参考資料

マイナンバー利用事務系に係る画面転送の方式と特定個人情報に関する安全管理措置について

総 務 省

令和７年１月31日

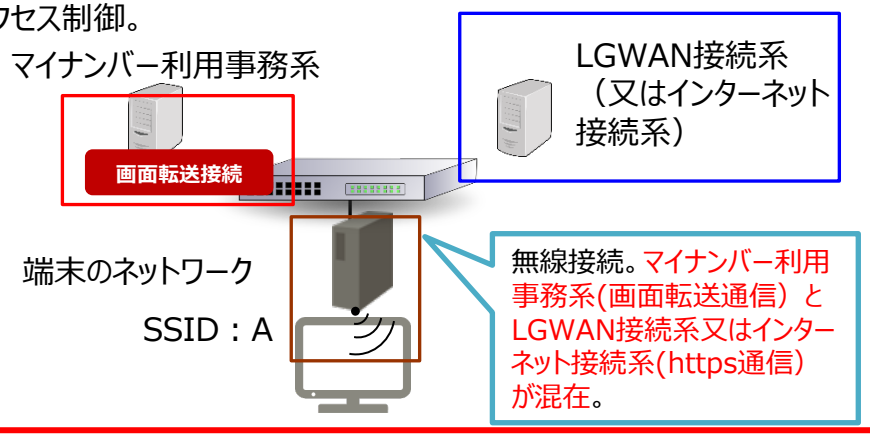
端末を１台に統合する場合の無線LAN/有線LAN利用

✓ 端末を１台に集約した場合、無線LANを利用する場合と有線LANを利用する場合の両方がありうる。

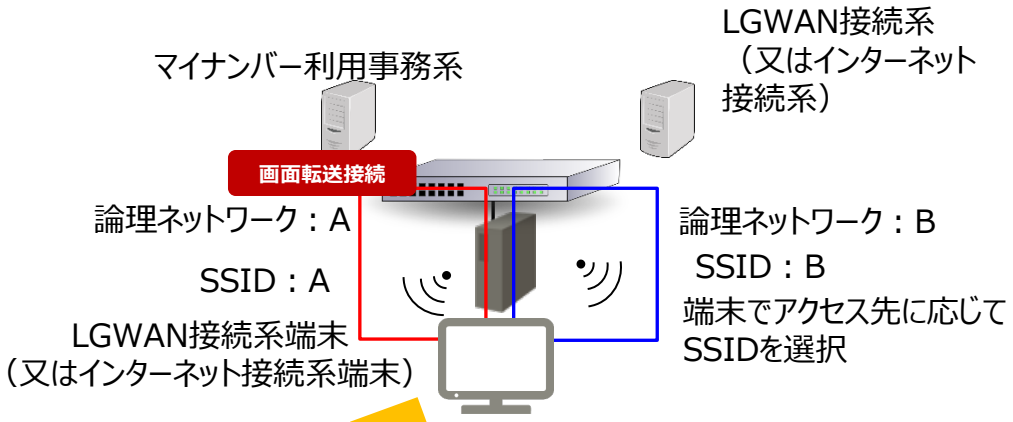
- 端末を１台に統合し有線LANを利用する場合と同じパターン（パターン①）を考えた場合、**マイナンバー利用事務系に係る画面転送の通信と、他のネットワーク系統の通信が混在する形になり、アクセス制御により通信をコントロールする**形になる。
- 端末を統合する場合においても、**SSIDの分離によりネットワークの分離が可能**と考えられる（パターン②）。

