別紙２

クラウドサービス提供における
情報セキュリティ対策ガイドライン
（第２版）

2018年　7月

総務省

目次

Ⅰ．序編

Ⅰ．１．はじめに

社会経済活動の ICT への依存が高まる中で、情報システムの構築の迅速化及び柔軟化並びに管理・運用費用の低廉化を実現する有効な手段として、クラウドサービスの利用が拡大し、社会経済活動を支える重要な ICT 基盤となっている。さらに、IoT が急速に注目を集めるようになり、本格的な IoT サービスの時代が到来しようとしている。他方、クラウドサービスでは、サービス形態、管理水準、サービスレベル等が異なる多様なサービスが提供され、クラウド利用者の選択肢が増えているにもかかわらず、情報セキュリティポリシーを満足できるクラウドサービスを適切に選択できていない場合が多い。この選択に失敗すると、クラウド利用者は情報漏えい等に直面しやすくなり、個別の是正要求もあまり受け入れられず、しかもサービスの乗り換えが難しいことが多い。

クラウドサービスの導入が本格化するに連れて、クラウドサービスの提供形態も分業が進んできた。元々は単独のクラウド事業者がサービスを提供する形態が多かったが、現在はインフラや実行環境ごとにサービスを提供する基幹事業者と、そのインフラを借り受けてアプリケーションサービスを中心にサービスを提供する事業者に分かれて協業が進んでいるほか、アプリケーションサービスを提供する事業者同士が連携してサービスを提供する事例も急増している。しかし、サービス提供形態の複雑化は、クラウド事業者によるクラウドサービス全体の統制を難しくする要因となっており、全体としてのサービスレベルの低下、ログ取得・保持やレビューの抜け漏れの発生等に直面しやすくなる。

このようなクラウドサービスを取り巻く環境の変化から生じる課題に対応するためには、クラウドサービスを安全・安心に利用するための情報セキュリティ対策が不可欠である。

本ガイドラインは、クラウド事業者が実施すべき情報セキュリティ対策を取りまとめたものである。第Ⅰ部では、「序編」として、ガイドラインの対象範囲と位置付け、利用方法等をまとめている。第Ⅱ部、第Ⅲ部では、「組織・運用編」、「物理的・技術的対策編」として、クラウドサービスの利用が企業等の生産性向上の健全な基盤となるよう、クラウド事業者における情報セキュリティ対策の促進に資するため、クラウド事業者が実施すべき情報セキュリティ対策をまとめている。ここでは自組織だけではなく、他組織との連携を考慮した、供給者関係（ICT サプライチェーン）における実務のポイントもまとめている。第Ⅳ部では、「IoT サービスリスクへの対応方針」として IoT サービスに関するリスク及び対応をまとめている。

なお、本ガイドラインは、「ASP・SaaS における情報セキュリティ対策ガイドライン」（2008 年１月）と「クラウドサービス提供における情報セキュリティ対策ガイドライン」（2014 年４月）を統合したものである。

Ⅰ．２．ガイドラインの位置付け

本ガイドラインは、クラウド事業者がクラウドサービスを提供する際に実施すべき情報セキュリティ対策のガイドラインである。クラウド事業者が提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として、可能な限り分かりやすくかつ具体的な対策項目を提示することを目指して策定されている。クラウド事業者は、本ガイドラインをそのまま利用することで、比較的容易に自ら提供するクラウドサービスに即した情報セキュリティ対策が実施できるよう構成されている。利用者との契約において、より厳しい対策を設定し実施する等、各クラウド事業者の実情に合わせて活用することも可能である。

なお、利用者がクラウド事業者との契約の範囲外で独自に利用するハードウェア及びソフトウェア（他のクラウドサービスを含む）並びに利用者が契約する通信回線及びインターネット・サービスにおける情報セキュリティ対策は、本ガイドラインの対象外である。

また、本ガイドラインは、利用者がクラウドサービスを選定する際に、クラウド事業者が実施している情報セキュリティ対策の状況を確認するための指標として活用することもできる。

参考として、クラウド事業者が参照する主なセキュリティに関するガイドラインを図表１に示す。

図表 １ クラウド事業者が参照する主なセキュリティに関するガイドライン

ガイドライン名	作成	公表年月
クラウドサービスの安全・信頼性に係る情報開示指針	総務省	2011.12 2017.3 改定
クラウドサービスの利用のための情報セキュリティマネジメントガイドライン	経済産業省	2011.4 2014.3 改定
クラウドサービス利用者の保護とコンプライアンス確保のためのガイド	ASPIC[1]	2011.7
クラウド情報セキュリティ管理基準	JASA[2]	2012.8 2016.3 改定
IoT セキュリティガイドライン Ver1.0	IoT 推進コンソーシアム・総務省・経済産業省	2016.7
サイバーセキュリティ経営ガイドライン Ver2.0	経済産業省	2015.12 2017.11 改定
重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）	内閣サイバーセキュリティセンター	2006.2 2018.4 改定
情報セキュリティサービス基準	経済産業省	2018.2

[1] 特定非営利活動法人 ASP・SaaS・IoT クラウド コンソーシアム
[2] 特定非営利活動法人 日本セキュリティ監査協会

Ⅰ．３．ガイドライン活用の効果

本ガイドラインは、クラウドサービスの特性に基づいたリスクアセスメントを実施し、クラウド事業者が実施すべき情報セキュリティ対策を取りまとめることにより、どのクラウド事業者にも実践的で取り組みやすい対策集となっている。本ガイドラインを活用することで、以下の三つの効果が見込まれる。

1.大企業と比較して、情報セキュリティ対策に人的・金銭的な資源を割くことが困難な中小のクラウド事業者に対して、独自の脅威分析の負担を軽減し、優先的に取り組むべき対策の指針を与える。

2.他のクラウドサービスと連携する際、連携クラウド事業者に対する情報セキュリティ対策の要求事項として、本ガイドラインが一定の指針となる。

3.これまで、クラウドの情報セキュリティ対策に関する明確な指針が存在しなかったため、利用者がクラウドサービスを選択するにあたり、そのクラウド事業者が実施している情報セキュリティ対策の妥当性を判断し得なかった。本ガイドラインは、利用者がクラウドサービスを選択する際の、一定の指針となる。

Ⅰ．４．ガイドラインの全体構成

本ガイドラインは、「序編」「組織・運用編」「物理的・技術的対策編」「IoT サービスリスクへの対応方針編」「参考資料」の五編から構成される。

１．序編

本ガイドラインの目的、対象とする範囲、利用方法、注意事項、用語の定義等を取りまとめた、「組織・運用編」「物理的・技術的対策編」をより良く活用するための導入編。

２．組織・運用編

情報セキュリティを確保するために求められる運用管理体制、外部組織との契約における留意事項、利用者に対する責任等の、組織・運用に係る対策を取りまとめた対策集。主に、経営者等の組織管理者によって参照されることを想定している。

３．物理的・技術的対策編

クラウドの典型的なシステム構成を基に、各構成要素[3]における情報資産[4]に対する情報セキュリティ対策を取りまとめた対策集。構成要素は「アプリケーション、プラットフォーム、サーバ・ストレージ」「ネットワーク」「建物、電源（空調等）」の三つに大きく分類し、どの構成要素にも属さない情報資産を「その他」としている。主に、実際にクラウドサービスを運用している現場の技術者等によって参照されることを想定している。

４．IoT サービスリスクへの対応方針編

IoT サービスリスクを詳しく解説するとともに、IoT サービスをモデル化するツールを提供し、これらのモデルに基づいて対処すべきリスクや分担すべき責任・役割を整理できる手順を説明する。この手法を適用することで、クラウド事業者が、自ら担う役割や運用する機材・IT 基盤・アプリケーション・要員等に従って取るべきリスク対策を容易に選択できる仕組みを提供する。

---

[3] 「Ⅰ．６ 用語の定義」参照。

[4] 「Ⅰ．６ 用語の定義」参照。「構成要素における情報資産」とは、サーバ等の構成要素及びサーバ上のデータ、ログ等の情報そのものを指すこととなる。

５．参考資料

本ガイドラインには参考資料として Annex 1 から Annex8 までを付属している。

Annex１・２は、『Ⅱ.組織・運用編』及び『Ⅲ.物理的・技術的対策編』それぞれの対策を一覧表にしたものであり、対策を実施する際の実施計画や実績管理等に使用できるようになっている。これらの資料についても、適宜参照されたい。

Annex３は、クラウドサービスの典型的な構成要素を図式化し、対策の対象となる情報資産を例示したものである。また、クラウドサービス種別のパターン化に関する解説を行っている。これらの資料についても、適宜参照されたい。

Annex４「利用者接点と ICT サプライチェーンに着目したクラウドサービスの特徴」は、クラウドサービス提供における供給者モデル及び利用者接点の実務の五つの観点について詳述しているので、適宜参照されたい。

Annex５「利用者接点と ICT サプライチェーンに着目した要求事項」は、ISO/IEC27002 との紐付けと利用者接点や ICT サプライチェーンに着目した要求事項について記述しているので、詳細理解の際に参照されたい。なお、クラウドサービスの提供に関わらない対策項目に対しては、ISO/IEC27002 との紐付けは行われていない。

Annex６「利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策」は、利用者・事業者連携インターフェイスの実務指針・ベストプラクティスとして参照・活用されたい。なお、クラウドサービスの提供に関わらない対策項目に対しては、ISO/IEC27002 との紐付けは行われていない。

Annex7「クラウド事業者が過度の責任を負わないための注意点」は、IoT 機器のコンポーネントリスクの処理戦略（①IoT 機器を自ら提供する、②IoT 機器は推奨に留め提供しない、について具体的な理解を助けるためのユースケースを例示）、モノのリスクと責任分担の基本、クラウド事業者が把握できていない「繋がり」におけるリスクについて記述しているので、適宜参照されたい。

Annex8「【事例集】 調査テンプレートの記入例」は、クラウド事業者の IoT サービスリスクに対する対応策の理解を深めることを目的として、特徴の異なる六つの IoT サービスを事例として記入例を提示しているので、適宜参照されたい。

Ⅰ．５．ガイドラインの利用方法

本ガイドラインを基に具体的な情報セキュリティ対策を実施する場合は、以下の手順に従って利用されたい。その際、利用手順を示す図表２を併せて参照すると良い。

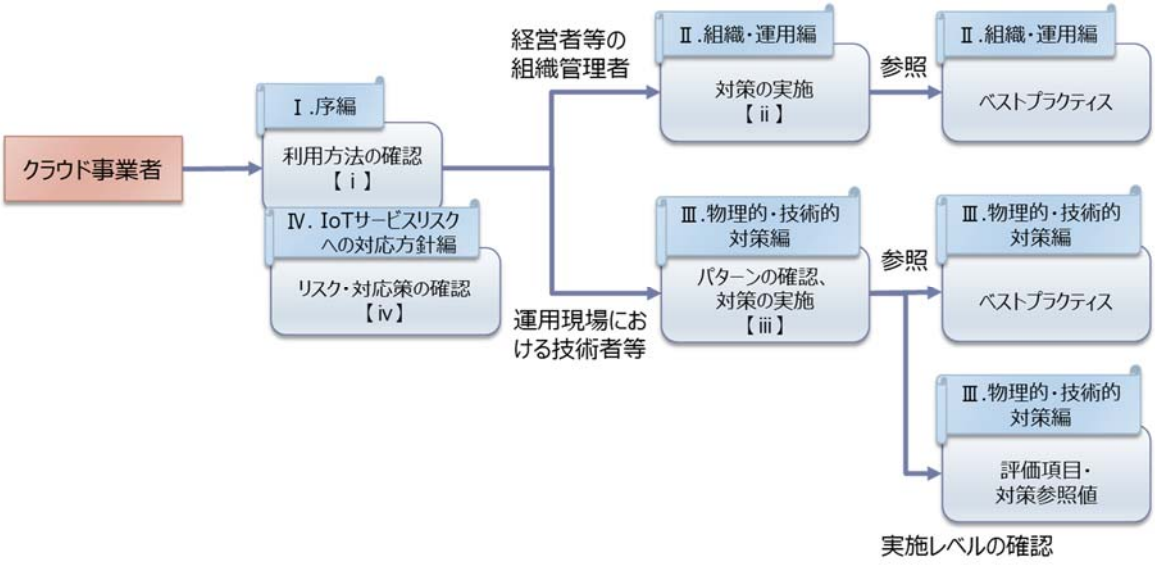
・経営者等の組織管理者

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。
ii. 『Ⅱ.組織・運用編』の対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。また、併せて Annex６も参照すると良い。
iv. 『Ⅳ.IoT サービスリスクへの対応方針編』を確認し、IoT サービスならではのリスクを理解、事例等を確認する。

・運用現場における技術者等

i. 『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。
iii. 『Ⅲ.物理的・技術的対策編』に基づき、自らが提供するクラウドサービスがどのパターンに該当するかを確認し、自分のパターンに該当する対策を実施する。「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。対策を実施する際には、ベストプラクティスを参照すると良い。また、評価項目を使用し、対策参照値を目安に対策の実施レベルを判断することができる。また、併せて Annex６も参照すると良い。
iv. 『Ⅳ.IoT サービスリスクへの対応方針編』に基づき、IoT サービスならではのリスクに対する対応策を確認し、具体的に実施することが望ましい。

図表２　利用手順



なお、「Ⅱ．組織・運用編」及び「Ⅲ．物理的・技術的対策編」では、以下１．から５．の各項目の意味をよく理解し、自らが行うべき情報セキュリティ対策を判定し、実施されたい。

１．対策項目（「Ⅱ．組織・運用編」及び「Ⅲ．物理的・技術的対策編」共通）

クラウド事業者が実施すべき情報セキュリティ対策事項。認証基準等で用いられるような実施必須事項を示すものではなく、情報セキュリティ対策を実施する上での指標となることを期待している。

２．基本・推奨（「Ⅱ．組織・運用編」及び「Ⅲ．物理的・技術的対策編」共通）

対策を「基本」と「推奨」に分類することで、対策実施の優先度を示している。

・基本：クラウドサービスを提供するにあたり、優先的に実施すべき情報セキュリティ対策
・推奨：クラウドサービスを提供するにあたり、実施することが望まれる情報セキュリティ対策

３．ベストプラクティス（「Ⅱ．組織・運用編」及び「Ⅲ．物理的・技術的対策編」共通）

対策を実施するにあたっての、具体的な実施手法や注意すべき点をまとめた参考事例。

４．評価項目（「Ⅲ．物理的・技術的対策編」のみ）

対策項目を実施する際に、その実施レベルを定量的あるいは具体的に評価するための指標。SLA[5]の合意事項として活用されることも想定される。

５．対策参照値（「Ⅲ．物理的・技術的対策編」のみ）

対策項目の実施レベルの目安となる評価項目の値で、パターンごとに設定されている。特に達成することが必要であると考えられる値については「＊」を付している。また、評価項目によっては、対策参照値が「-」となっているパターンが存在するが、これについては、クラウド事業者が任意に対策参照値を設定することで、対策項目の実施レベルを評価されたい。

[5] Service Level Agreement。クラウド事業者が利用者と締結するサービス品質保証契約。

Ⅰ．６．用語の定義

1. アグリゲーションサービス

   複数の供給者が提供するクラウドサービスを集積し、一つのクラウドサービスとして利用できるようにしたサービス形態。

2. アグリゲーションサービス事業者

   アグリゲーションサービスを提供するクラウド事業者。クラウド利用者との契約は、アグリゲーションサービス事業者が一括して行う。

3. エッジサービス

   IoT 機器・システムの近くにサーバを設置し、通信プロトコルの変換、遅延の少ない情報処理、セキュリティ強化、伝達するデータの絞込み等の機能を提供するサービスのこと。サーバは、IoT 機器・システムが設置される場所（企業の工場内等）と同じ場所に設置されることが多い。

4. エンドユーザ

   クラウドサービスの提供は行わず、クラウドサービスの利用のみを行う者。個人を示す場合は、エンドユーザ（個人）、組織を示す場合はエンドユーザ（組織）と表記することがある。本ガイドラインでは、エンドユーザ（組織）の中に個人事業主を含めている。

5. 外部組織

   連携クラウド事業者やクラウド事業者からサービスの一部を委託された企業等、クラウドサービスの提供にあたり契約関係のある組織の総称。

6. 外部ネットワーク

   情報処理施設とその外部とを結ぶネットワークの総称で、クラウド事業者と ISP 間、クラウド事業者と連携クラウド事業者間、クラウド事業者の保守管理用回線等を指す。本ガイドラインの対象外である、利用者が契約する通信回線及びインターネット・サービスは除く。

7. 可用性(JIS Q 27001 を基に定義)

   認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

8. 完全性(JIS Q 27001 を基に定義)

   資産の正確さ及び完全さを保護する特性。

9. 管理策(JIS Q 27001 を基に定義)

   リスクを管理する手段（方針、手順、指針、実践又は組織構造を含む。）であり、実務管理的、技術的、経営的又は法的な性質をもつことがあるもの。

10. 管理責任者

    クラウドサービスの提供に使用する設備の運用管理を担当する現場責任者。

11. 危害

    人の受ける物理的障害若しくは健康障害又は環境の受ける害（ISO/IEC Guide 51:2014 “Safety aspects: Guidelines for their inclusion in standards”を参考に定義）。

12. 機密性(JIS Q 27001 を基に定義)

認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。

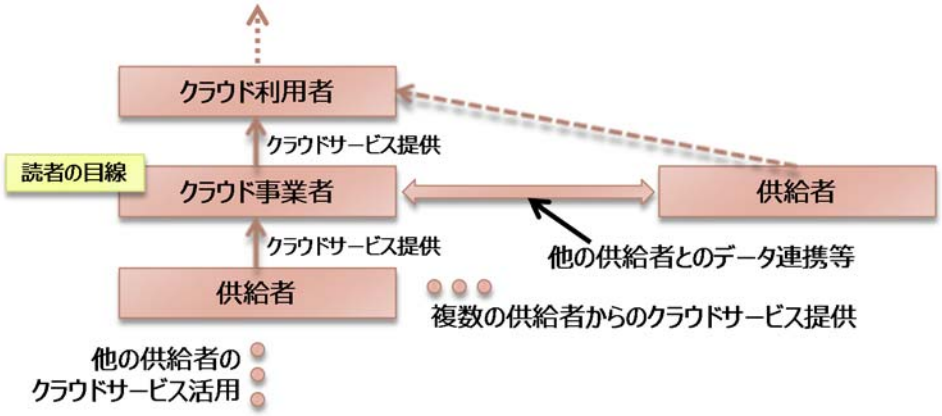
13. 脅威(JIS Q 27001 を基に定義)

組織に損害や影響を与えるリスクを引き起こす要因。

14. 供給者

ICT サプライチェーンの一部を構成し、クラウド事業者とデータ、サービス等で連携する組織。

（例）データ連携：クラウド事業者と供給者及び供給者間で行われる各々のデータベース間のデータ連携等、サービス連携：供給者からクラウド事業者及び他の供給者から供給者へのクラウドサービス提供等。



15. 供給者連携

クラウド利用者の利便性を向上するため、ICT サプライチェーンを構成するクラウド事業者と供給者（供給者が複数に渡る場合もある）が行うデータ、サービス等の連携。

16. 業務プロセス

クラウドサービスを提供するために行われる一連の活動。

17. クラウドコンピューティング

利用者による共有が可能であり、利用者の要求に応じたセルフサービス提供と管理の機能を併せ持つ、拡張性と弾力性に富んだ物理又は仮想資源のプールに、ネットワークを通じてアクセスすることを可能にする情報処理形態。

18. クラウドサービス

提供形態から、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）及びSaaS（Software as a Service）に分ける。

また、実現形態から、プライベートクラウド、パブリッククラウド及びハイブリッドクラウドに分けることができる。

・ プライベートクラウド：

クラウドサービスを、企業の情報セキュリティ管理区域内に閉じたシステム構成で提供。自

社開発システムとほぼ同様の運用管理方法で利用可能。利用者の要求に即した運用管理やカスタマイズが可能。

・ パブリッククラウド：

クラウドサービスを、企業の情報セキュリティ管理区域外に構築されたシステムにより提供。

・ ハイブリッドクラウド：

プライベートクラウドとパブリッククラウドの両者を組み合わせたクラウドサービス。

19. クラウド事業者

クラウドサービスをクラウド利用者に提供する組織。クラウドサービスを提供するため、別の組織である供給者から別のクラウドサービスの提供を受けて活用することや、供給者とのデータ連携等を行うこともある。

20. クラウド事業者のセキュリティ管理に係る内部統制保証報告書

受託業務（クラウドサービス）を提供するクラウド事業者の、セキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制を、クラウド利用者に対して保証する目的で、監査人等が作成する報告書のこと。クラウド利用者は、クラウド事業者からこの報告書の提供を受けることで、クラウド事業者を管理監督する責任を代替できる。

「クラウド事業者のセキュリティ管理に係る内部統制保証報告書」としては、我が国では、日本公認会計士協会が実務指針を公開した IT 委員会実務指針第 7 号「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書」（本ガイドラインでは「IT 実 7 号」という。）がある。海外では、米国で実務指針が策定された、サービス・オーガニゼーション・コントロール報告書（本ガイドラインでは「SOC2」という。）等がある。

21. クラウド事業者の内部統制保証報告書

財務報告に関連する受託業務（クラウドサービス）を提供するクラウド事業者の内部統制を、クラウド利用者に対して保証する目的で、監査人等が作成する報告書のこと。クラウド利用者は、クラウド事業者からこの報告書の提供を受けることで、クラウド事業者を管理監督する責任を代替できる。「クラウド事業者の内部統制保証報告書」の利用は、クラウド事業者の経営者、クラウド利用者及びその監査人に限定されている。

「クラウド事業者の内部統制保証報告書」としては、我が国では、日本公認会計士協会が実務指針を公開した監査・保証実務委員会実務指針第 86 号「受託業務に係る内部統制の保証報告書」（本ガイドラインでは「監保実 86 号」という。）がある。海外では、米国公認会計士協会（AICPA）が実施基準（米国保証業務基準書第 16 号）を策定した「ISAE3402/SSAE16 報告書」等がある。

22. クラウド利用者

クラウドサービスを利用する組織。エンドユーザ（組織）と、クラウドサービスを提供するため別の組織が提供するクラウドサービスを利用する組織に分かれる。

23. 構成要素

クラウドサービスの提供に用いるハードウェア、ソフトウェア、通信機器・回線、建物等の固定資産。

24. 個別契約連携クラウドサービス

ICT サプライチェーンでクラウドサービスを提供する際に、アグリゲーションサービスを編成せず、クラウド事業者や各供給者が個別にクラウド利用者と契約を締結するサービス形態。本ガイドラインでは、ICT サプライチェーン構築にあたり、ID 連携、機能連携、データ連携等を行う場合は、個別に仕組みを構築して連携を実現するもののみを、個別契約連携クラウドサービスの対象としている。

25. 個別契約連携クラウド事業者

個別契約連携クラウドサービスを提供するクラウド事業者。

26. コンポーネント

IoT サービスの構成要素であって、リスクを列挙する際の単位。IoT 機器、ローカル側（LAN 等）、ネットワーク・クラウド側（WAN 等）、アプリケーション（組込みアプリケーション等）がある。

27. サーバ・ストレージ

クラウドサービスを提供する際に利用するアプリケーション等を搭載する機器及びアプリケーション上の情報を蓄積・保存するための装置の総称。なお、付随する OS 等の基盤ソフトウェア、蓄積されているデータ・ログ等の情報を含む。

28. 従業員

クラウド事業者に所属し、当該クラウド事業者の提供するクラウドサービスの提供に携わる者で経営陣を除く者。派遣社員、アルバイト等を含む。

29. 情報開示

電子メール、電子ファイル、FAX、紙文書等の手段による、受領者に対する情報の引き渡し。

30. 情報公開

一般に向けた又は範囲を限定した、情報の公表・周知。

31. 情報資産

構成要素及び構成要素を介する情報。

32. 情報処理施設

クラウド事業者がサービスを提供するための設備が設置された建物。

33. 情報セキュリティ(JIS Q 27001 を基に定義)

情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。

34. 情報セキュリティインシデント(JIS Q 27001 を基に定義)

望ましくない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。

35. 情報セキュリティ事象(JIS Q 27001 を基に定義)

システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示していることをいう。

36. 情報セキュリティ対策機器

ファイアウォール、IDS 等、コンピュータウイルスや不正アクセス等の情報セキュリティ事象から、クラウド事業者の設備を防護するための機器。

37. 情報セキュリティポリシー

情報セキュリティに関する組織的取組についての基本的な方針及び情報セキュリティ対策における具体的な実施基準や手順等の総称。

38. 情報提供

情報公開、又は情報開示の実施。

39. ぜい弱性(JIS Q 27001 を基に定義)

脅威によって悪用される可能性がある欠陥や仕様上の問題。

40. 通信機器

ルータ、スイッチ等、通信を制御するための装置

41. データ流通市場

IoT サービスが生み出すビッグデータを相互に流通させることができる市場のこと。

42. 特権ユーザ

特権的な管理ツールの使用を許可された個人。クラウド事業者とクラウド利用者のどちらに所属するかは問わない。

43. フォグサービス

IoT 機器・デバイス（又はエッジサービス）とクラウドを結ぶインターネット上に、情報処理・ストレージ等のリソースを分散配置し、クラウド機能の一部を分担又は拡張することで、リソース配置の最適化と IoT サービス利用者に提供する付加価値向上を実現するサービスのこと。

44. プラットフォーム

認証、決済等の付加的機能を提供する、クラウドサービスで提供されるアプリケーションの基盤。

45. 物理時セキュリティ境界

情報処理施設の特定の領域を保護するために設置される壁、カード制御による出入口等の物理的な仕切り。

46. ユーザサポート

クラウドサービスに関する問い合わせ窓口（ヘルプデスク）とクラウドサービスの品質や継続性を維持するための組織の総称。

47. リスク(JIS Q 27001 を基に定義)

事象の発生確率と事象の結果との組合せ（目的に対して不確かさが与える影響）。

48. リスクアセスメント(JIS Q 27001 を基に定義)

リスク分析からリスク評価までの全てのプロセス。

49. リスク分析(JIS Q 27001 を基に定義)

リスク因子を特定するための、及びリスクを算定するための情報の系統的使用。

50. 利用者

クラウドサービスを利用する法人又は個人。

51. 利用者接点

クラウド利用者とクラウド事業者の間に存在する、資産・サービス等に係る責任・役割等の分担の境界、情報提供のインターフェイス等。

52. 連携クラウド事業者

自らのクラウドサービスに他のクラウドサービスを組み込むことにより、アプリケーション間の統合・連携を実施する際に、他のクラウドサービスを提供するクラウド事業者。

53. ロール

IoT サービスの提供にあたり必要となる役割のこと。IoT サービスの環境を整備・維持するロール（「利用者契約」「機器等提供」「機器等推奨」「構成管理」「契約管理」「データ監視・保全」）と IoT サービスを実行するためのロール（「計測」「ローカル伝送」「前処理」「インターネット接続」「取得」「集約・保管」「処理・分析」「表示・データ・コマンド提供」「データ外部提供」「駆動前処理」「駆動」）からなる。クラウド事業者がどのロールを担い責任を負うかは、個々のサービス毎に異なる。

54. IaaS（Infrastructure as a Service）

CPU、メモリ、ストレージ、ネットワークなどのハードウェア資産をサービスとして提供するクラウドサービス。

55. ICT サプライチェーン

クラウド事業者と供給者、並びに供給者間において、データ、サービス等で連携してクラウドサービスを提供する際に構築される、各事業者の情報処理施設がネットワークで連結された形態

56. IoT（IoT セキュリティガイドライン Ver1.0 を基に定義）。

情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラのこと。

57. IoT 機器

IoT を構成するネットワークに接続される機器のこと。通信を行う以外の主たる機能としては、計測（センサー）、制御（アクチュエータ）がある。センサー及びアクチュエータは、機器本体と通信・制御部の組み合わせで構成されるものである。ただし、制御部が外部コンピュータとして独立しているものはローカルコンピュータと呼ぶ。

58. IoT サービス

IoT サービス事業者が IoT 機器等を用いて提供するサービスのこと。

59. IoT サービスインテグレータ

IoT サービスを提供するため、準備した機器等を構築する企業等。

60. IoT サービス事業者

IoT サービス利用者に IoT サービスを提供する企業等。IoT サービスインテグレータとは必ずしも一致しない。

61. IoT サービスの類型図

IoT 機器・システム、エッジ/フォグサービス、クラウド（プラットフォーム・ストレージ、アプリケーション）等をネットワークで接続して、サービス・データ又は制御コマンドを IoT サービス利用者やデータ流通市場に提供する構造のこと。

62. IoT サービスモデル

システム・ネットワーク構造に基づくロールの配置と各ロールを担う関係企業等（クラウド事業者を含む。）の対応付けを示したもの。

63. IoT サービス利用者

IoT サービスを利用する企業等のこと。ただし、IoT サービスを利用する企業等が、サービスの契約者と異なる場合がある。

本ガイドラインでは、IoT サービスやクラウドサービスの利用者が消費者（個人）である場合を対象としていない。一方で、IoT サービス利用者（企業等）が、IoT サービスを利用して消費者にサービスを提供する場合は対象としている。

64. PaaS（Platform as a Service）

オペレーティングシステムや、アプリケーションの実行環境（開発環境を含む）をサービスとして提供するクラウドサービス。

65. SaaS（Software as a Service）

アプリケーションをサービスとして提供するクラウドサービス。

66. SLA（Service Level Agreement）

書面にしたサービス提供者と顧客との合意であって、サービス及び合意したサービスレベルを記述したもの（JIS Q 20000-1:2007）。

Ⅰ．７．参考文書

- JIS Q 27001:2006 (ISO/IEC 27001:2005)
- JIS Q 27001:2014 (ISO/IEC 27001:2013)
- JIS Q 27002:2006 (ISO/IEC 17799:2005)
- JIS Q 27002:2014 (ISO/IEC 27002:2013)
- JIS Q 27017:2016 (ISO/IEC 27017:2015)
- JIS Q 13335-1:2006
  （MICTS-1 : Management of Information and Communications Technology Security−Part1）
- MICTS-2[6]
  （Management of Information and Communications Technology Security−Part2）
- 総務省「公共 IT におけるアウトソーシングに関するガイドライン」
- 財団法人 金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書 第７版」

[6] ISO/IEC 27005 として 2011 年に規格化。

Ⅱ．組織･運用編

【凡例】

対策項目

クラウド事業者が実施すべき情報セキュリティ対策事項。認証基準等で用いられるような実施必須事項を示すものではなく、情報セキュリティ対策を実施する上での指標となることを期待している。

基本・推奨

対策を「基本」と「推奨」に分類することで、対策実施の優先度を示している。

・基本：クラウドサービスを提供するにあたり、優先的に実施すべき情報セキュリティ対策

・推奨：クラウドサービスを提供するにあたり、実施することが望まれる情報セキュリティ対策

ベストプラクティス

対策を実施するにあたっての、具体的な実施手法や注意すべき点をまとめた参考事例。

Ⅱ．１．情報セキュリティへの組織的取組の基本方針

Ⅱ．１．１．組織の基本的な方針を定めた文書

Ⅱ．１．１．１．【基本】

経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。

【ベストプラクティス】

i. 情報セキュリティに関する組織的取組とは、経営陣主導で組織全体が自ら定めた指針、ルール、具体的手続・手順等に従って、情報セキュリティ向上の実現に取り組むことを言う。

ii. 作成した情報セキュリティに関する組織的取組についての基本的な方針（以下「情報セキュリティに関する基本的な方針」という。）を定めた文書について、全ての従業員及び利用者並びに外部組織に対して公表し、通知することが望ましい。その際、事業所内の多くの場所に見やすく掲示する等、利用、理解しやすい形で、適切に知らせることが望ましい。

iii. 情報セキュリティに関する基本方針を定めた文書には、次の事項に関する記述を含めることが望ましい。

a) 情報セキュリティの定義、目的及び適用範囲
b) 事業戦略や事業目的に照らし合わせて、経営陣が情報セキュリティの重要性をどう考えているか
c) 経営陣が情報セキュリティへの組織的取組の目標と原則を支持していること
d) 体制の構築と情報資産保護への取組の宣言
e) 組織における遵守事項の宣言
    1) 法令、規制等の遵守
    2) 教育・訓練の実施
    3) 事件・事故の予防と対応への取組
    4) 管理責任者や従業員の義務
f) 見直し及び改善への取組の宣言　等

Ⅱ．１．１．２．【基本】

情報セキュリティに関する基本的な方針を定めた文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。この見直しの結果、変更の必要性が生じた場合には、経営陣の承認の下で改定等を実施すること。

Ⅱ．２．情報セキュリティのための組織

Ⅱ．２．１．内部組織

Ⅱ．２．１．１.【基本】

経営陣は、情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行うこと。

【ベストプラクティス】

i. 情報セキュリティに関する取組にあたっては、必要となる調整（各種判断や連絡・指示、協力等）が適切に行われるよう、関連する役割及び職務機能を持つ代表者（CIO[7]、CISO[8]等）を定めることが望ましい。
ii. 組織の規模によっては、取締役会などが CIO、CISO 等の役割を担ってもよい。
iii. 経営陣は、情報セキュリティに関する専門的な助言が必要と判断した場合には、CISO や内部の情報セキュリティ専門技術者（CSIRT 等）又は必要に応じて外部の専門家から助言を受け、その結果をレビューした上、組織内で調整することが望ましい。
iv. 経営陣は、情報セキュリティに関する取組にあたり、情報セキュリティ人材の育成を行うことが望ましい。

Ⅱ．２．１．２.【基本】

従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。

Ⅱ．２．１．３.【基本】

情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。

[7] Chief Information Officer（最高情報責任者）
[8] Chief Information Security Officer（最高情報セキュリティ責任者）

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

6.1 内部組織

【目的】組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

6.1.1 情報セキュリティの役割及び責任

【管理策】全ての情報セキュリティの責任を定め、割り当てることが望ましい。

6.1.2 職務の分離

【管理策】相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　198 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　226～227 ページを参照

Ⅱ．２．２．外部組織（データセンタを含む）

Ⅱ．２．２．１．【基本】

外部組織が関わる業務プロセスにおける情報資産に対するリスクを識別し、適切な対策を実施すること。

【ベストプラクティス】

i. 情報資産に対するリスクとしては、不正アクセス、情報資産の盗難・不正変更、情報処理設備の悪用・破壊等がある。

ii. これらのリスクを軽減するために、外部組織（特に、データセンタ、電気通信事業者、情報セキュリティサービス提供事業者等）による情報資産へのアクセスを、各クラウド事業者の実環境に合わせて管理・制限することが望ましい。以下に、情報資産にアクセス可能な外部組織を例示する。

   a) 情報処理施設に定期・不定期に出入りする外部組織（配送業者、設備点検等）
   b) 情報処理施設に常駐する外部組織（SE、警備会社等）
   c) ネットワークを通じサービスを提供する外部組織（連携クラウド事業者、ネットワーク監視サービス等）

iii. 情報資産へアクセスする手段を区別し、それぞれに対してアクセスを管理・制限する方針と方法を定めることが望ましい。

Ⅱ．２．２．２．【基本】

情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。

【ベストプラクティス】

i. 外部組織によるアクセス手法としては、以下のようなものが想定される。

   a) 物理的セキュリティ境界からの入退室
   b) 情報システムの管理用端末の利用
   c) 外部ネットワークからの接続
   d) データを格納した媒体の交換

ii. クラウドサービスの提供にあたっては、連携クラウド事業者等外部組織が多岐に渡ることが多いため、契約の締結を慎重に行うことが望ましい。

Ⅱ．３．連携クラウド事業者に関する管理

Ⅱ．３．１．連携クラウド事業者から組み込むクラウドサービスの管理

Ⅱ．３．１．１．【基本】

連携クラウド事業者が提供するクラウドサービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携クラウド事業者によって確実に実施されることを担保すること。

【ベストプラクティス】

i. 連携クラウド事業者からクラウドサービスの提供を受ける場合には、情報セキュリティに係る取決めを連携クラウド事業者が確実に実施するように、契約や SLA を締結することが望ましい。

ii. 連携クラウド事業者の提供するサービス内容が、同意なしに変更される等、サービスレベルが要求を満たさないことが無いように、契約や SLA を締結することが望ましい。

Ⅱ．３．１．２．【基本】

連携クラウド事業者が提供するクラウドサービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。

【ベストプラクティス】

i. 連携クラウド事業者が提供するクラウドサービスの確認及びレビューの実施例としては、連携クラウド事業者との契約等において、SLA 項目の計測方法及び計測結果を定期報告するように義務付けるとともに、定期的に実施結果を確認するという方法が考えられる。

ii. 連携クラウド事業者に起因する情報セキュリティインシデント及び問題点について、自らのログ記録により監査できるようにすることが望ましい。

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

１５.１供給者関係における情報セキュリティ

【目的】供給者がアクセスできる組織の資産の保護を確実にするため。

１５.１.１供給者関係のための情報セキュリティの方針

【管理策】組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化することが望ましい。

１５.１.３ICT サプライチェーン

【管理策】供給者との合意には、情報通信技術（以下、ICT という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５ 216～217 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６ 253～254 ページを参照

１５.２供給者のサービス提供の管理

【目的】供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。

１５.２.１供給者のサービス提供の監視及びレビュー

【管理策】組織は、供給者のサービス提供を定常的に監視し、レビューし、監査することが望ましい。

１５.２.２供給者のサービス提供の変更に対する管理

【管理策】関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５ 218 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６ 254～255 ページを参照

Ⅱ．４．情報資産の管理

Ⅱ．４．１．情報資産に対する責任

Ⅱ．４．１．１．【基本】

取り扱う各情報資産について、管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。

【ベストプラクティス】

i. 情報資産の目録を作成し、情報セキュリティインシデントから復旧するために必要な全ての情報を記載することが望ましい。
   例： 種類、形式、所在、バックアップ情報、ライセンス情報、業務上の価値 等
ii. 情報資産の目録における記載内容は、他の目録における記載内容と整合がとれていることが望ましい。また、不必要に重複しないことが望ましい。
iii. 情報資産の分類方法と各情報資産の管理責任者を定め、組織内での合意の下に文書化することが望ましい。
iv. 情報資産の重要度を業務上の価値に基づいて定め、組織内での合意の下に文書化することが望ましい。
v. 情報資産の保護のレベル（例：機密性・完全性・可用性に対する要求レベル）を各情報資産が直面するリスクの大きさに基づいて定め、組織内での合意の下に文書化することが望ましい。
vi. 全ての従業員及び外部組織に対して、情報資産の利用の許容範囲に関する規則に従うよう、義務付けることが望ましい。

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

８．１資産に対する責任

【目的】組織の資産を特定し、適切な保護の責任を定めるため。

８．１．１資産目録

【管理策】情報及び情報処理施設に関連する資産を特定することが望ましい。また、これらの資産の目録を、作成し、維持することが望ましい。

８．１．２資産の管理責任

【管理策】目録の中で維持される資産は、管理されることが望ましい。

８．１．５クラウド利用者から預託された情報の返却（※）

【管理策】クラウド利用者がクラウドサービスの利用を終了するにあたり、預託された情報を、クラウド利用者が取扱うことができる形でクラウド利用者に返却し、クラウドサービスの提供に供する情報処理施設等から二度と取り出せないようにすることが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　201 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　233～234 ページを参照

１２．３　バックアップ

【目的】データの消失から保護するため。

１２．３．１情報のバックアップ

【管理策】情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　210 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　246 ページを参照

（※）ISO/IEC27002 に記載は無いが、クラウドサービス提供の観点から、管理策を提示したもの

Ⅱ．４．２．情報の分類

Ⅱ．４．２．１．【基本】

組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。

【ベストプラクティス】

i. 情報資産の分類結果は、ラベル付け等により、従業員に対して明示することが望ましい。

ii. 情報資産の分類及び保護管理策の選定においては、情報資産の共有又は利用制限に係る業務上の必要性とこれにより生じる影響を考慮することが望ましい。

iii. 情報資産の分類は複雑すぎないことが望ましい（管理コストの増加をきたすため）。

iv. 外部組織からの文書に付いている分類ラベルは、定義が異なることがあるので、名称が同じか又は類似していたとしても、その解釈には注意する必要がある。

v. 情報資産の分類レベルごとに、安全な取扱い手順（処理・保存・伝達・秘密解除・破棄等）を定めることが望ましい。

vi. 取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを付与することが望ましい。システム出力の例としては、印刷された文書、スクリーン表示、記録媒体（例えば、テープ、ディスク、CD）、電子的なメッセージ及び転送ファイル等がある。

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

８.２　情報分類

【目的】組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

８.２.１情報の分類

【管理策】情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類することが望ましい。

８.２.３資産の取扱い

【管理策】資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　202 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　234～235 ページを参照

Ⅱ．４．３．情報セキュリティポリシーの遵守、点検及び監査

Ⅱ．４．３．１．【基本】

各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。

【ベストプラクティス】

i. 管理責任者は、レビュー及び見直しの方法をあらかじめ定めておくことが望ましい。

ii. 管理責任者が実施したレビュー及び見直しの結果を記録し、その記録を保管管理することが望ましい。

Ⅱ．４．３．２．【基本】

クラウドサービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること。

【ベストプラクティス】

i. 点検・監査は、十分な技術的能力及び経験を持つ内部の者（例：情報処理安全確保支援士資格を持ち、情報セキュリティに係る技術的対策の実務を一定年数以上経験している者）又は必要に応じて外部の専門家の監督の下で行うことが望ましい。

ii. 情報システムの点検・監査にあたっては、クラウドサービスの提供中断によるリスクを最小限に抑えるよう、考慮することが望ましい。

１２.７情報システムの監査に対する考慮事項

【目的】運用システムに対する監査活動の影響を最小限にするため。

１２.７.１情報システムの監査に対する管理策

【管理策】運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　213 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　250～251 ページを参照

１８.２情報セキュリティのレビュー

【目的】組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

１８.２.１情報セキュリティの独立したレビュー

【管理策】情報セキュリティ及びその実施の管理（例えば、情報セキュリティの管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、または、重大な変化が生じた場合に、独立したレビューを実施することが望ましい。

１８.２.２情報セキュリティのための方針群及び標準の順守

【管理策】権利者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューすることが望ましい。

１８.２.３技術的順守のレビュー

【管理策】情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューすることが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　223～224 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　261～262 ページを参照

Ⅱ．５．従業員に係る情報セキュリティ

Ⅱ．５．１．雇用前

Ⅱ．５．１．１．【基本】

雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。

【ベストプラクティス】

i. 雇用条件には、情報セキュリティに関する基本的な方針を反映させることが望ましい。

ii. 雇用条件では、次の事項を明確に記述することが望ましい。

a) 取扱注意情報へのアクセス権を与えられる全ての従業員に対して、アクセスが認められる前に、秘密保持契約書又は守秘義務契約書に署名を求める

b) 従業員の法的な責任と権利

c) 従業員が担うべき情報資産に対する責任

d) 雇用契約を締結する過程で取得した個人情報の扱いに関する組織の責任

iii. 雇用終了後も、一定期間は雇用期間における責任が継続するよう、雇用条件を規定することが望ましい。

Ⅱ．５．２．雇用期間中

Ⅱ．５．２．１．【基本】

全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。

Ⅱ．５．２．２．【基本】

従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えること。

【ベストプラクティス】

i. 雇用条件において、従業員が情報セキュリティポリシー等に従わない場合の対応手続等を明確にすることが望ましい。

Ⅱ．５．３．雇用の終了又は変更

Ⅱ．５．３．１．【基本】

従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にすること。

【ベストプラクティス】

i. 雇用終了時には、支給したソフトウェア、電子ファイル等の電子媒体、会社の書類、手引書等の紙媒体、モバイルコンピューティング装置、アクセスカード等の設備等、全ての返却を求めることが望ましい。
ii. 雇用終了後には、情報資産に対する個人のアクセス権を速やかに削除することが望ましい。
iii. 雇用の変更を行う場合には、新規の業務に対して承認されていない全てのアクセス権を削除することが望ましい。
iv. アクセス権の削除に当たっては、情報システムへの物理的なアクセスキー（情報処理施設の鍵、身分証明書等）及び電子的なアクセスキー（パスワード等）等を返却・消去することが望ましい。
v. 雇用終了後には、組織の現行の一員であることを認定する書類から削除することが望ましい。
vi. 雇用が終了又は変更となる従業員が、稼働中の情報システム等の情報資産にアクセスするために必要なアクセスキーを知っている場合には、雇用の終了又は変更時に当該情報資産へのアクセスキーを変更することが望ましい。

Ⅱ．６．情報セキュリティインシデントの管理

Ⅱ．６．１．情報セキュリティインシデント及びぜい弱性の報告

Ⅱ．６．１．１．【基本】

全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施を要求すること。 報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。

【ベストプラクティス】

i. 情報セキュリティインシデント及びぜい弱性をハンドリングする組織（CSIRT 等）と連携して情報セキュリティインシデントの正式な報告手順を、報告を受けた後のインシデント対応及び段階的取扱い（例：原因切り分け、部分復旧、完全復旧のフェーズに分けた取扱い）の手順と共に確立することが望ましい。また、情報セキュリティインシデントの報告手順は全ての従業員に周知徹底することが望ましい。

ii. 情報セキュリティインシデント報告のための連絡先を明確にすることが望ましい。さらに、この連絡先を全ての従業員が認識し、いつでも利用できるようにすることで、適切で時機を逸しない対応を確実に実施できることが望ましい。

iii. 全ての従業員に対し、情報システムのぜい弱性や情報セキュリティインシデントの予兆等の情報資産に対する危険を発見した場合には、いかなる場合であってもできる限り速やかに管理責任者に報告する義務があることを認識させておくことが望ましい。

iv. 収集した情報セキュリティインシデント情報を分析し、必要に応じて対策の見直しに資することが望ましい。

Ⅱ．７．コンプライアンス

Ⅱ．７．１．法令と規則の遵守

Ⅱ．７．１．１．【基本】

個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。

【ベストプラクティス】

i. 関連する法規としては、個人情報保護法、不正競争防止法、著作権法、e-文書法、電子帳簿保存法等が考えられる。

ii. 上記の法令を遵守するにあたり、下記に示すようなガイドライン等を参照することが望ましい。

a) 個人情報保護法関係のガイドライン
22 分野に 35 のガイドラインがある。
（参考）内閣府国民生活局「個人情報の保護に関するガイドラインについて」

b) 不正競争防止法関係のガイドライン
日本弁理士会「不正競争防止法ガイドライン」 等

c) 著作権法関係のガイドライン
文化庁「平成 19 年度著作権テキスト」、社団法人テレコムサービス協会「著作権関係ガイドライン」 等

d) e-文書法関係のガイドライン
経済産業省『文書の電磁的保存等に関する検討委員会』の報告書、タイムビジネス推進協議会「e-文書法におけるタイムスタンプ適用ガイドライン Ver1.1」 等

e) 電子帳簿保存法関係のガイドライン
国税庁 「電子帳簿保存法取扱通達」 等

iii. クラウドサービスの提供にあたり、海外にデータセンタがある場合等、海外法[9]が適用される場合があるので注意する必要がある。

[9] 新たに施行された EU 一般データ保護規則等で見られるように、世界各国において、個人データの越境移転や保管先に関する規制強化が拡大している。具体的には、個人情報保護法等によって、個人データの越境移転を制限していたり、同国内に個人データの保管サーバを置くことを義務付けている国がある。

Ⅱ．７．１．２．【基本】

クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。

【ベストプラクティス】

i. 記録類は、記録の種類（例：会計記録、データベース記録、ログ記録、運用手順等）によって大分類し、さらにそれぞれの種類において保存期間と記録媒体の種別（例：紙、光媒体、磁気媒体等）によって細分類することが望ましい。
ii. 記録の保存は媒体の製造業者の推奨仕様に従って行うことが望ましい。
iii. 媒体が劣化する可能性を考慮し、長期保存のためには紙又はマイクロフィルムを利用することが望ましい。
iv. 国又は地域の法令又は規制によって保存期間が定められている記録を確実に特定することが望ましい。

Ⅱ．７．１．３．【基本】

利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。

【ベストプラクティス】

i. 情報システム又は情報処理施設を利用しようとする者に対して、利用しようとしている情報システム又は情報処理施設がクラウド事業者の所有であること、認可されていない目的のためアクセスは許可されないこと等について、警告文を画面表示する等によって警告することが望ましい。
ii. 利用を継続するためには、警告に同意を求めることが望ましい。ただし、利用者については、サービスの利便性を考慮し、クラウドサービスの利用開始時にのみ同意を求めることで対応することも可能である。

Ⅱ．８．ユーザサポートの責任

Ⅱ．８．１．利用者への責任

Ⅱ．８．１．１．【基本】

クラウドサービスの提供に支障が生じた場合には、その原因が連携クラウド事業者に起因するものであったとしても、利用者と直接契約を結ぶクラウド事業者が、その責任において一元的にユーザサポートを実施すること。

【ベストプラクティス】

i. 連携クラウド事業者が提供しているクラウドサービス部分に係るユーザサポートについては、利用者便益を最優先した方法によって実施することが望ましい。このため、クラウド事業者は、連携クラウド事業者との間で利用者からの故障対応要求や業務問合せ、作業依頼等に対する取扱手続を定め、合意を得た手段で実施することが望ましい。
例：クラウド事業者が、連携クラウド事業者のサービス部分に係る問合せについても一括して受け付ける等

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

１６.１情報セキュリティインシデントの管理及びその改善

【目的】セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

１６.１.２情報セキュリティ事象の報告

【管理策】情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告することが望ましい。

１６.１.４情報セキュリティ事象の評価及び決定

【管理策】情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定することが望ましい。

１６.１.７証拠の収集

【管理策】組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　219～220 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　255～258 ページを参照

