

# 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 ガイドライン改定のポイントについて① (クラウド利用関係)



総務省

2023年1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

## これまでのガイドライン改定の経緯について

### これまでの検討経緯

- 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」（令和4年10月閣議決定）において、「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、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」とされたところであり、地方公共団体の標準準拠システム等のクラウド利用に関する情報セキュリティ対策について、ガイドラインに反映する必要がある。
- 昨年8月に今後のガイドラインの改定を行うにあたって、地方公共団体等にあらかじめ示す内容を取りまとめた「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」を示し、標準準拠システム等のクラウドサービス利用に関するセキュリティ対策の整理を行った。

# 「地方公共団体における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」（令和4年8月公表）について

## 改定方針の構成とポイント

- 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セキュリティ対策を整理。

### 第1章 本方針の目的

- ▷ガイドラインの次期改定において、記載予定の事項を方針として記載

### 第2章 本方針の範囲

- ▷地方公共団体がマイナンバー利用事務系のシステムを含む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整理

### 第3章 本方針の構成

- ▷クラウドサービスの提供や利用に関する情報セキュリティの国際規格(JISQ27017)に基づき、具体的な情報セキュリティ対策を記載

### 第4章 情報セキュリティ対策

#### 1.組織体制

- ▷クラウドサービス利用時の組織体制の構築、インシデント発生時の連絡体制の確認の必要性を記載

#### 2.情報資産の分類と管理

- ▷ライフサイクルに応じた情報資産の取扱いの明確化
- ▷暗号化消去について、データ消去の方法の一つとして記載

#### 3.情報システム全体の強靱性の向上

- ▷クラウドサービス上でのマイナンバー利用事務系等の取扱いを記載
- ▷マネージドサービス等を利用する場合の考え方を記載

#### 4.物理的セキュリティ

- ▷クラウドサービスの装置等の廃棄方法の確認等について記載

#### 5.人的セキュリティ

- ▷クラウドサービス利用時の職員等の意識向上、教育及び訓練について記載

#### 6.技術的セキュリティ

- ▷クラウドサービス利用時のバックアップの留意点、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の必要性について記載

#### 7.運用

- ▷ログの取得、監視、緊急時対応計画の必要性について記載






#### 8.業務委託と外部サービスの利用

- ▷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たサービス合意書の締結について記載

#### 9.評価・見直し

- ▷サービス選定時のみならず、評価・見直しの段階での監査報告書において確認する必要性について記載

## 今後のガイドライン改定の進め方について（案）

	1月	2月	3月
検討会開催	第7回 (1月12日)	第8回 (2月中旬)	
地方公共団体への意見照会 意見反映			
検討会結果反映			
パブリックコメントの実施 意見反映			
構成員確認			
ガイドライン改定・公表			

#### 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・ニ）

- サイバーセキュリティ等に関する標準化基準として、標準準拠システムのセキュリティ、可用性、性能・拡張性、運用・保守性、移行性、システム環境・エコロジーに係る機能要件以外の要件（非機能要件）について、指標、選択レベル及び選択時の条件の標準を定める。
- 上記のほか、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。

## ガイドライン改定案の構成について

- 第1編に政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針等を踏まえたクラウドサービス利用に関するメリットや留意点等を記載。
- 第4編にクラウド利用等に関する特則として、「ガイドライン改定方針」に基づき、標準準拠システム等のクラウド利用を行う場合の具体的な情報セキュリティ対策（セキュリティポリシーの例文・解説）を記載。

### <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

- ・クラウドサービスに関する特徴、サービスモデル、クラウドサービス利用における留意点等について、政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針、NIST※のクラウドサービスの定義等を参考に追記。

