IBM Power Systems Virtual Server 検証環境を使用した三和コムテック様の

セキュリティ製品の導入および稼働検証

概要

IBM Power Systems Virtual Server（以降、Power Virtual Server）環境で、以下のセキュリティ製品の導入および稼働検証を実施いたしました。

・iSecurity
・Assure Encryption
・SAVi

背景・課題

Power Virtual Server 環境において、以下のセキュリティ製品が正常に導入および動作するか、
パフォーマンスに問題ないか、などを検証する必要があり実施いたしました。

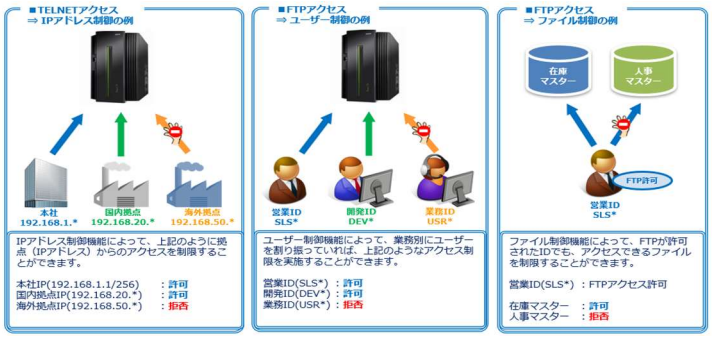
・iSecurity
・Assure Encryption
・SAVi

製品概要

●iSecurity

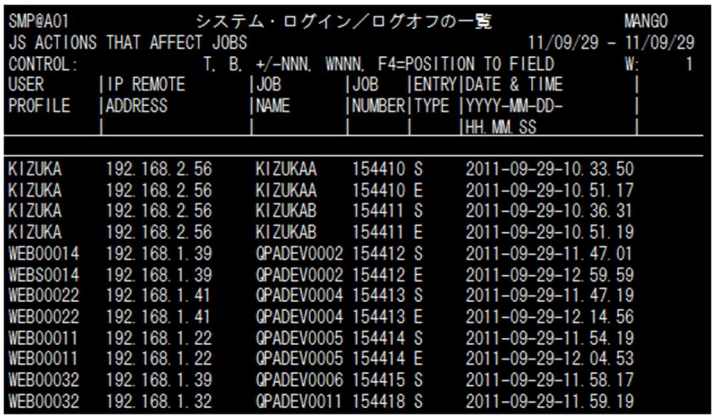
iSecurity は、IBM i のセキュリティ機能を総合的に補完・強化する製品です。検証した各モジュールの概要は以下の通りです。

■Firewall
Firewall は、FTP や TELNET、ODBC/JDBC などのネットワークのアクセスをログに記録します。それらのアクセスを特定の IP やユーザーに制限することができ、さらにアクセスするファイルの制限を加えることもできます。
ネットワークアクセスはログに記録され、制御結果(許可・拒否)を確認することも可能です。



■Audit

オブジェクトの操作やシステムの変更など、システム内部で発生したイベントを
リアルタイムにログに記録します。いつ・誰が・何をしたかなど、イベントを
分かりやすく表示することができます。また、取得したログから「システムのサインオン/
サインオフの履歴」、「高権限ユーザーの操作履歴」など様々な観点のレポートを作成することができます。

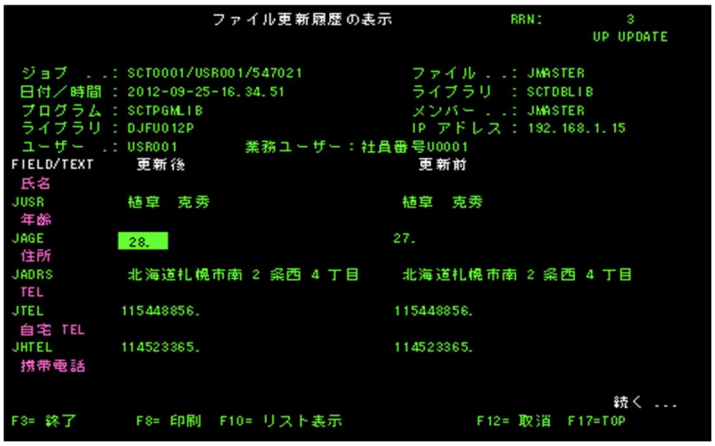


SMP@A01　　システム・ログイン／ログオフの一覧　　MANGO
JS ACTIONS THAT AFFECT JOBS　　11/09/29 - 11/09/29
CONTROL:　　T, B, +/-NNN, WNNN, F4=POSITION TO FIELD　　W:　1

