資料5

マイナンバー利用事務系に係る画面転送の方式について

総務省

令和７年●月●日

目 次

１．総論

はじめに

前　提

- **どのような対策を行ったとしても想定外の攻撃を受ける可能性はあるため、本リスク分析を踏まえた対策を実施しても100%リスクを回避をすることはできないことに留意すること。**（次ページのリスク分析結果全般を踏まえた留意事項も併せて参照）
- **マイナンバー利用事務系が、住民の個人情報を大量に保持するネットワーク系統であるところ、画面転送技術を利用し他のネットワーク系統との間の通信を通すことで、攻撃を受けるリスクが増大する点に留意すること。**
- **マイナンバー利用事務系において画面転送技術を利用する場合は、上記リスクを考慮し、自団体の幹部まで含め意思決定を行った上で、実装すること。**
- **各団体の状況に応じ、利便性とコスト、リスク、セキュリティ等を総合的に勘案して、本別紙で規定している画面転送の方式の採用について判断すること。**

技術的な留意点

- 画面転送の通信方式に標準化された方式はないため、通信方式は画面転送システムを提供するベンダの方式となるが、**通信の盗聴や改ざん防止のため、暗号通信を行うことを前提とする。**
  ※通信の暗号化は、「特定個人情報に関する安全管理措置（行政機関等編）」のF.技術的安全管理措置　d　漏えい等の防止 の実施のために必要な対策。
- **手元の端末がマルウェアに感染した場合、仮想環境上のマイナンバー利用事務系にまで被害が及ぶのを防ぐため、クリップボード、プリンタ、ディスクドライブ等の仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止する。**
  <例>
  - 仮想端末側で取得したファイルを画面転送で接続する手元の端末にファイルを引き渡すことができないよう制限し、逆方向の手元の端末のファイルを仮想端末側に引き渡すことができないよう制限する
  - 印刷するファイルを、仮想端末側から手元の端末にダウンロードし、手元の端末と接続するプリンタで印刷を行わないよう制限する。
- **画面転送システムの仮想機能（仮想端末、分離領域でのブラウザ等）は、利用後に仮想機能を第三者に悪用されることを防ぐため、手元の端末で仮想画面を閉じた際は、仮想機能もログオフする（手元端末から画面転送機能の利用終了時には、仮想機能も終了する）。**

※全パターンの対策の前提となる留意点であり、「全パターン共通の対策」として規定。

リスク分析結果全般を踏まえた留意事項

■ **攻撃シナリオ全体を評価する方法（事業被害ベースのリスク分析）では**、インターネット接続系とLGWAN接続系との間の分割ファイアウォールや、マイナンバー利用事務系とLGWAN接続系の間の分離ファイアウォール、CSPファイアウォール（DaaSとガバメントクラウドの間の通信経路、CSPを経由し庁舎のマイナンバー利用事務系に至る通信経路に構築するファイアウォール）で、**適切なアクセス制御が行われ、インターネット接続系からマイナンバー利用事務系への通信が画面転送に必要なもの以外は遮断される前提で、リスク値を算出**。

⇒ **全パターンにおいて、全項目のリスク値が３以下であり、「安全」と判断**

■ 他方、**個々の情報資産のリスク値を算出する方法（資産ベースのリスク分析）では、以下の①②について、悪意のあるWebにアクセスし、未知のマルウェアに感染するリスクがゼロにならない**場合がある。

① **インターネットに直接接続する端末**

インターネット接続系に端末を統合(一台化）する場合のインターネット接続系端末のみならず、LGWAN接続系に端末を統合（一台化）するが、一部の端末がインターネット接続系に残存する（＝**インターネットに直接接続する端末が残存する**）場合も、当該端末を踏み台にされ、LGWAN接続系やマイナンバー利用事務系が攻撃されるリスクがある。

② 端末内の分離された領域で動作する**セキュアブラウザ**

⇒ **一部の項目について、リスク値が６（脅威レベル×脆弱性レベルが３×2=6)**

✓ **端末を一台化するのであれば、LGWAN接続系に端末を統合する方式を採用すること。**

✓ **LGWAN接続系に端末を統合する過程でインターネット接続系に端末が残存する場合や、インターネット接続系への端末統合、セキュアブラウザの利用については、端末やセキュアブラウザが踏み台にされ、攻撃される重大なリスクがあることを認識した上で、首長まで含め意思決定を行い実装すること。**

✓ **上記の場合、脆弱性を突かれないようにセキュリティパッチを適用すること（※１）、マルウェア感染のリスクを前提とした、異常な挙動の端末を監視・検出・特定する対策（※２）を講じること、サイバー攻撃を受けた時の対応を訓練等を通じて把握しておくこと（※３）が一層重要になる。**

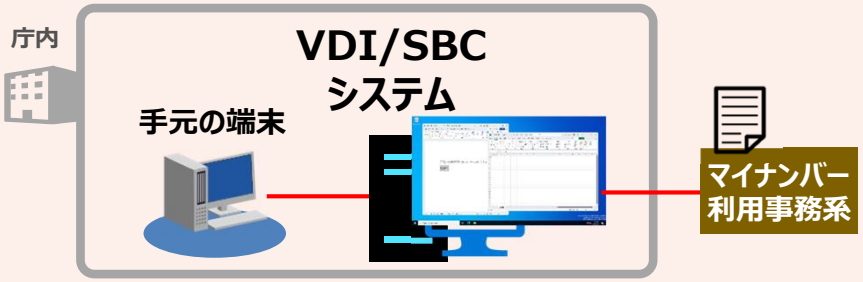
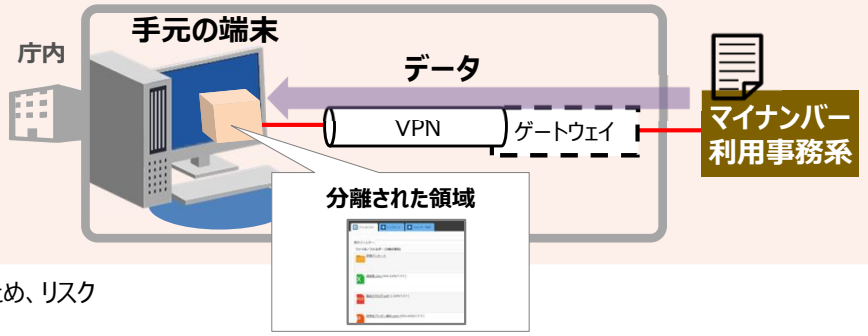
※１　仮想端末含め、各種機器にパッチを適用することを全パターンにおいて必須対策として規定。機器のパッチが未適用であったために正規職員になりすまされて情報が持ち出された事例も存在。（第16回検討会　資料２を参照）
※２　「未知の不正プログラム対策」として、全パターンにおいて必須対策として規定。
※３　「組織・人的な対応」として全パターンにおいて必須対策として規定。

注）　今回リスク分析を実施していないマイナンバー利用事務系の端末への端末統合（一台化）については、上記の他にもリスクが存在する可能性があることに留意すること。

端末仮想化の方式

✓ マイナンバー利用事務系の業務を、仮想化された環境で実施する場合、以下の方式が考えられる。

端末仮想化の各方式

方式	概要	
DaaS （Desktop as a Service）	仮想デスクトップ環境をクラウドサービスとして提供すること ガバメントクラウドのCSPにおいて、DaaSを提供している事業者も存在する	
オンプレミス仮想デスクトップ※	VDI（Virtual Desktop Infrastructure） サーバOS上でユーザ数分の仮想デスクトップを構築し、業務端末から利用する SBC（Server Based Computing） サーバOS上でマルチユーザーに対応した仮想環境を構築し、複数台の端末で共有する	
セキュアブラウザ	手元の端末に専用ブラウザをインストールすることで隔離された領域を確保し、専用ゲートウェイを介して、その領域内でWeb上のドキュメントやデータを表示することで、セキュアにWeb閲覧を行う ※サーバOS上のブラウザをセッション単位に仮想化する方式もある	

※VDIとSBCの違いは、主にOS上で仮想デスクトップを作成する単位（ユーザ数分作成かマルチユーザか）であるため、リスク評価上は同じ方式として扱う。

2．リスク分析の結果を踏まえた対策

全パターン共通の対策

組織的・人的対策

組織的・人的対策	対策の定義		「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
手続・規定	クラウドサービス(DaaS)を利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底しなければならない。		C.組織的安全管理措置　b 取扱規程等に基づく運用の実施のための対策	○
組織・人的な対応	職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定	職員等は、実践的サイバー防御演習（CYDER）などのセキュリティ研修やサイバー攻撃を受けた時の対応訓練を年1回以上受講する。	D.人的安全管理措置　b 事務取扱担当者等の教育　の実施のための対策	○
	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			
	情報セキュリティポリシーの見直し	情報セキュリティの監査及び自己点検の結果並びに内部及び外部の環境の変化から、定期的又は必要に応じて情報セキュリティポリシーを見直す。	B.取扱規程等の見直し等　に関連	○
事務取扱担当者の明確化	特定個人情報等を取り扱う職員（以下「事務取扱担当者」という。）をリスト化し、マイナンバー利用事務系への画面転送システムの利用を許可する者を明確化する。		安全管理措置の検討手順のうち、以下を実施するための対策 A 個人番号を取り扱う事務の範囲の明確化 C 事務取扱担当者の明確化	○
監査	定期的及び必要に応じ随時に監査（外部監査及び他部署等による点検を含む。）を行い、その結果を総括責任者に報告する。		C. 組織的安全管理措置　e 取扱状況の把握及び安全管理措置の見直し　の実施のための対策	○

物理的対策

物理的対策	対策の定義			「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
特定個人情報等を取り扱う区域の管理	事務取扱担当者の端末の保護	• 事務取扱担当者の端末は執務エリア（特定個人情報を取り扱う事務を行う区域であり、支所を含む）から原則持ち出しをしない運用ルールの徹底（注１） • 事務取扱担当者の端末にはのぞき見防止フィルターを装着する運用ルールの徹底		Ｅ.物理的安全管理措置　a　特定個人情報等を取り扱う区域の管理、b　機器及び電子媒体等の盗難等の防止　の実施のための対策	○
	入退室管理	事務取扱担当者と他部門の分離	事務取扱担当者（特定個人情報等を取り扱う職員）の庁内の執務エリア（部署単位）をまとめ、執務室を分ける、パーティションの設置等、特定個人情報が他部門に見えないよう分離する。	Ｅ.物理的安全管理措置　a　特定個人情報等を取り扱う区域の管理　の実施のための対策	○
	情報システム室等の管理	機器の物理的な保護	• 画面転送システム及び画面転送システムや無線LANにアクセス時の認証システム等を施錠やクラウドサービスなどの管理区域に設置し、第３者からの物理的アクセスからの保護 • 無線LAN APを手が届かない場所に設置し、第３者からの物理的アクセスからの保護	Ｅ.物理的安全管理措置　a　特定個人情報等を取り扱う区域の管理　の実施のための対策	○
		特権ID（注２）の管理	• 画面転送システムの特権IDを適正に管理	Ｅ.物理的安全管理措置　a　特定個人情報等を取り扱う区域の管理　の実施のための対策	○
電子媒体等の取扱いにおける漏えい等の防止	現行のガイドラインにおいて規定してあるように、原則、USBメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定する。（注１）			Ｅ.物理的安全管理措置　c　電子媒体等の取扱いにおける漏えい等の防止　の実施のための対策	○

注１）特定個人情報を取り扱う事務取扱担当者の端末を、執務エリアから原則持ち出しをしない運用や、原則、USBメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定する運用については、特定個人情報を扱う政府機関等や個人情報保護委員会の施策の動向を踏まえ、今後検討する余地がある。

注２）「特権ID 」とは、サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常のIDよりもシステムに対するより高いレベルでの操作が可能なIDをいう。

保守端末の対策

✓ 保守端末の対策は以下のとおりであり、業務委託により保守を実施する場合は、契約において対策の実施を担保する必要がある。

技術的対策	対策の定義	必須
接続先制限	保守端末の管理先以外へのインターネット接続を制限する。	○
マルウェア対策ソフト	パターンマッチング方式やヒューリスティック方式（不審な動作を行うコードが含まれていることを検出する振る舞い検知方式）などによる不正プログラム対策を行う。	○
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	○
多要素によるユーザ認証	保守担当者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	○
アクセスログ	管理先へのアクセスに係るログを記録する。	○
操作ログ	保守作業の操作ログを記録する。	○

技術的対策以外	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
監査	監査（外部監査又は内部監査）により、適正に保守業務が行われているか確認し、問題があれば是正する。		○
特定個人情報等を取り扱う区域の管理（情報システム室等の管理 ）	• 特権IDを用いたシステムの運用保守は業務端末とは分けた専用の保守端末で実施 • 保守端末を適正に管理	Ｅ.物理的安全管理措置　a 特定個人情報等を取り扱う区域の管理　の実施のための対策	○

その他

✓ 通信経路や仮想環境の運用に関する対策を以下のとおり示す。

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
通信経路に係る対策			
通信経路の暗号化	通信の盗聴や改ざん防止のため、画面転送に係る全ての通信経路で暗号化を行う（DaaS、VDI、セキュアブラウザ等の仮想環境を提供するサービスについて、通信経路を暗号化するものを選択する。） 通信経路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。 無線LANを通信に利用する場合は、WPA2又はWPA3といった強度の高い暗号を使用する。	F.技術的安全管理措置　d 漏えい等の防止 の実施のために必要な対策。	○
仮想環境の運用に関する対策			
デバイス、リソースの双方向における利用の禁止	手元の端末がマルウェアに感染した場合、仮想環境上のマイナンバー利用事務系にまで被害が及ぶのを防ぐため、クリップボード、プリンタ、ディスクドライブ等の仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止することとし、プリンタやスキャナを利用する場合は、仮想端末から、手元の端末を介さず、ネットワークを介して接続することとする。 ただし、キーボード、マウスやユーザ認証用のICカードリーダ、生体認証用の機器など、仮想端末そのものの操作に必要なデバイスを、手元の端末に接続して利用することは可能。 ＜例＞ • 仮想端末側で取得したファイルを画面転送で接続する手元の端末にファイルを引き渡すことができないよう制限し、逆方向の手元の端末のファイルを仮想端末側に引き渡すことができないよう制限する。 • 印刷するファイルを、仮想端末側から手元の端末にダウンロードし、手元の端末と接続するプリンタで印刷を行わないよう制限する。		○
仮想機能のログオフ	画面転送システムの仮想機能（仮想端末、分離領域でのブラウザ等）は、利用後に仮想機能を第3者に悪用されることを防ぐため、手元の端末で仮想画面を閉じた際は、仮想機能もログオフする（手元端末から画面転送機能の利用終了時には、仮想機能も終了する）。		○

自治体情報セキュリティクラウドに係る留意点

自治体情報セキュリティクラウドへの影響について

■ **インターネット接続系に端末を統合（一台化）し、画面転送の方式としてDaaSを利用する場合（通信経路（３）～（４）‘）**、DaaS経由のLGWAN接続系、マイナンバー利用事務系へのhttps通信や画面転送の通信が自治体情報セキュリティクラウドを通ることになり、**自治体情報セキュリティクラウドを通る通信量（トラフィック）が増加する。**

■ 画面転送の通信に係る通信量がどの程度増加するかはDaaSのシステムにより異なるが、**自治体情報セキュリティクラウドのランニングコストが増加する可能性がある**。

✓ **DaaS利用の検討時には、通信量を事前にDaaS提供事業者に確認し、自治体情報セキュリティクラウドの通信量への影響を予測する必要がある。**

✓ **自治体情報セキュリティクラウドの運用主体である都道府県にも、通信量やランニングコストへの影響から、必ず確認すること。**

✓ **自治体情報セキュリティクラウドに影響がある場合は、ガイドラインに沿ってローカルブレイクアウトの実施などを検討する必要がある。**

各パターンにおける対策

※各パターンの対策の表において、「全パターン共通の対策」等で掲げられているものについては灰色で着色。

通信経路パターン

✓ 接続要件の検討にあたっては、利用形態としてDaaSも想定し、下記の通り10パターンの通信経路についてリスク分析を実施。

	接続元 (業務端末の設置場所)	画面転送の方式	ページ
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする	P16
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする	P25
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合	P34
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する	P42
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合	P52
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する	P61
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする	P72
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）	P78
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする	P86
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ	P93

通信経路（1） LGWAN接続系端末に１台化　DaaS利用
リスク分析結果を踏まえた技術的対策

- マイナンバー利用事務系への影響　P18
- 対策群のイメージ図　　P19
- 対策群
  - 今回のリスク分析を踏まえた対策　P20・21
  - 前提となるα’モデルの対策　P23・24

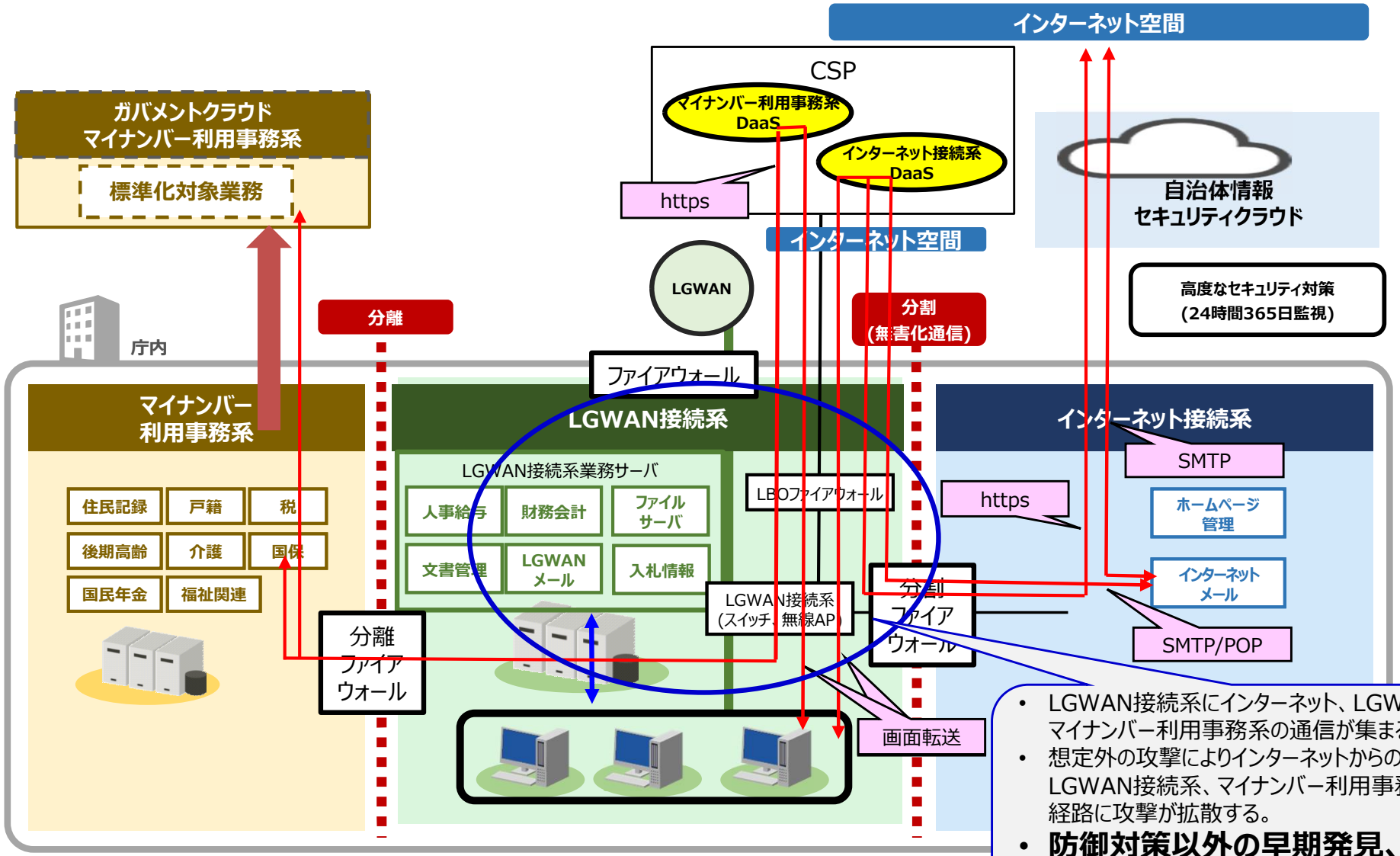
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**LGWAN接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系、マイナンバー利用事務系に影響が及ぶ**。

✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**

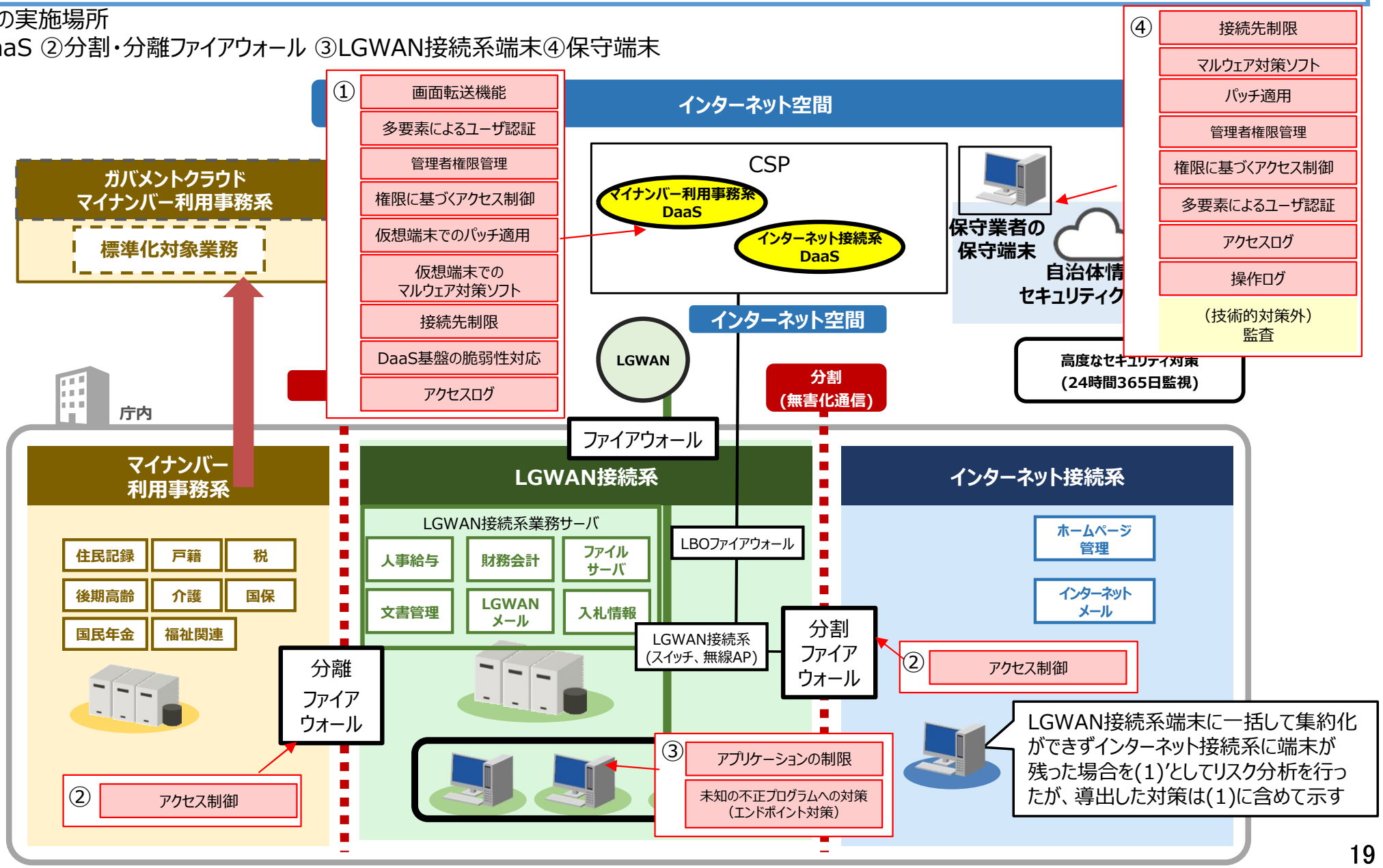


- LGWAN接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まる。
- 想定外の攻撃によりインターネットからの侵入を許すと、LGWAN接続系、マイナンバー利用事務系への接続経路に攻撃が拡散する。
- **防御対策以外の早期発見、早期対応も必要である。**

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用(異なるCSP) の対策イメージ

- ✓ α'モデルの対策を実施した上でLGWAN接続系からDaaSに接続する方式。
- ✓ リスクアセスメント結果を踏まえると、**α'モデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
①DaaS ②分割・分離ファイアウォール ③LGWAN接続系端末④保守端末



通信経路 (1)LGWAN接続系端末に１台化　DaaS利用(異なるCSP) の技術的対策①

✓LGWAN接続系端末からDaaS利用でのリスクアセスメントの結果を踏まえ必要な対策を示す。
※以下の対策の前に、α'モデルの対策を実施することが前提であることに留意。

(1) 利用するクラウドサービス（α'モデルと同じ考え方）
・ISMAPに登録されているクラウドサービスのDaaS

(2) 技術的対策（次項に続く）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス(DaaS)上での対策			
画面転送機能	仮想端末を画面転送するという分離対策により、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
多要素によるユーザ認証	DaaSのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a アクセス制御、b アクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a アクセス制御　の実施のための対策	○
仮想端末でのパッチ適用	仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
仮想端末でのマルウェア対策ソフト	仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。		○
接続先制限	LGWAN接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
DaaS基盤の脆弱性対応	DaaS基盤の脆弱性にパッチを適用する。**DaaS事業者の責任範囲となるため、DaaS事業者選定時の前提条件となる。**	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
アクセスログ	不正アクセス等による被害の防止等のため、DaaSのアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e 取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用(異なるCSP) の技術的対策②

(2) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
LGWAN接続系での対策（α'モデルの対策以外のもの）				
アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	接続元（インターネット接続系DaaS）と接続先（インターネット、インターネット接続系のメールサーバ）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、LGWAN接続系端末でのスクリーンショット機能を停止する。（注）			○
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。（パッチ適用、マルウェア対策ソフトの導入についてはα'モデルにおける必須対策として規定）

スクリーンショット機能の停止の目的と対策について

✓スクリーンショット機能は、画面転送に接続する手元の端末にて、マイナンバー、個人情報の画面を不正に取得され、漏えいすることを防止するために停止することが望ましい。
✓ただし、マルウェアによる攻撃の実例を鑑みると、ショートカットキーを利用せずにスクリーンショットを取得しているため、**パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的**であると考えられる。

- 故意によるスクリーンショットの取得の防止
  - 端末単位における**ショートカットキーの無効化により画面キャプチャを抑止**する。

画面キャプチャのショートカットキーは以下のとおり。

・[Windows キー] + [Shift] + [S]
・[PrtScr]
・[Alt] + [PrtScr]
・[Shift] + [PrtScr]
・[Windows キー] + [PrtScr]

注）ショートカットキーや実行ファイルを無効化しても、スマートフォン等による画面撮影により故意に情報を漏えいすることが可能であることに留意する。

  - 端末単位における**実行ファイル (exe ファイル)の無効化により画面キャプチャを抑止**する。
    例：「Snipping Tool」アプリの起動を制限する。

- マルウェアによるスクリーンショットの取得の防止
  - 以下のマルウェアの侵入防御、及び侵入時はマルウェアの動作を検知し防御する。

※1 **・パッチ適用**
・マルウェア対策ソフトの導入
＋
※2 **未知の不正プログラムへの対策（エンドポイント対策）**

参考）スクリーンショットを取得するマルウェアの例
2022年 マルウェア Screenshotter：exeファイルを実行して、デスクトップのスクリーンショットをキャプチャ
2021年 マルウェア Snake：OSの関数を実行して、デスクトップのスクリーンショットをキャプチャ

※1 α'モデルにおいて必須対策として規定　※2 β･β'モデルにおいて必須対策として規定

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用時(異なるCSP) の前提条件となる α'モデルの対策 ①

✓ 通信経路(1)の対策の前提となる、α'モデルの対策を示す（ガイドラインに既に規定）。
✓ DaaSに接続する際に講じる必要のある対策であり、接続先のDaaSは、α'モデルに沿ってISMAP登録サービスから選定する。

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス上での対策			
マルウェア対策	DaaSの仮想端末でマルウェア検査、不正ソフトウェア対策を行う。		○
LGWAN接続系での対策			
通信相手の証明書による認証	通信相手が本物であるか否か、正当性を確認する。		○
マルウェア対策ソフト	マルウェアを検知・除去する。パターンマッチング方式、不審な動作を行うコードが含まれていることを検出するヒューリスティック方式を行う。LGWAN接続系端末、LGWAN接続系業務サーバにて対応が必要。	F.技術的安全管理措置　c 不正アクセス等による被害の防止等 の実施のための対策	○
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。LGWAN接続系端末、LGWAN接続系業務サーバ、分離・分割ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。	F.技術的安全管理措置　c 不正アクセス等による被害の防止等 の実施のための対策	○
接続先制限	LGWAN接続系から外部へのアクセス先を**利用するDaaSのみに限定**する。	F.技術的安全管理措置　a アクセス制御の実施のための対策	○
LBO テナント（**自団体の領域**）へのアクセス制御	利用するクラウドサービスへのアクセスを自団体の領域のみに制限する。	F.技術的安全管理措置　a アクセス制御の実施のための対策	○
メール無害化/ファイル無害化	受信したメールの本文のテキスト化、インターネットメールの添付ファイルやインターネットからダウンロードしたファイルの無害化をする。DaaSの画面転送においては、DaaSの仮想端末の機能により代替とする。		○
権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限及び関連する属性に応じて適切に管理する。LGWAN接続系端末、LGWAN接続系業務サーバ、ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。		○
アクセス制御	不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う。LGWAN接続系端末、LGWAN接続系業務サーバ、分離・分割ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。	F.技術的安全管理措置　a アクセス制御の実施のための対策	○

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用時(異なるCSP) の前提条件となる α'モデルの対策 ②

(前項からの続き)

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
LGWAN接続系での対策				
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策			○
IDS/IPS	ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。		○	
DDoS 対策	DDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS 対策機器の導入やDDoS 対策サービスの利用によって、高負荷攻撃への耐性を向上する。負荷分散装置（「ロードバランサ」）による耐性向上を含む。			○
冗長化	LBOファイアウォールに対する攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。			○
通信路暗号化	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。	F.技術的安全管理措置　d　漏えい等の防止　の実施のための対策	○	

注）未知の不正プログラムへの対策（エンドポイント対策）はα'モデルでは推奨であるが、**想定外の攻撃や、脆弱性へのゼロデイ攻撃に対処するためには、未知の不正プログラムへの対策（エンドポイント対策）を導入し、侵入の早期発見、早期の対応を行うことが重要であるため、「α'モデルの対策以外のLGWAN接続系での対策」に必須対策として規定**する。

通信経路（２） LGWAN接続系端末に１台化　DaaS利用
リスク分析結果を踏まえた技術的対策

- マイナンバー利用事務系への影響　P27
- 対策群のイメージ図　　P28
- 対策群
  - 今回のリスク分析を踏まえた対策　P29～31
  - 前提となるα’モデルの対策　P32・33

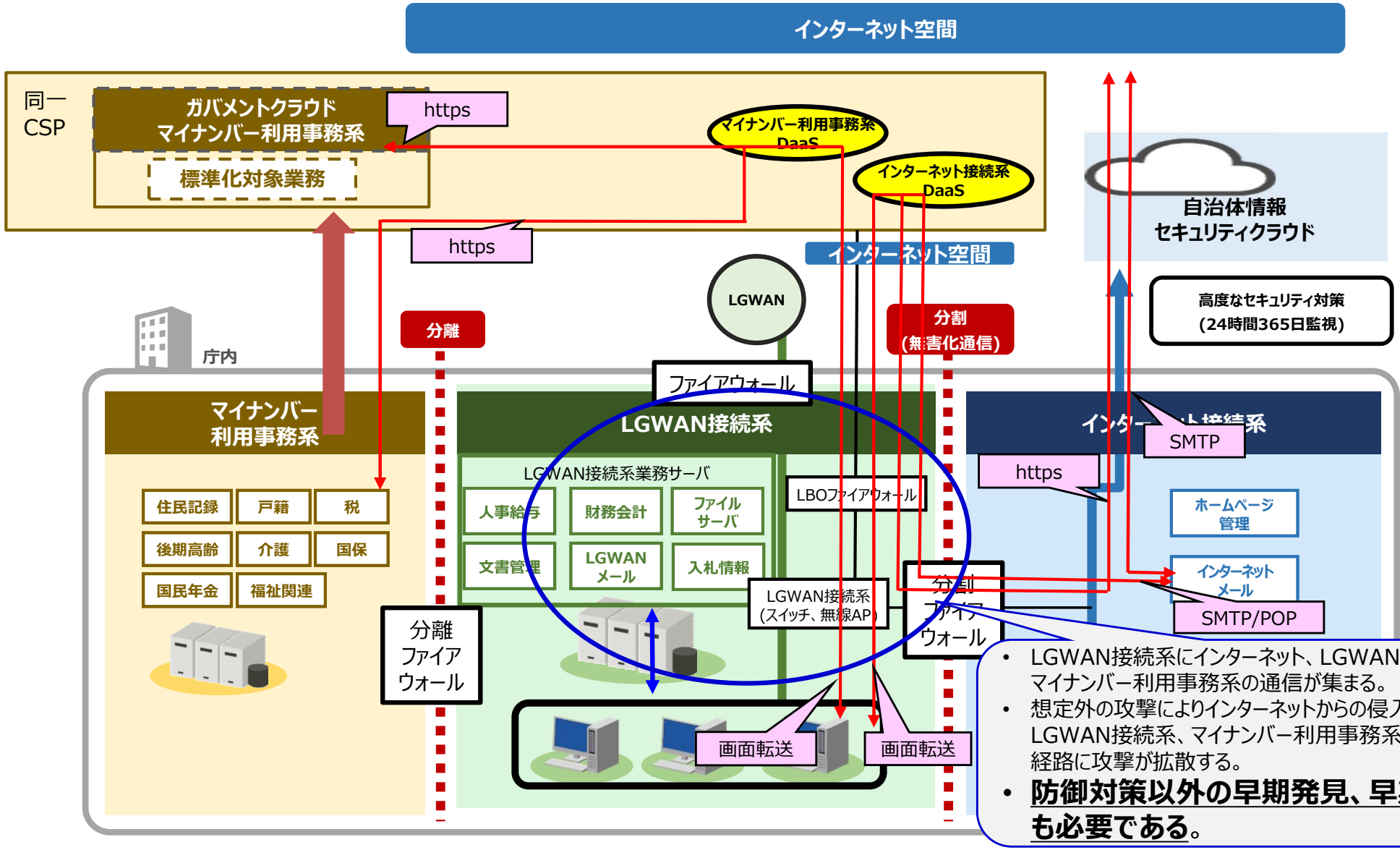
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**LGWAN接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系のみならずマイナンバー利用事務系に影響が及ぶ**可能性がある。

✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**

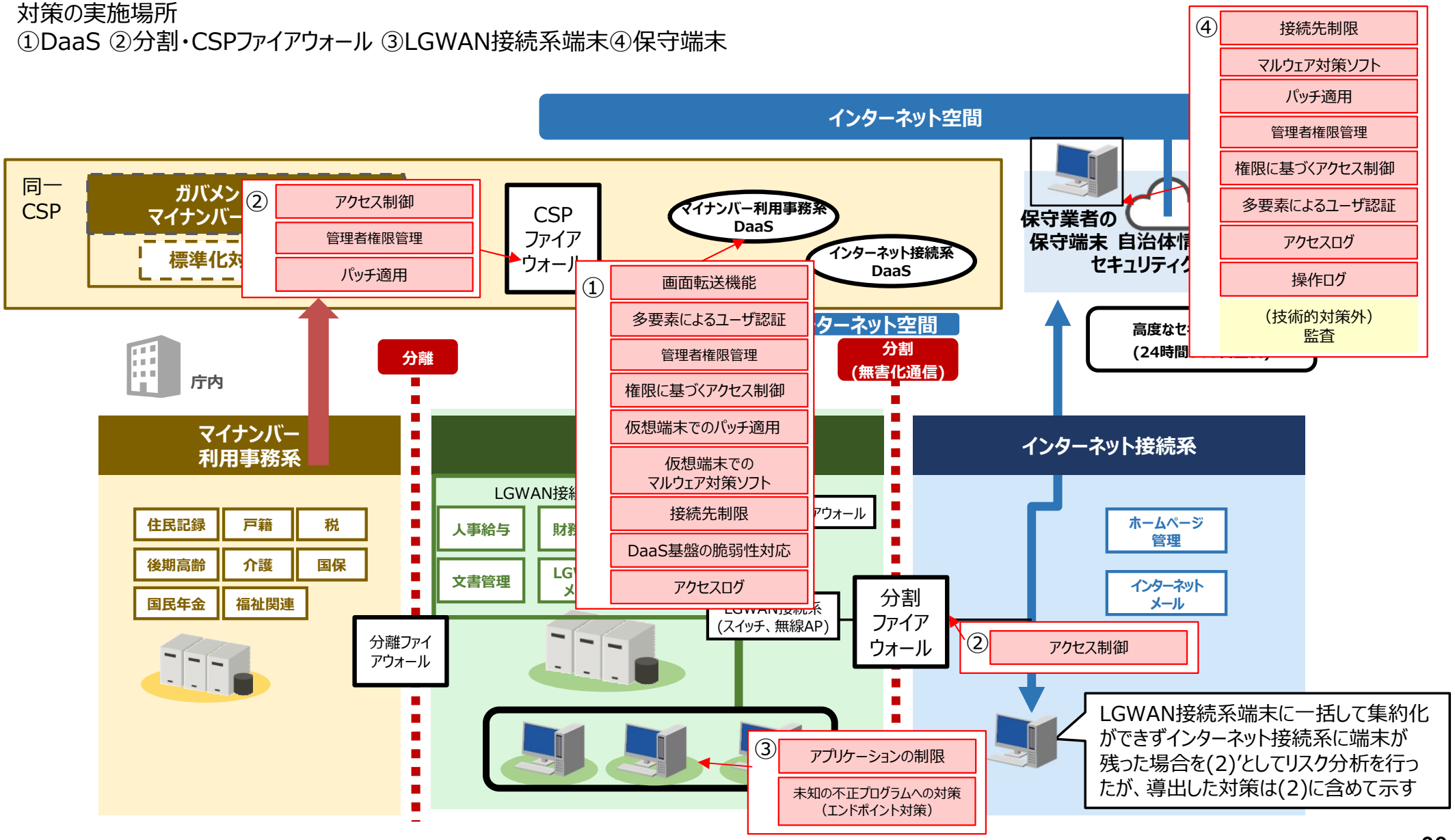


- LGWAN接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まる。
- 想定外の攻撃によりインターネットからの侵入を許すと、LGWAN接続系、マイナンバー利用事務系への接続経路に攻撃が拡散する。
- **防御対策以外の早期発見、早期対応も必要である。**

通信経路 (2)LGWAN接続系端末に１台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の対策イメージ

- ✓ α'モデルの対策を実施した上でLGWAN接続系からDaaSに接続する方式。
- ✓ リスクアセスメント結果を踏まえると、**α'モデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
①DaaS ②分割・CSPファイアウォール ③LGWAN接続系端末④保守端末



通信経路 (2)LGWAN接続系端末に１台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の技術的対策①

✓LGWAN接続系端末からDaaS利用でのリスクアセスメントの結果を踏まえ必要な対策を示す。
※以下の対策の前に、α'モデルの対策を実施することが前提であることに留意。

(1) 利用するクラウドサービス（※α'モデルと同じ考え方）
・ISMAPに登録されているクラウドサービスのDaaS

(2) 技術的対策（次項に続く）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス(DaaS)上での対策			
画面転送機能	仮想端末を画面転送するという分離対策により、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
多要素によるユーザ認証	DaaSのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a アクセス制御、b アクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a アクセス制御　の実施のための対策	○
仮想端末でのパッチ適用	仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
仮想端末でのマルウェア対策ソフト	仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。		○
接続先制限	LGWAN接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等の実施のための対策	○
DaaS基盤の脆弱性対応	DaaS基盤の脆弱性にパッチを適用する。**DaaS事業者の責任範囲となるため、DaaS事業者選定時の前提条件となる。**	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
アクセスログ	不正アクセス等による被害の防止等のため、DaaSのアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e 取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○

通信経路 (2)LGWAN接続系端末に１台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の技術的対策②

(2) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
クラウドサービス（CSP）上での対策				
アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するためにユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。CSPファイアウォールにて対応が必要。		○	
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。CSPファイアウォールにて対応が必要。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
LGWAN接続系での対策（α'モデルの対策以外のもの）				
アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	接続元（インターネット接続系DaaS）と接続先（インターネット、インターネット接続系のメールサーバ）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、LGWAN接続系端末でのスクリーンショット機能を停止する。注）			○

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。（パッチ適用、マルウェア対策ソフトの導入についてはα'モデルにおける必須対策として規定）
スクリーンショット機能の停止の詳細は、P22を参照のこと

通信経路 (2)LGWAN接続系端末に１台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の技術的対策③

(2) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
LGWAN接続系での対策（α'モデルの対策以外のもの）				
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。（パッチ適用、マルウェア対策ソフトの導入についてはα'モデルにおける必須対策として規定）

通信経路 (2)LGWAN接続系端末に１台化 DaaS利用ガバメントクラウド/DaaS(同一CSP) 時の前提条件となるα'モデルの対策 ①

✓ 通信経路(2)の対策の前提となる、α'モデルの対策を示す（ガイドラインに既に規定）。
✓ DaaSに接続する際に講じる必要のある対策であり、接続先のDaaSは、α'モデルに沿ってISMAP登録サービスから選定する。

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス上での対策			
マルウェア対策	DaaSの仮想端末でマルウェア検査、不正ソフトウェア対策を行う。		○
LGWAN接続系での対策			
通信相手の証明書による認証	通信相手が本物であるか否か、正当性を確認する。		○
マルウェア対策ソフト	マルウェアを検知・除去する。パターンマッチング方式、不審な動作を行うコードが含まれていることを検出するヒューリスティック方式を行う。LGWAN接続系端末、LGWAN接続系業務サーバにて対応が必要。		○
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。LGWAN接続系端末、LGWAN接続系業務サーバ、分離・分割ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。	F.技術的安全管理措置　c 不正アクセス等による被害の防止等　の実施のための対策	○
接続先制限	LGWAN接続系から外部へのアクセス先を**利用するDaaSのみに限定**する。	F.技術的安全管理措置　a アクセス制御の実施のための対策	○
LBO テナント（**自団体の領域**）へのアクセス制御	利用するクラウドサービスへのアクセスを自団体の領域のみに制限する。	F.技術的安全管理措置　a アクセス制御　の実施のための対策	○
メール無害化/ファイル無害化	受信したメールの本文のテキスト化、インターネットメールの添付ファイルやインターネットからダウンロードしたファイルの無害化をする。DaaSの画面転送においては、DaaSの仮想端末の機能により代替とする。		○
権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限及び関連する属性に応じて適切に管理する。LGWAN接続系端末、LGWAN接続系業務サーバ、ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。		○
アクセス制御	不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う。LGWAN接続系端末、LGWAN接続系業務サーバ、分離・分割ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。	F.技術的安全管理措置　a アクセス制御の実施のための対策	○

