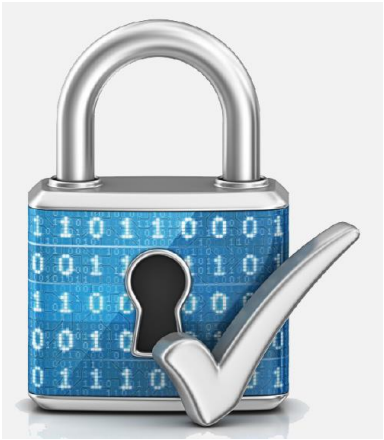
IBM i 2025

IBM i コンテンツ (2025年2月版)

IBM PowerSCを用いたIBM i セキュリティ強化のご紹介



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 PowerSCを用いたIBM i セキュリティ強化のご紹介

IBM PowerSCは、IBM i またはAIX/Linuxが稼働しているIBM Powerサーバー上の仮想化環境向けに最適化された、セキュリティーとコンプライアンスのソリューションです。（別途有償のソフトウェア製品になります）

昨年末に、最新のIBM PowerSC (v2.2.0.4) が出荷され、これまで、管理用にAIX/Linuxサーバーが必要であったものが、IBM i だけで、管理用のサーバーとクライアントの兼用が可能になりました。

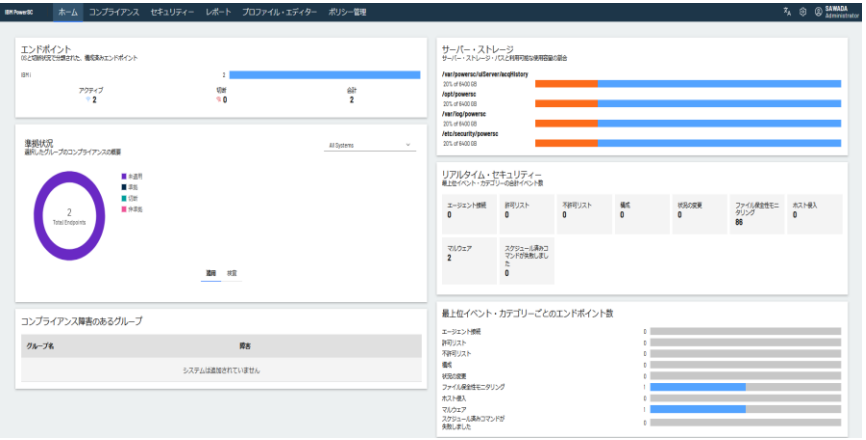
PowerSCには、多くのセキュティ関連の機能がありますが、IBM i のお客様にぜひ活用いただきたい「自動コンプライアンス」、「アンチウイルス(マルウェアの検出）」、「多要素認証」の３つの機能に絞ってご紹介します。

目次

1. PowerSCとは

（1）IBM Powerのセキュリティ管理ツール ~IBM PowerSCとは

Web UIによるセキュリティーの一元管理



- GUIでセキュリティー設定を一元管理
- システム全体のセキュリティー・イベントを表示
- イベントの分析レポートも出力可能

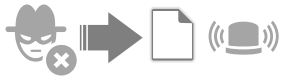
セキュリティー管理の簡素化・機能の強化

セキュリティー設定の モニタリングを簡素化

コンプライアンス違反を検出

パッチレベル違反を検知

不正アクセスの 検知機能を強化



ファイル改竄検知

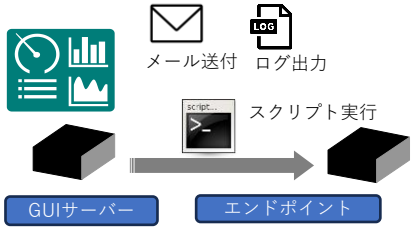
ウィルス・マルウェアを検出

アクセス制御機能の 強化・一元管理

マルウェアからシステムを防御

多要素認証で不正アクセス防止

セキュリティイベント 発生時の応答の強化



イベント発生時の応答を一元管理・自動化

解説：

・IBM PowerSC は、IBM i、AIX、Linux を実行する IBM Power サーバー上のOS環境向けに最適化されたセキュリティおよびコンプライアンス・ソリューションです。PowerSCは、Webベースのユーザー・インターフェースを提供し、OSのセキュリティとコンプライアンス機能を補完し、一元管理します。

・コンプライアンスという観点では、主に規制業界向けにあらかじめ構築された**コンプライアンス・プロファイル**を提供することです。顧客はカスタムプロファイルを作成できるため、事前に構築されたプロファイルからルールを引き出して、自社の環境に合わせてカスタマイズしたプロファイルを作成することができます。

・不正アクセスの検知の観点から、そのシステムを安全に保ち、リアルタイムで監視し、セキュリティを維持するためにさまざまな機能が利用できます。機能には以下のようなものがあります：
ファイル整合性監視は、監視対象ファイルのコンテンツやパーミッションが変更された場合にそれを認識し警告する。
アプリケーションコントロールは、PowerSC のマルウェア対策機能であるカーネルベースの「許可リスト」アプローチです。
ブロック・リスティングは、ハッシュ検索を使用してファイル・レベルで一連のウイルス・シグネチャを検索する脅威ハンティング機能です。その中には、トロイの木馬、ウイルス、マルウェア、その他の悪意のある脅威を検出するためのオープンソースの**ウイルス対策エンジンである ClamAV のマルウェア対策**が含まれています。

・アクセス制御機能の観点からは、**多要素認証**が利用できます。名前が示すように、多要素認証はユーザーを識別する２つ以上の要素を活用します。今、多要素認証は、大変注目されています。その理由は、不正やなりすましを防ぐ手段として、従来のパスワード認証よりも優れているからです。

