

# 強靱化要件を実現するセキュリティ製品/サービス一覧



| 対象           | 区分      | 要件 |   |    | セキュリティ対策                             | 製品/サービス名  |
|--------------|---------|----|---|----|--------------------------------------|---|
|              |         | α  | β | β' |                                      |   |
| ネットワーク       | 入口/出口対策 | △  | ○ | ○  | 不正接続対策(シャド-IT管理)                     | McAfee MVISION Cloud  |
|              | NW分離    | ◎  | △ | △  | メール無害化                               | SYNCDOT SanitizeFilter<br>FENCE-Mail For Gateway                |
|              |         | ◎  | △ | △  | ファイル無害化                              | FENCE-Works   |
|              |         | △  | △ | △  | WEB無害化                               | アイソレーションゲートウェイサービス(Menlo)                                       |
|              |         | ○  | ○ | ○  | 画面転送                                 | VMware Horizon<br>Citrix Virtual Apps and Desktops              |
| クライアント・サーバ共通 | マルウェア対策 | △  | ◎ | ◎  | エンドポイント(EDR)                         | Cybereason EDR<br>Trend Micro Apex One                          |
|              | 脆弱性対策   | △  | ◎ | ◎  | 資産管理                                 | Systemwalker Desktop Patrol<br>FENICS CloudProtectリアルタイム可視化サービス |
|              | 情報漏洩対策  | △  | ○ | ○  | DLP                                  | McAfee Data Loss Prevention                                     |
| クライアント       | なりすまし対策 | ◎  | ◎ | ◎  | 二要素認証(生体認証)                          | AuthConductor V2  |
|              | 情報漏洩対策  | ◎  | ◎ | ◎  | 外部媒体制限                               | Systemwalker Desktop Keeper<br>FENCE-G                          |
|              |         | ○  | ○ | ○  | 内部不正防止                               | INSTANTCOPY   |
| 運用・管理        | ログ管理    | △  | ◎ | ◎  | SIEM                                 | Splunk  |
|              |         | △  | ◎ | ◎  | 業務システムログ管理                           | MICJETセキュリティログWATCHER   |
|              | 運用監視    | △  | ◎ | ◎  | SOC強化                                | 富士通グローバルマネージドセキュリティサービス   |
| 機器の廃棄等       |         | ◎  | ◎ | ◎  | データ消去                                | FUJITSU LCMサービス データ 消去サービス                                      |
| 体制強化・訓練等     |         | ◎  | ◎ | ◎  | CSIRTの設置、役割の明確化                      | CSIRT構築支援<br>CISOマネジメント支援サービス                                   |
|              |         | ◎  | ◎ | ◎  | 情報セキュリティ研修、標的型攻撃訓練、セキュリティインシデント訓練の受講 | 標的型メール攻撃訓練サービス<br>ダークウェブ調査サービス                                  |

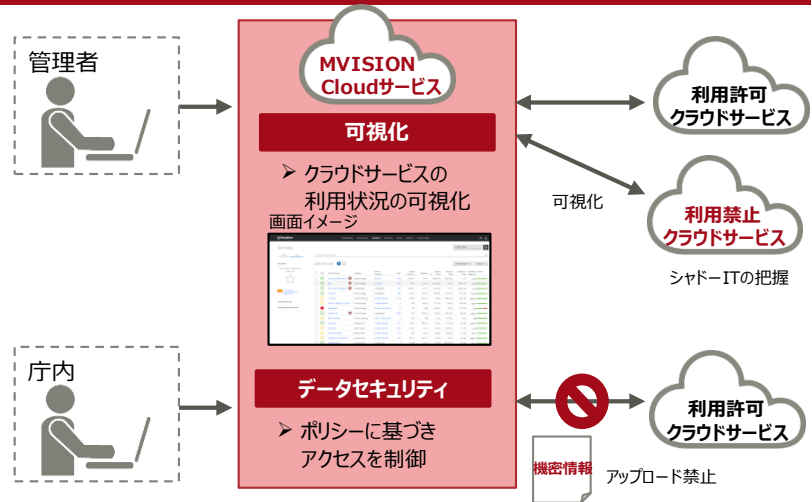
## 組織が許可していない外部接続先のサービスへのアクセスを監視、遮断

- ◆クラウドサービスへ機密情報の不正アップロードを防止
- ◆エージェントレス型の為、導入・運用が容易

### クラウドサービス利用の問題

- 庁内のクラウドサービスの利用状況が分からず、管理が出来ない。
- 許可していないクラウドサービス(シャドールIT)を利用している可能性がある
- 庁内、業者、お客様とのファイルの共有ミスや内部不正による情報漏えいのリスク

### MVISION Cloudでクラウド利用を統制



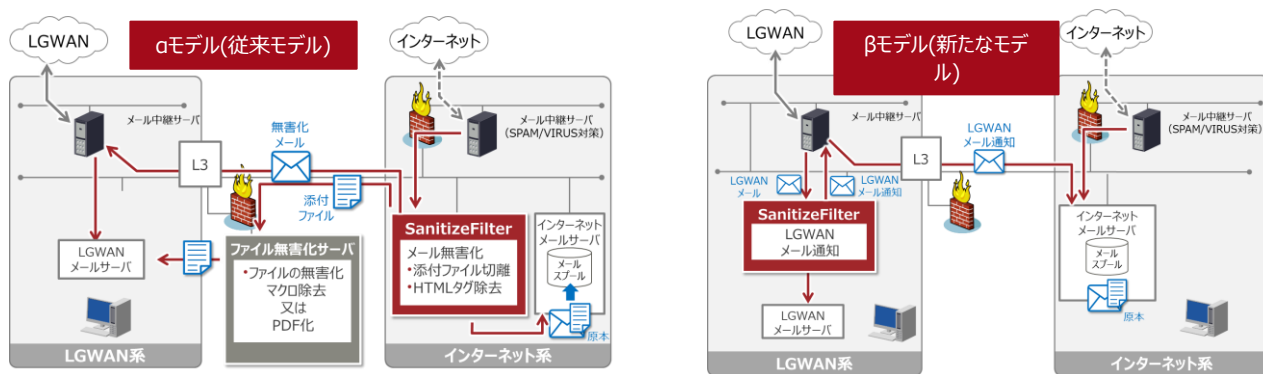
## インターネットメールによる標的型攻撃の脅威を無害化により軽減

### ◆特長 : 本文無害化と全ての添付ファイルを分離し攻撃を無害化

- \* HTMLメールのテキスト化、およびURLも含めたリンクの無効化と受信者への注意喚起
- \* 原本メールと無害化済メールをそれぞれ別メールサーバーへ配送可能
- \* βモデル(新たなモデル)に対応し、LGWANメール通知で利便性向上

