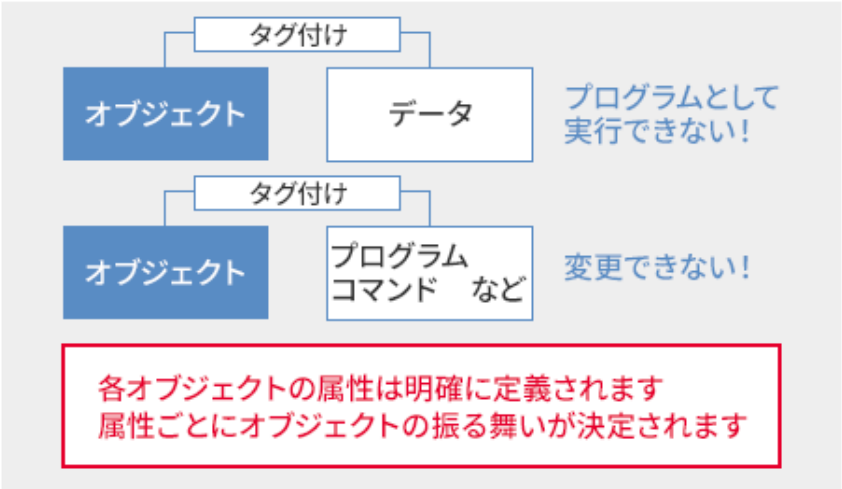


IBM i セキュリティ再認識②～堅牢なセキュリティを実現するIBM Power（IBM i） のアーキテクチャー

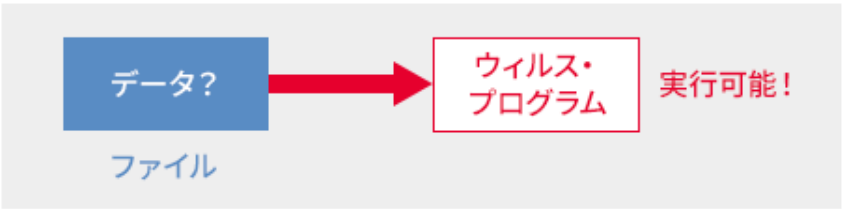
IBM i は1988年の出荷以来、ウィルスハッキング・クラッキング報告 ゼロ です！

- 機密保護機能をマイクロコード層に統合
  - ・C2レベルセキュリティ
  - ・耐ウィルス設計
  - ・ウィルスによるプログラムの改竄が難しい
  - ・IBM i の内部設計仕様は一般に公開されていない
- 優れた耐ウィルス設計としてオブジェクト思考アーキテクチャーを採用

