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

2024年1月17日

シンクライアント総合研究所
奥野克仁

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
・ISMS（JIS Q 27001）審査員

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．次期自治体情報セキュリティ強靭化の方向性について
３．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

１．セキュリティ強靭化策の現状と見直し

約6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。

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

個人情報保護の３原則

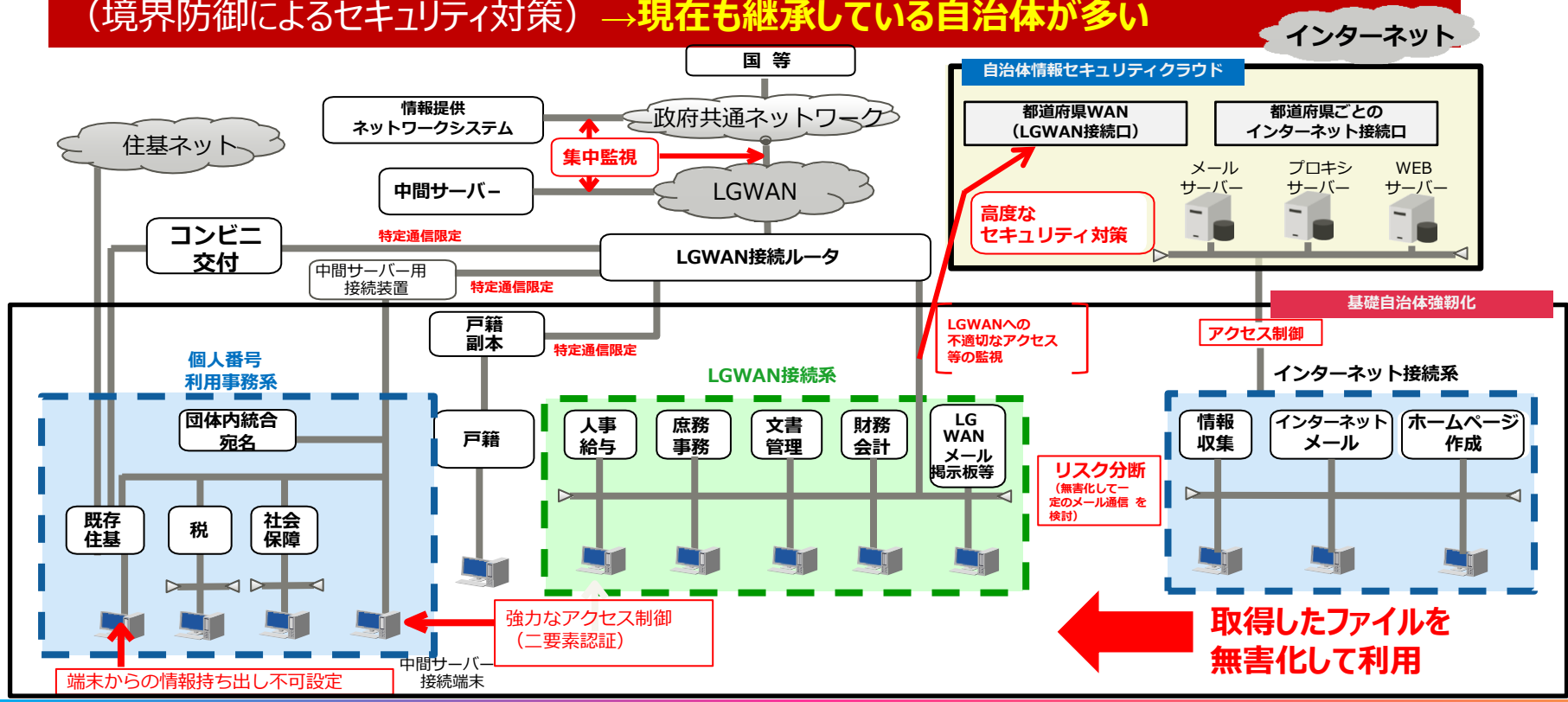
機密性	許可された者だけが情報にアクセスできるようにすること。 許可されていない利用者は、コンピュータやデータベースにアクセスできないようにしたり、データを閲覧できるが書き換えることはできないようにする。
可用性	許可された者が必要なときにいつでも情報にアクセスできるようにすること。可用性の維持は、情報を提供するサービスが常に動作するということ。
完全性	保有する情報が正確であり、完全である状態を保持すること。情報が不正に改ざんされたり、破壊されたりしないこと。

＜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。

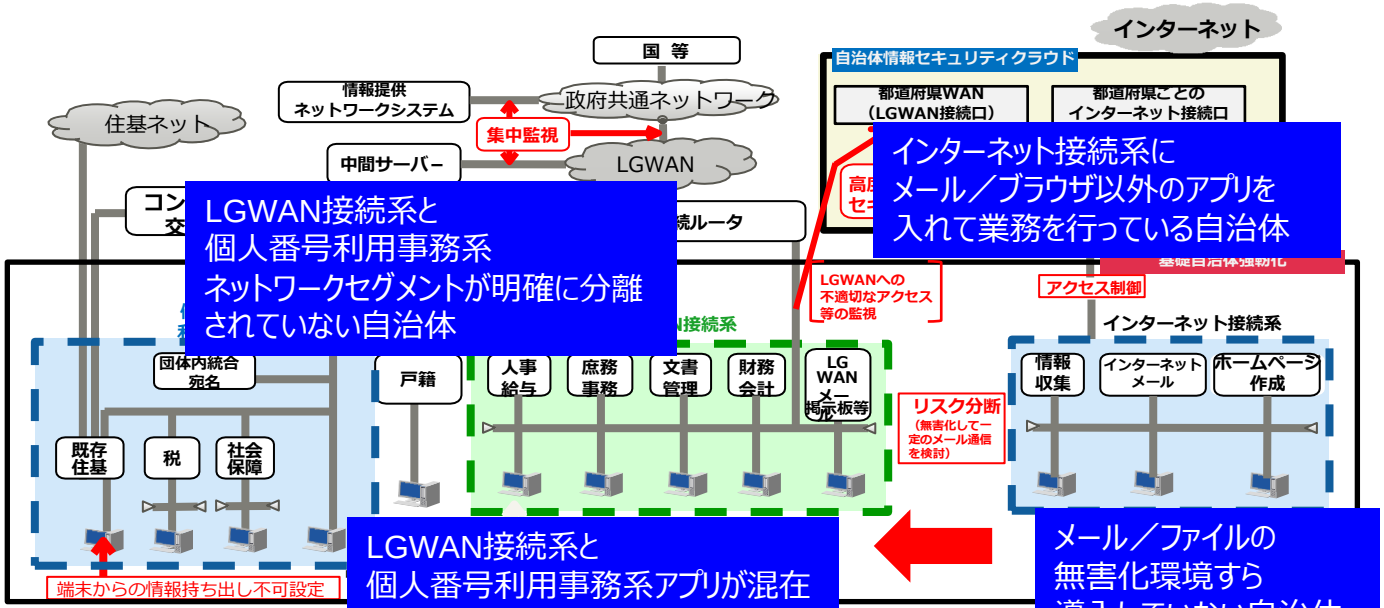
地方自治体のセキュリティ強靭化対策

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）**→現在も継承している自治体が多い**



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



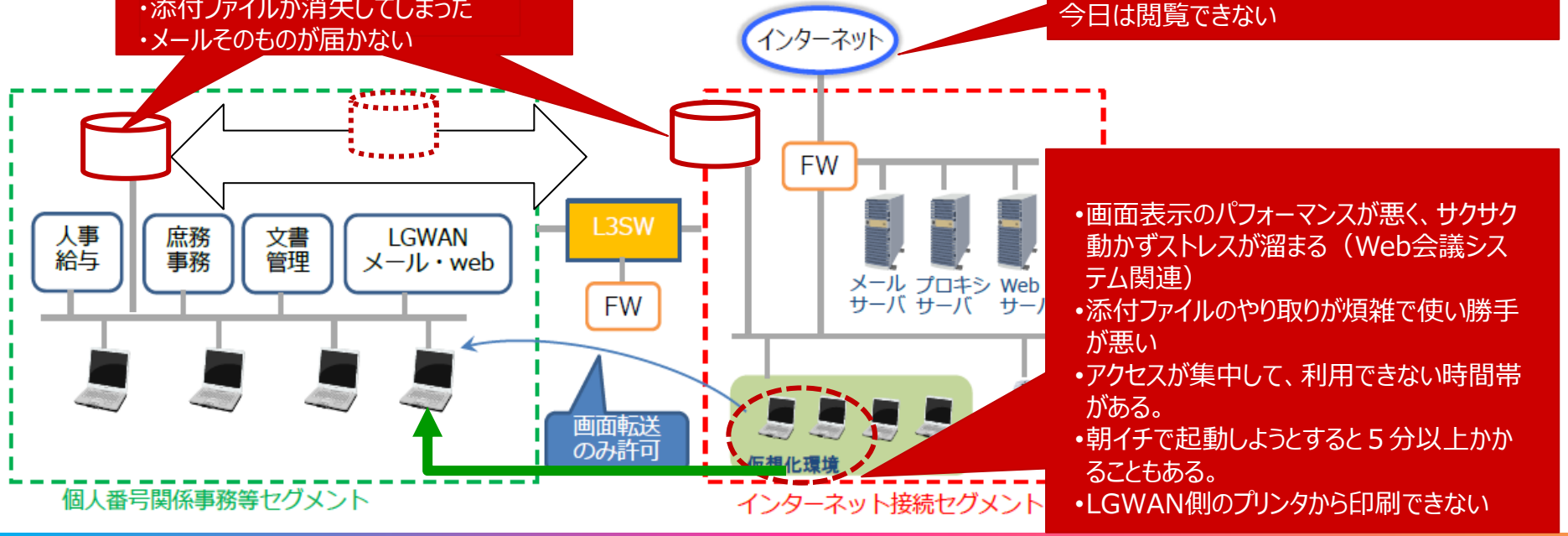
現行の無害化対策(大部分の自治体が仮想化環境を導入)

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（Web会議システム関連）
・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)