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

１８.１法的及び契約上の要求事項の順守

【目的】情報セキュリティに関連する法的、規制又は契約上の義務に対する違反及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

１８.１.１適用法令及び契約上の要求事項の特定

【管理策】各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つことが望ましい。

１８.１.２知的財産権

【管理策】知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施することが望ましい。

１８.１.３記録の保護

【管理策】記録は、法令、規制、契約及び業務上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護することが望ましい。

１８.１.４プライバシー及び個人を特定できる情報（PII）の保護

【管理策】プライバシー及び PII の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実にすることが望ましい。

１８.１.５暗号化機能に対する規制

【管理策】暗号化機能は、関連する全ての協定、法令及び規制を順守して用いることが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　222～223 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　259～261 ページを参照

Ⅲ．物理的･技術的対策編

【凡例】

対策項目

クラウド事業者が実施すべき情報セキュリティ対策事項。認証基準等で用いられるような実施必須事項を示すものではなく、情報セキュリティ対策を実施する上での指標となることを期待している。

基本・推奨

対策を「基本」と「推奨」に分類することで、対策実施の優先度を示している。

・基本：クラウドサービスを提供するにあたり、優先的に実施すべき情報セキュリティ対策

・推奨：クラウドサービスを提供するにあたり、実施することが望まれる情報セキュリティ対策

ベストプラクティス

対策を実施するにあたっての、具体的な実施手法や注意すべき点をまとめた参考事例。

評価項目

対策項目を実施する際に、その実施レベルを定量的あるいは具体的に評価するための指標。SLA の合意事項として活用されることも想定される。

対策参照値

対策項目の実施レベルの目安となる評価項目の値で、パターンごとに設定されている。特に達成することが必要であると考えられる値については「*」を付している。また、評価項目によっては、対策参照値が「-」となっているパターンが存在するが、これについては、クラウド事業者が任意に対策参照値を設定することで、対策項目の実施レベルを評価されたい。

クラウドサービス種別のパターン化

「機密性」、「完全性」、「可用性」に基づく、パターン分類の考え方は以下のとおりである（簡略化し整理したものを図表３に示す）。

【パターン 1】

機密性・完全性・可用性の全てへの要求が「高」いサービス

【パターン 2】

機密性・完全性への要求は「高」いが、可用性への要求は「中」程度のサービス

【パターン 3】

機密性・完全性への要求は「高」いが、可用性への要求は「低」[10]いサービス

【パターン 4】

機密性への要求は「低」いが、完全性・可用性への要求が「高」いサービス

【パターン 5】

機密性への要求は「低」いが、完全性への要求は「高」く、可用性への要求は「中」程度のサービス

【パターン 6】

完全性への要求は「高」いが、機密性・可用性への要求は「低」いサービス

図表３　各パターンの位置付け

パターン	機密性への要求	完全性への要求	可用性への要求
1	高	高	高
2	高	高	中
3	高	高	低
4	低	高	高
5	低	高	中
6	低	高	低

（注）詳細の考え方は、Annex３を参照されたい。

[10] 本ガイドラインでは、一定の条件に合致するかどうかを示す相対的な見出しとして「低」という表現を用いているが、これは情報セキュリティ要求レベルが絶対的に低いことを示すものではない。

Ⅲ．１．アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策

Ⅲ．１．１．運用管理に関する共通対策

Ⅲ．１．１．１．【基本】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。 稼働停止を検知した場合は、利用者に速報を通知すること。

【ベストプラクティス】

i. 監視対象機器の死活監視を行うための方法（ping[11]コマンドなど）、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にすることが望ましい。

ii. 実施基準・手順等に従い監視を行い、監視結果について評価・見直しを行うことが望ましい。

iii. 稼働停止を検知した場合は、短文の電子メール等で利用者に速やかに速報を通知することが望ましい。ここで、通知先には、利用者側の管理連絡窓口だけでなく、クラウドサービスを利用する全ての者を含むことが望ましい。

【評価項目】

a. 死活監視インターバル（応答確認）

パターン	対策参照値
1	1 回以上／5 分*
2	1 回以上／10 分*
3	1 回以上／20 分*
4	1 回以上／5 分*
5	1 回以上／10 分*
6	1 回以上／20 分*

[11] Packet INternet Groper。TCP/IP ネットワークの状態を診断するためのツール。監視対象機器に ping コマンドを送信すると受信した機器から応答が返ってくる。その応答状況から、対象機器の動作状態や通信に要する時間等を確認することができる。

b. 通知時間（稼働停止検知後、利用者に通知するまでの時間）

パターン	対策参照値
1	20 分以内*
2	60 分以内*
3	5 時間以内*
4	20 分以内*
5	60 分以内*
6	5 時間以内*

Ⅲ．１．１．２．【基本】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。 障害を検知した場合は、利用者に速報を通知すること。

【ベストプラクティス】

i. サービス稼働状態を監視するための方法、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にすることが望ましい。

ii. 実施基準・手順等に従い監視を行い、監視結果について評価・見直しを行うことが望ましい。

iii. 障害を検知した場合は、短文の電子メール等で利用者に速報を通知することが望ましい。ここで、通知先は利用者側の管理連絡窓口のみとすることが望ましい。

【評価項目】

a. 障害監視インターバル

パターン	対策参照値
1	1 回／10 分
2	1 回／30 分
3	1 回／60 分
4	1 回／10 分
5	1 回／30 分
6	1 回／60 分

b. 通知時間（障害検知後、利用者に通知するまでの時間）

パターン	対策参照値
1	20 分
2	60 分
3	5 時間
4	20 分
5	60 分
6	5 時間

Ⅲ．１．１．３．【推奨】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。 また、利用者との取決めに基づいて、監視結果を利用者に通知すること。

【ベストプラクティス】

i. 監視の実施にあたり、監視方法（コマンドの入力手順、監視ツールの操作手順等）、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にすることが望ましい。

ii. 監視の結果、クラウドサービスのレスポンス時間が大きく増加した場合には、SLA 等の利用者との取決めに基づいて、利用者に速報を通知することが望ましい。ここで、通知先は利用者側の管理連絡窓口のみとすることが望ましい。

iii. 管理責任者は、監視結果をレビューし、必要ならば実施基準・手順等の評価・見直しを行うことが望ましい。

【評価項目】

a. パフォーマンス監視インターバル

パターン	対策参照値
1	1 回／10 分
2	1 回／30 分
3	1 回／60 分
4	1 回／10 分
5	1 回／30 分
6	1 回／60 分

b. 通知時間（異常検知後、利用者に通知するまでの時間）

パターン	対策参照値
1	20 分
2	60 分
3	5 時間
4	20 分
5	60 分
6	5 時間

Ⅲ．１．１．４．【推奨】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。

【ベストプラクティス】

i. 監視結果の報告内容、報告時期、報告先等の実施基準・手順等を明確にすることが望ましい。

ii. 管理責任者への報告は電子メール、紙文書等で直接伝えることが望ましいが、管理用 Web ページに掲載して伝えることでも良い。

Ⅲ．１．１．５．【基本】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。

【ベストプラクティス】

i. タイムビジネス信頼・安心認定制度における時刻提供精度要求等を参考にして、日本標準時との同期を取ることが望ましい。

ii. クラウドサービスでは、責任分界の観点から、ログによる証拠保全が重要であるため、サーバ・ストレージ間でも時刻同期を取ることが望ましい。

iii. 全ての機器の時刻同期を行う方法、及び時刻に誤差が生じた場合の修正方法について明確にすることが望ましい。（例：NTP[12]サーバの利用）

iv. 定期的に時刻同期の状況を確認することが望ましい。

[12] Network Time Protocol。ネットワークを介してコンピュータの内部時計を同期する通信規約。

Ⅲ．１．１．６．【基本】

クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。

【ベストプラクティス】

i. 情報セキュリティに関する情報を提供している機関（@police、JPCERT/CC、IPA セキュリティセンター等）やセキュリティベンダ、ハードウェアベンダ、ソフトウェアベンダ、オープンソフトウェア・フリーソフトウェア等のセキュリティ情報を提供している Web サイト等からぜい弱性に関する情報を入手することができる。

ii. ぜい弱性が発見された場合は、提供されたパッチを適用することによる情報システムへの影響を確認した上で、パッチ適用を実施することが望ましい。

【評価項目】

a. OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 24 時間以内*
4	ベンダリリースから 3 日以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

Ⅲ．１．１．７．【推奨】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に報告すること。

【ベストプラクティス】

i. 定期報告書には、稼働率、SLA の実施結果、パフォーマンス監視結果等を含めることが望ましい。

ii. 定期報告内容は、月単位で集計することが望ましい。

【評価項目】

a. 定期報告の間隔（Web 等による報告も含む）

パターン	対策参照値
1	1ヶ月
2	3ヶ月
3	6ヶ月
4	1ヶ月
5	3ヶ月
6	6ヶ月

Ⅲ．１．１．８．【基本】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。

【ベストプラクティス】

i. 稼働停止、障害、パフォーマンス低下、その他の情報セキュリティ事象について、第一報（速報）に続いて、より詳しい分析報告を利用者に対して行うことが望ましい。ここで、報告先は利用者側の管理連絡窓口のみとすることが望ましい。

ii. 追加報告については、電子メールや FAX 同報等で実施することが望ましい。

iii. 原因の分析結果や復旧の予測を含んだ報告を行うことが望ましい。

【評価項目】

a. 第一報（速報）に続く追加報告のタイミング

パターン	対策参照値
1	発見後 1 時間
2	発見後 1 時間
3	発見後 12 時間
4	発見後 1 時間
5	発見後 12 時間
6	発見後 12 時間

Ⅲ．１．１．９．【基本】

情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。

【ベストプラクティス】

i. 運用・管理対象、運用・管理方法（コンピュータの起動・停止の手順、バックアップ、媒体の取扱い、情報セキュリティインシデントへの対応・報告、ログの記録と管理、パフォーマンス監視・評価、システム監査ツールの不正使用の防止等）、運用・管理体制等を明確にすることが望ましい。

ii. 管理責任者は、運用・管理報告についてレビューを実施し、必要であれば実施基準・手順等の評価・見直しを行うことが望ましい。

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

6.3 クラウド利用者とクラウド事業者の公平な取引を確保するための措置（※）

【目的】クラウド利用者の情報セキュリティマネジメント方針に適合したクラウドサービスの選択を確実にするため。

6.3.1 クラウドサービスの情報セキュリティマネジメントに係る提供条件の明確化（※）

【管理策】クラウドサービスの情報セキュリティマネジメントに係る責任範囲、サービスレベル、クラウド利用者個別に対応可能な範囲等の提供条件を明確に定め、文書化することが望ましい。

6.3.2 利用者接点とサプライチェーンにおける情報提供・共有（※）

【管理策】目的や場面に応じて、クラウド利用者が必要とする情報を提供できる仕組みを構築することが望ましい。インシデント発生時には、ICT サプライチェーンで情報を共有し、クラウド利用者が必要とする情報を早く提供することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex 5　199～200 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex 6　228～232 ページを参照

9．2 利用者アクセスの管理

【目的】システム及びサービスへの認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。

9．2．3 特権的アクセス権の管理

【管理策】特権的アクセス権の割当て及び利用は、制限し、管理することが望ましい。

9．2．4 利用者の秘密認証情報の管理

【管理策】秘密認証情報の割当ては、正式な管理プロセスによって管理することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex 5　204 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex 6　237 ページを参照

（※）ISO/IEC27002 に記載は無いが、クラウドサービス提供の観点から、目的・管理策を提示したもの

Ⅲ．２．アプリケーション、プラットフォーム、サーバ・ストレージ

Ⅲ．２．１．アプリケーション、プラットフォーム、サーバ・ストレージの運用・管理

Ⅲ．２．１．１．【基本】

クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率を規定すること。 また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。

【ベストプラクティス】

i. クラウドサービスを利用者に提供する時間帯（サービス時間帯）とは、契約サービス時間から定期保守時間を差し引いたものである。ここで、契約サービス時間とは、契約時に利用者に提示したクラウドサービスの提供時間（例：365 日/24 時間、休日・日祭日を除く 8:00-20:00 等）のことであり、定期保守時間とは、事前通知された定期保守によるクラウドサービス停止総時間（例：5 時間/１年）のことである。

ii. 稼働率とは、サービス時間帯に締める実稼働時間の割合のことである。ここで、実稼働時間とは、サービス時間帯において実際にクラウドサービスの提供が実施された時間のことである。

【評価項目】

a. クラウドサービスの稼働率

パターン	対策参照値
1	99.5%以上*
2	99%以上*
3	95%以上*
4	99.5%以上*
5	99%以上*
6	95%以上*

Ⅲ．２．１．２．【基本】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。

【ベストプラクティス】

i. 要求されたサービス性能を満たすことを確実にするために、アプリケーション、プラットフォーム、サーバ・ストレージの利用を監視・調整し、また、将来必要とする容量・能力を予測することが望ましい。

ii. 定期的にアプリケーション、プラットフォーム、サーバ・ストレージの利用状況を監視することが望ましい。

【評価項目】

a. 容量・能力等の要求事項を記録した文書の保存期間

パターン	対策参照値
1	サービス提供期間＋1 年間
2	サービス提供期間＋6 ヶ月
3	サービス提供期間＋3 ヶ月
4	サービス提供期間＋1 年間
5	サービス提供期間＋6 ヶ月
6	サービス提供期間＋3 ヶ月

Ⅲ．２．１．３．【基本】

利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。

【ベストプラクティス】

i. 利用者の利用状況、例外処理及び情報セキュリティ事象の記録として何を取得するか、取得した記録の保管期間、取得した記録の保管方法、取得した記録のチェック（監査等）方法等を明確にすることが望ましい。取得することが望ましい情報の例は以下のとおり。

a) 利用者 ID
b) 主要な事象の日時及び内容（例：ログオン、ログオフ、下記 d)e)g)h）の事象発生）
c) 可能な場合には，端末装置の ID 又は所在地
d) 情報システムへのアクセスの成功及び失敗した試みの記録
e) データ及び他の情報資産へのアクセスの成功及び失敗した試みの記録
f) 情報システム構成の変更
g) 特権の利用
h) 情報システムユーティリティ及びアプリケーションの利用
i) アクセスされたファイル及びアクセスの種類
j) ネットワークアドレス及びプロトコル
k) アクセス制御システムが発した警報
l) 保護システム（例えば、ウイルス対策システム、侵入検知システム、情報漏えい対策システム）の作動及び停止　等

ii. システム障害等によるログの欠損をできる限り少なくするために、スタンバイ機等を用いてログサーバの運転を迅速に再開できる状態にしておくことが望ましい。

【評価項目】

a. 利用者の利用状況の記録（ログ等）の保存期間

パターン	対策参照値
1	3ヶ月
2	1ヶ月
3	1週間
4	3ヶ月
5	1ヶ月
6	1週間

b. 例外処理及び情報セキュリティ事象の記録（ログ等）の保存期間

パターン	対策参照値
1	5年
2	1年
3	6ヶ月
4	5年
5	1年
6	6ヶ月

c. スタンバイ機による運転再開

パターン	対策参照値
1	可能（ホットスタンバイ[13]）
2	可能（コールドスタンバイ[14]）
3	-
4	可能（ホットスタンバイ）
5	可能（コールドスタンバイ）
6	-

[13] 使用する情報システムと同じものを別に用意し、同じ動作を行いながら待機状態にしておくことで、情報システムに障害が発生した際に即座に切り替えができるようにしておく冗長化手法。

[14] 使用する情報システムと同じものを別に用意するが、ホットスタンバイと異なり同じ動作を行うことはせず、情報システムに障害が発生した際に作動させ切り替える冗長化手法。

Ⅲ．２．１．４．【推奨】

クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。

【ベストプラクティス】

i. ぜい弱性の診断対象（アプリケーション等）、診断方法（ポートスキャンツールやぜい弱性診断ツールの使用等）、診断時期等の計画を明確にすることが望ましい。

ii. 診断によりぜい弱性に対する対策を実施した場合は、対策の実施についての記録を残すことが望ましい。

iii. クラウドサービスの提供に用いるアプリケーションについては、開発段階からぜい弱性診断を行うこと等により、導入前にあらかじめぜい弱性対策を実施しておくことが望ましい。

【評価項目】

a. ぜい弱性診断の実施間隔（サーバ等への外部からの侵入に関する簡易自動診断（ポートスキャン等））

パターン	対策参照値
1	1回／1ヶ月
2	1回／1ヶ月
3	1回／1ヶ月
4	1回／1ヶ月
5	1回／1ヶ月
6	1回／1ヶ月

b. ぜい弱性診断の実施間隔（サーバ等への外部からの侵入に関する詳細診断（ネットワーク関係、外部委託を含む））

パターン	対策参照値
1	1回／6ヶ月
2	1回／1年
3	1回／1年
4	1回／6ヶ月
5	1回／1年
6	1回／1年

c.　ぜい弱性診断の実施間隔（アプリケーションのぜい弱性の詳細診断（外部委託を含む））

パターン	対策参照値
1	1 回／1 年
2	1 回／1 年
3	1 回／1 年
4	1 回／1 年
5	1 回／1 年
6	1 回／1 年

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

１２.１運用の手順及び責任

【目的】情報処理施設の正確かつセキュリティを保った運用を確実にするため。

１２.１.１操作手順書

【管理策】操作手順は、文書化し、必要とする全ての利用者に対して利用可能とすることが望ましい。

１２.１.２変更管理

【管理策】情報セキュリティに影響を与える、組織、業務プロセス、情報処理施設及びシステムの変更は、管理することが望ましい。

１２.１.３容量・能力の管理

【管理策】要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　208～209 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　243～244 ページを参照

１２.４　ログ取得及び監視

【目的】イベントを記録し、証拠を作成するため

１２.４.１イベントログ取得

【管理策】利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューすることが望ましい。

１２.４.２ログ情報の保護

【管理策】ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護することが望ましい。

１２.４.３実務管理者及び運用担当者の作業ログ

【管理策】システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューすることが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　210～212 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　247～248 ページを参照

１２.５　運用ソフトウェアの管理

【目的】運用システムの完全性を確実にするため。

１２.５.１運用システムに関わるソフトウェアの導入

【管理策】運用システムに関わるソフトウェアの導入を管理するための手順を実施することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　212 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　249 ページを参照

Ⅲ．２．２．アプリケーション、プラットフォーム、サーバ・ストレージの情報セキュリティ対策

Ⅲ．２．２．１．【基本】

クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。

【ベストプラクティス】

i. 利用者によるサーバ・ストレージ上のデータへのアクセスに対して、ウイルス対策ソフトによるリアルタイムスキャン、情報システムの完全スキャン等による情報セキュリティ対策を行うことが望ましい。

ii. ウイルス対策ソフトについては、常に最新のパターンファイルを適用することが望ましい。

iii. ソフトウェアに対する情報セキュリティ対策として、ソフトウェアの構成管理（ソフトウェアのバージョンが正しいこと、意図しないソフトウェアが存在しないことの確認等）を行うことが望ましい。

iv. 提供するクラウドサービスの一環として、利用者によるダウンロードや HTTP/HTTPS 等を利用したクラウド間転送を許可するファイルについては、ウイルス等の不正なコードが含まれていないことを十分に確認してから提供することが望ましい。

【評価項目】

a. パターンファイルの更新間隔

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 3 日以内*
4	ベンダリリースから 24 時間以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

Ⅲ．２．２．２．【推奨】

データベースに格納されたデータの暗号化を行うこと。

【ベストプラクティス】

i. 特に、個人情報、機密情報等のデータについては、暗号化を行うことが望ましい。

ii. 暗号化・復号に使用する鍵については、改変、破壊、紛失から保護するために厳密に管理することが望ましい。

iii. 使用する暗号アルゴリズムは、電子政府推奨暗号リストに掲載されているアルゴリズムのように、その強度について評価、監視されているものが望ましい。

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

１０.１　暗号による管理策

【目的】情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。

１０.１.１　暗号による管理策の利用方針

【管理策】情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施することが望ましい。

１０.１.２　鍵管理

【管理策】暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　207 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　242～243 ページを参照

１２.２　マルウェアからの保護

【目的】情報及び情報処理施設がマルウェアから保護されることを確実にするため。

１２.２.１　マルウェアに対する管理策

【管理策】マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　209～210 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　245～246 ページを参照

Ⅲ．２．３．サービスデータの保護

Ⅲ．２．３．１．【基本】

利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。

【ベストプラクティス】

i. 業務要件、セキュリティ要件等を考慮して、バックアップ方法（フルバックアップ、差分バックアップ等）、バックアップ対象（利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報等）、バックアップの世代管理方法、バックアップの実施インターバル、バックアップのリストア方法等を明確にすることが望ましい。

【評価項目】

a. バックアップ実施インターバル

パターン	対策参照値
1	1 回／1 日
2	1 回／1 週間
3	1 回／1 ヶ月
4	1 回／1 日
5	1 回／1 週間
6	1 回／1 ヶ月

b. 世代バックアップ

パターン	対策参照値
1	５世代
2	２世代
3	１世代
4	５世代
5	２世代
6	１世代

Ⅲ．２．３．２．【推奨】

バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。

【ベストプラクティス】

i. 日常の定期確認においては、ファイルをリストアし、ファイルサイズを確認することが多い。より確実な方法としては復旧試験の実施がある。

ii. 定期的に復旧訓練を計画・実施し、結果のレビューを行い、必要に応じて方法の見直しを行うことが望ましい。

【評価項目】

a. バックアップ確認の実施インターバル（ディスクに戻してファイルサイズを確認する等）

パターン	対策参照値
1	バックアップ実施の都度
2	バックアップ実施の都度
3	バックアップ実施の都度
4	バックアップ実施の都度
5	バックアップ実施の都度
6	バックアップ実施の都度

Ⅲ．３．ネットワーク

Ⅲ．３．１．外部ネットワークからの不正アクセス防止

Ⅲ．３．１．１．【基本】

ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。

【ベストプラクティス】

i. 利用者、情報システム等の管理者、連携クラウド事業者等アクセスの主体ごとに、アクセス制御に適合する業務上の要求を明確に規定することが望ましい。

ii. i.で示した要求に基づいてアクセス制御方針を確立し、文書化し、レビューすることが望ましい。

iii. アクセス制御には、論理的な方法と物理的な方法があり、この両面を併せて考慮することが望ましい。

Ⅲ．３．１．２．【基本】

情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。

【ベストプラクティス】

i. アクセス制御方針に則り、情報システム管理者及びネットワーク管理者に情報システム又はネットワークへのアクセス権を与える場合は、正式な認可プロセスによってそのアクセス権の割当を管理することが望ましい。

ii. 特に、情報システム管理者及びネットワーク管理者に情報システム又はネットワークへのアクセス特権を与える必要がある場合は、必要最小限の者に限定し、かつ厳格にその割当を管理することが望ましい。

iii. 管理者権限の割当一覧を作成して管理することが望ましい。

iv. 管理者権限の割当又は使用制限を行うための実施マニュアルを整備することが望ましい。

Ⅲ．３．１．３．【基本】

利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。 また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。

【ベストプラクティス】

i. 情報システム管理者、ネットワーク管理者、連携クラウド事業者等が運用・管理・保守等の目的で遠隔から情報システム又はネットワークにアクセスする必要がある場合は、情報セキュリティポリシーに従って、適切な認証方法を利用し、なりすまし対策を行うことが望ましい。

ii. ID・パスワード等の認証情報は、文字列ではなくハッシュ値[15]を保存することが望ましい。

iii. 高い機密性、完全性が求められるサービスでは、記憶情報・所有情報・生体情報を組み合わせた多要素（二要素）認証を採用することが望ましい。

【評価項目】

a. 利用者のアクセス認証方法

パターン	対策参照値
1	生体認証 又は IC カード、あるいはこれらの組合せによる認証
2	IC カード 又は ID・パスワード、あるいはこれらの組合せによる認証
3	ID・パスワード
4	ID・パスワード
5	ID・パスワード
6	ID・パスワード

b. 情報システム管理者、ネットワーク管理者等のアクセス認証方法

パターン	対策参照値
1	デジタル証明書による認証、生体認証 又は IC カード、あるいはこれらの組合せによる認証
2	生体認証 又は IC カード、あるいはこれらの組合せによる認証
3	IC カード 又は ID・パスワード、あるいはこれらの組合せによる認証
4	生体認証 又は IC カード、あるいはこれらの組合せによる認証
5	IC カード 又は ID・パスワード、あるいはこれらの組合せによる認証
6	IC カード 又は ID・パスワード、あるいはこれらの組合せによる認証

[15] ハッシュ関数（入力データから固定長の疑似乱数を生成する関数）で演算することにより得られるデータ。ハッシュ値からは元のデータを復元できない。

Ⅲ．３．１．４．【基本】

外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシ[16]の導入等）を講じること。

【ベストプラクティス】

i. 外部からの不正アクセスを防止するためには、ファイアウォールを導入することが望ましい。
ii. ファイアウォールを導入する際には、情報セキュリティポリシーに基づいたソフトウェアやハードウェアを選定し、構築することが望ましい。
iii. ファイアウォールは、情報セキュリティポリシーに従って運用されることが望ましい。
iv. リバースプロキシを使用し、外部からサーバへの直接アクセスを制御することが望ましい。

Ⅲ．３．１．５．【推奨】

不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS[17]/IPS[18]の導入等）を講じること。

【ベストプラクティス】

i. 外部からの不正アクセスを検出するには、IDS/IPS 等を導入することが望ましい。
ii. IDS/IPS 等を導入する際には、業務要件や業務環境に適合したソフトウェアやハードウェアを選定し、構築することが望ましい。
iii. IDS/IPS 等は、業務要件や業務環境に合わせた設定により運用されることが望ましい。

【評価項目】

a. シグニチャ（パターンファイル）の更新間隔

パターン	対策参照値
1	1 回／1 日
2	1 回／3 週間
3	1 回／3 週間
4	1 回／1 日
5	1 回／3 週間
6	1 回／3 週間

[16] 外部ネットワークとクラウドサービスに用いられるアプリケーションの搭載されたサーバとの間に設置されるプロキシサーバ。利用者は必ずリバースプロキシを経由してサーバにアクセスすることとなるため、外部からサーバへの直接的な不正侵入や攻撃等を防止することができる。

[17] Intrusion Detection System。予め保持している不正パケットのパターン（シグネチャ）と通過パケットを照合することで、リアルタイムで不正パケットを検知するシステム。

[18] Intrusion Prevention System。IDS の機能を拡張し、不正な通過パケットを検知するだけでなく、不正パケットを遮断することで、内部システムへの侵入を防止するシステム。

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

９.４　システム及びアプリケーションのアクセス制御

【目的】システム及びアプリケーションへの、認可されていないアクセスを防止するため。

９.４.１　情報へのアクセス制限

【管理策】情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限することが望ましい。

９.４.４　特権的なユーティリティプログラムの使用

【管理策】システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　204～205 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　238～240 ページを参照

１３.１　ネットワークセキュリティ管理

【目的】ネットワークにおける情報の保護及びネットワークを支える情報処理施設の保護を確実にするため。

１３.１.４　仮想ネットワークにおいて重視すべきぜい弱性（※）

【管理策】仮想ネットワークの複雑な構成や設定に伴う管理ミスを防止する措置を講じることが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　214 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　251 ページを参照

（※）ISO/IEC27002 に記載は無いが、クラウドサービス提供の観点から、管理策を提示したもの

Ⅲ．３．２．外部ネットワークにおける情報セキュリティ対策

Ⅲ．３．２．１．【基本】

外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。

【ベストプラクティス】

i. 情報交換の手順については、以下の項目を考慮した手順書を作成することが望ましい。
   a) 電子メールの送受信における悪意のあるコードの検知及びそのコードからの保護手順
   b) 添付ファイルとして送受信される電子データの保護手順
   c) 特別なリスクが伴うことを考慮した、無線通信の利用手順
   d) 暗号技術の利用手順　等

ii. 管理者と連携クラウド事業者間の情報交換に外部ネットワークを利用する場合は、情報交換の実施基準・手順等を契約等において明確にすることが望ましい。

iii. 管理者間又は管理者と連携クラウド事業者間の情報交換に外部ネットワークを利用する場合は、交換手段（電子メール、インスタントメッセンジャ、電話、ファクシミリ、ビデオ等）ごとに、交換される情報を適切に保護するための対策（誤送信防止、盗聴防止、改ざん防止等）を講じることが望ましい。

Ⅲ．３．２．２．【推奨】

外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。

【ベストプラクティス】

i. 使用する暗号アルゴリズム・プロトコル及び実装については十分に新しく安全なものを使用するとともに、これらについてのぜい弱性に関する最新の情報を確認し、必要に応じて設定変更や機能変更等の対応をすることが望ましい。

ii. 使用する暗号アルゴリズムは、電子政府推奨暗号リストに掲載されているアルゴリズムのように、その強度について評価、監視されているものが望ましい。

【評価項目】

a. 通信の暗号化

パターン	対策参照値
1	IP 暗号通信（VPN(IPsec)[19]等） 又は HTTP 暗号通信（SSL (TLS)[20]等）
2	IP 暗号通信（VPN(IPsec)等） 又は HTTP 暗号通信（SSL(TLS)等）
3	IP 暗号通信（VPN(IPsec)等） 又は HTTP 暗号通信（SSL(TLS)等）
4	HTTP 暗号通信（SSL(TLS)等）
5	HTTP 暗号通信（SSL(TLS)等）
6	HTTP 暗号通信（SSL(TLS)等）

Ⅲ．３．２．３．【基本】

第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。

【ベストプラクティス】

i. なりすまし対策のために、正規のサーバ証明書を取得することが望ましい。

ii. 正規のサーバ証明書の取得に加え、紛らわしくないドメイン名を使うこと等により、利用者によるサーバ正当性の確認を容易にすることが望ましい。

[19] Virtual Private Network。インターネットや多数の利用者が帯域を共有するような公衆回線を専用線のように利用することができる仮想ネットワーク。IPSec は VPN における通信経路の暗号化方式の一つ。
[20] Secure Socket Layer。公開鍵暗号方式等を組み合わせ、送受信するデータを暗号化するプロトコル。TLS は SSL3.0 を基に作成された暗号化プロトコル。

Ⅲ．３．２．４．【基本】

利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。

【ベストプラクティス】

i. クラウド事業者と ISP 間、クラウド事業者の保守管理用、クラウド事業者と連携クラウド事業者間ごとに、情報セキュリティ特性、サービスレベル及び管理上の要求事項を特定することが望ましい。

ii. 提供するクラウドサービスに利用者の契約する通信回線が含まれていない場合には、利用者に対して当該通信回線については責任を負わない旨を明示することが望ましい。

Ⅲ．３．２．５．【推奨】

外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。

【ベストプラクティス】

i. クラウド事業者とISP 間、クラウド事業者の保守管理用、クラウド事業者と連携クラウド事業者間等、全ての外部ネットワークに対して監視を実施することが望ましい。

ii. クラウド事業者とISP 間、クラウド事業者の保守管理用、クラウド事業者と連携クラウド事業者間等、それぞれの外部ネットワークごとに管理責任者を設置し、障害を検知した場合には、それぞれの外部ネットワークの管理責任者に対して通報することが望ましい。

【評価項目】

a. 通報時間（障害が発生してから通報するまでの時間）

パターン	対策参照値
1	検知後 60 分以内
2	-
3	-
4	検知後 60 分以内
5	-
6	-

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

９．１　アクセス制御に対する業務上の要求事項

【目的】情報及び情報処理施設へのアクセスを制限するため。

９．１．１　アクセス制御方針

【管理策】アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューすることが望ましい。

９．１．２　ネットワーク及びネットワークサービスへのアクセス

【管理策】利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　203 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　235～237 ページを参照

９．５　仮想化されたクラウドサービスのアクセス制御（※）

【目的】仮想化されたクラウドサービスにおいて認可されていないアクセスを防止するため。

９．５．１　仮想化資源の分離の確実な実施（※）

【管理策】クラウドサービス上のクラウド利用者の仮想化資源を、他のクラウド利用者の仮想化資源やクラウドサービスの内部管理用の仮想化資源と確実に分離し、アクセス制御を確実にすることが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５　206 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６　241 ページを参照

（※）ISO/IEC27002 に記載は無いが、クラウドサービス提供の観点から、目的・管理策を提示したもの

１３.２ 情報の転送

【目的】組織の内部及び外部に転送した情報のセキュリティを維持するため。

１３.２.２ 情報転送に関する合意

【管理策】合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱うことが望ましい。

１３.２.４ 秘密保持契約又は守秘義務契約

【管理策】情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５ 215 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６ 251～252 ページを参照

Ⅲ．４．建物、電源(空調等)

Ⅲ．４．１．建物の災害対策

Ⅲ．４．１．１．【推奨】

クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、地震・水害に対する対策が行われていること。

【ベストプラクティス】

i. 情報処理施設は、地震や水害が発生しやすい地域の立地を避けることが望ましい。

ii. 情報処理施設には、激しい地震の振動にも耐えられるように、免震構造（建物の振動を緩和する仕組み）又は耐震構造（強い振動にも耐えうる頑強な構造）を採用した建物を利用することが望ましい。

iii. サーバルームは建物の 2 階以上に設置することが望ましい。また、屋上からの漏水の危険がある最上階や、水使用設備が隣室又は直上階にある場所は避けることが望ましい。

Ⅲ．４．２．電源・空調の維持と災害対策

Ⅲ．４．２．１．【基本】

クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じること。

【ベストプラクティス】

i. 非常用無停電電源（UPS 等）は、非常用発電機から電力の供給を受けられることが望ましい。

ii. 複数給電には、本線と予備線を需要家ごとに用意する方式、複数の需要家によってループ経路を形成する方式等がある。

iii. 非常用無停電電源と非常用発電機が非常時に正しく機能するよう、定期的に点検することが望ましい。

【評価項目】

a. 非常用無停電電源（UPS 等）による電力供給時間

パターン	対策参照値
1	10 分
2	10 分
3	10 分
4	10 分
5	10 分
6	10 分

b. 複数給電の実施

パターン	対策参照値
1	実施
2	実施
3	-
4	実施
5	実施
6	-

c. 非常用発電機の設置

パターン	対策参照値
1	実施
2	-
3	-
4	実施
5	-
6	-

Ⅲ．４．２．２．【推奨】

クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供すること。

【ベストプラクティス】

i. サーバルームには、サーバルーム専用の空調設備を設置することが望ましい。

ii. 空調能力の設計にあたっては、情報処理施設の構造、サーバルームの規模と発熱量、設置された機器の使用目的と使用条件等を考慮した検討を行うことが望ましい。

Ⅲ．４．３．火災、逃雷、静電気から情報システムを防護するための対策

Ⅲ．４．３．１．【推奨】

サーバルームに設置されているクラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。

【ベストプラクティス】

i. 代表的な汚損防止対策としては、ガス系消火設備の設置がある。

ii. ガス系消火設備としてよく利用されるのは二酸化炭素消火器である。二酸化炭素消火器は、液化二酸化炭素を圧力により放射して消火を行う消火器である。

【評価項目】

a. 汚損対策の実施

パターン	対策参照値
1	汚損対策消火設備（ガス系消火設備等）の使用
2	汚損対策消火設備（ガス系消火設備等）の使用
3	-
4	汚損対策消火設備（ガス系消火設備等）の使用
5	汚損対策消火設備（ガス系消火設備等）の使用
6	-

Ⅲ．４．３．２．【基本】

クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えること。

【ベストプラクティス】

i. 火災感知器は、熱感知器、煙感知器、炎感知器に大別される。設備メーカーと協議の上、これらの最適な組合せを検討することが望ましい。

ii. 火災感知器の取り付け場所、取り付け個数等は感知器の種類により決めることが望ましい。

iii. 火災の原因になりやすい通信・電力ケーブル類が多量にあるフリーアクセス床下にも火災検知器を設置することが望ましい。

Ⅲ．４．３．３．【基本】

情報処理施設に雷が直撃した場合を想定した対策を講じること。

【ベストプラクティス】

i. 情報処理施設には避雷針を設置することが望ましい。

Ⅲ．４．３．４．【推奨】

情報処理施設付近に誘導雷が発生した場合を想定した対策を講じること。

【ベストプラクティス】

i. 雷サージ（落雷により誘起された大きな誘導電圧）対策として、電源設備の電源引込口にできるだけ近い場所に、避雷器、電源保護用保安器、CVCF[21]等を設置することが望ましい。

ii. 情報処理施設は等電位化（全ての接地の一本化）を行うことが望ましい。

Ⅲ．４．３．５．【推奨】

クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じること。

【ベストプラクティス】

i. 静電気の発生を防止するため、サーバルームの床材には静電気を除去する帯電防止フリーアクセスフロア、アースシート等を使用することが望ましい。導電材を添加した塩化ビニルタイル、高圧ラミネート、帯電防止用カーペット等を使用することもできる。

ii. サーバルームの湿度を 40～60%程度に保つことが望ましい。

[21] Constant-Voltage Constant-Frequency。一定の電圧、周波数に維持された電力を供給する装置。

Ⅲ．４．４．建物の情報セキュリティ対策

Ⅲ．４．４．１．【基本】

重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。

【ベストプラクティス】

i. 入退室を確実に記録するため、常時利用する出入口は一ヶ所とすることが望ましい。

ii. 個人の資格確認による入退室管理を行うことが望ましい。

iii. 個人認証システムとしては、磁気カード照合、IC カード照合、パスワード入力照合、生体認証による照合等のシステムがある。

iv. 個人認証システムは、入退室者の氏名及び入退室時刻を記録することが望ましい。

【評価項目】

a. 入退室記録の保存

パターン	対策参照値
1	2 年以上*
2	2 年以上*
3	2 年以上*
4	2 年以上*
5	2 年以上*
6	2 年以上*

Ⅲ．４．４．２．【推奨】

重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像をあらかじめ定められた期間保存すること。

【ベストプラクティス】

i. 監視性を高めるため、死角を作らないことが望ましい。
ii. 監視カメラは、カラー撮影であり、デジタル記録が可能であることが望ましい。
iii. 監視カメラは用途に応じて十分な解像度を持つことが望ましい。
iv. 監視カメラは、撮影日時が画像内に時分秒まで記録可能であることが望ましい。
v. 非常時に防犯機関等への通報ができる非常通報装置を併設することが望ましい。
vi. 重要な物理的セキュリティ境界においては、個人認証システムと併設することが望ましい。

【評価項目】

a. 監視カメラの稼働時間

パターン	対策参照値
1	365 日 24 時間
2	365 日 24 時間
3	365 日 24 時間
4	-
5	-
6	-

b. 監視映像保存期間

パターン	対策参照値
1	6 ヶ月
2	1 ヶ月
3	1 週間
4	-
5	-
6	-

Ⅲ．４．４．３．【基本】

重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。

Ⅲ．４．４．４．【推奨】

重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置すること。

【ベストプラクティス】

i. 出入口の扉は十分な強度を有する破壊対策・防火扉を使用し、不法侵入、危険物の投込み、延焼を防止することが望ましい。

Ⅲ．４．４．５．【推奨】

重要な物理的セキュリティ境界に警備員を常駐させること。

【ベストプラクティス】

i. 警備員の常駐時間を定めることが望ましい。

【評価項目】

a. 警備員の常駐時間

パターン	対策参照値
1	365 日 24 時間
2	365 日 24 時間
3	-
4	365 日 24 時間
5	365 日 24 時間
6	-

Ⅲ．４．４．６．【基本】

サーバルームやラックの鍵管理を行うこと。

【ベストプラクティス】

i. ラックやサーバルームの出入口の鍵は定められた場所に保管し、管理は特定者が行うことが望ましい。

ii. ラックやサーバルームの出入口の鍵については、受渡し時刻と氏名を記録することが望ましい。

Ⅲ．５．その他

Ⅲ．５．１．機密性･完全性を保持するための対策

Ⅲ．５．１．１．【推奨】

電子データの原本性確保を行うこと。

【ベストプラクティス】

i. 電子データの原本性（真正性）確保の手段としては、時刻認証[22]による方法、署名（ハッシュ値によるもの等）による方法、印刷データ電子化･管理による方法等が考えられる。

【評価項目】

a. 原本性（真正性）確認レベル

パターン	対策参照値
1	時刻認証、署名 及び 印刷データ電子化･管理
2	署名 及び 印刷データ電子化･管理
3	印刷データ電子化･管理
4	時刻認証、署名 及び 印刷データ電子化･管理
5	署名 及び 印刷データ電子化･管理
6	印刷データ電子化･管理

[22] タイムスタンプ（特定の電子情報と時刻情報を結合したもの）を付与することにより、その時刻以前に電子データが存在していたこと（存在性）及び変更・改ざんされていないこと（非改ざん性）を電子的に証明する手法。

Ⅲ．５．１．２．【基本】

個人情報は関連する法令に基づいて適切に取り扱うこと。

【ベストプラクティス】

i. 個人情報を収集する際には、利用目的を明示し、各個人の同意を得た上で収集することが必要である。また、個人情報の漏洩、滅失、棄損を防止するための措置（例：従業員や協力会社要員に対する必要かつ適切な監督等）を講じる必要がある。

ii. 事前の本人同意無しに個人情報を第三者に提供してはならない。

iii. 本人から利用目的の通知、データ開示、データ訂正・追加・削除、データの利用停止等の求めがあった場合は、これに応じなければならない。また、本人から苦情があった場合には、迅速かつ適切に対応しなければならない。

iv. 法令の適用に際し、関連するガイドラインを参考にすることが望ましい。代表的なガイドラインとしては以下がある。

a)個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（経済産業省）

b)電気通信事業における個人情報保護に関するガイドライン（総務省）

c)金融分野における個人情報保護に関するガイドライン（金融庁）

d)雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針について（厚生労働省）

Ⅲ．５．２．クラウド事業者の運用管理端末における情報セキュリティ対策

Ⅲ．５．２．１．【基本】

運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。 従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。 技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。

【ベストプラクティス】

i. 運用管理端末の管理者権限の付与を厳しく制限することが望ましい。

ii. 運用管理端末において、従業員等が行うログイン・ログアウト、特定プログラムの実行、データベース接続などの重要操作等について、操作ログを取得し、保存することが望ましい。

iii. 許可されていないプログラム等を運用管理端末にインストールすることを禁止し、従業員に周知徹底し、違反した場合には罰則を課すことが望ましい。

iv. 運用管理端末は、ウイルス対策ソフトによるリアルタイムスキャン、システムの完全スキャン等による情報セキュリティ対策を行うことが望ましい。

v. ウイルス対策ソフトについては、常に最新のパターンファイルを適用することが望ましい。

vi. 情報セキュリティに関する情報を提供している機関（@police、JPCERT/CC、IPA セキュリティセンター等）や、ハードウェアベンダ、ソフトウェアベンダ、オープンソフトウェア・フリーソフトウェア等のセキュリティ情報を提供している Web サイト等からぜい弱性に関する情報を入手することができる。

vii. パッチは、運用管理機能への影響が無いと確認した上で適用することが望ましい。

【評価項目】

a. パターンファイルの更新間隔

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 3 日以内*
4	ベンダリリースから 24 時間以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

b. OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 24 時間以内*
4	ベンダリリースから 3 日以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

Ⅲ．５．３．媒体の保管と廃棄

Ⅲ．５．３．１．【基本】

紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。

【ベストプラクティス】

i. 個人情報、機密情報等を含む紙、これらのデータを格納した磁気テープ、光メディア等の媒体を保管する際には、鍵付きキャビネット（耐火金庫等）や施錠可能な保管室等を利用することが望ましい。また、保管中の媒体の閲覧記録の作成、コピー制限の設定等の対策を行うことが望ましい。

ii. 紙、磁気テープ、光メディア等の媒体の保管管理手順書を作成することが望ましい。

iii. 保管管理手順書に基づいて、媒体の管理記録を作成するとともに、保管期間を明確にすることが望ましい。

Ⅲ．５．３．２．【基本】

機器及び媒体を正式な手順に基づいて廃棄すること。

【ベストプラクティス】

i. 機器の廃棄作業に着手する前に、当該情報システムの運用が完全に終結していることを確認することが望ましい。

ii. 機器の廃棄にあたっては、当該機器の重要度を考慮し、機密保護、プライバシー保護及び不正防止のための対策を講じることが望ましい。内部の重要なデータの読み出しを不可能とすることが必要である。

iii. 機器の廃棄方法及び廃棄時期を明確にし、廃棄作業完了後には廃棄記録について管理責任者の承認を得ることが望ましい。

iv. 廃棄対象にソフトウェアが含まれる場合は、機器からのソフトウェアの削除に加えて、記録媒体とドキュメントを破壊・焼却・裁断等することが望ましい。

v. 紙媒体の廃棄については、機密性が求められるものは裁断又は焼却することが望ましい。

vi. 第３者に廃棄を委託する場合には、秘密保持契約を締結することが望ましい。

ISO/IEC27002 との紐付け、利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

６.２ モバイル機器及びテレワーキング

【目的】モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

６.２.１ モバイル機器の方針

【管理策】モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５ 198～199 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６ 227～228 ページを参照

１２.６ 技術的ぜい弱性管理

【目的】技術的ぜい弱性の悪用を防止するため。

１２.６.１ 技術的ぜい弱性の管理

【管理策】利用中の情報システムの技術的ぜい弱性に関する情報は、時期を失せずに獲得することが望ましい。さらに、それらと関連するリスクに対処するために、適切な手段をとることが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５ 213 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６ 250 ページを参照

１７.２ 冗長性

【目的】情報処理施設の可用性を確実にするため。

１７.２.１ 情報処理施設の可用性

【管理策】情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入することが望ましい。

【利用者接点と ICT サプライチェーンに着目した要求事項】

Annex５ 221 ページを参照

【利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策】

Annex６ 258 ページを参照

Ⅳ．IoT サービスリスクへの対応方針編

Ⅳ．１．概要

第Ⅰ部、第Ⅱ部及び第Ⅲ部では、クラウド事業者が本来の事業領域であるクラウドサービスを提供するにあたって検討すべきセキュリティ対策について示した。しかし、近年、IoT が急速に注目を集めるようになり、ビジネス環境は急変し、本格的な IoT サービスの時代が到来しようとしている。これに伴い、利活用価値が高いデータが急増して個々の IoT サービスの価値を高めるとともに、このデータがさらに外部に提供され組み合わされること等により、業種を超えた事業変革を生み出すものと期待されている。この市場動向を踏まえ、第Ⅳ部では、IoT サービスリスクとその対応に関するクラウド事業者の知識と理解を深めることで、クラウド事業者（特に ASP・SaaS 事業者）が IoT サービスに参入しやすい環境作りを促進することとした。

具体的には IoT サービスリスクの構造を詳しく解説するとともに、自らの IoT サービスをモデル化するツールを提供し、これらのモデルに基づいて自ら対処すべきリスクや移転すべき責任・役割を整理できる手順を説明する。この手順を適用することで、クラウド事業者が、自ら関わる役割や運用するコンポーネント等に従って取るべきリスク対策を容易に選択できる仕組みを提供する。

Ⅳ．１．１．IoT サービスを特徴付ける三つの観点

IoT サービスには、以下のような三つの特徴的な観点がある。

A　多様な事業者間連携

企業等に向けて提供される IoT サービス[23]は、一般に一つひとつ IoT サービス利用者のニーズに則してオーダーメイドで作り込まれており、IoT サービスは、多数の関係企業等の連携と全体統制の下で、クラウドを利用して構築・維持・運用されることが多い。具体的には、IoT サービス利用者とクラウド事業者の連携に加えて、連携事業者や関係企業等が新たに事業者連携構造に加わってくる。

B　ロールを実行するコンポーネントと運用・保守の多様な提供形態

IoT サービスの提供にあたっては、IoT サービス利用者、クラウド事業者、連携事業者及び関係事業者等がロール（Ⅰ．６．用語の定義参照）を分担し、IoT サービスの提供に必要なコンポーネント（Ⅰ．６．用語の定義参照）を運用・保守している。ロールの実行にあたっては、コンポーネントを運用・保守する人員も必要となってくる。

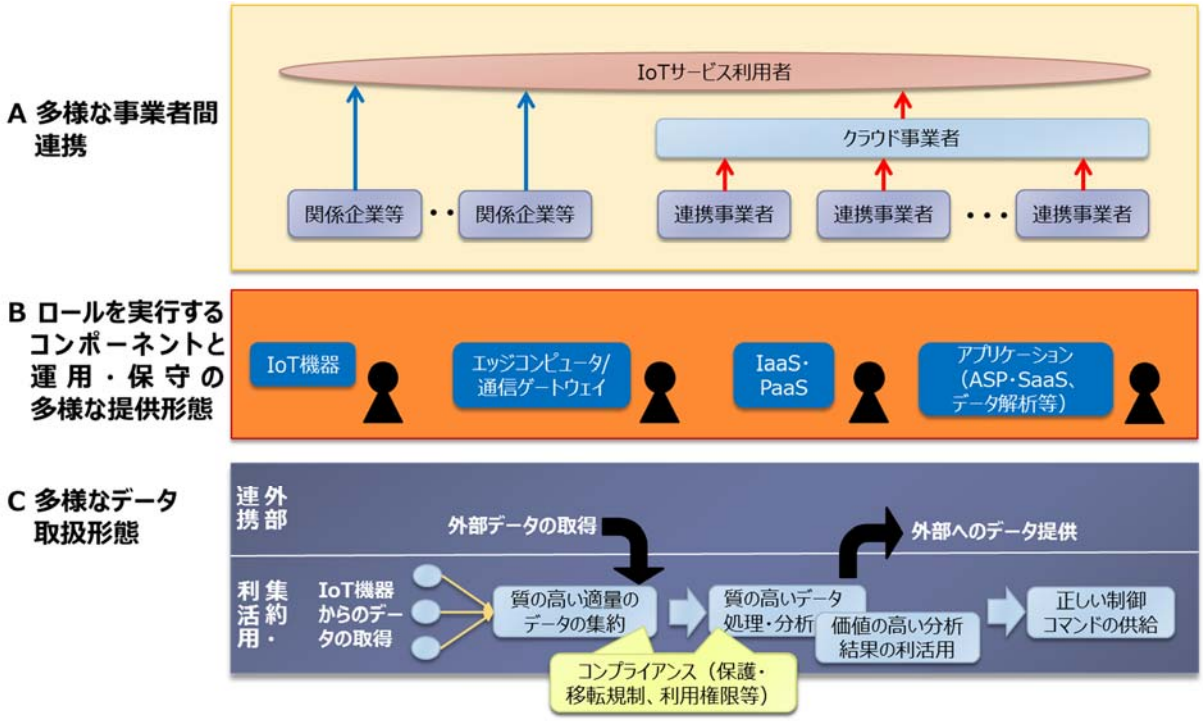
[23] 消費者に付加価値サービスを提供するために IoT サービスを利用する企業等も多い。