#### 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(例文・解説)

- ・標準準拠システム等の情報システムのクラウド利用を行う場合の具体的な情報セキュリティ対策について、「ガイドライン改定方針」に基づき追記。

#### 第5編 付録

※NIST（National Institute of Standards and Technology）・・・米国国立標準技術研究所

## 第1編 総則 クラウドサービスに関する全般的な留意点について

○ 第1編 総則についての主な記載内容は以下のとおり。

	主な記載内容
1. クラウドサービスにおけるサービスモデルと責任の分担	○ クラウドサービスのモデルに応じて、クラウドサービス事業者の責任の範囲が異なり、留意が必要なため、各モデル（IaaS、PaaS、SaaS）の特徴や一般的な管理主体の例を記載。
2. クラウドサービスの特性における留意事項	○ クラウドサービスの特性に伴い、次の事項に留意が必要であることを記載。 ① 自組織の情報セキュリティの要求事項を満たすか評価すること ② 情報セキュリティ対策の評価の際には、クラウドサービス事業者の公開情報等を参考にすること ③ 第三者認証の確認の際には、ISMAP等の取得状況を確認すること ④ 機密性が高い情報は、国内のデータセンターに保存されることを確認する必要があること
3. クラウドサービスを利用する際に関係する複数のステークホルダー	○ クラウドサービスを利用する際に複数のステークホルダーが存在する場合は、役割と責任の範囲を明確にし、契約締結が必要であることを記載。 ○ クラウドサービスのサプライチェーンの構成に応じた複数のステークホルダーとの契約関係、責任の範囲の例を記載。
4. クラウドサービスを利用する際のリスクの検討	○ クラウドサービスのリスク評価及び結果に応じた対応の確認をクラウドサービスの利用前に実施する必要があることを記載。 ○ ライフサイクルにおける管理、自組織の運用体制、自組織の情報セキュリティポリシーや業務継続に適しているか等の検討が必要であることを記載。

## 第4編 特則の概要：第1章 本編の目的について

### 第1章 本編の目的について

#### 特則のポイント

- 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ことを記載。
- ※ 今後、令和6年度末を目途に第4編特則と本編（第2編、第3編）との統合を予定。
- 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文書との対応表を作成し、参照することを記載。対応表は今後適時更新を行う。

### 第1章 本編の目的について（抜粋）

#### ○第1章 本編の目的 について

（略）

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。

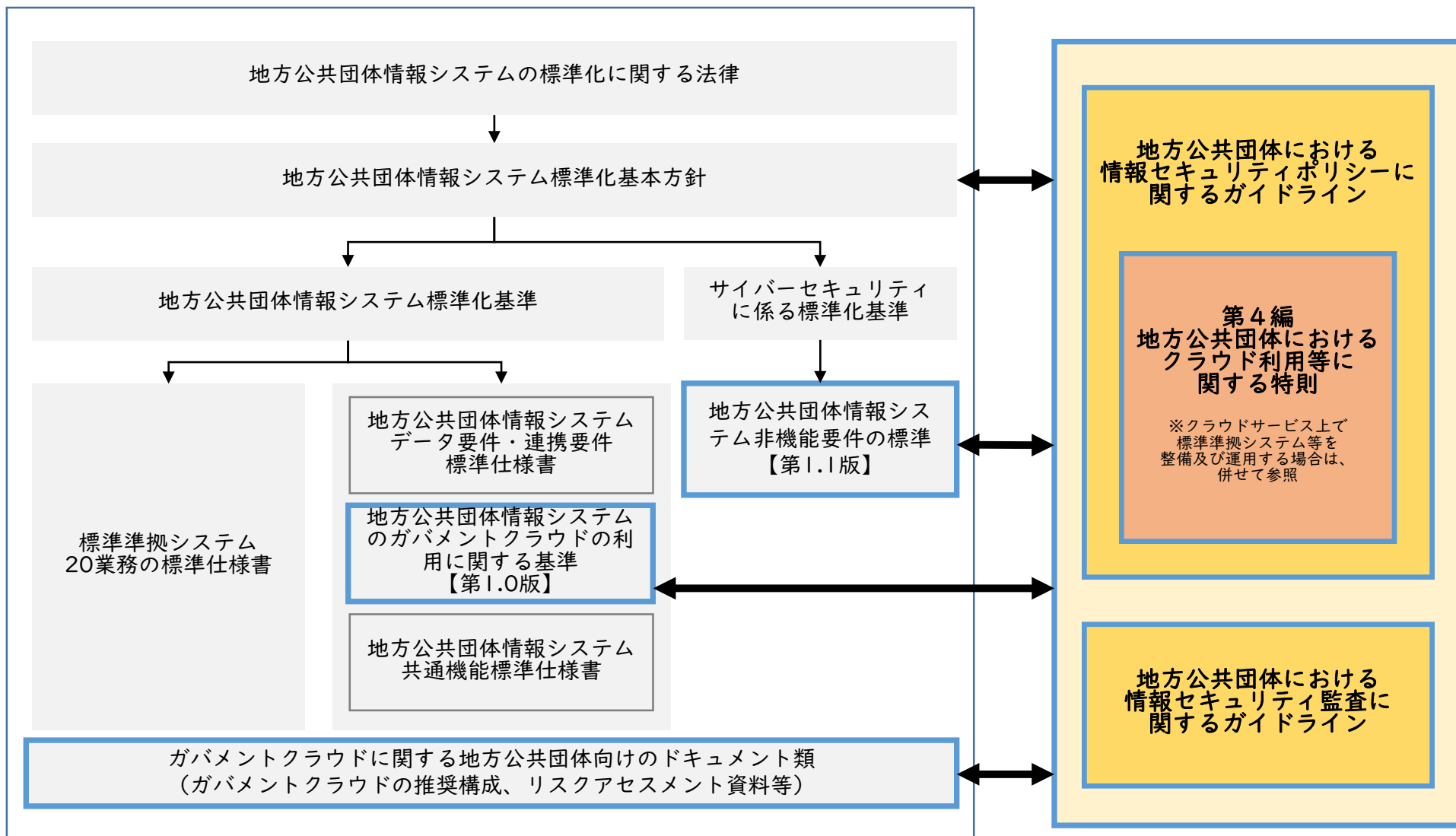
ガイドラインの記載事項とガバメントクラウドに関する対応については、デジタル庁が示すガバメントクラウドに関するドキュメント類の記載内容等を踏まえ、本ガイドラインの補足資料として、本編の対策基準との対応表を掲載し、適時更新を行う。



