研究会 Agenda

開始時間	終了時間	内容	講師
13:30	13:40	ガイダンス	事務局
13:40	14:25	自治体におけるゼロトラストネットワークとゼロトラストPCの必然性	奥野様
14:25	14:45	【事例紹介】αモデルで利便性を向上させた那覇市様の事例 ～端末内仮想化技術の活用～	奥野様
14:45	15:00	休憩	
15:00	16:10	情報共有会（ワークショップ）	山形様
16:10	16:20	アンケート・次回のご案内等	事務局

アジェンダ

１．自治体セキュリティ強靭化策の現状と見直し
２．サイバー攻撃の現状
３．次期自治体情報セキュリティ強靭化の方向性について
４．ゼロトラストネットワークによるセキュリティ強靭化モデル例

自己紹介

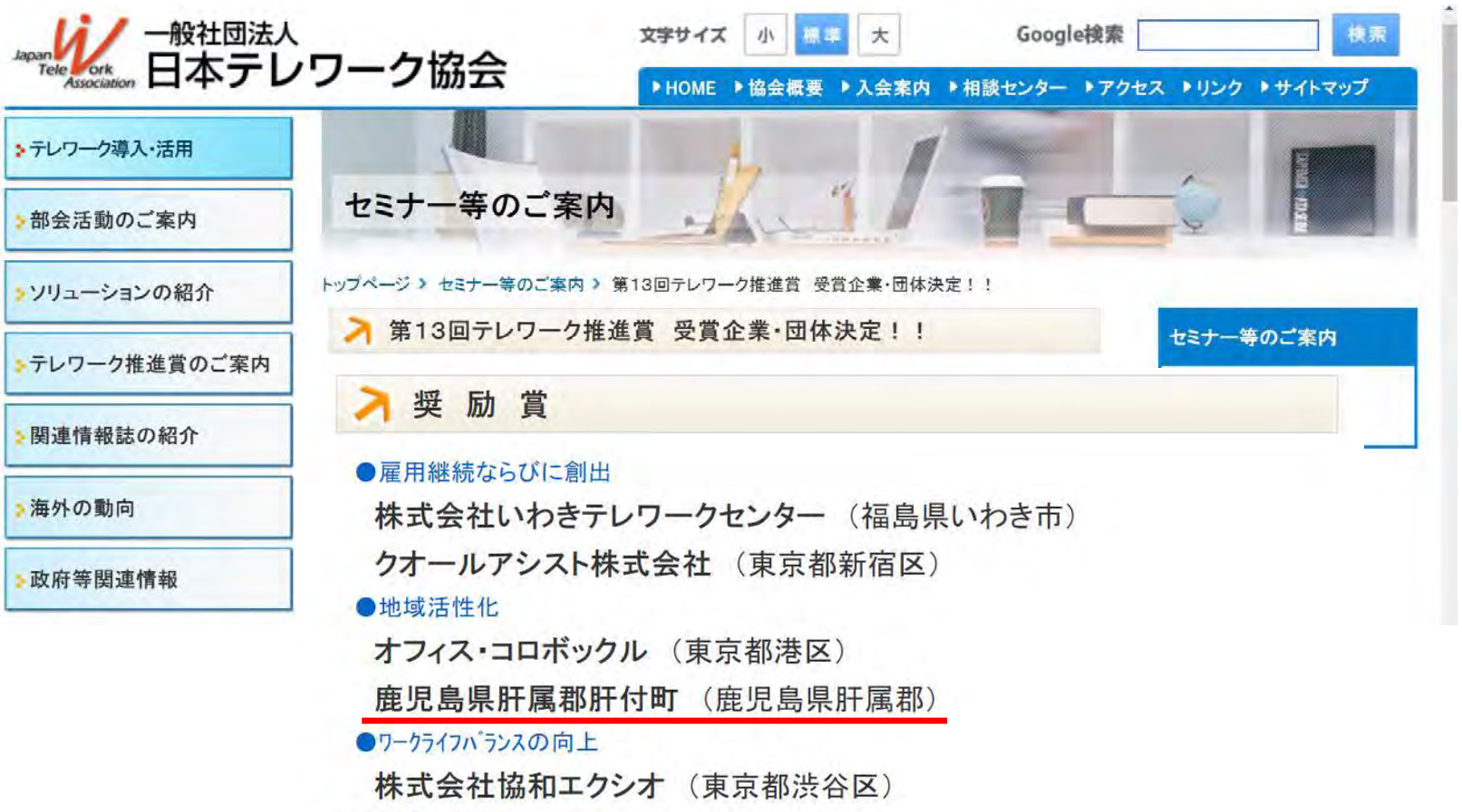
■　職名等
株式会社シンクライアント総合研究所　取締役

■　実績（経歴事項）
1993年NTTデータ通信株式会社（現株式会社NTTデータ）入社
公共システム事業本部在籍時より、情報システムの最適化支援活動に従事、総務省、経産省等の関連官庁と連携し、1999年特定非営利活動法人ASP・SaaSインダストリコンソーシアム（ASPIC）に発起人の一人として参画。初代事務局長としてASP・SaaS事業者、官公庁などの協力を得て、ASP・SaaSの普及啓発、市場創造などの活動を行い、政策・制度立案支援、コンサルティング活動に従事

NTTデータ退職後、2012年シンクライアント総合研究所設立（現取締役シニアコンサルタント）、政令指定都市、中核市、小規模自治体や、民間法人に対する情報基盤最適化対応支援　（コンサルティング）及びセキュリティ監査、リスクアセスメントに従事

現在
・沖縄県某自治体CIO補佐官
・某独立行政法人デジタル統括アドバイザー

活動実績



地方自治体で初のテレワーク推進賞受賞をコンサルタントとして支援
（鹿児島県肝属郡肝付町）

１．セキュリティ強靭化策の現状と見直し

約５年前：自治体情報強化のための抜本的対策「３層の構え」

年金機構はじめ、度重なる情報漏えい事件の影響から、H28年7月稼働予定のマイナンバーにおける情報提供ネットワークシステムの稼働を見据え、「機密性」はもとより、「可用性」や「完全性」の確保にも十分配慮された攻撃に強い内部ネットワーク等の構築を図ることが望まれる。

個人情報保護の３原則

情報セキュリティ＝「情報資産」全般の機密性、完全性、可用性を確保すること

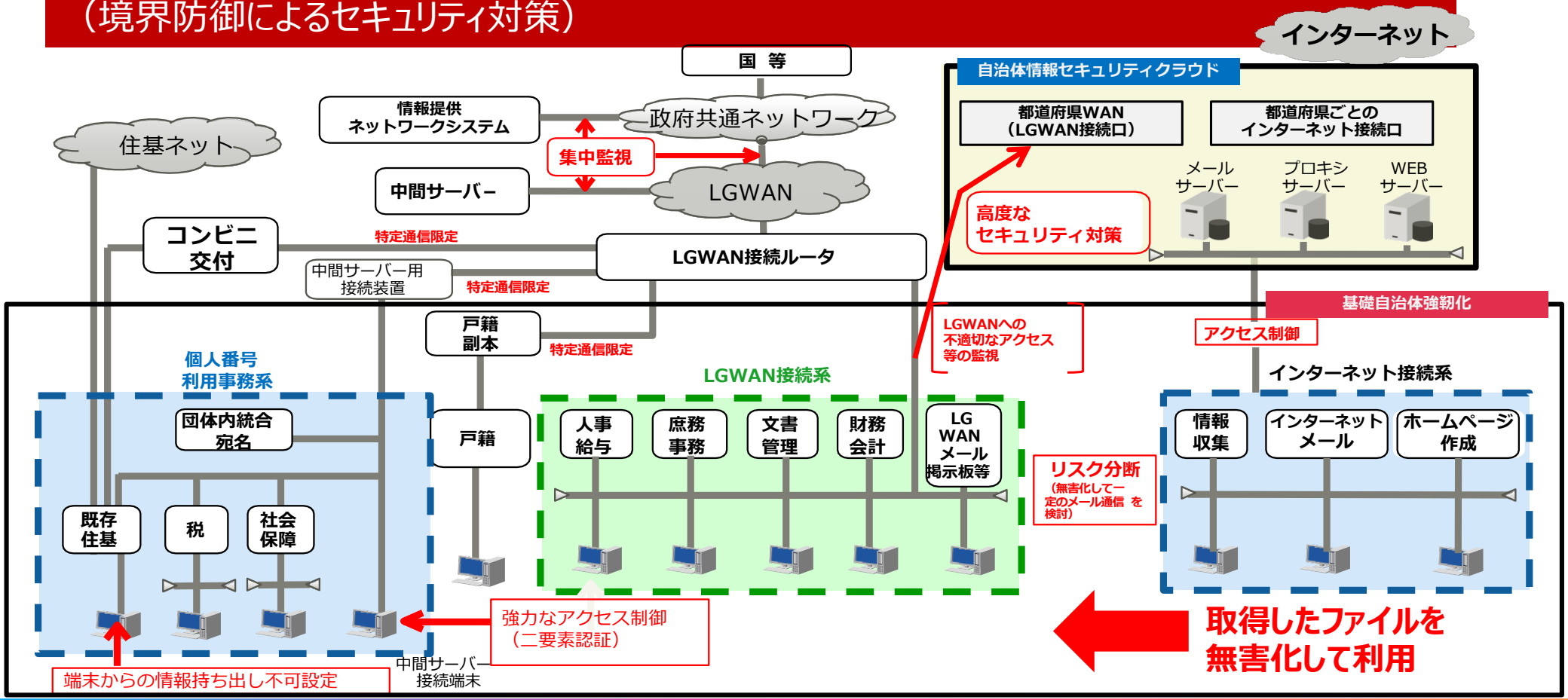
機密性	許可された者だけが情報にアクセスできるようにすること。 許可されていない利用者は、コンピュータやデータベースにアクセスできないようにしたり、データを閲覧できるが書き換えることはできないようにする。
可用性	許可された者が必要なときにいつでも情報にアクセスできるようにすること。可用性の維持は、情報を提供するサービスが常に動作するということ。
完全性	保有する情報が正確であり、完全である状態を保持すること。情報が不正に改ざんされたり、破壊されたりしないこと。

＜三層の構えで万全の自治体情報セキュリティ対策の抜本的強化を実施＞

1. マイナンバー利用事務系（既存住基、税、社会保障など）においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への二要素認証の導入等を図ることにより、住民（個人）情報の流出を徹底して防ぐこと。
2. マイナンバーによる情報連携に活用されるＬＧＷＡＮ環境のセキュリティ確保に資するため、財務会計などＬＧＷＡＮを活用する業務用システムと、Ｗｅｂ閲覧やインターネットメールなどのシステムとの通信経路を分割すること。なお、両システム間で通信する場合には、ウイルスの感染のない無害化通信を図ること（ＬＧＷＡＮ接続系とインターネット接続系の分割）。
3. インターネット接続系においては、都道府県と市区町村が協力してインターネット接続口を 集約した上で、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を講じること。

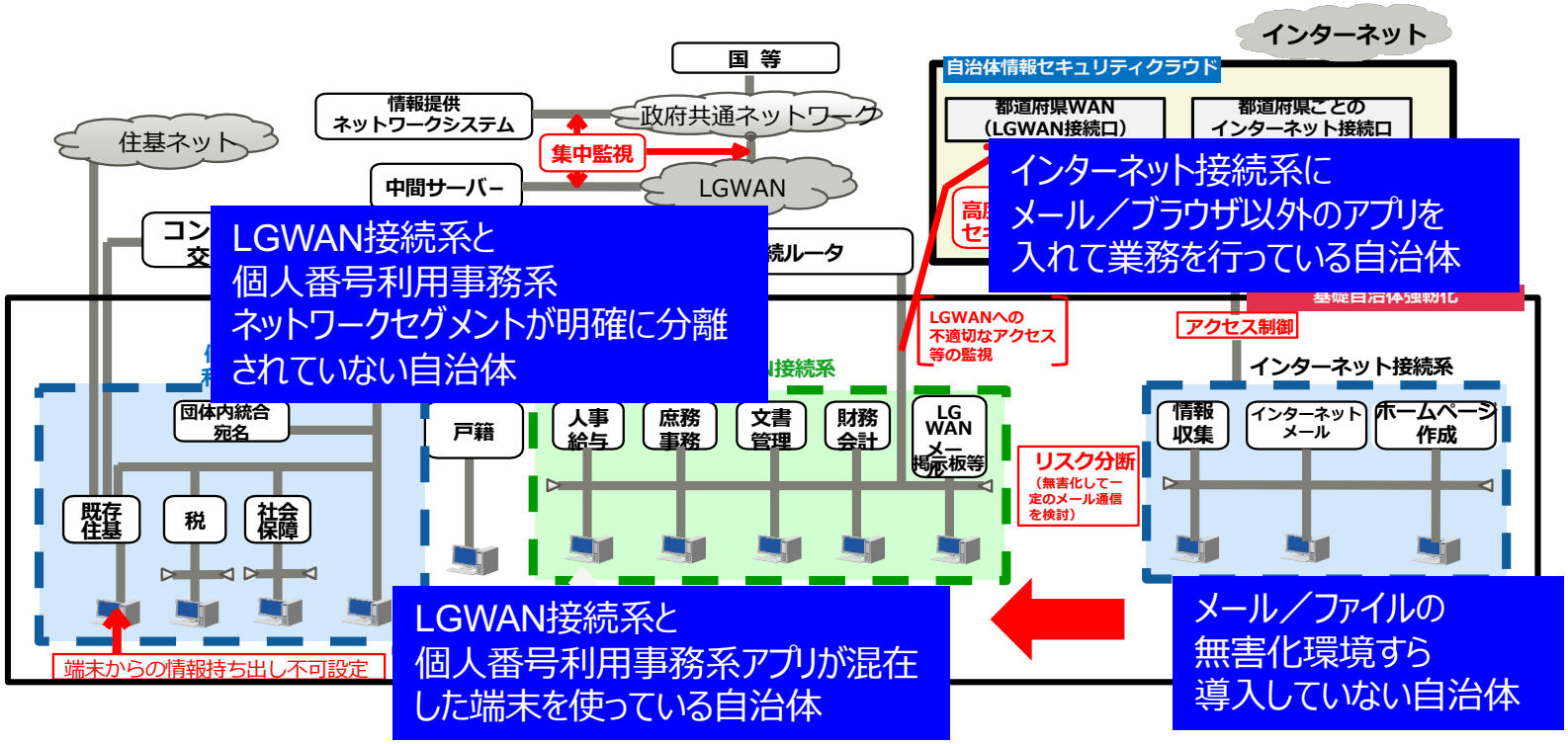
地方自治体のセキュリティ強靭化対策

平成28年度の補正予算により、一律環境整備
情報資産重要性分類により適切なネットワークエリアに分割して利用させる環境を整備
（境界防御によるセキュリティ対策）



実際は・・・

平成28年度の補正予算額の関係から対応できる対策は限られる
総務省のガイドラインに適合した環境整備を行っていない自治体は少なくない



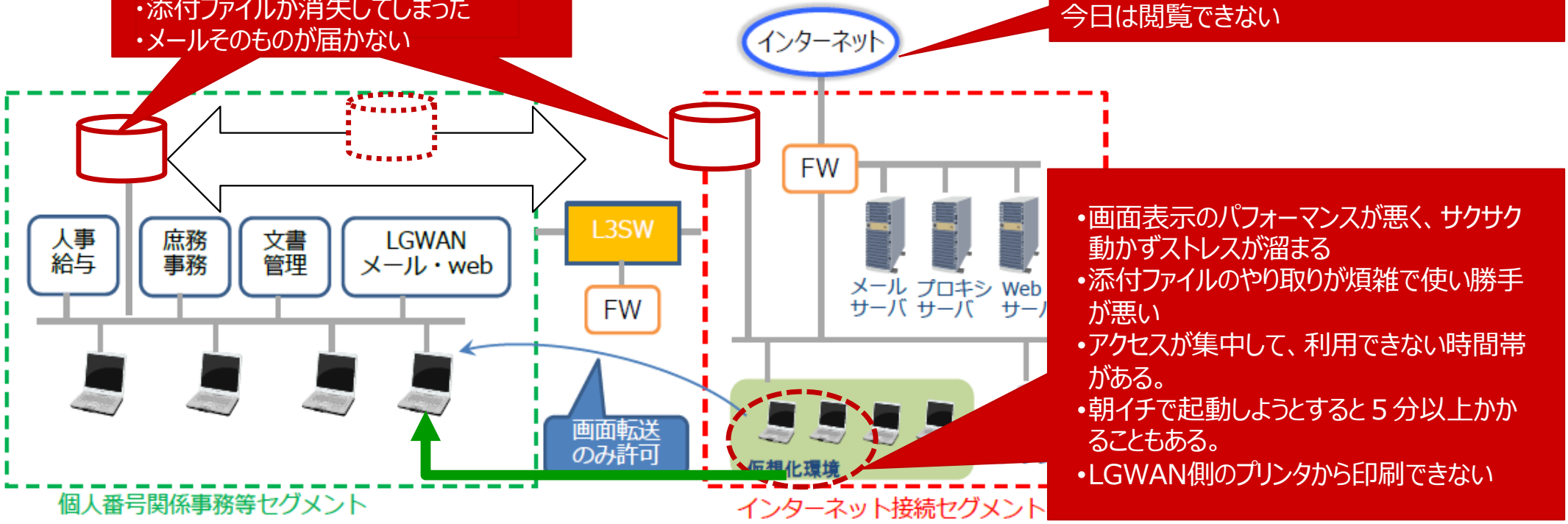
現行の無害化対策(大部分の自治体が仮想化環境を導入)

出典:
新たな自治体情報セキュリティ対策の抜本的強化(案)
等の報告について(2015.10.23)

・個人番号関係事務等セグメントとインターネット接続セグメントを分割する
・個人番号関係事務等セグメントの端末において、仮想化環境から転送された画面を操作してインターネットメール、Webが参照可能となる
・インターネットメール、Webの印刷はインターネット接続環境のプリンタを使用する

・ファイルによっては無害化できない
・添付ファイルが消失してしまった
・メールそのものが届かない

昨日閲覧できたWebサイトが
今日は閲覧できない



・画面表示のパフォーマンスが悪く、サクサク動かずストレスが溜まる
・添付ファイルのやり取りが煩雑で使い勝手が悪い
・アクセスが集中して、利用できない時間帯がある。
・朝イチで起動しようとすると５分以上かかることもある。
・LGWAN側のプリンタから印刷できない

