医療情報セミナー2017 in TOKYO

総務省指針の『標的型攻撃』対策 への対応について

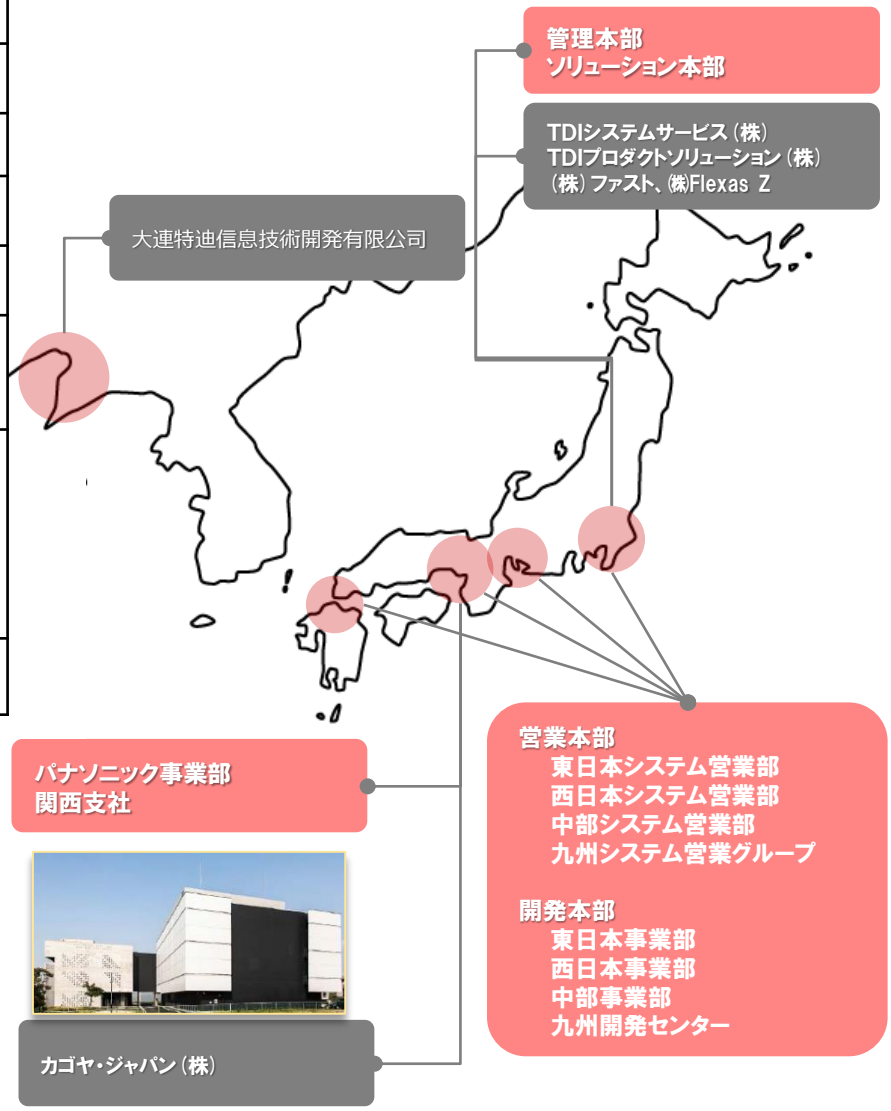
2017年2月22日

情報技術開発株式会社
ソリューション本部
iDC&セキュリティ事業推進部

1．弊社プロフィール

企業概要

商号	情報技術開発株式会社（略称：tdi）		
英文社名	T.D.I. CO., LTD （Technological Development of Information-processing）		
本社	東京都新宿区西新宿６丁目８番１号　住友不動産新宿オークタワー		
資本金	13億5,100万円	設立	1968年9月2日 （昭和43年）
従業員数	(連結) 1,337名 （2016年03月末現在）		
事業内容	ソフトウェア開発、情報処理サービス、 エンベデッド・ユビキタス／半導体関連、 データセンターサービス、ソフトウェア商品等の開発・販売		
子会社	TDIシステムサービス株式会社 TDIプロダクトソリューション株式会社 カゴヤ・ジャパン株式会社 株式会社ファスト 株式会社Ｆｌｅｘａｓ　Ｚ 大連特迪信息技術開発有限公司		
関連会社	株式会社アクトシティ レイヤーズ・TDIソリューションズ株式会社		



2. 標的型攻撃とは

標的型攻撃とは

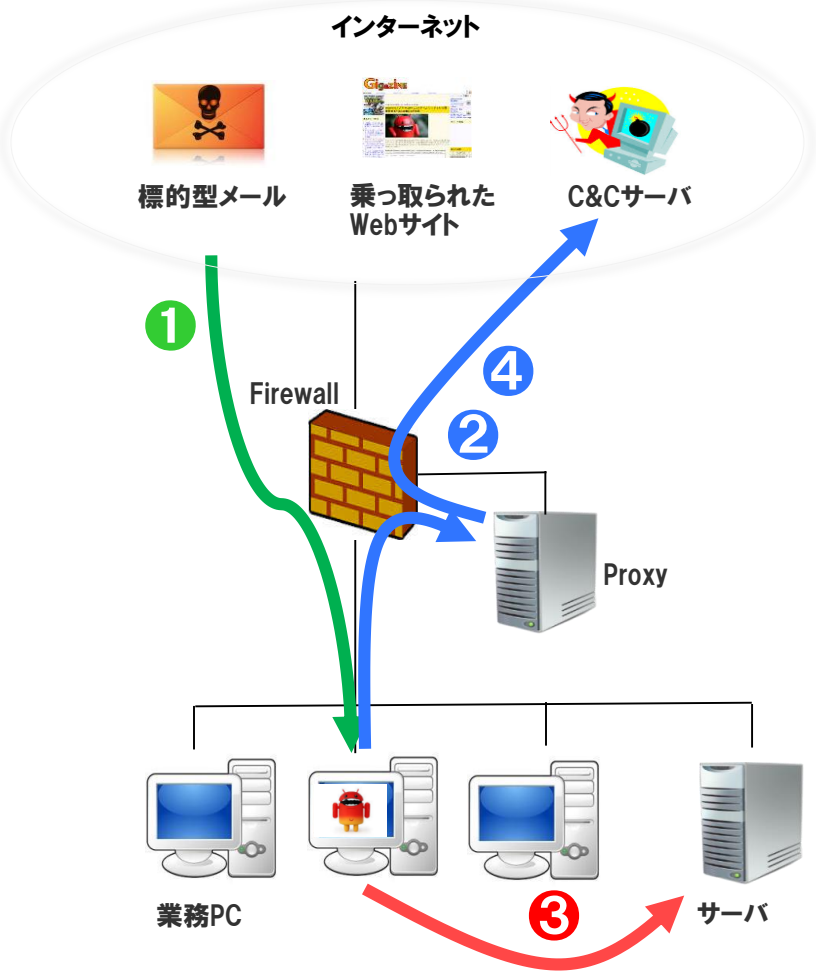
- 情報セキュリティ対策推進会議が「高度サイバー攻撃」として定義した攻撃手法
- 金銭や知的財産等の重要情報の不正な取得を目的として特定の標的に対して行われるサイバー攻撃で「プロの犯罪者」による窃盗行為が多いとみられている。