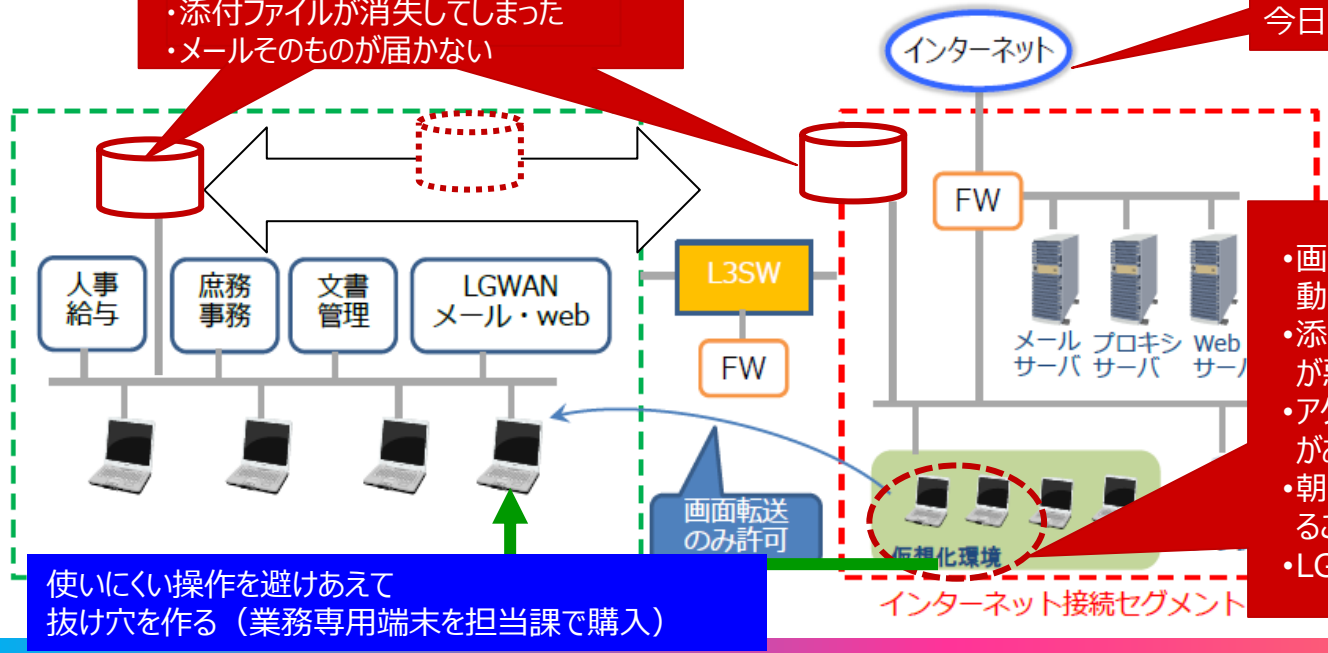
・個人番号関係事務等セグメントとインターネット接続セグメントを分割する
・個人番号関係事務等セグメントの端末において、仮想化環境から転送された
可能となる
ト接続環境のプリンタを

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)

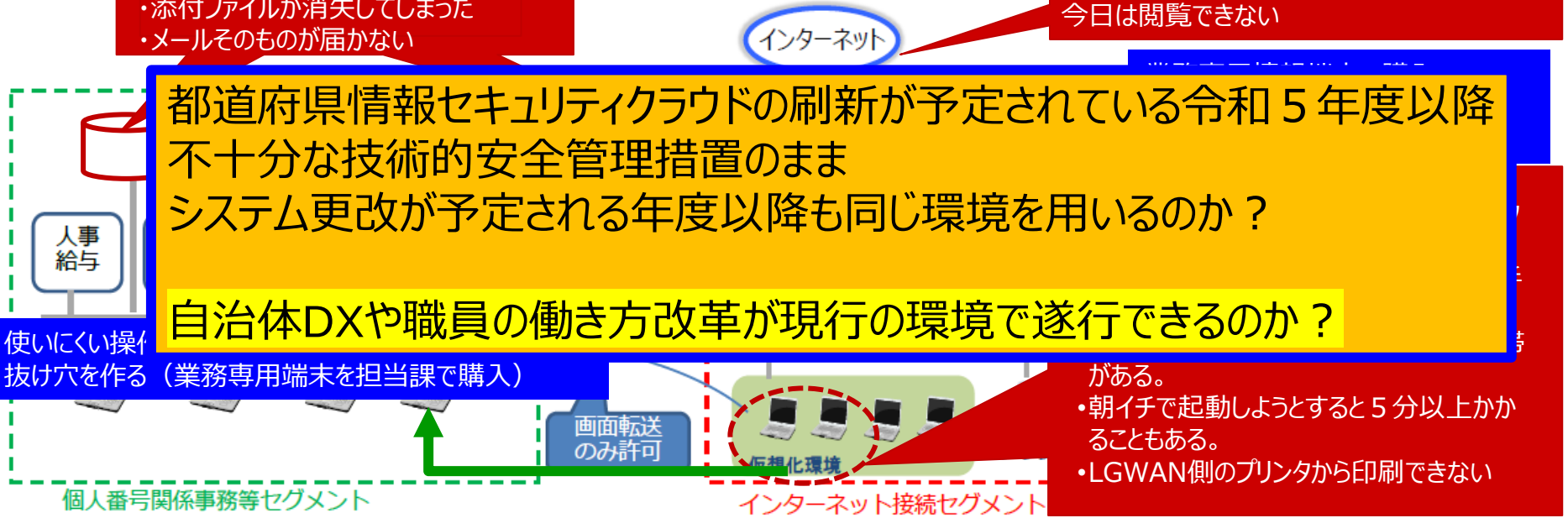
出典:
新たな自治体情報セキュリティ対策の抜本的強化(案)
等の報告について(2015.10.23)

・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



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？

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）

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

自治体DXとセキュリティー

自治体DX推進計画においては、以下①～⑥と関連2点を、重点取組事項としている。

重点取組事項	国の主な支援策等
⑤ テレワークの推進 テレワーク導入事例やセキュリティポリシーガイドライン等を参考に、テレワークの導入・活用を推進 前記の①、③による業務見直し等に合わせ、対象業務を拡大	● テレワーク導入円滑化のためのセキュリティポリシーガイドラインの改定【総務省】 ● LGWAN-ASPによるテレワーク環境の提供【総務省】 ● テレワーク導入事例等の提供【総務省】
⑥ セキュリティ対策の徹底 改定セキュリティポリシーガイドラインを踏まえ、適切にセキュリティポリシーの見直しを行い、セキュリティ対策を徹底	● 令和2年にセキュリティポリシーガイドラインの改定【総務省】 ● 自治体の標準化・共通化を踏まえ、「三層の対策」の抜本的見直しを含めた新たなセキュリティ対策の在り方の検討【総務省】 ● 令和2年度第3次補正予算において、次期自治体情報セキュリティクラウドへの移行を支援（国費1/2 29.3億円 令和4年度まで）【総務省】
自治体DXの取組みとあわせて取り組むべき事項	
① 地域社会のデジタル化 デジタル化によるメリットを享受できる地域社会のデジタル化を集中的に推進	● デジタル化によるメリットを享受できる地域社会のデジタル化を集中的に推進するため、新たに「地域デジタル社会推進費（仮称）」2000億円を計上（令和3・令和4年度 うち、道府県分800億円程度、市町村分1,200億円程度）【総務省】
② デジタルデバイド対策 「デジタル活用支援員」の周知・連携、NPOや地域おこし協力隊等地域の幅広い関係者と連携した地域住民に対するきめ細やかなデジタル活用支援	● 携帯ショップ等が主体となる「デジタル活用支援員」によって、オンラインによる行政手続・サービスの利用方法等に関する助言・相談等を実施【総務省】 ● [再掲] デジタル化によるメリットを享受できる地域社会のデジタル化を集中的に推進するため、新たに「地域デジタル社会推進費（仮称）」2000億円を計上（令和3・令和4年度 うち、道府県分 800億円程度、市町村分 1,200億円程度）【総務省】

参考　自治体・行政機関での情報セキュリティ事故（インシデント）例

- 日本年金機構での情報漏えい事故（平成27年５月）
- 岐阜市職員による「がん検診」入力ミスで誤通知→死亡に至る事例も　（令和元年7月）
- 岩手県釜石市職員による住基データ全件不正持出し（令和4年5月）
- 兵庫県尼崎市委託先関係者による住基・所得等データUSB紛失（令和4年６月）
- 千葉県南房総市　教育委員会でのランサムウエア（身代金要求型ウイルス）感染　（令和4年7月19日）　※最近多くの自治体で同様の被害が発生
- 東京都コロナ登録再委託先の派遣職員、37名の情報不正取得し知人に送信（令和5年6月4日）
- 職員のＵＳＢメモリー紛失、係長は上司に報告せず…判明日ずらすよう働きかけも（令和5年5月14日）静岡県函南町
- 岩手県大槌町　不正アクセスに伴う個人情報の漏えいのおそれに関する調査結果のご報告について（令和5年7月4日）

参考　セキュリティニュース（株式会社セキュアオンライン）

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
https://www.sankei.com/affairs/news/210107/afr2101070001-n1.html

- 福岡県は2021年1月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
- 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が、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。

出典：福岡県庁Web
https://www.pref.fukuoka.lg.jp/contents/covid19-rouei.html

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。

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）
FAXの誤送信も現在も数多く発生

セキュリティ強靭化対策の限界②

弘前市職員２７４７人の個人情報流出か　謎の通報で発覚

出典：朝日新聞2019年12月14日 https://www.asahi.com/articles/ASMDF4GFNMDFUBNB008.html

- 弘前市職員２７４７人分の氏名・性別から最終学歴・給料まで約７０項目に上る個人情報が外部に流出した可能性が高いことが明らかに
- 誰がどうやって、どんな目的で流出させたのか。市は深刻な事態と受け止め内部調査を進めているが、全容解明には時間がかかりそうだ。
- 人事課が２日から情報システム課と連携して内部調査を進めているが、職員が関与したのか外部から不正な侵入があったのかもまだ不明という。内部調査ではっきりしなければ、警察の協力も得て原因を解明する方針

市人事課によると、１１月１８日、同２６日、１２月２日、同１０日に「流出」を指摘する匿名のメールが同課に寄せられ、１２日には秘書課にも届いた。「このようなリストが流出してよいのか」「職員から流出している」「公表しないで隠すのか」「報道機関に発表して説明を求めます」などの趣旨の文言があり、２日のメールには８人分、１２日のメールには４２人分のデータも記載されていたという。

５通のメールは「匿名」「市民」の名前で届き、電話番号やアドレスは全部異なっているという。市は電話や返信をして連絡を取ろうとしているが、やり取りはできていないという。

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（最近では釜石市も内部職員による不正が発覚）

セキュリティ強靭化対策の限界③

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
https://www.sankei.com/article/20210322-QPFDGVAVAZIAPB7M37PJ7QWP6Y/

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

- 住宅政策推進の基本計画「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（うちマンション所有者氏名等の個人情報約８２００件）のデータが流出。
- サイバー攻撃を受けたコンサルタント会社は都市計画等を手掛けており、都が「都住宅マスタープラン」作成に当たり調査業務を委託し、業務に必要な情報を一部提供
- 会社のサーバに異常が見つかり、コンピューターウイルスの感染が判明
- コンサルタント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。

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④

神奈川県庁のハードディスク転売　消去委託社員がネット出品―警視庁が逮捕

出典：時事通信2019年12月07日
https://www.jiji.com/jc/article?k=2019120600913&g=soc

- 神奈川県庁は行政文書の管理に用いるサーバーのハードディスク（ＨＤＤ）１８個がインターネットオークションに出品され、全て落札されていたと発表
- ＨＤＤを持ち出していたのは、情報機器再利用会社「ブロードリンク」（都道府県中央区）社員。同社は警視庁に被害を相談し、同庁は６日、別のＨＤＤを盗んだとして、窃盗の疑いで社員の容疑者を逮捕した。容疑を認め、県庁のＨＤＤ持ち出しも認めている。
- サーバーのリース契約が終了したことに伴い、ブロード社がデータ消去を請け負った。同社はＨＤＤに穴を開けて復元不可能にする予定だったが、社員が処理前に持ち出し、７～８月に１８個が出品された。うち９個が回収され、中には自動車税申告書などの個人情報が残っていた。残りの所在は分からず、ＨＤＤの容量は計２７テラバイトあるという。

