資料３

新たな自治体情報セキュリティ対策に係る検討課題について（案）

総務省

2021年９月27日

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改定等に係る検討会

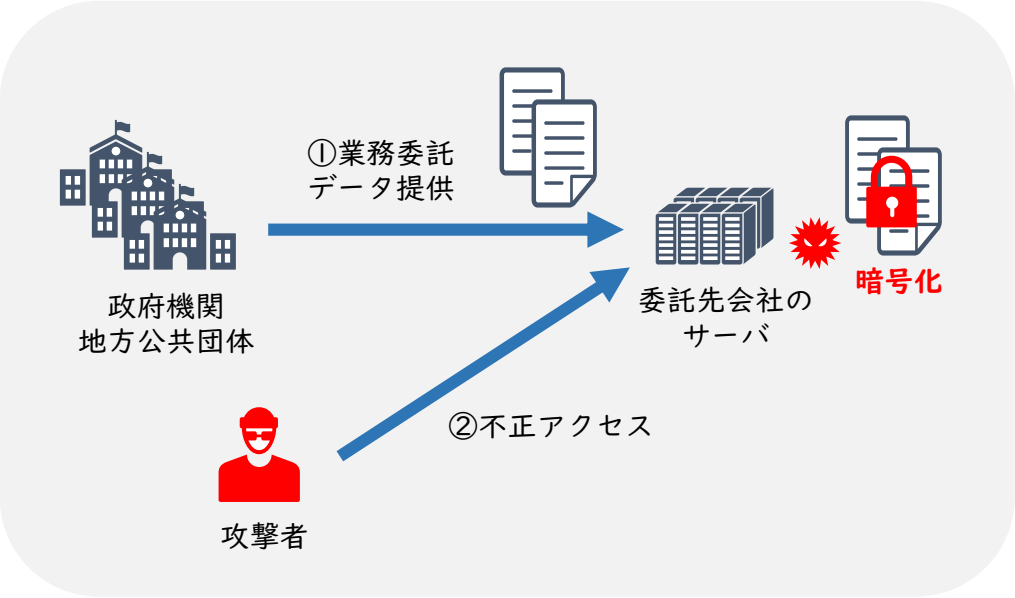
「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定について①

① 業務委託・外部サービス利用時の情報資産の取扱い

近年、地方公共団体において住民サービス向上の観点から業務委託・外部サービスの活用が進んでいるが、委託先が不正アクセス・ランサムウエア被害を受け、地方公共団体が委託先に提供していたデータなどが流出する事案も発生している。

インシデント実例

公共事業を広く受託していたコンサルタント会社が不正アクセス・ランサムウエア被害を受けた。被害を受けたサーバには、政府機関や地方公共団体などから受託したデータが保存されていたが、それらのファイルが暗号化された。



ガイドライン改定の方向性

- こうした事案を踏まえ、政府統一基準群の改定内容との整合を図りつつ、外部サービス利用時の規定、外部サービスの選定、情報資産の取扱い等の在り方について検討し、対策をガイドラインに反映させるのはどうか。

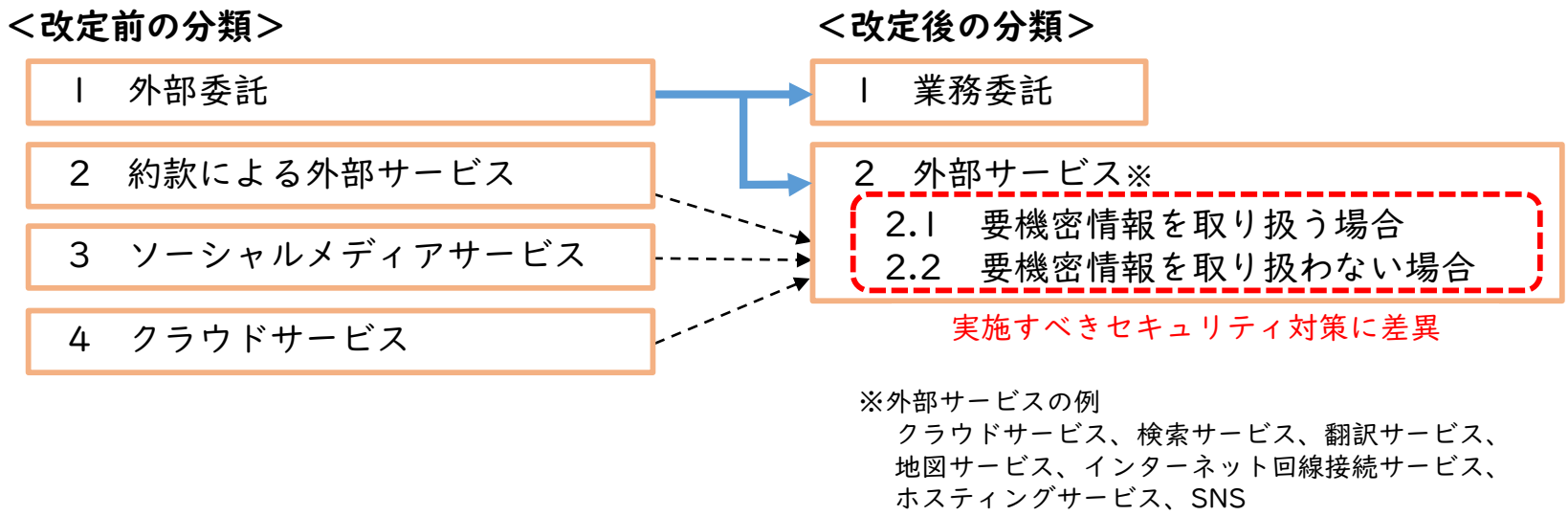
「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定について①

