資料１－①

地方公共団体等からの意見照会結果及び対応方針について

総務省

2022年８月30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

意見照会の実施概要・結果

○　前回の検討会で示した「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(案)」を全国の地方公共団体及び関係府省、企業等へ提示し、意見照会を行った。

（１）実施概要

項目	内容
期間	令和４年７月１３日～令和４年８月３日
対象	全都道府県及び全市区町村、標準化業務関係府省、APPLIC（全国地域情報化推進協会）
提示資料	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(案)など

（２）意見照会の実施結果（提出状況等）

	提出団体数	質問・意見数
都道府県	13団体	67件
市区町村	50団体	314件
関係府省	2団体	10件
APPLIC	－	37件
合計	65団体	428件

意見照会の結果概要　-主な意見と件数 -

○　全体として改定方針の方向性の見直しに関する意見は少なく、クラウドサービスを利用する際のインシデント対応等の具体的な方法に関して詳細な提示を求める意見が多く挙げられた。

	項目	主な意見	件数
１	クラウドの管理	クラウドサービスの利用に関する管理が難しいため、国で管理手順を提示することを求める意見	３６
２	インシデント対応、連絡体制等	具体的な連絡体制を求める意見	２７
３	ガバメントクラウドのインターネット接続	手順の提示やインターネット接続のリスクに対する意見	２１
４	監査に関する内容	監査の基準や項目等の提示を求める意見	１７
５	情報資産の管理	クラウドサービスを利用する際の情報資産の管理に関する方法の提示を求める意見	１６
６	三層の対策に関る内容	記載の明確化を求める意見	１６
７	リスクアセスメント	具体的な手順について提示を求める意見	１３
８	情報資産の廃棄	クラウドサービスを利用する際の情報資産の廃棄や鍵管理の方法の提示を求める意見	１１
９	ISMAP制度に関する内容	地方自治体のISMAP制度適用に関する意見	９
１０	クラウドサービス対象の範囲	ガイドラインの対象範囲の明確化を求める意見	８
１１	ガバメントクラウドとの接続	具体的な接続回線について示すことを求める意見	７
１２	教育・研修、人材等	ガバメントクラウド利用のマニュアルの提示を求める意見	７
１３	SLA	具体的な定量値を求める意見	６
１４	暗号化	クラウドサービスを利用する際の暗号強度や暗号化の範囲の提示を求める意見	６

ガイドライン改定の構成に関する意見への対応について

意　見：ガイドラインにクラウド利用等に関する情報セキュリティ対策を反映するとのことだが、クラウド版の対策として分かりやすくするために、クラウド版は別冊とするか、対策部分が明確になるようにしていただきたい。

対　応：ガイドラインの第４編に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として追加する。

＜現行ガイドライン＞

第１編 総則
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）
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）
第４編 付録

＜改定案＞

第１編 総則
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）
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）
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
第５編 付録

第１編から第３編の記載において、関連する事項は、必要に応じて第４編を参照する記載を追記

第４編　目次案

1.本編の目的
2.本編の適用範囲
3.本編の構成

第４編の内容の説明を前段に記載する。必要に応じて、用語集や関係する参照・参考資料を一覧化する。

4.組織体制
5.情報資産の分類と管理
6.情報システム全体の強靭性向上
7.物理的セキュリティ
8.人的セキュリティ
9.技術的セキュリティ
10.運用
11.業務委託と外部サービスの利用
12.評価・見直し
13.その他（用語集・参照／参考資料）

