資料１

サイバーセキュリティに関する基準及び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情報セキュリティポリシーガイドライン改定方針のポイントについて

総務省

2022年7月12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

第4回検討会での主なご意見と対応方針案①

ご意見	対応方針案
基準とガイドライン等の関係が分かりづらいため、地方公共団体にとって分かりやすいように整理をお願いしたい。	基準とガイドラインの位置付けについて、地方公共団体にとって分かりやすいように改めて整理を行う。
ガバメントクラウド上に構築されたマイナンバー利用事務系のシステムと、LGWAN接続系、インターネット接続系のシステムとの連携は、今後どのようになっていくか。	LGWAN接続系の業務システムをガバメントクラウド上に配置する場合には、マイナンバー利用事務系とネットワークを分離し、そのアクセスにおいては、LGWAN接続系の端末から接続することを記載する。 ガバメントクラウドと地方公共団体の接続方法等の検討の状況を踏まえ検討を行う。
地方公共団体はマイナンバー利用事務系以外にも多種多様なシステムを運用しており、地方公共団体が対応しやすいよう、今後の方針は早期に公表してもらいたい。	
クラウド・バイ・デフォルトの原則に従い、地方公共団体がクラウドを選択しやすくなる内容にしてもらいたい。併せて、現場の職員にとって分かりやすい内容にしてもらいたい。	ガイドライン改定時にクラウドサービスに関する章立ての整理等ガイドライン全体の構成の見直しを含め、分かりやすい内容となるよう検討を行う。
クラウドに障害が発生した際に、業務をどう維持、縮小するかを検討する必要があるため、緊急時対応計画に記載することを整理してもらいたい。 併せて、クラウド上のデータが消失するリスクを考慮して、バックアップに関する対策も検討してもらいたい。	障害時の対応、バックアップの確保方法について、現行ガイドラインの記載にクラウドサービス利用の際の記載を追記する方向で検討を行う。

第4回検討会での主なご意見と対応方針案②

ご意見	対応方針案
物理的セキュリティに関して、地方公共団体の負担軽減のため、ガバメントクラウド事業者が確認するような役割分担を検討してほしい。	ガバメントクラウドを利用することにより対応できる事項は、改定方針の中で明示する。
インシデント発生時の体制について、地方公共団体とガバメントクラウドベンダの間にデジタル庁が入るため、どういった体制、経路で情報を共有するかを考える必要がある。	連絡体制のフローについて、先行事業における連絡体制を踏まえて具体化を図る。
インターネットの通信について、アプリケーションのアクティベーションをするために通信が必要なケースもあることを考慮してもらいたい。	ガバメントクラウドにおける外部との通信について、デジタル庁で実施予定のリスクアセスメント結果等を踏まえ、どのような場合に外部との通信を認めるかについて、検討を行う。
保守端末を経由して、クラウドサービスへ侵入し攻撃を受けるケースが増えている。必ずしもセキュアな環境から保守作業をするわけではないことを想定し、脆弱性への対策が必要である。また、保守端末や保守要員の要件についても考慮する必要がある。	
クラウド上での暗号化消去に関して、誰が消去できるか、第三者によって消去されてしまうリスクはないか等、運用と留意点について検討する必要がある。	今後、政府機関やCRYPTRECの動向等を踏まえ、暗号化消去の手順等について検討を行う。

サイバーセキュリティに関する基準について

基準の内容について

○　地方公共団体情報システムの標準化に関する法律（以下「標準化法」という。）では、内閣総理大臣及び総務大臣は、サイバーセキュリティに係る事項等各地方公共団体情報システムに共通する基準（省令）を定めることとされている。

○　サイバーセキュリティに関する基準としては、標準準拠システムのセキュリティに関する標準非機能要件（※）を定め、それを満たす必要があることを規定することを予定している。

※　非機能要件とは、基幹業務システムの可用性、性能・拡張性、運用・保守性、移行性、セキュリティ、システム環境・エコロジーに係る機能要件以外の要件である。令和2年9月に内閣官房･総務省で定めた標準非機能要件をガバメントクラウド先行事業において検証中。

基準の記載事項（案）

○　標準準拠システムの整備及び運用当たっては、以下のサイバーセキュリティに関する標準非機能要件を満たすこと。

（記載事項例）
・順守すべき規程等の確認
・リスク分析を実施する範囲の検討
・管理権限を持つ主体の認証の実施
・システム上の操作制限
・伝送データの暗号化
・蓄積データの暗号化
・ログの取得　等

（参考）地方公共団体情報システムの標準化に関する法律（令和3年法律第40号）（抄）

第二章　基本方針

第五条　政府は、地方公共団体情報システムの標準化の推進を図るための基本的な方針（以下この条において「基本方針」という。）を定めなければならない。

２ 基本方針には、次に掲げる事項を定めるものとする。

（略）

三　各地方公共団体情報システムに共通する基準を定めるべき次に掲げる事項に関する基本的な事項

イ　電磁的記録において用いられる用語及び符号の相互運用性の確保その他の地方公共団体情報システムに係る互換性の確保に係る事項

ロ　サイバーセキュリティに係る事項

ハ　クラウド・コンピューティング・サービス関連技術を活用した地方公共団体情報システムの利用に係る事項

ニ　イからハまでに掲げるもののほか、各地方公共団体情報システムに共通する基準を定めるべき事項

（各地方公共団体情報システムに共通する基準）

第七条　内閣総理大臣及び総務大臣は、第五条第二項第三号イからニまでに掲げる事項について、デジタル庁令・総務省令で、地方公共団体情報システムの標準化のため必要な基準を定めなければならない。