政府統一基準群の主な改定内容（1/2）

➢ **外部サービスの再定義と取り扱う情報に応じた適切なセキュリティ対策の実施**

「外部委託」、「約款による外部サービス」、「ソーシャルメディアサービス」及び「クラウドサービス」の定義の境目が曖昧となっているため、「業務委託」と「外部サービス」に分けた上で、「外部サービス」上での要機密情報の取扱いの有無により求めるセキュリティ対策のレベルを整理し、外部サービスを選択する際には、セキュリティ確保のために必要な事項を十分に考慮した上で、外部サービスが当該セキュリティ要件を満たすことを確認することが求められる。

※民間事業者等が不特定多数の利用者に対して提供するSNS等の画一的な約款や規約等への同意のみで利用可能となる外部サービス（従来の「約款による外部サービス」）については、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできない点は、従前より変更なし。



※外部サービスの例
クラウドサービス、検索サービス、翻訳サービス、地図サービス、インターネット回線接続サービス、ホスティングサービス、SNS

「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」の改定について①

業務委託及び外部サービスの分類

	用語の定義		具体例
業務委託	機関等の業務の一部又は全部について、契約をもって外部の者に実施させる		➢ 情報システムの開発、構築及び運用業務 ➢ アプリケーション・コンテンツの開発業務 ➢ 業務運用支援業務（統計、集計、データ入力、媒体変換等） ➢ プロジェクト管理支援業務 ➢ 調査・研究業務（調査、研究、検査等）
外部サービス	機関等外の者が一般向けに情報システムの一部又は全部の機能を提供する	要機密情報を取り扱う場合	➢ クラウドサービス ➢ Ｗｅｂ会議サービス ➢ ＳＮＳ（ソーシャルネットワーキングサービス） ➢ 検索サービス、翻訳サービス、地図サービス ➢ ホスティングサービス
		要機密情報を取り扱わない場合	

政府統一基準群における「クラウドサービス」の定義
事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの

「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」の改定について①

政府統一基準群の主な改定内容（2/2）

➢ 外部サービス利用時のライフサイクルに渡るセキュリティ要件の追加

外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策のみならず、構築・運用・廃棄等のライフサイクルに渡ることから、要機密情報を取り扱う外部サービスの利用における導入・構築・運用・保守・更改・破棄の各フェーズのセキュリティ対策に係る規定を、ISO/IEC27017:2015を参考に追記

- 外部サービスを選定する場合は、取り扱う情報の格付及び取扱制限等を踏まえ、セキュリティ要件を定めること。
- 情報セキュリティ対策の実施について、外部サービス利用者が自ら行うべきこと、外部サービス提供者が行うべきことを明確にした上で、調達及び契約を進めること。
- 外部サービスを利用して情報システムを構築する際は、外部サービスの特性や責任分界点を踏まえ、構築時におけるアクセス制御、暗号化、開発及び設計・設定に係るセキュリティ対策を規定すること。
- 外部サービスを利用して情報システムを運用する際は、外部サービスの特性や責任分界点を踏まえ、運用・保守時における利用方針、教育、資産管理、アクセス制御、暗号化、通信、設計・設定、事業継続に係るセキュリティ対策を規定すること。また、インシデントを認知した際の対処手順を整備すること。
- 外部サービスを利用終了する際は、外部サービスの特性や責任分界点を踏まえ、更改・廃棄時における利用終了手順、情報の廃棄、アカウントの廃棄に係るセキュリティ対策を規定すること。

➢ 外部サービスに係るシャドーIT対策

組織の承認を得ずに職員等が外部サービスを利用するシャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。シャドーIT対策として、外部サービス利用時の組織内での承認・審査・申請の手続を規定

※従来の政府統一基準群では「約款による外部サービス」のみを承認等の対象としていたが、クラウドサービスを含む外部サービス全体が対象となった。

「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」の改定について①

①－１　外部サービス利用時に実施すべきセキュリティ対策に差異を設ける基準

政府統一基準群では、約款による外部サービス、ソーシャルメディアサービス、クラウドサービス等を外部サービスとして統合した上で、外部サービス利用時に実施すべきセキュリティ対策に差異を設ける基準として、「要機密情報」（機密性２以上の情報）を取り扱う場合と「要機密情報」を取り扱わない場合で求めるセキュリティ対策のレベルを区別している。