- 標的型攻撃による情報漏えいの事例
  - 日本年金機構/125万件の年金情報、　JTB/800万件の顧客情報

- 標的型攻撃の流れ
  - 他人になりすましウイルスに感染させるためのメールを送りつける。
  - ウイルス感染した端末を踏み台にサーバに不正アクセスを行う。
  - 管理者権限を取得して重要情報を窃取する。
  - ネットワーク上のファイルを暗号化するなどの破壊行為を行う。

標的型攻撃の代表的な手口

フィッシングメール（偽装メール）＋不正プログラム



❶ 標的型メールやWebサイト参照で
マルウェアに感染

❷ マルウェアがバックドア開設

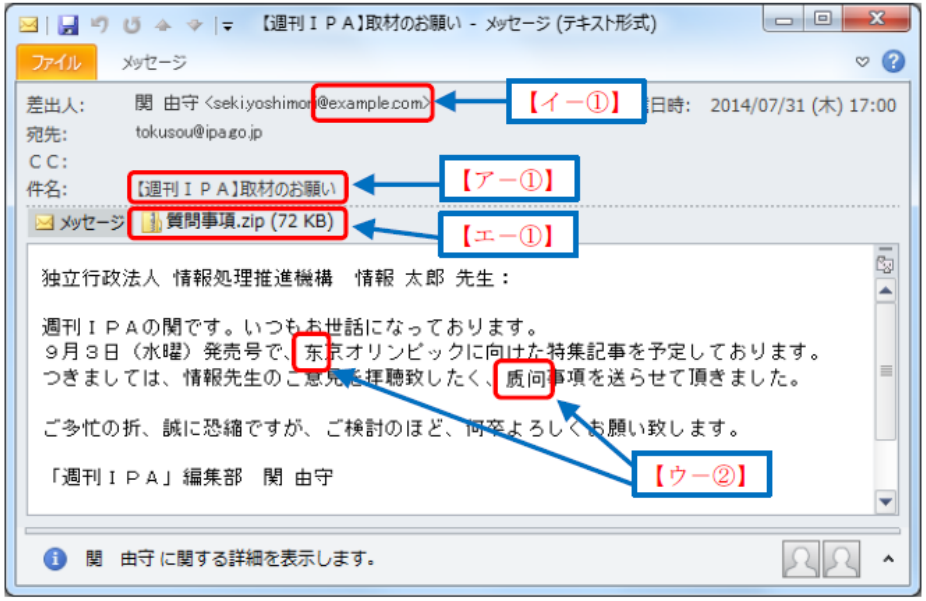
❸ PCを遠隔操作し
ネットワーク探索・感染拡大

❹ C&C(Command &Control)サーバへ
搾取情報を送信

不正プログラムは特別なものではなく、便利ツール等も使われるため、検知が困難。

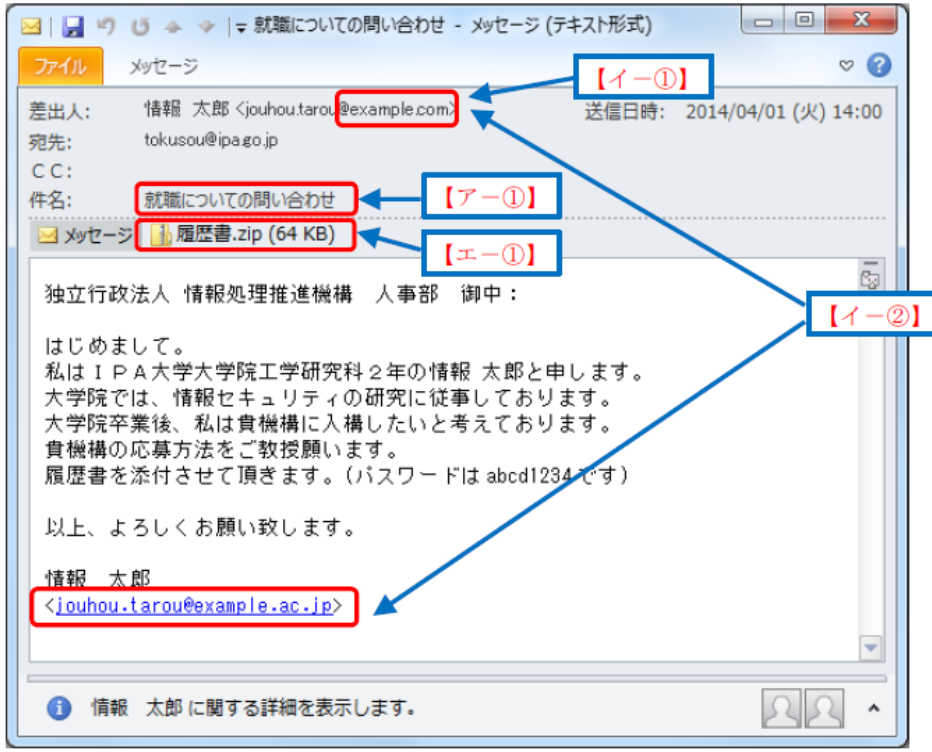
標的型メール攻撃の例(１)

