令和５年度　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における中間報告

総 務 省

令和６年３月25日

総務省自治行政局

デジタル基盤推進室

中間報告について

✓ 今年度は以下の項目について議論し、方向性が固まった**LGWAN接続系のローカルブレイクアウト（α'モデル）と、令和５年度NISC政府統一基準群改定に関する対応**について、早期に自治体の事務に資する観点から、**中間報告としてとりまとめる**。

✓ 残りの検討項目については、来年度も継続して議論。

検討項目

LGWAN接続系のローカルブレイクアウト（α'モデル）の検討 / β'モデル 移行のための支援方策の検討

令和５年度NISC政府統一基準群改定に関する対応

ガイドライン上の機密性分類と政府機関の機密性分類の考え方の違いや具体例の追記

情報システムの品質管理の推進に関する対応

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

✓ Web会議等の目的で、業務端末からインターネット経由で、特定のクラウドサービスを安全に利用するための対策（アクセス制御等）をα'モデルとして規定。

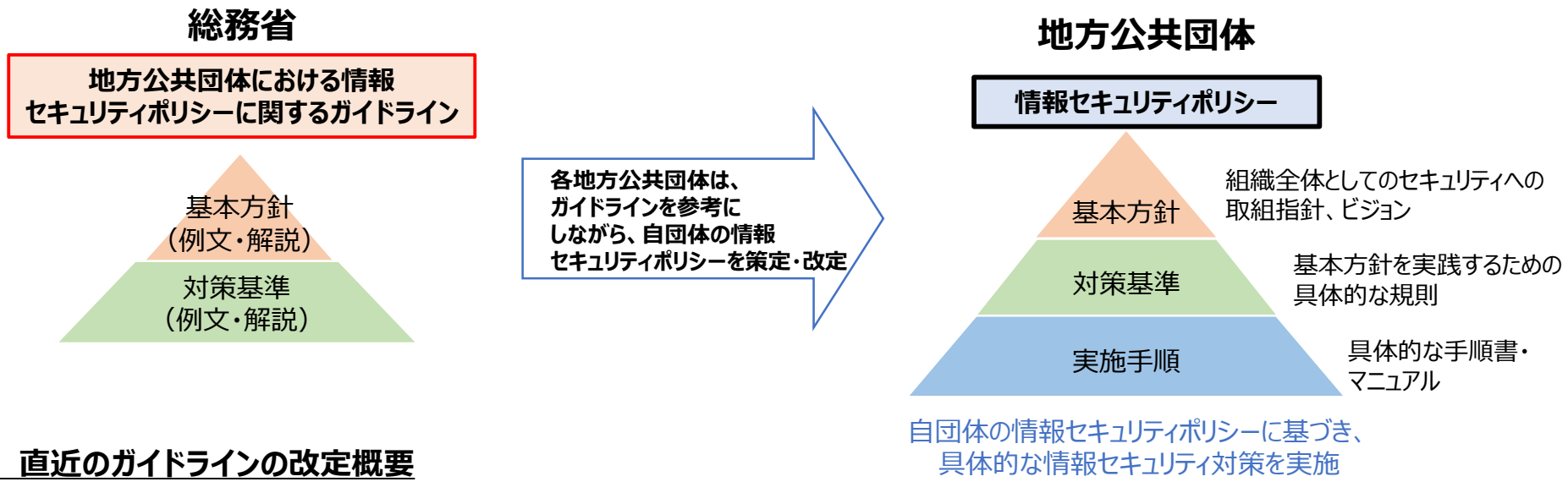
✓ β'移行の事例や移行にあたっての工夫を横展開することで、β'モデルへの移行を推進する。

✓ 政府統一基準の改定内容に沿って、業務委託の際に委託先に実施を求める対策の具体化、外部委託に関する分類の見直し等を実施。

「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」について

１．概要

各自治体のセキュリティー対策の指針として総務省が策定し助言。国における情報セキュリティ対策の動向やデジタル化の動向等を踏まえながら、有識者検討会での議論を経て、**年度ごとに改定を実施**。



２．直近のガイドラインの改定概要

改定時期	改定内容・理由
平成27年３月	「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（マイナンバー法）」、「サイバーセキュリティ基本法」の成立等の内容を反映
平成30年９月	平成27年の日本年金機構における情報流出事案を受け、総務省から地方公共団体へ要請を行った「三層の対策」等の情報セキュリティの抜本的強化策の内容を反映
令和２年12月	「三層の対策」の効果や課題、新たな時代の要請を踏まえ、セキュリティの確保と効率性・利便性向上の両立の観点から、情報セキュリティ対策の見直しを実施し、その内容を反映
令和４年３月	令和３年７月の「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群」の改定や地方公共団体のデジタル化の動向を踏まえた内容を反映
令和５年3月	標準準拠システム等のクラウドサービスの利用を想定し、クラウドサービスを利用する際の具体的な情報セキュリティ対策の内容を第4編（特則）に反映

（参考）ガイドラインの検討会

■ 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
井上 茂	港区芝地区総合支所区民課長
上原 哲太郎	立命館大学情報理工学部教授
大高 利夫	藤沢市総務部情報システム課
岡村 久道	弁護士 国立情報学研究所客員教授
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】
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
山崎 晋一	横浜市デジタル統括本部企画調整部担当課長

（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

（参考）ガイドラインの構成

第９回検討会資料再掲

- 地方公共団体が情報セキュリティポリシー（基本方針・対策基準）を策定、改定する際に、「第2編」の例文を参照し、活用することが可能な構成としている。
- 対策基準の例文の詳細な解説は、「第2編」の例文の構成と対応した内容で「第3編」に記載。
- クラウドサービス上で業務システムを利用する場合には、クラウドサービスの特性を踏まえた情報セキュリティ対策を考慮する必要があることから、「第4編」を特則として定めている。

編	項目	本編の主な内容	補足
第１編	総則	• ガイドラインの目的 • 地方公共団体における情報セキュリティとその対策 • 情報セキュリティ管理プロセス • 本ガイドラインの構成 • 対策レベルの設定 • クラウドサービスに関する留意点	• 情報セキュリティポリシーを策定するための前提となる事項を記載。 • 情報セキュリティポリシーの策定や改定のプロセス、クラウドサービスの留意点等を記載。
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）	• 情報セキュリティ基本方針（例文） • 情報セキュリティ対策基準（例文）	• 地方公共団体の基本方針、対策基準に定める文案の参考として、例文を記載。
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）	• 情報セキュリティ基本方針（解説） • 情報セキュリティ対策基準（解説）	• 第２編の例文と同様の構成で、具体的なセキュリティ対策の考え方を記載。
第４編	地方公共団体の情報システムのクラウド利用等に関する特則（例文・解説）	• 本編の目的 • 本編におけるクラウドサービスの範囲 • 本編における対策基準の構成 • 情報セキュリティ対策	• 標準準拠システム等のクラウド利用を行う場合に必要となる情報セキュリティ対策（対策基準）を、本編と同様の構成で例文と解説の形式で記載。
第５編	付録	• 権限・責任等一覧表	• 総務省セキュリティポリシーガイドラインで求められる役割を一覧で記載。

○「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」（令和５年３月28日改定）

https://www.soumu.go.jp/menu_news/s-news/01gyosei07_050328.html

現時点における改定案の構成

- ✓ **政府統一基準群の改定**に伴い、**第１編から第４編に至るまで、多くの項目について改定予定**。
- ✓ 第３編「３.情報システムの全体の強靭性の向上」において、**αモデルでローカルブレイクアウトを行いクラウドサービスを利用する際のセキュリティ要件**を追記予定。

第１編　総則
- 第1章　本ガイドラインの目的等
- 第2章　地方公共団体における情報セキュリティとその対策
- 第3章　情報セキュリティの管理プロセス
  - 1. 策定及び導入
  - 2. 運用
  - **3. 評価・見直し**（変更）

第２編・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（例文・解説）
- 第1章　情報セキュリティ基本方針
  - **8. 情報セキュリティポリシーの見直し**（変更）
- 第2章　情報セキュリティ対策基準
  - 1. 組織体制
  - 2. 情報資産の分類と管理
  - **3. 情報システム全体の強靭性の向上**（変更）（α'モデル追記）
  - 4. 物理的セキュリティ
    - 4.1 サーバ等の管理、 4.2 管理区域（情報システム室等）の管理
    - **4.3 通信回線及び通信回線装置の管理**（変更）
    - 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. 人的セキュリティ
    - 5.1 職員等の遵守事項、 5.2 研修・訓練
    - **5.3 情報セキュリティインシデントの報告**（変更）
    - 5.4 ID及びパスワード等の管理
  - 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**（変更）
    - **6.2 アクセス制御**（変更）
    - **6.3 システム開発、導入、保守等**（変更）
    - 6.4 不正プログラム対策、 6.5 不正アクセス対策
    - **6.6 セキュリティ情報の収集**（変更）
  - 7. 運用
    - **7.1 情報システムの監視**（変更）
    - 7.2 情報セキュリティポリシーの遵守状況の確認～ 7.6 懲戒処分等
  - **8. 業務委託と外部サービス（クラウドサービス）の利用**（見出し変更）
    - **8.1 業務委託**（変更）
    - **8.2 情報システムに関する業務委託**（新規作成）
    - **8.3 外部サービス（クラウドサービス）の利用（機密性２以上の情報を取り扱う場合）**（変更）
    - **8.4 外部サービス（クラウドサービス）の利用（機密性２以上の情報を取り扱わない場合）**（変更）
  - 9. 評価・見直し
    - **9.1 監査**（変更）
    - 9.2 自己点検
    - **9.3 情報セキュリティポリシー及び関係規程等の見直し**（変更）

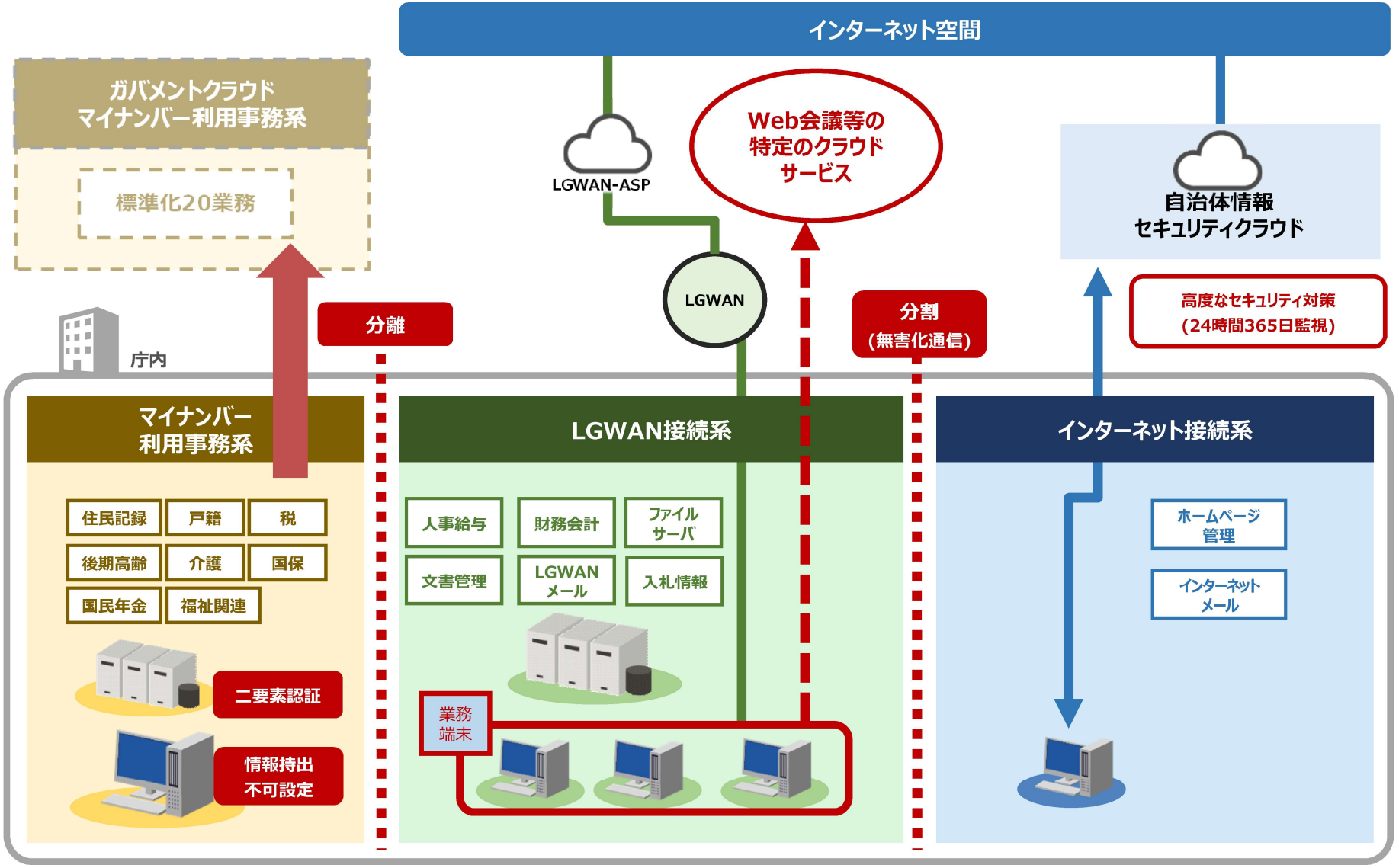
第4編　地方公共団体におけるクラウド利用等に関する特則
- 第1章　本編の目的について
- 第2章　本編におけるクラウドサービスの範囲について
- 第3章　本編における対策基準の構成について
- 第4章　情報セキュリティ対策について
  - 1. 組織体制～ 7. 運用
  - **8. 業務委託と外部サービス（クラウドサービス）の利用**（見出し変更）
  - 9. 評価・見直し

LGWAN接続系のローカルブレイクアウト（α'モデル）の検討

α'モデルについて　～LGWAN接続系からローカルブレイクアウト～

ガイドライン改定の方向性

- LGWAN接続系から外部のクラウドサービスに接続（ローカルブレイクアウト）するための、必要なセキュリティ対策をガイドライン上で規定する。
- α'モデルのリスク評価を行い、評価結果を踏まえてガイドラインに必要なセキュリティ対策を規定する。



リスクアセスメント概要

✓ 第三者認証制度による接続先の安全性担保、インターネット回線の利用を視野に入れてリスク評価を実施することとしてはいかがか。
✓ パブリッククラウドのサービス範囲に応じ、それぞれのケースを想定したセキュリティ対策を検討してはいかがか。

リスク評価の観点

✓ SaaS型サービスセキュリティは、ユーザ（自治体）側で完全に制御することが難しいため（※）、利用するパブリッククラウドの安全性を担保する方策が必要となる。
→ **ISMAPに登録されているサービス等、第三者認証により安全性が担保された接続先にのみ接続先を認める**方向性。

※例えば、ゲートウェイ機器をSaaSのデータセンターに自由に設置できないことなどが考えられる。

✓ 接続に用いる回線について、パブリッククラウドのサービス特性、帯域確保（特にWeb会議で利用する場合）および導入維持コストの観点を踏まえ、安全性を確保する必要がある。
→ **インターネット回線の利用を視野に入れた接続構成**にて検討。

✓ 利用するパブリッククラウドのサービス範囲に応じ、セキュリティリスクが異なる。
→ 認証のみ実施する場合と、外部とファイル送受信が発生する場合ではセキュリティリスクが異なるため、コストの観点から、**それぞれのケースを想定したセキュリティ対策を検討**。

