資料２

地方公共団体への意見照会の結果
－意見・質問について－

総 務 省

令和７年３月４日

総務省自治行政局

デジタル基盤推進室

提出された質問及び意見への対応について

提出された意見

以下を検討会資料として取り上げることとする。

- 改定案の修正が必要と考えられるもの
- 多数（3団体以上）の団体から同趣旨の意見があったもの
- 来年度の検討会において議論が必要と考えられるもの

提出された質問

運用上重要と考えられるものを検討会資料として取り上げることとする。

主な意見及び対応

主な意見①

意見：　手元の端末との通信に係る規定の緩和（画面転送）※５団体提出

画面転送の「クリップボード、プリンタ、ディスクドライブ等の仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止する。」という部分について、元の端末からのデバイス接続は許可する方向性で記載をお願いしたい。

【理由】

- 執務エリア内での印刷であれば、印刷については物理端末・仮想端末ともに取扱いに差異はないため、「同一フロア内で物理端末からは印刷可能で、仮想端末からは印刷不可能」という状況は避けたい。
- スキャナ等の利用も考えられるため。
- またデバイスでもGUIに類するもの（マウス・プリンタ等）や記憶装置を伴わない装置（プリンタ）等の使用は可能とするように記載をお願いしたい。
- 多要素認証に対応するための指紋センサーなどの生体認証用の機器については、例外として手元の端末に接続することで仮想端末でも利用可とするように修正すべき。

対応方針（案）

■ 本規定の趣旨が、**手元の端末がマルウェアに感染した場合、仮想環境上のマイナンバー利用事務系にまで被害が及ぶのを防ぐことにあることを明確にした上で**、**仮想端末の操作に必要なマウス、キーボード、認証用の機器等への接続**や、**手元の端末を介さずプリンタ、スキャナに接続することは認める**方針とし、追記してはいかがか。

※ 今回策定した別紙は、他のネットワークセグメントからマイナンバー利用事務系に、画面転送により接続する場合を想定し各種方式を規定するものである。同一のセグメント内で仮想環境と手元の端末との間で通信が完結する場合については、当該端末がマルウェアに感染する等のリスクを鑑みると、仮想環境と手元の端末の間のデータのやりとりを制限する方が望ましい。

「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」別紙

現行：全パターン共通の対策　その他

技術的対策		対策の定義
仮想環境の運用に関する対策		
	デバイス、リソースの双方向における利用の禁止	クリップボード、プリンタ、ディスクドライブ等の仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止する。 ＜例＞ • 仮想端末側で取得したファイルを画面転送で接続する手元の端末にファイルを引き渡すことができないよう制限し、逆方向の手元の端末のファイルを仮想端末側に引き渡すことができないよう制限する。 • 仮想端末側から手元の端末に接続するプリンタに印刷できないよう制限する。

修正案：全パターン共通の対策　その他

技術的対策		対策の定義
仮想環境の運用に関する対策		
	デバイス、リソースの双方向における利用の禁止	**手元の端末がマルウェアに感染した場合、仮想環境上のマイナンバー利用事務系にまで被害が及ぶのを防ぐため、**クリップボード、プリンタ、ディスクドライブ等の仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止**することとし、プリンタやスキャナを利用する場合は、仮想端末から、手元の端末を介さず、ネットワークを介して接続することとする。** **ただし、キーボード、マウスやユーザ認証用のICカードリーダ、生体認証用の機器など、仮想端末そのものの操作に必要なデバイスを、手元の端末に接続して利用することは可能。** ＜例＞ • 仮想端末側で取得したファイルを画面転送で接続する手元の端末にファイルを引き渡すことができないよう制限し、逆方向の手元の端末のファイルを仮想端末側に引き渡すことができないよう制限する。 • **印刷するファイルを、仮想端末側から手元の端末にダウンロードし、**手元の端末と接続するプリンタで印刷を行わないよう制限する。

「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」別紙

現行：はじめに

技術的な留意点

（略）

■ **クリップボード、プリンタ、ディスクドライブ等の仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止する。**

＜例＞

- 仮想端末側で取得したファイルを画面転送で接続する手元の端末にファイルを引き渡すことができないよう制限し、逆方向の手元の端末のファイルを仮想端末側に引き渡すことができないよう制限する
- 仮想端末側から手元の端末に接続するプリンタに印刷できないよう制限する