＜県及び一次請負業者の運用の不備＞
- 神奈川県は格納したデータの暗号化を実施せず。
- 返却の際は初期化作業を行いデータ全ての消去作業を実施。
- 返却から7カ月経過した後も富士通リースからHDDの消去証明書を受領しておらず。
- 神奈川県の担当者は富士通リースが廃棄処理をブロードリンクに委託していたことは把握しておらず、社名も知らなかった。
- 直接的な契約がないことから担当者が廃棄の現場の立会いは実施しなかった。

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（取引業者管理）

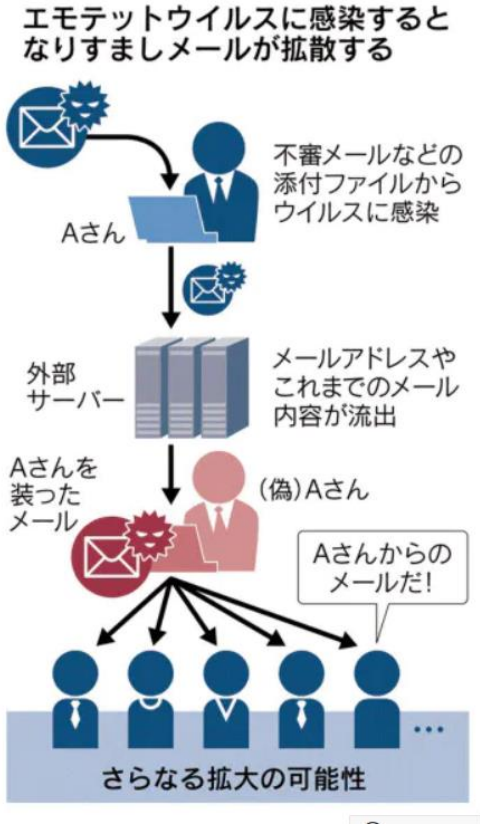
新種のウイルスも数多く出現

なりすましメール拡散のウイルス、日本に本格上陸

出典：日本経済新聞2019年11月29日
https://www.nikkei.com/article/DGXMZO52768110Z21C19A1TJ2000/

- 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。
- 首都大学東京の教員に過去にやりとりがあった海外の雑誌社から届いたメールの添付ファイルを開いたところ、複数の教職員に成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。

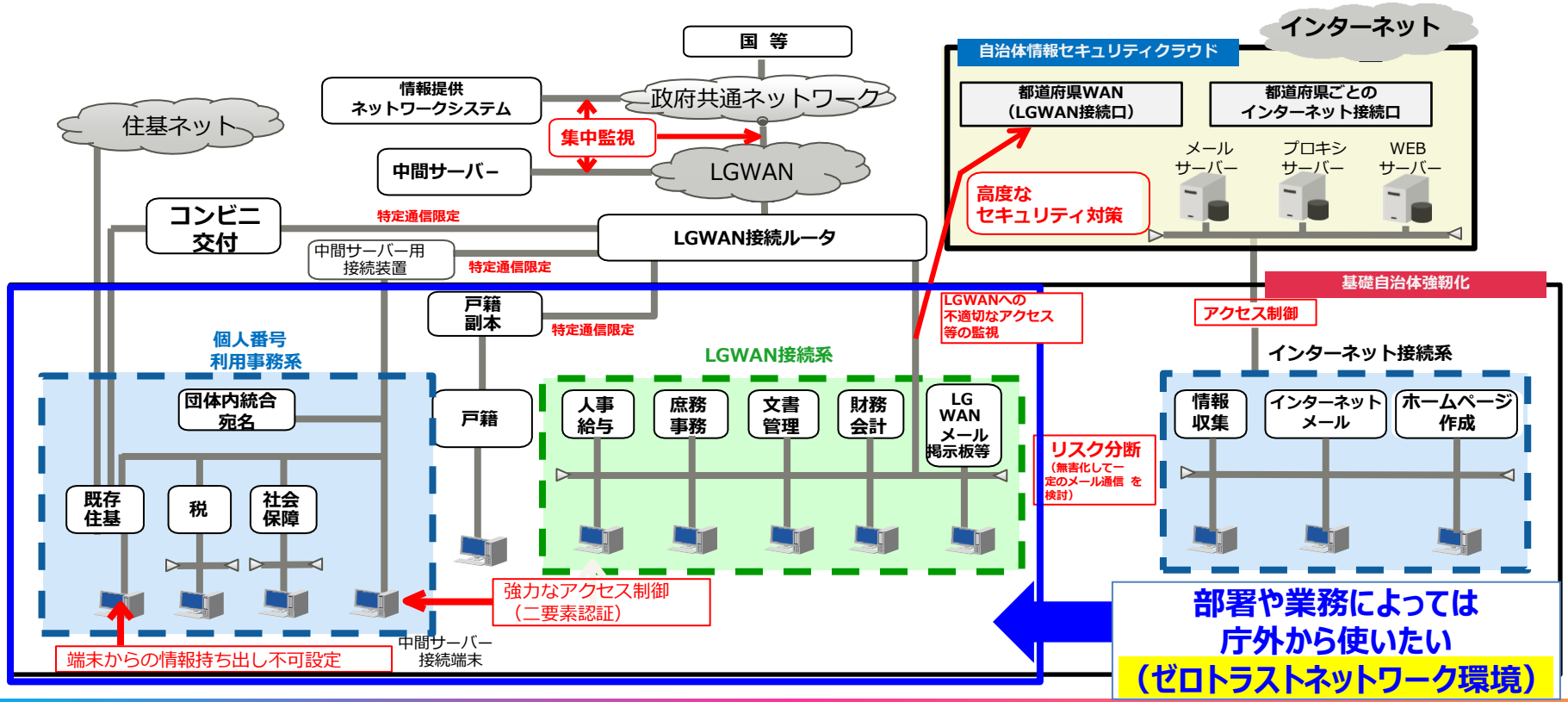
改正個人情報保護法（2022年4月）事業者の守るべき責務
- 漏えい等が発生した場合、個人情報保護委員会への報告、および本人への通知が義務化される（従来は努力義務）
- ペナルティ（罰金）の強化（法人による命令違反で課せられる罰金刑は、上限50万円から1億円）
- 不正アクセスによる漏えいは件数を問わず、たとえ1件であっても本人への通知が義務化



2023年以降も依然として猛威を振るっている状況
長期にわたり、PC端末やインターネットが利用できない事態も

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



２．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ポリシーの見直し

各自治体がDX推進と現状にあわせて情報セキュリティポリシーの改訂を現在検討中

「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」等の改定について

ガイドラインの位置づけ

地方公共団体における情報セキュリティは、各団体が保有する情報資産を守るにあたって自ら責任を持って確保するべきものであり、情報セキュリティポリシーは各団体が組織の実態に応じて策定するものである。
「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（以下「本ガイドライン」という。）」は、各団体が情報セキュリティポリシーを策定する際の参考となるよう情報セキュリティポリシーの考え方や内容を解説するとともに構成や例文を示したものである。

改定の背景

本件は、前回改定時（平成27年3月）以降の自治体情報セキュリティ対策検討チームの報告や「政府機関等の情報セキュリティ対策のための統一基準群」の改定等を踏まえて、今般、改定を実施するものである。

参考文献

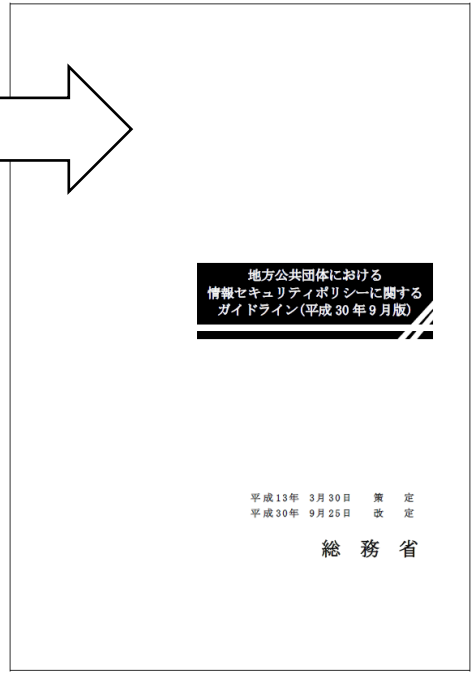
- 政府機関等の情報セキュリティ対策のための統一基準群（内閣官房内閣サイバーセキュリティセンター）
- 府省庁対策基準策定のためのガイドライン（内閣官房内閣サイバーセキュリティセンター）
- 新たな自治体情報セキュリティ対策の抜本的強化について～自治体情報セキュリティ対策検討チーム報告～（総務省）
- その他関係法令や通知など

検討組織

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に向けて、専門家へのヒアリング（平成30年2月、3月）及び検討会（平成30年8月）を実施。

主な改定内容

- 利活用しやすいように本ガイドラインを「総則」「例文」「解説」「付録」の4編構成に変更
- 自治体情報セキュリティ対策の抜本的強化にあたり、マイナンバー利用事務系、LGWAN接続系及びインターネット接続系において、情報システム全体の強靭性向上（強靭化）を講じることについて記載
- マイナンバー利用事務系ではパスワード認証、生体認証、スマートカード認証等から複数の認証を用いる多要素認証を実施しなければならないことについて記載
- 多要素認証において、認証情報を適切に管理し、認証情報の不正利用の防止をしなければならないことについて記載
- 情報セキュリティインシデントへの対処として、CSIRTの設置・役割について記載
- 本ガイドラインの改定内容を踏まえ「地方公共団体における情報セキュリティ監査に関するガイドライン」についても所要の改定を実施



①情報セキュリティとは？

情報の「機密性」「完全性」「可用性」を確保すること。

機密性	秘密情報が守られること ＝情報が「漏れない」	⇔	漏洩
完全性	情報の正しい状態を保持すること ＝情報の内容が「変わらない」	⇔	改竄
可用性	情報を必要なときに利用できること ＝利用が「止まらない」	⇔	中断

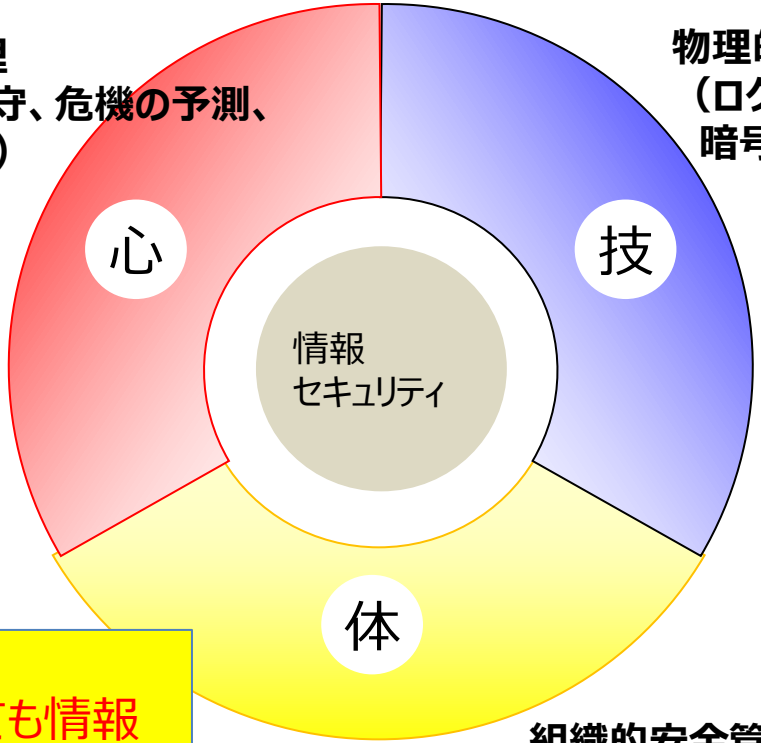
情報セキュリティリスク

これを維持・運用するのがISMS（Information Security Management Sysytem）：
ISO 27001およびそれと同等なJIS Q 27001に規定