1. PowerSCとは

（2）PowerSCフィーチャーの、OS毎に使える機能

機能	対応しているOS
コンプライアンスの自動化	✓ AIX, Linux, IBM i
コンプライアンス・レポート機能 (タイムラインを含む)	✓ AIX, Linux, IBM i
ファイル整合性監視	✓ AIX, Linux, IBM i
許可リスト / アプリケーションの制御	✓ AIX & Linux
ブロックリスト/脅威ハンティング (ハッシュ検索)	✓ AIX, Linux, IBM i
マルウェア対策 (ウイルスDB)	✓ AIX, Linux, IBM i
IBMセーフガードコピーとの統合	✓ AIX, Linux, IBM i
パッチ管理	✓ AIX, Linux, IBM i
エンドポイント検知とレスポンス (EDR)	✓ AIX, Linux, IBM i
侵入検知システム & 防御 / ファイアウォール (EDR)	✓ AIX & Linux
ログ検査と分析 (EDR)	✓ AIX, Linux, IBM i
異常検知、相関、インシデント・レスポンス (EDR)	✓ AIX, Linux, IBM i
レスポンス／アクション・トリガー (EDR)	✓ AIX, Linux, IBM i
イベント・コンテキストとフィルタリング (EDR)	✓ AIX, Linux, IBM i
多要素認証 (MFA)	✓ AIX, Linux, IBM i

解説：

・IBM PowerSC は、AIX、IBM i、Linux を実行する IBM Power サーバー上の仮想化環境向けに最適化されたセキュリティおよびコンプライアンス・ソリューションですが、OS毎に使用できる機能に制限があります。AIXとLinuxについては全機能を使用することができますが、IBM i をPowerSCクライアント（エンドポイント）にする場合は、

ー許可リスト・アプリケーション制御
ー侵入検知システム・防御・ファイヤーウォール

の２つの機能は、現時点（2025/02のPowerSC v2.2.0.4)では使用することができません。

・ただし、アプリケーション制御（ファイルごとのアクセス権の制御）や、侵入検知や防御についてもIBM iの標準機能で利用できます。
(詳しくは下記を参照してください)
https://www.jbcc.co.jp/products/files/ibmpowercolumn_202409.pdf

・それぞれのPowerSCの機能の概要については下記を参照してください。
https://www.ibm.com/docs/ja/powersc-standard/2.2?topic=concepts

1. PowerSCとは

（3）PowerSCで活用したいIBM iユーザー向けの機能

多くのお客様が心配されている以下のようなリスクに対してPowerSCは威力を発揮します。

リスク	PowerSCの機能
自社のセキュリティー・ルールがIBM i 区画で実施されてるのかわからない！	• **コンプライアンスポリシーのチェックと適用** • インタラクティブタイムラインレポート • パッチ管理 • セキュリティ/コンプライアンス・ダッシュボードでのわかりやすい状況表示
ランサムウエアでデータを失ったり、 不正なアプリケーションで被害を受けるかも？	• Endpoint Detection and Response (EDR) • **アンチウイルス機能(マルウェアの検出)** • ファイル・インテグリティ・モニタリング
ユーザーID/パスワードの流出で、 **不正アクセス**があるかも	• **MFA(多要素認証)のサポート**

解説：

・PowerSCでは、IBM iの標準機能にない、様々なメリットをもたらします。特に、お客様で
不安に思われている、下記の3点について、この資料で解説していきます。

1．自社のセキュリティー・ルールがすべてのIBM i 区画で適用されているかわからない、
というお客様のために、セキュリティの設定が自社のコンプライアンスにあっているかどうか
を自動的に点検する機能があります。IBM i のお客様向けには、IBMiベストプラクティスという
セキュリティ・プロファイルテンプレートが用意されています。

2．ランサムウェア対応は、全てのお客様に求められています。IBM iでは、ライブラリー・オブジェクトが
感染することはないですが、IFSを社内に公開している場合には、マルウェアの保菌者になる可能性が
あります。PowerSCには、このマルウェアを検出する機能を利用できます。

3．正規のユーザーID/パスワードが、流出する事案が増えています。
正規のパスワード流出した際にも安心・安全な、多要素認証の機能を使用できます。

2. 自動コンプライアンス機能

（1）自動コンプライアンス機能とは

- ✓ 業界標準の規制遵守のためには、システムのセキュリティを統一的に設定する必要がある。特定の規格を理解し、適用するのは面倒で、時間がかかり、ミスを犯しやすい。

- ✓ PowerSCの「自動コンプライアンス機能」は、業界標準をサポートするためにあらかじめ設定されたコンプライス・プロファイルを提供し、これを適用して、自動的に検査する機能を提供する（次ページにOSごとに適用できるプロファイル一覧）

- ✓ OS毎に提供されているコンプライアンス・プロファイルに準拠しているか「**シミュレート**」して、自社のOSセキュリティ設定が、それに準拠しているか確認できます。また、強制的にセキュリティ設定を適用して、業界標準のコンプライアンス基準に準拠するように変更することもできます。定期的にコンプライアンス状況を**検査**することで、基準を満たさない設定に変更された時に、アラートを上げることができます。コンプライス・プロファイルは、自社コンプライアンスに合わせて**カスタマイズ**することもできます。

2. 自動コンプライアンス機能

（2）提供されているコンプライアンス・プロファイル

PowerSCは、以下の規格について、セキュリティーおよびコンプライアンス構成の設定のシミュレート、適用、検査を自動化します。OS毎に用意されています。

AIX プロファイル

GDPR

PCI

CIS

HIPAA

NERC

DoD STIG

SAP Hardening

Oracle Systems Hardening

コンプライアンス

Linux プロファイル

GDPR

PCI

SAP Hardening

CIS

HMC Hardening

IBM i プロファイル

IBM i ベストプラクティス

CIS

解説：

・PowerSC 製品には、OS毎に、組み込みプロファイルが付属しています。これらのプロファイルを使用して、各エンドポイントがセキュリティー標準を満たすようにシステム・エンドポイントを構成することができます。

