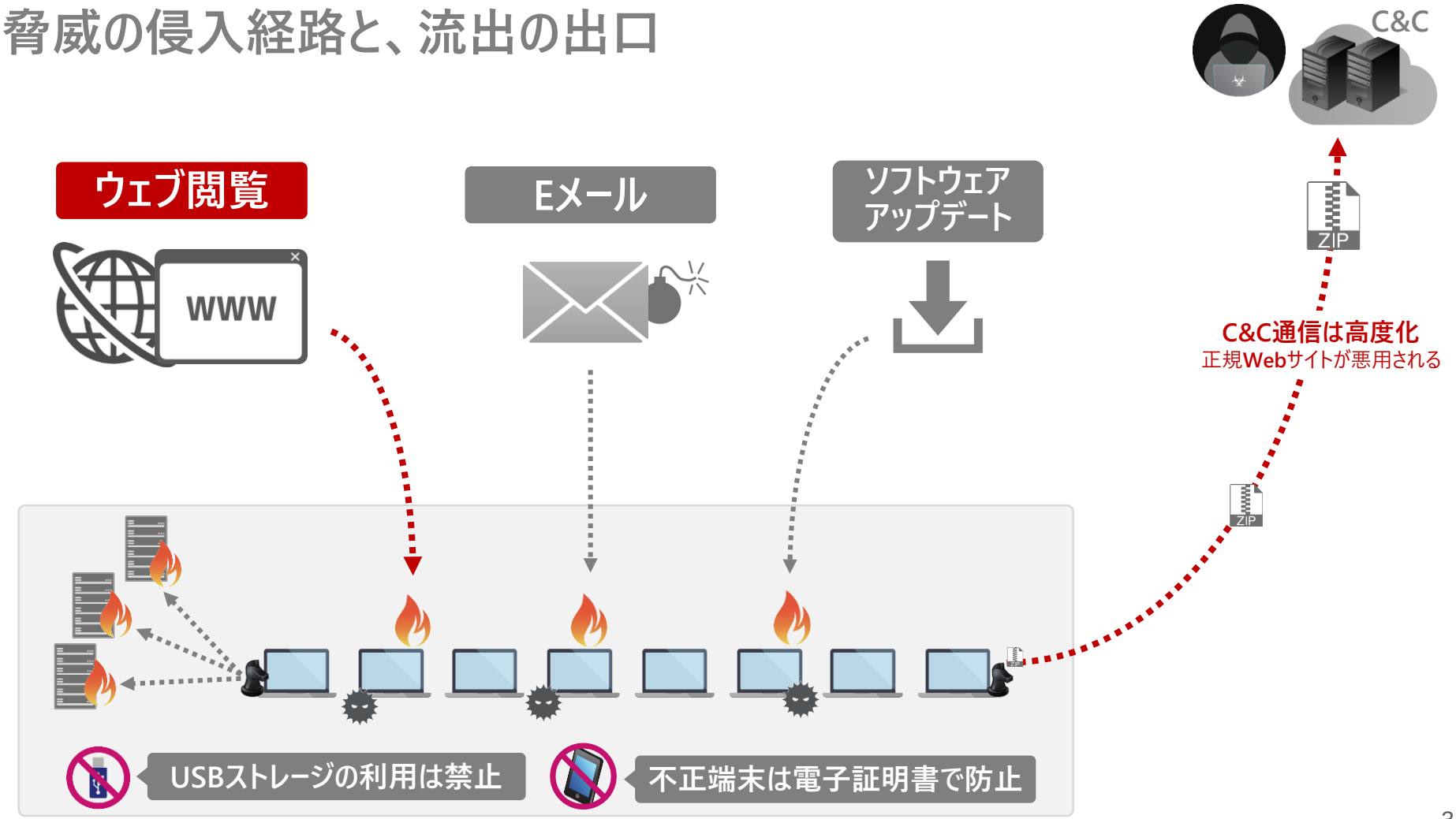
Windows 10 移行に併せた、インターネット分離の最適手法

- ウェブ閲覧と、ウェブ閲覧以外の脅威対策も実施する

V5-1811

目次

脅威の侵入経路と、流出の出口



“インターネット分離” 導入方式の変遷

VDI・SBC（仮想PCの画面転送）

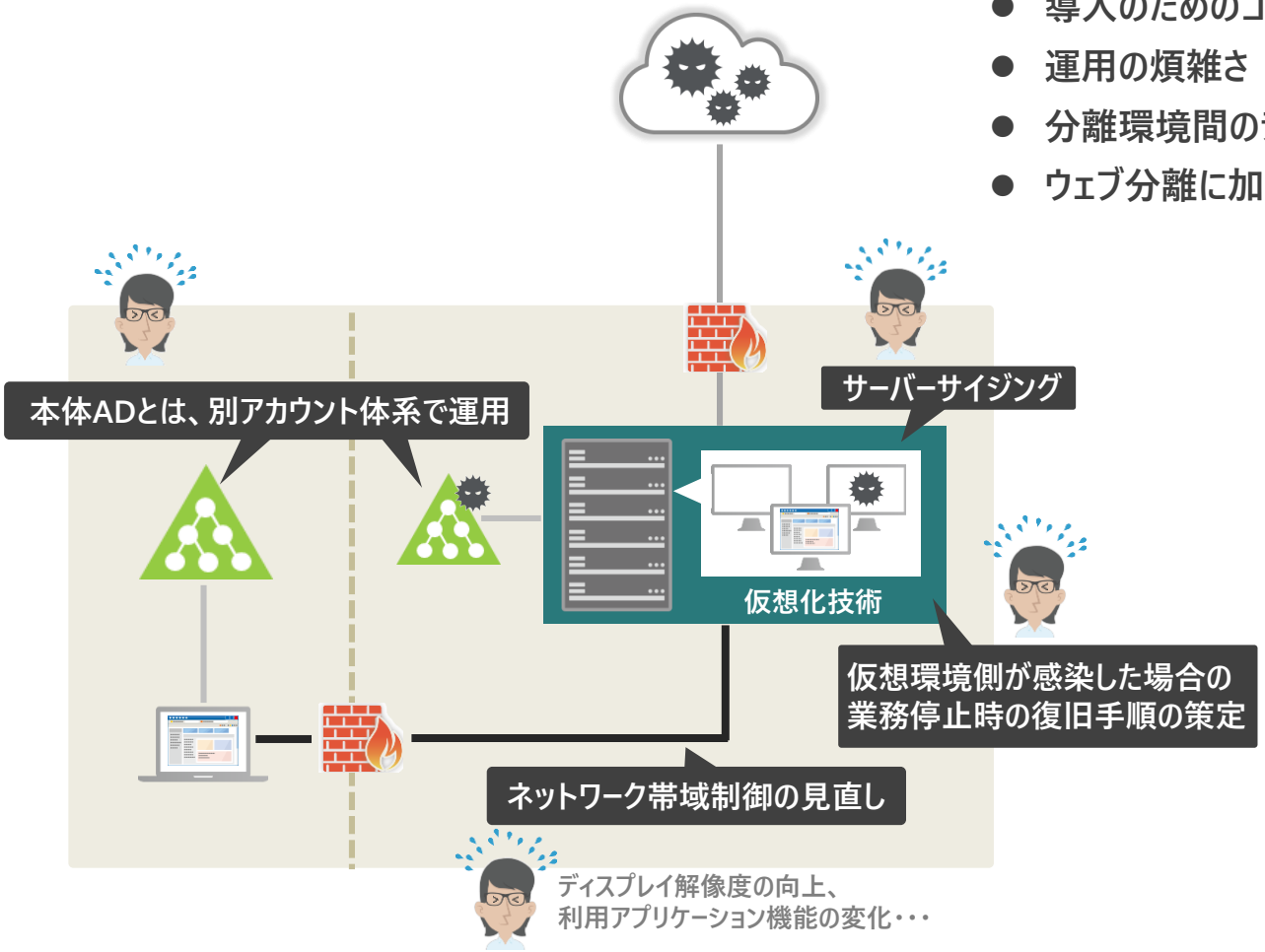
- ✓ 端末を2台用意しなくとも、仮想技術を利用すれば、業務LANとインターネットLANを分離出来るという発想が生まれた
- ✓ セキュリティを強化しなければならないメガバンクや重要インフラ企業には採用が進んだ一方、**コストと運用面の課題から採用が見送られるケースもあった**

Web画面転送方式

- ✓ Webの画面転送方式に特化することで、コストを抑えながら、仮想デスクトップに近いセキュリティ効果が見込めるようになった
- ✓ **Webブラウジング全般のレスポンスが悪いため、利用者からの不満が多く上がり、帯域やシステムの見直しを迫られるケースが出てきている**