# 本ガイドラインと標準化法に関連する規定・ドキュメント類との関係

標準準拠システム及びガバメントクラウド利用における関連文書

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考え方及び内容を解説したガイドライン



## 第4編 特則の概要：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2章 本編におけるクラウドサービスの範囲について

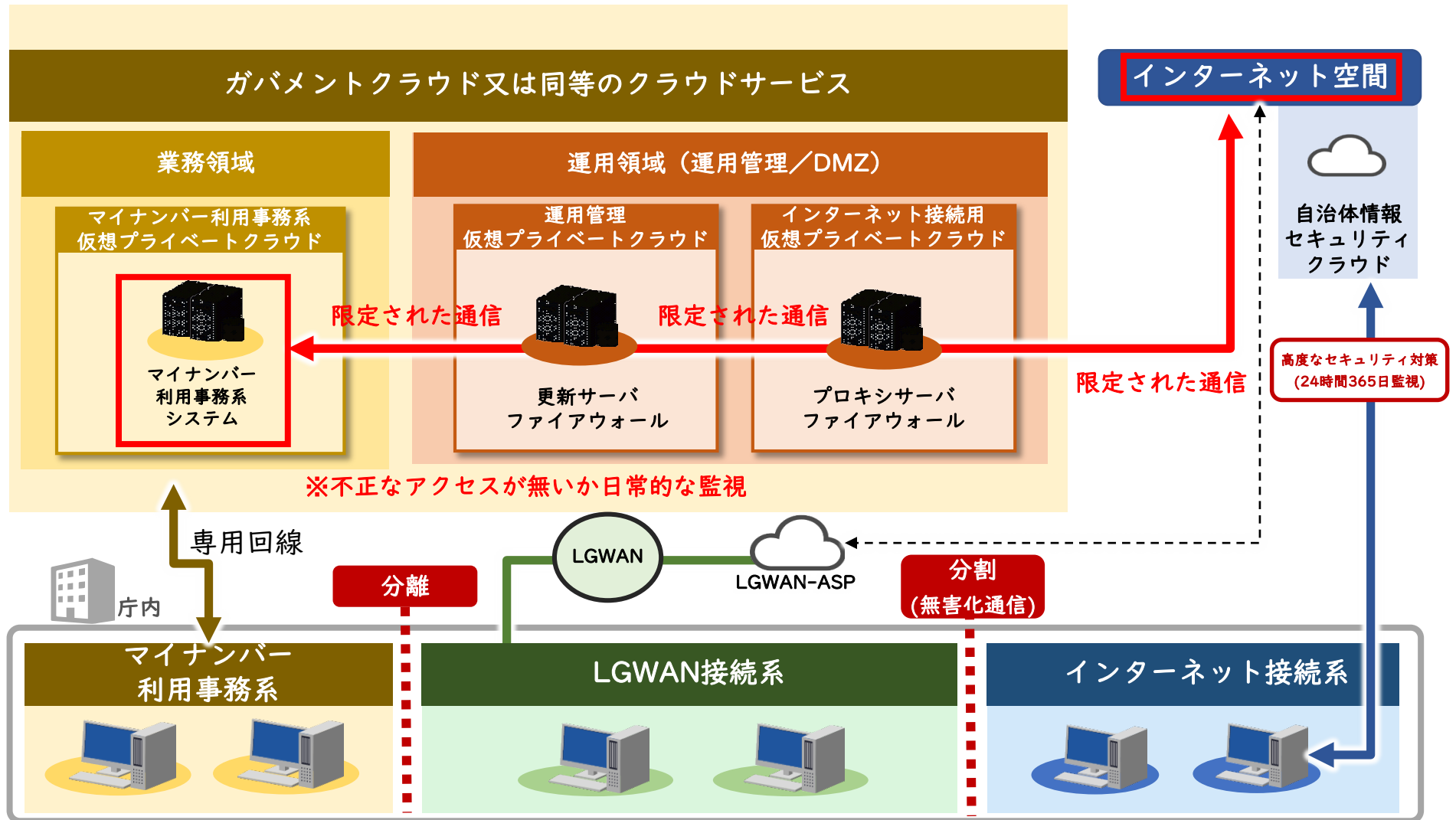
#### 特則のポイント

- ガバメントクラウド及びガバメントクラウドと同等の情報セキュリティの水準が維持可能なクラウドサービスについては、特段の場合（修正プログラムの適用、ソフトウェアのアクティベーションの実施及び管理コンソール接続）に例外的にインターネット接続を可能とすることを記載。

### 第2章 本編におけるクラウドサービスの範囲について

<p>○第2章 本編におけるクラウドサービスの範囲について</p>	<p>これまで地方公共団体の業務におけるクラウドサービスの利用においては、マイナンバー利用事務系、LGWAN 接続系ともに、インターネットからの脅威を極小化するため、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、インターネットと接続されるパブリッククラウドサービスについては、<math>\beta'</math> モデルを中心とした利用や公開情報を中心とした機密性が低い情報資産の運用等に限定してきた。