-Payment Card Industry - Data Security Standard (PCI-DSS) への準拠
-Payment Card Industry-Data Security Standard Compliance (PCI) for Linux®
-Sarbanes-Oxley 法令および COBIT への準拠 (SOX-COBIT)
-米国国防総省 (DoD) STIG への準拠
-医療保険の積算と責任に関する法律 (HIPAA) (Health Insurance Portability and Accountability Act (HIPAA))
-北米電力信頼度協議会 (NERC) への準拠
-一般データ保護規則 (GDPR) への準拠
-一般データ保護規則 (GDPR) への準拠 (Linux)
-AIX® の SAP コンプライアンス・プロファイル
-Linux の SAP HANA 準拠
-AIX および Linuxの Internet Security ベンチマーク・コンプライアンスのセンター。
-Center for Internet Security IBM® i ベンチマーク
-IBM i のベスト・プラクティス

それぞれの組み込みプロファイルには、セキュリティー要件を満たすために、エンドポイントに適用される必要があるルールが入っています。 これらのルールの一部のみまたは別の組み合わせを適用するか、またはコンプライアンス・レベルをカスタマイズする必要がある場合、カスタム・プロファイルを作成できます。ほとんどの環境で、問題となっているルールを除去するために、管理者はコンプライアンス・ファイルを頻繁に編集します。 互換性チェックが完了した後、コンプライアンス・ルール・ファイルは安定したものと見なされ、実動サーバーにデプロイされます。

2. 自動コンプライアンス機能

（3）IBM iで提供されているベスト・プラクティス

IBM iのシステムを保護するためのコンプライアンス・プロファイルとして
「IBM iベスト・プラクティス」が提供されます。設定値はマニュアルに記載されています。
https://www.ibm.com/docs/ja/powersc-standard/2.2?topic=concepts-i-best-practices

解説：

・IBM i用に提供されている、コンプライアンス・プロファイルは、「IBM i ベスト・プラクティス」と「CIS」のみです。IBM i ベスト・プラクティス」については、マニュアルに全設定値をみることができます。この値を参考にしてOS設定をするとより強固なセキュリティ設定になります。

・Center for Internet Security (CIS) は、ターゲットシステムの安全な設定のためのベンチマークを開発しています。 CIS ベンチマークは、政府、企業、産業界、および学界によって開発され、受け入れられている、コンセンサスに基づくベストプラクティスのセキュリティ構成ガイドです。詳しくは下記URLを参照してください。https://www.ibm.com/jp-ja/topics/cis-benchmarks

・IBM i 用の「CIS」は、バージョン毎に設定されていて、IBM i 7.4と7.5のコンプライアンス・プロファイルが用意されています。それぞれの設定値は、下記マニュアルに掲載されています。

-IBM i 7.4
https://www.ibm.com/docs/ja/powersc-standard/2.2?topic=concepts-center-internet-security-i-v7r4m0-benchmark
-IBM i 7.5
https://www.ibm.com/docs/ja/powersc-standard/2.2?topic=concepts-center-internet-security-i-v7r5m0-benchmark

2. 自動コンプライアンス機能

（4）IBM iで提供されているベスト・プラクティスを使った「シミュレート」機能を使ってみよう

①PowerSCのメインメニューから、「コンプライアンス」を選択すると、下記のように登録されたIBM i 区画が表示されます。

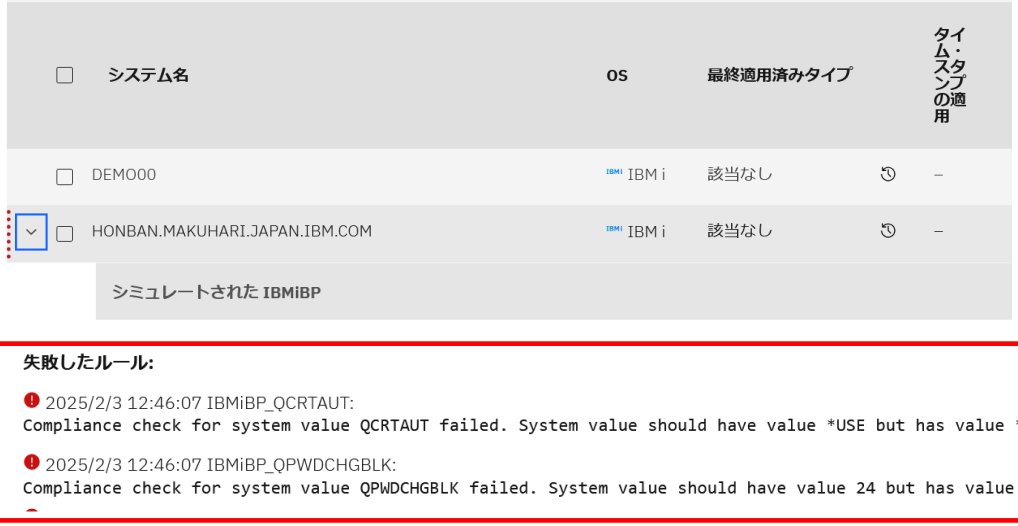
②IBM i 区画を選択すると、下記のように「適用」「シミュレート」「検査」などのメニューが表示されます。

2. 自動コンプライアンス機能

（4）IBM iで提供されているベスト・プラクティスを使った「シミュレート」機能を使ってみよう

③ここで「シミュレート」を選択すると下記のように利用できるコンプライス・プロファイルが表示されます。(IBM iの場合は下記の３つ)
一番上の「IBMi_best_practices」を選択し、「はい」を選択します。