従来方式の課題

- 導入のためのコスト
- 運用の煩雑さ
- 分離環境間のデータの受け渡し
- ウェブ分離に加え、メール分離・無害化の検討



“インターネット分離” 導入方式の変遷

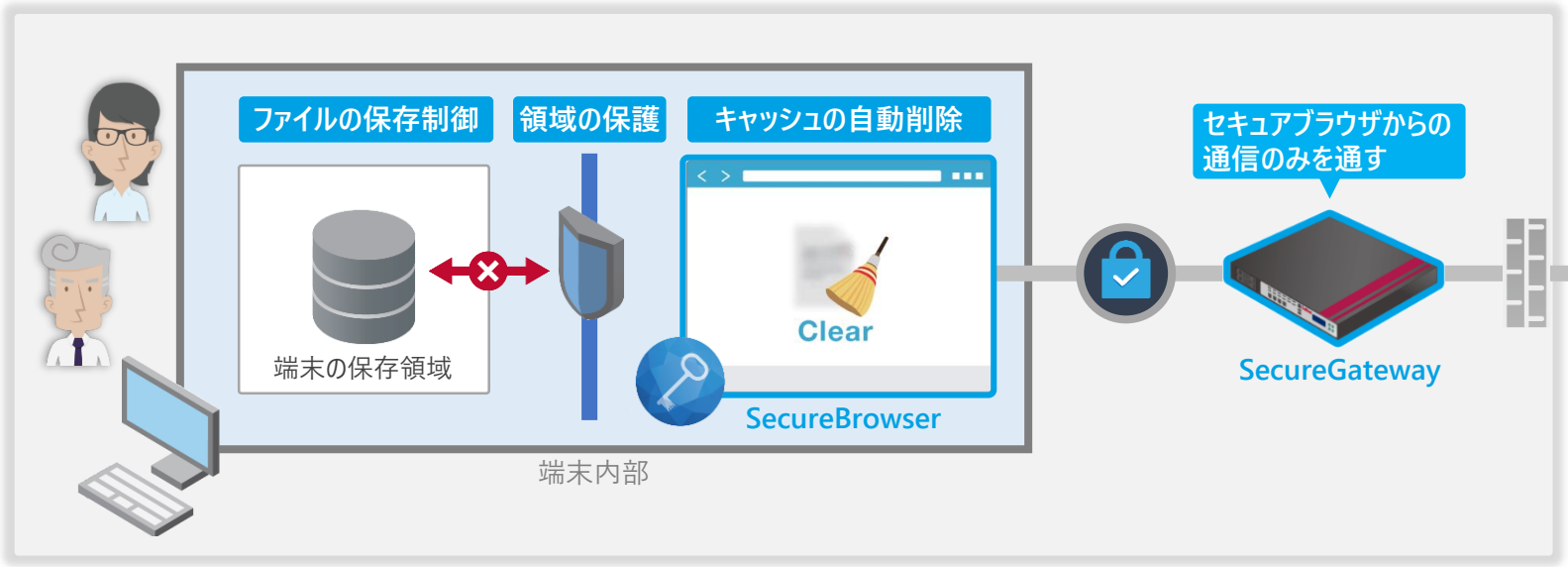
- VDI・SBC（仮想PCの画面転送）
  - ✓ 端末を2台用意しなくとも、仮想技術を利用すれば、業務LANとインターネットLANを分離出来るという発想が生まれた
  - ✓ セキュリティを強化しなければならないメガバンクや重要インフラ企業には採用が進んだ一方、**コストと運用面の課題から採用が見送られるケースもあった**
- Web画面転送方式
  - ✓ Webの画面転送方式に特化することで、コストを抑えながら、仮想デスクトップに近いセキュリティ効果が見込めるようになった
  - ✓ **Webブラウジング全般のレスポンスが悪いため、利用者からの不満が多く上がり、帯域やシステムの見直しを迫られるケースが出てきている**

端末内分離方式（セキュアブラウザ）

- ✓ 専用ゲートウェイとセキュアブラウザが一体化することにより、**通信を制御することができる**ようになり「漏洩」を防げるようになった
- ✓ 端末のローカル上で動作するため、**利用者の利便性が損なわれることが無くなった**
- ✓ **コスト面で実現性が高く**、ネットワークも既存の帯域を活かすことができ、導入が進んでいる

端末内分離で、安全なウェブ閲覧

Soliton SecureBrowser / SecureGateway は、端末からの情報漏洩・データ持出しを防止するソリューションです。
端末内の分離領域で動作するブラウザとして、インターネット分離や働き方改革（リモートワーク）で利用されています。



《端末内分離の特長》

- ブラウジングは快適。コンテンツ変換をしていないためレスポンスが良く、汎用ブラウザ同等の操作性
- 専用アプライアンスと専用ブラウザアプリ のシンプルな構成
- ドキュメントは専用ビューワーで閲覧

参考）テレワークに関する政府機関のガイドライン

総務省が平成30年4月に公開している「テレワークセキュリティガイドライン 第4版」では、テレワークの方法に応じた対策の考え方として、次の6種類のパターンに分類しています。

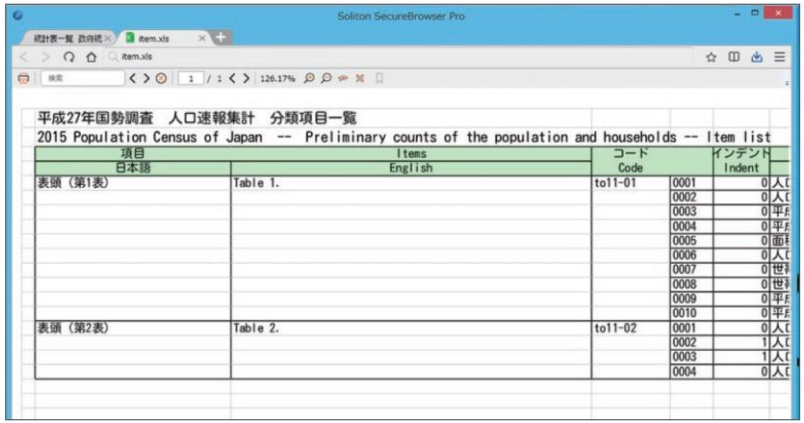
パターン	概要	
リモートデスクトップ方式	オフィスにある端末を遠隔操作	Soliton SecureDesktop
仮想デスクトップ方式	テレワーク用の仮想端末を遠隔操作	価格面や利便性で課題
クラウド型アプリ方式	クラウド上のアプリーションを 社内外から利用	安全性を確保しておく必要がある
セキュアブラウザ方式	**特別なブラウザを用いて端末へのデータの保存を制限**	Soliton SecureBrowser
アプリケーションラッピング方式	**テレワーク端末内への保存を不可とする機能を提供**	WrappingBox
会社PCの持ち帰り方式	オフィスの端末を持ち帰りテレワーク端末として利用	

Soliton SecureAccess は、この方式

ドキュメントを安全に閲覧、編集

- SecureBrowserは、MS OfficeやPDFなどの主要なドキュメントの閲覧に対応したビューワー※を搭載。
  インターネットから取得したファイルも安全に閲覧できます。
- ドキュメントデータはセキュアブラウザ内の安全な領域で表示され、ログアウト時などに自動的に消去。
- Zipファイルやパスワード付ファイルにも対応します。

PCの他、スマートデバイスにも対応

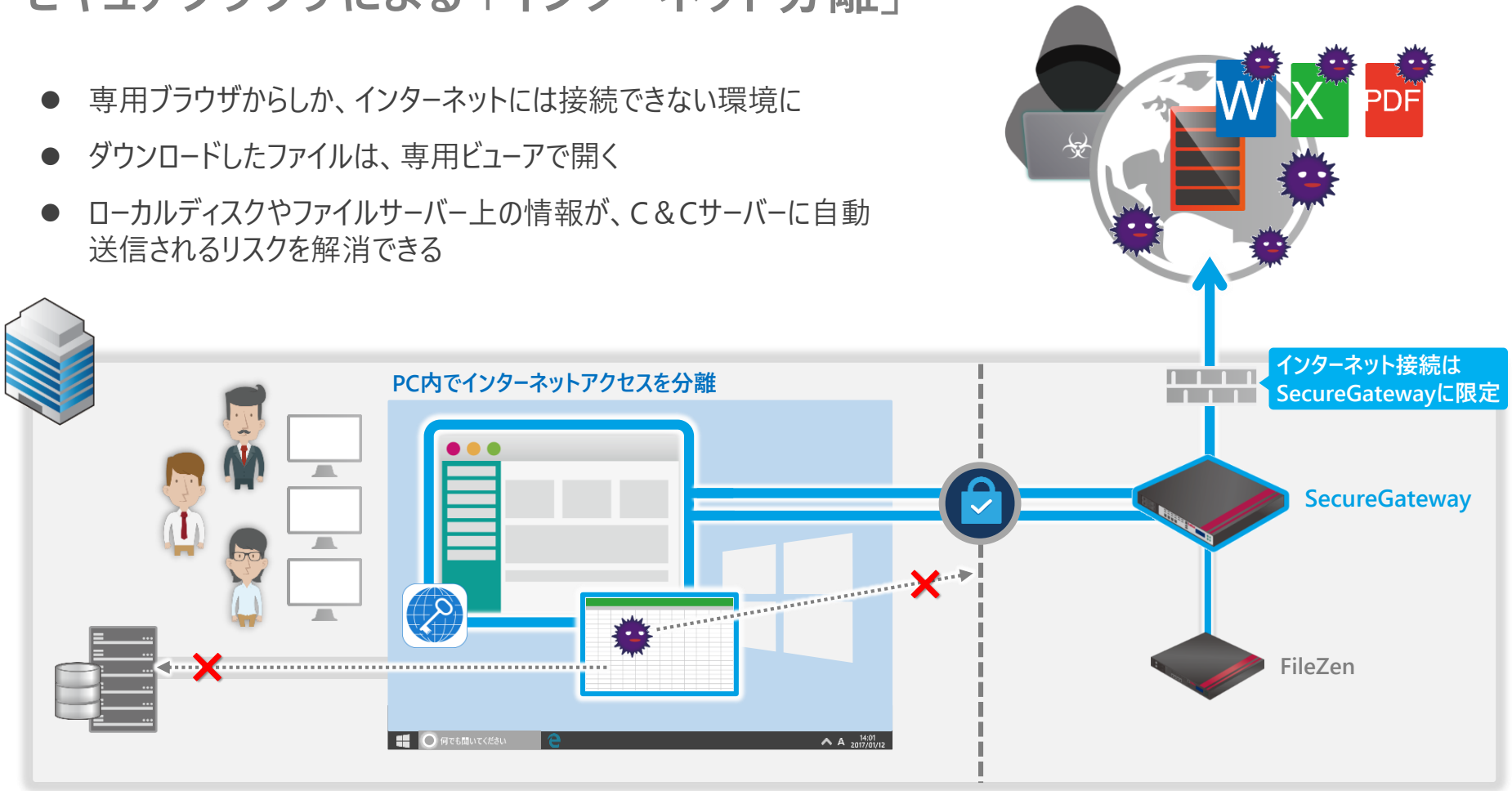


ローカル保存を禁止

※ ・MS Office、PDF、ZIPのパスワード付きファイルにも対応
・DocuWorks文書の閲覧にも対応
・ビューワーは、全てのファイルを正しく表示することを保証するものではありません。導入前に評価いただき動作をご確認ください。

