IBM i World 2023

IBM i コンテンツ　(2023年5月版)

IBM i のセキュリティ再認識

- IBM i をより安全に使うための 設定方法ご紹介します -

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
澤田英寿

© IBM 2023

目次

IBM iセキュリティ再認識

© IBM 2023

1. IBM i セキュリティ再認識: IBM i セキュリティ再認識 (1)

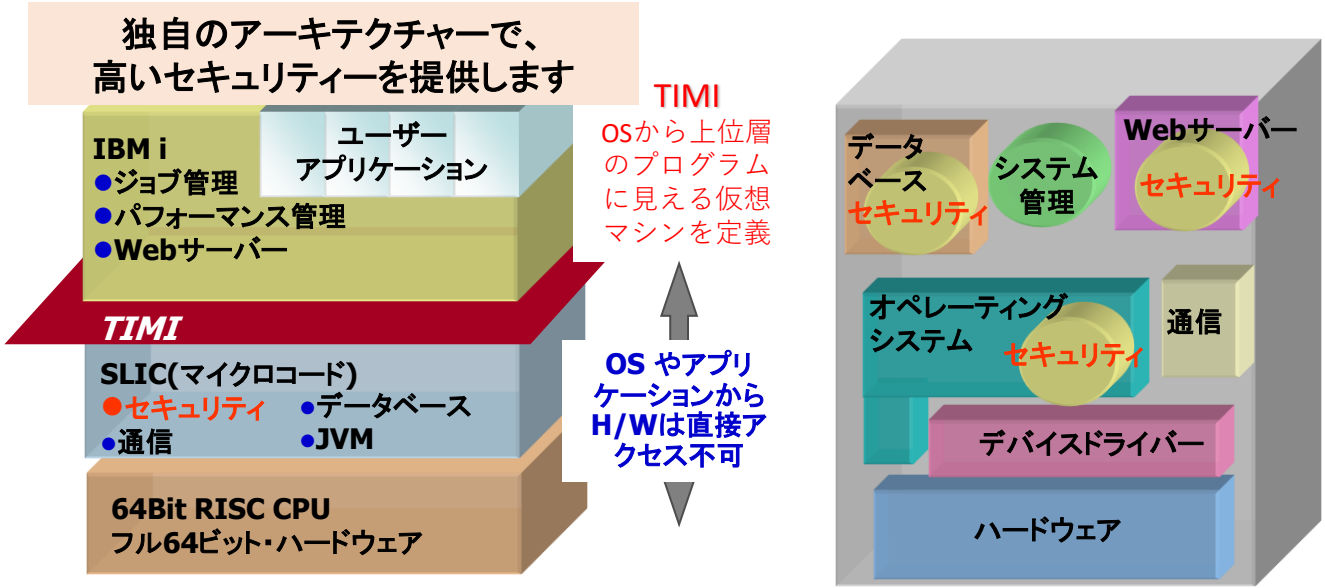
セキュリティーの堅牢性

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



© IBM 2023

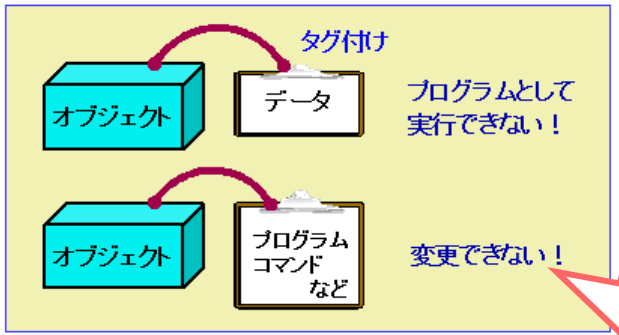
IBM i セキュリティ再認識（2）

IBM i の堅牢なセキュリティー

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しています

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!

IBM i では



他のサーバーでは

各オブジェクトの属性は明確に定義されます
属性ごとにオブジェクトの振る舞いが決定されます

© IBM 2023

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

侵入/不正アクセス

・ユーザー・プロファイル/パスワードによる保護
・特殊権限によるアクセス権管理
・オブジェクト毎にアクセス権を設定可

改ざん

・システム・オブジェクトをデジタル証明書で保護
・暗号化機能
- ASP (ディスク)
- テープ
- DB暗号化

POWER9/10が持つ暗号化アクセラレータにより、暗号化/復号化処理も高速！

IBM i

ウィルス

・独自アーキテクチャーによりウィルス被害ゼロ
・オープン系ファイル・システム(IFS)については ウィルス対策ソフトウェアで保護も可

漏洩

・RCAC (行/列レベル・アクセス制御) により DB内のデータへのアクセス制御 (IBM i 7.2以降)
・SSL, TLS, ssh, VPNなどセキュア・ネットワーク機能もサポート

監査ログ

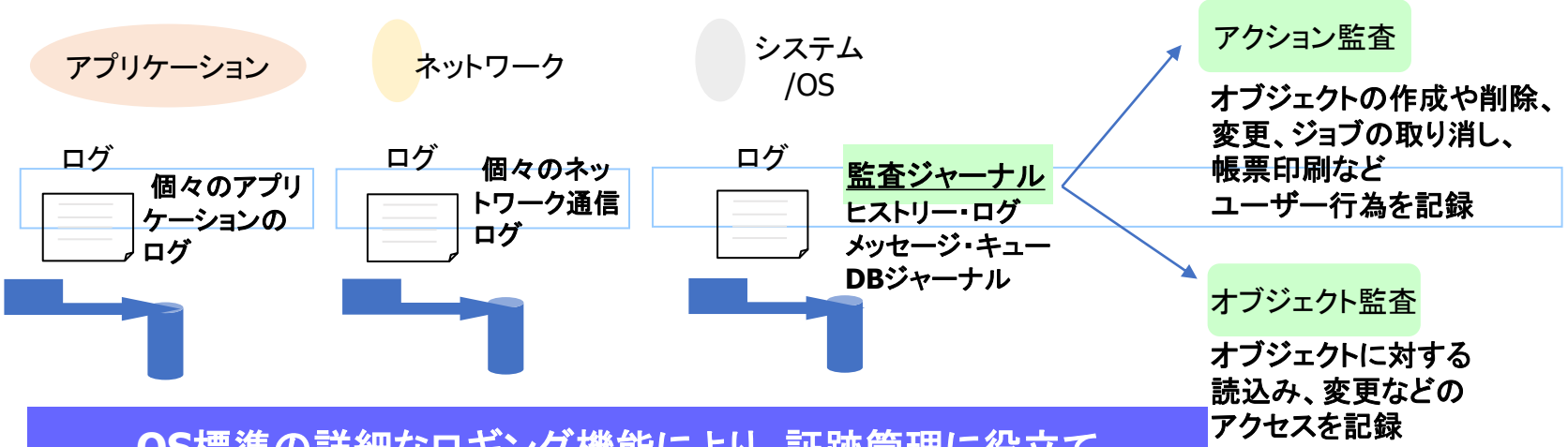
・OS標準の監査ジャーナル機能でシステム上のあらゆるアクセスを記録し、保管

© IBM 2023

IBMi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 2023

IBM i セキュリティ再認識（5）

実際に、

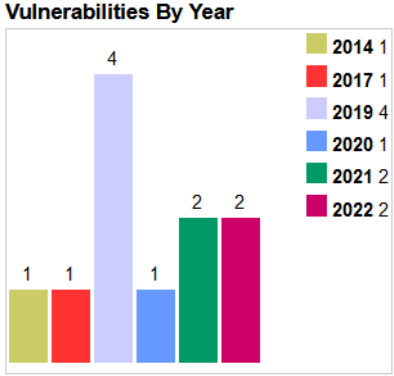
IBM iは、競合するオペレーティングシステムと比較して、セキュリティ上の脆弱性が桁違いに少ない

IBM i (全バージョン)