C　多様なデータ取扱形態

IoT 機器から生み出され、クラウドに集約されるデータとその処理・分析結果の質の高さが IoT サービスの価値を定め、さらにデータが外部に提供されることでデータを媒体とした新しいイノベーションが生まれてくる。

以上の三つの観点を、図表４に示す。クラウド事業者が IoT サービスの提供を行うためには、この三つの観点を良く理解し、各観点に則したリスクとリスク対応の方法を理解する必要がある。

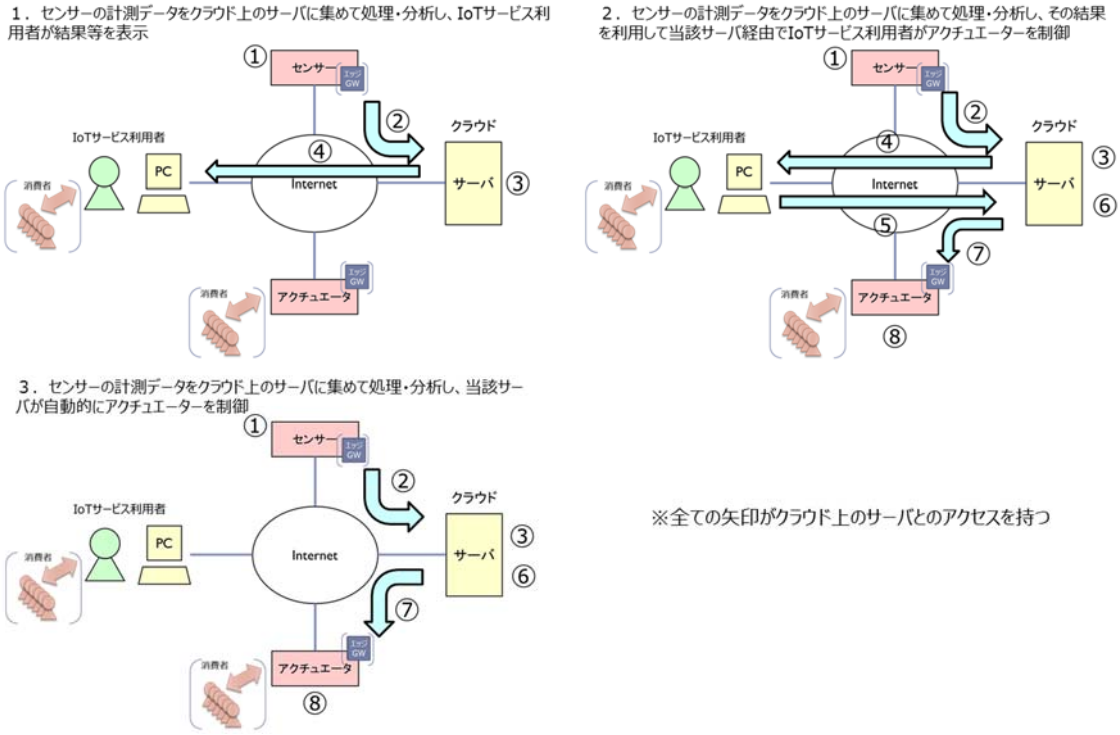
図表４　IoT サービスを特徴付ける三つの観点



Ⅳ．１．２．対象とするIoTサービスの構造

IoTサービスの構造は多岐に渡っているが、クラウド事業者がIoTサービスを提供する際のコンポーネント配置に焦点を当てる（図表５参照）。クラウド事業者は、IoT サービス利用者と契約を結ぶサービス提供の主体となるとともに、利用価値が高いデータを取り扱う主体としての役割を果たすことになる。

図表５　IoTサービスの三つの構造



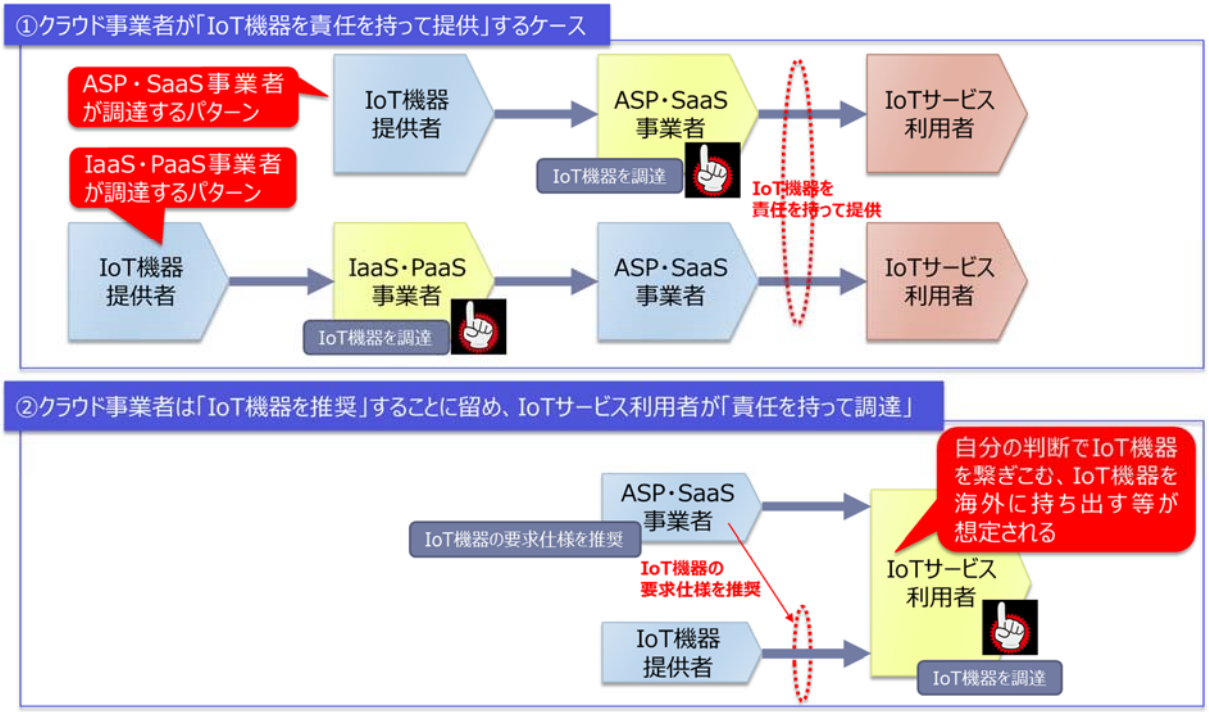
＜クラウド事業者及び連携事業者が果たすIoTサービス運用上の役割（Ⅳ．２．１．１．（イ）参照）＞

①データの計測・前処理等、②④⑤⑦インターネット接続、③データの取扱い（データ解析を含む）と表示等の提供、⑥制御コマンドの提供、⑧駆動前処理・駆動等

また、クラウド事業者が中心となって IoT サービスを提供する際の事業者連携構造は、図表 6 のとおり主として二つの形態があり、以下ではこの 2 形態を中心として取り扱う。

① クラウド事業者が「IoT 機器を責任を持って提供」するケース
② クラウド事業者は「IoT 機器を推奨」することに留め、IoT サービス利用者が「責任を持って調達」するケース

図表 6　クラウド事業者を中心とした IoT サービスの事業者連携構造（二つの主要な類型）



Ⅳ．１．３．IoT サービスにおいて重視すべきリスク

図表４に示した三つの観点のそれぞれにおける IoT サービスにおいて重視すべきリスクを列挙する。

A　【多様な事業者間連携】に起因する事業者連携等の問題がサービス全体に影響を及ぼすリスク（Ⅳ．２．２．A 参照）

事業者連携等の問題により、IoT サービスのセキュリティ強度/サービスレベルの維持、円滑なインシデント対応/サービス継続を阻害し、IoT サービス全体に影響を及ぼすリスク

① 連携事業者間で管理水準が異なることで生じる問題
② サービス継続性の阻害
③ 契約による責任分担の割り当てに関して生じる問題
④ 構成管理に関して生じる問題

B　【ロールを実行するコンポーネントと運用・保守の多様な提供形態】に起因するコンポーネントリスク（Ⅳ．２．２．B 参照）

① コンポーネントそのものに起因するリスク
（例）「モノが人に危害を与える」「情報セキュリティインシデント・情報漏えい」「ICT 障害」「コンプライアンスリスク（海外法の規制に抵触）」
② コンポーネントの運用・保守・要員に関わるリスク
（例）「適切な使い方をしていない」「スキルが足りない」「保守が正しく行われていない」

C　【多様なデータ取扱形態】に起因するデータ価値やデータに係る法令順守を毀損するリスク（Ⅳ．２．２．C 参照）

① データを取り扱うロールのどこかで、データの欠損、不十分な品質、改ざん・漏えい、質の低い解析・意図的に改ざんされた解析等が生じることで、IoT サービス利用者及び外部データ提供先から見たデータ価値が失われるリスク
② 外部から欠損、不十分な品質、改ざん・漏洩があるデータを取得することで、IoT サービス利用者及び外部データ提供先から見たデータ価値が毀損されるリスク
③ データに関する法令順守が毀損されるリスク
（例）「国内外の個人情報保護法に抵触する個人データの取扱い、越境移転、保管サーバ設置等の発生[24]」「海外のサイバーセキュリティ法制に抵触する重要データの越境移転が行われる」「データに関する権利関係が正しく処理されない」等

[24] 他国においては、個人情報保護法によって、同国内に個人データの保管サーバを置くことを義務付けている例がある。

これらのリスクは、大別すると、データの内容を見ないでも対処できるもの（データ量、コンプライアンス）とデータの内容を見ないと対処できないもの（データ品質：外部に提供するデータを含む、改ざん等）に分類できる。

なお、クラウド事業者が IoT サービスを提供するにあたり、過度のリスクと責任を負わないために特に注意すべき点については、Annex7 に取りまとめている。

Ⅳ．１．４．IoT サービスリスクへの対応の考え方

IoT サービスリスクへの対応策についても、IoT サービスリスクと同様に、三つの観点のそれぞれにおいて、対応策を列挙する。詳細はⅣ．５．で述べる。

A　【多様な事業者間連携】事業者連携等の問題がサービス全体に影響を及ぼすリスクへの対応策（Ⅳ．５．A 参照）

IoT サービス利用者とクラウド事業者の契約の適正化、クラウド事業者と連携事業者の契約の適正化、サービス全体で共通のセキュリティ設計基準を適用、サービス全体で共通の運用基準を適用、構成管理の一元化等

B　【ロールを実行するコンポーネントと運用・保守の多様な提供形態】コンポーネントリスクへの対応策（Ⅳ．５．B 参照）

クラウド事業者がコンポーネントの残留リスクを低減・回避する対応策、クラウド事業者がコンポーネントの残留リスクを移転する対応策、人によるコンポーネント取扱いを改善する対応策、コンポーネント管理（外国法の順守を含む）を強化する対応策等

C　【多様なデータ取扱形態】データ価値やデータに係る法令順守を毀損するリスクへの対応策（Ⅳ．５．C 参照）

クラウド事業者が中心となり、連携事業者との体制を構築して、協力して実施する対応策

Ⅳ．１．５．第Ⅳ部の活用方法

第Ⅳ部は、IoT サービスを提供している、または、提供を検討/計画しているクラウド事業者が読むのに適している。「Ⅳ．４．」で提供する手順に従って、クラウド事業者が自ら担う役割、連携事業者に移転するロール（＝外注委託、コンポーネントの調達等）、IoT サービス利用者に移転するロール（＝IoT 機器の調達）を明確に区分し、それぞれに対するリスクを理解し、必要なリスク対応策を具体的に検討できる。また、IoT サービス提供に関わる連携事業者にとっても、リスクの理解と必要なリスク対応策の検討に役立つ。

さらに、IoT サービス提供に関心を持つクラウド事業者やその他の事業者及び IoT サービス利用者にとっても、IoT サービスリスクやその対応のポイントを学ぶための教科書として役立つはずである。

第Ⅳ部は、以下の順で読み進めることを推奨する。

① まず「Ⅳ．１．」を読み、IoT サービスの特徴、サービス構造と事業者連携の形態、IoT サービスリスクの捉え方、リスク対応策の考え方、第Ⅳ部の活用方法等の概略を理解する。

② 次に、「Ⅳ．２．１．」を読み、IoT サービス提供における連携事業者間の役割分担の捉え方、IoT サービスを動作させるコンポーネントの考え方等について理解する。
なお、IoT サービスリスクの詳細に関心があれば、さらに「Ⅳ．２．２．」を読み進むことを推奨する。

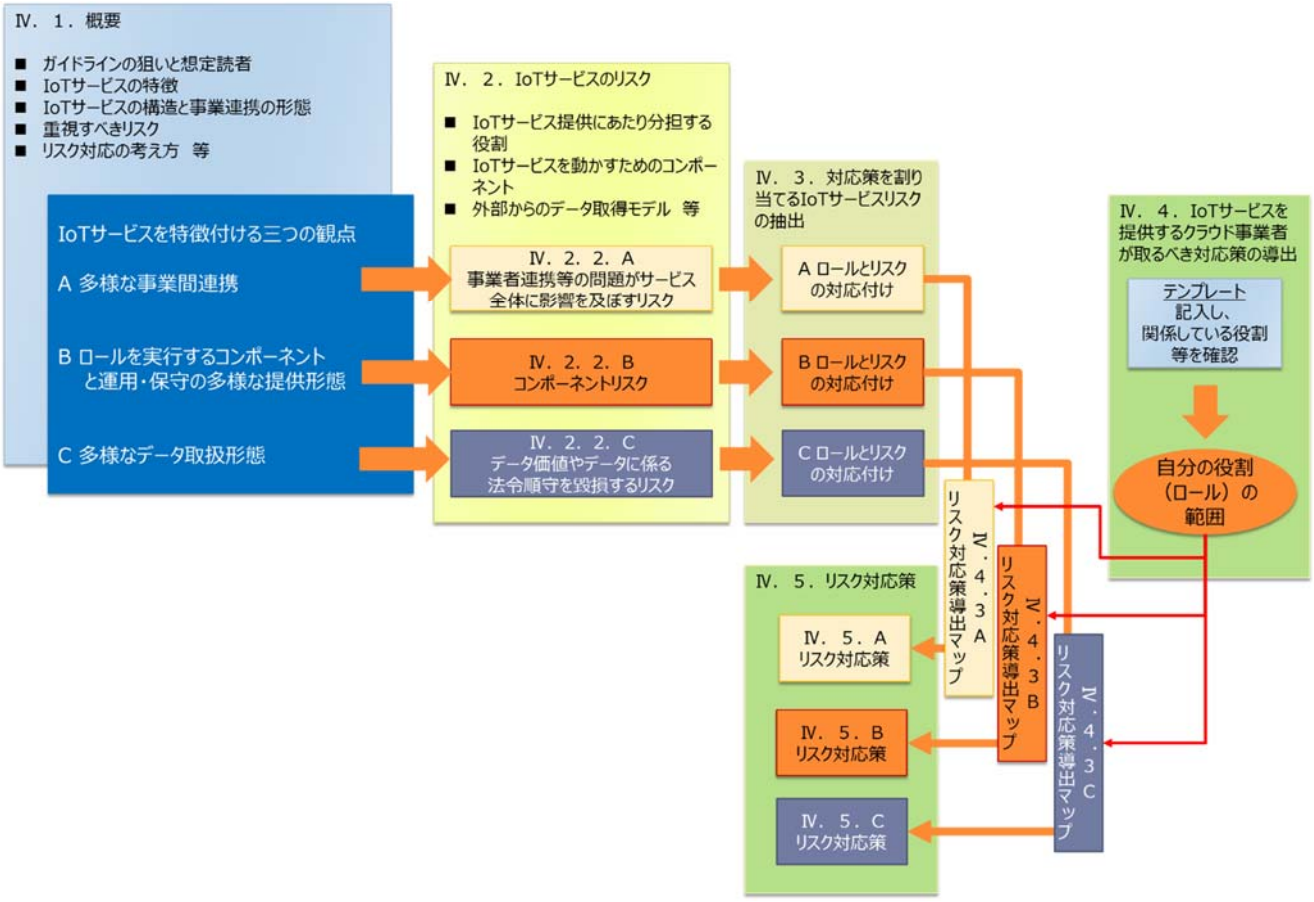
③ さらに「Ⅳ．３．」を読み、IoT サービスを特徴付ける三つの観点別に、どのような IoT サービスリスクが具体的に洗い出されているかを確認する。

④ 以上の準備をした上で「Ⅳ．４．１．」、「Ⅳ．４．２．」を読み、IoT サービス提供にあたりクラウド事業者が関わりを持つ役割を整理し、「Ⅳ．４．３．」の「ロール（＝役割）ごとのリスク対応策導出マップ」を活用することで、措置すべき IoT サービスリスクとそのリスク対応策（具体的な内容は「Ⅳ．５．」に記載）を特定する。（図表 17、図表 18、図表 19 参照）

⑤ 対応策の具体的な内容は「Ⅳ．５．」に列挙されている。「Ⅳ．４．」が示す手順に従って作業すれば、具体的にどのリスク対応策を見る必要があるかが示されているため、「Ⅳ．５．」は必要な箇所のみ読むことで足りるはずである。

第Ⅳ部では、リスクと対応策は、一貫して「IoT を特徴付ける三つの観点」ごとに整理されている（図表７参照）。「Ⅳ．４．」の方法に従って、自ら IoT サービス提供にあたり果たしている役割の範囲を確認することで、各観点において考慮すべきリスクと対応策を導出することができる。

図表７　第Ⅳ部の活用方法（概要）



図表７が示すように、IoT サービスリスクとリスク対応策は、以下では一貫して、【クラウド事業者が実行するロール/果たす役割】×【IoT サービスを特徴付ける三つの観点】のマトリクスで分類されている（図表８参照）。そして、セル（マトリクスの一つの四角）ごとにリスクとリスク対応策が紐付けられている。この配置を理解することで、IoT サービスリスクの確認や、リスク対応策の導出（リスク対応策導出マップを用いた対応策の特定）を行うことができる。

IoT サービスの提供構造は、連携事業者の存在により複雑になる。図表８では、「機器等提供」「機器等推奨」「契約管理」に現れている。連携事業者が存在しない最もシンプルなサービス提供形態（＝クラウド事業者が全ての機器を提供し、自分で全てのロールを実行する場合）では、図表８のうち、「実行」「提供」「主導」のみを実施すれば良く、「推奨」や「委託」は対象外となる。

凡例： Ⅳ. 4. 3. X → 「リスク対応策導出マップ」の記載箇所

図表８ クラウド事業者のリスクとリスク対応策の全体構成－ロール×三つの観点のマップ－

クラウド事業者が実行するロール/果たす役割		IoT サービスを特徴付ける三つの観点		
		A 多様な事業者間連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoT サービスの提供環境を整備・維持するロール（97ページ参照）	a 利用者契約	**実行 →対応策Ⅳ.4.3.A**		
	b 機器等提供		**提供 →対応策Ⅳ.4.3.B ①**	
	c 機器等推奨		**推奨 →対応策Ⅳ.4.3.B ②**	
	d 構成管理	**実行 →対応策Ⅳ.4.3.A**		
	e 契約管理		**委託 →対応策Ⅳ.4.3.B ③**	**委託 →対応策Ⅳ.4.3.C ②**
	f データ監視・保全			**主導 →対応策Ⅳ.4.3.C ①**
（イ）IoT サービスを実行するためのロール（100ページ参照）	a 計測		**実行 →対応策Ⅳ.4.3.B ④**	
	b ローカル伝送			
	…			
	k 駆動			

委託先全体のガバナンス維持のための管理

データ監視・保全への協力の委託管理

ロール実行の委託管理

Ⅳ．１．６．IoT セキュリティガイドライン[25]との関係

第Ⅳ部は、クラウド事業者が IoT サービスに参入することを念頭におき、そのサービス運用に関わるリスク対応を指し示すガイドラインである。したがって、クラウドサービス以外でも、クラウド事業者が事業領域を拡大する可能性がある IoT 機器（センサー、アクチュエータ）、エッジサービス、組込みアプリケーション、その他のアプリケーション（例：表示・データ・コマンド提供、データ解析等）等について幅広くカバーしている。また、企業向けの IoT サービスのみを対象としている。

一方、IoT セキュリティガイドラインは、IoT 機器のライフサイクル（方針、分析、設計、構築・接続、運用・保守）に焦点を当ててリスクと対策を示すガイドラインである。また、IoT サービスの利用者を企業に限定せず、一般消費者にまで広げている。

このように、第Ⅳ部と IoT セキュリティガイドラインは目的が大きく異なる指針であり、内容についても重複は少ない。しかし、IoT セキュリティガイドラインは IoT 機器のリスクとその対応について体系的に示しているため、第Ⅳ部では、IoT 機器リスクへの対応策として引用を行うとともに、IoT セキュリティガイドラインの記述との整合性を維持するように配慮している。

[25] IoT 推進コンソーシアム、総務省、経済産業省が 2016 年 7 月にバージョン 1.0 を公表

Ⅳ．２．IoT サービスのリスク

本章では、まず IoT サービスの提供における連携事業者間の役割分担の捉え方、IoT サービスを動作させるコンポーネントの考え方等について整理する。

次に、これらの整理に基づいて、「A 多様な事業者間連携」「B ロールを実行するコンポーネントと運用・保守の多様な提供形態」「C 多様なデータ取扱形態」の三つの観点のそれぞれに対し、具体的にどのような IoT サービスリスクが存在するかについて示す。

さらに、特に、クラウド事業者の参考となるように、クラウド事業者が過度の責任を負わないための注意点については、Annex 7 において解説する。

Ⅳ．２．１．IoT サービスの提供におけるロールとコンポーネント

Ⅳ．２．１．１．IoT サービスの提供におけるロール

ビッグデータに対する関心の高さを反映して、IoT サービスに参入する企業等は多岐に亘っており、クラウド事業者もその一つといえる。一つひとつオーダーメイドで構築される IoT サービスの提供においては、これらの多岐に亘る企業群が、型に捉われることなく自由にロールを分担している。このような多様なサービス提供形態を考慮し、ここでは IoT サービス提供に必要なロールをモデル化することで、IoT サービスを提供するクラウド事業者が実際に関わっているロールに基づき、措置すべきリスク対応の範囲を特定できるように配慮した。

ロールは、大きくは「IoT サービスの提供環境を整備・維持するロール」と「IoT サービスを実行するためのロール」の二つに分かれている。

（ア）IoT サービスの提供環境を整備・維持するロール

IoT サービスの提供環境を整備・維持するため、「利用者契約」「機器等提供」「機器等推奨」「構成管理」「契約管理」「データ監視・保全」という六つの役割をロールとして定義する（図表９参照）。これらのロールは、典型的には、IoT サービスを提供するクラウド事業者が実施する。

図表９　IoT サービスの提供環境を整備・維持するロールの定義

項番	ロール名	概要
a	利用者契約	IoT サービス利用者とサービス提供契約を締結
b	機器等提供	図表 11 の各ロールが実行できるように、供給する機器等をベンダーから購入・リース（又は自分で製造）して準備。ロールの実行者（主としてクラウド事業者を想定）は、サービス提供のために、準備した機器等を責任を持って提供する。
c	機器等推奨	IoT 機器等の購入・リース等を IoT サービス利用者に任せ、IoT サービスで使用するための要求事項等を IoT サービス利用者に対して推奨。IoT 機器を提供する責任は負わない。
d	構成管理	IoT サービスで用いる IoT 機器/ローカルコンピュータ、ICT 機器/基盤、アプリケーション、AI 等の構成を管理し、接続許可や変更管理を実施
e	契約管理	A 多様な事業者間連携に関するもの： 委託先全体のガバナンス維持のための管理（要求を契約上で明文化する等） B ロールを実行するコンポーネントと運用・保守の多様な提供形態に関するもの： ロール実行の委託管理（要求を契約上で明文化する等） C 多様なデータ取扱い形態に関するもの： データ監視・保全への協力の委託管理（要求を契約上で明文化する等）
f	データ監視・保全	IoT サービスで取り扱う（外部から取得するもの、外部に提供するものを含む）データの量、品質、権利関係の処理等を監視し、データを適切な状態に保全

図表 6 で示した IoT サービスの事業者連携構造の類型に照らして上記のロールを考えると、クラウド事業者が IoT 機器に関し **b** を担うのは、クラウド事業者が「IoT 機器を責任を持って提供」するケースである。このケースの中でも、IoT 機器を調達するのが ASP・SaaS 事業者である場合と IaaS・PaaS 事業者である場合が存在しており、後者の場合は ASP・SaaS 事業者が、IaaS・PaaS 事業者に IoT 機器準備の責任と役割を移転しているものと考えることができる。

これに対し、クラウド事業者が **c** を担うのは、「IoT 機器を推奨」することに留め、IoT サービス利用者が「責任を持って調達」するケースとなる（図表 6 参照）。

これらの選択により、クラウド事業者が責任を持って対応すべきリスクとその対応策が大きく変わってくる（Ⅳ．４．３．B、Ⅳ．５．B 参照）。

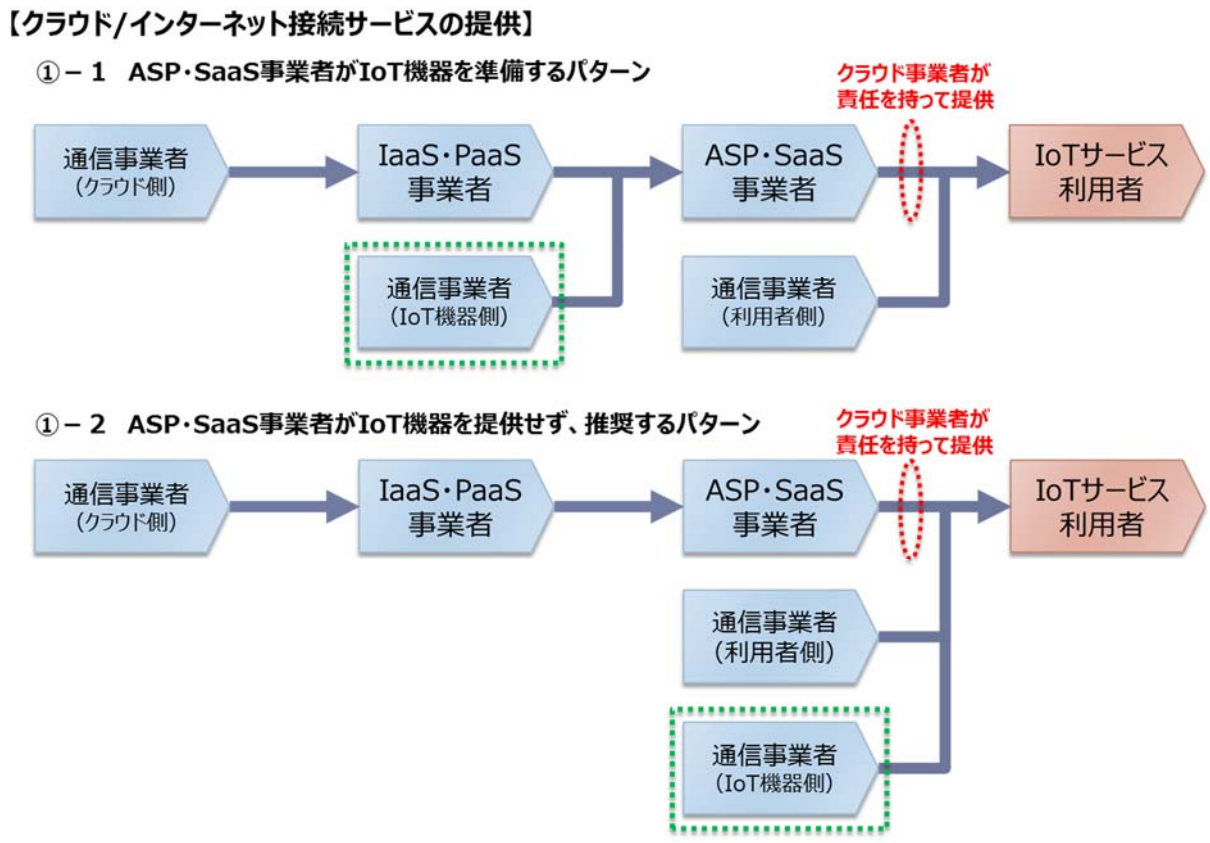
「**b** 機器等提供」のロールについては、クラウド事業者は IoT サービスを特徴付ける以下の主要コンポーネントの提供責任についても考えておく必要がある。

- クラウド（ASP・SaaS、IaaS/PaaS）及び必要なインターネット接続（WAN）
- エッジコンピュータ/通信ゲートウェイ
- アプリケーション（表示・データ・コマンド提供、解析等）

図表 10 に示したとおり、クラウド及び必要なインターネット接続、エッジコンピュータ[26]/通信ゲートウェイ、アプリケーションの大部分は、クラウド事業者が責任を持って準備・提供する（＝**b** のロールを担う）ことが一般的であり、これに従ってリスク処理やリスク対応策を検討することが求められる。

一方で、アプリケーション（特に解析アプリケーション）については、クラウド事業者は IoT サービス利用者に調達を任せる（＝**c** のロールを担う）ことで、リスクを IoT サービス利用者に移転することができる。IoT 機器以外の主要コンポーネントの準備についても、クラウド事業者が責任を持って対応すべきリスクとその対応策を整理した（Ⅳ．４．３．B、Ⅳ．５．B 参照）。

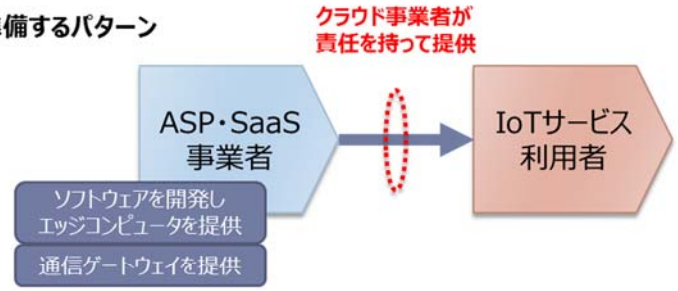
図表 10　IoT 機器以外の主要コンポーネントの準備・提供の現状



[26] 製造工場等では、IoT サービス利用者が IoT 機器を調達し、FA ベンダーからエッジコンピュータを導入することも多いことを付記しておく。

【エッジコンピュータ/通信ゲートウェイの提供】

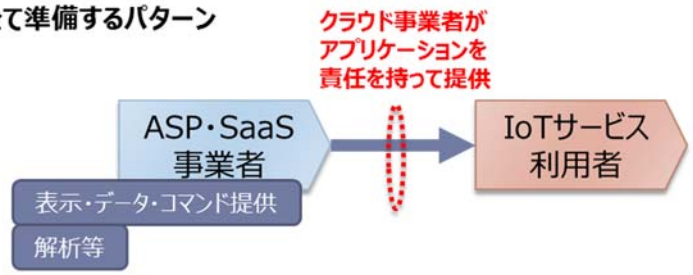
②－１　ASP・SaaS事業者が全て準備するパターン



②－２　通信ゲートウェイの提供を他の事業者に任せるパターン

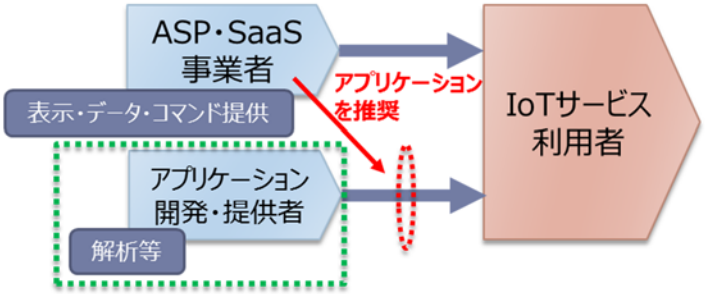
【アプリケーションの提供（表示・データ・コマンド提供、解析等）】

③－１　ASP・SaaS事業者が全て準備するパターン



③－２　解析等のアプリケーションを他の事業者から調達するパターン

③－３　解析等のアプリケーションは提供せず、推奨に留めるパターン



（イ）IoT サービスを実行するためのロール

IoT サービスを実行するため、「計測」「ローカル伝送」「前処理」「インターネット接続」「取得」「収集・保管」「処理・分析」「表示・データ・コマンド提供」「データ外部提供」「駆動前処理」「駆動」という 11 の役割をロールとして定義し（図表 11 参照）、この順序からなるロールの連鎖によって IoT サービス構造をモデル化する（図表 12 参照）。

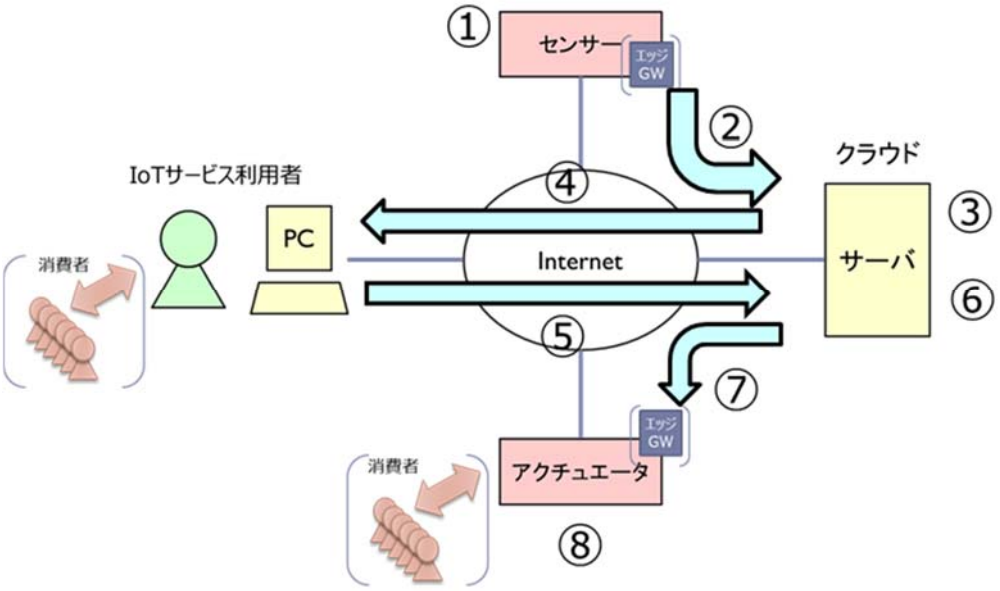
図表 11　IoT サービスを実行するためのロールの定義

項番	ロール名	概要	IoT サービスの類型図との関係*
a	計測	センサーデータの提供	①
b	ローカル伝送	IoT サービス利用者のローカル区画（フィールド、工場、職場等）内で行われるデータ伝送	①
c	前処理	エッジサービス等がデータに対して行う処理	①
d	インターネット接続	データ伝送のためのインターネットとの接続	②④⑤⑦
e	取得	クラウド上でのデータの取得	③
f	収集・保管	取得したデータのクラウド上での集約と保管	③
g	処理・分析	保管しているデータの処理・分析、加工済みデータの作成等	③
h	表示・データ・コマンド提供	IoT サービス利用者への処理・分析結果の提供（画面表示、加工済みデータのダウンロード等）	③
		IoT 機器への制御コマンドの提供（IoT サービス利用者の指示、処理・分析結果に基づく自動処理を含む）等	⑥
i	データ外部提供	加工済みデータの外部クラウド、外部組織等への提供	③
j	駆動前処理	IoT 機器を駆動する制御データの検証、加工等	⑧
k	駆動	アクチュエータを制御して駆動	⑧

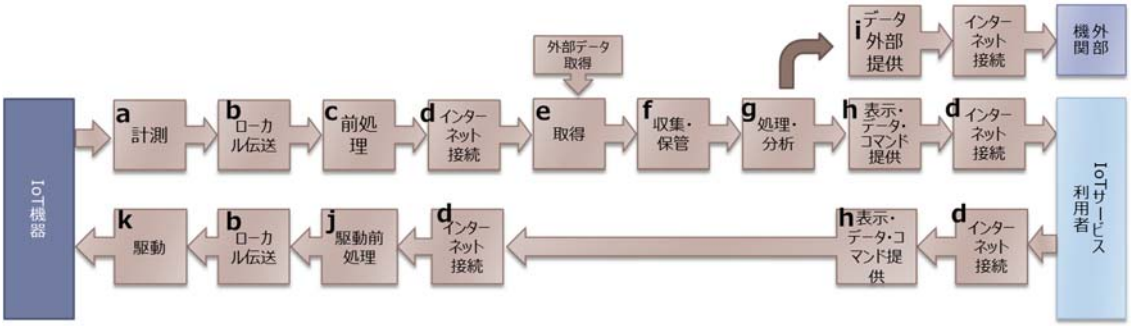
*下図中の番号を対応付けている

図表 12 IoT サービスの類型図と IoT サービスモデル

IoT サービスの類型図



IoT サービスモデル



IoT サービスでは、外部との間で積極的にデータ連携を行うことが特徴となっている。ここでは、外部からのデータ取得にあたり、外部データ計測系と接続してデータを取得するケースと、外部からデータだけを取得するケースを想定している。

データ取得のモデル化にあたり、「外部データ計測系との接続」と「外部データ取得」をどのロールで実施するかについて、以下のような想定を行う。また、これに従って、外部データの取得によりデータ価値が毀損されるリスクとその対応策を、どのロールと関係づけて整理すれば良いかを定めている。

（Ⅳ．４．３．C、Ⅳ．５．C 参照）

① 外部データ計測系との接続

LAN 経由で IoT サービスに繋ぐ場合：「前処理」に接続

WAN 経由で IoT サービスに繋ぐ場合：「取得」に接続

② 外部からデータを取得

「収集・保管」又は「処理・分析」（データ解析時にオープンデータ等を取得する場合）

Ⅳ．２．１．２．IoT サービスの提供に必要なコンポーネント

ロールを実行するためには、IoT 機器を始めとした各種の「コンポーネント」が必要となる。図表 13 に「コンポーネントの種別」を列挙した。また、これらのコンポーネントが主としてどのロールで使用されるかについても図表 14 に「ロールとコンポーネントの対応」を示した。

図表 13 コンポーネントの種別

分類	コンポーネント	例示
IoT 機器	IoT 機器	センサーやアクチュエータなどを組み込んだ機器を含むエンドデバイス。内蔵された制御装置も含めてセンサー・アクチュエータとする。
ローカル側（IoT 機器の繋ぎ込みからインターネットとの接点までの区間） ※IoT サービス利用者の PC 環境は含んでいない	LAN	LAN を構成する通信機器等
	ローカルコンピュータ	工場プラントの制御コンピュータ等、アクチュエータ等とは切り離されて外部コンピュータに搭載された制御システム
	エッジコンピュータ	エッジサービスの提供に用いられる ICT 機器/アプリケーション
	通信ゲートウェイ	LAN と WAN を接続する ICT 機器/ソフトウェア
ネットワーク・クラウド側	WAN	WAN を構成する通信機器等
	クラウド	ASP・SaaS
		PaaS、IaaS
アプリケーション	組込みアプリケーション	IoT 機器に組み込んで使用するソフトウェア
	アプリケーション（表示・データ・コマンド提供、データ解析等）	■ASP・SaaS のサービス提供で用いる業務ロジック処理用のアプリケーション等 ■データ解析を行うための AI 処理等（ディープラーニング、機械学習等）

図表 14　ロールとコンポーネントの対応

項番	ロール名	ロールの実行にあたり用いるコンポーネント
a	計測	IoT 機器、組込みアプリケーション
b	ローカル伝送	LAN
c	前処理	エッジコンピュータ
d	インターネット接続	通信ゲートウェイ、WAN
e	取得	クラウド（PaaS、IaaS）
f	収集・保管	クラウド（PaaS、IaaS）
g	処理・分析	クラウド（ASP・SaaS）、アプリケーション
h	表示・データ・コマンド提供	クラウド（ASP・SaaS）、アプリケーション
i	データ外部提供	クラウド（ASP・SaaS 、PaaS、IaaS）
j	駆動前処理	エッジコンピュータ
k	駆動	IoT 機器、ローカルコンピュータ、組込みアプリケーション

Ⅳ．２．２．三つの観点ごとのリスク

A【多様な事業者間連携】に起因する事業者連携等の問題がサービス全体に影響を及ぼすリスクの整理

事業者連携等の問題がサービス全体に影響を及ぼすリスクを、以下の四つの区分に分類・整理して示す。

a. 連携事業者間で管理水準が異なることで生じる問題
b. サービスの継続性の阻害
c. 契約による責任分担の割り当てに関して生じる問題
d. 構成管理に関して生じる問題

凡例：★下線→IoT サービスリスクとして特に重要なもの
下線→IoT サービスに特徴的なその他のリスク
何もなし→IoT サービスに特徴的とは言いがたいその他のリスク

分類	IoT サービスで特徴的な問題点	事業者連携等の問題がサービス全体に影響を及ぼすリスク
a. 連携事業者間で管理水準が異なることで生じる問題	一貫したポリシーや管理運用基準が存在しない	セキュリティ管理水準が低い連携事業者のセキュリティが破られるリスク 一部の連携事業者のため IoT サービス全体のサービスレベルが下がるリスク ★事故時にサービス全体で円滑な対応ができないリスク 連携事業者間で障害切り分けがばらばらに行われるリスク ★振る舞いがおかしい IoT 機器をすぐに止めることができないリスク
	IoT サービスで使用するコンポーネントのセキュリティ強度や信頼性のばらつきが大きい	セキュリティが弱いコンポーネントのセキュリティが破られるリスク 信頼性が低いコンポーネントが IoT サービス全体のサービスレベルを下げるリスク
	サービスレベルが保証しにくいロールがある	一部の連携事業者のため IoT サービス全体のサービスレベルが下がるリスク
	事故発生時の責任が契約等で十分に明示されず、あいまいになっている	連携事業者の管理強化への意識付けが働かないリスク ★クラウド事業者が想定外の責任を負うリスク
	クラウド事業者との契約関係がない（利用者が選定等）事業者の管理レベルが低い	契約関係がない事業者のセキュリティが破られるリスク 契約関係がない事業者のため IoT サービス全体のサービスレベルが下がるリスク ★事故時にサービス全体で円滑な対応ができないリスク
b. サービスの継続性の阻害	IoT サービス全体で事故時影響評価やサービス継続対策に取り組んでいない	★IoT サービスや外部データ提供が長時間停止するリスク ★特定のコンポーネントに長時間停止の原因が集中するリスク
c. 契約による責任分担の割	クラウド事業者と連携事業者間の契約が、全体として、IoT サービス全体の責任分担を網羅できていない	★クラウド事業者が想定外の責任を負うリスク

り当てに関して生じる問題	クラウド事業者と連携事業者間の契約がサイバー攻撃に対する責任分担を明示していない	★クラウド事業者が想定外の責任を負うリスク ★サイバー攻撃に対する責任分担が不明確となるリスク
	IoT サービス利用者の責任分担が契約で明示されず、あいまいになっている	★クラウド事業者が想定外の責任を負うリスク ★IoT サービス利用者が想定外の IoT 機器等を接続するリスク ★IoT サービス利用者が調達する IoT 機器/アプリケーション/事業者等をクラウド事業者が十分に統制できないリスク ★IoT サービス利用者が問題のあるアプリケーションやデータを使用するリスク（違法である等）
	特別な要求に対応できる契約をしていない	★加工済みデータ提供のサービスレベル（可用性や持続性）要求にミスマッチが生じるリスク
d. 構成管理に関して生じる問題	許可していないコンポーネントが使われている	★クラウド事業者が想定外の責任を負うリスク ★セキュリティが弱い簡易なコンポーネントが無断で使用されるリスク ★セーフティリスクを持つ IoT 機器や重要機器（医療機器、高い信頼性や可用性が求められる機器、秘匿性の高いデータを取得する機器等）の接続・使用を把握できないリスク
	コンポーネントのぜい弱性管理（パッチを当てる等）の運用がばらばらである	セキュリティが弱いコンポーネントのセキュリティが破られるリスク セキュリティが弱いコンポーネントの改善が進まないリスク
	リスクの高いコンポーネントの使用を把握していない	★クラウド事業者が想定外の責任を負うリスク ★セーフティリスクを適切に移転できないリスク

B【ロールを実行するコンポーネントと運用・保守の多様な提供形態】に起因するコンポーネントリスクの整理

コンポーネントリスクは、コンポーネントが内在するリスク、コンポーネントの正しい使い方・維持の仕方が守られないことで生じる人に関わるリスク、コンプライアンスリスクから構成される。以下では、コンポーネントリスクをコンポーネントごとに整理して示す。

(ア) IoT 機器のコンポーネントリスク

凡例：★下線→IoT サービスリスクとして特に重要なもの

下線→IoT サービスに特徴的なその他のリスク

何もなし→IoT サービスに特徴的とは言いがたいその他のリスク

分類	IoT サービスとしての問題点	IoT 機器のコンポーネントリスク
モノのリスク（人への危害）の発生	アクチュエータの乗っ取りにより、人に物理的障害・健康障害を生じる。機械的動作、通電、熱の発生、放射線の発生、墜落の誘発、危険な物質への接触、健康に害を及ぼす環境破壊等が関係する。	★サイバー攻撃を受けることで、人に物理的障害・健康障害を生じるリスク ★サイバー攻撃に対する責任の所在があいまいになるリスク
	アクチュエータの乗っ取りにより、人の環境を阻害する。騒音、振動、有害物質の漏えい、放射線の曝露等が関係する。	★サイバー攻撃を受けることで、人の環境を阻害するリスク ★サイバー攻撃に対する責任の所在があいまいになるリスク
IoT 機器の数量	IoT 機器の数が知らぬ間に急増する	IoT 機器の利用管理が破綻するリスク IoT サービスを不正利用されるリスク IoT サービスがリソース不足に陥るリスク
	多数の IoT 機器が一斉に再起動・再接続する	★バースト的なトラヒックによりクラウド側に急激なピーク負荷を掛けるリスク
	一つのゲートウェイに多数/無数の IoT 機器が繋がる	ゲートウェイの処理能力を超えるリスク
IoT 機器の種類	重要インフラ等へ直接/間接*につながる（知らぬ間につながることを含む）*提供データの転得等	★想定外の重い責任を負うリスク
	多様な OS・通信方式・データ形式の混在（長期間使われた古いものの混在を含む）	ぜい弱性が残るリスク ★DDoS で悪用されるリスク ★センサーデータの改ざん/欠損が生じるリスク セキュリティが弱い IoT 機器が残るリスク
	自動アップデートできない IoT 機器もある	管理コスト増大リスク ぜい弱性が残るリスク ★DDoS で悪用されるリスク ★センサーデータの改ざん/欠損が生じるリスク

	外国製のセキュリティを考慮して設計されていない IoT 機器を輸入して使用する（知らぬ間に使うことを含む）	ぜい弱性が残るリスク ★DDoS で悪用されるリスク ★センサーデータの改ざん/欠損が生じるリスク セキュリティが弱い IoT 機器が残るリスク ★コンプライアンスリスク
IoT 機器の品質	低品質・低性能の粗悪品が接続される	★野良デバイスが接続されるリスク ぜい弱性が残るリスク ★DDoS で悪用されるリスク ★センサーデータの改ざん/欠損が生じるリスク セキュリティが弱い IoT 機器が残るリスク 故障でセンサーデータが欠損するリスク
	サービスレベルが保証されない	★IoT サービス利用者が求めるサービスレベルを維持できないリスク
IoT 機器の移動	スマホなど不特定多数の IoT 機器がつながる	管理コスト増大リスク セキュリティが弱い IoT 機器が残るリスク
	使用場所/使用者が知らぬ間に変わる	管理されていない IoT 機器が接続されるリスク
	知らぬ間に国・地域を越える	★コンプライアンスリスク
	盗撮/盗聴などの犯罪に使用される	コンプライアンスリスク
IoT 機器の消滅	紛失	IoT 機器の紛失リスク 不測のデータ欠損リスク
	盗難	IoT 機器の盗難・破壊リスク 不測のデータ欠損リスク
	故障（破損/短絡/水没等）	IoT 機器の故障リスク 不測のデータ欠損リスク
	メモリーオーバー等によるフリーズ	IoT 機器が制御不能になる 不測のデータ欠損リスク
	電池切れ/限られた電源供給で動作する	不測のデータ欠損リスク
	ソフト不具合の放置/更新失敗	ぜい弱性が残るリスク IoT 機器が正しく動作しない/停止するリスク
IoT 機器からの情報漏えい	機器情報、機器認証情報、ソフトウェアの状態/設定情報等が漏えい	★IoT 機器への攻撃手法を考案するために悪用されるリスク
	個人情報や重要データ（営業秘密等）が漏えい	コンプライアンスリスク（個人情報保護） 事業が損失を受けるリスク
IoT 機器の管理責任	IoT サービス利用者が無許可の IoT 機器を接続する	野良デバイスとなるリスク ぜい弱性が残るリスク

