資料１

各検討項目の改定方針

総 務 省

令和６年９月４日

総務省自治行政局

デジタル基盤推進室

■ ガイドラインは、**学識経験者、自治体職員、システム調達契約や個人情報保護法に知見を有する弁護士が構成員となっている検討会で議論**。

検討会構成員

石井　夏生利	中央大学国際情報学部教授
上原 哲太郎	立命館大学情報理工学部教授
岡村 久道	弁護士 国立情報学研究所客員教授
柿崎 淑郎	東海大学情報通信学部情報通信学科 准教授
北村 卓司	香川県政策部デジタル戦略総室 情報システム課長
佐々木 良一	東京電機大学名誉教授兼 同大学サイバーセキュリティ研究所 客員教授　【座長】
佐藤 淳	中央区企画部副参事
澁谷 展由	弁護士 弁護士法人琴平綜合法律事務所
庄司 昌彦	武蔵大学社会学部メディア社会学科 教授
髙橋 邦夫	合同会社KUコンサルティング 代表社員 (元豊島区役所ＣＩＳＯ、一関市、北区等のCIO補佐官)
三輪 信雄	総務省最高情報セキュリティアドバイザー

（オブザーバ）デジタル庁、総務省サイバーセキュリティ統括官室、地方公共団体情報システム機構

※赤字は今回から新規参加。

今年度の主な検討項目

✓　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報告書等を踏まえ、今年度は主に以下を検討する予定。

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　報告書（一人一台端末・USBメモリ不可）

■ マイナンバー利用事務系と他の領域との画面転送要件の検討

■ ネットワーク系統をまたいだデータ連携の在り方

→ 今回の検討会で取り扱う

令和６年地方分権改革に関する提案（マイナンバー利用事務系への無線ＬＡＮ接続等を可能とする具体的対策の明示）

■ マイナンバー利用事務系における無線LAN利用

政府機関等の対策基準策定のためのガイドラインの一部改定（令和６年７月）

■ 政府統一基準ガイドライン改定に伴う対応

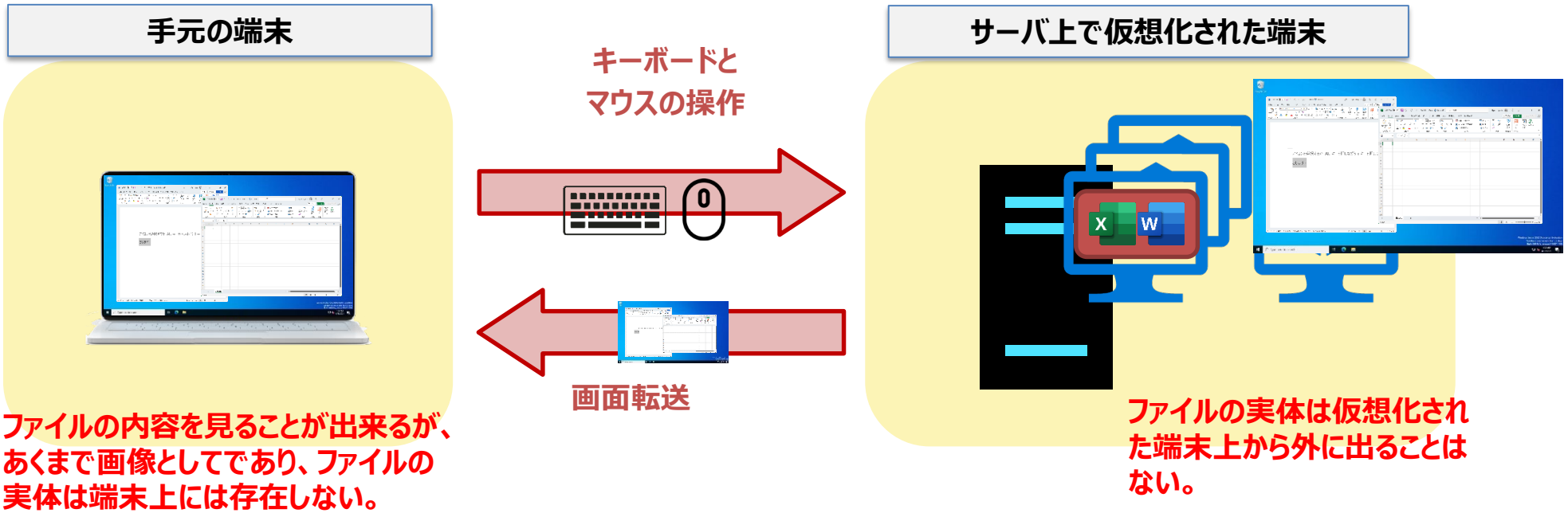
→ 今回の検討会で取り扱う

１．マイナンバー利用事務系と他の領域との画面転送要件の検討

仮想デスクトップ方式における画面転送とは

✓ 画面転送技術は、以下を実現するものである。