・現行の対策基準の項目に沿って例文と解説を記載する。

・「改定方針」が例文になり、解説に詳細事項やガバメントクラウドにおける対応（「改定方針」の「ガバメントクラウド個別事項」）等を記載予定。

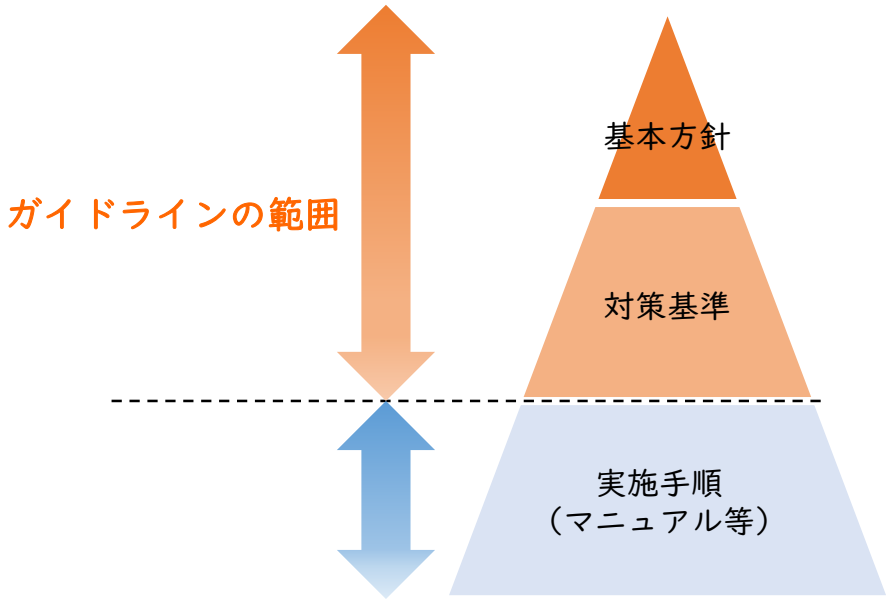
具体的な手順等の提示に関する意見への対応について

意　見：クラウドサービスを利用する際の方法について具体的な手順を示していただきたい。

対　応：ガイドラインと手順書の位置づけを改めて整理し、手順書に関する今後の対応を検討する。

ガイドラインと手順書の位置づけ

- これまで実施手順（マニュアル等）は、地方公共団体の規模等によって実態が異なることからガイドラインの範囲外として整理。



意見照会を踏まえた手順書に関する対応

【現状の課題】

- 地方公共団体の中には、具体的な手順を示さないとクラウドサービス利用規定の作成、評価等を適切に実施できないという状況があると考えられる。

【対応案】

- 一概に具体的な実施手順書を示すことは困難であるが、実施する上で確認が必要な観点を解説に記載する。
- 合わせて関係する資料を参照できるよう、参考資料を一覧化する。

1. クラウドサービス提供事業者（意見を踏まえた改定方針への反映）

意　見：本改定方針は、ガバメントクラウドだけでなく、様々なクラウドサービスの利用形式を想定したセキュリティ対策が記載される。CSP（クラウドサービスプロバイダ）、ASP（アプリケーションサービスプロバイダ）の記載があるが、利用形式によりCSP、ASPの存在が異なるため、クラウドサービス提供事業者へ修正すべきでないか。

対　応：CSP、ASPの記載について、クラウドサービス提供事業者に記載内容を修正する。 ガバメントクラウドに関する事項については、 CSP、ASPの存在が明確であるため記載の修正を行わない。また、今後、クラウドサービスの利用形式については想定される利用事例をガイドラインに追記する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

Ⅰ.組織体制

〇組織体制

・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。

〇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

＜修正案：改定方針＞ (P.４)

〇組織体制

・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（クラウドサービス提供事業者が想定される。）の存在を確認し、外部関係機関等が存在する場合は、必要な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。

〇情報セキュリティインシデントの報告

・地方公共団体は、上記連絡体制の対象者に対して、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上記連絡体制の対象者に報告する仕組み
－クラウドサービス提供事業者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

＊次ページ以降においても「CSP・ASP等」の表現をクラウドサービス提供事業者に修正

2.　情報セキュリティインシデントの報告（意見を踏まえた改定方針への反映）

意　見：ガバメントクラウドの利用においては、地方公共団体が検知したインシデントは、「地方公共団体よりCSPへ報告を行う」とあるが、CSPではなくデジタル庁へ報告すべきではないか。また、既存の報告ルートである「地方公共団体→（都道府県）→総務省→NISC（内閣サイバーセキュリティセンター）」に加え、クラウド基盤提供者のデジタル庁にも報告する流れとすべきではないか。

対　応：連絡体制の流れが明確に分かるよう記載内容を修正する。連絡体制の詳細については別途提供することとする。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

Ⅰ.組織体制

〇情報セキュリティインシデントの報告

【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。

＜修正案：改定方針＞（P.４）

〇情報セキュリティインシデントの報告

【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、デジタル庁・総務省へ報告を行うとともに、NISCへ同報を行う。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。連絡体制の詳細については、別途デジタル庁より提供するものとする。

3.　情報資産の分類と管理（意見を踏まえた改定方針への反映）

意　見：「情報資産が保存されている場所を管理する」とあるが、クラウドサービスによっては、データセンターの具体的な所在地を非開示としているものもあるため、そのような場合の保存場所の管理は難しいのではないか。

対　応：機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いが重要であるという趣旨のため、記載内容を修正する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

２.情報資産の分類と管理

〇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。

＜修正案：改定方針＞ (P.５)