現行の無害化対策(大部分の自治体が仮想化環境を導入)

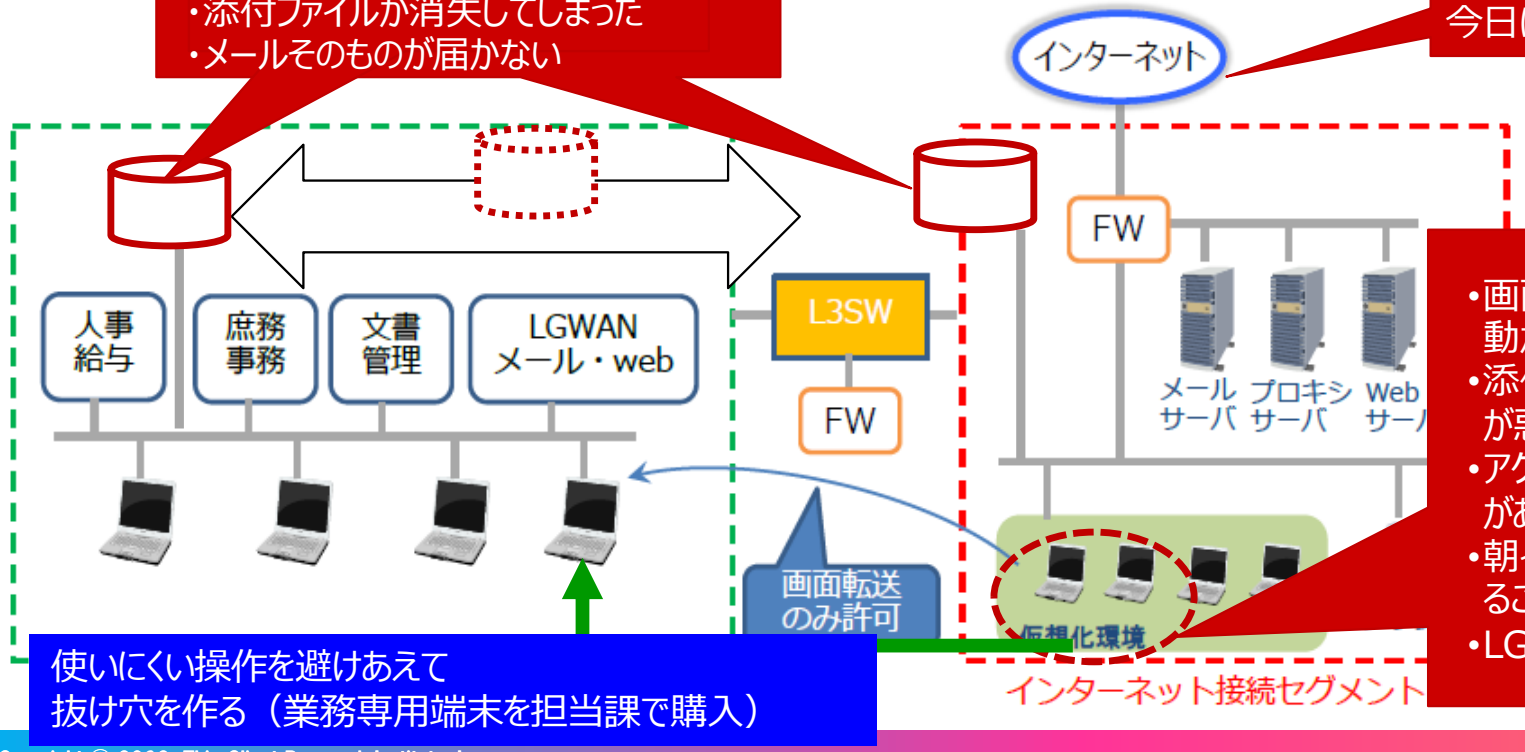
出典:
新たな自治体情報セキュリティ対策の抜本的強化(案)
等の報告について(2015.10.23)

・個人番号関係事務等セグメントとインターネット接続セグメントを分割する
・個人番号関係事務等セグメントの端末において、仮想化環境から転送された
可能となる
ト接続環境のプリンタを

無害化処理を介さないファイル交換が常態化
（一応ウィルススキャンはするけど）

・ファイルによっては無害化できない
・添付ファイルが消失してしまった
・メールそのものが届かない

昨日閲覧できたWebサイトが
今日は閲覧できない



業務専用情報端末の購入
（Web会議用、テレワーク用）
個人端末の持ち込み（シャドーIT）

- 画面表示のパフォーマンスが悪く、サクサク動かずストレスが溜まる
- 添付ファイルのやり取りが煩雑で使い勝手が悪い
- アクセスが集中して、利用できない時間帯がある。
- 朝イチで起動しようとすると５分以上かかることもある。
- LGWAN側のプリンタから印刷できない

使いにくい操作を避けあえて
抜け穴を作る（業務専用端末を担当課で購入）

現行の無害化対策(大部分の自治体が仮想化環境を導入)

出典:
新たな自治体情報セキュリティ対策の抜本的強化(案)
等の報告について(2015.10.23)

・個人番号関係事務等セグメントとインターネット接続セグメントを分割する
・個人番号関係事務等セグメントの端末において、仮想化環境から転送された
可能となる
ト接続環境のプリンタを

無害化処理を介さないファイル交換が常態化
（一応ウィルススキャンはするけど）

・ファイルによっては無害化できない
・添付ファイルが消失してしまった
・メールそのものが届かない

昨日閲覧できたWebサイトが
今日は閲覧できない

インターネット

都道府県情報セキュリティクラウドの刷新が予定されている令和５年度以降
不十分な技術的安全管理措置のまま
システム更改が予定される年度以降も同じ環境を用いるのか？

自治体DXや職員の働き方改革が現行の環境で遂行できるのか？

人事
給与

使いにくい操作
抜け穴を作る（業務専用端末を担当課で購入）

画面転送
のみ許可

仮想化環境

がある。
•朝イチで起動しようとすると５分以上かかることもある。
•LGWAN側のプリンタから印刷できない

個人番号関係事務等セグメント

インターネット接続セグメント

現行自治体システム強靭化の課題

◎サイバー対策副作用で業務に支障　４５都道府県の３００超市区町村
H28年11月のマイナンバー制度の本格運用を前に全国の自治体がサイバーセキュリティー対策を強化したところ、住民や民間業者からのメールや申請書類が届かないといったトラブルに見舞われ、４５都道府県の３００超の市区町村で業務に支障が出ていたことが、共同通信の調査で８日分かった。
高度なセキュリティーシステムを導入した結果、問題のないメールや添付書類が、迷惑メールや安全性が疑わしいファイルと誤認され、自動的に削除されるケースが続出した。安全対策の思わぬ「副作用」が、行政サービスの低下につながった形だ。政府も問題を把握しており、対策の検討に入った。

＜2018.1.9 共同通信ニュースサイトより＞

政府がマイナンバー制度の導入を推し進める上で最大の懸念事項である
特定個人情報の漏えいを防ぐための各種セキュリティ強靭化施策を徹底した結果、業務に支障が生じ、結果として業務生産性をかえって低下させている状況が顕在化し、自治体DXにおける新たな課題が発生

セキュリティ強靭化対策の限界①

9500人分のコロナ感染者情報流出　福岡県

出典：産経新聞Webサイト2021/1/6

福岡県は6日、県が管理する新型コロナウイルス感染者の氏名や症状などの個人情報約9500人分が外部に流出したと発表した。県内で確認された感染者のほぼ全員分。メールの誤送信により、部外者の男性がインターネット上で閲覧できる状態になっていた。県は、この男性以外が閲覧した可能性は低いとみている。
県は、2020年4月から入院先の調整のため、陽性判明者の居住自治体や年齢、性別なども含む書類をネット上の文書共有システムで管理していた。県のコロナ対策本部が同11月30日、医療関係者にシステムへのアクセス権が付いたメールを送ろうとした際、記入するアドレスを間違えた。

メールを受け取った男性が同日、対策本部に連絡。県は男性からのアクセスを遮断するための措置を取ったが、対応が不十分で、文書ファイルのURLを入力すれば閲覧できる状態が続いていた。
県は一部報道を受けて今月6日に流出が続いていることを把握し、システム上の関連書類を全て削除した。保健医療介護部の飯田幸生部長は記者会見で「個人情報の漏洩事案を起こし申し訳ない」と謝罪した。

職員の過失により、機微情報が流出する深刻な事態に発展（誤操作、設定ミス）

セキュリティ強靭化対策の限界②

都の委託業者にサイバー攻撃、個人情報など約９万件流出

出典：産経新聞Webサイト2021/3/21

東京都は２２日、住宅政策を推進するための基本計画「都住宅マスタープラン」作成業務の一部を委託していた都内のコンサルタント会社がサイバー攻撃を受け、都内のマンション管理組合へのアンケート結果など約８万７２００件のデータが流出した可能性があると発表した。このうち、マンション所有者の氏名など個人情報は約８２００件に上る。都によると、現時点でデータ流出による被害は確認されていないという。

サイバー攻撃を受けたコンサルタント会社は都市計画などを手がけており、都は「都住宅マスタープラン」の作成に当たり、調査業務をこの会社に委託し、業務に必要な情報も一部を提供した。調査の一環としてマンションの管理組合などにアンケートを実施しており、こうしたデータの一部が流出したという。

２月２３日に会社のサーバーに異常が確認され、コンピューターウイルスの感染が判明した。この会社は全国の自治体からコンサルタント業務を請け負っており、他の自治体のデータでも被害が確認されている。都は、３月末までに原因や今後の対策などの最終調査結果の報告を受けるといい、再発防止策などの検討を急いでいる。

報道発表資料　2021年03月22日　住宅政策本部

委託業務受託者のサーバーにおけるコンピューターウイルス感染について

住宅政策本部（以下「本部」という。）において業務委託を行っている事業者（以下「受託者」という。）のサーバーが第三者からのサイバー攻撃によりコンピューターウイルスに感染し、本部が貸与したデータがサーバーから流出した可能性があると報告を受けましたので、お知らせいたします。

1　委託内容

- 委託件名：新たな東京都住宅マスタープラン策定に係る調査委託
- 委託期間：令和2年9月29日から令和3年3月24日まで
- 受託者：ランドブレイン株式会社（東京都千代田区平河町1-2-10）

2　経緯

1. 2月23日（火曜日）未明に、受託者の本社サーバーがコンピューターウイルスに感染
2. 2月26日（金曜日）午後、受託者から本部に状況の報告
3. 3月22日（月曜日）受託者から本部に現在までの調査状況の中間報告

3　本部から受託者へ貸与し、流出の可能性のあるデータ

住民の個人情報収集は各々の根拠規定により目的が明示され、異なる事業の為にデータを抽出して委託業者に提供する場合、目的外利用や外部提供、自治体のの個人情報保護条例に抵触する行為

強靭化対策を徹底している「はずの」自治体でも「抜け穴」は必ず発生する（業務効率化の名のもとに）

セキュリティ強靭化対策の限界②

都の委託業者にサイバー攻撃、個人情報など約９万件流出

出典：産経新聞Webサイト2021/3/21

東京都は２２日、住宅政策を推進するための基本計画「都住宅マスタープラン」作成業務の一部を委託していた都内のコンサルタント会社がサイバー攻撃を受け、都内のマンション管理組合へのアンケート結果など約８万７２００件のデータが流出した可能性があると発表した。このうち、マンション所有者の氏名など個人情報は約８２００件に上る。都によると、現時点でデータ流出による被害は確認されていないという。

サイバー攻撃を受けたコンサルタント会社は都市計画などを手がけており、都は「都住宅マスタープラン」の作成に当たり、調査業務をこの会社に委託し、業務に必要な情報も一部を提供した。調査の一環としてマンションの管理組合などにアンケートを実施しており、こうしたデータの一部が流出したという。

２月２３日に会社のサーバーに異常が確認され、コンピューターウイルスの感染が判明した。この会社は全国の自治体からコンサルタント業務を請け負っており、他の自治体のデータでも被害が確認されている。都は、３月末までに原因や今後の対策などの最終調査結果の報告を受けるといい、再発防止策などの検討を急いでいる。

報道発表資料　2021年03月22日　住宅政策本部

委託業務受託者のサーバーにおけるコンピューターウイルス感染について

住宅政策本部（以下「本部」という。）において業務委託を行っている事業者（以下「受託者」という。）のサーバーが第三者からのサイバー攻撃によりコンピューターウイルスに感染し、本部が貸与したデータがサーバーから流出した可能性があると報告を受けましたので、お知らせいたします。

1　委託内容

- 委託件名：新たな東京都住宅マスタープラン策定に係る調査委託
- 委託期間：令和2年9月29日から令和3年3月24日まで
- 受託者：ランドブレイン株式会社（東京都千代田区平河町1-2-10）

2　経緯

1. 2月23日（火曜日）未明に、受託者の本社サーバーがコンピューターウイルスに感染
2. 2月26日（金曜日）午後、受託者から本部に状況の報告
3. 3月22日（月曜日）受託者から本部に現在までの調査状況の中間報告

3　本部から受託者へ貸与し、流出の可能性のあるデータ

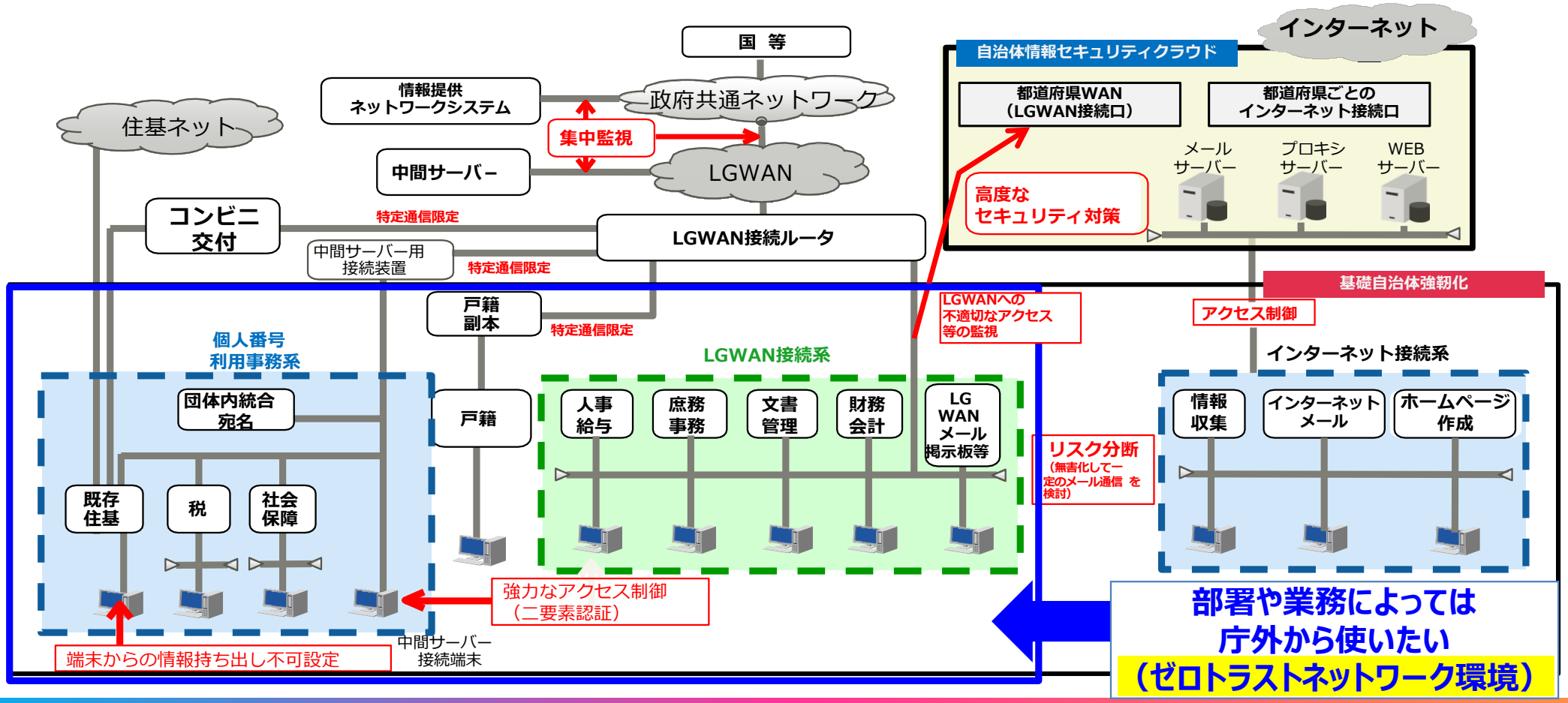
NTTデータ関西がEmotet感染、自治体等向けの電子申請サービス問い合わせメールが流出

株式会社NTTデータ関西は7月1日、Emotet感染による不審メールの送信について発表した。

株式会社NTTデータ関西は7月1日、Emotet感染による不審メールの送信について発表した。
これは同社が自治体等向けに提供する電子申請サービスのヘルプデスク業務で使用するPC8台のうち1台がEmotet感染し、当該PCに保存されていた過去に送受信したメールが流出し、同社ヘルプデスクを装った攻撃者からの不審メールの発信を確認したというもの。6月6日に、電子申請サービスのヘルプデスクアドレスを騙った不審メール1件の申告があり、その後、複数の団体から同様の申告があり発覚した。

強靭化対策の先にある業務環境

**自治体DXの視点から、少しでも使いやすい業務環境整備を目指し、出張時、緊急対応時
本庁以外の拠点（現場、出張所）で柔軟に利用できるシステム環境が求められている**



リモートアクセス環境整備における現行のセキュリティ要件

	臨時業務	出先業務	在宅業務
	通常の執務場所（庁舎等）以外の建物を臨時に執務場所として利用する。（一時的に占有した屋内）	庁外の公の場所や個人宅等で訪問業務を行う。	職員の自宅で業務を行う。
例	・選挙（共通投票所等） 8/10 報告 ・繁忙期の臨時窓口	・固定資産調査 ・介護認定、審査会	・在宅業務
利用場所	・臨時の執務環境、公共施設（ある程度のコントロール可能）	・公の場所、個人宅（コントロールが難しい）	・自宅
管理・モラル	・複数の職員と共同作業、上司の存在	・少人数ながら複数の職員で行動するケースが多い	・同僚不在
必要端末数	・拠点数×数台	・出先業務を行う課×数台	・全体職員数の一定割合
利用回線	・専用線または、それに準じるもの ・専用線、IP-VPN、SSL-VPN ・携帯回線（LTE）：暗号化		・携帯回線？ ・Wifi？ ・インターネット？
端末・認証	・貸与端末 ・シンクライアント／ハードディスクに情報を保存しない設定 ・（多要素認証）		・貸与端末？ ・私物の端末＋デバイス認証？
アクセス情報機　能	・外部からのアクセス用に限定された情報 ・一部機能		・限定された情報？
検討課題	・認証情報の登録（臨時職員）	・外部からアクセスできる情報、機能、収納するサーバ	・業務の切り分け