２ 内閣総理大臣及び総務大臣は、情報通信技術の進展その他の情報システムを取り巻く環境の変化を勘案し、前項の基準に検討を加え、必要があると認めるときは、これを変更しなければならない。

３ 内閣総理大臣及び総務大臣は、第一項の基準を定め、又は変更しようとするときは、あらかじめ、地方公共団体その他の関係者の意見を反映させるために必要な措置を講じなければならない。

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情報セキュリティポリシーガイドライン改定方針について

本方針の位置付け

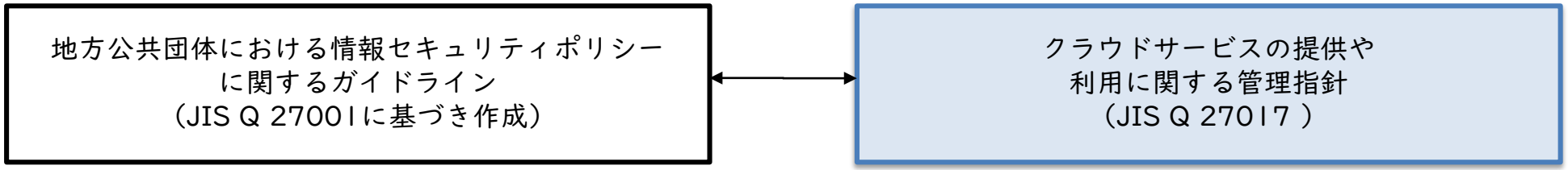
○　地方公共団体情報システムの標準化の推進を図るための基本的な方針である「地方公共団体情報システム標準化基本方針（案）」では、地方公共団体は、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下「ガイドライン」という。）を参考にしながら、セキュリティ対策を行うものとすることとされており、地方公共団体のクラウド利用等に関する情報セキュリティ対策について、ガイドライン上に反映する必要がある。

○　本方針は、今後ガイドラインの改定を行うに当たって、地方公共団体等にあらかじめ示す内容を取りまとめたものである。更なる詳細については、標準化基本方針やガバメントクラウド先行事業の検証結果等の状況を踏まえ、ガイドライン改定に向け引き続き検討を行うこととする。

本方針の構成

○　現行ガイドラインと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)を比較し、クラウドサービスの利用に関して追加的に定めるべき情報セキュリティ対策を現行ガイドラインの項目に沿って整理。

○　ガバメントクラウドを利用する際に、対応不要となる事項等についてはガバメントクラウド個別事項として追記。



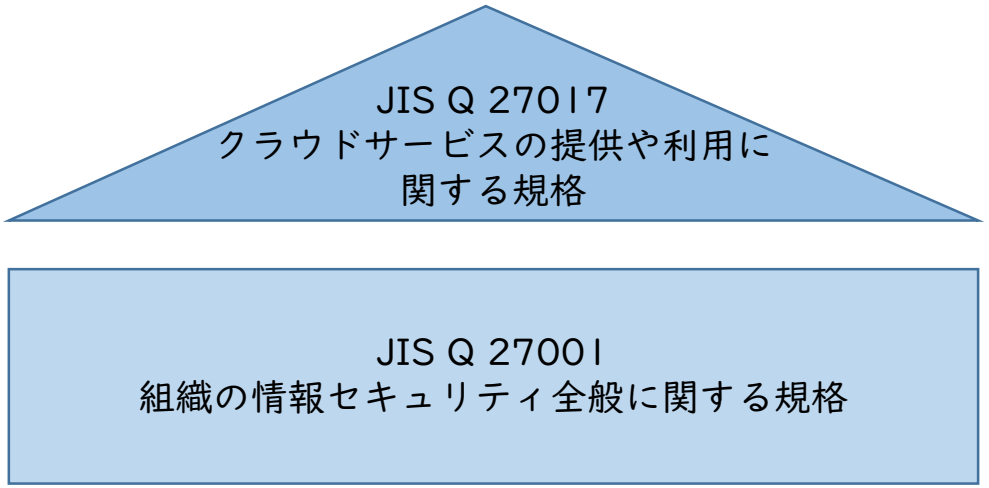
（参考）JIS Q 27001とJIS Q 27017

○JIS Q 27001

JIS Q 27001は、組織の情報セキュリティ全般を管理するための仕組み（ISMS）に関する日本産業規格。「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」は、JIS Q 27001に基づき作成されている。

○JIS Q 27017

JIS Q 27017は、クラウドサービスの提供や利用に関する日本産業規格。情報セキュリティ全般を管理するための仕組みであるJIS Q 27001 に加えて、 JIS Q 27017に記載されている対策を行うことで、クラウドサービスの提供や利用にも対応した情報セキュリティ管理体制を構築することが可能とされている。



JIS Q 27001に加えて、 JIS Q 27017の対策を行うことでクラウドサービスの提供や利用にも対応した情報セキュリティ管理体制を構築

（参考）デジタル社会の実現に向けた重点計画（令和4年6月7日閣議決定）（抄）

第６　デジタル社会の実現に向けた施策

５．デジタル社会を支えるシステム・技術

（２）地方の情報システムの刷新

②　標準化基準における共通事項の策定等

標準化基準における共通事項（非機能要件、データ要件・連携要件など）の策定等に取り組む（標準化基準における共通事項の策定等に関する具体的な施策について、以下を参照。）。

