資料３

無線LAN利用に係るガイドライン改定案等について

総 務 省

令和７年１月31日

総務省自治行政局

デジタル基盤推進室

無線LAN利用に係る改定案について

無線LAN利用に係るガイドライン改定の方向性について

- ✓ 既に地方公共団体向けに提示しているLGWAN接続系における無線LAN利用の要件（総行情第80号令和２年５月22日「自治体情報セキュリティ対策の見直しについて」の参考資料）
- ✓ 特定個人情報に関する安全管理措置の実施のための対策

- ■ LGWAN接続系における無線LAN利用について、ガイドラインにおいて明示的に規定
- ■ マイナンバー利用事務系における無線LAN利用については、LGWAN接続系における対策に加え、特定個人情報に関する安全管理措置の実施のための対策を追加で規定

LGWAN接続系における無線LAN利用の要件

- ✓ 現行のガイドラインで参照先として示している**「庁内無線LANのセキュリティ要件について」**（総行情第80号令和２年５月22日「自治体情報セキュリティ対策の見直しについて」の参考資料）**において、LGWAN接続系における無線LAN利用の要件として規定されている内容を、改めてガイドラインに図表で示す**こととしてはいかがか、
- ✓ 盗聴対策以外も含むため、**項番（13）のタイトルを「無線LANのセキュリティ対策」に変更する**こととしてはいかがか。

現行：対策基準（解説）

6.1. コンピュータ及びネットワークの管理
（１３）無線LAN及びネットワークの盗聴対策

無線LANを利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。特に、LGWAN接続系で無線LANを利用する場合は、盗聴及びなりすましアクセスポイント（AP）などによる情報漏えいや不正アクセスに対して、認証サーバを利用したWPA2/WPA3エンタープライズによる認証（IEEE802.1X認証）を採用する等、セキュリティ対策を実施しなければならない。遵守すべきセキュリティ要件は、「庁内無線LANのセキュリティ要件について」を参照されたい。なお、マイナンバー利用事務系においては、無線LANは利用しないこととしなければならない。

次ページ

改定案：対策基準（解説）

6.1. コンピュータ及びネットワークの管理
（１３）無線LANのセキュリティ対策~~及びネットワークの盗聴対策~~

無線LANを利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。

①LGWAN接続系

LGWAN接続系で無線LANを利用する場合は、盗聴及びなりすましアクセスポイント（AP）などによる情報漏えいや不正アクセスに対して、認証サーバを利用したWPA2/WPA3エンタープライズによる認証（IEEE802.1X認証）を採用する等、セキュリティ対策を実施しなければならない。~~遵守すべきセキュリティ要件は、「庁内無線LANのセキュリティ要件について」を参照されたい~~**下の図表に記載する。**

図表の挿入（「庁内無線LANのセキュリティ要件」の反映）※推奨も含む

図表XX　LGWAN接続系での無線LAN利用のセキュリティ要件

LGWAN接続系における無線LAN利用の要件（図表）

✓ 「庁内無線LANのセキュリティ要件について」で示されたLGWAN接続系における無線LANの利用要件は以下のとおり。

分類	要件	区分
無線セキュリティ規格	WPA２／WPA３によるセキュリティ規格の採用	**必須**
認証方式	正規利用者(認められた利用者）のみが無線ＬＡＮに接続されるよう認証サーバを利用したＷＰＡ２／ＷＰＡ３エンタープライズによる認証（IEEE802.1X認証）を行う。 具体的には、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、アクセスを認可	**必須**
正規利用者の管理	無線LANの接続状況の可視化やログの収集・保存・分析を実施する。	推奨
	外部からの不正な利用がなされないよう無線IDS/IPSを導入し、不正な利用やLGWAN接続系への外部からの侵入を防止する。	必要に応じて検討
アクセスポイントの管理	アクセスポイントの管理者パスワードを適切に設定する。（強固なID・パスワードの設定、アクセスポイント単位での管理 等） 無線接続する他の端末に格納されている情報の閲覧を防止し、また端末間の不正プログラム拡散防止のため、無線端末間同士の通信が行われないよう適切な設定を行う。	**必須**
端末の設定	端末に許可されたアクセスポイントのSSIDのみを表示し、接続が可能となるよう設定し、端末からインターネット接続用のアクセスポイント経由で直接インターネットへ接続されないよう徹底する。 （インターネットへの接続は画面転送での接続に限る）	**必須**
脆弱性の管理	自庁内に設置した各種無線LAN機器の構成管理(機器、OS、ソフトウェアの名称やバージョン）を実施するとともに脆弱性情報を収集し、脆弱性が発見された際に、影響度合を判断しながら適時修正パッチの適用を行う。	**必須**
電波調整・設定	電波の伝搬範囲の適切な設定をする。また、電波状況を監視する。	推奨

