資料４

地方公共団体の基幹業務システムのクラウド利用等に関する情報セキュリティ指針（仮称）について

総務省

令和４年６月２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)

地方公共団体の基幹業務システムのクラウド利用等に関する情報セキュリティ指針（仮称）の構成

指針策定の方向性

「地方公共団体の基幹業務システムのクラウド利用等に関する情報セキュリティ指針（仮称）」の構成については、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不足している項目を抽出することで、追加的に定めるべき情報セキュリティ対策の整理を行ってはどうか。

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（JIS Q 27001に基づき作成）

↔

クラウドサービスの提供や利用に関する管理指針（JIS Q 27017 ）

	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

↔

現行ガイドラインと比較し、クラウドサービスの利用に関して不足している項目を抽出することで、追加的に定めるべき情報セキュリティ対策を整理

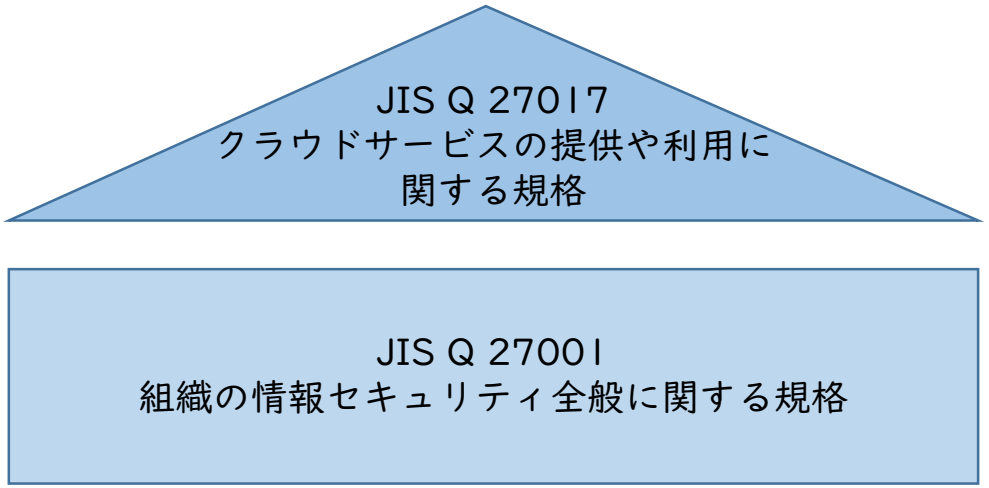
（参考）JIS Q 27001とJIS Q 27017

○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

地方公共団体の基幹業務システムのクラウド利用等に関する情報セキュリティ指針（仮称）骨子（案）①

第１章～第４章

第１章　指針の目的について
　地方公共団体情報システムの標準化に関する法律に基づく、指針の目的・位置づけを記載。

第２章　指針の範囲について
　指針で示すセキュリティ対策の範囲等を記載。

第３章　指針の構成について
　指針で示すセキュリティ対策について、国際標準等を参照し構成していることを記載。

第４章　クラウドサービスに関する留意点について
　地方公共団体がクラウドサービスを利用する際の留意点、リスク評価の重要性等について記載。

地方公共団体の基幹業務システムのクラウド利用等に関する情報セキュリティ指針（仮称）骨子（案）②

第５章

第５章　情報セキュリティ基準について

「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」における対策基準の項目ごとに、クラウドサービスを利用する際に追加的に必要となる情報セキュリティ対策の基準を記載。

１．組織体制

〇情報セキュリティインシデントに対処するための体制の設置・役割

最高情報セキュリティ責任者（CISO: Chief Information Security Officer）は、クラウドサービスにおける情報セキュリティインシデント管理についての責任分界を検証し、標準準拠アプリケーション提供事業者が、本基準の情報セキュリティインシデントに関する内容（５．人的セキュリティの項目）を満たすことを確認することを記載。

２．情報資産の分類と管理

〇情報資産の管理

クラウドサービス内に保管する情報資産の分類の表示、保管、廃棄、返却について、目録、ラベル付け等を行うことを記載。

３．情報システム全体の強靭性の向上

〇マイナンバー利用事務系

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領域についてもマイナンバー利用事務系として扱うことを記載。

地方公共団体の基幹業務システムのクラウド利用等に関する情報セキュリティ指針（仮称）骨子（案）③

第５章

４．物理的セキュリティ

〇サーバの冗長化等

クラウドサービス上で利用する標準準拠アプリケーションにおけるサーバの冗長化や同一データを保持できる仕組みの確認等、可用性を担保する仕組みについて、地方公共団体が標準準拠アプリケーション利用前に確認し、可用性が維持できる状態で利用できるのか確認することを記載。

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

クラウドサービスを利用するにあたり、責任分界の範囲と役割等の理解、クラウドサービス全般の利用における意識向上、教育及び訓練のプログラムを実施することを記載。

〇情報セキュリティインシデントの報告

標準準拠アプリケーションを利用する際に、標準準拠アプリケーションを提供する事業者又は委託事業者（運用・保守等を行う事業者）に情報セキュリティインシデント発生時の報告の仕組みについて、開示・報告を要求することを記載。

〇情報セキュリティインシデント原因の究明・記録、再発防止等

クラウドサービスの環境内で生成されるデジタル証拠となり得る情報及びその他の情報の提出要求に対応する手続について、地方公共団体は、クラウドサービスと標準準拠アプリケーションを提供する事業者、委託事業者、地方公共団体の各責任と役割を明確に定め、関係者と合意する必要があることを記載。