USER PROFILE	IP REMOTE ADDRESS	JOB NAME	JOB NUMBER	ENTRY TYPE	DATE & TIME YYYY-MM-DD- HH.MM.SS
KIZUKA	192.168.2.56	KIZUKAA	154410	S	2011-09-29-10.33.50
KIZUKA	192.168.2.56	KIZUKAA	154410	E	2011-09-29-10.51.17
KIZUKA	192.168.2.56	KIZUKAB	154411	S	2011-09-29-10.36.31
KIZUKA	192.168.2.56	KIZUKAB	154411	E	2011-09-29-10.51.19
WEB00014	192.168.1.39	QPADEV0002	154412	S	2011-09-29-11.47.01
WEBS0014	192.168.1.39	QPADEV0002	154412	E	2011-09-29-12.59.59
WEB00022	192.168.1.41	QPADEV0004	154413	S	2011-09-29-11.47.19
WEB00022	192.168.1.41	QPADEV0004	154413	E	2011-09-29-12.14.56
WEB00011	192.168.1.22	QPADEV0005	154414	S	2011-09-29-11.54.19
WEB00011	192.168.1.22	QPADEV0005	154414	E	2011-09-29-12.04.53
WEB00032	192.168.1.39	QPADEV0006	154415	S	2011-09-29-11.58.17
WEB00032	192.168.1.32	QPADEV0011	154418	S	2011-09-29-11.59.19

■AP-Journal

データベースのレコードレベルの変更履歴を管理する製品です。フィールド・トラッキングや監視を行い、誰が・いつ・どのデータベースをどのように変更したかを記録します。また、変更履歴のほか、読取りの監視も行うことができるので、誰がどのように変更したかのほか、誰が見たまで記録することができます。



ファイル更新履歴の表示　　RRN:　3
UP UPDATE

ジョブ　. .: SCT0001/USR001/547021　　ファイル . .: JMASTER
日付／時間 : 2012-09-25-16.34.51　　ライブラリ　: SCTDBLIB
プログラム : SCTPGMLIB　　メンバー . .: JMASTER
ライブラリ : DJFU012P　　IP アドレス : 192.168.1.15
ユーザー　.: USR001　　業務ユーザー：社員番号U0001

FIELD/TEXT	更新後	更新前
氏名 JUSR	植草　克秀	植草　克秀
年齢 JAGE	28.	27.
住所 JADRS	北海道札幌市南 2 条西 4 丁目	北海道札幌市南 2 条西 4 丁目
TEL 自宅 TEL JTEL	115448856.	115448856.
JHTEL 携帯電話	114523365.	114523365.

続く ...

F3= 終了　　F8= 印刷　F10= リスト表示　　F12= 取消　F17=TOP

■Capture

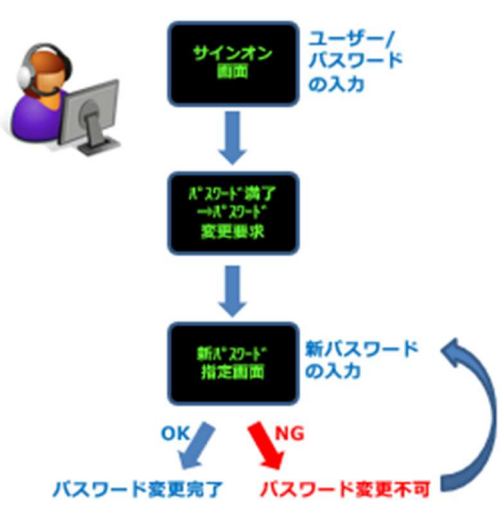
ユーザーがシステムのサインオン画面からサインオンしてからサインオフするまでの
操作(画面遷移)を全て記録します。対象のユーザーが実行キーや操作キーを押下した
タイミングで画面取得が行われます。ログには画面に入力された値、コマンド
なども記録されているため、ユーザーが実際に行った操作を視覚的に捉えることができます。