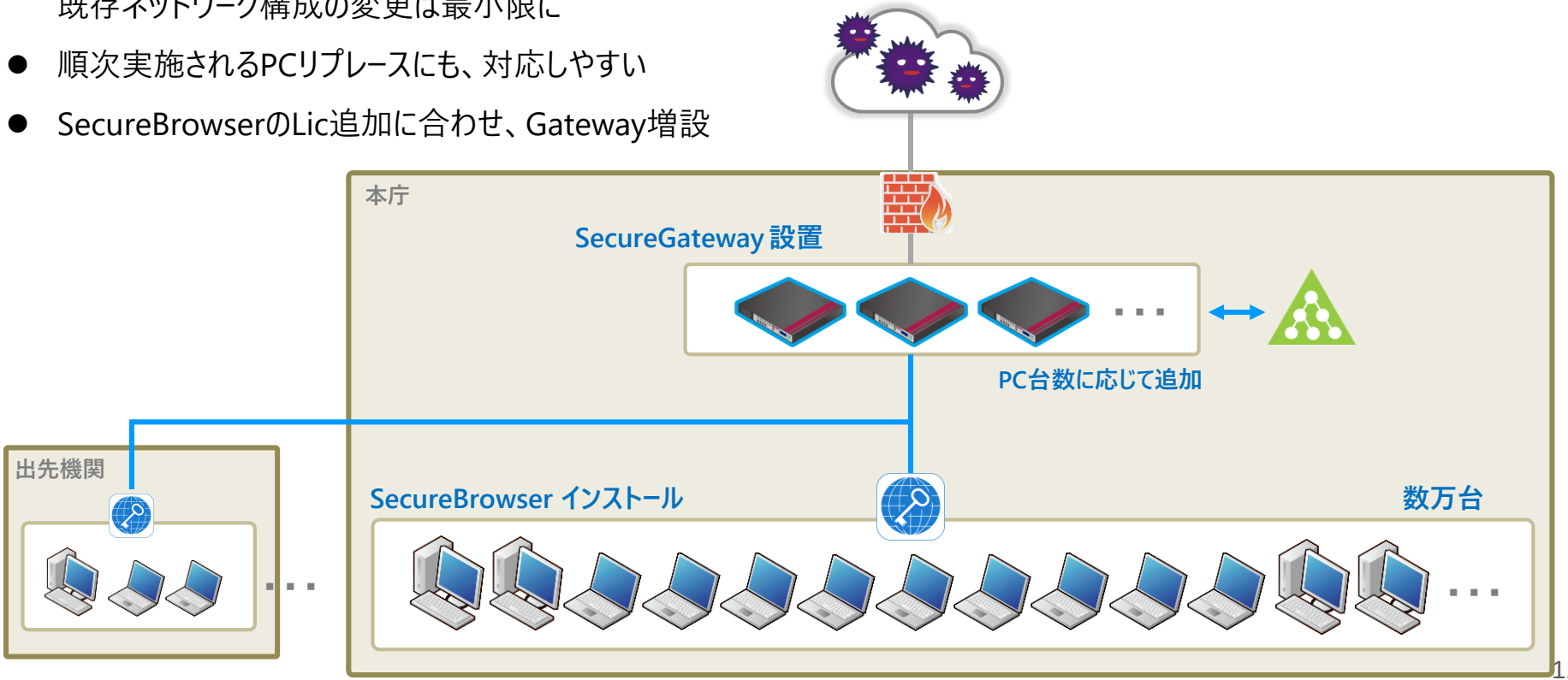
セキュアブラウザによる「インターネット分離」

- 専用ブラウザからしか、インターネットには接続できない環境に
- ダウンロードしたファイルは、専用ビューアで開く
- ローカルディスクやファイルサーバー上の情報が、C＆Cサーバーに自動送信されるリスクを解消できる



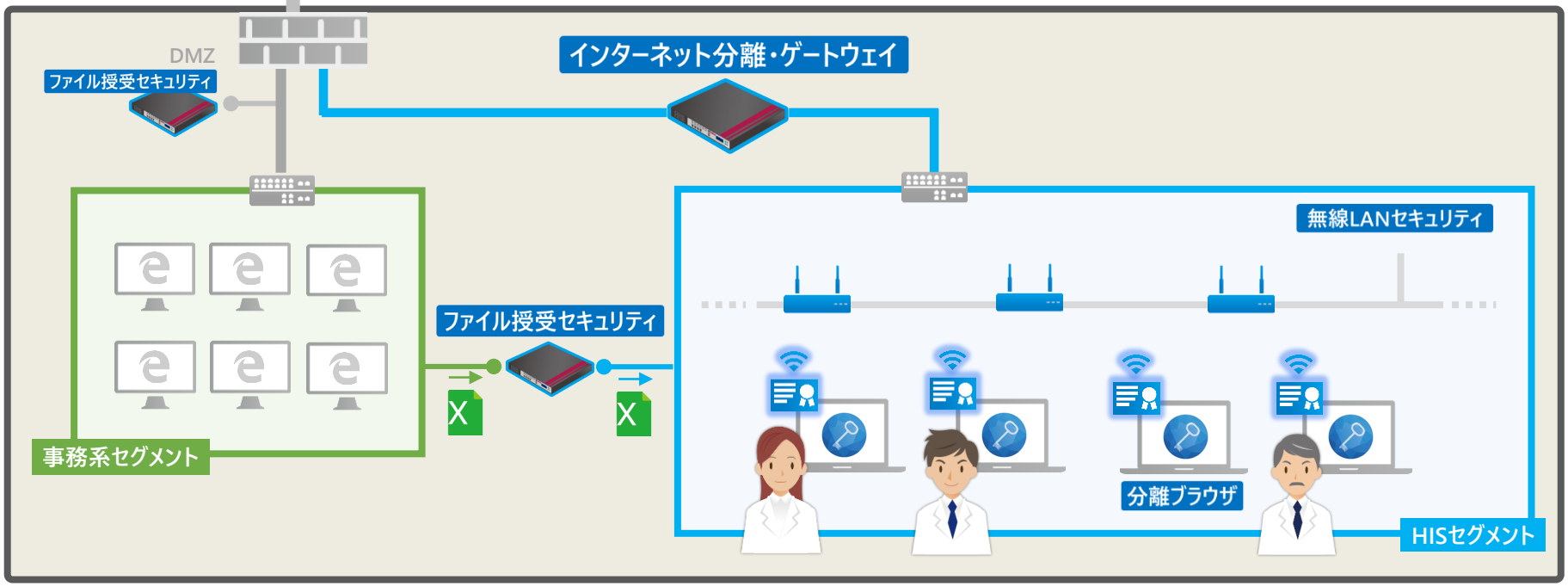
政令指定自治体様の「インターネット分離」例

- PC 数万台の規模（市民病院等へも適用）
- 専用プライアンス＋ブラウザ のシンプル構成で、
  既存ネットワーク構成の変更は最小限に
- 順次実施されるPCリプレースにも、対応しやすい
- SecureBrowserのLic追加に合わせ、Gateway増設

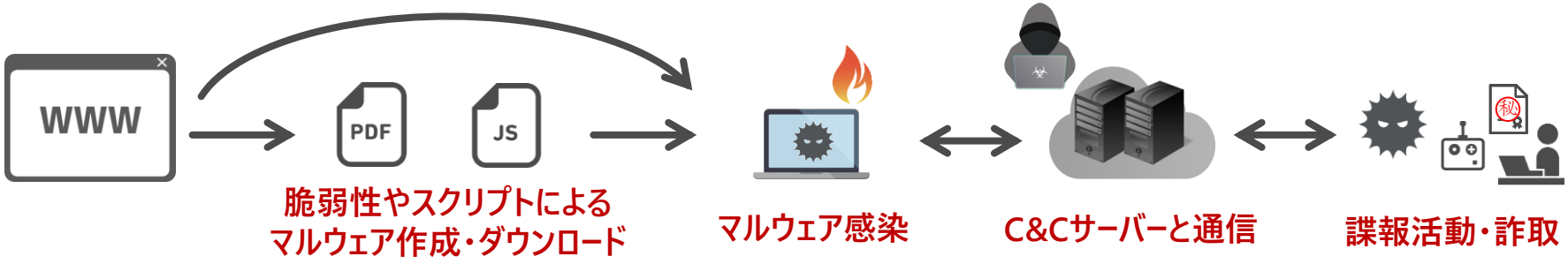


医療機関：電カル端末でセキュアにウェブ閲覧

- 電子カルテ端末でのウェブ閲覧に対する、先生方からのニーズは高い
- 医療機関で使えるセキュアなブラウザとして、全国で導入が進み始めています



● 標的型攻撃の流れ



《SecureBrowserなら》

- 厳格なMIMEスニッフィングを行い、実行形式ファイルのダウンロードの制限をします。
- SecureBrowserの分離領域内を利用して、攻撃者が不正なプロセスを実行させることは困難です。
- 分離領域内から分離領域外へ、ファイルを直接保存することを禁止することできます。
- OfficeやPDFファイルは専用ビューアーによる閲覧が可能であり、Office製品の脆弱性やマクロ機能の悪用を防止します。