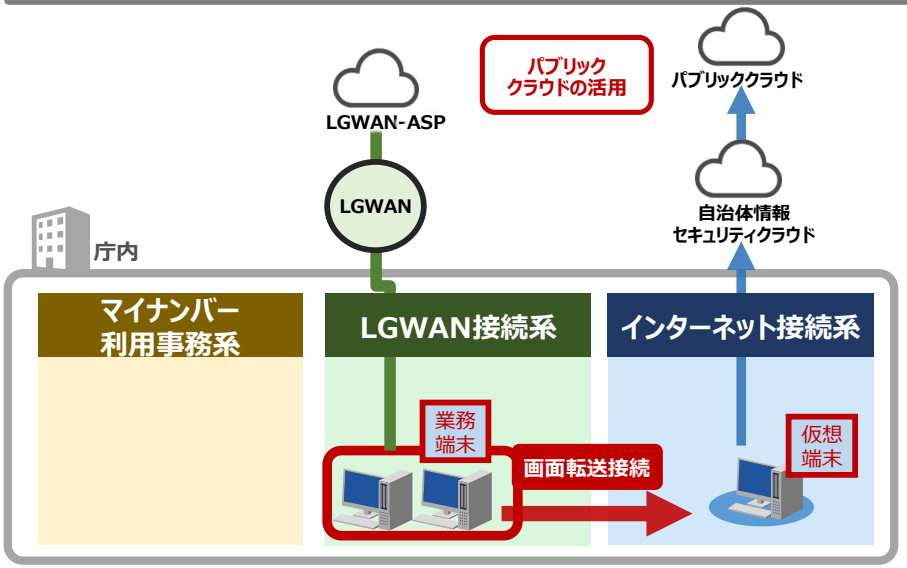
認証等	コミュニケーションツールの利用	外部とファイル送受信が発生
<例> ■ 認証・認可 ■ ウイルス定義ファイル配信	<例> ■ 認証・認可 ■ ウイルス定義ファイル配信 ■ Web会議、チャット	<例> ■ 認証・認可 ■ Web会議、チャット ■ ファイル送受信等

小 → セキュリティリスク → 大

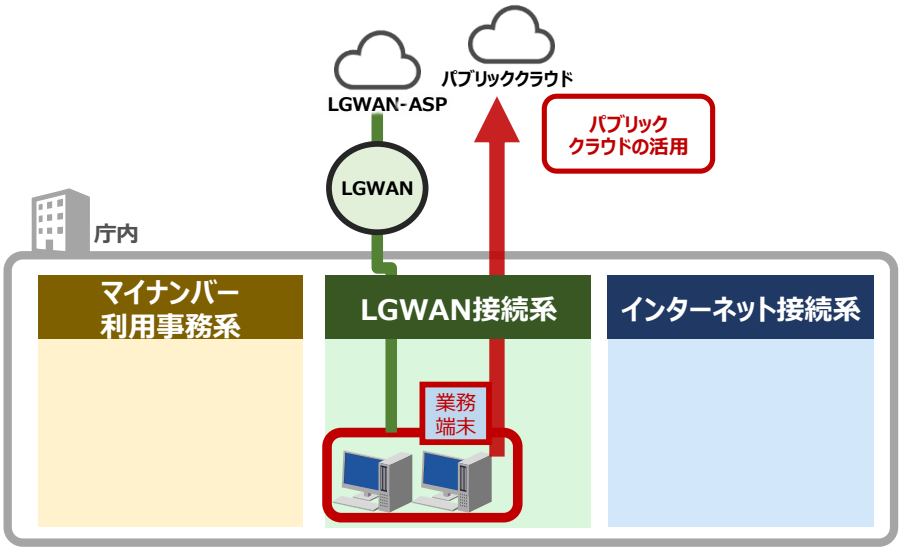
リスクアセスメント概要

✓現行ガイドラインで認められている都道府県セキュリティクラウド経由のローカルブレイクアウトを比較対象とし、LGWAN接続系からのローカルブレイクアウトのセキュリティリスクを分析する。

都道府県セキュリティクラウド経由のローカルブレイクアウト



LGWAN接続系からのローカルブレイクアウト



現行ガイドラインにおけるローカルブレイクアウトの記載

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

（３）インターネット接続系

自治体情報セキュリティクラウド構成団体からのクラウドサービスの利用増加等に伴うトラフィック増加に対応するため、ローカルブレイクアウトを行う場合には、その実施可否について、セキュリティ上のリスクを勘案し、都道府県、市区町村で協議の上、慎重に判断する必要がある。ローカルブレイクアウトを行う場合は、原則として、都道府県側の設定により、実施することとする。その場合、当該ルートを狙った攻撃等のリスクの増加を十分に理解した上で、例えば、信頼できる事業者が提供する特定のクラウドサービスのみローカルブレイクアウトを認める、構成団体と１対１で紐づく通信元IP・ポート番号と通信先IP・ポート番号をもとに通信をポリシーベースルーティングで振り分ける、ログイン状況やアプリケーションの利用状況の監視を行うなどといった適切なセキュリティ対策を講じるとともに、セキュリティインシデント発生時の対応手順をあらかじめ用意する必要がある。

資産ベースのリスク分析について

- ✓ リクスアセスメントは、**「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IPA）に沿って実施**。
- ✓ 上記ガイドに記載されている、資産ベースのリスク分析は、保護すべき制御システムを構成する資産群を明確化し、各資産に対するシステム構成上及び運用管理上に想定される脅威について、各資産の重要度と、その脅威の発生可能性と受容可能性（脆弱性）の相乗値によって、資産のリスクを評価するリスク分析手法である。
- ✓ なお本リスクアセスメントは、情報処理安全確保支援士が、その倫理綱領に従い、公正な立場で実施したものである。

資産ベースのリスク分析の流れ

順番	作業の概要
①	**資産の定義とその重要度を定義する** 分析対象の資産を、物理的なまとまりや論理的な機能単位（サーバ、端末、装置等）の観点で定義すると共に、各資産の重要度を定義する。
②	**各資産に対する脅威とそのレベルを定義する** 脅威レベルの判断基準を定義し、その基準を基に、各資産に対して、資産の機能、ネットワーク構成や利用環境等を考慮して、想定される脅威とその脅威レベル（それが実行される可能性）を定義する。
③	**資産の各脅威に対する脆弱性を評価する** 各脅威に対するセキュリティ対策の各資産における対策状況（対策レベル）を評価することにより、当該脅威に対する脆弱性を評価する。
④	**各資産の脅威に対するリスク値を算定する** ①と②③の相乗値によって、各資産の各脅威に対するリスク値を算定する。

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　IPA）
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

α'モデルにおけるクラウドサービス、接続回線の利用条件

(1) 利用するクラウドサービスの選定

・**ISMAPに登録されているクラウドサービスに限定する**

※ただし、ISMAP登録サービスであっても、自治体自身の責任で個々のサービスのセキュリティについて個別に検討し、必要な対策を実施する必要がある。

(2) クラウドサービスの利用条件

・**各団体専用領域（テナント）があり、当該団体職員のみが該当テナントにアクセスを許可する制御を行う。**

・クラウドサービスで利用するアプリケーションは以下を想定する。
  - Web会議システム(Micosoft社の例：Teams)
  - ファイル管理システム(Micosoft社の例：SharePoint、OneDrive)
  - メール(Micosoft社の例：Exchange)　※団体外部の組織からのメール受信することを想定している

・団体外部の組織から招待されたWeb会議は、インターネット接続系の業務端末で利用することを想定している。仮に当該Web会議をLGWAN接続系からブレイクアウトし、LGWAN接続系の業務端末から利用する場合は、ファイルの流出、流入に対する制御の設定等対策を実施する必要がある。**特にファイルの流入が想定される場合は、ファイル無害化等の対策を講じる必要がある。**

(3) 接続回線

・自治体からのニーズが大きいパブリッククラウドサービスが、インターネット回線での接続を前提としていることから、**インターネット回線が利用されることを前提とする。**

脅威に対するセキュリティ対策の考え方

脅威（攻撃手法）	考えられる主な対策 （太字は現在実施されていない対策または強化する対策）
外部（インターネット経由）不正アクセス ーインターネット経由で機器に侵入し、攻撃を実行する。	・権限管理 ・アクセス制御 ・パッチ適用
外部（インターネット経由）からのメール、Webアクセスによるマルウェア感染 ー攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	・通信相手の証明書による認証 ・マルウェア対策ソフト ・パッチ適用 **・LBOテナントアクセス制御** **・接続先制限** ・メール無害化/ファイル無害化 ・EDR
高負荷攻撃 ーインターネット経由のDDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。 または容量以上の通信トラフィックを発生させ、輻輳状態とする。	・DDoS対策 ・冗長化
プロセス不正実行 ー侵入したマルウェアが攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	・権限管理 ・アクセス制御 ・EDR
侵入した攻撃者、マルウェアの内部拡散 ー侵入したマルウェアが内部ネットワークの機器を探索し、残存する脆弱性やファイル共有等を利用し、通信可能な機器、システムに侵入を広げ、攻撃する。 または、マルウェアに感染したファイルがWeb会議等で共有され拡散する。	・マルウェア対策ソフト ・パッチ適用 ・IDS/IPS ・権限管理 **・LBOテナントアクセス制御** **・接続先制限** ・EDR
通信データ改ざん ーネットワーク上を流れる情報を改ざんする。	・通信路暗号化 ・通信相手の証明書による認証

※ローカルブレイクアウトとは直接関係のない物理的な脅威等は対象外とする。

（参考）対策レベルとリスク値

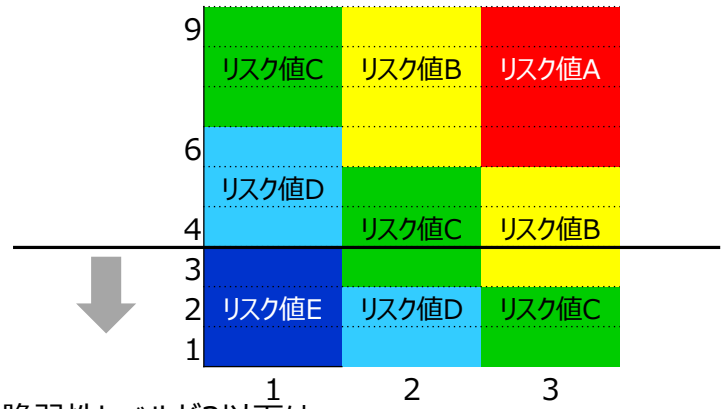
- ✓ 脅威レベルが最も高い3（脅威が発生しやすい）であっても、十分な対策により脆弱性が１であれば、脅威レベル×脆弱性レベル＝3となり安全である。
- ✓ 対策が不十分で脆弱性が3であっても、脅威レベルが最も低い1(脅威が発生しにくい）であれば、脅威レベル×脆弱性レベル＝3となり安全である。

対策レベルと脆弱性レベルの対応

対策レベル	判断基準	脆弱性レベル
3	当該脅威（攻撃手段）において、複数の「防御」「検知／被害把握」可能な対策項目を多層で実施しており、攻撃が成功する可能性は低い。（即ち、○が二つ以上）	1
2	当該脅威（攻撃手段）において、「防御」「検知／被害把握」可能な対策項目を実施している。 即ち、○が一つ以上ついているが、十分とは言えないため、攻撃が成功する可能性は中程度である。	2
1	当該脅威（攻撃手段）において、「防御」「検知／被害把握」可能な対策項目を実施していない。 即ち、○が一つもついておらず、攻撃が成功する可能性は高い。	3

リスク値

脅威レベル×脆弱性レベル



脅威レベル×脆弱性レベルが3以下は対策の効果があり、安全と考える対象とする

リスク値	意味
A	リスクが非常に高い。
B	リスクが高い。
C	リスクが中程度。
D	リスクが低い。
E	リスクが非常に低い。

資産の重要度

評価値	評価基準
3	・資産が失われた、もしくは不正に操作された場合、事業上の被害大となる。 －システムの停止が業務停止につながる
2	・資産が失われた、もしくは不正に操作された場合、事業上の被害中となる。 －システムの停止による業務停止が限定される
1	・資産が失われた、もしくは不正に操作された場合、事業上の被害小となる。 －システムの停止が業務間停止につながらない

リスクアセスメント結果（a'モデルと自治体情報セキュリテイクラウドのローカルブレイクアウト比較）

- ✓ **自治体情報セキュリテイクラウド**は、インターネットとの通信において、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施しており、**既にガイドラインで規定されているローカルブレイクアウトを実施した場合も、アクセス先のクラウドサービスの通信は同様に保護される**。
- ✓ 想定したa'モデルの技術的対策を実施した場合と、自治体情報セキュリテイクラウドにおけるローカルブレイクアウトを実施した場合のリスク値に差がなく（＝自治体セキュリティクラウドのローカルブレイクアウトと同様のセキュリティレベルが担保される）、かつ、**３以下であり安全性が確保された水準**であった。

１．a'モデルのローカルブレイクアウトのリスクアセスメント結果＜資産ベース＞

脅威 ＼ 資産	LGWAN接続系の各資産
重要度	
外部（インターネット経由）不正アクセス	資産別に脅威に対するリスクを対策と資産の重要度から評価
外部（インターネット経由）からのメール、Webアクセスによるマルウェア感染	
高負荷攻撃	
プロセス不正実行	
侵入した攻撃者、マルウェアの内部拡散	
通信データ改ざん	

リスク値が全て**脅威レベル×脆弱性レベル≦3**であり、対策が十分に行われており、安全だと判断する。

２．自治体情報セキュリテイクラウドのローカルブレイクアウトのリスクアセスメント結果＜資産ベース＞

脅威 ＼ 資産	LGWAN接続系やインターネット接続系の各資産
重要度	
外部（インターネット経由）不正アクセス	資産別に脅威に対するリスクを対策と資産の重要度から評価
外部（インターネット経由）からのメール、Webアクセスによるマルウェア感染	
高負荷攻撃	
プロセス不正実行	
侵入した攻撃者、マルウェアの内部拡散	
通信データ改ざん	

リスク値が全て**脅威レベル×脆弱性レベル≦3**であり、対策が十分に行われており、安全だと判断する。

α'モデルの対策（クラウドサービスのライセンス認証・認可のみの場合）

＜前提条件＞

（１）利用するクラウドサービス

・ ISMAPに登録されているクラウドサービス

（２）クラウドサービスの利用条件

・ アプリケーションを利用するためのライセンスの認証・認可でクラウドサービスにアクセスする
・ 各団体専用領域（テナント）を保有しない
・ Web会議システム、メールなどのアプリケーションを利用しない

●技術的対策（案）

対策を実施しなくてもリスクアセスメント結果において、リスク値が３以下となった対策は推奨とする。

技術的対策	対策の定義	必須	推奨
LGWAN接続系での対策			
接続先のクラウドサービスの証明書による認証	接続先のクラウドサービスが本物であるか否か、正当性を確認する。	○	
マルウェア対策ソフト	パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。	○	
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。	○	
接続先制限	LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。	○	
権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。	○	
DDoS対策	サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。	○	
冗長化	ローカルブレイクアウトファイアウォールに対するDDoS攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。		○
通信路暗号化	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。	○	