〇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、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にする。

・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クラウドサービス提供事業者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、各サービス利用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。

4. 情報システム全体の強靭性の向上（意見を踏まえた改定方針への反映）①

意　見： LGWAN接続系の扱いについて説明しているが、接続に関して「専用回線」や「閉域網」等の表現がない。庁内と外部接続先との通信について、記載を見直すべきではないか。

対　応： 現行のガイドラインの考え方を変更するものでないため、定義を明確化する観点から修正する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

３.情報システム全体の強靭性の向上

〇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。

＜修正案：改定方針＞（P.５）

〇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、その領域をLGWAN接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続する。

4. 情報システム全体の強靭性の向上（意見を踏まえた改定方針への反映）②

意見①：マイナンバー利用事務系とインターネットとの接続について、様々なセキュリティ施策を講じておきながら、常習的な利用につながる可能性があるため、慎重に議論すべきと考える。これにより情報漏洩が発生した場合、地方公共団体が責任を負うことになるのではと懸念している。

意見②：各地方公共団体におけるリスクアセスメントを実施するとの記載があるが、判断を地方公共団体任せにするのではなく、どのような場合に許容される、されない等の具体的な基準を提示いただきたい。

対　応：マイナンバー利用事務系とインターネットとの接続は従来通り認められないが、ガバメントクラウドに関しては、リスクアセスメントの結果等を踏まえ必要なセキュリティ対策を検討し、テンプレートによる制御等でセキュリティを確保することにしているため、例外的にガバメントクラウドのみ認めるよう記載内容を修正する。ガバメントクラウド以外のクラウドにおける対応については、標準化基本方針(案)において、「ガバメントクラウド以外のクラウド環境その他の環境の方が、性能面や経済合理性等を比較衡量して総合的に優れていると判断する場合には、当該ガバメントクラウド以外のクラウド環境その他の環境を利用することを妨げない。」とされていることから今後、ガバメントクラウド以外のクラウド環境に関する考え方を整理する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

３.情報システム全体の強靭性の向上

〇情報システム全体の強靭性の向上

【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。

＜修正案：改定方針＞（P.５，６）

〇情報システム全体の強靭性の向上

【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。

・マイナンバー 利用事務系におけるクラウドサービスの利用については、外部接続先がインターネットに接続していない閉域環境で利用するクラウドサービスの利用を前提としている。ガバメントクラウドの利用においては、テンプレートによる制御等の対策が実施され、修正プログラムの更新等及び運用保守を行う場合のリスクアセスメントが行われることを踏まえ、特段の場合について例外的にインターネット接続を可能とする。

　なお、ガバメントクラウド以外のクラウドにおけるマイナンバー利用事務系のインターネット接続については、基本方針において、「ガバメントクラウド以外のクラウド環境その他の環境の方が、性能面や経済合理性等を比較衡量して総合的に優れていると判断する場合には、当該ガバメントクラウド以外のクラウド環境その他の環境を利用することを妨げない。」とされていることから、今後、ガバメントクラウド以外のクラウド環境に関する考え方を整理する。

4. 情報システム全体の強靭性の向上（意見を踏まえた改定方針への反映）③

意　見：修正プログラム等の設定について、限定された通信の設定（FQDN （完全修飾ドメイン名）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）が記載されているが、インターネットからのアクセスは、業務上・システム運用保守上、不要の想定であるため、パブリックIPアドレスの付与禁止を追加すべきでないか。また、 WSUSの記載があるが、採用するOSにWindowsの指定等があるとも解釈されかねないため、記載方法について、修正すべきでないか。

対　応：パブリックIPアドレスの付与禁止は、手法の１つのため、インターネットからガバメントクラウド上へのインバウンド通信の禁止を追記する。また、WSUSの記載についても修正する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

３.情報システム全体の強靭性の向上

〇情報システム全体の強靭性の向上

【ガバメントクラウド個別事項】

・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。

＜修正案：改定方針＞（P.６）

〇情報システム全体の強靭性の向上

【ガバメントクラウド個別事項】

・ガバメントクラウド上で構築するマイナンバー利用事務系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、ガバメントクラウド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（修正プログラム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）によるガバメントクラウド上に構築したクライアント及びサーバ等からインターネットへのアウトバウンド通信の制御・インターネットからガバメントクラウド上に構築したクライアント及びサーバ等へのインバウンド通信の禁止）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。