▶

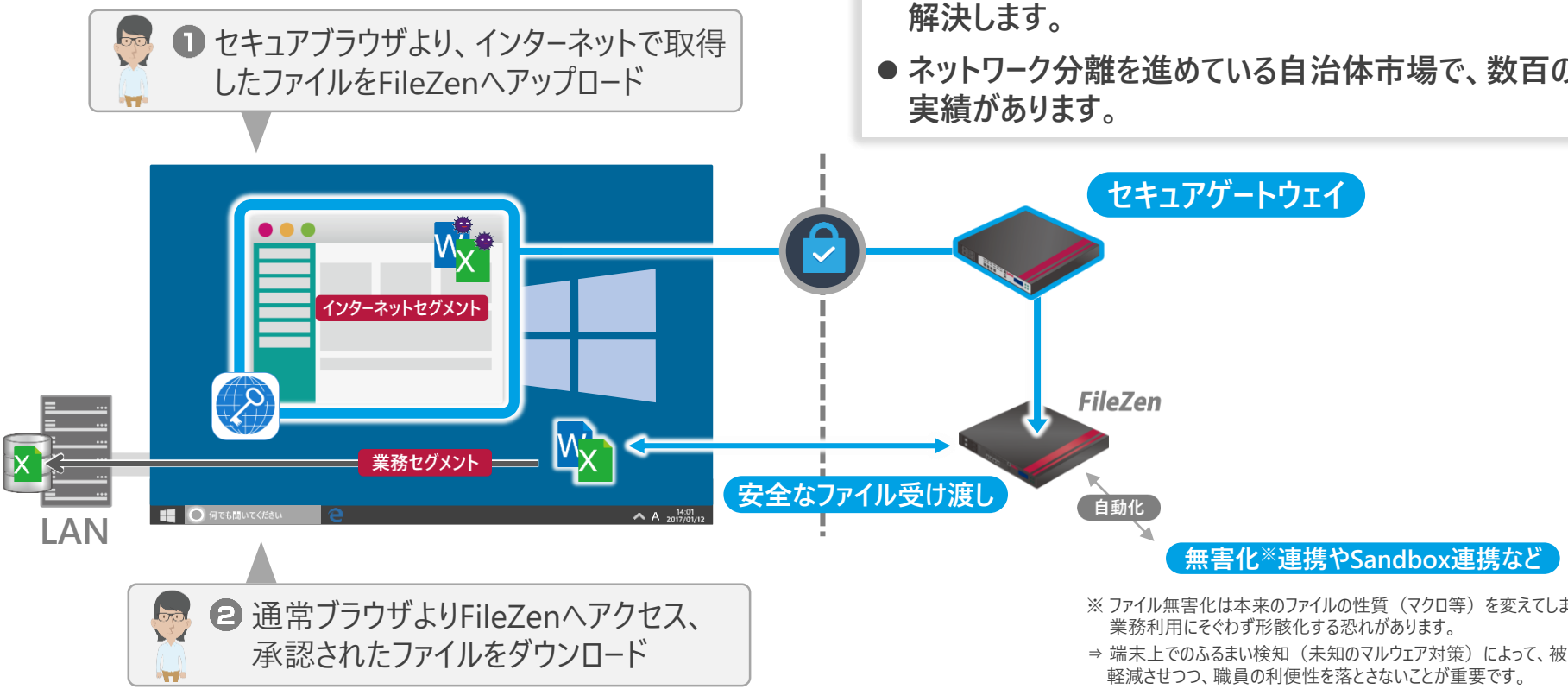
●侵入したプロセスが外部のC＆Cサーバと通信することはできません。

- 追加プログラムなどがダウンロードされることはありません。
- 不正なプロセスが業務LAN上のファイルをC&Cサーバーへ送信することはできません。
- 諜報活動や情報の詐取に必要な動作ができず、標的型攻撃の被害を免れます。

	VDI・SBC	Web画面転送	端末内分離（セキュアブラウザ）
方式	• 仮想PCの画面転送	• Webブラウザ専用の画面転送	・専用ブラウザのみインターネット接続が可能
導入効果	• マルウェアが侵入しても、ローカルPCは影響を受けない • 業務LAN側の感染時に漏洩を防ぐ	• Web閲覧から業務LANへのマルウェア侵入を防止 • 業務端末がマルウェアの感染を受けても外部通信が制御されるため漏洩を防ぐ	• マルウェア侵入の抑制、不正通信の防止 • 業務端末がマルウェアの感染を受けても外部通信が制御されるため漏洩を防ぐ
課題	• 仮想PCがマルウェア感染した際に、他の仮想PCや、同一ネットワークのサーバー（AD等）が2次感染 • 侵入に対してはメールも分離環境に置かなければ効果が小さい	• 侵入に対してはメールも分離環境に置かなければ効果が小さい	• メールやソフトウェアアップデートからの侵入を考慮し、NGAV（ゼロデイ脆弱性やファイルレス攻撃への対策）との組み合わせが有効
コスト	• 環境構築コストが高い。さらにOfficeライセンスも追加で必要 • 帯域の確保（ネットワークの見直し） ✕	• 帯域の確保（ネットワークの見直し） ▲	○
利便性	• 通常の端末とほぼ同様の操作が可能（※利用者は2つの端末を運用） • クライアント証明書の運用は煩雑	• ローカル端末の操作 • Web全般のレスポンスが悪い • **クライアント証明書が利用できない**	• ローカル端末の操作 • ローカルPC上で動作するため利用者の操作レスポンスは落ちない • **OSストアのクライアント証明書利用が可能**
実績	• 大手金融機関やその他重要インフラ企業、自治体での導入が進んだ	• 自治体を中心として導入が進んだ	• 政令指定自治体・金融・医療機関など導入が進んでいる（数万人規模も有）

分離環境でのファイル受け渡し

- ネットワーク分離で不満が続出する「ファイル受け渡しの悩み」を、承認機能付きファイル転送システムが解決します。
- ネットワーク分離を進めている自治体市場で、数百の実績があります。