- 手元の端末から、**マウスとキーボードの操作のみ**を、サーバ上で仮想化された端末に送信。
- サーバの仮想化された端末から、**ディスプレイに写す画面の情報のみを、手元の端末に送信**。

✓ **ファイルの実体は、サーバの仮想化された端末の外には出力されない**ため、以下の利点がある。
- データ流出を防ぐ手段として利用可能。
- 手元の端末には仮想化された端末のディスプレイに写す画面の情報のみが送られるため、**仮想化された端末がマルウエア感染や攻撃者に侵入されても、手元の端末に被害が拡大することはない**。



（日本マイクロソフト株式会社資料を元に作成）

リスク評価を行う上で踏まえるべき観点

✓ 以下の４つの観点に基づき、リスク評価を実施する。
✓ 実施にあたっては、マイナンバー利用事務系の業務システムがガバメントクラウドにリフトされる点や昨今一般的に利用されている画面転送製品の特性等を踏まえて検討を行う。

観点１：ネットワークモデルと接続先のセグメント

ネットワークモデル（α、α′、β、β′）によって、画面データ転送先（業務端末の設置セグメント）が異なるため、それぞれの**ネットワークモデルにおける画面転送の構成をパターン分けし、リスク評価を行う**必要がある。

観点２：接続要件

画面転送で使用される通信に関し、特定通信＊（マイナンバー利用事務系からインターネットに接続する場合に**最低限必要な、接続先特定のための通信**）を実施した場合のセキュリティリスクを分析し、実施可否および実施する場合の接続要件やセキュリティ対策基準を明確にする 。

(*)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）のレベルでの限定等を行う。

観点３：端末仮想化の方式

自治体で広く利用されている**DaaS、オンプレミス仮想デスクトップ、セキュアブラウザの３方式**についてセキュリティリスクを分析する。

観点４：業務運用

個人情報保護法や番号法上問題がないよう、技術的対策、人的対策を検討する。

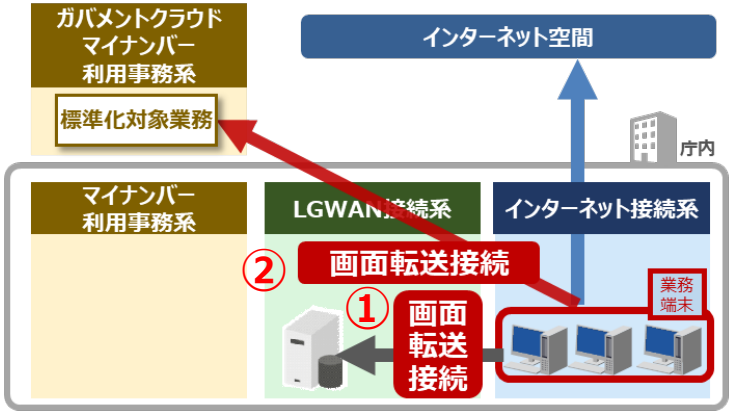
※ガバメントクラウド上のマイナンバー利用事務系の各システムとマイナンバー利用事務系の庁内LANの接続は、デジタル庁が策定した「地方公共団体情報システムのガバメントクラウドの利用について」に従って構成されているものとする。