4. 情報システム全体の強靭性の向上（意見を踏まえた改定方針への反映）④

意　見：「委託先の情報セキュリティ対策を直接管理する」という表現について、委託元として委託先に対する監督責任はあるものの、通常の業務委託（請負、委任、準委任）の場合、委託先の従業員への指揮権は委託先であることが一般的であると思われるため、修正いただきたい。

対　応：委託先の契約責任者に対して行うものであり、直接従業員に実施するものではないため、記載内容を修正する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

３.情報システム全体の強靭性の向上

〇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。

＜修正案：改定方針＞（P.７）

〇情報システム全体の強靭性の向上

・ガバメントクラウド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運用保守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委託先への要求事項を調達仕様書等に定め契約条件とし、当該条件が遵守されているか、委託先に定期的に確認し、遵守していない場合には、職員等が委託先に適切に指導を行うなどの対策が必要である。

4. 情報システム全体の強靭性の向上（意見を踏まえた改定方針への反映）⑤

意　見：ガバメントクラウドに関してデジタル庁において何を実施・確認していることが分かりにくいため誤解を招くのではないか。

対　応：デジタル庁が行うリスクアセスメントの実施、確認内容について記載内容を明確化する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

３.情報システム全体の強靭性の向上

〇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…中略…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。

＜修正案：改定方針＞（P.７）

〇情報システム全体の強靭性の向上

・ガバメントクラウドの管理コンソールに対して…中略…遵守していない場合には、職員等が委託先に適切に指導を行うなどの対策が必要である。

その上で、ガバメントクラウドに関しては、デジタル庁において運用保守に対する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。ガバメントクラウドのCSPに対する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、地方公共団体がCSPに対して行う監査に相当する確認をデジタル庁が実施している。

（※ISMAPクラウドサービスリストへの登録時・更新時(監査期間の末日の翌日から1年4ヶ月後まで有効)に、ISMAP管理基準を基にした第三者による監査が行われる。(ISMAP管理基準を含むISMAPの詳細についてはhttps://www.ismap.go.jp/を参照)）

5.　物理的セキュリティ（意見を踏まえた改定方針への反映）

意　見：「ISMAPクラウドサービスリストへの登録及びISO/IEC27017等」との記載があるが、これらの標準は、データセンターの物理的所在地が日本であるか、契約の解釈が日本法に基づくものであるかの記載がないため、記載いただきたい。

対　応：ご指摘の記載について、「地方公共団体の基幹業務システムのガバメントクラウドの利用に関する基準（案）」に記載があるため、記載内容を修正する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

４.物理的セキュリティ

〇資源（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。

５.人的セキュリティ

〇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。

＜修正案：改定方針＞ (P.８)

〇資源（装置等）のセキュリティを保った処分

・地方公共団体は、クラウドサービス提供事業者が利用する資源（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、クラウドサービス提供事業者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、クラウドサービス提供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、ISO/IEC 27017及び利用基準等、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。

〇情報セキュリティに関する研修・訓練

・地方公共団体は、クラウドサービスを利用する職員等及び委託先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。

6. 技術的セキュリティ（意見を踏まえた改定方針への反映）①

意　見：ガバメントクラウドの利用においては、間接利用方式が多いため、CSPからの情報は、ASPが入手する流れが多いのではないか。また、地方公共団体から委託を受けたASPがアクセス権限設定やアカウント管理作業を行うケースが多いため、その場合、ASPとは別の事業者(運用事業者、サポート事業者)が担う可能性があり、記載内容を修正いただきたい。

対　応：「地方公共団体の基幹業務システムのガバメントクラウドの利用に関する基準(案) 」において記載しており、ガバメントクラウド運用補助者が行う場合も想定した形で記載内容を修正する。

＊間接利用方式…地方公共団体が、ガバメントクラウド上のクラウドサービス等に対する管理を自らは行わずに、当該地方公共団体が指定するASPに行わせ、当該クラウドサービス等を利用した標準準拠アプリケーション等を利用する方式

＜現行：改定方針＞

第４章　情報セキュリティ対策について

６.技術的セキュリティ

〇アクセス制御

・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。

〇システム開発、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。

＜修正案：改定方針 ＞（P.10，11）

〇アクセス制御

・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、利用前にクラウドサービス提供事業者に確認する。

【ガバメントクラウド個別事項】

ガバメントクラウドの場合は、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実現できるのか、利用前にガバメントクラウド運用補助者に確認する場合も想定される。

〇システム開発、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、クラウドサービス提供事業者から情報を入手し、その変更履歴を管理する。