※ ファイル無害化は本来のファイルの性質（マクロ等）を変えてしまい、業務利用にそぐわず形骸化する恐れがあります。

⇒ 端末上でのふるまい検知（未知のマルウェア対策）によって、被害を軽減させつつ、職員の利便性を落とさないことが重要です。

分離ネットワーク間のファイル受け渡し

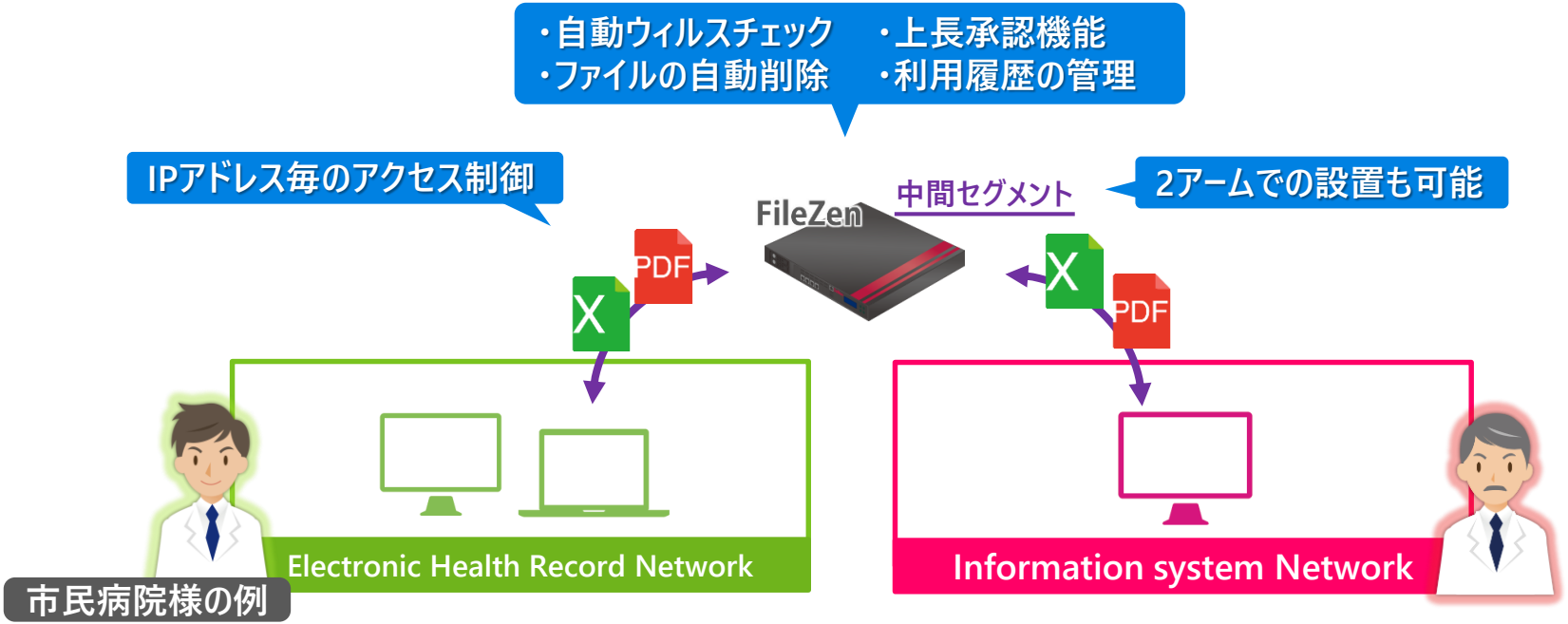
ネットワーク分離環境における、ファイル受け渡しのニーズ

- **セキュリティ機能があったとしても、クラウドサービスは使えない**
  インターネット接続がない、ルーティングしない、専用ボックスが望ましい

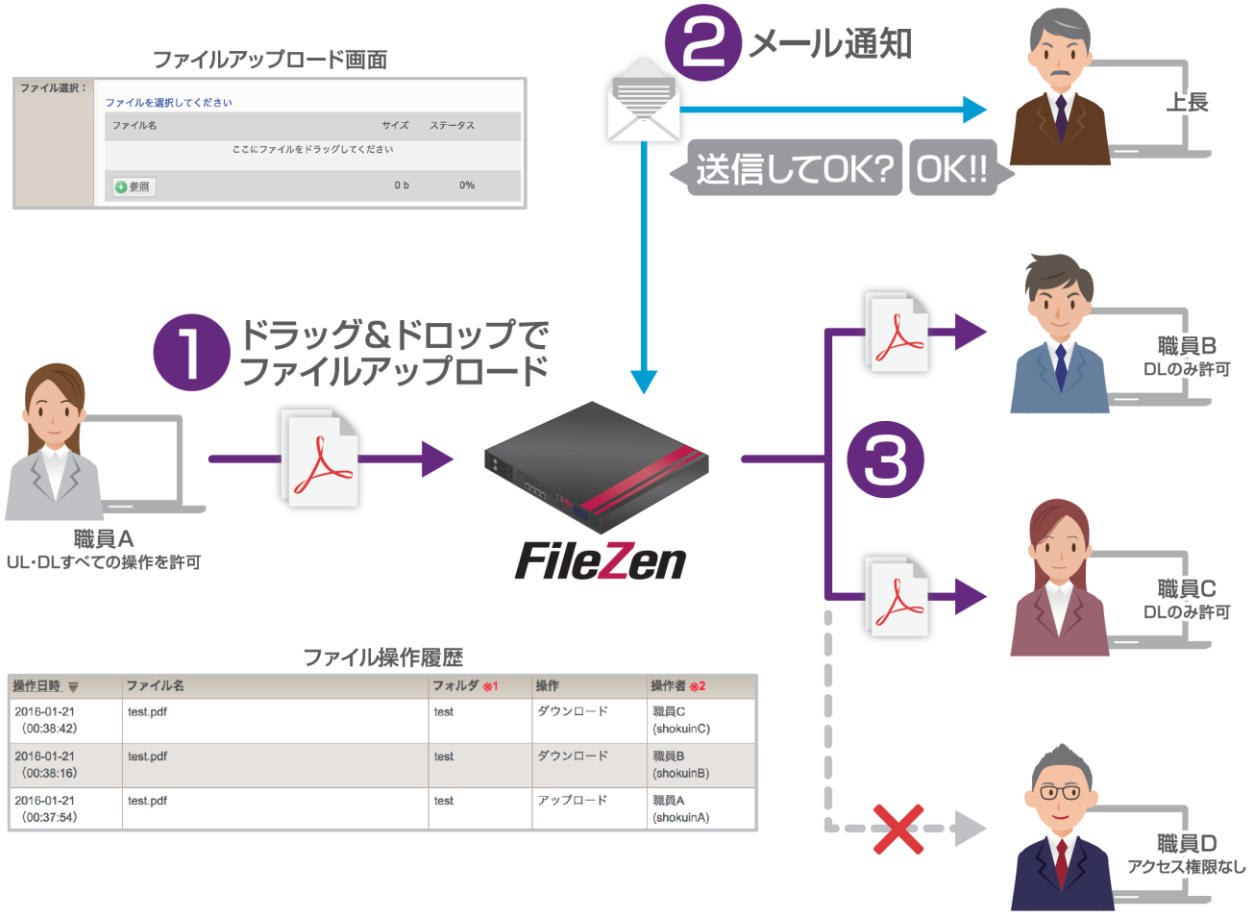
- **ファイル持ち出し時には、上長承認を行いたい**
  持出し禁止ファイルでないか、上長が中身も確認できるようにしたい

安全で利便性の高いファイル受け渡し

- 分離されたネットワークの間に、専用ボックス（FileZen）を設置するだけ
- 認証機能、上長承認、利用履歴記録、自動ウィルスチェックなど、標準装備



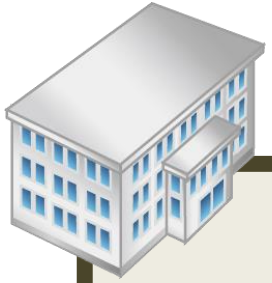
ファイルの受け渡し利用例



ファイル操作履歴

操作日時	ファイル名	フォルダ ※1	操作	操作者 ※2
2016-01-21 (00:38:42)	test.pdf	test	ダウンロード	職員C (shokuinC)
2016-01-21 (00:38:16)	test.pdf	test	ダウンロード	職員B (shokuinB)
2016-01-21 (00:37:54)	test.pdf	test	アップロード	職員A (shokuinA)

地方自治体様の例



FileZen Mail

FileZen 冗長構成

w/ PDF Converter

4,000 USER

FileZen

FileZen

LGWAN

Information System Network

WWW

4,000 USER

FileZen 冗長構成

The Social Security and Tax Number System Network

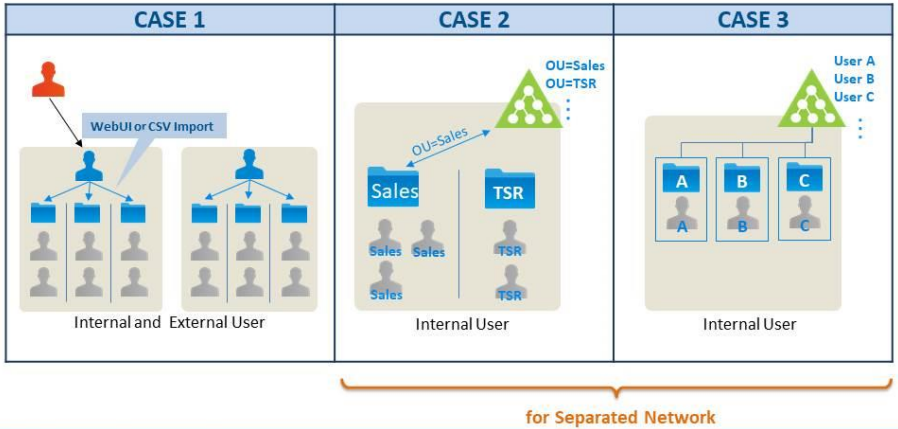
1,500 USER

セットアップは簡単 -海外向けトレーニング資料抜粋-

Soliton

Setup FileZen Service -3

4. USER / PROJECT and FOLDER



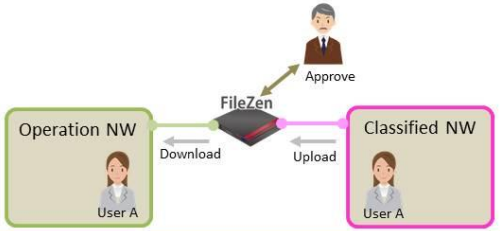
Soliton

Setup FileZen Service -4

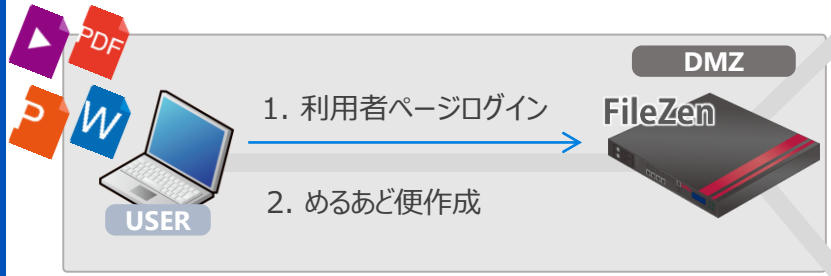
5. Make a "**Templete Folder**"

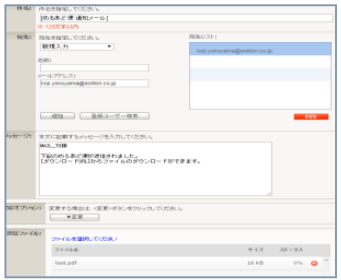
☐ [Folder] tab - List - Add

- Folder Name: **Template**
- Project Group Belongs: **ADTEST**
- Default Permissions **(check the box)**
- File Retention Period: **1days**
- File Disclosure Authorization Function: **Use (Unavailable to Download by owner)**
- Verification of Accessing IP Address:



外部とのやりとりにも





[めるあど便作成](#)

送付先Emailアドレスの指定、
件名・メッセージ入力

[受け取りフォルダ作成](#)

送付先Emailアドレスの指定、
件名・メッセージ入力

3. Email通知 Download URL付

4. Download

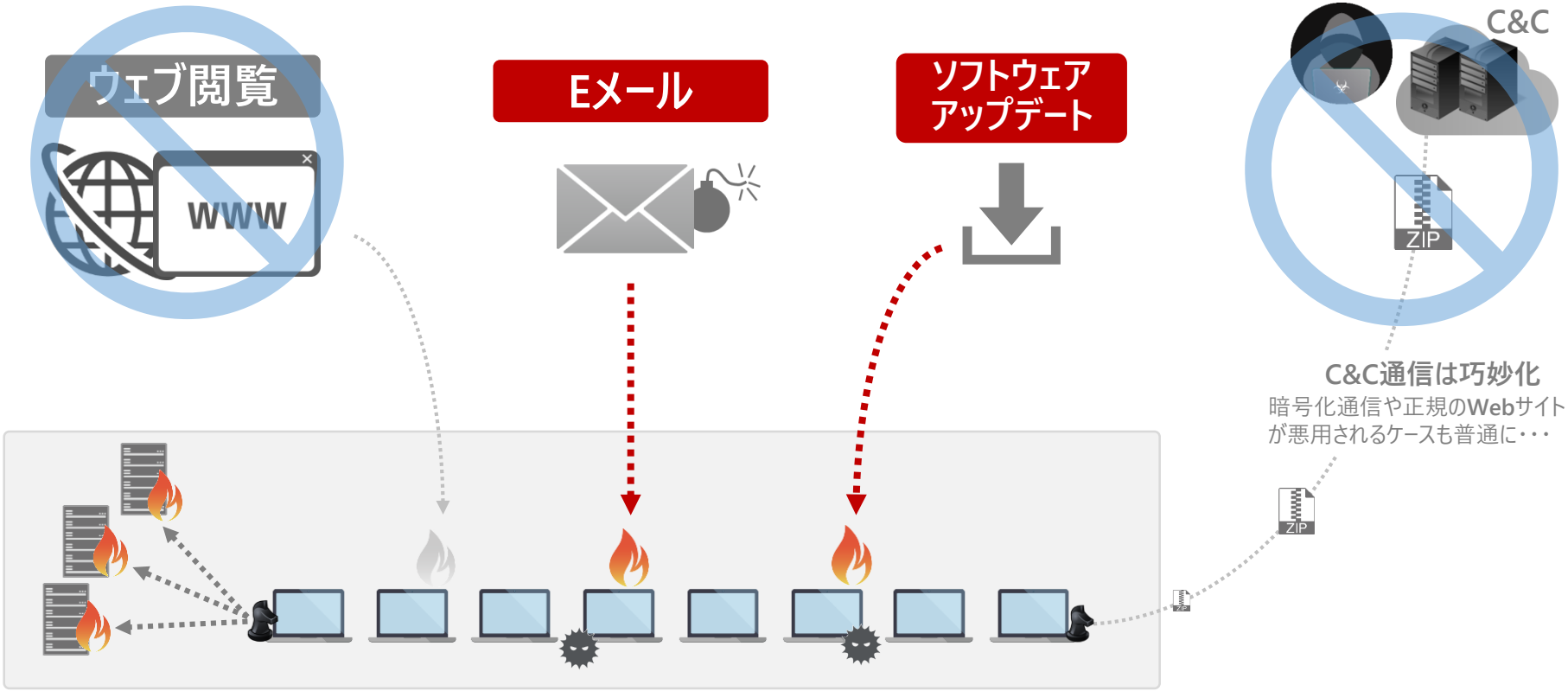
3. Email通知 Upload URL付

4. Upload

分離環境における、FileZenの特長

- **ネットワーク間への配置**
  ネットワーク独立性維持
- **利用履歴を記録**
  いつ、誰が、何を、どこから
- **ファイル受け渡し承認**
  上長による承認