α'モデルの対策（コミュニケーションツールを利用するがファイルを内部に取り込まない場合）①

＜前提条件＞

（１）利用するクラウドサービス

・ISMAPに登録されているクラウドサービス

（２）クラウドサービスの利用条件

・**各団体専用領域（テナント）があり、当該団体職員のみが該当テナントにアクセスを許可する**制御が可能

・**外部団体のテナントにアクセスする場合（外部団体から招待されたWeb会議に参加し、ファイル交換をする等）は、インターネット接続系の端末からアクセスする。**

・クラウドサービスで利用するアプリケーションは以下のとおり

- **Web会議システム**
- **ファイル管理システム**
- **メール**

なお、メールは、インターネット接続系のメール利用を前提とするが、災害時にインターネット接続系のメール利用不可となった時を考慮し、クラウドサービスでのメール利用も想定する。

・クラウドサービスの**Web会議やメールで取り扱うファイルのマルウェア検査が可能**（例：Defender）

・ファイルはクラウドサービス上での共有、編集を可能とし、**PCにはダウンロードさせない設定**が可能

●技術的対策（案）※次項に続く

対策を実施しなくてもリスクアセスメント結果において、リスク値が３以下となった対策は推奨とする。

技術的対策	対策の定義	必須	推奨
クラウドサービス上での対策			
マルウェア対策	クラウドサービス上でWeb会議やインターネットメールで取り扱うファイルのマルウェア検査を行う。		○
クラウドサービスからファイルダウンロード制限	クラウドサービス上から業務端末へのファイルダウンロードを制限する。	○	
LGWAN接続系での対策			
接続先のクラウドサービスの証明書による認証	接続先のクラウドサービスが本物であるか否か、正当性を確認する。	○	
マルウェア対策ソフト	パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。	○	
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。	○	

α'モデルの対策（コミュニケーションツールを利用するがファイルを内取り込まない場合）②

●技術的対策（案）※次項からの続き

技術的対策	対策の定義	必須	推奨
LGWAN接続系での対策			
接続先制限	LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。	○	
ローカルブレイクアウトテナントアクセス制御	利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する。	○	
メール無害化/ファイル無害化	ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネットからファイルを取り込む。なお、本対策におけるファイル無害化とは、インターネットメールに添付されたファイルの無害化を指す。	○	
権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。	○	
アクセス制御	不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認証・認可に基づき、アクセスの許可または拒否を行う。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。	○	
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。LGWAN接続系に配置する端末、業務サーバにて対応が必要。		○
IDS/IPS	ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。	○	
DDoS対策	サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。	○	
冗長化	ローカルブレイクアウトファイアウォールに対するDDoS攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。		○
通信路暗号化	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。	○	

α'モデルの対策（外部とファイル送受信を行う場合）①

＜前提条件＞

（１）利用するクラウドサービス

- ISMAPに登録されているクラウドサービス

（２）クラウドサービスの利用条件

- **各団体専用領域（テナント）があり、当該団体職員のみが該当テナントにアクセスを許可する**制御が可能
- クラウドサービスで利用するアプリケーションは以下のとおり
  - **Web会議システム**
  - **ファイル管理システム**
  - **メール**

    なお、メールは、インターネット接続系のメール利用を前提とするが、災害時にインターネット接続系のメール利用不可となった時を考慮し、クラウドサービスでのメール利用も想定する
- クラウドサービスのWeb会議やメールで取り扱う**ファイルのマルウェア検査が可能**（例：Defender）

●技術的対策（案）※次項に続く

対策を実施しなくてもリスクアセスメント結果において、リスク値が３以下となった対策は推奨とする。

技術的対策	対策の定義	必須	推奨
クラウドサービス上での対策			
マルウェア対策	クラウドサービス上でWeb会議やインターネットメールで取り扱うファイルのマルウェア検査を行う。		○
LGWAN接続系での対策			
接続先のクラウドサービスの証明書による認証	接続先のクラウドサービスが本物であるか否か、正当性を確認する。	○	
マルウェア対策ソフト	パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。	○	
パッチ適用	脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。	○	
接続先制限	LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。	○	
ローカルブレイクアウトテナントアクセス制御	利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する。	○	

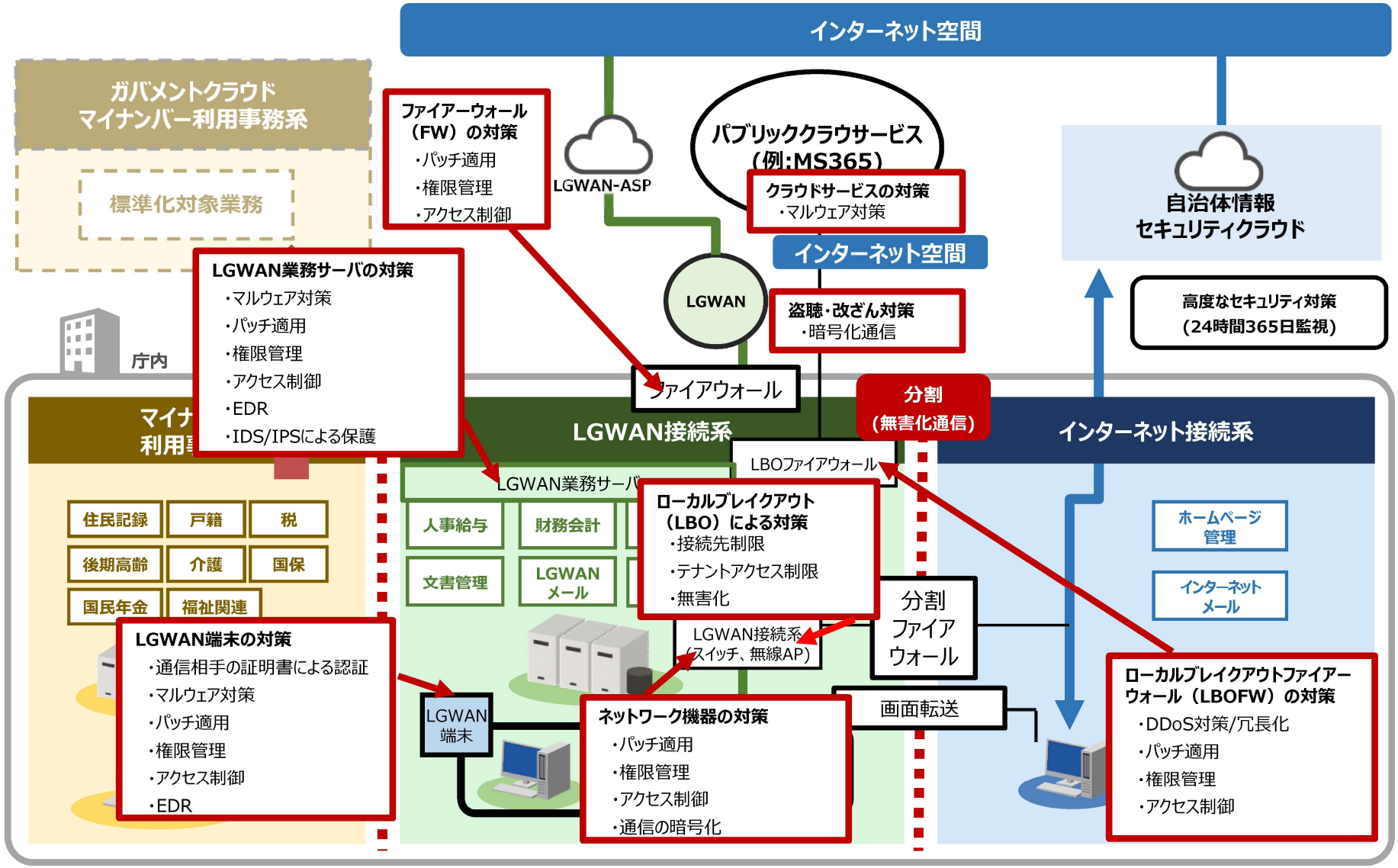
α'モデルの対策（外部とファイル送受信を行う場合）②

●技術的対策（案）※次項からの続き

技術的対策	対策の定義	必須	推奨
LGWAN接続系での対策			
メール無害化/ファイル無害化	ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネットからファイルを取り込む。 ※詳細は、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　（２）LGWAN接続系①LGWAN接続系とインターネット接続系の分割　を参照。	○	
権限管理	不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。	○	
アクセス制御	不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う。LGWAN端末、LGWAN業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。	○	
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。LGWAN接続系に配置する端末、業務サーバにて対応が必要。		○
IDS/IPS	ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。	○	
DDoS対策	サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。	○	
冗長化	ローカルブレイクアウトファイアウォールに対するDDoS攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。		○
通信路暗号化	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。	○	

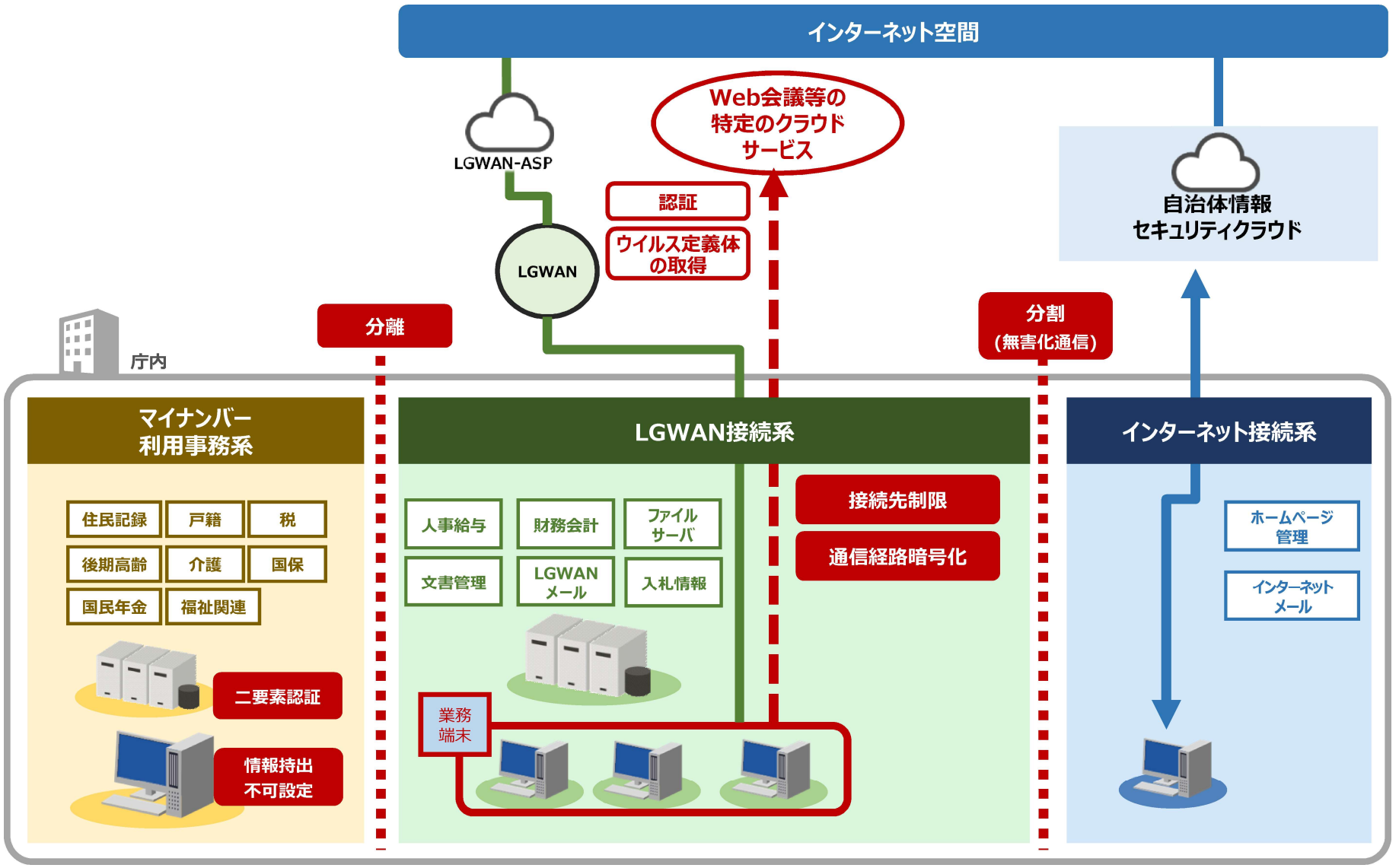
α'モデルの技術的対策

✓ 最もリスクの大きい、外部とファイル送受信を行う場合に必要な対策を以下に示す。



α'モデルの技術的対策（認証・ウイルス定義体の取得のみの場合）のイメージ図

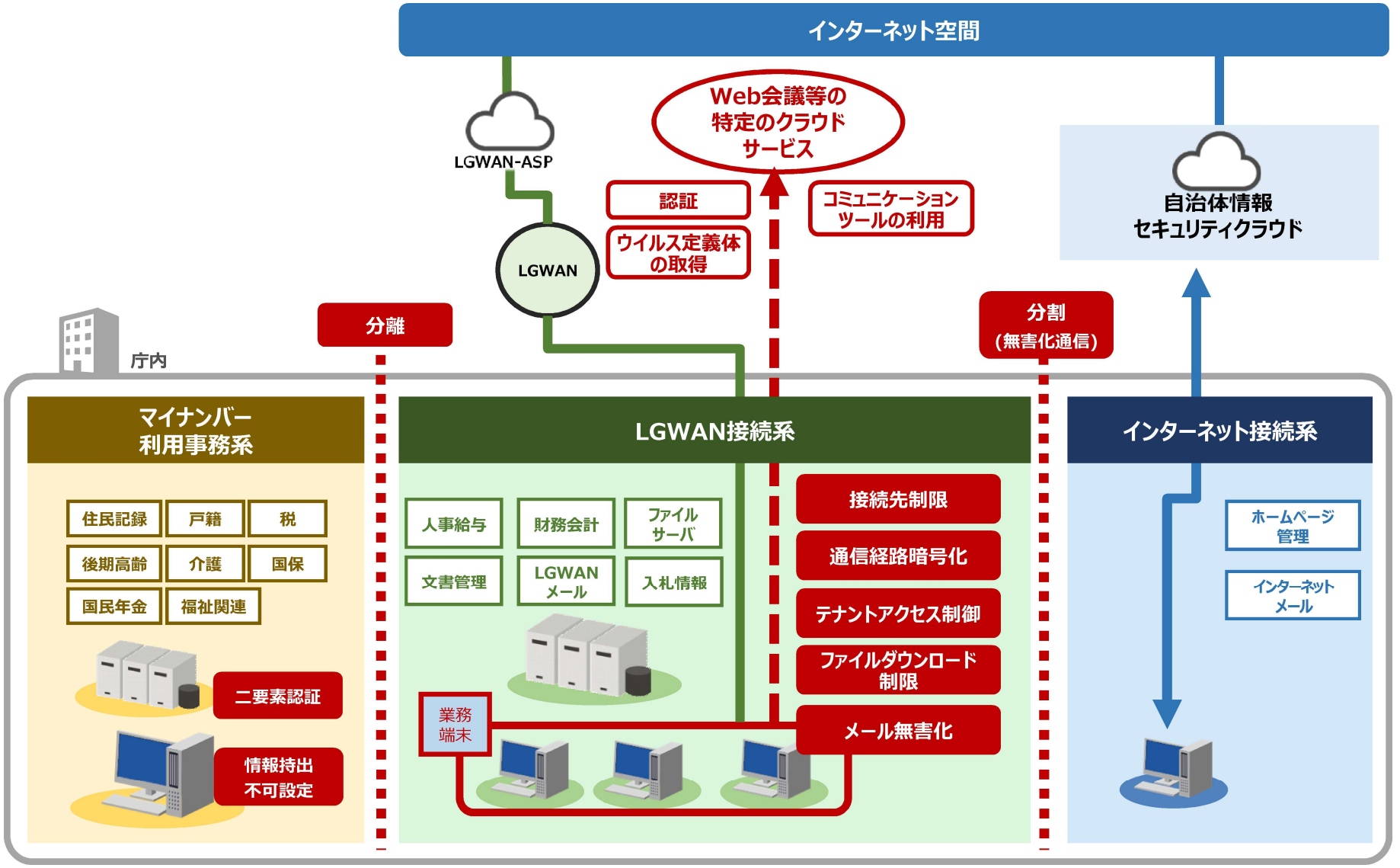
✓ 認証・ウイルス定義体の取得のみの場合におけるセキュリティ対策のネットワーク構成イメージは以下の通り。