【標準化基準における共通事項の策定等に関する具体的な施策】

②　非機能要件の拡充

標準非機能要件（セキュリティを含む。）については、先行事業での検証を踏まえて、令和４年（2022年）夏までに、必要に応じて拡充する。

このうちセキュリティについては、地方公共団体の業務システムの統一・標準化の取組を踏まえ、ガバメントクラウドの活用を前提とした新たなセキュリティ対策の在り方について検討を行う。

具体的には、デジタル庁及び総務省は、令和４年（2022年）の夏を目途に、標準化基準の作成と併せて、地方公共団体のガバメントクラウド活用に関するセキュリティ対策の方針を決定する。セキュリティ対策の方針においては、国・地方公共団体・クラウド事業者・アプリケーション提供事業者等の責任分担等について、先行事業での検証を踏まえて、具体化を進める。

このほか、クラウドロックインとならないための対策やマルチクラウド・マルチベンダーの相互接続・運用を円滑に行う方策等についても検討を行う。

③　地方公共団体によるガバメントクラウドの利用に関する基準の策定

（略）

ガバメントクラウド上に構築された標準準拠システムを地方公共団体が安心して利用できるようにするため、ガバメントクラウドへの移行に係る課題の検証を行う先行事業を令和３年度（2021年度）及び令和４年度（2022年度）にかけて実施する。

具体的には、ガバメントクラウド上に構築する基幹業務等のアプリケーションの対象範囲の検討、先行事業において構築したシステムが「地方自治体の業務プロセス・情報システムの非機能要件の標準（標準非機能要件）」が求める非機能要件（セキュリティ、可用性、性能・拡張性、移行性、運用・保守性等）を満たすことの検証、ガバメントクラウドに移行したシステムと移行しないシステムとの連携の有効性の検証、現行システムとの投資対効果との比較等を行う。(以下略)

（参考）地方公共団体情報システム標準化基本方針【第0.8版】（抄）

4.2　セキュリティに係る事項（案）（標準化法第５条第２項第３号ロ）

○　地方公共団体が利用する標準準拠システム等の整備及び運用に当たっては、総務省が作成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を参考にしながら、セキュリティ対策を行うものとする。

○　その際、ガバメントクラウド上に構築される標準準拠システム等については、次の考え方に従うものとする。

①　地方公共団体は、クラウドサービス等の提供、保守及び運用（4.3.5.1①）に基づき、地方公共団体の責任とされる範囲において具体的なセキュリティ対策を行う。

②　マイナンバー利用事務系（個人番号利用事務（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（平成25年法律第27号。以下「番号法」という。）第２条第10号に規定するものをいう。）又は戸籍事務等に関わる情報システム及びその情報システムで取り扱うデータをいう。）の端末・サーバ等と専用回線により接続されるガバメントクラウド上の領域についてもマイナンバー利用事務系として扱う。

○　上記以外で、ガバメントクラウド上に構築される情報システムであることに伴うセキュリティの取扱いの詳細については、デジタル庁及び総務省が別途定める。

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情報セキュリティポリシーガイドライン改定方針について

① 組織体制

方針のポイント

○ クラウドサービスを利用する際には外部関係機関等が複数存在するため、関係機関の存在・責任の所在を明確にする必要があることを記載。

○ 特にインシデント発生時には、関係機関との迅速な対応が求められるため、十分な連絡体制を構築することを記載。

○ ガバメントクラウドにおける連絡体制は、先行事業における連絡体制を踏まえて具体化が行われる予定。

Ⅰ．組織体制	
○組織体制	・地方公共団体は、クラウドサービスを利用する際に、関係する外部関係機関等（CSP 、ASP 等が想定される。）の存在を確認し、外部関係機関等が存在する場合は、連絡体制を構築する。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立する。
○情報セキュリティインシデントの報告	・地方公共団体は、CSP（ASPが存在する場合はASP含む）に対して、次に記載した情報セキュリティインシデントの報告の仕組みに関する内容を確認する。 －地方公共団体が検知した情報セキュリティインシデントをCSP（ASPが存在する場合はASP含む）に報告する仕組み －CSP（ASPが存在する場合はASP含む）が検知した情報セキュリティインシデントを地方公共団体に報告する仕組み －地方公共団体が報告を受けた情報セキュリティインシデントの状況を追跡する仕組み 【ガバメントクラウド個別事項】 ガバメントクラウドでは、地方公共団体が検知した情報セキュリティインシデントは、地方公共団体よりCSPへ報告を行う。また、CSPが検知した情報セキュリティインシデントはデジタル庁より地方公共団体へ報告を行う。

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情報セキュリティポリシーガイドライン改定方針について

②　情報資産の分類と管理

方針のポイント

○　クラウドサービスにおいて、重要な情報資産を扱う場合は、ライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）に応じた情報資産の取扱いを明確にする必要があることを記載。

○　情報資産を返却や破棄する際は、データ消去の方法として暗号化した鍵（暗号鍵）を削除することにより、情報資産が復元困難な状態とする方法が考えられるが、暗号化消去の具体的な手順等については、政府機関･CRYPTRECのガイドライン等を踏まえ、引き続き検討を行う。

※CRYPTREC（Cryptography Research and Evaluation Committees）・・・電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。 デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号技術評価委員会、暗号技術活用委員会で構成。

２．情報資産の分類と管理	
○情報資産の分類と管理	・地方公共団体は、クラウドサービスの環境に保存される情報資産について、台帳を作成し、情報資産が保存されている場所を管理する。 ・地方公共団体は、クラウドサービスで扱う情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。また、クラウドサービスを更改する際の情報資産の返却及び除去、並びにこれらの情報資産の全ての複製のCSP(ASPが存在する場合はASP含む)からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認する。 ・クラウドサービスで利用する全ての情報資産について、各サービスの終了時期のスケジュールを文書化し、クラウドサービスで扱う情報資産が適切に返却、除去、削除されるよう管理する。 （６.技術的セキュリティに記載） ・クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除することにより、その情報資産が復元困難な状態とする方法が考えられる(暗号化消去)。