他の侵入経路への対策



- 可用性を狙う破壊型攻撃などを考慮すると、エンドポイントでの未知マルウェア対策はやはり必要

➡ Windows 10 移行を考慮した、エンドポイントの脅威対策を整理

Windows 10 移行時に考慮すべき点

サードパーティ製アンチウイルスを、Windows 10 に標準搭載される
Windows Defender に置き換えて良いかどうか？

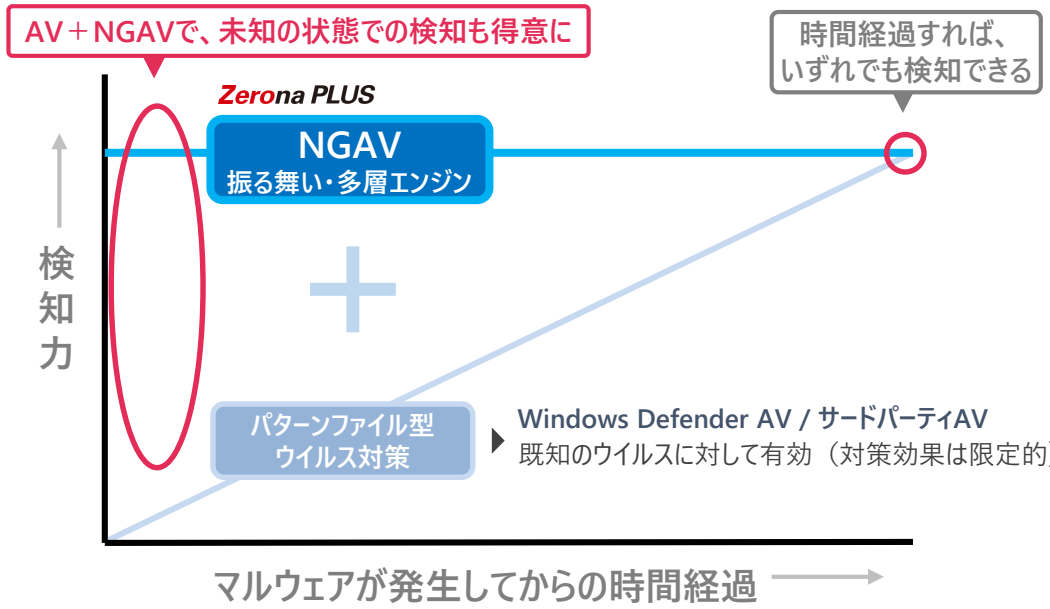
サードパーティ製アンチウイルスからの置き換えにあたり、確認すべき点

1）セキュリティレベルは下がらないか？

2）インシデント発生時の対応は？

確認1 セキュリティレベルは下がらないか？

アンチウイルス製品は、既知のウイルスの特徴を記録したパターンファイルにより、脅威を検知します。パターンファイルを持っていない、ゼロデイや未知のマルウェア、ファイルレス・マルウェア※1については、検知することができません。これは、サードパーティ製アンチウイルス製品でもOS標準のDefender ウイルス対策の場合でも同様です。**パターンファイル型対策製品のコストを抑え、未知マルウェア対策となるNGAV※2製品を導入することができれば、セキュリティレベルを飛躍的に向上させることが可能となります。**



※1 ファイルレス・マルウェアとは

実行ファイルを利用せず、端末に内蔵されている正規プログラムを利用して感染・攻撃を行うマルウェア。PowerShellが利用される点が注目されているが、Officeマクロやリンクファイル、WSH（Javaスクリプト等）を利用するものなど、様々な手口がある。

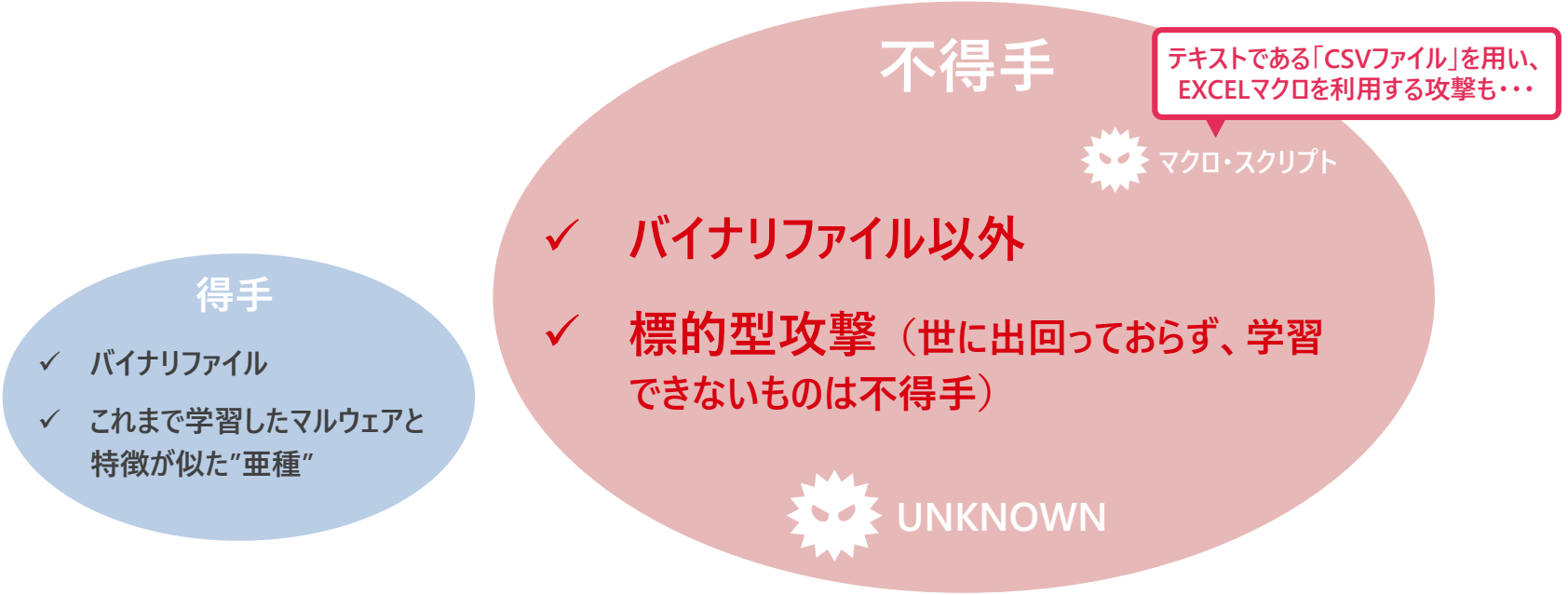
※2 NGAVとは

パターンファイルに依存せず、未知の高度な脅威を防ぐことを目的とした製品。機械学習や振る舞い解析、サンドボックス解析といった技術が用いられる。Next Generation Anti Virus（次世代アンチウイルスの略）。EPP=Endpoint Protectionと呼ばれることもある。

AI・機械学習は万能？

NGAVではAI・機械学習方式に注目が集まっています。静的な機械学習は、マルウェアのバイナリファイル（exeファイルやDLLファイル等）の特徴を抽出し学習することで、パターンファイルに依存せず、新種のマルウェアを検知します。

最新の攻撃では、**バイナリファイルを利用しないファイルレスマルウェア**に増加しており、機械学習だけで未知マルウェアを止めることは難しいことが明らかとなっています。



