資料１

番号法関連規定を踏まえた
マイナンバー利用事務系に係る画面転送・無線LAN利用について

総 務 省

令和６年11月27日

マイナンバー利用事務系の画面転送・無線LAN利用（※前回検討会において提示）

- ✓ 現行のガイドラインでは、**マイナンバー利用事務系以外の無線LANの利用が認められており**、盗聴対策や無許可での接続禁止が規定されている他、**「庁内無線LANのセキュリティ要件について」にセキュリティ要件が規定**されている。
- ✓ **国・地方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で提示された端末1台化に伴い、 LGWAN接続系端末や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に画面転送によるアクセスにおいて、無線LANを利用する形態ができる。**
- ✓ **従来のマイナンバー利用事務系端末から無線LANを利用したマイナンバー利用事務系システムへのアクセスの形態の要求もある。**

第3編　第2章 情報セキュリティ対策基準（解説）

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

6.技術的セキュリティ　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。

（注１０）暗号化方式の1つであるWEP（Wired Equivalent Privacy）/WPA（Wi-Fi Protected Access）については、既に脆弱性が公知となっているため、暗号強度が確認されている暗号方式（WPA2/WPA3）を採用しなければならない。

（注１１）アクセスポイントの管理者パスワードを適切に設定（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など）を行うとともに、無線端末間の通信が行われないよう適切な設定を行わなければならない。また、無線LANの不正利用調査を行い、探査ツール等を用い、無許可のアクセスポイントや使用されていないアクセスポイントが設置されていないことを点検することも有益である。

（１９）業務外ネットワークへの接続の禁止

セキュリティ上、ネットワークとの接続には適正な管理が必要であることから、無許可での接続を禁止する。あわせて、接続が許可されたものであることを確認するための措置を講じるとともに、許可手続を定める必要がある。（支給された端末以外を接続する場合も同様とする。）

（注１８）特に、庁内で無線LANを使用している場合に、職員等や委託事業者がパソコンやモバイル端末等を持込み、無許可でアクセスポイントへ接続する行為を禁止する必要がある。

庁内無線LANの想定されるリスクとセキュリティ対策（※前回検討会において提示）

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

無線LANの利用におけるリスクは、様々な角度から公表されている。無線LANの利用者に対する脅威、無線LANの設置者に対する脅威、無線LAN機器の脆弱性、などリスクが想定される。

脅威	考慮すべきリスク	リスクの概要	対策	脅威への技術的なセキュリティ対策
盗聴	無線LAN区間における通信内容の窃取及び改ざん	悪意のある第三者により無線LAN区間の通信を傍受され、通信内容が窃取及び改ざんされるおそれがある。	◎	WPA2/WPA3 の採用と適切な設定
			◎	アクセスポイントの管理者パスワードの適切な設定
不正アクセス	内部ネットワークへの侵入	悪意のある第三者に無線LANに不正に接続されることによって、内部の資産が窃取、改ざん及び破壊されるおそれがある。	◎	WPA2/WPA3 の採用と適切な設定
			◎	アクセスポイントの管理者パスワードの適切な設定
			○	電波の伝搬範囲の適切な設定（※1）
			○	ログの収集・保存・分析
			△	無線IDS/IPSの導入
	利用者へのなりすまし	悪意のある第三者に無線LANのアクセスポイントに不正に接続されることによって、当該無線LANの正当な利用者になりすまして、内部のネットワークからインターネット等の外部のネットワークに接続されるおそれがある。	◎	WPA2/WPA3 の採用と適切な設定
			◎	アクセスポイントの管理者パスワードの適切な設定
			○	電波の伝搬範囲の適切な設定（※1）
			○	ログの収集・保存・分析
			△	無線IDS/IPSの導入
	通信の妨害	悪意のある第三者によって、大量のパケット等が送信されることによるDoS（Denial of Service）攻撃、不正な電波発生源が設置されることによる電波干渉等により、通信速度が低下する又は通信が不可能となるおそれがある。	○	ログの収集・保存・分析
			△	管理フレームの暗号化・改ざん検知（IEEE802.11w）
			△	電波状況の監視
			△	無線IDS/IPSの導入
なりすましAP	不正なアクセスポイントによる通信内容の窃取	悪意のある第三者により不正なアクセスポイントが設置され、当該アクセスポイントを正規のアクセスポイントと誤認させられた利用者の端末が接続することで、通信内容が窃取されるおそれがある。また、外部ネットワーク(公衆 Wi-Fi や私物 Wi-Fi ルーター) に庁内端末が誤接続することにより、通信内容が外部に漏れる場合がある。	◎	WPA2/WPA3 の採用と適切な設定
			△	電波状況の監視
			△	無線IDS/IPSの導入

対策レベル 【 ◎:必須対策、○:追加的に実施することが有効な対策、△:情報セキュリティ対策をより強固にする場合に検討する対策 】

（※1）情報セキュリティ上の脅威に対する直接的な対策ではないが、電波の伝搬範囲を必要最低限とすることで、アクセスポイントの存在を悪意ある第三者に知らしめる危険性等を低減する効果が期待される。なお、電波の伝搬範囲は、アクセスポイントの設置箇所周辺の状況等の影響を受けるため、一定ではないことを注意する必要がある。

LGWAN接続系での無線LAN利用の要件（※前回検討会において提示）

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

分類		要件	区分
技術的対策	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。	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
運用による対策	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) また、無線端末間どうしの通信が行われないよう適切な設定を行う。	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
	LGWAN接続端末の設定	LGWAN接続系で許可されたアクセスポイントのSSIDのみを表示し、LGWAN接続系のみ接続する設定とし、LGWAN接続系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 (LGWAN接続系から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

前回検討会を踏まえた対応

■ 令和２年に示された「庁内無線LANのセキュリティ要件」を、明示的に「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下「ガイドライン」という。）に規定。

発言要旨
• **LGWAN 接続系における無線LAN利用に関する要件をさらに厳しくする方向になる**と思う。 • アクセスポイントの管理は、機器認証をクラウド側に束ねているやり方が増えているので、特定のシステムが想定されすぎないようにしないといけないと考える。 • 自治体の場合はリース物件を用いる場合があり、無線LANのセキュリティキー等々がそのままの形でリースバックされてしまう可能性がある。その場合は、誰もがアクセス可能な状態になってしまう。 • アクセスポイント管理に端末同士の通信が行われないように適切な設定があるが、動かなくなるアプリケーションが出るパターンを危惧している。

⇒　次回、ガイドラインの改定案を提示予定

■ マイナンバー利用事務系は特定個人情報を取り扱うため、**個人情報保護法・番号法上の安全管理措置との関係で論点となる部分を洗い出し、必要な対策を規定**する。
（端末を１台に集約する場合含め検討が必要）

今回提示

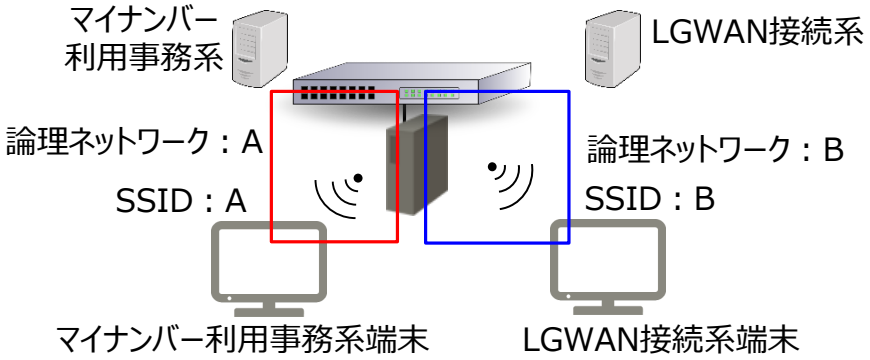
マイナンバー利用事務系における無線LAN利用（端末を分離する場合）

- マイナンバー利用事務系の端末を分離した上で無線LANを利用する場合、SSIDを分けた上でVLANで論理分離を行うことが考えられる。

無線LAN

端末分離

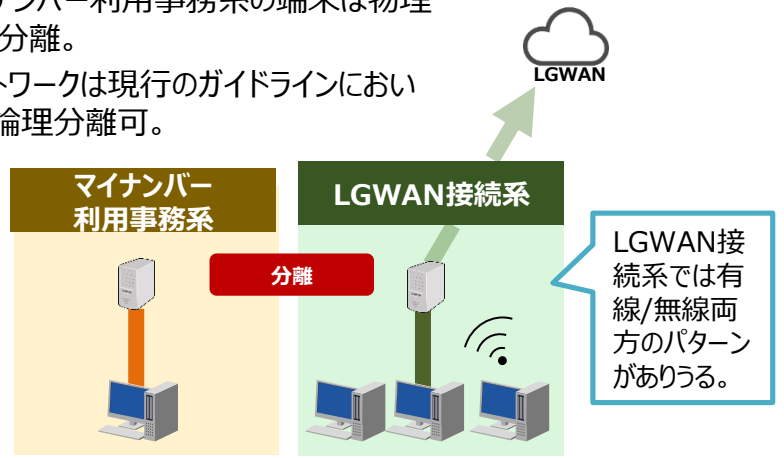
- 端末は物理的に分離し、SSID（ネットワークの識別子）を分け、VLANで論理分離を行う。