※各セキュリティ対策の性質に着目しセキュリティ対策を講じる場所を抽象化して表記している。また、すべての対策を網羅していないため、厳密な図とはなっていない。

α'モデルの技術的対策（コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合）のイメージ図

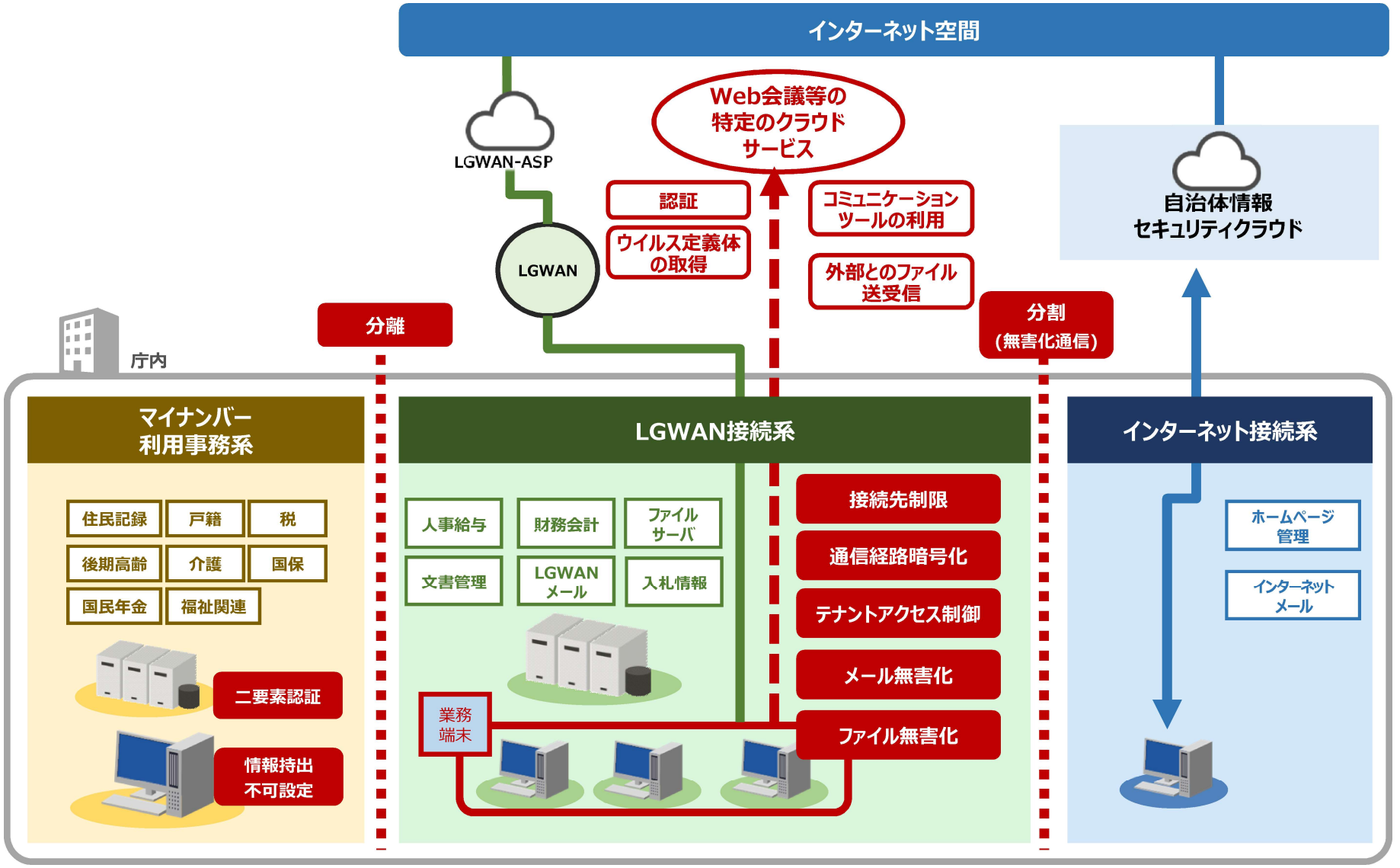
✓ コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合におけるセキュリティ対策のネットワーク構成イメージは以下の通り。



※各セキュリティ対策の性質に着目しセキュリティ対策を講じる場所を抽象化して表記している。また、すべての対策を網羅していないため、厳密な図とはなっていない。

α'モデルの技術的対策（外部とファイル送受信を行う場合）のイメージ図

✓ 外部とファイル送受信を行う場合におけるセキュリティ対策のネットワーク構成イメージは以下の通り。



※各セキュリティ対策の性質に着目しセキュリティ対策を講じる場所を抽象化して表記している。また、すべての対策を網羅していないため、厳密な図とはなっていない。

α'モデルの組織的・人的対策（案）

技術的対策	対策の定義	必須	推奨
組織的・人的対策			
手続・規定	クラウドサービスを利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底しなければならない。	○	
組織・人的な対応	以下の組織的・人的対策に加え、本ガイドラインの「５.人的セキュリティ」記載の組織的・人的対策を確実に実施する。 ・職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 ・職員等の実践的サイバー防御演習（CYDER）の受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し	○	

検討会における主な意見

- ✓ **地方公共団体は、自ら責任を持ってセキュリティを確保すべきであることを明示すべきであり、その旨を強調すべき**との意見があった。
- ✓ **クラウドサービスの設定確認は、サービスのアップデートの際にも行う必要がある**旨を明記すべきとの意見があった。

検討項目	視点	発言要旨
LGWAN接続系のローカルブレイクアウト（α'モデル）	責任の所在	• **インシデントが発生した際自治体の責任になるということを改めて留意する必要がある**。難しい話であればあるほど、最終的な判断が自治体側ではできず、自治体側が業者に頼んだ時点、クラウドに頼んだ時点、あるいは自治体ガイドラインやISMAPに載っている時点で手離れしてしまう可能性がある。

ガイドライン改定の方向性

- ➢ **情報セキュリティの確保は自治体の責任となることを改めて明記**する。

検討項目	視点	発言要旨
LGWAN接続系のローカルブレイクアウト（α'モデル）	品質の確保	• 接続先のクラウドサービスにおける設定に誤りがないか、定期的な確認を行うことが必要と書いてあるが、定期的だけでは足りない場合として、アップデートに伴う仕様変更で齟齬が生じたことがあるため、その点も明記をしてほしい。

ガイドライン改定の方向性

- ➢ クラウドサービスのアップデートに伴う仕様変更があった際も、設定の確認が必要なことを記載する。
- ➢ クラウドサービスのアップデートによる仕様変更に伴う事故事例を記載する。

ガイドライン改定案（見え消し）①

改定案：対策基準（解説）

第2章
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）
②LGWAN-ASPとの接続
（略）
③主に外部のクラウドサービスの利用を目的として、LGWAN接続系から接続先にローカルブレイクアウトする構成として、α’モデルが考えられる。
本モデルの採用を検討する際に、留意すべき観点は以下のとおりである。
まず、地方公共団体は、その保有する情報資産を守るにあたり、自ら責任を持ってセキュリティを確保すべきものであることを改めて認識することが重要である。

○サイバーセキュリティ基本法（平成26年法律第104号）
（地方公共団体の責務）
第五条　**地方公共団体は**、基本理念にのっとり、国との適切な役割分担を踏まえて、**サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する**。

LGWAN接続系に配置された業務端末から、インターネット接続により直接外部のクラウドサービスを活用することが可能となるため、外部からの脅威が増加することになる。その結果、LGWAN接続系に設置された業務システムの停止や重要な情報資産の漏えいなどに加え、LGWANへ脅威が侵入した場合は、更なる被害の拡大に繋がる恐れもある。このようなインシデントが発生した場合、上記のとおり、保有する情報資産を守る立場にあり、セキュリティ確保の責務を有する地方公共団体が責任を負うことになるため、セキュリティ対策に万全を期す必要がある。
このため、本モデルにおいて利用可能なクラウドサービスは、ISMAP管理基準を満たし、ISMAPクラウドサービスリストに登録されているサービスとする。
なお、ISMAPに登録されたクラウドサービスを基盤として構築されたことをもって、その構築されたサービスを、ISMAP登録サービスとして扱ってはならないことに留意する。ただし、セキュリティ関連サービス（ウィルス定義ファイルやIPアドレス、URLドメインリスト等の更新をインターネット経由で提供するサービス）については、更新情報の配信ツールであるため、
・行政文書や行政文書に相当する情報を扱わないこと
・利用するクラウドサービスの接続先のURLを確認の上、当該接続先のみに接続を制限すること
・信頼できる機関が発行した証明書を用いた認証の実施により、サービス提供元の真正性が担保されていること（この対策だけではなく、上記のURLを用いた接続先制限も併せて実施すること）
を条件に、ISMAPクラウドサービスリストに登録されていないクラウドサービスについても、利用を認めるものとする。
また、地方公共団体においては、採用したクラウドサービスへのみ、安全につなぐ（＝採用したクラウドサービス以外の通信を確実に遮断する）ことが重要となるため、接続先制限やアクセス制御、テナントアクセス制御等の技術的対策が必要となる。このようなテナントアクセス制御を適切に行うため、接続先のクラウドサービスにおける設定に誤りがないか、定期的な確認に加え、アップデートに伴う仕様変更の際の確認を行うことが必要であり、設定や確認作業等を外部に委託する場合は、そのサービスの品質が保証されるよう、契約で担保する必要がある（第２編、第３編8.1.業務委託参照）。

ガイドライン改定案（見え消し）②

改定案：対策基準（解説）

【仕様変更による事故事例】
・クラウドサービスの設定ミスにより、不適切なアクセス権限をデータに付与していた。それにより新しい機能がリリースされた際に、意図しない情報が外部から参照できる状態になってしまった。
以下の「Salesforce の製品の設定不備による意図しない情報が外部から参照される可能性について 」（2021年1月29日内閣官房内閣サイバーセキュリティセンター（NISC））参照）。
https://www.nisc.go.jp/pdf/policy/infra/salesforce20210129.pdf

・「クラウドサービス利用・提供における適切な設定のためのガイドライン」（2022年 10 月総務省）に以下のとおり事例を記載している。
Ⅱ．２ 設定不備の要因と対策
Ⅱ．2．１ 設定不備の事例と要因分析
事例１
クラウドサービス提供事業者が、提供している SaaS の機能変更を行った。これに伴い、当該 SaaS のユーザーアクセスに関する設定について、結果的にデフォルトでセキュリティレベルが下がってしまった。利用企業側はこれに気づかず、低いセキュリティレベルのまま利用し続けた結果、機密情報が大量に流出した。
事例３
ある企業の業務委託先が、サーバからクラウドサービスへのデータ移行を行う際に、ストレージの設定を公開設定としていた。これにより長期間機密情報が公開されている状態になった。
（https://www.soumu.go.jp/main_content/000843318.pdf）

ガイドライン改定案（見え消し）③

改定案：対策基準（解説）

第2章
3.情報システム全体の強靭性の向上
(２)LGWAN接続系
③
（前ページからの続き）
（略）

さらに、クラウドサービスへのアクセス状況やアプリケーションの利用状況についてログを取得し、状態監視を行うなど適切なセキュリティ対策を講じるとともに、セキュリティインシデント発生時の対応手順をあらかじめ用意する必要がある（第４編　情報セキュリティインシデントの報告　参照）。この点を、第２編、第３編の8.3.及び8.4.の外部サービス(クラウドサービス)の利用で規定している各事項と合わせて、留意すること。
α’モデルを採用する場合は、従来モデル（αモデル）と比較してインターネットからのリスクが増加し、より高度なセキュリティ対策の確実な実施が必要になることから、その実施について事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出することとする。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出することとする。なお、外部による事前確認や外部監査を行う者については、監査の対象となる情報資産に直接関与しない者であることが望ましい。

第2章
9.評価・見直し
9.1.監査
（略）
(２)監査を行う者の要件
（略）
（注２）監査業務を事業者に請け負わせる場合には、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監査サービスに係る部分）を活用することも考えられる。
参考：経済産業省「情報セキュリティサービス審査登録制度」（https://www.meti.go.jp/policy/netsecurity/shinsatourokuu/touroku.html）

ガイドライン改定案（見え消し）④

改定案：対策基準（解説）

α’モデルを利用する場合においては、利用するクラウドサービスのサービス範囲に応じて、セキュリティ対策を検討する必要があるため、以下の（ア）～（ウ）のとおり、利用範囲の異なる３つのケースを想定し、それぞれにセキュリティ対策を記載する。ただし、利用するクラウドサービスは多様であり、すべてのケースを想定することは困難であるため、α’モデルを採用する場合は、地方公共団体ごとのサービス利用範囲を踏まえて、個別に検討する必要がある。今回示す３つのケースは昨今の動向を踏まえた、最も基本的なケースであり、セキュリティ対策は、最終的には地方公共団体の責任でもって実施するとともに、記載しているセキュリティ対策以外の対策の導入も考えられることに留意すること。

クラウドサービスを利用した際のセキュリティリスクを低減するための対応として、（ア）～（ウ）に示されたもの以外の技術的対策の導入する場合は、定量的な分析によりリスクが低減されることを確認すること。

（ア）α’モデル：主に外部のクラウドサービスの利用を目的として、LGWAN接続系から接続先にローカルブレイクアウトする構成（認証・ウイルス定義体の取得のみの場合）

本モデルは以下のクラウドサービス利用の構成である。

- アプリケーションを利用するためのライセンスの認証・認可でクラウドサービスにアクセスする
- 各団体専用領域（テナント）を保有しない
- Web会議システム、メールなどのアプリケーションを利用しない

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

対策区分	セキュリティ対策	概要
技術的対策	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。
	接続先制限	・LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。
	権限管理	・不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。
	DDoS対策	・サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。
	通信路暗号化	・通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。
組織的・人的対策	手続・規定	・クラウドサービスを利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底しなければならない。
	組織・人的な対応	・以下の組織的・人的対策に加え、本ガイドラインの「5.人的セキュリティ」記載の組織的・人的対策を確実に実施する。職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 ・職員等の実践的サイバー防御演習（CYDER）の受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し