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情報セキュリティポリシーガイドライン改定方針について

③　情報システム全体の強靭性の向上

方針のポイント

○　当面は三層の対策を維持し、マイナンバー利用事務系の端末・サーバ等と接続されるクラウドサービス上の情報システムの領域については、マイナンバー利用事務系として扱い、当該地方公共団体の他の領域とはネットワークを分離するといった原則とすることを記載。

○　LGWAN接続系の業務システムをクラウドサービス上へ配置する場合は、マイナンバー利用事務系とネットワークを分離し、そのアクセスにおいては、LGWAN接続系の端末から接続することを記載。

○　クラウドサービスを利用する際に、マネージドサービスやOSの修正プログラム等の適用、ソフトウェアのアクティベーション等で、インターネットとの接続が必要となる場合がある。そのため、限定的にインターネットへ接続する場合は、リスクアセスメントを実施し、リスクの明確化と定期的な監査（内部監査又は外部監査）を行う必要があることを記載。

○　ガバメントクラウドにおいては、インターネット経由によるOS等の修正プログラム等の適用及びインターネット経由によるシステム運用・保守について、デジタル庁において実施するリスクアセスメント結果を提供予定。

3．情報システム全体の強靭性の向上	
○情報システム全体の強靭性の向上	・地方公共団体は、マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるクラウドサービス上の情報システムの領域については、マイナンバー利用事務系として扱い、当該地方公共団体の他の領域とはネットワークを分離する。 ・LGWAN接続系の情報システムをクラウドサービス上へ配置する場合は、マイナンバー利用事務系とネットワークを分離し、そのアクセスにおいては、LGWAN接続系の端末から接続する。 【ガバメントクラウド個別事項】 ガバメントクラウドでは、マイナンバー利用事務系、LGWAN接続系の情報システムが稼働する環境は、インターネット接続が出来ない設定があらかじめ行われている。

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情報セキュリティポリシーガイドライン改定方針について

３．情報システム全体の強靭性の向上	
○情報システム全体の強靭性の向上	・クラウドサービス上で構築するマイナンバー利用事務における脆弱性の対処を行うために、OS、ミドルウェア、アプリケーション等の修正プログラム及びウイルス対策ソフトのパターンファイルの更新、基幹業務システムを動作する上で必要となるソフトウェアのアクティベーションを実施する場合は、クラウドサービス上のマイナンバー利用事務系及びLGWAN接続系と異なる新たなネットワーク（ＤＭＺ）を構築し、そのネットワーク内に連携サーバ（WSUSのファイル更新サーバ及びウイルス対策ソフト等の更新サーバ）を配置した上で限定された通信の設定（FQDNのホワイトリスト設定、ファイアウォール（FW）によるアウトバウンド通信の制御）を行うとともに、不正なアクセスが無いか日常的な監視を徹底する。ただし、これらの対応については、地方公共団体が利用又は構築するクラウドサービスの環境によって異なる場合が考えられるため、地方公共団体は、リスクアセススメント（リスクの特定、リスクの分析、リスクの評価）を実施した上で、具体的なリスクに対する対応措置を行う。さらに、これらの対策が適切に実施されているのか、運用前の事前テストを実施し、確認するとともに、定期的に監査（内部監査又は外部監査）を行う。これらの対策とマネジメントにより、マイナンバーを含む重要な情報資産に対するリスクの低減に繋がる。万が一、サイバー攻撃等により、マイナンバー等の住民情報の漏えい等の事故が発生した場合、地方公共団体は、説明責任を果たす必要があることを認識する。また、OS、ミドルウェア、アプリケーション等の修正プログラム及びウイルス対策ソフトのパターンファイルの更新について、クラウドサービスの情報セキュリティ水準を証明する以下のいずれかの認証等を受けている若しくは同等の実績を有することが確認できるCSPが提供するマネージドサービスを利用することは妨げない。 ①　ISO/IEC27017又はISMSクラウドセキュリティ認証制度に基づく認証 ②　セキュリティに係る内部統制の保証報告書（SOC報告書（Service Organization Control Report）） 【ガバメントクラウド個別事項】 　ガバメントクラウドに関しては、デジタル庁においてリスクアセスメントを実施し、その結果を必要とする地方公共団体に対して情報提供する予定である。また、定期的な監査については、ISMAPクラウドサービスリストへの登録時および更新時に実施されており、地方公共団体の確認に相当する確認をデジタル庁が実施している。