		★DDoS で悪用されるリスク ★センサーデータの改ざん/欠損が生じるリスク セキュリティが弱い IoT 機器が残るリスク
	登録、接続管理、機器管理ができていない	★この表中の全ての分類の原因となりうる
	販売/レンタル/譲渡により当事者が変わる	管理されていない IoT 機器が接続されるリスク
	放置/放棄され管理者不在となる	野良デバイスとなるリスク ぜい弱性が残るリスク ★DDoS で悪用されるリスク ★センサーデータの改ざん/欠損が生じるリスク セキュリティが弱い IoT 機器が残るリスク
	無人の場所で自動運転される	IoT 機器の異常起動・運転・停止リスク IoT 機器を再起動できないリスク ★センサーデータの改ざん/欠損が生じるリスク ★IoT 機器が物理的に破壊されるリスク
	経験やスキルが足りない人員が IoT 機器を運用する	IoT 機器が正しく運用・保守されないリスク ★人材育成が技術の急速な進歩に追随できないリスク
	運用・保守要員の不足（地域的な偏在を含む）	人手不足のため正しい運用・保守を実施できないリスク

（イ）ローカル側のコンポーネントリスク

凡例：★下線→IoT サービスリスクとして特に重要なもの

下線→IoT サービスに特徴的なその他のリスク

何もなし→IoT サービスに特徴的とは言いがたいその他のリスク

大分類	中分類	IoT サービスとしての問題点	ローカル側のコンポーネントリスク
LAN	モノのリスクが残留する IoT 機器との接続	モノのリスク（＝人への危害）を発生させる IoT 機器と繋がる	★モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）
	通信方式	LPWA などの多様な方式が混在する	セキュリティが弱い方式が使われるリスク データ/コマンドが盗聴・改ざんされるリスク
		重要機器が脆弱な通信方式で繋がる	★データ/コマンドが盗聴・改ざんされるリスク ★秘密が漏えいするリスク
	管理責任	所有者・占有者・使用者・管理者の異なる複数の LAN を構成する通信機器等が繋がる	LAN を構成する通信機器等のうちセキュリティが弱いものを踏み台にして攻撃されるリスク
		所有・占有・使用・管理の会社が異なる場合もある	管理責任があいまいになるリスク
		構成機器の登録・接続管理・管理ができていない	LAN の全ての中分類の原因となる
ローカルコンピュータ	モノのリスクが残留する IoT 機器との接続	モノのリスク（＝人への危害）を発生させる IoT 機器と繋がる ※基本的には、IoT 機器の製造者がローカルコンピュータを提供している	★モノのサイバー攻撃に悪用されるリスク
	OS	多様な OS の混在	管理コスト増大リスク セキュリティが弱い OS を踏み台として攻撃されるリスク
		古い OS が長期使用される	★サポート切れでぜい弱性が残るリスク セキュリティが弱い OS を踏み台として攻撃されるリスク

	動作条件	停止 NG(常時動作必須)の PC がある	★停止で重大な損害を生じるリスク
		セキュリティパッチ NG の PC がある	★セキュリティが弱い OS を踏み台として攻撃されるリスク
	管理責任	構成機器の登録・接続管理・管理ができていない	ローカルコンピュータの全ての中分類の原因となる
エッジコンピュータ	モノのリスクが残留する IoT 機器との接続	モノのリスク（＝人への危害）を発生させる IoT 機器と繋がる	★モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）
	踏み台にされる	IoT 機器へのサイバー攻撃の踏み台にされる	★センサーデータの改ざん/欠損が生じるリスク
	DDoS 攻撃	IoT 機器が乗っ取られ DDoS 攻撃を受ける	DDoS 攻撃を受けるリスク
	アプリケーションソフト	サードパーティのアプリケーションが多用される	ぜい弱性が残るリスク 管理が徹底しないリスク ★運用保守者のスキルが不十分であるリスク
		オープンソースソフトウェアが多用される	ぜい弱性が残るリスク オープンソースの管理が徹底しないリスク
		クラウド上のソフトウェアをエッジ上で動かすことがある	管理が徹底しないリスク ★運用保守者のスキルが不十分であるリスク
	エッジサービスの品質	サービスレベルが保証されない	★IoT サービス利用者が求めるサービスレベルを維持できないリスク
	管理責任	構成機器の登録・接続管理・管理ができていない	エッジコンピュータの全ての中分類の原因となる
通信ゲートウェイ	モノのリスクが残留する IoT 機器との接続	モノのリスク（＝人への危害）を発生させる IoT 機器と繋がる	★モノのサイバー攻撃に悪用されるリスク
	DDoS 攻撃	IoT 機器が乗っ取られ DDoS 攻撃を受ける	DDoS 攻撃を受けるリスク
	踏み台にされる	IoT 機器へのサイバー攻撃の踏み台にされる	センサーデータの改ざん/欠損が生じるリスク
	提供形態	IoT 機器と一体提供される（組込 SIM）	ぜい弱性が残るリスク 管理が徹底しないリスク

	管理責任	販売/レンタル/譲渡により当事者が変わる	管理責任があいまいになるリスク 運用保守者のスキルが不十分であるリスク
		放置/放棄され管理者不在となる	管理されないリスク ぜい弱性が残るリスク 踏み台にされても気付かないリスク
		構成機器の登録・接続管理・管理ができていない	通信ゲートウェイの全ての中分類の原因となる

(ウ) ネットワーク・クラウド側のコンポーネントリスク

凡例：★下線→IoT サービスリスクとして特に重要なもの
下線→IoT サービスに特徴的なその他のリスク
何もなし→IoT サービスに特徴的とは言いがたいその他のリスク

大分類	中分類	IoT サービスとしての問題点	ネットワーク・クラウド側のコンポーネントリスク
WAN	提供事業者	従来の通信キャリア以外の企業も増加	サービスレベルが不足するリスク 緊急対応がうまくいかないリスク
		国内外の複数キャリアを併用	海外キャリアの管理が不十分であるリスク 外国法の規制を受けるリスク
	接続方式	グローバル SIM の利用が増える	海外キャリアの管理が不十分であるリスク 外国法の規制を受けるリスク
		LPWA など多様な方式が混在	★セキュリティが弱い方式が使われるリスク ★データが盗聴・改ざんされるリスク
クラウド	モノのリスクが残留する IoT 機器との接続	モノのリスク（＝人への危害）を発生させる IoT 機器と繋がる	★モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）
	DDoS 攻撃	IoT 機器が乗っ取られ DDoS 攻撃を受ける	DDoS 攻撃を受けるリスク
	踏み台にされる	IoT 機器へのサイバー攻撃の踏み台にされる	センサーデータの改ざん/欠損が生じるリスク
	通信回線	インターネットと閉域網の併用	インターネット側からの攻撃でクラウドに侵入されるリスク

	接続形態	用途により異なるクラウド基盤と繋がる（マルチクラウド構成）	★他のクラウドの先に重要インフラや人の命を脅かすリスクが残る IoT 機器が接続されているリスク
		SDN・NFV により動作場所が随時変化する	管理が徹底しないリスク 運用保守者のスキルが不十分であるリスク
	処理容量	バースト的な制御不能挙動への対抗手段	★バースト的なトラヒックによりクラウド側に急激なピーク負荷がかかるリスク
	IoT サービス利用者による違法な利用	（「サービス提供」のロールで、IoT サービス利用者が、自ら持つ別データの格納やこれを用いた解析、自ら持ってきたアプリケーション（特に解析用のもの）のインストールやこれを用いた解析等を行うことが可能な場合） IoT サービス利用者が、違法なデータ/アプリケーションを格納して利用	IoT サービス利用者による違法な利用に気付かないリスク
			違法な利用を行う IoT サービス利用者への捜査等が他の利用者に影響を及ぼすリスク

(エ) アプリケーションに関わるコンポーネントリスク

凡例：★下線→IoT サービスリスクとして特に重要なもの

下線→IoT サービスに特徴的なその他のリスク

何もなし→IoT サービスに特徴的とは言いがたいその他のリスク

大分類	中分類	IoT サービスとしての問題点	アプリケーションに関わるコンポーネントリスク
組込みアプリケーション	ぜい弱性	モノのリスクの発生に繋がりうるぜい弱性	★IoT 機器のモノのリスク（＝人への危害）を発生させるリスク（センサーデータや制御コマンドの改ざん）
	IoT 機器への攻撃	IoT 機器へのサイバー攻撃に悪用される	★センサーデータの改ざん/欠損が生じるリスク
	アップデート	マルウェアを組込む等で不正化されたアップデートの適用	リモートアップデートを悪用してマルウェアを送り込まれるリスク
	バックドア	アプリケーションを保守するバックドアの悪用	アプリケーション保守用のバックドアを悪用してマルウェアを送り込まれるリスク
	管理責任	登録・管理ができていない	組込みアプリケーションの全ての中分類の原因となる
アプリケーション（表示・データ・コマンド提供、データ解析等）	データ処理品質	不正確な AI 処理	不正確な AI 処理により加工済みデータの品質が低下するリスク
	セキュリティ管理	アプリケーションの不正な改ざん	改ざんされたアプリケーションが導出した不正な結果が利用されるリスク
	管理責任	登録・管理ができていない	アプリケーションの全ての中分類の原因となる

C【多様なデータ取扱形態】に起因するデータ価値やデータに係る法令順守を毀損するリスクの整理

データ価値やデータに係る法令順守を毀損するリスクを、以下の二つの区分に分類・整理して示す。

a. データ価値の毀損

b. データ提供の強制的な停止

凡例：★下線→IoT サービスリスクとして特に重要なもの

下線→IoT サービスに特徴的なその他のリスク

何もなし→IoT サービスに特徴的とは言いがたいその他のリスク

大分類	中分類	IoT サービスで特徴的な問題点	データ価値やデータに係る法令順守を毀損するリスク
a. データ価値の毀損	データ量	伝搬するデータ量が多すぎる	データ管理コストの増大リスク
	データ品質	形式不一致、単位誤り等	形式が食い違うデータが混在して伝搬されるリスク 単位が異なるデータが混在して伝搬されるリスク
		低品質のデータ	★精度が低いデータが混在して伝搬されるリスク ★欠損があるデータが混在して伝搬されるリスク
	サイバー攻撃	改ざんされたデータ	改ざんされたデータが伝搬されるリスク
	IoT 機器/IT 機器の故障	データの供給が停止（センサー単位、まとまったデータセット）	欠損があるデータが混在して伝搬されるリスク データ供給が長時間停止するリスク
	データ品質確保の実施体制	IoT サービス全体でデータ品質を確認する体制が整備されていない	★データ品質の確認が不十分になるリスク ★データ品質の確認について十分なスキルを持つ要員が配置されないリスク ★データ品質確保に対する役割と責任の分担があいまいになるリスク
	外部データの取得	あらかじめ定めた基準を満たさない外部データを取得（外部センサーネットワークとの接続はしない）	★低品質の外部データが混ざって伝搬されるリスク データ供給が長時間停止するリスク ★素性が分からないセンサー（IoT 機器）からのデータを取得するリスク
		不適切なオープンデータを取得	不適切な権利処理により取得したオープンデータが混ざるリスク コンプライアンス上問題がある公開データが混ざるリスク 品質が低い公開データが混ざるリスク
		あらかじめ定めた基準を満たさない外部センサーネットワークと接続して外部データを取得	★低品質の外部データが混ざって伝搬されるリスク ★データ供給が長時間停止するリスク

			★素性が分からないセンサー（IoT 機器）からのデータを取得するリスク
	データの外部提供	重要インフラや人の命に関わる用途等、想定外の相手に加工済みデータを提供	★加工済みデータの品質要求にミスマッチが生じるリスク ★加工済みデータの提供先に想定外の大きな損害を与えるリスク
		国内市場の活性化に資する高い価値を創出しうる、あるいは保護対象となるレベルのデータの海外流出	国内市場の活性化に資する高い価値を創出しうるデータが利益を求めて市場が大きい欧米等に流出してしまうリスク
	不正な制御コマンド	不正な制御コマンド	改ざんされた制御コマンドが伝搬するリスク 間違った制御コマンドが伝搬するリスク
b. データ提供の強制的な停止	権利関係の処理	不適切な権利処理	適切な権利処理がされないままデータが伝搬されるリスク
	法規制	プライバシー保護、越境データ移転	個人データ取扱いに係るコンプライアンスリスク

Ⅳ．３．対応策を割り当てる IoT サービスリスクの抽出

ここではまず、Ⅳ．２．２．A～Ⅳ．２．２．C で列挙した個々の IoT サービスリスクから、IoT サービスに限らず ICT システム一般に見られるリスクを取り除き、対応策を割り当てる IoT サービスリスクを抽出した。

次に、リスクとリスク対応策の関係付け（リスク対策導出マップ）を整理するため、IoT サービスリスクをロールと関係付けた上で、並べ替えて分類を付与した。付与した分類は分かりやすさを考慮し、「A 多様な事業者間連携」、「B ロールを実行するコンポーネントと運用・保守の多様な提供形態」及び「C 多様なデータ取扱形態」においては、「発生しうる問題の原因」で分類を行った[27]。その結果を以下に示す。

A 多様な事業者間連携（事業者連携等の問題がサービス全体に影響を及ぼすリスク）

ロール	分類	対応策を割り当てる IoT サービスリスク
利用者契約	利用者との関係	IoT サービス利用者が想定外の IoT 機器等を接続するリスク
		IoT サービス利用者が問題のあるアプリケーションやデータを使用するリスク（違法である等）
		IoT サービス利用者が調達する IoT 機器/アプリケーション/事業者等をクラウド事業者が十分に統制できないリスク
		セキュリティが弱い簡易なコンポーネントが無断で使用されるリスク
	弱点から全体への影響の波及	契約関係がない事業者のセキュリティが破られるリスク
		契約関係がない事業者のため IoT サービス全体のサービスレベルが下がるリスク
構成管理	弱点から全体への影響の波及	セキュリティが弱いコンポーネントのセキュリティが破られるリスク
		セキュリティ管理水準が低い連携事業者のセキュリティが破られるリスク
		信頼性が低いコンポーネントが IoT サービス全体のサービスレベルを下げるリスク
	他のクラウドとの関係	セーフティリスクを持つ IoT 機器や重要機器の接続・使用を把握できないリスク
契約管理	連携事業者との関係	クラウド事業者が想定外の責任を負うリスク
		サイバー攻撃に対する責任分担が不明確となるリスク
		セーフティリスクを適切に移転できないリスク
		加工済みデータ提供のサービスレベル（可用性や持続性）要求にミスマッチが生じるリスク
		連携事業者の管理強化への意識付けが働かないリスク

[27] 実際に付与した分類を以下に示す。
A 多様な事業者間連携：「利用者との関係」「弱点から全体への影響の波及」「他のクラウドとの関係」「連携事業者との関係」「ばらばらな事故対応、サービス継続性」
B ロールを実行するコンポーネントと運用・保守の多様な提供形態：「信頼性リスク」「セキュリティリスク」「物理的セキュリティリスク」「性能リスク」「品質リスク」「運用リスク」「保守リスク」「セーフティリスク」
C 多様なデータ取扱形態：「データ量」「コンプライアンス」「データ形式の齟齬」「低品質」「改ざん」「想定外の損害」

		セキュリティが弱いコンポーネントの改善が進まないリスク
	ばらばらな事故対応、サービス継続性	連携事業者間で障害切り分けがばらばらに行われるリスク
		事故時にサービス全体で円滑な対応ができないリスク
		振る舞いがおかしい IoT 機器をすぐに止めることができないリスク
		IoT サービスや外部データ提供が長時間停止するリスク
		特定のコンポーネントに長時間停止の原因が集中するリスク

B ロールを実行するコンポーネントと運用・保守の多様な提供形態（コンポーネントリスク）

ロール	コンポーネント	分類	対応策を割り当てる IoT サービスリスク
・機器等提供 **・機器等推奨**	IoT 機器	信頼性リスク	故障でセンサーデータが欠損するリスク
			不測のデータ欠損リスク
			IoT 機器の故障リスク
			IoT 機器の異常起動・運転・停止リスク
			IoT 機器を再起動できないリスク
		セキュリティリスク	IoT サービスを不正利用されるリスク
			ぜい弱性が残るリスク
			DDoS で悪用されるリスク
			センサーデータの改ざん/欠損が生じるリスク
			セキュリティが弱い IoT 機器が残るリスク
			IoT 機器への攻撃手法を考案するために悪用されるリスク
			コンプライアンスリスク（個人情報保護）
		性能リスク	IoT サービスがリソース不足に陥るリスク
			バースト的なトラヒックによりクラウド側に急激なピーク負荷をかけるリスク
			ゲートウェイの処理能力を超えるリスク
		品質リスク	IoT 機器が制御不能になる
			IoT 機器が正しく動作しない/停止するリスク
		セーフティリスク	サイバー攻撃を受けることで、人に物理的障害・健康障害を生じるリスク
			サイバー攻撃を受けることで、人の環境を阻害するリスク
	LAN	セキュリティリスク	セキュリティが弱い方式が使われるリスク
			データ/コマンドが盗聴・改ざんされるリスク
			秘密が漏えいするリスク
			セキュリティが弱い LAN を踏み台にして攻撃されるリスク

		セーフティリスク	モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）
	ローカルコンピュータ	セキュリティリスク	セキュリティが弱い OS を踏み台として攻撃されるリスク
			サポート切れでぜい弱性が残るリスク
		セーフティリスク	モノのサイバー攻撃に悪用されるリスク
	エッジコンピュータ	セキュリティリスク	ぜい弱性が残るリスク
			DDoS 攻撃を受けるリスク
			センサーデータの改ざん/欠損が生じるリスク
		セーフティリスク	モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）
	通信ゲートウェイ	セキュリティリスク	ぜい弱性が残るリスク
			DDoS 攻撃を受けるリスク
			センサーデータの改ざん/欠損が生じるリスク
		セーフティリスク	モノのサイバー攻撃に悪用されるリスク
	WAN	セキュリティリスク	外国法の規制を受けるリスク
	クラウド	セキュリティリスク	DDoS 攻撃を受けるリスク
		性能リスク	バースト的なトラヒックによりクラウド側に急激なピーク負荷がかかるリスク
		セーフティリスク	モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）
	組込みアプリケーション	セキュリティリスク	センサーデータの改ざん/欠損が生じるリスク
		セーフティリスク	IoT 機器のモノのリスク（＝人への危害）を発生させるリスク（センサーデータや制御コマンドの改ざん）
	アプリケーション（表示・データ・コマンド提供、データ解析等）	セキュリティリスク	改ざんされたアプリケーションが導出した不正な結果が利用されるリスク
		品質リスク	不正確な AI 処理により加工済みデータの品質が低下するリスク
・IoT サービスを実行するためのロール ・契約管理（ロールの実行の委託に関するもの）	IoT 機器	物理的セキュリティリスク	IoT 機器の紛失リスク
			IoT 機器の盗難・破壊リスク
		品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク
		運用リスク	IoT 機器の利用管理が破綻するリスク
			コンプライアンスリスク
		保守リスク	野良デバイスとなるリスク
		セーフティリスク	サイバー攻撃を受けることで、人に物理的障害・健康障害を生じるリスク
			サイバー攻撃を受けることで、人の環境を阻害するリスク

	LAN	運用リスク	管理責任があいまいになるリスク
	ローカルコンピュータ	運用リスク	停止で重大な損害を生じるリスク
	エッジコンピュータ	品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク
		運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク
		保守リスク	オープンソースの管理が徹底しないリスク
	通信ゲートウェイ	運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク
		保守リスク	管理責任があいまいになるリスク
			管理が徹底しないリスク
			管理されないリスク
	クラウド	運用リスク	クラウド連携先に繋がる重要機器等へのサイバー攻撃に悪用されるリスク
		運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク
		運用リスク・保守リスク	管理が徹底しないリスク
	組込みアプリケーション	セキュリティリスク	リモートアップデートを悪用してマルウェアを送り込まれるリスク
			アプリケーション保守用のバックドアを悪用してマルウェアを送り込まれるリスク
	アプリケーション（表示・データ・コマンド提供、データ解析等）	セキュリティリスク	改ざんされたアプリケーションが導出した不正な結果が利用されるリスク
		品質リスク	不正確なデータ処理により加工済みデータの品質が低下するリスク

C 多様なデータ取扱形態（データ価値やデータに係る法令順守を毀損するリスク）

ロール	役割の種別	分類	対応策を割り当てる IoT サービスリスク
・データ監視・保全・契約管理（データ監視・保全への協力を委託するもの）	データの内容を見なくても果たせる役割	データ量	データ管理コストの増大リスク
		コンプライアンス	不適切な権利処理により取得したオープンデータが混ざるリスク
			コンプライアンス上問題がある公開データが混ざるリスク
			適切な権利処理がされないままデータが伝搬されるリスク
	データの内容を見なければ果たせない役割	コンプライアンス	個人データ取扱いに係るコンプライアンスリスク
		データ形式の齟齬	形式が食い違うデータが混在して伝搬されるリスク
			単位が異なるデータが混在して伝搬されるリスク
		低品質	精度が低いデータが混在して伝搬されるリスク
			欠損があるデータが混在して伝搬されるリスク
			データ品質の確認が不十分になるリスク
			データ品質の確認について十分なスキルを持つ要員が配置されないリスク
			データ品質確保に対する役割と責任の分担があいまいになるリスク
			低品質の外部データが混ざって伝搬されるリスク
			素性が分からないセンサー（IoT 機器）からのデータを取得するリスク
			品質が低い公開データが混ざるリスク
			加工済みデータの品質要求にミスマッチが生じるリスク
			間違った制御コマンドが伝搬するリスク
		改ざん	改ざんされたデータが伝搬されるリスク
			改ざんされた制御コマンドが伝搬するリスク
		想定外の損害	加工済みデータの提供先に想定外の大きな損害を与えるリスク

Ⅳ．４．IoT サービスを提供するクラウド事業者が取るべき対応策の導出

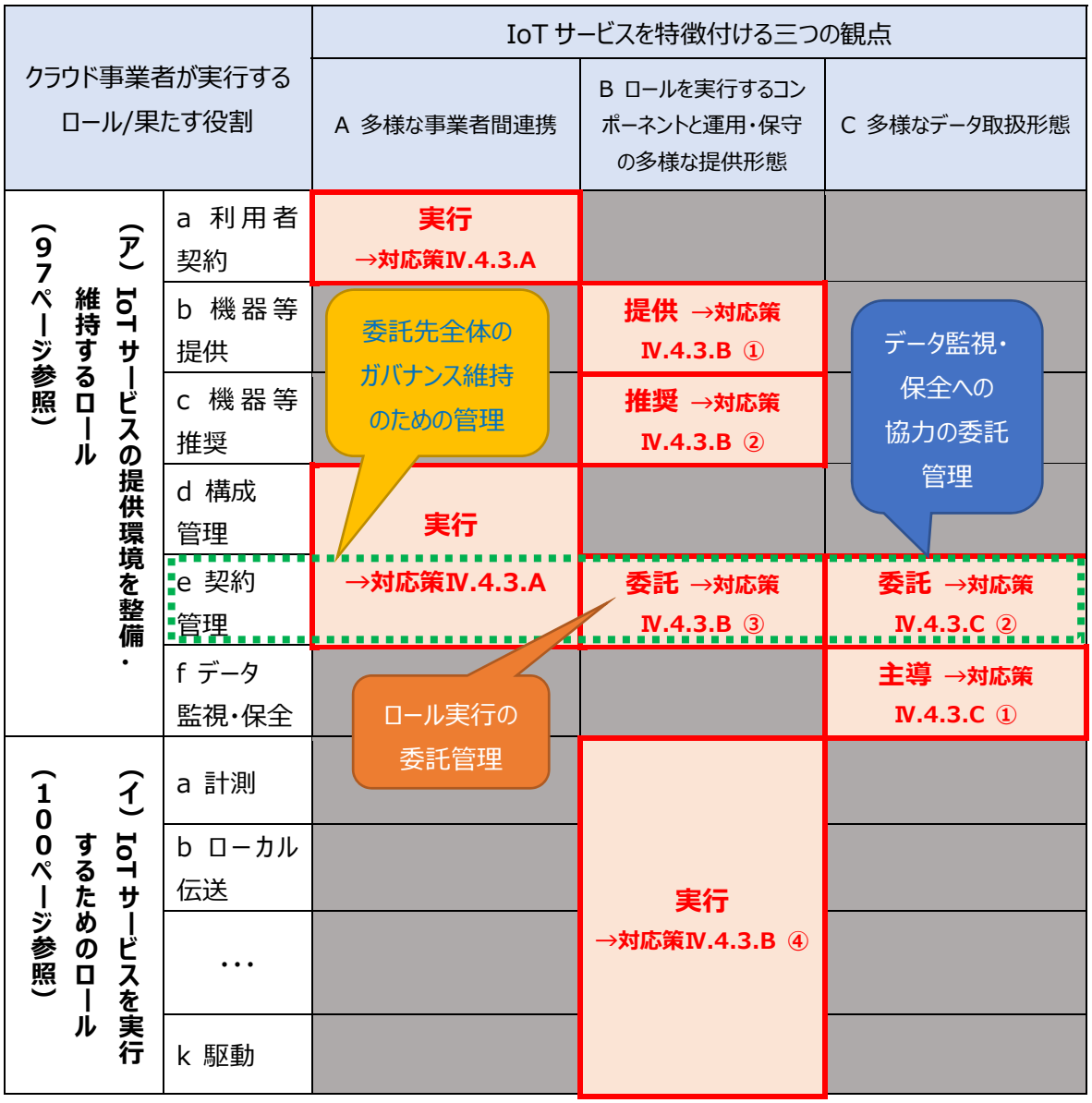
Ⅳ．４．１．対応策導出の流れ

Ⅳ．４．１．１．IoT サービスの三つの観点ごとのロール、リスク、リスク対応策の関係

第Ⅳ部では、「IoT サービス提供のロール→IoT サービスリスク→リスク対応策」の流れで読者が対応策を抽出できるように、「ロールと IoT サービスリスクの紐付け（Ⅳ．３．参照）」と「IoT サービスリスクとリスク対応策の紐付け」を整理し、これを「IoT サービスを特徴付ける三つの観点」ごとにリスク対応策導出マップとして取りまとめている。この概念について図表 15（再掲）に取りまとめた。

凡例： Ⅳ.4.3.X → 「リスク対応策導出マップ」の記載箇所

図表 15 クラウド事業者のリスクとリスク対応策の全体構成－ロール×三つの観点のマップ－



Ⅳ．４．１．２．クラウド事業者の責任範囲の把握

Ａ．「多様な事業者間連携」の観点に対するリスクと対応策

サービスによりクラウド事業者の責任範囲は変わらないため、クラウド事業者は全てのリスクに対し、対応策の実施を検討することになる。

Ｂ．「ロールを実行するコンポーネントと運用・保守の多様な提供形態」の観点に対するリスクと対応策

全てのロールにおいて、個々の IoT サービスごとにクラウド事業者の責任範囲が変化する。このため、自分が提供する IoT サービスの現状により責任範囲を把握する必要がある。

Ｃ．「多様なデータ取扱形態」の観点に対するリスクと対応策

データ内容を見るかによってクラウド事業者が考慮すべきリスクの範囲は変化し、対応策検討に係るクラウド事業者の責任範囲も、個々の IoT サービスごとに変化している。このため、自分が提供する IoT サービスの現状により責任範囲を把握する必要がある。

これを踏まえ、クラウド事業者が自ら提供する IoT サービスにおいて、どこまでの責任範囲を分担しているかを特定できる調査テンプレートを図表 16 に示す。

なお、リスク対応策導出マップから導出される対応策は、全て実施する必要があるという訳ではない。IoT サービスの実状を踏まえ、実施を検討する対応策の候補であると考えていただきたい。

図表 16　クラウド事業者の責任範囲を把握するための調査テンプレート

<table>
<tr><th colspan="3" rowspan="2">クラウド事業者が実行するロール/果たす役割</th><th colspan="2" rowspan="2">調査項目</th><th colspan="3">クラウド事業者の責任範囲（記入欄）　※○×を記入する</th></tr>
<tr><th>A 多様な事業者間連携</th><th>B ロールを実行するコンポーネントと運用・保守の多様な提供形態</th><th>C 多様なデータ取扱形態</th></tr>
<tr><td rowspan="24">（ア）IoTサービスの提供環境を整備・維持するロール</td><td>a 利用者契約</td><td colspan="2">全てのクラウド事業者が該当する</td><td>○</td><td></td><td></td></tr>
<tr><td rowspan="9">b 機器等提供（クラウド事業者が自ら機器を提供する場合）</td><td rowspan="9">提供するコンポーネント</td><td>IoT 機器</td><td></td><td rowspan="9">クラウド事業者が提供するコンポーネントに○</td><td></td></tr>
<tr><td>LAN</td><td></td><td></td><td></td></tr>
<tr><td>ローカルコンピュータ</td><td></td><td></td><td></td></tr>
<tr><td>エッジコンピュータ</td><td></td><td></td><td></td></tr>
<tr><td>通信ゲートウェイ</td><td></td><td></td><td></td></tr>
<tr><td>WAN</td><td></td><td></td><td></td></tr>
<tr><td>クラウド</td><td></td><td></td><td></td></tr>
<tr><td>組込みアプリケーション</td><td></td><td></td><td></td></tr>
<tr><td>アプリケーション（表示・データ・コマンド提供、データ解析等）</td><td></td><td></td><td></td></tr>
<tr><td rowspan="6">c 機器等推奨（クラウド事業者以外が機器を提供する場合）</td><td rowspan="6">推奨するコンポーネント</td><td>IoT 機器</td><td></td><td rowspan="6">IoT サービス利用者に推奨するコンポーネントに○</td><td></td></tr>
<tr><td>ローカルコンピュータ</td><td></td><td></td><td></td></tr>
<tr><td>エッジコンピュータ</td><td></td><td></td><td></td></tr>
<tr><td>通信ゲートウェイ</td><td></td><td></td><td></td></tr>
<tr><td>クラウド</td><td></td><td></td><td></td></tr>
<tr><td>アプリケーション（表示・データ・コマンド提供、データ解析等）</td><td></td><td></td><td></td></tr>
<tr><td>d 構成管理</td><td colspan="2">全てのクラウド事業者が該当する</td><td>○</td><td></td><td></td></tr>
<tr><td rowspan="12">e 契約管理</td><td colspan="2">全てのクラウド事業者が該当する</td><td>○</td><td></td><td></td></tr>
<tr><td colspan="2">データ内容を見てこれに責任を持つ</td><td></td><td></td><td>クラウド事業者がデータ内容を見る場合○</td></tr>
<tr><td rowspan="10">事業連携先に委託するロール</td><td>a 計測</td><td></td><td rowspan="10">連携事業者に実行を委託するロールに○</td><td>同左</td></tr>
<tr><td>b ローカル伝送</td><td></td><td>同左</td></tr>
<tr><td>c 前処理</td><td></td><td>同左</td></tr>
<tr><td>d インターネット接続</td><td></td><td>同左</td></tr>
<tr><td>e 取得</td><td></td><td>同左</td></tr>
<tr><td>f 収集・保管</td><td></td><td>同左</td></tr>
<tr><td>g 処理・分析</td><td></td><td>同左</td></tr>
<tr><td>h 表示・データ・コマンド提供</td><td></td><td>同左</td></tr>
<tr><td>i データ外部提供</td><td></td><td>同左</td></tr>
<tr><td>j 駆動前処理</td><td></td><td>同左</td></tr>
<tr><td>k 駆動</td><td></td><td></td><td></td></tr>
</table>

	f データ監視・保全	データ内容を見てこれに責任を持つ			クラウド事業者がデータ内容を見る場合○
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか		クラウド事業者が自ら実行するロールに○	
	b ローカル伝送				
	c 前処理				
	d インターネット接続				
	e 取得				
	f 収集・保管				
	g 処理・分析				
	h 表示・データ・コマンド提供				
	i データ外部提供				
	j 駆動前処理				
	k 駆動				

Ⅳ．４．１．３．対応策導出の流れ

「Ⅳ．４．１．１．」、「Ⅳ．４．１．２．」を踏まえ、IoT サービスを提供するクラウド事業者が、自ら提供している IoT サービスの実状に基づいてサービスがさらされているリスクを抽出し、それぞれについてどのような対応策を取ればいいかを見つけ出す手順について示す。具体的には、次のステップを踏むことになる。

① 図表 16 の調査テンプレートの「クラウド事業者の責任範囲（記入欄）」の赤枠で囲まれた部分に〇を記入し、各ロール/果たす役割に関するクラウド事業者の責任範囲を特定する。
② クラウド事業者の責任範囲となるロール/果たす役割に対し、これに対応するリスク対応策導出マップを確認し、自ら実施を検討すべき対応策、ロール実行を委託する者への依頼を検討すべき対応策の「項番」を抽出（図表 15、図表 17、Ⅳ．４．３．参照）
③ Ⅳ．５の対応策一覧から、「対応策項番」によって措置すべき対応策候補の内容を確認し、自ら提供している IoT サービスの実状に照らして実施を検討（Ⅳ．５．A～Ⅳ．５．C を参照）

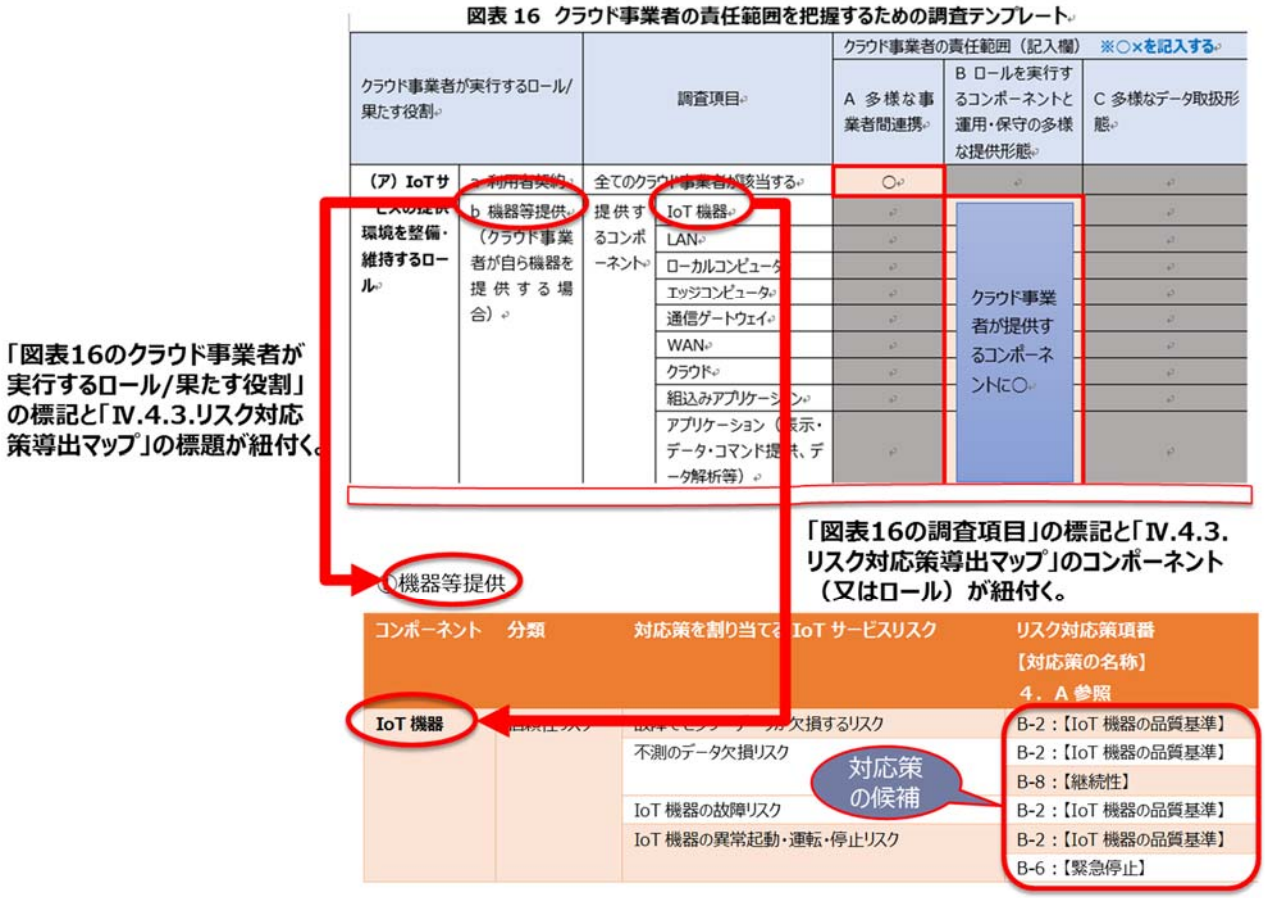
図表 17 リスク対応策導出マップの見方（1/3）

<table>
<tr><th colspan="3" rowspan="2">クラウド事業者が実行するロール/果たす役割</th><th colspan="2" rowspan="2">調査項目</th><th colspan="3">クラウド事業者の責任範囲（記入欄） ※○×を記入する</th></tr>
<tr><th>A 多様な事業者間連携</th><th>B ロールを実行するコンポーネントと運用・保守の多様な提供形態</th><th>C 多様なデータ取扱形態</th></tr>
<tr><td rowspan="15">（ア）IoTサービスの提供環境を整備・維持するロール</td><td>a 利用者契約</td><td colspan="2">全てのクラウド事業者が該当する</td><td>○</td><td></td><td></td></tr>
<tr><td rowspan="3">b 機器等提供（クラウド事業者が自ら機器を提供する場合）</td><td rowspan="3">提供するコンポーネント</td><td>IoT 機器/ローカルコンピュータ</td><td rowspan="15">Ⅳ.4.3. A の対応策を、候補として検討</td><td rowspan="3">Ⅳ.4.3. B ①を見て、○のコンポーネントに紐付くリスクの対応策を、候補として検討</td><td rowspan="3">・・・</td></tr>
<tr><td>・・・</td></tr>
<tr><td>アプリケーション（表示・データ・コマンド提供）</td></tr>
<tr><td rowspan="3">c 機器等推奨（クラウド事業者以外が機器を提供する場合）</td><td rowspan="3">推奨するコンポーネント</td><td>IoT 機器/ローカルコンピュータ</td><td rowspan="3">Ⅳ.4.3. B ②を見て、○のコンポーネントに紐付くリスクの対応策を、候補として検討</td><td rowspan="3">・・・</td></tr>
<tr><td>・・・</td></tr>
<tr><td>アプリケーション（データ解析）</td></tr>
<tr><td>d 構成管理</td><td colspan="2">全てのクラウド事業者が該当する</td><td>○</td><td></td><td></td></tr>
<tr><td rowspan="6">e 契約管理</td><td colspan="2">全てのクラウド事業者が該当する</td><td>○</td><td></td><td></td></tr>
<tr><td colspan="2">データ内容を見てこれに責任を持つ</td><td></td><td rowspan="5">Ⅳ.4.3 B ③を見て、○のロールに紐付くリスクの対応策を、候補として検討</td><td rowspan="5">Ⅳ.4.3 C ②を見て、データ内容を見る場合は全てのロールを、見ない場合は「データの内容を見なくても果たせる役割」の方のロールだけをそれぞれ対象とし、○のロールに紐付く対応策を、候補として検討（図表 19 (3/3)参照）</td></tr>
<tr><td rowspan="4">事業連携先に委託するロール</td><td>a 計測</td><td></td></tr>
<tr><td>b ローカル伝送</td><td></td></tr>
<tr><td>・・・</td><td>・・・</td></tr>
<tr><td>k 駆動</td><td></td></tr>
<tr><td>f データ監視・保全</td><td colspan="2">データ内容を見てこれに責任を持つ</td><td></td><td></td><td>○の場合はⅣ.4.3 C ①の全ての対応策を、○でない場合は「データの内容を見なくても果たせる役割」（図表 18 (2/3) 参照）のみを、候補として検討</td></tr>
<tr><td rowspan="4">（イ）IoTサービスを実行するためのロール</td><td>a 計測</td><td colspan="2" rowspan="4">クラウド事業者が自らロールを実行するか</td><td></td><td rowspan="4">Ⅳ.4.3 B ④を見て、○のロールに紐付くリスクの対応策を、候補として検討</td><td></td></tr>
<tr><td>b ローカル伝送</td><td></td><td></td></tr>
<tr><td>・・・</td><td>・・・</td><td>・・・</td></tr>
<tr><td>k 駆動</td><td></td><td></td></tr>
</table>

図表 18 リスク対応策導出マップの見方（2/3）

【B の機器等提供（Ⅳ．４．３．B ①）】の確認の仕方

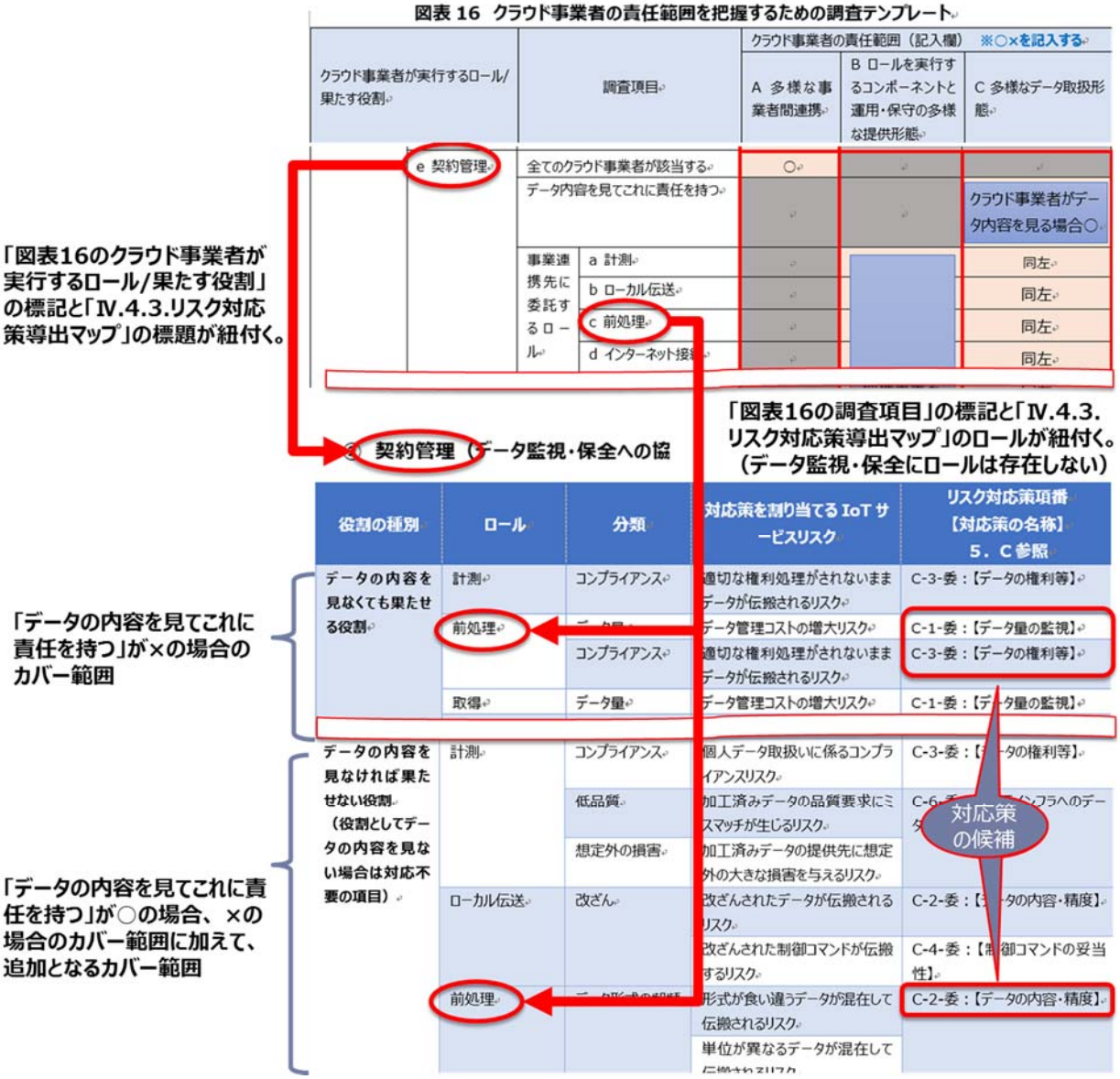
※機器等推奨（Ⅳ．４．３．B ②）、契約管理（Ⅳ．４．３．B ③）及び IoT サービスを実行するロール（Ⅳ．４．３．B ④）も同様



図表 19 リスク対応策導出マップの見方（3/3）

【C の契約管理（Ⅳ．４．３．C ②）】の確認の仕方

※データ監視・保全（Ⅳ．４．３．C ①）も同様



（注）外部データの取得に対する対応策（C-5-ク/C-5-委）は、以下の四つの状況のどれかが当てはまる場合に実施を検討すること。（Ⅳ．２．１．１．（イ）参照）

■「前処理」において、LAN 経由で外部データ計測系と接続

■「取得」において、WAN 経由で外部データ計測系と接続

■「収集・保管」において、外部からデータを取得

■「処理・分析」において、データ解析時にオープンデータ等を取得

（注）Ⅳ．５．C ②で対応策を特定する際には、「事業連携先に委託するロール」→「対応策項番」の順に探すこと。ロールが違うと、対応策項番が同じでも、「クラウド事業者からロールの実行者に移転すべき役割」の内容が異なる場合がある。

Ⅳ．４．２．調査テンプレートへの記入例

典型的なケースとして、以下の場合を想定する。この場合の調査テンプレートの記入例を図表 20 に示す。

- クラウド事業者が、全てのロールを自分で実行する
- 組込みアプリケーションを除く全てのコンポーネントを自分で提供する
- データ内容を見ている
- 外部からのデータ取得はしていない
- データの外部提供は行っている

この他に、巻末の Annex8 で IoT サービスの六つの事例を提示し、それぞれに対して調査テンプレートの記入例を示している。図表 20 及び巻末の六つの事例のうち、自ら提供している IoT サービスと形態が類似しているものを特定することができれば、対応する調査テンプレートの記入例を参考にすることで、記入がしやすい。

図表 20　典型的なケースでの調査テンプレートの記入例

クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄）　※○×を記入する		
				A 多様な事業者間連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器		○	
			LAN		○	
			ローカルコンピュータ		○	
			エッジコンピュータ		○	
			通信ゲートウェイ		○	
			WAN		○	
			クラウド		○	
			組込みアプリケーション		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		○	
	c 機器等推奨（クラウド事業者以外が機器を提供する場合）	推奨するコンポーネント	IoT 機器		×	
			ローカルコンピュータ		×	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			クラウド		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	

	d 構成管理	全てのクラウド事業者が該当する		○		
	e 契約管理	全てのクラウド事業者が該当する		○		
		データ内容を見てこれに責任を持つ				○
		事業連携先に委託するロール	a 計測		×	×
			b ローカル伝送		×	× *データ内容を見ない場合は記入不要
			c 前処理		×	×
			d インターネット接続		○	○ *データ内容を見ない場合は記入不要
			e 取得		×	×
			f 収集・保管		×	×
			g 処理・分析		×	×
			h 表示・データ・コマンド提供		×	×
			i データ外部提供		×	×
			j 駆動前処理		×	× *データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				○
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			○	
	b ローカル伝送				○	
	c 前処理				○	
	d インターネット接続				×	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				○	
	h 表示・データ・コマンド提供				○	
	i データ外部提供				○	
	j 駆動前処理				○	
	k 駆動				○	

Ⅳ．４．３．リスク対応策導出マップ

A 多様な事業者間連携

ロール	分類	対応策を割り当てる IoT サービスリスク	リスク対応策項番【対応策の名称】Ⅳ．５．A 参照
利用者契約	利用者との関係	IoT サービス利用者が想定外の IoT 機器等を接続するリスク	A-1：【利用者機器の接続】
		IoT サービス利用者が問題のあるアプリケーションやデータを使用するリスク（違法である等）	A-1：【利用者機器の接続】
		IoT サービス利用者が調達する IoT 機器/アプリケーション/事業者等をクラウド事業者が十分に統制できないリスク	A-1：【利用者機器の接続】
			A-2：【持ち出し IoT 機器等の事故時の責任分担】
			A-3：【利用者が設置したエッジコンピュータ】
		セキュリティが弱い簡易なコンポーネントが無断で使用されるリスク	A-1：【利用者機器の接続】
	弱点から全体への影響の波及	契約関係がない事業者のセキュリティが破られるリスク	A-1：【利用者機器の接続】
			A-5：【構成管理と使用の一時停止】
		契約関係がない事業者のため IoT サービス全体のサービスレベルが下がるリスク	A-4：【利用者が調達したロール実行者】
構成管理	弱点から全体への影響の波及	セキュリティが弱いコンポーネントのセキュリティが破られるリスク	A-IoT-2：【要点 17：出荷・リリース後も安全安心な状態を維持する】
			A-5：【構成管理と使用の一時停止】
			A-7：【使用者】
			A-8：【集中的なセキュリティ監視】
		セキュリティ管理水準が低い連携事業者のセキュリティが破られるリスク	A-IoT-2：【要点 17：出荷・リリース後も安全安心な状態を維持する】
			A-5：【構成管理と使用の一時停止】
			A-6：【セキュリティパッチ】
			A-8：【集中的なセキュリティ監視】
		信頼性が低いコンポーネントが IoT サービス全体のサービスレベルを下げるリスク	A-5：【構成管理と使用の一時停止】
			A-7：【使用者】
	他のクラウドとの関係	セーフティリスクを持つ IoT 機器や重要機器の接続・使用を把握できないリスク	A-5：【構成管理と使用の一時停止】