2.2.1. 新聞社や出版社からの取材申込のメール



ケース1
差出人のアドレスが、フリーメールである【イ－①】
日本語では使用されない漢字が使われている【ウ－②】
zip 圧縮ファイルが添付されている【エ－①】

2.2.2. 就職活動に関する問い合わせのメール

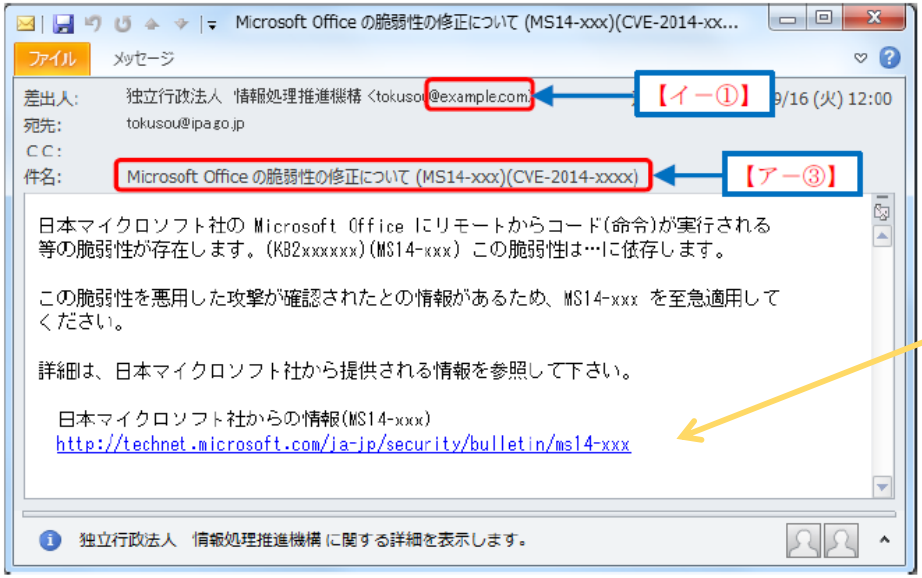


ケース2
差出人のアドレスと署名のアドレスが一致しない【イ－②】

出所:独立行政法人 情報処理推進機構 IPA Technical Watch「標的型メールの例と見分け方」より

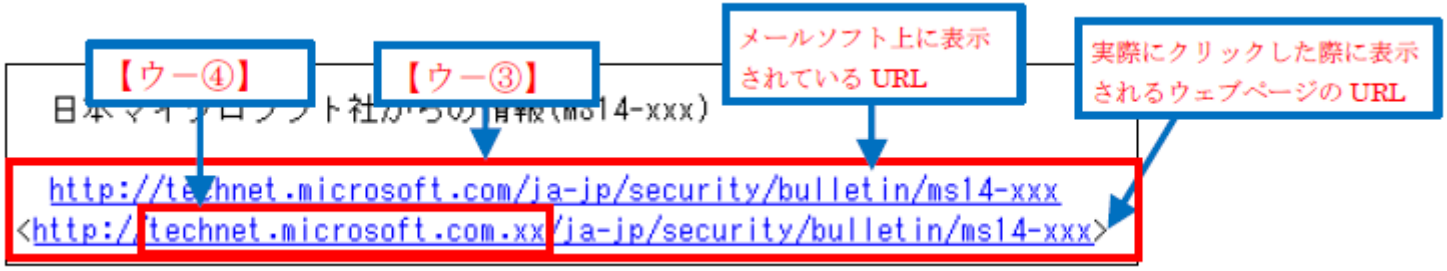
標的型メール攻撃の例（２） HTMLメール

2.2.4.　セキュリティに係る注意喚起のメール



HTMLメールでは
・表示されているURLと
・実際にURLをクリックした際に表示されるWEBページを
別々に設定することができる。

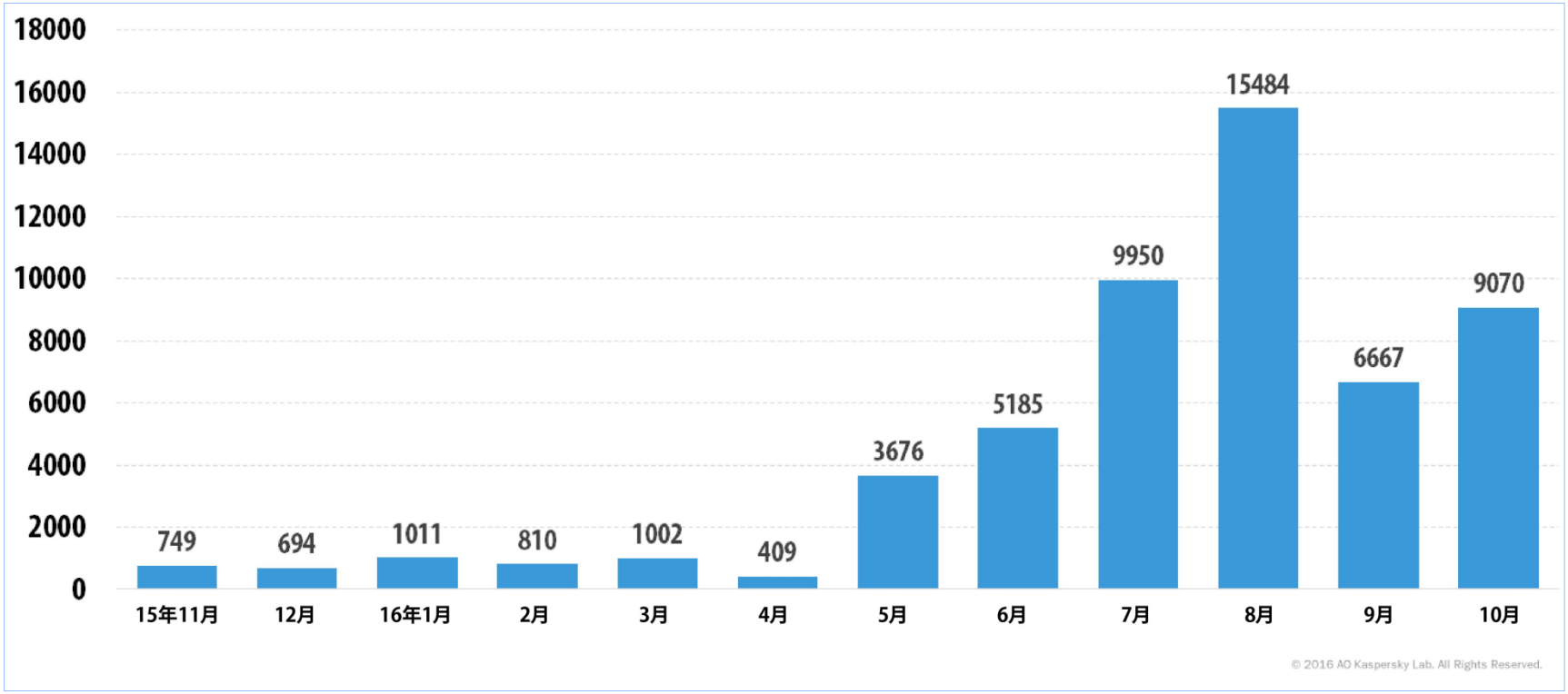
メールの表示形式を「テキスト表示」にすることで、
実際のURLを確認することができる。