マイナンバー利用事務系における無線LAN利用の要件

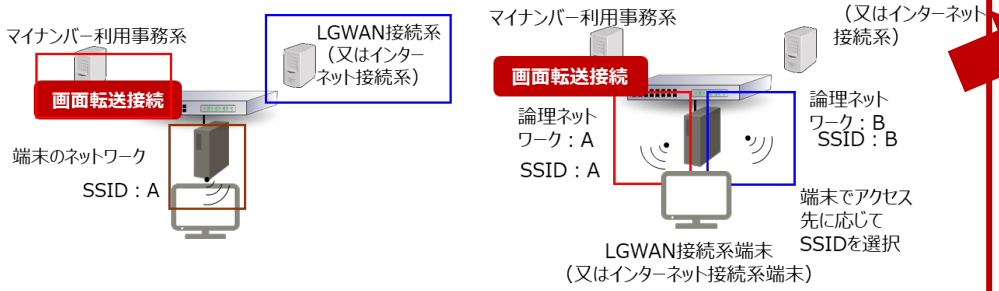
✓ マイナンバー利用事務系における無線LAN利用については、特定個人情報に係る安全管理措置を講じる必要がある旨を規定。
（端末を統合し、他のネットワーク系統の業務に利用している端末をマイナンバー利用事務系の業務を行う場合に、無線LANを利用する場合があるため、別紙を参照するように規定。）

現行：対策基準（解説）

6.1. コンピュータ及びネットワークの管理
（１３）無線LAN及びネットワークの盗聴対策

無線LANを利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。特に、LGWAN接続系で無線LANを利用する場合は、盗聴及びなりすましアクセスポイント（AP）などによる情報漏えいや不正アクセスに対して、認証サーバを利用したWPA2/WPA3エンタープライズによる認証（IEEE802.1X認証）を採用する等、セキュリティ対策を実施しなければならない。遵守すべきセキュリティ要件は、「庁内無線LANのセキュリティ要件について」を参照されたい。なお、マイナンバー利用事務系においては、無線LANは利用しないこととしなければならない。

端末を１台に統合する場合の無線LAN利用



改定案：対策基準（解説）

6.1. コンピュータ及びネットワークの管理
（１３）無線LANのセキュリティ対策

無線LANを利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。
①LGWAN接続系
（略）
②マイナンバー利用事務系
~~なお、マイナンバー利用事務系においては無線LANは使用しないこととしなければならない。~~マイナンバー利用事務系で無線LANを利用する場合は「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）に規定されている安全管理措置を講じる必要があることに留意する。セキュリティ要件は下の図表に記載する。なお、他のネットワーク系統の業務に利用している端末をマイナンバー利用事務系の業務で利用する場合は、別紙「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」も併せて参照すること。