ガイドライン改定の方向性

- 地方公共団体においても、政府統一基準群と同様に、約款による外部サービス、ソーシャルメディアサービス、クラウドサービス等を外部サービスとして統合した上で、外部サービス利用時に実施すべきセキュリティ対策に差異を設ける基準として、「機密性２以上の情報を取り扱う場合」と「機密性２以上の情報を取り扱わない場合」で区別するのはどうか。

【参考】「機密性２以上の情報」の例

◆機密性３…行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産
- 住民の個人情報
- 職員の個人情報
- 施設設計情報や入札予定価格など非公開情報

◆機密性２…行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産
- 政策検討に関する情報

※「新型コロナウィルスへの対応等を踏まえた地方公共団体におけるLGWAN接続系のテレワークセキュリティ要件について」（令和２年８月18日総務省通知）

「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」の改定について①

政府統一基準群における要機密情報の定義

要機密情報　＝　「機密性３情報」及び「機密性２情報」の総称

■政府機関等の情報サイバーセキュリティ対策のための統一基準（抜粋）

◆機密性３情報の定義

- 国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書としての取扱いを要する情報
- 独立行政法人及び指定法人における業務で取り扱う情報のうち、上記に準ずる情報

◆機密性２情報の定義

- 国の行政機関における業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
- 独立行政法人における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成13年法律第140号。以下「独法等情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報。また、指定法人のうち、独法等情報公開法の別表第一に掲げられる法人（以下「別表指定法人」という。）についても同様とする。
- 別表指定法人以外の指定法人における業務で取り扱う情報のうち、上記に準ずる情報

「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」の改定について①

①－２　要機密情報を取り扱う場合のクラウドサービス選定の指標・基準等

政府統一基準群では、要機密情報を取り扱う外部サービスのうちクラウドサービスの選定の指標・基準等として政府情報システムのためのセキュリティ評価制度（ISMAP）を活用することが記載されており、地方公共団体におけるクラウドサービス選定の指標・基準等の必要性について検討する。