通信経路 (2)LGWAN接続系端末に１台化 DaaS利用ガバメントクラウド/DaaS(同一CSP) 時の前提条件となるα'モデルの対策 ②

（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
LGWAN接続系での対策				
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策			○
IDS/IPS	ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。		○	
DDoS 対策	DDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS 対策機器の導入やDDoS 対策サービスの利用によって、高負荷攻撃への耐性を向上する。負荷分散装置（「ロードバランサ」）による耐性向上を含む。			○
冗長化	LBOファイアウォールに対する攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。			○
通信路暗号化	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。	F.技術的安全管理措置 d 漏えい等の防止 の実施のための対策	○	

注）未知の不正プログラムへの対策（エンドポイント対策）はα'モデルでは推奨であるが、**想定外の攻撃や、脆弱性へのゼロデイ攻撃に対処するためには、未知の不正プログラムへの対策（エンドポイント対策）を導入し、侵入の早期発見、早期の対応を行うことが重要であるため、「α'モデルの対策以外のLGWAN接続系での対策」に必須対策として規定**する。

通信経路（３)インターネット接続系端末に１台化　DaaS利用（異なるCSP)
リスク分析結果より　必要な技術的対策

- マイナンバー利用事務系への影響　P36
- 対策群のイメージ図　　P37
- 対策群
  - 今回のリスク分析を踏まえた対策　P38・39
  - 前提となるβモデルの対策　P40・41

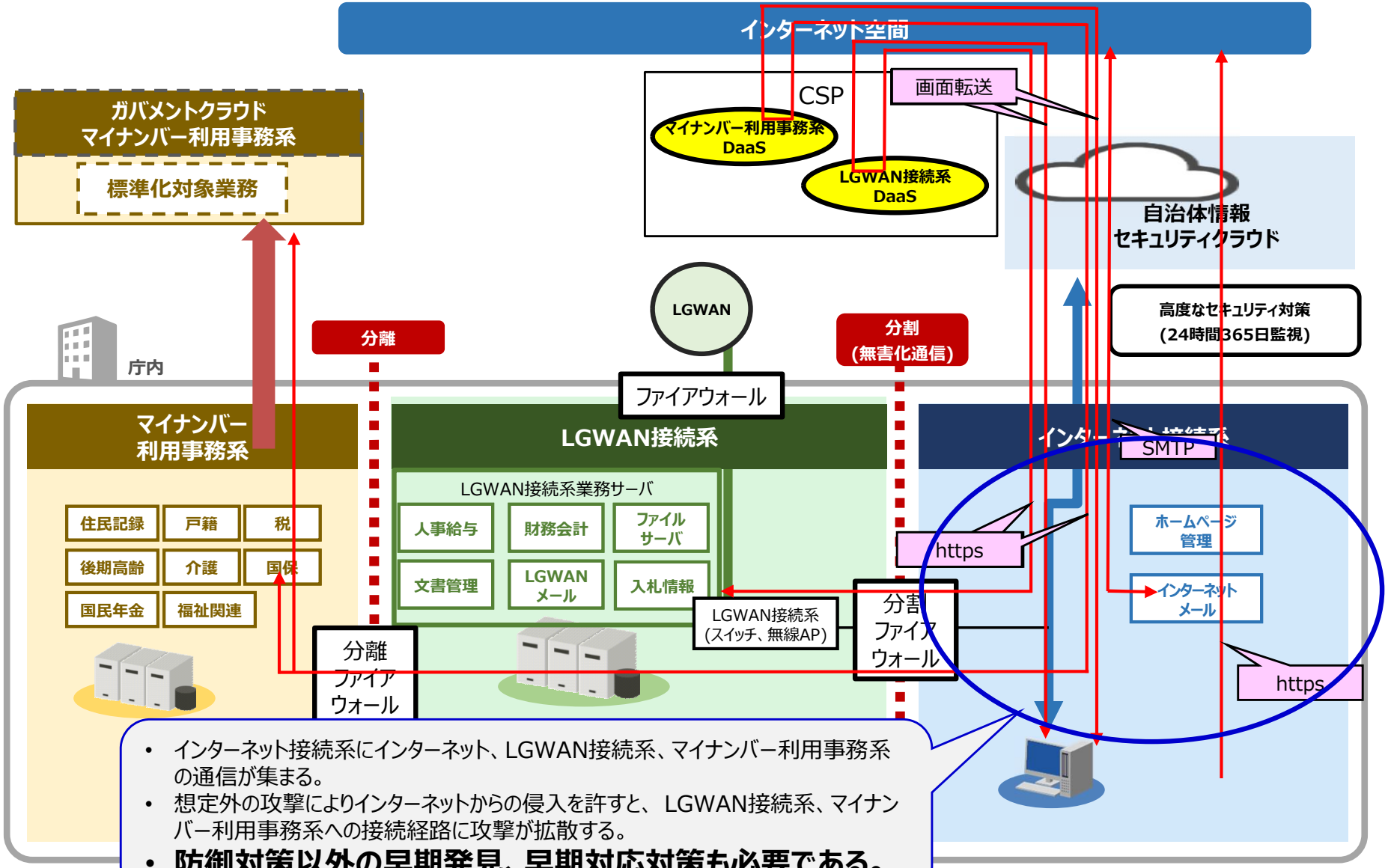
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系のみならずマイナンバー利用事務系に影響が及ぶ**可能性がある。

✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**

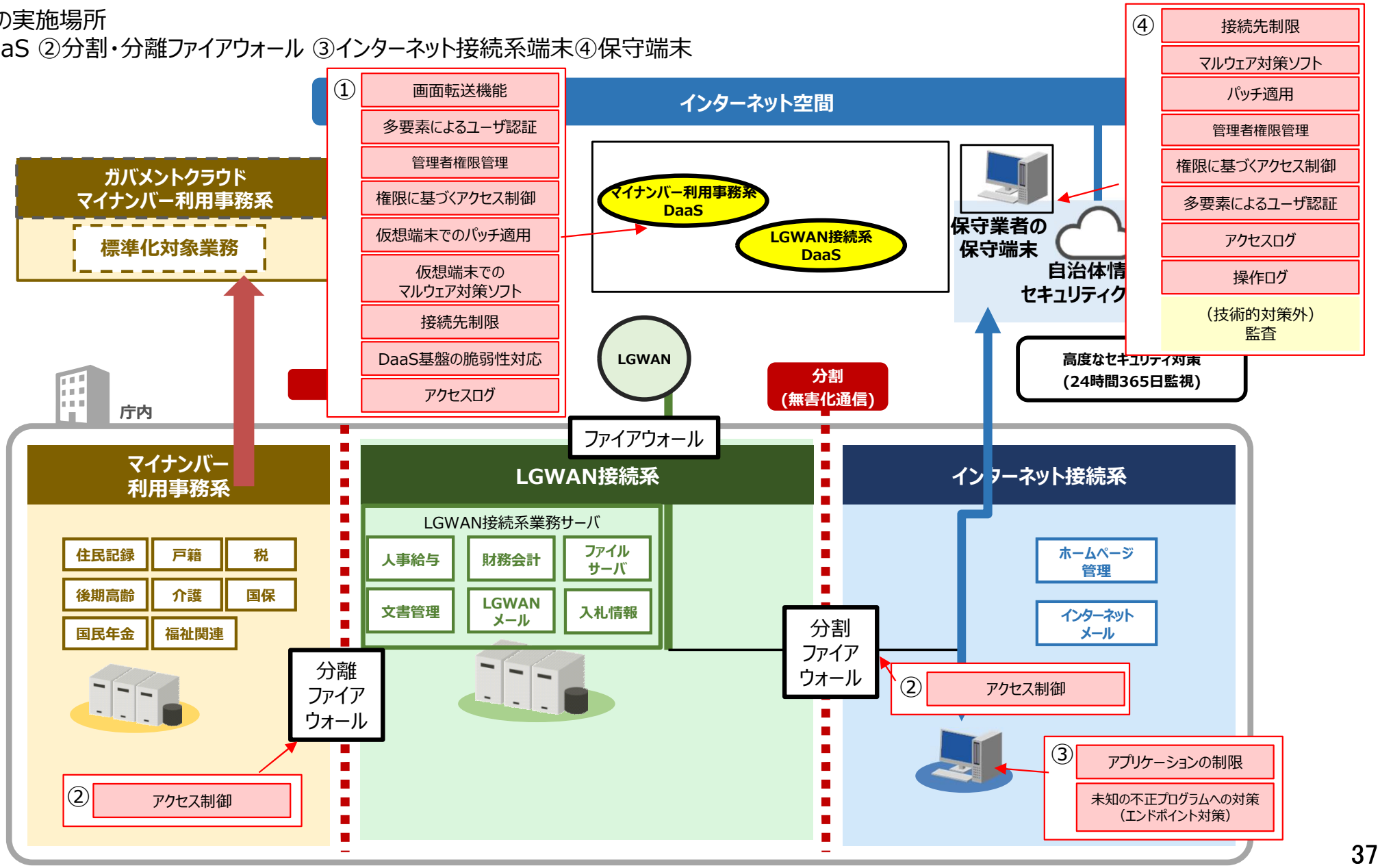


- インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まる。
- 想定外の攻撃によりインターネットからの侵入を許すと、 LGWAN接続系、マイナンバー利用事務系への接続経路に攻撃が拡散する。
- **防御対策以外の早期発見、早期対応対策も必要である。**

通信経路 (3)インターネット接続系端末に１台化　DaaS利用の対策(異なるCSP)の対策イメージ

- ✓ βモデルの対策を実施した上でインターネット接続系からDaaSに接続する方式。
- ✓ リスクアセスメント結果を踏まえると、**βモデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
①DaaS ②分割・分離ファイアウォール ③インターネット接続系端末④保守端末



通信経路 (3)インターネット接続系端末に１台化　DaaS利用(異なるCSP) の技術的対策①

✓ インターネット接続系端末からDaaS利用でのリスク分析の結果を踏まえ必要な対策を示す。
※以下の対策の前に、βモデルの対策を実施することが前提であることに留意。

(1)　利用するクラウドサービス
・ISMAPに登録されているクラウドサービスのDaaS
（通信経路(1)はα'モデルのため、ISMAPに登録されているクラウドサービスのDaaSが条件となる。
通信経路に係わらず、通信経路(3)もISMAPに登録されているクラウドサービスのDaaSを条件とする。）

(2) 技術的対策（次項に続く）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス(DaaS)上での対策			
画面転送機能	仮想端末を画面転送するという分離対策により、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
多要素によるユーザ認証	DaaSのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a　アクセス制御、b アクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a　アクセス制御　の実施のための対策	○
仮想端末でのパッチ適用	仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
仮想端末でのマルウェア対策ソフト	仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。		○
接続先制限	インターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
DaaS基盤の脆弱性対応	DaaS基盤の脆弱性にパッチを適用する。**DaaS事業者の責任範囲となるため、DaaS事業者選定時の前提条件となる。**	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
アクセスログ	不正アクセス等による被害の防止等のため、DaaSのアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○

通信経路 (3)インターネット接続系端末に１台化　DaaS利用(異なるCSP) の技術的対策②

(2) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
インターネット接続系での対策（βモデルの対策以外のもの）				
アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置　c　不正アクセス等による被害の防止等　の実施のための対策	○	
	LGWAN接続系DaaSとLGWAN接続系業務サーバとの通信のみにIPアドレス、通信ポートでアクセス制限する。	F.技術的安全管理措置　c　不正アクセス等による被害の防止等　の実施のための対策	○	
	インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置　c　不正アクセス等による被害の防止等　の実施のための対策	○	
アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、インターネット接続系端末でのスクリーンショット機能を停止する。（注）			○
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。
（パッチ適用（脆弱性管理）、未知の不正プログラムへの対策（エンドポイント対策）についてはβモデルにおける必須対策として規定）
スクリーンショット機能の停止の詳細は、P22を参照のこと

通信経路 (3)インターネット接続系端末に１台化　DaaS利用時(異なるCSP)の前提条件となるβモデルの対策　①

✓通信経路(3)の対策の前提となる、βモデルの対策を示す（ガイドラインに既に規定）。

(1) 技術的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
無害化処理	• 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、サニタイズ処理、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で危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。		○
LGWAN接続系の画面転送	• インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 • LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。		○
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、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○

通信経路 (3)インターネット接続系端末に１台化　DaaS利用時(異なるCSP)の前提条件となるβモデルの対策　②

(1) 技術的対策 (2)組織的・人的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
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。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
脆弱性管理	• OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、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する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
組織的・人的対策			
組織的なセキュリティ対策基準の遵守	• インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し　の実施のための対策	○
住民に関する情報をインターネット接続系に保存させない規定の整備	• 住民の名簿など、住民の個人情報（業務システムに保存されている場合は除く）をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。		○
本ガイドライン対策基準（例文）「１．組織体制（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 • 職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 • 職員等の実践的サイバー防御演習（CYDER）の受講 • 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 • 本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し		B 取扱規程等の見直し等　の実施のための対策 D.人的安全管理措置　b 事務取扱担当者等の教育　の実施のための対策	○

通信経路（３）‘インターネット接続系端末に１台化　DaaS利用（異なるCSP)
LGWAN接続系　α’モデルで接続　リスク分析結果より　必要な技術的対策

- マイナンバー利用事務系への影響　P44
- 対策群のイメージ図　　P45
- 対策群
  - 今回のリスク分析を踏まえた対策　P46・47
  - 前提となるβ、α‘モデルの対策　P48～51

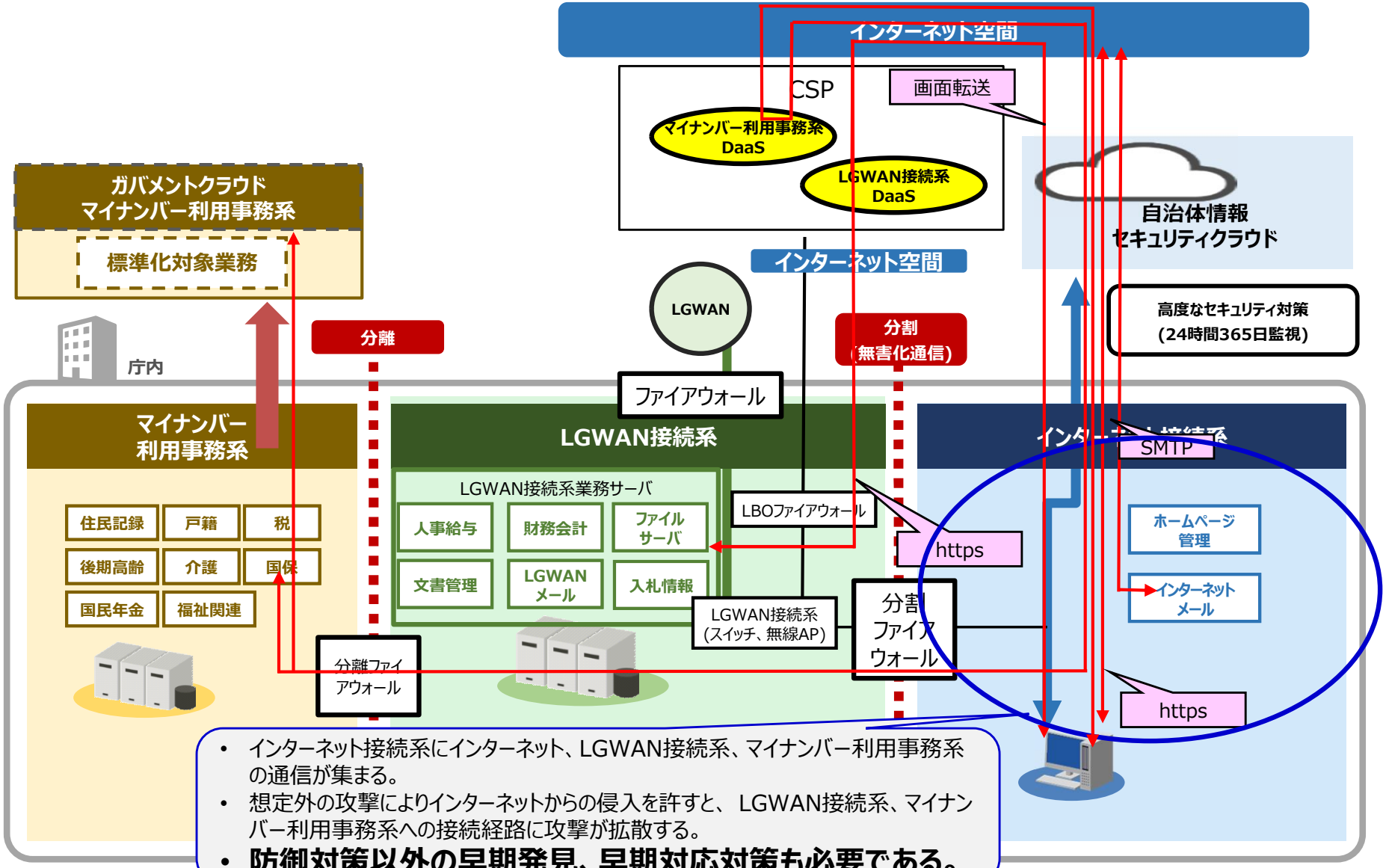
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系のみならずマイナンバー利用事務系に影響が及ぶ**可能性がある。

✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**

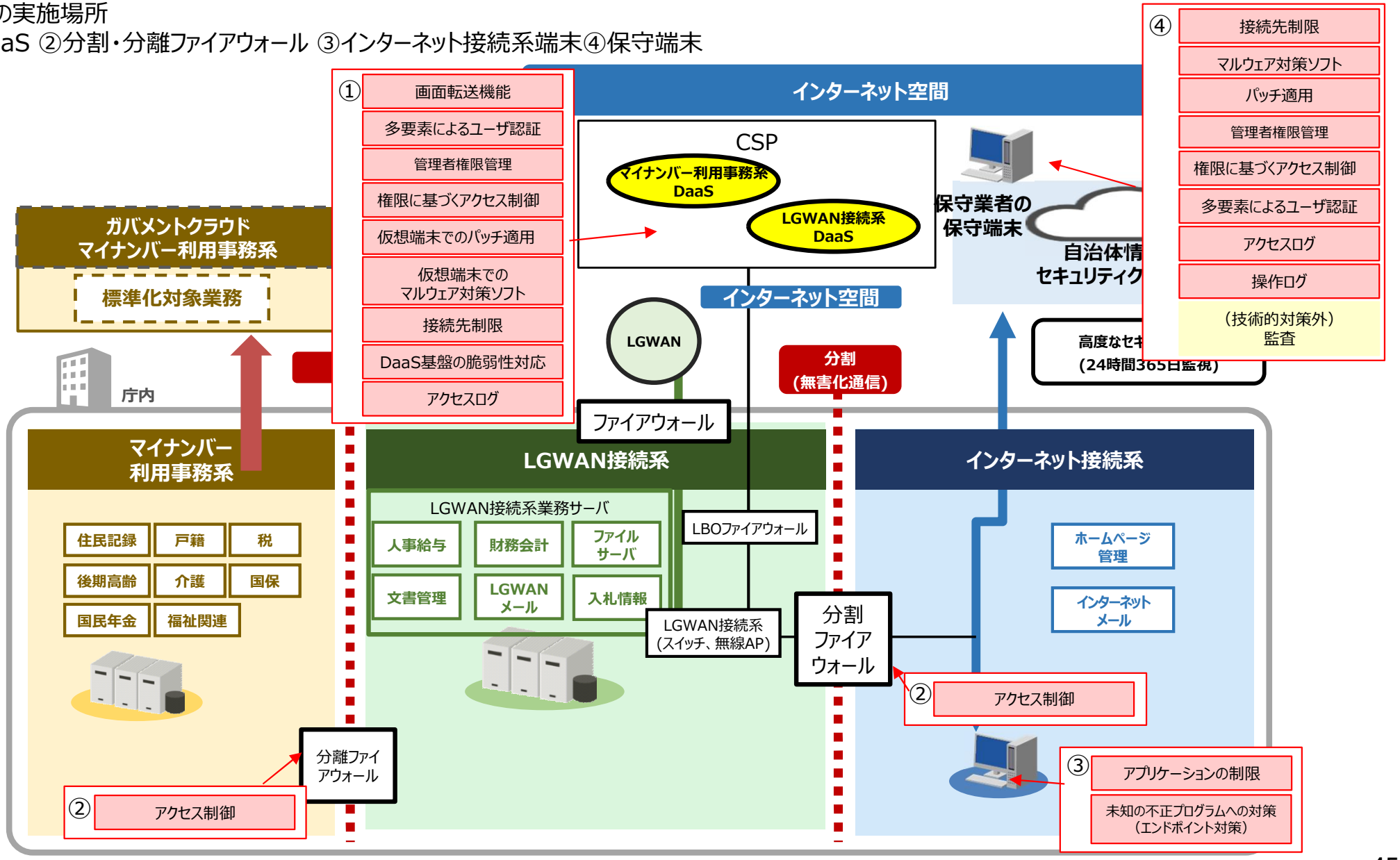


- インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まる。
- 想定外の攻撃によりインターネットからの侵入を許すと、 LGWAN接続系、マイナンバー利用事務系への接続経路に攻撃が拡散する。
- **防御対策以外の早期発見、早期対応対策も必要である。**

通信経路 (3)'インターネット接続系端末に１台化　DaaS利用(異なるCSP)
LGWAN接続系　α'モデルで接続の対策イメージ

- ✓ βモデル、α'モデルの対策を実施した上でインターネット接続系からからDaaSに接続する方式。
- ✓ リスクアセスメント結果を踏まえると、**βモデル、α'モデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
①DaaS ②分割・分離ファイアウォール ③インターネット接続系端末④保守端末



通信経路 (3)'インターネット接続系端末に１台化　DaaS利用(異なるCSP)
LGWAN接続系　α'モデルで接続の技術的対策①

✓ インターネット接続系端末からDaaS利用でのリスク分析の結果を踏まえ必要な対策を示す。
※以下の対策の前に、βモデル、α'モデルの対策を実施することが前提であることに留意。

(1)　利用するクラウドサービス
・ISMAPに登録されているクラウドサービスのDaaS
（通信経路(1)はα'モデルのため、ISMAPに登録されているクラウドサービスのDaaSが条件となる。
通信経路に係わらず、通信経路(3)もISMAPに登録されているクラウドサービスのDaaSを条件とする。）