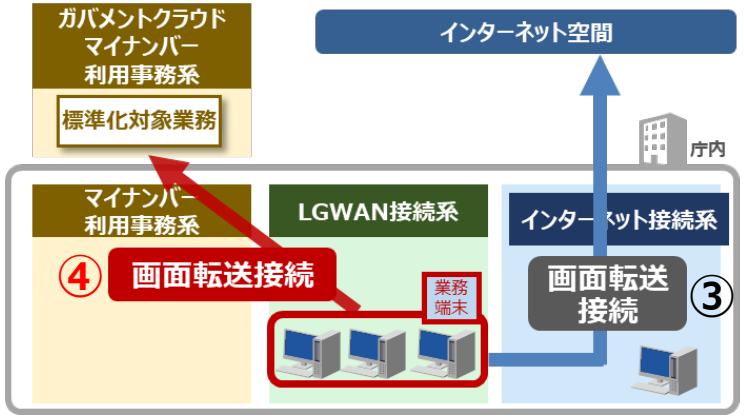
観点１：ネットワークモデルと接続先のセグメント

- ✓ 業務の中心はLGWAN接続系の端末（α/α'の場合）、インターネット接続系の端末（β/β'の場合）となる場合が多く、接続元がマイナンバー利用事務系の端末であるパターンは他のケースと比較し、ニーズが少ないものと推察される。
- ✓ マイナンバー利用事務系の端末は、マイナンバー業務を行う職員に配布されるため、庁内での台数は、LGWAN接続系の端末 、インターネット接続系の端末より少ないと想定される。
  - ⇒ **従って、端末一人一台の効果がより大きいLGWAN接続系の端末、インターネット接続系の端末が接続元であるケースを評価対象とする**。
- ※ 接続元がマイナンバー利用事務系の端末であるパターンについては、上記の理由により今回のリスクアセスメントの対象としない。

画面転送に係るセグメント間通信パターン

接続元＼接続先	インターネット接続系システム	LGWAN接続系システム	マイナンバー利用事務系システム	
			オンプレミス	ガバメントクラウド
インターネット接続系PC	－（同一セグメント）	**①今回リスクアセスメントの対象**	**②今回リスクアセスメントの対象**	
LGWAN接続系PC	③従前から画面転送可能	－（同一セグメント）	**④今回リスクアセスメントの対象**	
マイナンバー利用事務系PC	今回リスク評価の対象外		－（同一セグメント）	

