資料１
一部非公開

検討項目①
電磁的記録媒体を使用しないデータ連携について

総務省

令和８年　１月14日

総務省自治行政局住民制度課
サイバーセキュリティ対策室

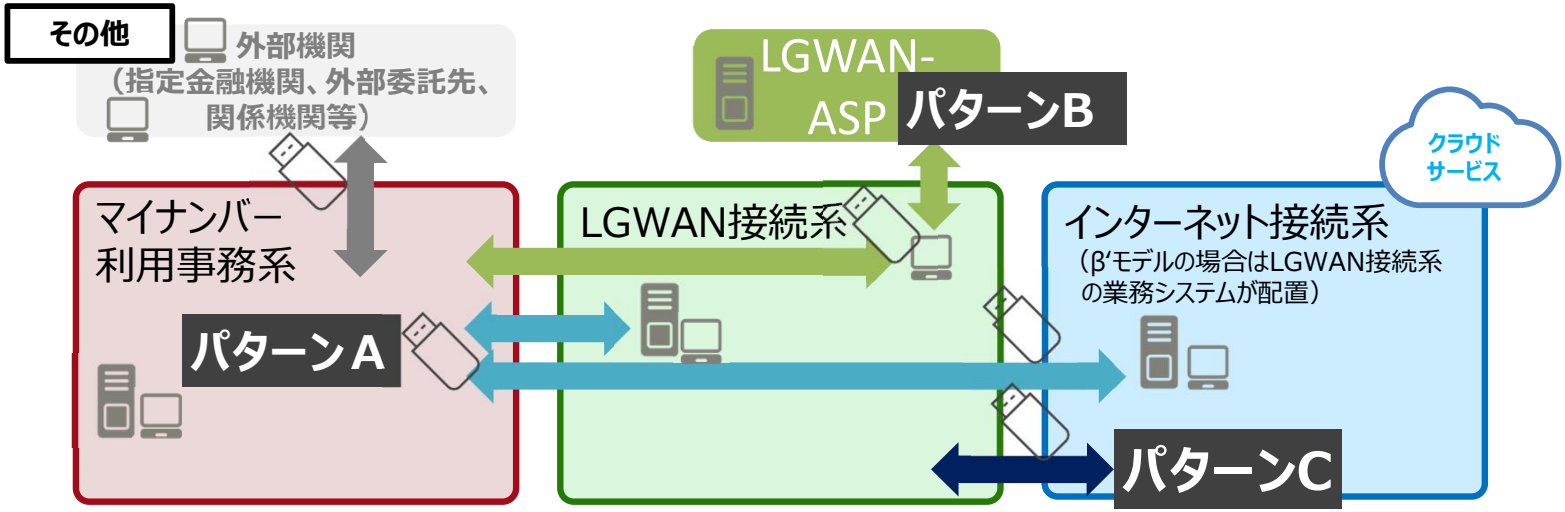
前回いただいたご意見

前回の検討会では、電磁的記録媒体の利用状況に関するアンケート結果の内容を踏まえ、
三層の対策による対応モデルと次世代モデルのリスクアセスメントを行い、今後の検討を進めていく方向でご意見をいただいた。

検討項目	視点	発言要旨
電磁的記録媒体（以降「USBメモリ等」という）を使用しないデータ連携	**1.USBメモリ等の利用の状況に関する整理（アンケートの実施）**	• アンケートの質問項目においてご指摘いただく。（アンケート修正済み） ➢ USBメモリの利用、申請を一定期間まとめて申請しているケースを追加 ➢ 今後のシステム利用形態に関する質問については、国・地方ネットワークの将来像を明記する • USBメモリ等を利用しない代替方法で既にデータ連携を実施している団体が存在する場合は、その理由を確認しておいたほうが良いのではないか。
	2.データ連携の在り方の検討（リスクアセスメントの実施）	• USBメモリ等に代わるデータ連携の在り方の検討については、**丁寧にリスクアセスメントを実施し、方向性を検討**する必要があるのではないか。
	3.USBメモリ等利用におけるリスクの整理（ガイドラインの改定を実施）	（ご意見なし） （政府統一基準群と差分を確認し、ガイドラインに追記する）