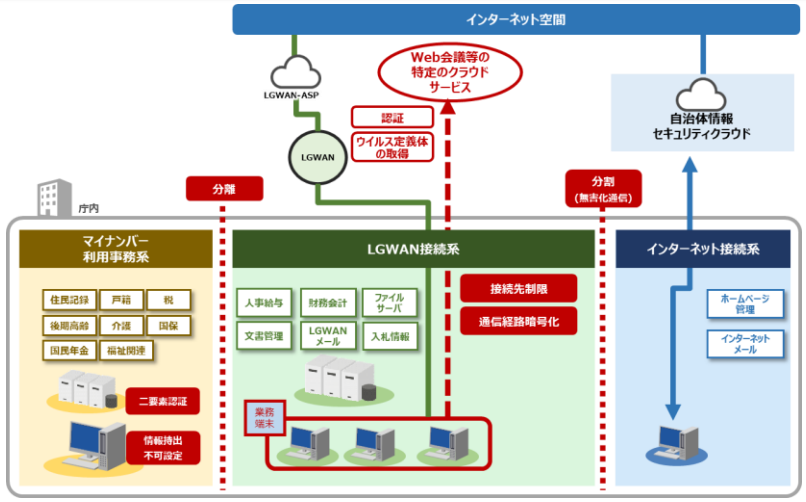
図表26　α’モデル（認証・ウイルス定義体の取得のみの場合）における必須のセキュリティ対策について

α’モデル（認証・ウイルス定義体の取得のみの場合）については、以下の対策も有効である。

・システムに対するDDoS攻撃発生時の継続稼働を保証するため、あるいは障害状態からの早期回復を実現するための、構成要素の冗長化

ガイドライン改定案（見え消し）⑤

改定案：対策基準（解説）



図表26 α’モデル（認証・ウイルス定義体の取得のみの場合）イメージ図
※セキュリティ対策の性質に着目し、セキュリティ対策を講じる場所を抽象化して表記している。
また、すべての対策を網羅していないため、厳密な図とはなっていない。

（イ）α’モデル：主に外部のクラウドサービスの利用を目的として、LGWAN接続系から接続先にローカルブレイクアウトする構成（コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合）

本モデルは以下のクラウドサービス利用の構成である。

・Web会議システム、団体外の組織を自テナントのWeb会議に招待し、会議を行うがLGWAN接続系へのファイルのダウンロードは制限する

※ 外部団体のテナントにアクセスする場合(外部団体から招待されたWeb会議に参加し、ファイル交換をする等）は、インターネット接続系の端末からアクセスする

・団体外の組織とファイル管理システムを通じ、ファイルの共有を行うが、LGWAN接続系にファイルのダウンロードは制限する

・メール、団体外の組織からのメール受信あり

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

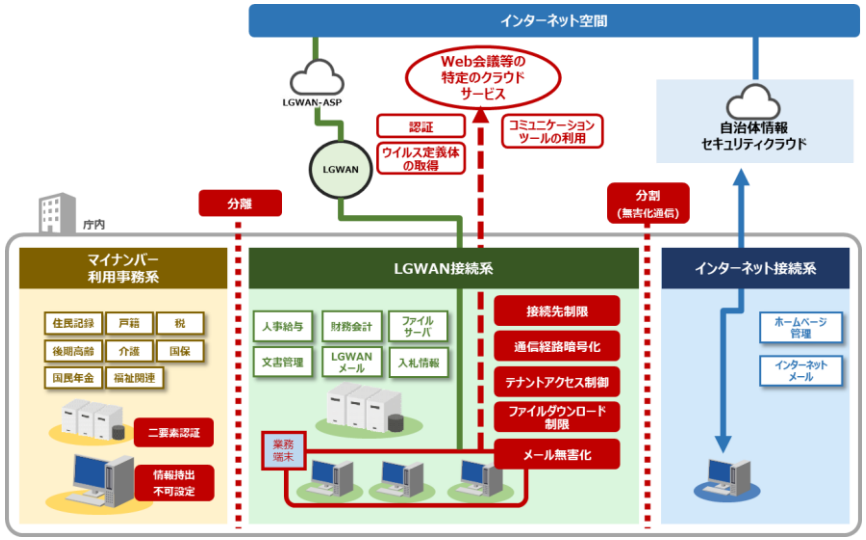
対策区分	セキュリティ対策	概要
技術的対策	クラウドサービスからファイルダウンロード制限	・クラウドサービス上から業務端末へのファイルダウンロードを制限する。
	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。
	接続先制限	・LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。
	ローカルブレイクアウトテナントアクセス制御	・利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する。
	メール無害化/ファイル無害化	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネットからファイルを取り込む。なお、本対策におけるファイル無害化とは、インターネットメールに添付されたファイルの無害化を指す。 ※詳細は、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(２)LGWAN接続系①LGWAN接続系とインターネット接続系の分割を参照。
	権限管理	・不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。
	アクセス制御	・不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認証・認可に基づき、アクセスの許可または拒否を行う。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。
	IDS/IPS	・ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。
	DDoS対策	・サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。
	通信路暗号化	・通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。
組織的・人的対策	手続・規定	・クラウドサービスを利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底しなければならない。
	組織・人的な対応	以下の組織的・人的対策に加え、本ガイドラインの「５.人的セキュリティ」記載の組織的・人的対策を確実に実施する。 ・職員等が毎年度最低１回は情報セキュリティ研修を受講可能となる研修計画の策定 ・職員等の実践的サイバー防御演習（CYDER）の受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し

図表28 α’モデル（コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合）における必須のセキュリティ対策について

ガイドライン改定案（見え消し）⑥

改定案：対策基準（解説）

α’モデル（コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合）については、以下の対策も有効である。
・システムに対するDDoS攻撃発生時の継続稼働を保証するため、あるいは障害状態からの早期回復を実現するための、構成要素の冗長化
・クラウドサービス上でのマルウェア対策
・未知の不正プログラムへの対策（エンドポイント対策）



図表28 α’モデル（コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合）イメージ図
※セキュリティ対策の性質に着目し、セキュリティ対策を講じる場所を抽象化して表記している。
また、すべての対策を網羅していないため、厳密な図とはなっていない。

（ウ）α’モデル：主に外部のクラウドサービスの利用を目的として、LGWAN接続系から接続先にローカルブレイクアウトする構成（コミュニケーションツールを利用し、外部とファイル送受信を行う場合）

本モデルは以下のクラウドサービス利用の構成である。
- Web会議システム、団体外の組織を自テナントのWeb会議に招待し、会議を行う
  ※ 外部団体のテナントにアクセスする場合(外部団体から招待されたWeb会議に参加し、ファイル交換をする等）は、インターネット接続系の端末からアクセスする
- 団体外の組織とWeb会議システムを通じ、ファイルの共有を行う
- 団体外の組織とファイル管理システムを通じ、ファイルの共有を行う
- メール、団体外の組織からのメール受信あり

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

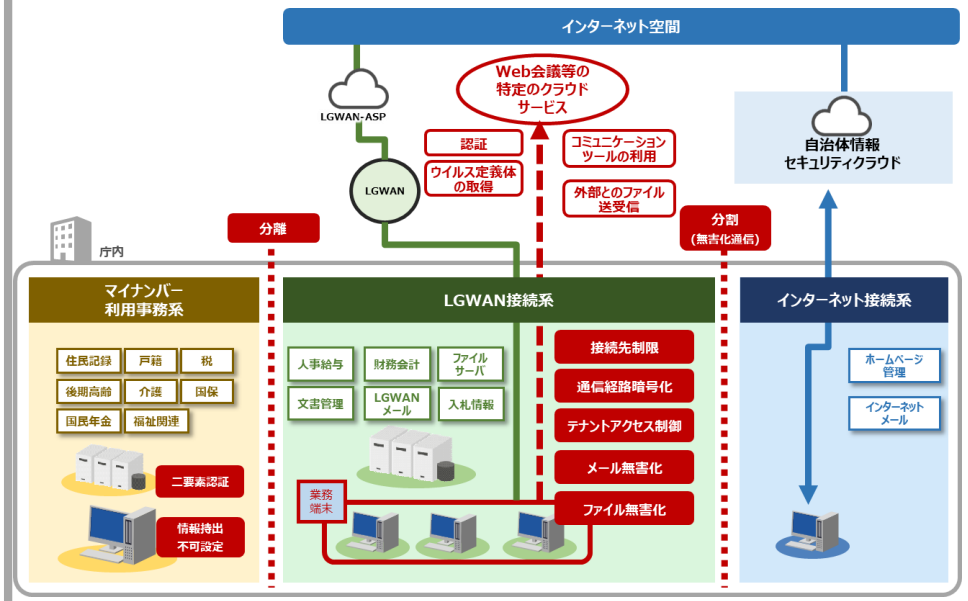
ガイドライン改定案（見え消し）⑦

改定案：対策基準（解説）

対策区分	セキュリティ対策	概要
技術的対策	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。
	接続先制限	・LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。
	ローカルブレイクアウトテナントアクセス制御	・利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する。
	メール無害化/ファイル無害化	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネットからファイルを取り込む。 ※詳細は、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(２)LGWAN接続系①LGWAN接続系とインターネット接続系の分割を参照。
	権限管理	・不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。
	アクセス制御	・不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う。LGWAN端末、LGWAN業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。
	IDS/IPS	・ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。
	DDoS対策	・サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。くす
	通信路暗号化	・通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。
組織的・人的対策	手続・規定	・クラウドサービスを利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底しなければならない。
	組織・人的な対応	以下の組織的・人的対策に加え、本ガイドラインの「５.人的セキュリティ」記載の組織的・人的対策を確実に実施する。 ・職員等が毎年度最低１回は情報セキュリティ研修を受講可能となる研修計画の策定 ・職員等の実践的サイバー防御演習（CYDER）の受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し

図表30　α’モデル（コミュニケーションツールを利用し、外部とファイル送受信を行う場合）における必須のセキュリティ対策について

α’モデル（コミュニケーションツールを利用し、外部とファイル送受信を行う場合）については、以下の対策も有効である。
・システムに対するDDoS攻撃発生時の継続稼働を保証するため、あるいは障害状態からの早期回復を実現するための、構成要素の冗長化
・クラウドサービス上でのマルウェア対策
・未知の不正プログラムへの対策（エンドポイント対策）

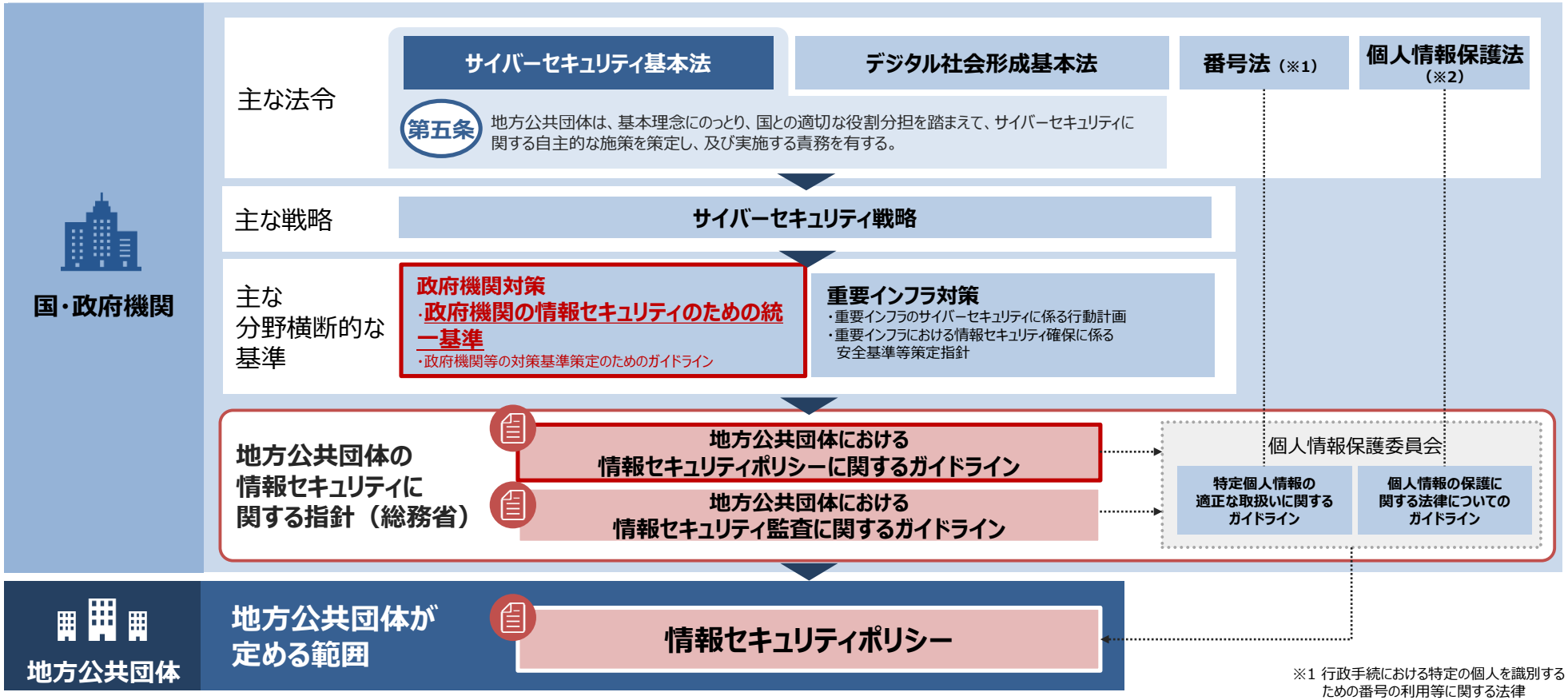


図表30 α’モデル（コミュニケーションツールを利用し、外部とファイル送受信を行う場合）イメージ図
※セキュリティ対策の性質に着目し、セキュリティ対策を講じる場所を抽象化して表記している。
また、すべての対策を網羅していないため、厳密な図とはなっていない。

NISC政府統一基準（令和５年度）の改定に係る対応について

NISC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、NISCの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

令和5年度における政府統一基準群の見直しについて

✓ 改定ポイントは大きく以下の５つ。

１．情報セキュリティに関するサプライチェーン対策の強化

- 業務委託における政府の情報を保護するため、米国NISTのサプライチェーン対策を参考に、情報へのアクセス制御、ログの取得・監視などの委託先に担保させるべき情報セキュリティ対策を契約に含めるとともに、委託期間を通じた実施を求める。

２．クラウドサービスの利用拡大を踏まえた対策の強化

- 独立行政法人等へのISMAP拡大や、ISMAP-LIU運用開始等を踏まえ、要機密情報を取り扱う場合のクラウドサービスはISMAPクラウドサービスリストから選定することを明記する。
- 要機密情報を取り扱わない場合においても、適切な主体認証やアクセス制御の管理などのクラウドサービスを安全に利用するための対策を講ずる。また、調達行為を伴わないクラウドサービスを利用する場合には、「調達行為を伴わないSNS等の外部サービスの利用等に関する申合せ」に基づき、講ずべき措置についてNISCに助言を求める。

３．ソフトウェア利用時の対策の強化

- 機器等調達時のIT調達申し合わせに基づく対応を必須のものとして明記する。また、重要なソフトウェアについて、設定手順の整備、設定の定期的な確認、教育の実施など、運用時の情報セキュリティ水準を維持するための対策を講ずる。
- 従来の対策に加え、サーバ装置や端末等の運用開始時において、脆弱性診断の実施などソフトウェアの脆弱性対策を強化する。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

- サイバー攻撃を受けることを念頭においた情報システムの防御に係る対策や情報システムの復旧のための対策を講ずる。
- 昨今のサービス不能攻撃（DDoS攻撃）を踏まえ、専用の対策装置やサービスの導入、サーバ装置や通信回線等の冗長化などの対策や、サービス不能攻撃を受けることを想定した監視方針の策定や脅威情報の収集等の対策を講ずる。
- クラウドサービスの利用の拡大に対応するため、常時診断・対応型セキュリティアーキテクチャを実装することを念頭に、情報資産等へのアクセスを常時診断・検証して、アクセスを許可又は拒否する新たな技術的手法を講じる際に必要な対策を規定（※）。 ※ゼロトラストアーキテクチャに該当。