②情報セキュリティ対策の三本柱（安全管理措置）

人的安全管理
（ルールの遵守、危機の予測、研修の実施）

物理的・技術的安全管理
（ログイン認証、暗号化、入退室管理）



組織的安全管理
（組織体制・ルールの整備）

安全管理措置の「心」「技」「体」全て欠けても情報漏えいにつながります

③業務別のネットワーク（三層分離）と情報セキュリティ対策

個人番号利用事務系（基幹系）

・基幹系システム（住民記録、税、福祉システム）の操作

内部情報事務系（情報系）

・行政機関に閉ざしたメール
・文書管理システム
・財務会計システム

インターネット系

・インターネットの閲覧
・インターネットメール（外部からのメール）

<昨今の事情>
① 厳格に分離した結果、インターネットやメールが利用しにくい環境に（αモデル）
② 昨今のクラウド上での有用なサービス利用の観点からインターネットの利用に重きを置くβ'モデルを利用する団体が増えている
③ インターネットにおいては全てを疑いセキュリテイ措置を行う**「ゼロトラスト」**を前提にする組織が増えている
④ コストはかかるが効率性は向上する

これまでの「インターネット系」環境で行う業務
①インターネットの閲覧
②インターネット経由で送られてきたメールの確認
③インターネット上の資料のダウンロード

④個人情報保護制度の変化

1. 改正個人情報保護法の施行（令和5年4月1日）により、地方公共団体等における個人情報等の取扱いに関する規律を法で規定することとなった。
2. これまで団体によって個人情報の定義や保護に関する措置、漏洩等の事故があった際の届出等の差異が解消された。
3. 個人情報保護委員会が公表している「個人情報の保護に関する法律についてのガイドライン　（行政機関等編）　」を参照してください。
   https://www.ppc.go.jp/files/pdf/230401_koutekibumon_guidelines.pdf
4. 地方公共団体等向け研修資料等も公開されています。
   https://www.ppc.go.jp/personalinfo/kensyuushiryou_gyousei/
5. 改正法の趣旨を理解されていますか？

皆様に業務遂行上セキュリティ面で常時意識していただきたいこと

1. 何がセキュリティ上の脅威なのか

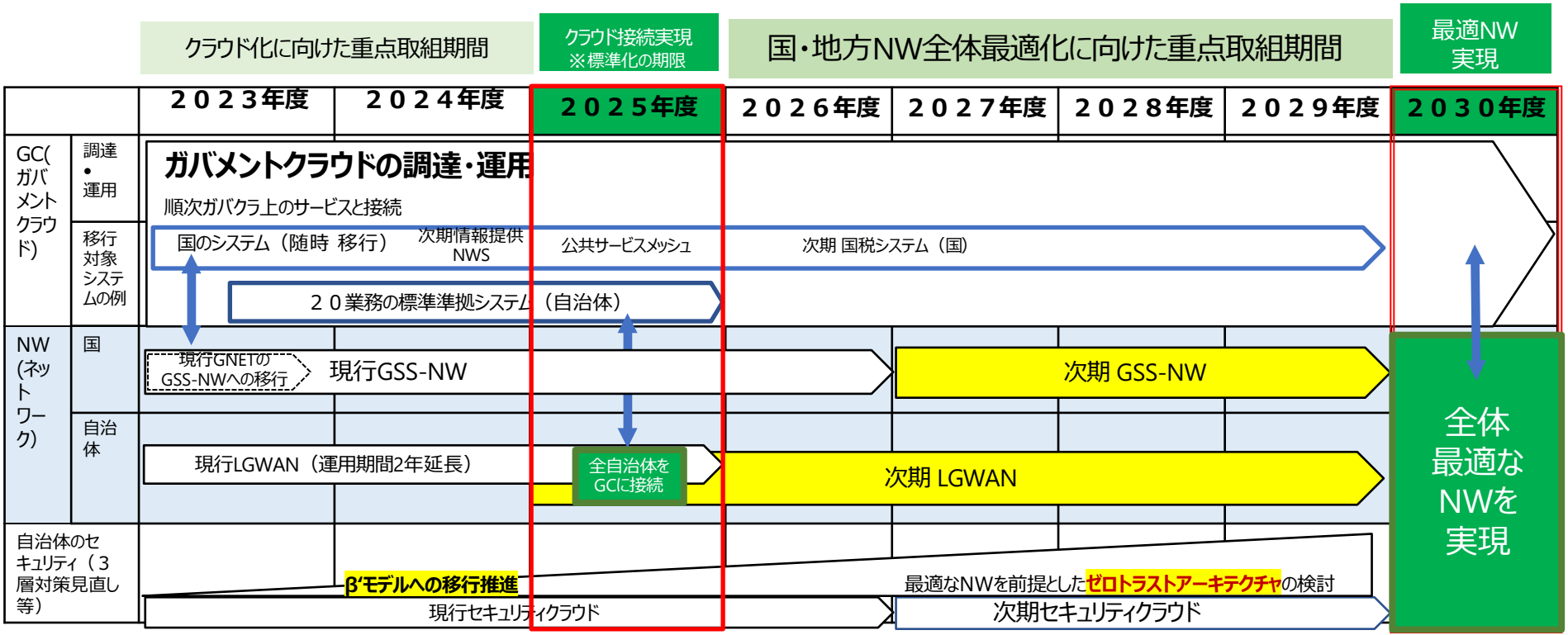
   情報の「機密性」「完全性」「可用性」を確保することへの影響は
   すべてセキュリティ上の脅威になる

2. 市民を守るには　　組織を守るには　　皆様を守るには
   どうしたら良いでしょうか

   ① 現状の確認‥例　誰が何をどう処理しているか？それは適切か？
   ② 日頃の執務状況の確認‥PCに向かって作業はしているけれど‥？
   ③ 管理職との対話
   ④ これらから課題の確認
   ⑤ 対応策の検討と決定、指示
   ⑥ 庁内・庁外等の情報共有と連携

３．ゼロトラストネットワークによるセキュリティ強靭化の方向性

全体最適の観点から望ましいネットワークの将来スケジュール（２０３０頃までに想定されるスケジュール）¥¥



出典：国・地方ネットワークの将来像及び実現シナリオに関する検討会（令和5年9月12日）

政府機関等のサイバーセキュリティ対策のための統一基準（令和５年度）の改定内容

- ✓ NISC政府統一基準にて、新たにゼロトラストアーキテクチャについて規定される。
- ✓ 最新の政府統一基準の内容を踏まえたセキュリティ対策の見直しを実施することが望ましい。

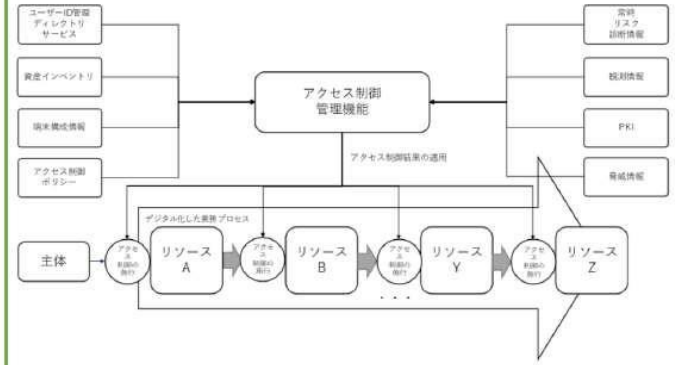
7.3 ゼロトラストアーキテクチャー（改定のポイント）

NISC

「7.3 ゼロトラストアーキテクチャ」

- 「ゼロトラストアーキテクチャ」は、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。
- 本節では、ゼロトラストアーキテクチャに基づく情報資産の保護策の１つであり、アクセス制御の仕組みを実現する機能の一部と考えられる動的アクセス制御（※）を実装する場合に特に必要となる対策事項を規定する。

※「動的なアクセス制御」とは、特定のアクセスに対して、セッションが確立してない操作ごとに、都度、アクセス元の信用情報を動的に評価し、アクセス先が信用できる状態であるかを検証したうえで、特定のリスクが検出された場合には追加の認証を求めることや、アクセスを拒否する等のアクセス制御を行うことを想定している。



ゼロトラストアーキテクチャ概念図
（出典）ゼロトラストアーキテクチャ適用方針（デジタル庁）

■改定のポイント

- 複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システムセキュリティ責任者を選任（7.3.1(1)）
- 動的なアクセス制御の導入方針を定めるにあたり、動的アクセス制御の対象とする情報システムと対象とする情報システムのリソース（ユーザーアカウント、機器等）を識別（7.3.1(2)）
- 動的なアクセス制御の実装にあたり、リソースの信頼情報の変化に応じた動的なアクセス制御のポリシーを作成し、動的なアクセス制御のポリシーに基づき、動的なアクセス制御を行う（7.3.1(3)）
- 動的なアクセス制御の運用に際し、アクセスパターンの変化に応じて、再度リスク評価を行い、動的なアクセス制御のポリシーを見直す。また、リソースの信頼情報の収集により検出されたリスクへ対処を行う。（7.3.2）

出典：地方公共団体のセキュリティ対策に係る国の動きと地方公共団体の状況について
（令和５年10月10日　総務省自治行政局　デジタル基盤推進室）

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 ※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。	・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

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

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。

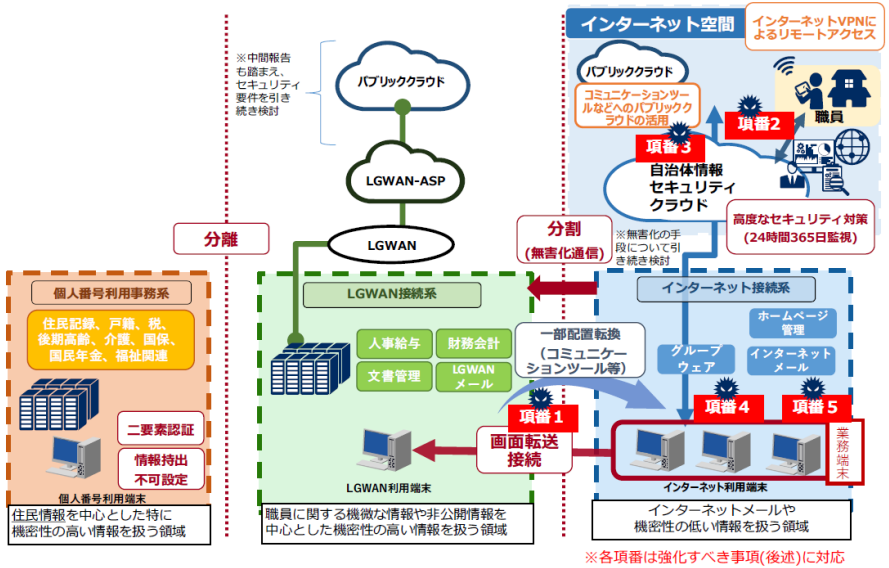
（注６）サニタイズ処理等を実現する手法は多岐にわたるため、適正な製品を選定し導入することが望ましい。