政府統一基準群の改定概要

要機密情報を取り扱う外部サービスのうちクラウドサービスを利用する場合には、その選定においてISMAP制度を活用することを追記

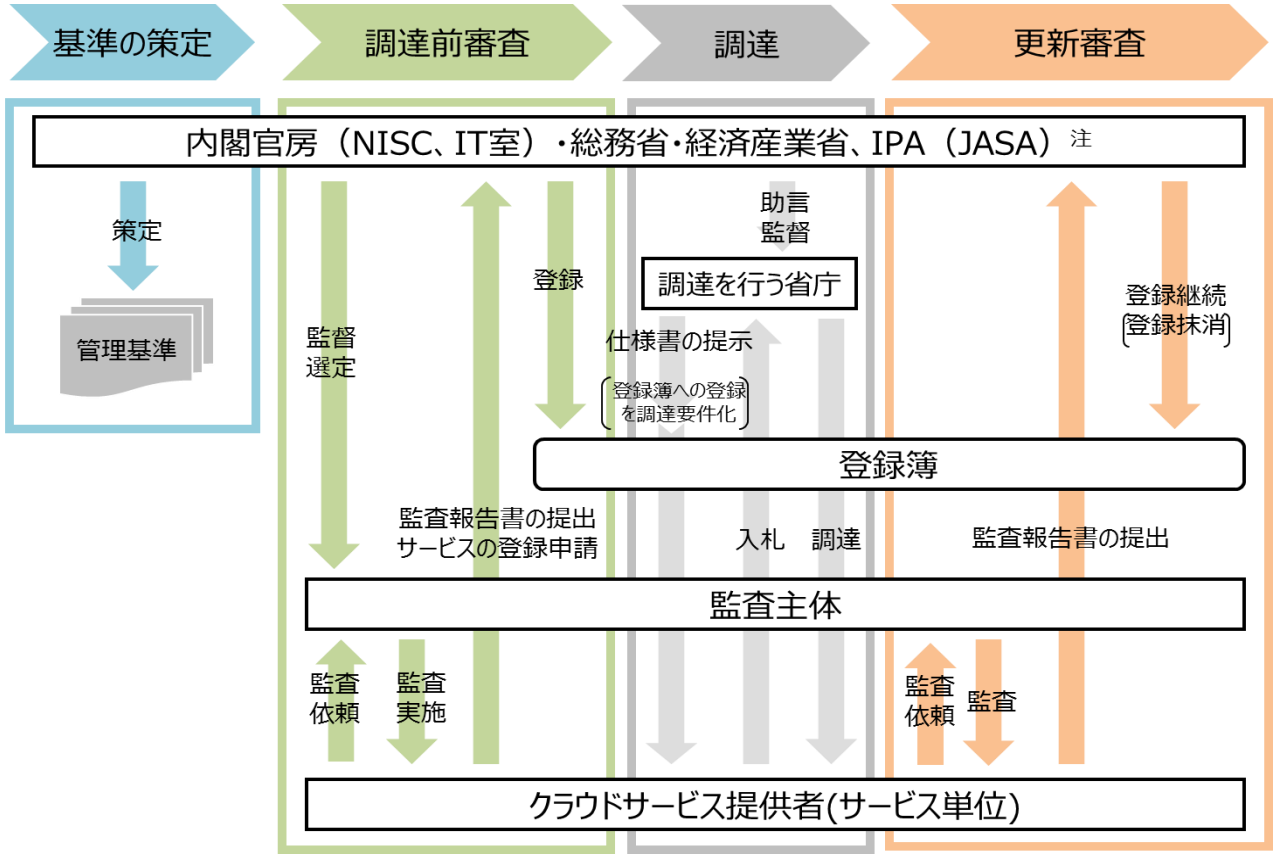
ガイドライン改定の方向性

- ISMAP制度については、要機密情報を取扱う外部サービスのうちクラウドサービス選定時の参考とすべき認証の１つとして記載するのはどうか。

【参考】政府情報システムのためのセキュリティ評価制度（ISMAP）について

- 「政府情報システムのためのセキュリティ評価制度」(ISMAP：Information system Security Management and Assessment Program) を令和２年６月に立上げ
- 国際標準等を踏まえて策定した基準に基づき、各基準が適切に実施されているか監査するプロセスを経て、基準を満たすクラウドサービスを登録する制度
- 各政府機関は、原則、安全性が評価され「登録簿」に掲載されたサービスから調達
- ３月10日、第１弾として10サービスを登録・公表　（９月13日時点で20サービス登録済み）

ISMAPの流れ



（注）制度運用に係る実務及び評価に係る技術的な支援をIPAが行い、うち、監査機関の評価及び管理に関する業務についてJASAに再委託

「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」の改定について①

➢ ガイドライン改定案のイメージ

＜現行：対策基準(解説)＞

8.4.　クラウドサービスの利用

⑤　情報セキュリティ管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

クラウドサービス事業者及び当該サービスの信頼性が十分であることを総合的に判断するためには、クラウドサービスで取り扱う情報の機密性・完全性・可用性が確保されるように、クラウドサービス事業者のセキュリティ対策を含めた経営が安定していること、クラウドやアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

このような評価に当たって、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。

なお、参考となる認証には、ISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、日本セキュリティ監査協会のクラウド情報セキュリティ監査やクラウドサービス事業者等のセキュリティに係る内部統制の保証報告書であるSOC報告書（Service Organization Control Report）を活用することも考えられる。

＜改定案：対策基準(解説)＞

8.x.　外部サービスの利用

⑤　情報セキュリティ管理者は、外部サービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

外部サービス事業者及び当該サービスの信頼性が十分であることを総合的に判断するためには、外部サービスで取り扱う情報の機密性・完全性・可用性が確保されるように、外部サービス事業者のセキュリティ対策を含めた経営が安定していること、クラウドやアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

このような評価に当たって、外部サービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用することが考えられる。

なお、参考となる認証には、ISO/IEC 27017 によるクラウドサービス分野におけるISMS 認証の国際規格がある。また、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の管理基準を満たすことの確認やISMAPクラウドサービスリスト等の確認のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査や外部サービス事業者等のセキュリティに係る内部統制の保証報告書であるSOC報告書（Service Organization Control Report）を活用することも考えられる。

「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」の改定について②

② 情報セキュリティ対策の動向を踏まえた記載の充実

従来からの境界型防御を補完するものとして、常時アクセス判断・許可アーキテクチャ（リソースへのアクセス毎に認証・認可を行い、利用者や端末、エリアなどを無条件に信頼しないという考え方）等の政府統一基準群に追加された対策をガイドラインに追加する必要があるか検討する。

政府統一基準群の改定概要

- 脆弱性管理、ＩＴ資産管理に関する解説を追記
- ＥＤＲ※1やＣＤＮ※2を検討すべき情報セキュリティ対策として追記

※1 端末やサーバ装置（エンドポイント）の活動を監視し、不正プログラム等の検知や対処を行うもの
※2 地理的に分散されたキャッシュサーバを利用してWebサイトのコンテンツを配信するというサービス

ガイドライン改定の方向性

- 最近の脅威やインシデント事例（VPNの脆弱性を突いたサイバー攻撃、ランサムウェア等）を踏まえて、政府統一基準群の改定で追加された対策について、補足説明を入れ、地方公共団体にとって分かりやすい記載とするのはどうか。