■Screen

放置されたセッションを自動でパスワードロックをかける 5250 エミュレーター用スクリーンセーバーです。一定期間操作を行わない場合に、画面をブラックアウトさせたり、自動的にサインオフさせることも可能です。ロックはサインオン中のパスワードを入力することで解除ができます。

■Password

専用のパスワード辞書を使用して、ユーザーが変更しようとしたパスワードの妥当性チェックを行います。専用のパスワード辞書を使用することで、簡単に推測されないパスワードを作成することができます。また、システム全体のパスワード・ポリシーを設定・一括管理することができます。

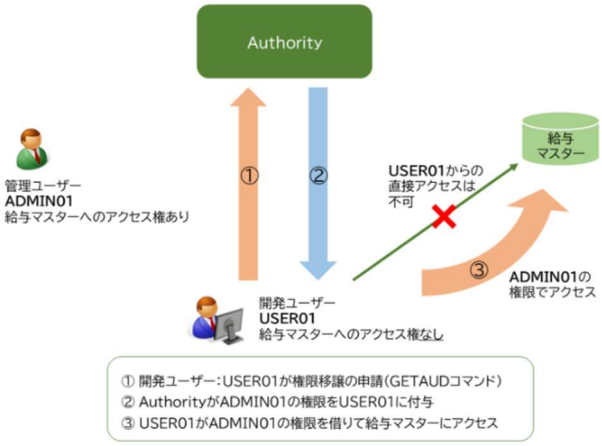


■Command

コマンドを特定のユーザーの実行に限定したり、パラメータの指定方法、パラメータの置き換えを行います。コマンドを使用する前に警告メッセージの表示や、パスワード入力をさせる設定なども可能です。

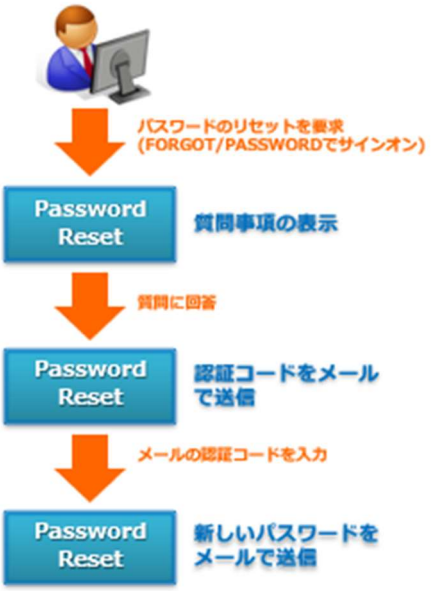
■Authority on Demand

権限を持たないユーザーへ一時的な権限付与を行います。



■Password Reset

エンドユーザーがサインオン時のユーザープロファイルのパスワードを忘れてしまった場合や、パスワード間違いによるサインオン失敗でユーザープロファイルが無効になった場合に、ヘルプデスクに代わって Password Reset がシステマティックに対応します。