（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。

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

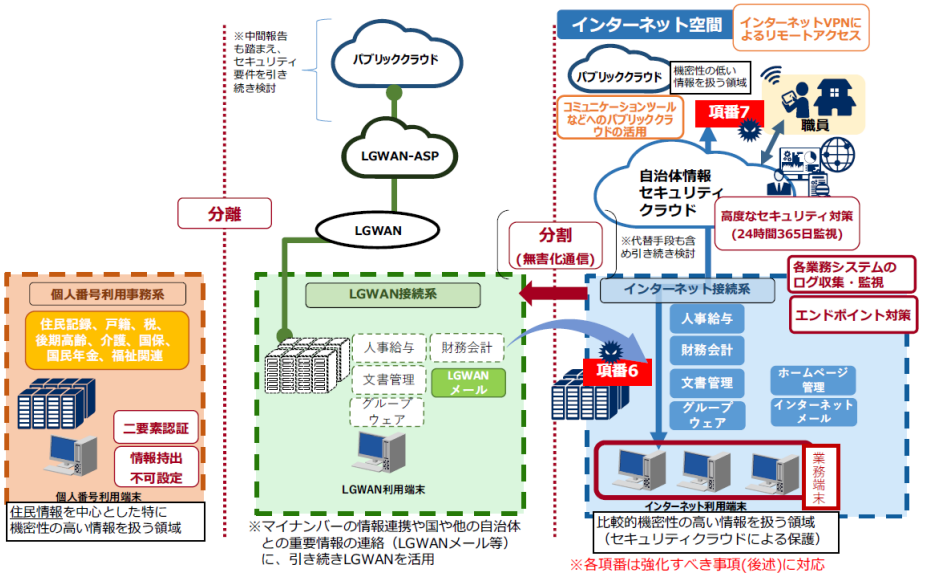
業務システムをLGWAN接続系に残しつつ、業務端末をインターネット接続系に移行し、画面転送によりLGWAN接続系業務システムを利用