５．組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

- 監査等から得られた組織横断的に改善が必要な事項について、進捗状況を定期的にCISOに報告し、CISOは監査結果に基づく改善進捗を把握・組織の統制を図る。
- 所管独法等の情報セキュリティ対策を支援するため、府省庁側に必要な体制を整備する。独法等は専門的知見を要する事項等について所管省庁等へ助言を求める。
- 情報システムの重要度より高度な対策情報システムの重要度の考え方を導入。全ての情報システムに求める必須の対策に加えて、基幹業務システムなどより重要度の高い情報システムについては、リアルタイムにログ分析を行う機能の導入などの高度な対策を求める。

１．情報セキュリティに関するサプライチェーン対策の強化

１．情報セキュリティに関するサプライチェーン対策の強化

1　業務委託に関し、委託先に実施を求める対策を具体化

政府統一基準群の主な改定内容

✓ 業務委託における政府の情報を保護するため、米国NISTのサプライチェーン対策を参考に、情報へのアクセス制御、ログの取得・監視などの委託先に担保させるべき情報セキュリティ対策（※）を契約に含めることを求める。

（※）NISTのSP800-171を参考に、以下の８類型の対策を規定
①インシデント等への対処能力の確立・維持、②アクセス主体の識別とアクセス制御、③ログの取得・監視、④機器等の物理的保護、
⑤要員への周知と統制、⑥資産管理・リスク評価、⑦システムの完全性の保護、⑧セキュリティ対策の検証・評価・見直し

ガイドライン改定の方向性

➢ 委託先に提供した情報が適切に保護されるよう、業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定する。

業務委託に係る規定の整備 → 業務委託実施前の対策 → 業務委託実施期間中の対策 → 業務委託終了時の対策

１．情報セキュリティに関するサプライチェーン対策の強化

➢ 委託先に提供した情報が適切に保護されるよう、**業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定**

業務委託に係る規定の整備 ＞ 業務委託実施前の対策 ＞ 業務委託実施期間中の対策 ＞ 業務委託終了時の対策

政府統一基準

4.1.1 業務委託

【例文】　（赤字が改定部分）

(1)　業務委託に係る運用規程の整備

(a)統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備すること。

(ア)委託先への提供を認める情報及び委託する業務の範囲を判断する基準（以下本款において「委託判断基準」という。）

(イ)委託先の選定基準

(2)　業務委託実施前の対策

（新設）

(a)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、以下を全て含む事項を実施すること。

(ア)委託する業務内容の特定

(イ)委託先の選定条件を含む仕様の策定

(ウ)仕様に基づく委託先の選定

(エ)契約の締結

(オ)委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

（新設）

(b)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託先に求めること。

(ア)仕様に準拠した提案

(イ)契約の締結

(ウ)委託先において要機密情報を取り扱う場合は、秘密保持契約（NDA）の締結

改定案：対策基準(例文)

8.1.業務委託

【例文】

(1)　業務委託に係る運用規程の整備

統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。

①委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

②委託事業者の選定基準

(2)　業務委託実施前の対策

①情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

（ア）委託する業務内容の特定

（イ）委託事業者の選定条件を含む仕様の策定

（ウ）仕様に基づく委託事業者の選定

（エ）情報セキュリティ要件を明記した契約の締結（契約項目）

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。

（略）

（オ）委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

②情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

（ア）仕様に準拠した提案

（イ）契約の締結

（ウ）委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結　（続く）

１．情報セキュリティに関するサプライチェーン対策の強化

➢ 委託先に提供した情報が適切に保護されるよう、**業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定**

業務委託に係る規定の整備 | 業務委託実施前の対策 | 業務委託実施期間中の対策 | 業務委託終了時の対策

政府統一基準

4.1.1 業務委託
【例文】
（続き）
（新設）
(3) 業務委託実施期間中の対策
(a)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策を実施すること。
(ア)委託判断基準に従った要保護情報の提供
(イ)契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認
(ウ)委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

(b)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策の実施を委託先に求めること。
(ア)情報の適正な取扱いのための情報セキュリティ対策
(イ)契約に基づき委託先が実施する情報セキュリティ対策の履行状況の定期的な報告
(ウ)委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処。
（続く）

改定案：対策基準(例文)

8.1. 業務委託
【例文】
（続き）

（３） 業務委託実施期間中の対策
①情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。
（ア）委託判断基準に従った重要情報の提供
（イ）契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
（ウ）統括情報セキュリティ責任者へ措置内容の報告（重要度に応じてCISOに報告）
（エ）委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

②情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。
（ア）情報の適正な取扱いのための情報セキュリティ対策
（イ）契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
（ウ）委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処
（続く）

１．情報セキュリティに関するサプライチェーン対策の強化

➢ 委託先に提供した情報が適切に保護されるよう、**業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定**

業務委託に係る規定の整備 → 業務委託実施前の対策 → 業務委託実施期間中の対策 → **業務委託終了時の対策**

政府統一基準

（新設）

4.1. 業務委託
4.1.1 業務委託

(4) 業務委託終了時の対策
(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の終了に際して以下を全て含む対策を実施すること。
(ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
(イ) 委託先に提供した情報を含め、委託先において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認
(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、業務委託の終了に際して以下を全て含む対策の実施を委託先に求めること。
(ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
(イ) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

改定案：対策基準(例文)

8.1. 業務委託
【例文】

（４） 業務委託終了時の対策
①情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。
（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
（イ）委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認
②情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。
（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
（イ）提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

2 外部委託に関する分類の見直し

政府統一基準群の主な改定内容

✓ 「業務委託」から「情報システムに関する業務委託」を切り出し、必要な対策を上乗せで規定する。
✓ 従来の「外部サービス」を「クラウドサービス」、「機関等向けに情報システムの一部の機能を提供するサービス※」に分離し、ISMAP原則利用の考え方に基づいた対策へと改定する。 ※業務委託に分類される。

<改定前の分類>

4.1 業務委託

4.2 外部サービス
4.2.1 要機密情報を取り扱う場合
4.2.2 要機密情報を取り扱わない場合

●外部サービスの例
クラウドサービス、Web会議サービス、検索サービス、翻訳サービス、地図サービス、SNS

ホスティングサービス、インターネット回線接続サービス

<改定後の分類>

4.1.1 業務委託 ※全ての「業務委託」に適用

4.1.2 情報システムに関する業務委託 ※「情報システムに関する業務委託」について上乗せで適用
(1) 共通的対策
(2) 構築の場合の対策
(3) 運用・保守の場合の対策
(4)機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

●情報システムに関する業務委託の例
情報システムの開発及び構築業務、
アプリケーション・コンテンツの開発業務、
情報システムの運用業務

4.2 クラウドサービス ※ISMAP原則利用
4.2.1、4.2.2 要機密情報を取り扱う場合
4.2.3 要機密情報を取り扱わない場合

●**クラウドサービスの例**
仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）、
データベースや開発フレームワーク等のミドルウェア等提供サービ（PaaS）、
Web会議サービス、ソーシャルメディア、検索サービス、翻訳サービス、地図サービス

１．情報セキュリティに関するサプライチェーン対策の強化

ガイドライン改定の方向性

- **業務委託は「業務委託」と「情報システムに関する業務委託」に区分して記載**

業務委託の中に情報システムに関す業務委託や情報システムの一部の機能を提供するサービスとの関係性を明確にする。

政府統一基準

4.1.1 業務委託

「業務委託」とは、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ことをいう。「委託」「準委任」「請負」といった契約形態を問わず、全てを含むものとする。
ただし、当該業務において機関等の情報を取り扱わせる場合に限る。

（例）
- **業務運用支援業務（統計、集計、データ入力、媒体変換等）の委託**
- **プロジェクト管理支援業務の委託**
- **調査・研究業務（調査、研究、検査等）の委託**

4.1.2 情報システムに関する業務委託

（例）
- **情報システムの開発及び構築業務の委託**
- **アプリケーション・コンテンツの開発業務の委託**
- **情報システムの運用業務の委託**
- ウェブサイトの運用業務の委託
- 機関等内でのみ利用される共通基盤システム（情報システムのリソースやソフトウェアの一部又は全部を共有する基盤を提供する情報システム）の運用業務（ホスティング型プライベートクラウド）

4.1.2(4)機関等向けに情報システムの一部の機能を提供するサービス

（例）
- ホスティングサービス
- インターネット回線接続サービス

改定案：対策基準(趣旨)

8.1. 業務委託

「業務委託」とは、本市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ことをいう。「委託」「準委任」「請負」といった契約形態を問わず、全てを含むものとする。
ただし、当該業務において本市の情報を取り扱わせる場合に限る。

（例）
- **業務運用支援業務（統計、集計、データ入力、媒体変換等）の委託**
- **プロジェクト管理支援業務の委託**
- **調査・研究業務（調査、研究、検査等）の委託**

8.2. 情報システムに関する業務委託

（例）
- **情報システムの開発及び構築業務の委託**
- **アプリケーション・コンテンツの開発業務の委託**
- **情報システムの運用業務の委託**
- ウェブサイトの運用業務の委託
- 本市内でのみ利用される共通基盤システム（情報システムのリソースやソフトウェアの一部又は全部を共有する基盤を提供する情報システム）の運用業務（ホスティング型プライベートクラウド）

8.2.(4)本市向けに情報システムの一部の機能を提供するサービス

（例）
- ホスティングサービス
- インターネット回線接続サービス

１．情報セキュリティに関するサプライチェーン対策の強化

➢ **業務委託は「業務委託」と「情報システムに関する業務委託」に区分して記載**

政府統一基準

（新設）

4.1.2 情報システムに関する業務委託
【遵守事項】

(1) 情報システムに関する業務委託における共通的対策
(a)情報システムセキュリティ責任者は、情報システムに関する業務委託の実施までに、委託先の選定条件に情報システムに機関等の意図せざる変更が加えられないための対策に係る選定条件を加え、仕様を策定すること。
(2) 情報システムの構築を業務委託する場合の対策
(a)情報システムセキュリティ責任者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託先に求めること。
(ア)情報システムのセキュリティ要件の適切な実装
(イ)情報セキュリティの観点に基づく試験の実施
(ウ)情報システムの開発環境及び開発工程における情報セキュリティ対策
(3) 情報システムの運用・保守を業務委託する場合の対策
(a)情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託先に実施を求めること。
(b) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めること。
（続く）

改定案：対策基準(例文)

8.2. 情報システムに関する業務委託
【例文】

（１） 情報システムに関する業務委託における共通的対策
情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。
（２） 情報システムの構築を業務委託する場合の対策
情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。
①情報システムのセキュリティ要件の適切な実装
②情報セキュリティの観点に基づく試験の実施
③情報システムの開発環境及び開発工程における情報セキュリティ対策
（３） 情報システムの運用・保守を業務委託する場合の対策
①情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。
②情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めなければならない。
（続く）

２．クラウドサービスの利用拡大を踏まえた対策の強化

２．クラウドサービスの利用拡大を踏まえた対策の強化

政府統一基準群の主な改定内容

- ✓ 独立行政法人等へのISMAP拡大や、ISMAP-LIU運用開始等を踏まえ、要機密情報を取り扱う場合のクラウドサービスはISMAPクラウドサービスリストから選定することを明記。
  （調達したい機能を有したクラウドサービスが登録されていない場合など、やむを得ずISMAPクラウドサービスリスト以外から選定する場合は、CISOの責任において、ISMAP制度で求めている要求事項や管理基準を満たしていることを確認）
- ✓ 要機密情報を取り扱わない場合においても、適切な主体認証やアクセス制御の管理などのクラウドサービスを安全に利用するための対策を講ずる。また、調達行為を伴わないクラウドサービスを利用する場合には、「調達行為を伴わないSNS等の外部サービスの利用等に関する申合せ」に基づき、講ずべき措置についてNISCに助言を求める。

ISMAP-LIUについて

ISMAPが対象とするクラウドサービスのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるSaaSサービスに対する仕組みであり、また情報システムの調達においては、業務・情報の影響度に応じたセキュリティを確保すべきとの考え方から、影響度が低いと評価される業務、情報に用いられるSaaSを対象とする制度として趣旨が広く理解されるよう、名称は、ISMAP for Low-Impact Use（通称：ISMAP-LIU） とする。

※出典：『ISMAP-LIUについて』（令和４年１１月１日 NISC、デジタル庁、総務省、経済産業省）

外部委託に関する分類の見直し

政府統一基準群の主な改定内容

- ✓ クラウドサービスに一般的なSaaSが含まれることを用語定義において明記し、従来の「外部サービス」を「クラウドサービス」、「機関等向けに情報システムの一部の機能を提供するサービス※」に分離し、ISMAP原則利用の考え方に基づいた対策へと改定する。
- ✓ 「機器等の調達」に関する規定を集約して記載する。

<改定前の分類>

4.1 業務委託

4.2 外部サービス

4.2.1 要機密情報を取り扱う場合

4.2.2 要機密情報を取り扱わない場合

●外部サービスの例

クラウドサービス、Web会議サービス、検索サービス、翻訳サービス、地図サービス、SNS

ホスティングサービス、インターネット回線接続サービス

<改定後の分類>

4.1.1 業務委託 ※全ての「業務委託」に適用

4.1.2 情報システムに関する業務委託 ※「情報システムに関する業務委託」について上乗せで適用

(1) 共通的対策
(2) 構築の場合の対策
(3) 運用・保守の場合の対策
(4)機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

●情報システムに関する業務委託の例
情報システムの開発及び構築業務、
アプリケーション・コンテンツの開発業務、
情報システムの運用業務

4.2 クラウドサービス ※ISMAP原則利用

4.2.1、4.2.2 要機密情報を取り扱う場合

4.2.3 要機密情報を取り扱わない場合

●**クラウドサービスの例**
仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）、
データベースや開発フレームワーク等のミドルウェア等提供サービ（PaaS）、
Web会議サービス、ソーシャルメディア、検索サービス、翻訳サービス、地図サービス

4.3 機器等の調達 ※サプライチェーン・リスク対応の明確化

●機器の例
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

政府統一基準における「クラウドサービス」の定義 ※下線部が改定により追加
「クラウドサービス」とは、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をいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、統一基準におけるクラウドサービスは、機関等外の一般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クラウドサービスであって、当該サービスにおいて機関等の情報が取り扱われる場合に限るものとする。

2．クラウドサービスの利用拡大を踏まえた対策の強化

➢ 統一基準の遵守事項で「セキュリティ要件を策定」となっている部分については、現行のガイドラインのまま、内容を具体的に記載。

政府統一基準

4.2.2 クラウドサービスの利用（要機密情報を取り扱う場合）
遵守事項

(1) クラウドサービスの利用に係る運用規程の整備
(a)統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備すること。
(b) 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備すること。
（略）
(2) クラウドサービスの利用に係るセキュリティ要件の策定
（略）
(b) クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係るセキュリティ要件を策定すること。

(3) クラウドサービスを利用した情報システムの導入・構築時の対策
(c) クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備すること。
(ア)クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
（略）
(4) クラウドサービスを利用した情報システムの運用・保守時の対策
(a) クラウドサービス管理者は、(1)(b)で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施すること。また、運用・保守時に実施状況を定期的に確認・記録すること。
（略）