6年: 11件

~2件 /年

https://www.cvedetails.com/product/26779/IBM-I.html?vendor_id=14

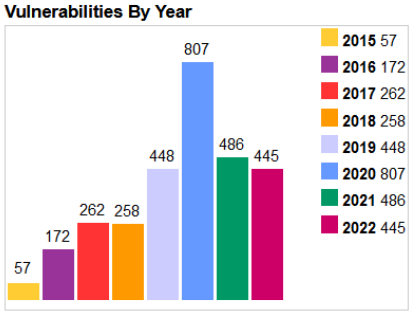


Windows 10

7年:2935件

~419件 /年

https://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor_id=26

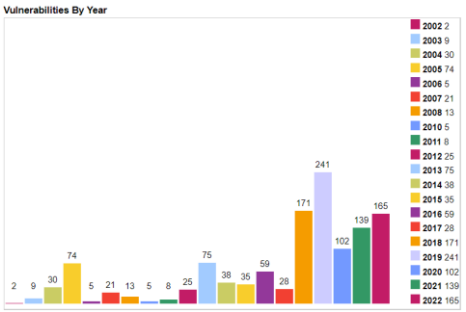


RHEL (全バージョン)

20年: 1245件

~62件/年

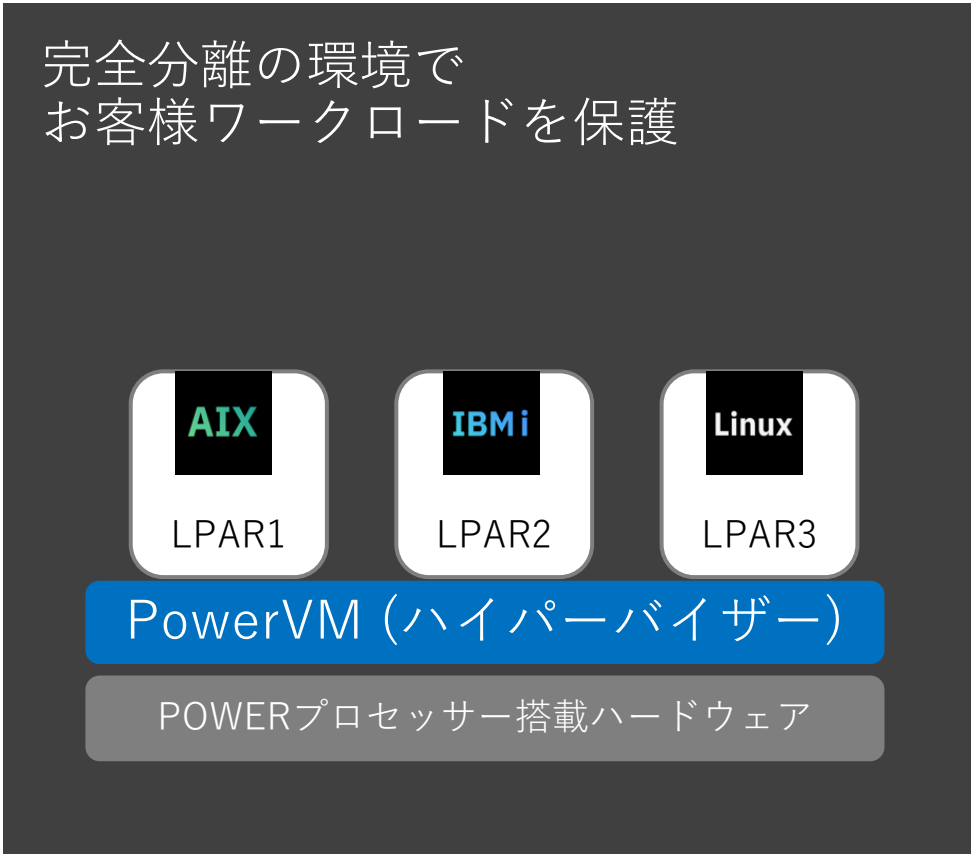
https://www.cvedetails.com/product/78/Redhat-Enterprise-Linux.html?vendor_id=25



© IBM 2023

IBM i セキュリティ再認識（6）

IBM Power の仮想化のセキュリティ：鉄壁のワークロード分離

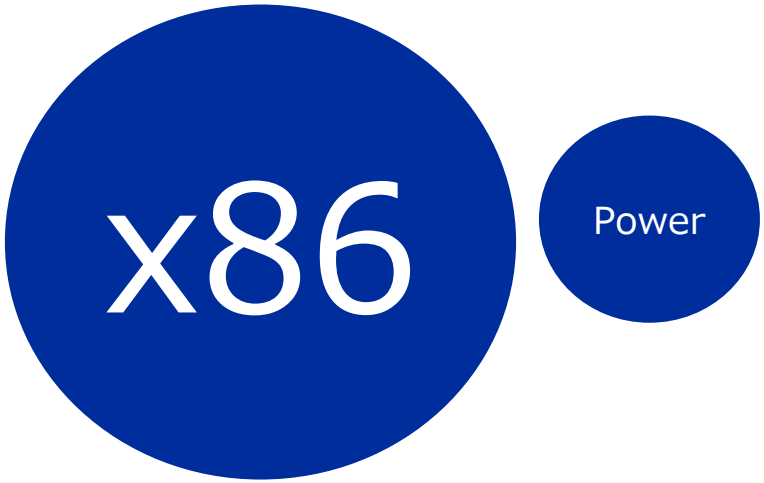


- ハイパーバイザーを Firmware 上に実装
  - OSと独立することでシステム全体を安全に保護
- 他の区画によるパフォーマンスの影響がない
  - マルチテナント環境でも安心して利用可能
  - ワークロードを集約しても安心
- LPAR 間で情報が秘匿される
  - マルチテナント環境でも安心して利用可能

Power10 ではパフォーマンスに影響のないサイドチャネル攻撃への対策が実装され、一層強固なワークロード分離が実現されています。

IBM i セキュリティ再認識（7）

Powerの仮想化は、後からインストールするのではなく、IBM Powerに組み込まれています。これにより、攻撃される可能性のある「表面積」を大幅に減らすことができます



Powerの仮想化基盤に対して公表された脆弱性は17年間でわずか4つだけです

VMwareは1999年以降536件、2021年だけで77件の脆弱性が公表されています

IBM Technology / Worldwide Power Spotlight / May 18th, 2022 / © 2022 IBM Corporation

© IBM 2023

IBM i セキュリティ再認識（8）

IBM i のセキュリティ機能は、新リリースごとに進化している

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

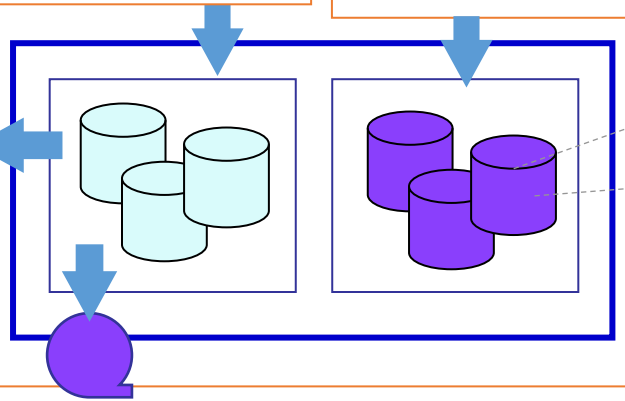
権限収集 – オブジェクト（IBM i 7.4）
・オブジェクトへのアクセスを精査し、必要な最低限の権限を報告

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

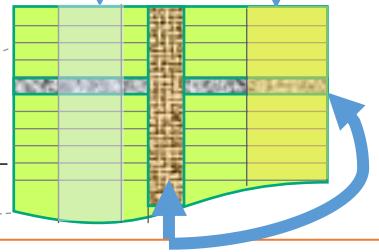
監査用追加カラム（IBM i 7.3-）OS が自動でデータ付与

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)



Db2 for i
テーブル・ビュー

RCAC（IBM i 7.2-）
- Row & Column Access Control レコード単位 またはカラム単位でアクセス制限
- 行（Row）アクセスに認証
- 列（Column）をマスク

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

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

© IBM 2023

IBM i セキュリティ再認識まとめ

IBM i セキュリティの考察

✓ 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

✓ IBM iは、新リリースでも、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 2023

2. IBM i ユーザー共通のリスクと推奨事項

- デフォルト・パスワード
- 共通権限ユーザー・プロファイル
- 認証なしの DDM アクセス
- SSH アクセス
- 特殊権限を持つユーザーの数が多い
- 作成されたオブジェクトに対する共通権限
- 未使用のネットワーク・サービスおよびデフォルト構成
- 無制限のリモート・データアクセス