- 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

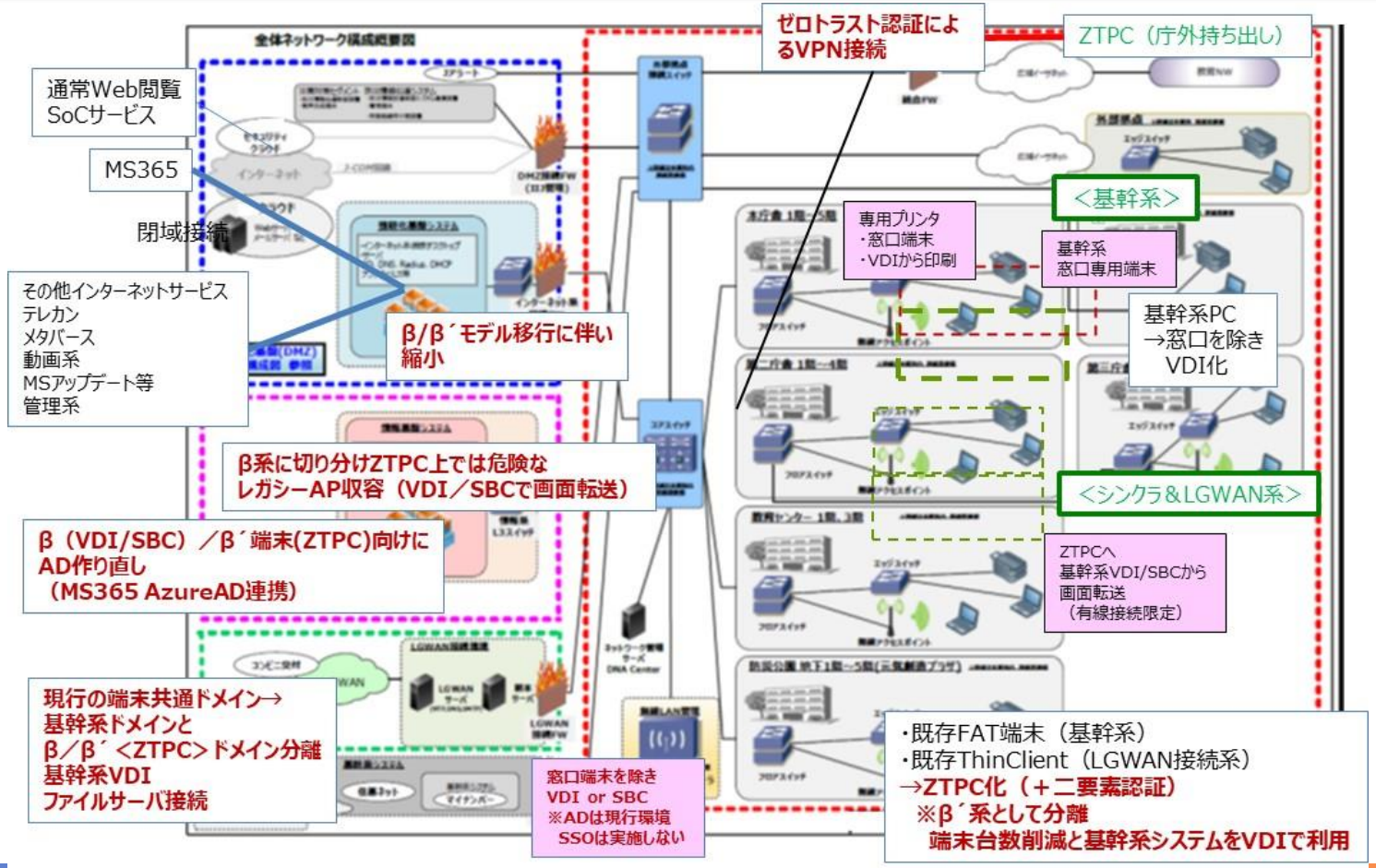
15

ゼロトラストPC要件

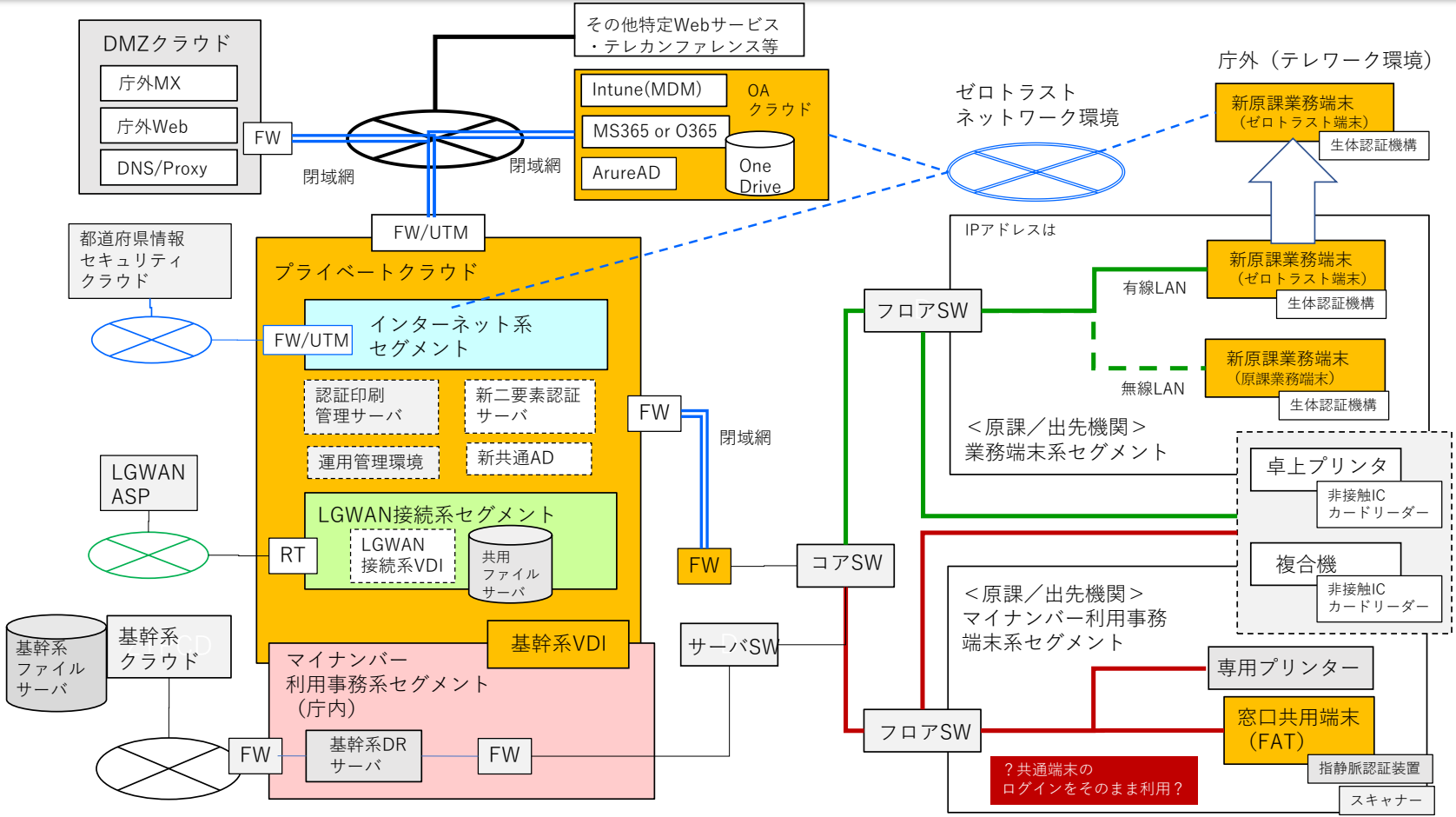
- 某省行政情報ネットワークシステムのクライアント調達仕様書（例）

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。

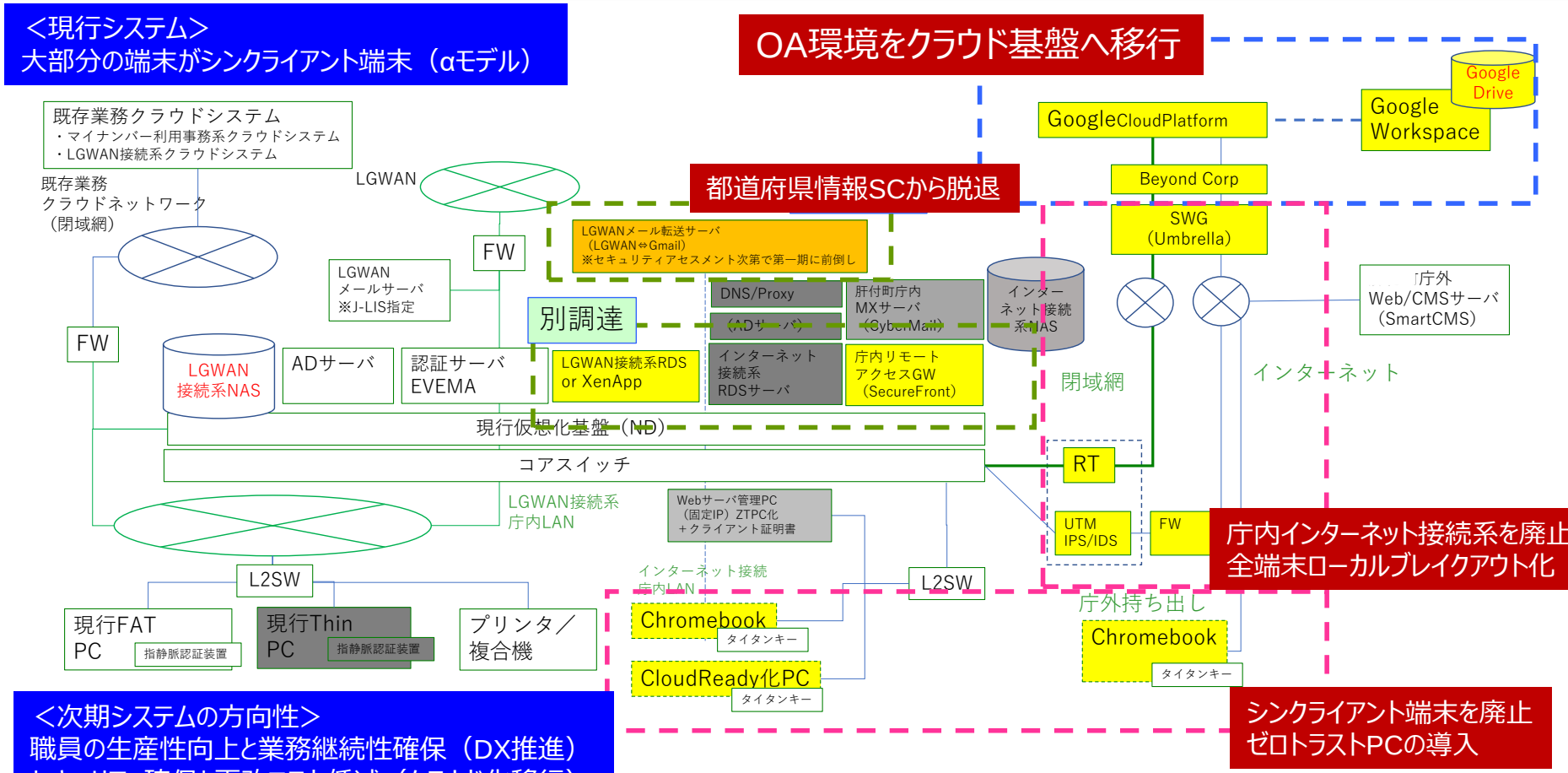
都内某自治体のβ´移行の方向性



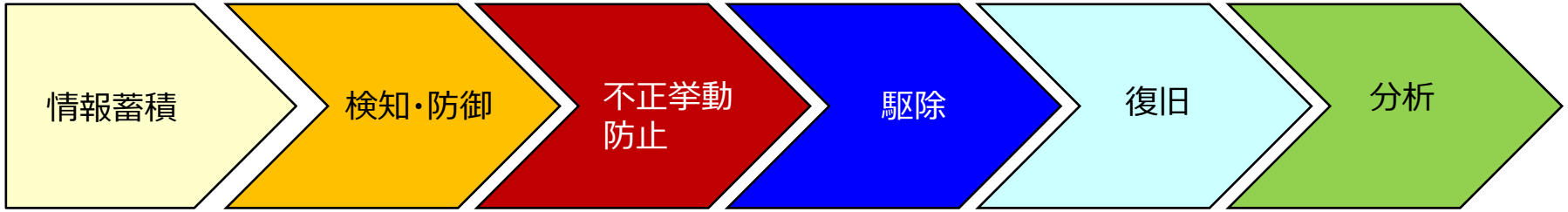
都内某自治体のβ´移行の方向性



都内某自治体のβ´移行の方向性



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

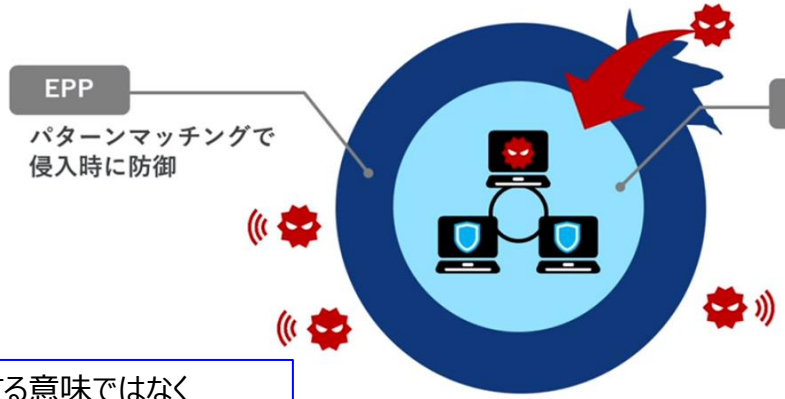
蓄積された情報外部から侵入しようとファイルを照合しマルウェア等を特定し侵入防止

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

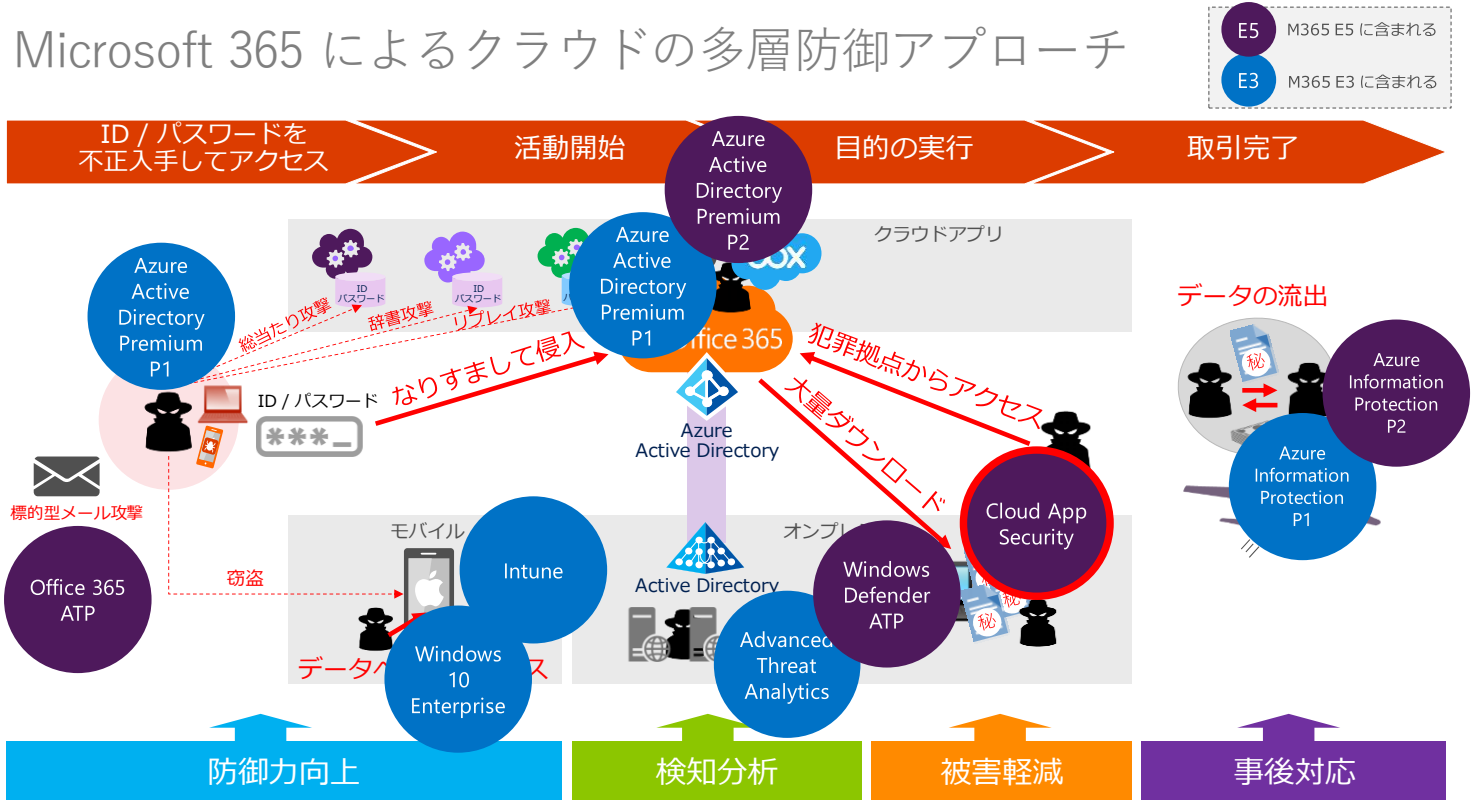
EDR
(Endpoint Detection and Responce)
不正な挙動を検知し、
感染後の対応を迅速に行うこと