図表の挿入

図表XX　マイナンバー利用事務系での無線LAN利用の要件

次ページ

マイナンバー利用事務系における無線LAN利用の要件（図表）①

✓ 前回検討会で整理した、特定個人情報に関する安全管理措置を実施するための対策を、LGWAN接続系における無線LANの利用の要件に加える形で以下のとおり示す。

分類		要件	区分	備考
技術的対策	**無線セキュリティ規格**	＜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)	**必須**	• 特定個人情報に関する安全管理措置における技術的安全管理措置 （漏えい等の防止）実施のための対策 • LGWAN接続系においても必須要件
	認証方式	＜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、アクセスを認可 • 無線LANの特権管理者の初期パスワードは変更し、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	**必須**	• 特定個人情報に関する安全管理措置における技術的安全管理措置 （アクセス制御、アクセス者の識別と認証 ）実施のための対策 • IEEE802.1X認証は、LGWAN接続系においても必須要件
	正規利用者の管理・不正アクセスの防止	＜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アクセスログの確認。 • 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	**必須**	特定個人情報に関する安全管理措置における組織的安全管理措置 （取扱状況の把握及び安全管理措置の見直し）、技術的安全管理措置（不正アクセス等による被害の防止等）実施のための対策
		＜ファームウェア、OS等の最新化＞ 無線LANを構成する機器のファームウェア、OS等の最新化	**必須**	特定個人情報に関する安全管理措置における技術的安全管理措置（不正アクセス等による被害の防止等）実施のための対策
		外部からの不正な利用がなされないよう無線IDS/IPSを導入し、不正な利用やマイナンバー利用事務系への外部からの侵入を防止する。	必要に応じて検討	LGWAN接続系と同様の扱い
	アクセスポイントの管理	• アクセスポイントの管理者パスワードを適切に設定する。（強固なID・パスワードの設定、アクセスポイント単位での管理 等） • 無線接続する他の端末に格納されている情報の閲覧を防止し、また端末間の不正プログラム拡散防止のため、無線端末間同士の通信が行われないよう適切な設定を行う。	**必須**	LGWAN接続系においても必須要件
	端末の設定	端末に許可されたアクセスポイントのSSIDのみを表示し、接続が可能となるよう設定し、端末からインターネット接続用のアクセスポイント経由で直接インターネットへ接続されないよう徹底する。	**必須**	LGWAN接続系においても必須要件
	脆弱性の管理	自庁内に設置した各種無線ＬＡＮ機器の構成管理(機器、OS、ソフトウェアの名称やバージョン）を実施するとともに脆弱性情報を収集し、脆弱性が発見された際に、影響度合を判断しながら適時修正パッチの適用を行う。	**必須**	LGWAN接続系においても必須要件
	電波調整・設定	電波の伝搬範囲の適切な設定をする。また、電波状況を監視する。	推奨	LGWAN接続系と同様の扱い