（略）

修正案：はじめに

技術的な留意点

（略）

■ 手元の端末がマルウェアに感染した場合、仮想環境上のマイナンバー利用事務系にまで被害が及ぶのを防ぐため、**クリップボード、プリンタ、ディスクドライブ等の仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止する。**

＜例＞

- 仮想端末側で取得したファイルを画面転送で接続する手元の端末にファイルを引き渡すことができないよう制限し、逆方向の手元の端末のファイルを仮想端末側に引き渡すことができないよう制限する
- 印刷するファイルを、仮想端末側から手元の端末にダウンロードし、手元の端末と接続するプリンタで印刷を行わないよう制限する。

（略）

主な意見②

意見：機器等の調達に係るひな型　※３団体提出（「運用面における課題」でも挙げられていた要望）

SBOMやIoT製品に対するセキュリティ適合性評価制度など今回改定で盛り込まれた観点について、機器等の調達基準に係る運用規程のひな型や調達仕様書のひな型等の形で示してほしい。

対応方針（案）

■ 来年度、政府機関における対応を参考に、**機器等の調達基準のひな型の作成し地方公共団体に提示**することとしてはいかがか。

■ 併せて、以下を情報提供することとしてはいかがか。

- 外部サービス（クラウドサービス）の利用に係る各種規定類のひな型（令和6年10月にガイドライン改定版とともに提供）を活用し、解説に規定してある「**開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること**」等を規定することが考えられる。
- **「IT 製品の調達におけるセキュリティ要件リスト」（平成30年２月28日経済産業省）**が参考になる。

  https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf
- 特にインターネットプロトコルを使用する通信機能を持つ製品の調達については、**セキュリティ要件適合評価及びラベリング制度（JC-STAR）上の、適合ラベルの取得を仕様書等で求める**ことなどが考えられる。

主な意見③

意見：今回リスク分析の対象としていない方式について　※３団体提出

今回リスク分析されていないが、自団体で実装している構成（以下）や、製品の利用について規定することを希望。

- 通信経路パターンとして、通信経路(５)と通信経路(７)の複合パターン（接続元：LGWAN接続系、マイナンバー系：オンプレミス画面転送（VDI/SBC）、インターネット系：オンプレミスセキュアブラウザ）を新設してほしい。
- 第４のNWセグメントを設けてインターネット系、LGWAN接続系、マイナンバー利用事務系のすべてのNWセグメント環境を、画面転送を前提とした業務端末の利用について評価してほしい。
- 同一端末内で設定を切り替えることで、アクセス可能なネットワーク（LGWAN系／マイナンバー系）、利用可能なソフトウェア、アクセス可能なストレージ・ネットワークフォルダ・サーバを切り替える製品

対応方針（案）

■　以下の考え方を提示することとしてはいかがか。

- 今回の画面転送のリスク分析では、リソースの問題から、すべてのパターンを想定し実施することは困難であるため、現行のガイドラインの規定や製品の動向を踏まえ、考えられうるパターンについて分析を実施しているものである。
- なお、当該団体が、ガイドラインや今回の別紙に規定していない構成をとっているということであれば、**当該構成について団体として慎重かつ徹底したリスク分析（※）を実施**した上で、その結果を踏まえ必要な対策を検討し、**自団体幹部にもリスク等を十分に説明し、了解を得て当該構成を実装する**ことや、仮にインシデントが発生した際に**住民に対して説明責任を果たせるように対応する**ことが重要。

※　今回のマイナンバー利用事務系に係る画面転送の方式を検討する際に利用した、「制御システムのセキュリティリスク分析ガイド第２版～セキュリティ対策におけるリスクアセスメントの実施と活用～」（2023年３月IPA）に沿った方式など、政府機関等により公表されている方式

主な意見④

意見：LGWAN接続系における無線LAN利用（アクセスポイントの管理）※３団体提出

今回LGWAN接続系における「アクセスポイントの管理」（図表42）において、**「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。」とあるが、この記述は削除すべき**。