### ◆他社差異化ポイント : 複数のファイル無害化ソリューションと連携が可能

- \* セキュアストレージSanitizeFilter連携、FENCE-Works連携、File-Zen連携



※インターネット系にLGWANメール受信を通知

## メールを「無害化」することで多層防御の入口を一層強化

## 受信メールを無害化し、標的型メールによるマルウェア感染を防止

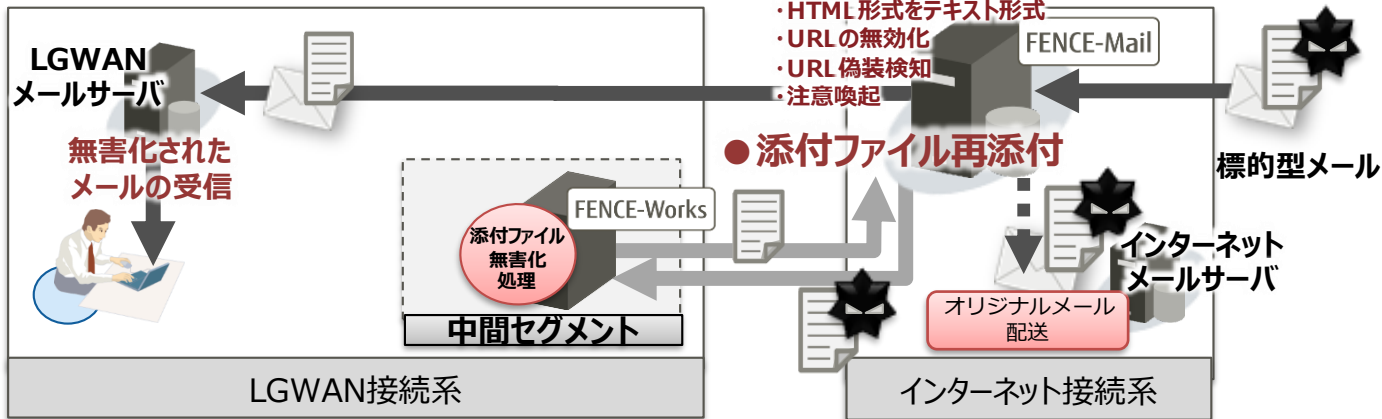
- HTML形式で書かれているメールをテキスト形式に変換し、URLの無効化、URL偽装検知と注意喚起で受信メールを無害化
- ファイル無害化製品「FENCE-Works」と連携し、添付ファイルを無害化し、メール本文に再添付

(2021年4月提供予定)

### ●メール本文の無害化

- ・HTML形式をテキスト形式
- ・URLの無効化
- ・URL偽装検知
- ・注意喚起

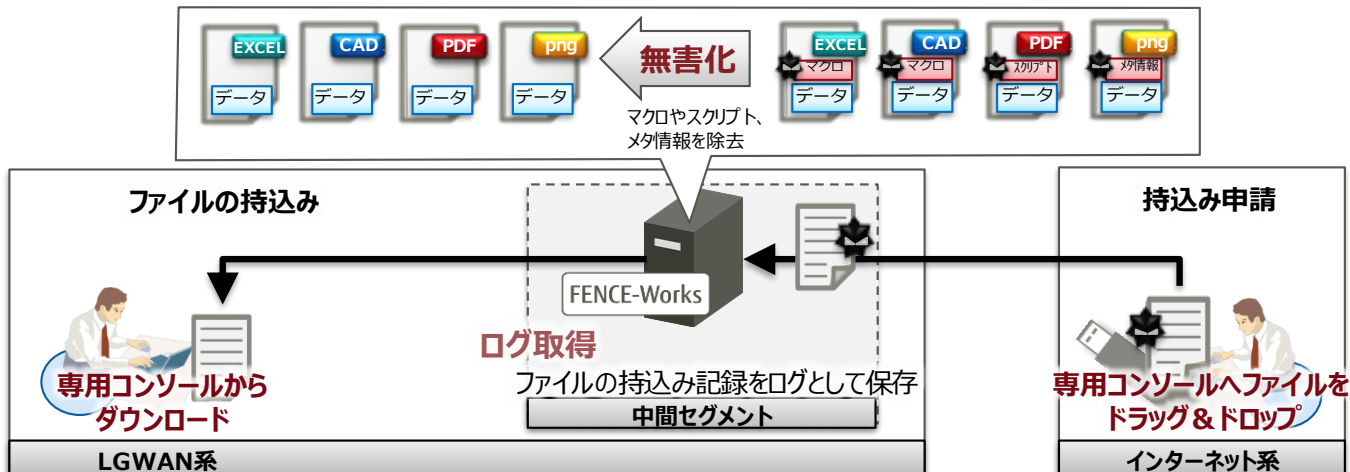
### ●添付ファイル再添付



メール受信対策「無害化」とメール送信対策「誤送信」を1台で実現

## LGWAN系に持込むファイルを無害化し、マルウェアの感染を防止

- ◆ 簡単操作でファイルの危険因子を自動除去し、  
安全なデータとしてLGWAN系に持ち込むことが可能(無害化対象ファイル※)
  - ・Active Directory連携によるSSOの実現で持込み申請時の手間や時間を軽減
- ◆ 情報の持ち出し対策(個人情報チェック・自動暗号)も標準装備



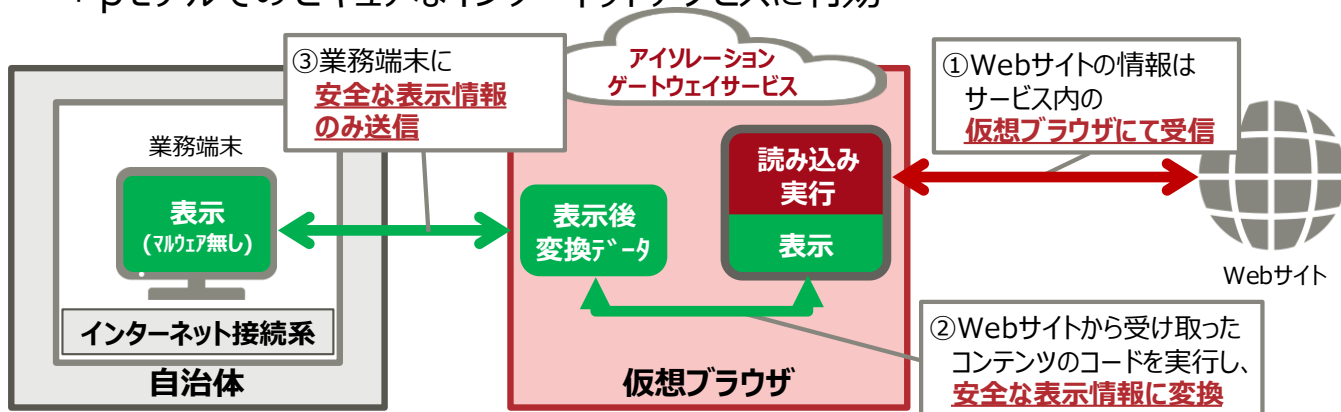
※無害化対象ファイル：Microsoft® Word/Excel®/PowerPoint®, 一太郎®, PDF、画像ファイル(jpeg/png/gif/tiff/bmp)、AutoCAD® (DXF/DWG)