有線LAN

従来

- マイナンバー利用事務系の端末は物理的に分離。
- ネットワークは現行のガイドラインにおいても論理分離可。



参考）ステルスSSIDについて

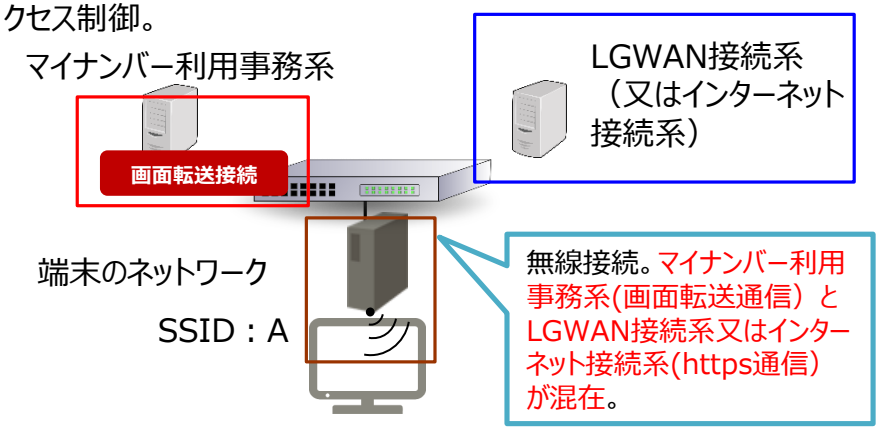
- ステルスSSIDを利用する場合、無線LANアクセスポイント（AP）が、SSIDを知らせる信号を停止するため、**端末のSSID一覧にステルスSSIDは表示されず、第3者が無線LANに接続する可能性が低くなる**。
- しかし、正規の端末からステルスSSIDに接続する際、**ステルスSSIDが漏えいする可能性がある（実際に漏えいしているケースも存在）**。
- また、**SSIDのステルス化とは関係なく、無線通信の暗号化、無線APへの接続時の認証(例：EAP-TLS）により、盗聴防止、不正アクセスの防止対策は必須**である

マイナンバー利用事務系における無線LAN利用（端末を１台に統合する場合）

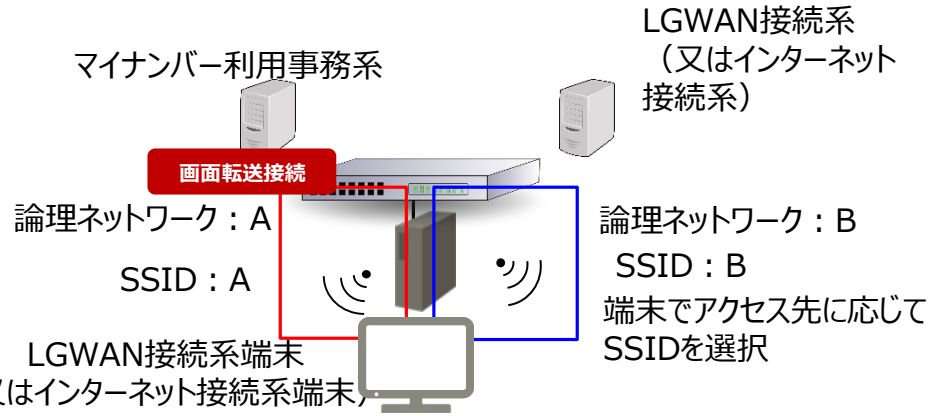
- 端末を統合する場合においても、**SSIDの分離によりネットワークの分離が可能**と考えられる（パターン②）。
- 端末を１台に統合し有線LANを利用する場合と同じパターン（パターン①）を考えた場合、**マイナンバー利用事務系に係る画面転送の通信と、他のネットワーク系統の通信が混在する形になり、アクセス制御により通信をコントロールする**形になる。

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。

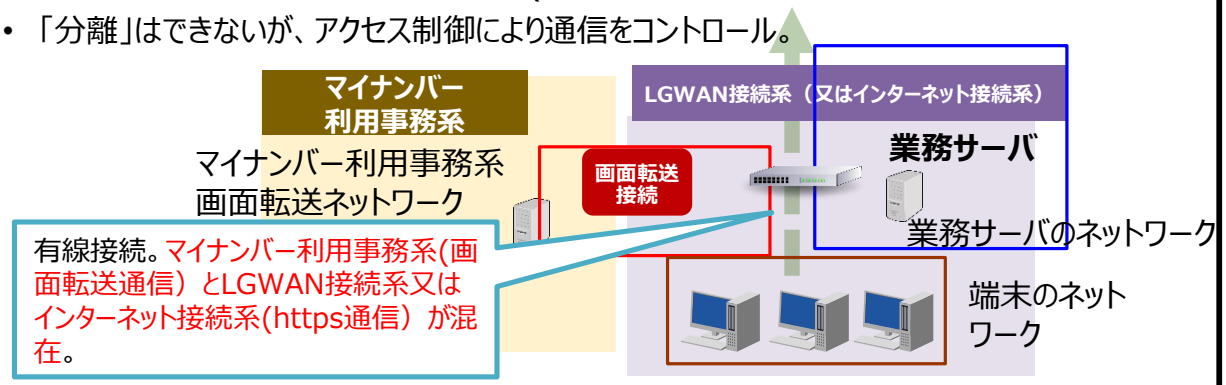


② 端末は集約するが、SSIDを分け、VLANで論理ネットワークにより分離。



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。

番号法上の安全管理措置との関係

- 「安全管理措置の検討手順」関係　　P９ ～ 11
- 「講ずべき安全管理措置の内容」関係　　P12 ～ P29
  - 「組織的安全措置」関係　　P12 ～ 17
  - 「物理的安全管理措置」関係　　P18 ～ 24
  - 「技術的安全管理措置」関係　　P25 ～ 29
- 安全管理措置実施のための対策イメージ（全体）　P30

※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

番号法上の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。

◎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。

「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

【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）

○：画面転送・無線LAN利用に係る対策について関連の深い事項
×：画面転送・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
１ 安全管理措置の検討手順	行政機関等は、個人番号及び特定個人情報（以下「特定個人情報等」という。）の取扱いを検討するに当たって、個人番号を取り扱う事務の範囲及び特定個人情報等の範囲を明確にした上で、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。）を明確にしておく必要がある。 これらを踏まえ、特定個人情報等の適正な取扱いの確保について組織として取り組むために、特定個人情報等の安全管理に関する基本方針（以下「基本方針」という。）を策定することが重要である。 行政機関等は、個人情報の保護に関する取扱規程等の見直し等を行い、特定個人情報等を取り扱う体制の整備及び情報システムの改修等を行う必要がある。 行政機関等は、特定個人情報等の取扱いに関する安全管理措置について、次のような手順で検討を行う必要がある。検討に際し、特定個人情報保護評価を実施した事務については、Ａ～Ｃを省略し、Ｄ～Ｅを実施することも考えられる。	－	－
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。**	○	○
Ｂ 特定個人情報等の範囲の明確化	行政機関等は、Ａで明確化した事務において取り扱う特定個人情報等の範囲を明確にしておかなければならない（注）。 （注）特定個人情報等の範囲を明確にするとは、事務において使用される個人番号及び個人番号と関連付けて管理される個人情報（氏名、生年月日等）の範囲を明確にすることをいう。 個人番号利用事務等において使用される個人番号及び個人番号と関連付けて管理される個人情報の範囲を明確にする要求事項のため、対象外	×	×
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。**	○	○
Ｄ 基本方針の策定	特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。→２ Ａ参照 基本方針を策定することへの要求事項のため、対象外	×	×
Ｅ 取扱規程等の見直し等	行政機関等は、個人情報の保護に関する取扱規程等の見直し等を行わなければならない。 →２ Ｂ参照 規程類の見直しを行うことへの要求事項のため、対象外	×	×