地方公共団体の基幹業務システムのクラウド利用等に関する情報セキュリティ指針（仮称）骨子（案）④

第５章

６．技術的セキュリティ

〇システム管理記録及び作業の確認

　クラウドサービス上での操作についてログを取得すること。ログが提供される場合は、そのログ取得機能が適切かどうか検証することを記載。

〇アクセス制御

　クラウドサービスへの利用者アクセスに関するアクセス制御方針を定める。また、情報へのアクセスをアクセス制御方針に従って制限できること及びそのような制限を実現することを確実にすることを記載。

〇 ID の管理

　クラウドサービス又は標準準拠アプリケーションを利用・運用を行う実務管理者に管理権限を与える場合、十分に強い認証技術（多要素認証等）を用いることを記載。

地方公共団体の基幹業務システムのクラウド利用等に関する情報セキュリティ指針（仮称）骨子（案）⑤

第５章

７．運用

〇緊急時対応計画の改訂

クラウドサービスを利用するにあたり、クラウドの障害発生時や情報セキュリティインシデントについての責任分界を検証し、それが地方公共団体のセキュリティポリシーを満たすことを確認すること、これらを踏まえて緊急時対応計画の改訂が必要となることを記載。

〇関係する規制等の遵守

クラウドサービスを利用するにあたり、地方公共団体は、関係する規制等に対する遵守の証拠について、標準準拠アプリケーションを提供する事業者又は委託事業者に要求すること、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ことを記載。

８．評価・見直し

〇監査

情報セキュリティポリシーの遵守について定期的に監査を行うこと。地方公共団体は、標準準拠アプリケーションを提供する事業者又は委託事業者が事前に提示した内容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こと、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）となる場合もあることを記載。

想定論点例①　クラウドサービス内に保管する情報資産の廃棄

現行のガイドラインでは、オンプレミス（ハウジング※やプライベートクラウドを含む）の場合を想定した情報資産の廃棄について言及をしているが、クラウドサービスにおけるサービス利用終了後のデータの抹消について、物理的な破壊が困難な場合のデータの抹消の在り方については記載がなされていない。

※ データセンターの設備等を提供するサービス

指針策定の方向性

クラウドサービス内の情報資産を廃棄する方法として、暗号化消去※が考えられるが、暗号化消去を認めるべきか。暗号化消去を認める場合には、留意点を検討し、地方公共団体が実施する対策を整理する必要があるのではないか。

※ 情報を電磁的記録メディアに暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる暗号鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする方法

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4.　物理的セキュリティ

(7)　機器の廃棄等

情報システム機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS及び記憶装置の初期化（フォーマット等）による方法は、ハードディスク等の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。また、原則として、以下の表に記載されている方法により、記録されている情報の機密性に応じて、情報システム機器の廃棄等を行わなければならない。なお、運用にあたっては、「情報システム機器の廃棄等時におけるセキュリティの確保について」（令和2年5月22日総行情第77号総務省自治行政局地域情報政策室長通知）を参照されたい。

想定論点例①　クラウドサービス内に保管する情報資産の廃棄

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

分類	機器の廃棄等の方法	確実な履行を担保する方法
（１）マイナンバー利用事務系の領域において住民情報を保存する記憶媒体 ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。
（２）機密性２以上に該当する情報を保存する記憶媒体（上記（１）に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（３）機密性１に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、（２）に記述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS及び記憶装置の初期化（フォーマット等）による方法は、HDDの記憶演算子にはデータの記憶が残った状態となるため、適当ではない	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。
※上記（１）は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む）		

想定論点例①　クラウドサービス内に保管する情報資産の廃棄

（参考）
一般社団法人ソフトウェア協会 データ適正消去実行証明協議会（ADEC）

第2章 暗号化消去（ CE: Cryptographic Erase）

暗号化消去（ CE ）について NISTSP800 88Rev.1 では以下のように記載しています。

- CE は、データがメディアに書き込まれるときに、最初の書き込みから暗号化が実行される場合に使うことができる抹消手法であり、データの抹消は、書き込まれたデータの上書き又は物理的な抹消ではなく、データの暗号化に使用される暗号鍵を抹消することによって行われます。
- CE は非常に高速にデータの抹消を実現することができ、部分的な抹消、例えば記録メディアの限定された一部の領域に対するデータの抹消にも利用することができます。部分的な抹消は、選択的抹消とも呼ばれ、クラウド等に用いられる大型サーバーシステム、スマートフォンやタブレット型端末などのモバイルデバイスに対しても有効なデータ抹消の方法です。

【別冊】データ消去技術ガイドブック暗号化消去技術 編（抄）
https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK_extra.pdf

想定論点例②　システム運用・保守時のインターネット経由で提供されるサービスの利用

現行のガイドラインでは、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とされているところ。

指針策定の方向性

クラウド上の標準準拠アプリケーションにおけるウイルス対策ソフト等を適用する際、クラウド上のマネージドサービス（クラウド上で提供される運用を自動化するサービス）等を利用することで地方公共団体のシステム管理、運用・保守の効率化等が期待される。

マネージドサービスを利用するには、限定的にインターネットからマイナンバー利用事務系への接続を認めることとなるが、認めるべきか。認める場合は、留意点を検討し、対策を整理する必要があるのではないか。

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）

（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。