ただし、ガバメントクラウドにおいては、性質上パブリッククラウドに位置づけられるものの、デジタル庁がクラウドサービス事業者（CSP）との契約を行い、テンプレートによる制御等の対策が実施され、さらに、修正プログラムの更新や管理コンソールのアクセス等の運用保守を行う場合のリスクアセスメントがデジタル庁にて行われることを踏まえ、安全性、信頼性が高いと言える。そのため、ガバメントクラウドにおいては、特段の場合（修正プログラムの適用、ソフトウェアのアクティベーションの実施及び管理コンソール接続）について例外的にインターネット接続を可能とする。</p> <p>また、ガバメントクラウド以外のクラウドサービスについては、ISMAP認証やクラウドサービスにおける第三者認証を取得したサービスにおいて、標準準拠システム等の利用・運用が想定される。この場合、修正プログラムの更新や管理コンソールのアクセス等の運用保守を行うにあたり、デジタル庁より示されたリスクアセスメントの結果等を参考とし、ガバメントクラウドと同等の情報セキュリティ対策が実施されていることを評価（内部監査・外部監査等）することを条件に、例外的にインターネット接続を可能とする。</p> <p>本編は、標準準拠システム等をガバメントクラウドにおいて利用することを前提として、その対策基準を示しているが、<math>\beta'</math> モデルにおいてクラウドサービスを利用する際の対策基準としても活用できるように策定している。<math>\beta'</math> モデルを活用して機密性の高い情報資産の運用をクラウドサービス上で運用する地方公共団体においては、本編を参考にして<math>\beta'</math> モデルにおける対策基準を定めることが望ましい。</p>
---------------------------------------	---