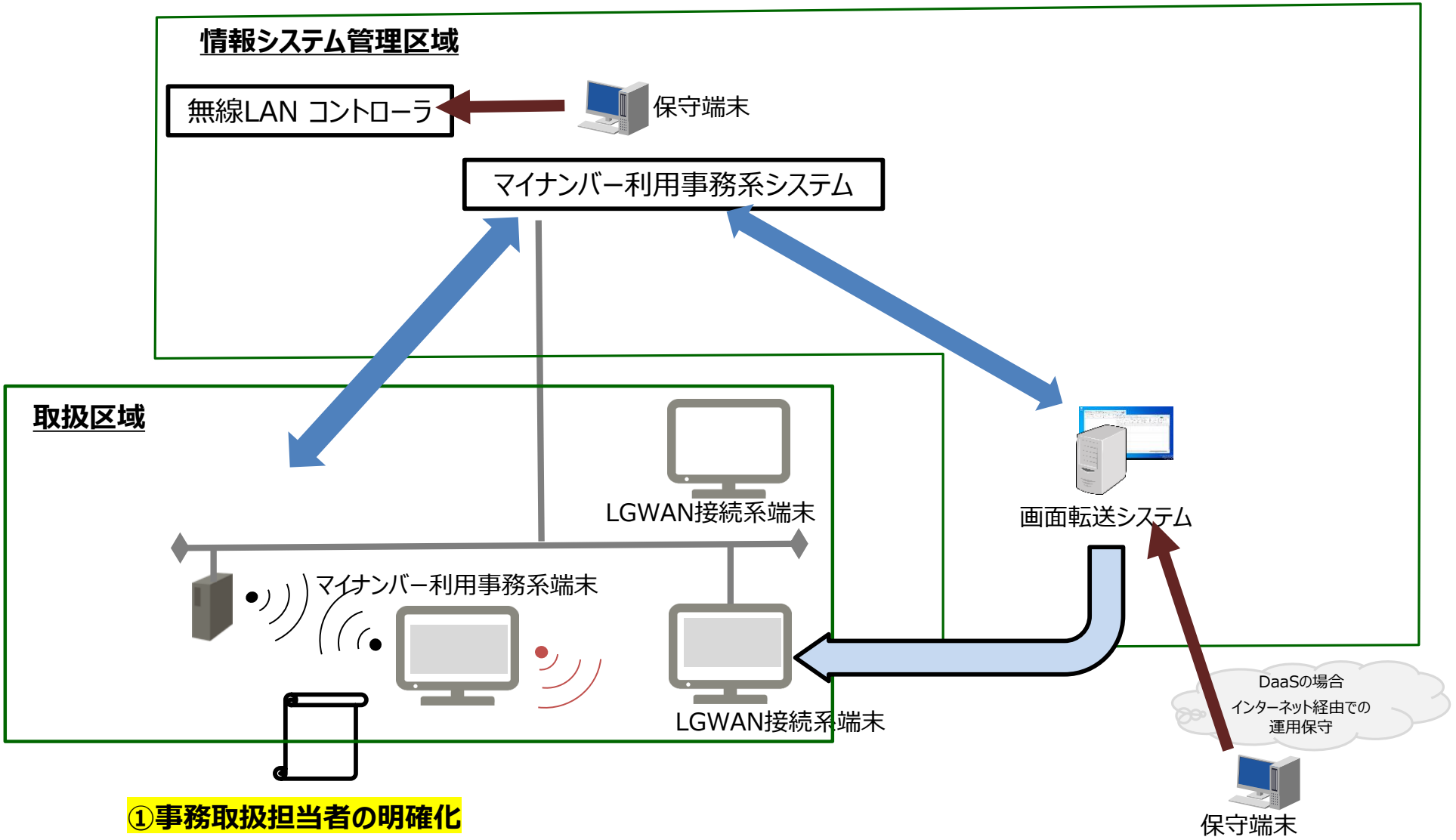
安全管理措置の検討手順の実施のための対策

✓ 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	－	－
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	

安全管理措置の検討手順実施のための対策イメージ



①事務取扱担当者の明確化

「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

○：画面転送・無線LAN利用に係る対策について関連の深い事項
×：画面転送・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
2 講ずべき安全管理措置の内容	本セクション２においては、特定個人情報等の保護のために必要な安全管理措置について本文で示し、その具体的な手法の例示を記述している。なお、手法の例示は、これに限定する趣旨で記載したものではなく、また、個別ケースによって別途考慮すべき要素があり得るので注意を要する。 行政機関等は、安全管理措置を講ずるに当たり、番号法、個人情報保護法等関係法令、本ガイドライン、個人情報保護法ガイドライン（行政機関等編）、事務対応ガイド及び政府機関等のサイバーセキュリティ対策のための統一基準等に準拠した各府省庁等における情報セキュリティポリシー等を遵守することを前提とする。 なお、地方公共団体においては、これらに加え、地方公共団体における情報セキュリティポリシーに関するガイドライン等を参考に地方公共団体において策定した情報セキュリティポリシー等を遵守することを前提とする。 個人番号と個人情報を紐付ける登録事務（以下「個人番号登録事務」という。）を実施する行政機関等は、デジタル庁が策定した「マイナンバー利用事務におけるマイナンバー登録事務に係る横断的なガイドライン」及び各制度の所管省庁等が策定した個人番号登録事務に係るガイドライン等を遵守することを前提とする。 行政機関等は、特定個人情報保護評価を実施した事務については、その内容を遵守するものとする。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等を遵守することを前提とする。	－	－
A 基本方針の策定	特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。 基本方針を策定することの要求事項のため、対象外	×	×
B 取扱規程等の見直し等	１Ａ～Ｃで明確化した事務において事務の流れを整理し、特定個人情報等の具体的な取扱いを定めるために、取扱規程等の見直し等を行わなければならない。特に、特定個人情報等の複製及び送信、特定個人情報等が保存されている電子媒体等の外部への送付及び持ち出し等については、責任者の指示に従い行うことを定めること等が重要である。 «手法の例示» ＊ 取扱規程等は、次に掲げる管理段階ごとに、取扱方法、責任者・事務取扱担当者及びその任務等について定めることが考えられる。具体的に定める事項については、C～F に記述する安全管理措置を織り込むことが重要である。 ① 取得段階 ② 利用段階 ③ 保存段階 ④ 提供段階 ⑤ 削除・廃棄段階 ＊ 個人番号利用事務の場合、例えば、次のような事務フローに即して、手続を明確にしておくことが重要である。 ① 住民等からの申請書を受領する方法（本人確認、個人番号の確認等） ② 住民等からの申請書をシステムに入力・保存する方法 ③ 個人番号を含む証明書等の作成・印刷方法 ④ 個人番号を含む証明書等を住民等に交付する方法 ⑤ 申請書及び本人確認書類等の保存方法 ⑥ 保存期間を経過した書類等の廃棄方法 ＊ 特定個人情報等の取扱いにおける人的ミスの発生を防止するため、本人確認及び個人番号の確認の手順、個人番号と個人情報の紐付けの際の複数人による確認（責任者による最終確認を含む。）等の確認の手順、情報連携を行う際の作業手順等、各管理段階における具体的な手順について、取扱規程等において明確にしておくことが重要である。 ＊ 取扱規程等は、関係法令、制度所管省庁によるガイドライン、通達等を踏まえ、継続的に見直しを行うことが重要である。 規程類の見直しを行うことの要求事項のため、対象外	×	×

