資料２-2

マイナンバー利用事務系の画面転送に係るリスク分析結果 (2)

総務省

令和６年11月27日

通信経路

本リスク分析は、下記の赤枠の通信経路のパターンについてまとめたものである。

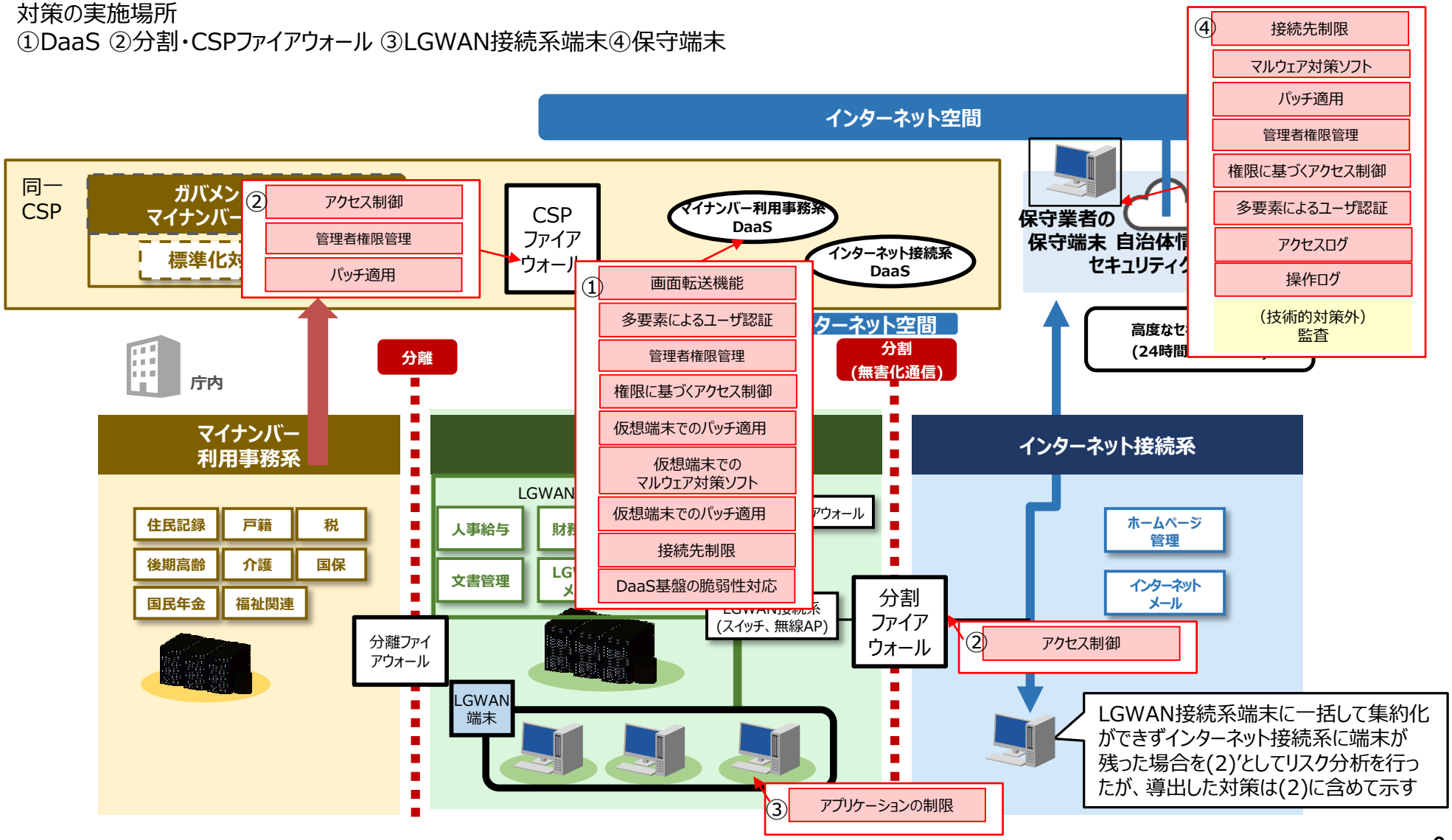
	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 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

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)
リスク分析結果を踏まえた技術的対策

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)の対策

- ✓ 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	必須
クラウドサービス(DaaS)上での対策		
画面転送機能	仮想端末と画面転送の分離により、仮想端末のマルウエア感染、不正プログラムの動作などが画面転送を通じ、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利用者、特権管理者を多要素認証する（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）。	○
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、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。	○
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。	○
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。	○
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	○
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事業者の担当となるため、DaaS事業者選定時の前提条件となる。**	○
クラウドサービスでの対策		
アクセス制限	接続元(マイナンバー利用事務系DaaS)、接続先（マイナンバー利用事務系システム、標準化システム）のIPアドレス、通信ポートでの通信に限定したアクセス制限する。	○
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、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。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。	○

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	必須
α'モデルの対策以外のLGWAN接続系での対策		
アクセス制限	マイナンバー利用事務系とLGWAN接続系の通信を遮断する。	○
	インターネット接続系DaaSとインターネット、メール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。	○
	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。	○
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の個人情報を表示した画面を、スクリーンショットで取得し、情報漏えいすることを防止するため、LGWAN接続系端末でスクリーンショット機能を停止する。（注）	○
保守端末での対策		
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、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。	○
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、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。	○
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	保守担当者を多要素認証する（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		
監査	内部監査を行う。	○

注）スクリーンショット機能の停止を規定した理由は、画面転送に接続する手元の端末において、マイナンバー利用事務系の住民の個人情報を表示した画面を不正に取得され、漏えいが発生することを防止するためであり、このような漏えいを最大限防ぐにあたり、どのような対策が望ましいかについては、有識者の意見等を踏まえ引き続き検討する。

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) 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	必須	推奨
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。	○	
接続先制限	LGWAN接続系から外部へのアクセス先をLGWAN-ASP、及び利用するクラウドサービスのみに限定する。	○	
LBO テナントアクセス制御	利用するクラウドサービスへのアクセスを自テナントのみに制限する。	○	
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。	○	

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	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、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。		○
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。	○	

注）LGWAN接続系や、マイナンバー利用事務系、インターネット接続系の全てが、LGWAN接続系に集約した端末からアクセスする構成となる。
LGWAN接続系端末への集約により、共通の通信経路部分が生じ、LGWAN接続系、マイナンバー利用事務系、インターネット接続系は同じ脅威にさらされる。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、 脅威への本対策の有効性について今後、引き続き検討する。

非公表

事業被害ベースと資産ベースのリスク分析結果の考察

※リスクアセスメント結果については攻撃ルートも含むため、
検討会において投影するのみとし、非公表とする。