IBM i では

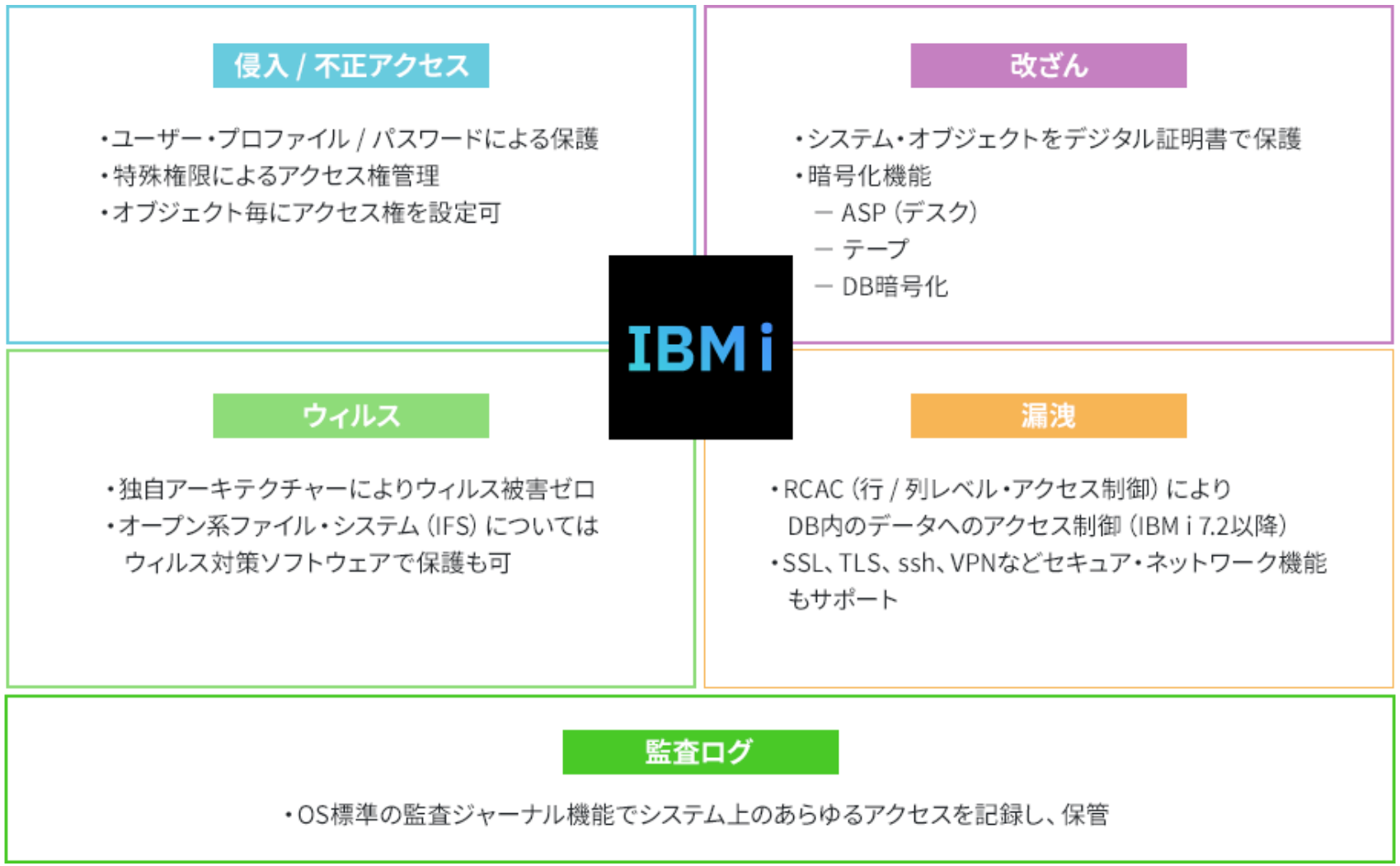


ほかのサーバーでは



IBM i セキュリティ再認識③

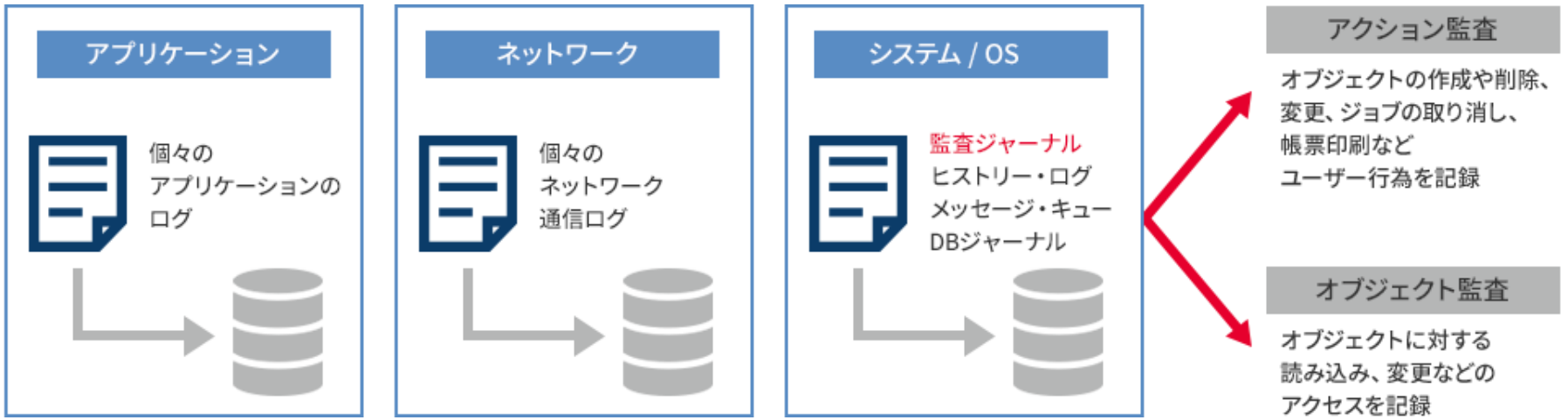
IBM i に組み込まれた強固なセキュリティー



IBM i セキュリティ再認識④

IBM i OS組込みの監査ログ機能

- **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**
- **詳細監査ログで内部統制の実施をサポート**



OS標準の詳細なロギング機能により、

証跡管理に役立て高いセキュリティーを維持することができます

IBM i セキュリティ再認識まとめ

セキュリティ・ポリシーは不可欠

- 企業のセキュリティー・ポリシーは、IT 環境全体で一貫性のあるセキュリティー設定を行うために不可欠です
  - すべての管理者は、何をすべきか、何をすべきでないか知っている（はず）

- IBM i セキュリティー構成は、完全に文書化する必要があります
  - 将来の参照用
  - 何が行われたのか、なぜ行われたのかを監査人に示すため
  - 構成の変更は、新規インストールまたはリリース・アップ後に実行される
    セットアッププログラム（つまり、CL プログラム）で文書化するのが最適