出典：地域力創造グループ地域情報政策室（平成31年4月25日）

コロナ禍においては、役所の貸与端末の取り扱いが煩雑で使い勝手が十分とは言えない

２．サイバー攻撃の現状

情報セキュリティリスクにおける脅威は多様

PCの置き忘れや誤送信などの過失を除いた場合、全体の8割以上が外部からの攻撃により漏洩しているのが現状です。

内部からの脅威

組織内部の人が脅威になっている

【故意】職員や関係者による脅威

・不正な持ち出し
(個人情報/機密情報の漏えい)

堺市職員の住民情報持ち出し
ベネッセ社の個人情報漏洩
弘前市職員個人情報漏えい
神奈川県庁取引業者のHDD売却

【過失】職員や関係者による脅威

・システムの誤操作/メールの誤送信
(情報漏えい、情報の消失・改変)

外部データセンターのデータ消失

・記録媒体の盗難/紛失、(情報漏えい)

大手Sierの個人情報漏えい

外部からの脅威

組織外部の人が脅威になっている

サイバー攻撃<不正アクセス型>

主にサーバへの直接攻撃
(個人情報漏洩、WEBサイト改ざん、WEBサイトのアクセス障害)

角川書店・トヨタ・日産のWebサイト改ざん
日本テレビ・プレイステーションnetの個人情報漏洩
日本政府に対するＤＤｏｓ攻撃

サイバー攻撃<標的型>

主に未知のマルウェアを利用した侵入
(機密情報漏洩、個人情報漏洩、システム不正操作と破壊)

JTBや日本年金機構、JALの個人情報漏洩
首都大学東京
京都市観光協会なりすましメール
本邦防衛関連団体に対する標的型攻撃
イラン原子力施設／ウクライナ変電所への攻撃
韓国・金融機関/マスメディアへのサイバーテロ

攻撃パターンと考えられる被害

◎標的型攻撃／ATP（Advanced Persistent Threat）攻撃

組織内の特定のユーザーまたは部門を標的とし、複数の手段（フィッシング攻撃、ドライブバイダウンロード攻撃など）で侵入し、さまざまな技術を用いて長時間潜伏し、データを盗み出します。従来からのウイルスソフトや脆弱性対策は、効果がありません。

通信機器（ルータ）や複合機、各課に設置しているポータブルNAS等の特定用途機器(IoT)機器もターゲットになります

◎ばらまき攻撃

ランサムウェアやトロイの木馬ウイルスなどへの感染を誘発する、不特定多数へ送りつけられる不審な電子メール攻撃です。
従来からのウイルスソフトや脆弱性対策で対応可能です。
一方で最近は様々な亜種（変異種）が多数登場し、本来の目的とは異なる挙動を示すなど、安全に除去できないケースも増えつつあります。

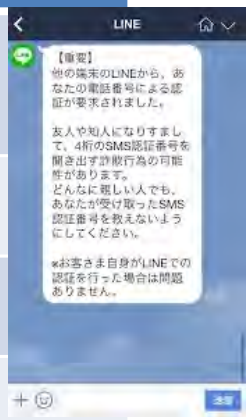
＜近年発生した最大級のランサムウェア被害＞
まる１日以上メールが利用できない
事態も発生しております。

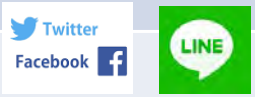
業務継続性において深刻なダメージも（最悪、PCの再インストールが必要な「破壊的攻撃」に派生）


日本経済新聞
2017年10月18日（水）
Web刊 速報 ビジネスリーダー マーケット テクノロジー アジア スポーツ マネー ライフ 朝刊・
トップ 紙面連動 連載 社説・春秋 特集 映像 FT オピニオン 統計 中国共産党大会 衆院選
サイバー攻撃、日立でシステム障害 企業・官公庁が警戒
2017/5/15 10:58（2017/5/15 13:08更新）
共有 保存 印刷 その他
世界中を襲う大規模なサイバー攻撃が発覚してから最初の平日を迎えた日本では、日立製作所の社内システムに障害が発生したことが分かった。企業や官公庁は警戒を強めており、出社した従業員に対し不審な電子メールを開かないよう注意喚起するなど対策を急ぐ。15日朝時点で公共交通機関や電気・ガス、金融など社会インフラへの影響は報告されていない。

自治体の業務環境において考えらえるセキュリティリスク要因

手段	セキュリティリスク
メール	• 私的メールの利用／私的メールへの転送 • アカウント乗っ取り、不特定多数の違法メール配信 • ビジネスメール詐欺（BEC）※市民／政府機関との連絡装う
Webブラウザ	• 外部不正サイトへの誘導（フィッシング） • ランサムウェア
ファイル交換	• 職員間 • 担当NASへの保存
SNS	• LINE（グループ）による連絡周知 • Twitterによる公開、拡散
クラウドサービス	• クラウドストレージ（Dropbox/GoogleDriveの利用）※アクセス設定により誰でも見れてしまう。
Webサイト	• 不正アクセス、外部サイトへの誘導 • 情報改ざん、利用不能 ※Webサイト管理機能を外部開放／古いバージョンのCMS利用に起因





全て庁外／校外／社外での利用も可能な環境を想定
【潜入段階】で近づく方法はメールとは限らない
業務遂行上、業務効率を高める意図で職員の恣意的な判断で「こっそり」利用するケースもあり、全てに確実な対策を実施するのは困難

情報セキュリティ10大脅威 2021

出典：IPA

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**4位**	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**7位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

職員の働き方改革／DX等の推進により
セキュリティリスクが拡大する恐れ

システムのクラウド化移行に伴い
今後もリスク拡大の恐れ

新種のウイルスも数多く出現

なりすましメール拡散のウイルス、日本に本格上陸

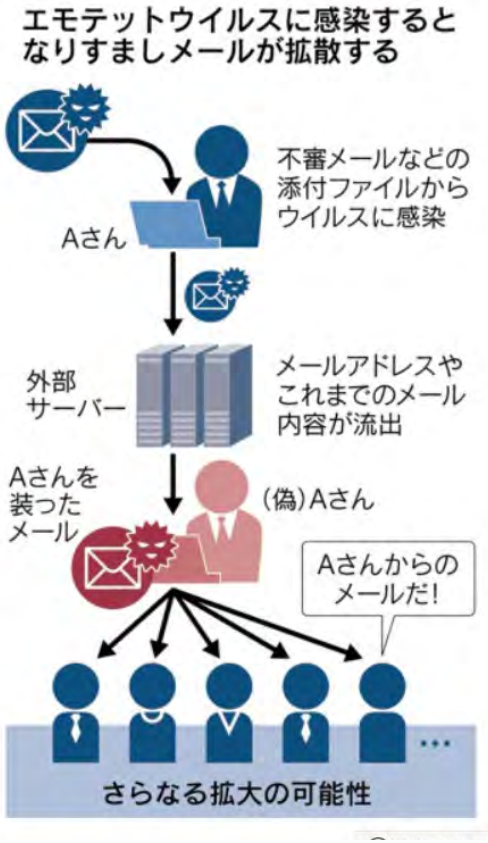
2019/11/29 15:35 | 日本経済新聞　電子版

欧米で流行しているコンピューターウイルス「Emotet（エモテット）」が日本に本格上陸し、被害が出始めた。感染するとメールアドレスや本文を盗まれ、本人になりすましたメールが次々と関係者に送られる。首都大学東京や京都市観光協会など少なくとも400以上の団体・企業で被害が出ているとされ、民間団体などが注意を呼びかけている。

10月18日、首都大学東京の教員に海外の雑誌社からメールが届いた。過去にやりとりがあったため、教員は疑問を持たずに添付ファイルを開いた。すると複数の教職員になりすましたメールが関係者に相次いで送信されるようになった。

教職員は自分の意思でメールを送っていないため、同大学は外部に調査を依頼、エモテットの被害だと判明した。添付ファイルやパスワードの外部流出、サーバーデータの暗号化の被害がなかったかどうか調べている。

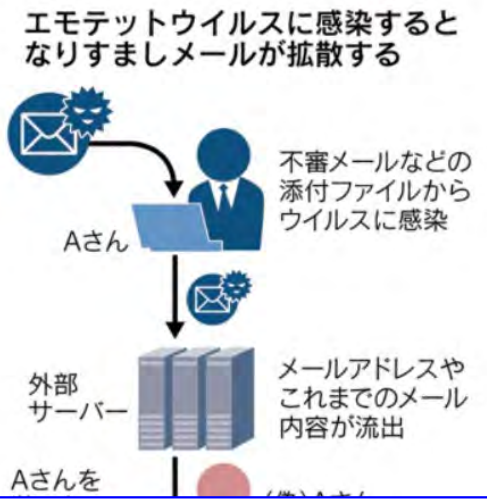
出典：日本経済新聞2019年11月29日



新種のウイルスも数多く出現

欧米で流行しているコンピューターウイルス「Emotet（エモテット）」が日本に本格上陸し、被害が出始めた。感染するとメールアドレスや本文を盗まれ、本人になりすましたメールが次々と関係者に送られる。首都大学東京や京都市観光協会など少なくとも400以上の団体・企業で被害が出ているとされ、民間団体などが注意を呼びかけている。

10月18日、首都大学東京の教員に海外の雑誌社からメールが届いた。過去にやりとりがあったため、教員は疑問を持たずに添付ファイルを開いた。すると複数の教職員になり



NTTデータ関西がEmotet感染、自治体等向けの電子申請サービス問い合わせメールが流出

株式会社NTTデータ関西は7月1日、Emotet感染による不審メールの送信について発表した。

株式会社NTTデータ関西は7月1日、Emotet感染による不審メールの送信について発表した。
これは同社が自治体等向けに提供する電子申請サービスのヘルプデスク業務で使用するPC8台のうち1台がEmotet感染し、当該PCに保存されていた過去に送受信したメールが流出し、同社ヘルプデスクを装った攻撃者からの不審メールの発信を確認したというもの。6月6日に、電子申請サービスのヘルプデスクアドレスを騙った不審メール1件の申告があり、その後、複数の団体から同様の申告があり発覚した。

2020年以降も依然として猛威を振るっている状況

VPN（閉域網）だから安全と思ってはいけない

海洋研究開発機構に不正アクセス、職員の情報1947件が窃取される

出典：日経X-Tech 2021/3/19

海洋研究開発機構（JAMSTEC）は2021年3月18日、不正アクセスにより同機構の職員情報1947件が3月8日に窃取されたと発表した。搾取されたのは、同職員などの名前や職員番号、アカウント、メールアドレス、暗号化（ハッシュ化）されたパスワードである。

不正アクセスは同機構職員になりすました攻撃者によるものだという。職員になりすました攻撃者がVPNで基幹ネットワークシステムに接続して情報を窃取した。同機構外の個人情報や機微情報などが窃取されていないかは継続して確認中だという。

海洋研究開発機構はVPNの使用を停止し、個人情報が窃取された人に連絡している。調査が完了し次第、適切な再発防止策を講じるという。

Fortinet製SSL-VPNの脆弱性にパッチ未適用のリスト約5万件が公開される。日本企業も含む。

昨年発見されたFortinet製SSL-VPN用の脆弱性CVE-2018-13379に未だパッチが適用されていない機器のIP一覧がサイバー攻撃者によって公開された。
サイバー攻撃者がこの情報を悪用すると、Fortinet製SSL-VPNからsslvpn_websessionファイルにアクセスし、ログイン資格情報を盗むことが可能になる。これらの盗まれた資格情報は、ネットワークを危険にさらし、ランサムウェアを展開するために使用される可能性がある。
攻撃条件の複雑さは低く、攻撃に必要な特権レベルも不要であり、緊急性が高い。

COVID-19の感染拡大に伴い、テレワークが急増、外部からのアクセス環境となるVPNの脆弱性を悪用するサイバー攻撃者の標的となっている。
脆弱性対策のため、パッチを適用する作業は専門機器のため業者に依頼するしかなく、作業費用が発生するため、棚上げになったり、そもそも業者のセキュリティ認識が低く放置しているケースも

３．次期情報セキュリティ強靭化の方向性について

自治体のセキュリティ対策の今後の課題

現行の自治体セキュリティ強靭化対策
- H28年度補正予算による補助金を財源に整備
- H29年度に整備、サービス開始を前提に構築

補助金がつくということで、とりあえずガイドラインにしたがって
- ネットワーク分離しました（インターネット接続系／LGWAN接続系）
- 仮想デスクトップ入れてみました。（インターネット接続系⇒LGWAN接続系）
- 二要素認証入れてみました。（個人番号利用事務＜マイナンバー＞端末）
- ファイル／メール無害化入れてみました。

現在の課題
- サポート契約上現行環境が使えるのは2021年度までだが「とりあえず」延長
- 次回の更改は国から補助金が出ない
- サイバー攻撃の手口が巧妙化するなかで現在の対策で来年度まで不透明
- 対策は本庁の事務に限定され、**教育委員会等もっと危険な部門は十分な対策が取れてない**
- コロナ禍によるテレワーク、リモートアクセスへの対応／自治体DX推進による庁外との連携利用拡大

次期情報セキュリティ強靭化対策整備課題

重要インフラ事業者のセキュリティ対策の変更要素

「2018サイバーセキュリティ戦略」 4.2.3(1)①
- エンドポイント（端末等）においてマルウェアの挙動を検知することにより、被害の未然防止及び拡大防止に取り組む

「政府機関等の情報セキュリティ対策のための統一基準」 6.2.2(1)(a)
- 情報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。（以下略）

「政府機関等の対策基準策定のためのガイドライン」【基本対策事項】 6.2.2(1)(a)
- 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、既知お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。

「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」 6.4不正プログラム対策
- 解説(1)-(注3) インターネットからの不正プログラム感染、侵入を防御するための方式として、パターンファイルで検知が難しい不正プログラムも存在することから、不正プログラムの挙動を検知する方式もある。

エンドポイントにおける挙動検知での未知のプログラム対策が重要なポイントに

参考:クラウド・バイ・デフォルト原則

✓ 2018年6月に政府が発表した「政府情報システムにおけるクラウドサービスの利用に係る基本方針」nにおいて、クラウドサービスの利用メリットから「クラウド・バイ・デフォルト原則」として、**クラウドサービスの利用を「第1候補(デフォルト)」として考える方針**を策定

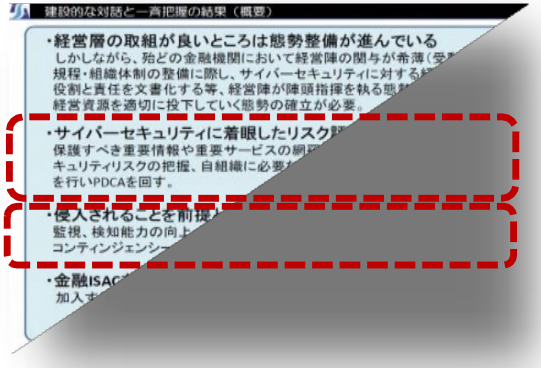
観点	クラウドサービスの利用メリット
効率性の向上	クラウドサービスでは、多くの利用者間でリソースを共有するため、一利用者当たりの費用負担は軽減される。また、クラウドサービスは、多くの場合、多様な基本機能があらかじめ提供されているため、導入時間を短縮することが可能となる。
セキュリティ水準の向上	多くのクラウドサービスは、一定水準の情報セキュリティ機能を基本機能として提供しつつ、より高度な情報セキュリティ機能の追加も可能となっている。また、世界的に認知されたクラウドセキュリティ認証等を有するクラウドサービスについては、強固な情報セキュリティ機能を基本機能として提供している。多くの情報システムにおいては、オンプレミス環境で情報セキュリティ機能を個々に構築するよりも、クラウドサービスを利用する方が、その激しい競争環境下での新しい技術の積極的な採用と規模の経済から、効率的に情報セキュリティレベルを向上させることが期待される。
技術革新対応力の向上	クラウドサービスにおいては、技術革新による新しい機能（例えば、ソーシャルメディア、モバイルデバイス、分析ツール等への対応）が随時追加される。そのため、クラウドサービスを利用することで、最新技術を活用し、試行することが容易となる。
柔軟性の向上	クラウドサービスは、リソースの追加、変更等が容易となっており、数ヶ月の試行運用といった短期間のサービス利用にも適している。また、一般に汎用サービス化した機能の組み合わせを変更する等の対応によって、新たな機能の追加のみならず、業務の見直し等の対応が比較的簡易に可能となるほか、従量制に基づく価格が公表されていることから、値下げ競争が起きている状況にある。
可用性の向上	クラウドサービスにおいては、仮想化等の技術利活用により、複数のサーバ等のリソースを統合されたリソースとして利用でき、さらに、個別のシステムに必要なリソースは、統合されたリソースの中で柔軟に構成を変更することができる。その結果、24 時間 365 日の稼働を目的とした場合でも過剰な投資を行うことなく、個々の物理的なリソースの障害等がもたらす情報システム全体への悪影響を極小化しつつ、大規模災害の発生時にも継続運用が可能となるなど、情報システム全体の可用性を向上させることができる。

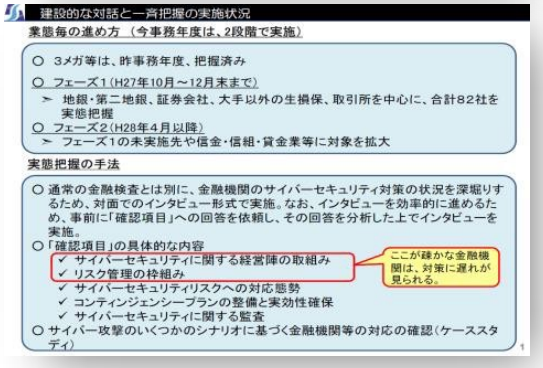
出典:https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