## メール対策製品との連携により、自動で添付ファイルの無害化を実現

## ブラウザ経由のマルウェア侵入を完全防御

### ◆インターネット接続専用端末を用いず、安全にインターネット接続

- \* アイソレーションは、全てのWEBサイトコンテンツを仮想ブラウザ上で安全な情報に変換業務端末へのマルウェア侵入を防ぐ技術
- \* βモデルでのセキュアなインターネットアクセスに有効



### ◆Menlo SecurityをSaaSで提供、24時間365日サポート

- \* 常に最新バージョンを提供



本サービスのWeb無害化機能は「Menlo Security」により実現

安全なインターネット接続環境を短期導入で提供

画面転送： VMware Horizon  
Citrix Virtual Apps and Desktops

FUJITSU

富士通を選んでいただく価値  
豊富なラインナップ

ライセンス売上  
国内No1

## VMware製品

クライアント仮想化ソフトウェア

VMware Horizon

## Citrix製品

クライアント仮想化ソフトウェア  
Citrix Virtual Apps  
and Desktops

### ◆富士通はクライアント仮想化市場においてシェアNo.1

※IDC Japan, April 2019「国内クライアント仮想化市場シェア、2018年：インテリジェントワークスペース実現へのロードマップ」(JPJ44015419)より

### ◆富士通グループ8万人へのVDI大規模導入実績

### ◆オンプレ型／サービス型とユーザーニーズに合わせた提供が可能

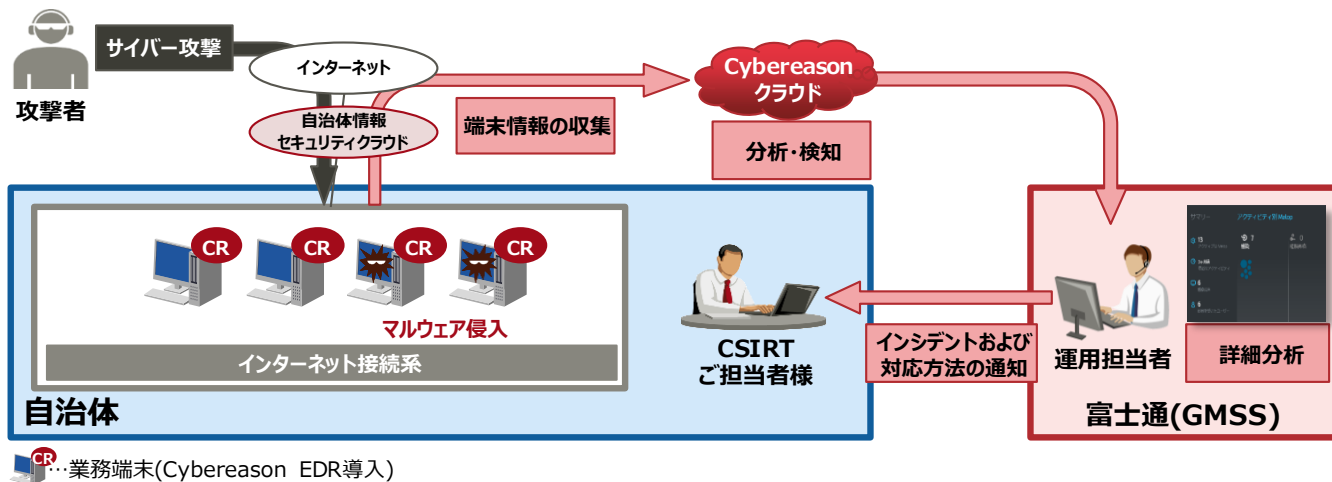
全てのお客様のご要望にお応えします

## 国内シェアNo.1の実績と安定したエンドポイントセキュリティ

### ◆多層防御をすり抜けた、未知かつ高度なサイバー攻撃に対応

\*「Cybereason EDR」は、EmotetやWannaCryのような未知のマルウェアの侵入を早期検知し、業務端末の被害を最小化

### ◆EDRに特化したセキュリティ運用部隊が24時間365日対応



国内トップクラスの運用サポート(GMSS)でβモデルの採用を支援



# エンドポイント(EDR) : Trend Micro Apex One

従来EPPのオプションとして、手軽にEDR機能を導入可能

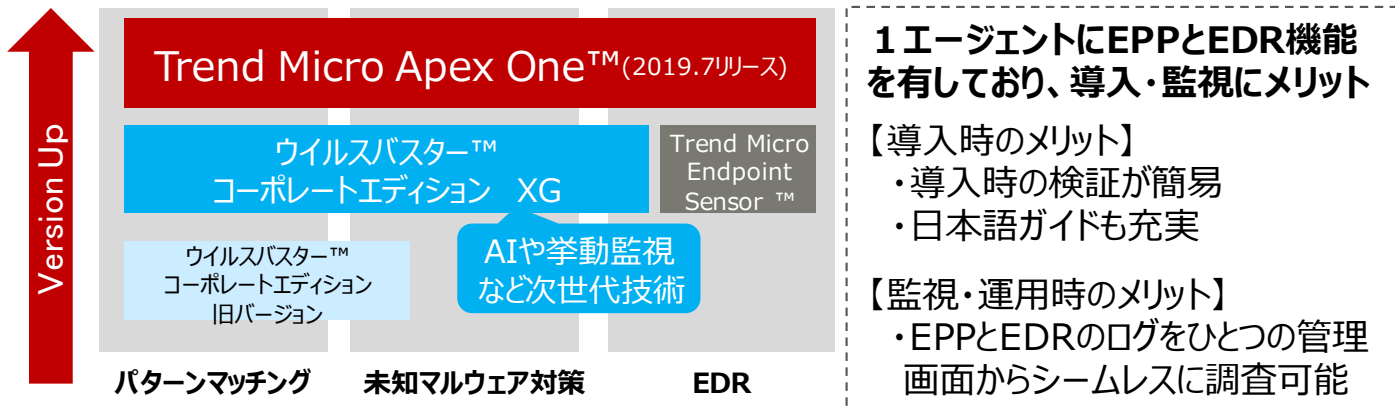
◆ **トレンドマイクロは自治体・官公庁・教育機関の  
エンドポイント市場で10年連続国内シェアNo.1※1を獲得**

