セキュリティ対策

FUJITSU Security Solution FENCE-Pro V8の機能強化

外部からの攻撃や社員による情報の持ち出し、PCの盗難・紛失・廃棄など、企業の重要データは、常に思わぬ危険にさらされています。FUJITSU Security Solution FENCE-Proを導入して暗号化セキュリティ基盤を整備することで、社内や社外で利用する重要データの情報漏えい対策を確実に実現できます。

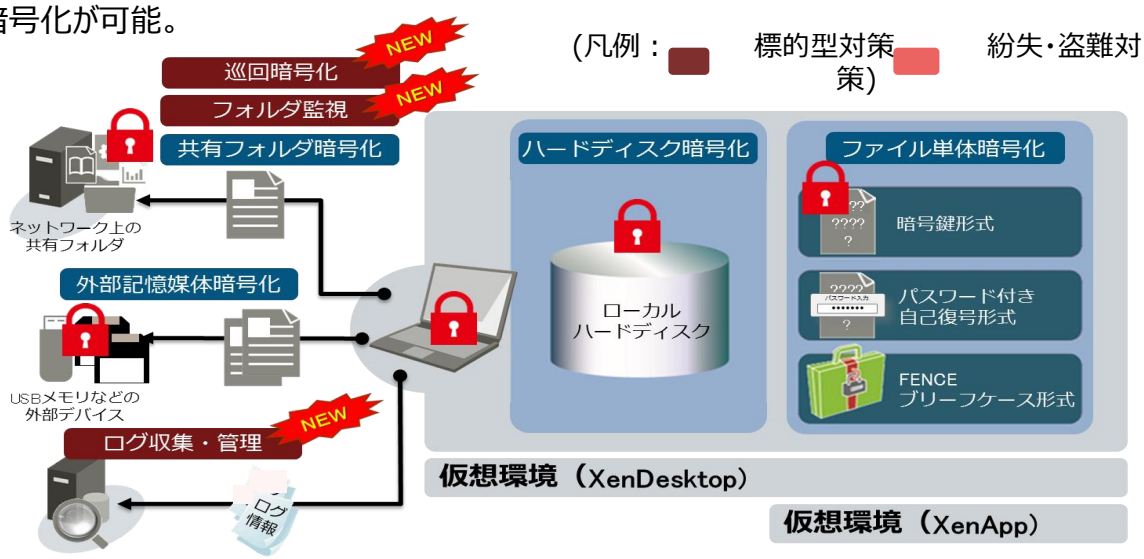
今回、標的型攻撃やランサムウェアの対策のため、下記３つの機能を提供開始しました。

【ここがポイント(今回の機能強化ポイント)】
①標的型攻撃出口対策対応（巡回暗号機能）
②標的型攻撃侵入経路検知（ログ取得機能）
③ランサムウェア対策機能（マルウェア監視機能）

FENCE-Pro概要

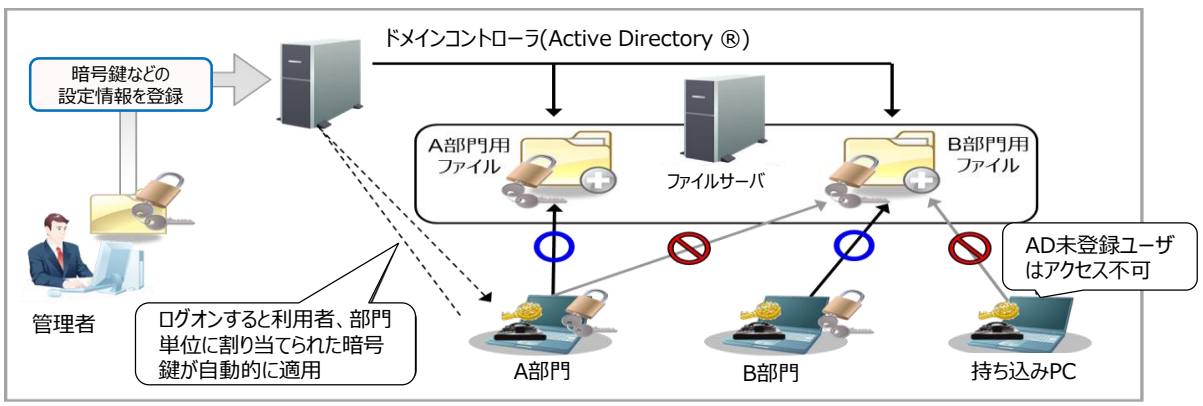
① 簡単・確実に暗号化

- パソコンのローカルディスク、サーバ、 ネットワーク上の共有フォルダやUSBメモリなどに格納されたデータを自動的に暗号化（利用者の特別な操作は一切不要）。
- AES暗号方式（256bit）の暗号アルゴリズムを実装し、利用者に暗号化を意識させない自動暗号化が可能。



② 容易な導入・運用

- Active Directory®との連携により、利用者やグループ単位にポリシー自動配布が可能。
- Citrix®の仮想化ソリューション（XenDesktop® , XenApp® ）との連携が可能。

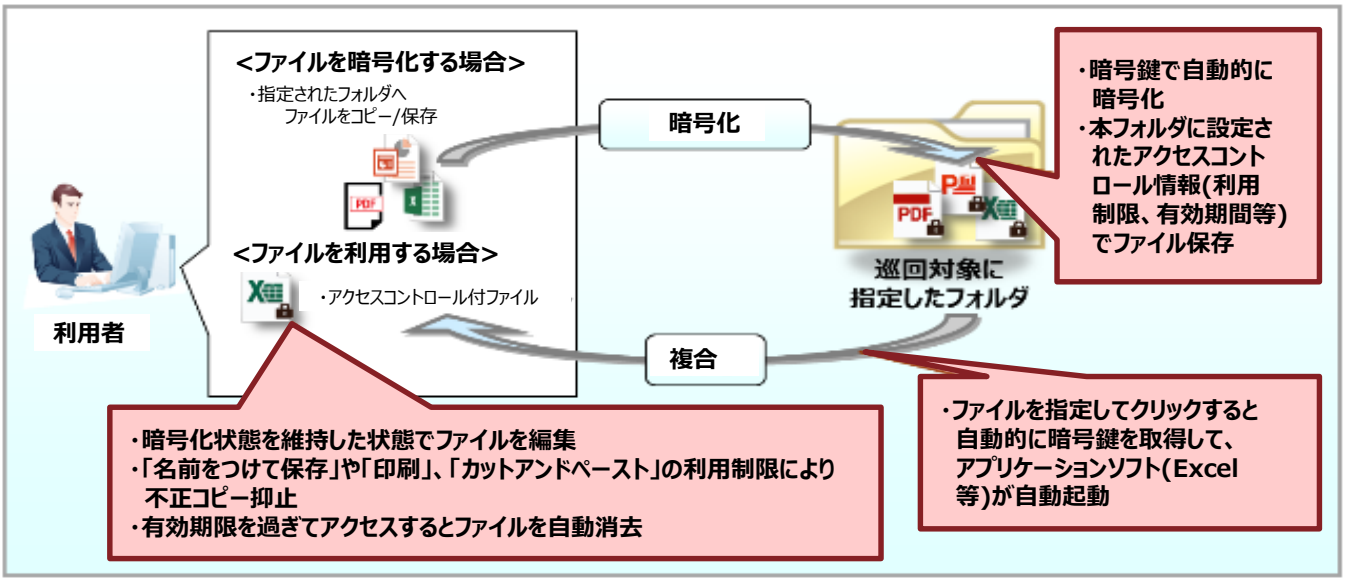


重要なデータは共有サーバで安全に暗号化管理！ADにて一元管理も可能！

今回の機能強化ポイント

①標的型攻撃出口対策対応（巡回暗号機能）

暗号ソフトウェアFENCE-Pro V8に巡回暗号(※1)を追加します。本機能は、従来のFENCE-Pro V8のレベルアップ版（V8L4)で提供します。
また、サーバ（Windows(R)Server）上で実現できるサーバ用ソフトウェア「FENCE-Pro Server V8」も新規に提供します。
※1　巡回暗号とは：FENCE-Proが常駐してドライブ内を巡回し、巡回暗号の対象に指定したフォルダにファイルが作成・コピーされた場合に、ファイル単位に暗号化する機能です。



②標的型攻撃侵入経路検知（ログ取得機能）

特定フォルダへのアクセスやファイル暗号化操作などログ収集・管理を行います。
ログ分析のほか、アラート通知機能を備え、ポリシー設定の範囲を越えた想定外のアクセス（WHITE LISTに登録していないアプリのアクセス）を検知した場合に管理者に通知することも可能です。
※本機能の提供には、オプションソフトウェア「FENCE-Pro V8ログ収集」が必要です。

