資料２

マイナンバー利用事務系の画面転送に係るリスク分析について

総 務 省

令和６年11月27日

ご意見と対応

✓ 前回の検討会、及び検討会後に構成員より意見をいただいた。

項番	ご意見	対応
1	・本リスク分析を踏まえた対策を実施しても、リスク分析で想定しえなかった攻撃を受ける可能性があることに留意すべき。 ・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ことと、他のネットワーク系統との間の通信を通すことで、攻撃を受け情報が漏洩するリスクが増大することに留意すべき。	・リスク分析の画面転送の機能の前提事項として、左記留意点をスライド２はじめに」に明記した。
2	・メンテナンス業者の端末等にもリスクが伴うため、その点を認識してリスク評価すること。	・メンテナンス業者の端末がマルウェア感染することを脅威に加え、リスク分析を行う。
3	・仮想端末自体は使いっぱなしではなく、週に1回ぐらいリフレッシュする、真っさらの端末に戻すことが必要。	・リスク分析の画面転送の機能の前提事項として、リフレッシュすることをスライド2「はじめに」に明記した。
4	・基盤自体のパッチ、脆弱性管理を認識してリスク評価すること。	・リスク分析するさいの対策に基盤へのパッチ適用を入れているため、求める対策に明記される。
5	・コピー＆ペーストの禁止（１方向なのか双方向なのかは議論）。 ・ファイル転送の禁止（１方向なのか双方向なのかは議論）。	・リスク分析の画面転送の機能の前提事項として、クリップボード、プリンター、ディスクドライブ等、仮想端末と手元の端末で共有を制限することをスライド2「はじめに」に明記した。
	・マイナンバー利用事務系ではコピペ不可設定をすることは必須とすべき。	
6	・オンプレミスでなくなり、より多くの端末からマイナンバー情報の閲覧ができるようになることが予想され、「スマホによる撮影」のリスクが増大する懸念がある。	・「マイナンバー利用事務系の画面転送・無線LAN利用に係る対策と番号法関係規定との対応」において無線LANには事務取扱担当者の端末のみに接続を制限。 ・リスク分析の対策に多要素認証により限定した者のみにアクセスを制限する対策を入れているため、求める対策に明記される。
7	・「画面転送」は通信路暗号化されているのか。	・リスク分析の画面転送の機能の前提事項として、画面転送は暗号化通信することをスライド2「はじめに」に明記した。
8	・自治体において「資産の重要度の評価基準」業務継続の観点はもちろん重要だが、以下が最も重要な評価ポイントであると考えられる。 － 個人情報の漏洩/毀損による政府への信頼の失墜。 また、マルウェア感染そのものは脅威ではなく、「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（情報漏洩などの被害の有無に関わらず）」が最も重要な評価ポイントであると考えられる。	・リスク分析における資産の重要度の基準の見直しを実施。

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。**
- **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。**

技術的な留意点

全パターン共通

- **クリップボード、プリンター、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
  - 仮想端末側から手元の端末に接続するプリンタに印刷できないよう制限する
- **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、手元の端末から画面転送機能を利用する度にリロードされ、再構築される（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）ようにする。**
- 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ーの方式となるが、**通信の盗聴、改ざん防止のため、暗号通信を行うことを前提とする。**

個別の観点

- **LGWAN接続系からローカルブレイクアウトによりクラウドのDaaSを利用する場合は、α'モデルとなるため、ガイドラインに記載する（ウ）のパターンの対策を行うことを前提とする。**
- **インターネット接続系の端末からLGWAN接続系の業務サーバに画面転送のDaaSを利用してアクセスする構成は、βモデルとみなせる。そのため、βモデルの対策を行うことを前提とする。**

リスク分析の前提

✓ その他、リスク分析における前提・考慮事項は以下のとおり。

■ 「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、情報処理安全確保支援士が、その倫理綱領に従い、公正な立場でリスクアセスメントを実施する。

■ 「国・地方の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」の報告書(2024年5月31日公開）の「Ⅲ 新たな国・地方のネットワークの将来像とそれを実現するための方策」において、「国・地方の職員が、セキュリティを確保しつつ、一人一台の端末で効率的に業務ができ、テレワーク等の柔軟な働き方が可能であること」と、端末１台化ついて言及されている。そのため、１台の LGWAN接続系端末又は、インターネット接続系端末から、マイナンバー利用事務系のシステムのみではなく、インターネット接続系、LGWAN接続系にもアクセスする。その実現のため、画面転送によるアクセス構成を検討し、リスク分析を行い必要な対策を明確化することを目的としている。

→ **端末１台化に伴い、マイナンバー利用事務系、LGWAN接続系、インターネット接続系で共通の通信経路が生じる**ため、**LGWAN接続系やインターネット接続系で発生したインシデントが、マイナンバー利用事務系も影響を及ぼす**ことを考慮する。

→ 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。

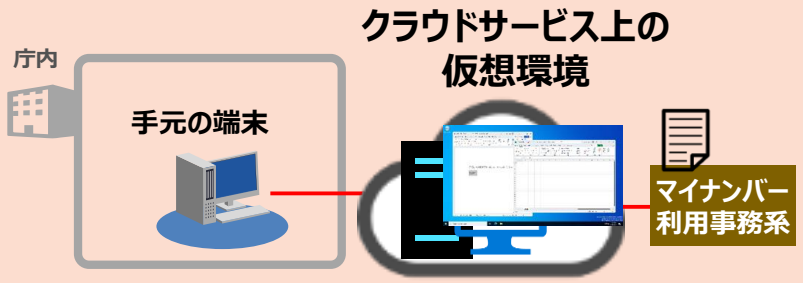
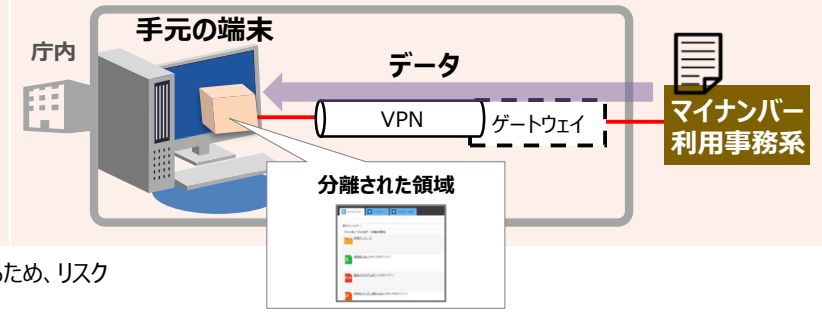
■ マルウェアに感染してしまったことの事実公表による**信用の失墜が最も重要な評価ポイント**であるため、資産の重要度の評価ポイントに、マイナンバー制度や地方公共団体への信頼が失墜することや、地方公共団体の業務に係るシステム、ネットワーク基盤が長期間停止することを入れている。

■ 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。

端末仮想化の方式

✓ 標準化対象業務がガバメントクラウドにリフトされることを受け、従前から利用されているオンプレミス型の仮想デスクトップ導入に加え、ガバメントクラウドのCSP（クラウドサービスプロバイダ）が提供するDaaSを検討する団体が増えている点に考慮し、**DaaSをリスク評価の対象に加える**。