(2) 技術的対策（次項に続く）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス(DaaS)上での対策			
画面転送機能	仮想端末を画面転送するという分離対策により、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
多要素によるユーザ認証	DaaSのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a アクセス制御、b アクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a アクセス制御　の実施のための対策	○
仮想端末でのパッチ適用	仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
仮想端末でのマルウェア対策ソフト	仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。		○
接続先制限	インターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
DaaS基盤の脆弱性対応	DaaS基盤の脆弱性にパッチを適用する。**DaaS事業者の責任範囲となるため、DaaS事業者選定時の前提条件となる。**	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
アクセスログ	不正アクセス等による被害の防止等のため、DaaSのアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○

通信経路 (3)’インターネット接続系端末に１台化　DaaS利用(異なるCSP)
LGWAN接続系　α’モデルで接続の技術的対策②

(2) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
インターネット接続系での対策（βモデルの対策以外のもの）				
アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置　c　不正アクセス等による被害の防止等　の実施のための対策	○	
	LGWAN接続系DaaSとLGWAN接続系業務サーバとの通信のみにIPアドレス、通信ポートでアクセス制限する。	F.技術的安全管理措置　c　不正アクセス等による被害の防止等　の実施のための対策	○	
	インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置　c　不正アクセス等による被害の防止等　の実施のための対策	○	
アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、インターネット接続系端末でのスクリーンショット機能を停止する。（注）			○
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。
（パッチ適用（脆弱性管理）、未知の不正プログラムへの対策（エンドポイント対策）についてはβモデルにおける必須対策として規定
マルウェア対策ソフトの導入についてはα‘モデルにおける必須対策として規定）
スクリーンショット機能の停止の詳細は、P22を参照のこと

通信経路 (3)’インターネット接続系端末に１台化(異なるCSP) １台化　DaaS利用(異なるCSP)
LGWAN接続　α‘モデル時　前提条件となるβモデルの対策　①

✓通信経路(3)’の対策の前提となる、βモデルの対策を示す（ガイドラインに既に規定）。

(1) 技術的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
無害化処理	• 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、サニタイズ処理、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で危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。		○
LGWAN接続系の画面転送	• インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 • LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。		○
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、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○

通信経路 (3)'インターネット接続系端末に１台化(異なるCSP) １台化　DaaS利用(異なるCSP) LGWAN接続　α'モデル時　前提条件となるβモデルの対策　②

(1) 技術的対策 (2)組織的・人的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
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。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
脆弱性管理	• OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、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する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
組織的・人的対策			
組織的なセキュリティ対策基準の遵守	• インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し　の実施のための対策	○
住民に関する情報をインターネット接続系に保存させない規定の整備	• 住民の名簿など、住民の個人情報（業務システムに保存されている場合は除く）をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。		○
本ガイドライン対策基準（例文）「１．組織体制（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 • 職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 • 職員等の実践的サイバー防御演習（CYDER）の受講 • 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 • 本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し		B 取扱規程等の見直し等　の実施のための対策 D.人的安全管理措置　b 事務取扱担当者等の教育　の実施のための対策	○

通信経路 (3)'インターネット接続系端末に１台化(異なるCSP) １台化　DaaS利用(異なるCSP) LGWAN接続　α'モデル時　前提条件となるα'モデルの対策　①

✓通信経路(3)'の対策の前提となる、α'モデルの対策を示す（ガイドラインに既に規定）。

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス上での対策			
マルウェア対策	DaaSの仮想端末でマルウェア検査、不正ソフトウェア対策を行う。		○
LGWAN接続系での対策			
通信相手の証明書による認証	通信相手が本物であるか否か、正当性を確認する。		○
マルウェア対策ソフト	マルウェアを検知・除去する。パターンマッチング方式、不審な動作を行うコードが含まれていることを検出するヒューリスティック方式を行う。LGWAN接続系端末、LGWAN接続系業務サーバにて対応が必要。		○
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。LGWAN接続系端末、LGWAN接続系業務サーバ、分離・分割ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。	F.技術的安全管理措置　c 不正アクセス等による被害の防止等　の実施のための対策	○
接続先制限	LGWAN接続系から外部へのアクセス先を**利用するＤaaSのみに限定**する。	F.技術的安全管理措置　a　アクセス制御　の実施のための対策	○
LBO テナント（**自団体の領域**）へのアクセス制御	利用するクラウドサービスへのアクセスを自団体の領域のみに制限する。	F.技術的安全管理措置　a　アクセス制御　の実施のための対策	○
メール無害化/ファイル無害化	受信したメールの本文のテキスト化、インターネットメールの添付ファイルやインターネットからダウンロードしたファイルの無害化をする。(3)'においてはメールの取り扱いがα'モデルの経路ではないため、対象外。		○
権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限及び関連する属性に応じて適切に管理する。LGWAN接続系端末、LGWAN接続系業務サーバ、ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。		○
アクセス制御	不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う。LGWAN接続系端末、LGWAN接続系業務サーバ、分離・分割ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。	F.技術的安全管理措置　a　アクセス制御　の実施のための対策	○

通信経路 (3)’インターネット接続系端末に１台化(異なるCSP) １台化　DaaS利用(異なるCSP)
LGWAN接続　α‘モデル時　前提条件となるα‘モデルの対策　②

(前項からの続き)

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
LGWAN接続系での対策				
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策			○
IDS/IPS	ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。		○	
DDoS 対策	DDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS 対策機器の導入やDDoS 対策サービスの利用によって、高負荷攻撃への耐性を向上する。負荷分散装置（「ロードバランサ」）による耐性向上を含む。			○
冗長化	LBOファイアウォールに対する攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。			○
通信路暗号化	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。	F.技術的安全管理措置　d　漏えい等の防止　の実施のための対策	○	

注）未知の不正プログラムへの対策（エンドポイント対策）はα‘モデルでは推奨であるが、**想定外の攻撃や、脆弱性へのゼロデイ攻撃に対処するためには、未知の不正プログラムへの対策（エンドポイント対策）を導入し、侵入の早期発見、早期の対応を行うことが重要であるため、「α‘モデルの対策以外のLGWAN接続系での対策」に必須対策として規定**する。

通信経路 (4)インターネット接続系端末に１台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)
リスク分析結果より　必要な技術的対策

- マイナンバー利用事務系への影響　P54
- 対策群のイメージ図　　P55
- 対策群
  - 今回のリスク分析を踏まえた対策　P56～58
  - 前提となるβモデルの対策　P59・60

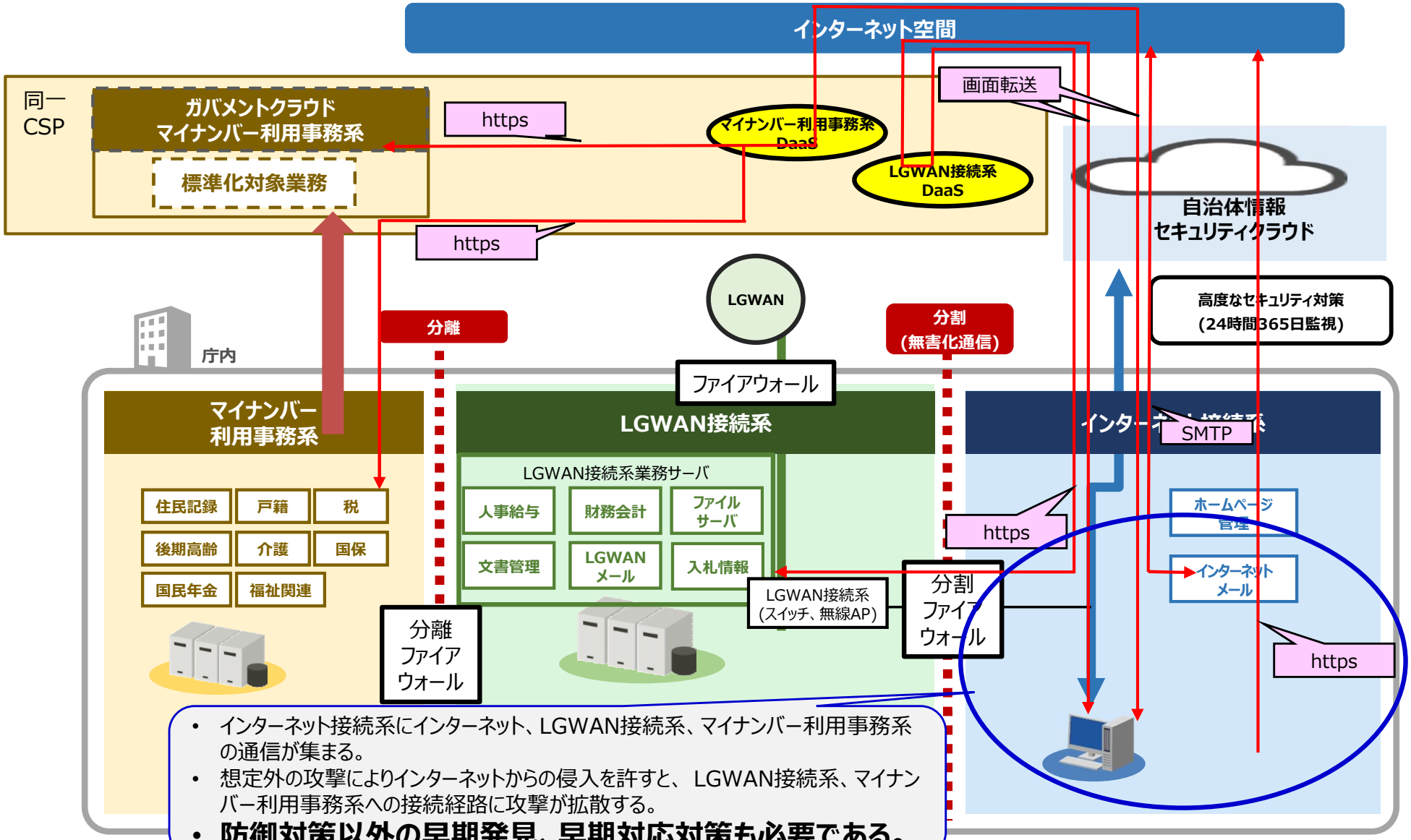
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系のみならずマイナンバー利用事務系に影響が及ぶ**可能性がある。

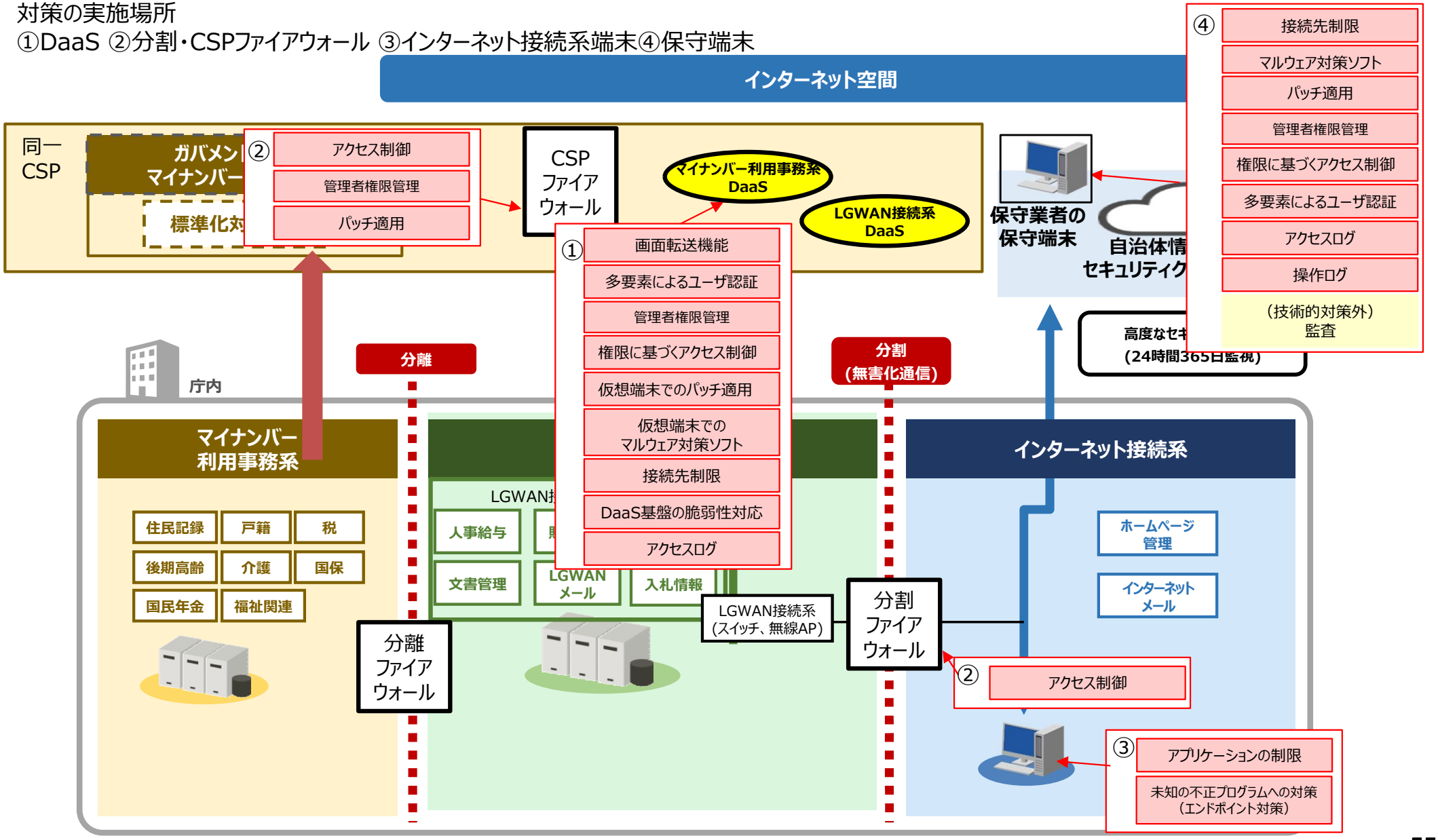
✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**



通信経路 (4)インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)の対策イメージ

- ✓ βモデルの対策を実施した上でインターネット接続系からDaaSに接続する方式。
- ✓ リスクアセスメント結果を踏まえると、**βモデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
①DaaS ②分割・CSPファイアウォール ③インターネット接続系端末④保守端末



通信経路 (4)インターネット接続系端末に１台化　DaaS利用 ガバメントクラウド/DaaS(同一CSP) の技術的対策①

✓ インターネット接続系端末からDaaS利用でのリスク分析の結果を踏まえ必要な対策を示す。
※以下の対策の前に、βモデルの対策を実施することが前提であることに留意。

(1)　利用するクラウドサービス
・ISMAPに登録されているクラウドサービスのDaaS
（通信経路(1)はα'モデルのため、ISMAPに登録されているクラウドサービスのDaaSが条件となる。
通信経路に係わらず、通信経路(4)もISMAPに登録されているクラウドサービスのDaaSを条件とする。）

(2) 技術的対策（次項に続く）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス(DaaS)上での対策			
画面転送機能	仮想端末を画面転送するという分離対策により、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
多要素によるユーザ認証	DaaSのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a アクセス制御、b アクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a アクセス制御　の実施のための対策	○
仮想端末でのパッチ適用	仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
仮想端末でのマルウェア対策ソフト	仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。		○
接続先制限	インターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
DaaS基盤の脆弱性対応	DaaS基盤の脆弱性にパッチを適用する。**DaaS事業者の責任範囲となるため、DaaS事業者選定時の前提条件となる。**	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
アクセスログ	不正アクセス等による被害の防止等のため、DaaSのアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e 取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○

(2) 技術的対策（前項からの続き）

技術的対策		対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
クラウドサービス（CSP）上での対策					
	アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するためにユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。CSPファイアウォールにて対応が必要。		○	
	パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。CSPファイアウォールにて対応が必要。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○	
インターネット接続系での対策（βモデルの対策以外のもの）					
	アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
		LGWAN接続系DaaSとLGWAN接続系業務サーバとの通信のみにIPアドレス、通信ポートでアクセス制限する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
		インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	

(2) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
インターネット接続系での対策（βモデルの対策以外のもの）				
アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、インターネット接続系端末でのスクリーンショット機能を停止する。（注）			○
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。
（パッチ適用（脆弱性管理）、未知の不正プログラムへの対策（エンドポイント対策）についてはβモデルにおける必須対策として規定）
スクリーンショット機能の停止の詳細は、P22を参照のこと

通信経路 (4)インターネット接続系端末に１台化　DaaS利用 ガバメントクラウド/DaaS(同一CSP)の前提条件となるβモデルの対策　①

✓通信経路(4)の対策の前提となる、βモデルの対策を示す（ガイドラインに既に規定）。

(1) 技術的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
無害化処理	• 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、サニタイズ処理、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で危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。		○
LGWAN接続系の画面転送	• インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 • LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。		○
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、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○

通信経路 (4)インターネット接続系端末に１台化　DaaS利用 ガバメントクラウド/DaaS(同一CSP)の前提条件となるβモデルの対策　②

(1) 技術的対策 (2)組織的・人的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
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。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
脆弱性管理	• OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、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する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
組織的・人的対策			
組織的なセキュリティ対策基準の遵守	• インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し　の実施のための対策	○
住民に関する情報をインターネット接続系に保存させない規定の整備	• 住民の名簿など、住民の個人情報（業務システムに保存されている場合は除く）をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。		○
本ガイドライン対策基準（例文）「１．組織体制（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 • 職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 • 職員等の実践的サイバー防御演習（CYDER）の受講 • 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 • 本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し		B 取扱規程等の見直し等　の実施のための対策 D.人的安全管理措置　b 事務取扱担当者等の教育　の実施のための対策	○

通信経路 (4)’インターネット接続系端末に１台化　DaaS利用
ガバメントクラウド/DaaS(同一CSP) LGWAN接続系　α‘モデル接続
リスク分析結果より　必要な技術的対策

- マイナンバー利用事務系への影響　P63
- 対策群のイメージ図　　P64
- 対策群
  - 今回のリスク分析を踏まえた対策　P65～67
  - 前提となるβ、α‘モデルの対策　P68～71

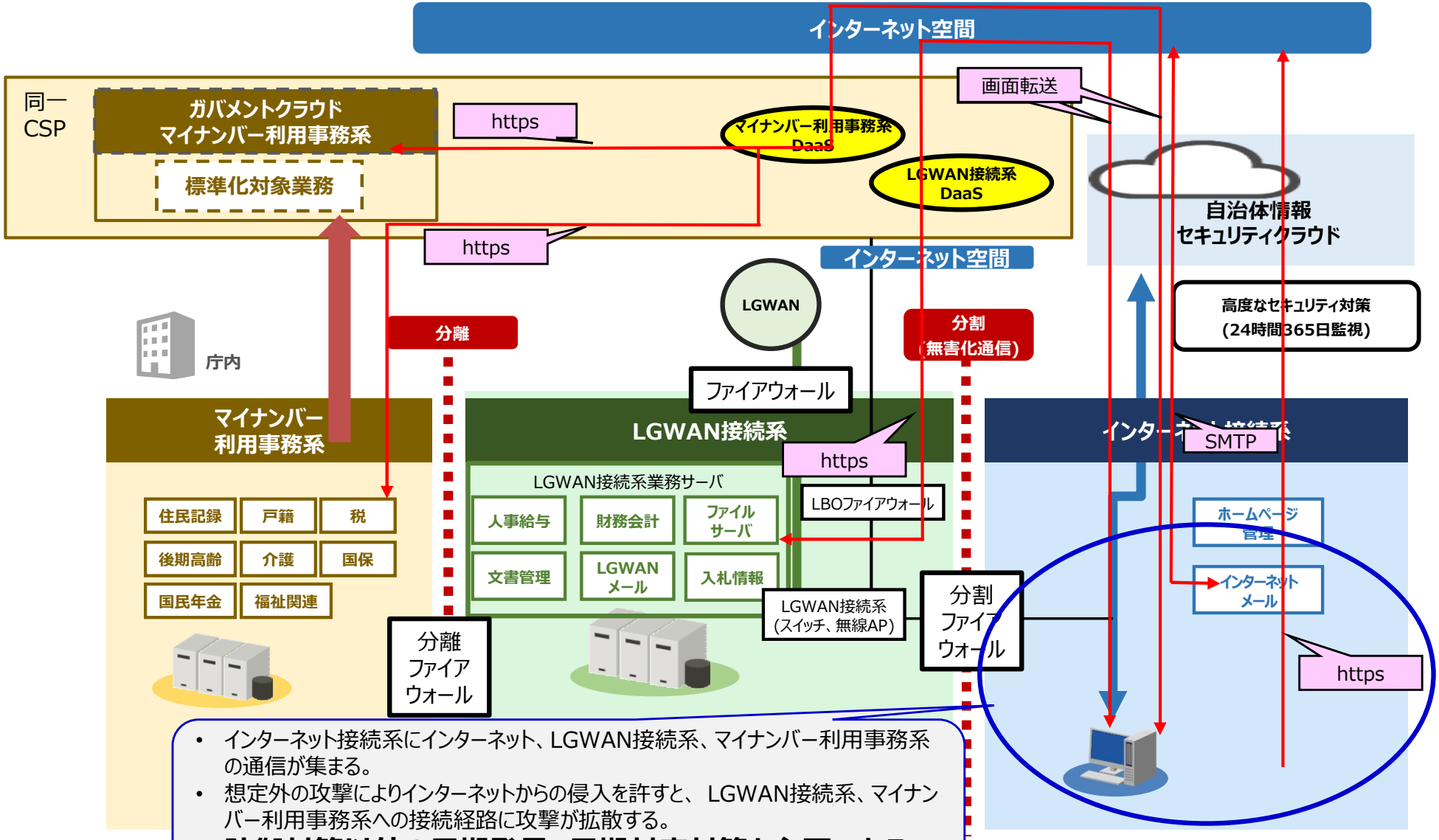
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系のみならずマイナンバー利用事務系に影響が及ぶ**可能性がある。

✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**

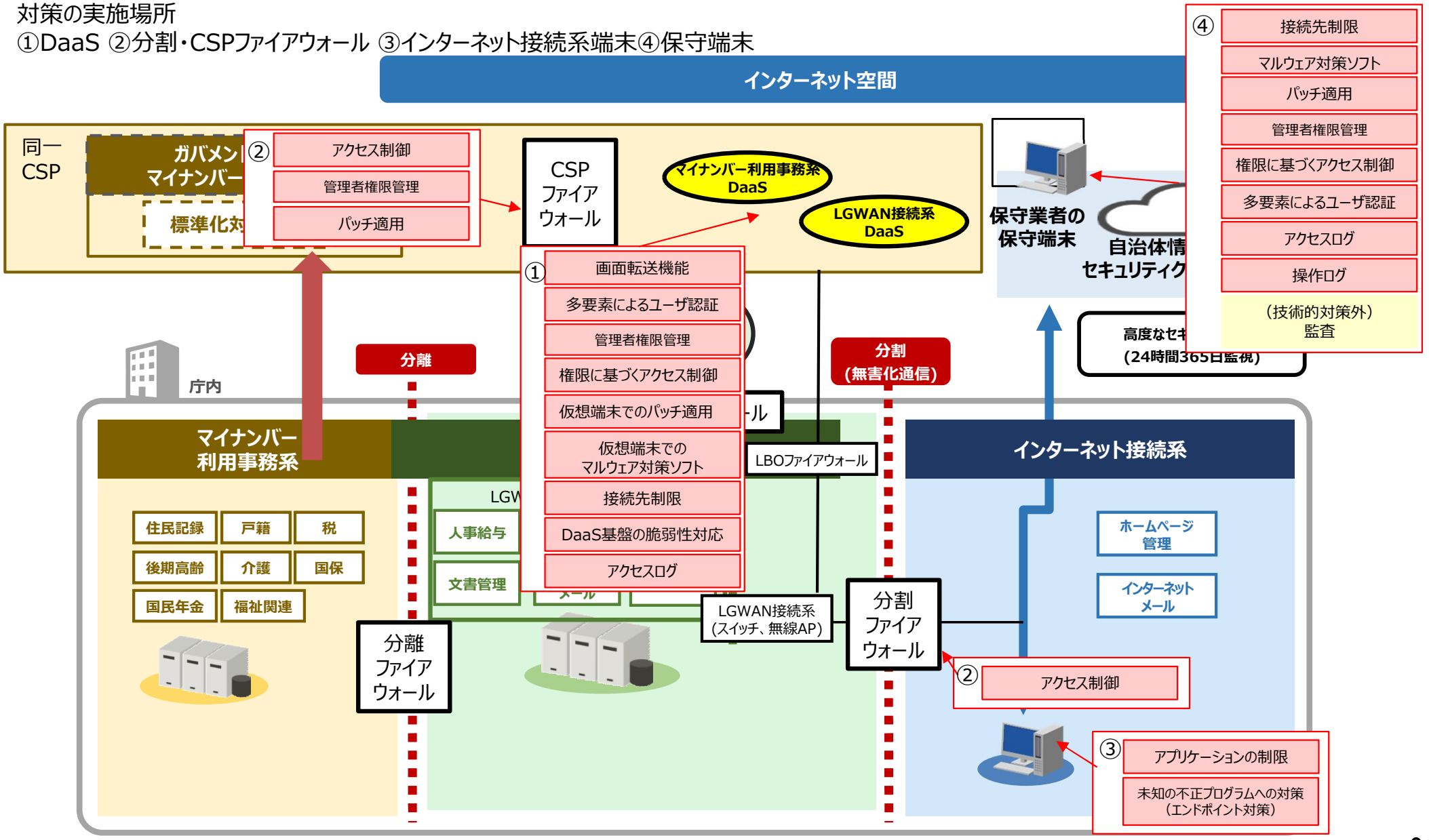


- インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まる。
- 想定外の攻撃によりインターネットからの侵入を許すと、 LGWAN接続系、マイナンバー利用事務系への接続経路に攻撃が拡散する。
- **防御対策以外の早期発見、早期対応対策も必要である。**

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の対策

- ✓ βモデル、α'モデルの対策を実施した上でインターネット接続系からDaaSに接続する方式。
- ✓ リスクアセスメント結果を踏まえると、**βモデル、α'モデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
①DaaS ②分割・CSPファイアウォール ③インターネット接続系端末④保守端末



通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の技術的対策①

✓ インターネット接続系端末からDaaS利用でのリスク分析の結果を踏まえ必要な対策を示す。
※以下の対策の前に、βモデル、α'モデルの対策を実施することが前提であることに留意。

(1)　利用するクラウドサービス
・ISMAPに登録されているクラウドサービスのDaaS
（通信経路(1)はα'モデルのため、同じ考え方によりISMAPに登録されているクラウドサービスのDaaSが条件となる。
通信経路に係わらず、通信経路(4)もISMAPに登録されているクラウドサービスのDaaSを条件とする。）

(2) 技術的対策（次項に続く）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス(DaaS)上での対策			
画面転送機能	仮想端末を画面転送するという分離対策により、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
多要素によるユーザ認証	DaaSのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a アクセス制御、b アクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a アクセス制御　の実施のための対策	○
仮想端末でのパッチ適用	仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
仮想端末でのマルウェア対策ソフト	仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。		○
接続先制限	インターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
DaaS基盤の脆弱性対応	DaaS基盤の脆弱性にパッチを適用する。**DaaS事業者の責任範囲となるため、DaaS事業者選定時の前提条件となる。**	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
アクセスログ	不正アクセス等による被害の防止等のため、DaaSのアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e 取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の技術的対策②

(2) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
クラウドサービス（CSP）上での対策				
アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するためにユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。CSPファイアウォールにて対応が必要。		○	
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。CSPファイアウォールにて対応が必要。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
インターネット接続系での対策（βモデルの対策以外のもの）				
アクセス制限	接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	LGWAN接続系DaaSとLGWAN接続系業務サーバとの通信のみにIPアドレス、通信ポートでアクセス制限する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置　c 不正アクセス等による被害の防止等　の実施のための対策	○	
アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、インターネット接続系端末でのスクリーンショット機能を停止する。（注）			○

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。（パッチ適用、マルウェア対策ソフトの導入についてはα'モデルにおける必須対策として規定）
スクリーンショット機能の停止の詳細は、 P22を参照のこと

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の技術的対策③

(2) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
インターネット接続系での対策（βモデルの対策以外のもの）				
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。
（パッチ適用（脆弱性管理）、未知の不正プログラムへの対策（エンドポイント対策）についてはβモデルにおける必須対策として規定）

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続 前提条件となるβモデルの対策　①

✓通信経路(4)'の対策の前提となる、βモデルの対策を示す（ガイドラインに既に規定）。

(1) 技術的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
無害化処理	• 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、サニタイズ処理、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で危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。		○
LGWAN接続系の画面転送	• インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 • LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。		○
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、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続 前提条件となるβモデルの対策　②

(1) 技術的対策 (2)組織的・人的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
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。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
脆弱性管理	• OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、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する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
組織的・人的対策			
組織的なセキュリティ対策基準の遵守	• インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し　の実施のための対策	○
住民に関する情報をインターネット接続系に保存させない規定の整備	• 住民の名簿など、住民の個人情報（業務システムに保存されている場合は除く）をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。		○
本ガイドライン対策基準（例文）「１．組織体制（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 • 職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 • 職員等の実践的サイバー防御演習（CYDER）の受講 • 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 • 本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し	B 取扱規程等の見直し等　の実施のための対策 D.人的安全管理措置　b 事務取扱担当者等の教育　の実施のための対策	○

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続 前提条件となるα'モデルの対策　①

✓通信経路(4)'の対策の前提となる、α'モデルの対策を示す（ガイドラインに既に規定）。

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
クラウドサービス上での対策			
マルウェア対策	DaaSの仮想端末でマルウェア検査、不正ソフトウェア対策を行う。		○
LGWAN接続系での対策			
通信相手の証明書による認証	通信相手が本物であるか否か、正当性を確認する。		○
マルウェア対策ソフト	マルウェアを検知・除去する。パターンマッチング方式、不審な動作を行うコードが含まれていることを検出するヒューリスティック方式を行う。LGWAN接続系端末、LGWAN接続系業務サーバにて対応が必要。		○
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。LGWAN接続系端末、LGWAN接続系業務サーバ、分離・分割ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。	F.技術的安全管理措置 c不正アクセス等による被害の防止等　の実施のための対策	○
接続先制限	LGWAN接続系から外部へのアクセス先を**利用するＤaaSのみに限定**する。	F.技術的安全管理措置 a アクセス制御 の実施のための対策	○
LBO テナント（**自団体の領域**）へのアクセス制御	利用するクラウドサービスへのアクセスを自団体の領域のみに制限する。	F.技術的安全管理措置 a アクセス制御 の実施のための対策	○
メール無害化/ファイル無害化	受信したメールの本文のテキスト化、インターネットメールの添付ファイルやインターネットからダウンロードしたファイルの無害化をする。(4)'においてはメールの取り扱いがα'モデルの経路ではないため、対象外。		○
権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限及び関連する属性に応じて適切に管理する。LGWAN接続系端末、LGWAN接続系業務サーバ、ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。		○
アクセス制御	不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う。LGWAN接続系端末、LGWAN接続系業務サーバ、分離・分割ファイアウォール、LBOファイアウォール、LGWAN接続系のスイッチ・無線APにて対応が必要。	F.技術的安全管理措置 a アクセス制御 の実施のための対策	○

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続 前提条件となるα'モデルの対策　②

(前項からの続き)

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
LGWAN接続系での対策				
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策			○
IDS/IPS	ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。		○	
DDoS 対策	DDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS 対策機器の導入やDDoS 対策サービスの利用によって、高負荷攻撃への耐性を向上する。負荷分散装置（「ロードバランサ」）による耐性向上を含む。			○
冗長化	LBOファイアウォールに対する攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。			○
通信路暗号化	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。	F.技術的安全管理措置　d　漏えい等の防止　の実施のための対策	○	

注）未知の不正プログラムへの対策（エンドポイント対策）はα'モデルでは推奨であるが、**想定外の攻撃や、脆弱性へのゼロデイ攻撃に対処するためには、未知の不正プログラムへの対策（エンドポイント対策）を導入し、侵入の早期発見、早期の対応を行うことが重要であるため、「α'モデルの対策以外のLGWAN接続系での対策」に必須対策として規定**する。

通信経路 (5)　LGWAN接続系端末に１台化　オンプレミス　画面転送システム
リスク分析結果を踏まえた技術的対策

- ■ マイナンバー利用事務系への影響　P74
- ■ 対策群のイメージ図　　P75
- ■ 対策群
  - ■ 今回のリスク分析を踏まえた対策　P76・77

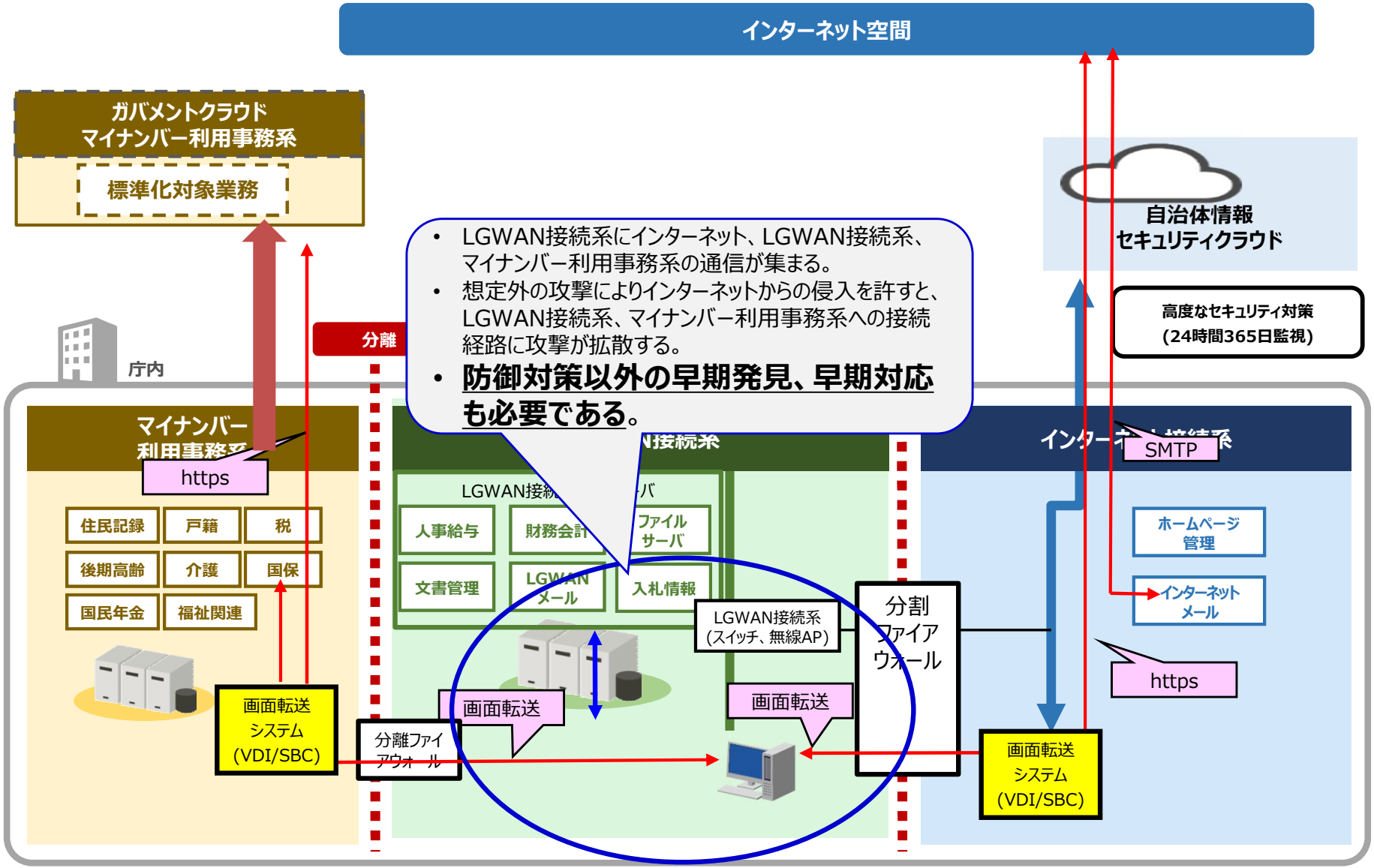
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**LGWAN接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系、マイナンバー利用事務系に影響が及ぶ。**

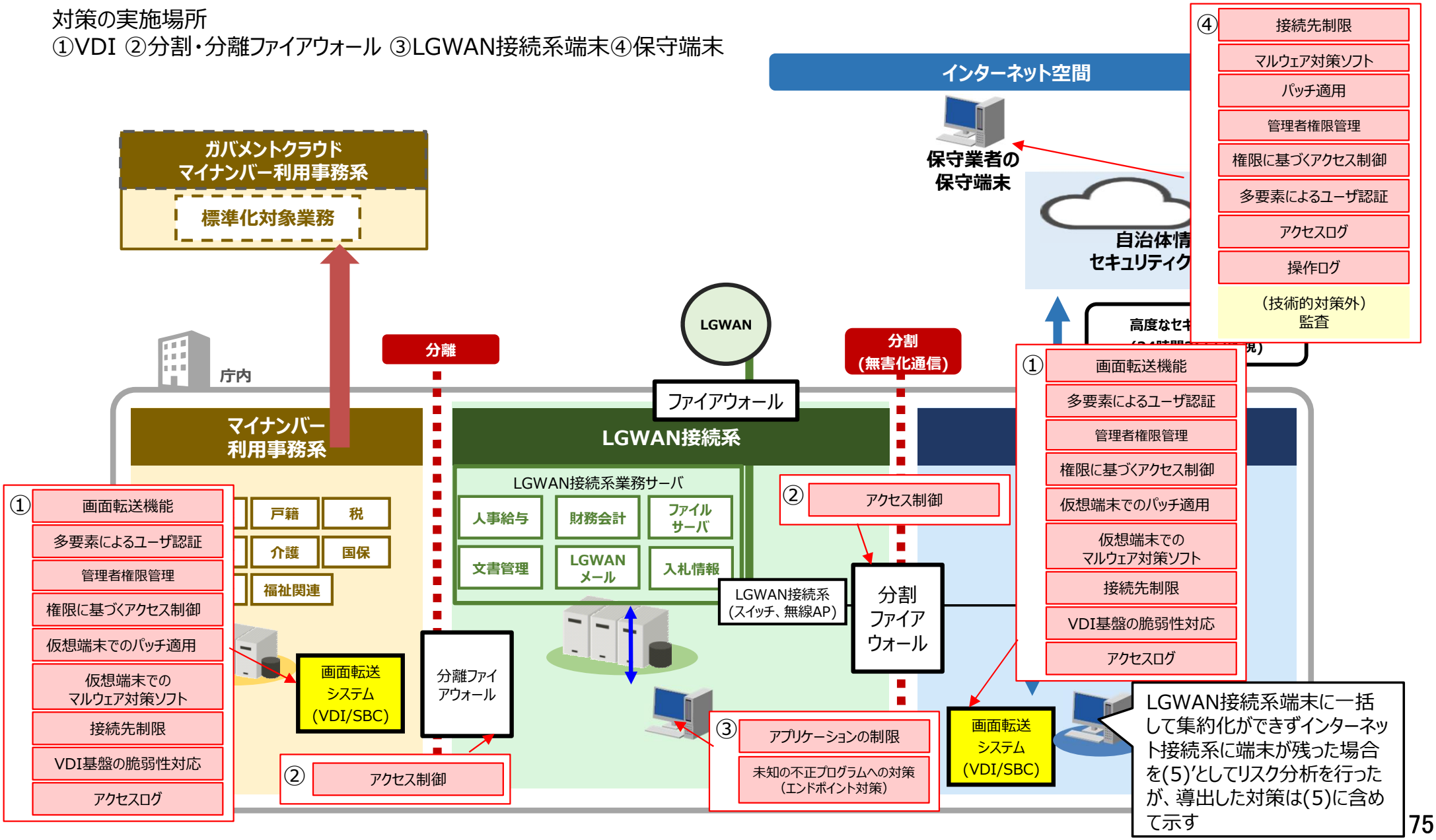
✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**



通信経路 (5) LGWAN接続系端末に１台化　オンプレミス　画面転送システムの対策

- ✓ αモデルの対策を原則とした上でLGWAN接続系からオンプレミス　画面転送システム（以下、VDI表記と両用)に接続する方式。
- ✓ リスクアセスメント結果を踏まえると、**αモデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
①VDI ②分割・分離ファイアウォール ③LGWAN接続系端末④保守端末



通信経路 (5) LGWAN接続系端末に１台化　オンプレミス　画面転送システムの技術的対策①

✓LGWAN接続系端末からVDI利用でのリスクアセスメントの結果を踏まえ必要な対策を示す。
※以下の対策の前に、αモデルの対策を実施することが前提であることに留意。
αモデルの対策はガイドラインの第3編第2章の「3.情報システム全体の強靭性の向上」を参照のこと。

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
VDIでの対策			
画面転送機能	仮想端末を画面転送するという分離対策により、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
多要素によるユーザ認証	VDIのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a アクセス制御、b アクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a アクセス制御　の実施のための対策	○
仮想端末でのパッチ適用	仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
仮想端末でのマルウェア対策ソフト	仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。		○
接続先制限	LGWAN接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○
VDI基盤の脆弱性対応	VDI基盤の脆弱性にパッチを適用する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
アクセスログ	不正アクセス等による被害の防止等のため、VDIのアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○

通信経路 (5) LGWAN接続系端末に１台化　オンプレミス　画面転送システムの技術的対策②

(1) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
LGWAN接続系での対策（αモデルの対策以外のもの）				
アクセス制限	接続元（マイナンバー利用事務系VDI）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	接続元（インターネット接続系VDI）と接続先（インターネット、インターネット接続系のメールサーバ）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、LGWAN接続系端末でのスクリーンショット機能を停止する。（注）			○
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。（パッチ適用、マルウェア対策ソフトの導入についてはα'モデルにおける必須対策として規定）
スクリーンショット機能の停止の詳細は、P22を参照のこと

通信経路経路 (6) インターネット接続系端末に１台化　オンプレミス　画面転送システム
リスク分析結果より　必要な技術的対策

- マイナンバー利用事務系への影響　P80
- 対策群のイメージ図　　P81
- 対策群
  - 今回のリスク分析を踏まえた対策　P82･83
  - 前提となるβモデルの対策　P84･85