※1 IDC Japan, 法人向けエンドポイントセキュリティー 2009-2018年連続(2019年度上半期も45.3%でNo.1)

◆ **同社製品の実績豊富なエフサスで運用監視サービスを提供※2**

※2 センターとの回線接続が必要となります

<既存Corp顧客はVerUP対応でApexOneに移行可能>



トレンドマイクロご利用ユーザには、VerUpでEDRが利用可能

# 資産管理 : Systemwalker Desktop Patrol

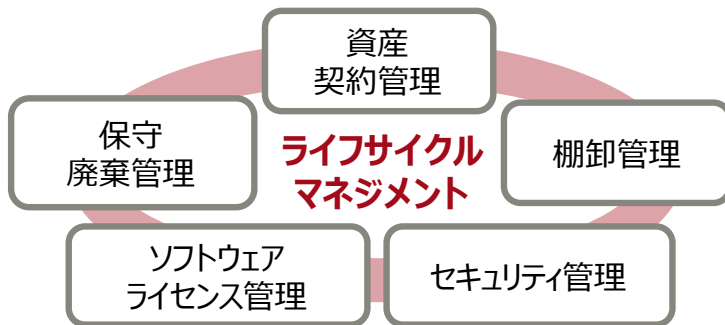
## ICT資産の資産管理とソフトウェア脆弱性対策を実現

### ◆ 庁内の端末状況を把握し、一斉管理が可能

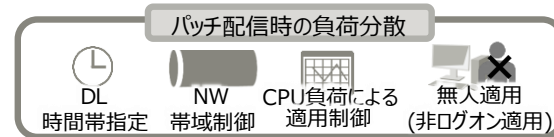
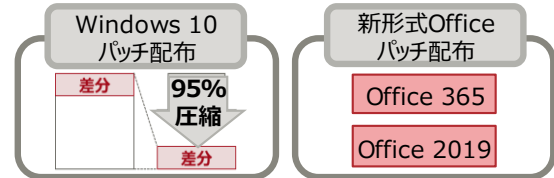
\* 管理端末のソフトウェア導入状況を管理し、セキュリティパッチ配布を一括管理

### ◆ Windows 10、Officeの一元更新管理が可能

\* WSUSサーバなくても、Windows 10、Office 365、Office 2019の一元更新管理の管理が可能



### 対応が遅れがちな最新Microsoft製品のパッチ管理に対応



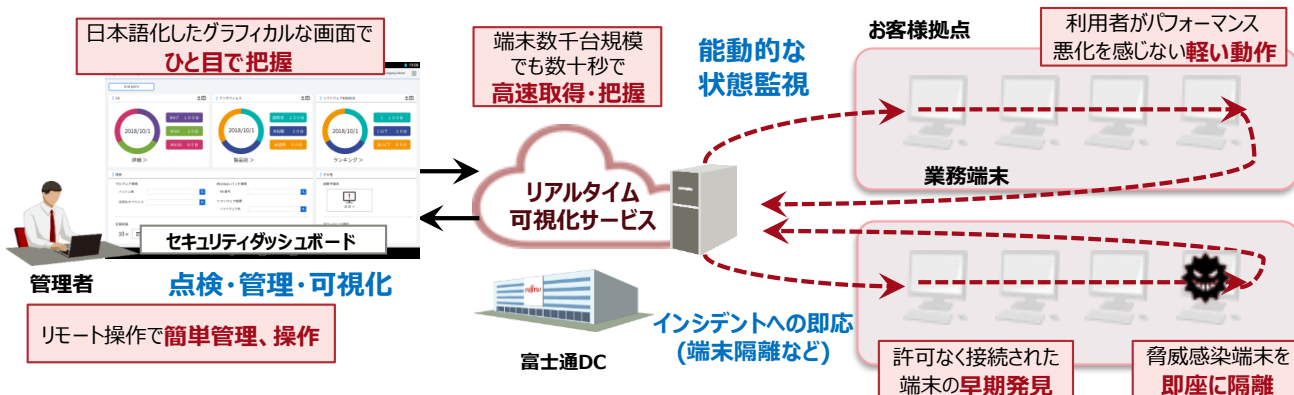
## 業務端末に潜むセキュリティリスクへ衛生管理で対策

### ◆セキュリティ対策状況の特定により、脅威に強い環境を維持

\* 管理外端末を含めたすべての端末管理により、庁内の脆弱性を早期に発見。  
インシデント発生前に脆弱性を即時対応(=衛星管理)

### ◆国内初、「Tanium Endpoint Platform」をサービス提供

\* 大量のエンドポイントの状態を即座に可視化出来る「Tanium Endpoint Platform」のサービス提供により、端末台数に合わせた提供が可能



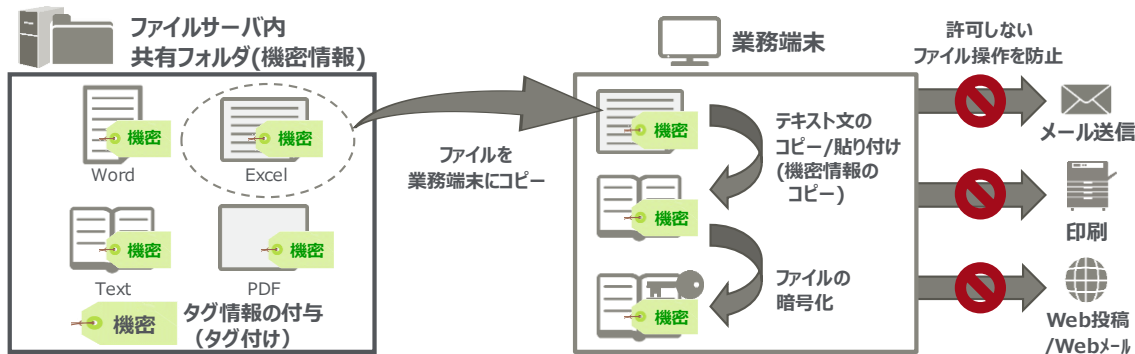
## マルウェア感染等による機密情報の漏えいを防止

### ◆ 機密情報を対象とした確実な保護

\* 機密情報を監視して操作制御する為、マルウェア感染等による情報漏えいを防止

### ◆ ファイルが暗号化されても監視し情報漏えいを防止

\* ファイルのコピーだけでなく、テキストの貼り付けや暗号化後も制御が可能



**DLP (Data Loss Prevention)** とは、

機密情報を特定し、対象のファイル操作制御する対策。マルウェア (EMOTET等) による情報漏えいを防止  
機密情報を直接監視する為、対象ファイルを1つ1つチェックする必要がなく、運用が容易