無線LAN　LGWAN接続系に端末集約＋画面転送（端末統合）

① 端末を集約し、SSIDを分離しない場合、L3スイッチ（ネットワーク機器）でアクセス制御。

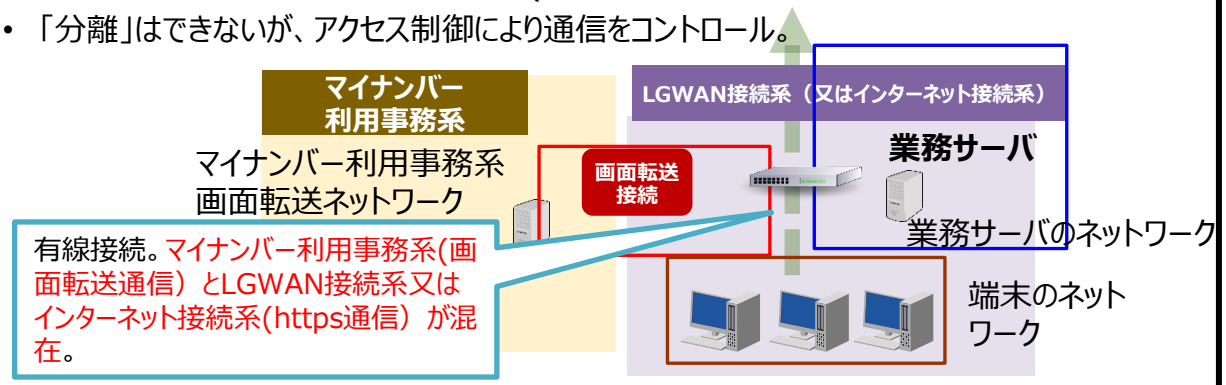


② 端末は集約するが、SSIDを分け、VLANで論理ネットワークにより分離。



有線LAN　LGWAN接続系に端末集約＋画面転送（端末統合）

- LGWAN接続系の、業務サーバ、マイナンバー利用事務系に係る画面転送、端末それぞれのネットワークの間の通信を、L3スイッチ(ネットワーク機器）でアクセス制御。
- 「分離」はできないが、アクセス制御により通信をコントロール。



LGWAN接続系（又はインターネット接続系）の業務により、**端末を庁舎外に持ち出す場合**、当該端末からマイナンバー接続系にアクセスできてしまうと、**運用によっては番号法上の安全管理措置（特定個人情報等を取り扱う区域の管理）を講じられなくなる**ことに留意が必要。

特定個人情報に関する安全管理措置との関係

- 「安全管理措置の検討手順」関係　　P3
- 「講ずべき安全管理措置の内容」関係　　P4～11
  - 「組織的安全措置」関係　　P5
  - 「物理的安全管理措置」関係　　P7～9
  - 「技術的安全管理措置」関係　　P10・11
- 安全管理措置実施のための対策イメージ（全体）　P12

※各安全管理措置に係るガイドラインの関連箇所については、本資料の「参考資料」参照

特定個人情報に関する安全管理措置について

- ✓ 番号法上の安全管理措置は、同法第12条に根拠があり、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」（平成26年12月18日個人情報保護委員会）の別添１に具体的な内容を規定している。
- ✓ マイナンバー利用事務系に係る画面転送、無線LAN利用の両方について、安全管理措置との対応関係を示す。

◎行政手続における特定の個人を識別するための番号の利用等に関する法律（番号法）（平成25年法律第27号）
（個人番号利用事務実施者等の責務）
第十二条　個人番号利用事務実施者及び個人番号関係事務実施者（以下「個人番号利用事務等実施者」という。）は、個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない。

【個人情報保護委員会「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」】
- 第４－２ 特定個人情報の安全管理措置等 （具体的な内容を別添１参照としている）
- （別添１）特定個人情報に関する安全管理措置（行政機関等編）

項目名に	説明
第４－２－⑵ 安全管理措置	（関係条文） ・番号法 第12条 ・個人情報保護法 第66条、第67条
安全管理措置（番号法第12条、個人情報保護法第66条、第67条）	個人番号利用事務等実施者は、個人番号（生存する個人のものだけでなく死者のものも含む。）の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない。また、行政機関の長等は、保有個人情報である特定個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報である特定個人情報の安全管理のために必要かつ適切な措置を講じなければならない。 **行政機関等は、安全管理措置の検討に当たり、番号法及び個人情報保護法並びに本ガイドライン（「（別添１）特定個人情報に関する安全管理措置（行政機関等編）」を含む。）、個人情報保護法ガイドライン（行政機関等編）及び事務対応ガイドを遵守することを前提とする。** また、行政機関等は、個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクを軽減するための措置として特定個人情報保護評価書に記載した全ての措置を講ずるものとする。