画面転送で利用が想定されるさ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 ※サーバー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。

接続要件

✓ 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評価を行う。

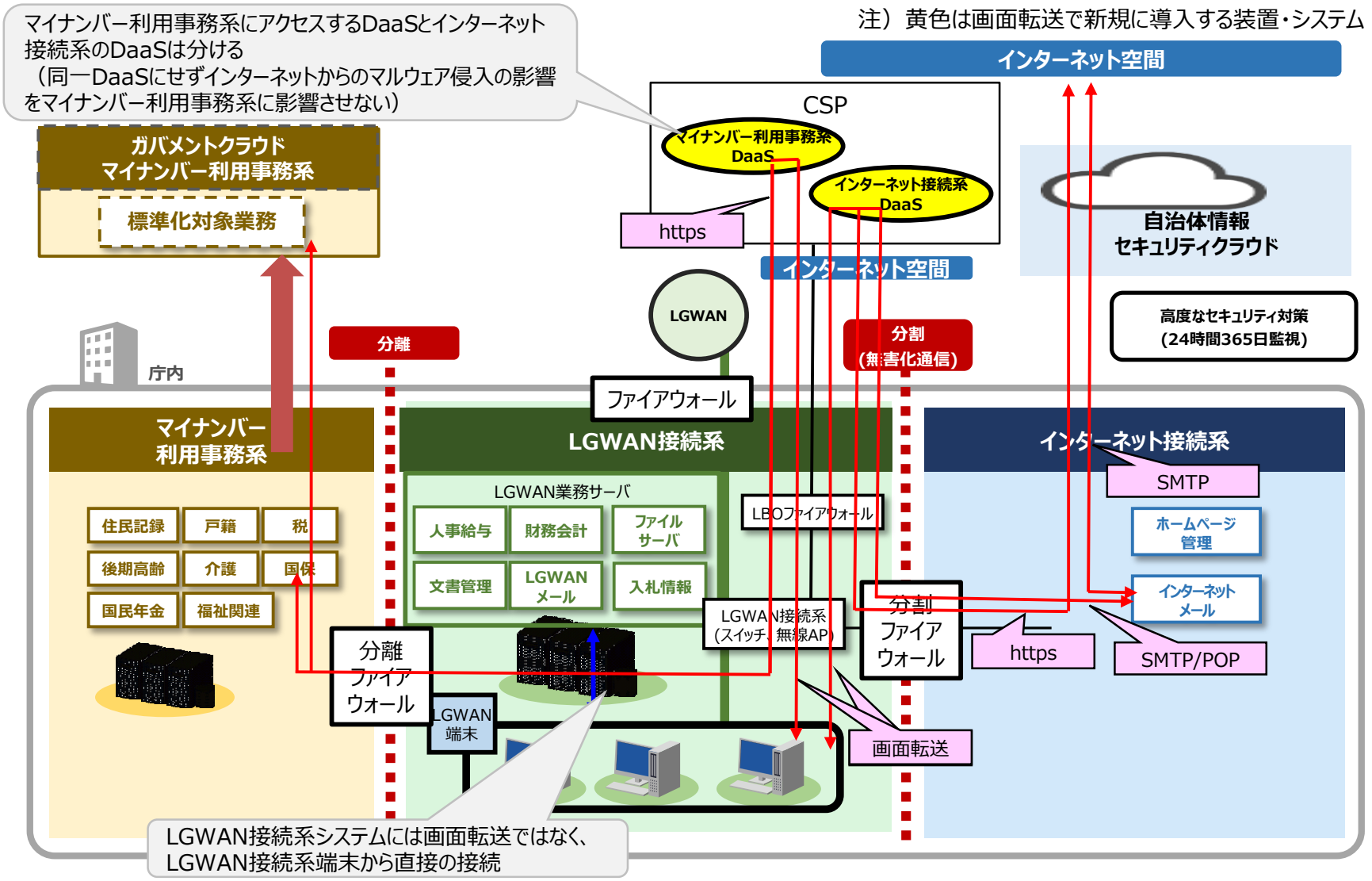
通信経路のパターン 赤枠はリスク分析実施済の通信経路

	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

1.画面転送のデータフロー

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用

- ✓ LGWAN接続系端末からDaaS経由でガバメントクラウド、マイナンバー利用事務系、インターネットにアクセス時のリスク分析の通信経路を示す。
- ✓ 本構成は、LGWAN接続系からローカルブレイクアウトでDaaSを利用することから、α'モデルである。そのため、α'モデルの対策を行うことを前提とする。