© IBM 2023

デフォルト・パスワード

- システムへのアクセスを容易にするための簡単な利用：ほとんどのシステムで見られる
- ほとんどのシステムで、デフォルト・パスワードを持つユーザーが *ALLOBJ を含む特殊権限をもっている
  - セキュリティ・アセスメントでは、デフォルトのパスワードを持つ数個から数千のプロファイルが示された
- 主に、IT 担当が原因のデフォルト・パスワード
  - 任意のパスワードを指定できます
  - パスワードは、パスワード・ポリシーに準拠する必要がない
- デフォルト・パスワードの分析 (ANZDFTPWD) をすると、ユーザー・プロファイルを表示できる

```
                    デフォルト・パスワードを使用するユーザー・プロファイル
5770SS1 V7R4M0 310522
 プロファイルに対して実行されたアクション . . . . . : *なし
 ユーザー
 プロファイル状況 PWDEXP テキスト
 APPSEC1 *ENABLED *NO HOS アプリケーション管理
 BR144122 *ENABLED *NO ブラチスラバ・アカウンティング
 MICHELE *ENABLED は、 Michele B を使用します。
 WLBLK22 *ENABLED - ウェイン・ L ・ウェイン
 WMERK813 *ENABLED を *NO に設定します。
```

© IBM 2023

デフォルト・パスワード - 推奨事項

- QPWDRULES システム値を使用してパスワード ポリシーを定義する
  - *ALLCRTCHG 構成値を含めて、管理者にもポリシーを強制します (IBM i 7.2 以降)*
- QPWDLVLシステム値の「3」を使用して、パスフレーズ、その他の特殊文字、および大文字と小文字の混在をサポートできるようにする
  - IBM i V7R5 は、新しいQPWDLVL（パスワード・レベル）の「4」を提供する (このレベルでは、以前のレベルで設定したユーザー・プロファイルからすべてのパスワードが除去)**
- パスワードポリシーに準拠する個別のパスワードを、各ユーザー・プロファイルに割り当てる

*,**詳細は下記参照

https://www.ibm.com/docs/ja/i/7.4?topic=passwords-password-rules-qpwdrules

https://www.ibm.com/docs/ja/i/7.5?topic=passwords-password-level-qpwdlvl

© IBM 2023

共通権限ユーザー・プロファイル

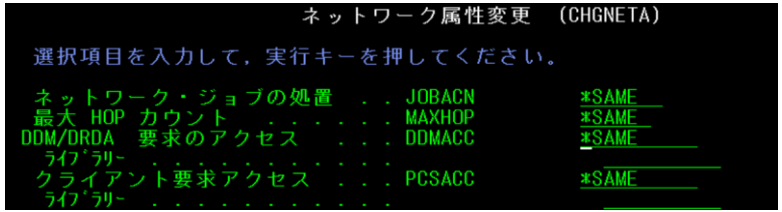
- **ユーザープロファイルの共通権限は*EXCLUDEでなければなりません**
- もし、共通権限が*USE以上の権限のユーザーは他のユーザーに乗っ取られる可能性あります。別のユーザーが、そのユーザーでジョブを投入できます。
- PRTPUBAUT OBJTYPE(*USRPRF) コマンドを使用して、*EXCLUDE **より高い共通権限を持つすべてのユーザーをリスト**する。
  - QDBSHR、QDBSHRDO 、および QTMPLPD は、より高い権限で出荷されます。
- **特定されたユーザーの(上記3つの IBM ユーザーを除く) 共通権限を*public *EXCLUDE に戻します。**
  - GRTOBJAUT OBJ(ADMIN) OBJTYPE(*USRPRF) **ユーザー**(*PUBLIC) AUT(*EXCLUDE)

```
                                  共通認可オブジェクト （ 全報告書）
5770SS1 V7R4M0 310522 I5OSP4 31.05.22 12:49:48 CEST
 オブジェクト・タイプ . . . . : *USRPRF
 指定されたライブラリー . . . : QSYS
                      ASP 認証 ----------オブジェクト-------- ------------データ----------
 ライブラリー・オブジェクト・デバイス所有者リスト権限がありません。変更要求が実行されていません。実行された読み取り追加を実行しません。
 QSYS QDBSHR *SYSBAS QSYS ユーザー定義 X X
 QSYS QDBSHRDO *SYSBAS QSYS ユーザー定義 X X
 QSYS QTMPLPD *SYSBAS QSYS ユーザー定義 X
 QSYS 管理 *SYSBAS QSECOFR *すべての X X X X X X X X X X X X X X X X X X X X X
 QSYS FTPUSER *SYSBAS 管理 *変更 X X X X X X
```

© IBM 2023

認証なしのDDM アクセス

- DDMを使用するユーザーの判別 (通常は BRMS および HA ソリューション)
  - DDMACC パラメーターは、サーバー・システムとしての IBM® iが、他のサーバーから出された DDM 要求をどのように 処理するかを制御します。
  - ネットワーク属性の DDMACCにおける 出口プログラムが役立つ



- 接続を開始するすべてのシステムで、まだリストされていないユーザーごとに、サーバー認証エントリーを、以下のように追加する
  - 例:ADDSVRAUTE USRPRF(QBRMS) SERVER (QDDMSERVER) USRID(BRMSUSER) PASSWORD('パスワード')
- すべてのユーザーを追加したら、認証を要求するように、DDM サーバーの属性を変更。 少なくとも以下を指定 する
  - CHGDDMTCPA PWDRQD(*USRENCPWD)

© IBM 2023

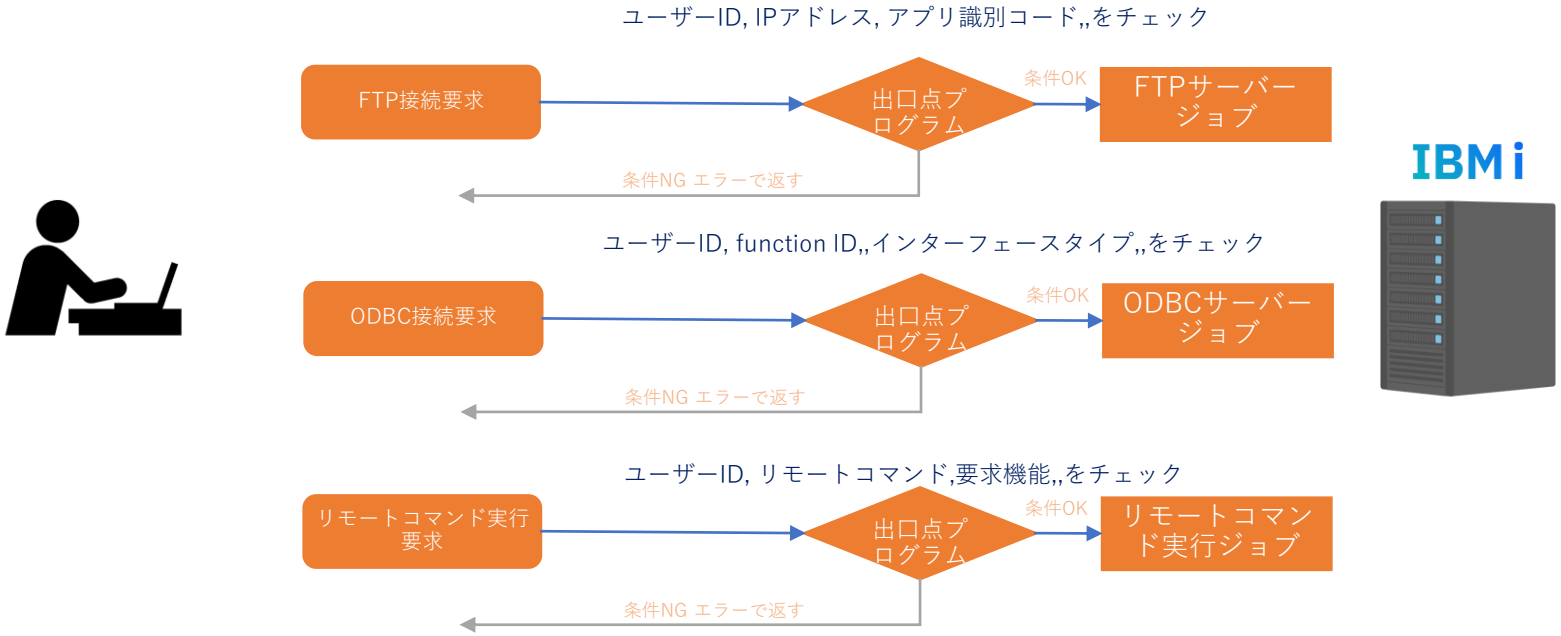
SSH アクセス

- OpenSSH デーモンは多くのシステムで稼働する
  - 主に、暗号化ファイル転送 (sftp または scp) に使用される
- このリスクは、有効なパスワードまたは構成された公開鍵認証を持つすべてのユーザーが、ssh 経由で IBM i に接続できる
  - ユーザーは PASEシェルおよび IBM i のCL コマンドを実行可能
    - ユーザー・プロファイルの機能制限は効果がない
  - ファイル転送も許可され、出口点プログラムを介して制御することは不可