参考：内閣サイバーセキュリティセンター（NISC）の方針

重要インフラ専門調査委員会

重要インフラ専門調査委員会にて、**金融庁はこれまでの監査結果**「金融機関におけるサイバーセキュリティの対応状況」（H28.6/15）





従来の境界防御から
侵入されることを前提とした対策強化が必要と明言
（ゼロトラストセキュリティ）

政府機関等の対策基準策定のためのガイドライン（令和３年度版）

6.2.2 不正プログラム対策
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。

6.2.4標的型攻撃対策
標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

近年は攻撃対象の組織に対する直接的な攻撃だけでなく、委託先等の関連組織への間接的な攻撃も確認されており、より幅広い対策の検討が求められる。

現行強靭化対策の見直しの方向性

総務省発行「自治体情報セキュリティ対策の見直しのポイント」
https://www.soumu.go.jp/main_content/000688753.pdf

検討の経緯

「三層の対策」 2015年の年金機構の情報漏えい事案を受け、**短期間**で自治体の情報セキュリティ対策を抜本的に強化 ＝「三層の対策」

⇒ **インシデント数の大幅な減少を実現**

一方で、

①ユーザビリティへの影響

- ✓ **自治体内の情報ネットワークの分離・分割による事務効率の低下**
  例：マイナンバー利用事務系のシステムへのデータの取込み、インターネットメールの添付ファイルの取得など

②新たな時代の要請

- ✓ **行政アプリケーションを自前調達方式からサービス利用式へ**（政府における「クラウド・バイ・デフォルト」原則）
- ✓ **行政手続を紙から電子へ**（デジタル手続法を受けた行政手続のオンライン化）
- ✓ **働き方改革**（テレワーク等のリモートアクセス）
- ✓ **サイバー攻撃の増加、サイバー犯罪における手口の巧妙化** 等

「三層の対策」の効果や課題、新たな時代の要請を踏まえ、
効率性・利便性を向上させた新たな自治体情報セキュリティ対策を検討
※「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の改定等に係る検討会」において検討

「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」にも反映

1

新たなインターネットサービスに対応した
効率性・利便性を向上させた
新たな自治体情報セキュリティ対策を検討

「三層の対策」の見直し
・LGWAN接続系とインターネット接続系の分割に係る見直し

ポイント①：「三層の対策」の見直し

見直しの方向性

○マイナンバー利用事務系の分離に係る見直し
- 住民情報の流出を徹底して防止する観点から**他の領域との分離は維持**
- 十分にセキュリティが確保されていると**国が認めた特定通信（ガイドラインに明記、ex. eLTAX、マイナポータルを活用したぴったりサービス）に限り**、インターネット経由の申請等のデータの**電子的移送を可能**とし、**ユーザビリティの向上**及び**行政手続のオンライン化に対応**

○LGWAN接続系とインターネット接続系の分割に係る見直し
- クラウド・バイ・デフォルト原則やテレワーク等の新たな時代の要請を踏まえて、従来の**「三層の対策」の基本的な枠組みを維持**しつつ、効率性・利便性の高いモデルとして、**インターネット接続系に業務端末・システムを配置した「新たなモデル」（βモデル）を提示**
- ただし、自治体によっては対応可能なセキュリティ対策のレベルには差があることから、新たなモデルの採用に当たっては、情報資産単位でのアクセス制御、監視体制やCSIRTなど緊急時即応体制の整備、個々の職員のリテラシー向上など**人的セキュリティ対策の実施が条件となる。**

5

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改正の方向性

令和２年度改定

■地方公共団体の効率性・利便性の向上とセキュリティ確保の両立の観点からガイドラインを改定

「三層の対策」の一部見直し（マイナンバー利用事務系の特定通信、LGWAN接続系とインターネット接続系の分割の見直し）、LGWAN接続系へのリモートアクセス等について改定を実施

令和３年７月の政府統一基準群改定のポイント

1. クラウドサービスの利用拡大を見据えた記載の充実
2. 情報セキュリティ対策の動向を踏まえた記載の充実
3. 多様な働き方を前提とした情報セキュリティ対策の整理

令和３年度改定の方向性

■令和２年度の改定内容を維持しつつ、政府統一基準群の改定内容や最新の動向を踏まえた情報セキュリティ対策を追加

※ガバメントクラウド活用に関する新たなセキュリティ対策の在り方については、デジタル庁における検討と連携し、随時検討を行う

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改正の方向性

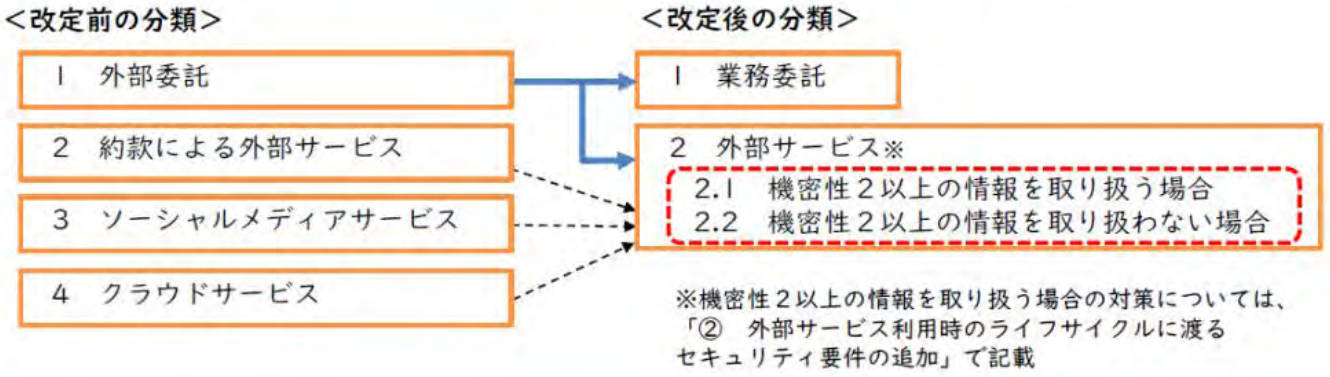
改定のポイント１：業務委託・外部サービス利用時の情報資産の取扱い（１/４）

①　外部サービスを再定義した上で取り扱う情報に応じた適切なセキュリティ対策の実施

改定の概要

- 「外部委託」、「約款による外部サービス」、「ソーシャルメディアサービス」及び「クラウドサービス」の定義の境目が曖昧となっているため、政府統一基準群と同様に「業務委託」と「外部サービス」に分けた上で、「機密性２以上の情報を取り扱う場合」と「機密性２以上の情報を取り扱わない場合」により求めるセキュリティ対策のレベルの整理を行う。

※民間事業者等が不特定多数の利用者に対して提供するSNS等の画一的な約款や規約等への同意のみで利用可能となる外部サービス（従来の「約款による外部サービス」）については、機密性２以上の情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として機密性２以上の情報を取り扱うことはできない点は、従前より変更なし。



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改正の方向性

改定のポイント２：情報セキュリティ対策の動向を踏まえた記載の充実（１/１）

改定の概要

- 政府統一基準群では、常時アクセス判断・許可アーキテクチャの考え方があることを紹介した上で、採用する際の対策としてEDR等の対策が示された。現行ガイドラインでは、インターネット接続系に業務端末を配置したモデル（βモデル、β’モデル）について、従来のモデルと比較してセキュリティ上のリスクが高まることからEDR等の対策を記載している。
- 今回新たに政府統一基準群に記載された対策については、既に現行ガイドラインで同様の記載がなされていることから対策導入に関する新たな記載の見直しは行わないが、導入後の運用面に関する記載については不十分であることから追記を行う。

＜現行：対策基準（解説）＞

３　情報システム全体の強靭性の向上
（注１０）未知の不正プログラムへの対策（エンドポイント対策）
　未知の不正プログラム対策として、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、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。

運用面に関する記載を追記

＜改定案：対策基準(解説)＞

３　情報システム全体の強靭性の向上
（注１１）未知の不正プログラムへの対策（エンドポイント対策）
　未知の不正プログラム対策として、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、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。なお製品の導入だけでは未知の不正プログラムの対策とはならない。監視体制やCSIRTとの連携等、組織的な対策と合わせて検討が必要となることに留意する必要がある。

出典：＜総務省＞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の改定等に係る検討会（第2回）資料より

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改正の方向性

改定のポイント３：多様な働き方を前提とした情報セキュリティ対策（１/１）

改定の概要

①テレワーク実施時のセキュリティ対策

現行ガイドラインでは、令和２年度の検討会での検討結果を踏まえ、テレワークとして想定される技術的なモデル（LGWAN-ASPサービスを利用したモデル、インターネット接続系を経由したモデル等）を記載しているが、運用面に係る対策の記載がないため、政府統一基準群の記載を参考に、テレワーク実施場所等の運用面に係る対策を追記する。

・テレワーク実施前及び実施後に職員がチェックすべき項目を定めチェックを実施させること
・画面ののぞき見や盗聴を防止できるような環境を選定すること　等

②支給以外の端末（BYOD）利用時のセキュリティ対策

現行ガイドラインにおいても、BYODの利用手順や技術的な対策を一部記載しているが、政府統一基準群で対策の詳細な内容が記載されたことから、政府統一基準群の記載を参考に、端末に情報を保存できないようにするための機能を設けることや利用端末を限定する等の対策を追記する。

・IPアドレス、MACアドレス等の認証情報を利用し、端末を制限すること
・利用申請手続（利用者、目的、利用する情報、端末等）を職員に遵守させること　等

③Web会議サービス利用時のセキュリティ対策

現行ガイドラインでは、Web会議サービス利用に特化したセキュリティ対策の記載がないため、政府統一基準群の記載を参考に、 Web会議に無関係の者が参加できないような対策等を記載する。

・なりすましが疑われるなどの不審な参加者を会議室から退室させること
・ビデオカメラで撮影されれば会議内容は保存されるため、会議で取り扱う情報を確認する必要があること　等

出典：＜総務省＞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の改定等に係る検討会（第2回）資料より

無害化の定義（総務省ガイドライン抜粋）

総務省発行“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(令和4年3月版)” iii-41ページ～iii-42ページ

（２） LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

分割とは、一旦両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすることをいう。

（ア）インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

LGWAN 接続系へインターネットメールを転送する際には、インターネットメールの転送に必要な特定サーバ間以外の通信を遮断するとともに、LGWAN 環境とインターネット環境はSMTP以外の Web 通信を始めとするプロトコルを遮断し、インターネットメールの添付ファイルの削除及び HTML メールのテキスト化を行う。

（イ）インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

インターネット接続系の端末を仮想デスクトップ化し、LGWAN 接続系の端末から添付ファイルも含むメールの閲覧を可能とする。

（ウ）危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

危険因子が埋め込まれたファイルを LGWAN 接続系に取り込んだ場合、脆弱性を突いた悪意あるコード等が実行される恐れがある。インターネット接続系から LGWAN 接続系にファイルを取り込む際は、以下のような手法により、危険因子をファイルから除去又は危険因子がファイルに含まれていないことの確認を行った上で、取り込まなければならない。

（いずれかの手法のみ又は複数の手法を組み合わせて採用することが考えられる。）

・ファイルからテキストのみを抽出

・ファイルを画像PDF に変換

・サービス等を活用してサニタイズ処理（ファイルを一旦分解した上で危険因子を除去した後、ファイルを再構築し、分解前と同様なファイル形式に復元する）

・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等で危険因子が含まれていないことを確認

なお、上記のいずれか又は複数の手法による対策を実施した場合であっても、マルウェア等の除去が完全に保証されるものではないため、 LGWAN接続系において以下のようなセキュリティ対策を実施しなければならない。

・OS 等の修正プログラムの適時適用（自治体情報セキュリティ向上プラットフォームの利用等）

・アンチウイルスソフトウェアの最新化（定義ファイルのアップデート等）

・業務に必要なファイルやメール等の定期的なバックアップの実施 また、上記の LGWAN 接続系における対策に加え、業務システムの停止を狙ったマルウェアの感染を防ぐ対策として、LGWAN接続系端末にアプリケーションホワイトリストを設定し、実行できるアプリケーションの制限等を行うことを強く推奨する。

（注５）「目視で確認」とは、ファイルが添付されたメールを開く際に、送信元は適切か（見覚えのないアドレス、フリーアドレス又は正規の組織名若しくはドメインに似せたアドレスではないか）、メールの件名や内容が適切か
（見慣れない日本語やフォントが使用されていないか）などを確認することである。未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等の製品の導入に加え、人的対策として「目視で確認」を求めるものである。

（注６）サニタイズ処理等を実現する手法は多岐にわたるため、適正な製品を選定し導入することが望ましい。

（注７）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系から LGWAN 接続系へマルウェア感染を防ぐ必要がある。

４．ゼロトラストネットワークによるセキュリティ強靭化モデル例

次期強靭化の方向性

（２）LGWAN接続系とインターネット接続系の分割（まとめ）

効率性・利便性の高いモデルとして、インターネット接続系に業務端末・システムを配置した「新たなモデル」（βモデル）を提示（ただし、採用には十分な人的セキュリティ対策の実施が条件）

		αモデル（従来モデル） 業務効率性・利便性：低 必要な対策のレベル：現行と同じ	βモデル（重要な情報資産配置なし） 業務効率性・利便性：中 必要な対策のレベル：中	β'モデル（重要な情報資産配置あり） 業務効率性・利便性：高 必要な対策のレベル：高
モデルの特徴		・これまでの「三層の対策」による強靭化モデルを強化・改善	・業務システムをLGWAN接続系に残しつつ、業務端末をインターネット接続系に移行し、画面転送によりLGWAN接続系業務システムを利用	・βモデルに加え、文書管理、人事給与、財務会計等の業務システム（マイナンバー利用事務系を除く。）をインターネット接続系に移行し、業務の効率性を改善
業務端末		LGWAN接続系	インターネット接続系	インターネット接続系
配置例	マイナンバー利用事務系	住民記録、戸籍、税、後期高齢、介護、国保、国民年金、福祉関連	住民記録、戸籍、税、後期高齢、介護、国保、国民年金、福祉関連	住民記録、戸籍、税、後期高齢、介護、国保、国民年金、福祉関連
	LGWAN接続系	マイナンバーに係る情報連携、証明書等のコンビニ交付、防災・人命に係る重要通信（J-ALERT等）、文書管理、人事給与、財務会計、LGWANメール、グループウェア	マイナンバーに係る情報連携、証明書等のコンビニ交付、防災・人命に係る重要通信（J-ALERT等）、文書管理、人事給与、財務会計、LGWANメール	マイナンバーに係る情報連携、証明書等のコンビニ交付、防災・人命に係る重要通信（J-ALERT等）、LGWANメール
	インターネット接続系	インターネットメール、ホームページ管理システム	インターネットメール、ホームページ管理システム、グループウェア	インターネットメール、ホームページ管理システム、グループウェア、文書管理、人事給与、財務会計
主なセキュリティ対策	技術的対策	・無害化処理 ・インターネット接続系の画面転送	・無害化処理 ・LGWAN接続系の画面転送 ・EDR(エンドポイント対策）※ ・業務システムログ管理	・EDR(エンドポイント対策）※ ・業務システムログ管理
	組織・人的対策	・インシデント対応チーム（CSIRT）の設置及び役割の明確化 ・啓発や訓練を通じた各自治体の職員のセキュリティ・リテラシーの向上 ・実践的サイバー防御演習（CYDER）の確実な受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有の推進 ・自治体情報セキュリティポリシーガイドラインに沿った情報セキュリティポリシーの策定・遵守	左記対策の確実な実施	左記対策の確実な実施に加えて、 ・情報資産単位でのアクセス制御 ・組織的なセキュリティ対策基準の遵守 ・セキュリティの継続的な検知・モニタリング体制

※従来のウイルス対策ソフトを標準的なツールで代替し、新たにエンドポイント製品を導入することも考えられる。

その他の検討ポイント（現行環境）

- LGWANメールとインターネットメールどちらの利用頻度が高いか
- 外部インターネットメールは、個人アカウントではなく、組織代表アカウントで送付しているか。
- （同様に）LGWANメールは、個人アカウントではなく、組織代表アカウントで送付しているか。
- 外部Webサイトを利用する頻度はどのくらい多いか
- グループウェアではメールの他、主にどの機能を使っているか
- 作業ファイルは、個人フォルダではなく組織（担当）でグループフォルダで管理しているか
- Web会議の頻度は最近増えているか
- 庁外での業務頻度は最近増えているか。

- DX推進において、上記の環境が足かせになっている部分はないか

次期強靭化の方向性（αモデル）

（２）LGWAN接続系とインターネット接続系の分割（まとめ）

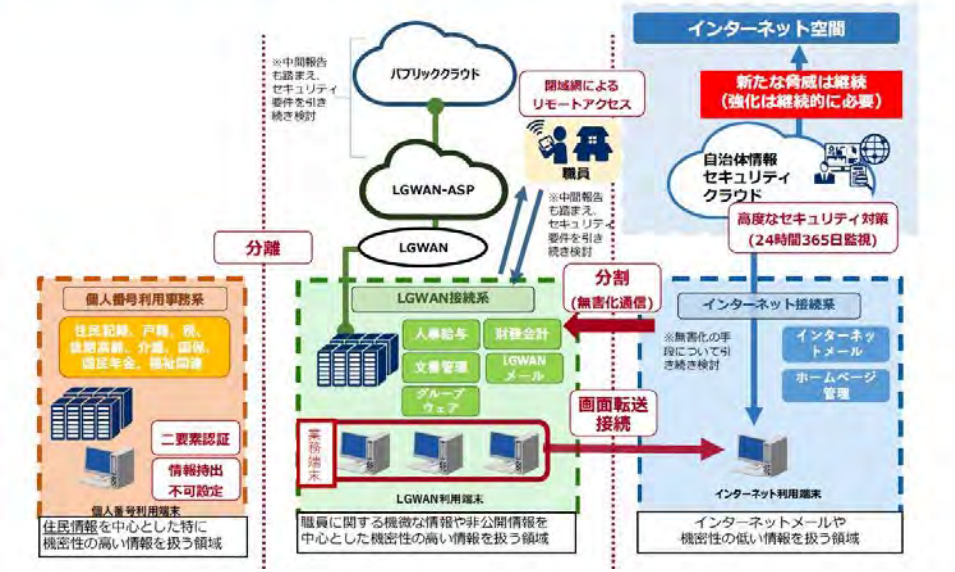
効率性・利便性の高いモデルとして、インターネット接続系に業務端末・システムを配置した「新たなモデル」（βモデル）を提示（ただし、採用には十分な人的セキュリティ対策の実施が条件）