③ランサムウェア対策機能（マルウェア監視機能）

特定のフォルダに対して、許可していないアプリケーションのアクセスを禁止します。
※本機能の提供には、オプションソフトウェア「FENCE-Pro V8ログ収集」と「FENCE-Pro V8ログ収集　マルウェア監視」が必要です。

動作環境

PC 動作環境 (対応OS)
- Windows®10 Pro
- Windows®10 Home
- Windows®10 Enterprise
- Windows®10 Education
- Windows® 8.1
- Windows® 8.1 Pro
- Windows® 8
- Windows® 8 Pro
- Windows® 7 Home Premium SP 1
- Windows® 7 Professional SP 1
- Windows® 7 Enterprise SP 1
- Windows® 7 Ultimate SP 1
- Windows Vista® Home Basic SP2
- Windows Vista® Home Premium SP2
- Windows Vista® Enterprise SP2
- Windows Vista® Business SP2
- Windows Vista® Ultimate SP2

サーバ動作環境 (対応OS)
- Windows Server® 2008 R2
- Windows Server® 2012
- Windows Server® 2012 R2

セキュリティ対策

FireEye NX Essentialsシリーズ

FireEye NX Essentialsシリーズ (以下、FireEye NX Essentials)は、FireEye社製脅威対策プラットフォームであるFireEye NXシリーズの低価格版「標的型攻撃対策アプライアンス製品」です。

【ここがポイント】
①従来製品と同等の性能をもち、低価格化（従来比約50%オフ）を実現した製品を追加しました。
②ネットワークのミラーポートに接続するだけで、高度で複雑な手法を用いるAPT※などの標的型攻撃を検知することが出来ます。
③ネットワーク構成変更が不要なため、トライアル導入で手軽にFireEyeの価値を体感いただけます。

※APT：Advanced Persistent Threatは、標的型攻撃の一種に分類されるサイバー攻撃です。

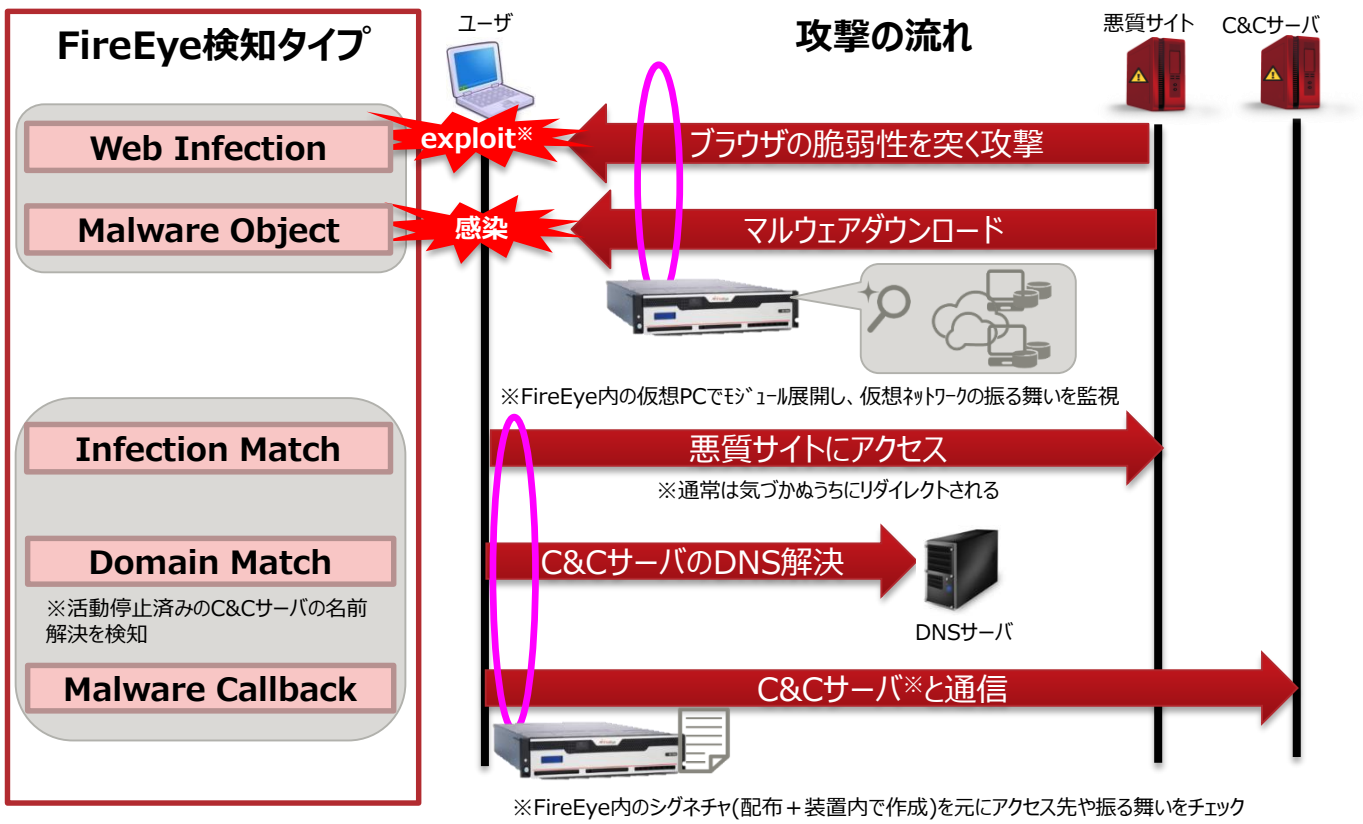
このような悩みを「FireEye NX Essentials」が解決します！

- 高度で複雑な手法を用いるAPTなどの標的型攻撃の脅威を早期発見したい
- サンドボックス※製品をすり抜けるような新たな攻撃に対して、本当に対策が取れるか不安
- たくさんのアラートにより、本当に重要なアラートを見逃さないか不安

※サンドボックス：保護された領域内でプログラムを動作させることで、その外へ悪影響が及ぶのを防止するセキュリティモデル。

FireEye NX Essentialsによる標的型攻撃対策とは

FireEye NX Essentialsは、既存の社内スイッチ機器に接続する(ミラーポート接続)だけで、Web通信を経由して侵入してくる脅威や、感染した端末からの不正な通信を検知可能な標的型攻撃の対策アプライアンス製品です。
FireEye NX Essentialsで使われるMVXエンジンは、多くのサンドボックス型標的型攻撃対策製品が行っている、ファイル単体の検査ではなく、攻撃の一連のフローを解析し、攻撃のステップにあわせたアラートを上げます。攻撃のステップは、そのまま重要度にもなっており、本当に必要なものに絞って対策を採ることが出来ます。



※ C&Cサーバ：コマンド＆コントロールサーバの略。攻撃者は、C&Cサーバを用意し、そのサーバを使って、遠隔操作をし、情報窃取や、より高い権限を持つ端末への侵入等を実施する。マルウェアに感染した端末は、C&Cサーバと接続するために、コールバック通信を行います。

※ exploit：エクスプロイトは（悪意ある）プログラムであり、その中に含まれるデータや実行可能コードが、ローカルコンピュータやリモートコンピュータで動作するソフトウェアの脆弱性を悪用します。

FireEye NX Essentialsの特徴

他社のサンドボックス製品に無い以下の特徴があり、高度で複雑な攻撃であっても、検知することが出来ます。

ネットワーク・メモリ環境も再現

C&Cサーバーへの通信やメモリへ直接ロードするモジュールなど、複雑なマルウェアのプロセスを徹底的に再現します

2000パターンにも及ぶ仮想実行環境

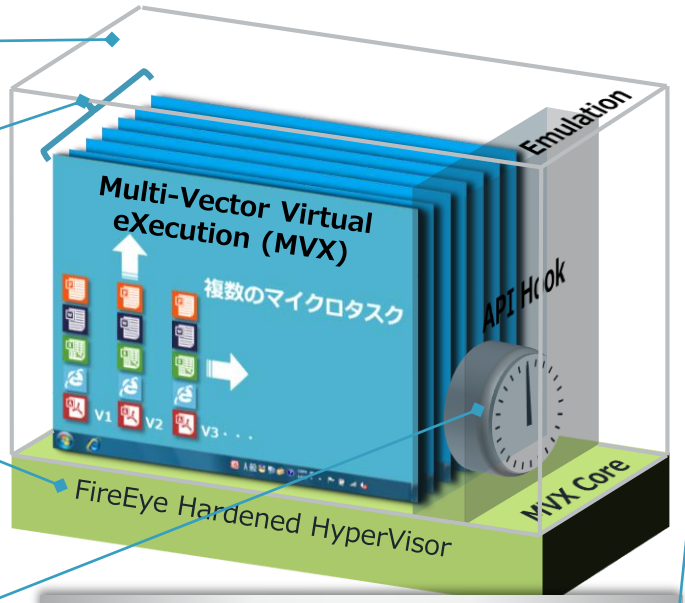
特定のOS、アプリのバージョンを狙うマルウェアの意図を確実に把握する多彩な実行環境をライセンス含めてご提供します