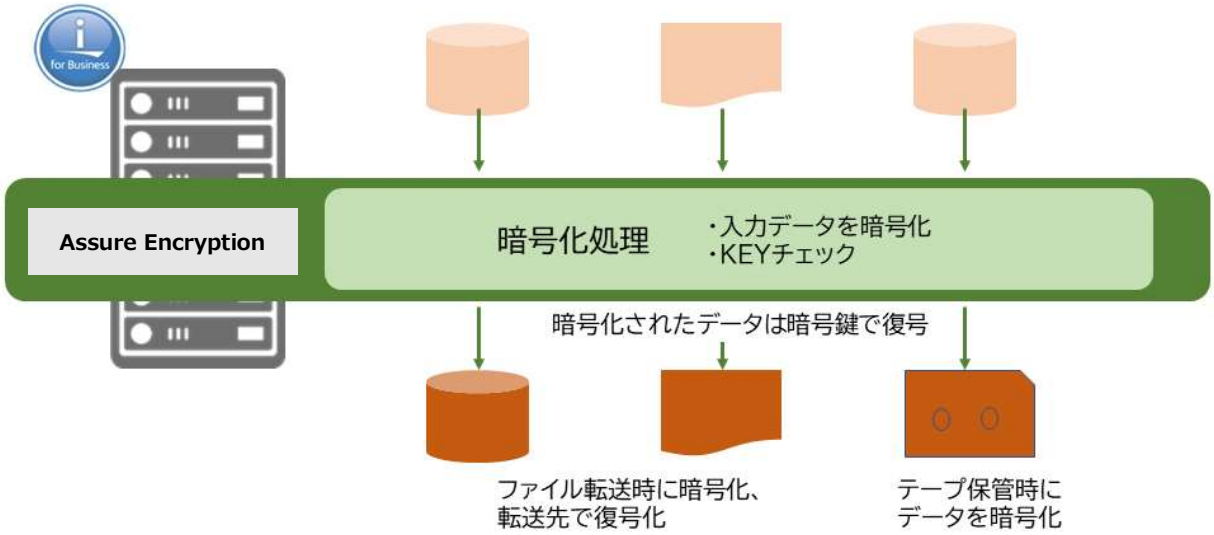
■iSecurity GUI

各モジュールの設定を GUI 画面で行うことができます。また、サブシステムの起動やログ参照も可能です。

●Assure Encryption

セキュリティ性の最も高い米国標準規格の暗号化方式である「AES256bit」に対応して、IBM i のデータを暗号化／復号化するためのソリューションです。メニュー選択もしくはコマンド操作による簡易なユーザーインターフェースにより、テープ媒体への保管時やファイル転送時の暗号化、転送先での復号化に対応し、データ交換やファイル転送時のデータ漏洩リスクを防止します。クレジットカード業界の国際標準である PCI DSS 要件に対応しています。

Db2 ファイル、IFS 上のファイル、保管ファイルなどファイル単位で暗号化／復号化



【製品の特長】

Field Procedure 機能を利用した暗号化／復号化

・物理ファイルのフィールド単位で、暗号化／復号化のプログラムをセットします。
・暗号化／復号化のプログラム（プロシージャ）を自動作成します。
・DFU や QUERY、外部からの SQL アクセスなどでも暗号化／復号化に対応します。
・データのマスキングなどのユーザーごとのコントロールが可能です。

コマンド選択／メニュー操作による暗号化

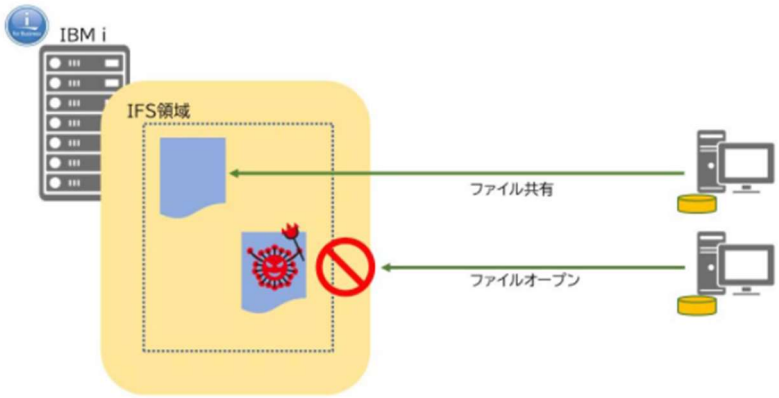
・メニュー選択もしくはコマンド操作によって、Db2 ファイル、IFS 上のファイル、保管ファイルなどファイル単位の暗号化／復号化処理が可能です。

スプールファイルの暗号化とアーカイブ

・ジョブ名、ユーザー名、スプールファイル名などで識別し、暗号化とアーカイブ化をサポートします。
・暗号化されたアーカイブの閲覧や再印刷処理が可能です。

●SAVi

IBM i 上のファイルのウイルス・チェックを行い、IBM i のセキュリティを高める製品です。オープン/クローズ操作が実施された際にリアルタイムで自動スキャンを行う**リアルタイムスキャン**と、5250 画面から対話ジョブ/バッチジョブでスキャンを行う**フルスキャン**の 2 つの方法で、IBM i の IFS 領域のウイルス有無をチェック・記録します。



構成内容

・使用した機器の仕様は以下の通りです。

■Power Virtual Server

・データセンター：東京 04

・マシン：S922

・OS: V7R4

・ディスク容量：180GB

・メモリ：8GB

・コア数：0.25

・一次言語：2962(日本語)