契約管理	連携事業者との関係	クラウド事業者が想定外の責任を負うリスク	A-11：【セーフティリスクの責任分担】
		サイバー攻撃に対する責任分担が不明確となるリスク	A-11：【セーフティリスクの責任分担】
		セーフティリスクを適切に移転できないリスク	A-11：【セーフティリスクの責任分担】
		加工済みデータ提供のサービスレベル（可用性や持続性）要求にミスマッチが生じるリスク	A-12：【外部へのデータ提供の可用性・継続性】
		連携事業者の管理強化への意識付けが働かないリスク	A-10：【事故対応時の義務】
			A-11：【セーフティリスクの責任分担】
		セキュリティが弱いコンポーネントの改善が進まないリスク	A-10：【事故対応時の義務】
			A-11：【セーフティリスクの責任分担】
	ばらばらな事故対応、サービス継続性	連携事業者間で障害切り分けがばらばらに行われるリスク	A-9：【事故対応時の行動基準】
			A-10：【事故対応時の義務】
		事故時にサービス全体で円滑な対応ができないリスク	A-9：【事故対応時の行動基準】
			A-10：【事故対応時の義務】
		振る舞いがおかしい IoT 機器をすぐに止めることができないリスク	A-9：【事故対応時の行動基準】
			A-10：【事故対応時の義務】
		IoT サービスや外部データ提供が長時間停止するリスク	A-12：【外部へのデータ提供の可用性・継続性】
		特定のコンポーネントに長時間停止の原因が集中するリスク	A-12：【外部へのデータ提供の可用性・継続性】

B ロールを実行するコンポーネントと運用・保守の多様な提供形態

① 機器等提供

コンポーネント	分類	対応策を割り当てる IoT サービスリスク	リスク対応策項番 【対応策の名称】 5．B 参照
IoT 機器	信頼性リスク	故障でセンサーデータが欠損するリスク	B-2：【IoT 機器の品質基準】
		不測のデータ欠損リスク	B-2：【IoT 機器の品質基準】
			B-8：【継続性】
		IoT 機器の故障リスク	B-2：【IoT 機器の品質基準】
		IoT 機器の異常起動・運転・停止リスク	B-2：【IoT 機器の品質基準】
			B-6：【緊急停止】
			B-8：【継続性】
		IoT 機器を再起動できないリスク	B-2：【IoT 機器の品質基準】
	セキュリティリスク	IoT サービスを不正利用されるリスク	B-1：【IoT 機器の選定】
			B-9：【セーフティリスク以外の責任分担】
			B-10：【ローカル側セキュリティ強化】
		ぜい弱性が残るリスク	B-1：【IoT 機器の選定】
		DDoS で悪用されるリスク	B-1：【IoT 機器の選定】
			B-10：【ローカル側セキュリティ強化】
		センサーデータの改ざん/欠損が生じるリスク	B-IoT-3：「要点 14：機能及び用途に応じて適切にネットワーク接続する」
			B-1：【IoT 機器の選定】
			B-9：【セーフティリスク以外の責任分担】
			B-10：【ローカル側セキュリティ強化】
		セキュリティが弱い IoT 機器が残るリスク	B-1：【IoT 機器の選定】
		IoT 機器への攻撃手法を考案するために悪用されるリスク	B-IoT-3：「要点 14：機能及び用途に応じて適切にネットワーク接続する」
			B-10：【ローカル側セキュリティ強化】
		コンプライアンスリスク（個人情報保護）	B-IoT-3：「要点 14：機能及び用途に応じて適切にネットワーク接続する」
			B-7：【持ち出し検知】
	性能リスク	IoT サービスがリソース不足に陥るリスク	B-6：【緊急停止】
		バースト的なトラヒックによりクラウド側に急激なピーク負荷をかけるリスク	B-6：【緊急停止】
		ゲートウェイの処理能力を超えるリスク	B-6：【緊急停止】
	品質リスク	IoT 機器が制御不能になる	B-6：【緊急停止】
		IoT 機器が正しく動作しない/停止するリスク	B-2：【IoT 機器の品質基準】
			B-8：【継続性】
	セーフティリスク	サイバー攻撃を受けることで、人に物理的障害・健康障害を生じるリスク	B -IoT-1：【要点 10：安全安心を実現する設計の整合性を取る、要点 12：安全安心を実現する設計の検証・評価を行う】
			B-3：【セーフティリスクを持つ IoT 機器の提供】
			B-4：【セーフティリスクへの対応】

			B-5：【セーフティリスクに係る責任分担】
			B-10：【ローカル側セキュリティ強化】
		サイバー攻撃を受けることで、人の環境を阻害するリスク	B -IoT-1：【要点 10：安全安心を実現する設計の整合性を取る、要点 12：安全安心を実現する設計の検証・評価を行う】
			B-3：【セーフティリスクを持つ IoT 機器の提供】
			B-4：【セーフティリスクへの対応】
			B-5：【セーフティリスクに係る責任分担】
			B-10：【ローカル側セキュリティ強化】
LAN	セキュリティリスク	セキュリティが弱い方式が使われるリスク	B-IoT-3：【軽量暗号技術を採用する】
		データ/コマンドが盗聴・改ざんされるリスク	B-10：【ローカル側セキュリティ強化】
		秘密が漏えいするリスク	B-10：【ローカル側セキュリティ強化】
		セキュリティが弱い LAN を踏み台にして攻撃されるリスク	B-10：【ローカル側セキュリティ強化】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）	B-10：【ローカル側セキュリティ強化】
ローカルコンピュータ	セキュリティリスク	セキュリティが弱い OS を踏み台として攻撃されるリスク	B-10：【ローカル側セキュリティ強化】
		サポート切れでぜい弱性が残るリスク	B-10：【ローカル側セキュリティ強化】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク	B-10：【ローカル側セキュリティ強化】
エッジコンピュータ	セキュリティリスク	ぜい弱性が残るリスク	A-5：【構成管理と使用の一時停止】
		DDoS 攻撃を受けるリスク	B-1：【IoT 機器の選定】
			B-11：【ローカル側の責任分担】
		センサーデータの改ざん/欠損が生じるリスク	B-11：【ローカル側の責任分担】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）	B-11：【ローカル側の責任分担】
通信ゲートウェイ	セキュリティリスク	ぜい弱性が残るリスク	A-5：【構成管理と使用の一時停止】
		DDoS 攻撃を受けるリスク	B-1：【IoT 機器の選定】
			B-11：【ローカル側の責任分担】
		センサーデータの改ざん/欠損が生じるリスク	B-11：【ローカル側の責任分担】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク	B-11：【ローカル側の責任分担】
WAN	セキュリティリスク	外国法の規制を受けるリスク	B-7：【持ち出し検知】
クラウド	セキュリティリスク	DDoS 攻撃を受けるリスク	B-1：【IoT 機器の選定】
	性能リスク	バースト的なトラヒックによりクラウド側に急激なピーク負荷がかかるリスク	B-6：【緊急停止】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）	B-5：【セーフティリスクに係る責任分担】
組込みアプリケーション	セキュリティリスク	センサーデータの改ざん/欠損が生じるリスク	B-IoT-4：【要点 8 ：個々でも全体でも守れる設計にする】
			B-12：【自社組込みアプリの責任分担】
	セーフティリスク	IoT 機器のモノのリスク（＝人への危害）を発生させるリスク（センサーデータや制御コマンドの改ざん）	B-IoT-4：【要点 8 ：個々でも全体でも守れる設計にする】
			B-12：【自社組込みアプリの責任分担】

アプリケーション（表示・データ・コマンド提供、データ解析等）	セキュリティリスク	改ざんされたアプリケーションが導出した不正な結果が利用されるリスク	B-14：【アプリケーションのセキュリティ機能】
	品質リスク	不正確な AI 処理により加工済みデータの品質が低下するリスク	B-13：【アプリケーションの能力確保】
			B-15：【アプリケーションの責任分担】

② 機器等推奨

コンポーネント	分類	対応策を割り当てる IoT サービスリスク	リスク対応策項番【対応策の名称】5．B 参照
IoT 機器	信頼性リスク	故障でセンサーデータが欠損するリスク	B-17：【IoT 機器の品質基準】
		不測のデータ欠損リスク	B-17：【IoT 機器の品質基準】
			B-22：【継続性】
		IoT 機器の故障リスク	B-17：【IoT 機器の品質基準】
		IoT 機器の異常起動・運転・停止リスク	B-17：【IoT 機器の品質基準】
			B-20：【緊急停止】
			B-22：【継続性】
		IoT 機器を再起動できないリスク	B-17：【IoT 機器の品質基準】
	セキュリティリスク	IoT サービスを不正利用されるリスク	B-16：【IoT 機器の推奨】
			B-23：【ローカル側セキュリティ強化】
		ぜい弱性が残るリスク	B-16：【IoT 機器の推奨】
		DDoS で悪用されるリスク	B-16：【IoT 機器の推奨】
			B-23：【ローカル側セキュリティ強化】
		センサーデータの改ざん/欠損が生じるリスク	B-IoT-7：「要点 14：機能及び用途に応じて適切にネットワーク接続する」
			B-16：【IoT 機器の推奨】
			B-23：【ローカル側セキュリティ強化】
		セキュリティが弱い IoT 機器が残るリスク	B-16：【IoT 機器の推奨】
		IoT 機器への攻撃手法を考案するために悪用されるリスク	B-IoT-7：「要点 14：機能及び用途に応じて適切にネットワーク接続する」
			B-23：【ローカル側セキュリティ強化】
		コンプライアンスリスク（個人情報保護）	B-IoT-7：「要点 14：機能及び用途に応じて適切にネットワーク接続する」
			B-21：【持ち出し検知】
	性能リスク	IoT サービスがリソース不足に陥るリスク	B-20：【緊急停止】
		バースト的なトラヒックによりクラウド側に急激なピーク負荷がかかるリスク	B-20：【緊急停止】
		ゲートウェイの処理能力を超えるリスク	B-20：【緊急停止】
	品質リスク	IoT 機器が制御不能になる	B-20：【緊急停止】
		IoT 機器が正しく動作しない/停止するリスク	B-17：【IoT 機器の品質基準】
			B-22：【継続性】
	セーフティリスク	サイバー攻撃を受けることで、人に物理的障害・健康障害を生じるリスク	B-IoT-5：【要点 10：安全安心を実現する設計の整合性を取る、要点 12：安全安心を実現する設計の検証・評価を行う】

			B-18：【セーフティリスクを持つ IoT 機器の推奨】
			B-19：【セーフティリスクへの対応】
			B-23：【ローカル側セキュリティ強化】
		サイバー攻撃を受けることで、人の環境を阻害するリスク	B-IoT-5：【要点 10：安全安心を実現する設計の整合性を取る、要点 12：安全安心を実現する設計の検証・評価を行う】
			B-18：【セーフティリスクを持つ IoT 機器の推奨】
			B-19：【セーフティリスクへの対応】
			B-23：【ローカル側セキュリティ強化】
ローカルコンピュータ	セキュリティリスク	セキュリティが弱い OS を踏み台として攻撃されるリスク	B-23：【ローカル側セキュリティ強化】
		サポート切れでぜい弱性が残るリスク	B-23：【ローカル側セキュリティ強化】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク	B-23：【ローカル側セキュリティ強化】
エッジコンピュータ	セキュリティリスク	ぜい弱性が残るリスク	A-5：【構成管理と使用の一時停止】
		DDoS 攻撃を受けるリスク	B-16：【IoT 機器の推奨】
		センサーデータの改ざん/欠損が生じるリスク	B-23：【ローカル側セキュリティ強化】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）	B-19：【セーフティリスクへの対応】
通信ゲートウェイ	セキュリティリスク	ぜい弱性が残るリスク	A-5：【構成管理と使用の一時停止】
		DDoS 攻撃を受けるリスク	B-16：【IoT 機器の推奨】
		センサーデータの改ざん/欠損が生じるリスク	B-23：【ローカル側セキュリティ強化】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク	B-19：【セーフティリスクへの対応】
クラウド	セキュリティリスク	DDoS 攻撃を受けるリスク	B-16：【IoT 機器の推奨】
	性能リスク	バースト的なトラヒックによりクラウド側に急激なピーク負荷がかかるリスク	B-20：【緊急停止】
	セーフティリスク	モノのサイバー攻撃に悪用されるリスク（センサーデータや制御コマンドの改ざん）	B-19：【セーフティリスクへの対応】
アプリケーション（データ解析）	セキュリティリスク	改ざんされたアプリケーションが導出した不正な結果が利用されるリスク	B-25：【アプリケーションのセキュリティ機能】
	品質リスク	不正確な AI 処理により加工済みデータの品質が低下するリスク	B-24：【アプリケーションの能力確保】

（注） 機器等推奨に LAN、WAN が記載されていない理由として、推奨した時点で、クラウド事業者が IoT サービス利用者側の LAN、WAN 環境を監視等行うことは不可能となるため、クラウド事業者が負うべきリスクの対象範囲外となる。

推奨した場合、契約管理において、紐付く対応策を実施することとなる。（具体的には、C-2-委のローカル伝送の役割を確認すると「データ伝送中の不達や改ざんの原因調査と対策実施に協力」とある。）

③ 契約管理（ロールの実行の委託に関するもの）

実行するロール（クラウド事業者）	コンポーネント	分類	対応策を割り当てる IoT サービスリスク	リスク対応策項番【対応策の名称】5．B 参照
計測	IoT 機器	品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク	B-26：【リスク評価＆運用マニュアル】
				B-29：【ぜい弱性テストの実施】
				B-30：【必要なスキルを持つ要員の配置】
				B-31：【重要機器の接続】
				B-32：【重要機器接続時の措置】
		運用リスク	IoT 機器の利用管理が破綻するリスク	B-30：【必要なスキルを持つ要員の配置】
			コンプライアンスリスク	B-28：【IoT 機器の SIM 管理】
		保守リスク	野良デバイスとなるリスク	B-30：【必要なスキルを持つ要員の配置】
	組込みアプリケーション	セキュリティリスク	リモートアップデートを悪用してマルウェアを送り込まれるリスク	B-IoT-11：【要点 17：出荷・リリース後も安全安心な状態を維持する】
			アプリケーション保守用のバックドアを悪用してマルウェアを送り込まれるリスク	B-IoT-11：【要点 17：出荷・リリース後も安全安心な状態を維持する】
ローカル伝送	LAN	運用リスク	管理責任があいまいになるリスク	B-30：【必要なスキルを持つ要員の配置】
				B-33：【セーフティリスク対策】
前処理	エッジコンピュータ	品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク	B-33：【セーフティリスク対策】
				B-34：【エッジ上のアプリケーションの管理】
				B-35：【エッジコンピュータのなりすまし】
		運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク	B-34：【エッジ上のアプリケーションの管理】
		保守リスク	オープンソースの管理が徹底しないリスク	B-34：【エッジ上のアプリケーションの管理】
インターネット接続	通信ゲートウェイ	運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク	B-30：【必要なスキルを持つ要員の配置】
		保守リスク	管理責任があいまいになるリスク	B-30：【必要なスキルを持つ要員の配置】
				B-33：【セーフティリスク対策】
			管理が徹底しないリスク	B-30：【必要なスキルを持つ要員の配置】
			管理されないリスク	B-30：【必要なスキルを持つ要員の配置】

取得 **収集・保管** **処理・分析** **表示・データ・コマンド提供** **データ外部提供**	クラウド	運用リスク	クラウド連携先に繋がる重要機器等へのサイバー攻撃に悪用されるリスク	B-37：【クラウド連携の際の責任分担】
		運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク	B-30：【必要なスキルを持つ要員の配置】
				B-33：【セーフティリスク対策】
				B-36：【仮想化技術】
		保守リスク	管理が徹底しないリスク	B-30：【必要なスキルを持つ要員の配置】
	アプリケーション（表示・データ・コマンド提供、データ解析等）	セキュリティリスク	改ざんされたアプリケーションが導出した不正な結果が利用されるリスク	B-39：【セキュリティ管理の実行】
				B-40：【アプリケーション起因の損害の責任分担】
		品質リスク	不正確なデータ処理により加工済みデータの品質が低下するリスク	B-38：【解析するデータの確認】
				B-41：【データ品質低下の責任分担】
				B-42：【スキルを持つデータ解析要員】
駆動前処理	エッジコンピュータ	品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク	B-33：【セーフティリスク対策】
				B-34：【エッジ上のアプリケーションの管理】
				B-35：【エッジコンピュータのなりすまし】
		運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク	B-34：【エッジ上のアプリケーションの管理】
		運用リスク・保守リスク	オープンソースの管理が徹底しないリスク	B-34：【エッジ上のアプリケーションの管理】
駆動	IoT 機器	品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク	B-26：【リスク評価＆運用マニュアル】
				B-29：【ぜい弱性テストの実施】
				B-30：【必要なスキルを持つ要員の配置】
				B-31：【重要機器の接続】
				B-32：【重要機器接続時の措置】
		運用リスク	IoT 機器の利用管理が破綻するリスク	B-30：【必要なスキルを持つ要員の配置】
			コンプライアンスリスク	B-28：【IoT 機器の SIM 管理】
		保守リスク	野良デバイスとなるリスク	B-30：【必要なスキルを持つ要員の配置】
		セーフティリスク	サイバー攻撃を受けることで、人に物理的障害・健康障害を生じるリスク	B-26：【リスク評価＆運用マニュアル】
				B-27：【残留セーフティリスクの回避】
			サイバー攻撃を受けることで、人の環境を阻害するリスク	B-26：【リスク評価＆運用マニュアル】

				B-27：【残留セーフティリスクの回避】
	ローカルコンピュータ	運用リスク	停止で重大な損害を生じるリスク	B-26：【リスク評価＆運用マニュアル】
				B-30：【必要なスキルを持つ要員の配置】
				B-33：【セーフティリスク対策】
	組込みアプリケーション	セキュリティリスク	リモートアップデートを悪用してマルウェアを送り込まれるリスク	B-IoT-11：【要点 17：出荷・リリース後も安全安心な状態を維持する】
			アプリケーション保守用のバックドアを悪用してマルウェアを送り込まれるリスク	B-IoT-11：【要点 17：出荷・リリース後も安全安心な状態を維持する】

④ IoT サービスを実行するためのロール

実行を委託するロール	コンポーネント	分類	対応策を割り当てる IoT サービスリスク	リスク対応策項番【対応策の名称】5．B 参照
計測	IoT 機器	物理的セキュリティリスク	IoT 機器の紛失リスク	B-IoT-9：【要点 6 ：物理的なリスクを認識する】
			IoT 機器の盗難・破壊リスク	B-IoT-9：【要点 6 ：物理的なリスクを認識する】
		品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク	B-IoT-8：「要点 3 ：守るべきものを特定する」
				B-IoT-11：【要点 17：出荷・リリース後も安全安心な状態にする】
				B-43：【リスク評価＆運用マニュアル】
				B-46：【ぜい弱性テストの実施】
				B-47：【必要なスキルを持つ要員の配置】
				B-48：【重要機器の接続】
				B-49：【重要機器接続時の措置】
		運用リスク	IoT 機器の利用管理が破綻するリスク	B-IoT-10：【要点 16：認証機能を導入する】
				B-47：【必要なスキルを持つ要員の配置】
			コンプライアンスリスク	B-45：【IoT 機器の SIM 管理】
		保守リスク	野良デバイスとなるリスク	B-IoT-10：【要点 16：認証機能を導入する】
				B-47：【必要なスキルを持つ要員の配置】

	組込みアプリケーション	セキュリティリスク	リモートアップデートを悪用してマルウェアを送り込まれるリスク	B-IoT-10：【要点 16：認証機能を導入する】
			アプリケーション保守用のバックドアを悪用してマルウェアを送り込まれるリスク	B-IoT-10：【要点 16：認証機能を導入する】
ローカル伝送	LAN	運用リスク	管理責任があいまいになるリスク	B-47：【必要なスキルを持つ要員の配置】
				B-50：【セーフティリスク対策】
前処理	エッジコンピュータ	品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク	B-IoT-8：「要点 3 ：守るべきものを特定する」
				B-IoT-10：【要点 16：認証機能を導入する】
				B-50：【セーフティリスク対策】
				B-51：【エッジ上のアプリケーションの管理】
				B-52：【エッジコンピュータのなりすまし】
				B-53：【クラウド側要求事項の合意】
		運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク	B-51：【エッジ上のアプリケーションの管理】
		保守リスク	オープンソースの管理が徹底しないリスク	B-51：【エッジ上のアプリケーションの管理】
インターネット接続	通信ゲートウェイ	運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク	B-47：【必要なスキルを持つ要員の配置】
		保守リスク	管理責任があいまいになるリスク	B-47：【必要なスキルを持つ要員の配置】
				B-50：【セーフティリスク対策】
			管理が徹底しないリスク	B-47：【必要なスキルを持つ要員の配置】
			管理されないリスク	B-47：【必要なスキルを持つ要員の配置】
取得 **収集・保管** **処理・分析** **表示・データ・コマンド提供** **データ外部提供**	クラウド	運用リスク	クラウド連携先に繋がる重要機器等へのサイバー攻撃に悪用されるリスク	B-55：【クラウド間の接続】
		運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク	B-47：【必要なスキルを持つ要員の配置】
				B-50：【セーフティリスク対策】
				B-56：【仮想化技術】
		運用リスク・保守リスク	管理が徹底しないリスク	B-47：【必要なスキルを持つ要員の配置】
				B-53：【クラウド側要求事項の合意】
				B-54：【高リスクの IoT 機器接続対策】
				B-57：【ピーク時運用】
	アプリケーション（表示・データ・コマンド提供、データ解析等）	セキュリティリスク	改ざんされたアプリケーションが導出した不正な結果が利用されるリスク	B-IoT-8：「要点 3 ：守るべきものを特定する」
				B-IoT-11：【要点 17：出荷・リリース後も安全安心な状態にする】

				B-59：【セキュリティ管理の実行】
				B-60：ぜい弱性テストの実施
		品質リスク	不正確なデータ処理により加工済みデータの品質が低下するリスク	B-58：【解析するデータの確認】
				B-61：【スキルを持つデータ解析要員】
駆動前処理	エッジコンピュータ	品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク	B-IoT-8：「要点 3 ：守るべきものを特定する」
				B-50：【セーフティリスク対策】
				B-51：【エッジ上のアプリケーションの管理】
				B-52：【エッジコンピュータのなりすまし】
				B-53：【クラウド側要求事項の合意】
		運用リスク・保守リスク	運用保守者のスキルが不十分であるリスク	B-51：【エッジ上のアプリケーションの管理】
		保守リスク	オープンソースの管理が徹底しないリスク	B-51：【エッジ上のアプリケーションの管理】
駆動	IoT 機器	物理的セキュリティリスク	IoT 機器の紛失リスク	B-IoT-9：【要点 6 ：物理的なリスクを認識する】
			IoT 機器の盗難・破壊リスク	B-IoT-9：【要点 6 ：物理的なリスクを認識する】
		品質リスク	IoT サービス利用者が求めるサービスレベルを維持できないリスク	B-IoT-8：「要点 3 ：守るべきものを特定する」
				B-IoT-11：【要点 17：出荷・リリース後も安全安心な状態にする】
				B-43：【リスク評価＆運用マニュアル】
				B-46 ：【ぜい弱性テストの実施】
				B-47：【必要なスキルを持つ要員の配置】
				B-48：【重要機器の接続】
				B-49：【重要機器接続時の措置】
		運用リスク	IoT 機器の利用管理が破綻するリスク	B-IoT-10：【要点 16：認証機能を導入する】
				B-47：【必要なスキルを持つ要員の配置】
			コンプライアンスリスク	B-45：【IoT 機器の SIM 管理】
		保守リスク	野良デバイスとなるリスク	B-IoT-10：【要点 16：認証機能を導入する】
				B-47：【必要なスキルを持つ要員の配置】

		セーフティリスク	サイバー攻撃を受けることで、人に物理的障害・健康障害を生じるリスク	B-IoT-8：「要点３：守るべきものを特定する」
				B-43：【リスク評価＆運用マニュアル】
				B-44：【残留セーフティリスクの回避】
			サイバー攻撃を受けることで、人の環境を阻害するリスク	B-IoT-8：「要点３：守るべきものを特定する」
				B-43：【リスク評価＆運用マニュアル】
				B-44：【残留セーフティリスクの回避】
	ローカルコンピュータ	運用リスク	停止で重大な損害を生じるリスク	B-IoT-8：「要点３：守るべきものを特定する」
				B-43：【リスク評価＆運用マニュアル】
				B-47：【必要なスキルを持つ要員の配置】
				B-50：【セーフティリスク対策】
	組込みアプリケーション	セキュリティリスク	リモートアップデートを悪用してマルウェアを送り込まれるリスク	B-IoT-10：【要点 16：認証機能を導入する】
			アプリケーション保守用のバックドアを悪用してマルウェアを送り込まれるリスク	B-IoT-10：【要点 16：認証機能を導入する】

C 多様なデータ取扱形態

① データ監視・保全

役割の種別	分類	対応策を割り当てる IoT サービスリスク	リスク対応策項番【対応策の名称】Ⅳ．５．C 参照
データの内容を見なくても果たせる役割	データ量	データ管理コストの増大リスク	C-1-ク：【データ量の監視】
	コンプライアンス	不適切な権利処理により取得したオープンデータが混ざるリスク	C-3-ク：【データの権利等】
		コンプライアンス上問題がある公開データが混ざるリスク	
		適切な権利処理がされないままデータが伝搬されるリスク	
データの内容を見なければ果たせない役割	コンプライアンス	個人データ取扱いに係るコンプライアンスリスク	C-3-ク：【データの権利等】
	データ形式の齟齬	形式が食い違うデータが混在して伝搬されるリスク	C-2-ク：【データの内容・精度】
		単位が異なるデータが混在して伝搬されるリスク	
	低品質	精度が低いデータが混在して伝搬されるリスク	C-2-ク：【データの内容・精度】
		欠損があるデータが混在して伝搬されるリスク	
		データ品質の確認が不十分になるリスク	
		データ品質の確認について十分なスキルを持つ要員が配置されないリスク	
		データ品質確保に対する役割と責任の分担があいまいになるリスク	
		低品質の外部データが混ざって伝搬されるリスク	C-5-ク：【外部データの取得】
		素性が分からないセンサー（IoT 機器）からのデータを取得するリスク	
		品質が低い公開データが混ざるリスク	
		加工済みデータの品質要求にミスマッチが生じるリスク	C-6-ク：【重要インフラへのデータ提供】
		間違った制御コマンドが伝搬するリスク	C-4-ク：【制御コマンドの妥当性】
	改ざん	改ざんされたデータが伝搬されるリスク	C-2-ク：【データの内容・精度】
		改ざんされた制御コマンドが伝搬するリスク	C-4-ク：【制御コマンドの妥当性】
	想定外の損害	加工済みデータの提供先に想定外の大きな損害を与えるリスク	C-6-ク：【重要インフラへのデータ提供】
			C-7-ク：【提供データの品質】

（注）外部データの取得に対する対応策（C-5-ク）は、以下の四つの状況のどれかが当てはまる場合に実施を検討すること。（Ⅳ．２．１．１．（イ）参照）

- 「前処理」において、LAN 経由で外部データ計測系と接続
- 「取得」において、WAN 経由で外部データ計測系と接続
- 「収集・保管」において、外部からデータを取得
- 「処理・分析」において、データ解析時にオープンデータ等を取得

② 契約管理（データ監視・保全への協力を委託するもの）

役割の種別	ロール	分類	対応策を割り当てる IoT サービスリスク	リスク対応策項番【対応策の名称】Ⅳ．５．C 参照
データの内容を見なくても果たせる役割	計測	コンプライアンス	適切な権利処理がされないままデータが伝搬されるリスク	C-3-委：【データの権利等】
	前処理	データ量	データ管理コストの増大リスク	C-1-委：【データ量の監視】
		コンプライアンス	適切な権利処理がされないままデータが伝搬されるリスク	C-3-委：【データの権利等】
	取得	データ量	データ管理コストの増大リスク	C-1-委：【データ量の監視】
	収集・保管	データ量	データ管理コストの増大リスク	C-1-委：【データ量の監視】
		コンプライアンス	不適切な権利処理により取得したオープンデータが混ざるリスク	C-3-委：【データの権利等】
			コンプライアンス上問題がある公開データが混ざるリスク	
			適切な権利処理がされないままデータが伝搬されるリスク	
	処理・分析	コンプライアンス	不適切な権利処理により取得したオープンデータが混ざるリスク	C-3-委：【データの権利等】
			コンプライアンス上問題がある公開データが混ざるリスク	
			適切な権利処理がされないままデータが伝搬されるリスク	
	表示・データ・コマンド提供	コンプライアンス	適切な権利処理がされないままデータが伝搬されるリスク	C-3-委：【データの権利等】
	データ外部提供	コンプライアンス	適切な権利処理がされないままデータが伝搬されるリスク	C-3-委：【データの権利等】
データの内容を見なければ果たせない役割（役割としてデータの内容を見ない場合は対応不要の項目）	計測	コンプライアンス	個人データ取扱いに係るコンプライアンスリスク	C-3-委：【データの権利等】
		低品質	加工済みデータの品質要求にミスマッチが生じるリスク	C-6-委：【重要インフラへのデータ提供】
		想定外の損害	加工済みデータの提供先に想定外の大きな損害を与えるリスク	
	ローカル伝送	改ざん	改ざんされたデータが伝搬されるリスク	C-2-委：【データの内容・精度】
			改ざんされた制御コマンドが伝搬するリスク	C-4-委：【制御コマンドの妥当性】
	前処理	データ形式の齟齬	形式が食い違うデータが混在して伝搬されるリスク	C-2-委：【データの内容・精度】
			単位が異なるデータが混在して伝搬されるリスク	
		低品質	精度が低いデータが混在して伝搬されるリスク	
			欠損があるデータが混在して伝搬されるリスク	
			データ品質の確認が不十分になるリスク	

			データ品質の確認について十分なスキルを持つ要員が配置されないリスク	
			データ品質確保に対する役割と責任の分担があいまいになるリスク	
			低品質の外部データが混ざって伝搬されるリスク	C-5-委：【外部データの取得】
			素性が分からないセンサー（IoT機器）からのデータを取得するリスク	
		改ざん	改ざんされたデータが伝搬されるリスク	C-2-委：【データの内容・精度】
		コンプライアンス	個人データ取扱いに係るコンプライアンスリスク	C-3-委：【データの権利等】
		低品質	加工済みデータの品質要求にミスマッチが生じるリスク	C-6-委：【重要インフラへのデータ提供】
		想定外の損害	加工済みデータの提供先に想定外の大きな損害を与えるリスク	
	インターネット接続	改ざん	改ざんされたデータが伝搬されるリスク	C-2-委：【データの内容・精度】
			改ざんされた制御コマンドが伝搬するリスク	C-4-委：【制御コマンドの妥当性】
	取得	低品質	精度が低いデータが混在して伝搬されるリスク	C-2-委：【データの内容・精度】
			欠損があるデータが混在して伝搬されるリスク	
			データ品質の確認が不十分になるリスク	
			データ品質の確認について十分なスキルを持つ要員が配置されないリスク	
			データ品質確保に対する役割と責任の分担があいまいになるリスク	
		改ざん	改ざんされたデータが伝搬されるリスク	
		低品質	低品質の外部データが混ざって伝搬されるリスク	C-5-委：【外部データの取得】
			素性が分からないセンサー（IoT機器）からのデータを取得するリスク	
	収集・保管	コンプライアンス	個人データ取扱いに係るコンプライアンスリスク	C-3-委：【データの権利等】
		低品質	低品質の外部データが混ざって伝搬されるリスク	C-5-委：【外部データの取得】
			素性が分からないセンサー（IoT機器）からのデータを取得するリスク	

	処理・分析	低品質	精度が低いデータが混在して伝搬されるリスク	C-2-委：【データの内容・精度】
			欠損があるデータが混在して伝搬されるリスク	
			データ品質の確認について十分なスキルを持つ要員が配置されないリスク	
		コンプライアンス	個人データ取扱いに係るコンプライアンスリスク	C-3-委：【データの権利等】
		低品質	品質が低い公開データが混ざるリスク	C-5-委：【外部データの取得】
			加工済みデータの品質要求にミスマッチが生じるリスク	C-6-委：【重要インフラへのデータ提供】
		想定外の損害	加工済みデータの提供先に想定外の大きな損害を与えるリスク	C-6-委：【重要インフラへのデータ提供】
				C-7-委：【提供データの品質】
	表示・データ・コマンド提供	コンプライアンス	個人データ取扱いに係るコンプライアンスリスク	C-3-委：【データの権利等】
		低品質	間違った制御コマンドが伝搬するリスク	C-4-委：【制御コマンドの妥当性】
		改ざん	改ざんされた制御コマンドが伝搬するリスク	
	データ外部提供	コンプライアンス	個人データ取扱いに係るコンプライアンスリスク	C-3-委：【データの権利等】
		低品質	加工済みデータの品質要求にミスマッチが生じるリスク	C-6-委：【重要インフラへのデータ提供】
		想定外の損害	加工済みデータの提供先に想定外の大きな損害を与えるリスク	C-6-委：【重要インフラへのデータ提供】
				C-7-委：【提供データの品質】
	駆動前処理	低品質	間違った制御コマンドが伝搬するリスク	C-4-委：【制御コマンドの妥当性】
		改ざん	改ざんされた制御コマンドが伝搬するリスク	

（注）外部データの取得に対する対応策（C-5-委）は、以下の四つの状況のどれかが当てはまる場合に実施を検討すること。（Ⅳ．２．１．１．（イ）参照）

■「前処理」において、LAN 経由で外部データ計測系と接続

■「取得」において、WAN 経由で外部データ計測系と接続

■「収集・保管」において、外部からデータを取得

■「処理・分析」において、データ解析時にオープンデータ等を取得

（注）Ⅳ．４．C ②で対応策を特定する際には、「事業連携先に委託するロール」→「対応策項番」の順に探すこと。ロールが違うと、対応策項番が同じでも、「クラウド事業者からロールの実行者に移転すべき役割」の内容が異なる場合がある。

Ⅳ. ５．リスク対応策

IoT サービス提供にあたり、クラウド事業者が実施すべきリスク対応策を以下でまとめる。ここでは多数の対応策が列挙されているが、これらが等しく重要ということではない。クラウド事業者は、自らが提供する IoT サービスの現状を踏まえ、以下の候補リストから実際に実施する対応策を取捨選択していただければ良い。

A 多様な事業者間連携

クラウド事業者が、多様な事業者間連携によって生じる、「事業者連携等の問題がサービス全体に影響を及ぼすリスク」への対応として実施すべき対応策の候補を、以下にロールごとに示す。対応策の主語は一貫して、IoT サービス利用者や連携事業者と契約を締結するクラウド事業者となっている。

【IoT セキュリティガイドラインに従って実施すべきリスク対応策】

ロール	項番	IoT セキュリティガイドラインが示すリスク対応策の要点
構成管理	**A-IoT-1**	「要点 16：認証機能を導入する」に従って、IoT 機器認証の仕組みを提供すること
	A-IoT-2	「要点 17：出荷・リリース後も安全安心な状態を維持する」に従い、自動アップデートの悪用を防止すること。また、自動アップデートができない IoT 機器の防御策を連携事業者に提供すること

【本ガイドラインで提示するリスク対応策】

ロール	項番	リスク対応策	具体的なアクション
利用者契約	**A-1**	【利用者機器の接続】 IoT サービス利用者が自分で接続する IoT 機器、組込むアプリケーションやデータについても構成管理の対象に含めるよう、IoT サービス利用者との契約にあたり折衝すること	❑IoT サービス利用者が自分で IoT 機器を接続する前に、当該機器の情報を取得し、それが IoT サービス設計時に設定した共通基準に適合しているかを確認できるよう、IoT サービス利用者との契約条件に明記している ❑上記の契約条件に基づき、IoT サービス利用者が自分の IoT 機器を実際に接続する前に、IoT 機器の情報を取得し、確認している ❑上記の確認で得られた情報を、構成管理の対象として登録・管理している ❑IoT サービス利用者が自分でクラウド上に組込むアプリケーションとデータについても、IoT サービス利用者から情報を取得できるように、IoT サービス利用者との契約条件に明記している ❑上記の契約条件に基づき、IoT サービス利用者から提供を受けた情報を、構成管理の対象として登録・管理している
	A-2	【持ち出し IoT 機器等の事故時の責任分担】 IoT サービス利用者がクラウド事業者に無断で IoT 機器を海外に持ち出した時、IoT サービス利用者がクラウド事業者の許可無く IoT 機器の使用者を変えた時に発	❑IoT 機器が海外に持ち出されることのリスクを評価している ❑IoT 機器を海外に持ち出すことで生じるコンプライアンス違反を特定している（例：暗号化機能の不正な取扱い、電波等の技術適合基準・輸出管理基準等を満たさない等）

		生した事故等の責任範囲と免責を定め、契約で明記すること	❑ 上記評価に基づき、クラウド事業者に無断で IoT 機器が海外に持ち出された場合の免責事項を、IoTサービス利用者との契約で定めている ❑ IoT サービス利用契約において、IoT 機器の使用者が許可なく変わることの禁止、または、これに対する免責事項を定めている
	A-3	【利用者が設置したエッジコンピュータ】 IoT サービス利用者が設置/増設したエッジコンピュータとクラウドを確実に接続するため、相互認証の方法と事故時の責任範囲を定め、契約で明記すること	❑ クラウドとエッジコンピュータの相互認証のため、証明書を用いたサーバ認証技術を適用している ❑ 偽のエッジコンピュータと接続させられる事故が発生した際の免責事項について、IoT サービス利用者と協議し、合意している ❑ この合意を契約書に明記している
	A-4	【利用者が調達したロール実行者】 利用者が調達したロール実行者の管理水準が不十分で IoT サービス全体のサービスレベルに影響が及んだ場合の免責を利用者との契約等で明示すること	❑ IoT サービス利用者に対し、IoT サービス全体で確保するサービスレベルを提示している ❑ 利用者が調達したロールの実行者に対し、利用者が要求すべき管理水準を推奨している ❑ 利用者が調達したロールの実行者に起因する全体のサービスレベル低下には責任を持たないことを、契約等で明記している
構成管理	**A-5**	【構成管理と使用の一時停止】 IoT 機器やその他のハードウェア/ソフトウェア/アプリケーションについて、事業連携先で協力して構成管理（ID、OS のバージョン、ぜい弱性管理とパッチ適用の状況、設置場所等）を実施すること この構成情報は認証にも活用可能 IoT サービス利用者が自分で接続した IoT 機器については、ぜい弱性が発見された際に使用者を特定し、ぜい弱性がある機器の使用を一時停止するように依頼すること	❑ 接続されている IoT 機器を全て登録し、構成管理している（IoT サービス利用者が自分で接続した IoT 機器を含む） ❑ 使用されているエッジコンピュータ/通信ゲートウェイ、LAN の通信機器、アプリケーション（表示・データ・コマンド提供、データ解析等）のハードウェア/ソフトウェアを全て登録し、構成管理している ❑ IoT サービス利用者がクラウド上に自ら乗せたアプリケーションについても、情報提供を要請している ❑ IoT 機器以外の機器・アプリケーションに対しても、導入時及び運用中にぜい弱性チェックを実施している ❑ IoT 機器に新しいぜい弱性情報が見つかった際には、登録されている情報に基づき、IoT サービス利用者が自分で接続した IoT 機器を対象として、ぜい弱性が見つかった機器とその使用者を特定している ❑ 上記で特定された使用者に対し、ぜい弱性についての情報を提供した上で、機器を停止させるかどうかの判断を依頼している
	A-6	【セキュリティパッチ】 ぜい弱性公表時に、IoT サービス提供に関わる企業等が皆で対応を協議し、定められた期間内に一斉にセキュリティパッチを適用する等の取組みを検討すること	❑ 事業連携先との間で、ぜい弱性公表時に、IoT サービス提供に関わる企業等が皆で対応を協議する体制を構築している ❑ この体制を活用し、1 日以内に一斉にセキュリティパッチを適用する等の取組を実施している
	A-7	【使用者】 IoT 機器の使用者を定期的に確認する仕組みを構築すること	❑ IoT 機器の使用者を定期的に確認している ❑ 確認作業を省力化するため、自動的に確認できる機能を構築している
	A-8	【集中的なセキュリティ監視】 IoT サービス全体で SOC を整備すること	❑ クラウド事業者が IoT サービス全体を集中監視する SOC を整備している
契約管理（委託先全体のガバナン	**A-9**	【事故対応時の行動基準】 IoT サービスに事故が発生した場合や、振る舞いのおかしい機器が発生した場合	❑ IoT サービスの設計段階で、サービス全体に影響を及ぼすインシデントに連携して対応する手順等を定めた共通基準を策定している

スに関する対応策）		は、設計時にあらかじめ定められた共通基準を適用し、事業連携先と一貫性のある対応を実施すること	❑ IoT サービスの設計段階で、振る舞いのおかしい機器を早期検知できる仕組みを設計している ❑ IoT サービスの設計段階で、振る舞いのおかしい機器を検知した場合に連携して対応する手順等を定めた共通基準を策定している ❑ この共通基準を適用し、事業連携先と一貫性のある対応を実施している
	A-10	【事故対応時の義務】 ロール実行（運用保守）の委託/受託の契約において、事故対応や振る舞いのおかしい機器等への対応について、設計時に定めた共通の行動基準を順守するように求めること	❑ IoT サービスの設計段階で、事故対応や振る舞いのおかしい機器等への対応について、連携して実施する手順を定めた共通基準を策定している ❑ 上記の共通基準をロールの実行者が順守するように、運用保守委託契約で求めている
	A-11	【セーフティリスクの責任分担】 ロールが使用するコンポーネントがサイバー攻撃の踏み台にされて、残留リスクとして開示された IoT 機器のセーフティリスクが発現した場合の、踏み台にされたコンポーネントの提供者とロールの実行者の責任範囲と免責を調整し、対応する契約等に明示すること	❑ ロールの実行者に対し、セーフティリスクが残存する IoT 機器が接続されていることを情報提供している ❑ ロールの実行者に対し、セキュリティ対策の強化を指示している ❑ 踏み台にされたコンポーネントの提供者とロールの実行者の責任範囲と免責を、クラウド事業者が主導して調整し、対応する契約等に明示している
	A-12	【外部へのデータ提供の可用性・継続性】 外部に加工済みデータを提供するにあたり、IoT サービス設計時に定めた目標に従って、可用性と継続性を維持すること	❑ IoT サービス設計時に、可用性・継続性の目標を定めている ❑ 上記の目標達成を定期的にレビューし、達成できていない場合は、事業連携先と協力して改善措置を定めている ❑ 上記で定めた改善措置を連携事業先が確実に実施するように、契約等でその責任を明示している

B ロールを実行するコンポーネントと運用・保守の多様な提供形態

クラウド事業者が、ロールを実行するコンポーネントと運用・保守の多様な提供形態によって生じる「コンポーネントリスク（運用に関するもの）」への対応として実施すべき対応策の候補を、以下に列挙して示す。対応策の主語は一貫して、機器等提供/機器等推奨を実行する、連携事業者と契約を締結する、または、コンポーネントを用いてロールを実行するクラウド事業者となっている。

① 機器等提供

【IoT セキュリティガイドラインに従って実施すべきリスク対応策】

項番	IoT セキュリティガイドラインが示すリスク対応策の要点
B-IoT-1	「要点 10：安全安心を実現する設計の整合性をとる、要点 12：安全安心を実現する設計の検証・評価を行う」に従い、サイバー攻撃に伴うセーフティリスクを低減する設計を実施した IoT 機器を責任を持って提供すること
B-IoT-2	「要点 11：不特定の相手とつなげられても安全安心を確保できる設計をする」に従い、不意にセーフティリスクを持つ IoT 機器や重要インフラと繋がってもリスクが低減される設計を実施した IoT 機器を責任を持って提供すること
B-IoT-3	「要点 14：機能及び用途に応じて適切にネットワーク接続する（IoT 機器設計、セキュリティゲートウェイの設置等）」に従う「軽量暗号技術を採用する」等により、IoT 機器からの情報漏えい・改ざんを防止する対策を検討し、必要な機器等を責任を持って提供すること
B-IoT-4	「要点 8：個々でも全体でも守れる設計にする」に従い、組込みアプリケーションのバックドア悪用を防止する対策を組み込んだ上で、当該アプリケーションを提供すること

【本ガイドラインで提示するリスク対応策】

項番	リスク対応策	具体的なアクション
B-1	【IoT 機器の選定】 IoT 機器に対し、あらかじめ定めたセキュリティバイデザインの共通基準を適用する、または、要求を満足する IoT 機器を選定すること	❑ IoT 機器に関し、セキュリティに係るセキュリティバイデザインの共通基準をあらかじめ策定している ❑ IoT 機器の設計に協力し、この共通基準に従った設計を実施している ❑ IoT 機器の設計プロセスが、セキュリティバイデザインの共通基準に適合しているかを確認の上、適合している機器を選定している ❑ セキュリティバイデザインの共通基準への適合では取り除くことができない残留リスクを把握している
B-2	【IoT 機器の品質基準】 国、業界団体等が公開した関連するガイドライン等を参考にし、IoT 機器のセキュリティ、信頼性、相互運用性等に係る品質基準を定め、この基準に合致した IoT 機器を提供すること	❑ IoT 機器のセキュリティ対策（物理的セキュリティを含む）の評価基準を定めている ❑ IoT 機器の信頼性、継続性、データ計測精度、制御性能・精度の評価基準を定めている ❑ IoT 機器の相互接続性試験の方法を定めている（SIM が動作するか等） ❑ 上記に基づいて IoT 機器を評価・試験し、合格した機器を提供している
B-3	【セーフティリスクを持つ IoT 機器の提供】 サイバー攻撃に伴う「モノ」のセーフティリスクを低減する設計を行うとともに、残存リスクを情報開示している IoT 機器を提供すること	❑ サイバー攻撃に対するセーフティリスク低減設計に自らの意見を反映している ❑ サイバー攻撃に対する残留セーフティリスクの開示を受けている ❑ セーフティリスクの残留する IoT 機器の選定基準を定めており、これに基づいて機器を選定している
B-4	【セーフティリスクへの対応】	❑ セーフティリスクが残留する IoT 機器であるかを事前に確認している

	IoT 機器にセーフティリスクが残留しているかを事前に確認すること（原則として、残留している場合は提供しないことが望ましい。） 残留リスクを承知で提供する場合は、開示された範囲内で、残留したセーフティリスクが発現しないよう、必要なセキュリティ対策を講じること	❑ 当該機器のサイバー攻撃に対する残留セーフティリスクの開示内容を確認している。非開示の場合は採用しない。 ❑ サイバー攻撃を受けて、残留リスクとして開示されたセーフティリスクが発現しないように、IoT 機器のセキュリティ対策に係る採用基準の強化、エッジコンピュータ/通信ゲートウェイを用いたセキュリティ対策の強化等の対策を実施している
B-5	【セーフティリスクに係る責任分担】 IoT 機器提供者によるサイバー攻撃に対する残留リスクの開示状況を確認した上で、開示された範囲内だけで責任を分担できるように、IoT 機器提供者にどこまで責任を移転できるかの範囲を明確に定めること	❑ サイバー攻撃を受けて、残留リスクとして開示がないセーフティリスクが発現した場合は、IoT 機器提供者の責任であり、クラウド事業者は免責であることを契約等で明記している。免責で合意できない場合は、保険によるリスク移転を検討する。 ❑ サイバー攻撃を受けて、残留リスクとして開示されたセーフティリスクが発現した場合、IoT 機器提供者にどこまで責任を移転できるかの範囲を、契約で明示している
B-6	【緊急停止】 異常な動作をしている場合、遠隔操作で緊急停止させられる IoT 機器を提供すること	❑ IoT 機器に組み込まれた「遠隔操作による緊急停止」機能の動作を試験で確認している ❑ 動作確認が取れた IoT 機器を選定し、提供している ❑ 障害を切り分け、緊急停止すべき IoT 機器を特定する手順を定め、この実現に必要な機器を関係するロールに提供している
B-7	【持ち出し検知】 クラウド事業者に無断で海外に持ち出されることを検知できる仕組みを組み込んだ IoT 機器を提供すること	❑ GPS、SIM 等により、IoT 機器の大まかな位置を把握できる ❑ この位置情報に基づき、IoT 機器が海外に持ち出されていることを検知できる ❑ IoT 機器を海外に持ち出すことで生じるコンプライアンスリスク（暗号化機能やその他の先端技術の輸出管理、電波基準/技術適合基準の違反等）を、機器提供先に警告している
B-8	【継続性】 安定した電源が得られない場合でも継続性高く使用できる IoT 機器を、必要に応じて設計・提供すること	❑ 提供する IoT 機器が省電力設計されている ❑ 提供する IoT 機器にバッテリーを内蔵している ❑ IoT 機器と UPS を組み合わせて提供している
B-9	【セーフティリスク以外の責任分担】 IoT 機器へのサイバー攻撃により、セーフティリスク以外のリスクが発現した場合、IoT 機器提供者にどこまで責任を移転できるかの範囲を明確に定めること	❑ サイバー攻撃を受けて、IoT 機器による計測データの欠損、改ざん及び IoT 機器からの情報漏えいが生じた場合の責任の範囲と、IoT 機器提供者にどこまで責任を移転できるかについて調整し、契約で明示している
B-10	【ローカル側セキュリティ強化】 IoT 機器の特性（セキュリティ対策が不十分な機器が多い）、LAN の特性（セキュリティが弱い通信方式が使われる場合がある）、ローカルコンピュータの特性（多様な OS、古い OS、常時動作必須、セキュリティパッチ NG 等）を考慮し、セキュリティ強化対策として、エッジ/通信ゲートウェイを提供すること	❑ 繋がる IoT 機器とローカルコンピュータを把握している ❑ 繋がる IoT 機器とローカルコンピュータのぜい弱性について把握している ❑ IoT 機器とローカルコンピュータのセキュリティ強化対策として、エッジ/通信ゲートウェイを提供する ❑ エッジ/通信ゲートウェイには強固なセキュリティ対策を組み込み、その先に接続される IoT 機器やローカルコンピュータを防護している
B-11	【ローカル側の責任分担】 エッジコンピュータ/通信ゲートウェイの誤動作・セキュリティ事故に対する責任の所在を明確に定めること	❑ エッジコンピュータ/通信ゲートウェイに関し、IoT サービス設計時に、信頼性・セキュリティに係る共通基準をあらかじめ策定している ❑ この共通基準に適合しているかを確認した上で機器を選定している ❑ 上記を前提として、エッジコンピュータ/通信ゲートウェイの誤動作・セキュリティ事故に対する責任を開発ベンダーに移転できる範囲を調整し、契約に明示している
B-12	【自社組込みアプリの責任分担】 IoT 機器に自ら追加した組込みアプリケーションに関わる事故について、製造物責任との関わりも含め、責任の所在を明確に定めること	❑ 自ら IoT 機器に追加して提供した組込みアプリケーションに関わる事故の責任範囲と免責事項を、提供条件として明示している ❑ この提供条件について、連携事業者の同意を得た上で、組込みアプリケーションを提供している