## 庁内に存在する機密情報の一元管理が可能

# 二要素認証(生体認証) : AuthConductor V2

## 2016年度に引き続き、「非接触」で認証可能な手のひら静脈

### ◆自治体様、生体認証シェア1位

- \* 「物(カード)の管理」にとらわれない生体認証が推奨
- \* 高い認証精度により、ストレスフリーを実現

其他方式の課題例 **指紋認証** : 1割程度認証しづらい人が発生、接触型のため抵抗感が強い  
(ユーザーコメント) **顔認証** : 誤認証の発生、カメラを利用する他システム(オンライン会議等)との競合

### ◆つながる「手のひら」で様々なシーンへ

- \* 導入済団体は、**静脈データ**の移行が容易
- \* 端末ログオンに限定しない、様々なシーンへ



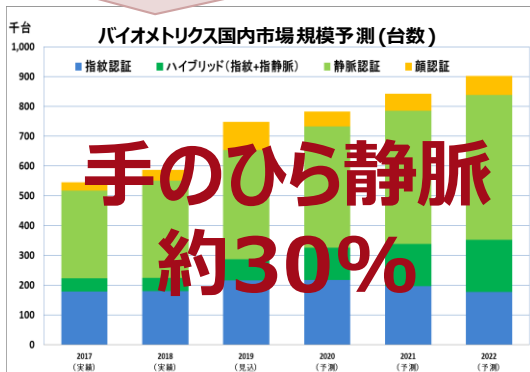
認証印刷

入退管理装置

マイナンバーカード  
読取対応

勤怠打刻  
(IPK連携等)

法人セキュリティ向け生体認証は依然として**静脈**の採用が多い



出典：富士経済「2019セキュリティ関連市場の将来展望」

# 外部媒体制限：Systemwalker Desktop Keeper **FUJITSU**

## 外部記憶媒体による情報の持ち出し管理を徹底

### ◆ 利用事務系端末からの情報持ち出しの禁止や制限を実現

- \* 外部記憶媒体等の持ち出し制御を一元管理可能。  
印刷管理やBluetooth接続などデバイス以外の漏洩もシャットアウト

### ◆ 外部媒体制限以外にも操作ログ記録機能を実装



端末における情報持ち出し管理をオールインワンで実現

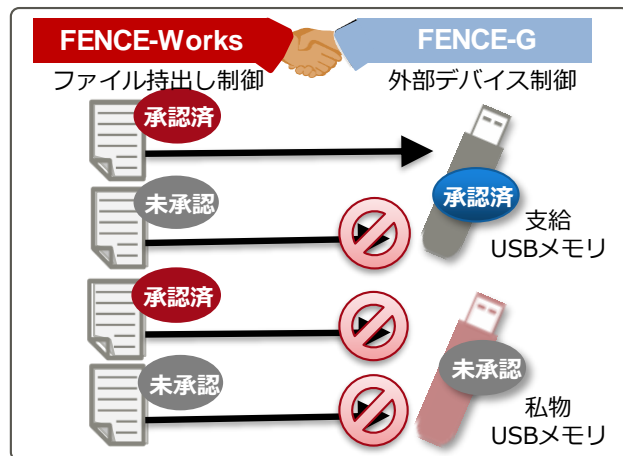
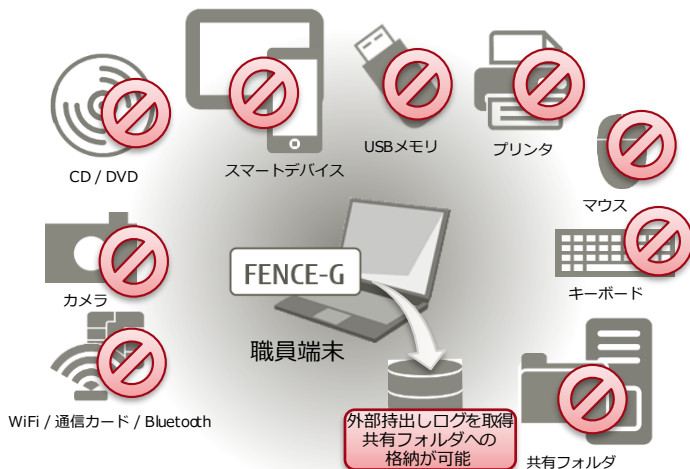
## 外部デバイスへの情報持出し制御を安価かつ容易に実現

### ◆サーバ不要のスタンドアロンでデバイス制御が可能

\* 利用事務系端末からの情報漏洩を低コストでシャットアウト

### ◆「FENCE-Works」と連携し、ファイル単位での持出し制御が可能

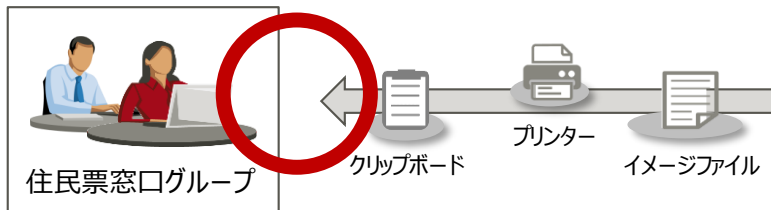
\* 外部デバイス/ファイル単位での運用フローに則った持出し制御を実現



ファイルレベルでの持出し制限でワンランク上のセキュリティ対策を実現

# 内部不正防止：INSTANTCOPY

故意、過失問わず画面キャプチャーを抑止し、内部からの情報漏えいを防ぐ



| No | 個人番号         | 氏名   |
|----|--------------|------|
| 1  | 111111111111 | 藤田信長 |
| 2  | 222222222222 | 豊臣秀吉 |
| 3  | 333333333333 | 徳川家康 |
| 4  | 444444444444 | 伊達正宗 |
| 5  | 555555555555 | 上杉謙信 |
| 6  | 666666666666 | 武田信玄 |
| 7  | 777777777777 | 足利義昭 |