【ガバメントクラウド個別事項】

ガバメントクラウドの場合は、ガバメントクラウド運用補助者からクラウドサービス上の設定に関する情報を入手し、その変更履歴を管理する場合も想定される。

6.　技術的セキュリティ（意見を踏まえた改定方針への反映）②

意　見：「ガバメントクラウドにおいては、基本方針(案)及び利用基準(案)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。」とあるが、どのような趣旨か。

対　応：記載内容について再検討を行った。ガバメントクラウドにおいては、原則として他のクラウドと同様に地方公共団体が自組織のセキュリティポリシーを満たしているか評価する必要があるが、地方公共団体の負担軽減のため、特定個人情報評価の記載例等の参考となる情報をデジタル庁が提供するという趣旨の記載に修正する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

６.技術的セキュリティ

〇システム開発、導入、保守等

・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。

＜修正案：改定方針＞ (P.11,12)

〇システム開発、導入、保守等

・地方公共団体は、クラウドサービス提供事業者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、デジタル庁が地方公共団体で実施する特定個人情報保護評価の記載例等の参考となる情報を提供する。

7.　運用（意見を踏まえた改定方針への反映）

意　見：障害時の対応に関しては、ガバメントクラウド個別事項として具体的な定義が必要であるため、記載内容を修正いただきたい。

対　応：「地方公共団体の基幹業務システムのガバメントクラウドの利用に関する基準(案)」を参照してもらうよう記載内容を修正する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

７.運用

〇障害時の対応等

・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。

＜修正案：改定方針 ＞ (P.14)

〇障害時の対応等

・地方公共団体は、クラウドサービス提供事業者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。

【ガバメントクラウド個別事項】

・情報セキュリティインシデントの責任分界については、利用基準を参照する。

　また、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。

8.　外部サービスの利用（意見を踏まえた改定方針への反映）

意　見：「地方公共団体は、クラウドサービス提供事業者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。」とあるが、一般的なクラウドサービスで地方公共団体とCSPで個別のSLAの合意ができるか懸念される。「合意する」といった表現ではなく、「CSPの定める条件を考慮して、受容可能か判断する」といった表現を含めた方が良いと考えるため、記載内容を修正いただきたい。

対　応：地方公共団体がCSPの定める条件を考慮して、受容可能か判断できるよう記載内容を修正する。

＜現行：改定方針＞

第４章　情報セキュリティ対策について

８.業務委託と外部サービスの利用

〇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。

＜修正案：改定方針＞ (P.14)

〇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、クラウドサービス提供事業者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確認する。クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定める。クラウドサービス提供事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス提供事業者の定める条件を鑑み、その規約内容が地方公共団体によって受容可能か判断する。

【ガバメントクラウド個別事項】

・ガバメントクラウドにおけるCSP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ガバメントクラウド上でサービスを提供するASPとサービス合意書を締結できる。

主なご意見と対応（ガイドライン改定に向け補足・検討を行うもの）

章	ご意見	対応方針
第4章 2. 情報資産の分類と管理	ガバメントクラウドにおいて情報資産を返却・破棄する際のデータ消去の方法については、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手法について検討するとされているが、地方公共団体においては、データ消去が適切に処理されたことをどう確認するかという視点も重要となる。効率性、確実性を考慮した、データ消去完了の確認方法についても併せて検討し、お示しいただきたい。	暗号化消去の具体的な手順等については、政府機関･CRYPTREC等検討状況を踏まえ、引き続き検討を行う。
第4章 ５. 人的セキュリティ	「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。」とありますが、クラウドバイデフォルトを進める上で、研修資料を提供いただきたい。	地方公共団体情報システム機構が地方公共団体向けに実施しているリモートランニング（情報セキュリティコース）等において、クラウドサービスの利用に関する情報セキュリティ対策が学べるような内容を盛り込み、地方公共団体への提供を行うことができないか検討を行う。
第4章 ７. 運用	クラウドサービスの利用に当たっては、ステークホルダーが多く、また契約等のバリエーションも多岐にわたるため、具体的な事例等を踏まえた対応例や記載例を提示いただきたい。	地方公共団体において想定されるクラウドサービスの具体的な利用事例を踏まえ、ガイドラインの解説に補足を追記していく。
その他	外部サービスの利用に係る基準について、機密性2以上の情報を扱う場合は「ISMAP認証」を取得したものに限定するなど、どの自治体でも簡単に一定のセキュリティレベルが確保できるような基準としていただきたい。	ISMAP制度については、ISMAPの簡易版であるISMAP-LIU（エルアイユー）の導入等が進められているところであり、制度の動向を踏まえ、今後検討を行う。