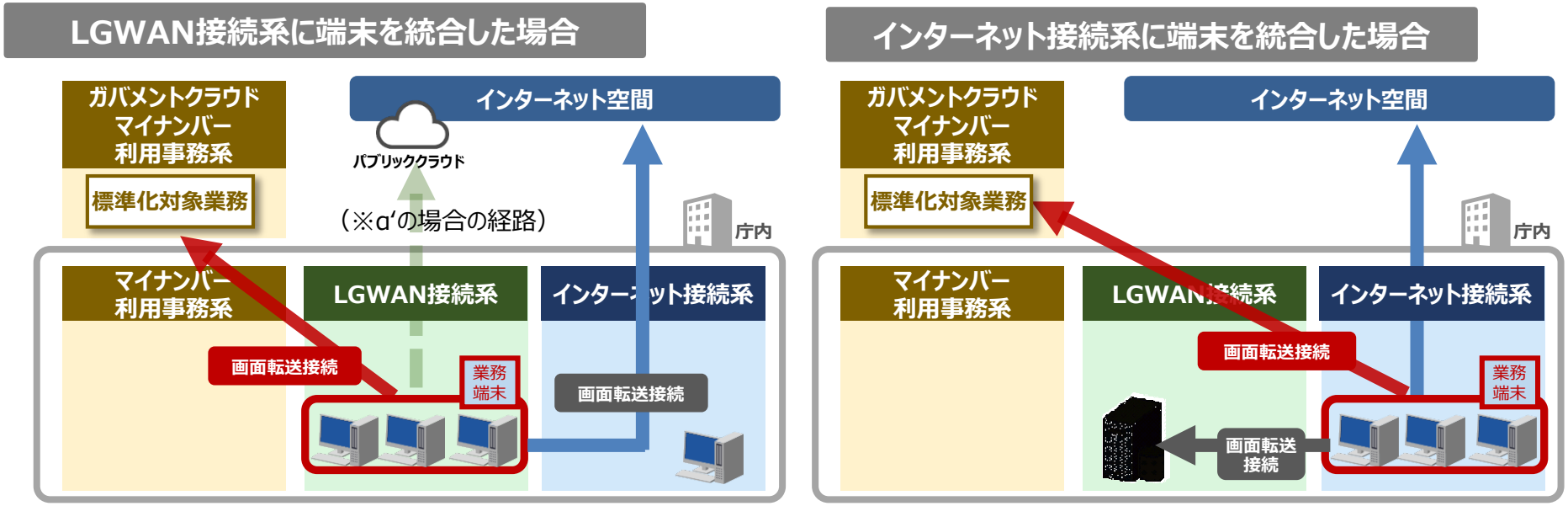




観点２：接続要件

✓ **<u>LGWAN接続系又はインターネット接続系のどちらかに端末を統合</u>**し、**<u>１台の業務端末（LGWAN接続系の端末又はインターネット接続系の端末）から、マイナンバー利用事務系の業務システムのみではなく、インターネットやLGWAN接続系にもアクセスすることを想定</u>**する。

（なお、同じ庁内でLGWAN接続系端末１台に統合するパターンと、インターネット接続端末１台に統合するパターンの両方を存在させた場合、端末や画面転送システムの管理が複雑となるため、どちらか一方のパターンに集約する前提でリスクアセスメントを実施する。）



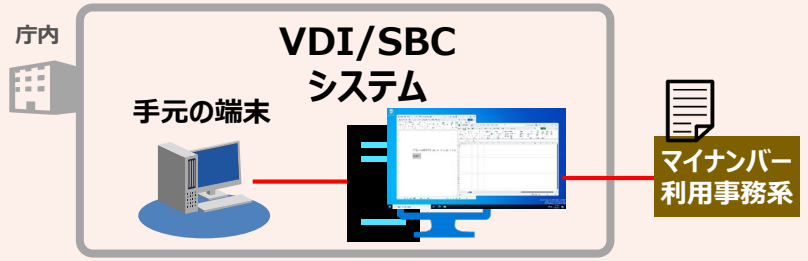
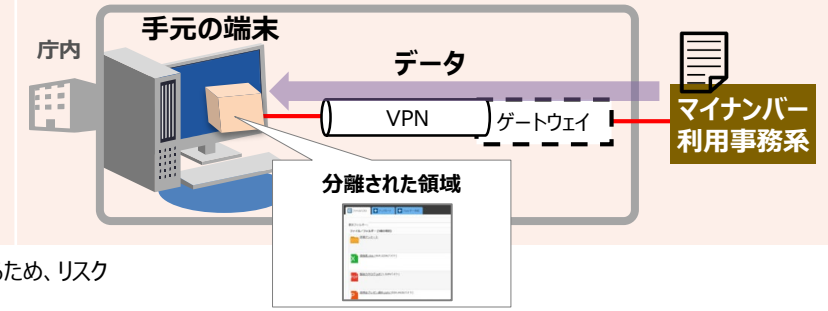
✓ ただし、手元の端末をLGWAN接続系PC１台に集約する過程において、一斉に集約することが困難である等の事情により、**<u>インターネット接続系に置かれた端末（インターネットに接続可能な状態のPC）が残る状況を考慮する</u>**必要がある。

✓ **<u>インターネットに接続可能な状態では、マルウェアの侵入、攻撃者の侵入の脅威が大きくなる</u>**ため、インターネット接続系に置かれた端末が残る状況を想定しリスクアセスメントを実施。

観点３：端末仮想化の方式

✓ 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ることを想定し、**DaaSをリスク評価の対象に加える**。

一人１台端末を実現するときの各端末における仮想化の方式

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。

観点２：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９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

	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
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
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 ※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）
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
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