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情報セキュリティポリシーガイドライン改定方針について

３．情報システム全体の強靭性の向上	
○情報システム全体の強靭性の向上	・クラウドサービスの管理コンソールに対して、例外的にインターネット経由でアクセスする場合は、多要素認証によりアクセスを行う。また、許可された端末からのアクセスに限定する必要があるため、端末認証(MACアドレス、シリアル番号、電子証明書等)又は、接続する機器や拠点のIP アドレス等の認証情報を利用し端末を制限する。さらに、操作履歴などの監査ログを取得することやアクセス者に対して必要最小限の権限設定を行う。ただし、これらの対応については、地方公共団体が利用又は構築するクラウドサービスの環境によって異なる場合が考えられるため、地方公共団体は、リスクアセススメント（リスクの特定、リスクの分析、リスクの評価）を実施した上で、具体的なリスクに対する対応措置を行う。さらに、これらの対策が適切に実施され、外部からの攻撃や脅威に対するリスクが低減されているのか、運用前に事前テストを実施し、確認するとともに、定期的に監査（内部監査又は外部監査）を行う。運用保守等により、これらのアクセスを外部委託で行う場合は、委託先の情報セキュリティ対策が確実に実施されるよう職員等が当該委託先の情報セキュリティ対策を直接管理することや、委託先への要求事項を調達仕様書等に定め、契約条件とするなどの対策が必要である。 【ガバメントクラウド個別事項】 　ガバメントクラウドに関しては、デジタル庁においてリスクアセスメントを実施し、その結果を必要とする地方公共団体に対して情報提供する予定である。また、CSPの定期的な監査については、ISMAPクラウドサービスリストへの登録時及び更新時に実施されており、地方公共団体の確認に相当する確認をデジタル庁が実施している。

（参考）マイナンバー利用事務系とインターネットとの接続に関する現行ガイドラインの記載

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

対策基準3.　情報システム全体の強靭性の向上（解説）

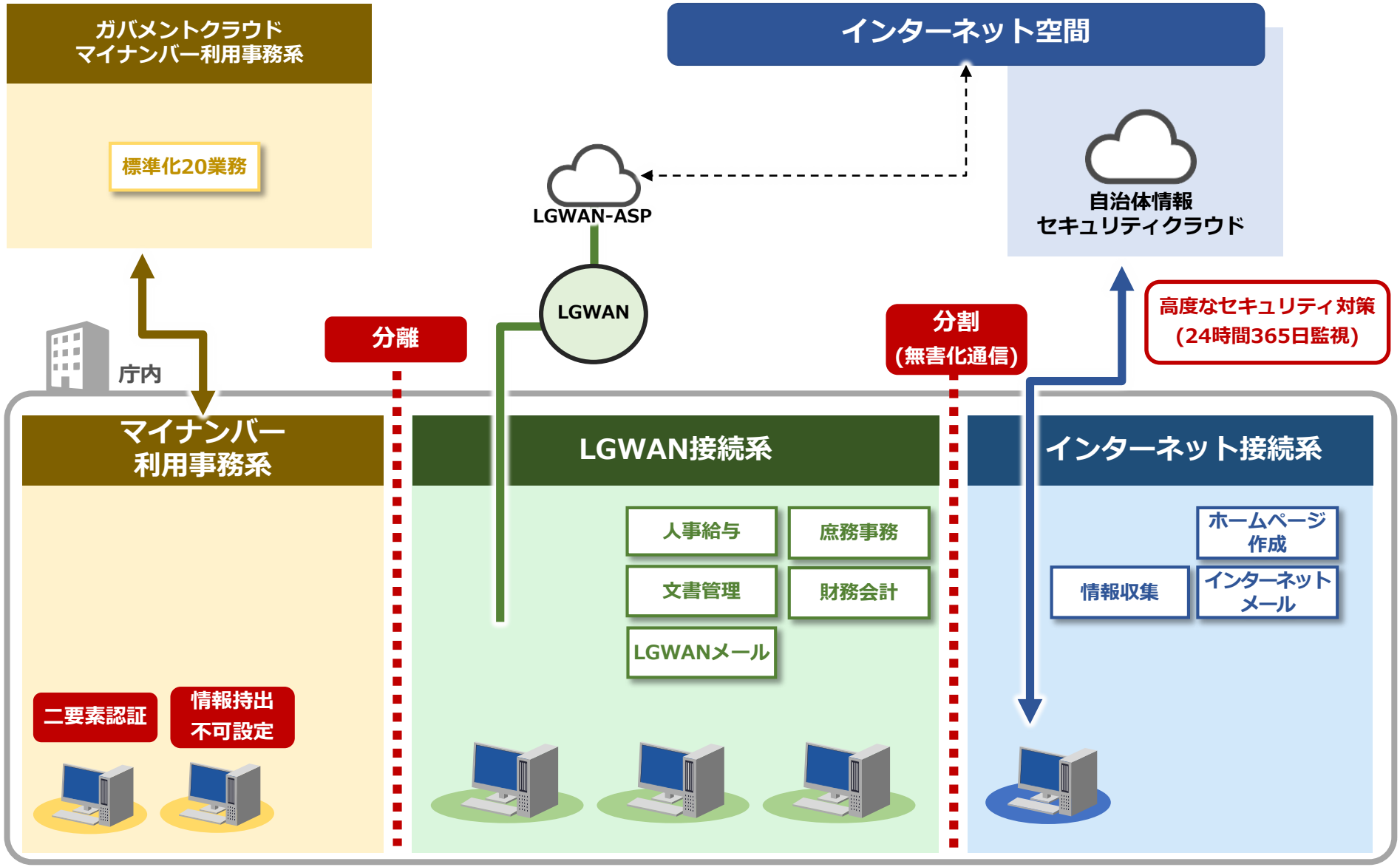
（１）マイナンバー利用事務系
（注２）（注１）※の接続先以外の外部接続先については、止むを得ずインターネットとデータをやり取りする場合は、専用回線を新たに設置し、必要最小限の通信とし、外部のネットワークと通信する専用の端末を管理区域内に設置した上で、電磁的記録媒体を経由したデータのやり取りを行わなければならない。その際には情報システム管理者の許可を受けた上で、電磁的記録媒体の接続禁止設定を一時的に解除し、他の職員の立ち合い又は監視カメラで撮影された状態で、管理区域内において作業を行うなどの取扱いを行わなければならない。
　また、保守用の外部接続先がある場合は、保守の委託先の情報セキュリティ対策が確実に実施されるよう職員等が当該委託先の情報セキュリティ対策を直接管理したり、委託先への要求事項を調達仕様書等に定め、契約条件とするなどの対策が必要である。その他、運用面として保守用の外部接続先との通信は保守の時のみに限定するなどの対策も考えられる。なお、外部接続先との通信については、本解説の「（４）⑤VPN 接続による外部との通信」も参照されたい。