④しばらく待つと、シミュレート結果が、下部に、「失敗したルール」「合格したルール」などと表示されます。ここで、どの部分がルールに適していないかを確認できます。



2. 自動コンプライアンス機能

（4）IBM iで提供されているベスト・プラクティスを使った「シミュレート」機能を使ってみよう

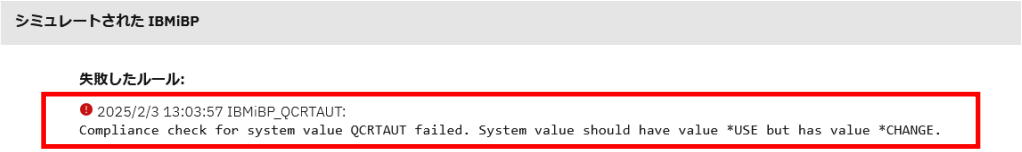
⑤最初のメニューで「レポート」を選択すると下記のように先ほど実行したコンプラインスの「シミュレート」結果の詳細レポートが表示できます。

⑥イベント・タイプで、[Check]を選択すると「合格数」「不合格数」の集計値が表示できます。ここでは、合格数17、不合格数19でした。

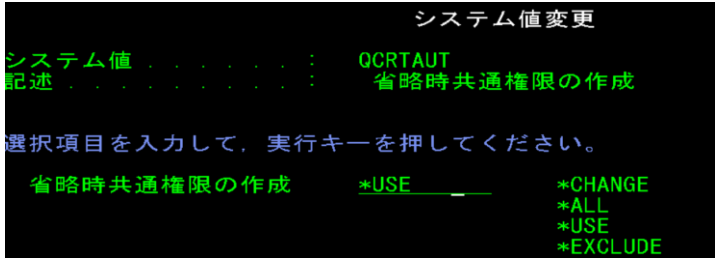
2. 自動コンプライアンス機能

（4）IBM iで提供されているベスト・プラクティスを使った「シミュレート」 機能を使ってみよう。

⑦失敗したルールの一番上に、システム値「QCRTAUT」の値が*CHANGEになっているので、ここは*USEにすべきと指示がありました。



⑧システムを*USEに変更してみます。



⑨再度、「シミュレート」を実行して、レポートの詳細をみると合格が18で不合格が18になり、合格が１つ増えました。

このように、シミュレータ結果の「失敗したルール」の詳細を見て、自社環境のセキュリティ・レベルを少しずつ改善していくことができます。

解説：

・ここでは、自動コンプライアンスの「シミュレート」の機能を解説しました。それ以外の機能としては「適用」を実行すると、該当のIBM iのシステムに対して、強制的に、プロファイルの設定を適用する機能があります。「適用」すると、システム値や、TCPIPの設定値が強制的に変更されますが、失敗する値もあります。（手動での変更が必要なシステム値もあります）「適用」するのは、稼働中のシステムの大きな影響があるので、テスト環境などで十分テストを行ってから本番環境で実施してください。

・推奨されるのは、「シミュレート」で、失敗した設定値を確認してから、１つづつ手動で変更することです。セキュリティ関連のマニュアルを熟読しながら実施してください。

・PowerSCで提供されているオリジナルのコンプライス・プロファイルが自社に合わない場合には、カスタムプロファイルを作成することもできます。（ルールが必要かどうか検討してください）

・「検査」機能は、コンプライス・プロファイルを適用した場合に、その適用したプロファイルに値があっているかを検査する機能です。スケジューラーで定期的に検査する機能があるので自社のコンプライス・プロファイルにあった設定になっているかを確認することができます。

3. アンチウィルス（マルウェア検知）機能

（1）IBM i 上でマルウェア検出が必要な理由

- ✓ 他のプラットフォーム(Windows, x86 Linux等）と比べて、Power上で稼働するIBM iに対するサイバー攻撃頻度やPowerアーキテクチャー上で実行されるマルウェアの報告数を**少なく**抑えられています。

- ✓ しかし、他プラットフォームのサーバーやPCから IBM i上のIFS(統合ファイルシステム)ファイルにはアクセスできるため、IBM i **自身がマルウェアキャリア**となり、気づかないうちに**周辺システムにマルウェアを拡散**してしまうリスクがあります。

- ✓ たとえIBM iでは実行されないマルウェアであったとしても、周辺システムへの影響を拡大させないために、**IBM i 上でもマルウェアそのものを検知する**ことが重要です。

3. アンチウィルス（マルウェア検知）機能
（2）PowerSCで稼働するアンチウィルス・エンジン：ClamAV

ClamAVとは？

✓ トロイの木馬、ウィルス、マルウェア、およびその他の悪意のある脅威を検出するためのオープン・ソースのアンチウィルス・エンジン

✓ PowerSC GUI を使用して、PowerSC GUI エージェント(AIX、IBM i、Linux) 上に導入されている ClamAV に対して以下の操作が可能
- ➢ スキャン設定
- ➢ スキャンの実行 (＋スケジューリング)
- ➢ レポート出力 (＋メール送付)

ClamAVの詳細は、下記参照
https://www.clamav.net/about

解説：

・PowerSCには、トロイの木馬、ウイルス、マルウェア、その他の悪意のある脅威を検出するための
オープンソースのウイルス対策エンジンであるClamAVのマルウェア対策サポートが含まれています。

・ClamAV は、検出されたマルウェアを PowerSC エンドポイント上の隔離ディレクトリに移動または
コピーし、タイムスタンプ付きの接頭辞を付けて、ファイルのパーミッションを無効にして、開いたり
使用したりできないようにします。

・IBM i上にClamAVをインストールするためには、いくつかの前提ソフトウェアが必要です。
詳細は下記を参照してください。(*事前にいくつかのオープンソース導入が必要です)
https://www.ibm.com/docs/ja/powersc-standard/2.2?topic=i-anti-malware-installation-requirements