セキュリティ要件について、アクセス制御、暗号化等については現行のガイドラインのまま具体的に記載（統一基準では「基本対策事項」に記載）

改定案：対策基準(例文)

8.3.外部サービス(クラウドサービス)の利用（機密性２以上の情報を取り扱う場合）

全ての文言を外部サービス(クラウドサービス）に変更すると読みにくくなるため、以下「クラウドサービス」とする。

【例文】
（２）クラウドサービスの利用に係る運用規程の整備
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
②統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
（略）
（６） クラウドサービスを利用した情報システムの導入・構築時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。
（ア）不正なアクセスを防止するためのアクセス制御
（イ）取り扱う情報の機密性保護のための暗号化
（略）
③クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。
（ア）クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
（略）
（７） クラウドサービスを利用した情報システムの運用・保守時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。
（略）
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化

２．クラウドサービスの利用拡大を踏まえた対策の強化

ガイドライン改定の方向性

- **なお、「第４編　地方公共団体におけるクラウド利用等に関する特則」におけるクラウドサービスは、情報システムの標準化に伴うガバメントクラウド利用を念頭においた記載であることを明確にする。**

現行：第４編

第Ⅰ章 本編の目的について

（略）

このような状況を踏まえ、今後、地方公共団体においては、ガバメントクラウドの利用を中心として、マイナンバー利用事務系の標準準拠システム等のクラウドサービスの利用が浸透することが想定されるため、本編においては、クラウドサービス上で標準準拠システム・関連システム等の業務システム（以下「標準準拠システム等」という。）を整備及び運用する場合の考え方とその対策基準を示す。

対策基準の内容については、クラウドサービスの特性を踏まえた情報セキュリティ対策を考慮する必要があることから、「クラウドサービスの利用に関する情報セキュリティの国際規格（JIS Q 27017：JIS Q27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）」の内容を参考にしている。

地方公共団体においては、クラウドサービス上での標準準拠システム等の整備及び運用を開始するまでに、本編に示された対策基準（例文及び解説）の内容を参考にセキュリティポリシーの見直しを行う必要がある。

ガイドラインの記載事項とガバメントクラウドに関する対応については、デジタル庁が示すガバメントクラウドに関するドキュメント類の記載内容等を踏まえ、本ガイドラインの補足資料として、本編の対策基準との対応表を掲載し、適時更新を行う。

現行の第４編は、左記マーカー部分で示す通り、**標準準拠システムをガバメントクラウド上で利用することを念頭においた本編の対策基準が記載されている**ため、改定しないこととする。

２．クラウドサービスの利用拡大を踏まえた対策の強化

ガイドライン改定の方向性

- ISMAPについては、登録事業者側の費用負担増加に伴いサービス継続が困難となる可能性等を鑑み、引き続き、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つとする
- ISMAP-LIUについては、**対象とする範囲が限定的**なことに加え、利用する団体（地方公共団体）自身による影響度評価の実施など、地方公共団体側に負担が伴う可能性があることから、ISMAP同様、参考とすべき認証の１つと位置付ける

政府統一基準

4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）

【解説】
（2）クラウドサービスの選定
クラウドサービスの選定においては、原則としてISMAP 等クラウドサービスリストから選定する必要がある。やむを得ずISMAP 等クラウドサービスリスト以外のクラウドサービスを選定する場合は、ISMAP の原則利用の考え方に基づき、最高情報セキュリティ責任者の責任において、ISMAP 制度で求めている要求事項や管理基準を満たしていることを確認する必要がある。

改定案：対策基準(解説)

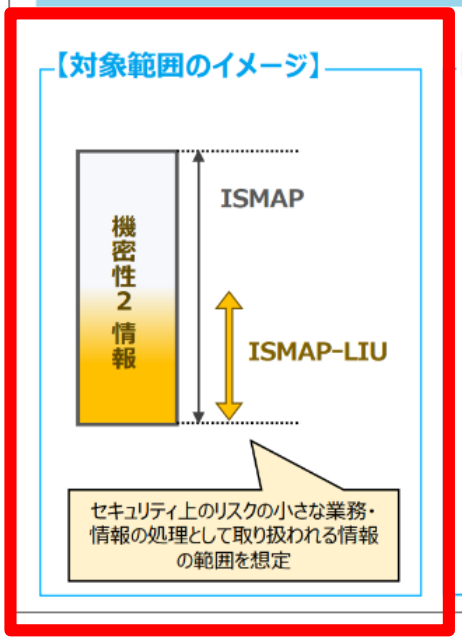
8.3.外部サービス(クラウドサービス)の利用（機密性２以上の情報を取り扱う場合）
【解説】
（３）クラウドサービスの選定
⑦情報セキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。
（略）
このような評価に当たって、クラウドサービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。
なお、選定条件となる認証には、ISO/IEC27017に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、ISMAP又はISMAP-LIUの管理基準を満たすことの確認やISMAP又はISMAP-LIUクラウドサービスリスト等のほか、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クラウドサービス提供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）を活用することを推奨する。クラウドサービス利用時のセキュリティ対策や内部統制に関する報告書等については、以下を参照されたい。
（続く）

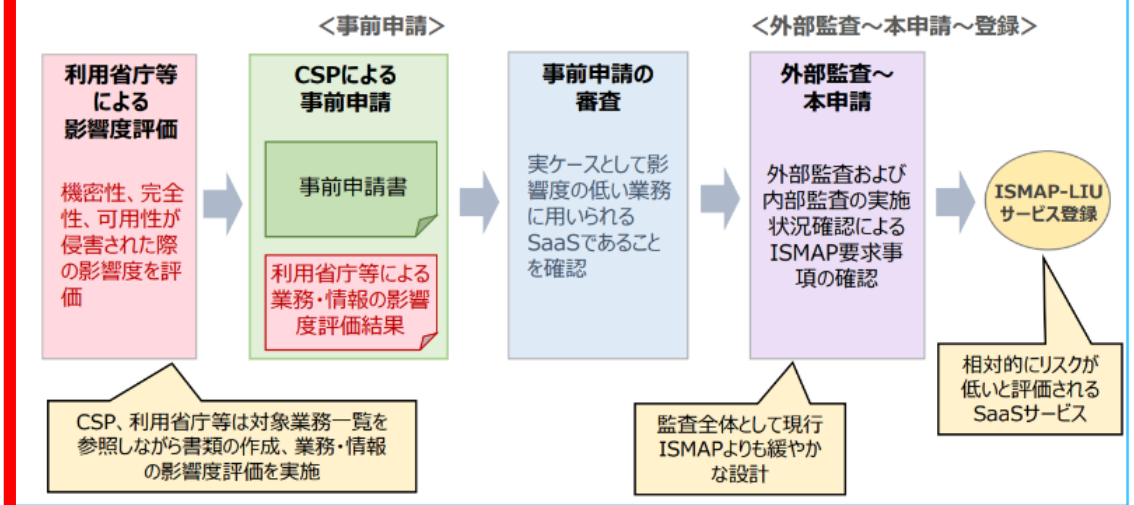
（参考）ISMAP-LIUについて

✓ **ISMAP-LIUの対象は、セキュリティ上のリスクの小さな業務・情報処理**とされており、ISMAPの代わりにはなり得ない。

ISMAP-LIUの基本的な仕組み・登録までの流れ

- ISMAP-LIUの対象は、SaaSの中でもセキュリティ上のリスクの小さな業務・情報の処理に用いるもの。
- ISMAP-LIU該当性の判断に当たっては、**利用する各省庁における業務・情報の影響度※評価の提出を必須とし、実ケースとして影響度の低い業務に用いられるSaaSであることを確認。**
  ※業務・情報の影響度は、クラウドサービスで取り扱われ処理される各種情報において、機密性・完全性・可用性が損なわれた場合の影響度を示す。
- その際、CSP、各省庁による効率的な申請・業務・情報の影響度評価を促すため、**ISMAP-LIUにおける業務・情報の影響度が低位である蓋然性が高い業務（対象業務一覧）を提示。**





※出典：『ISMAP-LIUについて』（令和４年１１月１日　NISC、デジタル庁、総務省、経済産業省）

３．機器・ソフトウェアの利用時の対策の強化

3．機器・ソフトウェア利用時の対策の強化

政府統一基準群の主な改定内容

- ✓ サプライチェーンリスクの明確化のため、「機器等の調達」に関する規定を集約して記載する。
- ✓ 機器等調達時のIT調達申し合わせに基づく対応を必須のものとして明記。また、重要なソフトウェア(※)について、設定手順の整備、設定の定期的な確認、教育の実施など、運用時の情報セキュリティ水準を維持するための対策を講ずる。
  （※）端末やサーバ装置の制御、統合的な主体認証管理、資産管理、ネットワーク監視など、情報システムを制御する上でセキュリティ上の重要な機能を有しているソフトウエアをいう
- ✓ 従来の対策に加え、サーバ装置や端末等の運用開始時において、脆弱性診断の実施などソフトウェアの脆弱性対策を強化する。

4.3 機器等の調達

●用語の定義
用語定義：「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。

＜情報システムの基盤を管理又は制御するソフトウェアの例＞
・端末やサーバ装置、通信回線装置等を制御するソフトウェア
・統合的な主体認証を管理するソフトウェア
・ネットワークを制御・管理するソフトウェア
・資産を管理するソフトウェア
・監視に関連するソフトウェア
・情報システムのセキュリティ機能として使用するソフトウェア

6.5.1 情報システムの基盤を管理又は制御するソフトウェア

●ソフトウェア導入時の対策
ソフトウェア自体を保護するための措置を講ずること、ソフトウェアの情報セキュリティ水準の維持に関する手順の整備、ソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順の整備

●ソフトウェア運用時の対策
ソフトウェアのセキュリティを維持するための対策、脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

権限設定やアクセス制御、セキュリティ設定が適切であるか定期的な確認（脆弱性対策）

3．機器・ソフトウェア利用時の対策の強化

ガイドライン改定の方向性

➢ 機器及びソフトウェアの調達においては、それらの選定基準の一つとして、情報システムの開発時のみならず、運用開始後も不正な変更が加えられない管理がなされ、その管理を地方公共団体が確認できるよう記載を見直す。

政府統一基準

（新設）

4.3. 機器等の調達
4.3.1 機器等の調達
遵守事項

(1)機器等の調達に係る運用規程の整備
(a)統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機関等が確認できることを加えること。
(b)統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

改定案：対策基準(例文)

（新設）

6.3. システム開発、導入、保守等
【例文】

（1） 機器等の調達に係る運用規程の整備
①統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。
②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、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。
（2） 機器等及び情報システムの調達
（略）

「機器等の選定基準」、「必要に応じて」、「不正な変更が加えられないような対策」を具体的に示すため【解説】に説明を追加する。

- 選定基準としては、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が考えられる。
- 取り扱う情報の分類及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮し、その適用要否を判断した上で、選定基準を整備。
- 不正な変更が行われないような対策としては、機器等の製造工程における不正行為の有無について、**定期的な監査**を行っていること、機器等の**製造環境にアクセス可能な従業員が適切に制限され、定期点検が行われている**こと、**各製造工程の履歴が記録されている**などの厳格な管理されていることが考えられる。

3．機器･ソフトウェア利用時の対策の強化

ガイドライン改定の方向性

- 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おける脆弱性対策の状況を、定期的及び適時に確認することを記載する。

→ アプリケーション･コンテンツの開発時の対策についても記載。

政府統一基準

（新設）

6.6.1 アプリケーション・コンテンツの作成・運用時の対策
【遵守事項】

(3)アプリケーション・コンテンツの開発時の対策

(α)情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。

改定案：対策基準(例文)

6.3. システム開発、導入、保守等
【例文】

（３）情報システムの開発

④アプリケーション・コンテンツの開発時の対策
情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

【解説】に脆弱性の排除や脆弱性診断についての説明を追加する。

- **脆弱性を排除したウェブアプリケーションを実装する方法**の詳細については、**独立行政法人情報処理推進機構（IPA）による「安全なウェブサイトの作り方」やOWASPのASVS（Application Security Verification Standard：アプリケーションセキュリティ検証標準）を参照**することも考えられる。
- **開発者の気付かない脆弱性が存在してしまう可能性があるため、脆弱性対策の状況を確認するために脆弱性診断を行う**ことが考えられる。
- 脆弱性診断には、ソースコード診断、ウェブアプリケーション診断等の種類があり、必要に応じて脆弱性診断を使い分けて実施する必要がある。

3．機器･ソフトウェア利用時の対策の強化

- 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おける脆弱性対策の状況を、定期的及び適時に確認することを記載する。

政府統一基準

（新設）
6.5.1 情報システムの基盤を管理又は制御するソフトウェア
【遵守事項】

(2) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策
(a) 情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施すること。
(ア) 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策
(イ) 脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

6.2.1 サーバ装置
【遵守事項】
(2) サーバ装置の運用時の対策
(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行うこと。

改定案：対策基準(例文)

6.3. システム開発、導入、保守等
【例文】

（６） 情報システムの基盤を管理又は制御するソフトウェア運用時の対策
①情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施しなければならない。【推奨事項】
（ア）情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策
（イ）脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

追加のツール等を導入して、端末やサーバ等を保護する必要があり、財政面での負担が発生するため推奨事項とする。

②情報システム管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

3． 機器･ソフトウェア利用時の対策の強化

➢ 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おける脆弱性対策の状況を、定期的及び適時に確認することを記載する。

政府統一基準

6.1　端末
6.1.1 端末
遵守事項
(1) 端末の導入時の対策

(e) 情報システムセキュリティ責任者は、端末において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。（新設）

6.2　サーバ装置
6.2.1 サーバ装置
遵守事項
(1) サーバ装置の導入時の対策

(f) 情報システムセキュリティ責任者は、サーバ装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。（新設）

6.4　通信回線
6.4.2　通信回線装置
遵守事項
(1) 通信回線装置の導入時の対策

(d)情報システムセキュリティ責任者は、通信回線装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。（新設）

改定案：対策基準(例文)

6.6. システム開発、導入、保守等
【例文】

(1)　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等
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、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

統一基準で追記された「公開された脆弱性への対応」については、現行ガイドラインで既に記載されているため、サーバ装置、端末及び通信回線装置等の対象を追加するに留める。

＜該当箇所＞
6.6.
（1）セキュリティホールに関する情報の収集･共有及びソフトウェアの更新等
（2）不正プログラム等のセキュリティ情報の収集･周知
（3）情報セキュリティに関する情報の収集及び共有

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

1 サイバー攻撃を受けることを念頭においた情報システムの防御・復旧やバックアップに係る対策の強化

政府統一基準群の主な改定内容

✓ サイバー攻撃を受けることを念頭においた情報システムの防御に係る対策や情報システムの復旧のための対策を講ずる。
（情報システムへの監視機能やクラウドサービスの管理者権限を有する主体などの厳格な主体認証が必要な場合における多要素主体認証の導入、情報セキュリティインシデント発生に備えた情報システムの復旧手順の整備や適切なバックアップの取得、バックアップ要件・復旧手順の見直しなど）

現行ガイドラインにおける「情報システムの防御・復旧に係る対策」の記載

第２編　例文　第２章

6.1.　コンピュータ及びネットワークの管理

（２）バックアップの実施

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、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

6.2. アクセス制御等

（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、システム上制限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。

7.3.　侵害時の対応等

（１）緊急時対応計画の策定

CISO 又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、地方公共団体の導入費用等も考慮しながら記載を見直す。