B-13	【アプリケーションの能力確保】 アプリケーションの能力を事前に確認・評価した上で、提供するアプリケーション（表示・データ・コマンド提供、データ解析等）を選定すること	❑アプリケーション（表示・データ・コマンド提供、データ解析等）の能力の評価基準を定めている ❑ この評価基準に基づいて比較評価した上で、アプリケーションを選定している ❑ 上記で選定したアプリケーションを提供している
B-14	【アプリケーションのセキュリティ機能】 セキュリティ機能を事前に確認・評価した上で、提供するアプリケーション（表示・データ・コマンド提供、データ解析等）を選定すること	❑ アプリケーション（表示・データ・コマンド提供、データ解析等）のセキュリティ機能の評価基準を定めている ❑この評価基準に基づいて比較評価した上で、アプリケーションを選定している ❑ 上記で選定したアプリケーションを提供している
B-15	【アプリケーションの責任分担】 アプリケーション（表示・データ・コマンド提供、データ解析等）の信頼性、ぜい弱性、能力不足等に起因する損害が生じた場合、責任を開発ベンダーにどこまで移転できるかの範囲を明確に定めること	❑ 能力やセキュリティ機能の評価基準に従ってアプリケーション（表示・データ・コマンド提供、データ解析等）を選定している ❑ 上記を前提として、質の低いデータ解析結果の提供や、解析計算の長期停止により損害が生じた場合、その責任を開発ベンダーに移転できる範囲を調整し、契約に明示している

② 機器等推奨

【IoT セキュリティガイドラインに従って実施すべきリスク対応策】

項番	IoT セキュリティガイドラインが示すリスク対応策の要点
B-IoT-5	「要点 10：安全安心を実現する設計の整合性をとる、要点 12：安全安心を実現する設計の検証・評価を行う」に従い、サイバー攻撃に伴うセーフティリスクを低減する設計を実施した IoT 機器を IoT サービス利用者等に推奨すること
B-IoT-6	「要点 11：不特定の相手とつなげられても安全安心を確保できる設計をする」に従い、不意にセーフティリスクを持つ IoT 機器や重要インフラと繋がってもリスクが低減される設計を実施した IoT 機器を IoT サービス利用者等に推奨すること
B-IoT-7	「要点 14：機能及び用途に応じて適切にネットワーク接続する（IoT 機器設計、セキュリティゲートウェイの設置等）」に従う「軽量暗号技術を採用する」等の IoT 機器からの情報漏えい・改ざんを防止する措置を IoT サービス利用者等に推奨すること

【本ガイドラインで提示するリスク対応策】

項番	リスク対応策	具体的なアクション
B-16	【IoT 機器の推奨】 あらかじめ定めたセキュリティバイデザインの共通基準に基づき、この要求を満足する IoT 機器を IoT サービス利用者等に推奨すること	❑ IoT 機器に関し、信頼性・セキュリティに係るセキュリティバイデザインの共通基準をあらかじめ策定している ❑ この共通基準に基づき、IoT 機器の設計プロセスに対する要求事項を列挙している ❑ IoT サービス利用者等に、この要求事項を満足する IoT 機器の採用を推奨している ❑ セキュリティバイデザインの共通基準への適合では取り除くことができない残留リスクを把握している
B-17	【IoT 機器の品質基準】 国、業界団体等が公開した関連するガイドライン等を参考にし、IoT 機器のセキュリティ、信頼性、相互運用性等に係る品質基準を定め、この基準に合致した IoT 機器を IoT サービス利用者等に推奨すること	❑ IoT 機器のセキュリティ対策（物理的セキュリティを含む）の評価基準を定めている ❑ IoT 機器の信頼性、継続性、データ計測精度、制御性能・精度の評価基準を定めている ❑ IoT 機器の相互接続性試験の方法を定めている（SIM が動作するか等） ❑ 上記に基づいて IoT 機器を評価・試験し、合格した機器を採用するように、IoT サービス利用者等に推奨している

B-18	【セーフティリスクを持つ IoT 機器の推奨】 サイバー攻撃に伴う「モノ」のセーフティリスクを低減する設計に取り組み、残留リスクを情報開示している IoT 機器を推奨すること	❑ サイバー攻撃によるセーフティリスクを低減する設計に取り組む IoT 機器を確認している ❑ 当該機器について、開示された残留セーフティリスクを評価し、許容範囲であると確認している ❑ その上で、IoT サービス利用者等に推奨している
B-19	【セーフティリスクへの対応】 サイバー攻撃により、残留セーフティリスクが発現しないように、必要なセキュリティ対策を取るよう推奨すること	❑ エッジコンピュータ/通信ゲートウェイを用いたセキュリティ強化を、IoT サービス利用者等に推奨している
B-20	【緊急停止】 異常な動作をしている場合、遠隔操作で緊急停止させられる IoT 機器を推奨すること	❑ 遠隔操作による緊急停止の機能が組み込まれている IoT 機器をリストアップしている ❑ 当該リストに基づき、IoT サービス利用者等に機器を推奨している
B-21	【持ち出し検知】 クラウド事業者に無断で海外に持ち出されることを検知できる仕組みを組み込んだ IoT 機器を推奨すること	❑ GPS、SIM 等により、IoT 機器の大まかな位置を把握できる ❑ この位置情報に基づき、IoT 機器が海外に持ち出されていることを検知できる ❑ 上記を望ましい要件として、IoT サービス利用者等に推奨している
B-22	【継続性】 安定した電源が得られない場合でも継続性高く使用できる IoT 機器を、必要に応じて推奨すること	❑ 省電力設計、バッテリー内臓、UPS との組合せ等を必要要件として示している ❑ 安定した電源が得られない環境で IoT 機器を使用する際に、上記の必要要件を満たす機器を採用することを、IoT サービス利用者等に推奨している
B-23	【ローカル側セキュリティ強化】 IoT 機器の特性（セキュリティ対策が不十分な機器が多い）、LAN の特性（セキュリティが弱い通信方式が使われる場合がある）、ローカルコンピュータの特性（多様な OS、古い OS、常時動作必須、セキュリティパッチ NG 等）を考慮し、セキュリティ強化対策として、エッジ/通信ゲートウェイの採用とセキュリティ強化を推奨すること	❑ 繋がる IoT 機器とローカルコンピュータを把握している ❑ 繋がる IoT 機器とローカルコンピュータのぜい弱性について把握している ❑ IoT 機器とローカルコンピュータのセキュリティ強化対策として、エッジ/通信ゲートウェイを推奨している ❑ エッジコンピュータ/通信ゲートウェイのセキュリティ強化基準を推奨している
B-24	【アプリケーションの能力確保】 アプリケーションの能力を事前に確認・評価した上で、提供するアプリケーションを選定するように推奨すること	❑ アプリケーション（表示・データ・コマンド提供、データ解析等）の能力の評価基準を定めている ❑ この評価基準に基づき、アプリケーションの能力のチェックポイントを列挙している ❑ このチェックポイントに基づいてアプリケーションを選定するように、IoT サービス利用者に推奨している
B-25	【アプリケーションのセキュリティ機能】 IoT サービス利用者等に対し、アプリケーションのセキュリティ機能を、事前に確認・評価した上で選定するように推奨すること	❑ アプリケーション（表示・データ・コマンド提供、データ解析等）のセキュリティ機能の評価基準を定めている ❑ この評価基準に基づき、アプリケーションのセキュリティ機能のチェックポイントを列挙している ❑ このチェックポイントに基づいてアプリケーションを選定するように、IoT サービス利用者等に推奨している

③ 契約管理（ロールの実行の委託に関するもの）

項番	リスク対応策	具体的なアクション
B-26	【リスク評価＆運用マニュアル】 委託契約等で、IoT 機器やローカルコンピュータの運用マニュアルとリスク評価マニュアルを策定して適用し、定期的にレビューして内容の改善を図ることを、連携事業者に求めること	❑ 連携事業者への運用・保守委託契約において、以下を要求している - IoT 機器やローカルコンピュータの運用マニュアル/リスク評価マニュアルの作成 - マニュアルの適用と PDCA による持続的改善
B-27	【残留セーフティリスクの回避】 残存するセーフティリスクを理解し、IoT 機器を安全に使用することを、連携事業者に求めること	❑ IoT 機器提供者から得た残留セーフティリスクと安全な運用・保守方法の情報を、連携事業者に提供している ❑ 連携事業者への運用・保守委託契約において、安全を保つことができる運用・保守方法を確保することを要求している
B-28	【IoT 機器の SIM 管理】 IoT 機器に差し込む組込 SIM、グローバル SIM を管理し、外国法のコンプライアンス確保（データの越境移転等）に必要な措置を講じることを連携事業者に求めること	❑ 連携事業者に、組込 SIM/グローバル SIM が組み込まれた IoT 機器が海外にあるかを確認できる手段を提供している ❑ 連携事業者への運用・保守委託契約書において、海外に持ち出された IoT 機器を検知・報告するように求めている
B-29	【ぜい弱性テストの実施】 IoT 機器の運用中に、定期的にぜい弱性テストを実施し、ぜい弱性が見つかった場合は、必要に応じてパッチを適用することを連携事業者に求めること	❑ 連携事業者への運用・保守委託契約において、以下を要求している - IoT 機器の運用中に定期的にぜい弱性テストを実施 - テスト結果をクラウド事業者に報告 - 必要なパッチを適用 - 構成管理データを用いて、IoT サービス利用者が接続した IoT 機器のうちパッチをあてる必要がある機器を特定し、クラウド事業者に報告
B-30	【必要なスキルを持つ要員の配置】 IoT 機器やその他のコンポーネントの運用に必要なスキルを有する要員を適切に配置することを連携事業者に求めること	❑ 連携事業者への運用・保守委託契約において、以下を要求している - 必要なスキルを持つ要員の適切な配置 - PDCA による継続的改善
B-31	【重要機器の接続】 重要機器が接続される場合はそのセキュリティ要求を特定するよう、連携事業者に求めること	❑ 連携事業者への運用・保守委託契約において、以下を要求している - IoT サービス利用者が接続するものも含めて、重要機器（IoT 機器）が接続されることを事前に把握し、そのリスクの大きさを評価すること - 結果をクラウド事業者に報告すること
B-32	【重要機器接続時の措置】 接続された重要機器のセキュリティ要求を満足する措置を講じるように連携事業者に求めること	❑ 連携事業者への運用・保守契約において、以下を要求している -セキュアな通信方式の適用、セキュリティが強固な通信ゲートウェイによる防御等の措置を運用すること
B-33	【セーフティリスク対策】 踏み台にされて、モノのリスクが残留する IoT 機器の攻撃に悪用されないように、残留セーフティリスクの発現を妨げるセキュリティ対策を講じることを連携事業者に求めること	❑ セーフティリスクが残留する IoT 機器の接続と、当該機器のサイバー攻撃に対する残留セーフティリスクの開示内容について、連携事業者に情報提供している ❑ 連携事業者との運用・保守契約において、以下を要求している - サイバー攻撃の踏み台とされて、残留リスクとして開示されたセーフティリスクが発現しないように、セキュリティ対策を強化すること
B-34	【エッジ上のアプリケーションの管理】 エッジコンピュータ上で稼動するサードパーティ製のアプリケーションやオープンソースを一貫したポリシーで管理するとともに、十分なスキルを持つ要員に運用保守させることを連携事業者に求めること	❑ 連携事業者との運用・保守契約において、以下を要求している - エッジコンピュータのソフトウェアを管理する一貫したポリシーを策定し、適用すること - 十分なスキルを持つ要員を運用保守に配置し、上記ポリシーの順守を確保すること

B-35	【エッジコンピュータのなりすまし】 エッジコンピュータのなりすましを防止するための措置を連携事業者に求めること	❑ 連携事業者との運用・保守契約において、クラウドがエッジコンピュータと接続する際に、電子証明書を用いた認証を行うことを求めている
B-36	【仮想化技術】 仮想化技術（SDN、NFV 等）を運用できる体制を構築するように、連携事業者に求めること	❑ 仮想化技術が適用されている場合は、どのような技術が適用されているかを連携事業者に情報提供している ❑ 連携事業者との運用・保守契約において、仮想化技術の運用スキルを持つ要員を、クラウド/ネットワークの運用保守に配置するよう求めている
B-37	【クラウド連携の際の責任分担】 IoT サービス内に存在する他クラウドの先に接続されている重要インフラや人に危害を与える IoT 機器へのサイバー攻撃の踏み台にされることに関する責任の範囲と免責を検討・適用すること	❑ 他のクラウドの先に重要インフラや人に危害を与える IoT 機器が繋がっている場合は、重要インフラ停止や人の危害への責任を回避するため、クラウドサービスの提供条件にこれへの責任の範囲と免責を明示し、適用している
B-38	【解析するデータの確認】 データ解析アプリケーションにかける前に、解析するデータの妥当性を確認するように、連携事業者に求めること	❑ 連携事業者との運用・保守契約において、以下を要求している - 解析するデータの妥当性を、解析アプリケーションにかける前に、都度確認（自動化されている場合は定期的にレビュー）する - IoT サービス利用者が自分で解析アプリケーションを使用する場合は、データの改ざん/漏えいがないことを保証する
B-39	【セキュリティ管理の実行】 アプリケーション（表示・データ・コマンド提供、データ解析等）のセキュリティ管理を行うように、連携事業者に求めること	❑ 連携事業者との運用・保守契約において、以下を要求している - ぜい弱性チェックを実施し、その結果をクラウド事業者に報告すること - アプリケーション（表示・データ・コマンド提供、データ解析等）と処理結果の改ざんを防止するセキュリティ対策を実施すること
B-40	【アプリケーション起因の損害の責任分担】 データ解析アプリケーションに起因する損害が生じた場合の連携事業者の責任範囲を調整し、契約に明示すること	❑ データ解析アプリケーションに起因する損害が生じ、損害が発生した場合の責任の範囲と免責を契約に明示している
B-41	【データ品質低下の責任分担】 データ解析の不備に起因するデータ品質低下についての連携事業者の責任範囲を契約で明示すること	❑ データ解析の不備による影響（インパクト）を、解析手法が変更されるごとに評価している ❑ 影響評価結果に基づき、データ解析の不備に起因する損害の責任範囲と免責を契約で明示している
B-42	【スキルを持つデータ解析要員】 データ解析について必要なスキルを持つ要員を配置するように、連携事業者に求めること	❑ 連携事業者との運用・保守契約において、以下を要求している - 十分なスキルを持つ人材に解析を実施させること - PDCA によりスキルの十分性を継続的に改善すること

④ IoT サービスを実際に動かすためのロール

【IoT セキュリティガイドラインに従って実施すべきリスク対応策】

分類*	項番	IoT セキュリティガイドラインが示すリスク対応策の要点
IoT 機器側	**B-IoT-8**	「要点 3 ：守るべきものを特定する」に従い、保護すべき情報・秘密を特定
	B-IoT-9	「要点 6 ：物理的なリスクを認識する」に従い、紛失・盗難・破壊への対抗策を取るとともに、無人場所での自動運転を保護
	B-IoT-10	「要点 16：認証機能を導入する」に従い、IoT 機器の機器認証と構成管理と組み合わせることで、接続されている IoT 機器の構成管理を徹底
	B-IoT-11	「要点 17：出荷・リリース後も安全安心な状態を維持する」に従い、ぜい弱性情報を収集し、パッチを適用。IoT 機器/アプリケーションの選定時及び運用中にぜい弱性チェックを実施
ローカル側	B-IoT-10	B-IoT-10 に同じ
アプリケーション（表示・データ・コマンド提供、データ解析等）	B-IoT-11	B-IoT-11 に同じ

*それぞれ、IoT 機器側＝「IoT 機器」、ローカル側＝「LAN、ローカルコンピュータ、エッジコンピュータ/通信ゲートウェイ」、ネットワーク・クラウド側＝「WAN、クラウド」、アプリケーション＝「組込みアプリケーション、アプリケーション（表示・データ・コマンド提供、データ解析等）」を示す。

【本ガイドラインで提示するリスク対応策】

分類*	項番	リスク対応策	具体的なアクション
IoT 機器側	**B-43**	【リスク評価＆運用マニュアル】 IoT 機器の運用マニュアルとリスク評価マニュアルを策定し、適用すること。また、定期的にレビューして内容の改善を図ること	❑ IoT 機器の運用マニュアルを作成している ❑ IoT 機器運用のリスク評価マニュアルを定めている ❑ リスク評価マニュアルで「リスク移転＝保険の活用」について定めている ❑ 上記マニュアルを定期的にレビューし、必要な改訂を実施している
	B-44	【残留セーフティリスクの回避】 残存するセーフティリスクを理解し、IoT 機器を安全に使用すること	❑ IoT 機器提供者から、残留セーフティリスクと安全な運用・保守方法の情報共有を受けている ❑ この情報を理解し、安全を保つことができる方法で、運用・保守を実施している
	B-45	【IoT 機器の SIM 管理】 IoT 機器に差し込む組込 SIM、グローバル SIM の国内外での管理を徹底するとともに、外国法のコンプライアンス確保（データの越境移転等）に必要な措置を講じること	❑ エッジコンピュータ又はクラウドにおいて、組込 SIM/グローバル SIM が組み込まれた IoT 機器の位置を把握している ❑ 海外にある IoT 機器については、海外法の個人情報/重要データ等の越境移転/サーバ設置場所規制等に抵触しないかを確認している ❑ 抵触する場合は、海外法が定めた措置を実施するか、あるいは IoT 機器を当該国に持ち出さないように制限している
	B-46	【ぜい弱性テストの実施】 IoT 機器の運用中に、定期的にぜい弱性テストを実施し、ぜい弱性が見つかった場合は、必要に応じてパッチを適用すること	❑ IoT 機器の運用中に定期的にぜい弱性テストを実施している ❑ 構成管理でぜい弱性テストの結果を管理している ❑ 構成管理データを用いてパッチをあてる IoT 機器を特定し、パッチを適用している ❑ IoT サービス利用者が接続した IoT 機器については、パッチをあてる必要がある機器を特定し、その機器を接続した利用者に通知して、パッチを当てるかそのまま使うかを決めてもらっている
	B-47	【必要なスキルを持つ要員の配置】	❑ 必要なスキルを有する要員を計画的に養成・採用している ❑ 定期的に研修・訓練を行い、スキルレベルを確認している

		IoT 機器の運用に必要なスキルを有する要員を適切に配置しているかを定期的にレビューすること	❑ 必要なスキルを持つことが確認された要員を、各所に必要なだけ配置していることを、定期的にレビューしている ❑ 要員不足が判明した際には、増員や配置変更による改善措置を実施している
ローカル側	**B-48**	【重要機器の接続】 重要機器が接続されるかを把握し、接続される場合はそのセキュリティ要求を特定すること	❑ IoT サービス利用者が接続するものも含めて、重要機器（IoT 機器）が接続されることを、事前に把握している ❑ 接続される重要機器が求めるセキュリティ要求を特定している ❑ 重要機器が接続されることで生じるリスクの大きさを評価している
	B-49	【重要機器接続時の措置】 接続された重要機器のセキュリティ要求を満足する措置を講じること	❑ リスク評価結果に基づき、セキュアな通信方式の適用、セキュリティが強固な通信ゲートウェイによる防御等の措置を実施し、重要機器のセキュリティを強化している
	B-50	【セーフティリスク対策】 モノのリスクが残留する IoT 機器と繋がるのかを事前に確認し、繋がる場合は当該 IoT 機器のサイバー攻撃に対する残留セーフティリスクの開示を確認すること 踏み台にされて、モノのリスクが残留する IoT 機器の攻撃に悪用されないように、残留セーフティリスクの発現を妨げるセキュリティ対策を講じること	❑ セーフティリスクが残留する IoT 機器の接続を事前に確認している ❑ 接続する場合は、当該機器のサイバー攻撃に対する残留セーフティリスクの開示内容を確認している。非開示の場合は接続させない。 ❑ サイバー攻撃の踏み台とされて、残留リスクとして開示されたセーフティリスクが発現しないように、ICT 機器（ハードウェア/ソフトウェア）のセキュリティ対策に係る採用基準の強化、エッジコンピュータ/セキュリティが強固な通信ゲートウェイを防御壁としたセキュリティ対策の強化等の対応策を実施している
	B-51	【エッジ上のアプリケーションの管理】 エッジコンピュータ上で稼動するサードパーティ製のアプリケーションやオープンソースを一貫したポリシーで管理するとともに、十分なスキルを持つ要員に運用保守させること	❑ IoT サービスの提供にあたりエッジコンピュータが持つリスクを評価している ❑ マルチベンダーで構成されるエッジコンピュータのソフトウェアを管理する一貫したポリシーを策定し、適用している ❑ 十分なスキルを持つ要員を運用保守に配置し、上記ポリシーの順守を確保している ❑ 要員のスキルと人数を定期的にレビューし、必要に応じて改善を実施している
	B-52	【エッジコンピュータのなりすまし】 エッジコンピュータのなりすましを防止するための措置を実施すること	❑ クラウドがエッジコンピュータと接続する際に、電子証明書を用いた認証を行っている
	B-53	【クラウド側要求事項の合意】 エッジサービスが SLA を提供できない場合は、クラウドとの間でお互いに要求事項を提示し合い、合意事項として定め、定期的に見直しを行うこと	❑ 接続されるクラウドに対する要求事項を特定している ❑ クラウドとの間でお互いに要求事項を提示し合い、合意形成を行っている ❑ 合意内容は定期的に見直している
ネットワーク･クラウド側	B-45	B-45 に同じ	
	B-50	B-50 に同じ	
	B-53	B-53 に同じ	
	B-54	【高リスクの IoT 機器接続対策】 重要インフラや人に危害を与える IoT 機器が接続されるかを事前に確認し、接続される場合はセキュリティ要件が厳しい用途向けのクラウドサービスを適用すること	❑ 重要インフラや人に危害を与える IoT 機器が接続されるかを事前に確認している ❑ 重要インフラや人に危害を与える IoT 機器が繋がっている場合は、重要インフラ停止や人の危害への責任を回避するため、より厳しいセキュリティ要件に適合するクラウドサービスを採用している
	B-55	【クラウド間の接続】 IoT サービス内に存在する他のクラウドの接続先に、重要インフラや人に危害を与える IoT 機器がないかを確認し、存在す	❑ IoT サービスがマルチクラウド構成であることを把握し、他のクラウドの接続先を確認している ❑ 他のクラウドの接続先に、重要インフラや人に危害を与える IoT 機器がないかを確認している

		る場合は、セキュリティ要件が厳しい用途向けのクラウドサービスを適用すること	❑ 重要インフラや人に危害を与える IoT 機器が繋がっている場合は、重要インフラ停止や人の危害への責任を回避するため、より厳しいセキュリティ要件に適合するクラウドサービスを採用している
	B-56	【仮想化技術】 仮想化技術（SDN、NFV 等）を運用できる体制を構築すること	❑ 仮想化技術が適用されていることを把握している ❑ どのような技術が適用されているかを理解している ❑ 仮想化技術の運用スキルを持つ要員を育成している ❑ この要員をクラウド/ネットワークの運用保守に配置している
	B-57	【ピーク時運用】 バースト的な制御不能挙動に対抗する技術的措置を講じること	❑ IoT 機器の接続数と扱うデータに基づき、ピーク時の通信量を予測している ❑ ピーク時の通信量予測に基づき、クラウドサービスの処理容量に必要なスケーラビリティを持たせている ❑ ピーク時の通信量予測に基づき、適切な容量を持つ WAN を選択している
アプリケーション（表示・データ・コマンド提供、データ解析等）	**B-58**	【解析するデータの確認】 データ解析アプリケーションにかける前に、解析するデータの妥当性を確認すること	❑ 解析するデータの妥当性を、解析アプリケーションにかける前に、都度確認（自動化されている場合は定期的にレビュー）している ❑ IoT サービス利用者が自分で解析アプリケーションを使用する場合は、解析するデータの内容を見ることができない場合が多いため、データの改ざん/漏えいがないことだけを保証している
	B-59	【セキュリティ管理の実行】 アプリケーション（表示・データ・コマンド提供、データ解析等）のセキュリティ管理を行うこと	❑ 導入時及び運用中にぜい弱性チェックを実施すること ❑ データ解析アプリケーションと解析結果の改ざんを防止するセキュリティ対策を実施すること
	B-60	【ぜい弱性テストの実施】 アプリケーション（表示・データ・コマンド提供、データ解析等）の運用中に、定期的にぜい弱性テストを実施し、ぜい弱性が見つかった場合は、必要に応じてパッチを適用すること	❑ アプリケーション（表示・データ・コマンド提供、データ解析等）の運用中に定期的にぜい弱性テストを実施し、必要に応じてパッチを適用している ❑ 構成管理でぜい弱性テストの結果を管理している ❑ IoT サービス利用者が導入したアプリケーションについては、パッチをあてる必要がある旨を利用者に通知して、パッチを当てるかそのまま使うかを決めてもらっている
	B-61	【スキルを持つデータ解析要員】 データ解析について必要なスキルを持つ要員を配置すること	❑ 必要な解析スキルを持つ人材を育成・採用している ❑ データ解析の不備を防止し、付加価値を高めるため、十分なスキルを持つ人材に解析を実施させている ❑ スキルの十分性を定期的にレビューし、必要な改善を実施している

*それぞれ、以下を示す。

・IoT 機器側＝「IoT 機器」

・ローカル側＝「LAN、ローカルコンピュータ、エッジコンピュータ/通信ゲートウェイ」

・ネットワーク・クラウド側＝「WAN、クラウド」

・アプリケーション＝「組込みアプリケーション、アプリケーション（表示・データ・コマンド提供、データ解析等）」

C 多様なデータ取扱形態

クラウド事業者が、多様なデータ取扱形態によって生じる「データ価値やデータに係る法令順守を毀損するリスク」への対応として実施すべき対応策の候補を、以下に列挙して示す。ここで示す対応策は、クラウド事業者がリーダーシップを執り、必要に応じて連携事業者に役割を移転して実施することになる。このため、クラウド事業者の視点からは、「ロール実行」の一環として自ら行うべきこと（データ監視・保全）と、「ロール実行」の委託契約に書き込んで連携事業者に求めるべきこと（契約管理）から構成されている。

① データ監視・保全

項番	リスク対応策	具体的なアクション	クラウド事業者が主導すべき役割
C-1-ク	【データ量の監視】 データ量を監視し、適正な範囲に保つこと	❑ 前処理で監視し、クラウドに送付するデータ量を制限している ❑ クラウドで収集・保管する際にデータ量をレビューし、必要に応じてエッジコンピュータの処理を調整している ❑ 処理・分析後の加工済みデータ量を確認し、必要に応じてデータ量を削減する対策を講じている	❑ 適正なデータ量についての基準を定める（取得するデータ、加工済みデータ） ❑ データ量の監視・レビューを統括する
C-2-ク	【データの内容・精度】 データ内容/欠損を確認し、正確に保つこと。データ精度を評価する統計手法等を適用すること	❑ 前処理でデータ欠損、計測精度、データ形式、単位を確認し、必要に応じてデータ補正・補完を行っている ❑ 計測精度の確認には統計的手法等を適用し、その信頼性を確保している ❑ 欠損・誤計測が見られる IoT 機器の振る舞いを確認し、必要に応じて遠隔からリセットしている ❑ データ伝送中に不達や改ざんが生じていないかを確認している	❑ データの正確さを評価する基準を定める ❑ データの標準的な形式と単位を定めることを主導する ❑ 適用する統計的手法の調整を主導する ❑ データ伝送中に不達や改ざんが発生した場合の原因調査と対応策実施を主導する ❑ 対応策の有効性を定期的にレビューし、必要に応じて改善策を講じる ❑ 必要なスキルを有する専門要員を配置する
C-3-ク	【データの権利等】 データに係るコンプライアンス（権利処理、個人情報保護等）の順守を定期的にレビューし、必要に応じて是正措置を取ること	❑ IoT サービス利用者、クラウド事業者、計測・前処理の実行者等の間で、データ利用権を調整し、定めている ❑ 個人情報保護法の違反、外国の個人情報保護法の違反（越境移転、サーバ設置場所等）等が発生していないかをレビューし、違反を是正している ❑ 営業秘密侵害がないかをレビューし、侵害を是正している	❑ データ利用権の調整を主導する（加工済みデータを含む） ❑ コンプライアンス違反のレビューを主導する ❑ コンプライアンス違反の是正を主導する
C-4-ク	【制御コマンドの妥当性】 制御コマンドの妥当性を監視・確認する仕組みを組込むこと。これを実施	❑ コマンド提供機能が発出する制御コマンドの妥当性を常時検証している ❑ 上記による発見された問題点を是正している	❑ 制御コマンド提供の問題点の是正を主導する

	するための、事業連携先との協力体制を構築すること	❑ 駆動前処理でも異常な制御コマンドを検知・棄却している ❑ 制御コマンド伝送中に不達や改ざんが生じていないかを確認している	❑ 制御コマンド伝送中に不達や改ざんが発生した場合の原因調査と対策実施を主導する ❑ 対応策の有効性を定期的にレビューし、必要に応じて改善策を講じる
C-5-ク	【外部データの取得】 外部からのデータ取得にあたり、設計時等に定めた IoT サービス共通の基準に従って、データ取得先の管理状況を確認すること	❑ IoT サービスの設計時に、外部データ取得先の管理状況を確認するための共通基準を策定している ❑ IoT サービスの設計時に、外部データを取得するための、データ品質評価に係る共通基準を策定している ❑ 上記基準に基づき、外部データ取得先を事前に評価した上で、データを取得している ❑ 上記基準に基づき、外部データ取得先の管理状況を定期的にレビューし、必要に応じて改善策を講じている	❑ 外部データ取得先の管理状況を確認するための共通基準の策定と持続的改善を主導する ❑ 外部データ取得先の管理状況の定期的レビューと問題点の改善を主導する
C-6-ク	【重要インフラへのデータ提供】 外部に加工済みデータを提供するにあたり、設計時等に定めた IoT サービス共通の基準に従って、提供先が特別なリスクを有していないかを確認すること（重要インフラ等）	❑ IoT サービスの設計時に加工済みデータ提供先が特別なリスクを有するかを確認する共通基準を策定している ❑ 上記基準に基づき、事前に加工済みデータ提供先を評価の上、提供している	IoT サービスの設計時に、加工済みデータ提供先が特別なリスクを有しているかを確認する共通基準の策定を主導する
C-7-ク	【提供データの品質】 外部に提供する加工済みデータの品質をレビュー・確認し、一定水準以上を保つこと	❑ 外部に提供する加工済みデータの品質基準を定めている ❑ 上記品質基準に準拠した加工済みデータのみを外部に提供している ❑ データ解析結果の妥当性を定期的にレビューし、改善措置を講じている	外部に提供する加工済みデータの品質基準の策定を主導する

② 契約管理（データ監視・保全への協力を委託するもの）

【対応策を、委託先となるロール順に示した表】

ロール	項番	リスク対応策	クラウド事業者からロールの実行者に移転すべき役割
計測	C-3-委	【データの権利等】 データに係るコンプライアンス（権利処理、個人情報保護等）の順守を定期的にレビューし、必要に応じて是正措置を取ること	❑ データ利用権調整に加わる ❑ コンプライアンス違反のレビューに必要なログ等の提供 ❑ コンプライアンス違反の是正への協力
	C-6-委	【重要インフラへのデータ提供】 外部に加工済みデータを提供するにあたり、設計時等に定めた IoT サービス共通の基準に従って、提供先が特別なリスクを有していないかを確認すること（重要インフラ等）	加工済みデータ提供先について情報共有
ローカル伝送	C-2-委	【データの内容・精度】 データ内容/欠損を確認し、正確に保つこと。データ精度を評価する統計手法等を適用すること	データ伝送中の不達や改ざんの原因調査と対策実施に協力

	C-4-委	【制御コマンドの妥当性】 制御コマンドの妥当性を監視・確認する仕組みを組込むこと。これを実施するための、事業連携先との協力体制を構築すること	制御コマンド伝送中に不達や改ざんが発生した場合の原因調査に協力
前処理	C-1-委	【データ量の監視】 データ量を監視し、適正な範囲に保つこと	❑ クラウドに送るデータ量の監視・制御（送付間隔、フィルタリングの範囲等） ❑ エッジコンピュータが複数ある場合は、全体のデータ量を監視できる仕組みを構築
	C-2-委	【データの内容・精度】 データ内容/欠損を確認し、正確に保つこと。データ精度を評価する統計手法等を適用すること	❑ データ欠損と計測精度を確認し、必要に応じてデータを補正・補完（推論、予測） ❑ データ形式と単位を合わせる ❑ 上記を済ませた上で、前処理のためのデータを受け入れ（受信したデータを全て受け入れない） ❑ データ品質の確認に必要なスキルを持つ要員の配置 ❑ 欠損・誤計測が見られる IoT 機器の振る舞いを確認し、必要に応じて遠隔からリセット ❑ データ伝送中の不達や改ざんがないかを確認 ❑ データ伝送中の不達や改ざんの原因調査と対策実施に協力 ❑ データ解析で必要な場合は、解析者の精度要求に則したタイムスタンプ（1/10 秒レベル、ミリ秒レベル、マイクロ秒レベル等）を付与
	C-3-委	【データの権利等】 データに係るコンプライアンス（権利処理、個人情報保護等）の順守を定期的にレビューし、必要に応じて是正措置を取ること	❑ データ利用権調整に加わる ❑ コンプライアンス違反のレビューに必要なログ等の提供 ❑ コンプライアンス違反の是正への協力
	C-5-委	【外部データの取得】 外部からのデータ取得にあたり、設計時等に定めた IoT サービス共通の基準に従って、データ取得先の管理状況を確認すること	❑ 外部のデータ計測系との接続にあたり、IoT サービスの設計時に定めた共通基準に従って事前評価を実施 ❑ 外部のデータ計測系の管理状況を定期的にレビューし、問題点の改善を依頼
	C-6-委	【重要インフラへのデータ提供】 外部に加工済みデータを提供するにあたり、設計時等に定めた IoT サービス共通の基準に従って、提供先が特別なリスクを有していないかを確認すること（重要インフラ等）	加工済みデータ提供先について情報共有
インターネット接続	C-2-委	【データの内容・精度】 データ内容/欠損を確認し、正確に保つこと。データ精度を評価する統計手法等を適用すること	データ伝送中の不達や改ざんの原因調査と対策実施に協力
	C-4-委	【制御コマンドの妥当性】 制御コマンドの妥当性を監視・確認する仕組みを組込むこと。これを実施するための、事業連携先との協力体制を構築すること	制御コマンド伝送中に不達や改ざんが発生した場合の原因調査に協力
取得	C-1-委	【データ量の監視】 データ量を監視し、適正な範囲に保つこと	前処理でデータ量を適正に制御しているかを確認
	C-2-委	【データの内容・精度】 データ内容/欠損を確認し、正確に保つこと。データ精度を評価する統計手法等を適用すること	❑ 前処理でデータを正確に保つことができているかを確認 ❑ データ品質の確認に必要なスキルを持つ要員の配置 ❑ データ伝送中の不達や改ざんがないかを確認

			❑ データ伝送中の不達や改ざんの原因調査と対策実施に協力
	C-5-委	【外部データの取得】 外部からのデータ取得にあたり、設計時等に定めた IoT サービス共通の基準に従って、データ取得先の管理状況を確認すること	❑ 外部のデータ計測系との接続にあたり、IoT サービスの設計時に定めた共通基準に従って事前評価を実施 ❑ 外部のデータ計測系の管理状況を定期的にレビューし、問題点の改善を依頼
収集・保管	C-1-委	【データ量の監視】 データ量を監視し、適正な範囲に保つこと	クラウドに保管されたデータ量をレビュー、前処理のデータ量制御ポリシーを調整
	C-3-委	【データの権利等】 データに係るコンプライアンス（権利処理、個人情報保護等）の順守を定期的にレビューし、必要に応じて是正措置を取ること	外部から取得したデータについての確認を実施
	C-5-委	【外部データの取得】 外部からのデータ取得にあたり、設計時等に定めた IoT サービス共通の基準に従って、データ取得先の管理状況を確認すること	❑ 外部データ取得にあたり、IoT サービスの設計時に定めたデータ品質評価に係る共通基準に従って事前評価を実施 ❑ 外部データの品質を定期的にレビューし、問題点の改善を依頼
処理・分析	C-2-委	【データの内容・精度】 データ内容/欠損を確認し、正確に保つこと。データ精度を評価する統計手法等を適用すること	❑ 過去に取得したデータ、外部から取得したデータとの間で、データの正確性の度合いを比較評価し、必要に応じて「データの正確さを評価する基準」の修正を提案 ❑ データ品質の確認に必要なスキルを持つ要員の配置
	C-3-委	【データの権利等】 データに係るコンプライアンス（権利処理、個人情報保護等）の順守を定期的にレビューし、必要に応じて是正措置を取ること	❑ 外部から取得したデータについての確認を実施 ❑ 加工済みデータの利用権調整に加わる
	C-5-委	【外部データの取得】 外部からのデータ取得にあたり、設計時等に定めた IoT サービス共通の基準に従って、データ取得先の管理状況を確認すること	❑ 外部データ取得（オープンデータを含む）にあたり、IoT サービスの設計時に定めたデータ品質評価に係る共通基準に従って事前評価を実施 ❑ 外部データの品質を定期的にレビューし、問題点の改善を依頼
	C-6-委	【重要インフラへのデータ提供】 外部に加工済みデータを提供するにあたり、設計時等に定めた IoT サービス共通の基準に従って、提供先が特別なリスクを有していないかを確認すること（重要インフラ等）	加工済みデータ提供先について情報共有
	C-7-委	【提供データの品質】 外部に提供する加工済みデータの品質をレビュー・確認し、一定水準以上を保つこと	❑ 加工済みデータの品質基準に従ってデータを加工 ❑ データ解析結果の妥当性を定期的にレビューし、必要な改善を実施
表示・データ・コマンド提供	C-3-委	【データの権利等】 データに係るコンプライアンス（権利処理、個人情報保護等）の順守を定期的にレビューし、必要に応じて是正措置を取ること	❑ 加工済みデータのコンプライアンス違反をレビュー ❑ 加工済みデータのコンプライアンス違反を是正
	C-4-委	【制御コマンドの妥当性】 制御コマンドの妥当性を監視・確認する仕組みを組込むこと。これを実施するための、事業連携先との協力体制を構築すること	❑ コマンド提供機能が発出する制御コマンドの妥当性を常時検証 ❑ 発生した問題点の是正
データ外部提供	C-3-委	【データの権利等】	加工済みデータの提供にあたり、コンプライアンスの順守について契約等で明示し、合意する

		データに係るコンプライアンス（権利処理、個人情報保護等）の順守を定期的にレビューし、必要に応じて是正措置を取ること	
	C-6-委	【重要インフラへのデータ提供】 外部に加工済みデータを提供するにあたり、設計時等に定めた IoT サービス共通の基準に従って、提供先が特別なリスクを有していないかを確認すること（重要インフラ等）	IoT サービス設計時に定めた、加工済みデータ提供先が特別なリスクを有するかを確認する共通基準に基づき、提供先を評価の上、提供
	C-7-委	【提供データの品質】 外部に提供する加工済みデータの品質をレビュー・確認し、一定水準以上を保つこと	加工済みデータが品質基準に合致することを確認の上、外部に提供
駆動前処理	C-4-委	【制御コマンドの妥当性】 制御コマンドの妥当性を監視・確認する仕組みを組み込むこと。これを実施するための、事業連携先との協力体制を構築すること	❑ 伝送中の不達や改ざんがないかを確認 ❑ 制御コマンド伝送中に不達や改ざんが発生した場合の原因調査に協力

【参考：対応策を項番順に示した表】

項番	リスク対応策	具体的なアクション	クラウド事業者からロールの実行者に移転すべき役割	
			ロール	役割
C-1-委	【データ量の監視】 データ量を監視し、適正な範囲に保つこと	❑ 前処理で監視し、クラウドに送付するデータ量を制限している ❑ クラウドで収集・保管する際にデータ量をレビューし、必要に応じてエッジコンピュータの処理を調整している ❑ 処理・分析後の加工済みデータ量を確認し、必要に応じてデータ量を削減する対策を講じている	前処理	❑ クラウドに送るデータ量の監視・制御（送付間隔、フィルタリングの範囲等） ❑ エッジコンピュータが複数ある場合は、全体のデータ量を監視できる仕組みを構築
			取得	前処理でデータ量を適正に制御しているかを確認
			収集・保管	クラウドに保管されたデータ量をレビュー、前処理のデータ量制御ポリシーを調整
C-2-委	【データの内容・精度】 データ内容/欠損を確認し、正確に保つこと。データ精度を評価する統計手法等を適用すること	❑ 前処理でデータ欠損、計測精度、データ形式、単位を確認し、必要に応じてデータ補正・補完を行っている ❑ 計測精度の確認には統計的手法等を適用し、その信頼性を確保している ❑ 欠損・誤計測が見られるIoT 機器の振る舞いを確認し、必要に応じて遠隔からリセットしている ❑ データ伝送中に不達や改ざんが生じていないかを確認している	ローカル伝送	データ伝送中の不達や改ざんの原因調査と対策実施に協力
			前処理	❑ データ欠損と計測精度を確認し、必要に応じてデータを補正・補完（推論、予測） ❑ データ形式と単位を合わせる ❑ 上記を済ませた上で、前処理のためのデータを受け入れ（受信したデータを全て受け入れない） ❑ データ品質の確認に必要なスキルを持つ要員の配置 ❑ 欠損・誤計測が見られる IoT 機器の振る舞いを確認し、必要に応じて遠隔からリセット ❑ データ伝送中の不達や改ざんがないかを確認 ❑ データ伝送中の不達や改ざんの原因調査と対策実施に協力 ❑ データ解析で必要な場合は、解析者の精度要求に則したタイムスタンプ（1/10 秒レベル、ミリ秒レベル、マイクロ秒レベル等）を付与
			インターネット接続	データ伝送中の不達や改ざんの原因調査と対策実施に協力
			取得	❑ 前処理でデータを正確に保つことができているかを確認 ❑ データ品質の確認に必要なスキルを持つ要員の配置 ❑ データ伝送中の不達や改ざんがないかを確認 ❑ データ伝送中の不達や改ざんの原因調査と対策実施に協力
			処理・分析	❑ 過去に取得したデータ、外部から取得したデータとの間で、データの正確性の度合いを比較評価し、必要に応じて「データの正確さを評価する基準」の修正を提案 ❑ データ品質の確認に必要なスキルを持つ要員の配置
C-3-委	【データの権利等】 データに係るコンプライアンス（権利処理、個人情報保護等）の順守を定期的にレビューし、必要に	❑ IoT サービス利用者、クラウド事業者、計測・前処理の実行者等の間で、データ利用権を調整し、定めている ❑ 個人情報保護法の違反、外国の個人情報保護法の	計測	❑ データ利用権調整に加わる ❑ コンプライアンス違反のレビューに必要なログ等の提供 ❑ コンプライアンス違反の是正への協力
			前処理	❑ データ利用権調整に加わる ❑ コンプライアンス違反のレビューに必要なログ等の提供 ❑ コンプライアンス違反の是正への協力

	応じて是正措置を取ること	違反（越境移転、サーバ設置場所等）等が発生していないかをレビューし、違反を是正している ❑ 営業秘密侵害がないかをレビューし、侵害を是正している	収集・保管	外部から取得したデータについての確認を実施
			処理・分析	❑ 外部から取得したデータについての確認を実施 ❑ 加工済みデータの利用権調整に加わる
			表示・データ・コマンド提供	❑ 加工済みデータのコンプライアンス違反をレビュー ❑ 加工済みデータのコンプライアンス違反を是正
			データ外部提供	加工済みデータの提供にあたり、コンプライアンスの順守について契約等で明示し、合意する
C-4-委	【制御コマンドの妥当性】 制御コマンドの妥当性を監視・確認する仕組みを組込むこと。これを実施するための、事業連携先との協力体制を構築すること	❑ コマンド提供機能が発出する制御コマンドの妥当性を常時検証している ❑ 上記による発見された問題点を是正している ❑ 駆動前処理でも異常な制御コマンドを検知・棄却している ❑ 制御コマンド伝送中に不達や改ざんが生じていないかを確認している	ローカル伝送	制御コマンド伝送中に不達や改ざんが発生した場合の原因調査に協力
			インターネット接続	制御コマンド伝送中に不達や改ざんが発生した場合の原因調査に協力
			表示・データ・コマンド提供	❑ コマンド提供機能が発出する制御コマンドの妥当性を常時検証 ❑ 発生した問題点の是正
			駆動前処理	❑ 伝送中の不達や改ざんがないかを確認 ❑ 制御コマンド伝送中に不達や改ざんが発生した場合の原因調査に協力
C-5-委	【外部データの取得】 外部からのデータ取得にあたり、設計時等に定めたIoT サービス共通の基準に従って、データ取得先の管理状況を確認すること	❑ IoT サービスの設計時に、外部データ取得先の管理状況を確認するための共通基準を策定している ❑ IoT サービスの設計時に、外部データを取得するための、データ品質評価に係る共通基準を策定している ❑ 上記基準に基づき、外部データ取得先を事前に評価した上で、データを取得している ❑ 上記基準に基づき、外部データ取得先の管理状況を定期的にレビューし、必要に応じて改善策を講じている	前処理	❑ 外部のデータ計測系との接続にあたり、IoT サービスの設計時に定めた共通基準に従って事前評価を実施 ❑ 外部のデータ計測系の管理状況を定期的にレビューし、問題点の改善を依頼
			取得	❑ 外部のデータ計測系との接続にあたり、IoT サービスの設計時に定めた共通基準に従って事前評価を実施 ❑ 外部のデータ計測系の管理状況を定期的にレビューし、問題点の改善を依頼
			収集・保管	❑ 外部データ取得にあたり、IoT サービスの設計時に定めたデータ品質評価に係る共通基準に従って事前評価を実施 ❑ 外部データの品質を定期的にレビューし、問題点の改善を依頼
			処理・分析	❑ 外部データ取得（オープンデータを含む）にあたり、IoT サービスの設計時に定めたデータ品質評価に係る共通基準に従って事前評価を実施 ❑ 外部データの品質を定期的にレビューし、問題点の改善を依頼
C-6-委	【重要インフラへのデータ提供】 外部に加工済みデータを提供するにあたり、設計時等に定めた IoT サービス共通の基準に従って、提供先が特別なリスクを有していないかを確認すること（重要インフラ等）	❑ IoT サービスの設計時に加工済みデータ提供先が特別なリスクを有するかを確認する共通基準を策定している ❑ 上記基準に基づき、事前に加工済みデータ提供先を評価の上、提供している	計測	加工済みデータ提供先について情報共有
			前処理	加工済みデータ提供先について情報共有
			処理・分析	加工済みデータ提供先について情報共有
			データ外部提供	IoT サービス設計時に定めた、加工済みデータ提供先が特別なリスクを有するかを確認する共通基準に基づき、提供先を評価の上、提供

C-7-委	【提供データの品質】 外部に提供する加工済みデータの品質をレビュー・確認し、一定水準以上を保つこと	❑ 外部に提供する加工済みデータの品質基準を定めている ❑ 上記品質基準に準拠した加工済みデータのみを外部に提供している ❑ データ解析結果の妥当性を定期的にレビューし、改善措置を講じている	処 理・分析	❑ 加工済みデータの品質基準に従ってデータを加工 ❑ データ解析結果の妥当性を定期的にレビューし、必要な改善を実施
			デ ー タ外部提供	加工済みデータが品質基準に合致することを確認の上、外部に提供

Ⅴ．参考資料

Annex 1 組織･運用編　対策項目一覧表

項番	対策項目	区分	実施チェック
Ⅱ．１．　情報セキュリティへの組織的取組の基本方針			
Ⅱ．１．１．組織の基本的な方針を定めた文書			
Ⅱ．１．１．１．	経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。	基本	
Ⅱ．１．１．２．	情報セキュリティに関する基本的な方針を定めた文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。この見直しの結果、変更の必要性が生じた場合には、経営陣の承認の下で改定等を実施すること。	基本	
Ⅱ．２．　情報セキュリティのための組織			
Ⅱ．２．１．　内部組織			
Ⅱ．２．１．１．	経営陣は、情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行うこと。	基本	
Ⅱ．２．１．２．	従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。	基本	
Ⅱ．２．１．３．	情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。	基本	
Ⅱ．２．２．　外部組織（データセンタを含む）			
Ⅱ．２．２．１．	外部組織が関わる業務プロセスにおける情報資産に対するリスクを識別し、適切な対策を実施すること。	基本	
Ⅱ．２．２．２．	情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。	基本	
Ⅱ．３．　連携クラウド事業者に関する管理			
Ⅱ．３．１．　連携クラウド事業者から組み込むクラウドサービスの管理			
Ⅱ．３．１．１．	連携クラウド事業者が提供するクラウドサービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携クラウド事業者によって確実に実施されることを担保すること。	基本	
Ⅱ．３．１．２．	連携クラウド事業者が提供するクラウドサービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。	基本	
Ⅱ．４．　情報資産の管理			
Ⅱ．４．１．　情報資産に対する責任			
Ⅱ．４．１．１．	取り扱う各情報資産について、管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。	基本	
Ⅱ．４．２．　情報の分類			
Ⅱ．４．２．１．	組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。	基本	
Ⅱ．４．３．　情報セキュリティポリシーの遵守、点検及び監査			
Ⅱ．４．３．１．	各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。	基本	