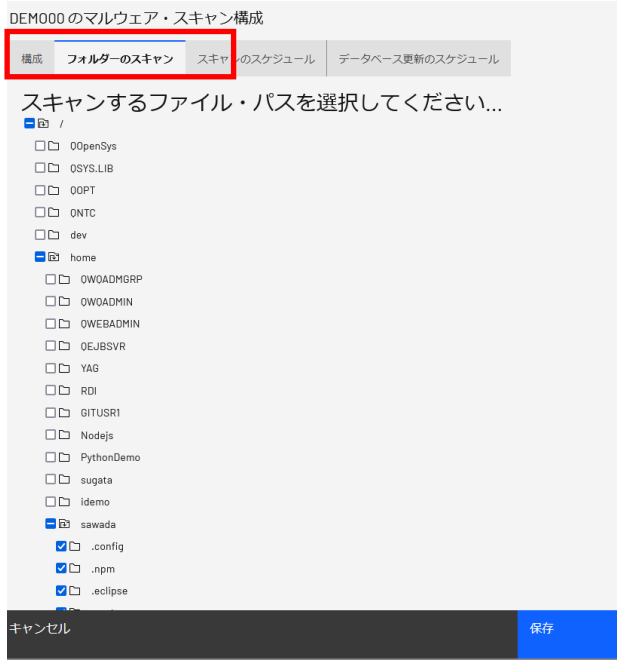
3. アンチウィルス（マルウェア検知）機能

（3）ClamAVによるマルウェアスキャンの設定と実行

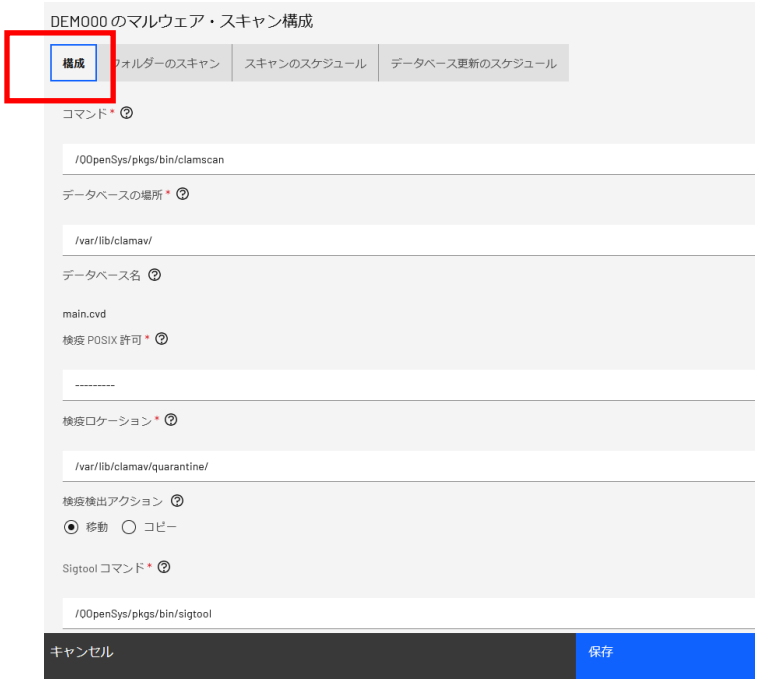
①PowerSC GUIのメインメニューから、「セキュリティ」を選択し、登録されたIBM i 区画が表示されます。アンチウィルス設定をしたい、IBM i 区画(ここではDEMO00）を選択し、「アクション」->「マルウェア」->「マルウェアの構成」をクリックします。

3. アンチウィルス（マルウェア検知）機能
（3）ClamAVによるマルウェアスキャンの設定と実行

②「フォルダーのスキャン」タブを選択します。
スキャン対象のディレクトリーを選択します
（下記例では/home/sawada を選択しています）

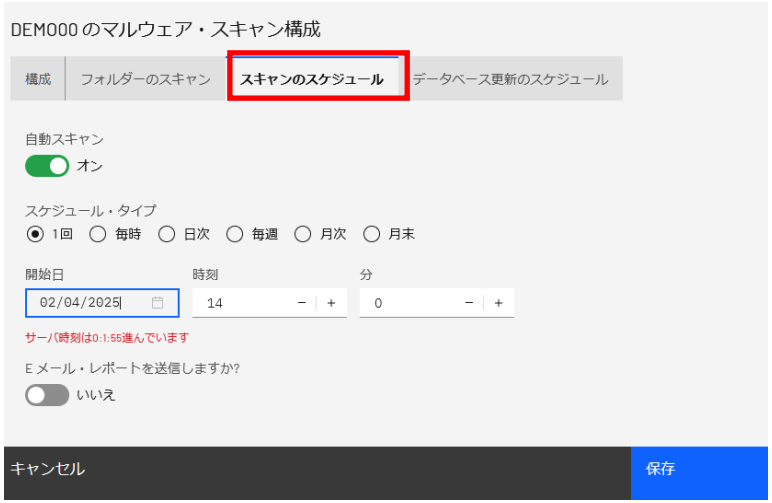


③「構成」タブを選択します。（ここの設定は
clamAVのエンドポイントの導入時の設定に
合わせます。(基本的には自動設定)



3. アンチウィルス（マルウェア検知）機能
（3）ClamAVによるマルウェアスキャンの設定と実行

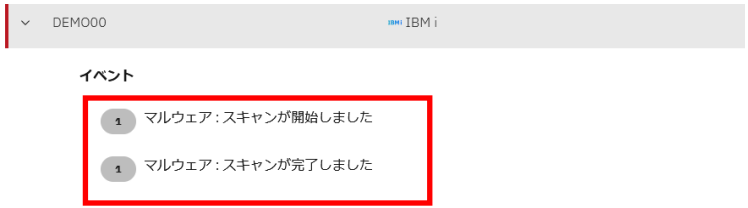
④「スキャンのスケジュール」タブを選択します。
「自動スキャン」をオンにします。
スケジュール・タイプを設定し、
スケジュール設定して、保存します。
（下記例では2/4 14:00 を選択しています）