独自開発によりマルウェアに見抜かれない仮想技術

一般的なハイパーバイザーと違い、マルウェアに"SandBox内にいる"ということを気づかせません

時間経過を再現

発症遅延型マルウェアの潜伏・侵入を許しません



マルチフロー解析により多段階攻撃にも対抗

ファイルだけでなく攻撃者との通信そのものを解析するため、巧みな攻撃にも対抗可能です

これらの技術を駆使し、対象のExpolitやObjectを実行した結果を詳細に解析できるため、誤検知が少なく、確実に攻撃を検知

IPCOM EXシリーズ連携　～検知した脅威をIPCOMで防御～

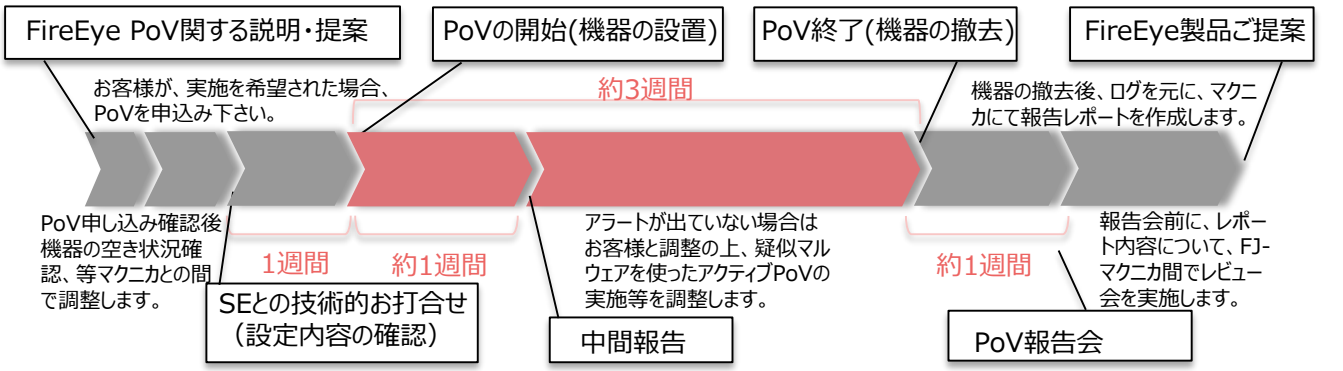
■C&Cサーバとの通信を遮断することで、情報漏えいを防止します。

・FireEye NX Essentialsで未知の脅威を検知し、通信先のC&Cサーバ情報をアラートとして通知

・IPCOM EXシリーズ(LB除く)と連携し、インターネット出口のIPCOMで、コールバック通信の遮断が可能

トライアルによるFireEyeの価値の体感

標的型攻撃対策ソリューションであるFireEyeをお客様環境に3週間程度導入させて頂き、FireEyeの提供するソリューション（シグネチャでは検知することのできない未知の攻撃や高度な標的型攻撃を検知するソリューション）を体感頂けます。



※PoV (Proof of Value)：導入前検証(PoV)として無償トライアルおよび標的型攻撃の診断サービスを提供している。

価格例(標準価格)

■ 従来製品

NX2400 Essentials（本体＋DTI 2-way 1年ライセンス）	¥5,658,660

約60% OFF

■ 今回提供製品

NX2500 50Mbps Essentials（本体＋DTI 2-way 1年ライセンス）	¥2,265,300

※：SDK保守が別途必須となります。

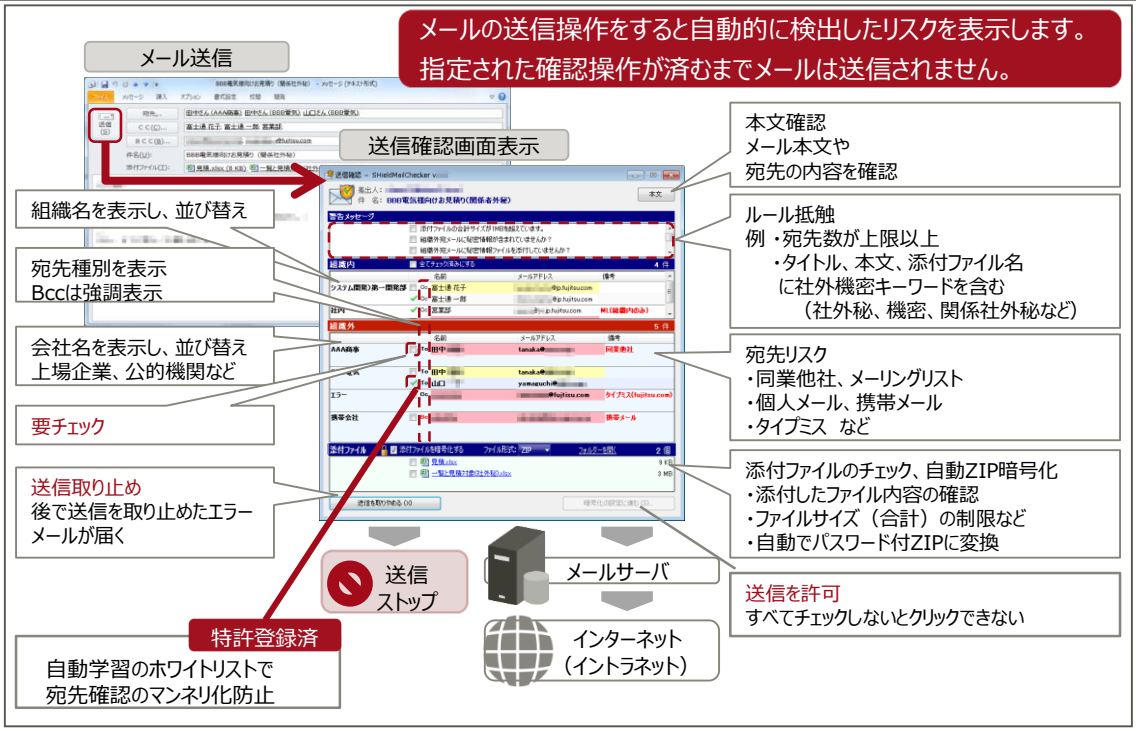
セキュリティ対策

FUJITSU Security Solution SHieldMailChecker 誤送信防止

FUJITSU Security Solution SHieldMailChecker 誤送信防止は、メール送信時に、送信先アドレスのミスや添付ファイルの誤りなど送信リスクの再確認を促すことで、メールの誤送信を未然に防止するソリューションです。「うっかりミス」による情報漏えいを防ぐことができます。

【ここがポイント】
①クライアントへ導入するだけで、対策が完了します。
②送信確認画面にて、検出したリスクだけでなくメール本文や添付ファイルの内容も最終確認できます。

SHieldMailChecker誤送信防止概要



特長

■ 既存サーバ環境のまま、短期間で簡単導入
・SMTP プロトコルを利用する主要メールソフトに対応し、クライアントへ導入するだけで適用完了
（マニュアルに従い、お客様自身でご導入いただけます。）
・コミュニケーションプラットフォームとして人気の高い Microsoft Exchange Server および Office 365 に対応

■ 共通ポリシーにより、メール送信に関する組織内ルールを統一
・製品同梱のサンプルポリシーを元に、組織共通ポリシーを設定して配付可能
・メール送信時にポリシー違反／抵触を警告し、セキュリティレベルを統制

【ポリシーの定義例】
□ 社外に送信する場合、宛先確認が必要
□ 宛先が20件以上の場合、警告を表示
□ 件名、本文、添付ファイル名に注意すべきキーワード（社外秘等）を含む場合、警告を表示
□ 本文、添付ファイルを再確認しないと送信不可
□ 宛先が200件以上の場合、送信をブロック