マイナンバー利用事務系における無線LAN利用の要件（図表）②

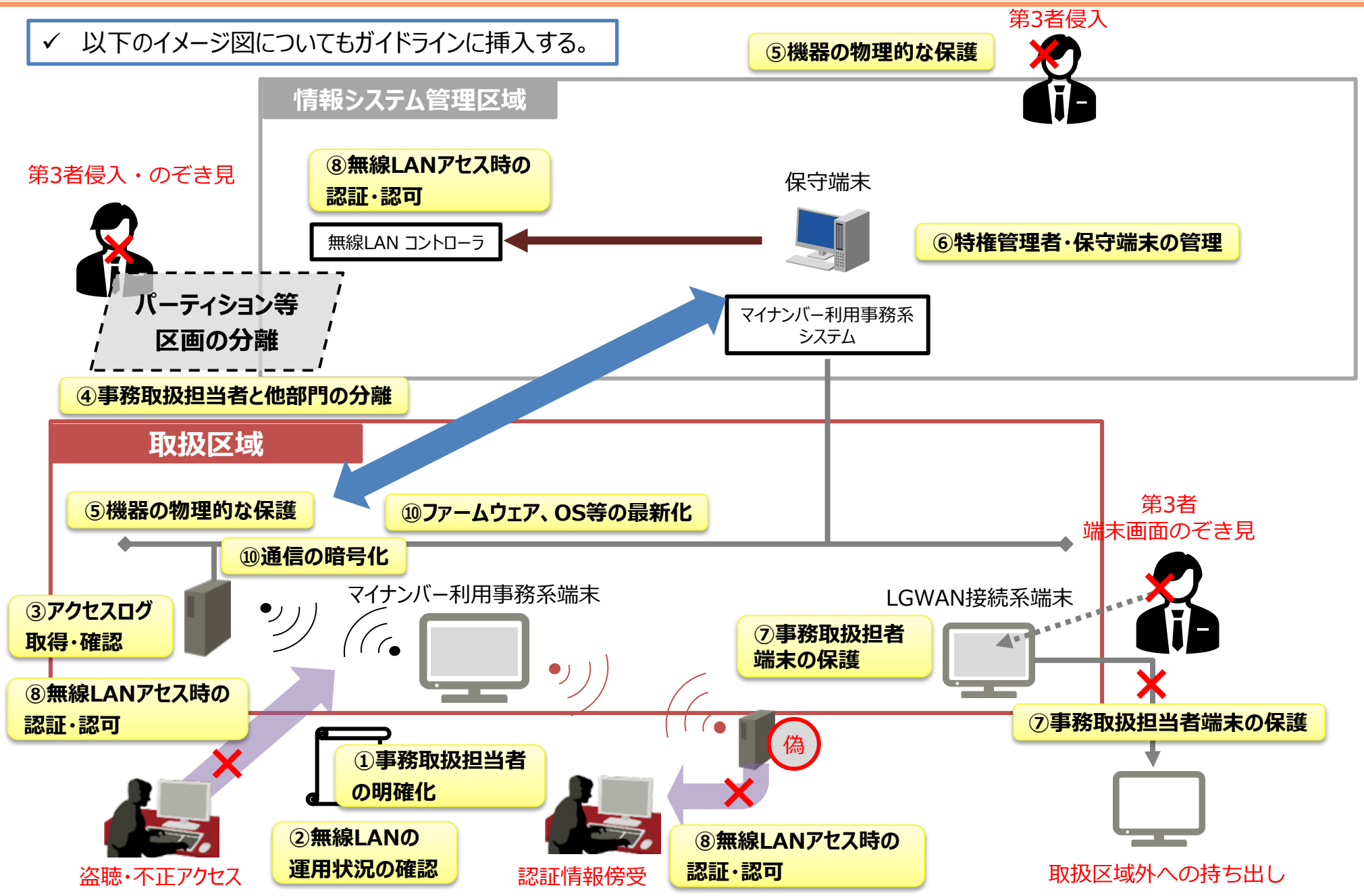
✓ 前ページの続き

分類		要件	区分	備考
組織的対策	正規利用者の管理・不正アクセスの防止	＜特定個人情報等を取り扱う職員（事務取扱担当者）の明確化＞ • 事務取扱担当者のリスト化 • 無線LAN利用を許可する者のリスト化	必須	特定個人情報に関する安全管理措置における安全管理措置の検討手順（個人番号を取り扱う事務の範囲の明確化、事務取扱担当者の明確化）実施のための対策
		＜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 • 事務取扱担当者の無線LANの運用状況を確認	必須	特定個人情報に関する安全管理措置における組織的安全管理措置（取扱状況の把握及び安全管理措置の見直し）実施のための対策
物理的対策	事務取扱端末の保護	• 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） • 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	必須	特定個人情報に関する安全管理措置における物理的安全管理措置（特定個人情報等を取り扱う区域の管理）実施のための対策
	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	必須	特定個人情報に関する安全管理措置における物理的安全管理措置（特定個人情報等を取り扱う区域の管理）実施のための対策
	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保護 • 無線LANのアクセスポイント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保護	必須	特定個人情報に関する安全管理措置における物理的安全管理措置（特定個人情報等を取り扱う区域の管理）実施のための対策
	特権管理者・保守端末の管理	• 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 • 無線LANの特権管理者、保守端末を適正に管理	必須	特定個人情報に関する安全管理措置における物理的安全管理措置（特定個人情報等を取り扱う区域の管理）実施のための対策

注）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。

特定個人情報に関する安全管理措置実施のための対策イメージ（全体）

✓ 以下のイメージ図についてもガイドラインに挿入する。



（参考）「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）」の安全管理措置の規定との対応関係①

✓ 前回検討会で提示した内容を以下のとおり示す。

【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）」】

- 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）

特定個人情報に関する安全管理措置（行政機関等編）		対応
1 安全管理措置の検討手順		―
A 個人番号を取り扱う事務の範囲の明確化	**行政機関等は、個人番号利用事務等の範囲を明確にしておかなければならない。**	**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
C 事務取扱担当者の明確化	**行政機関等は、Aで明確化した事務に従事する事務取扱担当者を明確にしておかなければならない。**	
2 講ずべき安全管理措置の内容 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	**監査責任者は、特定個人情報等の管理の状況について、定期に及び必要に応じ随時に監査（注）（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。** **総括責任者は、監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。** **（注）監査の方法については、その実効性が担保される限りにおいて、デジタル技術を活用した方法によることも可能である。**	**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 ・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

（参考）「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）」の安全管理措置の規定との対応関係②

特定個人情報に関する安全管理措置（行政機関等編）			対応
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	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。**	**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	・**情報システム室等**に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。また、情報システム室等に特定個人情報等を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。 ・必要があると認めるときは、**情報システム室等**の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずる。 ・必要があると認めるときは、入室に係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。	**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
	② 情報システム室等の管理	・外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。	**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