「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

○：画面転送・無線LAN利用に係る対策について関連の深い事項
×：画面転送・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
2 講ずべき安全管理措置の内容		–	–
C 組織的安全管理措置	行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。	–	–
a 組織体制の整備	安全管理措置を講ずるための組織体制を整備する。 行政機関等は、組織体制の整備として、次に掲げる事項を含める。 ・総括責任者（行政機関等に各１名）の設置及び責任の明確化 ・保護責任者（個人番号利用事務等を実施する課室等に各１名）の設置及び責任の明確化 ・監査責任者の設置及び責任の明確化 ・事務取扱担当者及びその役割の明確化 ・事務取扱担当者が取り扱う特定個人情報等の範囲の明確化 ・特定個人情報等の取扱いにおける人的ミスの発生を防止するための確認体制の整備 ・事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制の整備 ・個人番号の漏えい、滅失又は毀損等（以下「漏えい等」という。）事案の発生又は兆候を把握した場合の職員から責任者等への報告連絡体制の整備 ・特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化 組織体制の整備を行うことの要求事項のため、対象外	×	×
b 取扱規程等に基づく運用	取扱規程等に基づく運用を行うとともに、その状況を確認するため、特定個人情報等の利用状況等を記録し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する。記録については、改ざん、窃取又は不正な削除の防止のために必要な措置を講ずるとともに、分析等を行う。 «手法の例示» ＊ 記録する項目としては、次に掲げるものが挙げられる。 ・特定個人情報ファイルの利用・出力状況の記録 ・書類・媒体等の持ち運びの記録 →「持ち運び」については、２Ｅｃ参照 ・特定個人情報ファイルの削除・廃棄記録 ・削除・廃棄を委託した場合、これを証明する記録等 ・特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録 ＊ 情報システムの利用状況等の記録に関する分析等としては、ログイン実績、アクセスログ等を定期に及び必要に応じ随時に分析することが考えられる。また、ログと関連する書面の記録を照合し、確認することが考えられる。 →２Ｆｃ参照 規程に基づく運用を行うことの要求事項のため、対象外	×	×

「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

○：画面転送・無線LAN利用に係る対策について関連の深い事項
×：画面転送・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
2 講ずべき安全管理措置の内容		－	－
C 組織的安全管理措置	行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。	－	－
c 取扱状況を確認する手段の整備	特定個人情報ファイルの取扱状況を確認するための手段を整備する。行政機関等は、次に掲げる項目を含めて記録する。 なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。 ・特定個人情報ファイルの名称 ・行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称 ・特定個人情報ファイルの利用目的 ・特定個人情報ファイルに記録される項目及び本人として特定個人情報ファイルに記録される個人の範囲 ・特定個人情報ファイルに記録される特定個人情報等の収集方法 特定個人情報ファイルの取扱状況を確認するための手段を整備することの要求事項のため、対象外	×	×
d 漏えい等事案に対応する体制等の整備	漏えい等事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制及び手順等を整備する。 漏えい等事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。 （※）行政機関等において、漏えい等事案が発生した場合等の対応の詳細については、「（別添２）特定個人情報の漏えい等に関する報告等（行政機関等編）」を参照のこと。 «手法の例示» ＊ 漏えい等事案の発生時に、次のような対応を行うことを念頭に、体制及び手順等を整備することが考えられる。 ・漏えい等事案が発覚した際の報告・連絡等 ・事実関係の調査及び原因の究明 ・影響を受ける可能性のある本人への通知 ・委員会への報告 ・再発防止策の検討及び決定 ・事実関係及び再発防止策等の公表 ＊ 不正アクセス、ウイルス感染の事案に加え、標的型攻撃等の被害を受けた場合の対応について、関係者において定期的に確認又は訓練等を実施することが考えられる。 漏えい等事案の発生又は兆候を把握時の体制及び手順等を整備することの要求事項のため、対象外	×	×

「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

○：画面転送・無線LAN利用に係る対策について関連の深い事項
×：画面転送・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
2 講ずべき安全管理措置の内容		－	－
C 組織的安全管理措置	行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。	－	－
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。**	○	○
D 人的安全管理措置	行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。	－	－
a 事務取扱担当者の監督	総括責任者及び保護責任者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。 事務取扱担当者に対する監督責任に関する要求事項のため、対象外	×	×
b 事務取扱担当者等の教育	総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。 また、特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、特定個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。 総括責任者は、保護責任者に対し、課室等における特定個人情報等の適切な管理のために必要な教育研修を行う。 前記教育研修については、教育研修への参加の機会を付与するとともに、研修未受講者に対して再受講の機会を付与する等の必要な措置を講ずる。 なお、サイバーセキュリティの研修については、番号法に基づき特定個人情報ファイルを取り扱う事務に従事する者に対して、次に掲げるところにより、特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティ（「サイバーセキュリティ基本法」（平成 26 年法律第104 号）第２条に規定するサイバーセキュリティをいう。）の確保に関する事項その他の事項に関する研修を行う（番号法第 29 条の２、番号法施行令第 32 条）。 ・研修の計画をあらかじめ策定し、これに沿ったものとすること。 ・研修の内容は、特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティの確保に関する事項として、情報システムに対する不正な活動その他のサイバーセキュリティに対する脅威及び当該脅威による被害の発生又は拡大を防止するため必要な措置に関するものを含むものとすること。 ・特定個人情報ファイルを取り扱う事務に従事する者の全てに対して、おおむね一年ごとに研修を受けさせるものとすること。 事務取扱担当者への教育に関する要求事項のため、対象外	×	×
c 法令・内部規程違反等に対する厳正な対処	法令又は内部規程等に違反した職員に対し、法令又は内部規程等に基づき厳正に対処する。 法令又は内部規程等に違反した職員の対処に関する要求事項のため、対象外	×	×