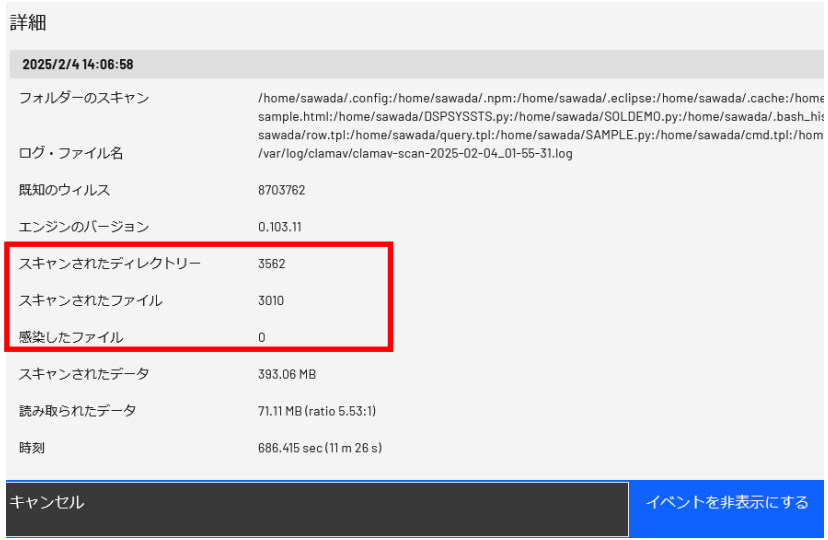
⑤（参考）スケジュール時間になると、
ClamAVのスキャンが稼働します。
下記のように、ユーザー（QIBMPSC)で稼働しています。

3. アンチウィルス（マルウェア検知）機能
（3）ClamAVによるマルウェアスキャンの設定と実行

⑥スキャンが完了すると、下記のように、開始と完了のログが表示されます。



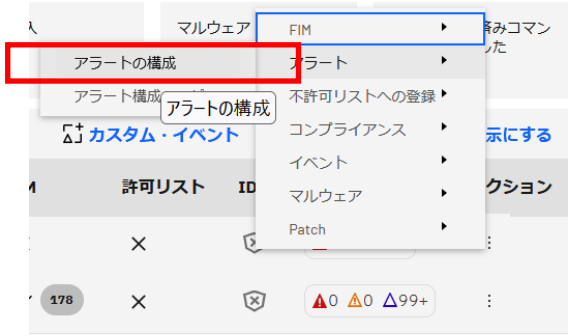
⑦ 「マルウェア・スキャンが完了しました」の行をクリックすると下記のように詳細が表示されます。
例では、スキャンされたファイルは3010個で感染したファイルは0でした。



解説：

・さらに、PowerSC GUIのアラート機能を用いることで、マルウェアを検知した後の対応(メール、ログ出力、カスタムスクリプト)を設定することができます。イベントの検知から応答までをもれなく対策することができます。

「アクション」->「アラート」
->[アラートの構成」をクリックします。



「マルウェア」の各項目ごと(メッセージ毎)
にメールやコマンドで即時、ユーザーに通知することができます。(あるいは即時回線オフなども可能)

4. 多要素認証機能

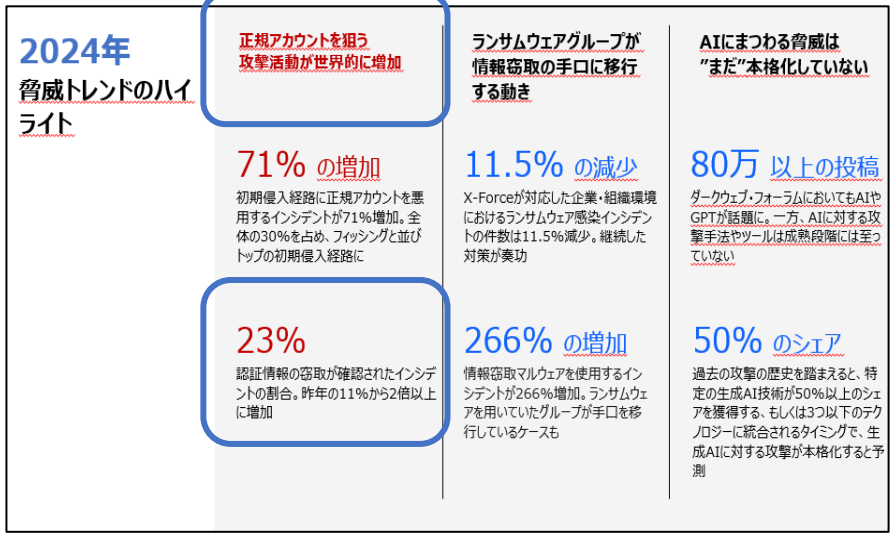
（1）多要素認証機能が注目されている理由

- ランサムウェアなどの外部攻撃や内部不正等による情報漏洩リスクが増加傾向にあります。

- 上記の対策として今、**多要素認証(Multi-Factor Authentication：MFA)**が注目されています。

身近なところでの「多要素認証」の例：

✓ 銀行アプリでの「ワンタイム・パスワード」
✓ オンラインクレジットカード決済での「ワンタイム・パスワード」



IBM：https://www.ibm.com/jp-ja/reports/data-breach

解説：

・ランサムウェア被害のニュースを頻繁に耳にします。公開されていないものも数多くあると思われます。
IBMが毎年発表している「データ侵害のコストに関する調査2024」（下記のリンク参照）に
よると「データ侵害コスト」の平均額は前年比10％増の488万ドル（約7億円）で、過去最高額を記録しました。 https://www.ibm.com/jp-ja/reports/data-breach