# インターネット経由による標準準拠システムの修正プログラム適用イメージ



## 第4編 特則の概要：第3章 本編における対策基準の構成について

### 第3章 本編における対策基準の構成について

#### 特則のポイント

- マイナンバー利用事務系のシステムをクラウドサービスにおいて利用する場合は、個人情報保護委員会が示す「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）」の対応が必要であることを記載。
- 個人情報保護法の改正（令和5年4月施行）に伴い、個人情報保護委員会の行政機関等に係るガイドライン等を参照し、安全管理措置に関する対応を行う必要があることを記載。

### 第3章 本編における対策基準の構成について

○第3章  
本編における対策基準の構成について

本編の構成は、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、クラウドサービスの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参考にし、クラウドサービス上で標準準拠システム等を整備及び運用する場合の具体的な対策基準について、例文と解説で示している。

（略）

第1編第4章で示した通り、マイナンバー利用事務系をクラウドサービスで利用する場合には、特定個人情報を扱う場合があることから、本編とは別に、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。また、改正個人情報保護法が、令和5年4月から地方公共団体等の機関に適用されるため、個人情報保護委員会の行政機関等に係るガイドライン等を参照し、安全管理措置に関する対応を行う必要がある。個人情報保護法における安全管理措置に関しては、本ガイドラインの第1編第2章1.地方公共団体における情報セキュリティの考え方を参照されたい。

## 第4編 特則の概要：第4章 情報セキュリティ対策について①

### 第4章 情報セキュリティ対策について / 1.組織体制

#### 特則のポイント

- クラウドサービスを利用する際には、複数の事業者が存在するため、複数の事業者の存在・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、複数事業者との迅速な対応が求められるため、十分な連絡体制を確立することを記載。