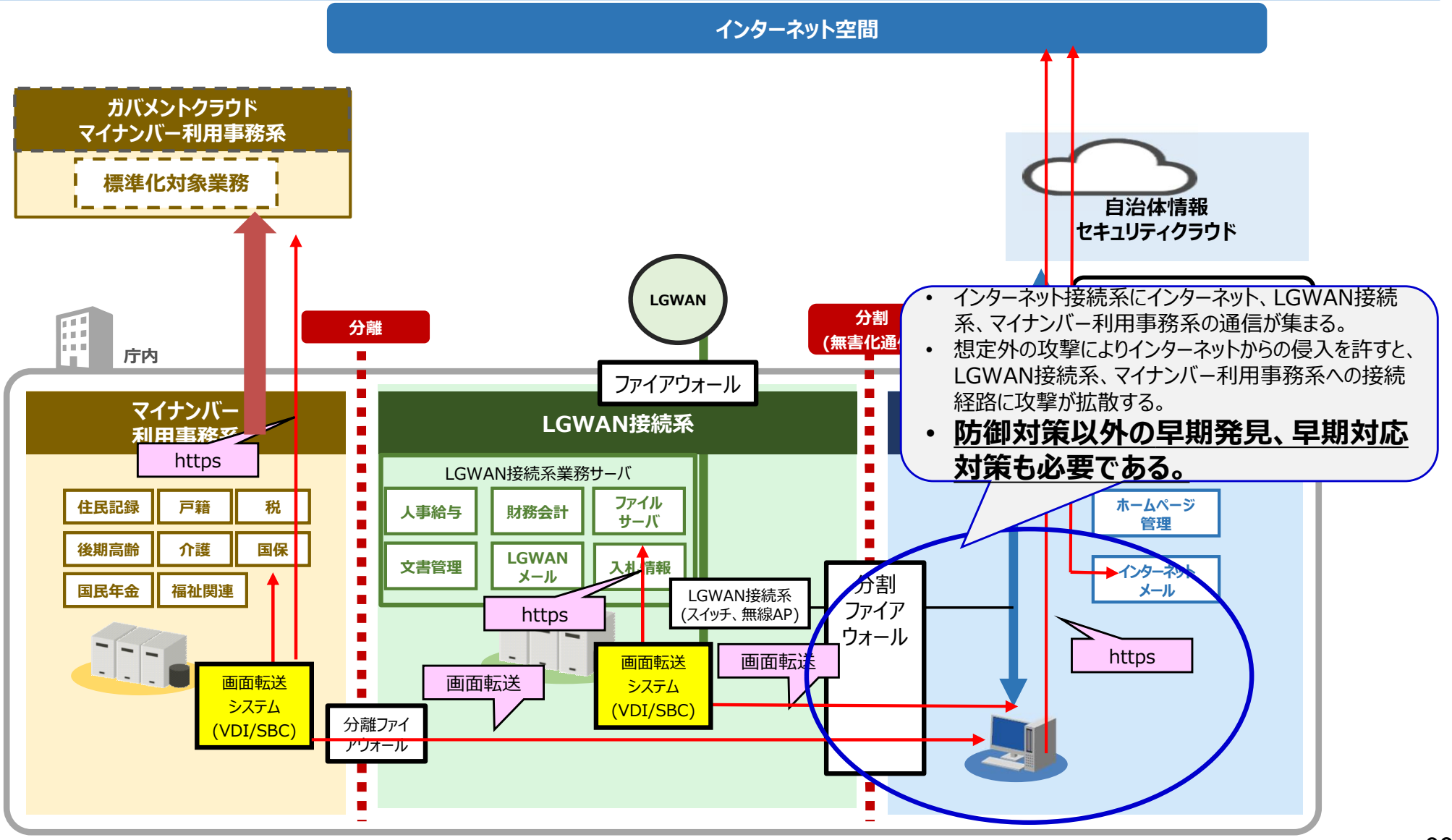
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系のみならずマイナンバー利用事務系に影響が及ぶ**可能性がある。

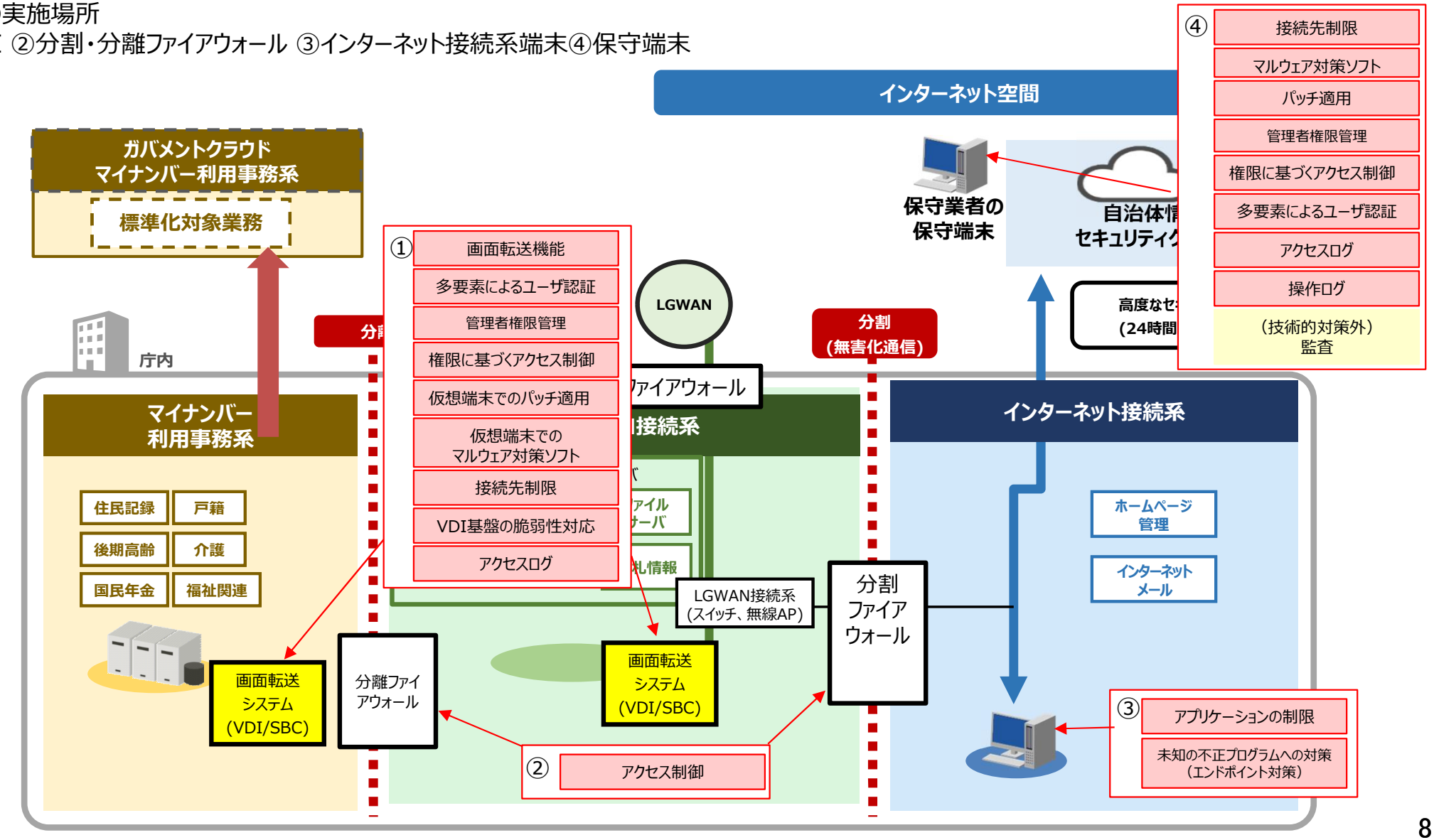
✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**



通信経路 (6) インターネット接続系端末に１台化　オンプレミス　画面転送システムの対策

- ✓ インターネット接続系からオンプレミス　画面転送システム（以下、VDI表記と併用)に接続する方式。
- ✓ インターネット接続系へのLGWAN接続系からの画面転送はβモデルとしてガイドラインに規定済。
- ✓ マイナンバー利用事務系からの画面転送を行うにあたり、リスクアセスメント結果を踏まえると、**βモデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
①VDI ②分割・分離ファイアウォール ③インターネット接続系端末④保守端末



通信経路 (6) インターネット接続系端末に１台化　オンプレミス　画面転送システムの技術的対策①

✓インターネット接続系端末からVDI利用でのリスクアセスメントの結果を踏まえ必要な対策を示す。
※以下の対策の前に、βモデルの対策を実施することが前提であることに留意。

(1) 技術的対策（次項に続く）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
VDIでの対策			
画面転送機能	仮想端末を画面転送するという分離対策により、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
多要素によるユーザ認証	VDIのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a アクセス制御、b アクセス者の識別と認証　の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a アクセス制御　の実施のための対策	○
仮想端末でのパッチ適用	仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c不正アクセス等による被害の防止等　の実施のための対策	○
仮想端末でのマルウェア対策ソフト	仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。		○
接続先制限	インターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限。	F.技術的安全管理措置 c不正アクセス等による被害の防止等　の実施のための対策	○
VDI基盤の脆弱性対応	VDI基盤の脆弱性にパッチを適用する。	F.技術的安全管理措置 c不正アクセス等による被害の防止等　の実施のための対策	○
アクセスログ	不正アクセス等による被害の防止等のため、VDIのアクセスログを取得し、確認する。	F.技術的安全管理措置 c不正アクセス等による被害の防止等　の実施のための対策	○

通信経路 (6) インターネット接続系端末に１台化　オンプレミス　画面転送システムの技術的対策②

（1）技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
インターネット接続系、LGWAN接続系での対策（βモデルの対策以外のもの）				
アクセス制限	接続元（マイナンバー利用事務系VDI）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○	
	接続元（LGWAN接続系VDI）と接続先（LGWAN接続系システム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置　c 不正アクセス等による被害の防止等 の実施のための対策	○	
	インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○	
アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、インターネット接続系端末でのスクリーンショット機能を停止する。（注）			○
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。（パッチ適用、マルウェア対策ソフトの導入についてはα'モデルにおける必須対策として規定）

スクリーンショット機能の停止の詳細は、P22を参照のこと

通信経路 (6)インターネット接続系端末に１台化　オンプレミス　画面転送システムの前提条件となるβモデルの対策　①

✓通信経路(6)の対策の前提となる、βモデルの対策を示す（ガイドラインに既に規定）。

(1) 技術的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
無害化処理	• 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、サニタイズ処理、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で危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。		○
LGWAN接続系の画面転送	• インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 • LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。		○
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、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○

通信経路 (6)インターネット接続系端末に１台化　オンプレミス　画面転送システムの前提条件となるβモデルの対策　②

(1) 技術的対策 (2)組織的・人的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
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。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
脆弱性管理	• OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、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する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
組織的・人的対策			
組織的なセキュリティ対策基準の遵守	• インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し　の実施のための対策	○
住民に関する情報をインターネット接続系に保存させない規定の整備	• 住民の名簿など、住民の個人情報（業務システムに保存されている場合は除く）をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。		○
本ガイドライン対策基準（例文）「１．組織体制（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 • 職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 • 職員等の実践的サイバー防御演習（CYDER）の受講 • 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 • 本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し		B 取扱規程等の見直し等　の実施のための対策 D.人的安全管理措置　b 事務取扱担当者等の教育　の実施のための対策	○

通信経路 (7)　LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザ
リスク分析結果を踏まえた技術的対策

- マイナンバー利用事務系への影響　P88
- 対策群のイメージ図　　P89
- 対策群
  - 今回のリスク分析を踏まえた対策　P90 ～ 92

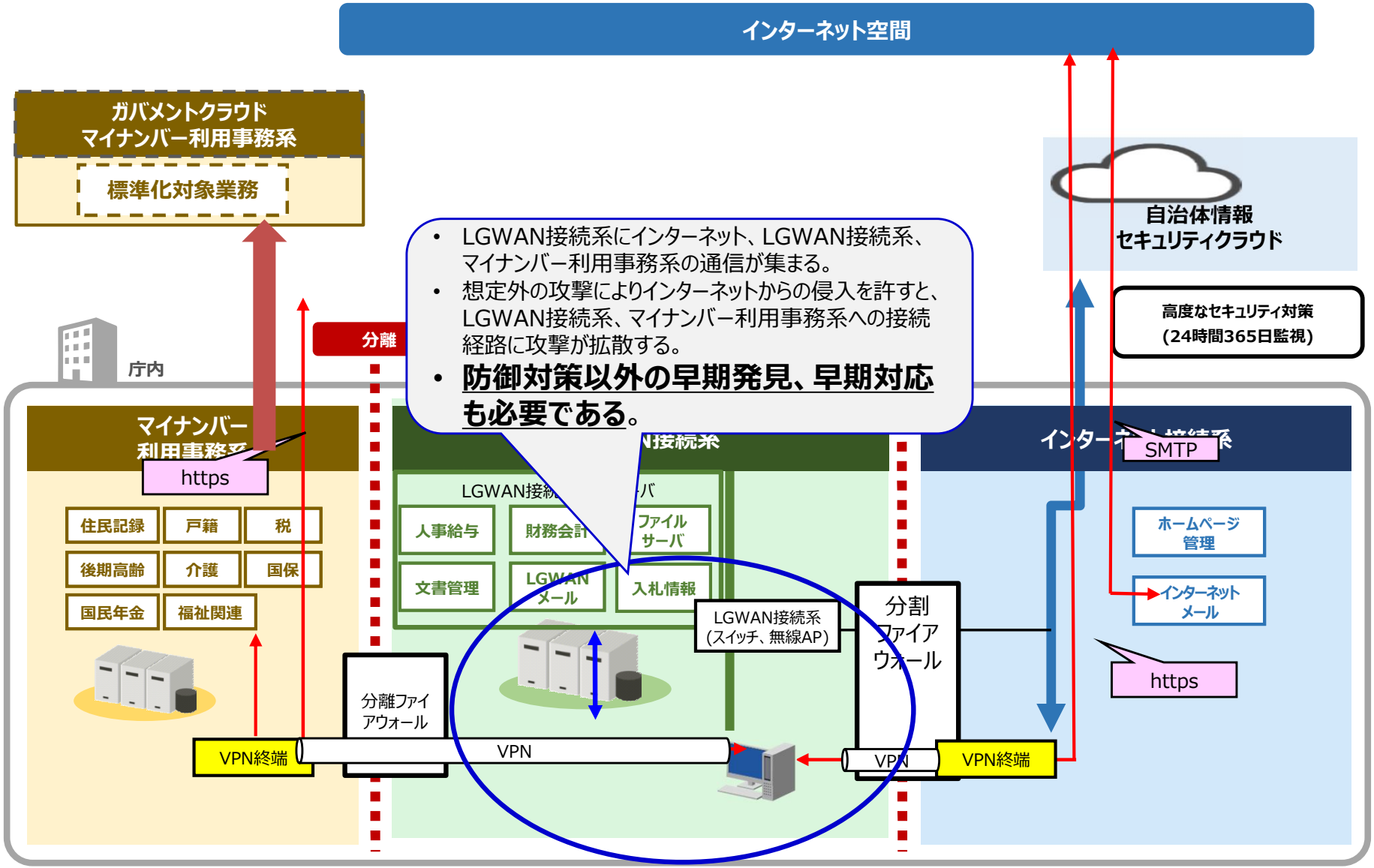
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**LGWAN接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系、マイナンバー利用事務系に影響が及ぶ。**

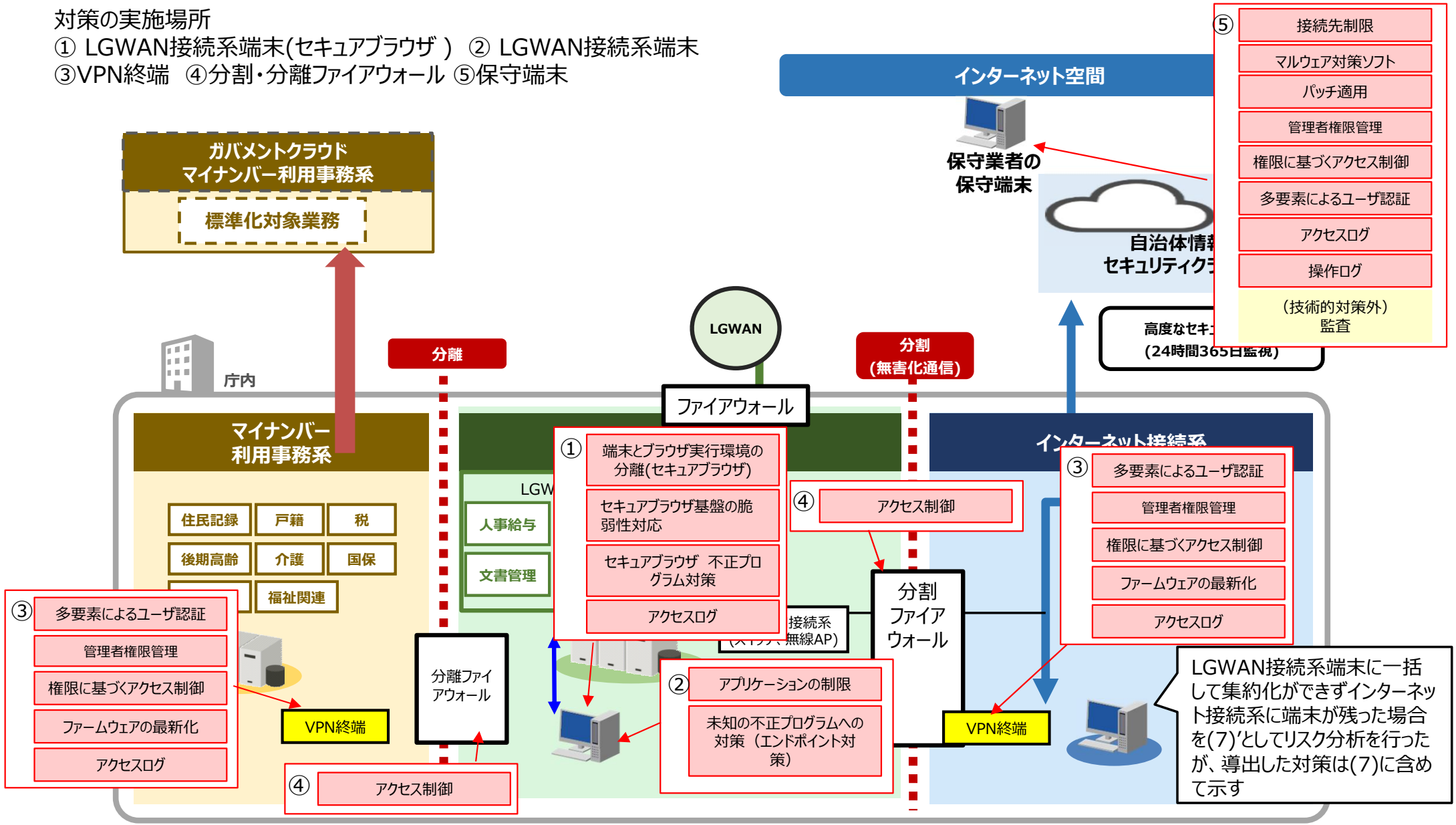
✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**



通信経路 (7) LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザの対策イメージ

- ✓ αモデルの対策を実施した上でLGWAN接続系からオンプレミス　セキュアブラウザに接続する方式。
- ✓ リスクアセスメント結果を踏まえると、**αモデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
① LGWAN接続系端末(セキュアブラウザ)　② LGWAN接続系端末
③VPN終端　④分割・分離ファイアウォール ⑤保守端末



通信経路 (7) LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザの技術的対策①

✓ LGWAN接続系端末からオンプレミス　セキュアブラウザ利用でのリスクアセスメントの結果を踏まえ必要な対策を示す。
※以下の対策の前に、αモデルの対策を実施することが前提であることに留意。αモデルの対策はガイドラインの第3編第2章の「3.情報システム全体の強靭性の向上」を参照のこと。

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
LGWAN接続系端末　セキュアブラウザでの対策			
画面転送機能	端末とブラウザ実行環境の分離対策により、ブラウザ実行環境上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
セキュアブラウザの選定	ディスク領域（ファイル・レジストリ）の分離、メモリ領域の分離（プロセス分離）、ローカルと分離環境間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性の対応、任意のプログラム実行禁止が可能なセキュアブラウザを選定する。		○
セキュアブラウザ基盤の脆弱性対応	セキュアブラウザ基盤の脆弱性にパッチを適用する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
セキュアブラウザでの不正プログラム対策	ブラウザ実行環境上で認可プログラムのみ実行を許可するなどにより、不正プログラム対策を行う。		○
アクセスログ	不正アクセス等による被害の防止等のため、セキュアブラウザのアクセスログを取得し、確認する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○
VPN終端での対策			
多要素によるユーザ認証	VPNのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　a　アクセス制御、b アクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　a　アクセス制御　の実施のための対策	○

通信経路 (7) LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザの技術的対策②

(1) 技術的対策（前項からの続き）

技術的対策		対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
VPN終端での対策（続き）					
	ファームウェア最新化	VPN終端の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	アクセスログ	不正アクセス等による被害の防止等のため、VPN終端のアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等の実施のための対策	○	
LGWAN接続系での対策（aモデルの対策以外のもの）					
	アクセス制限	接続元（LGWAN接続系端末）と接続先（マイナンバー利用事務系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
		接続元（LGWAN接続系端末）と接続先（インターネット接続系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
		インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○	
	アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、LGWAN接続系端末でのスクリーンショット機能を停止する。（注）			○

通信経路 (7) LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザの技術的対策③

(1) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
LGWAN接続系での対策（αモデルの対策以外のもの）				
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。（パッチ適用、マルウェア対策ソフトの導入についてはα'モデルにおける必須対策として規定）
スクリーンショット機能の停止の詳細は、P22を参照のこと

通信経路 (8)　インターネット接続系端末に１台化　オンプレミス　セキュアブラウザ
リスク分析結果を踏まえた技術的対策

- マイナンバー利用事務系への影響　P95
- 対策群のイメージ図　　P96
- 対策群
  - 今回のリスク分析を踏まえた対策　P97～99
  - 前提となるβモデルの対策　P100・101