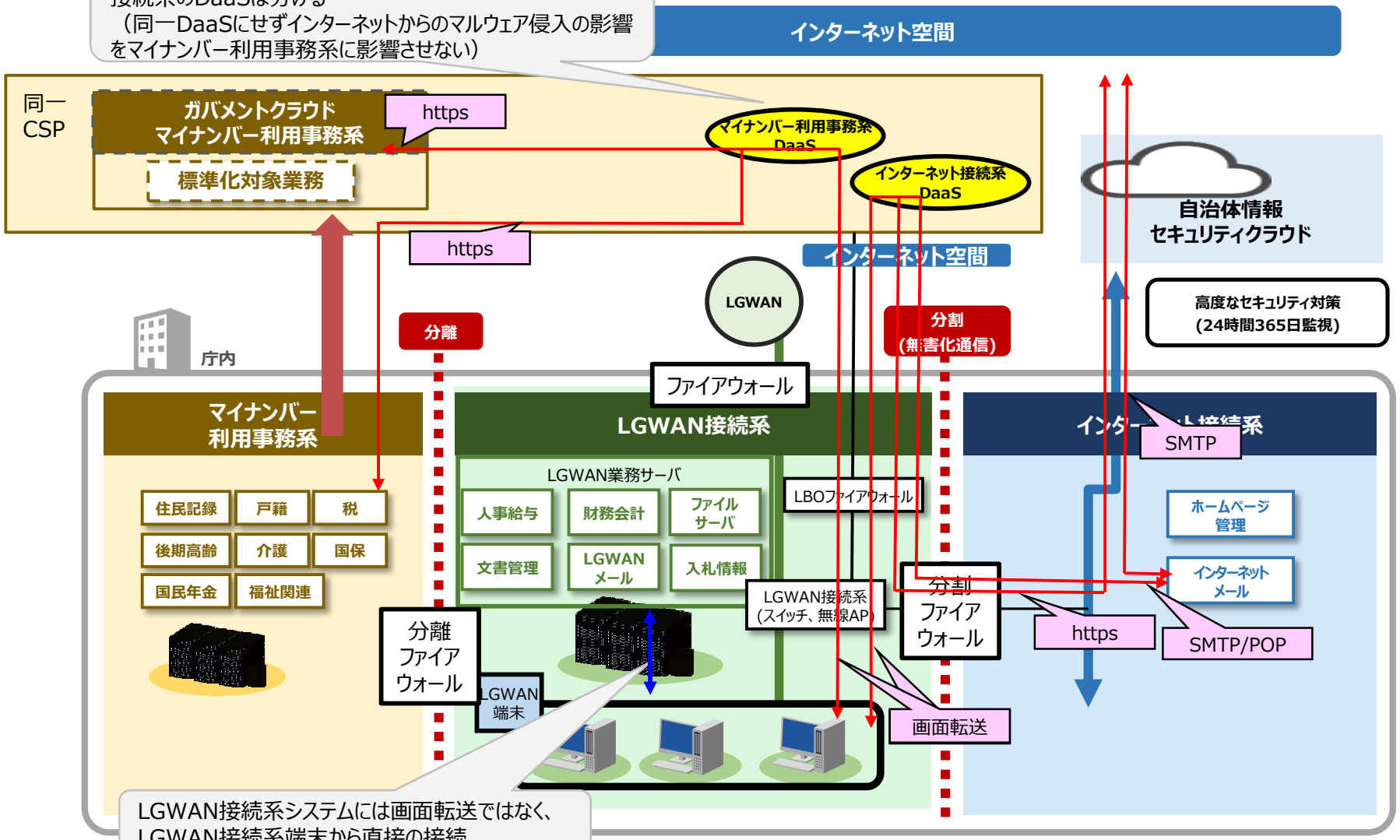


通信経路 (2) LGWAN接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)

- ✓ ガバメントクラウド、DaaSが同一CSPに実装時、LGWAN接続系端末からDaaS経由でインターネット接続、マイナンバー利用事務系にアクセス時のリスク分析の通信経路を示す。
- ✓ 本構成は、LGWAN接続系からLローカルブレイクアウトでDaaSを利用することから、α'モデルである。そのため、α'モデルの対策を行うことを前提とする。

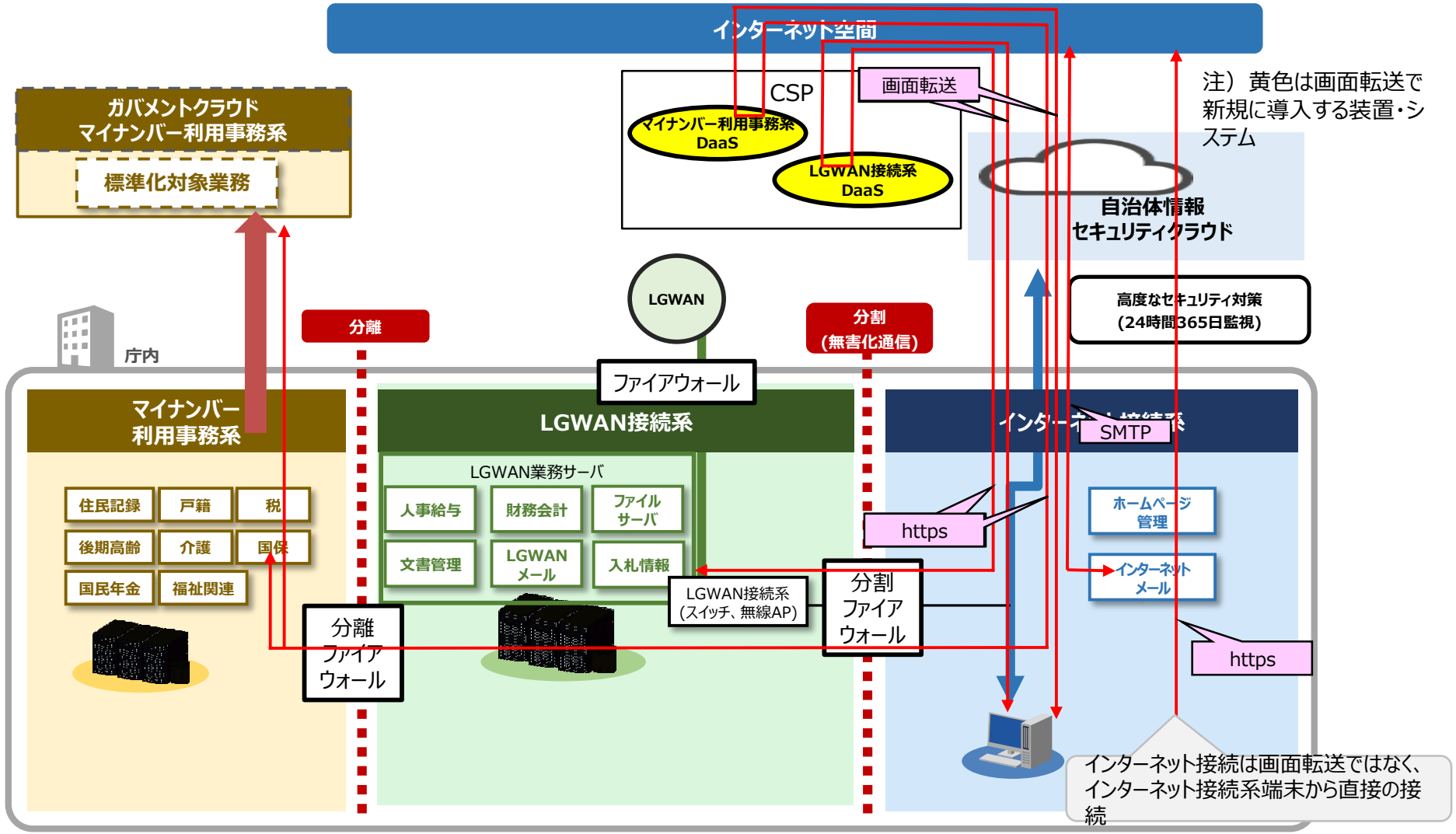
マイナンバー利用事務系にアクセスするDaaSとインターネット接続系のDaaSは分ける
（同一DaaSにせずインターネットからのマルウェア侵入の影響をマイナンバー利用事務系に影響させない）