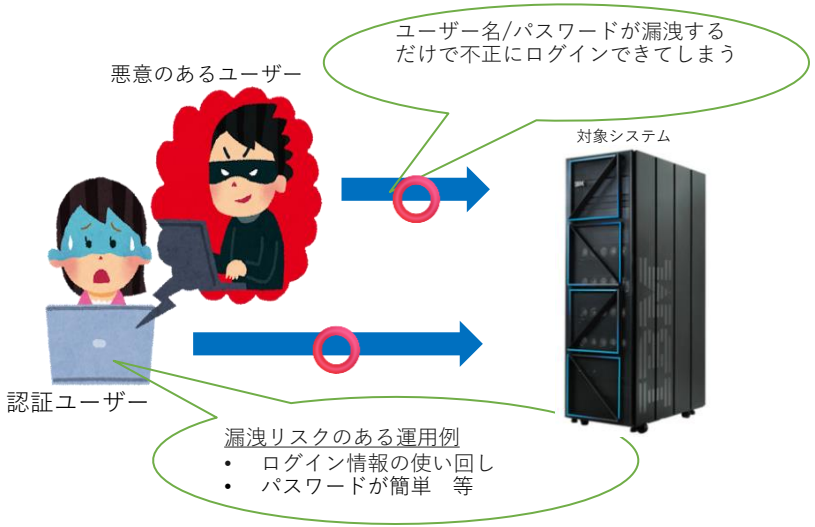
・調査レポートによると、正規アカウントを狙う攻撃活動が世界的に増加しています。認証情報の窃取が
確認されたインシデントの割合は23％と昨年の11％から2倍以上に増加しています。

・またレポートによると、認証情報が盗まれたか、悪意のあるインサイダーによって使用されたかを問わず、
攻撃の特定と封じ込めにかかる時間が増加し、平均合計時間はそれぞれ292日と287日となりました。
防御側は、ネットワーク上の正当なユーザー活動と悪意のあるユーザー活動を区別する必要があるため、
脅威の特定が余計に困難でした。

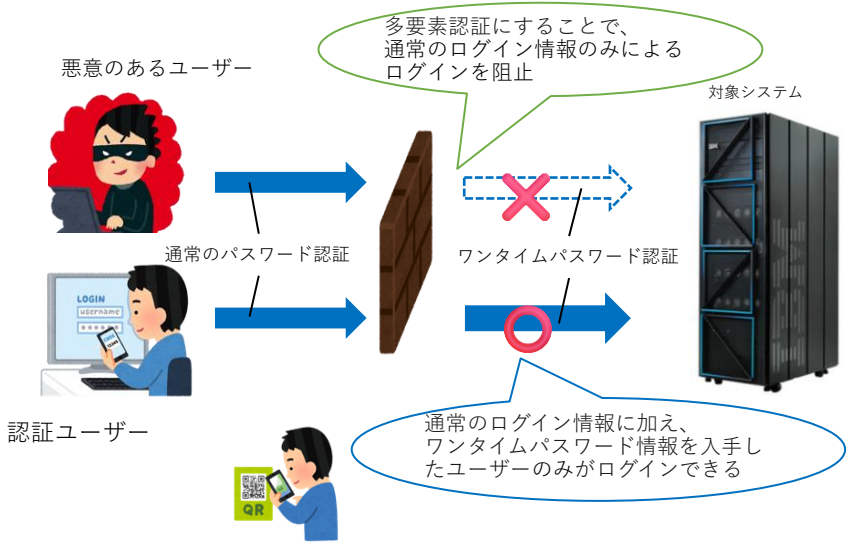
・通常のパスワード認証のみではリスクが高いため、近年では多要素認証が注目されるようになりました。
2種類以上の異なる認証要素を利用する多要素認証は、第三者による不正アクセスをされにくく、
セキュリティを高めることができます。

4. 多要素認証機能
（2）もしOSログインに多要素認証を実装しないと・・

多要素認証がない場合のログイン例



多要素認証を実装した場合のログイン例



多要素認証をOSログインに利用することで、ログイン情報流出による不正アクセスを阻止できます！

4. 多要素認証機能

（3）PowerSC MFAで用いられる多要素認証方式

- ✓ 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時に、　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。
- ✓ PowerSCでは主要な認証方式が利用できます。

名前
PIV/CAC or X.509 Certificate
LDAP Simple Bind
Password Authentication
Generic RADIUS
Thales SafeNet RADIUS
RSA SecurID Authentication API
RSA SecurID RADIUS
Time-based One Time Password (TOTP)
Yubico OTP

- ✓ この後のIBM iの例では、Webでよく使われる認証方式である、Time-Based One-Time Password（TOTP)アルゴリズムを利用しています。

解説：

・PowerSCで利用できる認証方式の詳細については下記を参照してください。
https://www.ibm.com/docs/en/powersc-mfa/2.2?topic=mfa-configuring-powersc-authentication-methods

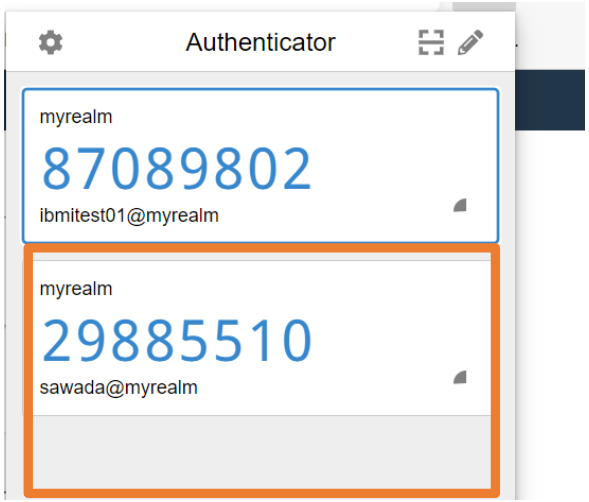
・PowerSCのTOTPの仕様はRFC6238に詳細が記述してあります。
https://tex2e.github.io/rfc-translater/html/rfc6238.html

・RFC 6238は、Microsoft、Google、Facebook、Symantec、およびAmazonなどで採用されています。
・RFC 6238は2要素実装の基礎としてのWebサービスで、この幅広い採用により、オーセンティケーターには以下のような多くのオプションがあります
– Windows WinAuth、1Password、KeePass、Yubico
– Mac OS（OS X）1Password、KeePass
– iOS（およびApple Watch）Google Authenticator、Microsoft Authenticator、Authy
– Android（およびAndroid Wear）Google Authenticator、Microsoft Authenticator、Authy
– ハードウェアトークンProtectimus
その他