1．USBメモリ等の利用状況に関する整理（アンケートの実施）

USBメモリ等を利用したデータの受け渡しの実態に関するアンケートを実施（10月7日から10月31日）



区分	アンケート項目
パターンA	**マイナンバー利用事務系とLGWAN接続系** **マイナンバー利用事務系とインターネット接続系**
パターンB	**マイナンバー利用事務系とLGWAN接続系** （LGWAN-ASPの業務システムのデータをマイナンバー利用事務系の業務システムとデータ連携が必要な場合）
パターンC	**LGWAN接続系とインターネット接続系**
その他	マイナンバー利用事務系と外部ネットワーク接続用の端末や委託先事業者

アンケート結果の整理

（1）マイナンバー利用事務系と他の領域とのデータ連携
① フロントヤードとバックヤード間の業務連携
② バックヤード間の業務連携
③ 非定型業務における連携
④ USBメモリ等の利用なし

（2）LGWAN接続系とインターネット接続系とのデータ連携
① フロントヤードとバックヤード間の連携
② バックヤード間の連携
③ USBメモリ等の利用なし

（3）その他
マイナンバー利用事務系と外部ネットワーク接続用の端末や委託先事業者とデータを受け渡し

アンケート結果のまとめ

■ **データの受け渡し**を行う業務が幅広く存在している。
- USBメモリ等を介したデータの受け渡しが様々な業務で発生している。（某市の実態：17課52業務で利用）
- 複数のネットワーク領域間によるUSBメモリ等を利用したデータの受け渡しがされている。

<データの受け渡しが多い背景>

■ **様々な関係機関や事業者**とのデータの受け渡しが存在する。
- 外部機関等（国・広域連合・金融機関・収納代行事業者・委託事業者等）
- 住民（申請手続き）
- 事業者（見積、資料等）

■ 多岐に渡る**民間サービスが展開**されており、デジタル化が進展している。
- 公金収納に関するアウトソーシングサービス
- 電子申請サービスや電子決裁システムの導入　等

<データの受け渡しが多い理由>

■ 自治体内の**ネットワークが分離**しており、複数のネットワーク領域間を跨ぐデータ連携が難しい。

■ 各業務システムにおいて直接データ連携を行う**インターフェース（API）**が用意されておらず、必然的に**ファイルの受け渡しが発生**する。

まずは現行の業務システムへの影響を最小限とし、改善可能な対応を検討するのは如何か。

2.データ連携の在り方の検討（リスクアセスメントの実施）

- 当面の対応を検討する上で、**オンプレミス環境**による対応、**クラウド環境**による対応のモデルについてリスクアセスメントを実施するのは如何か。
  （アンケート結果では2030年頃には半数近くの団体がマイナンバー利用事務系・LGWAN接続系・インターネット接続系がクラウド環境で運用を予定）
- 加えて、今年度の国地方ネットワークの検証事業の結果を踏まえ、「**ゼロトラストアーキテクチャの考え方を採用**」したモデルに対し、リスクアセスメントを実施するのは如何か。
- また、情報システム全体の最適化を踏まえ、将来の方向性を念頭に「**API連携**」を想定したモデルに対し、リスクアセスメントを実施するのは如何か。

データ連携パターン	リスクアセスメント実施の方向性
マイナンバー利用事務系と他の領域間	次のモデルについてリスクアセスメントを実施する。 • オンプレミス環境、クラウド環境をベースとしたモデル • 「ゼロトラストアーキテクチャの考え方」を採用したモデル • 「API連携」を想定したモデル
LGWAN接続系とインターネット接続系間	主に非定型業務間の連携でUSBメモリ等を利用しており、代替案として既にβ'モデルがあることからリスクアセスメントは実施しない。
その他	外部機関等のデータ送受信の仕組みに準じる必要があり、すぐに対応案の検討が難しいことからリスクアセスメントは実施しない