出所:独立行政法人　情報処理推進機構　IPA Technical Watch「標的型メールの例と見分け方」より

ランサムウェアの実態（１）

■ カスペルスキーによるレポート： 2015年11月～2016年10月の1年間
暗号化型ランサムウェアの62のファミリーと54,000の亜種を「新たに」確認。

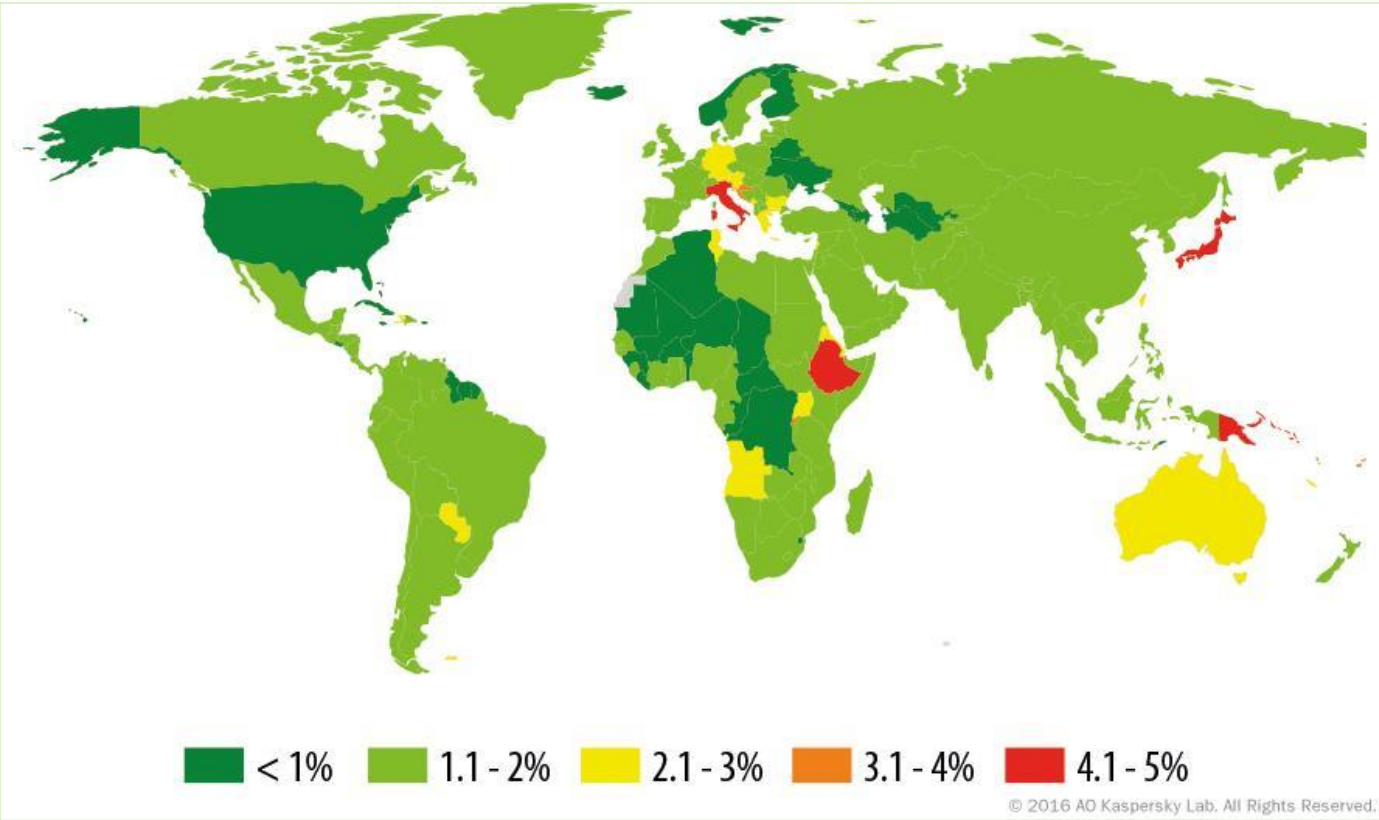


新たに作成された暗号化型ランサムウェアの亜種の数
（2015年11月～2016年10月）

出所：カスペルスキー社 「Kaspersky Security Bulletin 2016 2016年驚異の統計概要」より

ランサムウェアの実態（２）

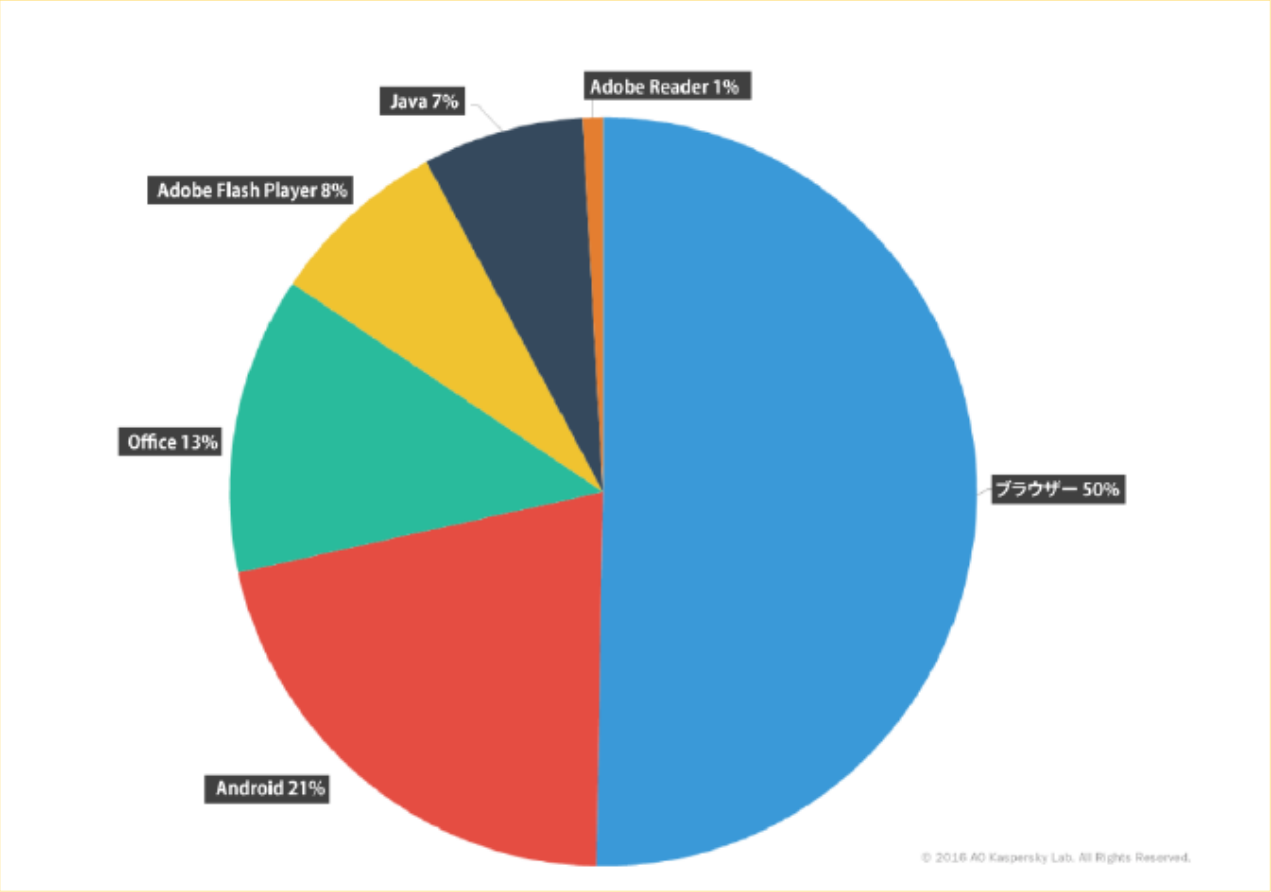
■ もっとも多く暗号化型ランサムウェアの攻撃が確認された国は**日本（4.46%）**