【参考】現行ガイドラインにおけるβ・β’モデルを採用する場合の技術的対策

■「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」（抜粋）

3.情報システム全体の強靭性の向上
（３）インターネット接続系③　【解説】

β’モデルを採用する場合の必須のセキュリティ対策

対策区分	セキュリティ対策	概要
技術的対策	未知の不正プログラム対策（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、未知及び既知のマルウェア等による悪意ある活動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。
	業務システムログ管理	・インシデントの兆候検知や、インシデント発生後の調査に使用するため、業務システムのログの収集、分析、保管を実施する。
	情報資産単位でのアクセス制御	・情報資産の機密性レベルに応じて業務システム単位でのアクセス制御を行う。文書を管理するサーバ等は課室単位でのアクセス制御を必須とし、係単位でのアクセス制御は推奨とする。

β’モデルについては、定期的な脆弱性診断、プラットフォーム診断等の実施が有効である。加えて、情報漏えいに対する対策として、以下の対策も有効である。

・万一ファイルが外部に漏えいしても解読できないよう、データベースやファイルの暗号化
・組織が定義したポリシーに従ってデータへの操作を監視・制限し情報の流出を防止（Data Loss Prevention）
・組織が許可していない外部接続先のサービスへのアクセスを監視、遮断

（注１０）未知の不正プログラムへの対策（エンドポイント対策）

未知の不正プログラム対策として、OSのプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名やIPアドレスなどの情報をログとして取得し、管理者へ通知する必要がある。

【参考】政府統一基準群における常時アクセス判断・許可アーキテクチャ等に関する記載

政府統一基準群（抜粋）

- **「ゼロトラストアーキテクチャ」とは、**データやサービス等のリソースへのアクセス毎に認証・認可を行い、利用者や端末、エリアなどを無条件に信頼しないという考え方をとるモデルである。

- **基本対策事項6.1.2(1)-1 f）「常時アクセス判断・許可アーキテクチャ」について**

従来の境界型セキュリティアーキテクチャ（守るべき情報が機関等内にあることを前提とし、これらを機関等外の脅威から守るためにインターネットとの境界で防御を行うことを基本とする情報セキュリティ対策の考え方。）では、信頼されたエリアからのアクセスについては、アクセス制御がされない事も多く、一度アクセスを許可した端末・ユーザや信頼できると判断された内部イントラネット等からの脅威に対応できない課題があった。常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ、ゼロトラストセキュリティ等と呼称される。）では、データやサービス等のリソースへのアクセス毎に認証・認可を行い、利用者や端末、エリアなどを無条件に信頼しないという考え方をとるモデルを基本とすることでその課題に対応する。

常時アクセス判断・許可アーキテクチャにおいて、アクセスルールを策定する際には、業務に必要な最小限の権限とし、可能な限り細かく設定される必要がある。そのためには組織の資産や業務について十分な理解と分析が必要となることから、組織全体へ一度に適用することは難しいため、組織のリスク評価等を踏まえ適用を優先するケースから段階的に導入する事が考えられる。

また、常時アクセス判断・許可を行うための機器等に対して不正アクセスやサービス停止が発生した際には対象の業務全体への影響が発生することから、それら機器等については適切な構成管理と監視、冗長構成とするなどの対応が必要である。

- **基本対策事項6.2.2(1)-6「感染拡大の防止」について**

端末やサーバ装置（エンドポイント）の活動を監視し、不正プログラム等の検知や対処を行うEDR（Endpoint Detection and Response）ソフトウェア等を利用し、複数台にわたって統合的に監視を行うことで、感染した装置を早期にネットワークから切り離す仕組みの導入。ただし、一般的にEDRソフトウェアは導入後の運用・保守段階において、専門的な知識を持った人材による膨大なログの分析が必要になることから、マネージドセキュリティサービス（Managed Security Service：MSS）と呼ばれる、ログ分析等を行うSOC（Security Operation Center）業務を委託できるサービスの利用なども検討するとよい。

【参考】政府統一基準群における常時アクセス判断・許可アーキテクチャ等に関する記載

政府統一基準群（抜粋）

➢ **●遵守事項6.2.1(1)(c)「サーバ装置、端末及び通信回線装置上で利用するソフトウェア」について**

情報システムの構築時に、ソフトウェアを効率的に開発するために使用するソフトウェアフレームワークやソフトウェア部品が情報システムに組み込まれて納入される場合があることについても考慮する必要がある。当該フレームワークや部品についても脆弱性対策の状況を定期的に確認することが求められる。これを確実に実施するためには、対象とするソフトウェアの管理簿を作成しておくことが望ましい。また、これらのソフトウェアには外部から入手するもののみでなく、機関等が自ら開発するもの及び委託により開発するものについても含まれる。

➢ **●基本対策事項6.2.1(1)-5 b)「自動でソフトウェアを更新する機能を有するIT資産管理ソフトウェア」について**

IT資産管理ソフトウェアにはOSやその他アプリケーションのセキュリティパッチを管理する機能を持つものがあり、サーバ装置及び端末に導入されたソフトウェアの種類やバージョンの管理と併せて統合的に管理を行うことができる。