マイナンバー利用事務系と他の領域間におけるリスクアセスメント検証仮モデルについて

- 住民サービスへの影響を踏まえ、**フロントヤードとバックヤード間の業務連携**を考慮したユースケースをもとに、LGWAN-ASPまたは　パブリッククラウドにおける電子申請サービスと各領域（マイナンバー利用事務系、LGWAN接続系、インターネット接続系）間をデータ連携を行うモデルに対し、**リスクアセスメントを実施**するのは如何か。
- 各々の検証モデルに対して、「セキュリティリスク」、「業務の生産性」等の観点で評価を行う。

マイナンバー利用事務系と他の領域間におけるリスクアセスメント検証モデル一覧

区分	運用環境	セキュリティ・アプローチ
検証仮モデル①a	オンプレミス（連携サーバ）	境界セグメントを配置
検証仮モデル①b	オンプレミス（ファイル交換システム）	境界セグメントを配置
検証仮モデル①c	オンプレミス（クラウドストレージ）	ローカルブレイクアウト
検証仮モデル②	クラウド	クラウドにおけるアクセス制御
検証仮モデル③*	クラウド	ゼロトラストアーキテクチャ
検証仮モデル④*	クラウド	API連携

＊検証モデル③④については、「令和7年度　国・地方ネットワークの将来像の実現に向けた検証事業」の結果も踏まえ、次年度の検討会においてモデル案を提示予定

リスクアセスメントの手法の概要

- リスクアセスメントは、**「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月版 IPA）に沿って実施する**。
- セキュリティ対策については、マイナンバー利用事務系の情報資産の重要性に十分に考慮し、導出するものとする。
- マルウェアに感染してしまったことの事実公表による信用の失墜も重要な評価ポイントであるため、**資産の重要度の評価ポイントに、マイナンバー制度や地方公共団体への信頼が失墜することや、地方公共団体の業務に係るシステム、ネットワーク基盤が長期間停止することを入れる**。
- クラウド環境においては、特定のクラウドを想定せずにアセスメントを行う。

以下の2通りの手法でリスクアセスメントを行う。
両方のリスク分析を行うことで相互補完性を考慮し総合的な評価につなげる。

（1）資産ベースのリスク分析

保護すべきシステムを構成する各資産（端末、サーバ、ネットワーク機器等）を対象に、その「重要度（価値）」、想定される脅威の「発生可能性」、脅威に対する「脆弱性」の3つを評価指標として、リスクを評価する分析手法。

（2）事業被害ベースのリスク分析（攻撃シナリオと攻撃ツリーによる分析）

システムで実現している事業やサービスに対して、「事業被害とそのレベル」、事業被害を引き起こす「攻撃ツリーの発生可能性」、攻撃に対する「脆弱性」の3つを評価指標として、リスクを評価する分析手法。

α´モデルやマイナンバー利用事務系における画面転送の対応を検討した際（令和6年度）も同様の手順で実施

クラウドサービスに関する脅威や攻撃ツリー等に関しては、当ガイドに限らず参考となる各情報を参照して実施

出典：「制御システムのセキュリティリスク分析ガイド第２版」（2023年３月版）,IPA
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

今後の予定

- 今年度末までに各自治体にリスクアセスメントを実施するモデルについて意見交換を行い、各モデルを精査する。来年度の検討会にリスクアセスメントのモデルを提示予定。
- リスクアセスメントについては、令和8年度の上半期に実施予定。

項目	令和7年度			令和８年度	
	1/14	1/下旬～2/下旬	３月	4月	5月
リスクアセスメント実施仮モデルの提示	第20回検討会		第21回検討会で状況を説明		
自治体との個別ヒアリング＊		→	→	→	
関係事業者との意見交換		→	→	→	
令和7年度　国・地方ネットワークの将来像の実現に向けた検証事業		検証期間		→	
各意見反映後のリスクアセスメントモデル（想定脅威、攻撃シナリオ等）の提示					第22回検討会