注）黄色は画面転送で新規に導入する装置・システム



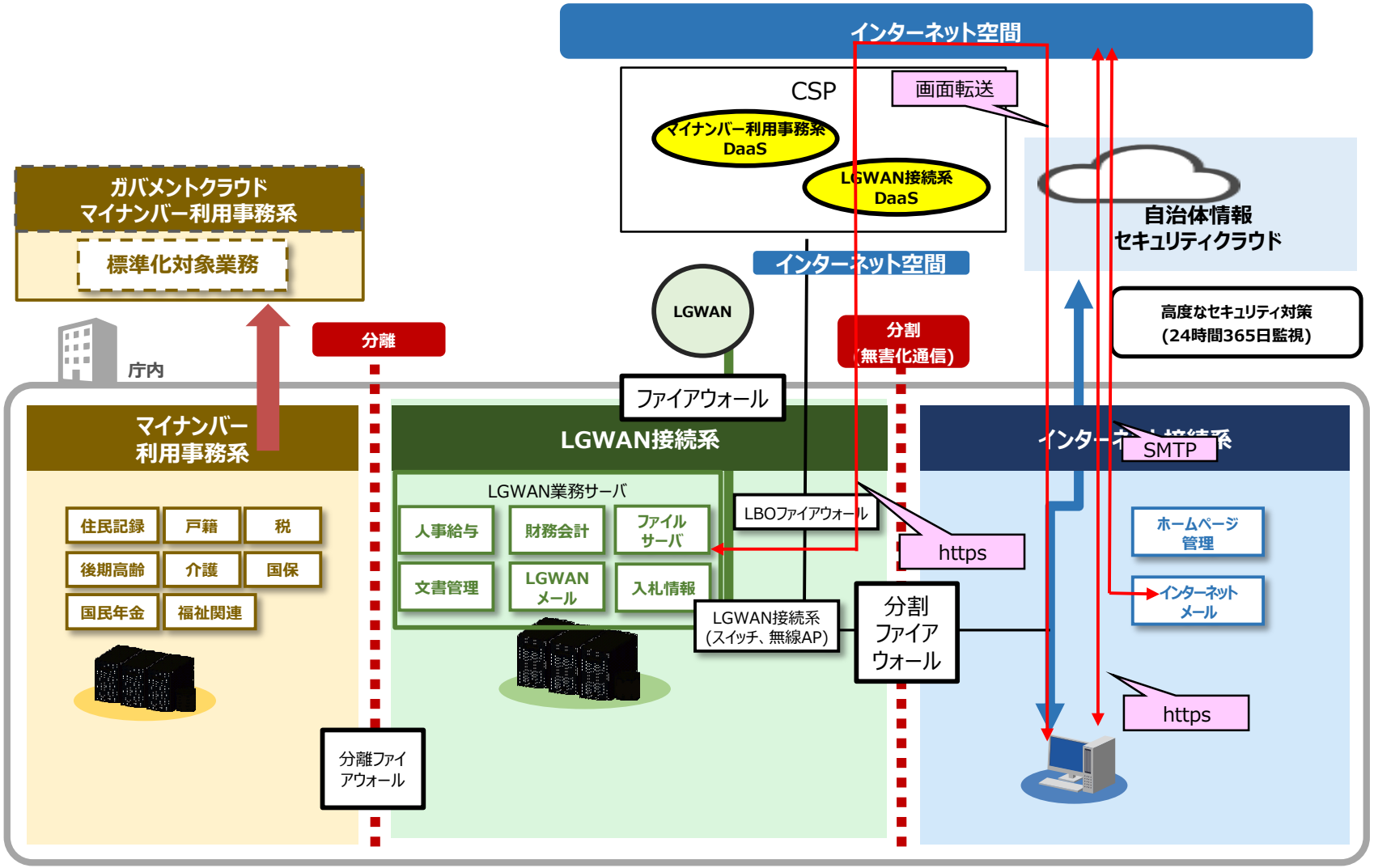
通信経路 (3) インターネット接続系端末に１台化　DaaS利用

- ✓ インターネット接続系端末からDaaS経由でガバメントクラウド、マイナンバー利用事務系、LGWAN接続系にアクセス時のリスク分析の通信経路を示す。
- ✓ 本構成は、インターネット接続系の端末からLGWAN接続系の業務サーバに画面転送のDaaSを利用してアクセスすることから、βモデルとみなせる。そのため、βモデルの対策を行うことを前提とする。



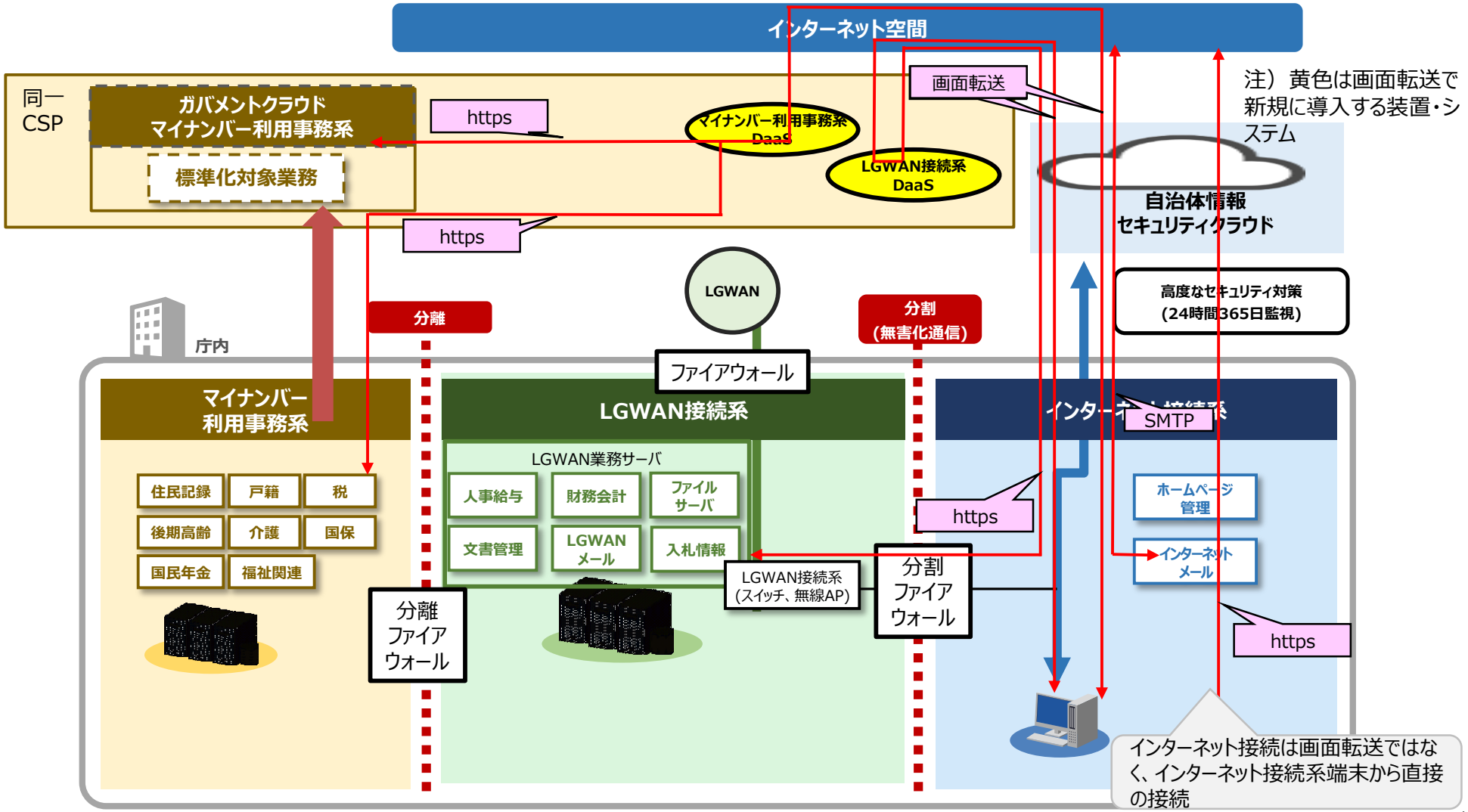
通信経路 (3)’インターネット接続系PCに１台化　DaaS利用
LGWAN接続系　α’モデルで接続