※（注１）とは、「国等の公的機関が構築したインターネットに接続されたシステム等で十分に安全性が確保された外部接続先との通信としてeLTAX、マイナポータル、自治体情報セキュリティ向上プラットフォーム」の事を指している。

対策基準3.　情報システム全体の強靭性の向上（解説）

（４）　その他のセキュリティ対策
③修正プログラム及びパターンファイルの更新
　マイナンバー利用事務系及びLGWAN 接続系では、OS・アプリケーションの修正プログラム及びウイルス対策ソフトのパターンファイルの更新等においても、インターネットに接続して利用してはならない。
　LGWAN-ASP 等を利用して修正プログラム等を取得し適用することが望ましい。WSUS のファイル更新サーバ及びウイルス対策ソフトのパターンファイル更新サーバ等についても、マイナンバー利用事務系及び LGWAN 接続系からのインターネット接続は認められない。

ガバメントクラウドと地方公共団体の接続イメージ



※ガバメントクラウドと地方公共団体の接続方法については、LGWANを活用した接続又はデジタル庁が示すガバメントクラウドへの標準的な接続サービス（ガバメントクラウド接続サービス）を活用した接続を想定し検討中。

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情報セキュリティポリシーガイドライン改定方針について

④　物理的セキュリティ

方針のポイント

○　基幹業務システムで扱う情報資産は機密性が高いため、これらの情報資産をクラウドサービスに保存する場合は、クラウドサービスを利用する装置等の廃棄方法について確認しておく必要があることを記載。

○　ガバメントクラウドにおいては、ISMAPクラウドサービスリストへの登録及びISO/IEC 27017等、上記の認証に対する地方公共団体の確認に相当する確認をデジタル庁が実施していることを記載。

４．物理的セキュリティ	
○資源（装置等）のセキュリティを保った処分	・地方公共団体は、CSPが利用する資源（装置等）の処分（廃棄）について、セキュリティを確保した対応となっているか、CSPの方針及び手順について確認をする。 　当該確認にあたっては、CSP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。 【ガバメントクラウド個別事項】 　ガバメントクラウドにクラウドサービスを提供するCSPは、ISMAPクラウドサービスリストへの登録及びISO/IEC 27017等、上記の認証に対する地方公共団体の確認に相当する確認をデジタル庁が実施している。

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情報セキュリティポリシーガイドライン改定方針について

⑤　人的セキュリティ

方針のポイント

○　クラウドサービスの利用における情報セキュリティの考え方等の研修を地方公共団体の幹部層、情報セキュリティ担当者、利用者等の各層に対して実施し、理解や意識を浸透させることが必要であることを記載。

○　今後、地方公共団体情報システム機構で実施している地方公共団体への研修内容等を確認した上で、必要な内容を検討。

○　ガバメントクラウドにおいては、ガバメントクラウドに関する技術概要やマニュアル等を提供予定。

５．人的セキュリティ	
○情報セキュリティに関する研修・訓練	・地方公共団体は、クラウドサービスの利用に合わせた情報セキュリティポリシー、対策基準を定め、クラウドサービスの管理者や利用する職員等に対して、クラウドサービスの利用に関する自らの役割及び責任を意識させる。 ・地方公共団体は、クラウドサービスを利用する職員等及び委託者を含む関係者の情報セキュリティに関する意識向上、教育及び訓練を実施する。その際、以下の内容を盛り込む。 －クラウドサービスの利用のための手順 －クラウドサービスに関連する情報セキュリティリスク及びそれらのリスク管理方法 －クラウドサービスの利用に伴うシステム及びネットワーク環境のリスク管理方法 －適用法令（裁判管轄・準拠法に関する事項や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等）に関する考慮事項 【ガバメントクラウド個別事項】 ガバメントクラウドでは、今後、ガバメントクラウドに関する技術概要やマニュアル等を提供予定である。

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情報セキュリティポリシーガイドライン改定方針について

⑥　技術的セキュリティ

方針のポイント

○　バックアップについては、過去の地方公共団体におけるインシデント事案を踏まえて、情報資産の重要度に応じたバックアップのレベルの例や契約書・仕様書に記載すべき事項について、すでにガイドラインに記載されているが、今後、クラウドサービス利用の際のバックアップの対応例と留意点の具体例をガイドラインに記載予定。

（参考：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 iii－144）
④～略～特に、バックアップについては、契約において、各業務システムの重要度を勘案した適切なバックアップレベルを設定し、別途のバックアップの取得など、レベルに応じた適切な対策を実施することが重要である。

6．技術的セキュリティ	
○コンピュータ及びネットワークの管理	・地方公共団体が、マイナンバー利用事務の情報システムをクラウドサービスにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度をもつ必要がある。 また、CSP又はASPが暗号に関する対策を行う場合、地方公共団体は、CSP又はASPが提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行う。 ・バックアップについて、CSP又はASPのバックアップ機能を利用する場合、地方公共団体は、CSP又はASPにバックアップ機能の仕様を要求し、その仕様を確認する。また、その仕様がバックアップに関する地方公共団体が求める要求事項を満たすことを確認する。CSP又はASPからバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、地方公共団体が自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行う必要がある。