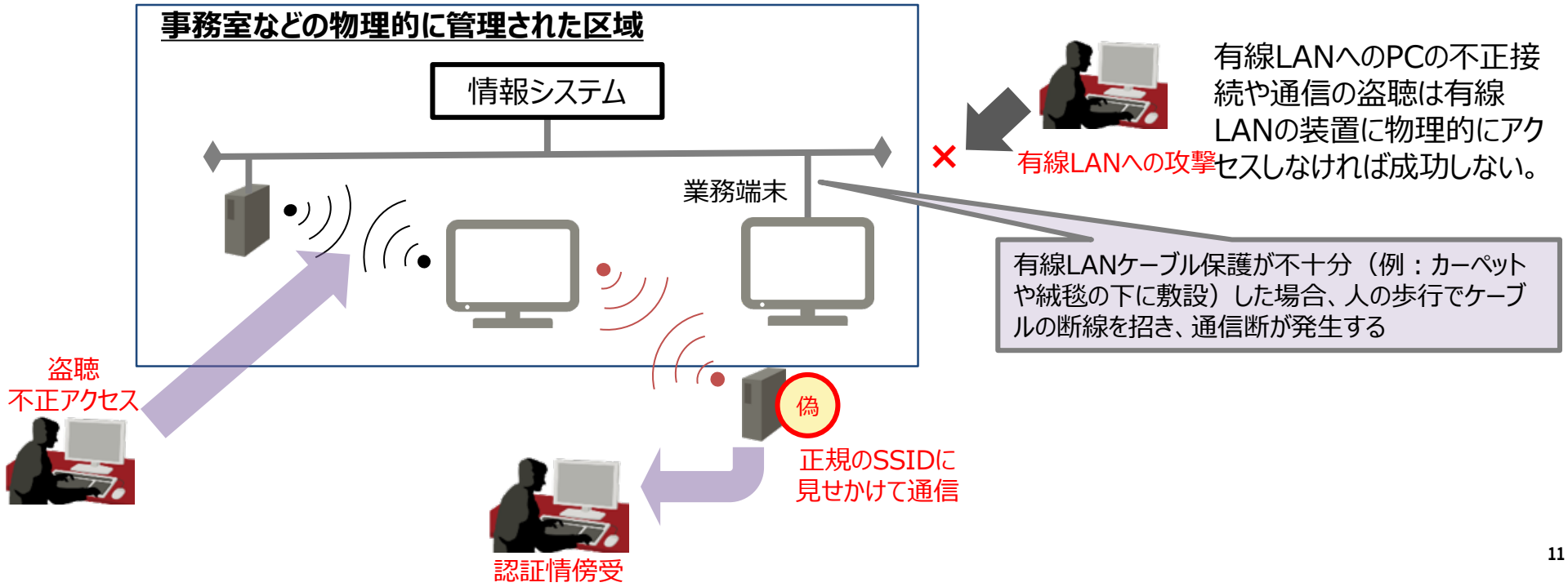
２．マイナンバー利用事務系の無線LAN利用

無線LAN利用に係るリスク

■ **盗聴**
通信内容が傍受されるおそれ。
SSID(アクセスポイントの識別子）は暗号化されていないためツールを使えば簡単に盗聴できてしまう。

■ **不正アクセス**
MACアドレスの詐称などにより無線LANが不正に利用されるおそれ。
MACアドレスは、暗号化されていないためツールを使えば簡単に盗聴できてしまう。また、MACアドレスはツールによって簡単に書き換えが可能なため、盗聴したＭＡＣアドレスを用意した端末のMACアドレスに書き換えてしまえば、正規の利用者になりすまし接続が可能となる。

■ **なりすまし**
SSIDをなりすまして不正なアクセスポイント（AP）に誘導され、認証情報などを傍受されるおそれ。



現行のガイドラインにおける規定

- ✓ 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。
- ✓ **無線LANを利用しているLGWAN接続系端末やインターネット接続系端末でマイナンバー利用事務系へのアクセスが可能**になるため、**個人情報保護法や番号法上問題がないよう、技術的対策、人的対策を検討**するため、画面転送の要件検討の際にも留意する。