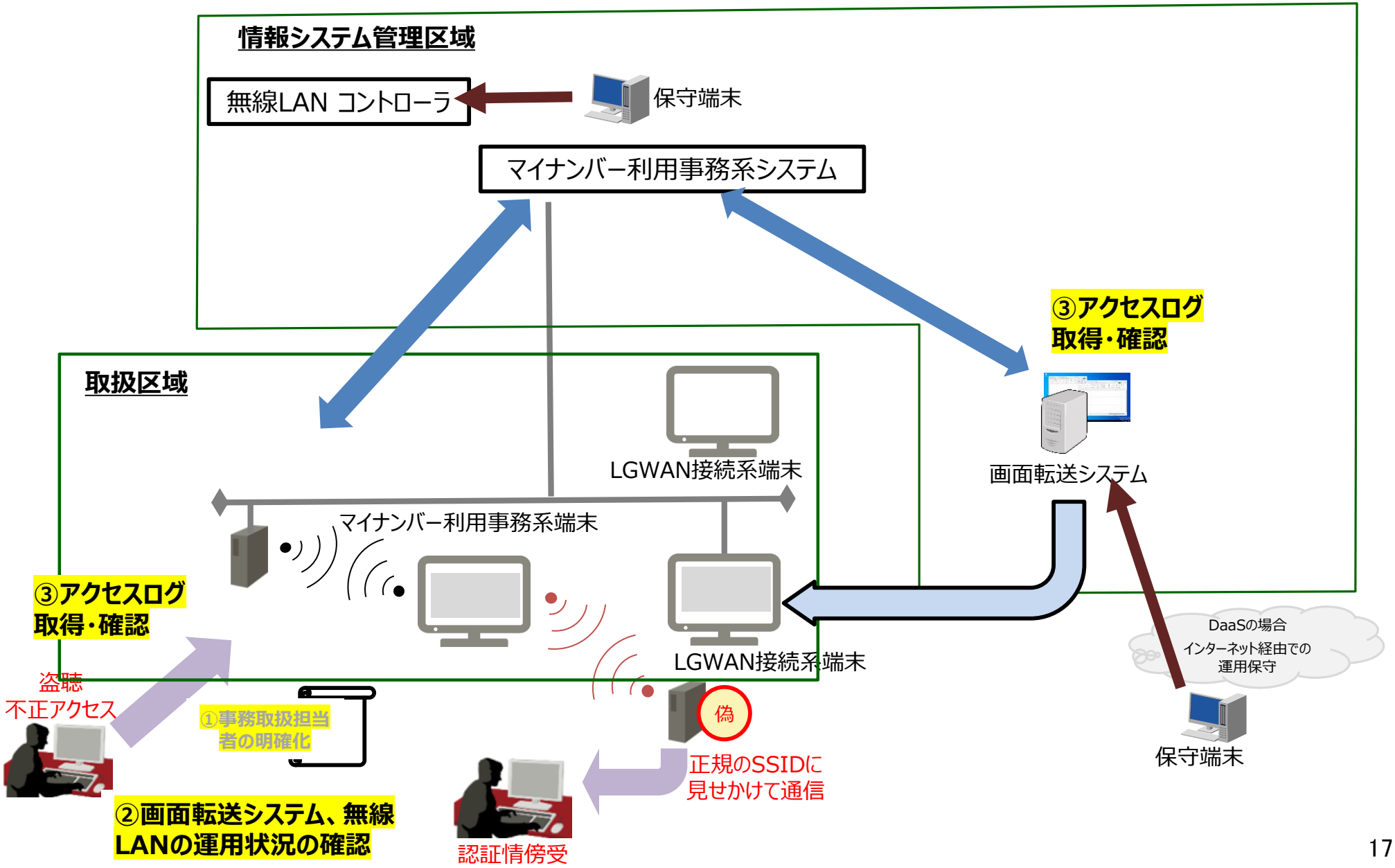
組織的安全管理措置の実施のための対策

✓ 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

組織的安全管理措置実施のための対策イメージ



「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

○：画面転送・無線LAN利用に係る対策について関連の深い事項
×：画面転送・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
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。 ガイドライン「第2編 第2章 4.2.管理区域（情報システム室等）の管理」に関連の規定あり	○	○
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。	○	○
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。	○	○
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。 ガイドライン「第2編 第2章 4.4.職員等の利用する端末や電磁的記録媒体等の管理」 「第2編 第2章 5.1.職員等の遵守事項」に関連の規定あり «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。**	○	○

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	

「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

○：画面転送システム・無線LAN利用に係る対策について関連の深い事項
×：画面転送システム・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
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	－	－
c 電子媒体等の取扱いにおける漏えい等の防止	**許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずる**。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。 取扱規程等の手続に基づき、特定個人情報等が記録された電子媒体又は書類等を持ち運ぶ必要が生じた場合には、容易に個人番号が判明しないよう安全な方策を講ずる。 **「持ち運ぶ」とは、特定個人情報等を管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、庁舎内での移動等であっても、特定個人情報等の紛失・盗難等に留意する必要がある。** ガイドライン「第２編第２章「第2編 第2章　3.情報システム全体の強靭性の向上」 「第2編 第2章　4.4.職員等の利用する端末や電磁的記録媒体等の管理」 「第2編 第2章　5.1.職員等の遵守事項」 「第3編 第3章　6.2. アクセス制御」に関連する規定あり **«手法の例示»** ＊ 特定個人情報等が記録された電子媒体を安全に持ち運ぶ方法としては、持ち出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。 ＊ 特定個人情報等が記載された書類等を安全に持ち運ぶ方法としては、封緘、目隠しシールの貼付を行うこと等が考えられる。	○	○
d 個人番号の削除、機器及び電子媒体等の廃棄	特定個人情報等が記録された電子媒体及び書類等について、文書管理に関する規程等によって定められている保存期間を経過した場合には、個人番号をできるだけ速やかに復元不可能な手段で削除又は廃棄する。 →ガイドライン第４－３－(4)Ｂ参照 個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したこと について、証明書等により確認する。 «手法の例示» ＊ 特定個人情報等が記載された書類等を廃棄する場合、焼却又は溶解、復元不可能な程度に細断可能なシュレッダーの利用、個人番号部分を復元不可能な程度にマスキングすること等の復元不可能な手段を採用することが考えられる。 ＊ 特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用することが考えられる。 ＊ 特定個人情報等を取り扱う情報システム又は機器等において、特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合、容易に復元できない手段を採用することが考えられる。 ＊ 個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定めることが考えられる。 特定個人情報等が記載された書類等を廃棄に関する要求事項のため、対象外	×	×

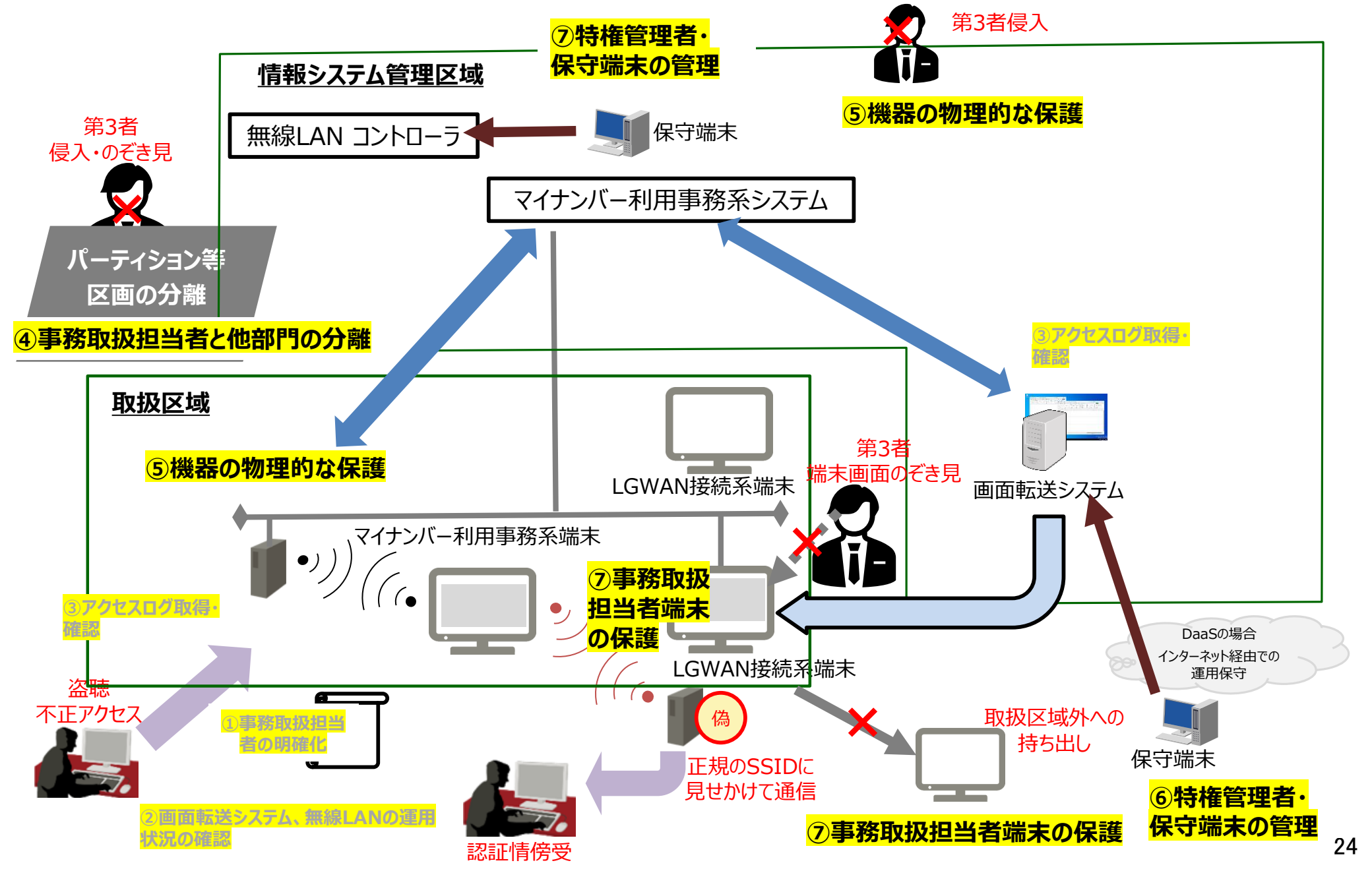
現行のガイドラインにおいては、原則、USBメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定する旨規定

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**	

物理的安全管理措置実施のための対策イメージ



「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

○：画面転送・無線LAN利用に係る対策について関連の深い事項　×：画面転送・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
2 講ずべき安全管理措置の内容		－	－
F 技術的安全管理措置	行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。	－	－
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**。 ガイドライン 「第2編 第2章　6.1.コンピュータ及びネットワークの管理」 「第2編 第2章　6.2.アクセス制御」に関連の規定あり	○	○
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。 ガイドライン 「第2編 第2章　3.情報システム全体の強靭性の向上」 「第2編 第2章　4.4.職員等の利用する端末や電磁的記録媒体等の管理」 「第2編 第2章　6.1.コンピュータ及びネットワークの管理」に関連の規定あり	○	○