- ✓ インターネット接続系端末からDaaS利用におけるガバメントクラウド、マイナンバー利用事務系、LGWAN接続系(α’モデル接続）へのアクセス経路での脅威を示す。
- ✓ 本構成はLGWAN業務サーバにはLGWAN接続系からのローカルブレイクアウトでアクセスする。
- ✓ α’モデル、βモデルの対策を実施し安全性を担保していることを前提とする。



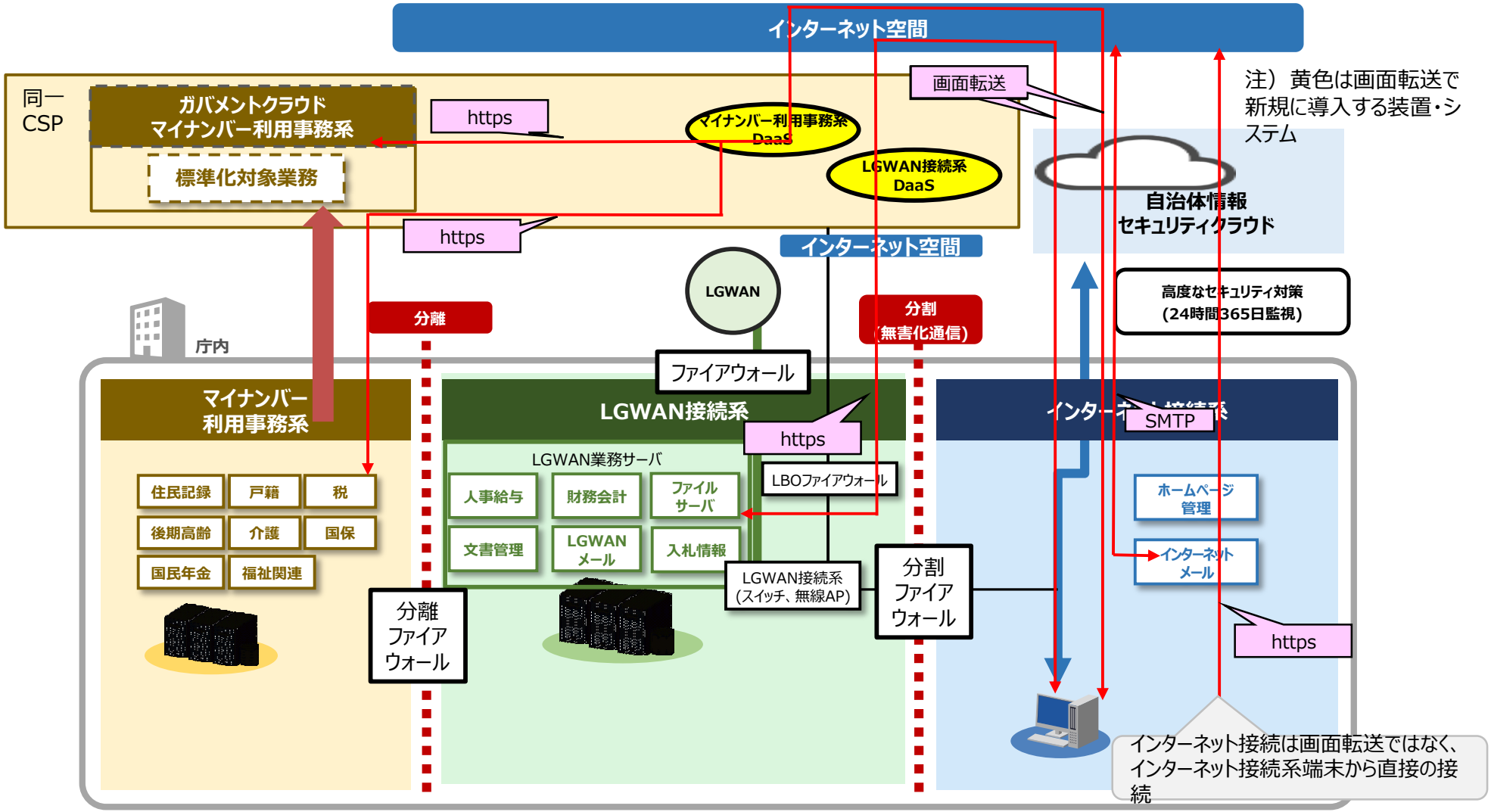
通信経路 (4)インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)

- ✓ ガバメントクラウド、DaaSが同一CSPに実装時、インターネット接続系端末からDaaS経由でガバメントクラウド、マイナンバー利用事務系、LGWAN接続系にアクセス時のリスク分析の通信経路を示す。
- ✓ 本構成は、インターネット接続系の端末からLGWAN接続系の業務サーバに画面転送のDaaSを利用してアクセスすることから、βモデルとみなせる。そのため、βモデルの対策を行うことを前提とする。