マイナンバー等の指定した**特定文字列を画像から検知!**(当社独自)

新潟県新潟市  
山梨県甲府市  
京都府京都市

表示 閉じる

抑止例：マイナンバーを含む画面



## 情報の持ち出しを阻止

- ✓ マイナンバーなどの個人情報を含む**画面キャプチャーを抑止**
- ✓ **権限(グループ)**に応じた、**抑止制御**が可能

## 管理者によるキャプチャー操作の監視

- ✓ 抑止対象をキャプチャーした場合、**管理者にメッセージ通知**
- ✓ いつ、誰が、どの画面をキャプチャーしたか**確認可能**



## タイムスタンプ付きのあらゆるログを一元管理

### ◆リアルタイムの状況把握・分析と障害時の迅速なログ解析が可能

\* インターネットからの高度なサイバー攻撃をセキュリティ機器単独ではなく、複数のログを相関分析することで検知し、早期対処を実現

### ◆富士通の導入実績を元にした各種ツールにより、最適な環境を整備

\* 富士通が独自に提供している各種ツールを適用することでセキュリティ・リテラシーの低い職員でも効率的にCSIRTを運用することができ、導入コストも削減

|                      |  |
|----------------------|--|
| セキュリティ               | <ul style="list-style-type: none"><li>✓ サイバー攻撃対策</li><li>✓ 内部統制対策</li><li>✓ SOC/CSIRT運用</li></ul>                      |
| コンプライアンス             | <ul style="list-style-type: none"><li>✓ PCI DSS/J-SOX等セキュリティ基準達成</li><li>✓ 監査対応</li><li>✓ 迅速なインシデント調査・定期レポート</li></ul> |
| インフラ<br>マネジメント       | <ul style="list-style-type: none"><li>✓ デバイス・アプリ毎の性能監視・レポート<br/>-ネットワーク、サーバ、ミドル、DB等</li><li>✓ 既知の問題のアラート</li></ul>     |
| Webアクセス解析<br>BI etc. | <ul style="list-style-type: none"><li>✓ クラウドサービスの可視化</li><li>✓ センサーデータの集計</li><li>✓ アノマリー分析、統計・未来データ予測</li></ul>       |

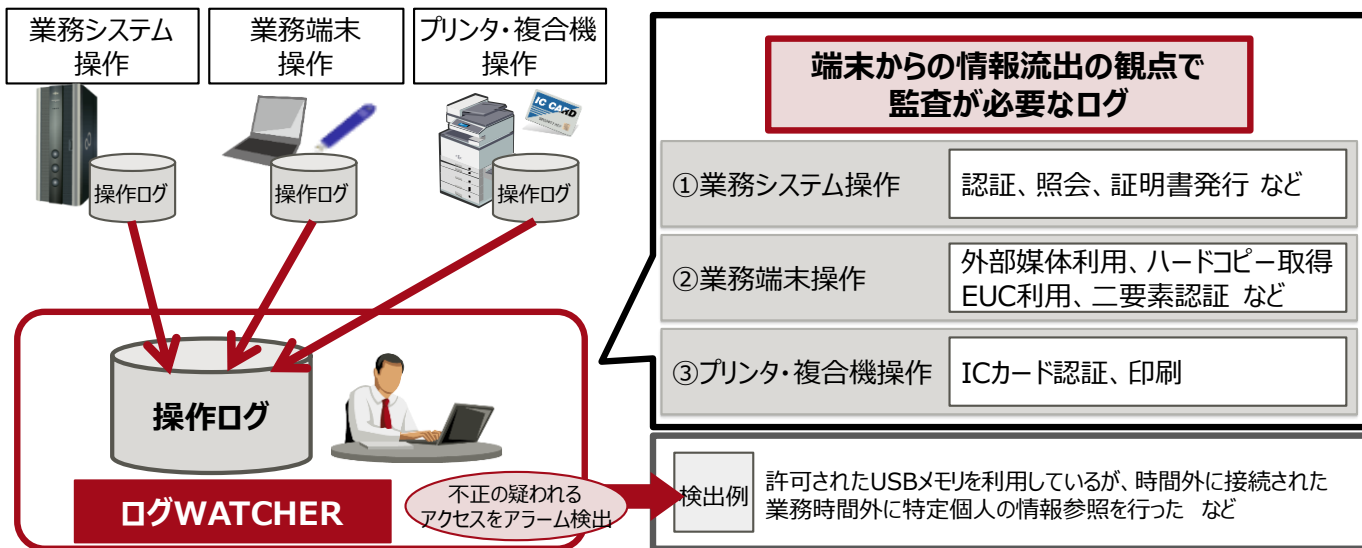


# ログ管理(業務システムログ管理) : MICJETセキュリティログWATCHER

## ログの分析機能により不正抑止と内部監査の負荷を大幅に軽減

### ◆ 業務システムに特化した監査機能を提供

- \* 業務システムと端末に係る操作ログを収集し、個人情報のアクセス状況を可視化
- \* 不正が疑われるログを自動検出し、内部監査を効率化



# 運用監視（SOC強化）

：富士通グローバルマネージドセキュリティサービス(GMSS※)