Ⅱ．４．３．２．	クラウドサービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること。	基本	
Ⅱ．５．　従業員に係る情報セキュリティ			
Ⅱ．５．１．　雇用前			
Ⅱ．５．１．１．	雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。	基本	
Ⅱ．５．２．　雇用期間中			
Ⅱ．５．２．１．	全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。	基本	
Ⅱ．５．２．２．	従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えること。	基本	
Ⅱ．５．３．　雇用の終了又は変更			
Ⅱ．５．３．１．	従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にすること。	基本	
Ⅱ．６．　情報セキュリティインシデントの管理			
Ⅱ．６．１．　情報セキュリティインシデント及びぜい弱性の報告			
Ⅱ．６．１．１．	全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施を要求すること。 報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。	基本	
Ⅱ．７．　コンプライアンス			
Ⅱ．７．１．　法令と規則の遵守			
Ⅱ．７．１．１．	個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。	基本	
Ⅱ．７．１．２．	クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。	基本	
Ⅱ．７．１．３．	利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。	基本	
Ⅱ．８．　ユーザサポートの責任			
Ⅱ．８．１．　利用者への責任			
Ⅱ．８．１．１．	クラウドサービスの提供に支障が生じた場合には、その原因が連携クラウド事業者に起因するものであったとしても、利用者と直接契約を結ぶクラウド事業者が、その責任において一元的にユーザサポートを実施すること。	基本	

Annex 2 物理的･技術的対策編　対策項目一覧表

				機密性	高			低			
				可用性	高	中	低	高	中	低	
					パターン１	パターン２	パターン３	パターン４	パターン５	パターン６	
対策項目番号	評価項目番号	対策項目	区分	評価項目※	対策参照値※※						実施チェック
				※対策項目を実施する際に、その実施レベルを定量的あるいは具体的に評価するための指標。SLA の合意事項として活用されることも想定される。	※※対策項目の実施レベルの目安となる評価項目の値で、パターンごとに設定されている。特に達成することが必要であると考えられる値については、「*」を付している。また、評価項目によっては、対策参照値が「-」となっているパターンが存在するが、これについては、クラウド事業者が任意に対策参照値を設定することで、対策項目の実施レベルを評価されたい。						
Ⅲ．１．アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策											
Ⅲ．１．１．運用・管理に関する共通対策											
Ⅲ．１．１．１．	a	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。 稼働停止を検知した場合は、利用者に速報を通知すること。	●	死活監視インターバル（応答確認）	1 回以上／5 分*	1 回以上／10 分*	1 回以上／20 分*	1 回以上／5 分*	1 回以上／10 分*	1 回以上／20 分*	
	b			通知時間（稼動停止検知後、利用者に通知するまでの時間）	20 分以内*	60 分以内*	5 時間以内*	20 分以内*	60 分以内*	5 時間以内*	
Ⅲ．１．１．２．	a	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。 障害を検知した場合は、利用者に速報を通知すること。	●	障害監視インターバル	1 回/10 分	1 回/30 分	1 回/60 分	1 回/10 分	1 回/30 分	1 回/60 分	
	b			通知時間（障害検知後、利用者に通知するまでの時間）	20 分	60 分	5 時間	20 分	60 分	5 時間	
Ⅲ．１．１．３．	a	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。 また、利用者との取決めに基づいて、監視結果を利用者に通知すること。	★	パフォーマンス監視インターバル	1 回/10 分	1 回/30 分	1 回/60 分	1 回/10 分	1 回/30 分	1 回/60 分	
	b			通知時間（異常検知後、利用者に通知するまでの時間）	20 分	60 分	5 時間	20 分	60 分	5 時間	
Ⅲ．１．１．４．		クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。	★								
Ⅲ．１．１．５．		クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。	●								
Ⅲ．１．１．６．		クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。	●	OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間	ベンダーリリースから 24 時間以内*	ベンダーリリースから 24 時間以内*	ベンダーリリースから 24 時間以内*	ベンダーリリースから 3 日以内*	ベンダーリリースから 3 日以内*	ベンダーリリースから 3 日以内*	
Ⅲ．１．１．７．		クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に報告すること。	★	定期報告の間隔（Web 等による報告も含む）	1 ヶ月	3 ヶ月	6 ヶ月	1 ヶ月	3 ヶ月	6 ヶ月	
Ⅲ．１．１．８．		クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。	●	第一報（速報）に続く追加報告のタイミング	発見後 1 時間	発見後 1 時間	発見後 12 時間	発見後 1 時間	発見後 12 時間	発見後 12 時間	
Ⅲ．１．１．９．		情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。	●								

Ⅲ．２．アプリケーション、プラットフォーム、サーバ・ストレージ											
Ⅲ．２．１．アプリケーション、プラットフォーム、サーバ・ストレージの運用・管理											
Ⅲ．２．１．１．	-	クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率を規定すること。 また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。	●	クラウドサービスの稼働率	99.5%以上*	99%以上*	95%以上*	99.5%以上*	99%以上*	95%以上*	
Ⅲ．２．１．２．	-	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。	●	容量・能力等の要求事項を記録した文書の保存期間	サービス提供期間＋１年間	サービス提供期間＋６ヶ月	サービス提供期間＋３ヶ月	サービス提供期間＋１年間	サービス提供期間＋６ヶ月	サービス提供期間＋３ヶ月	
Ⅲ．２．１．３．	a	利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。	●	利用者の利用状況の記録（ログ等）の保存期間	３ヶ月	１ヶ月	１週間	３ヶ月	１ヶ月	１週間	
	b			例外処理及び情報セキュリティ事象の記録（ログ等）の保存期間	５年	１年	６ヶ月	５年	１年	６ヶ月	
	c			スタンバイ機による運転再開	可能 (ホットスタンバイ)	可能 (コールドスタンバイ)	-	可能 (ホットスタンバイ)	可能 (コールドスタンバイ)	-	
Ⅲ．２．１．４．	a	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。	★	ぜい弱性診断の実施間隔（サーバ等への外部からの侵入に関する簡易自動診断（ポートスキャン等））	１回/１ヶ月	１回/１ヶ月	１回/１ヶ月	１回/１ヶ月	１回/１ヶ月	１回/１ヶ月	
	b			ぜい弱性診断の実施間隔（サーバ等への外部からの侵入に関する詳細診断（ネットワーク関係、外部委託を含む））	１回/６ヶ月	１回/１年	１回/１年	１回/６ヶ月	１回/１年	１回/１年	
	c			ぜい弱性診断の実施間隔（アプリケーションのぜい弱性の詳細診断（外部委託を含む））	１回/１年	１回/１年	１回/１年	１回/１年	１回/１年	１回/１年	
Ⅲ．２．２．アプリケーション、プラットフォーム、サーバ・ストレージの情報セキュリティ対策											
Ⅲ．２．２．１．	-	クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。	●	パターンファイルの更新間隔	ベンダーリリースから24時間以内*	ベンダーリリースから24時間以内*	ベンダーリリースから３日以内*	ベンダーリリースから24時間以内*	ベンダーリリースから３日以内*	ベンダーリリースから３日以内*	
Ⅲ．２．２．２．	-	データベースに格納されたデータの暗号化を行うこと。	★								
Ⅲ．２．３．サービスデータの保護											
Ⅲ．２．３．１．	a	利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。	●	バックアップ実施インターバル	１回/１日	１回/１週間	１回/１ヶ月	１回/１日	１回/１週間	１回/１ヶ月	
	b			世代バックアップ	５世代	２世代	１世代	５世代	２世代	１世代	
Ⅲ．２．３．２．	-	バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。	★	バックアップ確認の実施インターバル（ディスクに戻してファイルサイズを確認する等）	バックアップ実施の都度	バックアップ実施の都度	バックアップ実施の都度	バックアップ実施の都度	バックアップ実施の都度	バックアップ実施の都度	
Ⅲ．３．ネットワーク											
Ⅲ．３．１．外部ネットワークからの不正アクセス防止											
Ⅲ．３．１．１．	-	ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。	●								
Ⅲ．３．１．２．	-	情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。	●								

Ⅲ．３．１．３．	a	利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。 また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。	●	利用者のアクセス認証方法	生体認証 又は IC カード	IC カード 又は ID・パスワード	ID・パスワード	ID・パスワード	ID・パスワード	ID・パスワード	
	b			情報システム管理者、ネットワーク管理者等のアクセス認証方法	デジタル証明書による認証、生体認証 又は IC カード	生体認証 又は IC カード	IC カード 又は ID・パスワード	生体認証 又は IC カード	IC カード 又は ID・パスワード	IC カード 又は ID・パスワード	
Ⅲ．３．１．４．	-	外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。	●								
Ⅲ．３．１．５．	-	不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS/IPS の導入等）を講じること。	★	シグニチャ（パターンファイル）の更新間隔	1 回/1 日	1 回/3 週間	1 回/3 週間	1 回/1 日	1 回/3 週間	1 回/3 週間	
Ⅲ．３．２．外部ネットワークにおける情報セキュリティ対策											
Ⅲ．３．２．１．	-	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。	●								
Ⅲ．３．２．２．	-	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。	★	通信の暗号化	IP 暗号通信（VPN(IPsec)等） 又は HTTP 暗号通信（SSL(TLS)等）	IP 暗号通信（VPN(IPsec)等） 又は HTTP 暗号通信（SSL(TLS)等）	IP 暗号通信（VPN(IPsec)等） 又は HTTP 暗号通信（SSL(TLS)等）	HTTP 暗号通信（SSL(TLS)等）	HTTP 暗号通信（SSL(TLS)等）	HTTP 暗号通信（SSL(TLS)等）	
Ⅲ．３．２．３．	-	第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。	●		－	－	－	－	－	－	
Ⅲ．３．２．４．	-	利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。	●								
Ⅲ．３．２．５．	-	外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。	★	通報時間（障害が発生してから通報するまでの時間）	検知後 60 分	-	-	検知後 60 分	-	-	
Ⅲ．４．建物、電源（空調等）											
Ⅲ．４．１．建物の災害対策											
Ⅲ．４．１．１．	-	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、地震・水害に対する対策が行われていること。	★								
Ⅲ．４．２．電源・空調の維持と災害対策											
Ⅲ．４．２．１．	a	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	●	非常用無停電電源（UPS 等）による電力供給時間	10 分	10 分	10 分	10 分	10 分	10 分	
	b			複数給電の実施	実施	実施	-	実施	実施	-	
	c			非常用発電機の設置	実施	-	-	実施	-	-	
Ⅲ．４．２．２．	-	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供すること。	★								
Ⅲ．４．３．火災、逃雷、静電気から情報システムを防護するための対策											
Ⅲ．４．３．１．	-	サーバルームに設置されているクラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。	★	汚損対策の実施	汚損対策消火設備（ガス系消火設備等）の使用	汚損対策消火設備（ガス系消火設備等）の使用	-	汚損対策消火設備（ガス系消火設備等）の使用	汚損対策消火設備（ガス系消火設備等）の使用	-	
Ⅲ．４．３．２．	-	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えること。	●								
Ⅲ．４．３．３．	-	情報処理施設に雷が直撃した場合を想定した対策を講じること。	●								

Ⅲ．４．３．４．	-	情報処理施設付近に誘導雷が発生した場合を想定した対策を講じること。	★								
Ⅲ．４．３．５．	-	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じること。	★								
Ⅲ．４．４．建物の情報セキュリティ対策											
Ⅲ．４．４．１．	-	重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。	●	入退室記録の保存	2 年以上*	2 年以上*	2 年以上*	2 年以上*	2 年以上*	2 年以上*	
Ⅲ．４．４．２．	a	重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像をあらかじめ定められた期間保存すること。	★	監視カメラの稼働時間	365 日 24 時間	365 日 24 時間	365 日 24 時間	-	-	-	
	b			監視映像保存期間	6 ヶ月	1 ヶ月	1 週間	-	-	-	
Ⅲ．４．４．３．	-	重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。	●								
Ⅲ．４．４．４．	-	重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置すること。	★								
Ⅲ．４．４．５．	-	重要な物理的セキュリティ境界に警備員を常駐させること。	★	警備員の常駐時間	365 日 24 時間	365 日 24 時間	-	365 日 24 時間	365 日 24 時間	-	
Ⅲ．４．４．６．	-	サーバルームやラックの鍵管理を行うこと。	●								
Ⅲ．５．その他											
Ⅲ．５．１．機密性・完全性を保持するための対策											
Ⅲ．５．１．１．	-	電子データの原本性確保を行うこと。	★	原本性(真正性)確認レベル	時刻認証、署名及び印刷データ電子化・管理	署名 及び印刷データ電子化・管理	印刷データ電子化・管理	時刻認証、署名及び印刷データ電子化・管理	署名 及び印刷データ電子化・管理	印刷データ電子化・管理	
Ⅲ．５．１．２．	-	個人情報は関連する法令に基づいて適切に取り扱うこと。	●								
Ⅲ．５．２．クラウド事業者の運用管理端末における情報セキュリティ対策											
Ⅲ．５．２．１．	a	運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。 従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。	●	パターンファイルの更新間隔	ベンダーリリースから 24 時間以内*	ベンダーリリースから 24 時間以内*	ベンダーリリースから 3 日以内*	ベンダーリリースから 24 時間以内*	ベンダーリリースから 3 日以内*	ベンダーリリースから 3 日以内*	
	b	技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。		OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間	ベンダーリリースから 24 時間以内*	ベンダーリリースから 24 時間以内*	ベンダーリリースから 24 時間以内*	ベンダーリリースから 3 日以内*	ベンダーリリースから 3 日以内*	ベンダーリリースから 3 日以内*	
Ⅲ．５．３．媒体の保管と廃棄											
Ⅲ．５．３．１．	-	紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。	●								
Ⅲ．５．３．２．	-	機器及び媒体を正式な手順に基づいて廃棄すること。	●								

Annex 3 典型的なクラウドサービスのパターン化とクラウドサービスの典型的な構成要素の図式化

○ 典型的なクラウドサービスのパターン化

典型的なクラウドサービスについて、クラウドのサービス種別の特性を考慮してパターンごとに分類した結果が、図表 Annex3-1 である。本ガイドラインに基づいて「Ⅲ．物理的・技術的対策編」の対策を実施する場合は、提供するサービスがどのパターンに分類されているかによって、具体的な対策が異なってくるので、注意が必要である。

図表 Annex3-1 パターンごとのサービス種別

パターン	サービス種別
1	受発注、人事給与・勤怠管理・経理、ERP（財務会計等）、EC サポート（電子商取引のアウトソーシング）、ネットショッピング支援（仮想店舗貸しサービス）、コールセンター支援、金融業特化型サービス（地銀・信金共同アウトソーシング）、医療・介護・福祉業特化型サービス、電子入札、公共住民情報、決済サービス、不正アクセス監視
2	販売管理・売掛金管理、公共窓口業務、在庫管理、建設業特化型サービス、卸売・小売・飲食業特化型サービス、保険業特化型サービス（生命保険見積）、宿泊業特化型サービス、公共電子申請、公共個別部門業務、グループウェア、アドレス帳サービス、位置時間証明サービス、統合型校務支援サービス、保護者メール
3	購買支援、CRM（顧客管理）・営業支援、販売支援、契約、採用管理、資産管理、ネットショッピング（自らの売買支援）、金融業特化型サービス（信用情報提供）、保険業特化型サービス（自賠責保険見積）、アフィリエイト、メール配信、学習系サービス
4	ネットワーク監視
5	EC サポート（産地直送等、物流・決済を一括で提供）
6	広告、IT 資産管理、ニュースリリース業務、運輸業特化型サービス、電話会議・TV 会議・Web 会議、乗り換え、不動産物件検索、検索サービス（一般向け）
※	文書管理、オンラインストレージ、Web サイトのホスティング、ブログ・コミュニティコーディネート、コンテンツデリバリー・ストリーミングサービス、GIS（地図情報システム）/GIS 応用、映像監視、メディア・言語変換サービス、検索サービス（個別用途）、認証サービス、セキュリティサービス、IoT サービス

※一律にパターンを設定することが困難なサービス

なお、図表 Annex3-1 は全てのクラウドサービスの特性を網羅しているものではない。したがって、自らが提供するクラウドサービスが、図表 Annex3-1 で分類されているパターンにそぐわない場合、図表 Annex3-1 中に存在しない場合、「一律にパターンを設定することが困難なサービス」に該当する場合等は、「Ⅲ．物理的・技術的対策編」に示した凡例に基づき、該当するパターンを独自に判定することが望ましい。

クラウド事業者が提供するサービスは、基幹系業務システムからグループウェアに至るまで多岐に渡っており、その取り扱う情報の違いから、各クラウドサービスに要求される「機密性」「完全性」「可用性」のレベルも必然的に異なってくる。

そこで、本ガイドラインでは、「Ⅲ．物理的・技術対策編」の凡例においては、クラウドのサービス種別を「機密性」「完全性」「可用性」の観点から、その特性ごとに６パターンに分類している。また、この分類を基に「物理的・技術的対策編」の対策項目をパターン化している。

ここでの「機密性」、「完全性」、「可用性」への要求の高低に関する考え方は次のとおりである。

【機密性への要求】

以下の情報を扱う場合には、その件数に関わりなく、機密性への要求は「高」い。

(1)個人情報

利用者及び利用者の顧客に関する、特定の個人を識別することができる情報。

(2)営業秘密情報

秘密として管理されている生産方法、販売方法、その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの。

【完全性への要求】

クラウド事業者が利用者のデータを管理するという特性上、そのデータに改ざん・削除等のインシデントが発生した場合、顧客の事業継続に多大な影響を与えるものと考える。また、クラウド事業者が提供する情報においても、その情報に改ざん等のインシデントが発生した場合、その情報に依存している顧客にとって大きな損害が発生することが想定される。したがって、クラウド事業者においては、そのサービス種別にかかわらず、完全性への要求は「高」いものと考える。

【可用性への要求】

(1)可用性への要求が「高」いサービス

a 定められたサービス提供期間中は、必ず稼働させておくことが求められるサービス

b サービスが停止することで、利用者に多大な経済的損失や人命に危害が生じるおそれのあるサービス

(2)可用性への要求が「中」程度のサービス

a サービスが停止することで、利用者に部分的な経済的損失が生じるおそれのあるサービス

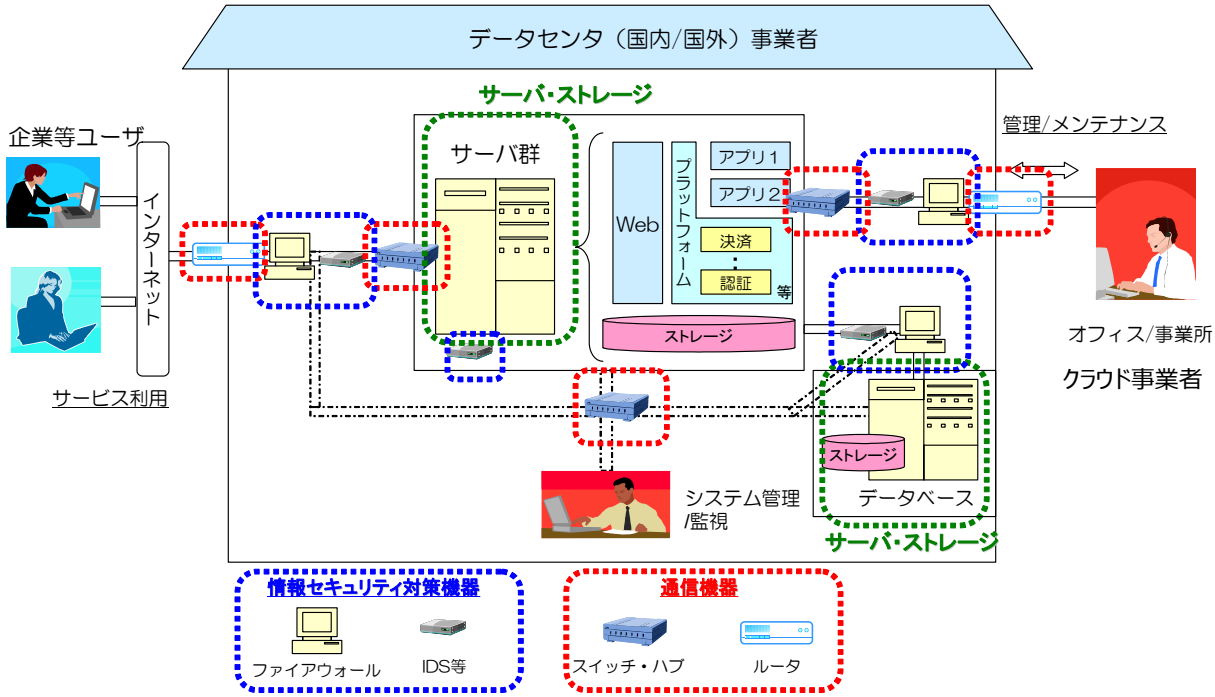
b サービスが停止することで、利用者の基幹業務に明確な影響を及ぼすサービス

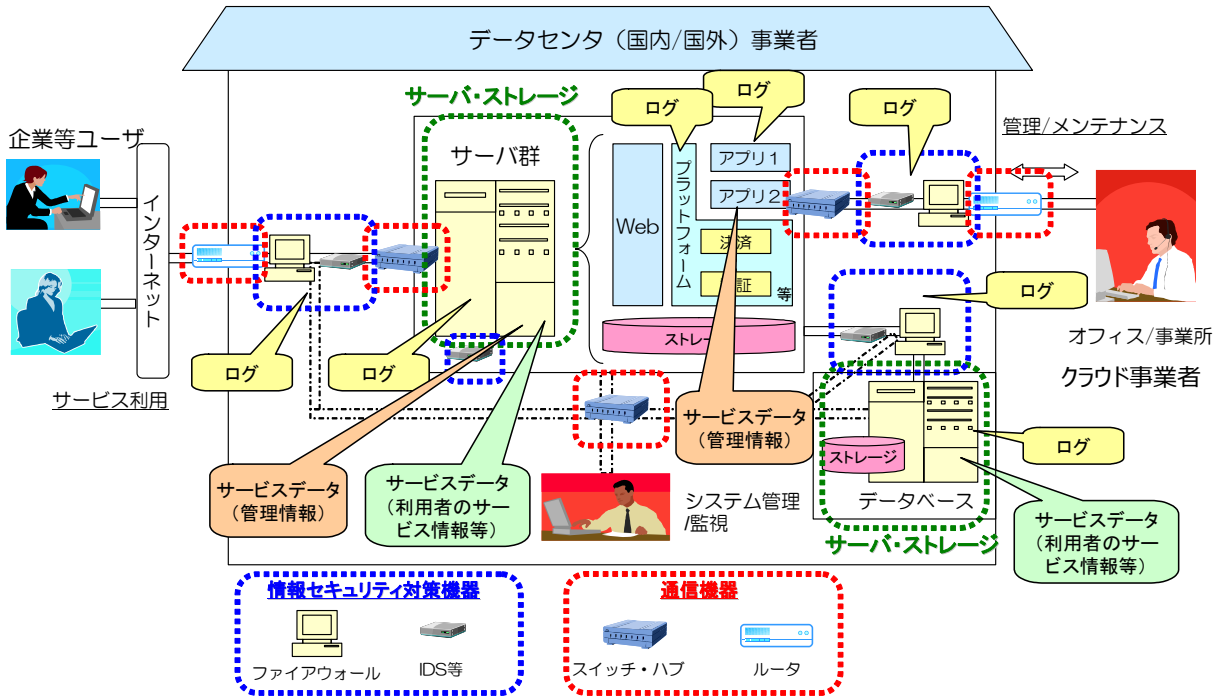
(3)可用性への要求が「低」いサービス

(1)、(2)以外のサービス

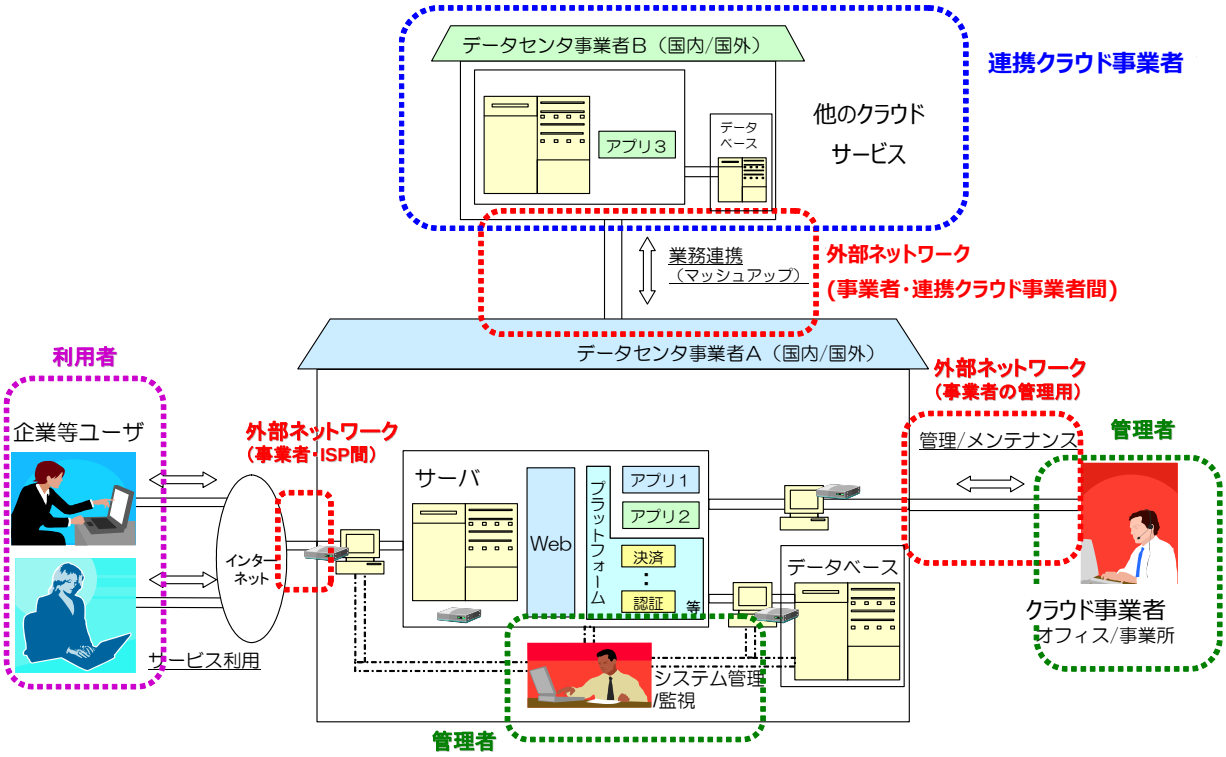
○ **クラウドサービスの典型的な構成要素の図式化**

Ⅲ． １． アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策

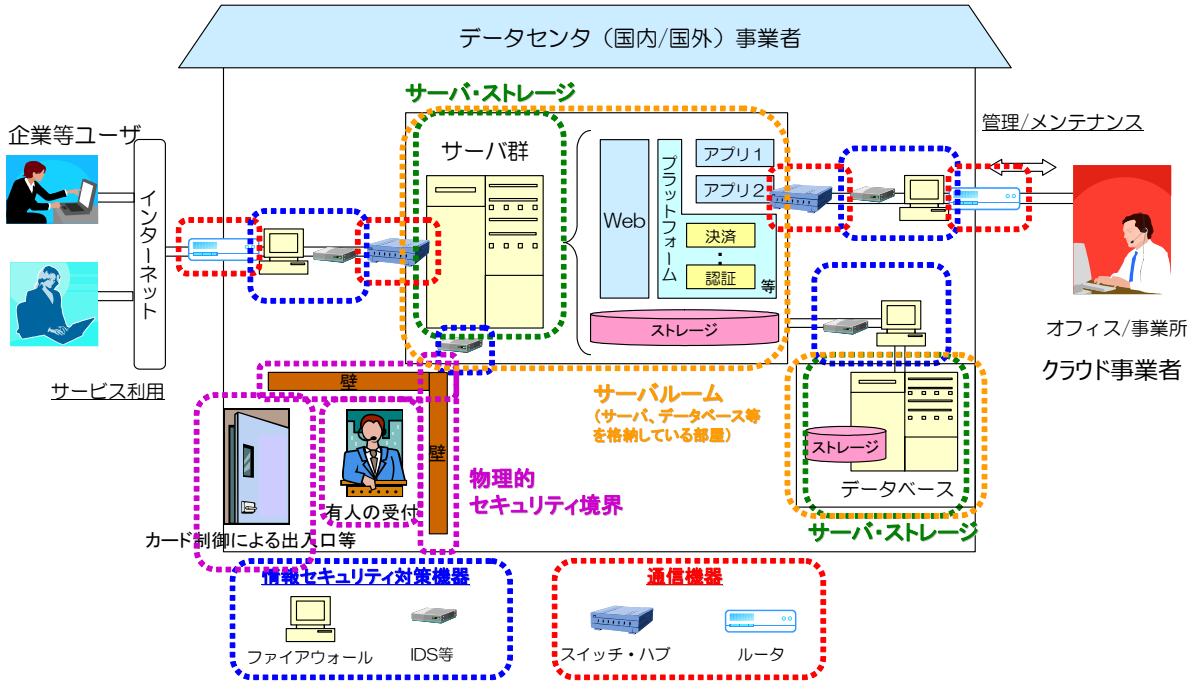



データセンタ（国内/国外）事業者
企業等ユーザ
インターネット
サービス利用
サーバ・ストレージ
サーバ群
ログ
ログ
ログ
ログ
ログ
ログ
Web
プラットフォーム
アプリ1
アプリ2
決済
認証
等
ストレージ
管理/メンテナンス
オフィス/事業所
クラウド事業者
サービスデータ（管理情報）
サービスデータ（利用者のサービス情報等）
サービスデータ（管理情報）
サービスデータ（利用者のサービス情報等）
システム管理/監視
ストレージ
データベース
サーバ・ストレージ
情報セキュリティ対策機器
ファイアウォール
IDS等
通信機器
スイッチ・ハブ
ルータ

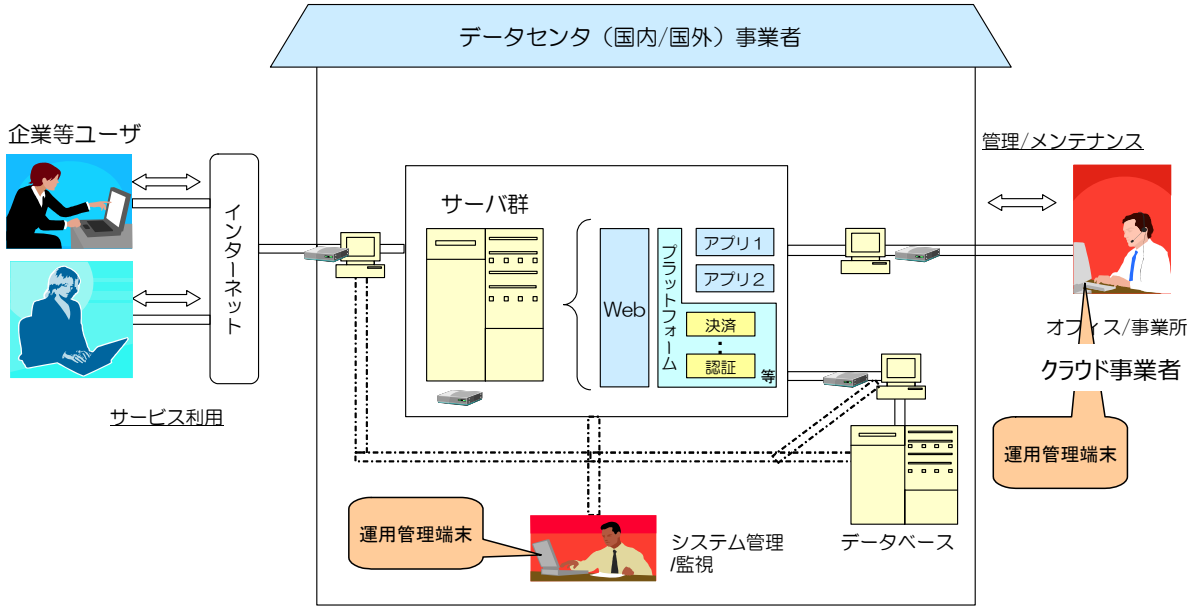
Ⅲ． 3．ネットワーク


データセンタ事業者Ｂ（国内/国外）
連携クラウド事業者
アプリ３
データベース
他のクラウド
サービス
業務連携
（マッシュアップ）
外部ネットワーク
(事業者･連携クラウド事業者間)
データセンタ事業者Ａ（国内/国外）
外部ネットワーク
（事業者の管理用）
利用者
企業等ユーザ
外部ネットワーク
（事業者･ISP間）
管理/メンテナンス
管理者
サーバ
Web
プラットフォーム
アプリ１
アプリ２
決済
：
認証
等
データベース
インターネット
サービス利用
クラウド事業者
オフィス/事業所
システム管理
/監視
管理者

Ⅲ．４．建物、電源（空調等）


データセンタ（国内/国外）事業者
サーバ・ストレージ
企業等ユーザ
インターネット
サービス利用
サーバ群
Web
プラットフォーム
アプリ1
アプリ2
決済
認証
等
ストレージ
管理/メンテナンス
オフィス/事業所
クラウド事業者
壁
壁
有人の受付
カード制御による出入口等
物理的
セキュリティ境界
サーバルーム
（サーバ、データベース等
を格納している部屋）
ストレージ
データベース
サーバ・ストレージ
情報セキュリティ対策機器
ファイアウォール
IDS等
通信機器
スイッチ・ハブ
ルータ

Ⅲ．５．その他


データセンタ（国内/国外）事業者
企業等ユーザ
インターネット
サービス利用
サーバ群
Web
プラットフォーム
アプリ1
アプリ2
決済
認証
等
管理/メンテナンス
オフィス/事業所
クラウド事業者
運用管理端末
運用管理端末
システム管理
/監視
データベース

Annex 4 利用者接点と ICT サプライチェーンに着目したクラウドサービスの特徴

○利用者接点と ICT サプライチェーンに着目する必要性

クラウドサービスの導入が本格化するにつれて、クラウドサービスのサービスメニューもアプリケーション領域（ASP・SaaS）から実行環境・インフラ領域（PaaS、IaaS 等）に拡大し、クラウドサービスの提供形態も分業が進んできた。元々は単独のクラウド事業者がサービスを提供する形態が多かったが、現在はインフラや実行環境ごとサービス提供する基幹事業者と、そのインフラを借り受けてアプリケーションサービスを中心にサービスを提供する事業者に分かれて協業が進んでいるほか、アプリケーションサービスを提供する事業者同士が連携してサービスを提供する事例も急増している。

このように、ICT サプライチェーンを編成してクラウドサービスを提供する形態が現在の主流であると言える。しかし、このサービス提供形態の複雑化は、クラウド事業者によるクラウドサービス全体の統制を難しくする要因となっており、全体としてのサービスレベルの低下、ログ取得・保持やレビューの抜け漏れの発生等に直面しやすくなる。これらはクラウド事業者から見た課題である。

このようなクラウドサービスを取り巻く環境の変化から生じる課題に対応するためには、クラウドサービスを安全・安心に利用するための十全な情報セキュリティマネジメントが不可欠である。クラウド事業者が、クラウド利用者及び ICT サプライチェーンを構成する供給者との間で十分な信頼と協力関係を築き上げ、安全・安心なクラウドサービスを提供することができるよう、実践するべき利用者接点の実務を理解する必要がある。

○供給者関係のモデル

クラウド利用者とクラウド事業者の間の役割と責任の分担及び ICT サプライチェーンを構成するクラウド事業者と供給者間の役割と責任の分担に伴って発生する様々な問題を正しく理解するためには、クラウド利用者とクラウド事業者と ICT サプライチェーンの供給者がどのような関係にあるかの類型（以下「供給者関係のモデル」という。）を理解している必要がある。

本ガイドラインでは、供給者関係のモデルを、エンドユーザ（組織）と複数のクラウド事業者がどのような契約形態を取るかによって、「垂直連携型」と「水平連携型」の二つのモデルに分類する。

クラウド事業者は、ICT サプライチェーンを構築して提供しているクラウドサービスが、垂直連携型なのか水平連携型なのかを良く理解した上で、各モデルの特徴に従って利用者接点の実務を実施することが求められる。

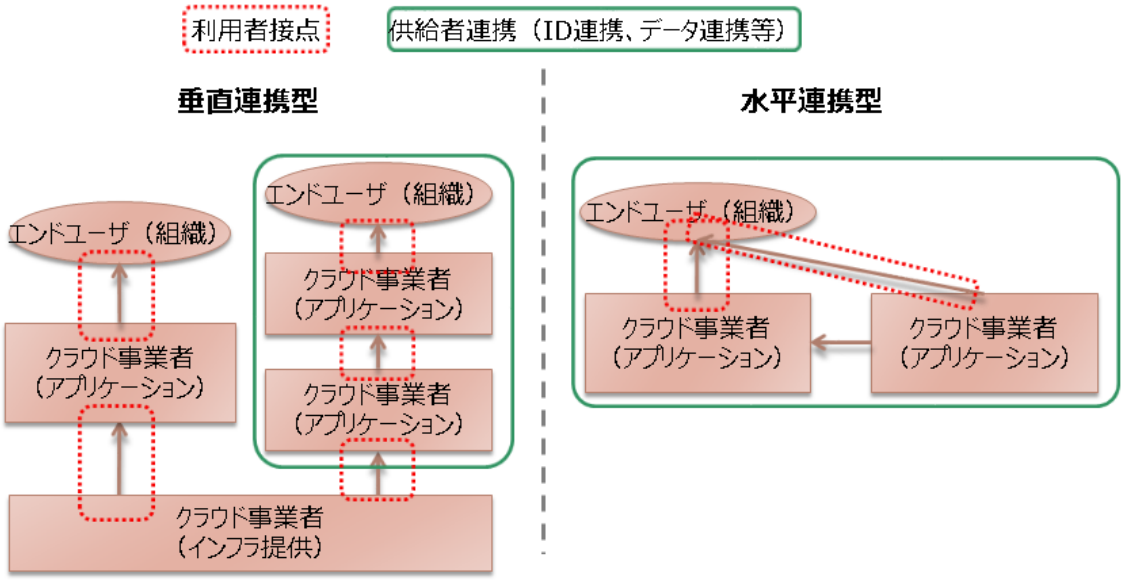
「垂直連携型」では、アプリケーションサービス提供側がアグリゲーションサービス事業者となって、基幹事業者からインフラ又は実行環境を借り受ける。サービス品質の良いインフラを提供し続けるのは基幹事業者の役割であり、エンドユーザ（組織）との間の接点の実務を処理するのはアプリケーションサービス提供側の役割となる。

「水平連携型」では、ICT サプライチェーンを構成する個別契約連携クラウド事業者は、エンドユーザ（組織）との契約関係においても、エンドユーザ（組織）との接点の実務を処理する責任についても対

等である。一方、ICT サプライチェーン全体での統制を取る役割のクラウド事業者がいないことから、クラウドサービスの品質は最低のサービスレベルを提供する個別契約連携クラウド事業者によって決まる。

ICT サプライチェーンにおいて、エンドユーザ（組織）と複数のクラウド事業者が ID 連携、データ連携等を行う場合がある。この場合には、関係する全てのステークホルダー組織（エンドユーザ（組織）を含む）が構成する供給者連携に対して、クラウド情報セキュリティマネジメントの実務を行う必要がある。供給者関係のモデルについて図表 Annex4-1 に示す。

図表 Annex4-1 供給者関係のモデル



○「垂直連携型」とは

エンドユーザ（組織）にクラウドサービスを提供するクラウド事業者が、アグリゲーションサービス事業者である場合である。この場合、アグリゲーションサービス事業者が、ICT サプライチェーンを代表してエンドユーザ（組織）と一括契約を締結し、ワンストップサービスを提供する。エンドユーザ（組織）は、ICT サプライチェーンの存在を気にかける必要はない。このため、エンドユーザ（組織）とクラウド事業者の接点における実務は単純になるが、ICT サプライチェーンではアグリゲーションサービス事業者が供給者全体を統制する必要が生じる。

○「水平連携型」とは

エンドユーザ（組織）が、ICT サプライチェーンを構成する各々の個別契約連携クラウド事業者と個別に契約を結ぶ形態である。この場合は、個別契約連携クラウド事業者によって実務対応に違いが出てしまい、個別契約連携クラウド事業者間での綿密な調整が必要になるなど、エンドユーザ（組織）とクラウド事業者の接点における実務対応は複雑になる。

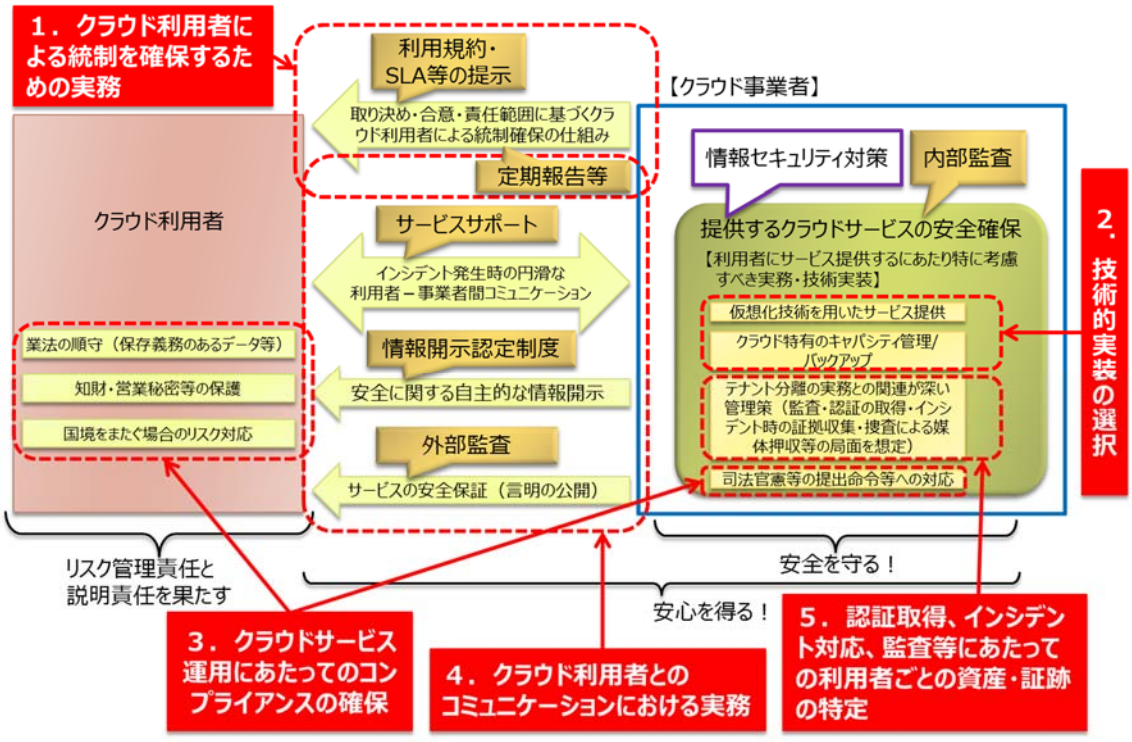
○クラウドサービス提供において留意すべき五つの観点

クラウドサービスの提供において留意すべき五つの観点は以下のとおりである。

1．「クラウド利用者による統制を確保するための実務」
2．「技術的実装の選択」
3．「クラウドサービス運用にあたってのコンプライアンスの確保」
4．「クラウド利用者とのコミュニケーションにおける実務」
5．「認証取得、インシデント対応、監査等にあたっての利用者ごとの資産・証跡の特定」

利用者接点と ICT サプライチェーンに着目したクラウドサービスにおいて留意すべき五つの観点について、図表 Annex4-2 に示す。

図表 Annex4-2 クラウドサービス提供において留意すべき五つの観点



クラウド利用者は、ICT 初期投資・運用コストの削減、情報処理資源のオンデマンド利用、常に最新化される機能の利用、グローバル化への対応、情報セキュリティマネジメント向上と業務負荷/投資軽減等の様々な期待を持って、自身が管理する設備内に情報システムを設置・運用する形態（以下「オンプレミス」という。）からクラウドサービスに移行してくる。

しかし、たとえクラウドサービスへの移行によって便益を確保できたとしても、クラウド利用者が自ら情報セキュリティマネジメントの確保において不利な条件を選択してしまったら、オンプレミスの際には確保できていた自組織の情報セキュリティポリシーの実践が困難になり、対応に苦慮することになる。

このような課題を克服するため、クラウド事業者としては、Annex 6 で述べる「利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策」を適用し、クラウド利用者とクラウド事業者の公平な取引を促進するための措置を講じることに努める必要がある。

なお、五つの観点の具体的な留意すべき点は以下のとおりである。

（1）クラウド利用者による統制を確保するための実務

クラウド利用者による統制を確保するための実務とは、クラウド利用者がクラウド事業者を自らの方針に従って統制できるように、必要な取決め・合意・責任の範囲の設定等を行うことである。ICT サプライチェーンにおいては、アグリゲーションサービス事業者が ICT サプライチェーン全体を統制する実務と、個別契約連携クラウド事業者の間で責任の範囲と役割の分担を設定する実務がある。それぞれの実務についての本ガイドラインにおける記述の概要を図表 Annex4-3 に示す。

図表 Annex4-3 クラウド利用者による統制を確保するための実務の概要

分類	実務の概要
クラウド利用者 – クラウド事業者間の実務	・クラウド利用者とクラウド事業者の責任の分担の設定 ・クラウド利用者のポリシーに沿うクラウドサービス選択を促進するための支援 ・クラウド利用者の運用措置（監査、預託情報のバックアップ等）の支援と役割分担の明確化　等
アグリゲーションサービス事業者 – 供給者間の実務（垂直連携型の場合）	・ICT サプライチェーン全体としてのサービスレベル確保 ・ICT サプライチェーン全体としての管理要求の統制　等
個別契約連携クラウド事業者の間の実務（水平連携型の場合）	・個別契約連携クラウド事業者間の責任範囲と役割の分担の設定 ・他の個別契約連携クラウド事業者が提供するサービスに及ぼす影響や、他の個別契約連携クラウド事業者が提供するサービスから受ける影響を緩和するための措置　等

（2）技術的実装の選択

技術的実装の選択とは、クラウドサービスの情報セキュリティマネジメントを実践するにあたり、技術の適切な実装方法を選択し、その選択によってクラウド利用者の運用管理の実務に変更の必要性が生じた場合は、必要な技術情報をクラウド利用者に提供することである。

(3)クラウドサービス運用にあたってのコンプライアンスの確保

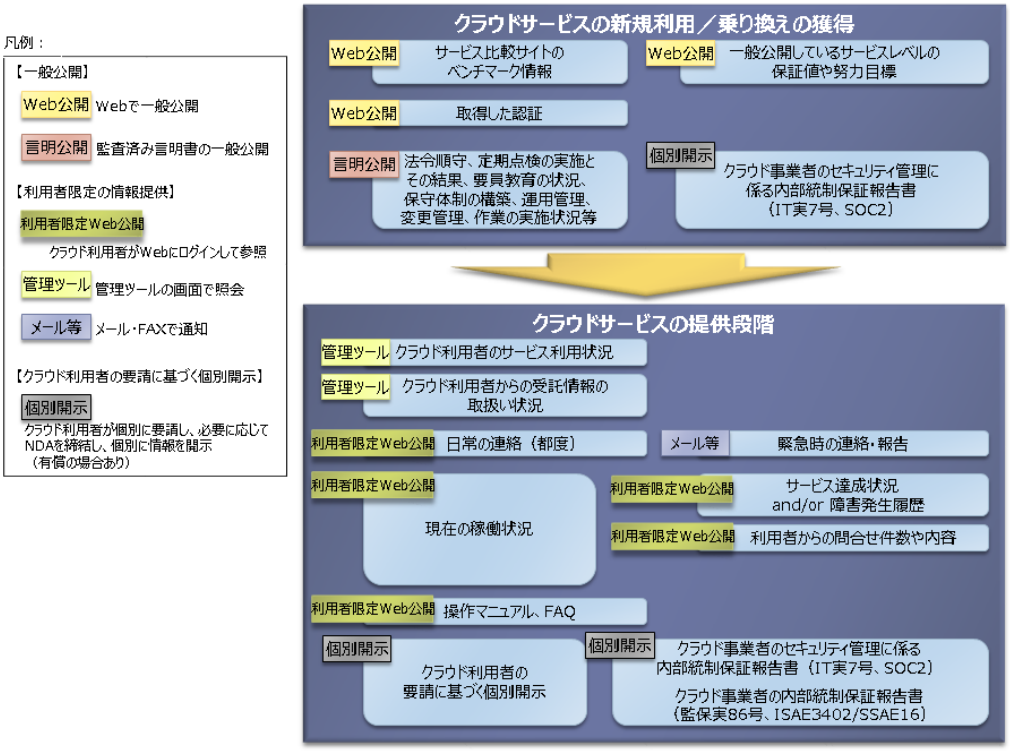
クラウドサービス運用にあたってのコンプライアンスの確保とは、クラウドサービスを運用することによって生じうるクラウド利用者側及びクラウド事業者側のコンプライアンス違反の予防である。特に、クラウド利用者から預託されたデータを、裁判管轄権を跨いで保存した場合のコンプライアンス確保への対処が重要になる。本ガイドラインでは、以下に列挙する実務について指針を示している。