© IBM 2023

(参考資料) IBM i 出口点プログラムについて(1)

- IBM i は様々な出口点を提供しており、ユーザー作成の出口点プログラムを登録してユーザーアクセスや操作を制御（制限）することができます。一例を以下に示します。



© IBM 2023

(参考資料) IBM i 出口点プログラムについて(2)

- IBM i の出口点は **WRKREGINF** コマンドで一覧表示、編集することができます。
- 以下はいくつかの出口点とセキュリティの観点での活用ユースケース例です。**出口プログラムはCLコマンドやILE C などで作成できます。**

出口点	出口点の説明	ユースケース例
QIBM_QTMF_SVR_LOGON	IBM i FTPサーバーにログオンする際に実行される	ユーザーIPアドレスによるアクセス可否、作業ディレクトリの変更等
QIBM_QTMF_SERVER_REQ QIBM_QTMF_CLIENT_REQ	FTPクライアント（サーバー）からの操作要求を検査し実行を制御する	リモートIP, 要求された操作（ディレクトリ操作、ファイル操作、CLコマンド実行等）によって操作の許可・不許可を制御
QIBM_QTG_DEVINIT	TELNET接続を行う際に実行される	TELNETの端末IDの指定、自動サインオン可否、環境オプション指定等
QIBM_QTG_DEVTERM	TELNETセッションを切断した際に実行される	TELNET接続終了時にログ出力や監査アクティビティを実行する
QIBM_QZDA_INIT	ODBCの開始要求時に実行される	ユーザーID, Function ID, インターフェースID等をチェックして実行を制御する
QIBM_QZDA_NDB1	Db2 for i のネイティブデータベース機能を要求された際に実行される	要求されたデータベース操作（PF, LF, SRCPF, SAVFの作成、変更、削除、クリア、複製等）を取得し実行を制御する
QIBM_QZRC_RMT	リモート・コマンド呼び出し要求または分散プログラム呼び出し要求の際に実行される	ユーザーID、要求された機能、要求されたプログラム名、ライブラリー名、コマンドストリング等を取得し実行を制御する
QIBM_QZSO_SIGNONSRV	IBM i サインオンサーバーに接続要求された際実行される	ユーザーID, 要求された機能を取得して実行を制御する

© IBM 2023

SSH アクセス（続き）

- SSH アクセスを制限することを推奨
- 通常、管理者またはITユーザーのみに ssh アクセスを許可
- 個々のユーザーまたはグループに対してアクセスを拒否または許可できる方法があります
- 優先順位は下記
  - DenyUsers
  - AllowUsers
  - DenyGroups
  - AllowGroups ← ベストプラクティス（推奨）
- 例: グループ sshgrp のユーザーのみが ssh を使用してログインできる必要がある場合

```
ユーザー・プロファイルの表示 - 基本
ユーザー・プロファイル . . . . . : SAWADA
グループ・プロファイル . . . . . : SSHGRP
```

/QOpenSys/QIBM/UserData/SC1/OpenSSH/SC1/OpenSSH/etc/sshd_config

```
# インストール済み。 将来的には、デフォルトで明示的なものが必要になります
# プロトコル 1 の活動化
Protocol 2
AllowGroups sshgrp
ibmpaseforienv PASE_USRGRP_LIMITED=N
```

© IBM 2

特殊権限

- 特殊権限は、ユーザーに高い特権を付与するため、特殊と呼ばれる
- IBM i の 8 つの特殊権限すべてが、多くのユーザーに割り当てられると、リスクと見なされる

  - *ALLOBJ　　：システム上のすべてのオブジェクトにアクセスする
  - *AUDIT　　：監査機能の実行
  - *IOSYSCFG：ネットワーク構成の実行 (例：TCP/IP)
  - *JOBCTL　　：　自分以外のジョブの制御
  - *SAVSYS　　：　全てのオブジェクトの保管、復元、および記憶域の解放
  - *SECADM　　：　セキュリティー管理者、ユーザー管理
  - *SERVICE　　：　システム保守ツール(STRSST)の起動など、実行サービス機能
  - *SPLCTL　　：　全てのスプール制御機能（スプールファイルの変更・削除・保留等）やすべてのジョブ待ち行列に対する制御

© IBM 2023

（ご参考）システム管理ユーザーに割り当てる特殊権限の例

システム管理に必要な機能から、ユーザーの責任範囲を決める場合に参考にしてください。

システム機能[1]	説明	必要なユーザー・クラス[2]	必要な特殊権限[3]
システム操作	印刷装置出力の管理、システム・メッセージへの応答、通常の操作の監視、処理IPLの実行	*SYSOPR	*JOBCTL
システム・ハウスキーピング	自動クリーンアップのスケジュール作成やディスク使用率の監視などシステム・クリーンアップ機能の実行	*SYSOPR	*JOBCTL
システム・バックアップ	アプリケーションおよびシステムのライブラリー、セキュリティー情報の定期的な保管	*SYSOPR	*SAVSYS
プロファイル管理	新規ユーザー・プロファイルの追加、既存プロファイルの保守	*SECADM	*SECADM
資源保護管理	システム上のオブジェクトに対する権限の保守	*SECOFR	*ALLOBJ
プログラム保守	IBM提供のライブラリーに対するPTFの適用やアプリケーション・ライブラリーの変更	*SECOFR	*ALLOBJ
セキュリティー監査	セキュリティー監査機能の設定。監査の対象となるイベント、ユーザー、およびオブジェクトの決定		*AUDIT[4]
システム構成	システムにおける装置の追加、変更および除去		*IOSYSCFG[4]

1．これらの責任を与えるユーザーには「制限機能」を*NOに設定してください
2．これは、最低限必要なユーザー・クラスを示しています。このユーザー・クラスには、機能の実行に必要なコマンドやメニュー・オプションを使用するための権限が含まれています。
3．これは、ジョブの責任を果たすために必要な特定の特殊権限を示しています。指定されているユーザー・クラスには、他の付加的な特殊権限が含まれている場合もあります。
4．これらの特殊権限には、対応するユーザークラスがありません。*SECOFRクラスにはこれらの権限はふくまれていますが、おそらく*SECOFRがもっているその他の特殊権限は必要ないでしょう。そのため、個別に担当者には特殊権限を設定することをお勧めします。

© IBM 2023

特殊権限 (続き)

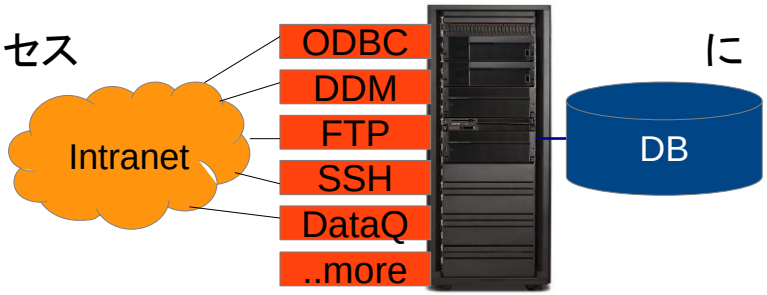
- グループ・プロファイル を介して特殊権限を付与することを推奨
- 一般的に、*SECOFR クラスの特殊権限を与えない
- 特定の特権アクションを許可するために、借用権限を持つラッパー・プログラムを使用
- 出力待ち行列の場合は 、, 任意のファイルの表示 (DSPDTA), オペレーター制御 (OPRCTL) , および検査権限 (AUTCHK) パラメーターを、出力待ち行列オブジェクト許可と組み合わせて 、グループユーザーへのアクセス権を付与する
- *例:グループのメンバーであるユーザーは、出力待ち行列内のすべてのスプール・ファイルを表示、コピー 、および制御することができる。（下記設定）*