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。

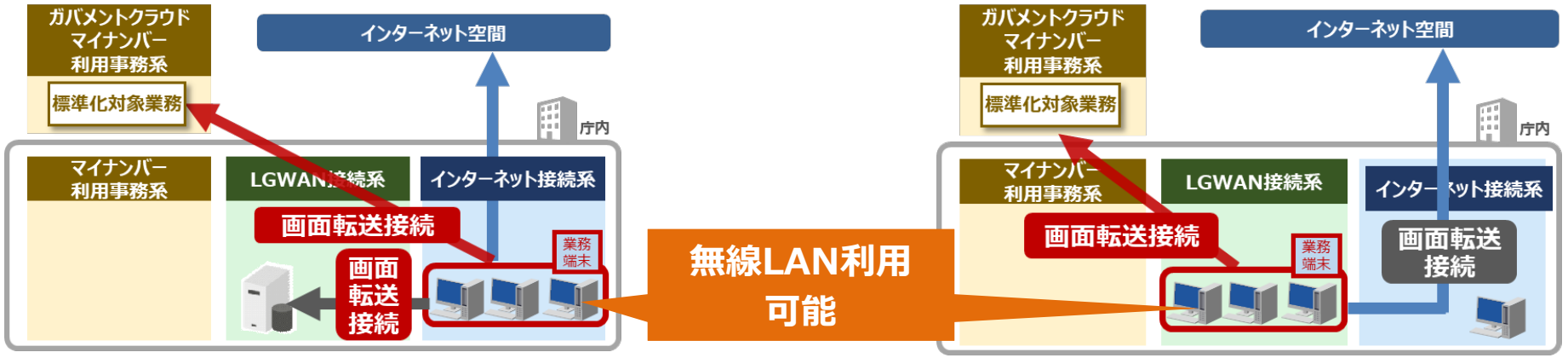
（注１０）暗号化方式の1つであるWEP（Wired Equivalent Privacy）/WPA（Wi-Fi Protected Access）については、既に脆弱性が公知となっているため、暗号強度が確認されている暗号方式（WPA2/WPA3）を採用しなければならない。

（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

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

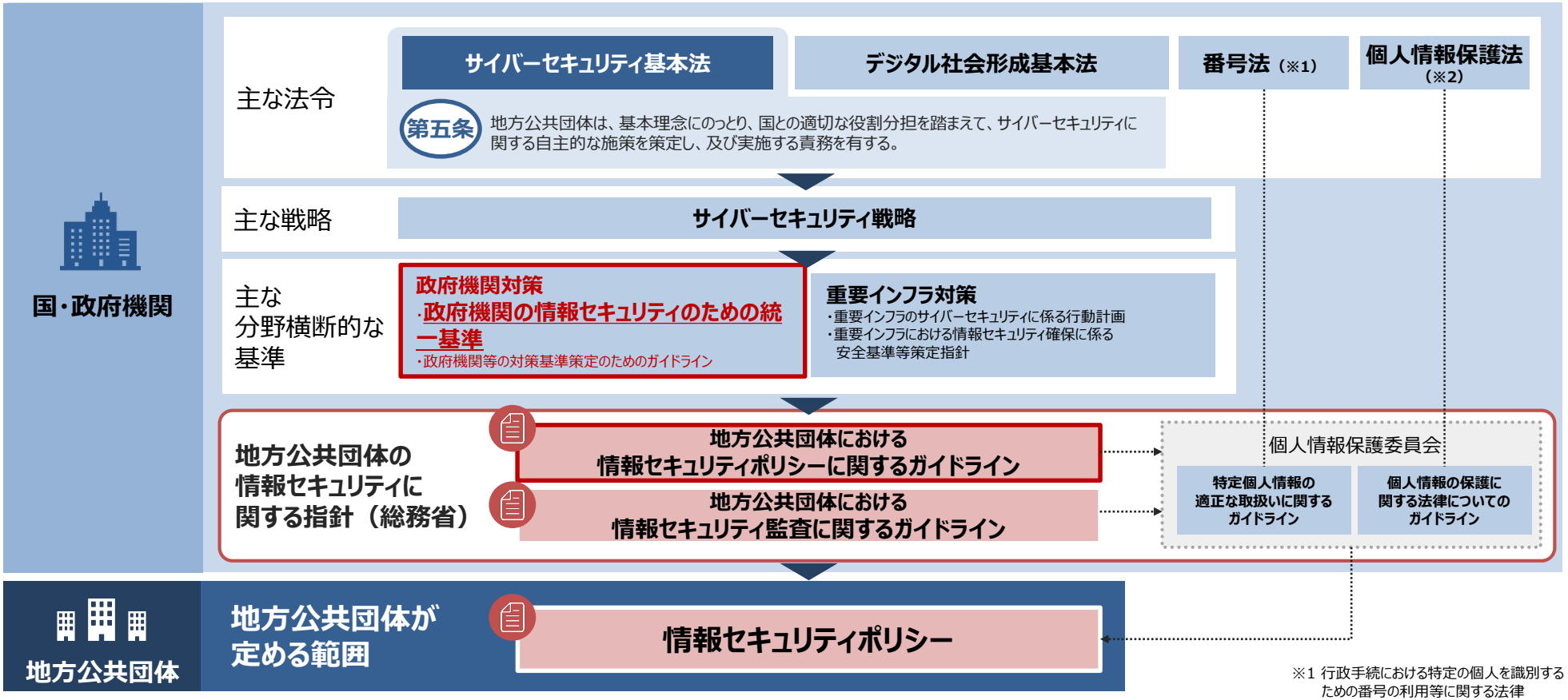
総行情第80号令和２年５月22日
「自治体情報セキュリティ対策の見直しについて」の参考資料