（参考）「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）」の安全管理措置の規定との対応関係③

特定個人情報に関する安全管理措置（行政機関等編）		対応
E 物理的安全管理措置		―
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。**	**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
F 技術的安全管理措置		―
a アクセス制御	情報システムを使用して個人番号利用事務等を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。 «手法の例示» ＊ アクセス制御を行う方法としては、次に掲げるものが挙げられる。 ・ 特定個人情報ファイルを取り扱うことのできる情報システム端末等を限定する。 ・ 各情報システムにおいて、アクセスすることのできる特定個人情報ファイルを限定する。 ・ ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。 ・ 特定個人情報ファイルへのアクセス権を付与すべき者を最小化する。 ・ アクセス権を有する者に付与する権限を最小化する。 ・ 情報システムの管理者権限を有するユーザーであっても、情報システムの管理上特定個人情報ファイルの内容を知らなくてもよいのであれば、特定個人情報ファイルへ直接アクセスできないようにアクセス制御をする。 ・ 特定個人情報ファイルを取り扱う情報システムに導入したアクセス制御機能の脆弱性等を検証する。	**⑧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、アクセスを認可 ・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
b アクセス者の識別と認証	特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。 «手法の例示» ＊ 事務取扱担当者の識別方法としては、ユーザーＩＤ、パスワード、磁気・ＩＣカード、生体情報等が考えられる。	

（参考）「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）」の安全管理措置の規定との対応関係④

特定個人情報に関する安全管理措置（行政機関等編）		対応
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	情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組み等を導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。個人番号利用事務において使用する情報システムについて、**インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。** **«手法の例示»** ＊ 特定個人情報等を取り扱う情報システムと外部ネットワーク（又はその他の情報システム）との接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断することが考えられる。 ＊ 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入し、不正ソフトウェアの有無を確認することが考えられる。 ＊ 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とすることが考えられる。 ＊ 定期に及び必要に応じ随時にログ等の分析を行い、不正アクセス等を検知することが考えられる。→２Ｃｂ参照 ＊ 不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用することが考えられる。 ＊ 情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講ずることが考えられる。	**⑨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	**特定個人情報等をインターネット等により外部に送信する場合、通信経路における漏えい等を防止するための措置を講ずる。** **特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、暗号化又はパスワードにより秘匿する。** **«手法の例示»** ＊ 通信経路における漏えい等の防止策としては、通信経路の暗号化等が考えられる。 ＊ 暗号化又はパスワードによる秘匿に当たっては、不正に入手した者が容易に復元できないように、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮する。	**⑩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）

画面転送を利用した端末統合に関する改定案について

画面転送を利用した端末統合に関する改定案①

✓ **画面転送を利用して端末を統合し、マイナンバー利用事務系の業務を行う方式については、別紙にまとめて規定する**こととしてはいかがか。

現行：対策基準（解説）

３．情報システム全体の強靭性の向上
（Ⅰ）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離
　マイナンバー利用事務系においては、住民情報の流失を防ぐ必要があることから、他の領域（LGWAN接続系及びインターネット接続系）との通信をできないようにしなければならない。統合パッケージシステムを利用している場合であっても、マイナンバー利用事務系とLGWAN接続系との端末は分けなければならない。
（略）

改定案：対策基準（解説）

３．情報システム全体の強靭性の向上
（Ⅰ）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離
　マイナンバー利用事務系においては、住民情報の流失を防ぐ必要があることから、**画面転送技術により信頼される特定先と接続する場合を除いて、**他の領域（LGWAN接続系及びインターネット接続系）との通信をできないようにしなければならない。~~統合パッケージシステムを利用している場合であっても、マイナンバー利用事務系とLGWAN接続系との端末は分けなければならない。~~**他のネットワーク系統で利用している端末から、画面転送技術を利用してマイナンバー利用事務系の業務を行う場合については、 別紙「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」に規定する。**
（略）

画面転送を利用した端末統合に関する改定案②

✓ マイナンバー利用事務系と、LGWAN接続系やインターネット接続系との特定通信について、現行の規定のままでは画面転送の通信も認めないことになるため、画面転送技術を利用する場合については、特定通信として接続することを認める形に修正する。