安全管理措置の検討手順の実施のための対策

✓ 安全管理措置の検討手順の実施のため、必要と考えられる対策は以下のとおり。

画面転送:端末1台化に伴う無線LANを利用した画面転送
無線LAN:マイナンバー利用事務系端末の無線LAN利用

特定個人情報に関する安全管理措置（行政機関等編）の項目名	**対策**	
	画面転送	**無線LAN**
1 安全管理措置の検討手順	ー	ー
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	**①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。）の明確化** ・事務取扱担当者のリスト化 ・画面転送システム、無線LAN利用を許可する者のリスト化	

組織的安全管理措置の実施のための対策

✓ 組織的安全管理措置の実施のため、必要と考えられる対策は以下のとおり。

画面転送:端末1台化に伴う無線LANを利用した画面転送
無線LAN:マイナンバー利用事務系端末の無線LAN利用

特定個人情報に関する安全管理措置（行政機関等編）の項目名	対応	
	画面転送	無線LAN
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 端末を庁舎外に移動する運用を行っていた場合、端末の場所によっては、当該職員以外が端末や関連機器等の取扱状況を客観的に評価することは極めて困難になる場合がある。	**②画面転送システム、無線LANの運用状況の確認** **・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** ・事務取扱担当者の画面転送システム、無線LANの運用状況を確認	
	③アクセスログの取得・確認 ・画面転送システム（無線LAN含む）へのアクセスログを確認し、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	**③アクセスログの取得・確認** ・無線LANへのアクセスログを確認し、マイナンバー利用事務系の端末のみがアクセスしていることを確認

端末の持ち出しについて

- ✓ 物理的安全管理措置として、特定個人情報を取り扱う事務を実施する区域（取扱区域）に係る対策として以下が規定されている。
  - ➢ 事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないよう留意する必要がある。
  - ➢ 取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。
- ✓ 端末を取扱区域から持ち出した場合、**事務取扱担当者等以外の者が住民の特定個人情報等を閲覧できる**可能性や、盗難又は紛失等を防止する**物理的な安全管理措置（施錠、セキュリティワイヤー等による固定）が区域外で徹底されないリスクが生じる**。
- ✓ **住民の特定個人情報を扱う個人番号利用事務の重要性を鑑み、端末の取扱区域外への持ち出しについては、原則禁止せざるを得ないのではないか**。

※特に庁舎外への持ち出しを認めた場合、P16に記載したとおり、端末や関連機器等の取扱状況を客観的に評価することが困難となるため、十分な安全性が確保できなくなる可能性がある。

項目名	説明
2 講ずべき安全管理措置の内容	
E 物理的安全管理措置	行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。
a 特定個人情報等を取り扱う区域の管理	特定個人情報ファイルを取り扱う情報システム（サーバ等）を管理する区域（以下「管理区域」という。）を明確にし、物理的な安全管理措置を講ずる。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。 **また、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）について、事務取扱担当者等以外の者が特定個人情報等を容易に閲覧等できないよう留意する必要がある。** 行政機関等は、管理区域のうち、基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合には、情報システム室等について、次の①及び②に掲げる措置を講ずる。
b 機器及び電子媒体等の盗難等の防止	管理区域及び**取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる**。また、電子媒体及び書類等の庁舎内の移動等において、紛失・盗難等に留意する。 **«手法の例示»** **＊ 特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット、書庫又は必要に応じて耐火金庫等へ保管することが考えられる。** **＊ 特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定すること等が考えられる。**

物理的安全管理措置の実施のための対策①

✓ 物理的安全管理措置の実施のため、必要な対策は以下のとおり。

画面転送:端末1台化に伴う無線LANを利用した画面転送
無線LAN:マイナンバー利用事務系端末の無線LAN利用

特定個人情報に関する安全管理措置（行政機関等編）の項目名	対応	
	画面転送	無線LAN
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	**⑦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 ・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	
① 入退室管理	**④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	

物理的安全管理措置の実施のための対策②

画面転送:端末1台化に伴う無線LANを利用した画面転送　無線LAN:マイナンバー利用事務系端末の無線LAN利用

特定個人情報に関する安全管理措置（行政機関等編）の項目名	対応	
	画面転送	無線LAN
E 物理的安全管理措置	ー	ー
a 特定個人情報等を取り扱う区域の管理	ー	ー
② 情報システム室等の管理 注）「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。	**⑤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 **⑥特権管理者・保守端末の管理** ・特権ID(注) 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 ・画面転送システム、無線LANの特権管理者、保守端末を適正に管理	**⑤機器の物理的な保護** ・無線LAN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 **⑥特権管理者・保守端末の管理** ・特権ID(注) 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 ・無線LANの特権管理者、保守端末を適正に管理
b 機器及び電子媒体等の盗難等の防止	**⑦事務取扱担当者端末の保護** ・**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 ・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	