【理由】

- **「不正プログラム拡散防止」であれば、無線LANに限らず、クライアントネットワーク全体に適用されるべき事項**である。
- この部分がどうしても真に必須なことと考えられる場合は、**無線に限らず有線でも同様であるため、無線LANの対策項目ではなく有線・無線共通の項目として別途記載すべき**。
- ベンダと協議した結果、これらを制御する場合、それらを集約するL3スイッチに大量のアクセスリストを記載するなど、様々な本来不要な設定を追加する必要があるので実装が困難。

分類	要件	区分
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**

図表42　LGWAN 接続系における無線LAN 利用の要件（抜粋）

対応方針（案）

- **本規定の趣旨は、無線端末間の同一のネットワークセグメントにある他の端末にマルウェアを拡散しないようにすること**にあるため、**無線LANの対策として規定**しているものであり、（注11）において、「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」旨はすでに規定されているので、本規定は新たな制限を加えるものではない。
- 有線においても必要な対策であるとの意見を踏まえ、**不正プログラム対策として、有線においても端末間の通信が行われないようにすることを新たに規定**してはいかがか。
- また、アクセスポイント以外（端末等）において端末間の通信が行われないように設定することも可能であるため、**「無線端末同士の通信の防止」として、アクセスポイントにおける設定以外の方策でも可能なように規定することとしてはいかがか**。

ガイドライン改定案

現行の改定案：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
（略）

分類	要件	区分
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**

図表42　LGWAN接続系における無線LAN利用の要件

（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。

修正案：対策基準（解説）

タイトル修正については後述

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**及びネットワーク盗聴対策**
（略）

分類	要件	区分
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**
無線端末同士の通信の防止	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。具体的には、アクセスポイントや端末における設定が考えられる。	**必須**

図表42　LGWAN接続系における無線LAN利用の要件

（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。

参考情報及びガイドライン改定案

■ 無線LANに係る攻撃動向

- ✓ 無線LANについては、近接する別の組織のネットワークが踏み台にされて自組織のアクセスポイントへ接続され、攻撃を実施した例も報道されている。
- ✓ **<u>無線LANについては、別組織であっても近接していれば電波が到達し、通信が可能である</u>**ことに留意する必要がある。

＜参考：地球の裏側からWi-Fiで社内ネットワークに侵入、世界初「最近接攻撃」の脅威 | 日経クロステック＞
https://xtech.nikkei.com/atcl/nxt/column/18/00676/122400185/

■ 有線・無線両方に係るガイドライン改定案

現行の改定案：対策基準（解説）

6.5. 不正アクセス対策
(４)内部からの攻撃
庁内ネットワークに接続したパソコン、モバイル端末及び不正プログラムに感染した庁内サーバを使って、庁内のサーバや外部のサーバ等に攻撃を仕掛けられる場合があり、これらを監視しなければならない。
（略）

修正案：対策基準（解説）

6.5. 不正アクセス対策
(４)内部からの攻撃
庁内ネットワークに接続したパソコン、モバイル端末及び不正プログラムに感染した庁内サーバを使って、庁内のサーバや外部のサーバ等に攻撃を仕掛けられる場合があり、これらを監視し、**有線・無線を問わず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。なお、無線LAN利用のセキュリティ要件については、「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盗聴対策」を参照すること。**
（略）

その他ガイドラインの改定関係①

意見：「未知の不正プログラム対策（エンドポイント対策）」関係

- 「未知の不正プログラム対策（エンドポイント対策）」の概要欄に記載されている「セキュリティ専門家の経歴 」について、「経歴」のみでは知識レベルがわかりにくいため、「セキュリティ専門家の経歴及び保有資格」に修正。
- 「未知の不正プログラム対策（エンドポイント対策）」の概要欄に記載されている、「・当該サービスにより、その団体の情報が国外に持ち出される可能性があるか。」については、「当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。」といった表現の方が、他の記載とのバランス上適当。
- **サービス選定の際の評価の観点について、検知率が高いことも重要であることも踏まえ、「未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい」と入れるべき。現在の評価の観点のみでは、サービスが限定され、結果、競争原理が働かず高額で提供されるようになってしまう可能性がある。**

対応方針（案）

- ご意見を踏まえ、以下のように修正することとしてはいかがか。

現状

技術的対策	対策の定義
未知の不正プログラムへの対策（エンドポイント対策）	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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられる。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性があるか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策