暗号化型ランサムウェア攻撃の地理的分布
（攻撃を受けたユーザーの割合）

出所：カスペルスキー社 「Kaspersky Security Bulletin 2016 2016年驚異の統計概要」より

エクスプロイトのアプリケーション種類別分布



サイバー攻撃に利用されたエクスプロイトのアプリケーション種類別分布（2016年）

出所:カスペルスキー社 「Kaspersky Security Bulletin 2016 2016年驚異の統計概要」より

3．自治体での標的型攻撃への取り組み

自治体における情報連携システムについて

現在

総合行政ネットワーク「LGWAN」(2001年開始)、住民基本台帳ネットワーク(2002年開始)等の接続により、約1,800の自治体を結ぶネットワークシステムが現在運用されている。

今後

2017年7月から、マイナンバー制度の「情報提供ネットワークシステム」の運用が開始される。

- 国の機関、教育委員会、健康保険組合等、5,000以上の団体との情報連携ネットワークの運用が始まる。
- 本ネットワークではマイナンバーは直接用いない。各機関ごとに振り出された「符号」を用いて情報を連携することで、芋づる式に情報が漏えいすることを防止する。

自治体での情報セキュリティ強化の背景(１)

- 2015年1月　サイバーセキュリティ基本法施行
- 2015年5月　日本年金機構での個人情報の流出事件
- 2015年8月　日本年金機構事件に関する調査結果報告
- 2015年10月　マイナンバー制度(行政手続番号法)施行
- 2015年11月　総務省報告書
  「新たな自治体情報セキュリティ抜本的強化に向けて」
  - 自治体情報システム強靱性向上モデル
- 2015年度補正予算 「情報セキュリティ強化対策補助金」

自治体での情報セキュリティ強化の背景（２）

■ 日本年金機構における個人情報流出事案に関する原因究明調査結果

➢ 「4.2. 標的型攻撃に対する情報システム防御策等の考え方」

- メールに添付された実行形式のファイルを取り込まない、起動できないシステム設定とする。

- ウェブ表示がシステム攻撃への糸口を与えることとなることを認識し　～（中略）～　システムの分離を確実に行う。

自治体情報システム強靭性向上モデルの要件

■ 個人番号利用

➢ 個人情報の流出を防ぐこと

- 他システムとの通信禁止、端末からの情報持ち出し禁止、
  端末の二要素認証などの対策を施すこと。

■ LGWAN利用

➢ 通信経路を分離すること

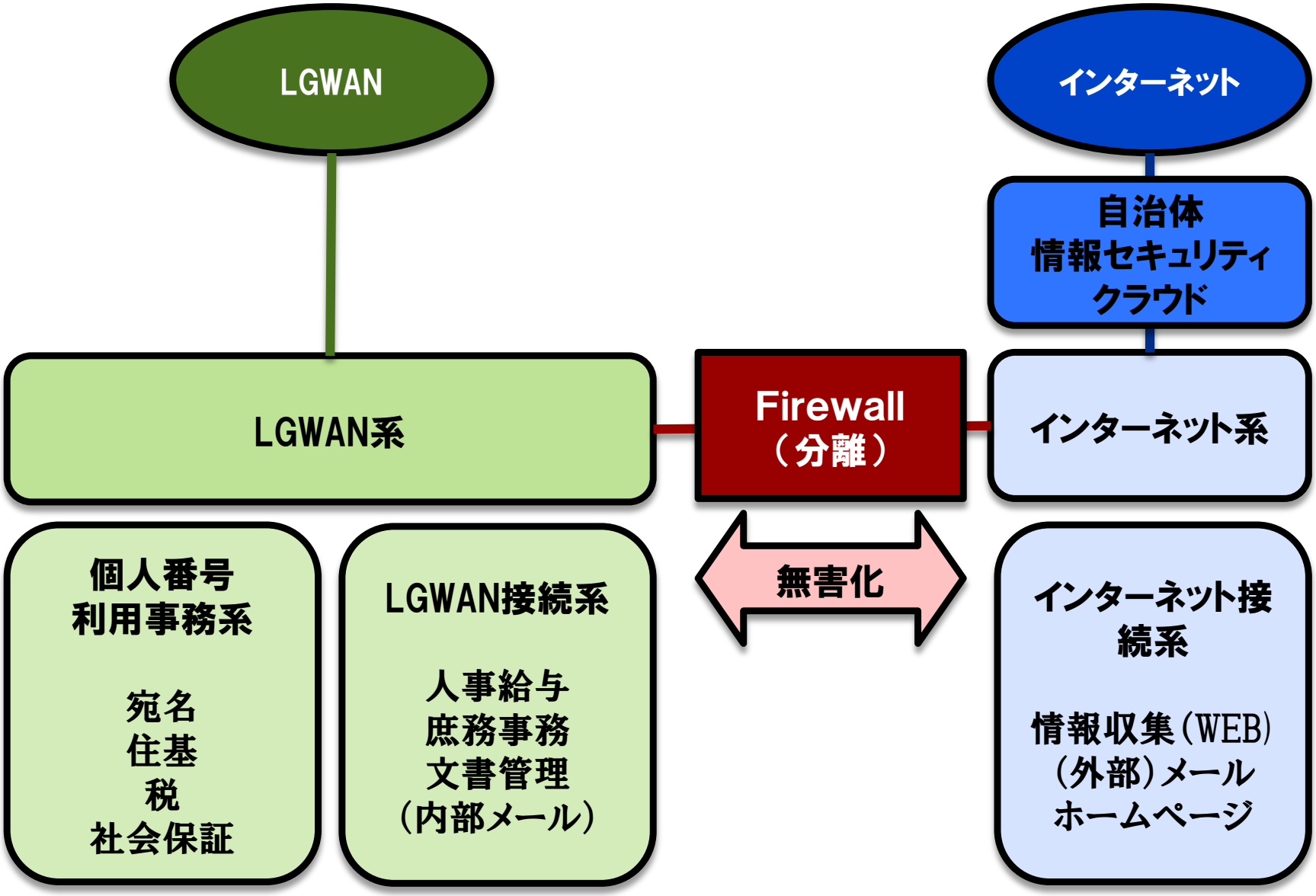
- LGWAN系（業務）とインターネット系（WEB、インターネットメール等）
  の通信経路を分離すること。
- 止むを得ず両ネットワーク間で情報交換を行う際は無害化を図ること。