4. 多要素認証機能

（4）多要素認証を使ったサインオンを使ってみよう

①ブラウザーのGoogle Authenticator で
認証用のトークンを取得
（下記例では、ブラウザーの拡張機能を
使って、ユーザーID：SAWADA用の8桁
の認証トークンを取得）

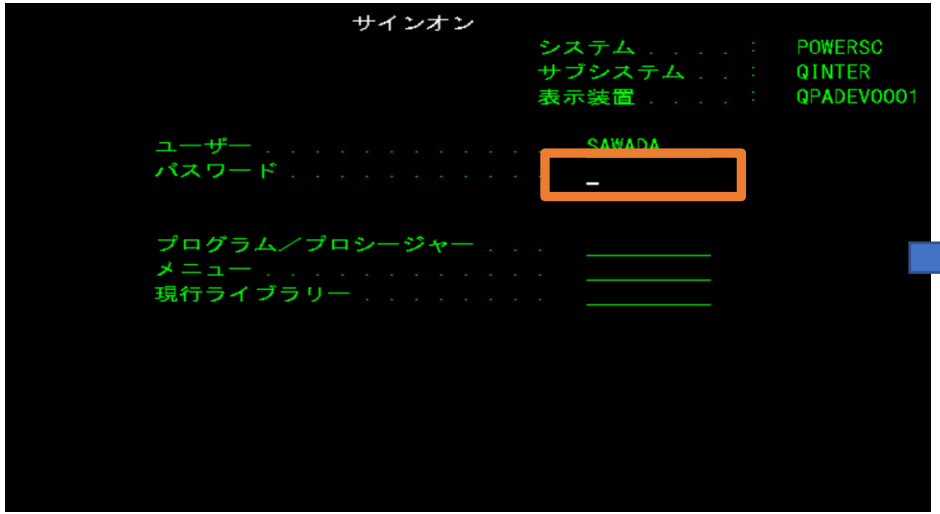


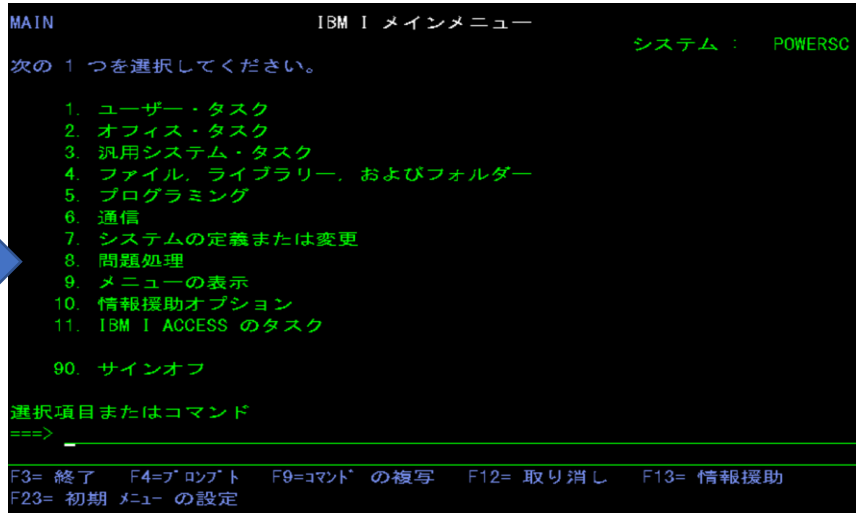
②PowerSCの多要素認証サーバーに接続し、
IBM iのユーザーIDと認証トークンを入力し、
送信をクリックする。
そうすると、認証完了し、キャッシュトークンを
受け取れる。これがIBM i のパスワードになる。

4. 多要素認証機能

（4）多要素認証を使ったサインオンを使ってみよう

③「このCTCをクリップボードにコピー」して、5250画面のパスワードに張り付けサインオンします。





IBM PowerSCを用いたIBM i セキュリティ強化のまとめ：

- ✓ IBM PowerSCは、業界標準コンプライアンスに準拠しているか確認するために、事前構成されたコンプライアンス・プロファイルを提供します。
  IBM iでは、 ベストプラクティスのコンプライアンス・ルールに準拠しているか確認し、適用できます。

- ✓ IBM i上に影響がないマルウェアの場合でも、IFSを介して周辺の他システムに影響を及ぼす可能性があるため、IBM i 上でもマルウェアを検知する仕組みを実装することは重要です。PowerSCではClamAVによるウィルス検知が可能です。

- ✓ パスワード流出等による不正ログインやなりすましを防ぐ手段として、従来のパスワード認証よりも優れているという理由から、多要素認証が大きく注目を集めています。PowerSCは、IBM iの5250ログインに対しても多要素認証を実装することができます。

IBM PowerSCの導入をぜひご検討ください

5. 補足情報

1. IBM PowerSCのホームページ(無料評価版もここから取得できます)
   https://www.ibm.com/jp-ja/products/powersc

2. IBM PowerSC 2.2 のマニュアル
   https://www.ibm.com/docs/ja/powersc-standard/2.2

3. IBM PowerSCご紹介動画（英語）
   https://video.ibm.com/recorded/134043019

4. IBM Power Security Catalog (redbook : 英語)
   https://www.redbooks.ibm.com/abstracts/sg248568.html

IBM i 関連情報 (2025/02/03 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 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

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

IBM i RiSING - IBM i 若手技術者コミュニティー
https://ibm.biz/ibmirising2025

これから使う人のためのIBM i入門ガイド
https://www.imagazine.co.jp/imagazine-7071/

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

IBM i 製品とサポートのロードマップ
https://ibm.biz/ibmiroadmap2024

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」「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 Systems Virtual Server 情報
https://ibm.biz/pvsjapan