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導出予定）

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

「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

○：画面転送・無線LAN利用に係る対策について関連の深い事項　×：画面転送・無線LAN利用に係る対策について関連の薄い事項

項目名	説明	画面転送	無線LAN
2 講ずべき安全管理措置の内容		－	－
F 技術的安全管理措置	行政機関等は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。	－	－
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。 ガイドライン「第2編 第2章　3.情報システム全体の強靭性の向上」 「第3編 第3章　3.情報システム全体の強靭性の向上」に関連の規定あり	○	○
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。** ガイドライン　「第2編 第2章　6.1.コンピュータ及びネットワークの管理」 「第3編 第3章　4.3.通信回線及び通信回線装置の管理」に関連の規定あり **«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。	○	○
G 外的環境の把握	行政機関等が、外国において特定個人情報等を取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、特定個人情報等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。 外国において特定個人情報の取り扱いに関する要求事項のため、対象外	×	×

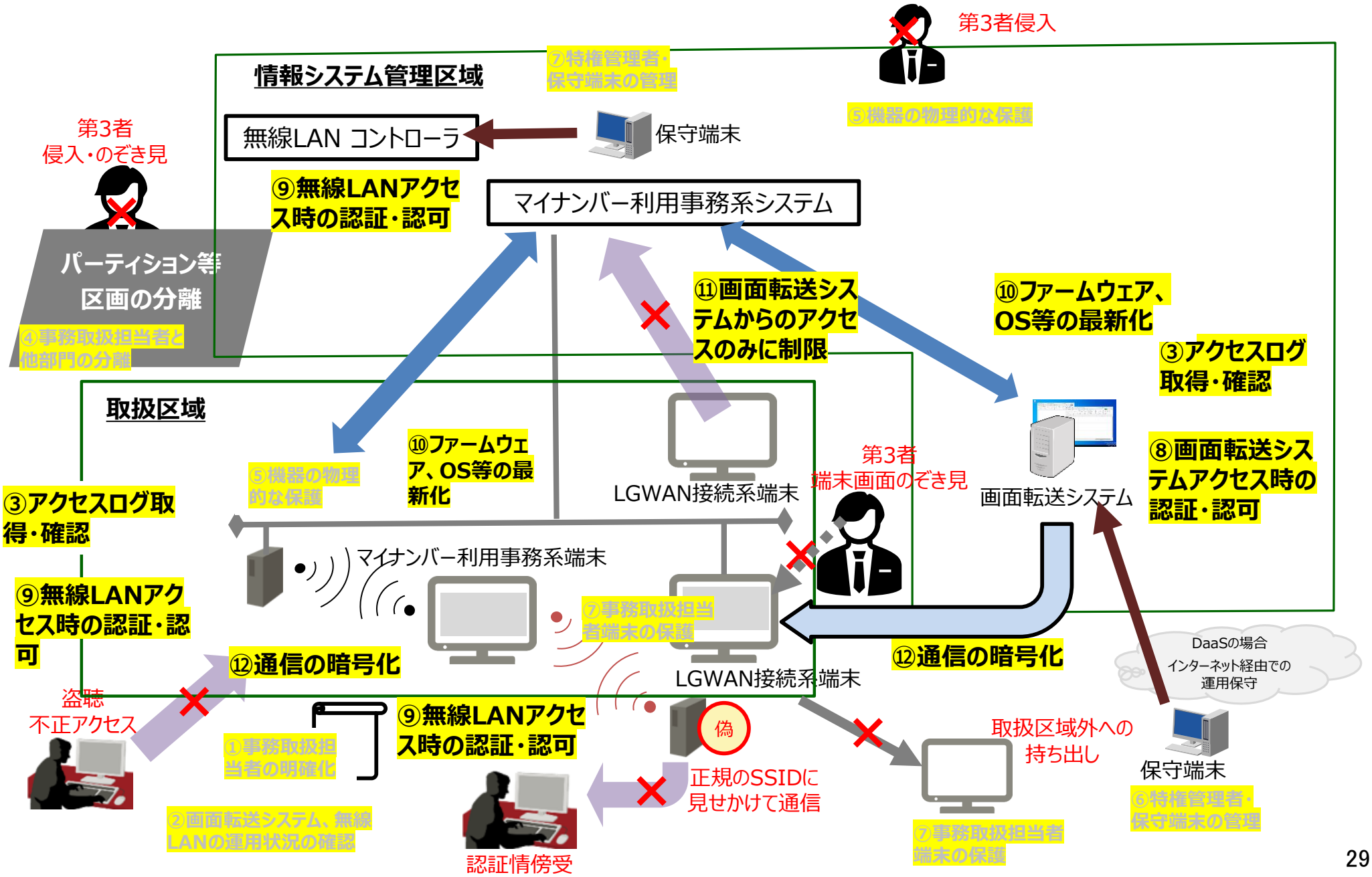
技術的安全管理措置の実施のための対策②

✓ 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導出予定）

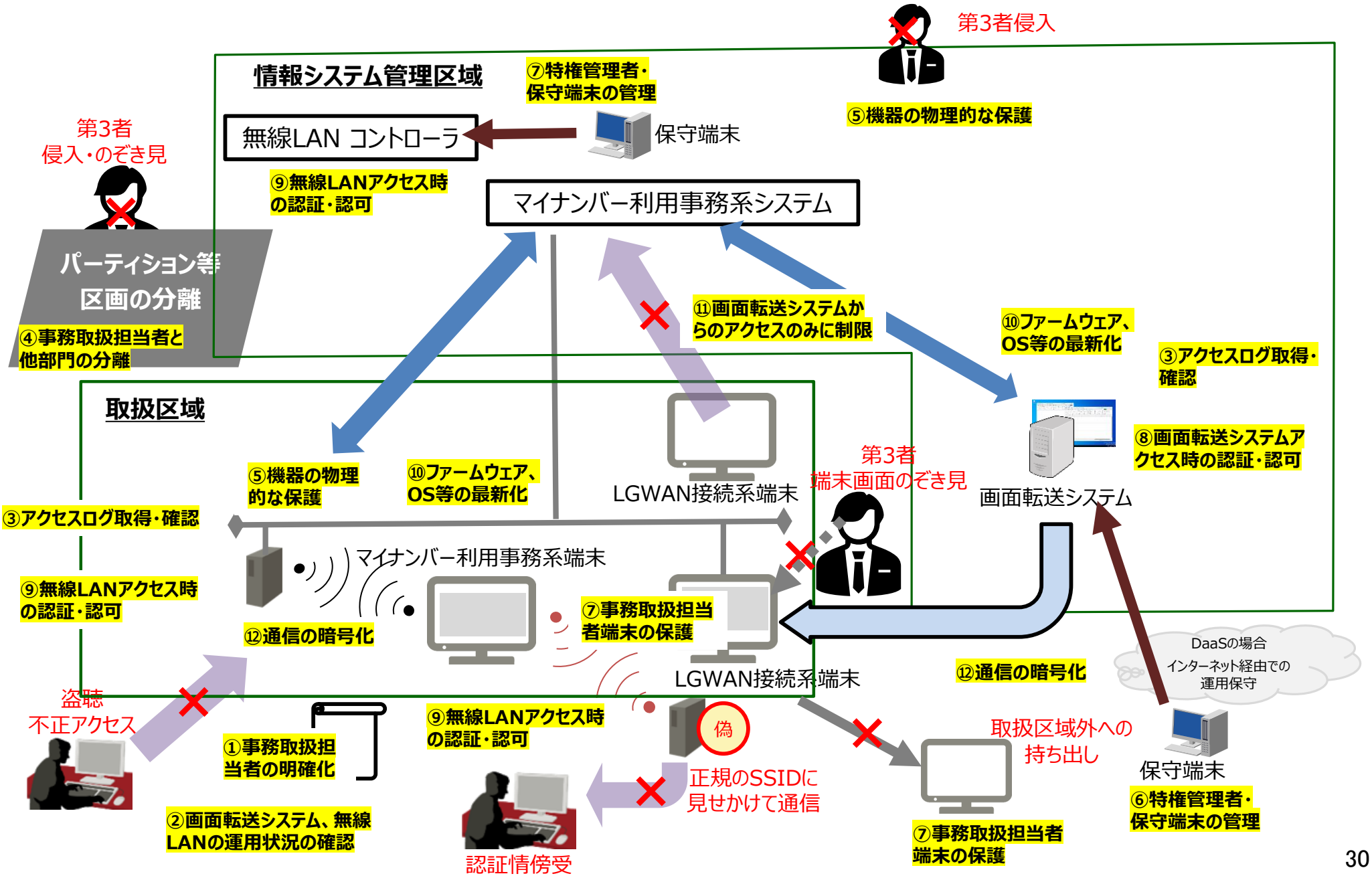
画面転送:端末1台化に伴う無線LANを利用した画面転送　無線LAN:マイナンバー利用事務系端末の無線LAN利用