オブジェクト	パラメーター/権限	値
出力待ち行列 (OUTQ)	*Public 権限	*EXCLUDE
出力待ち行列 (OUTQ)	ユーザー / グループ権限	* CHANGE
出力待ち行列 (OUTQ)	データの表示 (DSPDTA)	*YES
出力待ち行列 (OUTQ)	オペレーター制御 (OPRCTL)	*YES
出力待ち行列 (OUTQ)	権限検査 (AUTCHK)	* DTAAUT

© IBM 2023

共通オブジェクト権限

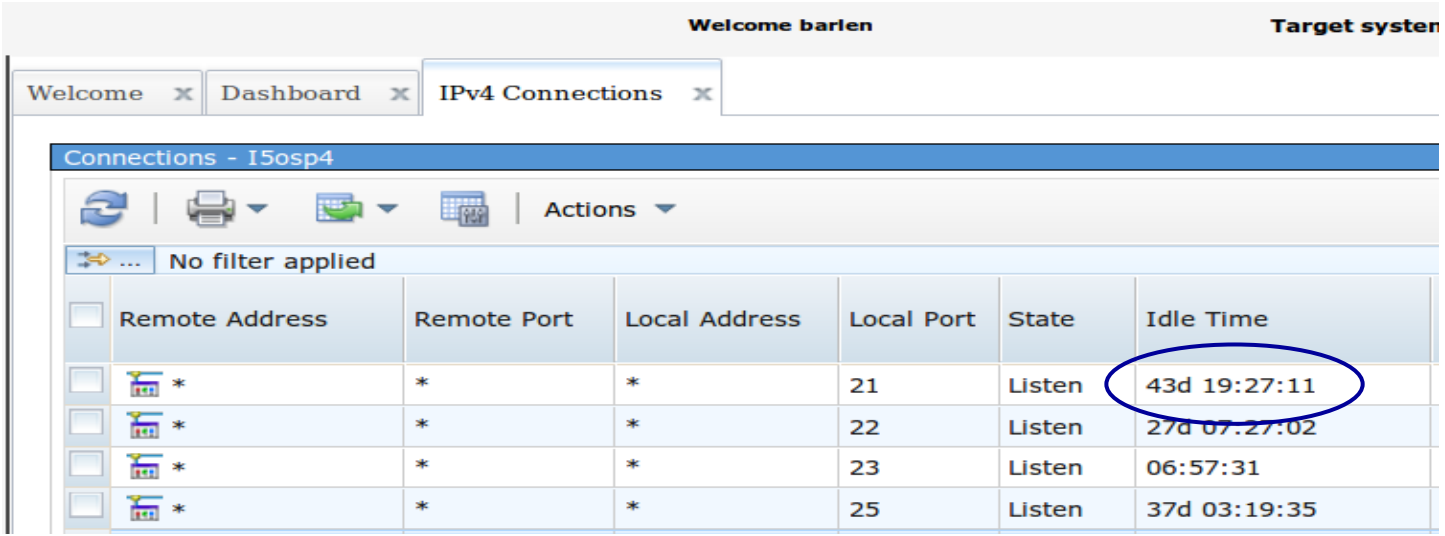
- プログラム (*PGM), モジュール (*MODULE), コマンド (*CMD) などのすべての実行可能コードには
  共通オブジェクト権限： *USE が必要
  - 本番システム上の実行コードには、*public *USE 以外のものを使わないようにすべき
- ライブラリーは、*USE より高い共通権限を持つべきではない
- IFS ディレクトリーには、最大で、public *RX にすべき
- もし、アプリケーションが、借用権限およびオブジェクトへのpublicアクセスを使用するように作成されていない場合 (例えば、データベースが、*USE またはそれ以上の権限を付与されている (*CHANGE または *ALL) 場合には、出口点プログラムを使用してネットワークを介したアクセスを厳密に制御する必要がある
- IBM i 7.3では、権限収集機能を使用して、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の実行がさらに容易になります。



© IBM 2023

未使用または、不適切に構成されたネットワーク・サービス

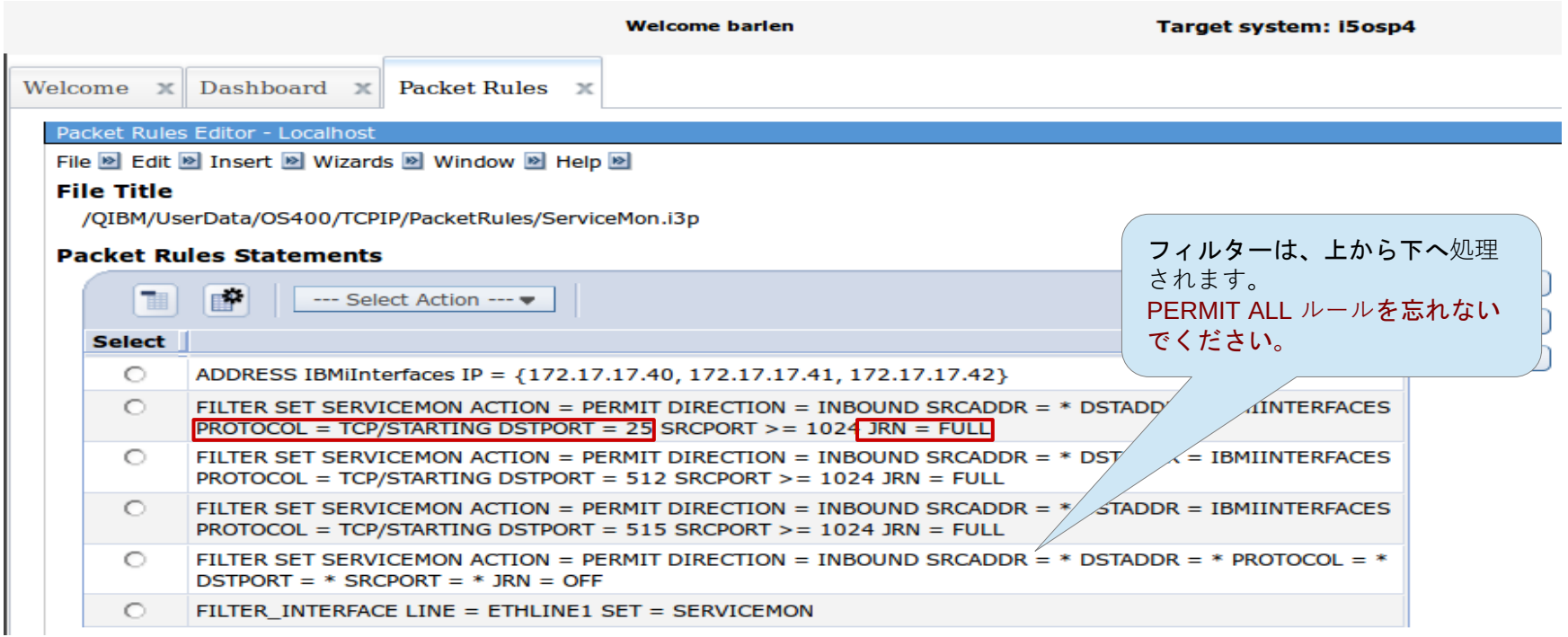
- 使用されていないすべてのネットワーク・サービスは、DoS攻撃の、潜在的な候補となる
- NETSTAT *CNN コマンドでの表示、または同等のNavigator for iインターフェースのアイドル時間タイマーを使用して、LPD や REXEC などのネットワーク・サービスが、使用されているかどうかを判別
  - 最後の IPL 以降にサービスが使用されていない場合は、サービスを停止する



© IBM 2023

未使用または、不適切に構成されたネットワーク・サービス（続き）

- IP パケットフィルタリングは、ネットワーク・サービスがまだ使用されているかどうかを判断するのに適している



© IBM 2023

未使用または、不適切に構成されたネットワーク・サービス（続き）

- QIPFILTER ジャーナルを使用する

```
CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE)
    TOLIB(BARLEN) NEWOBJ(IPFILT)

DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF))
    OUTPUT(*OUTFILE)OUTFILFMT(*TYPE4)
    OUTFILE(BARLEN/IPFILT) ENTDTALEN(*VARLEN *CALC)
```

- 出力ファイルの照会
  - 下記の例は、監視対象のポート 25のみを示しています。

```
LINE        FILTER ACTION  SOURCE          SOURCE  DESTINATIO      DESTINATIO
                           V4 ADDRESS      PORT    V4 ADDRESS      PORT
ETHLINE1       PERMIT      172.17.17.31    16343   172.17.17.40         25
ETHLINE1       PERMIT      172.17.8.149    41766   172.17.17.40         25
```