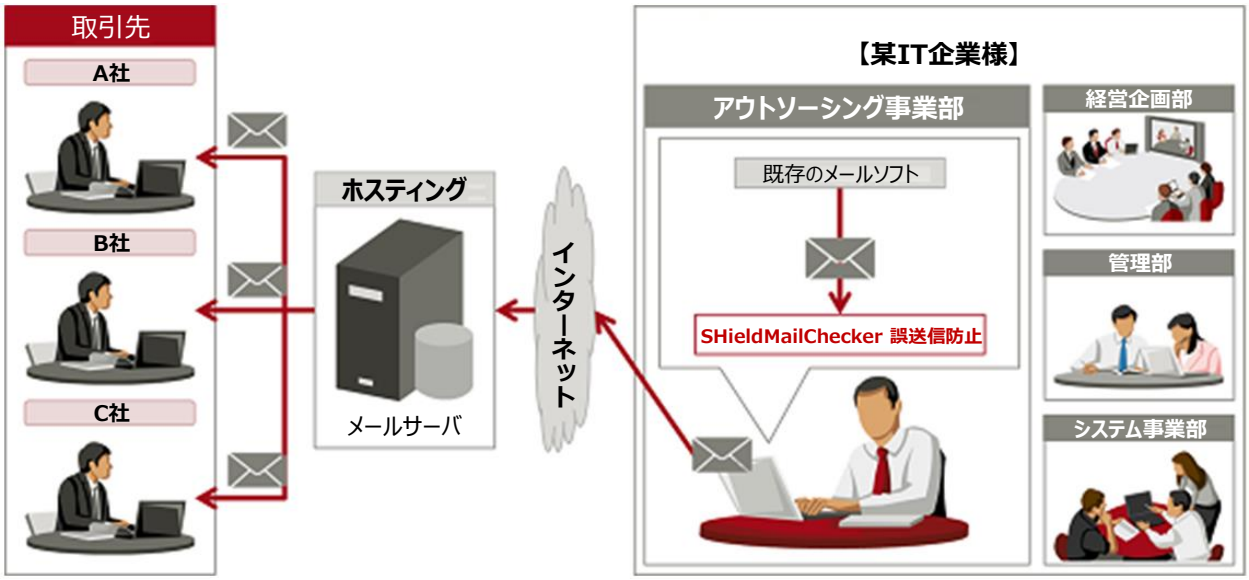
■ 慣れによる見落としを抑止 自動学習ホワイトリスト 特許登録済（注1）
・利用者ごとの送信行動を統計分析し、最近よく送る宛先をホワイトリストに自動登録
・過剰な警告を抑止し、利用者の慣れによるチェック効果の低下を防止
注1: 株式会社富士通研究所と株式会社富士通ソーシャルサイエンスラボラトリによる共同登録

■ Outlookの一部のような操作感
・メール編集と誤送信リスク確認の切り替えがスムーズ
・会議出席やタスクなどの各種依頼をする際も宛先確認画面を表示

■ ストレージサービスと連携し、添付ファイルのセキュアな送信が可能※
・メールに添付されたファイルを自動的に分離し、メール本文とは別経路(https通信)で送信することが可能
※別途Confidential Postingのご契約および設定が必要です。Confidential Postingは富士通FIPが提供する暗号化ファイル伝送ツールです。

■ 豊富な導入実績
・富士通グループ内利用含めて460社以上、約22万ユーザーが利用（2017年3月現在）

導入事例



導入前の状況	・同部では、取引先との情報のやり取りを、主にメールにて実施している。 ・1人の担当者が複数の取引先を担当しており、複数の宛先にメールを同時配信することも頻繁に起こる。 ・メールによる情報漏えいについては、添付ファイルの暗号化、アドレスの直入力禁止などの送信者による人為的な対応が中心であった。
導入の狙い	メール誤送信による情報漏えいのリスクを従来以上に減少させるため、システム的な対応を実施したい。
選定理由	・メール送信宛先が、社内外の区別/所属組織/リスクによる分類整理ができ、視覚的に表示されることでメール利用者に的確に気づきを与え、誤送信防止に効果的である。 ・サーバ導入不要で、クライアントへの導入により適用完了するため、既存のメール環境を維持したまま段階的導入が可能である。 ・ホワイトリストの自動学習機能により、過剰な警告を抑止し、慣れによる実効性低下が防止される。
導入効果	・不注意やうっかりミスによるメール誤送信のリスクを効果的に低減できた。 ・メール利用者が安心感を持って、メール送信できるようになった。 ・メール利用者ひとりひとりのセキュリティ意識が向上した。

動作環境/対応言語

対応プロトコル		SMTP※1、MAPI(接続先：Microsoft Exchange Server 2010/2013/2016)
動作確認済みのメールサーバ		■SMTP：sendmail[8.13]、Postfix[2.3]、qmail[1.03] ■MAPI：Microsoft Exchange Server[2010][2013][2016]、Office 365(Microsoft Exchange Online) ※2
クライアントPC	**OS**	Windows 7 SP1以降 (32bit/64bit)、Windows 8.1(32bit/64bit)、Windows 10(32bit/64bit)
	必要ソフトウェア	.NET Framework 3.5 SP1以降
	確認済みメールソフト (括弧内は対応プロトコル)	・AL-Mail32[1.13a](SMTP)　・Becky! Internet Mail [2.58.00](SMTP) ・Microsoft Outlook [2007 SP3](SMTP、MAPI)※3※4　・Microsoft Outlook [2010 SP2](SMTP、MAPI)※3 ・Microsoft Outlook [2013 SP1](SMTP、MAPI)※3　・Microsoft Outlook [2016](SMTP、MAPI)※3 ・Thunderbird[31.2](SMTP)※3　・秀丸メール[5.70](SMTP)

※1 SSL/TLSには、対応しておりません。
※2 2017年3月現在のバージョンで動作確認済です。最新バージョンには順次対応していきます。
※3 Microsoft Windows の英語OS、英語版でも動作確認済です。
※4 Microsoft Outlook [2007 SP3](SMTP、MAPI)のサポートは、日本マイクロソフト社によるサポートの期限である2017年10月10日で終了します。
注) Confidential Postingの動作環境については富士通FIPにお問い合わせください。

対応言語：日本語/英語（設定で切換可能）
※マニュアルについては日本語版・英語版をそれぞれご用意。
注) Confidential Postingと同時にご使用になる場合は、英語表示に対応しておりません

価格

パック名	ライセンス価格(税別)	年間保守料(税別)	備考
基本ライセンスパック10	45,000円	12,000円	10ユーザーまでご利用になれます。
基本ライセンスパック50	180,000円	36,000円	50ユーザーまでご利用になれます。
基本ライセンスパック100	300,000円	45,000円	100ユーザーまでご利用になれます。
基本ライセンスパック10,000	20,000,000円	3,000,000円	10,000ユーザーまでご利用になれます。

【価格例】1,000ユーザの場合　　ライセンス： 3,000,000円　　年間保守料： 450,000円
各種基本ライセンスパックを組み合わせてご購入ください。

セキュリティ対策

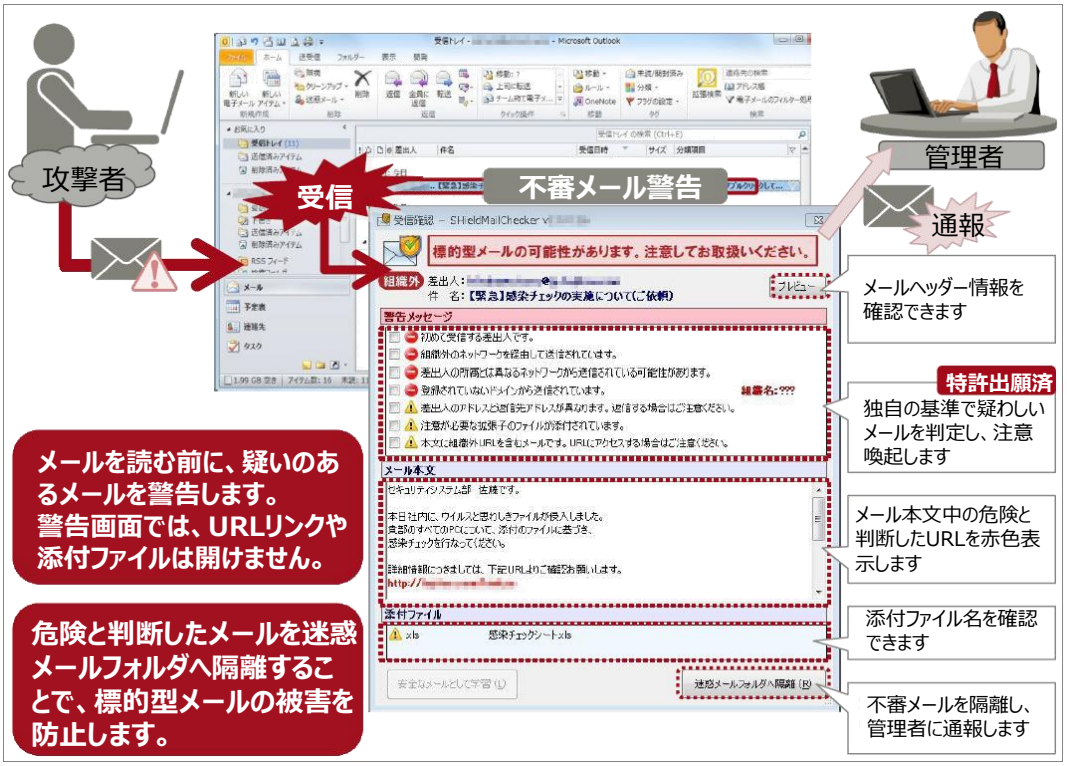
FUJITSU Security Solution SHieldMailChecker 標的型メール対策