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)

技術的安全管理措置実施のための対策イメージ



安全管理措置実施のための対策イメージ（全体）



参考資料

参考）ガイドラインと番号法上の安全管理措置の対応関係

2　講ずべき安全管理措置の内容　-　E　物理的安全管理措置　a-①②　関係

第2編 地方公共団体における情報セキュリティポリシー（例文）
第2章 情報セキュリティ対策基準（例文）
4. 物理的セキュリティ
4.2.管理区域（情報システム室等）の管理
(2) 管理区域の入退室管理等
①情報システム管理者は、**管理区域への入退室を許可された者のみに制限**し、IC カード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

2　講ずべき安全管理措置の内容　–E　物理的安全管理措置　–c　関係

第2編 地方公共団体における情報セキュリティポリシー（例文）
第2章 情報セキュリティ対策基準（例文）
4. 物理的セキュリティ
4.4.職員等の利用する端末や電磁的記録媒体等の管理
①情報システム管理者は、盗難防止のため、**執務室等で利用するパソコンのワイヤーによる固定**、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
5.人的セキュリティ
5.1.職員等の遵守事項
②業務以外の目的での使用の禁止
職員等は、**業務以外の目的で情報資産の外部への持ち出し**、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。
③**モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限**
（ア）CISO は、**自治体機密性２以上、自治体可用性２、自治体完全性２の情報資産を外部で処理する場合における安全管理措置**を定めなければならない。
（イ）職員等は、本市の**モバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可**を得なければならない。
第3編 地方公共団体における情報セキュリティポリシー（解説）
第2章 情報セキュリティ対策基準（解説）
6.2. アクセス制御
(2) 職員等による外部からのアクセス等の制限
（注７）**画面ののぞき見や盗聴を防止**できるような環境を選定することで情報の漏えい対策につながる。また、テレワーク実施時の離席時の端末等の盗難に注意する。

参考）「地方公共団体における情報セキュリティポリシーに関するガイドライン」の記載

2　講ずべき安全管理措置の内容　－　F　技術的安全管理措置　－a　関係

第2編 地方公共団体における情報セキュリティポリシー（例文）
第2章 情報セキュリティ対策基準（例文）
6.技術的セキュリティ
6.1.コンピュータ及びネットワークの管理
(8) ネットワークの接続制御、経路制御等
②統括情報セキュリティ責任者は、不正アクセスを防止するため、**ネットワークに適正なアクセス制御**を施さなければならない
6.2.アクセス制御
(1)アクセス制御等
①アクセス制御
統括情報セキュリティ責任者又は情報システム管理者は、所管する**ネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない**。
②利用者ID の取扱い
（ア）統括情報セキュリティ責任者及び情報システム管理者は、**利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ID の取扱い等の方法**を定めなければならない。
（イ）職員等は、**業務上必要がなくなった場合は、利用者登録を抹消**するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。
（ウ）統括情報セキュリティ責任者及び情報システム管理者は、**利用されていないIDが放置されないよう**、人事管理部門と連携し、点検しなければならない。
（エ）統括情報セキュリティ責任者及び情報システム管理者は、主体から対象に対する**不要なアクセス権限が付与されていないか定期的に確認**しなければならない。
③特権を付与されたID の管理等
（ア）統括情報セキュリティ責任者及び情報システム管理者は、**管理者権限等の特権を付与されたID を利用する者を必要最小限**にし、当該ID のパスワードの漏えい等が発生しないよう、当該ID 及びパスワードを厳重に管理しなければならない。

参考）「地方公共団体における情報セキュリティポリシーに関するガイドライン」の記載

2　講ずべき安全管理措置の内容　－　F　技術的安全管理措置　　-b　関係

第2編 地方公共団体における情報セキュリティポリシー（例文）
第2章 情報セキュリティ対策基準（例文）
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
②情報のアクセス及び持ち出しにおける対策
（ア）情報のアクセス対策
情報システムが正規の利用者かどうかを判断する**認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない**。
また、業務毎に専用端末を設置することが望ましい。
（イ）情報の持ち出し不可設定
原則として、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しなければならない。
4.物理的セキュリティ
4.4.職員等の利用する端末や電磁的記録媒体等の管理
②情報システム管理者は、情報システムへの**ログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要**とするように設定しなければならない。
④情報システム管理者は、**マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証**）を行うよう設定しなければならない。
6.技術的セキュリティ
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
①統括情報セキュリティ責任者は、**無線LAN の利**用を認める場合、**解読が困難な暗号化及び認証技術の使用を義務付け**なければならない。

参考）「地方公共団体における情報セキュリティポリシーに関するガイドライン」の記載

2　講ずべき安全管理措置の内容　－　F　技術的安全管理措置　－c　関係

第2編 地方公共団体における情報セキュリティポリシー（例文）
第2章 情報セキュリティ対策基準（例文）
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

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と**外部との通信をする必要がある場合**は、**通信経路の限定(MAC アドレス、IP アドレス 及び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。また、その**外部接続先についてもインターネット等と接続してはならない**。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、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

第3編 地方公共団体における情報セキュリティポリシー（解説）
第2章 情報セキュリティ対策基準（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
(注1)
(前略)

・マイナンバー利用事務系のサーバ、端末については、**ウイルス対策ソフトを導入**し、**最新の定義ファイルを常時更新**する。また、**OS の修正プログラムについても最新の修正プログラムを常時更新**する運用や対策を行わなければならない。
・マイナンバー利用事務系のサーバの**OS 等への修正プログラムの常時適用が困難な場合**は、**IPS**（ホスト型・ネットワーク型侵入検知システム）や**WAF**（Web Application Firewall Firewall）等を用いて、脆弱性を悪用した攻撃を防ぐといった対処も考えられる。これらの対処においては、シグネチャ（既知の不正な通信や攻撃パターンを識別するためのルール）の更新が必要な場合があるが、マイナンバー利用事務系においては、インターネットとの接続が出来ないため、シグネチャの更新方法（自治体情報セキュリティ向上プラットフォームの活用や媒体による手動更新等）を確認する必要がある。また、脆弱性を根本的に解決するためには、サーバのOS 等の修正プログラムの適用が必須となるため、これらの暫定的対処を行っている間に、修正プログラム適用の計画、テスト、実施等を進める必要がある。
・悪意のあるソフトウェアや攻撃者は一つの脆弱性だけでなく、複数の脆弱性や、サーバ・ネットワークの設定不備等も組み合わせた上で攻撃を行う場合がある。そのため、**サーバの設定の確認（不要なポート閉じる、サービスを停止させる等）**を行うことや、ネットワークの**通信ログの取得・監視等**も重要な対策となる。

(中略)

・ウェブアプリケーションを利用しているシステムの場合は、**ウェブアプリケーションの実装面として脆弱性を作り込まない対策**、**定期的な診断**などを行って脆弱性を検出・対処する対策が必要となる。脆弱性を作り込まない対策としては「6.3. システム開発、導入、保守等（解説）（８）（注１１）」を、脆弱性の検出・対処の対策としては「6.6. セキュリティ情報の収集（解説）（１）（注４）」を参照されたい。

参考）「地方公共団体における情報セキュリティポリシーに関するガイドライン」の記載

2　講ずべき安全管理措置の内容　−F　技術的安全管理措置　−d　関係

第2編 地方公共団体における情報セキュリティポリシー（例文）
第2章 情報セキュリティ対策基準（例文）
6.技術的セキュリティ
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
②統括情報セキュリティ責任者は**、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置**を講じなければならない。
4.物理的セキュリティ
4.3.通信回線及び通信回線装置の管理
⑤統括情報セキュリティ責任者は、**自治体機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合**、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、**送受信される情報の暗号化**を行わなければならない。