- 長時間にわたってモニターされ、ポートが使用されていない場合は、IT を停止して自動開始を *NO に変更する

© IBM 2023

未使用または、不適切に構成されたネットワーク・サービス（続き）

- NetServer は ランサムウェア攻撃の主要なエントリー・ポイントになる
  - 多くの場合、共用は読み取り/書き込みモード (*RW) で作成される
  - 共用ディレクトリーおよびファイルに対する共通権限は *RWX
  - IFS ルートが共有される
- **推奨事項**
  - **ダウンロードまたは読み取り専用コンテンツの場合、*R (読み取り専用) モードでのみ共有を作成する**
  - **共有コンテンツに対して、Public *W アクセス権を付与しない**
  - **IFS ルート・ディレクトリーを共有しない**
  - **アンチウィルス製品のインストールを検討する**
  - **IBM i 7.5の場合: 権限リストを使用して、NetServer へのアクセスを制限する。**

© IBM 2023

未使用または、不適切に構成されたネットワーク・サービス（続き）

- デフォルト構成もリスクを引き起こす可能性がある
- 例 → シンプル・ネットワーク管理プロトコル (SNMP)
  - デフォルト構成で開始すると、誰でも下記を取得できる …

```
barlen@ubuntu1:~$ snmpwalk -v 1 -c public 172.17.17.40
iso.3.6.1.2.1.1.1.0 = STRING: "IBM OS/400 V7R3M0"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.2.6.11
iso.3.6.1.2.1.1.3.0 = Timeticks: (264462635) 30 days, 14:37:06.35
iso.3.6.1.2.1.1.5.0 = STRING: "i5osp4.ai.stgt.spc.ihost.com"
iso.3.6.1.2.1.4.20.1.1.127.0.0.1 = IpAddress: 127.0.0.1
iso.3.6.1.2.1.4.20.1.1.172.17.17.6 = IpAddress: 172.17.17.6
iso.3.6.1.2.1.4.20.1.1.172.17.17.8 = IpAddress: 172.17.17.8
iso.3.6.1.2.1.4.20.1.1.172.17.17.40 = IpAddress: 172.17.17.40
iso.3.6.1.2.1.4.20.1.1.172.17.17.41 = IpAddress: 172.17.17.41
iso.3.6.1.2.1.4.20.1.1.172.17.17.42 = IpAddress: 172.17.17.42
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.21.0.0.0.0.0 = INTEGER: 21
iso.3.6.1.2.1.6.13.1.3.0.0.0.0.22.0.0.0.0.0 = INTEGER: 22
```

システムの情報

既存の全てのIPｲﾝﾀｰﾌｪｲｽ

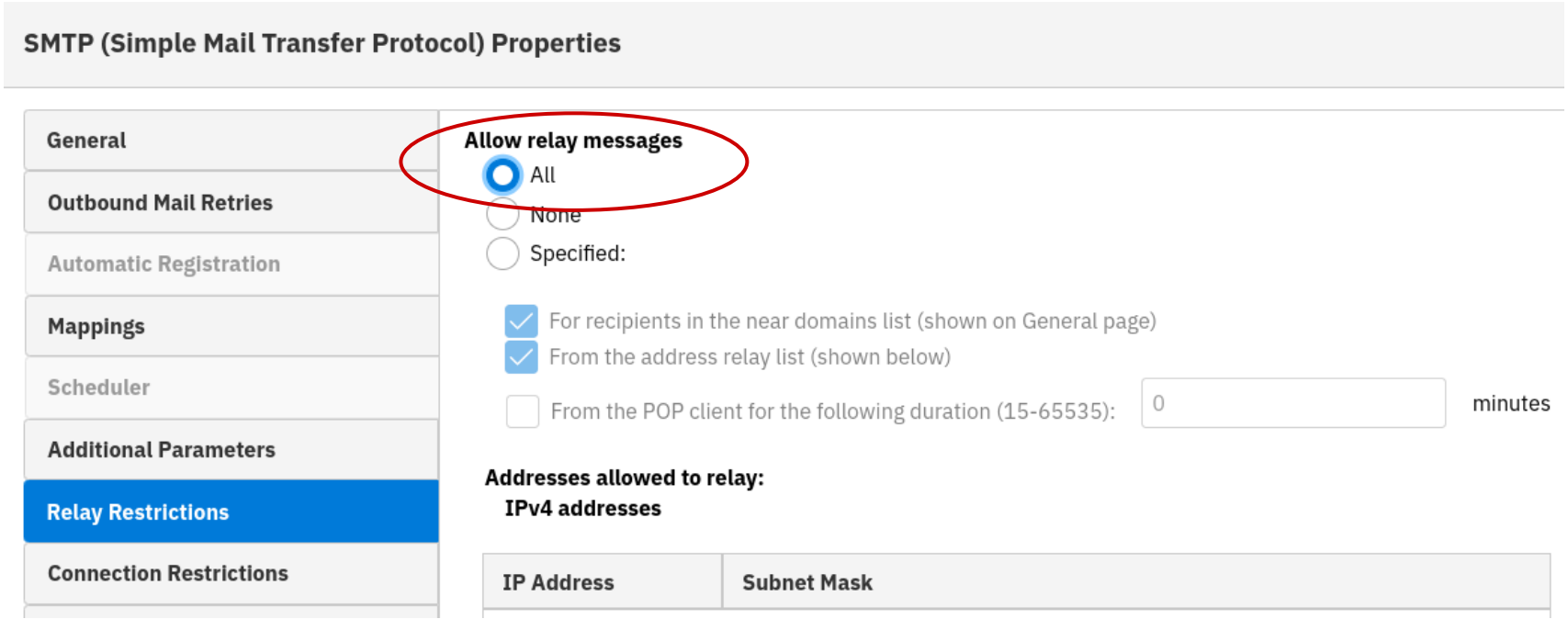
全ての開きポート番号

インストールされているハードウェア、ファイル システム名、
インストールされているライセンス プログラムなどを含む 2800 を超えるエントリが返された

© IBM 2023

未使用または、不適切に構成されたネットワーク・サービス（続き）

- 例 → シンプル・メール転送プロトコル (SMTP)
  - デフォルトでは、オープン・メール・リレー → 迷惑メールとして機能してしまう



© IBM 2023

無制限のリモート・データベース・アクセス

- ほとんどすべての企業が、本番データベースへの ODBC/JDBC アクセスを許可している
  - 多くの場合、*CHANGE または *ALL のデータ・アクセスを許可している
- ここでのリスクは、業務アプリケーション以外でのデータの盗難およびデータ操作
- リモート・アクセスを制限するオプションが使用可能

1

システム機能 (WRKFCNUSG) を使用して、ユーザーまたはグループに
ODBC/JDBC または DDM/DRDA アクセスを認可する
- QIBM_DB_DDMDRDA - DDM および DRDA アプリケーション・サーバー・アクセス
- QIBM_DB_ZDA - ODBC/JDBC Toolbox アプリケーション・サーバー・アクセス