＊リスクアセスメントモデルに関して、各団体に対して丁寧な説明が必要なことから一斉の意見照会ではなく、個別ヒアリングによる対応を予定

3．USBメモリ等利用におけるリスクの整理

（参考）政府機関等の対策基準策定のためのガイドラインと総務省ガイドラインとの比較

赤字は現行の総務省ガイドラインに記載が無い対策（USBメモリ等の利用に特化した形で明記がされていない）
青字は現行の総務省ガイドラインにおいて一部記載がある対策

脅威	対策		対策の種類
①不正プログラム感染	**主体認証機能や暗号化機能を備える外部電磁的記録媒体を導入する。**	**（ア）**	調達時の対策
	不正プログラムの検疫・駆除機能を備える外部電磁的記録媒体を導入する。		調達時の対策
	情報を暗号化するための機能を備えたソフトウェアを導入する。	**（ア）**	調達時の対策
	外部電磁的記録媒体の検疫・駆除機能を備える不正プログラム対策ソフトウェアを導入する。		調達時の対策
	サーバ装置及び端末の自動再生（オートラン）機能や自動実行機能を無効にする。		技術的な設定
	サーバ装置及び端末において使用を想定しないUSBポート等を無効にする。	**（イ）**	技術的な設定
	外部電磁的記録媒体の使用前に、不正プログラム対策ソフトウェアや外部電磁的記録媒体に備わる機能による不正プログラムの検疫・駆除を行う。		利用時の対策
②情報漏えい	**運搬の際等に主体認証機能や暗号化機能の利用等の安全管理措置を講ずる。**	**（ウ）**	利用時の対策
	要機密情報は保存される必要がなくなった時点で速やかに削除する。	**（エ）**	**利用時の対策**
③サプライチェーン・リスク	**安全と考えられる製造元、製造過程の製品を調達する。**	**（オ）**	**調達時の対策**
①②③共通	使用可能な媒体の制限や利用方法等に関する手順を定める。		管理対策
	組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。	**（カ）**	**管理対策 調達時の対策**

出展：「政府機関等の対策基準策定のためのガイドライン」表8.1.1-1 USBメモリ等の外部電磁的記録媒体に関する対策の例（抜粋）

① 不正プログラム感染対策（ア）

■ 統一基準群に記載されている調達時の対策について追記する。

現行：対策基準（解説）

6.3. システム開発、導入、保守等

（２） 機器等及び情報システムの調達
機器等及び情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、機器等及び情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等である 。
（略）

改定案：対策基準（解説）

6.3. システム開発、導入、保守等

（２） 機器等及び情報システムの調達
機器等及び情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、機器等**(外部電磁的記録媒体を含む)**及び情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、**アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等**である 。
（略）

主体認証機能や暗号化機能を用いた
外部電磁的記録媒体を調達する旨を追記

① 不正プログラム感染対策（イ）（カ）

■ 統一基準群に記載されている技術的な設定について追記する。

現行：対策基準（解説）

4.4. 職員等の利用する端末や電磁的記録媒体等の管理

（注１）USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順には、以下の事項を含めることが望ましい。
・職員等は支給された外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により外部の組織との間で取り決めた外部の組織から受け取った外部電磁的記録媒体を使用すること。
・外部の組織から受け取った外部電磁的記録媒体は、情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずること。
（略）

改定案：対策基準（解説）

4.4. 職員等の利用する端末や電磁的記録媒体等の管理

（注１）USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順には、以下の事項を含めることが望ましい。
・職員等は支給された外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により外部の組織との間で取り決めた外部の組織から受け取った外部電磁的記録媒体を使用すること。
・外部の組織から受け取った外部電磁的記録媒体は、情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講ずること。
（略）
（注6）必要に応じて端末及びサーバのUSBポートの利用を製品やサービスで制限することで、USBメモリ等の外部電磁的記録媒体を接続することにより生じる情報セキュリティインシデントの抑止につながる。