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情報セキュリティポリシーガイドライン改定方針について

６．技術的セキュリティ	
○コンピュータ及びネットワークの管理	・地方公共団体は、監査及びデジタルフォレンジックに必要となるCSP（ASPが存在する場合はASP含む）の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス側に提出を要求するための手続を明確にし、関係者と合意をする必要がある。 【ガバメントクラウド個別事項】 　ガバメントクラウドにおけるアクセスログ等のCSPの管理責任の範囲にある情報の地方公共団体への提供については、利用基準に定められている。 ・地方公共団体は、仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施)を確実に実施する。SaaSを利用する場合は、これらの対応が、CSP側でされているのか、サービスを利用する前に確認する。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にCSP又はASPに報告を求める。これらは、CSP又はASPが作成した文書や外部又は内部監査報告書で代替する場合もある。 【ガバメントクラウド個別事項】 　ガバメントクラウドにクラウドサービスを提供するCSPは、定期的な監査については、ISMAPクラウドサービスリストへの登録時及び更新時に実施されており、地方公共団体の確認に相当する確認をデジタル庁が実施している。

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情報セキュリティポリシーガイドライン改定方針について

⑥　技術的セキュリティ

方針のポイント

○　クラウドサービスにおける技術的対策については、認証・認可に関係するＩＤ管理、クラウドサービス内のネットワークの分離、アクセス制御、仮想環境におけるセキュリティ対策や構成管理、脆弱性管理等の整理が必要であることを記載。

○　ガバメントクラウドにおいては、多要素認証等の情報セキュリティ上最低限必要となる機能についてテンプレートによる設定がなされる予定。

６．技術的セキュリティ	
○アクセス制御	・地方公共団体は、地方公共団体が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか、利用前にCSP（ASPが存在する場合はASP含む）に確認する。 ・地方公共団体は、クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせる。 【ガバメントクラウド個別事項】 　ガバメントクラウドにおける上記内容については、地方公共団体のための環境構築時に、多要素認証等の情報セキュリティ上最低限必要となる機能についてテンプレートによる設定がなされる。 ・地方公共団体は、パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、地方公共団体が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認する。 ・クラウドコンピューティング環境においてユーティリティプログラム を利用する場合は、各地方公共団体のクラウドサービスにおける管理策に影響がないよう留意する。

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情報セキュリティポリシーガイドライン改定方針について

６．技術的セキュリティ	
○システム開発、導入、保守等	・地方公共団体は、クラウドサービス上の設定が変更された場合は、CSP（ASPが存在する場合はASP含む）から情報を入手し、その変更履歴を管理する。 ・地方公共団体は、クラウドサービスを利用する際は、適切な設定（情報資産へのアクセス権限の設定、不要アカウントの削除等）を付与する責任があることに留意する。適切な設定を実施しない場合、重要な情報資産の情報漏えいに繋がるおそれがあることを認識する。 ・地方公共団体は、CSP（ASPが存在する場合はASP含む）に対して情報セキュリティに関する対策や機能に関する情報の提供を求め、利用するクラウドサービスが、地方公共団体が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価する。 【ガバメントクラウド個別事項】 ガバメントクラウドにおいては、基本方針及び利用基準で示される国と地方公共団体の責任分界に基づき、地方公共団体の責任とされる範囲に関する事項を基本とし、上記の評価がされている。 ・地方公共団体は、情報セキュリティに配慮した開発の手順及び実践になっているか、CSP又はASPに情報を求め、その内容を確認する。 【ガバメントクラウド個別事項】 ガバメントクラウドにクラウドサービスを提供するCSPは、定期的な監査については、ISMAPクラウドサービスリストへの登録時及び更新時に実施されており、地方公共団体の確認に相当する確認をデジタル庁が実施している。
○セキュリティ情報の収集	・地方公共団体は、CSP（ASPが存在する場合はASP含む）に対して、利用するクラウドサービスに影響し得る技術的ぜい弱性の管理内容について情報を求め、地方公共団体の業務に対する影響や保有するデータへの影響について特定する。そして、技術的ぜい弱性に対する脆弱性管理の手順について、CSP（ASPが存在する場合はASP含む）と合意をし、合意書等の文書に定める。

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情報セキュリティポリシーガイドライン改定方針について

⑦　運用

方針のポイント

○　ログの取得や監視の必要性について記載。ガバメントクラウドにおいては、機能の実装について確認した上で、具体的な内容をガイドラインに記載予定。

○　ガバメントクラウドにおいては、ログの取得や監視がCSP側で実施されているため、CSPに関する確認については、改めて確認する必要はないことを記載。

7．運用	
○情報システムの監視	・地方公共団体は、クラウドサービスで提供されるリソースの容量・能力について、CSP（ASPが存在する場合はASP含む）に要求し、合意した内容を満たすことを確認する。 　また、利用するクラウドサービスの使用状況を監視し、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努める。 ・地方公共団体は、イベントログ 取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認する。 ・地方公共団体は、特権的な操作及び操作のパフォーマンスについてログを取得する。CSP（ASPが存在する場合はASP含む）からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討する。 ・地方公共団体は、利用するクラウドサービスで使用する時刻の同期が適切になされているのか確認する。 ・地方公共団体は、CSP（ASPが存在する場合はASP含む）が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、CSP（ASPが存在する場合はASP含む）に対応内容に関する情報を求め、記録に関する保護が実施されているのか確認をする。ただし、ガバメントクラウドを利用する場合、これらの措置がCSP側で実施されているため、CSPに関する確認については、改めて確認する必要はない。