		αモデル（従来モデル） 業務効率性・利便性：低 必要な対策のレベル：現行と同じ	βモデル（重要な情報資産配置なし） 業務効率性・利便性：中 必要な対策のレベル：中	β'モデル（重要な情報資産配置あり） 業務効率性・利便性：高 必要な対策のレベル：高
モデルの特徴		・これまでの「三層の対策」による強靭化モデルを強化・改善	・業務システムをLGWAN接続系に残しつつ、業務端末をインターネット接続系に移行し、画面転送によりLGWAN接続系業務システムを利用	・βモデルに加え、文書管理、人事給与、財務会計等の業務システム（マイナンバー利用事務系を除く。）をインターネット接続系に移行し、業務の効率性を改善
配置例	マイナンバー利用事務系	住民記録、戸籍、税、後期高齢、介護、国保、国民年金、福祉関連	住民記録、戸籍、税、後期高齢、介護、国保、国民年金、福祉関連	住民記録、戸籍、税、後期高齢、介護、国保、国民年金、福祉関連
	LGWAN接続系	マイナンバーに係る情報連携、証明書等のコンビニ交付、防災・人命に係る重要通信（J-ALERT等）、文書管理、人事給与、財務会計、LGWANメール、グループウェア	マイナンバーに係る情報連携、証明書等のコンビニ交付、防災・人命に係る重要通信（J-ALERT等）、文書管理、人事給与、財務会計、LGWANメール	マイナンバーに係る情報連携、証明書等のコンビニ交付、防災・人命に係る重要通信（J-ALERT等）、LGWANメール
	インターネット接続系	インターネットメール、ホームページ管理システム	インターネットメール、ホームページ管理システム、グループウェア	インターネットメール、ホームページ管理システム、グループウェア、文書管理、人事給与、財務会計
主なセキュリティ対策	技術的対策	・無害化処理 ・インターネット接続系の画面転送	・無害化処理 ・LGWAN接続系の画面転送 ・EDR(エンドポイント対策）※ ・業務システムログ管理	・EDR(エンドポイント対策）※ ・業務システムログ管理
	組織・人的対策	・インシデント対応チーム（CSIRT）の設置及び役割の明確化 ・啓発や訓練を通じた各自治体の職員のセキュリティ・リテラシーの向上 ・実践的サイバー防御演習（CYDER）の確実な受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有の推進 ・自治体情報セキュリティポリシーガイドラインに沿った情報セキュリティポリシーの策定・遵守	左記対策の確実な実施	左記対策の確実な実施に加えて、 ・情報資産単位でのアクセス制御 ・組 ・セ

※従来のウイルス対策ソフトを標準的なツールで代替し、新たにエンドポイント製品を導入することも考えられる。

（２－１） αモデル(従来モデル)のイメージ

・これまでの「三層の対策」による強靭化モデルを継続利用
・新たな脅威に備えセキュリティ対策は強化・改善

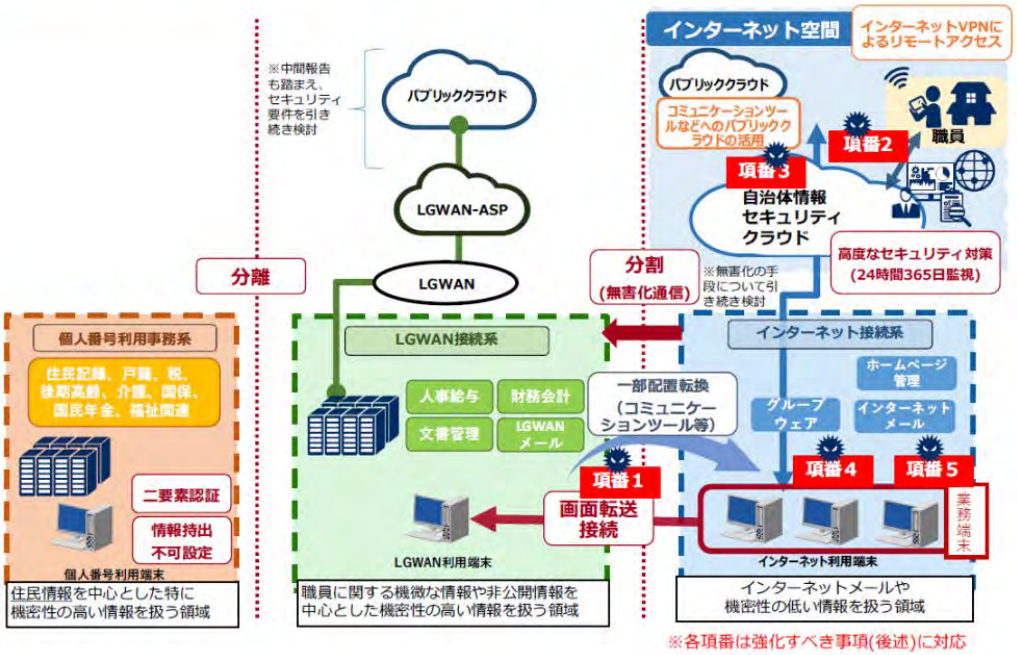


- 前回も同方式で調達しているから大幅な変更はしたくない
- 特にセキュリティインシデントも発生していない
- 操作性の問題はセキュリティ確保のため我慢してもらおう
- コスト掛けられないのでVDIの同時アクセス率は絞る（30%程度）
- テレカンやGIS（Google）使えない
- インターネット接続系のファイルは保存できないから不便
- コロナ禍で密になるから登庁控えられているのに庁外や自宅からリモートアクセスできない
- （遅くて使えないから）個人のタブレット、スマホ持ち込んでインターネット接続して業務しよう

次期強靭化の方向性（β／β´モデル）

（２－２） βモデル(重要な情報資産配置無し)のイメージ

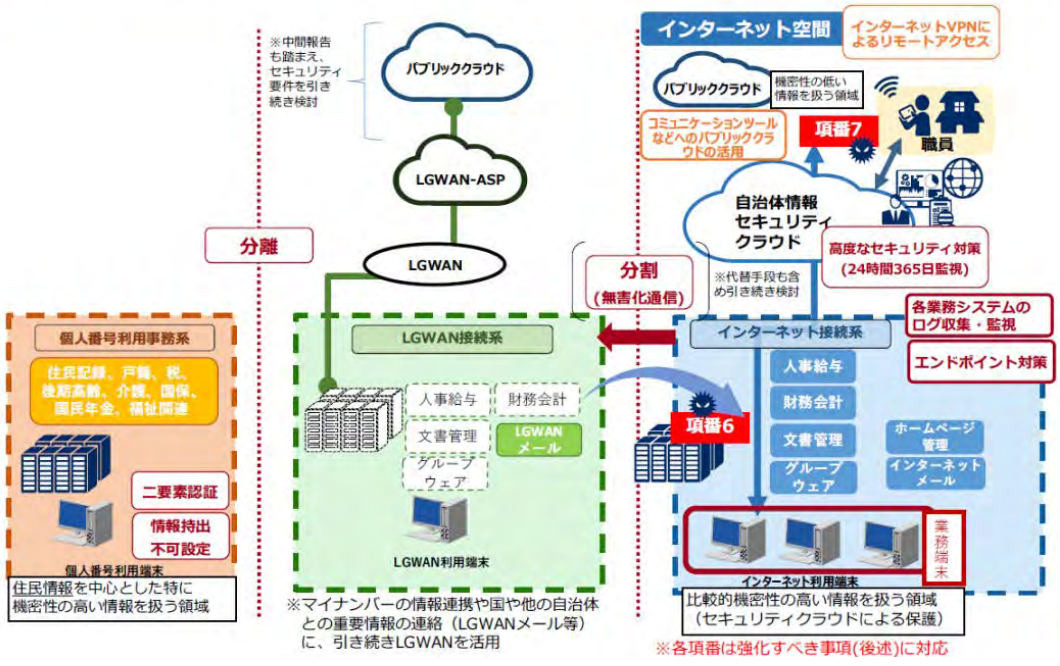
業務システムをLGWAN接続系に残しつつ、業務端末をインターネット接続系に移行し、画面転送により
LGWAN接続系業務システムを利用



- LGWAN接続系端末はほぼ全職員が使うので、α´モデルより大規模なVDIが必要（αモデルよりコストが高くなる）
- システム運用管理が煩雑
- インターネット接続系PCにLGWAN接続系アプリケーションを一部配置転換配置された状態では連携作業が困難。

（２－３） β'モデル(重要な情報資産配置あり)のイメージ

業務システム（マイナンバー利用事務系を除く。）をインターネット接続系に移行し、業務の効率性を改善



- 機密性の高いデータをβ´に置いて大丈夫なのか？機密データをどのように取り扱えばよいのか。（リスクアセスメント）
- β´モデルに必要なEDRの要件がわからない。
- 一次RFI提案してきたシステム常時監視（マネージドサービス／SoC）はコスト面でハードル高い

β'モデル(重要な情報資産配置あり)で強化すべき事項

業務システムをインターネット接続系に移行することにより新たに発生するリスクを考慮
<一部重要な情報資産をインターネット接続系配置する>

No	考慮すべきリスク(**黄色背景は追加項目**)	考えられる主な対策 **(現在実施されていない対策または強化する対策)** **(赤字必須　青字オプション)**	対策場所
1	インターネット接続系にある業務端末が乗っ取られ、画面転送接続経由でLGWAN接続系の情報を不正に閲覧・操作される	・ネットワーク監視・防御 ・脆弱性対策（**資産管理※※**、パッチ適用等） ・ウイルス対策(パターンマッチング) **・ログ管理（SIEM等）** **・EDR ※業務端末が設置されているため必須事項**	・各自治体による対応 （EDRログをセキュリティクラウドのログ管理・SOC監視することも可能）
2	インターネット接続系にある業務端末に不正なリモートアクセスをして重要情報を不正に閲覧・操作される	「自治体職員による庁内情報環境へのリモートアクセスに関するセキュリティ要件について（中間報告）」より **・端末認証、端末の持ち出し管理**など	各自治体による対応
3	サイバー攻撃の検知漏れにより、インターネット接続系に不正に侵入される	・ネットワーク監視・防御 **・SOCの強化**	セキュリティクラウドによる対応
4	標的型メールの添付ファイルからのマルウェア感染による機密情報の漏えい（Emotet等）	・ネットワーク監視・防御 ・メールセキュリティ（サンドボックス） ・脆弱性管理（**資産管理※※**、パッチ適用） ・ウイルス対策(パターンマッチング) **・ファイル暗号化** ・アクセス制御（アクセス権の局所化） **・EDR ※業務端末が設置されているため必須事項** **・DLP**	・ゲートウェイ対策はセキュリティクラウド ・内部メールサーバ、グループウェア等のセキュリティ対策は、各自治体での対応
5	標的型メールの添付ファイルからのランサムウェア感染によるグループウェアやメール利用停止（WannaCry等）	・ネットワーク監視・防御 ・メールセキュリティ（サンドボックス） ・脆弱性管理（**資産管理※※**、パッチ適用等） ・ウイルス対策(パターンマッチング) ・アクセス制御（アクセス権の局所化） ・EDR ※業務端末が設置されているため必須事項 ・バックアップ	・ゲートウェイ対策はセキュリティクラウド ・端末のセキュリティ対策は、各自治体での対応
6	端末、サーバ、ソフトウェア等の脆弱性を悪用し、不正なコードが実行される	・ネットワーク監視・防御 ・脆弱性対策（**資産管理※※**、パッチ適用等） ・ウイルス対策 **・EDR※業務端末が設置されているため必須事項** **・業務システムログ管理（ログ収集、監視）**	・ゲートウェイ対策はセキュリティクラウド ・業務システムサーバ等のセキュリティ対策は、各自治体による対応
7	職員が組織に許可されていないクラウドサービスに機密情報を不正にアップロードする	**・シャドーIT管理**	・セキュリティクラウドまたは各自治体による対応

※※OSやソフトウェアのバージョンなどを漏れなく管理することで、脆弱性の所在の効率的な把握を可能とし、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応できる。

SoC/SIEMとも
情報セキュリティクラウド側で対応する前提

都道府県がが対応しない場合
SoC/SIEMを独自に整備しなければならない

β’モデル(重要な情報資産配置あり)で強化すべき事項

【参考】現行ガイドラインにおけるβ・β’モデルを採用する場合の技術的対策

現行ガイドラインの記載

■「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」（抜粋）

3.情報システム全体の強靭性の向上
（3）インターネット接続系③　【解説】

β’モデルを採用する場合の必須のセキュリティ対策

対策区分	セキュリティ対策	概要
技術的対策	未知の不正プログラム対策（エンドポイント対策）	・従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。
	業務システムログ管理	・インシデントの兆候検知や、インシデント発生後の調査に使用するため、業務システムのログの収集、分析、保管を実施する。
	情報資産単位でのアクセス制御	・情報資産の機密性レベルに応じて業務システム単位でのアクセス制御を行う。文書を管理するサーバ等は課室単位でのアクセス制御を必須とし、係単位でのアクセス制御は推奨とする。

β’モデルについては、定期的な脆弱性診断、プラットフォーム診断等の実施が有効である。加えて、情報漏えいに対する対策として、以下の対策も有効である。
・万一ファイルが外部に漏えいしても解読できないよう、データベースやファイルの暗号化
・組織が定義したポリシーに従ってデータへの操作を監視・制限し情報の流出を防止（Data Loss Prevention）
・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
（注１０）未知の不正プログラムへの対策（エンドポイント対策）
未知の不正プログラム対策として、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、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。

出典：＜総務省＞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の改定等に係る検討会（第2回）資料より

βモデル／β´モデルで配置されるアプリケーション

方式	β´モデル（ゼロトラスト対策PC）	βモデル（仮想デスクトップ） VDI or SBC
インターネット接続系アプリケーション	・最新のWebブラウザ ・テレカンファレンス関連（ZOOM等） ・ISMAP準拠クラウドアプリケーション ・MS365	
LGWAN接続系アプリケーション	• 最新のブラウザ（Edge/chrome）で稼働するWebアプリケーション • LGWAN-ASPで提供される アプリケーション • 仮想ブラウザ／仮想アプリケーション機能を実装し、端末にインストールすることなく実行可能なアプリケーション • ライセンス上個々のPCにインストールが必要なアプリケーション • EdgeのIEモード不可 • LGWANメール（ブラウザアプリ）	• 旧OS上で稼働しているアプリケーション • IE11で稼働しているアプリケーション • インストールプログラム等によりインストールが必要なアプリケーション • JAVA（JRE）等が実装されたアプリケーション • LGWANメール
EDR等	リスク評価後必要な要件を選択 • ローカルストレージの暗号化 • ローカルストレージ保管制限設定 • PC状態監視 • 異常時にネットワークから隔離	

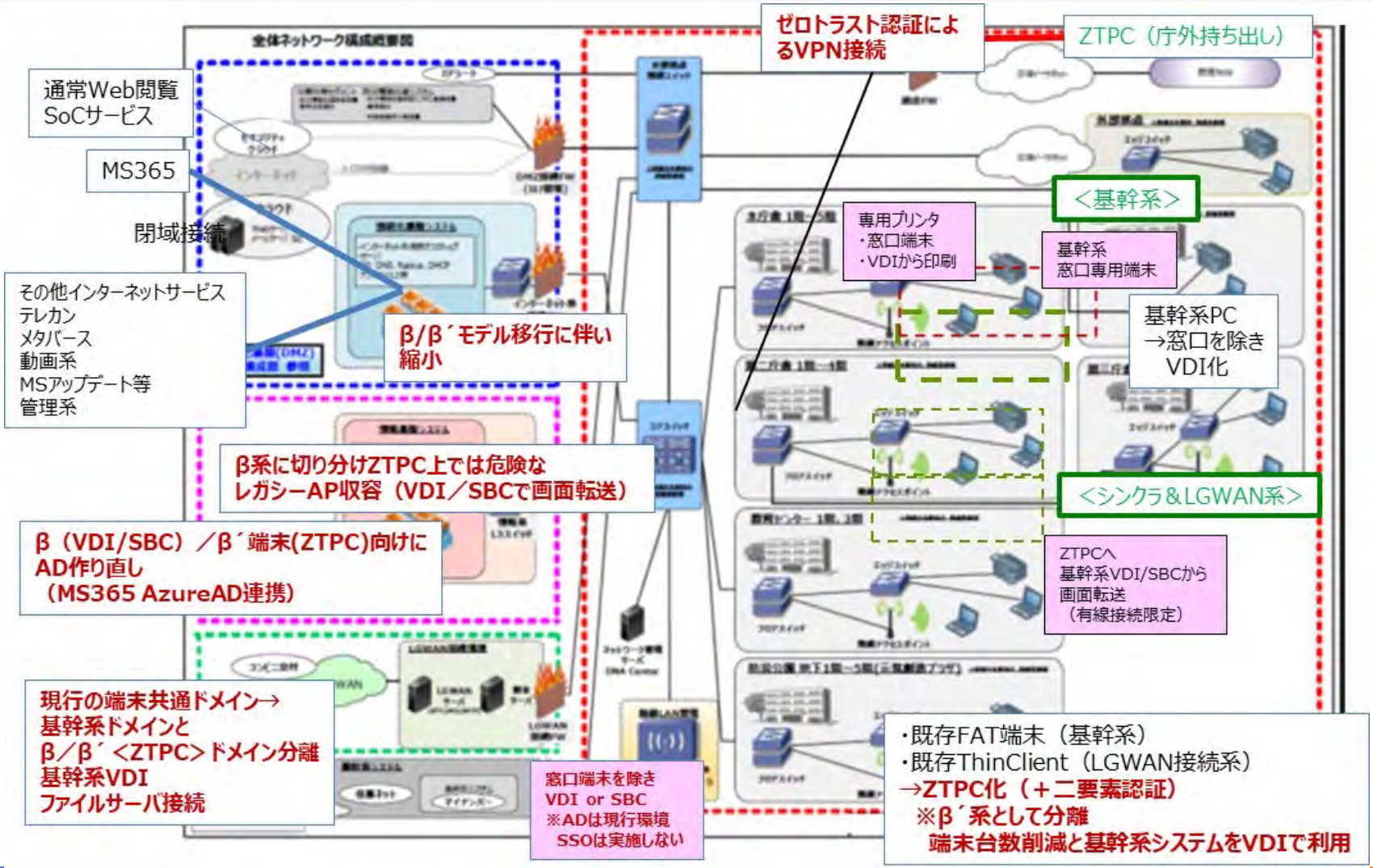
業務単位で配置を検討するのではなく、アプリケーションの構造（アーキテクチャ）で判断すべき
取り扱うデータの重要度とインシデント発生時の影響度を分析評価した上で、EDR／SoCの要件を決定する。