・QCCSID：5035

検証内容

●iSecurity

■Firewall
・製品導入が正常に終了することを確認
・ネットワークアクセス制御ができることを確認
・ネットワークアクセスログが取得できることを確認
■Audit
・製品導入が正常に終了することを確認
・システム内部イベントログが取得できることを確認
・ジョブやメッセージ待ち行列を監視してメッセージを送信できることを確認
■AP-Journal
・製品導入が正常に終了することを確認
・データベース更新履歴が取得できることを確認
■Capture
・製品導入が正常に終了することを確認
・ユーザーの操作ログが取得できることを確認
■Screen
・製品導入が正常に終了することを確認
・ユーザー/端末ごとに設定した時間にロック、サインオフされることを確認
■Password
・製品導入が正常に終了することを確認
・パスワード妥当検査ができることを確認
■Command
・製品導入が正常に終了することを確認
・コマンド実行の制御ができることを確認
■Authority on Demand
・製品導入が正常に終了することを確認
・ユーザーに権限を付与できることを確認
■Password Reset
・製品導入が正常に終了することを確認
・ユーザーパスワードをリセットできることを確認

■iSecurity GUI
・製品導入が正常に終了することを確認
・各モジュールの設定、ログ表示やサブシステム起動ができることを確認

●Assure Encryption

・製品の導入が正常完了することを確認
・製品主要機能が正常稼働することを確認

●SAVi

・製品導入が正常に終了することを確認

・ディレクトリ、CD でのウイルス定義の更新が正常に終了することを確認

・フルスキャン実施時、ウイルスが検知され、ウイルスファイルが隔離されることを確認

・リアルタイムスキャン時、ウイルスが検知され、ウイルスファイルを参照できないことを確認

・スキャン結果がログファイルに記録されることを確認

検証結果

製品	検証日	導入結果	検証結果	備考
Firewall	2021/3/24	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
Audit	2021/3/29	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
AP-Journal	2021/3/23	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
Capture	2021/3/23	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
Screen	2021/3/23	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
Password	2021/3/23	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
Command	2021/3/23	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認

製品	検証日	導入結果	検証結果	備考
Authority on Demand	2021/3/24	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
Password Reset	2021/3/29	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
iSecurity GUI	2021/3/24	正常終了	正常終了	製品導入および設定を行い、主要機能の稼働検証を実施し、問題ないことを確認
Assure Encryption	2021/03/26	正常終了	正常終了	製品導入、主要機能の稼働検証を実施し問題ないことを確認 導入において、オンプレミス環境と比較し時間がかかった。
SAVi	2021/3/29	正常終了	正常終了	SAVi 導入およびウイルススキャン機能の稼働検証を実施で問題なし。

所感

Power Virtual Server 環境においてセキュリティ製品が使用できることが確認できました。

●iSecurity

Power Virtual Server で検証した結果、オンプレミス環境と同様に問題なく稼働することが分かりました。
Firewall のアクセスを検知してメールを送信するといったモジュール間の連携も、正常に動作することを確認しました。
インストールでは、クラウド環境のため光ディスクドライブが使用できないので、仮想光ディスク装置を使用してインストールを行います。
インストールモジュールのアップロードには、通常 FTP を使用しますが、FTP を使用できない SSH 接続環境でも統合ファイルシステムからモジュールをアップロードすることでインストールすることできました。

●Assure Encryption

パフォーマンスには影響は見られませんでしたが、IFS 上のストリームファイルの実行による製品インストール作業において、類似スペックの弊社オンプレミス環境と比較すると時間がかかったため、ご利用いただく際は今回検証した構成より上のスペックを推奨いたします。

●SAVi

リアルタイムスキャン・フルスキャンともに、オンプレミス環境と同様に問題なく稼働することを確認しました。
ログ出力やウイルス定義更新も正常に動作することを確認しました。
インストールモジュールのアップロードには、FTP を使用するため、VPN 接続が必要です。SSH 接続の場合は FTP を使用できないため、統合ファイルシステムからモジュールをアップロードする必要があります。
また、クラウド環境のため光ディスクドライブが使用できないので、仮想光ディスク装置を使用してインストールを行います。

イグアスより

Power Virtual Server 環境では通常英語環境（一次言語：2924）で提供されますが、弊社では日本語環境（一次言語：2962）で提供し、ネットワークは「プライベート・ネットワーク接続環境」にて検証して頂くことが出来ました。
三和コムテック様のセキュリティ製品の検証結果を元にして、多くの IBM i ユーザー様に安心してご利用いただければと存じます。