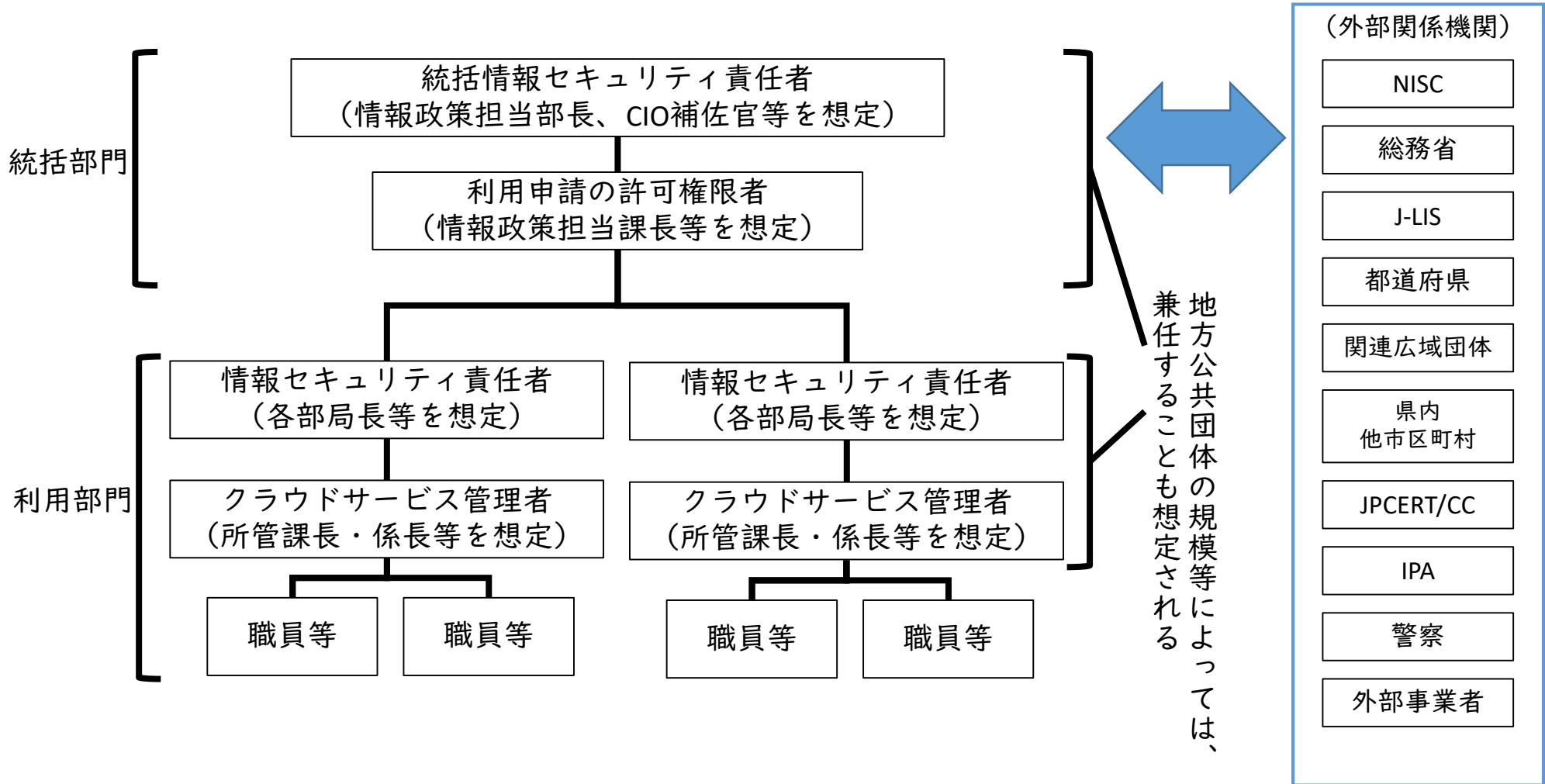
#### 第4章 情報セキュリティ対策について（例文）

##### 1.組織体制

（10）クラウドサービス利用における組織体制

①統括情報セキュリティ責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。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しなければならない。

# クラウドサービス利用における組織体制例



## 第4編 特則の概要：第4章 情報セキュリティ対策について②

### 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

#### 特則のポイント

- 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も、機密性、完全性及び可用性により、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）の取扱いを定める必要があることを記載。
  - 情報資産の廃棄時、クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理する必要があることを記載。
- ※ 情報資産を廃棄する際は、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、情報資産を復元困難な状態とする方法が考えられるが、ガバメントクラウドにおける暗号化消去の対応については、引き続き検討し、地方公共団体に提示予定。

#### 第4章 情報セキュリティ対策について（例文）

##### 2.情報資産の分類と管理

##### (2) 情報資産の管理

##### ①管理責任

(ウ) 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も(1)の分類に基づき管理しなければならない。また、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。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス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しなければならない。

##### ⑩情報資産の廃棄等

(エ) クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

## 第4編 特則の概要：第4章 情報セキュリティ対策について③

### 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靱性の向上

#### 特則のポイント

- マイナンバー利用事務系の端末・サーバ等と接続されるガバメントクラウド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ことを原則とすることを記載。
- ※ LGWAN接続系において安全にクラウドサービスを利用するために必要なセキュリティ対策については、今後検討し、整理を行う予定。

#### 第4章 情報セキュリティ対策について（例文）

<p>3.情報システム全体の強靱性の向上</p>	<p>(1) マイナンバー利用事務系</p> <p>③マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い  <u>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ガバメントクラウド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、本市の他の領域とはネットワークを分離しなければならない。</u></p> <p>(2) LGWAN接続系</p> <p>②LGWAN接続系と接続されるクラウドサービス上での情報システムの扱い          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しなければならない。</p>
--------------------------	---



## 第4編 特則の概要：第4章 情報セキュリティ対策について④

### 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

#### 特則のポイント

- 標準準拠システムでは、機密性の高い情報資産を扱うため、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の方針及び手順の確認が必要であることを記載。
- 当該確認に当たり、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取  
得している場合には、その監査報告書や認証等の利用が可能であることを記載。

#### 第4章 情報セキュリティ対策について（例文）

4.物理的セキュ  
リティ

(7) 機器の廃棄等

②クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等  
を取得している場合には、その監査報告書や認証等を利用する必要がある。