ゼロトラストPC要件

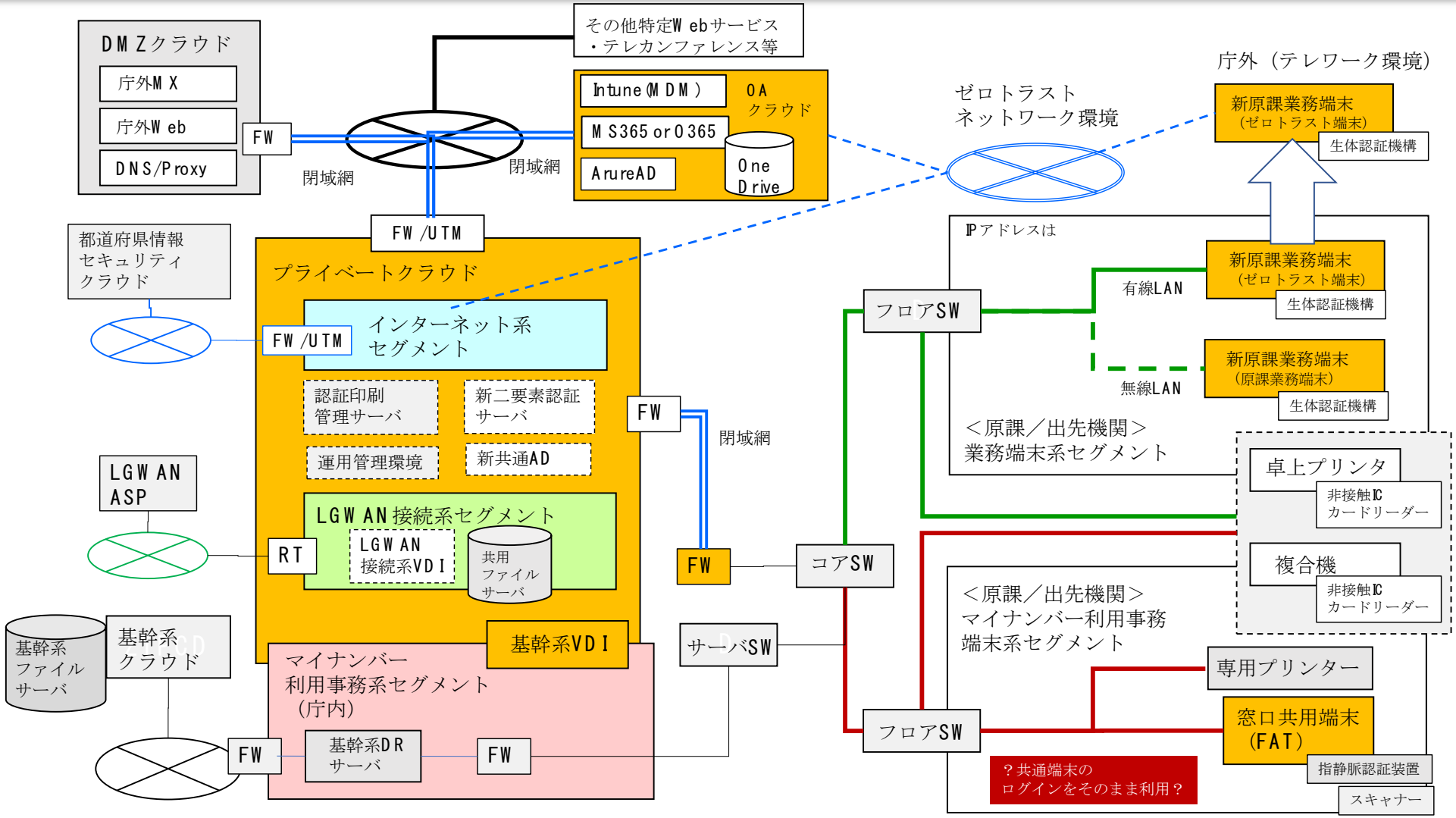
- 某省行政情報ネットワークシステムのクライアント調達仕様書（例）

ハードウェア・ルートオブトラスト クライアントPC上でセキュリティの信頼性を担保するために、メインのCPUとは独立し、かつ、TPMとは別のセキュリティチップを起点とした、ハードウェア・ルートオブトラストが実現できていること。
ディスクリートTPM クライアントPCに搭載されたTPMは、セキュリティレベルを高めるために、専用のHW上に実装されていること。
第三者機関によりセキュリティチップの認証 クライアントPCに搭載されたセキュリティチップ（TPM等）のセキュリティレベルを担保するために、第三者機関によるセキュリティに関する認証を取得していること。
BIOS/UEFIの保護、復元 • BIOS/UEFI、および、その設定が改ざんされた場合には、リアルタイムに改ざんを検知し、改ざん前の状態に復元できること。 • NIST SP800-193に準拠したBIOS/UEFIを搭載していること。
GPTの保護、復元 ストレージのGUID Partition Table(GPT)が破損または改ざんされた際に正常な状態に復元する機能をもつこと。
ブラウザ経由のウィルス対策 Webサイト経由でのウィルス感染を防止するため、ブラウザの実行環境がクライアントPC上でハードウェアレベル（仮想マシン）で隔離されていること。
メーラー経由のウィルス対策 メール添付ファイルからのウィルス感染を防止するため、安全性が確認されていないOfficeファイル(Word/Excel/PowerPoint)およびPDFファイルを表示する場合は、実行環境がクライアントPC上でハードウェアレベル（仮想マシン）で隔離されていること。
セキュリティ機能、構成の統一管理 クライアントPCにおける、ハードウェア、ソフトウェアにおけるセキュリティコンポーネントに関して、センター側で構成、設定を統一管理できること。

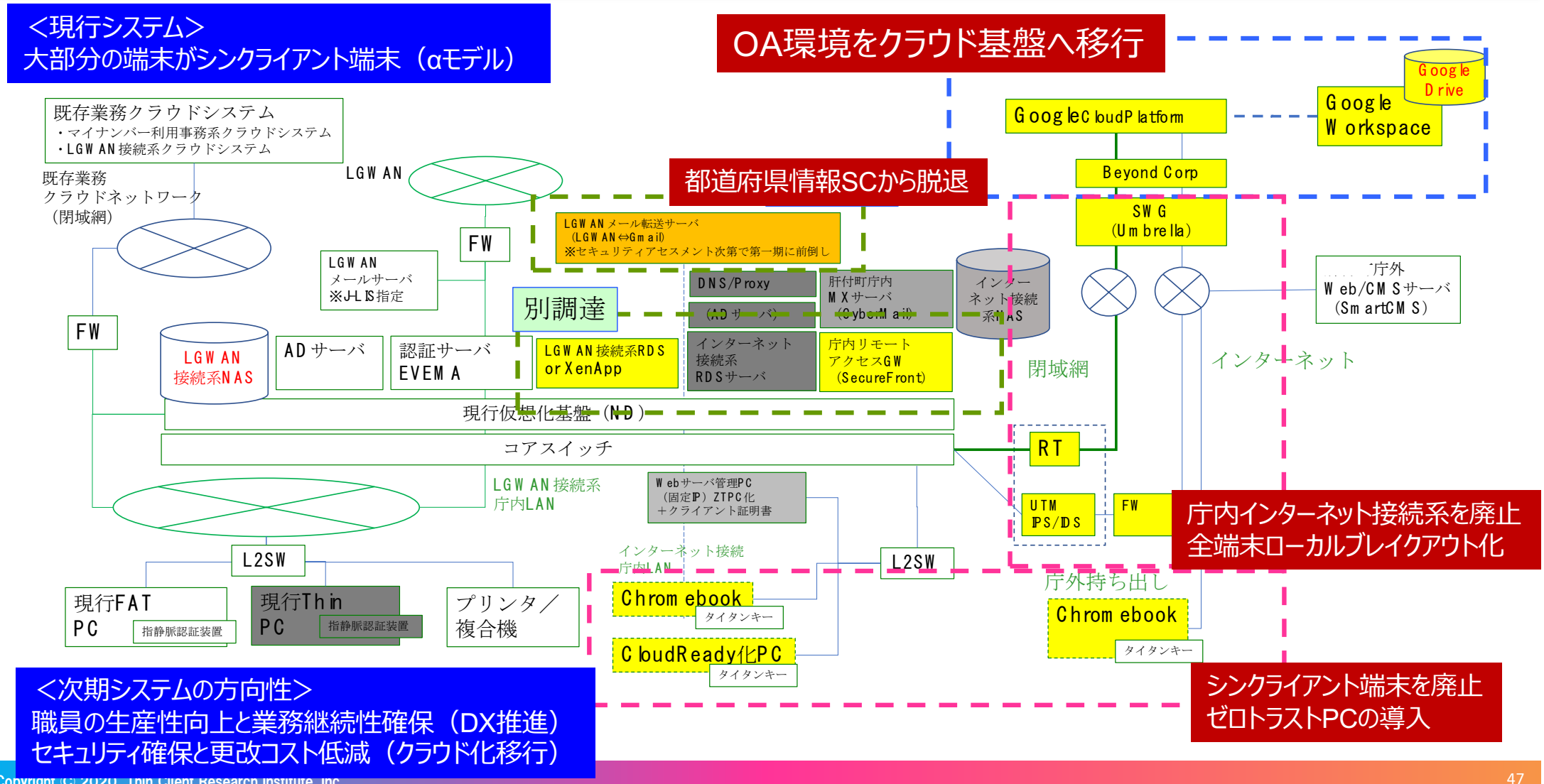
某自治体のβ´移行の方向性



某自治体のβ´移行の方向性



某自治体のβ´移行の方向性



セキュリティリスクアセスメントの方向性

リスクアセスメント実施においては、IPA(情報処理推進機構)セキュリティセンターが発行している、以下のガイドラインに従ってリスク分析を実施

『制御システムのセキュリティリスク分析ガイド　第2版（2020年3月発行）』

本ガイドでは、リスク分析は以下のフェーズに分かれています。

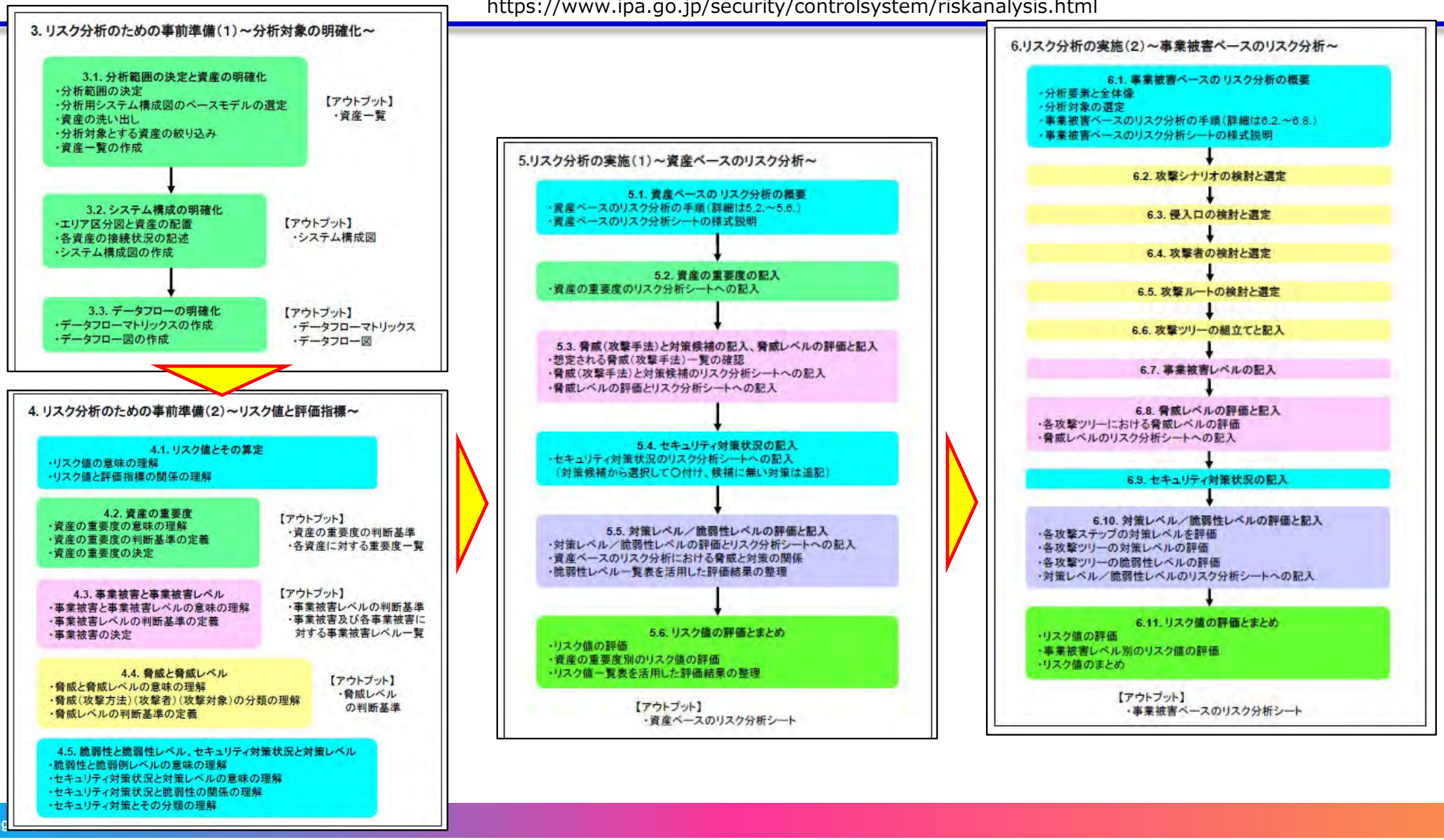
- リスク分析のための事前準備（１）～分析対象の明確化～
- リスク分析のための事前準備（２）～リスク値と評価指標～
- リスク分析の実施（１）～資産ベースのリスク分析～
- リスク分析の実施（２）～事業被害ベースのリスク分析～

自治体情報システムの、インターネット接続系とLGWAN接続系内のサーバ、端末、ネットワーク機器を構成要素（資産）とし、インターネット接続系業務端末、および、LGWAN接続系業務端末を分析対象として、ガイドに従って分析。

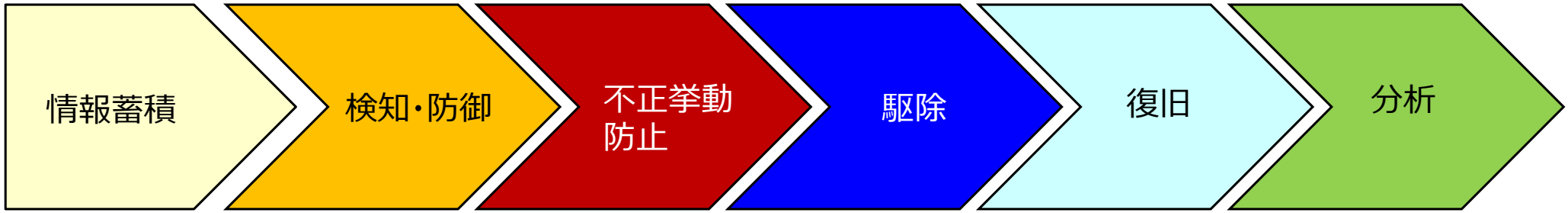
※2 制御システムのセキュリティリスク分析ガイド 第2版 (2020年3月発行)
https://www.ipa.go.jp/files/000080712.pdf

リスク分析のフロー（例）

※IPA発行 ”制御システムのセキュリティリスク分析ガイド 第2版”より抜粋
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html



エンドポイントにおけるセキュリティ対策フロー（ゼロトラストPC）



同様の攻撃が発生した
際、排除できるよう
過去に発生した
マルウェア等の情報蓄積

蓄積された情報
外部から侵入しようとした
ファイルを照合し
マルウェア等を特定し
侵入防止

侵入を許した
マルウェア等を発見
駆除

駆除しきれず
損害を出した部分を
排除

損害発生状況から
マルウェアの挙動を分析
防御の強化点を再検討

SOC／SIEM

従来の境界防御対策
情報セキュリティクラウドからなる入口対策

EDR
(Endpoint Detection and Responce)