現行：対策基準（解説）

３．情報システム全体の強靭性の向上
（１）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離
（中略）
マイナンバー利用事務系と外部との通信の必要がある場合は、通信経路の限定（MACアドレス、IPアドレス）に加えて、アプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。これらの限定を行った通信を特定通信という。
特定通信を行う際は、以下の点に留意しなければならない。
（ア）L2SW/L3SWによる通信経路限定、ファイアウォールによる通信プロトコル限定等を行うことで通信を制限すること。
（イ）その他外部ネットワークとの通信が発生する場合は専用回線サービス（IP-VPNやSSL-VPNなど仮想技術を利用した通信を含む）を検討すること。
（ウ）特定通信は、マイナンバー利用事務系が、住民基本台帳ネットワーク、中間サーバ連携、コンビニ交付やLGWAN-ASPサービスなど接続先が信頼される特定先との通信のことであり、マイナンバー利用事務系は、LGWAN接続系やインターネット接続系と特定通信として接続してはならない。
（中略）

改定案：対策基準（解説）

３．情報システム全体の強靭性の向上
（１）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離
（中略）
マイナンバー利用事務系と外部との通信の必要がある場合は、通信経路の限定（MACアドレス、IPアドレス）に加えて、アプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。これらの限定を行った通信を特定通信という。
特定通信を行う際は、以下の点に留意しなければならない。
（ア）L2SW/L3SWによる通信経路限定、ファイアウォールによる通信プロトコル限定等を行うことで通信を制限すること。
（イ）その他外部ネットワークとの通信が発生する場合は専用回線サービス（IP-VPNやSSL-VPNなど仮想技術を利用した通信を含む）を検討すること。
（ウ）特定通信は、マイナンバー利用事務系が、住民基本台帳ネットワーク、中間サーバ連携、コンビニ交付やLGWAN-ASPサービスなど接続先が信頼される特定先との通信のことであり、マイナンバー利用事務系は、**「別紙「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」に規定される方式を除いて**LGWAN接続系やインターネット接続系と特定通信として接続してはならない。
（中略）

画面転送を利用した端末統合に関する改定案③

✓ 特定通信となる外部接続の例についての箇所にも、別紙を参照する旨規定してはいかがか。

現行：対策基準（解説）

３．情報システム全体の強靭性の向上
（Ⅰ）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離
（中略）
（ウ）特定通信は、マイナンバー利用事務系が、住民基本台帳ネットワーク、中間サーバ連携、コンビニ交付やLGWAN-ASPサービスなど接続先が信頼される特定先との通信のことであり、マイナンバー利用事務系は、LGWAN接続系やインターネット接続系と特定通信として接続してはならない。
特定通信となる外部接続の例として、住民基本台帳ネットワークシステム、マイナンバー制度における中間サーバ連携や住民票の写し等のコンビニ交付用のLGWAN 接続、データバックアップセンターや共同利用／クラウドセンター等、十分に情報セキュリティが確保された通信先との限定的な接続がある。また、特定通信を行う外部接続先についても、インターネット等と接続されていてはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、LGWAN を経由してマイナンバー利用事務系にデータの移送を可能とする。
（中略）

改定案：対策基準（解説）

３．情報システム全体の強靭性の向上
（Ⅰ）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離
（中略）
（ウ）特定通信は、マイナンバー利用事務系が、住民基本台帳ネットワーク、中間サーバ連携、コンビニ交付やLGWAN-ASPサービスなど接続先が信頼される特定先との通信のことであり、マイナンバー利用事務系は、**「別紙「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」に規定される方式を除いて**LGWAN接続系やインターネット接続系と特定通信として接続してはならない。
特定通信となる外部接続の例として、住民基本台帳ネットワークシステム、マイナンバー制度における中間サーバ連携や住民票の写し等のコンビニ交付用のLGWAN 接続、データバックアップセンターや共同利用／クラウドセンター等、十分に情報セキュリティが確保された通信先との限定的な接続がある。**なお、上記に関し、画面転送技術を利用して他のネットワーク系統で利用している端末から、画面転送技術を利用してマイナンバー利用事務系の業務を行う場合については、 別紙「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」を参照すること。**また、特定通信を行う外部接続先についても、インターネット等と接続されていてはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、LGWAN を経由してマイナンバー利用事務系にデータの移送を可能とする。
（中略）