修正案

技術的対策	対策の定義
未知の不正プログラムへの対策（エンドポイント対策）	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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられるが、未知のマルウェアを検知するための仕組みや検知率等踏まえ、総合的な評価を行うことが望ましい。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性がないか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴及び保有資格 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策

その他ガイドラインの改定関係②

意見：仮想デスクトップの方式

「3.情報システム全体の強靭性の向上 (2)LGWAN接続系 （注7） 」の「仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。」の後に次のような記載を追加すべき。

「クライアントPCに設けられた隔離領域（コンテナ、仮想マシン等）で動作し、無害化されていないファイルのダウンロードや端末内のデータの漏洩が不可能なよう設計されたブラウザと、そのブラウザからに限りインターネットへのアクセス要求を受け付けるゲートウェイとの組み合わせで構成されたシステムもアプリケーション仮想化の一種と考えることができる。」

【理由】

- 自団体において、上記構成をとっているがインシデントが一切発生していないことと、画面転送型であるVDIやSBCと異なり、サーバーリソース・ライセンス費ともに劇的に低減できるメリットがあると考えているため。
- 本記載が追加されることで、画面転送型の莫大な経費負担に喘ぐ全国の団体にとって非常に有益なものと考えるため。

【解説】
3.情報システム全体の強靭性の向上
(2) LGWAN接続系
①LGWAN接続系とインターネット接続系の分割
（注７）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系からLGWAN接続系へマルウェア感染を防ぐ必要がある。

対応方針（案）

■ 本規定は、仮想デスクトップ方式の種類についての説明であることと、当該意見の方式は、マイナンバー利用事務系に係る画面転送の検討においてリスク分析の対象としているセキュアブラウザに相当するものであるから、意見を踏まえ、セキュアブラウザの定義であることがわかるような記載にして改定することとしてはいかがか。

ガイドライン改定案（見え消し）

現行：対策基準（解説）

3.情報システム全体の強靭性の向上
(2) LGWAN接続系
①LGWAN接続系とインターネット接続系の分割
（略）
（注７）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系からLGWAN接続系へマルウェア感染を防ぐ必要がある。

修正案：対策基準(解説)

3.情報システム全体の強靭性の向上
(2) LGWAN接続系
①LGWAN接続系とインターネット接続系の分割
（略）
（注７）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。クライアントPCに設けられた隔離領域（コンテナ、仮想マシン等）で動作し、無害化されていないファイルのダウンロードや端末内のデータの漏洩が不可能なよう設計されたブラウザと、そのブラウザからに限りインターネットへのアクセス要求を受け付けるゲートウェイとの組み合わせで構成されたシステムであるセキュアブラウザも、アプリケーション仮想化の一種と考えることができる。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系からLGWAN接続系へマルウェア感染を防ぐ必要がある。

その他ガイドラインの改定関係③

用語等の修正

以下について意見があったため、意見を踏まえ修正。

- 「3.情報システム全体の強靭性の向上　（２）LGWAN 接続系　①LGWAN 接続系とインターネット接続系の分割」の「必要な通信だけを許可できるようにすること」について、必要であれば必ずしも安全でなくても良い、と解釈できてしまうため、「**安全が確保された通信を必要最低限許可する**。」に修正する。
- 「5.1.職員等の遵守事項 (1)職員等の遵守事項　（注３）」の、持ち出し専用パソコンに関する規定について、「**4.4. 職員等の利用する端末や電磁的記録媒体等の管理 ⑤セキュリティチップの暗号化機能」に規定されているハードディスクの暗号化機能を利用することも対策としてありうる**ため、追記する。
- 「ウェブサイトを構築する場合は、『lg.jp』を含むドメイン名の使用を調達仕様書に含める」との規定があるが、例えば電子申請システムは「ウェブサイト」ではなく「システム」なので関係ない」という誤解を生む恐れがあるため、

  「**対外的に公表するウェブサイトやシステムを構築する場合は、その構築基盤がどこにあるかを問わず、lg.jpドメイン名の使用を調達仕様書に含める**」

  と改めるべき。

ガイドライン改定案

現行の改定案：対策基準（解説）

3.情報システム全体の強靭性の向上
（２）LGWAN 接続系
①LGWAN 接続系とインターネット接続系の分割
分割とは、一旦両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすることをいう。