不正な挙動を検知し、
感染後の対応を迅速に行うこと

OSのルールに基づく
プロセスの正しい
挙動以外を防止する
対策

侵入されても
発症しないような
対策

損害が発生しても
庁内／庁外に波及しない
損害が限定（極小化）され
る対策

ゼロトラスト対策PCによる内部対策

ローカルPCでアプリケーションを実行することによる操作性の向上
端末のセキュリティ管理（アップデート）負担を軽減

エンドポイントにおけるセキュリティ対策フロー（ゼロトラストPC）

情報蓄積 → 検知・防御 → 不正挙動防止 → 駆除 → 復旧 → 分析

同様の攻撃が発生した際、排除できるよう過去に発生したマルウェア等の情報蓄積

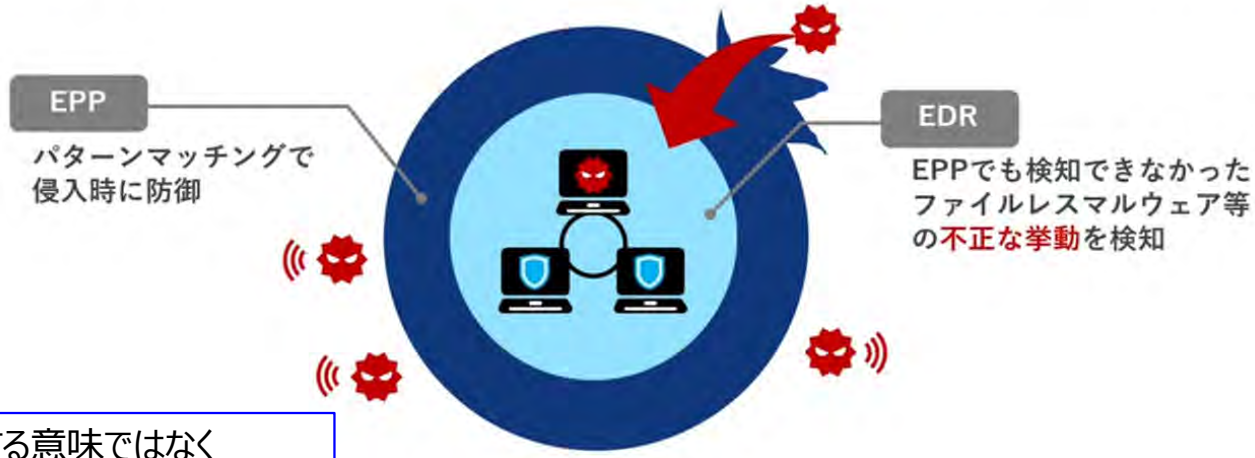
蓄積された情報外部から侵入しようとファイルを照合しマルウェア等を特定し侵入防止

従来の境界防御対策
情報セキュリティクラウドからなる入口対策

EDR
(Endpoint Detection and Responce)
不正な挙動を検知し、
感染後の対応を迅速に行うこと

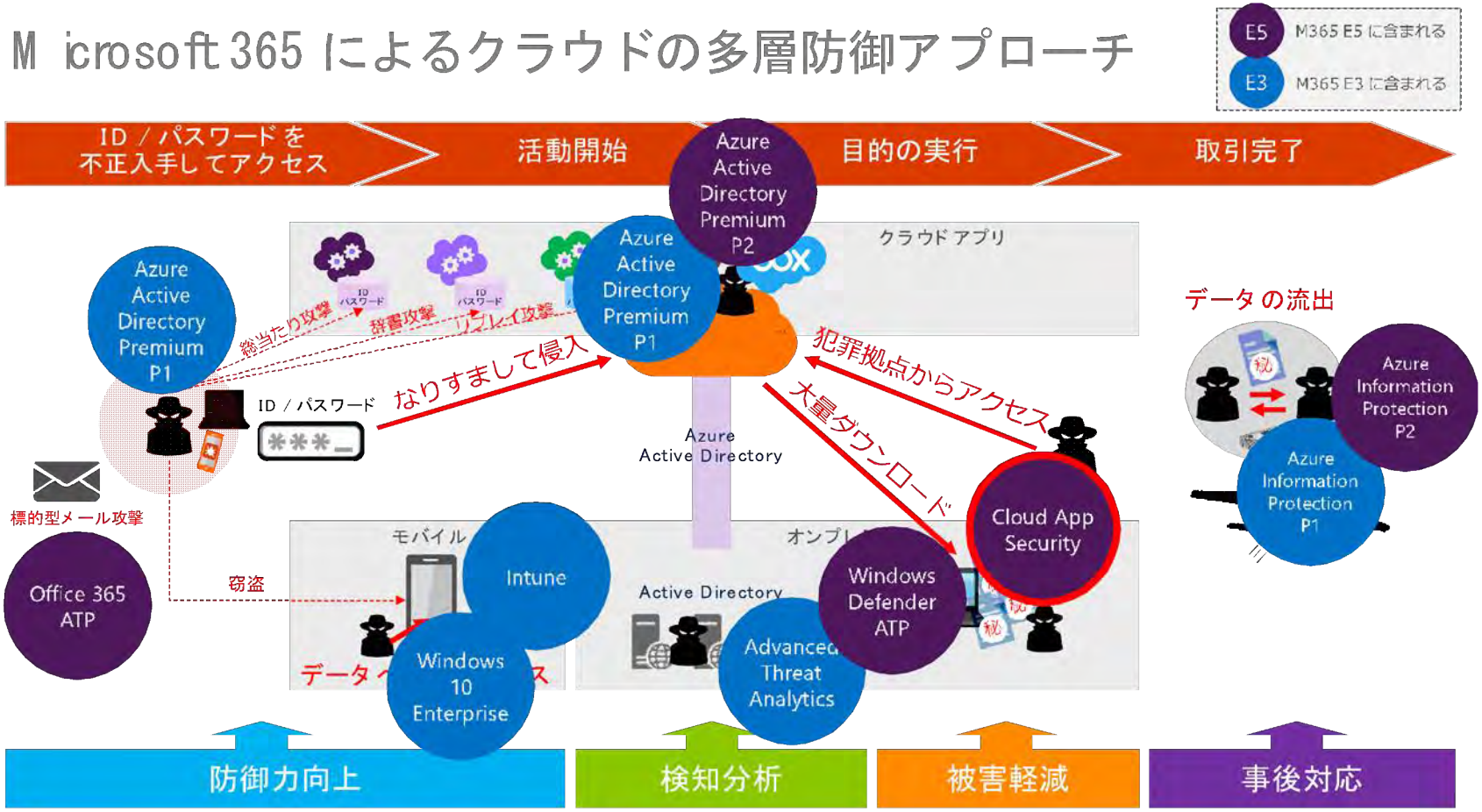
EDR（Endpoint Detection and Response）

「不正な挙動を検知し、感染した後の対応を迅速に行うこと」を目的とする



EDRそのものを導入する意味ではなく
「EDR的」な要件を持つ環境の導入が必須

参考：MS365のクラウドセキュリティ

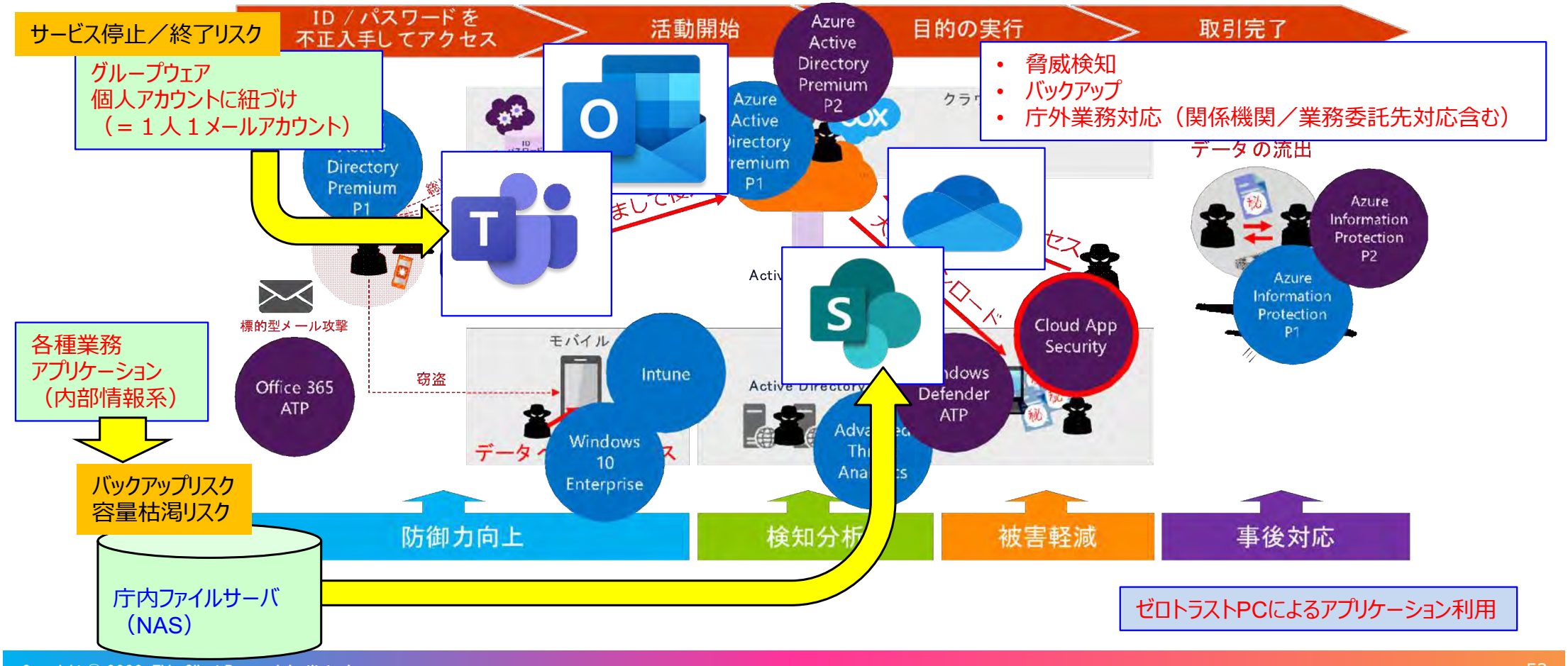


Offceを利用する限りでは十分なEDR環境を提供している

参考：庁内環境（ファイルサーバ／メール／グループウェア環境）のゼロトラストネットワーク環境への移行

庁内環境（ファイルサーバ、メール／グループウェア等）をクラウドに移行することにより
セキュリティ強化と事業継続性確保を実現

E5 M365 E5 に含まれる
E3 M365 E3 に含まれる



無害化の定義（総務省ガイドライン抜粋）

総務省発行“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(令和4年3月版)” iii-41ページ～iii-42ページ

（２） LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

分割とは、一旦両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすることをいう。

（ア）インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

LGWAN 接続系へインターネットメールを転送する際には、インターネットメールの転送に必要な特定サーバ間以外の通信を遮断するとともに、LGWAN 環境とインターネット環境はSMTP以外の Web 通信を始めとするプロトコルを遮断し、インターネットメールの添付ファイルの削除及び HTML メールのテキスト化を行う。

（イ）インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

インターネット接続系の端末を仮想デスクトップ化し、LGWAN 接続系の端末から添付ファイルも含むメールの閲覧を可能とする。

（ウ）危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

危険因子が埋め込まれたファイルを LGWAN 接続系に取り込んだ場合、脆弱性を突いた悪意あるコード等が実行される恐れがある。インターネット接続系から LGWAN 接続系にファイルを取り込む際は、以下のような手法により、危険因子をファイルから除去又は危険因子がファイルに含まれていないことの確認を行った上で、取り込まなければならない。

（いずれかの手法のみ又は複数の手法を組み合わせて採用することが考えられる。）

・ファイルからテキストのみを抽出

・ファイルを画像PDF に変換

・サービス等を活用してサニタイズ処理（ファイルを一旦分解した上で危険因子を除去した後、ファイルを再構築し、分解前と同様なファイル形式に復元する）

・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等で危険因子が含まれていないことを確認

なお、上記のいずれか又は複数の手法による対策を実施した場合であっても、マルウェア等の除去が完全に保証されるものではないため、 LGWAN接続系において以下のようなセキュリティ対策を実施しなければならない。

・OS 等の修正プログラムの適時適用（自治体情報セキュリティ向上プラットフォームの利用等）

・アンチウイルスソフトウェアの最新化（定義ファイルのアップデート等）

・業務に必要なファイルやメール等の定期的なバックアップの実施 また、上記の LGWAN 接続系における対策に加え、業務システムの停止を狙ったマルウェアの感染を防ぐ対策として、LGWAN接続系端末にアプリケーションホワイトリストを設定し、実行できるアプリケーションの制限等を行うことを強く推奨する。

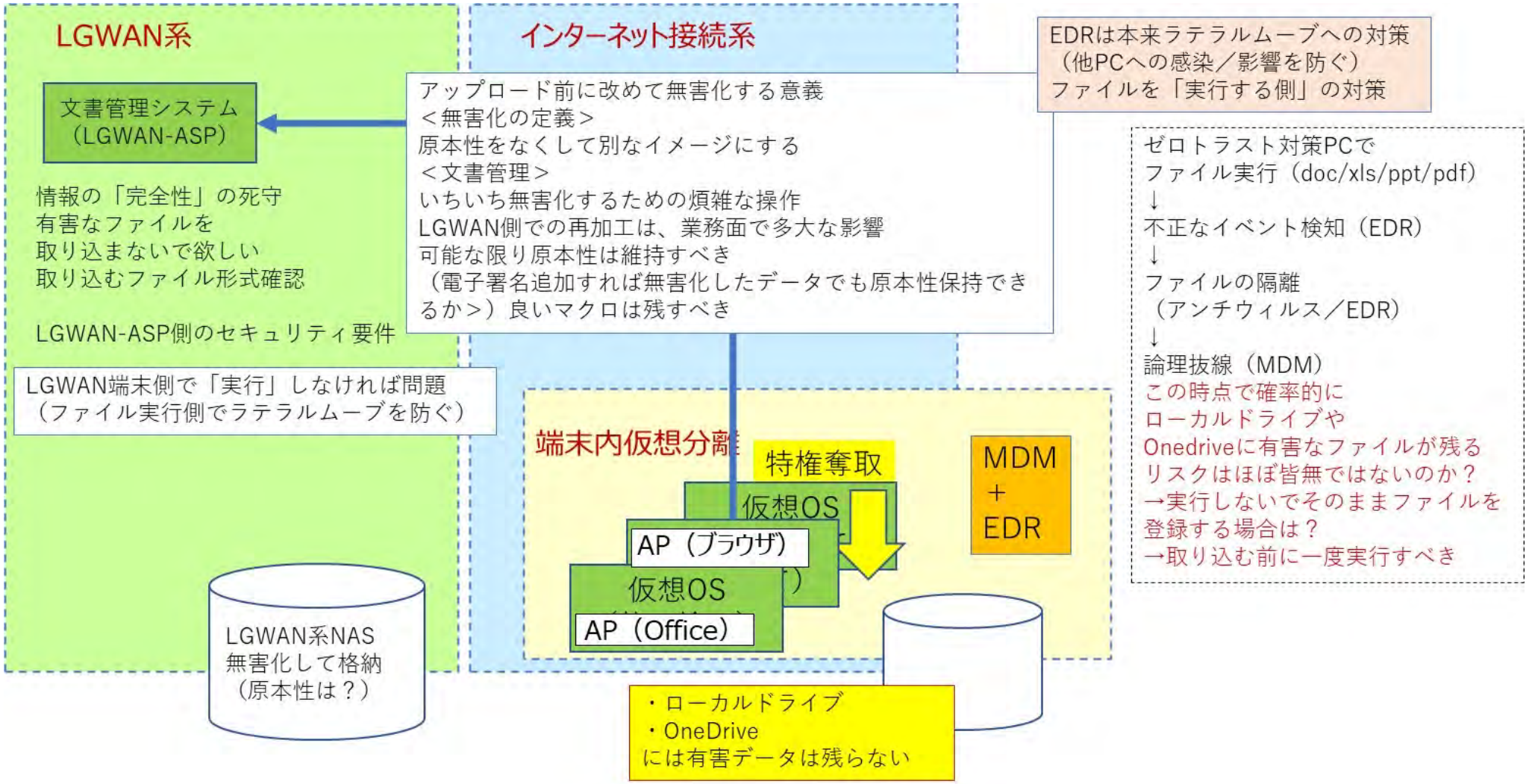
（注５）「目視で確認」とは、ファイルが添付されたメールを開く際に、送信元は適切か（見覚えのないアドレス、フリーアドレス又は正規の組織名若しくはドメインに似せたアドレスではないか）、メールの件名や内容が適切か

（見慣れない日本語やフォントが使用されていないか）などを確認することである。未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等の製品の導入に加え、人的対策として「目視で確認」を求めるものである。

（注６）サニタイズ処理等を実現する手法は多岐にわたるため、適正な製品を選定し導入することが望ましい。

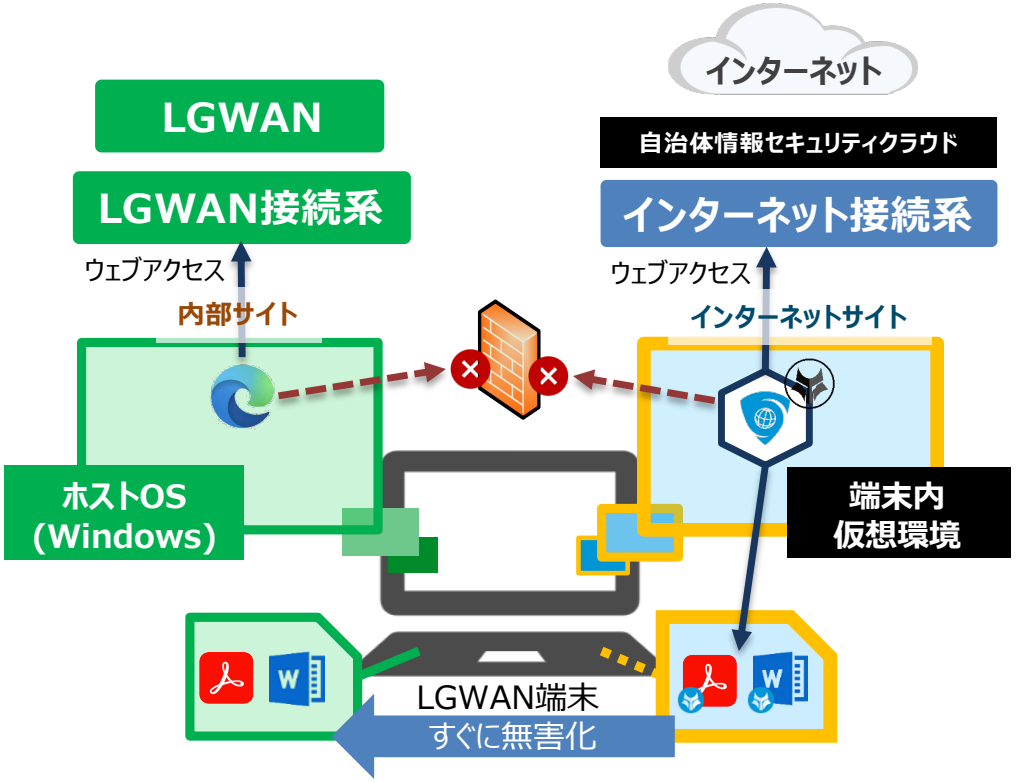
（注７）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系から LGWAN 接続系へマルウェア感染を防ぐ必要がある。

ゼロトラストセキュリティにおけるファイル「無害化」



アルファモデルで利便性を向上させた那覇市様の事例　～端末内仮想化技術の活用～

端末内仮想ブラウザソリューション(HP Sure Click Enterprise) ならブラウザを軽量なマイクロVMで隔離実行し、端末内でネットワーク分離を実現します。脆弱性を狙われウイルスが実行されたとしても、ホストOSを完全に保護します。