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情報セキュリティポリシーガイドライン改定方針について

⑦　運用

方針のポイント

○　クラウドサービスに関しては、クラウドサービス側で環境がコントロールされている事もあり、予期せぬ停止等がある程度の頻度で発生する事を受容せざるを得ないことが想定される。緊急時対応計画の策定について、現行ガイドラインの記載にクラウドサービス利用の際の記載の追記を検討。

７．運用	
○情報システムの監視	・地方公共団体は、クラウドサービス利用における重大なインシデントに繋がるおそれのある重要な操作に関して、その手順を文書化する。 重要な操作の例には次のものがある。 －サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除 －クラウドサービス利用の終了手順 －バックアップ及び復旧 文書では、監督者がこれらの操作を監視すべきことを明記する。 ・地方公共団体は、CSP（ASPが存在する場合はASP含む）に対して、クラウドサービスで利用可能なサービス監視機能に関する情報を求め、その内容を確認する。
○障害時の対応等	・地方公共団体は、CSP（ASPが存在する場合はASP含む）と情報セキュリティインシデント管理における責任と役割の分担を明確にする。また、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画の作成が必要となる。
○法令遵守	・クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、地方公共団体は、ソフトウェアにおけるライセンス規定を定め、その手順に従い対応を行う。

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情報セキュリティポリシーガイドライン改定方針について

⑧　業務委託と外部サービスの利用

方針のポイント

○　ＳＬＡ（サービス合意書）については、過去の地方公共団体におけるインシデント事案を踏まえて、ガイドラインに記載しているが、クラウドサービスにおいては情報の非対象性（情報がクラウドサービス側に多く、利用者が少ない状況）が存在する。

○　ガバメントクラウドにおいては、デジタル庁とＣＳＰの間でＳＬＡが締結されているが、ガバメントクラウド上の基幹業務アプリケーションの契約は、地方公共団体と基幹業務アプリケーション事業者の間で締結するため、地方公共団体にとって不十分な契約とならないよう具体的にＳＬＡで締結する内容を記載。

８．業務委託と外部サービスの利用	
○外部サービスの利用（機密性２以上の情報を取り扱う場合）	・地方公共団体は、CSP（ASPが存在する場合はASP含む）と情報セキュリティに関する役割及び責任の分担についてクラウドサービスの利用前に合意し、その内容についてサービス合意書（SLA）に定める。なお、ガバメントクラウドにおけるCSP及び間接利用方式におけるASPとのサービス合意書はデジタル庁にて締結されるが、地方公共団体は個別にASPとサービス合意書を締結できる。 ・地方公共団体は、CSP又はASPが委託事業者の扱いになる場合は、外部委託に関する情報セキュリティの方針に含めて管理する。なお、ガバメントクラウドにおけるCSPとの契約は、デジタル庁にて行う。 ・地方公共団体は、サービス合意書（SLA）に次の事項を含むクラウドサービスに関連する情報セキュリティの役割及び責任を定める。 －マルウェアからの保護への対応 －バックアップに関する内容 －暗号による対策と鍵管理の内容 －ぜい弱性管理の手順 －インシデント管理の方法 －技術的遵守の確認方法 －セキュリティ試験の内容 －監査の対応 －ログ及び監査証跡を含む証拠の収集、保守及びログの保護 －サービス合意の終了時における各情報の保護 －認証及びアクセス制御 －ID管理及びアクセス管理

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情報セキュリティポリシーガイドライン改定方針について

⑨　評価・見直し

方針のポイント

○　ガバメントクラウドのセキュリティ対策の状況等の確認において、監査報告書の確認などが考えられるが、現行のガイドラインでは、サービスの選定時に監査報告書の確認を行うことが記載されている。

○　ガバメントクラウドにおいては、ＩＳＭＡＰが取得されている前提となっているが、ガバメントクラウド上の基幹業務アプリケーションについては、現時点ではＩＳＭＡＰの登録は求められていない。
また、情報セキュリティマネジメントの観点では、ＰＤＣＡの各サイクルを適切に実行していく事が求められる。そのため、基幹業務アプリケーションについては、サービス選定時のみならず、評価・見直しのフェーズの中で、地方公共団体が監査報告書の内容を確認し、セキュリティ対策の状況を評価していく旨を記載。

９．評価・見直し	
○監査	・地方公共団体は、関係する規制及び標準に対するそれらの遵守状況を確認するために、CSP（ASPが存在する場合はASP含む）にその証拠（文書等）の提示を求める。これは、第三者の監査人が発行する証明書をこの証拠とする場合がある。ただし、ガバメントクラウド及びISMAPクラウドサービスリストに登録されているクラウドサービスについては、ISMAPの認証の過程でこれらの監査を実施しているため、それらの情報を活用できる。 ・地方公共団体は、CSP（ASPが存在する場合はASP含む）における情報セキュリティポリシーの遵守について監査を定期的に行う。これは、地方公共団体が事前にCSP（ASPが存在する場合はASP含む）に対して提示した仕様、サービス合意書のとおり実施されていたかどうかについて、文書化した証拠を要求する場合もあるが、その証拠は、関係する標準への適合の証明書（外部機関の監査報告書）で代替可能である。ただし、ガバメントクラウド及びISMAPクラウドサービスリストに登録されているクラウドサービスについては、ISMAPの認証の過程でこれらの監査を実施しているため、それらの情報を活用できる。