5.1.職員等の遵守事項
（1）職員等の遵守事項
（略）
（注３）（略）情報セキュリティリスクが相対的に高いと考えられる庁舎外への持ち出しにおいては、第三者による物理的なアクセスのリスクを十分に考慮する必要がある。第三者が端末に物理的にアクセスしやすく、情報が持ち出される可能性が高い環境下においては、例えば、使用する端末のUSBポート等を物理的にロック（塞ぐ）して封印、システム設定で端末のUSB ポート等を無効にするといった対策を施した持ち出し専用パソコンで業務を行うことが根本的な対策として考えられる。

6.3. システム開発、導入、保守等
（８）情報システムにおける入出力データの正確性の確保
（略）
（注１１）（略）また、ウェブサイトを構築する場合は、「lg.jp」を含むドメイン名の使用を調達仕様書に含めることが必要である。

修正案：対策基準（解説）

3.情報システム全体の強靭性の向上
（２）LGWAN 接続系
①LGWAN 接続系とインターネット接続系の分割
分割とは、一旦両環境間の通信環境を分離した上で、~~必要な通信だけを許可できるようにする~~安全が確保された通信を必要最低限許可することをいう。

5.1.職員等の遵守事項
（1）職員等の遵守事項
（略）
（注３）（略）情報セキュリティリスクが相対的に高いと考えられる庁舎外への持ち出しにおいては、第三者による物理的なアクセスのリスクを十分に考慮する必要がある。第三者が端末に物理的にアクセスしやすく、情報が持ち出される可能性が高い環境下においては、例えば、使用する端末のUSBポート等を物理的にロック（塞ぐ）して封印、システム設定で端末のUSB ポート等を無効にするといった対策を施した持ち出し専用パソコンで業務を行うことが根本的な対策として考えられる。なお、本ガイドラインの「4.4. 職員等の利用する端末や電磁的記録媒体等の管理 ⑤セキュリティチップの暗号化機能」に規定されているハードディスクの暗号化機能を利用することも考えられる。

6.3. システム開発、導入、保守等
（８）情報システムにおける入出力データの正確性の確保
（略）
（注１１）（略）また、対外的に公表するウェブサイトや情報システムを構築する場合は、その構築基盤がどこにあるかを問わず、「lg.jp」を含むドメイン名の使用を調達仕様書に含めることが必要である。

その他ガイドラインの改定関係④

用語等の修正

以下について意見があったため、意見を踏まえ修正。

- 図表42「 LGWAN 接続系における無線LAN 利用のセキュリティ要件」において、「LGWAN接続系」と記載すべきところを「マイナンバー利用事務系」として記載していたため修正
- 「WPA2」や「WPA3」の表記を半角英数字に統一
- 「(13)無線LANのセキュリティ対策」の例文②は、無線LANに限らないネットワークの盗聴対策が規定されているため、「(13)ネットワーク盗聴対策及び無線LANのセキュリティ対策」に修正する。

【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 のセキュリティ対策
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。
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。

「無線LANのセキュリティ対策及びネットワーク盗聴対策」に修正

- 「非常勤職員や臨時職員等」の語句を、公表されている「令和６年度 会計年度任用職員制度の施行状況等に関する調査結果 （任用件数等）」で使用されている「臨時・非常勤職員」の名称に修正。

ガイドライン改定案

現行の改定案：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
（略）

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

図表42　LGWAN接続系における無線LAN利用の要件

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

図表43　マイナンバー利用事務系における無線LAN利用の要件

修正案：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盗聴対策
（略）

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、LGWAN接続系端末を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

図表42　LGWAN接続系における無線LAN利用の要件

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

図表43　マイナンバー利用事務系における無線LAN利用の要件

来年度に検討が必要と考えられる意見

意見：機器の廃棄について

図表 41「情報の機密性に応じた機器の廃棄等の方法」について、**(1)の「機器の廃棄等の方法」を(2)と同等にして良いのではないか**。「研究所レベルの攻撃」とあるが、近年のHDDやSSDに対して、(2)以外の(3)に記載された対策を実施したあとに、研究所レベルの方法でデータを取り出すことができた事例や論文等があればご教示されたい。

【理由】

- (2)の方法でデータ消去としては十分であるため。リース契約では原則として物品はリース会社に返却すべきであるため。
- (1)のすべての記憶媒体を分解・粉砕・溶解・焼却・細断等の方法(良くある「穴開け」のみでは要件を満たさないと解釈しています)で破壊するにはコストが高すぎるため。