静的解析も、振る舞いも、機械学習も、一度に

「Zerona PULS」なら、5つのエンジンで検知・防御

NGAV Zerona PLUS

アプリケーションの脆弱性を守る

ZDPエンジン（動的解析）
・任意コード実行型脆弱性攻撃を防御

マルウェアの存在を検知してブロック

Staticsエンジン（静的解析）
・ファイルをスキャンしてプログラムの構造を静的に分析

Sandboxエンジン（半動的解析）
・仮想環境上でプログラムを実行して分析

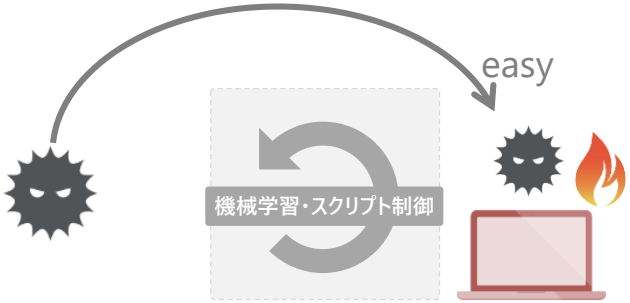
マルウェアの振る舞いを検知してブロック

HIPSエンジン（動的解析）
・実行中プログラムの動作を監視し、悪意ある挙動の有無を分析

機械学習エンジン（動的解析）
・ビッグデータ上の振る舞い特性を抽出し、機械学習で分析した特徴により、端末上の悪意ある挙動を分析

多層防御（マルチエンジン）の利点

NGAV Zerona PLUS



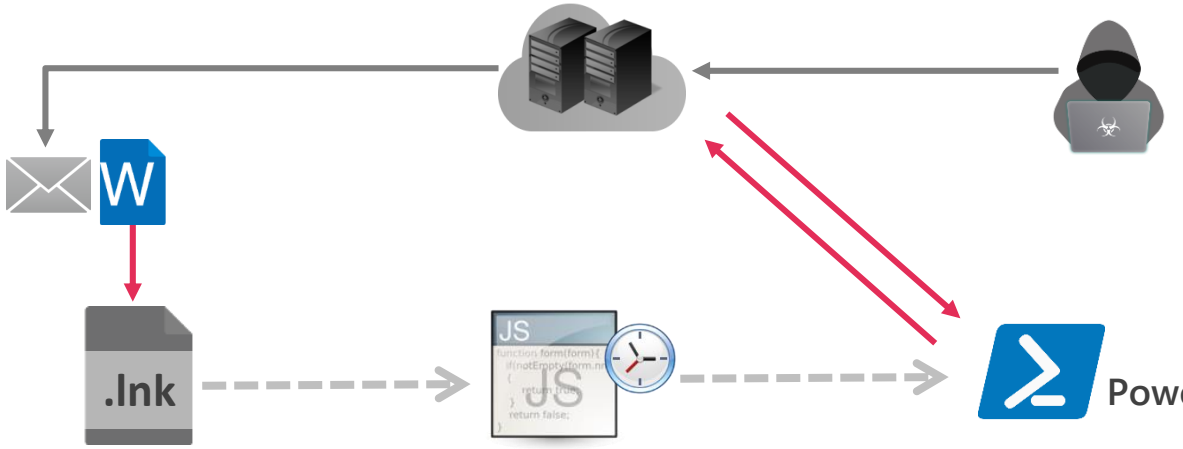
単一エンジンのバイパス（回避）は簡単・・・

多層エンジンなので検知ロジックが複雑。
１つ回避しても他のエンジンに捕まる。

多層エンジンで、ファイルレス マルウェアにも対応

NGAV Zerona PLUS

実行ファイルを利用せず、端末に内蔵されている正規プログラムを利用して感染・攻撃を行うマルウェア。PowerShellが利用される点が注目されていますが、Officeマクロやリンクファイル、WSH（Javaスクリプト等）を利用するものなど、様々な手口があります。



メール添付されたRTFファイルの「ボタン」をクリックすると、悪意あるショートカットファイル(.lnk)が生成される

.lnkから難読化されたJavaScriptが実行され、スケジュールタスクに次の攻撃ステップで実行する内容が登録される（1分のDelay）

PowerShellがDNS経由でMetapreterをダウンロードし
メモリ上に展開して脆弱性攻撃を実行
（暗号化されておりメモリスキャンでは検知困難）

パターンファイルでは間に合わず、機械学習では対象外のことが多い

パターンファイル・機械学習では検知不可

Staticで検知

HIPSでブロック

ZDPで防御

Zerona PLUS

Zerona PLUS

Zerona PLUS

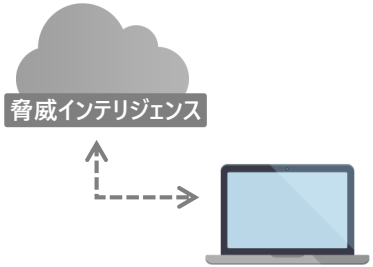
PowerShellが起動する、前の前の段階で、止めています。

標的型攻撃に脅威インテリジェンスは有効？

NGAVの多くは、クラウドの脅威情報との連携を前提としています。世界中のユーザーから収集した脅威情報を利用できるため、特に、瞬時に増殖する亜種検知に有効です。

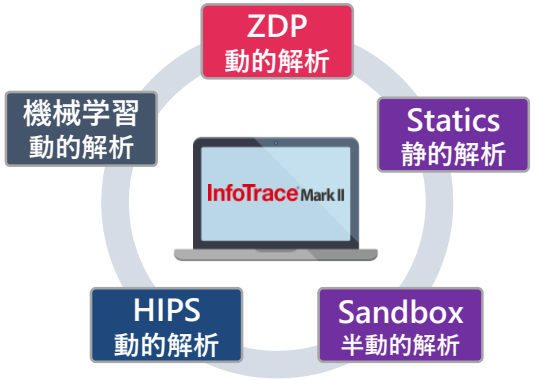
反面、どこにも出回っていない、真の未知攻撃を事前に収集しておく事ができないため、標的型攻撃など前例の少ない攻撃には注意が必要です。また製品によっては、クラウドと連携できない間の検知力が、大きく低下する場合があることにも注意が必要です。

脅威インテリジェンス利用



世界中のユーザーから収集した既知の脅威情報を利用できる。特に亜種検知に効果が高い。

検知ロジック自立型



クライアントの検知ロジックのみで検知できる。クライアントに高度な検知ロジックを持たせることで、標的型攻撃など前例の少ない攻撃であっても検知する

日本の組織を狙った攻撃にも強い

防御実績（未知マルウェア）

被害発生以前にリリースされたバージョンで未知マルウェアを排除

発生・報道 時期	防御エンジン リリース時期	当時の未知脅威 及び標的型攻撃	Mark II（Zerona） 検知&防御エンジン
2018年1月	半年以上前	ランサムウェア「Rapid」	Static分析エンジン
2017年12月	半年以上前	仮想通貨採掘マルウェア「CoinMiner」	HIPSエンジン
2017年12月	半年以上前	「楽天カード株式会社」を装ったマルウェア	HIPSエンジン
2017年10月	半年以上前	ランサムウェア「Bad Rabbit」	Static分析エンジン
2017年8月	半年以上前	国内防衛産業を標的としたマルウェア	Static分析エンジン
2017年5月	半年以上前	仮想通貨採掘マルウェア「Adylkuzz」	Static分析エンジン
2017年5月	半年以上前	ランサムウェア「WannaCry/WannaCrypt」	Static分析エンジン
2017年1月	4 か月前	IoTマルウェア「Mirai」	Static分析エンジン
2017年1月	4 か月前	ランサムウェア「Spora」	Static分析エンジン
2016年5月	半年以上前	不正送金マルウェア「Gozi/Ursnif」	HIPSエンジン
2016年3月	半年以上前	ランサムウェア「Cerber」	機械学習エンジン
2016年2月	半年以上前	ランサムウェア「Locky」	HIPSエンジン
2015年12月	半年以上前	ランサムウェア「TeslaCrypt（vvvウイルス）」	Static分析エンジン
2014年11月	3 か月前	医療費通知偽装 マルウェア「Emdivi」	Static分析エンジン
2013年1月	半年以上前	機密情報を盗み出すマルウェア「Daserf」	Static分析エンジン

防御実績（ゼロデイ脆弱性攻撃）

被害発生以前にリリースされたバージョンでゼロデイ脆弱性を排除

発生・報道 時期	防御エンジン リリース時期	当時の未知脅威 及び標的型攻撃	Mark II（Zerona） 検知&防御エンジン
2018年5月	半年以上前	Adobe Acrobat Readerの脆弱性 (CVE-2018-4990)	ZDPエンジン
2017年1月	半年以上前	Firefoxの脆弱性 (CVE-2017-5375)	ZDPエンジン
2015年7月	1年以上前	Adobe Flash Playerの脆弱性 (CVE-2015-5119、CVE-2015-5122)	ZDPエンジン
2015年6月	1年以上前	Adobe Flash Playerの脆弱性 (CVE-2015-3113)	ZDPエンジン
2015年1月	2か月前	Adobe Flash Playerの脆弱性 (CVE-2015-0311)	ZDPエンジン
2014年11月	3か月前	一太郎の0-day脆弱性 (CVE-2014-7247)	ZDPエンジン
2014年2月	3か月前	IEの0-day脆弱性 (CVE-2014-0322)	ZDPエンジン

日本の組織がターゲットとなったゼロデイに対応

政府機関等の対策基準策定のためのガイドライン（平成30年度版）

NGAVの選定ポイント

6.2.2 不正プログラム対策

目的・趣旨

情報システムが不正プログラムに感染した場合、情報システムが破壊される脅威や、当該情報システムに保存される重要な情報が外部に漏えいする脅威が想定される。さらには、不正プログラムに感染した情報システムは、他の情報システムに感染を拡大させる、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される、標的型攻撃における拠点として利用されるなどが考えられ、当該情報システム以外にも被害を及ぼすおそれがある。このような事態を未然に防止するため、不正プログラムへの対策を適切に実施することが必要である。

遵守事項

(1) 不正プログラム対策の実施

(a) 情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

(b) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

(c) 情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。

【 基本対策事項 】

＜6.2.2(1)(a)関連＞

6.2.2(1)-1 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。

6.2.2(1)-2 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。

6.2.2(1)-3 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態なるように構成すること。

6.2.2(1)-4 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

6.2.2(1)-5 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

＜6.2.2(1)(b)関連＞

6.2.2(1)-6 情報システムセキュリティ責任者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機

- **基本対策事項 6.2.2(1)-1「既知及び未知の不正プログラムの検知及びその実行の防止の機能を有する」について**

Windows Defender AVが担う

既知の不正プログラムについては、不正プログラム対策ソフトベンダにより、その不正プログラムに関するシグネチャが対策ソフトの定義ファイルに反映されることにより感染を防止することができる。一方で、標的型攻撃等の攻撃手法においては、不正プログラムのソースコードを部分的に改変する亜種や、ソフトウェアの新たな脆弱性を突く不正プログラムなど、不正プログラム対策ソフトウェア等の検知を回避しようとする攻撃が多く見られる。