FUJITSU

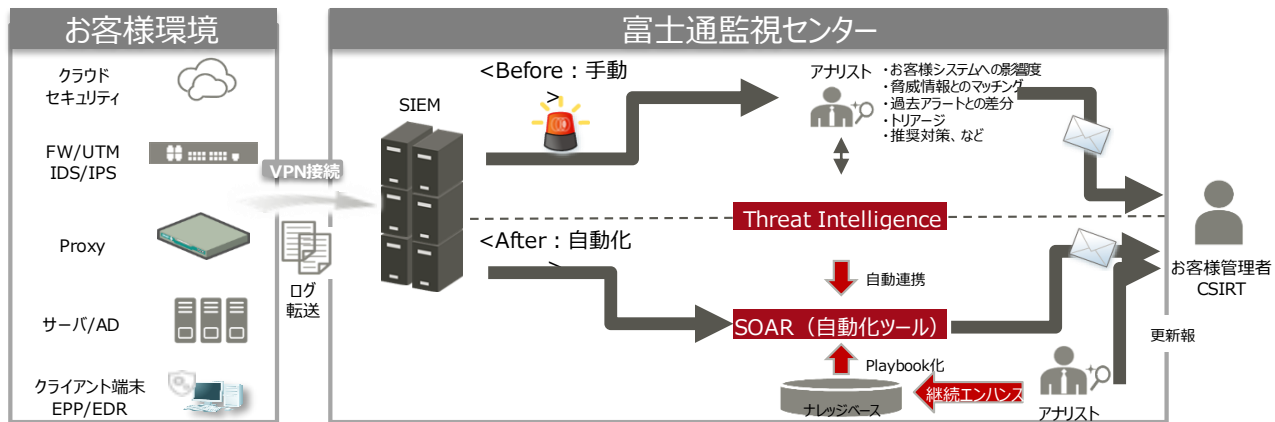
## セキュリティ運用を富士通が24時間365日トータルサポート

### ◆迅速な侵入検知/初動対応（検知力）

\* 経験から得られた何百もの運用ルール/アナリスト知見をPlaybook化  
自動分析、解析により、お客様への第一報を大幅短縮

### ◆ワンストップダッシュボードを実現

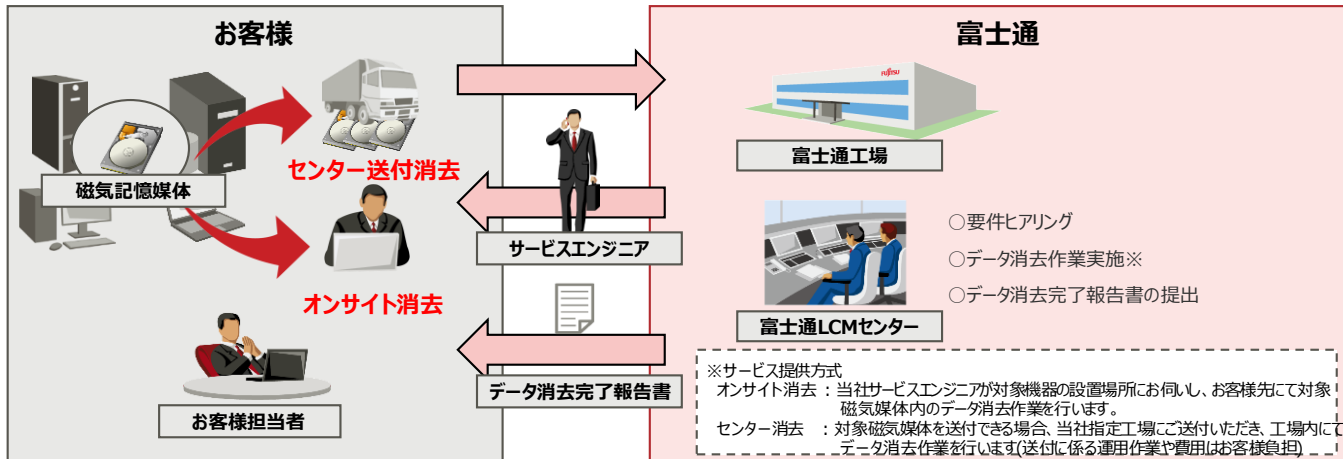
\* インシデント状況をリアルタイムに反映し、密でセキュアなコミュニケーションを実現



※GMSS (Global Managed Security Service)

## 迅速且つ確実なデータ消去によりデータ流出を防止

- ◆全国8,000名のサービスエンジニアがお客様先を訪問し、目の前で消去作業を実施
  - \* 消去対象製品を富士通工場にご送付頂く「センター送付消去」でのサービス提供も可能
- ◆パソコン、サーバ、ストレージまで富士通の独自ツールにより確実な消去を短時間でご提供
  - \* お客様のご要望により、DoD(米国防総省準拠方式)、NSA(米国家安全保障局準拠方式)といった海外のデータ消去規格にも対応
- ◆消去作業の完了後、「データ消去完了報告書」を提出する事により、作業内容をご報告



## 次期ガイドラインでは役割を明確化しなければならないと位置づけ

### ■ 自治体におけるCSIRTとは

2002年の住基ネットの本稼働に合わせて各自治体で設置が義務化。  
2016年に開始したマイナンバー制度により、強化対応要件でその体制強化が進められている。

### ■ CSIRT体制の現状

- 主となる部門と関連部門において、**役割分担や最適な権限の付与が出来ていない**  
(例：総務部門と情報システム部門の役割分担など)
- セキュリティ事故発生時の**対応計画・対応ルールが明確になっていない**

【抜粋】「地方公共団体における情報セキュリティポリシーに関するガイドライン」より

#### ■ CSIRTの設置・役割

情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生状況のとりまとめ、CISO・CIOへの報告、報道機関等への通知・公表、関係機関との情報共有など、情報セキュリティインシデントに関するコミュニケーションの核となる体制を、危機管理等の既存の枠組み等を活用するなどして構築する必要がある。

### ■ CSIRT構築支援内容

| 作業項目 |          | 実施内容  |
|------|----------|---|
| 企画   | 現状把握     | ・既存ルール等の把握                                  |
|      | 基本構想の検討  | ・基本方針・ミッション案の決定<br>・取扱うインシデントの決定            |
|      | サービスの検討  | ・CSIRT対象範囲の決定<br>・サービス内容の決定<br>・CSIRT定義書の作成 |
|      | 社内外体制の検討 | ・CSIRT/SOC役割分担表の作成                          |
|      | リソースの検討  | ・インシデント対応フローの作成<br>・判断基準の作成                 |
| 構築   | ドキュメント整備 | ・CSIRTマニュアルの作成                              |

## セキュリティインシデント発生時に即時対応できる組織作りが必要

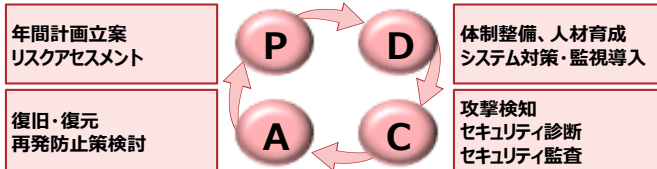
## CISOの補佐役として、組織のセキュリティ対応力強化をサポート

### ■ セキュリティ専門家がセキュリティマネジメントサイクルを支援

\* 国から求められるセキュリティ体制強化においてCISOの担う役割は重要かつ必須  
富士通がCISOの補佐役としてセキュリティマネジメントサイクルを支援

### ■ 教育や訓練ではなく、業界初のCISO支援サービスを提供

#### セキュリティマネジメントサイクル



#### CISOマネジメント支援サービス

- 定例会の実施(月1回)
- 業種セキュリティ動向の情報提供
- 役員会等での情報発信の支援

マネジメントサイクル  
年間計画テンプレート

情報提供  
業種、政府同行解説

アドバイス  
経営報告レビュー

専門サービスご紹介

#### <定例会の議題(例)>

- ① セキュリティマネジメント
- ② 年間活動計画
- ③ 情報セキュリティ研修と自己点検
- ④ 情報セキュリティ監査計画
- ⑤ 職員向け情報セキュリティ研修
- ⑥ 中間活動報告
- ⑦ 情報セキュリティ監査
- ⑧ 情報セキュリティの動向
- ⑨ 自己点検結果の振り返り
- ⑩ 情報セキュリティ監査の振り返り
- ⑪ 年間活動報告
- ⑫ 次年度活動計画