分類	機器の廃棄等の方法	確実な履行を担保する方法
（１）マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	**当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊**し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。なお、職員による左記措置の完了までの立ち会いについては、委託先事業者の作業状況が確認出来る場合、カメラによるリアルタイムでの監視やカメラ映像の記録の確認などで代替できる。
（２）自治体機密性２以上に該当する情報を保存する記憶媒体（上記（１）に該当するものを除く。）	**一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当**である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。

図表 41　情報の機密性に応じた機器の廃棄等の方法（抜粋）

対応方針

■ 機器の廃棄方法については、**政府統一基準群（「政府機関等の対策基準策定のためのガイドライン（令和５年度版）」の「(7) 情報の消去」）等を踏まえ、詳細な検討が必要**。

「政府機関等の対策基準策定のためのガイドライン（令和５年度版）」「(7) 情報の消去」

- ✓ 以下の表のとおり、現行のガイドラインで規定されていない方法が示されている。
- ✓ 地方公共団体が実施するにあたり支障になる点はないか等、整理が必要。

電磁的記録媒体	抹消方法	注意点
磁気媒体（注１）	データ抹消ソフトウェア（もとのデータに異なるランダムなデータを１回以上上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法	（ハードディスクの場合） データ抹消ソフトウェアがハードディスクの不良セクタ用の退避領域及びOSが認識不可能な隠し領域にアクセスすることができない場合、当該領域に対して上書きが行われないことに注意が必要である。
フラッシュメモリ媒体（注２）	データ抹消ソフトウェア（もとのデータに異なるランダムなデータを２回以上上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法	ソリッドステートドライブ（以下本解説において「SSD」という）等のフラッシュメモリタイプの電磁的記録媒体は、データ書き込み回数に制限（寿命）があることからウェアレベリングと呼ばれるディスク領域全体を均一に使用する機能や動作の高速化等を目的に、媒体本体のファームウェアが管理する領域を持っており、データ抹消ソフトウェアによる上書きを１回実施した場合は実際にはデータの書き込みが行われず、消去すべき情報がそのまま残ってしまう現象が発生する可能性があるが、２回以上の上書きとすることにより、当該情報は抹消される。 また、データ抹消ソフトウェアが不良セクタ用の退避領域及びOSが認識不可能な隠し領域にアクセスすることが出来ない場合、当該領域に対して上書きが行われないことに注意が必要である。
	（SSDの場合） ATAコマンドの「SECURITY ERASE UNIT」コマンドを使用する方法	コマンドがサポートされていることに注意が必要である。 また、OSが認識できないため、不良セクタ用の退避領域に対してコマンドによる上書きが行われないことや、USB接続ではサポートされないことに注意が必要である。
光学媒体（注３）	物理的に破壊する方法	メディアシュレッダーやメディアクラッシャー等の専用の機器を用いることによって情報を記録している記録層を破壊する必要がある。なお、専用の機器は電磁的記録媒体に応じて存在するため、光学媒体以外の電磁的記録媒体を物理的に破壊する際においても、それぞれに対応した専用の機器を用いるとよい。

注１）ハードディスクやフロッピーディスク等の磁気媒体
注２）SSDやUSBメモリ等のフラッシュメモリ媒体
注３）CD-R/RW、DVD-R/RW等の光学媒体

（参考）図表41　情報の機密性に応じた機器の廃棄等の方法について

分類	機器の廃棄等の方法	確実な履行を担保する方法
（１）マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	**当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊**し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。なお、職員による左記措置の完了までの立ち会いについては、委託先事業者の作業状況が確認出来る場合、カメラによるリアルタイムでの監視やカメラ映像の記録の確認などで代替できる。
（２）自治体機密性２以上に該当する情報を保存する記憶媒体（上記（１）に該当するものを除く。）	**一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当**である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（３）自治体機密性１に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、（２）に記述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS及び記憶装置の初期化（フォーマット等）による方法は、HDDの記憶演算子にはデータの記憶が残った状態となるため、適当ではない	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。
※上記（１）は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む）		