「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」の改定について③

③ 多様な働き方を前提とした情報セキュリティ対策

令和２年度のガイドライン改定において、新型コロナウィルスへの対応等を踏まえ、テレワークの導入に当たっての基本的な考え方や安全性の高い方式を提示。

現在自治体で行われているテレワークの事例を取り上げつつ、必要な追加のセキュリティ対策を検討する。（大阪市、J-LISの実証事業の事例を紹介）

政府統一基準群の改定概要

➢ テレワーク・Ｗｅｂ遠隔会議利用拡大に伴う規程の整備を追記

■政府機関等の情報サイバーセキュリティ対策のための統一基準（抜粋）

➢ **遵守事項 8.1.1(8)Web会議サービスの利用時の対策**

(a) 職員等は、機関等の定める利用手順に従い、Web会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

(b) 職員等は、Web会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

➢ **遵守事項8.1.3(3)実施時における対策**

(a) 情報システムセキュリティ責任者は、テレワーク実施前及び実施後に職員等がチェックするべき項目を定め、職員等に当該チェックを実施させること。

(b) 職員等は、画面ののぞき見や盗聴を防止できるようテレワークの実施場所を選定すること。また、自宅以外でテレワークを実施する場合には、離席時の盗難に注意すること。

(c) 職員等は、原則として情報セキュリティ対策の状況が定かではない又は不十分な機関等外通信回線を利用してテレワークを行わないこと。

ガイドライン改定の方向性

➢ テレワーク・Ｗｅｂ遠隔会議実施の際の運用面等に関する対策を追加するのはどうか。

「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」の改定について③

β’モデルの活用例（大阪市）

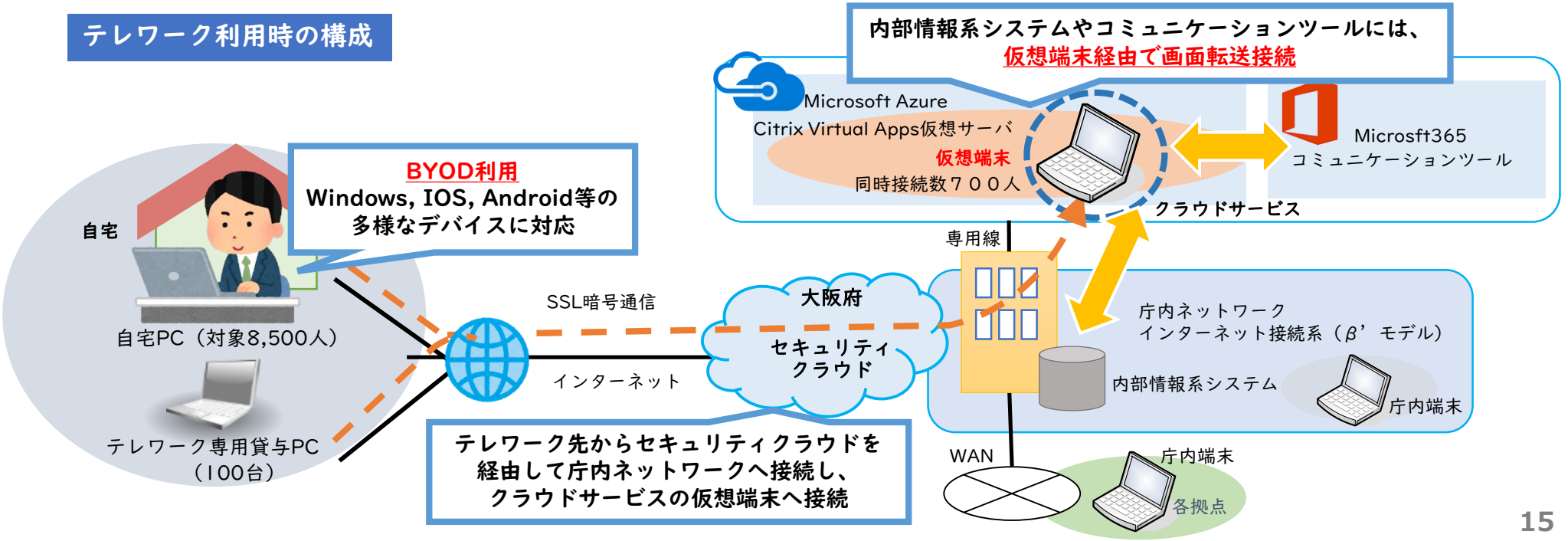
◆現状

- 2018年度から育児・介護を対象にテレワーク制度を導入・運用開始し、2020年度からは対象を全職員に拡大
- 現在、庁内情報パソコンを利用する職員数が約24,000人の内、申請を行った約8,500人が利用可能
- 画面転送方式により、文書管理、財務会計、コミュニケーションツール等が利用可能（印刷は不可）
- テレワークによりWeb会議が浸透し、日常の業務においても集合会議が減少