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

３．政府統一基準群の改定に伴う対応

政府統一基準について

- ✓ サイバーセキュリティ基本法の枠組みの中で、政府統一基準において国・政府機関に必要なセキュリティ対策を規定することとされている。
- ✓ 国・政府機関のセキュリティ対策を踏まえ、地方公共団体の情報セキュリティに関する指針を策定する必要があることから、統一基準の改定内容を、ガイドラインに反映させている。



※1 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

※2 個人情報の保護に関する法律

政府機関等の対策基準策定のためのガイドラインの一部改定（令和６年７月）

✓ 改定のあった以下のポイントについて、ガイドラインに反映することとする。

１．サプライチェーン・リスク対策の強化

- 以下を例とするリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、調達の可否を決定する必要
  - 機器等を開発・供給する事業者やそのサプライヤー・委託先事業者（再委託先事業者等を含む）、及び当該機器等の設置や保守等の役務を提供する事業者やその委託先事業者（再委託先事業者等を含む）について、当該事業者等の本社等（当該事業者等の総株主等の議決権の過半数を直接又は間接に保有する者の本社等を含む）の立地する場所の**法的環境や外部主体の指示等により、当該機器等に係る開発・供給又は役務の提供等の適切性が影響を受け、これにより悪意ある機能や不正な変更が機器等に組み込まれる又は当該機器等が取り扱う情報が窃取・破壊される等のリスク**

2.　IoT製品に対するセキュリティ対策の強化

- **IoT製品に対するセキュリティ適合性評価制度**の活用
  - IoT 機器等に対する要求すべきセキュリティ要件に関連して、2024 年度中（2025 年３月頃）に「IoT 製品に対するセキュリティ適合性評価制度」の☆１のラベル付与が開始される予定であり、今後の調達における活用が考えられる。
  - ☆１は機器等共通の最低限満たすべきセキュリティ項目を満たしていることを製造業者が自己で評価し、その適合性を宣言することで取得可能となるもの。