快適な操作性

・端末内で実行される軽量な仮想マシンのため、ブラウザによる快適な操作性を実現。

ファイル利用が楽

・ダウンロードファイルは保存後すぐに無害化しLGWAN環境で閲覧、編集、印刷可能。

コスト削減

・端末内仮想環境のため、仮想環境用サーバが不要となり、構築、運用コストを削減。

アルファモデルで利便性を向上させた那覇市様の事例　利用イメージ（ブラウザを開く）

Chrome、Edgeと同じエンジン(Chromium)を使っており、見た目、機能はほぼGoogle Chromeと同じです。
また、上部のバーを青くすることにより、ユーザは仮想ブラウザであることが見た目でわかります。

インターネットサイトを閲覧する場合は、デスクトップ上の仮想ブラウザのアイコンをクリックします。認証も不要です。LGWANサイトを閲覧する場合は、ネイティブブラウザを開きます。

ブラウザは、端末内仮想環境で実行されるため、脆弱性を狙われウイルスに感染しても、Windows環境へ影響はありません。もし万が一感染したとしてもブラウザを閉じるだけで、なかったことになります。

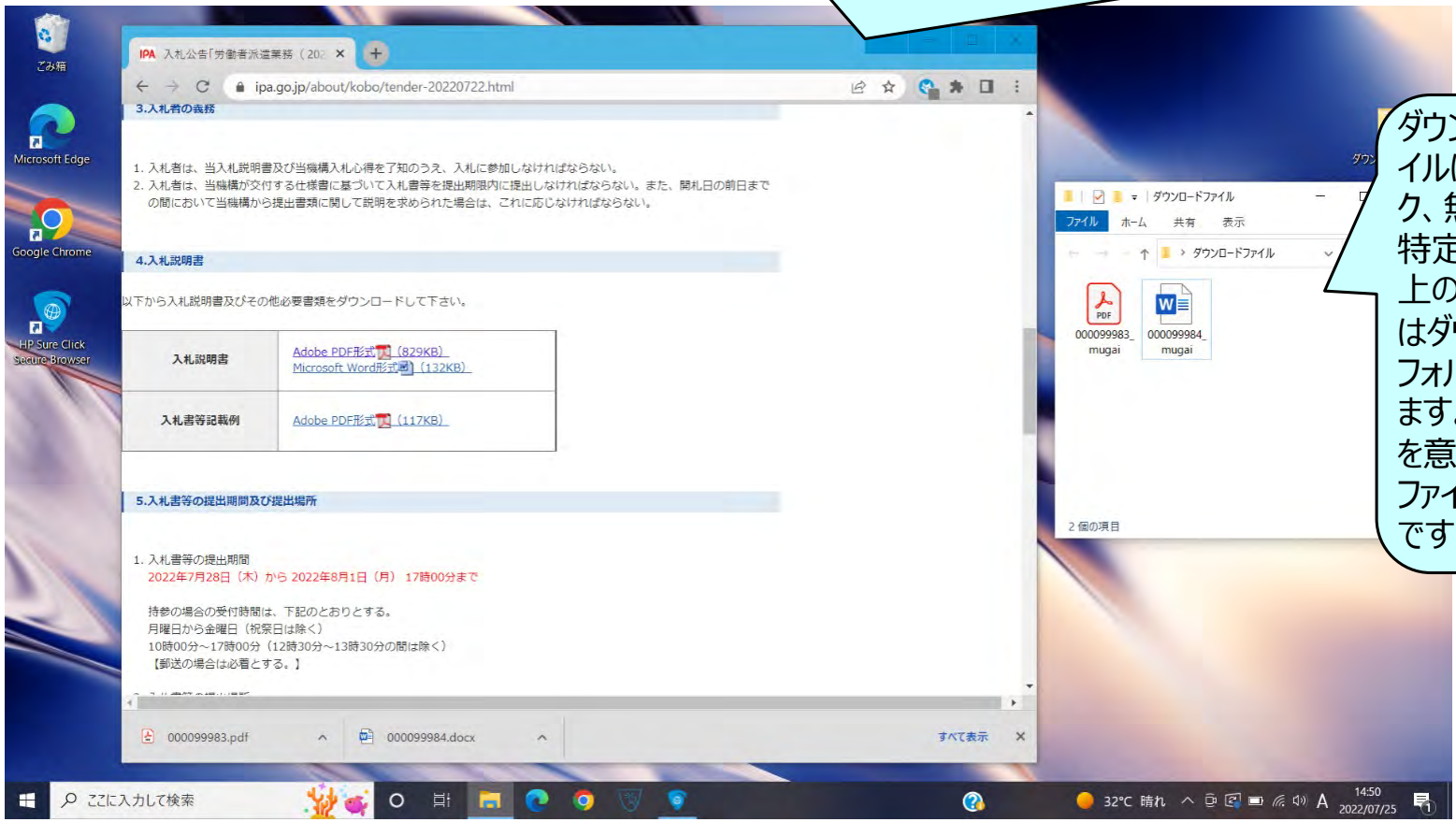
アルファモデルで利便性を向上させた那覇市様の事例　利用イメージ（ユーザの操作感）

音声(スピーカー、マイク)が使えるため、動画配信をみたり、ブラウザでWeb会議に参加することもできます。
ただし、その場合はネットワークへの帯域負荷がかかることが予想されるため、ネットワーク側で帯域制限をかけたり、Web会議は職員端末からせず専用端末のみとする、などの制限を検討する必要があります。

仮想ブラウザは端末内の仮想環境で動作し、端末内で画面転送している仕組みとなります。
ですので、操作感（レスポンス）が、サーバ型のソリューションに比べて格段によくなります。

アルファモデルで利便性を向上させた那覇市様の事例　利用イメージ（ファイルダウンロード）

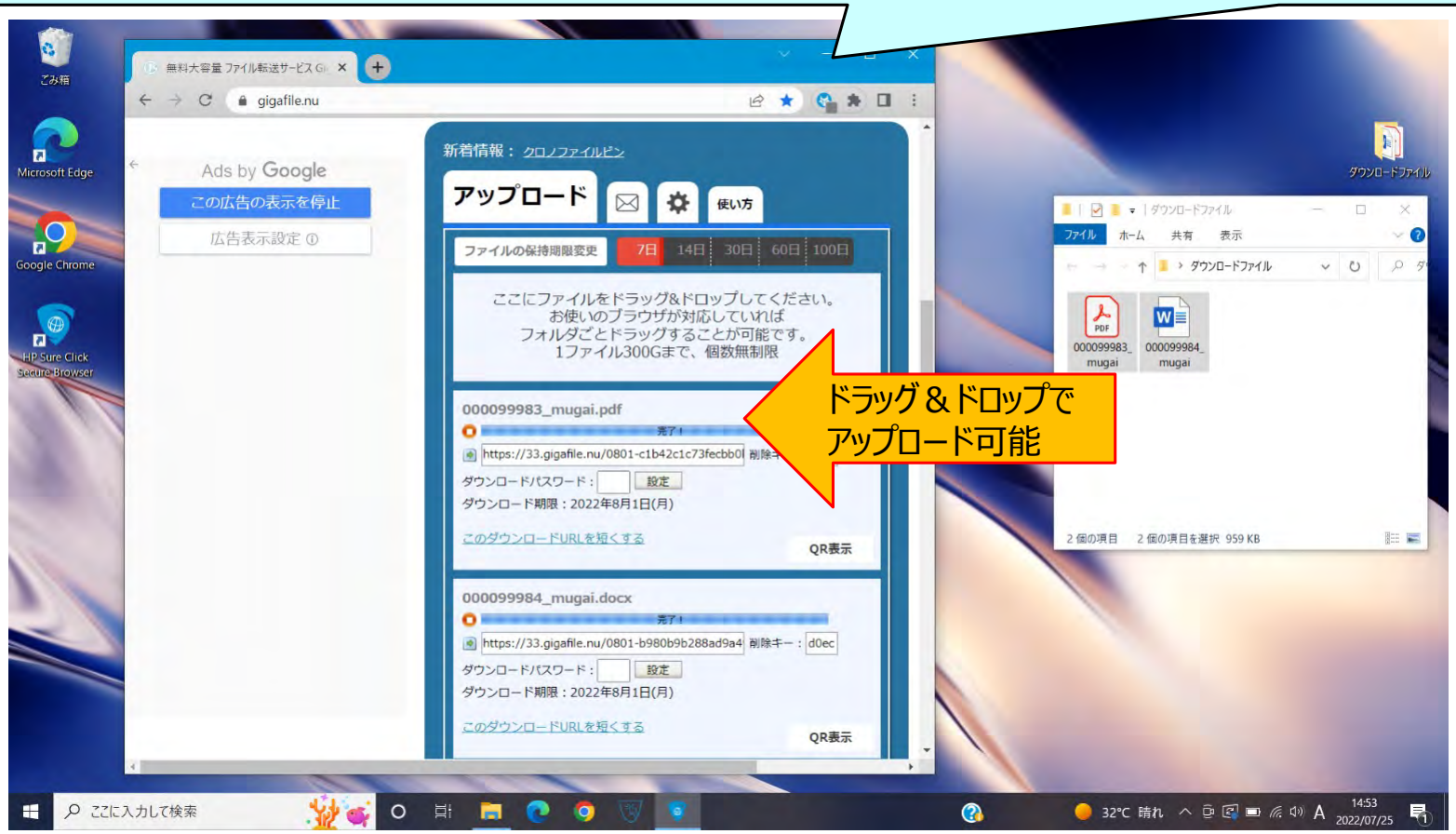
通常のブラウザと同じように、ダウンロードしたいファイルを指定します。ただし、保存先フォルダは指定できません。
ダウンロードしたファイルは、ウイルスチェック、無害化処理が自動で行われます。



ダウンロードされたファイルは、ウイルスチェック、無害化処理後、特定のファイルサーバ上のフォルダ（ここではダウンロードファイルフォルダ）に保存されます。職員は無害化を意識せず、すぐにファイルを利用可能です。

アルファモデルで利便性を向上させた那覇市様の事例　利用イメージ（ファイルアップロード）

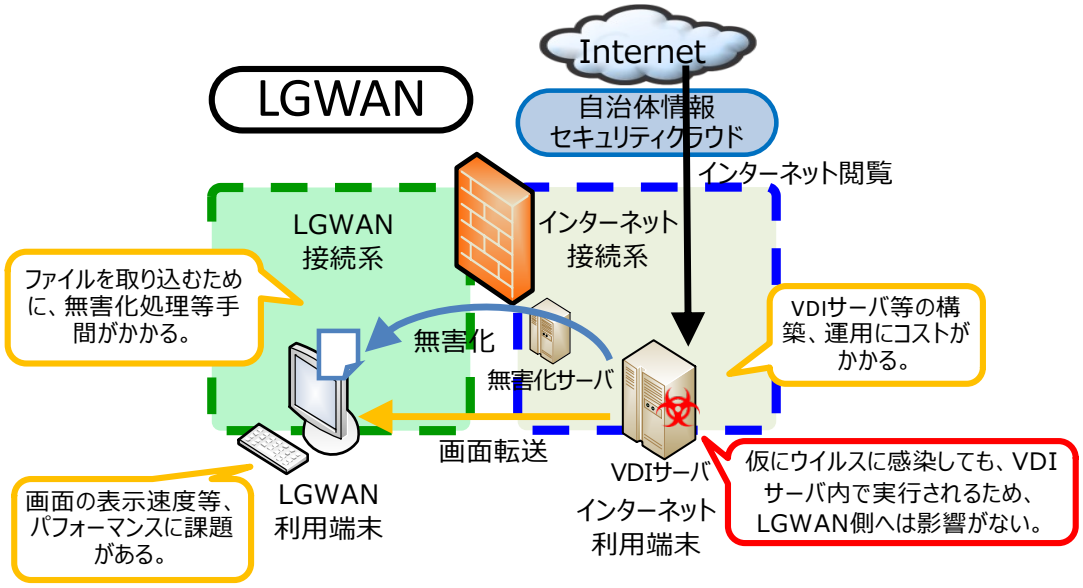
通常のブラウザと同じように、仮想ブラウザ経由でファイルアップロード（ドラッグ＆ドロップ、あるいは別ウィンドウでのファイル指定）が可能です(製品仕様)。ただし、そのままだと情報漏洩につながる恐れがあるため、アップロードを全面禁止する、あるいは、特定の職員のみ特定のURLへアップロードする、ような制御を検討しています。



アルファモデルで利便性を向上させた那覇市様の事例　システム構成の概要、メリット

サーバ型仮想環境の場合

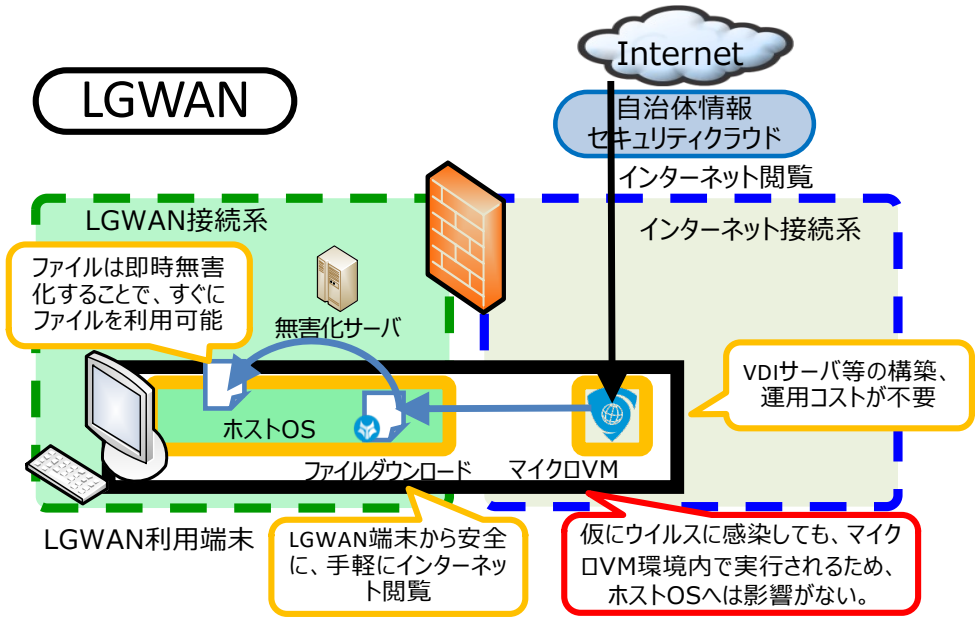
サーバ型仮想環境（VDIや仮想ブラウザサーバ）でインターネットにアクセスする場合、以下の課題が挙げられます。
・画面の表示速度等、パフォーマンスに課題がある。
・ファイルを取り込むために、無害化等手間がかかる。
・VDIサーバ等の同時接続数などの拡張性や、可用性を考慮する必要があり、設計、構築、運用にコストがかかる。



サーバ型仮想環境の場合のシステム構成

端末内仮想ブラウザ(HP Sure Click Enterprise)の場合

端末内仮想ブラウザでインターネットにアクセスし、即時無害化させる那覇市様の構成の場合、以下のメリットがあります。
・LGWAN端末から安全に、手軽にインターネット閲覧
・ファイルは無害化等処理せずに内容を確認、編集可能
・VDIサーバ等で考慮が必要な、同時接続性や可用性を考慮する必要がなく、設計、構築、運用コストが不要



端末内仮想ブラウザ導入時のシステム構成

アルファモデルで利便性を向上させた那覇市様の事例　参考：他ソリューションとの比較

端末内仮想ブラウザソリューション(HP Sure Click Enterprise) は、インターネット仮想分離環境を実現するサーバ型ソリューションに比べて、ユーザ操作性や、システム構成で、以下のようなメリットがあります。

項目	端末内仮想ブラウザソリューション		仮想ブラウザサーバ		仮想デスクトップ(VDI)サーバ	
操作性(性能)	○	仮想ブラウザ用の仮想マシンは、端末内で実行される軽量な仮想マシンのため、快適な操作性を実現。	△	ブラウザは仮想サーバ側で実行され、画面転送により端末側で描画されるため、ネットワークの遅延によるレスポンスの遅れがある。	△	仮想デスクトップ環境上で実行されたブラウザを、画面転送により端末側で描画するため、ネットワークの遅延によるレスポンスの遅れがある。
操作性(見た目)	○	Chromiumベースのため、Edge、Chromeなどのブラウザを実行するのと同じ操作感で実行可能。また、ブラウザ上部の色を変更し、セキュアブラウザと認識させることが可能	×	製品によっては、描画エンジンが独自開発となるため、ネイティブブラウザと見た目やメニューが異なったり、起動メニューが独自の構成となる。	△	仮想デスクトップ環境への接続は専用アプリとなるが、接続後は通常のWindowsデスクトップ環境として操作可能。
ファイル利用	○	端末内のファイルシステムを利用して、セキュアブラウザ経由で直接ファイルをダウンロード、アップロードすることが可能。また、ダウンロードしたファイルは、無害化製品と連携し、自動で無害化させることが可能。	△	パソコン端末と仮想ブラウザ用サーバのセグメントが異なるため、中間にファイルサーバ等でファイルを共有、無害化する仕組みが必要。製品によっては、無害化機能が含まれているものもある。	×	パソコン端末と仮想デスクトップ用サーバのセグメントが異なるため、中間にファイルサーバ等でファイルを共有、無害化する仕組みが必要
システム構成	○	パソコン端末内でブラウザを仮想化し、端末内で画面転送するため、仮想ブラウザ用サーバを構築不要。	△	仮想ブラウザサーバでブラウザを仮想化し、パソコン端末へ画面転送するため、仮想ブラウザ用サーバが必要台数、構築する必要がある。	×	仮想デスクトップ環境は、接続管理等複数のサーバの組み合わせでの大規模なシステム構成となる。
システム設計	○	仮想ブラウザ用サーバが不要で、端末内仮想環境から直接インターネットへ接続するため、同時接続数、拡張性、負荷分散など、一般的なサーバ設計を考慮する必要がない。	△	仮想ブラウザ用サーバのスペックにより、サーバ１台に同時に接続できる端末数に上限があり、拡張性や負荷分散を考慮し設計する必要がある。	△	仮想デスクトップ用サーバのスペックにより、サーバ１台に同時に接続できる端末数に上限があり、拡張性や負荷分散を考慮し設計する必要がある。
システムコスト	○	仮想ブラウザ用サーバが不要のため、HW/SWコスト、サーバ構築/運用コストが不要となる。	△	仮想ブラウザ用サーバが必要なため、HW/SWコスト、サーバ構築/運用コストが必要となる。	×	仮想デスクトップ用サーバが必要なため、HW/SW(リモートデスクトップライセンス含む）コスト、サーバ構築/運用コストが必要となる。

ありがとうございました