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)LGWAN接続系　α’モデルで接続

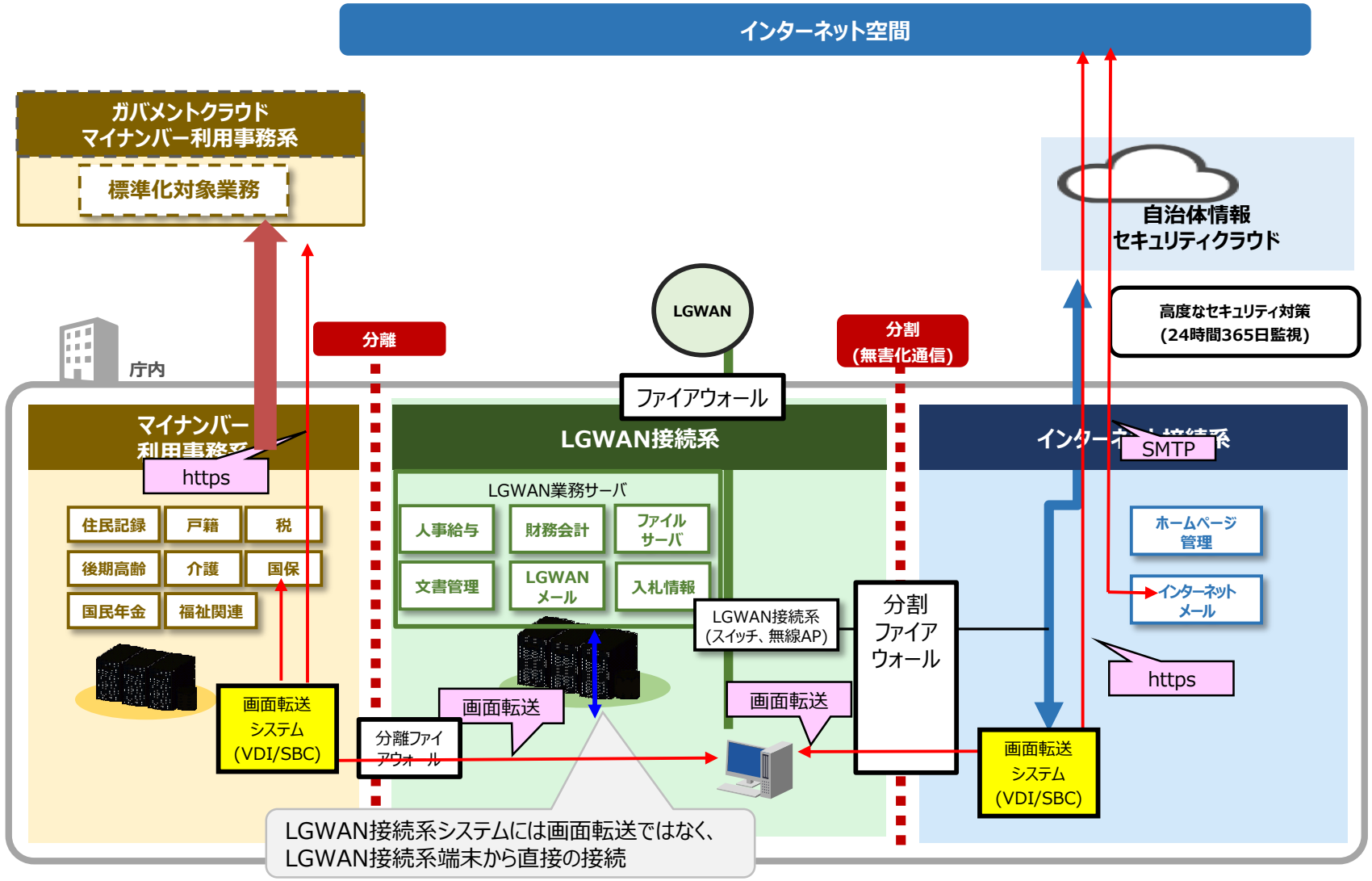
- ✓ ガバメントクラウド、DaaSが同一CSPに実装時、インターネット接続系端末からDaaS経由でガバメントクラウド、マイナンバー利用事務系、LGWAN接続系にアクセス時のリスク分析の通信経路を示す。
- ✓ 本構成はLGWAN業務サーバにはLGWAN接続系からのローカルブレイクアウトでアクセスする。
- ✓ 本構成は、βモデル、α‘モデルの混合とみなせる。そのため、βモデル、α’モデルの対策を行うことを前提とする。



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

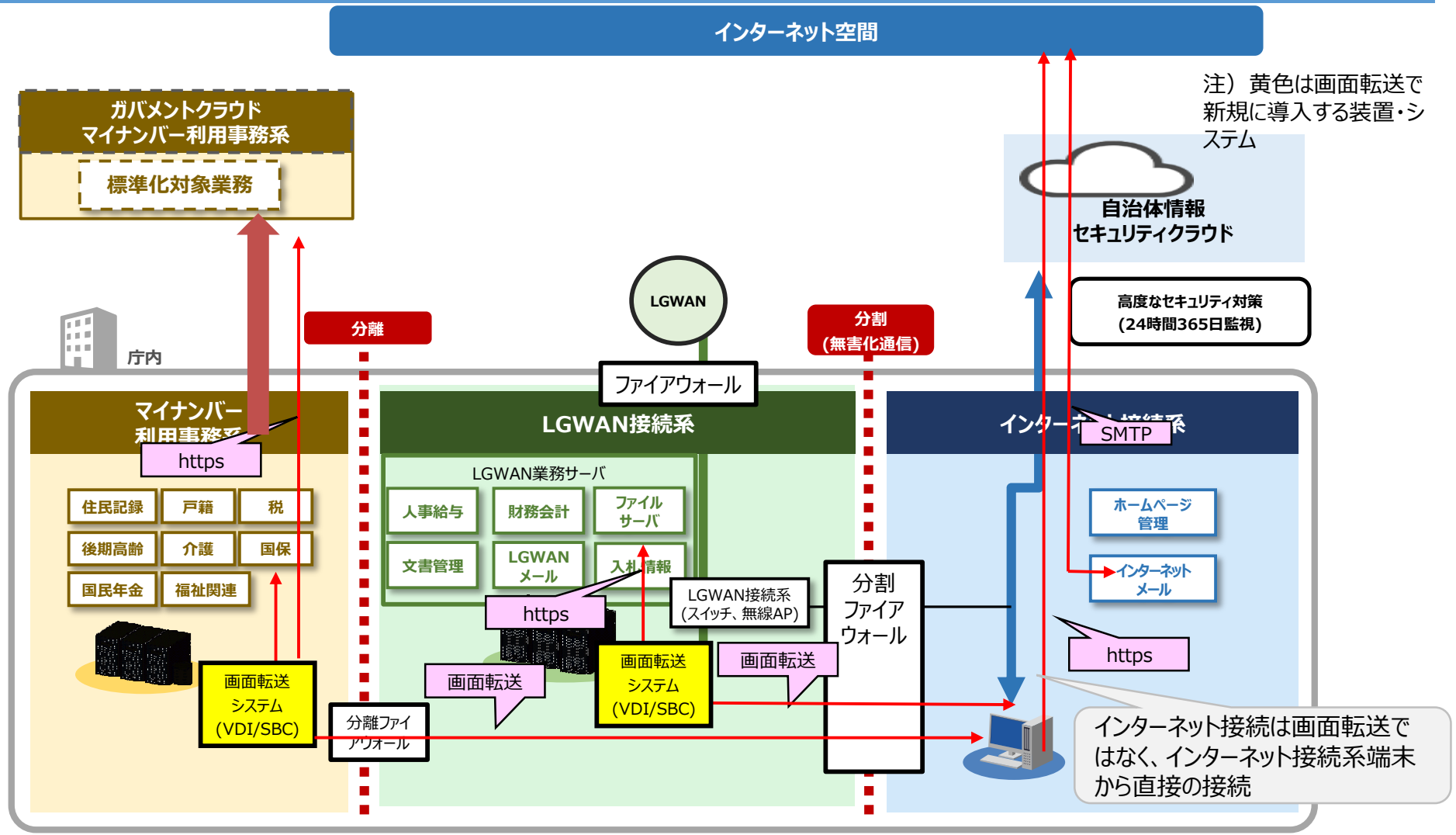
✓ LGWAN接続系端末からオンプレミスの画面転送経由でガバメントクラウド、マイナンバー利用事務系、インターネットにアクセス時のリスク分析の通信経路を示す。