3.　ソフトウェアコンポーネントの管理、脆弱性管理の強化

- SBOM（Software Bill of Materials：ソフトウェア部品表）の追記

4.　要管理対策区域外での端末利用時の対策の強化

- リモートワークを考慮した要管理対策区域外での端末の対策

5.　BYOD対策の強化

- 機微な情報はBYOD端末では取り扱わない等、BYOD利用における対策を強化

6.　電子メール不正中継対策の強化

- 電子メールの不正な中継を行わないように、中継を許可する電子メールを必要最小限とする設定を電子メールサーバに行うことが必要。

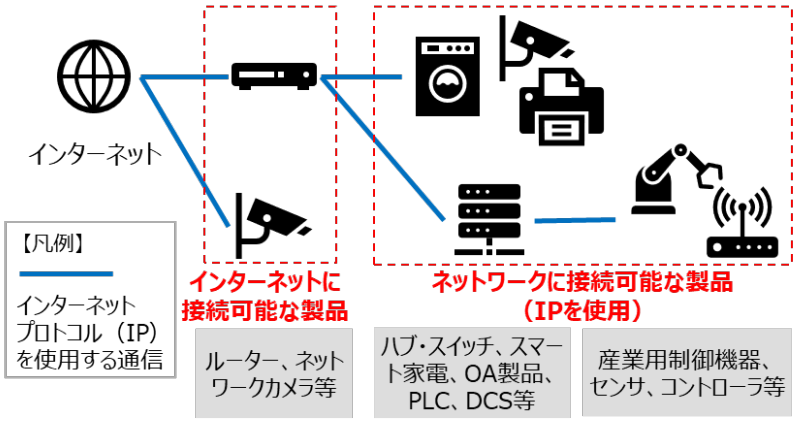
（参考）IoTセキュリティ適合性評価制度

✓ **ルータ、ハブ・スイッチ、監視カメラ等**、インターネットに直接的又は間接的に接続される製品が対象となる。

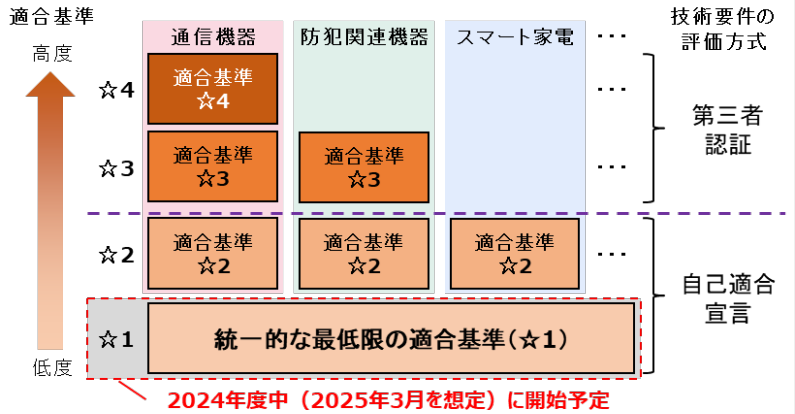
IoTセキュリティ適合性評価制度の概要

- IoT製品の脆弱性を狙ったサイバー脅威が高まっていることを踏まえ、経済産業省にて、IoTセキュリティ適合性評価制度を構築中。2024年3月～４月に制度構築方針（案）のパブリックコメントを実施。パブリックコメントを踏まえた**最終制度構築方針(※1)を8月23日に公表**。
- インターネットに直接的又は間接的に接続されるIoT製品を対象とし、複数のレベル（☆1～4）を用いた任意制度を構築予定。まずは、**全ての対象製品の統一的な最低限の基準（☆１）について、2024年度末（2025年3月頃）に受付を開始**予定。IoT製品類型ごとの特徴に応じた基準（☆2～☆4）については、順次策定予定。
- G7各国を中心に、諸外国においても同様のIoT製品の適合性評価制度の検討が進んでいる。IoT製品ベンダーの負担を抑えるため、**米国やEUの当局と相互承認に向けた議論を実施中**。

対象製品の概要(※2)



適合性評価レベル（☆1～☆4）のイメージ



レベル	位置付け	適合基準	技術要件の評価方式
☆3以上	**政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定**したIoT製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを**独立した第三者が評価して示す**もの	製品類型別	第三者認証
☆2	**IoT製品類型ごとの特徴を考慮**し、☆1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型別	自己適合宣言
☆1	IoT製品として共通して求められる**最低限のセキュリティ要件**を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型共通	自己適合宣言

(※1)経済産業省, IoT製品に対するセキュリティ適合性評価制度構築方針 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html
(※2)国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外

(経済産業省資料)

令和６年度のガイドライン改定の進め方について（イメージ）

✓ 以下のようなスケジュールで、検討会や地方公共団体への意見照会等を行い、ガイドライン改定を実施。

イベント等	４～６月	７～９月	10～12月	１～３月
検討会（年度の中での回数を記載）	－	第14回（９月４日）	第15回	第16回 第17回
各項目の検討	→	→	→	
ガイドライン改定案の提示	各項目について方針の頭出し		★	★
地方公共団体への意見照会・意見反映			リスク評価の結果及び対策案等の説明	→
ガイドライン修正案の提示				★
パブリックコメントの実施・意見反映				→
ガイドライン改定、公表				改定・公表