■ インターネット接続

➢ 自治体情報セキュリティクラウドを構築

- 都道府県・市町村が連携のうえインターネット接続口を集約し
  高度なセキュリティ対策を講じること。

自治体情報システム強靭性向上モデルのイメージ

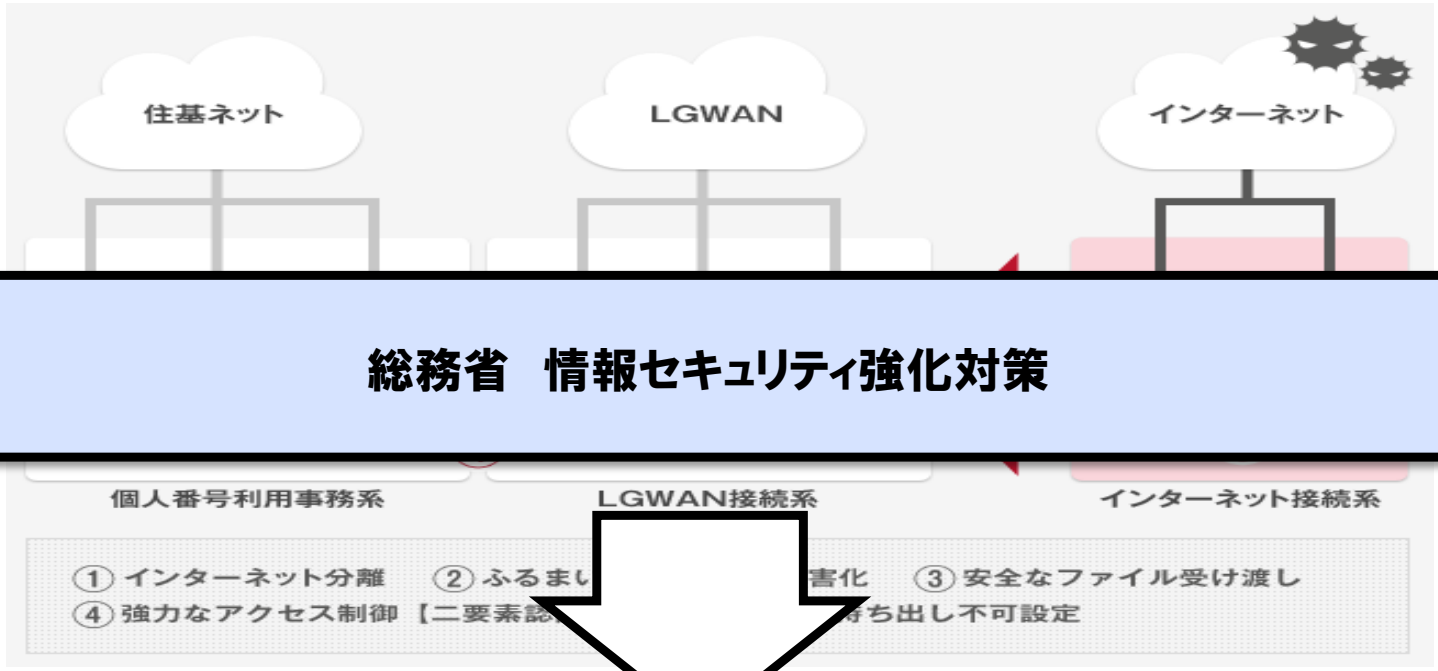


自治体情報システム強靭性向上における対策のポイント

- WEB閲覧・インターネットメールのシステムは分離して構築する。
  - ブラウザの分離→仮想ブラウザ
  - メールの無害化→本文、添付ファイルのサニタライズ