FUJITSU Security Solution SHieldMailChecker 標的型メール対策は、クライアントPCにインストールして標的型メール攻撃の対策を行うことができるソフトウェアです。
標的型メールを読む前に警告／隔離することで、安全を守ります。

【ここがポイント】
①疑わしいメールを判断／警告し、利用者が対処しやすくすることでセキュリティを強化します。
②疑わしいメールを隔離することにより、標的型メールによる被害を防止します。

SHieldMailChecker標的型メール対策概要

1．標的型メールを読む前に警告・隔離し、社員の注意喚起を高めます
2．人では判断が難しい不審メールを技術的に判断し内部侵入リスクを低減



特長

■ 独自の識別情報による、なりすまし防止 特許出願済（注1）
・メール送信時に、組織内共通の識別情報を付与し、なりすましを検知/警告します。

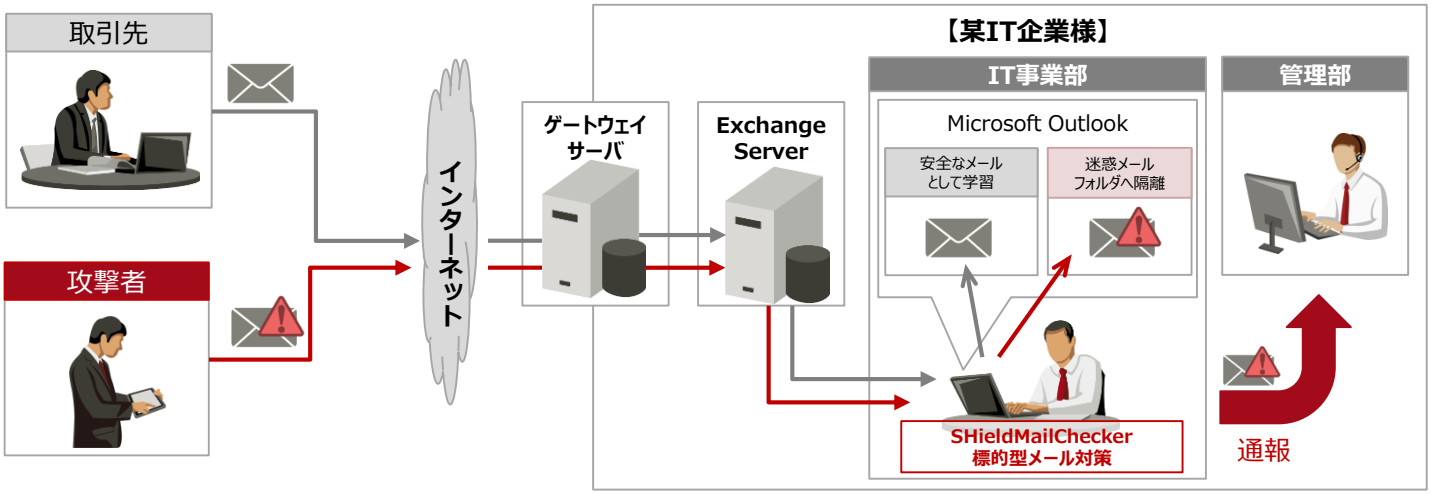
■ 受信履歴を基にした差出人毎の特徴分析 特許出願済（注1）
・過去に受信したメールから差出人毎の特徴を学習し、送信経路の変化など普段と特徴が異なるメールを検知/警告します。(注2)

■ わかりやすい警告画面で受信者に注意を喚起
・危険度に応じ、レベル分けして警告を表示します。
・メール本文中のURLリンクをホワイトリストなどと比較して、注意すべき場合は赤文字で表示します。

■ 組織全体の標的型攻撃リスクを把握
・利用者が隔離した不審メールを、管理者に通報します。
・各社員の受信メールの傾向や隔離状況などをログに蓄積します。
・ログをサーバーで集約することも可能です。

注1：富士通株式会社による出願
注2：ネットワークによっては適用できない場合がありますので、事前に評価版を試用してご確認ください。

導入事例



導入前の状況	・標的型メール攻撃が危険だとわかっているが、社員の端末（クライアント）にウイルス対策以外の対策は実施していない。 ・社員全体に標的型メール攻撃の危険性や見分け方の情報共有は行っていた。
導入の狙い	・標的型メールに対する社員のセキュリティ意識を向上させたい。 ・社員が受信したメールと怪しいと判断する補助のために、メール情報を機械的にチェックしたい。
選定理由	・Outlookとのシームレスな連携で、メールを開く前にメール内容を安全に確認/隔離できる。 ・サーバ導入不要で、クライアントへの導入により適用完了するため、既存のメール環境を維持したまま段階的導入が可能である。 ・差出人毎のメール特徴学習機能により、過剰な警告が抑止される。
導入効果	・組織外から送信されたメールの、URLや添付ファイルを安易に開く回数が減った。 ・不審なメールに対する社員のリテラシー（セキュリティ意識）が向上した。

動作環境

対応プロトコル		MAPI(接続先：Microsoft Exchange Server 2010/2013/2016)
対応メールサーバ		Microsoft Exchange Server[2010][2013][2016]、Office 365(Microsoft Exchange Online) ※1
クライアントPC	**OS**	Windows 7 SP1以降 (32bit/64bit) Windows 8.1 (32bit/64bit) Windows 10 (32bit/64bit)
	必要ソフトウェア	.NET Framework 3.5 SP1以降
	対応メールソフト	Microsoft Outlook [2007 SP3] ※2 Microsoft Outlook [2010 SP2] Microsoft Outlook [2013 SP1]　Microsoft Outlook [2016]

※1 2017年3月現在のバージョンで動作確認済です。最新バージョンには順次対応していきます。
※2 Microsoft Outlook [2007 SP3] のサポートは、日本マイクロソフト社によるサポートの期限である2017年10月10日で終了します。

価格

パック名	ライセンス価格(税別)	年間保守料(税別)	備考
基本ライセンスパック10	45,000円	12,000円	10ユーザーまでご利用になれます。
基本ライセンスパック50	180,000円	36,000円	50ユーザーまでご利用になれます。
基本ライセンスパック100	300,000円	45,000円	100ユーザーまでご利用になれます。
基本ライセンスパック10,000	20,000,000円	3,000,000円	10,000ユーザーまでご利用になれます。

【価格例】1,000ユーザの場合　　ライセンス： 3,000,000円　　年間保守料： 450,000円
各種基本ライセンスパックを組み合わせてご購入ください。

セキュリティ対策

情報漏えい対策ソフト FUJITSU Software Portshutter Premium V2

「Portshutter Premium」は、不正なデバイスやネットワークを使わせないパソコンの情報漏えい対策ソフトウェアです。仮想PCに対応した「Portshutter Premium V2」を販売開始しました。
「Portshutter Premium」はWindows搭載の富士通法人向けパソコンにも標準搭載されています。