注）黄色は画面転送で新規に導入する装置・システム



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

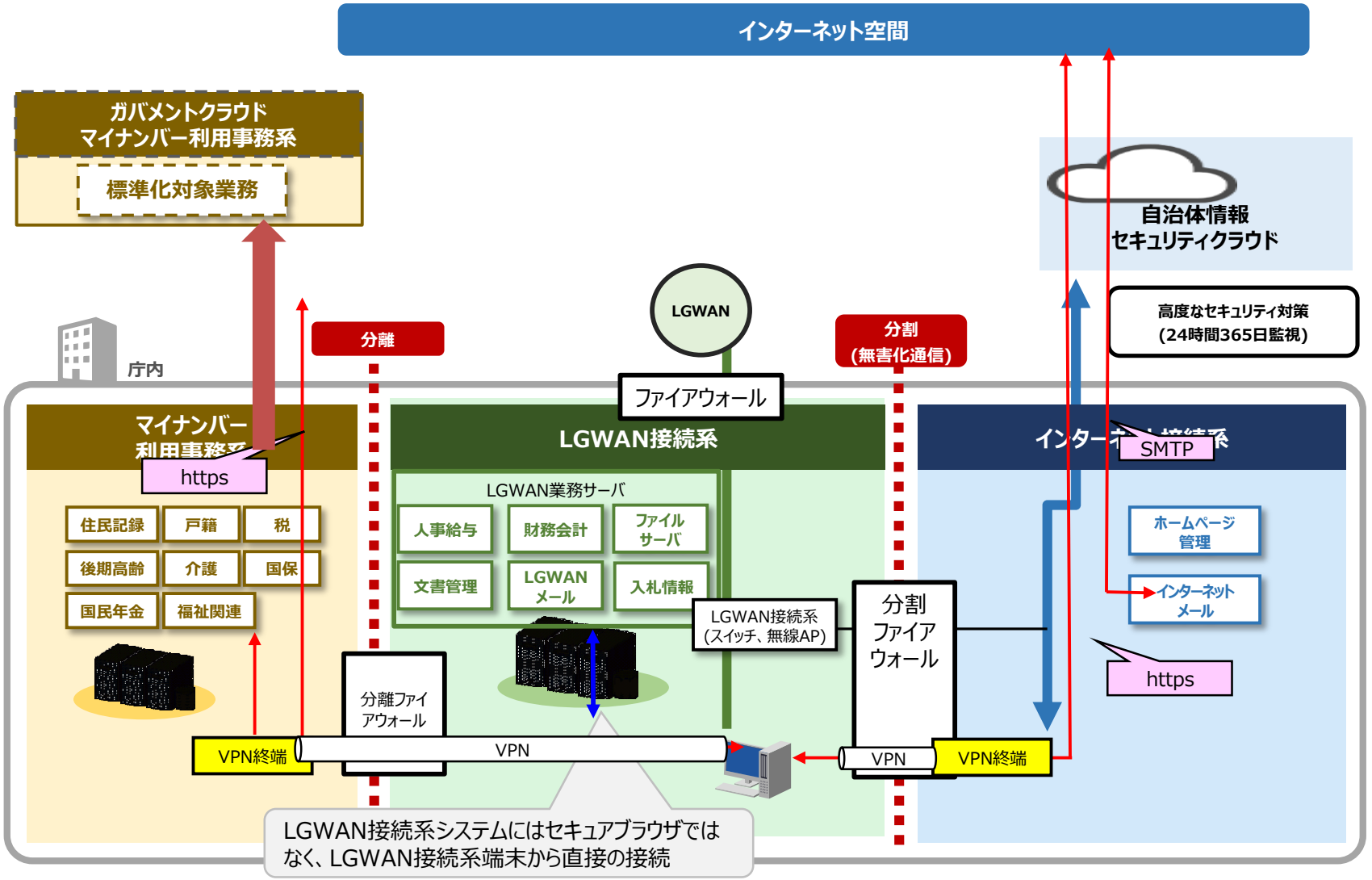
- ✓ インターネット接続系端末からオンプレミスの画面転送経由でガバメントクラウド、マイナンバー利用事務系、LGWAN接続系にアクセス時のリスク分析の通信経路を示す。
- ✓ 本構成は、インターネット接続系の端末からLGWAN接続系の業務サーバに画面転送のDaaSを利用してアクセスすることから、βモデルとみなせる。そのため、βモデルの対策を行うことを前提とする。



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

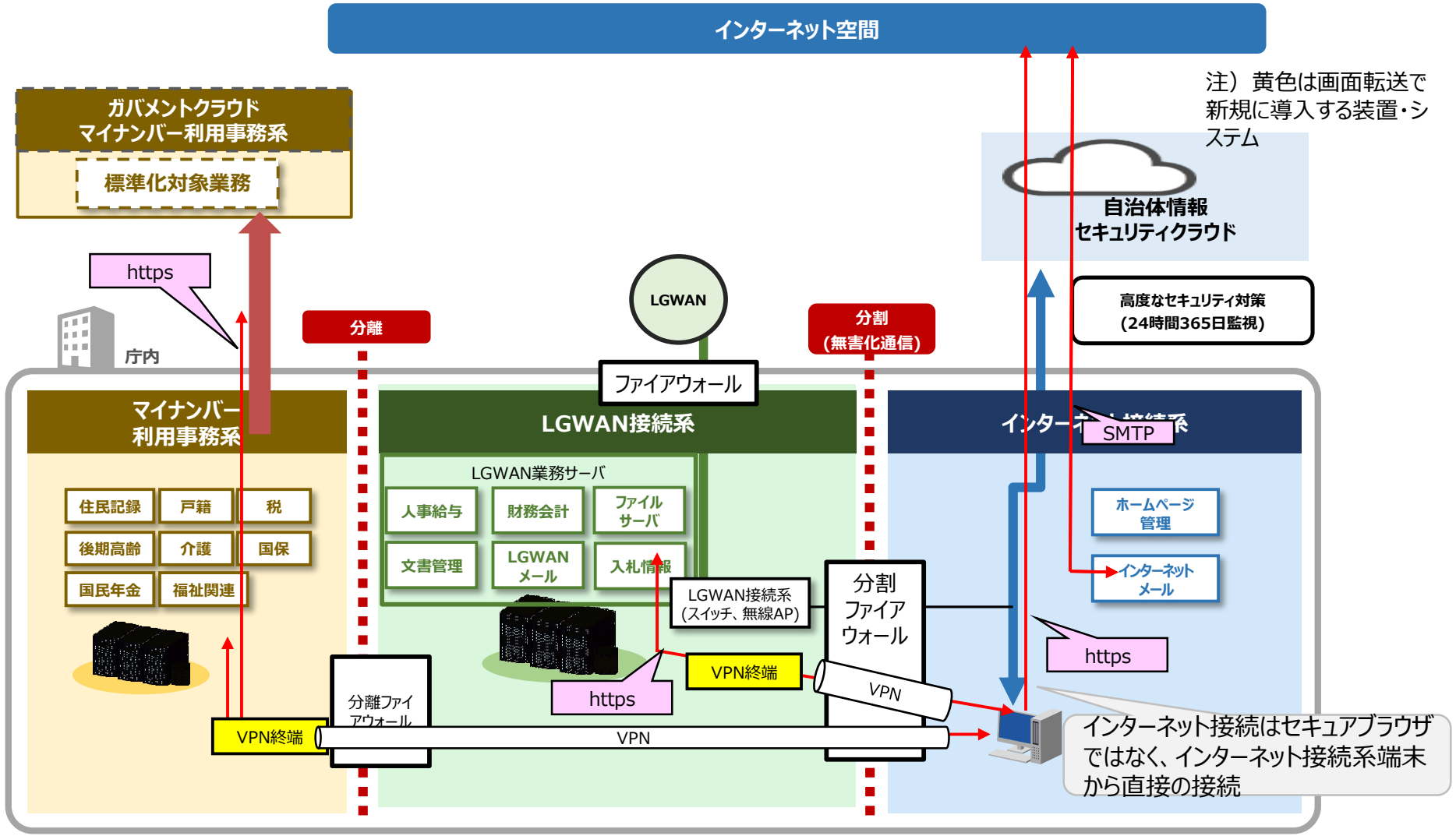
✓ LGWAN接続系端末からセキュアブラウザによるガバメントクラウド、マイナンバー利用事務系、インターネットにアクセス時のリスク分析の通信経路を示す。