## 第4編 特則の概要：第4章 情報セキュリティ対策について⑤

### 第4章 情報セキュリティ対策について / 5.2人的セキュリティ

#### 特則のポイント

- 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の研修を定期的にクラウドサービスを利用する職員等や委託先を含む関係者に対して実施し、理解や意識を浸透させることが必要であることを記載。

#### 第4章 情報セキュリティ対策について（例文）

5.2人的セキュリティ

○情報セキュリティに関する研修・訓練

(1) 情報セキュリティに関する研修・訓練

②CISOは、定期的に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しなければならない。

## 第4編 特則の概要：第4章 情報セキュリティ対策について⑥

### 第4章 情報セキュリティ対策について / 6.1技術的セキュリティ

#### 特則のポイント

- 情報資産のバックアップが確実に取得されるよう、クラウドサービス事業者が提供する機能を利用するか、自らバックアップに関する機能を設けて実施するか確認する必要があることを記載。  
(バックアップについては、ランサムウェアへの対応にも記載を追記。)
- ログが確実に取得されるよう、クラウドサービス事業者が提供するログ管理の機能を確認し、十分でない場合は、クラウドサービス事業者に提出を要求するための手続を明確にする必要があることを記載。  
(ログ取得の目的や適正な保存、確認等については、第3編 6.1も参照。)

#### 第4章 情報セキュリティ対策について (例文)

6.1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

○情報システムの監視

(2) バックアップの実施

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、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その仕様がバックアップに関する本市が求める要求事項を満たすことを確認しなければならない。クラウドサービス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、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わなければならない。

(6) ログの取得等

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、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。なお、クラウドサービス事業者が収集し、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、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

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、監査及びデジタルフォレンジックに必要となるクラウドサービス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、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

## 第4編 特則の概要：第4章 情報セキュリティ対策について⑦

### 第4章 情報セキュリティ対策について / 6.6技術的セキュリティ

#### 特則のポイント

- 脆弱性が放置されることがないように、利用するクラウドサービスに影響しうる脆弱性情報の提供をクラウドサービス提供事業者に求め、影響を特定し、脆弱性管理の手順を確認する必要があることを記載。

#### 第4章 情報セキュリティ対策について（例文）

6.6技術的セキュリティ  
○セキュリティ情報の収集

(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、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市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、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者を確認しなければならない。

## 第4編 特則の概要：第4章 情報セキュリティ対策について⑧

### 第4章 情報セキュリティ対策について / 7.3運用

#### 特則のポイント

- 情報セキュリティインシデントに備えて、クラウドサービス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必要があることを記載。
- 庁内では、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を定めておき、インシデント発生時には当該計画に従って適正に対処する必要があることを記載。

#### 第4章 情報セキュリティ対策について（例文）

7.3運用 ○障害時の対応等	(1) 緊急時対応計画の策定 ②CISO又は情報セキュリティ委員会は、 <u>クラウドサービス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し、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。</u>
-------------------	---

## 第4編 特則の概要：第4章 情報セキュリティ対策について⑨

### 第4章 情報セキュリティ対策について / 7.5運用

#### 特則のポイント

- ソフトウェアによっては、オンプレミス用とクラウド用でライセンス体系が異なる場合があります。オンプレミス環境で使用しているソフトウェアをクラウド環境でも利用する際は、改めてライセンスの体系や条項を確認し、ライセンス違反とならないよう注意する必要があることを記載。

#### 第4章 情報セキュリティ対策について（例文）

7.5運用 ○法令遵守	(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、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、 <u>利用するソフトウェアにおけるライセンス規定に従わなければならない。</u>
----------------	---

# 「地方公共団体における情報セキュリティ監査に関するガイドライン」について

## 地方公共団体における情報セキュリティ監査に関するガイドライン

地方公共団体が情報セキュリティ監査を実施する際の参考としてもらうため、情報セキュリティ監査の標準的な監査手順と監査項目を示すもの。

監査項目は、「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」の対策基準に即した構成となっているため、平成15年の策定以来、「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に合わせて随時改定を行っている。