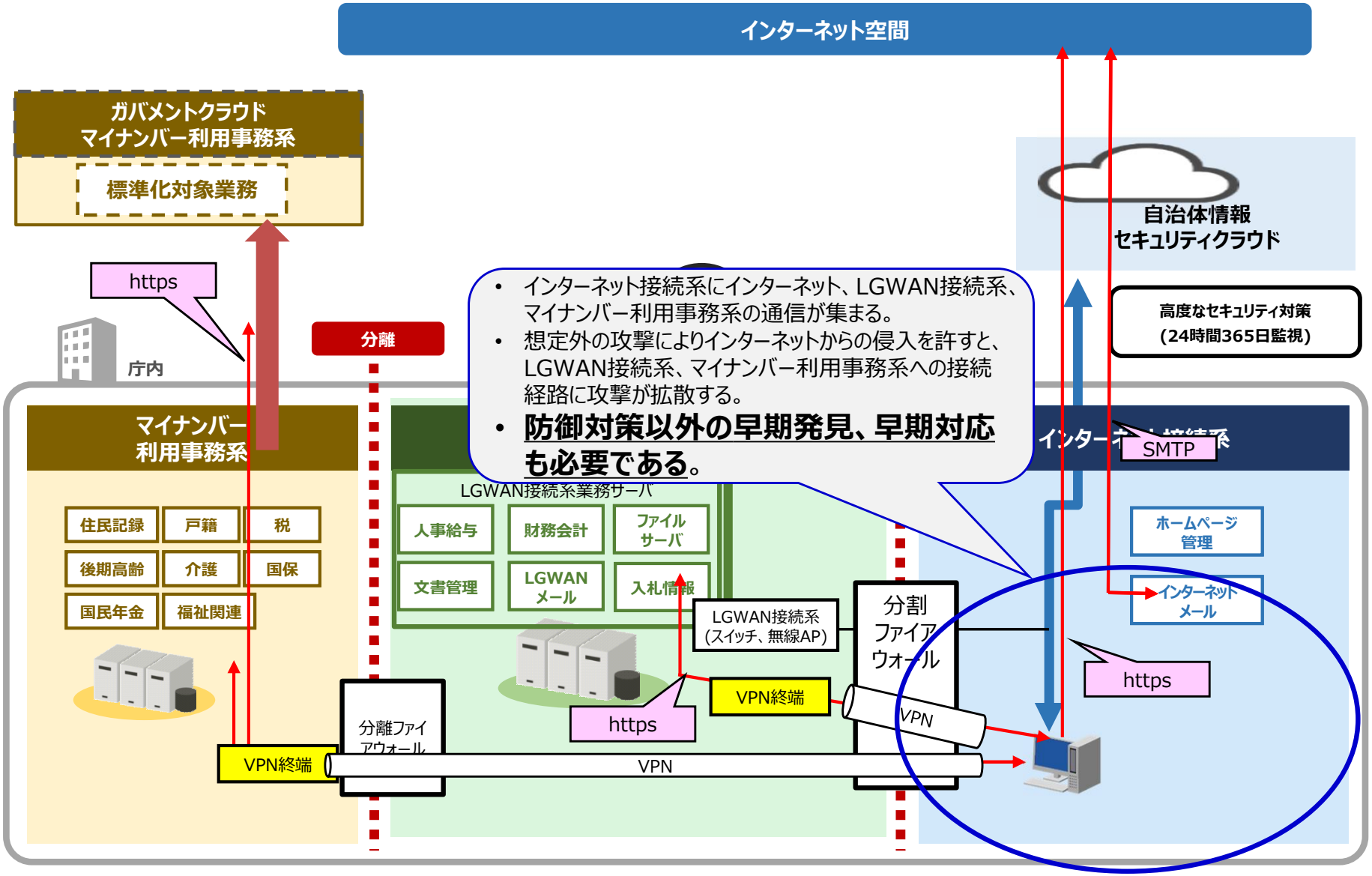
通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

マイナンバー利用事務系への影響

✓ 本構成は、**インターネット接続系にインターネット、LGWAN接続系、マイナンバー利用事務系の通信が集まるため、インターネットからの攻撃者の侵入を許した場合、LGWAN接続系、マイナンバー利用事務系に影響が及ぶ。**

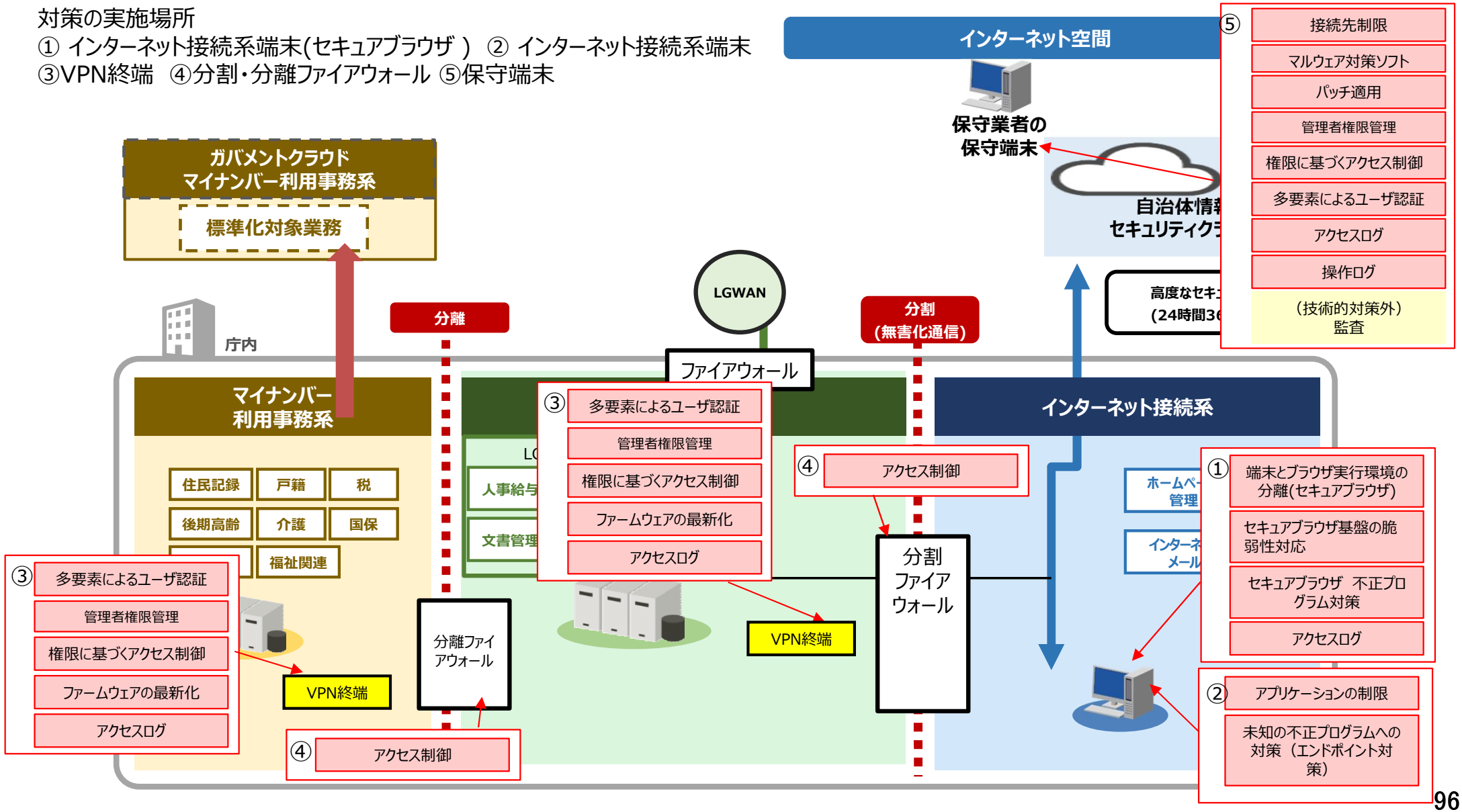
✓ マイナンバー利用事務系における情報資産の重要度を鑑み、**防御対策以外の早期発見、早期対応のための運用に係る対策も定義する。**



通信経路 (8) インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの対策イメージ

- ✓　インターネット接続系からオンプレミス　セキュアブラウザに接続する方式。
- ✓　インターネット接続系へのLGWAN接続系からの画面転送はβモデルとしてガイドラインに規定済。
- ✓　マイナンバー利用事務系からの画面転送を行うにあたり、リスクアセスメント結果を踏まえると、**βモデルの対策に、以下の図に示す対策を追加で実施**する必要がある。

対策の実施場所
① インターネット接続系端末(セキュアブラウザ) ② インターネット接続系端末
③VPN終端　④分割・分離ファイアウォール ⑤保守端末



通信経路 (8) インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの技術的対策①

✓ インターネット接続系端末からオンプレミス　セキュアブラウザ利用でのリスクアセスメントの結果を踏まえ必要な対策を示す。
※以下の対策の前に、βモデルの対策を実施することが前提であることに留意。。

(1) 技術的対策（次項に続く）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
インターネット接続系端末　セキュアブラウザでの対策			
画面転送機能	端末とブラウザ実行環境の分離対策により、ブラウザ実行環境上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。		○
セキュアブラウザの選定	ディスク領域（ファイル・レジストリ）の分離、メモリ領域の分離（プロセス分離）、ローカルと分離環境間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性の対応、任意のプログラム実行禁止が可能なセキュアブラウザを選定する。		○
セキュアブラウザ基盤の脆弱性対応	セキュアブラウザ基盤の脆弱性にパッチを適用する。	F.技術的安全管理措置 c不正アクセス等による被害の防止等　の実施のための対策	○
セキュアブラウザでの不正プログラム対策	ブラウザ実行環境上で認可プログラムのみ実行を許可するなどにより、不正プログラム対策を行う。		○
アクセスログ	不正アクセス等による被害の防止等のため、セキュアブラウザのアクセスログを取得し、確認する。	F.技術的安全管理措置 c不正アクセス等による被害の防止等 の実施のための対策	○
VPN終端での対策			
多要素によるユーザ認証	VPNのユーザや特権管理者について多要素認証を行う（「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証）。	F.技術的安全管理措置　ａアクセス制御、ｂアクセス者の識別と認証 の実施のための対策	○
管理者権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。		○
権限に基づくアクセス制御	権限に応じたアクセス制御を行う。	F.技術的安全管理措置　ａアクセス制御　の実施のための対策	○

通信経路 (8) インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの技術的対策②

(1) 技術的対策（前項からの続き）

技術的対策		対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
VPN終端での対策（続き）					
	ファームウェア最新化	VPN終端の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	F.技術的安全管理措置 c不正アクセス等による被害の防止等　の実施のための対策	○	
	アクセスログ	不正アクセス等による被害の防止等のため、VPN終端のアクセスログを取得し、確認する。事務取扱担当者及び事務取扱担当者の端末のみがアクセスしていることを確認する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し、F.技術的安全管理措置 c 不正アクセス等による被害の防止等の実施のための対策	○	
インターネット接続系での対策（βモデルの対策以外のもの）					
	アクセス制限	接続元（インターネット接続系端末）と接続先（マイナンバー利用事務系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○	
		接続元（インターネット接続系端末）と接続先（LGWAN接続系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○	
		インターネット接続系からマイナンバー利用事務系への通信を遮断する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等 の実施のための対策	○	
	アプリケーションの制限	マイナンバー利用事務系の住民個人情報が表示された転送画面を、手元の端末でスクリーンショットを撮って外部に漏えいすることを防止するため、インターネット接続系端末でのスクリーンショット機能を停止する。（注）			○

通信経路 (8) インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの技術的対策③

(1) 技術的対策（前項からの続き）

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須	推奨
インターネット接続系での対策（βモデルの対策以外のもの）				
未知の不正プログラムへの対策（エンドポイント対策）（注）	従来のパターンマッチング型の検知に加えて、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○	

注）故意による画面キャプチャ取得を防止するのであれば効果的であるが、マルウェア対策であれば、パッチ適用、マルウェア対策ソフトの導入、エンドポイント対策を実施する方が効果的である。（パッチ適用、マルウェア対策ソフトの導入についてはα'モデルにおける必須対策として規定）
スクリーンショット機能の停止の詳細は、P22を参照のこと

通信経路 (8)インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの前提条件となるβモデルの対策　①

✓通信経路(8)の対策の前提となる、βモデルの対策を示す（ガイドラインに既に規定）。

(1) 技術的対策

技術的対策		対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策				
	無害化処理	• 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、サニタイズ処理、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で危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。		○
	LGWAN接続系の画面転送	• インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 • LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。		○
	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、情報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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策		○

通信経路 (8)インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの前提条件となるβモデルの対策　②

(1) 技術的対策 (2)組織的・人的対策

技術的対策	対策の定義	「特定個人情報に関する安全管理措置（行政機関等編）」との関連	必須
技術的対策			
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。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
脆弱性管理	• OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、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する。	F.技術的安全管理措置 c 不正アクセス等による被害の防止等　の実施のための対策	○
組織的・人的対策			
組織的なセキュリティ対策基準の遵守	• インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。	C.組織的安全管理措置　e　取扱状況の把握及び安全管理措置の見直し　の実施のための対策	○
住民に関する情報をインターネット接続系に保存させない規定の整備	• 住民の名簿など、住民の個人情報（業務システムに保存されている場合は除く）をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。		○
本ガイドライン対策基準（例文）「１．組織体制（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 • 職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 • 職員等の実践的サイバー防御演習（CYDER）の受講 • 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 • 本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し	B 取扱規程等の見直し等　の実施のための対策 D.人的安全管理措置　b 事務取扱担当者等の教育　の実施のための対策	○

（参考）リスク分析について

総論

- リスク分析は、**「制御システムのセキュリティリスク分析ガイド　第２版　～セキュリティ対策におけるリスクアセスメントの実施と活用～」（2023年３月IPA）に沿って実施**。
- 本リスク分析は、情報処理安全確保支援士が、その倫理綱領に従い、公正な立場で実施したものである。
- セキュリティ対策については、マイナンバー利用事務系の情報資産の重要性に十分に考慮し、導出するものとする。
- マルウェアに感染してしまったことの事実公表による信用の失墜が最も重要な評価ポイントであるため、**資産の重要度の評価ポイントに、マイナンバー制度や地方公共団体への信頼が失墜することや、地方公共団体の業務に係るシステム、ネットワーク基盤が長期間停止することを入れている**。
- ガバメントクラウド自体に係るリスクの分析については対象としない。

「情報処理安全確保支援士倫理綱領」（2019年３月26日制定）（抄）
１．公正と誠実 情報処理安全確保支援士は、業務上の判断を行うにあたり、先入観をもたず、他者からの不当な影響を受けず、常に公正な立場を堅持し、公正・誠実に業務を遂行しなければならない。
※出典：情報処理安全確保支援士 倫理綱領制定委員会 2019年3月27日 制定

出典：「制御システムのセキュリティリスク分析ガイド第２版」（2023年３月　IPA）
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

画面転送に係る脅威

脅威レベルの考え

✓ リスクアセスメントには資産への脅威の大きさに応じた分析が必要。

脅威レベル	判断基準
3	・インターネットから直接、到達可能な脆弱性を突く攻撃や侵入行為、電子メールによる攻撃
2	・内部に侵入したマルウェアや攻撃者による内部の脆弱性を突く攻撃や侵入行為
2	・内部に侵入したマルウェアや攻撃者による内部拡散、リモートからの攻撃
1	・内部不正や隔離されたネットワークへの電子媒体を経由した攻撃
1	・物理的に区分、隔離された区域に不正に侵入した攻撃

脅威一覧

✓ 脅威とその脅威レベルを示す。
✓ 物理的な脅威はリスク分析の対象から外す。（グレー色）

脅威一覧（1/2)

脅威（攻撃手法）	説明	具体例	脅威レベル	備考
外部（インターネット経由）不正アクセス（悪意のある攻撃者の場合）	インターネット経由で機器に侵入し、攻撃を実行する。	・不正入手した認証情報の悪用（不正ログイン） ・認証機構を持たない機器への侵入 ・機器に内在する脆弱性の悪用 ・設定不備（不要プロセス動作や不要ポート開放等）の悪用	3	
外部（インターネット経由）不正アクセス（管理インタフェースへの攻撃者に侵入された管理端末）	インターネット経由で機器に侵入し、攻撃を実行する。	・不正入手した認証情報の悪用（不正ログイン） ・認証機構を持たない機器への侵入 ・機器に内在する脆弱性の悪用 ・設定不備（不要プロセス動作や不要ポート開放等）の悪用	2	
外部（インターネット経由）からのメール、Webアクセスによるマルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	・外部（インターネット経由）からのメールのマルウェア付き（不正プログラム）の添付ファイルを開封しマルウェアに感染 ・外部（インターネット経由）からのメールに記載された攻撃者が用意したサイトのURLをクリックしマルウェアに感染 ・OS、アプリが最新化でないLGWAN接続系端末から攻撃者に侵入されたWebサイトにアクセスしマルウェアに感染	3	情報窃取、情報改ざん、情報破壊、不正送信などはマルウェア感染の結果のため、脅威とはしない
高負荷攻撃	インターネット経由のDDoS 攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。 または容量以上の通信トラフィックを発生させ、輻輳状態とする。	・機器に対する大量データ送信 ・機器の脆弱性を悪用したサービス例外処理要求 ・DDoS攻撃により回線容量以上の通信トラフィックを発生させる	3	
プロセス不正実行	侵入したマルウェアが攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	・プログラム／コマンドの不正実行 ・サービスの不正起動	2	

脅威一覧

✓ 脅威とその脅威レベルを示す。
✓ 物理的な脅威はリスク分析の対象から外す。（グレー色）
✓ 第14回検討会での構成員からの指摘を踏まえ、委託先の保守端末での不正操作（保守端末に侵入した攻撃者も含む）をリスク分析の対象に追加した。

脅威一覧（2/2）

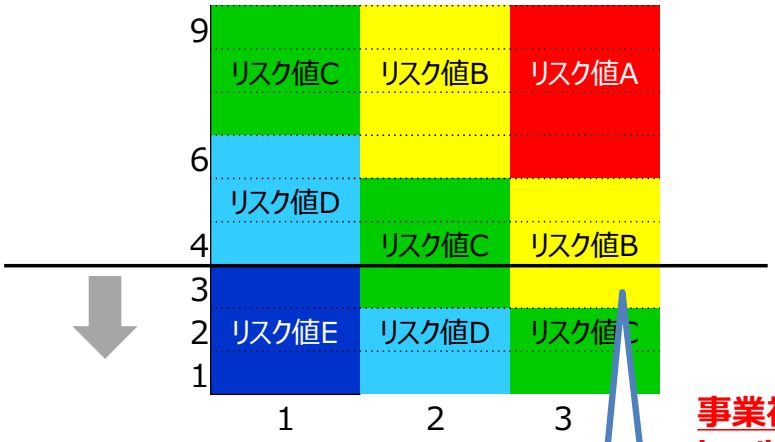
脅威（攻撃手法）	説明	具体例	脅威レベル	備考
侵入した攻撃者、マルウェアの拡散	侵入したマルウェアが内部ネットワークの機器を探索し、残存する脆弱性やファイル共有等を利用し、通信可能な機器、システムに侵入を広げ、攻撃する。 または、マルウェアに感染したファイルがWeb会議等で共有され拡散する。	・内部システムの機器に内在する脆弱性の悪用 ・共有ファイルの悪用 ・内部システムの設定不備（不要プロセス動作や不要ポート開放等）の悪用 ・メール等でマルウェアに感染後、C&Cサーバとの通信により攻撃の拡散 ・不正入手した認証情報の悪用（不正ログイン）	2	
物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。 あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	・敷地内／計器室／サーバ室への不正侵入 ・ラック／設置箱の不正開放	1	
不正操作 (保守端末のみを対象)	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	・不正入手した認証情報の悪用（不正ログイン） ・認証機構を持たない機器への侵入 ・機器に内在する脆弱性の悪用	1	
過失操作	内部関係者（社員や協力者のうち、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	・マルウェアに感染した正規媒体の持ち込み ・メール添付ファイル開封	1	
不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVD やUSB 機器等）を接続し、攻撃を実行する。	・不正媒体の接続 ・不正媒体からの読み込み／不正媒体への書き出し	1	
窃盗	機器を窃盗する。	・機器のネットワークからの切り離し、不正持出 ・保守用モバイル端末の盗み出し	1	
経路遮断	通信ケーブルを切断し、通信を遮断する。 あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	・サーバ室に不正侵入し通信ケーブルを切断 ・建屋に引き込む通信ケーブルを遮断	1	
無線妨害	無線通信を妨害する。	・妨害電波の送出	3	
盗聴	ネットワーク上を流れる情報を盗聴する。	・ネットワーク機器のモニタリング機能の悪用、またはトラフィックをモニタリング可能はネットワーク機器を回線上に挿入	1	
通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	・中間者攻撃によりクライアント-サーバ間の通信に割り込み、情報を改ざんする	1	
不正機器接続	ネットワーク上に不正機器を接続する。	・無許可のモバイル端末 不正接続 ・不正な無線中継器の設置	1	

事業被害ベースリスク分析

事業被害レベルとリスク値

✓　事業被害レベルと脅威レベル×脆弱性レベルから導くリスク値の考え方を示す。

脅威レベル×脆弱性レベル



脅威レベル×脆弱性レベルが3以下は対策の効果があり、「安全」と考える対象とする。

リスク値	意味
A	リスクが非常に高い。
B	リスクが高い。
C	リスクが中程度。
D	リスクが低い。
E	リスクが非常に低い。

脅威レベルが３の場合、脆弱性レベルを対策を行うことにより最小の１にしても、リスク値（脅威レベル×脆弱性レベル）は３になる。

脅威レベル	判断基準
3	・インターネットから直接、到達可能な脆弱性を突く攻撃や侵入行為、電子メールによる攻撃
2	・内部に侵入したマルウェアや攻撃者による内部の脆弱性を突く攻撃や侵入行為
2	・内部に侵入したマルウェアや攻撃者による内部拡散、リモートからの攻撃
1	・内部不正や隔離されたネットワークへの電子媒体を経由した攻撃
1	・物理的に区分、隔離された区域に不正に侵入した攻撃

対策レベルと脆弱性レベルの対応　（資産ベースのリスクアセスメントと一貫性を持たせるため同一）

対策レベル	判断基準	脆弱性レベル
3	当該脅威（攻撃手段）において、複数の「防御」「検知／被害把握」可能な対策項目を多層で実施しており、攻撃が成功する可能性は低い。（即ち、○が二つ以上）	1
2	当該脅威（攻撃手段）において、「防御」「検知／被害把握」可能な対策項目を実施している。 即ち、○が一つ以上ついているが、十分とは言えないため、攻撃が成功する可能性は中程度である。	2
1	当該脅威（攻撃手段）において、「防御」「検知／被害把握」可能な対策項目を実施していない。 即ち、○が一つもついておらず、攻撃が成功する可能性は高い。	3