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

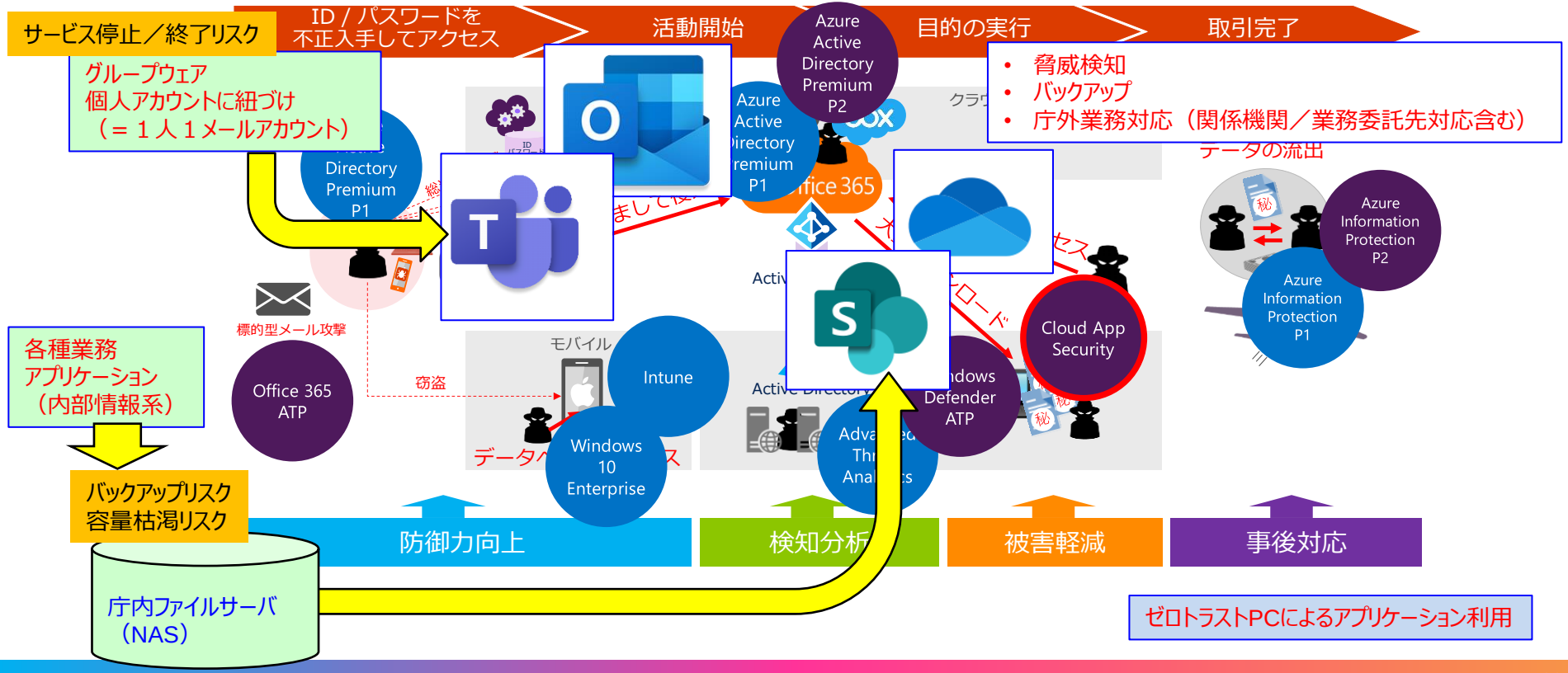


Offceを利用する限りでは十分なEDR環境を提供している

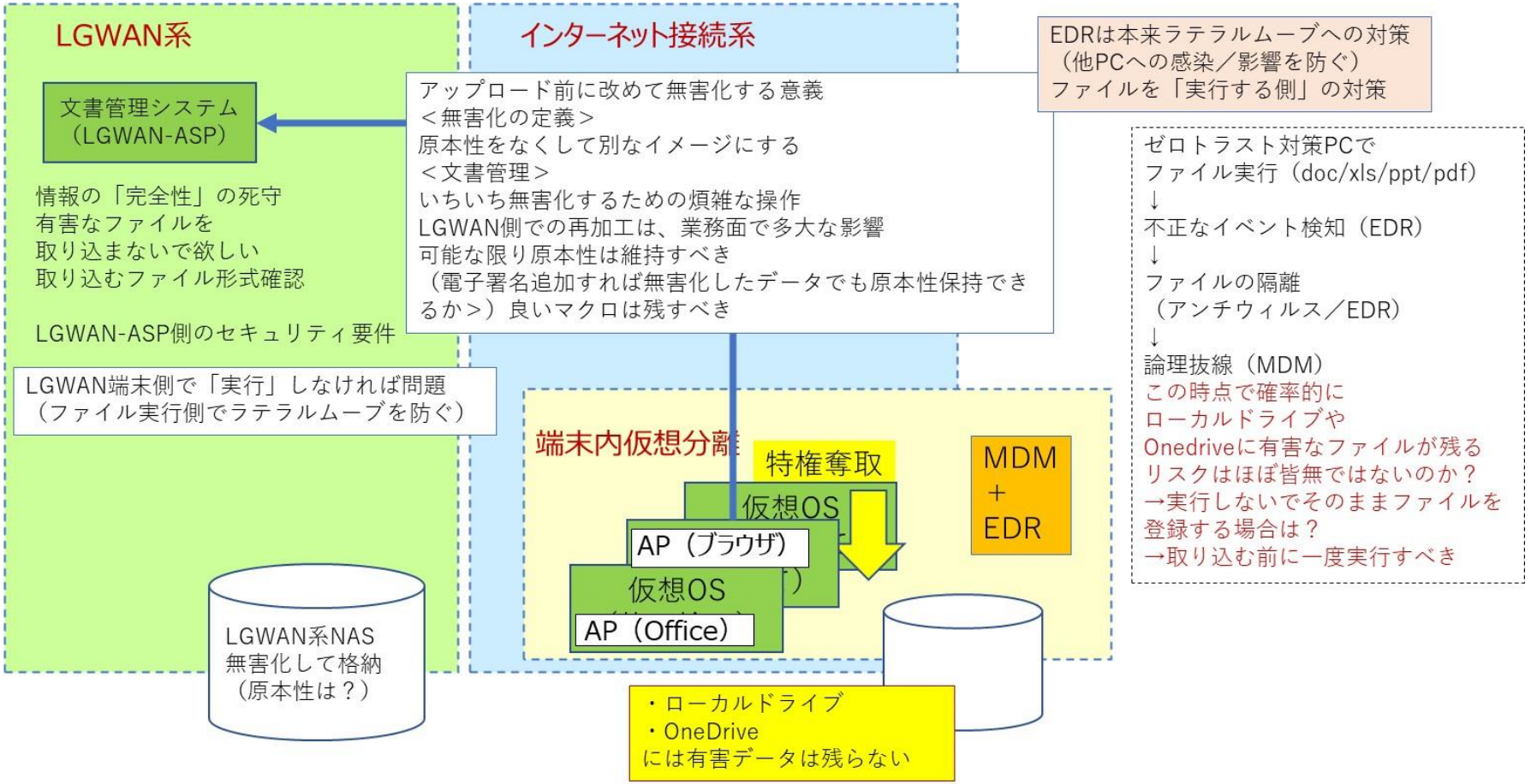
参考：庁内環境（ファイルサーバ／メール／グループウェア環境）のゼロトラストネットワーク環境への移行

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

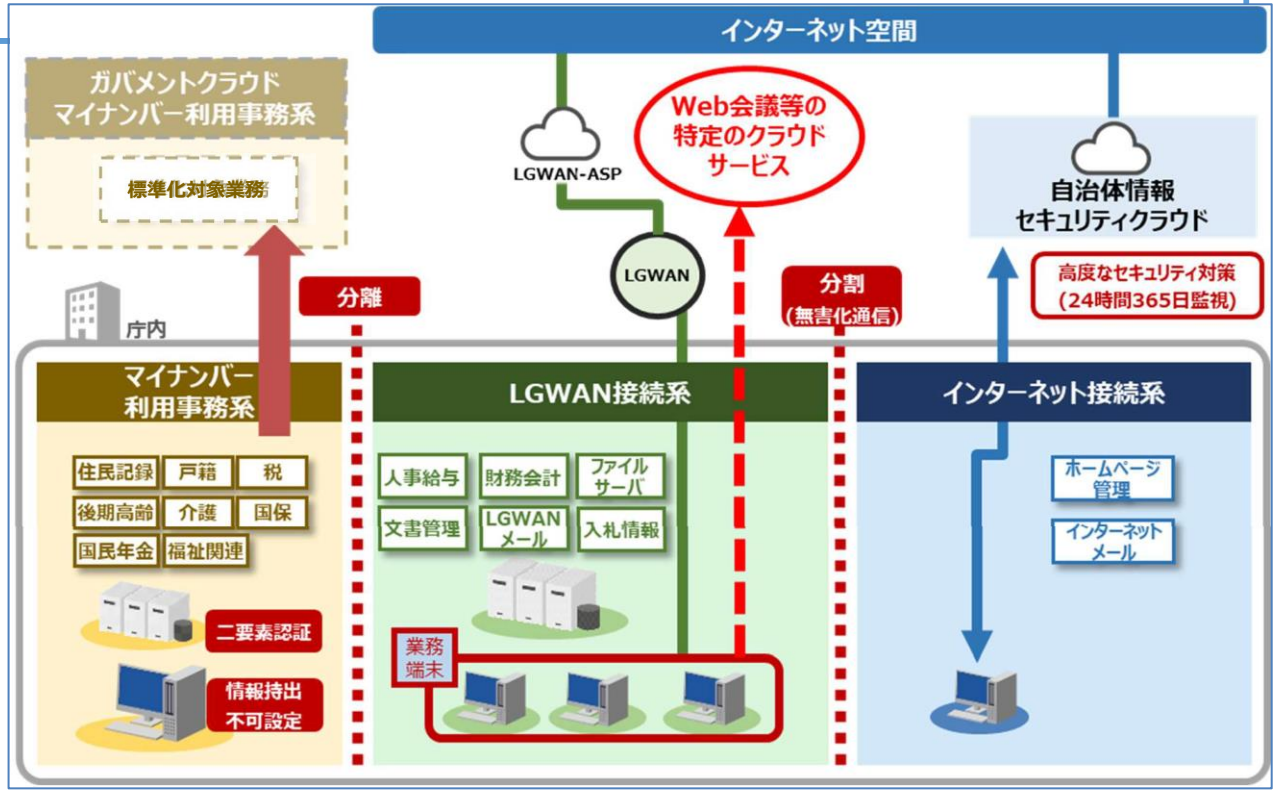


ゼロトラストセキュリティにおけるファイル「無害化」



α´モデルについて～LGWAN接続系からローカルブレイクアウト～

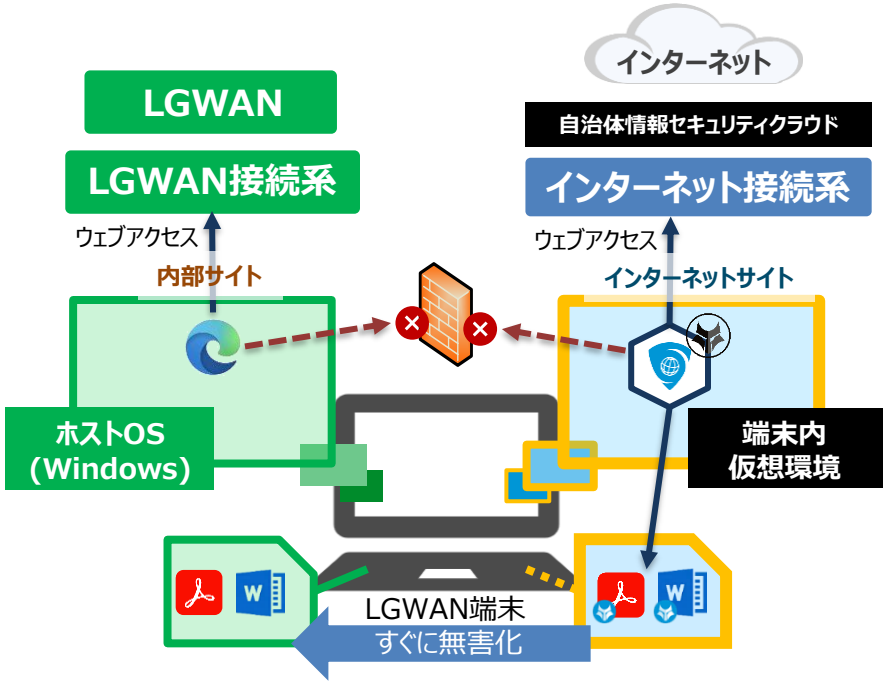
✓ 国はLGWAN接続系から外部のクラウドサービスに接続（ローカルブレイクアウト）するための、必要なセキュリティ対策をガイドライン上で規定する方向で検討中**<u>α'モデルについてもリスク評価を行い</u>**、評価結果を踏まえてガイドラインに必要なセキュリティ対策を規定することに。