V2では新たに以下の機能を提供します。

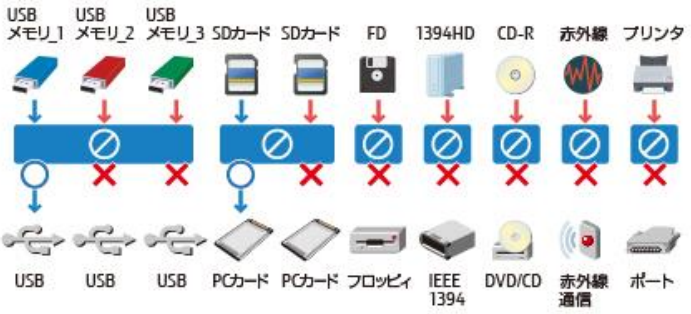
- 不正なUSBデバイス/PCカードが接続された時に証跡ログを出力します。
- 不正なワイヤレスネットワーク接続のアクセスポイント表示を制限します。
- Bluetoothを遮断していても特定の通信（HID／オーディオなど）のみを使用可能とします。
- 仮想PC 環境（VMware）にインストールすることで、仮想PC 内で使用するデバイスの制限をすることができます。

デバイス接続を遮断

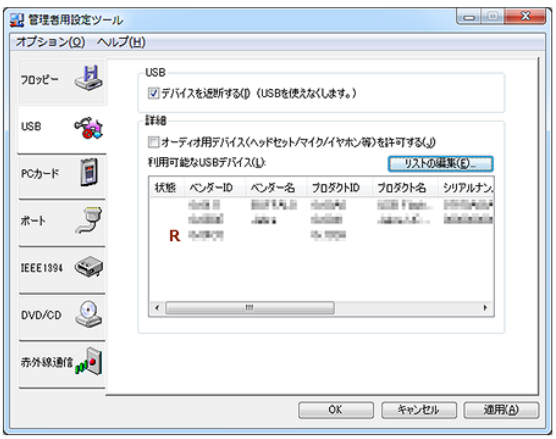
デバイス制御

記憶媒体へのポートを遮断し使用制限

パソコンに接続する記憶媒体などのポートを遮断し、それぞれの使用を制限します。 記憶媒体による情報の持ち出し・持ち込みを制限します。
USB やPC カードは、許可していないデバイスが接続された時にイベントログに証跡ログを出力させることもできます。



▶ 簡単操作で記憶媒体への出口を個別に制御



デバイスの使用制限を簡単に指定

■ デバイスの使用制限は「管理者用設定ツール」で簡単に指定できます。ドライブ（DVD、CD、フロッピィなど）、スロット（PC カード、Express Card、メモリーカードなど）、ポート（シリアル、パラレル、USB、IEEE1394、赤外線通信など）のすべてを遮断（ロック）することも、個別に使用制限することもできます。

▶ USB 機器、PCカードは「機器」ごとに制御

機器ごとに有効／無効／読み取り許可を設定

■ USB およびPC カードデバイスは、「機器」ごとに制御できます。指定した特定メーカーの特定のUSB機器や、特定のハードウェアIDのPCカードしか利用できないように、使用制限できます。例えば、USB 接続のキーボードを許可しながらUSB メモリの使用を制限し、 同時にUSB オーディオ機器を許可することもできます。

■ また、DVD、CD、フロッピィ、USB のストレージデバイスは、読み取りだけを許可することも可能です。

■ 仮想PC 環境にインストールすることで、仮想PC 内で使用するデバイスの制限をすることができます。

※仮想PC環境はVMwareをサポートしています。

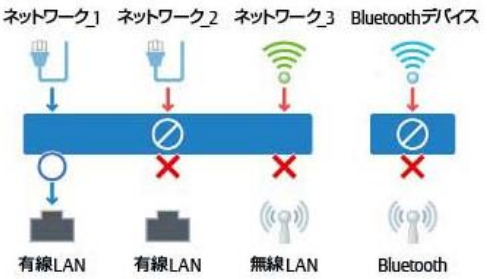
ネットワーク接続を遮断

ネットワーク制御

ネットワークとBluetoothを遮断し使用制限

LANポートやBluetooth搭載機器とのペアリングを遮断（※）し、ネットワークの使用を制限します。登録したネットワーク以外での情報を持ち出し・持ち込みを制限します。

※Windows標準のドライバで動作するデバイスの場合、マウスやマイクなどの一部種類のBluetooth 機器だけを使用可能にすることもできます。



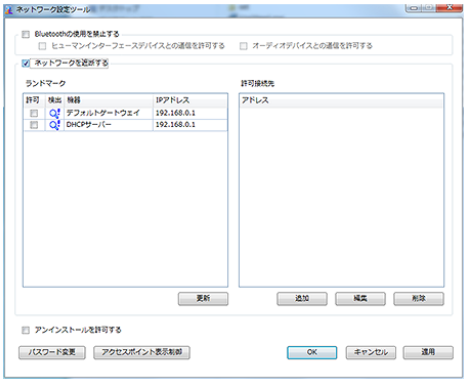
▶ 自動検出したパソコンのネットワーク設定をもとに制御

必要なネットワークのみ使用を許可

- ネットワーク全体を遮断後、自動検出したランドマーク（※）の一覧から、使用を許可したいネットワークに所属する機器を選択することでネットワーク使用の許可を設定します。

※ランドマークとは、社内ネットワークや部署のネットワークなど目印となる機器を指します。一覧は、パソコンに設定済みのインターネットプロトコルなどから自動検出した機器から作成されます。

- ワイヤレスネットワーク接続の一覧に表示させるアクセスポイントのネットワーク名を制限することが可能です。

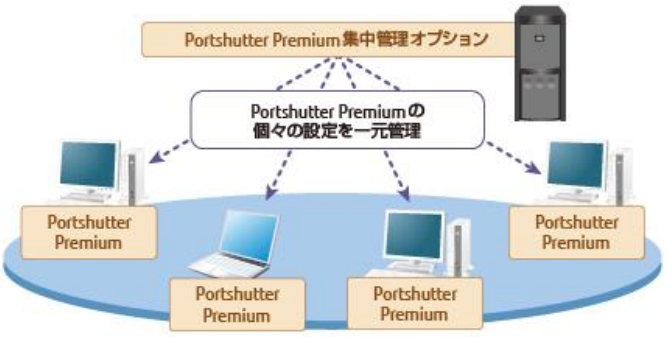


Portshutter Premium をサーバ上で一元管理

有償オプション

デバイスやネットワークの個々の設定を組織的に管理

集中管理オプション（有償）を利用すれば、ネットワーク上のサーバから各クライアントパソコンのPortshutter Premiumの設定を迅速かつ一括で行えます。管理の負荷が軽減され、設定ミスや設定もれなどを防ぐことができます。



※価格はすべて税抜きです。

商品体系と価格

■Portshutter Premium 本体(必須)

メディアパック

製品	価格
Portshutter Premium V2 メディアパック	5,000円

※Portshutter Premiumのインストールメディア商品です。
※本商品の使用にあたり、別途、必要数分のライセンスをご購入ください。

ライセンス(必要ライセンス購入)

ライセンス数	価格	仮想環境同時接続価格
1 ライセンス	3,600 円	3,900 円
50 ライセンス	170,000 円	185,000 円
100 ライセンス	320,000 円	351,000 円
200 ライセンス	600,000 円	663,000 円
500 ライセンス	1,400,000 円	1,560,000 円
1000 ライセンス	2,600,000 円	2,920,000 円
2000 ライセンス	4,400,000 円	5,070,000 円

※「メディアパック」のご購入は必須です。
※「メディアパック」と「ライセンス」を組み合わせて、必要なライセンス数をご購入ください。
※表に記載のないライセンス数は、製品Webサイトをご覧ください。

■Portshutter Premium 集中管理オプション(任意)

メディアパック

製品	価格
Portshutter Premium V2 集中管理オプション メディアパック	5,000円

※Portshutter Premium 集中管理オプションのインストールメディア商品です。
※本商品の使用にあたり、別途、必要数分のライセンスをご購入ください。

クライアントライセンス

クライアントライセンス数	価格
50 ライセンス	80,000 円
100 ライセンス	150,000 円
200 ライセンス	180,000 円
500 ライセンス	200,000 円
1000 ライセンス	300,000 円
2000 ライセンス	580,000 円

※Portshutter Premium 集中管理オプションはPortshutter Premium V1以降に対応しています。
※表に記載のないライセンス数は、製品Webサイトをご覧ください。

■年間プログラムサポート

ライセンスプログラムサポート数	価格	ライセンスプログラムサポート数	価格
50 ライセンスプログラムサポート	25,500 円	500 ライセンスプログラムサポート	210,000 円
100ライセンスプログラムサポート	48,000 円	1000 ライセンスプログラムサポート	390,000 円
200ライセンスプログラムサポート	90,000 円	2000 ライセンスプログラムサポート	660,000 円