◆今後

- 本来は利用するＰＣやデバイスを市で用意する必要があるが、専用貸与ＰＣの数が少ないため、BYODで対応
  将来的には庁内端末をシンクライアントへ移行することでテレワークにも利用できるようにすることを検討

テレワーク利用時の構成



「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」の改定について④

④ マイナンバー利用事務系から外部接続先（eLTAX、ぴったりサービス）へのデータのアップロード

令和２年度のガイドライン改定において、今後のオンライン手続の増加などを見据えて、十分に安全性が確保された外部接続先（例：eLTAX、ぴったりサービス）に限り、インターネット経由の申請等のデータをマイナンバー利用事務系へ電子的に移送（片方向通信）することを可能としたが、その逆向きのデータの流れを認めることができないか検討する。

ガイドライン改定が必要な理由

- 電子申請の不備を申請者へ通知する場合等マイナンバー利用事務系から外部接続先への通信を許容する必要がある。
- 令和３年度税制改正に基づき、
  - ・eLTAXを通じた納税に係る対象税目の拡大（令和５年度から）
  - ・個人住民税における特別徴収税額通知（納税義務者用）の電子的送付（令和６年度から）

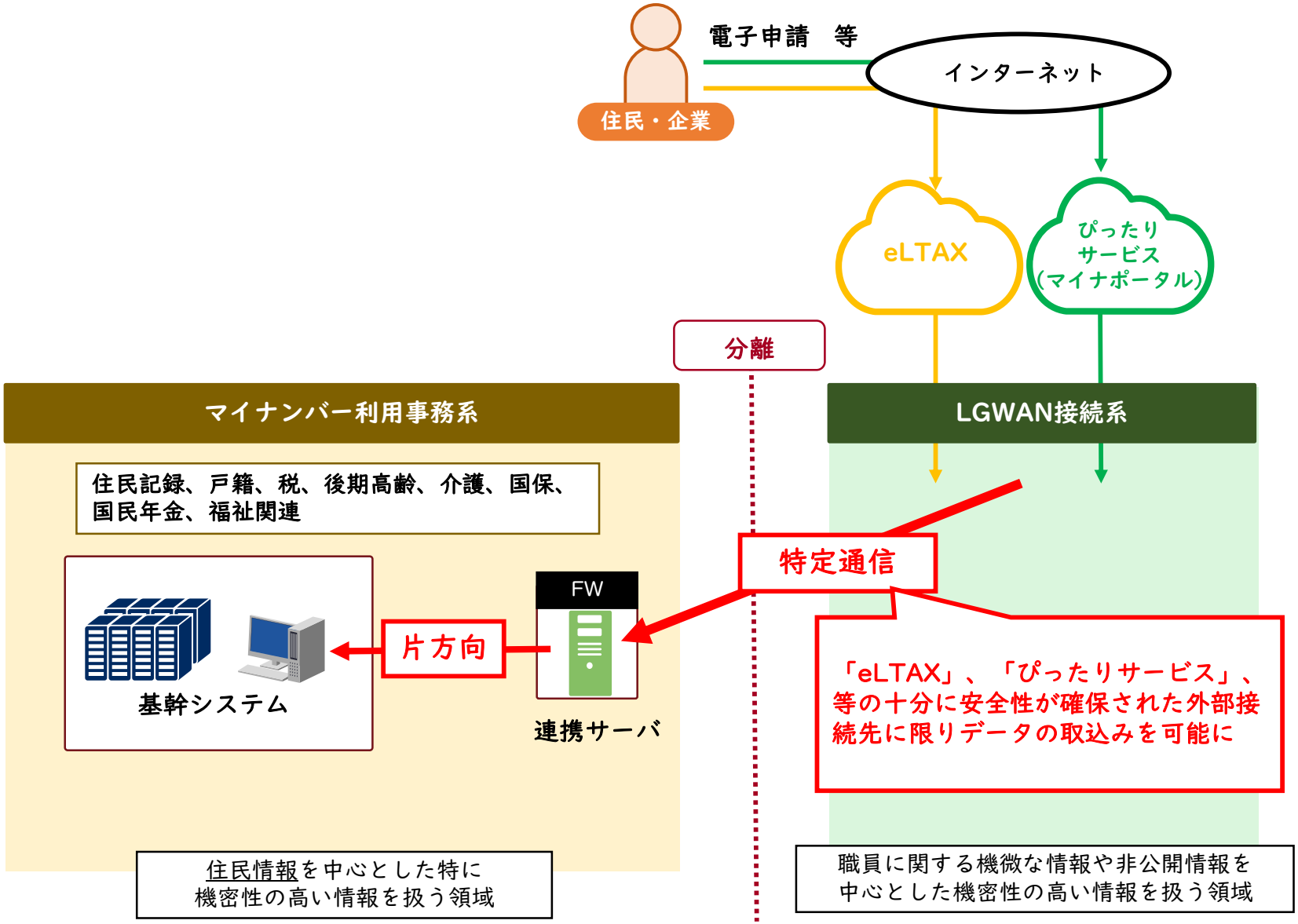
  が行われることとされており、その際、自治体の税務システムからeLTAXへ税務情報を電子的に送付する必要がある。