出典：地方公共団体のセキュリティ対策に係る国の動きと地方公共団体の状況について
（令和５年10月10日　総務省自治行政局　デジタル基盤推進室）

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。

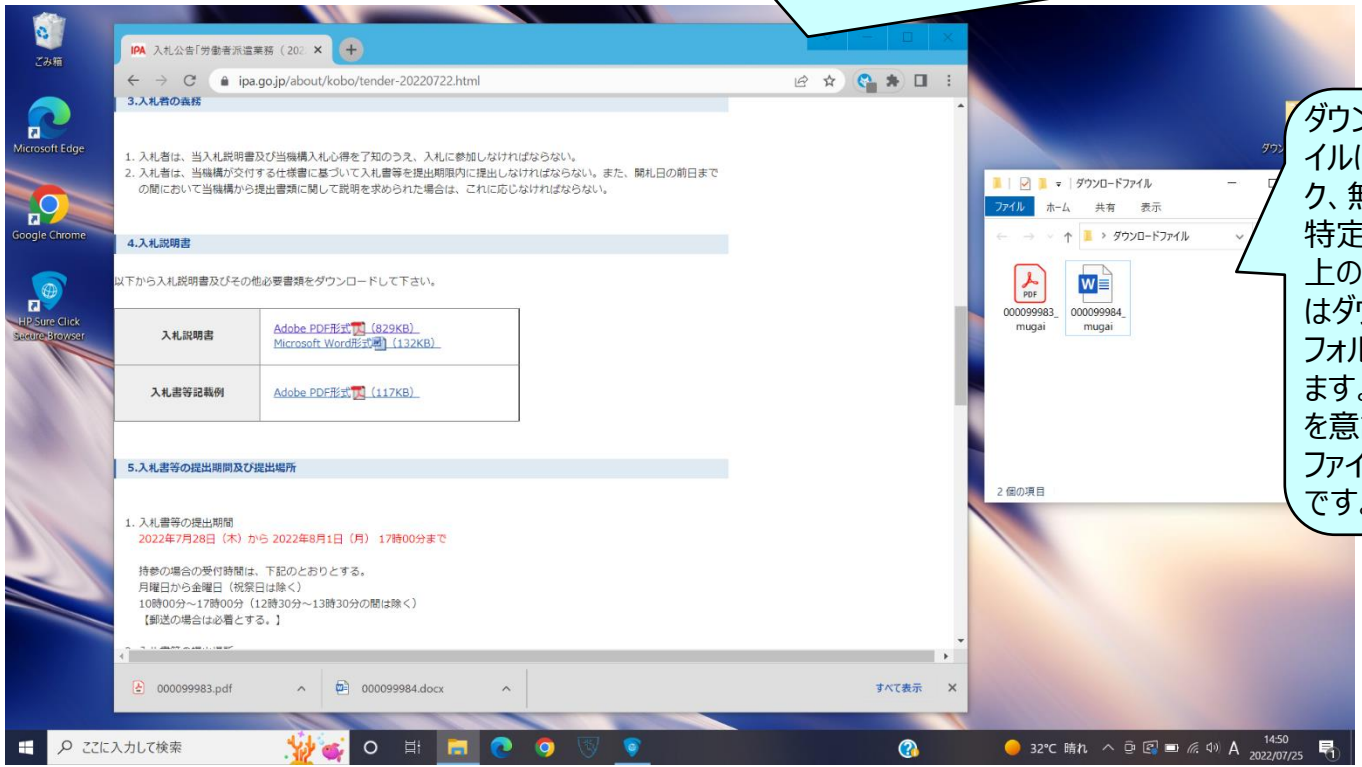
アルファモデルで利便性を向上させた那覇市様の事例　利用イメージ（ユーザの操作感）

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）

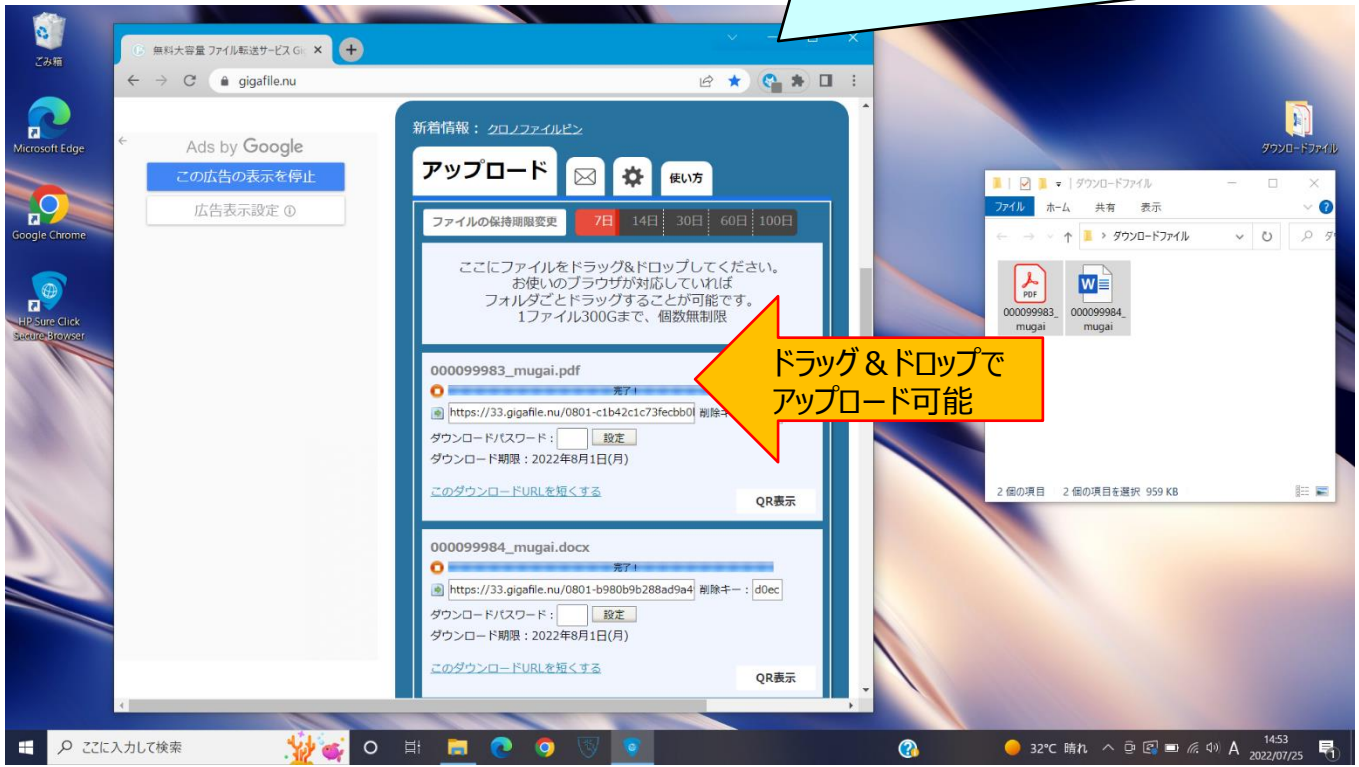
通常のブラウザと同じように、ダウンロードしたいファイルを指定します。ただし、保存先フォルダは指定できません。
ダウンロードしたファイルは、ウイルスチェック、無害化処理が自動で行われます。



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）

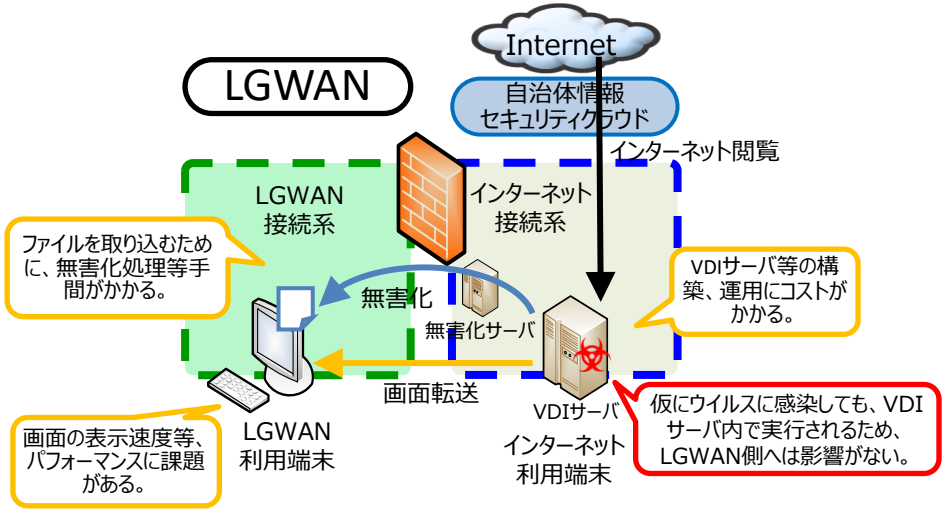
通常のブラウザと同じように、仮想ブラウザ経由でファイルアップロード（ドラッグ＆ドロップ、あるいは別ウィンドウでのファイル指定）が可能です(製品仕様)。ただし、そのままだと情報漏洩につながる恐れがあるため、アップロードを全面禁止する、あるいは、特定の職員のみ特定のURLへアップロードする、ような制御を検討しています。



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

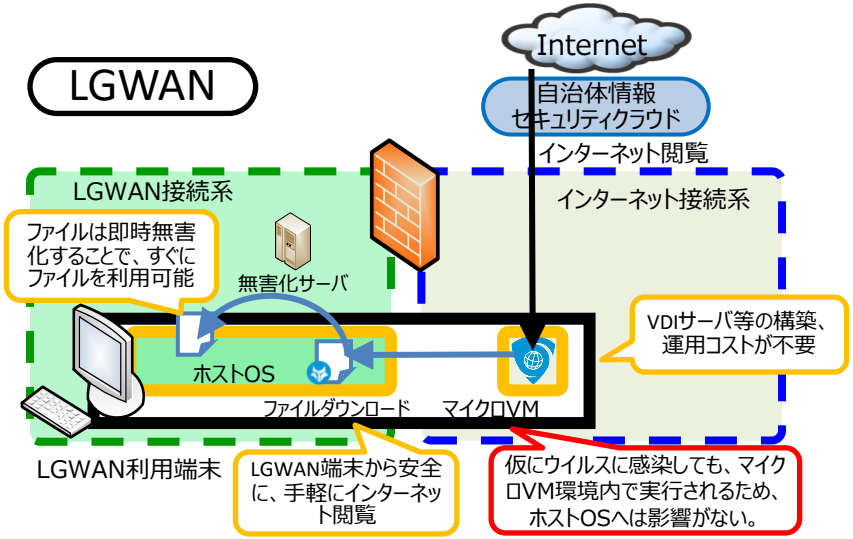
サーバ型仮想環境（VDIや仮想ブラウザサーバ）でインターネットにアクセスする場合、以下の課題が挙げられます。
・画面の表示速度等、パフォーマンスに課題がある。
・ファイルを取り込むために、無害化等手間がかかる。
・VDIサーバ等の同時接続数などの拡張性や、可用性を考慮する必要があり、設計、構築、運用にコストがかかる。



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