事業被害レベル

事業被害レベル

評価値	評価基準
3	・資産が失われた、もしくは不正に操作された場合、事業上の被害大となる。 －マイナンバーの漏えい、毀損やマイナンバー利用事務系のシステムがマルウェア感染した場合、マイナンバー制度への信頼が失墜する －システムの停止がマイナンバー利用事務系の業務停止につながる －不正利用によりマイナンバー利用事務系の業務継続に支障をきたす
2	・資産が失われた、もしくは不正に操作された場合、事業上の被害中となる。 －マイナンバー利用事務系に影響はなく、LGWAN接続系、インターネット接続系の業務に一部、限定されるなどの支障をきたす
1	・資産が失われた、もしくは不正に操作された場合、事業上の被害小となる。 －マイナンバー利用事務系に影響はなく、他の業務にも情報漏えいなどはなく業務への影響はない

攻撃ツリー・攻撃ルート・攻撃シナリオ一覧の見方

✓ IPAが提供する攻撃ルートの検討フォーマット（攻撃ルート、最終攻撃を含む攻撃シナリオ、及び攻撃ツリー）の見方を示す。通信経路(1)攻撃ルート①を例示する。

攻撃ルート
攻撃のルートとその番号

事業被害レベルの出し方
- 攻撃ルートで脅威が攻撃対象に到達し、攻撃対象が最終攻撃に記載する被害を受けた時の事業被害の大きさを前項の判断基準に基づき決定する

攻撃ツリー

攻撃ルート

攻撃シナリオ

攻撃ツリー	誰が	攻撃ルート	どこから	どうやって							攻撃シナリオ	どこで		何をする	事業被害レベル
	攻撃者		侵入口	経由 1	経由 2	経由 3	経由 4	経由 5	経由 6	経由 7		攻撃拠点	攻撃対象	最終攻撃	
1	インターネットの悪意のある第三者のWebサイト	①	インターネット	インターネット	セキュリティクラウド接続ファイアウォール	分割ファイアウォール	LGWAN接続系(スイッチ、無線AP)	インターネット接続系DaaS(インターネットアクセス)(LBO 回線)	インターネット接続系DaaS(画面転送)(LBO 回線)	LGWAN接続系端末	1-1	インターネット接続系DaaS	LGWAN接続系端末	不正ソフトウェアが置かれたインターネットの不正サイトにインターネット接続系DaaSがアクセスし、インターネット接続系DaaSに不正ソフトウェアが侵入したことにより、インターネット接続系DaaSを利用するLGWAN接続系端末に拡散し、LGWAN接続系端末の操作権限、特権を攻撃者が乗っ取る。	2
2	インターネットの悪意のある第三者からのメール	①	インターネット	インターネット	インターネットメールサーバ	分割ファイアウォール	LGWAN接続系(スイッチ、無線AP)	インターネット接続系DaaS(インターネットアクセス)(LBO 回線)	インターネット接続系DaaS(画面転送)(LBO 回線)	LGWAN接続系端末	1-1	インターネット接続系DaaS	LGWAN接続系端末	インターネット接続系DaaSにてインターネットからのマルウェア付きのメールを開封し、インターネット接続系DaaSに不正ソフトウェアが侵入したことにより、インターネット接続系DaaSを利用するLGWAN接続系端末に拡散し、LGWAN接続系端末の操作権限、特権を攻撃者が乗っ取る。	2

攻撃ツリー
攻撃者、攻撃ルート、攻撃シナリオの横軸単位
攻撃ツリーの番号は、通番で付与

攻撃シナリオ番号
x-yの形式で攻撃シナリオに割り振った番号
xは最終攻撃の被害の単位（上記の場合、情報の外部への送信）で通番で付与
yはxの攻撃の違い（不正アクセスとマルウェア感染)、または攻撃拠点の違いで通番で付与

攻撃シナリオ
攻撃拠点、攻撃対象、最終攻撃でまとめた単位

事業被害ベースリスク分析シート

✓IPAが提供する事業被害ベースのリスク分析シートを示す。通信経路(1)攻撃ルート①を例示する。

攻撃ツリー/攻撃ステップ　：攻撃シナリオに含まれる攻撃拠点・攻撃対象・最終攻撃に加えて、攻撃シナリオを実現する侵入者・侵入口・経由を具体化した一連の攻撃手順
脅威レベル　：攻撃ツリー単位で「3.画面転送の脅威」で定義した脅威毎の脅威の大きさを示す
脆弱性レベル　：対策レベルに応じた攻撃ツリー全体での脆弱性のレベル
事業被害レベル　：想定した攻撃ツリーが行われた場合の被害範囲や会社経営上の打撃の大きさを表す
リスク値　：事業被害レベルと脅威レベル×脆弱性レベルから導くリスク値
対策レベル　：防御、検知/被害把握等の対策状況から判断基準に基づく対策のレベル
資産ベースのリスク分析と一貫性を持たせるため対策は同一
なお、丸付数字はリスク分析シートの各項目の設定の順番を示す（次項に続く）

項番	攻撃シナリオ 最終攻撃	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	対策レベル 攻撃ステップ	対策レベル 攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	攻撃ツリー番号 構成ステップ（項番）
1－1	LGWAN接続系端末の操作権限、特権を攻撃者が乗っ取る。（LGWAN接続系端末からα'モデルでマイナンバー利用事務系DaaS、インターネット接続系DaaSを利用）													
1	攻撃ツリー	【M】侵入口=インターネット接続系DaaS 不正ソフトウェアが置かれたインターネットの不正サイトにインターネット接続系DaaSがアクセスし、インターネット接続系DaaSに不正ソフトウェアが侵入する。					自治体情報セキュリティクラウドの保護 ○ 仮想端末での不正プログラム対策 ○ 仮想端末でのパッチ適用 ○ 画面転送機能(仮想端末と画面転送の分離) ○ クラウドサービス事業者によるDaaS基盤の脆弱性対応等 ○				3			
2	攻撃ステップ	インターネット接続系DaaSに侵入した不正ソフトウェアが接続するLGWAN接続系端末に画面転送通信の経路を利用し不正アクセスする。					不正プログラム対策 ○ パッチ適用 ○ 画面転送機能(仮想端末と画面転送の分離) ○				3			
3		LGWAN接続系端末に不正ソフトウェアが侵入し操作権限、特権を攻撃者が乗っ取る。	2	1	2	D	不正プログラム対策 ○ 画面転送機能(仮想端末と画面転送の分離) ○ 管理者権限管理 ○ 権限に基づくアクセス制御 ○				3	3	1	1,2,3

攻撃ｽﾃｯﾌﾟ番号
毎分析シート内で攻撃ステップ毎に通番で付与

①前述の攻撃ルート、シナリオの攻撃を具体化した手順を攻撃ツリー/攻撃ステップに記載

②攻撃ツリー単位で「 3.画面転送の脅威」で定義した脅威レベルを攻撃ステップの攻撃の脅威に応じて設定

③攻撃ツリー単位で想定した攻撃が行われたさいの事業被害レベルを設定

前述の攻撃シナリオの攻撃ツリー番号

攻撃ツリーの攻撃ｽﾃｯﾌﾟ番号

事業被害ベースリスク分析シート

✓IPAが提供する事業被害ベースのリスク分析シートを示す。

攻撃ツリー/攻撃ステップ　：攻撃シナリオに含まれる攻撃拠点・攻撃対象・最終攻撃に加えて、攻撃シナリオを実現する侵入者・侵入口・経由を具体化した一連の攻撃手順
脅威レベル　：攻撃ツリー単位で「 3.画面転送の脅威」で定義した脅威毎の脅威の大きさを示す
脆弱性レベル　：対策レベルに応じた攻撃ツリー全体での脆弱性のレベル
事業被害レベル　：想定した攻撃ツリーが行われた場合の被害範囲や会社経営上の打撃の大きさを表す
リスク値　：事業被害レベルと脅威レベル×脆弱性レベルから導くリスク値
対策レベル　：防御、検知/被害把握等の対策状況から判断基準に基づく対策のレベル
資産ベースのリスク分析と一貫性を持たせるため対策は同一
なお、丸付数字はリスク分析シートの各項目の設定の順番を示す（前項からの続き）

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	1－1	LGWAN接続系端末の操作権限、特権を攻撃者が乗っ取る。（LGWAN接続系端末からα'モデルでマイナンバー利用事務系DaaS、インターネット接続系DaaSを利用）												
1		【N】侵入口=インターネット接続系DaaS 不正ソフトウェアが置かれたインターネットの不正サイトにインターネット接続系DaaSがアクセスし、インターネット接続系DaaSに不正ソフトウェアが侵入する。					自治体情報セキュリティクラウドの保護 仮想端末での不正プログラム対策 仮想端末でのパッチ適用 画面転送機能(仮想端末と画面転送の分離) クラウドサービス事業者によるDaaS基盤の脆弱性対応等	○ ○ ○ ○ ○			3			
2		インターネット接続系DaaSに侵入した不正ソフトウェアが接続するLGWAN接続系端末に画面転送通信の経路を利用し不正アクセスする。					不正プログラム対策 パッチ適用 画面転送機能(仮想端末と画面転送の分離)	○ ○ ○			3			
3		LGWAN接続系端末に不正ソフトウェアが侵入し操作権限、特権を攻撃者が乗っ取る。	2	1	2	D	不正プログラム対策 画面転送機能(仮想端末と画面転送の分離) 管理者権限管理 権限に基づくアクセス制御	○ ○ ○ ○			3	3	1	1,2,3

④各攻撃ステップ毎に対策状況を設定し、対策レベルの判断基準に基づき対策のレベルを設定

⑤攻撃ツリー全体で対策レベルを判断基準に基づき設定

⑥対策レベルに応じた脆弱性レベルを算出

事業被害ベースリスク分析シート

✓IPAが提供する事業被害ベースのリスク分析シートを示す。

攻撃ツリー/攻撃ステップ　：攻撃シナリオに含まれる攻撃拠点・攻撃対象・最終攻撃に加えて、攻撃シナリオを実現する侵入者・侵入口・経由を具体化した一連の攻撃手順
脅威レベル　：攻撃ツリー単位で「 3.画面転送の脅威」で定義した脅威毎の脅威の大きさを示す
脆弱性レベル　：対策レベルに応じた攻撃ツリー全体での脆弱性のレベル
事業被害レベル　：想定した攻撃ツリーが行われた場合の被害範囲や会社経営上の打撃の大きさを表す
リスク値　：事業被害レベルと脅威レベル×脆弱性レベルから導くリスク値
対策レベル　：防御、検知/被害把握等の対策状況から判断基準に基づく対策のレベル
資産ベースのリスク分析と一貫性を持たせるため対策は同一
なお、丸付数字はリスク分析シートの各項目の設定の順番を示す（前項からの続き）

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	1－1	LGWAN接続系端末の操作権限、特権を攻撃者が乗っ取る。（LGWAN接続系端末からα'モデルでマイナンバー利用事務系DaaS、インターネット接続系DaaSを利用）												
1		【N】侵入口=インターネット接続系DaaS 不正ソフトウェアが置かれたインターネットの不正サイトにインターネット接続系DaaSがアクセスし、インターネット接続系DaaSに不正ソフトウェアが侵入する。					自治体情報セキュリティクラウドの保護 仮想端末での不正プログラム対策 仮想端末でのパッチ適用 画面転送機能(仮想端末と画面転送の分離) クラウドサービス事業者によるDaaS基盤の脆弱性対応等	○ ○ ○ ○ ○			3			
2		インターネット接続系DaaSに侵入した不正ソフトウェアが接続するLGWAN接続系端末に画面転送通信の経路を利用し不正アクセスする。					不正プログラム対策 パッチ適用 画面転送機能(仮想端末と画面転送の分離)	○ ○ ○			3			
3		LGWAN接続系端末に不正ソフトウェアが侵入し操作権限、特権を攻撃者が乗っ取る。	2	1	2	D	不正プログラム対策 画面転送機能(仮想端末と画面転送の分離) 管理者権限管理 権限に基づくアクセス制御	○ ○ ○ ○			3	3	1	1,2,3

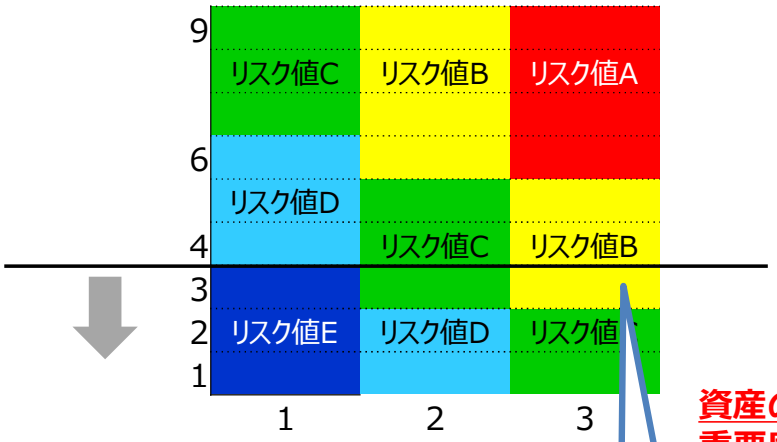
⑦脅威レベル、脆弱性レベルと事業被害レベルからリスク値を算出

資産ベースリスク分析

資産の重要度とリスク値

✓資産の重要度と脅威レベル×脆弱性レベルから導くリスク値の考え方を示す。

脅威レベル×脆弱性レベル



脅威レベル×脆弱性レベルが3以下は対策の効果があり、「安全」と考える対象とする。

リスク値	意味
A	リスクが非常に高い。
B	リスクが高い。
C	リスクが中程度。
D	リスクが低い。
E	リスクが非常に低い。

資産の重要度

脅威レベル	判断基準
3	・インターネットから直接、到達可能な脆弱性を突く攻撃や侵入行為、電子メールによる攻撃
2	・内部に侵入したマルウェアや攻撃者による内部の脆弱性を突く攻撃や侵入行為
2	・内部に侵入したマルウェアや攻撃者による内部拡散、リモートからの攻撃
1	・内部不正や隔離されたネットワークへの電子媒体を経由した攻撃
1	・物理的に区分、隔離された区域に不正に侵入した攻撃

対策レベルと脆弱性レベルの対応

対策レベル	判断基準	脆弱性レベル
3	当該脅威（攻撃手段）において、複数の「防御」「検知／被害把握」可能な対策項目を多層で実施しており、攻撃が成功する可能性は低い。（即ち、○が二つ以上）	1
2	当該脅威（攻撃手段）において、「防御」「検知／被害把握」可能な対策項目を実施している。 即ち、○が一つ以上ついているが、十分とは言えないため、攻撃が成功する可能性は中程度である。	2
1	当該脅威（攻撃手段）において、「防御」「検知／被害把握」可能な対策項目を実施していない。 即ち、○が一つもついておらず、攻撃が成功する可能性は高い。	3

資産の重要度

評価値	評価基準
3	・マイナンバーの漏えい、毀損やマイナンバー利用事務系のシステムがマルウェア感染した場合、マイナンバー制度への信頼が失墜する ・LGWAN接続系、インターネット接続系のシステムからの情報の漏えいや情報の毀損、システムがマルウェア感染した場合、地方公共団体への信頼が失墜する ・システム、ネットワークの基盤が攻撃されマルウェア感染、設定の改ざんなどの攻撃をされた場合、地方公共団体の業務に係るシステム、ネットワーク基盤が長期間停止する
2	・マルウェア感染、侵入などの攻撃をされた場合、地方公共団体の業務に係るシステムが一定期間停止する
1	・資産が攻撃された場合、システム停止が短期間、または代替が可能である ・資産が攻撃された場合、住民サービスに影響がない、業務影響が限定的である

脅威レベルが３の場合、脆弱性レベルを対策を行うことにより最小の１にしても、リスク値（脅威レベル×脆弱性レベル）は３になる。

資産ベースリスク分析シート

✓IPAが提供する資産ベースのリスク分析シートを示す。通信経路(1)を例示する。

脅威レベル　：「 3.画面転送の脅威」で定義した脅威毎の脅威の大きさを示す
脆弱性レベル　：対策レベルに応じた資産の脆弱性のレベル
資産の重要度　：「 2.画面転送の資産の重要度」で定義した資産の重要度の判断基準に基づく各資産の重要度
リスク値　：資産の重要度と脅威レベル×脆弱性レベルから導くリスク値
脅威　：対象の資産に想定される脅威
対策レベル　：防御、検知/被害把握等の対策状況から判断基準に基づく対策のレベル
なお、丸付数字はリスク分析シートの各項目の設定の順番を示す（次項に続く）

②「3.画面転送の脅威」で定義した脅威レベルを脅威に応じて設定

①「2.画面転送の資産」で定義した資産の重要度を設定

③脅威毎に対策を洗い出し、資産と脅威の関係から有効な対策を選択し、○を設定。その対策数（○がついた対策）から、前項の対策レベルの判断基準に基づき、脅威への対策レベルを設定

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策						対策レベル
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			防御				検知/被害把握	事業継続	脅威毎
									侵入/拡散段階		目的遂行段階				
1	マイナンバー利用事務系資産	マイナンバー利用事務系DaaS	3	1	3	B	外部（インターネット経由）不正アクセス（悪意のある攻撃者）	・不正入手した認証情報の悪用（不正ログイン） ・認証機構を持たない機器への侵入 ・機器に内在する脆弱性の悪用 ・設定不備（不要プロセス動作や不要ポート開放等）の悪用	多要素によるユーザ認証	○					3
									管理者権限管理	○					
									仮想端末でのパッチ適用	○					
									権限に基づくアクセス制御	○					
									LGWAN接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限	○					
									クラウドサービス事業者によるDaaS基盤の脆弱性対応等	○					

（参考）各攻撃手法と対策について

- ✓ 「制御システムのセキュリティリスク分析ガイド　第２版　～セキュリティ対策におけるリスクアセスメントの実施と活用～」（2023年３月IPA）では以下のとおり攻撃手法と対策の例が示されている。
- ✓ このような例を参考にしつつ、各攻撃手法に有効と考えられる対策を「対策」欄に記入する。

表 4-15 資産（機器）に対する脅威（攻撃手法）

#	脅威（攻撃手法）	説明	具体例
1	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	● 不正入手した認証情報の悪用（不正ログイン） ● 認証機構を持たない機器への侵入 ● 機器に内在する脆弱性の悪用 ● 設定不備（不要プロセス動作や不要ポート開放等）の悪用
2	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。 あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	● 敷地内／計器室／サーバ室への不正侵入 ● ラック／設置箱の不正開放
3	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	● 不正入手した認証情報の悪用（不正ログイン） ● 認証機構を持たない機器への侵入 ● 機器に内在する脆弱性の悪用
4	過失操作	内部関係者（社員や協力者のうち、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	● マルウェアに感染した正規媒体の持ち込み ● メール添付ファイル開封
5	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVD や USB 機器等）を接続し、攻撃を実行する。	● 不正媒体の接続 ● 不正媒体からの読み込み／不正媒体への書き出し
6	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	● プログラム／コマンドの不正実行 ● サービスの不正起動
7	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	

表 4-33 脅威（攻撃手法）と技術的対策／物理的対策の候補一覧（1/3）

#	資産（機器）に対する脅威（攻撃手法）	技術的／物理的対策候補			
		防御		検知／被害把握	事業継続
		初期侵入段階／内部侵攻・拡散段階	目的遂行段階		
1	不正アクセス	・FW（パケットフィルタリング型）[1] ・FW（アプリケーションゲートウェイ型）[2] ・一方向ゲートウェイ [3] ・プロキシサーバ [4] ・WAF [11] ・通信相手の認証 [7] ・IPS／IDS [5] ・パッチ適用 [15] ・脆弱性回避 [16]		・IPS/IDS [5] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	
2	物理的侵入	・入退管理 [43] ・施錠管理 [46]		・監視カメラ [44] ・侵入センサ [45]	
3	不正操作	・操作者認証 [18]			
4	過失操作	・URL フィルタリング／Web レピュテーション [12] ・メールフィルタリング [13]			
5	不正媒体・機器接続	・デバイス接続・利用制限 [19]	・デバイス接続・利用制限 [19]	・デバイス接続・利用制限 [19] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	
6	プロセス不正実行	・権限管理 [23] ・アクセス制御 [24] ・重要操作の承認 [20]	・権限管理 [23] ・アクセス制御 [24] ・重要操作の承認 [20]	・機器異常検知 [34] ・機器死活監視 [33] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	

資産ベースリスク分析シート

✓IPAが提供する資産ベースのリスク分析シートを示す。

脅威レベル　：「 3.画面転送の脅威」で定義した脅威毎の脅威の大きさを示す
脆弱性レベル　：対策レベルに応じた資産の脆弱性のレベル
資産の重要度　：「2.画面転送の資産の重要度」で定義した資産の重要度の判断基準に基づく各資産の重要度
リスク値　：資産の重要度と脅威レベル×脆弱性レベルから導くリスク値
脅威　：対象の資産に想定される脅威
対策レベル　：防御、検知/被害把握等の対策状況から判断基準に基づく対策のレベル
なお、丸付数字はリスク分析シートの各項目の設定の順番を示す（前項からの続き）

④対策レベルに応じた脆弱性レベルを算出

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	マイナンバー利用事務系資産	マイナンバー利用事務系DaaS	3	1	3	B	外部（インターネット経由）不正アクセス（悪意のある攻撃者）	・不正入手した認証情報の悪用（不正ログイン） ・認証機構を持たない機器への侵入 ・機器に内在する脆弱性の悪用 ・設定不備（不要プロセス動作や不要ポート開放等）の悪用	多要素によるユーザ認証	○							3
									管理者権限管理	○							
									仮想端末でのパッチ適用	○							
									権限に基づくアクセス制御	○							
									LGWAN接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限	○							
									クラウドサービス事業者によるDaaS基盤の脆弱性対応等	○							

⑤脅威レベル、脆弱性レベルと資産の重要度からリスク値を算出