このような未知の不正プログラムの検知及び感染防止への対応として、ソフトウェアの脆弱性への適切な対策に加えて、シグネチャにより検知する方式以外の手法を用いる製品やサービスを導入することの重要性も高まっている。例えば、シグネチャに依存せずに OS のプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、攻撃にスクリプト等を使用するファイルレスマルウェアの対策としても効果が期待できる。その他にも、サンドボックス、ふるまい検知等の技術があり、必要に応じこれら複数の検知方式の組み合わせにより、不正プログラムの検知精度を向上させることで、端末及びサーバ装置に対する不正プログラム感染リスクの低減を図ることも可能となる。

▼

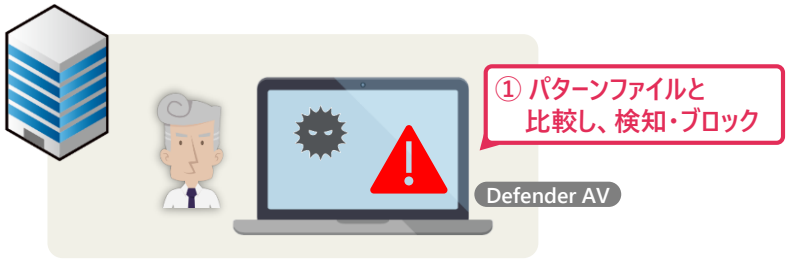
Zerona PLUS で担える

出展：政府機関等の情報セキュリティ対策ため統一基準（平成30年度版）
https://www.nisc.go.jp/active/general/pdf/guide30.pdf

確認2 インシデント発生時の対応は？

＜サードパーティー製アンチウイルスの場合＞

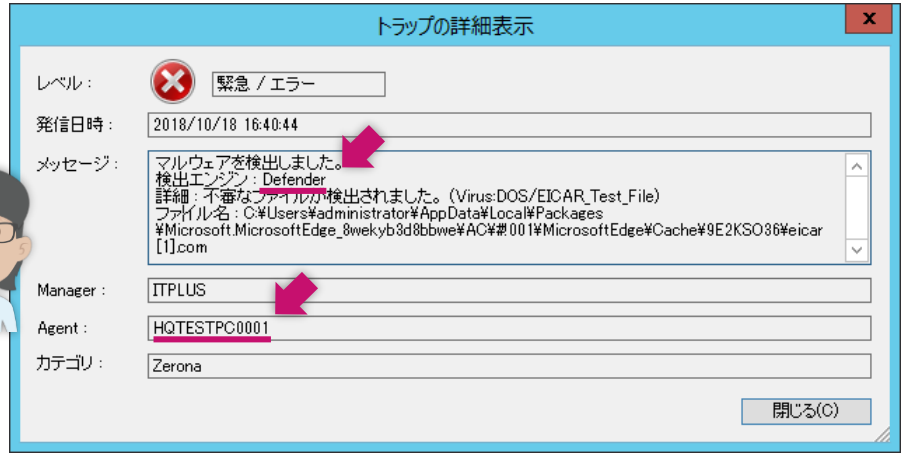
＜Windows Defender ウイルス対策の場合＞



**管理者へのアラート通知がない
ため、状況把握できない・・・**

Zerona PLUSなら、Defenderのアラートも管理者が把握できる

管理者へアラート通知



課題を補い・・・ どのPCで、Defenderが検知したのか、瞬時に把握可能。

インシデント対応コストも低減できる Defenderで検知した既知マルウェアも、NGAVで検知した未知マルウェアも、Zerona PLUSの操作ログ機能により、インシデント調査が可能です。

クライアントの操作ログによる全容把握

NGAV Zerona PLUS

例：脆弱性攻撃の要因となったファイル特定

マルウェア検知アラート

日時：	2014/05/08 17:10:50
メッセージ：	脆弱性攻撃を検出しました。 検出エンジン：脆弱性攻撃防御 アクション：プロセスを終了させました（ユーザー名：takahashi） ファイル名：C:¥Program Files¥Adobe¥Reader 11.0¥Reader¥AcroRd32.exe
Agent：	ITP-WIN7
Group：	ITP-WIN2012R2/Windows/Soliton3F/ITP-WIN7

Acrobat Reader（AcroRd32.exe）への脆弱性攻撃を防御した

PC操作ログで、時間・端末・プログラム名を条件に検索

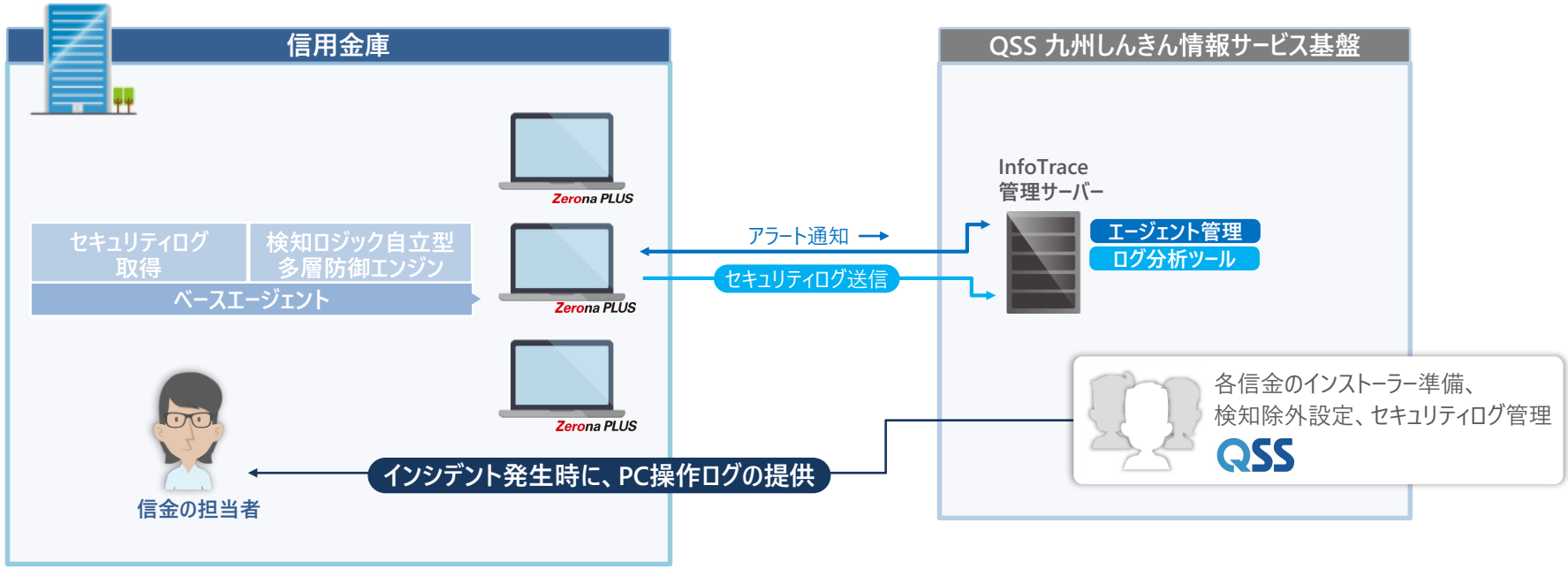
「講習会アンケート集計結果.pdf」を開いたためであったことが判明

株式会社 九州しんきん情報サービス

Zerona PLUS

操作ログを活用して被害状況を確認

侵入を考慮した、被害を拡大させない仕組みづくり



侵入を前提とした対策にも力を入れたいと考え、製品を探していました

QSS

信金担当者に負荷をかけずに運用できる製品にしたいと考えました

QSS

検討から製品決定まで約半年ほどと、早いスピードで進められました

QSS

インシデント発生時の対応を迅速・的確に行える対策に力を入れていく

QSS

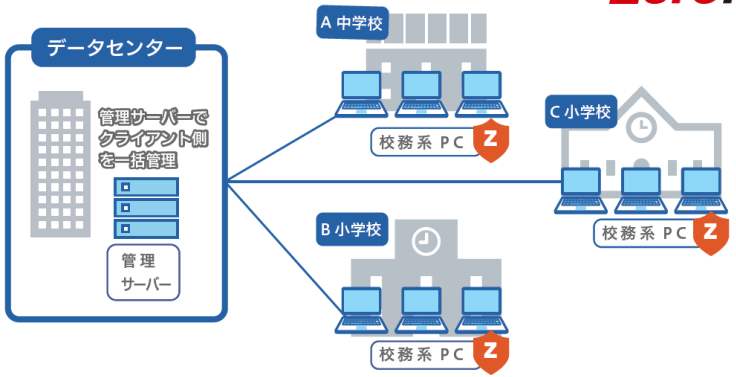
Zerona PLUS

岩井コスモ証券

標的型攻撃メール対策とCSIRT、システム面と組織面のセキュリティを強化

1 金融庁の監督指針を満たすレベルでサイバーセキュリティを強化したい	パターンファイルに依存しない、振る舞い検知機能で未知のマルウェアを防御
2 エンドポイントでの標的型メール対策を強化したい	ゲートウェイ対策に加えた対策実施で多層防御を実現
3 全社的な取り組みで継続的なセキュリティ強化を行いたい	脅威に繋がるユーザー操作の把握で社員教育にも役立てられる

Zerona PLUS



1日に数万件のサイバー攻撃を受けていた出雲市、新たな攻撃の防御に成功

1 USB経由も含めた、新しい攻撃にも対応できる対策製品を導入したい	パターンファイルに依存しないクライアント型の対策製品でエンドポイントを強化
2 インシデント発生時など、万が一の時に、迅速に状況を把握したい	PC操作ログを常時取得 状況把握できる環境を整備
3 市内50カ所に分散しているPCを一括管理したい	管理サーバーで各PCを一括管理 クライアント側での個別対応が不要

【お問合せ】 株式会社ソリトンシステムズ

ITセキュリティ営業部　netsales@soliton.co.jp