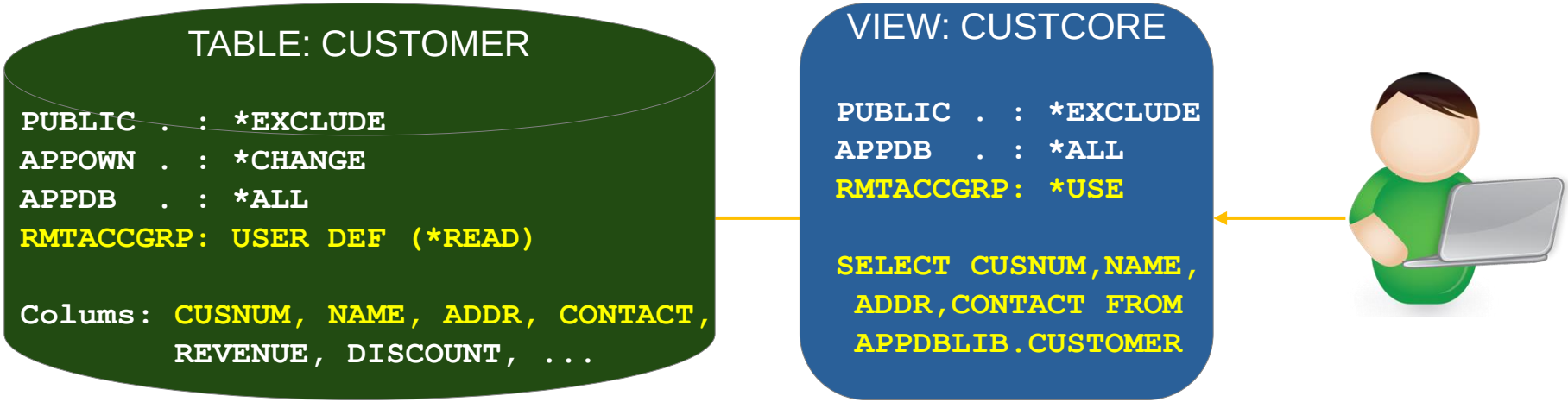
```
機能使用の表示
 機能 ID . . . . : QIBM_DB_ZDA
 関数名 . . . . : ツールボックス・アプリケーション・サーバー・アクセス
 説明 . . . . : ツールボックス・アプリケーション・サーバー・アクセスの保護をサポートします
 プロダクト . . . . . : QIBM_BASE_OPERATING_SYSTEM
 グループ . . . . . : QIBM_DB
 省略時の権限 . . . . . : *拒否
 *ALLOBJ 特殊権限 . . . . . : *ノット
 ユーザー・タイプ使用ユーザー・タイプ使用量
GRPODBC ユーザー  *ALLOWED
```

© IBM 2023

無制限のリモート・データベース・アクセス（続き）

2

VIEWS を使用してグループ経由で、ユーザーに読み取りアクセス権限のみを提供
- 表全体ではなく、特定の列へのアクセスのみを提供
- QIBM_DB_ZDA - ODBC/JDBC Toolbox アプリケーション・サーバー・アクセス



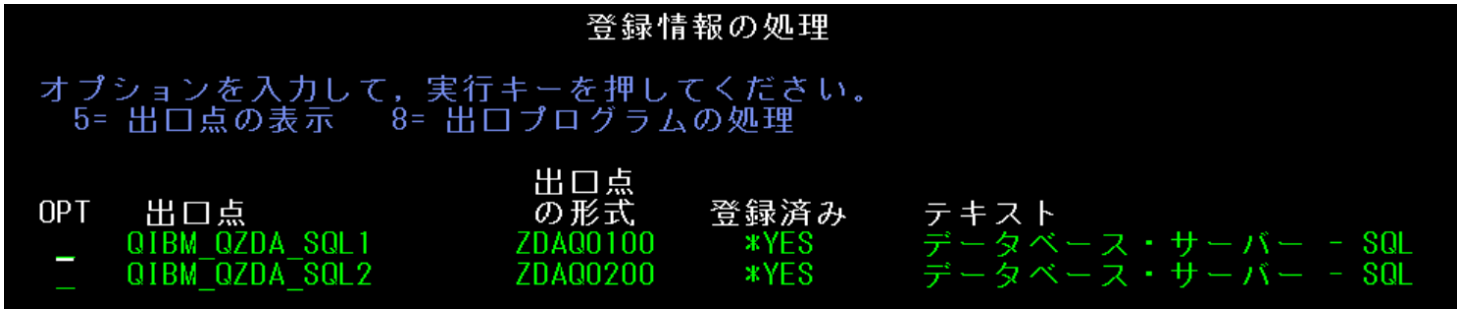
© IBM 2023

無制限のリモート・データベース・アクセス（続き）

3

前の**オプション**では**十分でない**場合、又は、**より詳細な制御が必要な場合は、出口プログラムを使用してアクセスを制御**、及び**制限する**

- ログ**の目的でも使用できます (つまり**、どの誰がどの**ファイルにアクセスしたか)**
- **出口プログラムは**自分で作成するか、**サード・パーティー・ベンダーから購入する**



© IBM 2023

データへのアクセスを制限

- データは最も価値ある資産であり、適切に保護される必要があります。
- IBM i は、データを保護するため、さまざまなオプションを提供

  - 行および列のアクセス制御 (RCAC: Row and Column Access Control)　IBM i 7.2～
  - データベース暗号化
    - 業務アプリケーション内で、暗号化を実装できる→
      ただし、アプリケーション・コードの変更が必要
    - フィールド・プロシージャーを使用してデータベースに暗号化を実装することできる→
      アプリケーションに対して透過的

© IBM 2023

データへのアクセスを制限 - RCAC

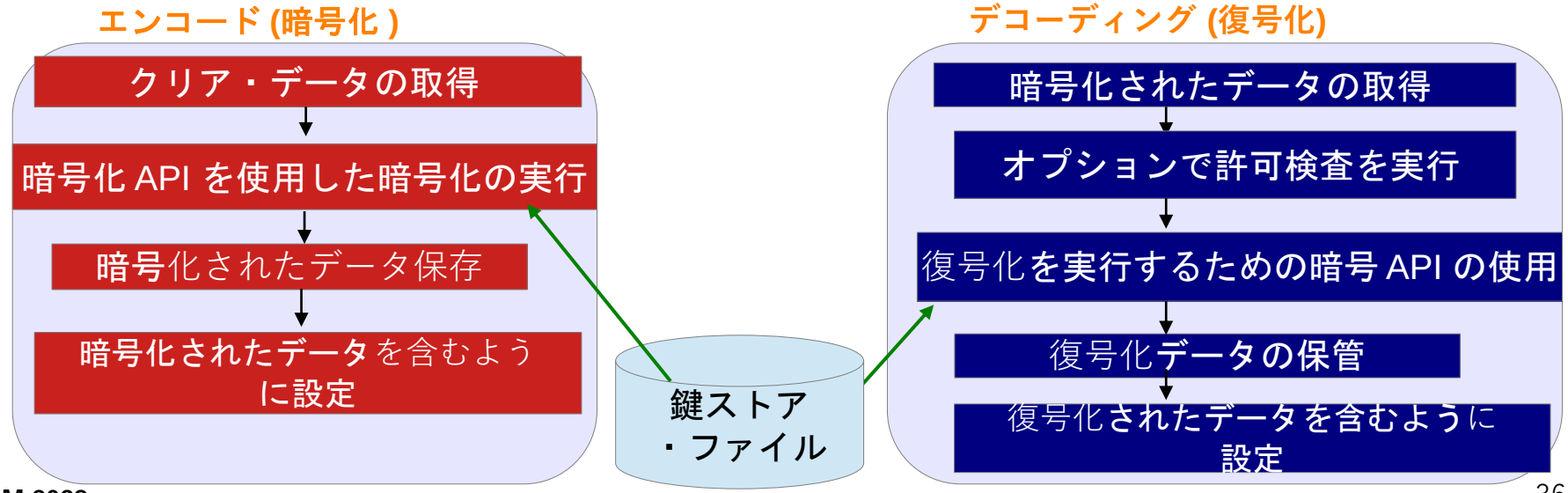
- 行アクセス
  - ユーザーがアクセス権限を持つ行のみを返す
- 列アクセス
  - ユーザーがアクセス権限を持たないデータをマスクする
- *ALLOBJ ユーザーなどの高水準の特権ユーザーも、これらの規則から除外されません
- データベース・エンジンによる強制

Custno	Name	City	Country	Revenue
33123	Star hotels	Mainz	DE	*******
44541	Super hotels	Athens	GR	*******
45211	Bakery No 1	London	GB	32223.33
66541	Golden Pub	Manchester	GB	787611.32

© IBM 2023

データへのアクセスを制限 —フィールド・プロシージャーによるデータ暗号化

- DB2 列レベル (フィールド・レベル)の 出口点サポート
- 列の挿入 / 更新 / 読み取り時に呼び出される出口点プログラム (フィールド・プロシージャー)
  - 「トリガー」に似ていますが、暗号化を有効にするための追加サポート
- 暗号化/複号化は、選択した暗号化API を使用して実装する必要がある
- 列毎に、1 つの出口点



