資料Ⅰ－②

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）

目次

第１章　本方針の目的について

今般の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）」（以下「基本方針」という。）では、①地方公共団体が利用する標準準拠システム（標準化基準（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。以下「標準化法」という。）第６条第１項及び第７条第１項に規定する標準化基準をいう。）に適合する基幹業務システムをいう。以下同じ。）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」（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、②地方公共団体は、基本方針及び「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）」（以下「利用基準」という。）で示される国と地方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おいて具体的なセキュリティ対策を行うこと、③マイナンバー利用事務（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ガイドライン上のマイナンバー利用事務系として扱うとの方針が示されているところである。

本方針は、ガイドラインの次期改定において記載することを予定する事項について、現時点における方針を地方公共団体等の関係者に示すことを目的としてまとめたものである。

第２章　本方針の範囲について

地方公共団体における情報セキュリティ対策は、各地方公共団体が保有する情報資産を守るにあたって自ら責任を持って確保すべきものであり、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書である情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。総務省では、これまで各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説した文書であるガイドラインを策定し、地方公共団体の情報セキュリティ対策の支援を実施してきた。

現行のガイドラインにおいては、クラウドサービスの活用を見据えた外部サービスの利用としてのセキュリティ対策について、取扱う情報に応じた適切なセキュリティ対策や情報資産のライフサイクルに渡るセキュリティ要件等について記載がなされているものの、マイナンバー利用事務系の情報システムを含め、情報システムをクラウド上（IaaS や

PaaS を含む）で整備及び運用する場合等における各対策基準ついては、具体的には記載がなされてないところである。

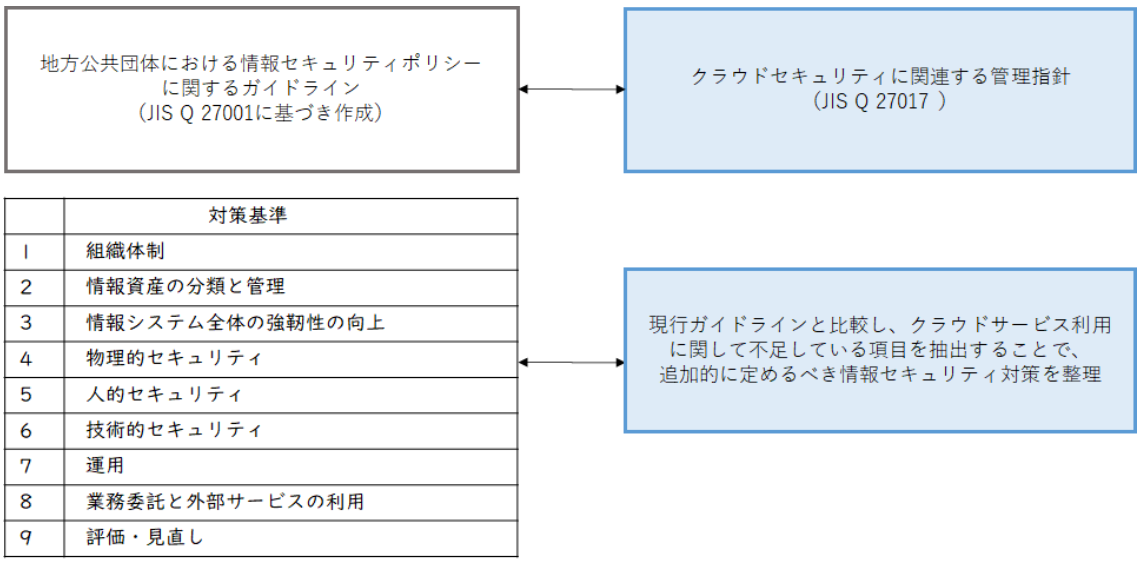
よって、今後、基本方針やガバメントクラウド先行事業の検証結果等の状況を踏まえ、ガイドラインの改定を行い、地方公共団体が情報システムをクラウドサービス上で整備及び運用する場合を範囲として講ずるべき情報セキュリティ対策を記載することとし、地方公共団体においては、これを参考にしながら、各地方公共団体の情報セキュリティポリシーを改定し、適切な情報セキュリティ対策を実施する必要がある。

第３章　本方針の構成について

クラウドサービスを利用するにあたっては、必要となる情報セキュリティ管理策を定めた国際標準等を参考にすることが有用である。本方針の構成としては、地方公共団体が参照しやすいようにガイドラインの対策基準において規定されている項目に沿って、クラウドサービス提供や利用に関する情報セキュリティの国際規格（JIS Q 27017）のクラウドサービスの利用者に求められる事項を加え、具体的な情報セキュリティ対策を規定した。

本方針においては、地方公共団体の情報システムがクラウドサービスを利用する場合の一般の記載を行った後に、マイナンバー利用事務系の情報システムがガバメントクラウドを利用する場合に関する個別事項について記載することとしている。

なお、~~地方公共団体の~~マイナンバー利用事務系においては特定個人情報を扱う場合がある事から、本方針とは別に、個人情報保護委員会「特定個人情報に関する安全管理措置（行政機関等・地方公共団体等編）」を参照し、安全管理措置に関する対応を行う必要がある。



	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
4	物理的セキュリティ
5	人的セキュリティ
6	技術的セキュリティ
7	運用
8	業務委託と外部サービスの利用
9	評価・見直し

第４章　情報セキュリティ対策について

１．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~~[1]、~~ASP~~[2]~~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。