高度セキュリティ専門家がセキュリティマネジメントへのアドバイスを実施

## 急増する標的型メール攻撃による情報漏えいを予防・軽減

### ■ 標的型攻撃メールとは

受信者に関係が深い話題のメールを送り、添付ファイルや外部URLにアクセスさせてマルウェアに感染させる。

### ■ 標的型攻撃メールの特徴

|        | 従来型ウイルスメール                        | 標的型攻撃メール                |
|--------|-----------------------------------|-------------------------|
| 攻撃対象   | セキュリティ対策の不十分なパソコン                 | 特定の組織の情報                |
| 宛先     | 不特定多数                             | 少数の組織                   |
| 記述言語   | ほとんど英語                            | 日本語                     |
| 感染後の症状 | 何らかの異常な症状<br>・処理が遅い<br>・シャットダウンする | 特に気付くような症状なし            |
| 話題     | 誰にでも関係のある話題                       | 受信者に関係が深い話題             |
| 送信者    | 知らない人                             | 信頼できそうな組織や人を詐称          |
| 添付ファイル | 実行形式 (EXE)                        | 文書形式<br>※PDF,Word,Excel |
| ウイルス対策 | 大半は検知                             | ほとんど検知不可                |

### ■ 効果

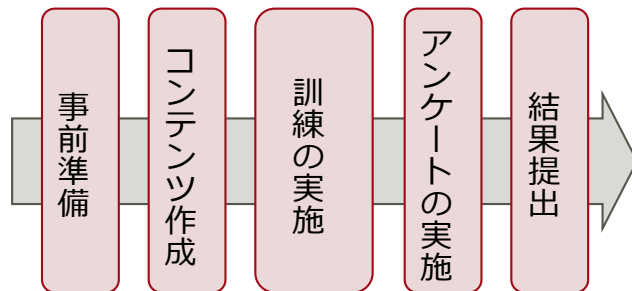
#### セキュリティ意識の向上

標的型メール攻撃の危険性を従業員に注意喚起し、耐性を強化・維持することが可能。

#### 現状に則したセキュリティ対応策の検討が可能

実際の訓練結果を詳細に分析することで、より効果的なセキュリティ教育の立案が可能。

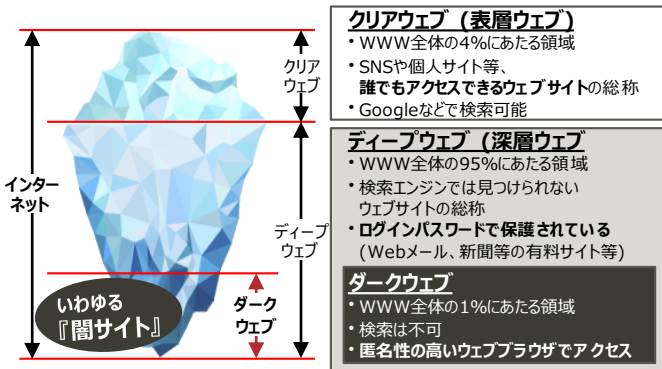
### ■ 訓練実施の流れ



攻撃の疑似体験によりセキュリティ意識や不審メールへの注意力向上

## 脅威情報を収集・分析し、予防的なインシデント対策を支援

### ■ダークウェブとは



### 【ダークウェブ上で取り扱われる情報例】

|             |  |
|-------------|--|
| 漏えいした機密情報   | <ul style="list-style-type: none"> <li>職員のアカウント/パスワード</li> </ul>                           |
| セキュリティの脆弱情報 | <ul style="list-style-type: none"> <li>Webサーバの脆弱性</li> </ul>                               |
| サイバー攻撃計画    | <ul style="list-style-type: none"> <li>攻撃者によって作られたバックドア情報</li> <li>DDoSターゲットリスト</li> </ul> |
| フィッシング関連情報  | <ul style="list-style-type: none"> <li>サイバー攻撃の予告</li> </ul>                                |
| ブランド関連情報    | <ul style="list-style-type: none"> <li>ふるさと納税等を装った偽装サイト情報</li> <li>市長を騙ったSNS情報</li> </ul>  |

### ■自治体が抱える悩み

- アカウントが漏えいして乗っ取りの危険は無いのか
- 偽装サイトなどでフィッシングに悪用されていないか
- サイバー攻撃のターゲットになっていないか

### ■効果

**脅威に繋がる情報を把握することで早期対応が可能**  
 ダークウェブ上の情報から関係する脅威を把握し、対応が可能

**最適なセキュリティ改善の立案が可能**  
 調査の結果、即時対応が必要な対処や中長期的な改善支援

### ■調査レポート例

**データベースファイルのダークウェブ上での売買**

情報ソース: 公開日: 2018/05/16  
 http://xxxxxx.xdss.com/idsaasafidfa

| アカウントID        | 関連アカウント            | タイプ  | 掲載エリア | 対応   |    |
|----------------|--------------------|------|-------|------|----|
| 相連データベースファイルの漏 | Sample xxxxx, Inc. | 情報漏洩 | High  | High | 推奨 |

注 (DATA LEAKAGE)


データベースファイルの詳細情報を元に、実在するデータベースファイルかどうかを確認いただくことを推奨します。該当するデータベースファイルの存在を確認した場合、該当サーバのセキュリティチェック状況や管理者への状況ヒアリング等実施し、情報の事実確認を推奨します。状況によっては、法執行機関への相談やデジタルフォレンジックによる原因調査等をおこなうことも視野にいれて対応をご検討ください。

検知したアラートを分析し、脅威のタイプや危険度に応じたスコアリングを提示 (0~3の4段階)

発見した脅威への対応策を提示

潜む脅威を把握することでより効果的なセキュリティ提案が可能





**FUJITSU**

shaping tomorrow with you