- 分離ネットワークをまたぐ通信は無害化を図ること。
  - 安全なファイル交換→ファイルのPDF化など

標的型攻撃対策の必要性の高まり



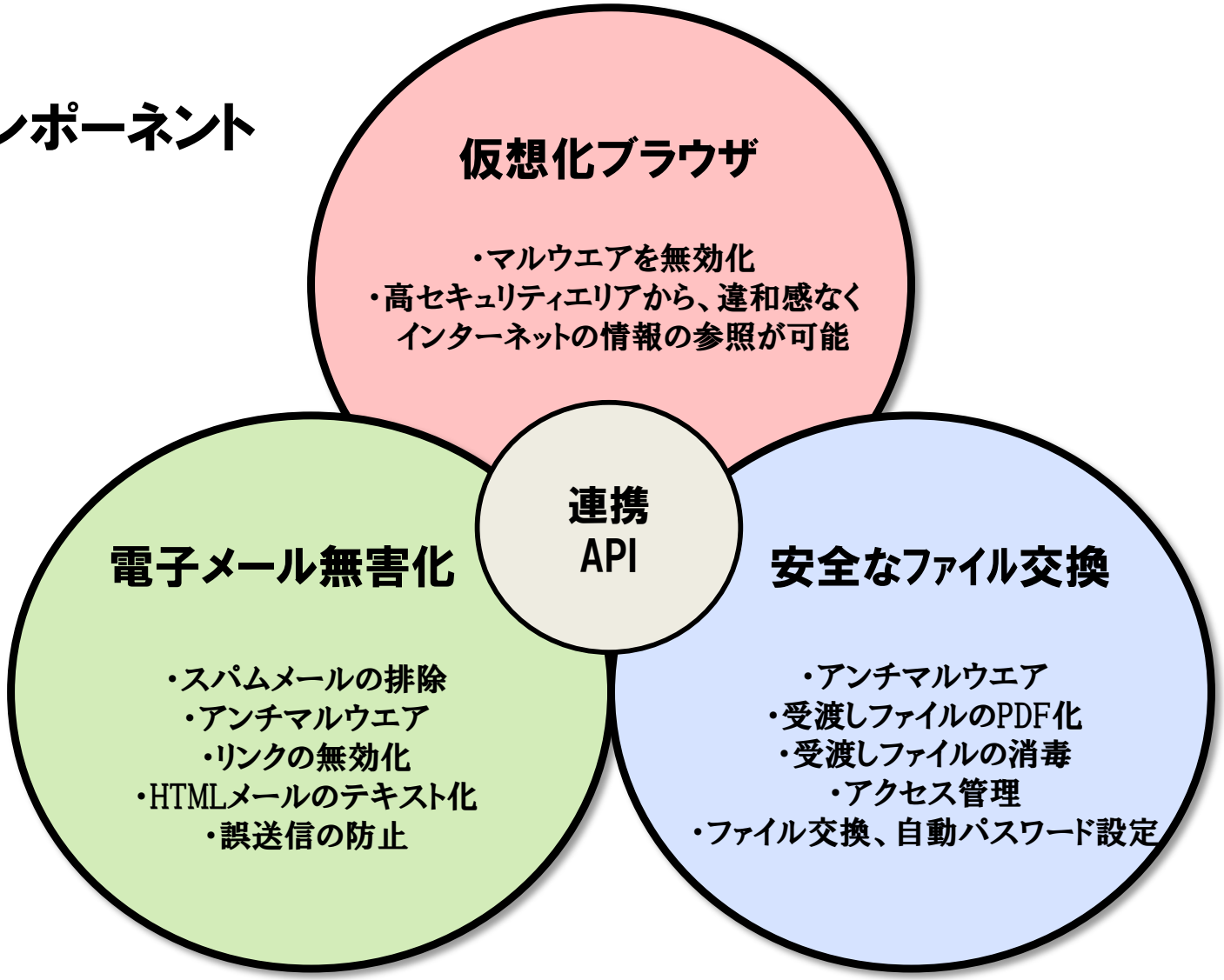
総務省　情報セキュリティ強化対策

金融庁、厚生労働省、文部科学省など他省庁でも同様の動きに。
民間企業でもネットワーク分離の検討が進む。

4. ソリューション例

標的型攻撃対策ソリューションの製品構成

主要コンポーネント

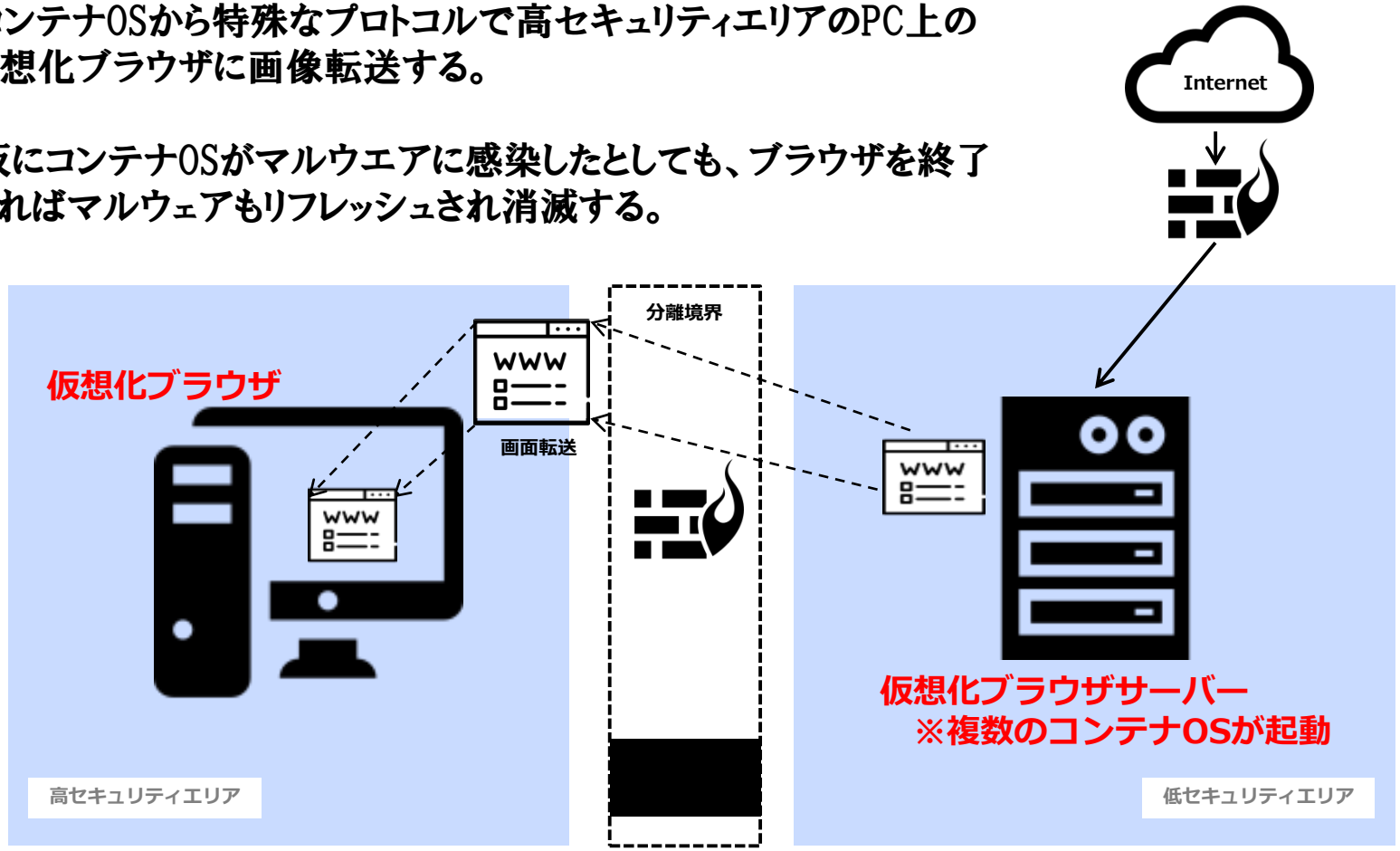


標的型攻撃対策ソリューション(１)仮想ブラウザ

①インターネットへは仮想化ブラウザサーバー上で一時的に起動する
コンテナOSから接続する。

②コンテナOSから特殊なプロトコルで高セキュリティエリアのPC上の
仮想化ブラウザに画像転送する。

③仮にコンテナOSがマルウエアに感染したとしても、ブラウザを終了
すればマルウェアもリフレッシュされ消滅する。

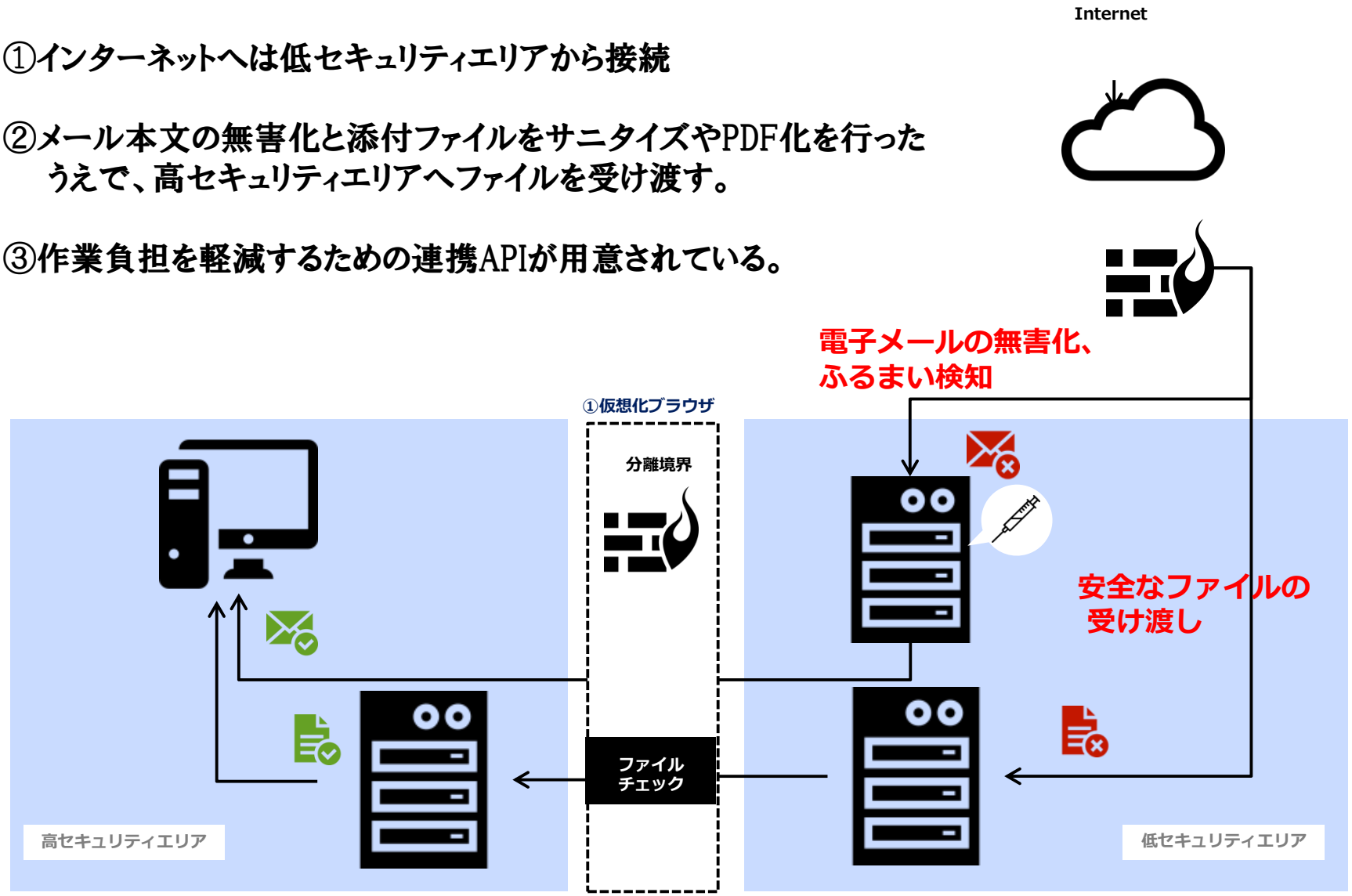


標的型攻撃対策ソリューション(２)メール無害化、ファイル交換

①インターネットへは低セキュリティエリアから接続

②メール本文の無害化と添付ファイルをサニタイズやPDF化を行った
うえで、高セキュリティエリアへファイルを受け渡す。

③作業負担を軽減するための連携APIが用意されている。