注）黄色は画面転送で新規に導入する装置・システム



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

- ✓ インターネット接続系端末からセキュアブラウザによるガバメントクラウド、マイナンバー利用事務系、 LGWAN接続系にアクセス時のリスク分析の通信経路を示す。
- ✓ 本構成は、インターネット接続系の端末からLGWAN接続系の業務サーバにセキュアブラウザを利用してアクセスすることから、βモデルとみなせる。そのため、βモデルの対策を行うことを前提とする。



2.画面転送の資産の重要度

資産の重要度の考え

✓資産ベースのリスクアセスメントには資産の重要度に応じた分析が必要。
✓資産の重要度の評価基準は以下のとおりであり、**資産が被害にあった場合の影響の大きさ**を基準とする。

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

3.画面転送に係る脅威

脅威レベルの考え

✓資産ベースの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。
✓脅威レベルの基準を以下とする。

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

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エアに感染	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	

非公表

４.画面転送の通信経路における攻撃ルート

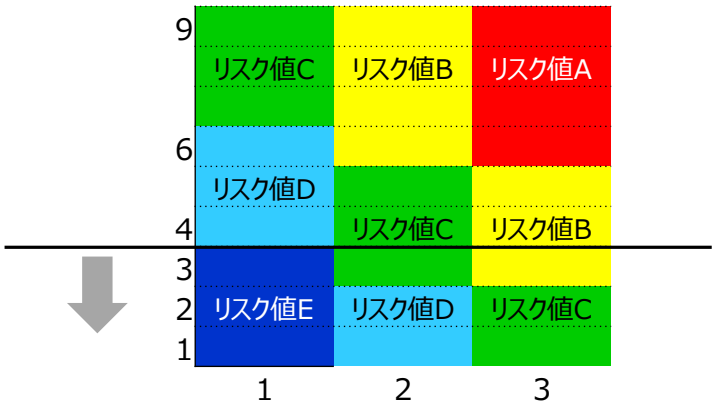
※本章のスライドについては、検討会において投影のみ実施することとし、非公表とする。

５.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。

脅威レベルが最も高い3（脅威が発生しやすい）であっても、十分な対策により脆弱性が１であれば、脅威レベル×脆弱性レベル=3となり「安全」である。
対策が不十分で脆弱性が3であっても、脅威レベルが最も低い1(脅威が発生しにくい）であれば、脅威レベル×脆弱性レベル=3となり「安全」である。

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	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

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。 －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 －マイナンバー利用事務系の情報漏えい、不正アクセス等により社会的な問題となる
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

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

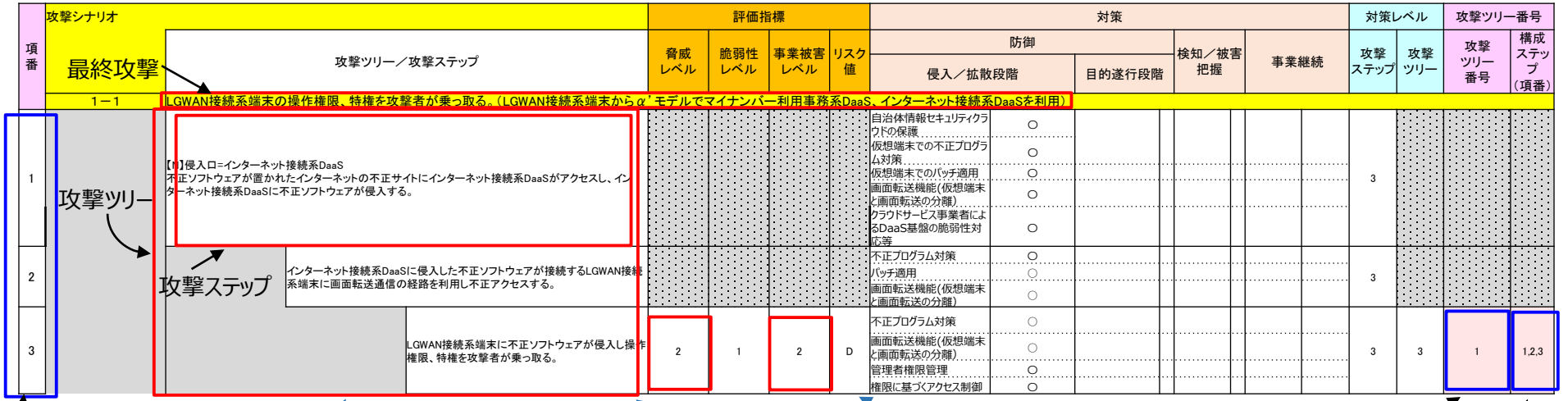
攻撃シナリオ番号
x-yの形式で攻撃シナリオに割り振った番号
xは最終攻撃の被害の単位（上記の場合、情報の外部への送信）で通番で付与
yはxの攻撃の違い（不正アクセスとマルウェア感染）、または攻撃拠点の違いで通番で付与

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）



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 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	【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

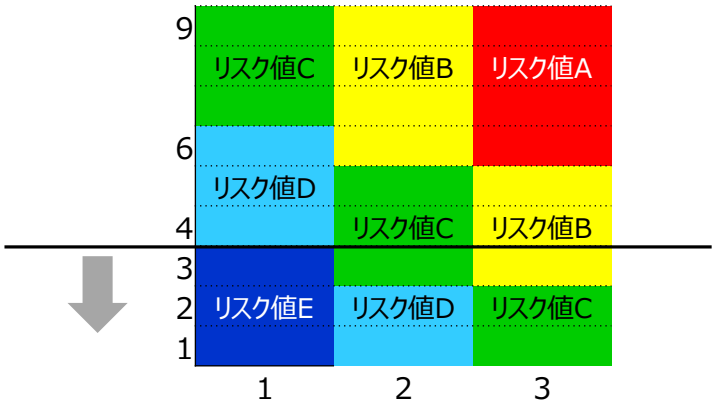
⑦脅威レベル、脆弱性レベルと事業被害レベルからリスク値を算出

６.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。

脅威レベルが最も高い3（脅威が発生しやすい）であっても、十分な対策により脆弱性が１であれば、脅威レベル×脆弱性レベル=3となり「安全」である。
対策が不十分で脆弱性が3であっても、脅威レベルが最も低い1(脅威が発生しにくい）であれば、脅威レベル×脆弱性レベル=3となり「安全」である。

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	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

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（次項参照）
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（次項参照）
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