端末やサーバのUSBポートの利用を制御することでUSBメモリを媒介したウイルス感染を抑止できることを追記

② 情報漏えい対策（ウ）（エ）

■ 統一基準群に記載されている利用時の対策について追記する。

現行：対策基準（解説）

2.情報資産の分類と管理

（２）情報資産の管理

③～⑩

（注８）委託事業者等の外部へ重要な情報資産を電磁的記録媒体で運搬する場合は、機密情報を運搬する専用のサービスを利用するなど安全な運搬措置を行うこと。インターネットを利用したクラウドサービス等で委託事業者等へ重要な情報資産を運搬する場合は、アクセス制御等のシステム設定が適切にされているか、重要な情報資産を暗号化して保存しているか、インターネットを利用したクラウドサービスと接続する通信が暗号化されているか等を確認する必要がある。また、委託事業者等に重要な情報資産が運搬された後の情報の管理を徹底することも重要となる。

外部電磁的記録媒体を利用する際の留意点（データの暗号化やデータの速やかに削除）を追記

改定案：対策基準（解説）

2.情報資産の分類と管理

（２）情報資産の管理

③～⑩

（注８）委託事業者等の外部へ重要な情報資産を電磁的記録媒体で運搬する場合は、機密情報を運搬する専用のサービスを利用するなど安全な運搬措置を行うこと。**外部電磁的記録媒体の運搬に当たっては、必要最小限の情報のみを保存するよう留意するとともに、盗難・紛失等による情報漏えいに備え、主体認証機能、暗号化機能を適切に利用する必要がある。**インターネットを利用したクラウドサービス等で委託事業者等へ重要な情報資産を運搬する場合は、アクセス制御等のシステム設定が適切にされているか、重要な情報資産を暗号化して保存しているか、インターネットを利用したクラウドサービスと接続する通信が暗号化されているか等を確認する必要がある。また、委託事業者等に重要な情報資産が運搬された後の情報の管理を徹底することも重要となる。**外部電磁的記録媒体の利用後は、当該情報を速やかに削除するよう留意する。**

③　サプライチェーンリスク対策（オ）

■ 統一基準群に記載されているサプライチェーンリスク対策について追記する。

現行：対策基準（解説）

6.3.　システム開発、導入、保守等

①「機器等の選定基準」について
(略)
このサプライチェーン・リスクに対応する方法として、地方公共団体が、国内外の情報セキュリティに関する情報を収集し、こうした知見をもとにサプライチェーン・リスクを当該調達に関する要件の一つとして取り上げることにより、開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。
このような対応をする手段の一つとして、機器等の調達において、相対の交渉が可能な契約であれば、調達に係る契約の相手方に対して、サプライチェーン・リスクに係る十分な知見をもとに、機器等に関し必要な要件を備えるべく、交渉を通じて個別に求めることが考えられる。

改定案：対策基準（解説）

6.3.　システム開発、導入、保守等

①「機器等の選定基準」について
(略)
このサプライチェーン・リスクに対応する方法として、地方公共団体が、国内外の情報セキュリティに関する情報を収集し、こうした知見をもとにサプライチェーン・リスクを当該調達に関する要件の一つとして取り上げることにより、開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。
このような対応をする手段の一つとして、機器等**（外部電磁的記憶媒体を含むことに留意する）**の調達において、相対の交渉が可能な契約であれば、調達に係る契約の相手方に対して、サプライチェーン・リスクに係る十分な知見をもとに、機器等に関し必要な要件を備えるべく、交渉を通じて個別に求めることが考えられる。

機器等に外部電磁的記録媒体は含まれることを用語の定義に含めているが、対策基準の解説の機器等に外部電磁的記録媒体を含むことを追記

参考

10.用語の定義

●「機器等」
「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、**外部電磁的記録媒体**等の総称をいう。→用語の定義に外部電磁的記録媒体は「機器等」に含めている。