ガイドライン改定の方向性

- マイナンバー利用事務系からeLTAX、ぴったりサービスへデータをアップロードすることを認め、その際に必要となるセキュリティ対策を追記するのはどうか。

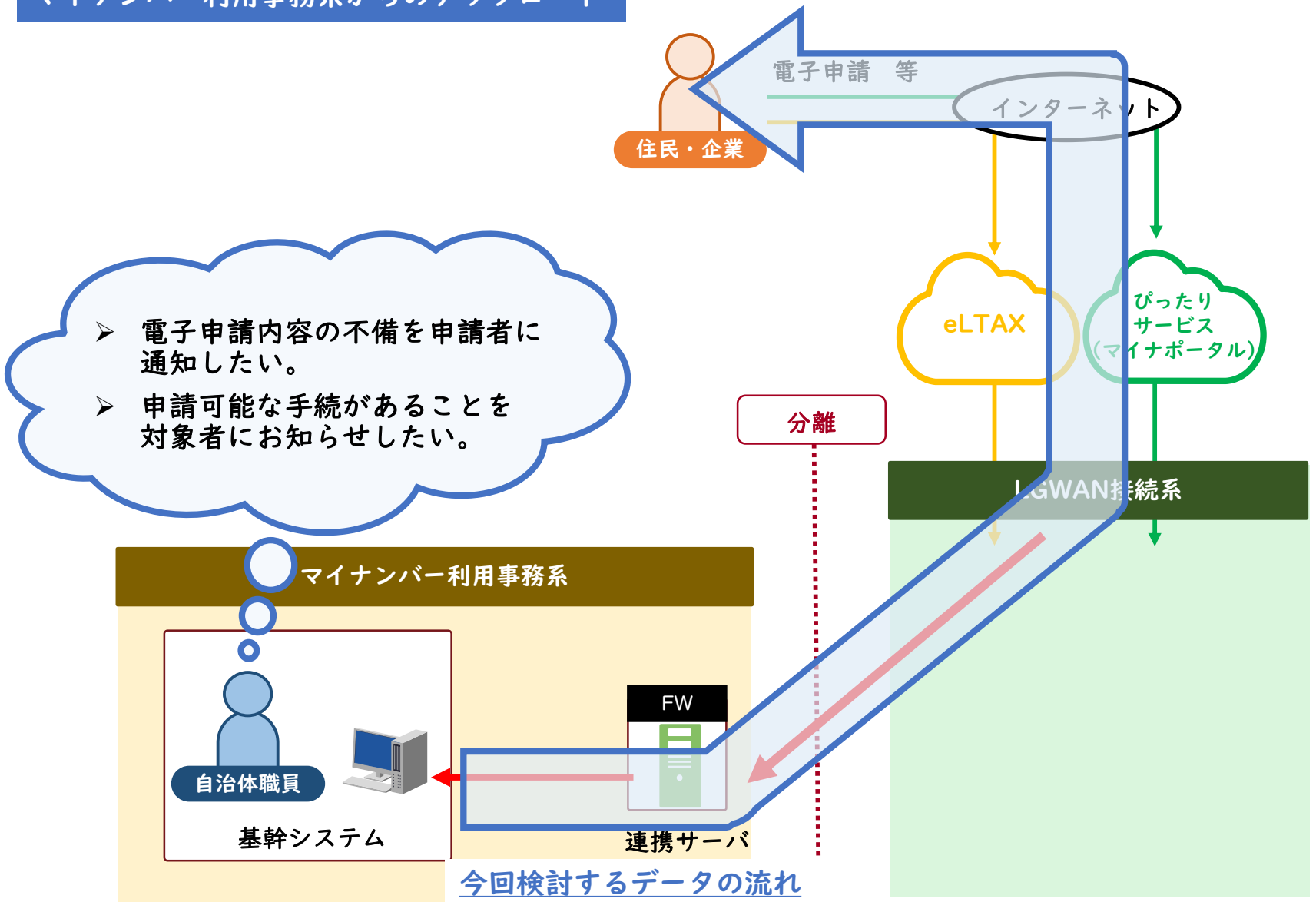
「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定について④

➢ 令和２年度のマイナンバー利用事務系の分離の見直し



「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」の改定について④

マイナンバー利用事務系からのアップロード



- 電子申請内容の不備を申請者に通知したい。
- 申請可能な手続があることを対象者にお知らせしたい。