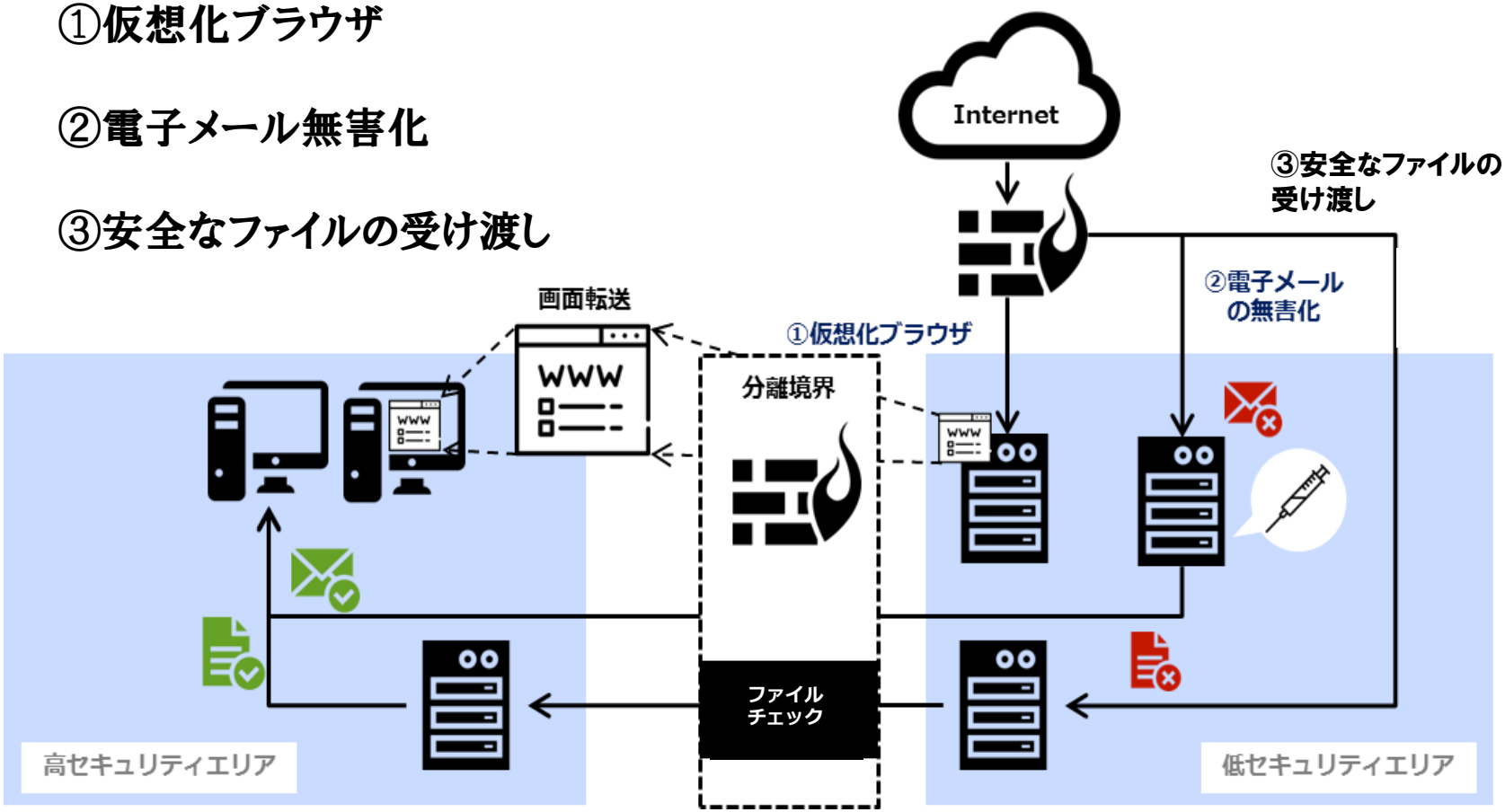
標的型攻撃対策ソリューション(３)全体構成

３つの製品で、総務省指針を実現

①仮想化ブラウザ

②電子メール無害化

③安全なファイルの受け渡し



5. 製品選定における考慮点

仮想ブラウザ選定時の考慮点

機能

- 利用するブラウザの種類：IE、Chrome、Firefox
- 動画・音声再生の要否
- 同時利用ユーザ数

費用

- サーバのハードウェアリソース
- マイクロソフトのRDS (Remote Deskotp Services) ライセンス

無害化機能選定時の考慮点

- **無害化の定義を明確にする**
  - アンチスパム、アンチウイルスソフトによるチェック
  - HTMLパートの削除
  - 添付ファイルのテキスト化、添付ファイルのPDF化
  - ファイルのマクロ無効化
  - ファイルの正規フォーマットに応じた無害化処理の実行
    - 実行可能コードが埋め込まれ得る箇所を無害化
    - 本来のファイル機能に影響し得ない不明な領域を削除
  - 対応するアプリケーションの確認
    - マイクロソフトOffice、一太郎、CADソフトなど
  - 日本語対応
    - メニュー・メッセージの日本語化
    - 2バイトコードに対応したスキャンエンジン

ご清聴ありがとうございました