→ サーバ装置と通信回線装置について記載。

政府統一基準

6.2.1 サーバ装置
【遵守事項】
(1) サーバ装置の導入時の対策

(g) 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得すること。（新設）

6.4.2 通信回線装置
【遵守事項】
(2) 通信回線装置の運用時の対策

(b) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。（新設）

改定案：対策基準(例文)

6.1. コンピュータ及びネットワークの管理
【例文】

(2)バックアップの実施
①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、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。
②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、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。
③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、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

【解説】にバックアップについての説明を追加。
- 許容される停止時間等を踏まえる。
- OS やアプリケーションなどを含むサーバ装置全体をバックアップする方法やサーバ装置の複製をバックアップとして用意しておく方法などが存在する。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、地方公共団体の導入費用等も考慮し記載を見直す。

→ 権限の管理に関し、アクセス制限について追記。

政府統一基準

7.1.3 権限の管理
【遵守事項】

(1)権限の管理
(a)情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を必要最小限の範囲で適切に設定するよう、措置を講ずること。
(略)
(c)情報システムセキュリティ責任者は、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すること。
（続く）

（赤字が改定部分）

「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」について、以下を【解説】に記載。

- 特に管理者権限を付与した主体については、管理者権限の付与が不要になった時点で権限を変更するなどの対策を実施する必要がある。
- 保守やメンテナンスなどを実施するため、特定の主体に対して一時的に付与した権限については、必要な作業等が終了したら確実に権限の付与を削除する必要がある。

改定案：対策基準(例文)

6.2. アクセス制御
【例文】

（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。
（続く）

2 サービス不能攻撃

政府統一基準群の主な改定内容

✓ 昨今のサービス不能攻撃(DDoS攻撃)を踏まえ、専用の対策装置やサービスの導入、サーバ装置や通信回線等の冗長化などの対策や、サービス不能攻撃を受けることを想定した監視方針の策定や脅威情報の収集等の対策を講ずる。

現行ガイドラインにおける「サービス不能攻撃（DDoS攻撃）に対する対策」の記載

✓ ガイドラインが対象とする脅威に含まれており、情報セキュリティ対策基準の解説にて、情報システムの可用性確保の対策として、情報システムを構成する機器の装備している機能による対策の実施等が例示されている。また、都道府県情報セキュリティクラウドの標準要件において、DDoS攻撃を想定した機能について記載している。

第２編　例文　第２章

6.5.　不正アクセス対策

（６）サービス不能攻撃

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、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

次期自治体情報セキュリティクラウド要件シート（令和２年８月１８日「次期自治体情報セキュリティクラウドの標準要件について」）

対策手段	要件概要・目的	要件補足事項及び推奨事項
CDN	住民への継続的な情報発信のために、Webサイトを公開するWebサーバの負荷分散をする	・DDoS対策機能、WAF機能をオプションとして用意されていることが望ましい

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、現行の自治体情報セキュリティクラウドとの関係性を踏まえながら、地方公共団体の導入費用等も考慮し記載を見直す。

→ ネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施する旨を記載。

政府統一基準

6.4.2 通信回線装置
【遵守事項】

(ｉ)通信回線装置の導入時の対策

(ｃ)情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施すること。（新設）

改定案：対策基準(例文)

4.3.　通信回線及び通信回線装置の管理
【例文】

①統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。
②統括情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。
③～⑤　（略）

「適切なセキュリティ対策を実施」の内容について、以下を【解説】に記載。

・ インターネット等の外部ネットワークを接続する場合は、**不正アクセス等のリスクを低減するためのネットワーク構成**等を構築する必要がある。
・ 通信回線装置を設定する際は、当該通信回線装置を提供している提供者が提示している**推奨設定や業界標準、ベストプラクティス等を参照し、通信回線装置の各種設定を行い、設定の不備等がないようにする**必要がある。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、地方公共団体の導入費用等も考慮し記載を見直す。

→ 通信回線装置が動作するために必要なソフトウェアに関する事項ついて記載。

政府統一基準

6.4.1 通信回線
【遵守事項】
(２)機関等外通信回線の接続時の対策
(b) 情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間及び機関等内通信回線内の不正な通信の有無を監視するための措置を講ずること。

6.4.2 通信回線装置
【遵守事項】
(１)通信回線装置の導入時の対策
(ｂ) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めること。
(2) 通信回線装置の運用時の対策
(c) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講ずること。

（赤字が改定部分）

改定案：対策基準(例文)

4.3.　通信回線及び通信回線装置の管理
【例文】
（続き）
⑥統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。
⑦統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。
⑧統括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

通信回線装置が動作するために必要な「ソフトウェアに関する事項」を具体的に示すため、以下のような説明を【解説】に追加。

- 通信回線装置で使用するソフトウェアについて、バージョンを含めて定めておくことが望ましい。
- 通信回線装置の更新ソフトウェアの提供を受けた際は、修正された脆弱性についての影響度と緊急度を判断し、影響度や緊急度に応じて更新ソフトウェアを適用するまでの時間をできるだけ短くするなどの対策を検討する必要がある。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、現行の自治体情報セキュリティクラウドとの関係性を踏まえながら、地方公共団体の導入費用等も考慮し記載を見直す。

→ 監視を含むセキュリティ機能について記載。

政府統一基準

（新設）

5.2.3. 情報システムの運用・保守

【遵守事項】

(l) 情報システムの運用・保守時の対策

(a) 情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用すること。

(d) 情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

(e) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をすること

改定案：対策基準(例文)

7.1. 情報システムの監視

【例文】

(１) 情報システムの運用・保守時の対策

①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、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

②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、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

③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、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

「監視を含むセキュリティ機能」の例として、以下を【解説】に記載。

- 主体認証機能
- アクセス制御機能
- 権限の管理
- ログの取得・管理
- 暗号・電子署名
- 監視機能

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

➢ 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、現行の自治体情報セキュリティクラウドとの関係性を踏まえながら、地方公共団体の導入費用等も考慮し記載を見直す。

→ 監視に係る運用管理機能について記載。

政府統一基準

（新設）

7.1.6. 監視機能
【遵守事項】

(1)監視機能の導入・運用
(a) 情報システムセキュリティ責任者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装すること。
(b) 情報システムセキュリティ責任者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用すること。
(c) 情報システムセキュリティ責任者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直すこと。

6.2.1. サーバ装置
【遵守事項】
(2)サーバ装置の運用時の対策
(c) 情報システムセキュリティ責任者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講ずること。

改定案：対策基準(例文)

7.1. 情報システムの監視
【例文】

（２） 情報システムの監視機能
①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、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。
②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、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。
③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、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

④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、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

「監視機能を実装」を具体的に示すため、以下の内容を【解説】に記載。

- 監視するイベントとしては、通信回線を通してなされる不正アクセス又は不正侵入並びにC&Cサーバ等への不正な通信、情報システムの管理者・運用者又は利用者の誤操作若しくは不正操作、サーバ装置等機器の動作、許可されていない者の要管理対策区域への立入り等があり得る。
- 職員等による情報窃取等の不正な動作を監視し、これらの不正な動作を検知・防止する内部脅威対策機能を備えたDLPの仕組みの導入を検討してもよい。

3 動的アクセス制御の実装について

政府統一基準群の主な改定内容

✓ クラウドサービスの利用の拡大に対応するため、常時診断・対応型セキュリティアーキテクチャを実装することを念頭に、情報資産等へのアクセスを常時診断・検証して、アクセスを許可又は拒否する新たな技術的手法を講じる際に必要な対策を規定する。

○ 7.3　ゼロトラストアーキテクチャ

・「ゼロトラストアーキテクチャ」は、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。

・ゼロトラストアーキテクチャに基づく情報資産の保護策の１つであり、アクセス制御の仕組みを実現する機能の一部と考えられる動的アクセス制御（※）を実装する場合に特に必要となる対策事項を規定する。

※「動的なアクセス制御」とは、特定のアクセスに対して、セッションが確立してない操作ごとに、都度、アクセス元の信用情報を動的に評価し、アクセス先が信用できる状態であるかを検証したうえで、特定のリスクが検出された場合には追加の認証を求めることや、アクセスを拒否する等のアクセス制御を行うことを想定している。

- 複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システムセキュリティ責任者を選任。
- 動的なアクセス制御の導入方針を定めるにあたり、動的アクセス制御の対象とする情報システムと対象とする情報システムのリソース（ユーザーアカウント、機器等）を識別。
- 動的なアクセス制御の実装にあたり、リソースの信頼情報の変化に応じた動的なアクセス制御のポリシーを作成し、動的なアクセス制御のポリシーに基づき、動的なアクセス制御を行う。
- 動的なアクセス制御の運用に際し、アクセスパターンの変化に応じて、再度リスク評価を行い、動的なアクセス制御のポリシーを見直す。また、リソースの信頼情報の収集により検出されたリスクへ対処を行う。

現行ガイドラインにおける「アクセス制御」の記載

- ✓ 例文にて、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、システム上制限しなければならない、とされている。
- ✓ 解説にて、β´モデルを採用する場合の必須セキュリティ対策として規定されている。
- ✓ いずれも、静的なアクセス制御に関する記載となっている。

第２編　例文　第２章

6. 技術的セキュリティ

6.2.　アクセス制御

アクセス制御、職員等による外部からのアクセス等の制限、自動識別の設定、ログイン時の表示等、認証情報の管理、特権（管理者権限等）による接続時間の制限について規定

第３編　解説　第２章

３．情報システム全体の強靭性の向上

(中略)

(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	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。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

➢ **ゼロトラストアーキテクチャを実現する機能の一部と考えられる「動的なアクセス制御」**に関し、**実装する場合に特に必要な対策について、解説編に参考として記載する**。

政府統一基準

（新設）

7.3.1.動的なアクセス制御の実装時の対策

【目的・趣旨】

従来、組織内ネットワーク上の情報資産の保護においては、インターネット等の機関等外通信回線と組織内ネットワークである機関等内通信回線との境界にファイアウォール等を設置し防御を行い、組織内のネットワークに一定の信頼を置く「境界モデル」の対策が一般的であった。クラウドサービスの普及や、テレワークによる業務システム環境の変化等により、組織内の情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界モデルによる防御だけでは十分なセキュリティ対策の実施は困難になりつつある。特に、境界内部に設置されたサーバ装置等の情報資産について、境界での対策を過信しており、内部に侵入された際の横断的侵害（横方向の侵害やラテラルムーブメントとも呼称される）への情報セキュリティ対策が不足している可能性がある。

（続く）

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

【解説】

（５）ゼロトラストアーキテクチャ

「デジタル社会の実現に向けた重点計画」(令和５年６月９日閣議決定)において、ゼロトラストアーキテクチャの考えに基づくネットワーク構成への対応が掲げられている。
また、内閣官房内閣サイバーセキュリティセンター（NISC）の政府統一基準では以下のとおり、ゼロトラストアーキテクトについて紹介されている。

＜参考：政府機関の情報セキュリティ対策のための統一基準＞

従来、組織内ネットワーク上の情報資産の保護においては、インターネット等の外部通信回線と組織内ネットワークである内部通信回線との境界にファイアウォール等を設置し防御を行い、組織内のネットワークに一定の信頼を置く「境界モデル」の対策が一般的であった。クラウドサービスの普及や、テレワークによる業務システム環境の変化等により、組織内の情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界モデルによる防御だけでは十分なセキュリティ対策の実施は困難になりつつある。

特に、境界内部に設置されたサーバ装置等の情報資産について、境界での対策を過信しており、内部に侵入された際の横断的侵害（横方向の侵害やラテラルムーブメントとも呼称される）への情報セキュリティ対策が不足している可能性がある。

（続く）

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

政府統一基準

（新設）

7.3.1. 動的なアクセス制御の実装時の対策

【目的・趣旨】
（続き）

ゼロトラストアーキテクチャは、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。また、ゼロトラストアーキテクチャは中長期的な政府情報システムに係るライフサイクル全体にわたって適用されるものであり、特定の実装やソリューションを指すものではない。
ゼロトラストアーキテクチャに基づく情報資産の保護策の１つとして、情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。本款では、このような仕組みを実現する機能の一部と考えられる「動的なアクセス制御」を実装する場合に特に必要な対策について記載する。

【遵守事項】
(1) 動的なアクセス制御における責任者の設置
(a) 統括情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システムセキュリティ責任者を選任すること。
（続く）

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
（５）ゼロトラストアーキテクチャ
【解説】
（続き）

ゼロトラストアーキテクチャは、組織内外を問わずネットワークは常に侵害されている ものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。また、ゼロトラストアーキテクチャは中長期的な情報システムに係るライフサイクル全体にわたって適用されるものであり、特定の実装やソリューションを指すものではない。
ゼロトラストアーキテクチャに基づく情報資産の保護策の１つとして、情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。本款では、このような仕組みを実現する機能の一部と考えられる「動的なアクセス制御」を 実装する場合に特に必要な対策について記載する。

①動的なアクセス制御における責任者の設置
統括情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システム管理者を選任すること。
（続く）

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

政府統一基準

（新設）

7.3.1. 動的なアクセス制御の実装時の対策

【遵守事項】
（続き）

(2) 動的なアクセス制御の導入方針の検討
(a) 情報システムセキュリティ責任者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定めること。
(3) 動的なアクセス制御の実装時の対策
(a) 情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシー（以下「アクセス制御ポリシー」という。）を作成すること。
(b) 情報システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行うこと。

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
（５）ゼロトラストアーキテクチャ
【解説】
（続き）

②動的なアクセス制御の導入方針の検討
情報システム管理者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定めること。
③動的なアクセス制御の実装時の対策
・情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシーを作成すること。
・情報システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行うこと。

５．組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

５．組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

政府統一基準群の主な改定内容

✓ 監査等から得られた組織横断的に改善が必要な事項について、進捗状況を定期的にCISOに報告し、CISOは監査結果に基づく改善進捗を把握・組織の統制を図る。

ガイドライン改定の方向性

➢ 監査報告書の指摘事項に対する改善計画が完了していない場合について、CISOに対する進捗状況の定期的な報告を規定する。

政府統一基準

2.3.2　情報セキュリティ監査
【遵守事項】

(３) 情報セキュリティインシデントに係る情報共有
(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示すること。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示すること。
(b) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、機関等内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告すること。
(c) 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告すること。

改定案：対策基準(例文)

9.1. 監査
【例文】

(７) 監査結果への対応
①CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。
②CISOは、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

（赤字が改定部分）

６．過去に改定されなかった箇所の反映

６．過去に改定されなかった箇所の反映

ガイドライン改定の方向性

- 黒塗りを施した報告書が閲覧可能であった事案が発生したことを受けて、外部公開する際の黒塗りの手順について追記してはいかがか。

政府統一基準

3.1.1 情報の取扱い
(5)情報の提供・公表
(d)「不用意な情報漏えい」について
【遵守事項】

情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDF ファイルの「しおり」等に残留した不要な情報を除去する必要がある。
また、ソフトウェアを用いて文書の特定の部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

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情報の作成～⑩情報資産の廃棄
【解説】

（注9）情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDFファイルの「しおり」等に残留した不要な情報を除去する必要がある。 また、ソフトウェアを用いて文書の特定部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

今後のスケジュール

✓　中間報告の内容や、令和５年度から６年度にかけて継続して議論した結果を踏まえ、ガイドラインの改定を6月下旬～７月に実施。

３月13日	検討会
３月末	**中間報告　公表**
４～６月中旬	検討会
６月下旬～７月	**改定・公表**