参考）IEEE802.1ｘ　EAP認証比較

- 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」の参考資料の「LGWAN接続系での無線LAN利用の要件」の認証方式において、「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）を行う。」ことを求めている。
- 無線LANへの接続時のIEEE802.1x認証には、下表に示す方式がある。
- LGWAN接続系端末に1台化時におけるマンナンバー利用事務系の無線LAN利用時の認証は、LGWAN接続系の認証サーバを利用した認証が求められることになるが、EAP-TLS、EAP-TTLS、EAP-PEAPが対象となる。
- EAP-TLS、EAP-TTLS、EAP-PEAPのうち、クライアントの識別も電子証明書で行うEAP-TLSがセキュリティの強度が最も高いため、マンナンバー利用事務系に無線LANでアクセスする場合の認証は、 EAP-TLSの導入を推奨する。

タイプ	クライアント識別方法	認証方法	長所	短所
EAP-MD5	•利用者のID、パスワード	CHAPに似たチャレンジ方式	•導入が簡単 •標準的にサポート	•パスワードに対する辞書攻撃の危険性
EAP-TLS	•電子証明書	認証サーバとクライアントの電子証明書による相互認証方式	•他EAPの中で高い認証強度	•CA局設置によるクライアント証明書の運用負担高
EAP-TTLS	•利用者のID、パスワード	サーバ認証は電子証明書で、クライアント認証はユーザID/パスワード	•EAP-TLSと比較して導入しやすい	•パスワードに対する辞書攻撃の危険性
EAP-PEAP	•利用者のID、パスワード	サーバ認証は電子証明書で、クライアント認証はユーザID/パスワード	•Windows 端末で標準搭載	•パスワードに対する辞書攻撃の危険性

参考）EAP-PEAPとEAP-TLSの比較

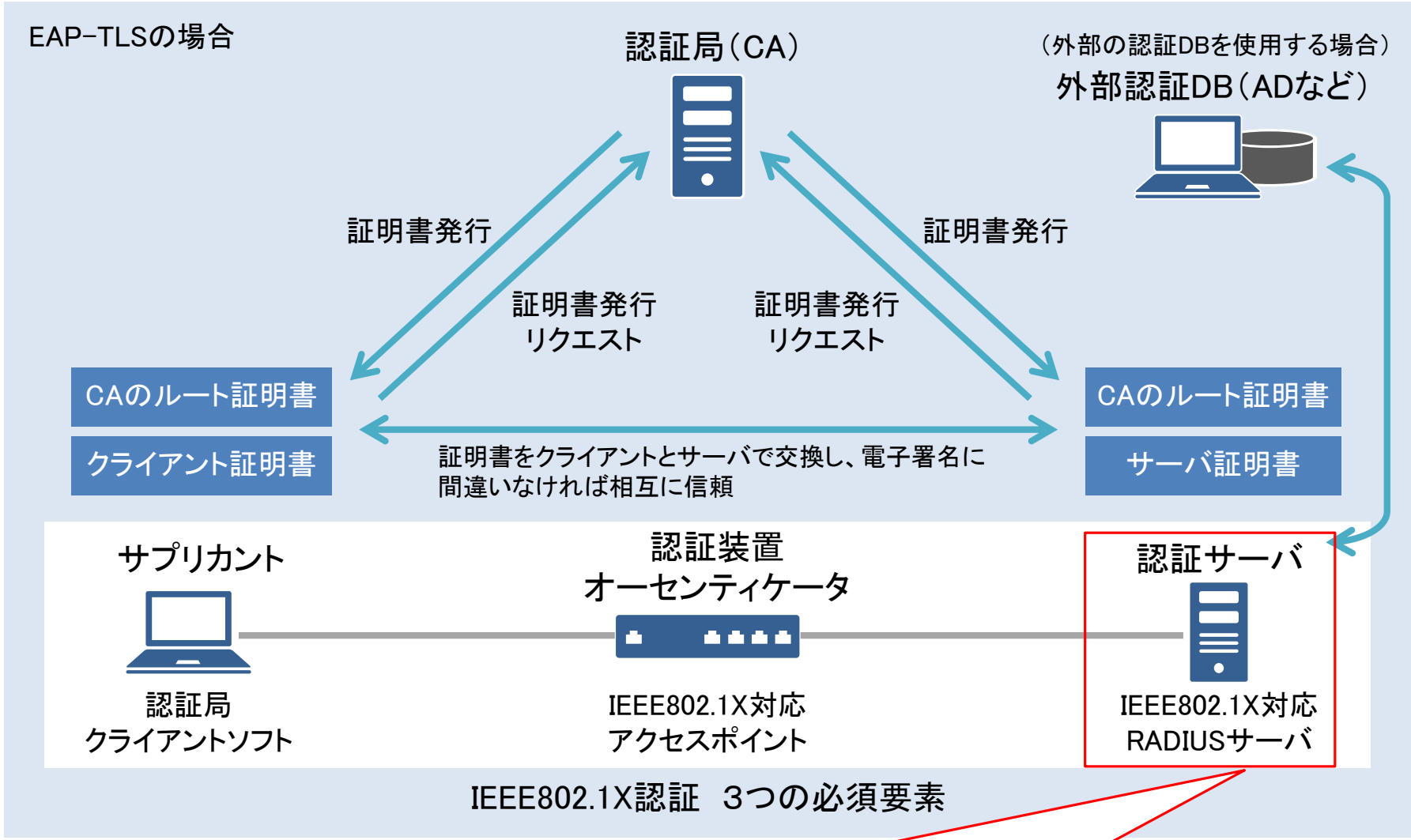
認証サーバを利用した認証でよく利用される認証方式のEAP-TLS、EAP-PEAPの比較を参考までに示す。

識別	Active Directory認証	証明書認証
特徴	EAP-PEAP	EAP-TLS
	EAP（Extensible Authentication Protocol）の実装の一種で、SSL/TLSで通信経路を暗号化して認証情報を送信する方式。**認証サーバとはサーバ証明書を利用**して認証を行う。	EAP（Extensible Authentication Protocol）の実装の一種で、IDやパスワードではなく**デジタル証明書によって認証（サーバ証明書とクライアント証明書を利用）**を行う方式。
認証方式	ドメインアカウントを利用したユーザ認証 （認証サーバが端末を認証する場合はIDとパスワード）	アクセスを許可する証明証を発行する CA（Certificate Authority）局を別途構築して認証
利用	• ADを認証サーバとするため、専用の認証サーバを構築する必要がない。 • ADのアカウント管理のみで運用が出来る。 • 認証サーバのサーバ証明書を検証するため端末側にCAが発行した証明書をインストールする。	• 証明書を利用したデバイス認証。 • 証明書がインストールされているデバイスのみアクセス可能なためiOSやAndroidも対応可能。 • CA局が必要。 • 証明書の発行や失効等の運用が必要で難易度が高い。 • デバイス毎にクライアント証明書のインストールが必要。
セキュリティ	AD管理に依存するため、セキュリティレベルが高いとは言いにくい。	端末が認証されるため、紛失時を除き、リスクが低く抑えられる。
導入に向けての課題	無線LAN接続時に、**IDとパスワードが要求**される。 IDがメールアドレス等推測可能な運用の場合、その情報が第三者に知られると、ネットワークへの接続自体はパスワード管理のみとなる。	無線LAN接続時に、**証明書が要求**される。 IDとパスワードが不要のため、ログインの手間は減らせるが、初回インストールや、定期更新等の手間がかかる。 シンクライアントの利用や、端末を固定しない運用、持出し端末利用等が行われる場合は、証明書の運用を徹底する必要がある。
メリットデメリット	【メリット】：端末側にクライアント証明書の設定が必要がないため運用が比較的容易 【デメリット】：IDとパスワードが流出した場合、不正接続されるリスクが高まる	【メリット】：クライアント証明書が個別にインストールされているため、端末紛失時にも特定のクライアント証明書を無効化すれば、無線LAN接続を不可とすることが可能。 【デメリット】：端末にクライアント証明書のインストールが必要（作業工数がかかる）。また、クライアント証明書の管理が必要。

参考）EAP-TLSの仕組み

EAP-TLSの認証の構成要素、各要素間での認証情報の流れを参考までに示す。

IEEE802.1X認証における構成要素



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」の参考資料の「LGWAN接続系での無線LAN利用の要件」の認証方式で求められている認証サーバ