○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）~~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 ~~CSP（ASP が存在する場合は ASP 含む）に~~上記連絡体制の対象者に報告する仕組み

－~~CSP（ASP が存在する場合は ASP 含む）~~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

【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~~ 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。

２．情報資産の分類と管理

○情報資産の分類と管理

---

[1] ~~クラウドサービスプロバイダ~~各クラウドサービスを提供するサービス事業者である 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）を指す。

[2] ~~アプリケーションサービスプロバイダ~~

・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~~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 ~~CSP(ASP が存在する場合は ASP 含む)~~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。

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、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、~~そのアクセスにおいては、LGWAN 接続系の端末から~~専用回線を用いて接続する。

【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。

・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。

・ガバメントクラウド~~サービス~~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~~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~~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。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。~~ガバメントクラウドにおいて提供されるマネージドサービスを利用することを妨げない。

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】~~

また、ガバメントクラウドに関しては、デジタル庁においてマイナンバー利用事務系における脆弱性の対処を行う場合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。また、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[3]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~~の確認~~に相当する確認をデジタル庁が実施している。

・ガバメントクラウド~~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運用保守~~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~~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】~~

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。また、ガバメントクラウドの CSP に対する~~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~~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。

[3] 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)

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~~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[4]となっているか、~~CSP~~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、~~CSP~~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~~及び~~、ISO/IEC 27017 等、~~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。

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~~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。

－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、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

[4] NIST SP 800-88 Rev1,Rev2「媒体のデータ抹消処理（サニタイズ）に関するガイドライン」が参考となる。

供予定である。

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系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[5]をもつ必要がある。

また、~~CSP 又は ASP~~ クラウドサービス提供事業者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~~ クラウドサービス提供事業者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。

・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[6])。

・バックアップについて、~~CSP 又は ASP~~ クラウドサービス提供事業者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~~ クラウドサービス提供事業者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~~ クラウドサービス提供事業者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。

・地方公共団体は、監査及びデジタルフォレンジック[7]に必要となる ~~CSP（ASP が存在する場合は ASP 含む）~~ クラウドサービス提供事業者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】

---

5 暗号が十分な強度を持つかどうかについては、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」(平成25年3月1日(令和3年4月1日最終更新)総務省・経済産業省)及び同リストを策定したCRYPTREC の今後の報告が参考となる。

6 ISMAP 管理基準では「暗号化消去もデータ消去(もしくは抹消)の一つ」と示している。暗号化消去の手順等については、政府機関や CRYPTREC のガイドライン等を踏まえ、引き続き検討を行う。

7 電子データを調査分析することで事実解明及び証拠保存を行うための技術のこと。

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[8]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[9]を利用する場合は、これらの対応が、~~CSP~~ クラウドサービス提供事業者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~~ クラウドサービス提供事業者に報告を求める。これらは、~~CSP 又は ASP~~ クラウドサービス提供事業者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、~~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、地方公共団体の確認に相当する確認をデジタル庁が実施している。

○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）~~ 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。

・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】

---

[8] ソフトウェアによって仮想的に再現された、物理的なコンピュータと同等の機能を有するコンピュータのこと。

[9] Software as a Service の略。サービスの形で提供されるソフトウェアであり、利用者には CSP のインフラストラクチャ上で稼動している ASP 由来のアプリケーションが提供される。

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、地方公共団体において多要素認証の設定を求める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[10]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。

○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）~~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。

・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[11]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）~~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、~~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~~

10 補助的な機能を提供するソフトウェアのこと。

11 独立行政法人情報処理推進機構セキュリティセンター「情報セキュリティ 10 大脅威 2022」,p22

~~評価がされている。~~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。

・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がされているか、~~CSP 又は ASP~~ クラウドサービス提供事業者に情報を求め、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、~~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）~~クラウドサービス提供事業者に対して、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~~脆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）~~クラウドサービス提供事業者と合意をし、合意書等の文書に定める。

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）~~クラウドサービス提供事業者に要求し、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[12]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[13]及び操作のパフォーマンスについてログを取得する。

---

12 コンピュータ内で起こった特定の現象・動作の記録のこと。

13 サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常の ID よりもシステムに対するより高いレベルでの操作のこと。

~~CSP（ASP が存在する場合は ASP 含む）~~クラウドサービス提供事業者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[14]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）~~クラウドサービス提供事業者が収集し、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）~~クラウドサービス提供事業者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。

【ガバメントクラウド個別事項】
~~ただし、~~ ガバメントクラウドを利用する場合、これらの措置がガバメントクラウドの 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）~~クラウドサービス提供事業者に対して、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。

[14] NIST コンピュータセキュリティログ管理ガイドでは、「各システムの時計を標準時刻と同期した状態に保ち、タイムスタンプがほかのシステムで生成されるものと一致するようにする」と記載されている。（NIST Special Publication 800-92）

○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）~~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。

○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[15]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。

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）~~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。~~なお、~~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 及び間接利用方式における ASP~~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。

・地方公共団体は、~~CSP 又は ASP~~ クラウドサービス提供事業者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

[15] Infrastructure as a Service の略。サービスの形で提供されるインフラストラクチャであり、利用者には演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースが提供される。

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
－~~ぜゃ~~脆弱性管理の手順
－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

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）~~クラウドサービス提供事業者にその証拠（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）~~クラウドサービス提供事業者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）~~クラウドサービス提供事業者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。