※プログラムサポートをご購入いただいていないお客様からは、ご購入後の製品に関する一切のご質問をお受けすることができません。Portshutter Premium をお買い上げいただく際には、同時にプログラムサポートを購入いただくことを強く推奨いたします。
※プログラムサポートには「Portshutter Premium 集中管理オプション」のサポートも含みます。

※年間プログラムサポートは、50ライセンス以上からのご契約となります。50ライセンス未満の場合、50ライセンスのご契約をお願いします。
※サポートサービスの詳細は、製品Webサイトをご覧ください。
※表に記載のないライセンス数は、製品Webサイトをご覧ください。

セキュリティ対策

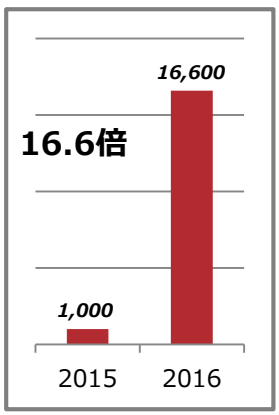
ランサムウェア対策

感染したパソコンをロックして操作不能にしたり、重要なファイルを暗号化したりする「ランサムウェア」による被害が、日本国内でも急増しています。ロック解除や暗号化されたファイルを復元することと引き換えに「身代金」を要求します。感染すると業務継続できないため、ビジネス活動に大きな影響を及ぼします。パソコンに限らず、病院や教育機関などの業務システムでの感染例も報告されています。
ランサムウェアの対策について富士通のソリューションをご紹介します。

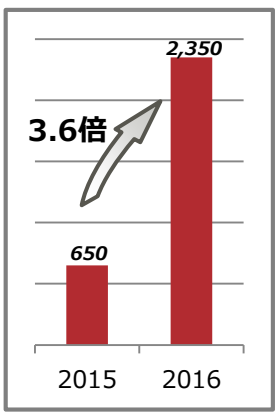
感染被害が急増しているランサムウェア

システムやデータを使用不能にして金銭を要求するランサムウェア攻撃の感染被害が今年に入り急増しています。
主な感染経路は偽装メールの添付ファイルや改ざんされたWebサイト閲覧などになります。

ランサムウェアの被害が一年で急増



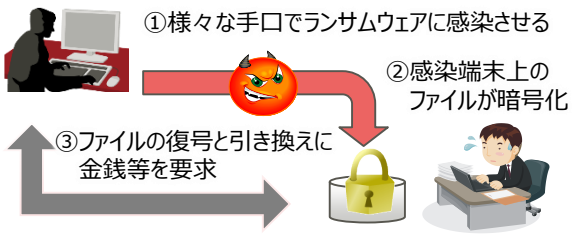
ランサムウェア検出台数
(国内・法人)



ランサムウェア被害報告件数
(国内・法人)

出典：トレンドマイクロ2016年セキュリティラウンドアップ

企業において業務が停止する恐れ

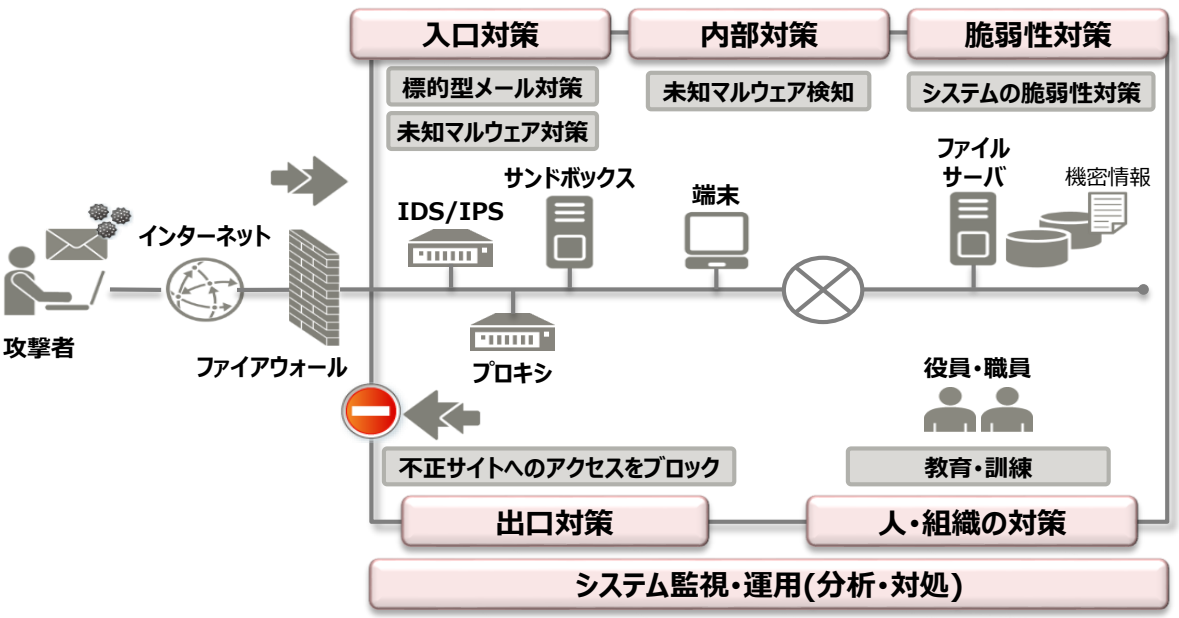


ランサムウェアは2種に大別されます

- 端末ロック型ランサムウェア [端末を人質]
  画面ロックやアプリの強制終了などの手口で感染端末を操作不能にするタイプ
- 暗号化型ランサムウェア [データを人質]
  感染端末内のデータやファイルサーバー上のデータを暗号化して使用不能にするタイプ

ランサムウェア対策の考え方

ランサムウェアもマルウェアの一種で感染経路も同じため、対策も他の不正プログラムと同様に標的型攻撃対策が有効です。攻撃の全体像を把握した上で、多層防御によりランサムウェアの侵入や感染を防ぎます。



ランサムウェアによる被害を最小限に抑える対策

サイバー攻撃の手法は年々巧妙になっており、ランサムウェアの確実なブロックは保証できません。ランサムウェア感染を前提に、業務への影響を最小限に抑えることがセキュリティマネジメントには必要です。最も効果的な方法は「バックアップ」です。復旧できる唯一の手段となりますので、バックアップ先が被害に遭わないようにすること、感染済のデータでバックアップを上書きしないよう、世代管理運用が重要となります。

ランサムウェア対策に有効なバックアップの考え方

復旧対策

① 業務影響を最小限に抑える

- クライアントPC全台数分のバックアップは有効ですが、大容量の確保やネットワーク負荷、管理面において多額のコストが掛かることを考慮する必要があります。
- PC内も含め社内に散在するデータを棚卸し、データの重要度/機密性に応じてデータを仕分ける。業務への影響がある重要なデータは、必ずPC以外に保存する運用を徹底し、バックアップ容量も削減する。

② ランサムウェアがアクセスできない場所に保存する

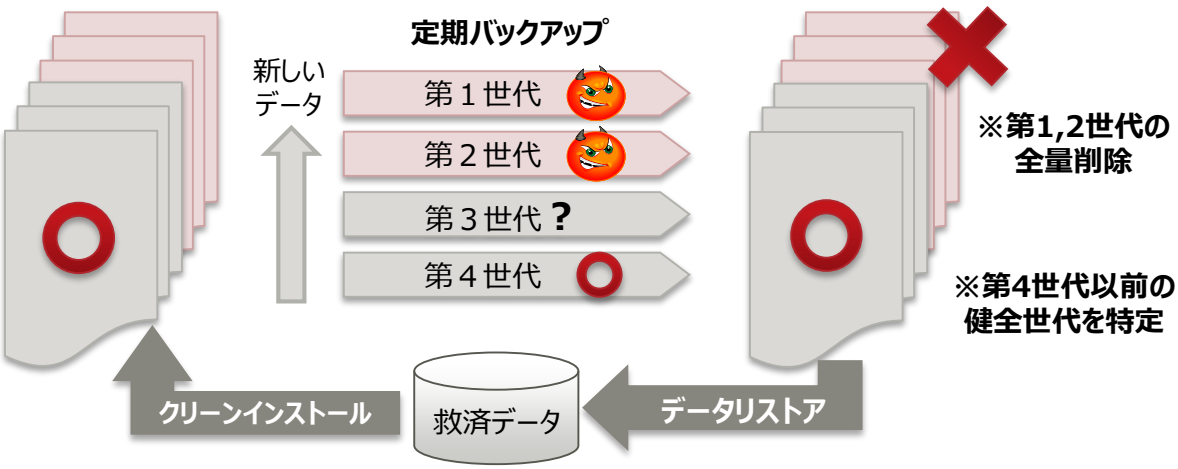
- ランサムウェアは、感染したPCだけでなく組織のネットワーク共有上のデータも暗号化する動作をします。仕分けした重要データの保存先も暗号化されるリスクがある為、バックアップソフト等を使用し、感染PCからアクセスできない場所（ネットワークから隔離されている）へのバックアップが求められます。
- ディザスタリカバリー観点のデータロスト防止策として、遠隔地（物理的に別の場所）へのバックアップも考慮します。