主な質問及び回答

主な質問

Q1	**今回別紙で規定された画面転送の方式や無線LANを利用することで、庁内の、マイナンバー利用事務系の担当課以外の場所で、マイナンバー利用事務系にアクセスして業務を行うことは可能なのでしょうか。**
Q２	**マイナンバー利用事務系について、テレワークを行うことは可能なのでしょうか。**

回答

特定個人情報に関する物理的安全管理措置の中で、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ます。

✓ 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ことや、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）の実施のために、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になるため、端末の取扱区域外への持ち出しについては、現時点において庁内であっても原則禁止としています。

ただ、このような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と考えております。

主な質問

Q３	**データセンター所在地の国の法律や国内にデータセンターがあったとしてもクラウドサービス提供者の本社を有する国の法律が適用されるリスクについて記載されていたと認識しています。 今回、「適正なかつ透明性のある手続」によれば外国の法執行機関等に開示されても問題ないとも読み取れますが、この解釈で問題ないでしょうか。**

【解説】
8.1. 業務委託と外部サービス（クラウドサービス）の利用
8.1. 業務委託
(１) 業務委託に係る規定の整備
①「委託判断基準」について
（略）特に、委託業務で取り扱われる情報に対して国外の法令等が適用される場合があり、国内であれば不適切と判断されるアクセス等が行われる可能性があることに注意が必要である。具体的には、適切なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形で、外国の法執行機関の命令により、データセンター内のデータが強制的に開示されるといったリスクがあると判断される場合には留意が必要である。

（３）クラウドサービスの選定
②インターネットを介して提供されるクラウドサービスの利用に当たっては、クラウドサービス提供者の事業所の場所にかかわらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、適正なかつ透明性のある手続(例：令状主義、透明性の確保、不利益処分に関する手続）に則らない形でクラウドサービス内の情報が外国の法執行機関の命令により強制的に開示されるといったリスクがあると判断される場合には留意が必要である。クラウドサービスの利用においては、利用するクラウドサービスの形態及び仕様によって情報が保存される国や地域を指定することができるものもある。また、定型約款等において情報の保存される国や地域が指定されているサービスも存在する。そのため、クラウドサービスで取り扱う情報を保存できる国や地域を事前に定めておく必要がある。

回答

本規定は、委託業務で取り扱われる情報に対して国外の法令等が適用される場合、具体的に「データセンター内のデータが強制的に開示される」といったリスクがありうることを説明するものです。情報資産の取り扱いについては、一義的には各団体において策定された情報セキュリティポリシー等の規程に従っていただくことになりますが、適正なかつ透明性のある手続であっても、データセンターの所在地の国の法律の適用を受け、外国の法執行機関等に開示される、つまり、外国に当該情報資産が流出するリスクを鑑み、クラウドサービスで取り扱う情報を保存できる国や地域を事前に定めておく必要があります。

主な質問

Q４

「サービスを選定する際には、以下の観点で評価することが考えられる」との記載がありますが、評価する上で参考となる情報があればご教示いただけますでしょうか。

図表37　βモデルにおける必須のセキュリティ対策について
未知の不正プログラム対策（エンドポイント対策）
サービスを選定する際には、以下の観点で評価することが考えられる。
・当該サービスにより、その団体の情報が国外に持ち出される可能性があるか。
・マネージドサービスが国内で提供されているか。
・情報セキュリティ専門家の経歴
・監視・検出・特定を行う際に使用する機器等の情報セキュリティ対策

現状

技術的対策	対策の定義
未知の不正プログラムへの対策（エンドポイント対策）	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、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）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。 サービスを選定する際には、以下の観点で評価することが考えられる。 ・当該サービスにより、その団体の情報が国外に持ち出される可能性があるか。 ・マネージドサービスが国内で提供されているか。 ・セキュリティ専門家の経歴 ・監視・検出・特定を行う際に使用する機器等のセキュリティ対策

回答

マネージドサービスで受ける恩恵（マルウェアの検知率向上）のみならず、遠隔で操作するサービス提供者等のセキュリテイの確保についても留意することが非常に重要です。

具体的には、不正なプログラムの検知に係る通知や不正なプログラムを含むファイルの確認・隔離が、マネージドサービスの遠隔操作によって実施されるため、当該サービス提供者のセキュリティが確保されていない場合、かえってリスクを生むことになります。