物理的安全管理措置の実施のための対策③

画面転送:端末1台化に伴う無線LANを利用した画面転送
無線LAN:マイナンバー利用事務系端末の無線LAN利用

特定個人情報に関する安全管理措置（行政機関等編）の項目名	対応	
	画面転送	無線LAN
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	現行のガイドラインにおいては、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旨規定 ⇒ **特定個人情報の重要性を鑑み、現時点においては引き続き同様の整理をすることとしてはいかがか**	

技術的安全管理措置の実施のための対策①

✓ 技術的安全管理措置の実施のために必要と考えられる対策の例は以下のとおり。
（画面転送の技術的対策についてはリスクアセスメントにより定義するため、各通信経路パターンの対策を参照）

画面転送:端末1台化に伴う無線LANを利用した画面転送
無線LAN:マイナンバー利用事務系端末の無線LAN利用

特定個人情報に関する安全管理措置（行政機関等編）の項目名	**対応**	
	画面転送	**無線LAN**
F 技術的安全管理措置 （※下記は安全管理措置から考えられる対策の例。**画面転送に係る技術的対策の詳細は、リスクアセスメントにより導出**）		
a アクセス制御 b アクセス者の識別と認証	**⑧画面転送システムアクセス時の認証・認可** ・画面転送システム(例：DaaS)にアクセス時、事務取扱担当者のみをユーザ認証により画面転送システムへのアクセスを認可 ・画面転送システム(例：DaaS)に保守運用でアクセス時、特権管理者のみをユーザ認証によりアクセスを認可	**⑨無線LANアクセス時の認証・認可** ・無線LANに接続時、マイナンバー利用事務系端末をIEEE802.1xのクライアント証明書により認証(ユーザID・パスワードを使わない、EAP-TLS等の機器認証を行うことで、正規の端末からの接続であることを担保)し、アクセスを許可 ・無線LANに保守運用でアクセス時、特権管理者のみをユーザ認証によりアクセスを認可

技術的安全管理措置の実施のための対策②

✓ 技術的安全管理措置の実施のために必要と考えられる対策の例は以下のとおり。
（画面転送の技術的対策についてはリスクアセスメントにより定義するため、各通信経路パターンの対策を参照）

画面転送:端末1台化に伴う無線LANを利用した画面転送　無線LAN:マイナンバー利用事務系端末の無線LAN利用

特定個人情報に関する安全管理措置（行政機関等編）の項目名	**対応**	
	画面転送	**無線LAN**
F 技術的安全管理措置 （※下記は安全管理措置から考えられる対策の例。**画面転送に係る技術的対策の詳細は、リスクアセスメントにより定義**）		
c 不正アクセス等による被害の防止等	**⑩ファームウェア、OS等の最新化** ・無線LANのファームウェア等の最新化 ・画面転送(例:DaaS)システムの基盤、及び仮想化端末OSの最新化 **③アクセスログの取得・確認** ・無線LAN、画面転送システムへのアクセスログの取得とログ確認 **⑪画面転送システムからのアクセスのみに制限** ・マンナンバー利用事務系のシステムへのアクセスは画面転送システムもしくはマンナンバー利用事務系の専用端末のみにアクセスを制限する	**⑩ファームウェア、OS等の最新化** ・無線LANのファームウェア等の最新化 **③アクセスログの取得・確認** ・無線LANへのアクセスログの取得とログ確認
d 漏えい等の防止	**⑫通信の暗号化** ・無線LAN通信の強度の高い暗号化による盗聴対策(WPA2又はWPA3) ・画面転送通信の強度の高い暗号化による盗聴対策	**⑫通信の暗号化** ・無線LAN通信の強度の高い暗号化による盗聴対策(WPA2又はWPA3)

安全管理措置実施のための対策イメージ（全体）