③ バックアップの世代管理でリスクを下げる

- ランサムウェア感染の発見が遅く、暗号化されてしまったデータをバックアップしてしまうリスクがあります。また、バックアップデータの中に、ランサムウェア自体が含まれていることも考えられます。
- 最新のデータだけでなく複数世代管理のバックアップを実施することで、感染の発見が遅れても希望するデータを復旧できる可能性が高くなります。
- より安全にリストアするべく、バックアップデータにマルウェアが含まれていないか確認します。

＊マルウェアには多くの亜種が存在するため、全てのマルウェアの検出は保証されません。

複数世代管理バックアップ

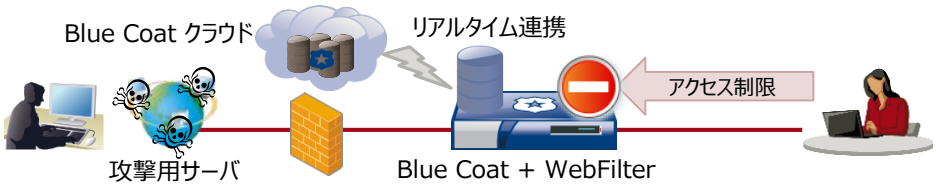


ランサムウェア対策ソリューションの提供

入口対策 **出口対策** **不正サイトのアクセスをブロック** ➢ 危険なWebサイトへの**アクセスを遮断**

例：Blue Coat ProxySG +WebFilter

■脅威が含まれているサイトやC&Cサーバ等、外部への不正なアクセスをリアルタイムでブロック
■C&Cホスト、1日限定ホストに関する世界中の共有情報を利用し、攻撃用サーバとの不正通信をブロック



入口対策 **出口対策** **標的型メール対策** **未知マルウェア対策** ➢ 未知マルウェアによる**侵入を検知**

例：Palo Alto Networks PAシリーズ

■仮想実行(sandbox)環境でプログラムを実行することで振る舞いベースでマルウェアを検知
迅速にシグネチャを生成し標的型攻撃への対応を強化

既知のファイルと比較 **シグネチャ自動生成**
サンドボックス環境で実行 **管理用Webポータル**

・PAシリーズがファイルをWildFireクラウドに送信
・新しいシグネチャをPAシリーズに配信、マルウェアフォレンジックを表示

内部対策 **未知マルウェア検知** ➢ 標的型攻撃で利用される**未知の脆弱性やマルウェアを検知・防御**

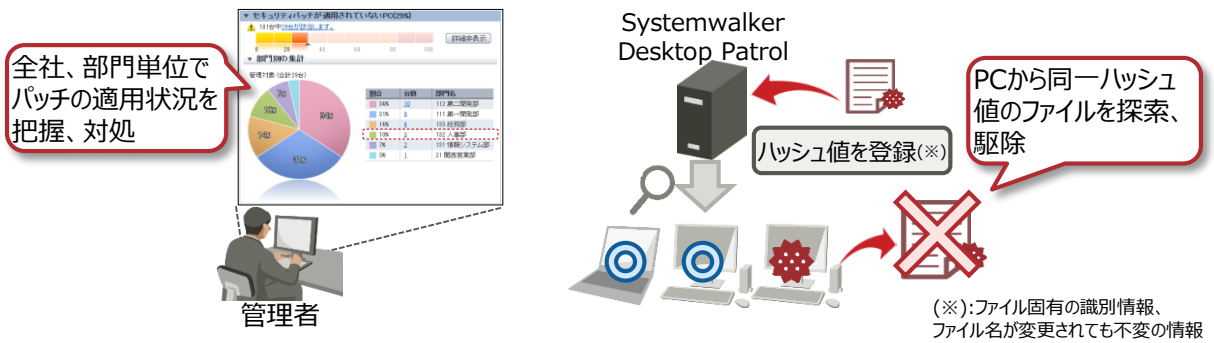
例：FFR yarai

■ウイルスパターンファイルに依存しないヒューリスティック・エンジンを活用し、未知のウイルスを検知して動作を阻止
■外部媒体(USBメモリ等)からの侵入も防御

脆弱性対策 **システムの脆弱性対策** ➢ ランサムウェアに利用される**脆弱性の管理**

例：Systemwalker Desktop Patrol

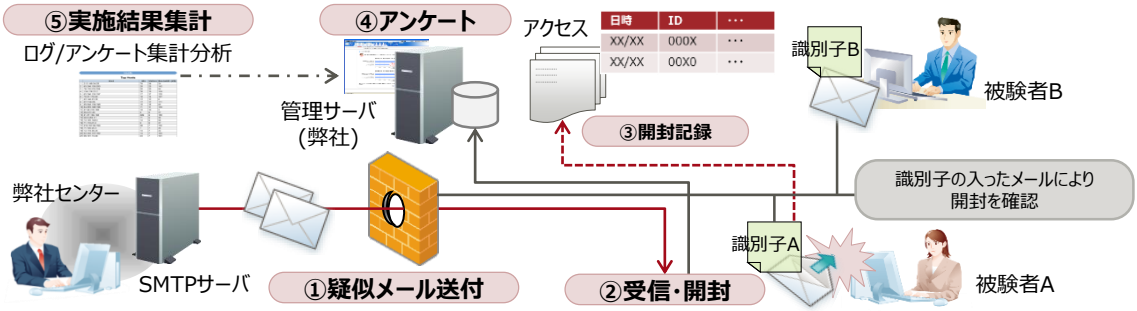
- Windowsのセキュリティパッチ、ウイルス定義ファイルが最新にアップデートされているか管理
- マルウェアのファイルと同一ファイルの所持状況を把握、警告メッセージ通知やファイルを隔離などの対処



人・組織の対策 **教育・訓練** ➢ 不審なメールに対する**職員のリテラシーを向上**

例：標的型メール攻撃訓練サービス

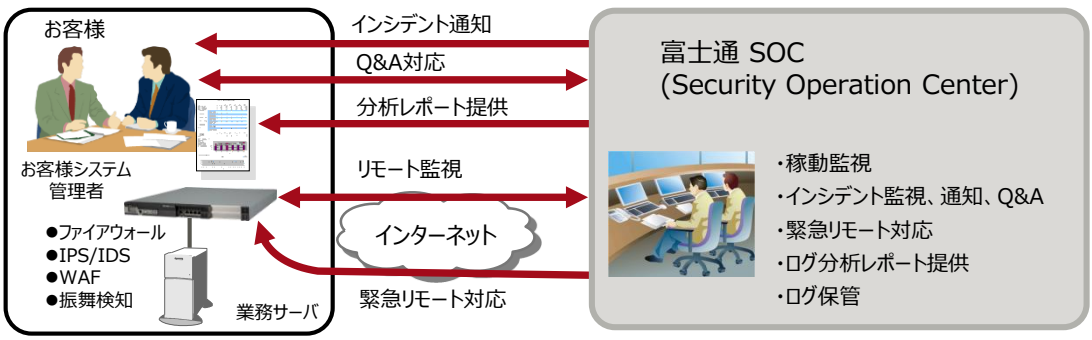
■訓練用に作成した疑似攻撃メールを対象者に送信し、添付ファイルの開封やURLのクリック状況を集計
■標的型メール攻撃を体験することで、的確な知識と判断能力を身につける体験型教育プログラム



監視・運用 **システム監視** ➢ **24時間365日**お客様のシステムに対する**不正アクセスを監視**

例：セキュリティ最適化サービス 不正アクセス監視モデル

■24時間365日、外部からの不正アクセス監視だけでなく、内部侵入したマルウェアの振る舞い監視にも対応



復旧対策 **データバックアップ** ➢ PC、ファイルサーバのシステム、**データの復旧**

例：Acronis Backup Advanced

■PCのシステム、データを、定期的にテープへ世代管理バックアップ
■万が一 ランサムウェアに感染して重要なデータが暗号化されてしまった場合、システムごと重要なデータをテープから復旧