© IBM 2023

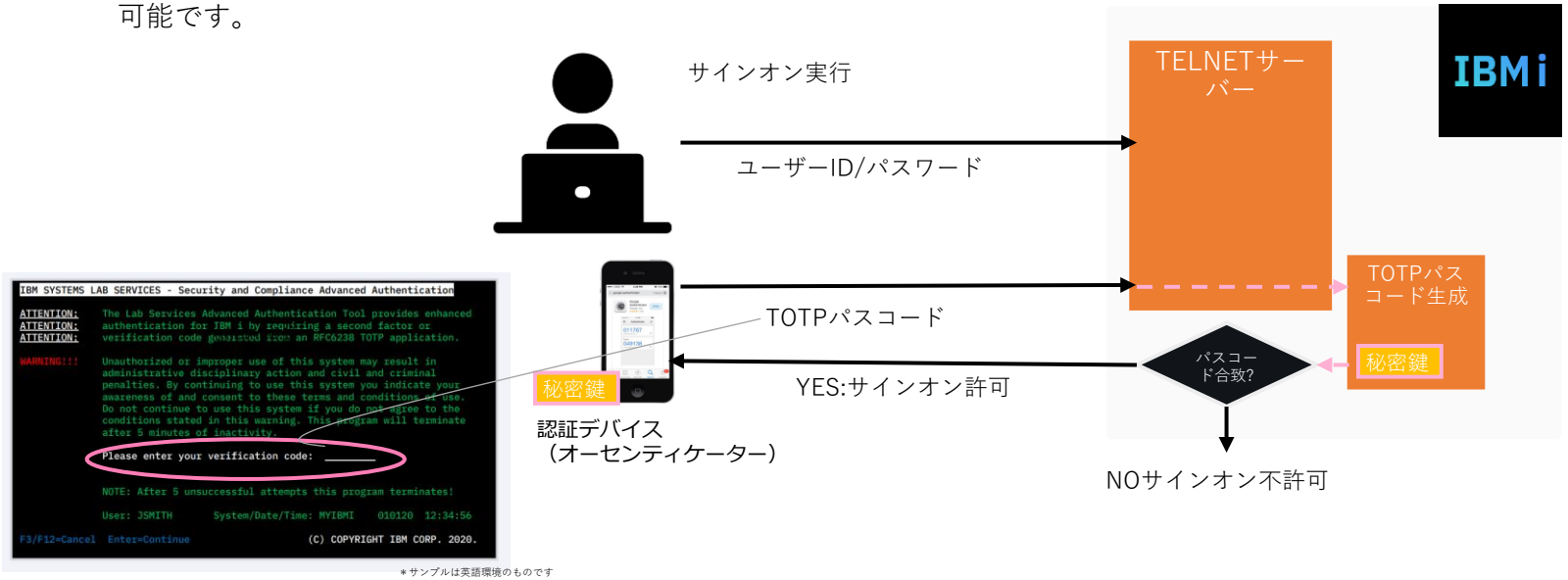
セキュリティ・ポリシーは不可欠

- 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る
  - 将来の参照用
  - なにが行われたのか、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です。

© IBM 2023

3. Security & Compliance tools for iによるIBM i MFA（多要素認証）

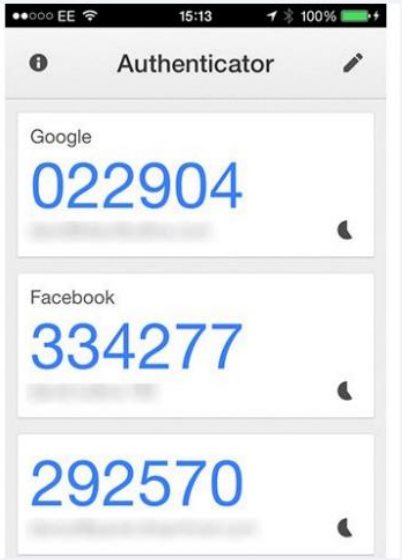
- **ユーザーID/パスワードが盗まれた場合の、不正アクセス対策には多要素認証による防御により、リスクを低減できます。**
- 5250アプリケーション実行時に、IBM i ユーザープロフィールによるサインオンに加え、パスコードによる認証方式を組合わせた多要素認証（二要素認証）を実装することが可能です。
- 追加の認証方式は**RFC6238(TOTP: Time-Based One-Time Passwordアルゴリズム)**で定義されたパスコードをIBM i とユーザー側認証デバイス（オーセンティケーター）で生成し認証を行う方式です。
- RFC6238対応のオーセンティケーターは様々な種類があり、ユーザーが使用する認証デバイスは柔軟に選択可能です。
- このPower SC toolによる多要素認証はインターネットはじめ外部ネットワークと接続する必要なしに多要素認証を実現します。
- IBM Power（AIX,Linux含む）がサポートするPower SCは当ページの説明とは別個のMFA技術でウェブベースでの多要素認証が可能です。



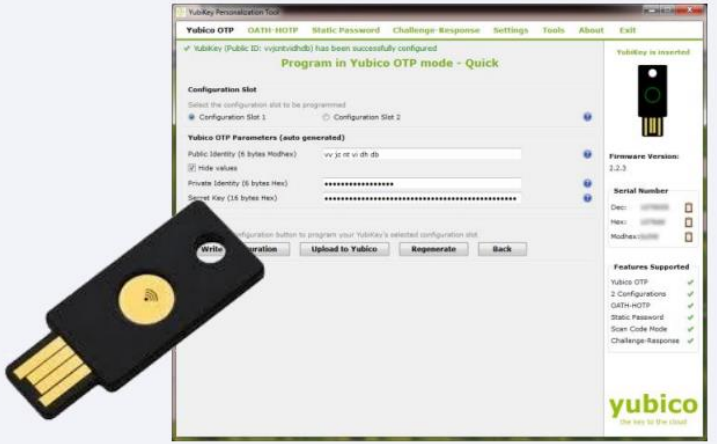
＊サンプルは英語環境のものです

© IBM 2023

RFC6238オーセンティケーターの例



AUTHY



© IBM 2023

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。**

  -> 当資料で解説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みます。

- **また、以下の考慮点もあわせてご検討ください**

  - 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
  - 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 テクノロジー・サービスなど社外セキュリティ評価による可視化を推奨いたします。

© IBM 2023

IBM i 情報

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

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

IBM i World 2021 オンデマンド・セミナー
https://ibm.biz/iworld2021

IBM i ホワイトペーパー 2021年日本語版
https://www.ibm.com/downloads/cas/JB8AXO9V

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

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

IBM i 情報 Facebook
https://www.facebook.com/iusersjapan

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

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 7.4 技術資料
https://www.ibm.com/docs/ja/i/7.4

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 2023

© IBM 2023

ワークショップ、セッション、および資料は、IBMによって準備され、IBM独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる読者に対しても法律的またはその他の指導や助言を意図したものではなく、またそのような結果を生むものでもありません。本資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、IBMは責任を負わないものとします。 本資料に含まれている内容は、IBMまたはそのサプライヤーやライセンス交付者からいかなる保証または表明を引きだすことを意図したものでも、IBMソフトウェアの使用を規定する適用ライセンス契約の条項を変更することを意図したものでもなく、またそのような結果を生むものでもありません。
本資料でIBM製品、プログラム、またはサービスに言及していても、IBMが営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本資料で言及している製品リリース日付や製品機能は、市場機会またはその他の要因に基づいてIBM独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来の製品または機能が使用可能になると確約することを意図したものではありません。本資料に含まれている内容は、読者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したものでも、またそのような結果を生むものでもありません。パフォーマンスは、管理された環境において標準的なIBMベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。
記述されているすべてのお客様事例は、それらのお客様がどのようにIBM製品を使用したか、またそれらのお客様が達成した結果の実例として示されたものです。実際の環境コストおよびパフォーマンス特性は、お客様ごとに異なる場合があります。
IBM、IBM ロゴ、ibm.com、Db2、Rational、Power、POWER8、 POWER9、AIXは、世界の多くの国で登録されたInternational Business Machines Corporationの商標です。
他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。
現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml をご覧ください。

インテル, Intel, Intelロゴ, Intel Inside, Intel Insideロゴ, Centrino, Intel Centrinoロゴ, Celeron, Xeon, Intel SpeedStep, Itanium, およびPentium は Intel Corporationまたは子会社の米国およびその他の国における商標または登録商標です。
Linuxは、Linus Torvaldsの米国およびその他の国における登録商標です。
Microsoft, Windows, Windows NT および Windowsロゴは Microsoft Corporationの米国およびその他の国における商標です。
ITILはAXELOS Limitedの登録商標です。
UNIXはThe Open Groupの米国およびその他の国における登録商標です。
JavaおよびすべてのJava関連の商標およびロゴは Oracleやその関連会社の米国およびその他の国における商標または登録商標です。

© IBM 2023