- クラウド利用者が業法等による要求事項等を確保できるようにするための支援（サービス機能の提供等）
- 国際的に展開されたクラウドサービスにおいて、海外における適用法の違いによってクラウド利用者及び預託された情報に生じるリスクを緩和するための、クラウド利用者側及びクラウド事業者側の措置に係る実務
- 海外の司法官憲等の捜査等により、海外にある資産・サービスに起因するクラウドサービス全体の停止等を予防するための実務　等

(4)クラウド利用者とのコミュニケーションにおける実務

クラウド利用者とのコミュニケーションにおける実務とは、クラウドサービス提供の各段階において、クラウド事業者からクラウド利用者に対して行う情報の公開・開示である。具体的には、クラウドサービスの新規顧客/乗り換えを獲得する段階と、クラウドサービスを提供する段階で、クラウド利用者に対して提供する情報の内容や提供手段は異なる。図表 Annex4-4 にその概要を示す。

図表 Annex4-4 クラウドサービス提供の各段階と公開・開示する情報の関係



○クラウドサービスの新規顧客/乗り換えを獲得する段階での情報開示

開示すべき情報は以下のとおり。

1. クラウドサービスが保証又は努力目標とするサービスレベルの公開
2. 取得した認証
3. 監査済み言明書の公開（法令遵守、定期点検の実施とその結果、要員教育の状況、保守体制の構築、運用管理、変更管理、作業の実施状況等）
4. クラウド事業者のセキュリティ管理に係る内部統制保証報告書（IT 実 7 号、SOC2 等）

（参考）クラウドサービスが保証又は努力目標とするサービスレベルの具体的な指標

例えば故障回復時刻、故障通知時刻、サービス提供時間、ヘルプデスク提供時間、サービス稼働率、平均応答時間、情報セキュリティ対策・設備の措置、ログ記録、サービス継続のための措置、バックアップ、暗号化に対応できるサービスの範囲などが設定される。また、SLA 文書の内容を公開している例も見られる。

○クラウドサービスの提供段階での情報開示

提供すべき情報は、以下のとおり。

1. クラウド利用者のサービス利用状況
2. クラウド利用者が預託された情報の取扱い状況
3. 日常の連絡
4. 緊急時の連絡・報告
5. 現在の稼働状況
6. サービス達成状況（障害発生履歴の情報公開を含む）
7. クラウド利用者からの問合せ件数や内容
8. 操作マニュアル・FAQ
9. クラウド事業者のセキュリティ管理に係る内部統制保証報告書（IT 実 7 号、SOC2 等）
10. クラウド事業者の内部統制保証報告書（監保実 86 号、ISAE3402/SSAE16 等）
11. その他クラウド利用者個別に提供する詳しい情報

（参考）具体例

○クラウド利用者のサービス利用状況

・利用者のログイン実績、利用時間、利用ログなどの情報開示。

・日常の連絡としては、計画的サービス停止/定期保守の案内、バージョンアップの案内、マニュアル類の最新版公開の案内、利用規約/SLA の改訂、技術的ぜい弱性情報・情報漏えいに繋がる脅威情報（フィッシング、マルウェア等）、サービス提供に係る関係国の適用法に関連したリスク情報等の提供

・緊急時の連絡・報告として、障害発生/復旧時刻の通知、障害経過の通知、障害内容・原因・対処・再発防止策等に係る事後報告等の情報提供

○サービス達成状況

・稼働率、平均応答時間、サポートサービス応答率などの月次実績等の情報提供

・障害発生履歴の詳細情報の提供

○その他(クラウド利用者個別に提供する情報)

・クラウド利用者が希望する種別のインシデント情報（月次等で定期報告）

・第三者機関による監査レポート・ぜい弱性検査レポート

・クラウド事業者が行うバックアップの仕様（範囲・スケジュール、方法・データフォーマット、保存期間、バックアップデータの完全性確認やリストアの手順等）

・イベントログ記録の仕様（ログ記録のタイプとタイプ別の保存期間、クラウド利用者がログを検査する権利と検査手順等）

・ID 管理の権限設定の細かさ・ID 連携の有無

・供給者関係の中で誰がどこでデータを保管し何を記録しているか

・契約終了後の受託情報の抹消方法

・SLA の内容等

○クラウド利用者個別の情報開示を行うにあたっての留意事項

クラウド利用者個別の情報開示を行う場合、以下の５点に留意する。

1. クラウド事業者は、以下の二つのトレードオフを判断すべき。
   ・クラウド利用者にとっての知るメリットと、同様の情報が他のクラウド利用者にも共有されることによるクラウド利用者の情報セキュリティマネジメント上のデメリットの間のトレードオフ
   ・クラウド利用者にとっての知るメリットと、クラウド事業者にとっての情報開示するデメリットの間のトレードオフ
2. クラウド利用者が細かい情報を要求し、自ら詳しく判断・管理しようとする場合は、クラウド利用者に対して開示可能な情報の範囲や粒度、頻度について事前に説明を行い、提供するサービスがクラウド利用者の要求を満足するかの正確な判断を促進すべき
3. 有償の場合がある
4. 通常は NDA を締結の上で情報開示する
5. 対策の実施状況に係る言明を、監査により合理的な水準で保証を受けた上で、クラウド利用者に対し開示することも検討すべき

一方、上述した情報をクラウド利用者に提供する手段としては、管理ツールによる情報照会機能の提供、利用者限定 Web 公開、メール等による通知、クラウド利用者の要請に基づく個別開示が行われている。提供する情報と用いる手段の関係については図表 Annex4-4 を確認していただきたい。

（５）認証取得、インシデント対応、監査等にあたっての利用者ごとの資産・証跡の特定

認証取得、インシデント対応、監査等にあたっての利用者ごとの資産・証跡の特定とは、クラウド利用者やクラウド事業者による認証取得・監査、並びにインシデント対応等にあたり、クラウド事業者が特に要求された場合に、クラウド利用者ごとの資産（預託された情報）・証跡を特定・分離することである。マルチテナントサービスを提供する場合のテナント分離の要求であると言える。

Annex 5 利用者接点と ICT サプライチェーンに着目した要求事項

クラウドサービスの提供に関わらない対策項目に対しては、ISO/IEC27002 との紐付けは行っていない。したがって、Annex 5 において、章、節番号は連続していない。

6　情報セキュリティのための組織

6.1　内部組織

クラウド利用者とクラウド事業者の間及びクラウド事業者と供給者の間において、ガバナンスの実態が異なる組織が利用者接点を形成することから、その両側の組織の間で情報セキュリティマネジメントの統制が不十分になりやすく、これに対する管理策が必要である。

6.1.1　情報セキュリティの役割及び責任

クラウド利用者とクラウド事業者の間及びクラウド事業者と供給者の間において、ガバナンスの実態が異なる組織間で管理責任等の範囲を設定することから、その範囲の設定内容の細部に係る同意や、内容に関する解釈が不明確になりやすいため、資産と情報セキュリティプロセスの識別を慎重に行い、明確な責任の範囲の割当を行うことが求められる。

6.1.2　職務の分離

システム設計・構築やサービス運用・設定における人為的ミスが、多数のクラウド利用者に影響を及ぼし、クラウド事業者の信用低下に繋がるおそれがあることから、人為的ミスを発見して取り除くための確認を徹底することが求められる。

6.2　モバイル機器及びテレワーキング

モバイル機器から業務用クラウドサービスを利用する際の課題は、モバイル機器からの情報漏洩、クラウド事業者によるモバイル機器から取得されたビジネス価値の高い情報の不正利用等である。これらに対する管理策が求められる。

6.2.1　モバイル機器の方針

クラウドサービスを利用するエンドユーザ（組織）の従業員等がモバイル機器を業務で利用する際には、モバイル機器にキャッシュされる秘密認証情報や業務データが漏洩するリスクが高く、これを防止する対策が求められる。特に BYOD など、対応が不十分なモバイル機器が利用されることで、エンドユーザ（組織）における情報セキュリティマネジメントに関する統制が取れず、その結果、エンドユーザ（組織）で講じている管理策の全てが徹底されず、不正プログラムが入るなど情報が漏えいするおそれがあるため、十分な対策が求められる。

モバイル機器には、スマートフォン/タブレット、携帯電話及びノート PC 等のデバイスがある。これらのデバイスごとに、取るべき対策の内容や、対策の取りやすさも異なっている。しかし、共通しているのは、クラウドサービスが、それぞれのデバイスに適合した認証方法を提供することにより、アクセス制御を確実にすることが求められるということである。

他方、モバイル機器からの業務用 ASP・SaaS 利用においては、今後、クライアントアプリケーションを開発してクラウド利用者に配布し、モバイル機器にインストールして利用する形態が増えていく。このクライアントアプリケーションの不具合により、モバイル機器から個人情報や業務データが意図せず漏洩する事象が発生しうることから、クライアントアプリケーションの試験には特に注意が必要となる。モバイル機器の位置情報のように、ビジネス等で価値の高い情報を、クライアントアプリケーションを用いて収集することも可能になるため、クラウド利用者から収集する情報の内容や利用方法を、アプリケーション設計時から明確にしておくことが求められる。

また、モバイル機器からの業務用 ASP・SaaS 利用において、モバイル機器のブラウザ等を用いてクラウドサービスを利用する場合、HTML5 等の先進的な Web 技術を用いるケースが増えており、これらに特有のぜい弱性を持ち込む可能性が高まるため、Web サービスの開発段階から留意する必要がある。

6.3 クラウド利用者とクラウド事業者の公平な取引を確保するための措置

クラウドサービスは、その特性から、クラウド利用者による個別の情報セキュリティ要求に応えられる範囲が限定される。このため、クラウドサービス提供にあたり、どこまでがクラウド利用者の責任範囲であり、クラウド利用者がクラウドサービスの情報セキュリティマネジメントをどこまで統制することができ、どこまでのサービスレベルが得られ、どこまでの範囲で個別対応が可能かについて、クラウド利用者の理解を深めることにより、クラウド利用者のニーズに適合したクラウドサービスを選択できる環境を構築していくことが求められる。

6.3.1 クラウドサービスの情報セキュリティマネジメントに係る提供条件の明確化

クラウド利用者に、クラウドサービスの情報セキュリティマネジメントに係るクラウド利用者とクラウド事業者の責任範囲、サービスレベル、クラウド利用者個別に対応可能な範囲等の提供条件の正しい認識を定着させるために、あらかじめ文書化しておくことが求められる。また、この文書に係る情報提供により、提供条件を理解しているクラウド利用者の範囲を広げることで、自らのニーズに適合するクラウドサービスを選択するクラウド利用者を増やしていくことが望ましい。

6.3.2　利用者接点とサプライチェーンにおける情報提供・共有

クラウド事業者からクラウド利用者への情報提供の目的は、クラウドサービス提供の段階によって異なる。ここで、情報とは「情報セキュリティマネジメントに影響を及ぼす情報」のことを指す。一つの目的はクラウドサービスの新規利用/乗り換え利用を目論むクラウド利用者への情報提供であり、もう一つの目的はクラウドサービスを提供している段階でのクラウド利用者への情報提供である。

新規利用者への情報提供においては、クラウド利用者が自組織の統制要求を満たすことができないクラウドサービスを選択してしまうと、係争の原因となるばかりでなく、利用者個別の要求を増加させる要因にもなる。このため、クラウド利用者の選択に必要な情報を提供し、自組織の統制を満たすことができるクラウドサービスを選択することを促すことが求められる。

一方、クラウドサービス提供段階では、ガバナンスの実態が異なる組織であるクラウド利用者とクラウド事業者の信頼関係を損なわないように、情報セキュリティマネジメントの統制に係る協力的な情報提供を確立することが求められる。情報セキュリティインシデント発生時には、長時間サービスが停止したり、クラウド利用者が納得する状況報告が適時にできないことにより、クラウド利用者からの信用を失ってしまうおそれがある。このため、ICT サプライチェーン全体でクラウド利用者に提供する情報を共有し、クラウド利用者に早く正確な情報を提供することが求められる。

8　資産の管理

8.1　資産に対する責任

クラウド利用者による、重要度が高い預託情報に対する格別の保護要求と、クラウド事業者及びそのサービスに係る情報セキュリティマネジメント並びにそのガバナンスの実態とが整合せず、預託情報の保護に支障をきたすことを防ぐ必要がある。

8.1.1　資産目録

クラウドサービスがクラウド利用者の持つ重要な情報に対する保護要求方針を満足できないにもかかわらず、クラウド利用者がこの重要情報をクラウドサービスに預託してしまうと、この預託情報の保護が困難になるおそれがある。そこで、クラウド利用者自身が、その重要度判断とその保護要求方針に従って、クラウドサービス上で取り扱うことができるクラウド利用者の情報を選別して預託できるように、その判断に必要な情報を提供することが求められる。

8.1.2　資産の管理責任

クラウド利用者が作成し管理する目録の中の各々の預託情報が求める管理水準を確実にするため、これらの資産が保存されるクラウド事業者の情報処理施設等（仮想化資源を含む）の管理ポリシーに基づいて、クラウド利用者の要求に沿う管理水準を提供できるサービスを選択することが求められる。

8.1.5　クラウド利用者から預託された情報の返却

クラウド利用者がクラウドサービスの利用を終了するにあたり、他のクラウドサービスへの乗換を行うことが想定される。クラウド利用者によるクラウドサービス選定の自由を守るため、預託された情報を他のクラウドサービスに引き継ぐことを確実にすることが求められる。

また、クラウドサービス利用終了後に、クラウド事業者から預託情報が流出しないようにすることが求められる。

8.2 情報分類

クラウドサービスの提供にあたっては、多数のクラウド利用者が存在することに伴い、クラウド利用者の預託情報が、他のクラウド利用者の預託情報と明確に分離できる形で管理されていないおそれがある。また、複数のクラウドサービスを提供する場合には、クラウド利用者の預託情報が、サービスごとに分類されていないおそれがある。その結果として、クラウド利用者から預託された情報に対し、クラウドサービスごとに適切な情報セキュリティポリシーや管理水準が適用されなかったり、預託情報がクラウド利用者ごとに保護されなかったりといった事態を生じうる。

したがって、クラウド利用者から寄託を受ける情報及び提供するそれぞれのクラウドサービスにおいて供する情報資産等について、クラウド利用者ごと及びクラウドサービスごとに適切に管理ができるように、必要となる情報の分類を行うことが求められる。

8.2.1 情報の分類

クラウドサービスにおいては、一つの資源を用いて同時に複数のサービスを提供することがある。その場合、クラウド利用者が預託する情報は、それぞれのサービスで重要度が異なることがあるにもかかわらず、同一の管理が行われることになる。その結果として、預託情報の重要度に応じた管理ができないために、クラウド利用者の重要な預託情報が脅威にさらされるおそれがある。これを避ける観点から、クラウド利用者から預託を受けた情報をクラウドサービスごとに区分し、その重要度に応じた管理を行うことが求められる。

8.2.3 資産の取扱い

クラウドサービスにおいては、複数のクラウド利用者から預託を受け、返却が必要となる情報[28]を、同一の資源において取り扱うことになる。預託されたクラウド利用者の情報が、他のクラウド利用者のものと明確に分離できる形で管理されていない場合には、預託された情報の返却等が生じた場合に、他のクラウド利用者から預託を受けた情報を混同して返却してしまう等、情報漏えいを生じるおそれがある。

[28] ASP・SaaS は、クラウド利用者がコンピュータで情報処理するために、情報の預託を受けるサービスである。PaaS や IaaS は利用者にコンピュータ資源や実行環境を提供するサービスであり、一般にはクラウド利用者に返却すべき情報がない。

９　アクセス制御

９.１　アクセス制御に対する業務上の要求事項

クラウドサービスは、インターネットを経由してサービス提供されることから、クラウド事業者、クラウド利用者以外の第三者による不正なアクセスや攻撃の脅威にさらされる。

加えて、クラウドサービスでは、クラウド事業者と供給者によるサービス連携がなされうること、サービスに供する資源を複数のクラウド利用者が利用することなどから、アクセス制御に係るぜい弱性などにより、クラウド事業者やクラウド利用者による不正アクセス等も生じうる。また、不完全なアクセス制御などに伴うサービス提供の不完全性などの課題も生じる。

このようなアクセス制御のぜい弱性や不完全性により、クラウド事業者及びそのサービスの信用に大きな悪影響を及ぼすおそれがある。しかし、クラウド事業者は、その高いリスクを認識していないことも多い。このリスクに対処するため、アクセス制御サービスの提供機構の冗長化、ソフトウェアの高信頼化と試験の徹底、操作ミスの防止、運用手順書の質の向上など、幅広い対策を考慮することが求められる。

９.１.１　アクセス制御方針

クラウドサービスにおいては、供給者によるクラウド利用者のアクセス制御に依拠してサービスを提供し、あるいはクラウド事業者の行うアクセス制御に基づいて供給者がサービス提供を行うことがある。その際に、クラウド事業者と供給者の間でアクセス制御に関する業務方針が共有されていないことにより、クラウド事業者及びそれぞれの供給者において本来依拠すべきアクセス制御の方針が順守できないおそれがある。これに伴い、供給者による認可されていないアクセスの可能性や供給者内従業員の特権の悪用などの不正、及び特権の勝手な拡大によるアクセス制御/認証/権限付与等への影響を排除できない等の影響が生じる。

９.１.２　ネットワーク及びネットワークサービスへのアクセス

クラウドサービスでは、クラウド利用者が、クラウド事業者の情報セキュリティの管理外からアクセスすることが一般的である。このため、アクセス制御の対象となるクラウドサービスに供するネットワーク、ネットワークサービス等が適切にコントロールされていない場合には、第三者による不正アクセスをもたらすおそれがある。

また、クラウド利用者が、許可されていない情報資産等へのアクセスを行うことにより、クラウドサービス上のクラウド利用者情報の盗聴、改ざん、システムの破壊のほか、利用が許諾されていないサービスへのアクセス等の不適切な利用などの事態を招くおそれがある。

さらに、外部ネットワークサービスの選択によってクラウドサービスが直面しうる脅威と責任の所在について、情報提供により、クラウド利用者が正しい認識を得られるようにすることが求められる。

９.２　利用者アクセスの管理

クラウドサービスではクラウド事業者、クラウド利用者、第三者等による認可されていないアクセスによって、システム及びサービスが侵害され、クラウドサービスに供する情報資産の機密性と完全性を危険にさらす事態を招くおそれがある。このような事態を避けるため、秘密認証情報の割当を正式なプロセスによって管理運用することが求められる。

９.２.３　特権的アクセス権の管理

供給者のクラウドサービスを利用してクラウドサービスの提供を行うクラウド事業者に所属する特権ユーザは、特権的アクセス権を付与されて供給者が提供している特権的なユーティリティプログラムを使用することができる場合がある。この特権的アクセス権が第三者に詐称されると、供給者が提供している特権的ユーティリティプログラムが悪用され、Annex５ 9.4.4 で述べるように、第三者が、供給者が提供するクラウドサービスに不正アクセスするための踏み台とされるおそれがある。この課題を解決するため、特権的アクセス権の保護には、一般のエンドユーザ（個人）とは異なる格別の対策が求められる。

９.２.４　利用者の秘密認証情報の管理

クラウドサービスは一般に規模の大きな共有サービスとなるため、ぜい弱な秘密認証情報の割当てによってアクセス制御が破られた場合の影響が大きくなるおそれがある。特に、特権的なユーティリティプログラムの秘密認証情報が漏えいした場合の影響は深刻である。このため、秘密認証情報の割当てに係る管理を厳しくし、アクセス制御を確実にすることが求められる。

９.４　システム及びアプリケーションのアクセス制御

クラウドサービスは、オープンなネットワーク及びネットワークサービスを用いてサービスが提供されることも多く、クラウド事業者、クラウド利用者以外の第三者による不正なアクセスや攻撃が生じやすい。したがって、システム及びアプリケーションに対するアクセス制御のための措置を十分講じていないと、クラウドサービスに供するシステム、アプリケーション、データ等の情報資産に対する改ざん、破壊、情報漏えい等が生じるおそれがある。

加えて、クラウドサービスでは、クラウド事業者と供給者によるサービス連携が行われる場合があること、サービスに供する資源を複数のクラウド利用者が利用することなどから、アクセス制御に係るぜい弱性などにより、クラウド事業者、クラウド利用者及び供給者による不正アクセス等の事態も生じうる。また、不完全なアクセス制御などに伴う、サービス提供の不完全性などを生じるおそれもある。

これらの課題に対応するため、システム及びアプリケーションへのアクセスを、認可されている者に限定するための措置を講じるほか、逆に認可しているアクセスについては、完全に機能できるような対応を図ることが求められる。

９.４.１　情報へのアクセス制限

クラウドサービスではクラウド利用者が、クラウド事業者の情報セキュリティの管理外からアクセスすることが一般的である。このため、アクセス制御の対象となるクラウドサービスに供する情報及びアプリケーション機能等が適切に管理されていない場合には、第三者による不正アクセスをもたらすおそれがある。

また、クラウド利用者が、許可されていない情報資産等へのアクセスを行うことにより、クラウドサービス上のクラウド利用者から預託された情報の盗聴、改ざん、システムの破壊のほか、利用が許諾されていないサービス機能へのアクセス等の不適切な利用などの事態を招くおそれも生じる。

また、クラウド利用者側の環境（利用する Web ブラウザ、OS、その他のアプリケーション、デバイス等）におけるぜい弱性により、クラウドサービスへの重大な影響が生じるおそれがあるため、これに対応する措置を講じる必要がある。

９.４.４　特権的なユーティリティプログラムの使用

クラウドサービスでは、クラウドサービスの提供を目的とするクラウド利用者に対して、サービス提供に必要な範囲で特権的ユーティリティプログラムを利用できるようにする場合がある。この場合に、特権的ユーティリティプログラムに関するアクセス制御が適切に実施されない等のぜい弱性がある場合には、第三者あるいはクラウド利用者による、クラウド事業者又は供給者が提供するサービスに対する不正アクセス等が生じるおそれがある。

また、エンドユーザ（組織）の管理者に対して、クラウドサービス利用の管理に関する特権的なユーティリティプログラムを利用できるようにするケースがあるが、この場合も、特権的ユーティリティプログラムに関するアクセス制御が適切に実施されない、あるいは情報セキュリティマネジメントに関するぜい弱性がある場合には、クラウド利用者による他のクラウド利用者の情報資産への不正アクセス等の可能性が生じる。その結果、組織の評判、顧客の信頼および従業員の経験等にも間接的な影響がもたらされる。このため、エンドユーザ（組織）の管理者による、特権的な機能を有するユーティリティプログラムの使用にかかる権限管理を徹底することが求められる。

９.５　仮想化されたクラウドサービスのアクセス制御

仮想化されたクラウドサービスにおいては、ソフトウェアによる分離機能のぜい弱性によって、クラウド利用者からの預託情報やクラウドサービス提供のために用いられるクラウド事業者の情報処理施設等に対する不正アクセスが生じることがある。これに対する管理策が求められる。

９.５.１　仮想化資源の分離の確実な実施

仮想化された資源を用いてクラウドサービスを提供する場合は、クラウド利用者のニーズに合わせて個別に仮想化マシンを構成することで、マルチテナント型のクラウドサービスを提供している。この場合、仮想化マシンの分離は物理的な分離ではなく、ソフトウェアにより実現されているため、ソフトウェアの分離機能にぜい弱性が生じると、マルチテナント環境において、クラウド利用者が、他のクラウド利用者やクラウドサービス提供に係る情報やシステムに対して不正アクセスし、情報、システム等の改ざん、破壊、盗聴、漏えい等を行うおそれがある。このため、仮想化マシンの分離を適切に実施し、アクセス制御を確実にするための措置を講じる必要がある。

１０ 暗号

１０.１　暗号による管理策

クラウドサービスは、オープンなネットワーク及びネットワークサービスを用いてサービスが提供されることが多いことから、暗号は、情報セキュリティマネジメント上非常に重要な役割を担っている。クラウドサービスにおける暗号の適用範囲、暗号化の強度、暗号鍵管理の確実性はサービスレベルに依存することから、クラウド利用者が、自らが求める要求レベルを確保したクラウドサービスを確実に選択できる環境整備が求められる。

１０.１.１暗号による管理策の利用方針

クラウドサービス提供において、暗号は、保管又は伝送される情報の機密性確保/完全性・真正性の検証、アクセス制御における認証、否認防止等に役立てられるため、情報セキュリティマネジメント上非常に重要な役割を担っている。

しかし、これらに係るサービスレベルはクラウド事業者により異なることから、クラウド利用者が、自らが求める要求レベルに達しないクラウドサービスを誤って選択すると、クラウド利用者から預託された情報が容認できないリスクにさらされるおそれがある。これを防止するための管理策が求められる。

１０.１.２鍵管理

クラウド事業者が管理する暗号鍵の不正利用は、クラウドサービスの機密性・完全性を損なう。また、クラウド事業者が管理する暗号鍵の喪失は、クラウド利用者の暗号化されたデータの完全性を損なう。このため、暗号鍵の保護と管理（暗号鍵を実際に用いる段階での管理を含む）を確実にすることが求められる。

１２ 運用のセキュリティ

１２.１　運用の手順及び責任

クラウド利用者とクラウド事業者の間で締結した SLA 等に基づくクラウドサービスの提供は、サービス設計、構築、運用に至る過程で処理等の不整合が発生した場合、責任不履行といった事態を招くおそれがある。このような事態を回避するためにも、提供するクラウドサービスの SLA 等に係る適切な利用ができるように、運用管理情報やクラウド利用者が必要とする運用操作に関する情報を提供することが望ましい。

１２.１.１　操作手順書

クラウド利用者の不適切な操作等に起因して、クラウドサービスの機密性・完全性・可用性が守れなくなることがある。この課題の克服のために、クラウド利用者がそのエンドユーザ（個人）のために作成する操作手順書の活用が効果的である。そこで、クラウド利用者が操作手順書を作成するにあたり基になる情報を提供することが求められる。

１２.１.２　変更管理

クラウドサービスは、ネットワークを通じてサービス提供を行うため、第三者等からサービスに供するシステムに対する攻撃がなされる脅威があり、これによって悪意のあるプログラムの改ざん、変更、破壊等がなされるおそれがある。また、クラウドサービスにおいては、クラウド利用者が多数に及ぶことがあるため、過失等により誤ったプログラムの適用や削除、破壊等が生じることで、クラウドサービスの提供に影響を及ぼす。これによって、多数のクラウド利用者に影響するサービス停止やサービスレベル低下をきたす可能性が生じ、その影響によってサービスや企業の信頼が低下するおそれがある。このため、クラウド事業者は定期的に変更管理の状況を確認するとともに、変更管理に関する手順等を文書化し、適切な変更管理を行うとともに、意図しない変更が行われた場合に、速やかに元の構成に戻せる措置を講じることが求められる。

１２.１.３　容量・能力の管理

クラウドサービスは、ネットワークを通じてサービス提供を行うため、第三者等からサービスに対する攻撃を受ける脅威があり、これによって不測の資源不足が発生し、これに伴うサービスの停止、低下が生じるおそれがある。また、クラウド利用者による悪意のあるサービス利用や、一部のクラウド利用者による不正な資源の占有などにより、これに伴うサービスの停止、サービスレベル低下が生じるおそれがある。

さらに、クラウドサービスはオンデマンドサービスとしての性格を持つため、クラウドサービスの提供に必要な資源は統計的な予測に従って割り当られていることが多い。そのため、予測の範囲を超えたクラウド利用者のニーズの集中が発生すると、資源が枯渇し、クラウドサービスの提供に支障を

来すおそれが生じる。具体的には、資源の設定・割り当てに際して、不正確なモデリング又はクラウドのインフラ基盤に対する不十分な投資の下で行われることで、クラウド事業者において、以下の事態を招く可能性がある。

(a) 特定の資源を集中的に使用するアプリケーションが存在する場合に、その資源使用の予測に必要な仕組みを構築しないことに伴い、特定の資源の枯渇が予測できなかった場合には、アプリケーションの起動が停止し、または著しく動作が低下するなどにより、サービスの停止、クラウド利用者が預託するデータの滅失などが生じる。

(b) システムに必要な資源の枯渇により、システムの停止等が生じ、その結果として例えば IPS のフィルタリング機能が動作しないままで運用されてしまう等のぜい弱性が生じ、アクセス制御が侵害される。

(c) クラウド利用者のサービス利用に関する要求や求められるサービスレベルの達成に対応することができず、クラウド事業者において、経済的損失、評判の低下等が生じる。

(d) 資源のニーズに関する不正確な予測によって、サービス提供に際して、インフラ資源の過剰な拡張が生じ、これに伴う費用の拡大等により収益性の悪化が生じる。

このため、全てのクラウドサービス提供に供する資源に求められる容量・能力の監視・調整を行うとともに、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(f)(g)から手法を選択し、クラウド利用者に現状に関する情報を適切に提供する必要がある。

１２.２ マルウェアからの保護

クラウドサービスの特性上、クラウド事業者がサービスに供するシステムにマルウェアが感染した場合には、サービスに供するシステムの改ざん、破壊等による、システムの停止、管理しているクラウド利用者の預託データ等の漏えい等の発生、クラウド利用者が利用するシステム等への感染といった深刻な事態を招くおそれがある。

また、あるクラウド利用者が利用するシステム等へのマルウェア感染によって、提供しているクラウドサービスが影響を受け、あるいはクラウド事業者のシステムに感染するなどにより、上述のような事態が生じることもありうる。

このため、マルウェア対策を行うとともに、クラウド事業者のどの情報処理施設が感染したかを、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(f)(h)から手法を選択して、クラウド利用者に情報提供することが求められる。

１２.２.１ マルウェアに対する管理策

クラウドサービスは、オープンなネットワーク及びネットワークサービスを用いてサービスが提供されることが多いため、第三者による攻撃のほか、クラウド利用者を経由して、クラウド事業者がサービス提供に供するシステムに感染する可能性がある。このため、マルウェアに対する管理策をクラウド事業者において行うとともに、クラウド利用者に対してもマルウェア対策などを呼びかけ、対応を促す必要がある。

また、マルウェアに感染した場合は、再発防止策を実施するとともに、クラウド事業者のどの情報処理施設が感染したかを、クラウド利用者に迅速に情報提供する仕組みを構築することが求められる。

１２.３ バックアップ

クラウドサービスでは、一部のクラウド利用者の預託データについて、証拠提出の要請や、司法官憲等による提出命令などが生じた場合に、当該クラウド利用者に関するデータだけではなく、他のクラウド利用者の預託データまでもが一緒に提出されてしまうおそれがある。ハードディスクが提出された場合だけでなく、クラウド事業者が取得したバックアップが提出された場合も同等のことが生じうる。これによって、多くのクラウド利用者の預託データが提出先の管理下に置かれる等の事態を生じ、結果としてクラウド事業者やクラウドサービスの信用低下などに繋がりかねない。したがって、これを防止する措置を講じることが求められる。

１２.３.１ 情報のバックアップ

クラウドサービスでは、マルチテナントサービスとしての特性から、複数のクラウド利用者の預託データを一括してバックアップを取得することが多い。このため、一部のクラウド利用者が預託したデータについて、証拠提出の要請や、司法官憲等による提出命令などが生じた場合に、当該クラウド利用者に関する預託データだけではなく、クラウドサービス提供に不可欠な設定などに関するデータや、他の多くのクラウド利用者の預託データも含んだバックアップが提出の対象となってしまう可能性がある。この場合、サービス障害時の備えが不十分となり、サービスレベルを保証したクラウドサービスの提供が阻害されるおそれがあるため、これを防止する措置を講じる必要がある。

１２.４ ログ取得及び監視

クラウドサービスの特徴として、ネットワークを活用すること、クラウド事業者、供給者及び多数のクラウド利用者がクラウドサービス提供に係る資源にアクセスすることなどが挙げられる。このため、外部及び内部からの攻撃等の脅威にさらされやすくなるため、ログを取得して監視を行うことで、分析等に基づく予防的対策や、情報セキュリティインシデントの事後のトレース等に役立てることができる。

クラウドサービスにおけるログの取得に関しては、二つの重要な課題が存在している。

一つは、供給者が規定しているログ取得・管理に対するポリシーや取得範囲等がクラウド事業者の要求を満足していない、又はこれらの規定が不明確・曖昧になっている場合は、その供給者が必要なイベント等のログを取得しない、あるいは取得したログを保持しないといった課題が生じうることである。

もう一つは、マルチテナントサービスとしての性質上、多数のクラウド利用者に係るログを、ひとまとめにして取得している場合の課題である。この場合、一部のクラウド利用者の行為に関して、第三者から法令等に基づくログ提出を求められる、あるいは司法官憲等からのログの提出命令等があった場合に、他の多数のクラウド利用者のログまでもが一括して提出されてしまうおそれがある。その結果として、他のクラウド利用者のログが提出先の管理下に置かれることになり、クラウド事業者やクラウドサービスの信用低下などに繋がる場合がある。

１２.４.１ イベントログ取得

クラウドサービスでは、多数のクラウド利用者がサービス提供に供する同一の資源を利用するため、一部のクラウド利用者の不正行為や、不適切なサービス利用により、他のクラウド利用者に対するサービス提供が損なわれ、サービスレベル低下や事業者の信用低下などに至るおそれがある。また、特権ユーザによる悪意の行為や外部からの攻撃などによっても、情報の漏えい等が発生する可能性がある。

これらへの対応措置の一つとして、脅威となるイベント等に対するログ取得が挙げられる。しかし、供給者が規定しているログ取得・管理ポリシーやログ取得範囲等がクラウド事業者の要求を満足していない、または、これらの規定が不明確・曖昧になっている場合は、その供給者が必要なイベント等のログを取得しない、あるいは取得したログを保持しないといった課題が生じうる。そこで、供給者の選定にあたっては、供給者が取得するログの範囲、内容、粒度等が、クラウド事業者が要求する管理水準を満足できることを事前に確認しておくことが望ましい。ただし、データ連携等を行うために、個別の仕組みを新たに構築して対応する場合は、ログ取得・管理ポリシーやログ取得範囲等について、供給者との間で合意することが求められる。

一方、アグリゲーションサービス事業者においては、アグリゲーションサービス全体について、統一したポリシーでログ取得等を行うことが求められる。

１２.４.２ ログ情報の保護

ログ機能及びログ情報の保護に関する管理策が行われていないと、必要なログの記録の削除や、改ざん、設定の変更などによって、クラウド利用者や特権ユーザによる不正なサービス資源の利用等や、外部からの攻撃の監視が不十分になるおそれがある。また、アグリゲーションサービスを提供する場合は、供給者との間で、ログ情報の保護に関する方針や対応策について、統一したポ

リシーが適用されていない場合には、アグリゲーションサービス全体として講ずべき情報セキュリティマネジメントに必要なログの保護がなされないおそれが生じる。

１２.４.３ 実務管理者及び運用担当者の作業ログ

クラウドサービスでは、クラウド事業者と供給者によるサービスを連携して提供することがあるが、クラウド事業者は連携関係にある供給者のクラウドサービスの利用者として、当該サービスが有する管理機能等により特権利用を行うことがある。管理機能に対して適切な権限設定やログ機能に対する保護措置が取られていない場合には、管理機能を悪用する危険性がある。

また、クラウド利用者（エンドユーザ（組織）、供給者のクラウドサービスを利用するクラウド事業者）の特権利用状況を全体的に把握するためには、クラウド事業者及び全ての供給者において取得するログを突合する必要等が生じるが、クラウド事業者が、供給者が取得するログで対象とするイベントの範囲や、イベントにおける詳細事項について確認し、同意していない場合には、ログの分析に必要な情報が記録されないおそれがある。

１２.５ 運用ソフトウェアの管理

クラウド利用者がクラウド上にインストールしたソフトウェアが悪意を持った動作をすることで、クラウドサービスの継続や信用に影響を及ぼすおそれがある。このため、これに対する管理策が求められる。

１２.５.１ 運用システムに関わるソフトウェアの導入

クラウド利用者がクラウドサービスに供する資源上にインストールしたソフトウェアが悪意を持った動作をすることで、当該クラウドサービス資源上にぜい弱性が生じ、DDoS 攻撃の踏み台となったり、情報漏えいが生じたり、サービスの利用が困難になるおそれがある。また、これらに伴い、司法官憲等による犯罪証拠の提出命令を受ける可能性も生じる。

このため、クラウド利用者がクラウドサービス上にインストールするソフトウェアについて、マルウェアに感染していないことを事前に確認すること、アップロードや変更の証跡を記録しその記録を保存・保護すること、不正な挙動を示した場合はその原因となったソフトウェアを特定できる措置を講じること等が求められる。

１２.６　技術的ぜい弱性管理

技術的ぜい弱性の悪用により、クラウドサービスの継続に影響を被ることに留まらず、クラウド利用者の事業・権利保護・コンプライアンス確保に支障をきたすことがありうる。この場合、クラウド事業者のサービス・組織・経営等に対する、クラウド利用者からの信頼を失うおそれがある。このため、技術的ぜい弱性の悪用防止には、重点を置いて取り組むことが求められる。

１２.６.１　技術的ぜい弱性の管理

技術的ぜい弱性が、攻撃者による攻撃、クラウド利用者の不正、クラウド事業者の内部不正等で悪用された場合、クラウド利用者の預託データの機密性・完全性が失われたり、DDoS 攻撃・インシデント対応・司法官憲等による犯罪証拠の提出命令等によって長時間サービスが停止して可用性が失われたり、他のクラウド利用者の不正行為によって利用しているクラウドサービスの IP アドレスが外部サービスによりブロックされたりといった事態が発生するおそれがある。このため、技術的ぜい弱性の悪用を防止する管理策を実施することが求められる。

１２.７ 情報システムの監査に対する考慮事項

運用システムの点検を伴う監査要求事項及び活動は、クラウドサービスの運用業務プロセスの中断を招くおそれがある。このため、監査要求事項及び活動がクラウドサービスのサービスレベル低下に繋がらないための措置を講じることが求められる。

１２.７.１ 情報システムの監査に対する管理策

運用システムの点検を伴う監査要求事項及び活動が、クラウドサービスの運用業務プロセスの中断を招くことがないように、監査に必要な点検活動を最小限に留め、運用業務プロセスの中断リスクを最小化する措置を講じることが求められる。

１３ 通信のセキュリティ

１３.１ ネットワークセキュリティ管理

ネットワークの設計ミスや設定ミスは、クラウドサービスの提供に広範囲な影響を及ぼしやすく、クラウドサービスの全面停止や可用性喪失を生じやすい。その結果、多数のクラウド利用者に影響を及ぼし、クラウド事業者及び提供するサービスに対する著しい信頼低下をきたすおそれがある。このため、クラウドサービスの提供にあたっては、ネットワークの設計・設定ミスの防止について、特に慎重な管理を行うことが求められる。

１３.１.４ 仮想ネットワークにおいて重視すべきぜい弱性

仮想ネットワークを構築してクラウドサービスを提供する場合、仮想ネットワークの構成や設定が複雑で、物理ネットワークの構成や設定と一貫していない場合には、運用管理に係る経験やノウハウが共通化されず、仮想ネットワークの管理ミスを生じやすくなる。また、IaaS/PaaS を提供している場合は、クラウド利用者がオンプレミスからクラウドサービスに移行するタイミングを狙い撃ちして悪意の攻撃を行い、これによって潜在した脅威を、クラウドサービスの新しい仮想ネットワーク上に持ち込ませることが増えており、注意を要する。

１３.２ 情報の転送

クラウドサービス提供においては、情報転送は不可欠であり、安全な情報転送が確保されないと、クラウドサービスの提供自体の安全性が損なわれることになる。

具体的には、情報転送に必要な資源の割当がなされないと、サービス低下を招く可能性があるほか、クラウド事業者による供給者のサービス利用において、所定の情報転送がなされないと、サービスの完全性を損なうことにつながる。また、内外の情報転送において、必要な安全措置が講じられていないと、盗聴等の情報漏えいが生じる等の可能性が生じる。

１３.２.２ 情報転送に関する合意

ICT サプライチェーンにおいて、データ連携に係る標準的な規格や仕様等に係る合意ができないことにより、クラウド事業者と供給者間の情報転送において遅延や欠損等が生じ、クラウドサービス提供の完全性を損なうおそれがある。

また、提供するクラウドサービス内、あるいは外部とのデータ連携において、必要な暗号化や資源の隔離等がなされていない、あるいはクラウド利用者のユーザ ID 窃取に対する必要な措置が施されていない場合には、盗聴等による情報漏えい等が生じるおそれがある。

さらに、クラウドサービスの利用終了時に預託された情報の返却を行うにあたり、クラウド利用者からデータ規格、仕様等に係る同意を事前に得ていない場合には、クラウド利用者に対して適正な形で預託情報を返却できず、クラウド利用者からの信頼喪失などを招くおそれがある。

これらの三つの課題に対応する管理策の実施が求められる。

１３.２.４ 秘密保持契約又は守秘義務契約

クラウドサービスは複数国の資源やサービスを利用してサービス提供を行うことがあるため、これらの資源やサービスを提供する他国の供給者に対して、サービス運用・技術等に係る情報を提供する場合には、秘密保持契約や守秘義務契約を締結する。しかし、知的財産に関する法制度の違いから秘密が保持されない、あるいは適用法や裁判管轄の違いから各種契約に基づく強制力が及ばない等の事態が生じうる。

１５ 供給者関係

１５.１ 供給者関係における情報セキュリティ

クラウドサービスの一つの特徴として、クラウド事業者と供給者が ICT サプライチェーンを構成してサービスを提供するケースが多いことが挙げられる。これにより、クラウド事業者及び供給者は効率的に自らの資源を活用するための「選択と集中」が実施しやすくなり、エンドユーザ（組織）においても、様々なサービスの比較を行いながら、柔軟な形でクラウドサービスを選択することができるようになる。

他方、クラウド事業者と供給者の間でサービス連携がうまくいかず、結果としてエンドユーザ（組織）へのサービス提供に支障をきたすおそれがある。例えば、クラウド事業者と供給者の間の情報セキュリティマネジメントに対するポリシーの違いに起因したぜい弱性の発生や、障害時における対応等に係る管理責任等の範囲についての認識の齟齬などに伴う対応の遅延等を挙げることができる。このように、クラウド事業者と供給者の間でのポリシーの違い等から生じる実装面、運用面のリスクへの管理策が必要となる。

１５.１.１ 供給者関係のための情報セキュリティの方針

クラウドサービスの提供を、クラウド事業者と供給者が ICT サプライチェーンを構成して行う場合に、提供するサービスおよびこれに関連する対応範囲をクラウド事業者と供給者の間で明確にする必要がある。クラウド事業者と供給者の間で対応範囲の認識に不一致があると、ガバナンスの喪失が生じ、これに伴う情報セキュリティ対応に未実施、あるいは不完全な部分が生じる。このため、クラウド利用者において不測の情報漏えいや障害等が発生し、あるいはアグリゲーションサービスにおいて、予期しないシステムの機密性、完全性、可用性の喪失が生じるおそれがある。

また、クラウド事業者による供給者の選定において、依拠するガバナンスに対する確認が行われない場合には、クラウドサービス全体として均一なガバナンスが確保されないことになり、これに伴う提供サービスの制限、不完全等が生じうるほか、不測のセキュリティホールや情報漏えい等の可能性が高まる。

クラウドサービスを連携して提供する場合に、いずれかのサービスの障害等に伴い、エンドユーザ（組織）が利用するサービス全体の完全性が損なわれる、あるいは連携する他のサービスでも障害が誘発されるケースがある。この場合、供給者が規定する障害に対する対応方針が、クラウド事業者の要求を満足していることを確認していない場合には、障害発生後の対応が円滑に行われないことにより、障害の影響範囲が拡大するおそれが高まる。

供給者が規定するクラウドサービスに係る管理方針等が、クラウド事業者の要求を満足していることを確認していない場合には[29]、クラウド事業者と供給者における管理責任や管理権限の範

[29] データ連携等を行うにあたり、個別の仕組みを新たに構築して対応する場合は、特定の供給者との間で、管理方針に係る内容調整や合意が求められる。

囲が、本来の管理対象と整合しない事態が生じうる。そのため、例えば管理用インターフェイスの悪用や、管理機能の欠如などの事象が発生しうる。

供給者が規定するクラウドサービス提供に関わる従事者に対するガバナンス等の方針が、クラウド事業者の要求を満足していることを確認していない場合には、サービス提供に係るモラルの均一化が図れないほか、従業者の業務対応の管理が不十分であることに伴う不正の発生等が生じる可能性が高まり、これがクラウド事業者及び他の供給者に対する不測のサービス提供上のリスクを生じさせる。

また、クラウドサービスの提供に関して、一連のサービス提供状況、アクセス管理状況等の証跡については、クラウド事業者及び供給者が自らのシステムに関するものは記録、管理しているものの、記録対象となる情報内容や取得方法が異なる可能性がある。さらに、接続しているサービス間での証跡に係る方針等を利用規約、SLA 等で規定して同意していない場合には[30]、クラウド事業者及び全ての供給者において証跡が記録されない可能性がある。

１５.１.３ ICT サプライチェーン

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、一部の供給者が提供するサービスにおいて情報セキュリティ要求事項が満たされないことにより、ICT サプライチェーン全体のサービス継続性が損なわれ、あるいは不測のセキュリティホールが生じる等のリスクがある。

[30] サービス間の接続を、個別の仕組みを新たに構築して実現する場合は、特定の供給者との間で、証跡に係る方針等について個別の取決めを行うことが求められる。

１５.２　供給者のサービス提供の管理

ICT サプライチェーンにおいては、Annex６の 15.1.3 により合意又は明確になった情報セキュリティマネジメントの要求事項が一部の供給者により管理されないことで、クラウドサービス全体の提供品質や情報セキュリティに影響を及ぼすおそれがある。

１５.２.１　供給者のサービス提供の監視及びレビュー

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、クラウド事業者が提供するサービスの提供状況を監視するだけでは、クラウド事業者が定めるサービスレベルを達成できないことがある。例えば、供給者が提供するサービスにおいて情報セキュリティマネジメント上のぜい弱性がある場合に、連携しているクラウド事業者のサービスへの影響が生じることも想定される。

特にアグリゲーションサービス事業者の場合には、供給者のサービス提供状況に起因する、クラウドサービス全体としてのサービスレベル低下に対する責任が生じるため、供給者全体のサービスに対する管理が求められる。

１５.２.２　供給者のサービス提供の変更に対する管理

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、一部の供給者が提供するサービスの変更が、他の供給者のサービスや、クラウド事業者が提供するサービス全体に影響を及ぼすおそれがある。これに伴い、不測の原因によって、クラウドサービス上の障害や情報漏えいを生じる可能性が生じる。

１６　情報セキュリティインシデント管理

１６.１　情報セキュリティインシデントの管理及びその改善

情報セキュリティインシデントに関し、特に留意すべき課題は以下に示すように数多く存在している。

(a) ICT サプライチェーンを構成するクラウド事業者と供給者間における不明確な管理責任等の範囲
(b) 仮想化に伴うネットワーク管理とサーバ管理の管理責任の範囲の不明確化（仮想スイッチ等）
(c) (a)(b)等に起因する情報セキュリティ事象の発見の遅れや対応切り分けの失敗
(d) 発見された情報セキュリティ事象の通報受付体制の不備による対応の起動の遅れ
(e) 深刻な情報セキュリティインシデントをそうでないと誤判断したことによる、対応やクラウドサービス利用者等への初報の遅れ
(f) 資源やインフラの集約による情報セキュリティインシデントの影響範囲の拡大
(g) (a)(b)等に起因する不十分な対応による情報セキュリティインシデントの影響範囲の拡大
(h) SLA を守れないことや、クラウド利用者が納得する状況報告ができないことによるクラウド事業者又はクラウドサービスに対する信用の失墜
(i) 監督官庁が定める業法、知的財産権や個人情報の保護等の法令を守れないことによるクラウド事業者又はクラウドサービスに対する信用の失墜
(j) クラウド利用者とクラウド事業者、クラウド事業者と供給者間のコミュニケーション不足による状況認識の食い違いや紛争の発生
(k) クラウド利用者に捜査が及んだ場合の司法官憲等による提出命令に際し、記録媒体や共有資源（RAM、ネットワーク等）のテナント分離の限界に伴って発生する情報漏えい
(l) 複数の司法権を跨がってデータ格納を行う場合の、海外の供給者に対して海外の司法官憲等が行う提出命令（特定のクラウド利用者の犯罪等によるもの）、クラウドサービス提供に供する記録媒体等の差押え（供給者の不正によるもの）等に伴うサービス停止の発生

情報セキュリティインシデントの兆候を早期に把握し、明確な管理責任や役割の範囲の分担に基づいて対応を的確に切り分け、深刻な情報セキュリティインシデントを判別して円滑に対応（クラウドサービス利用者等への初報を含む）を起動し、影響範囲を限定し、クラウド利用者と同意した SLA や報告義務を順守し、法令を順守し、供給者と状況認識を共有し、クラウド利用者の不正行為に対する証拠を情報漏えいを生じることなく収集し、司法権管轄の違いに対応する。こういった一連の情報セキュリティインシデント対応において、一貫性のある効果的な取組を行うことが求められる。

１６.１.２　情報セキュリティ事象の報告

仮想化によるネットワーク管理に対する管理責任等の内容や範囲の不明確化、クラウド事業者と供給者間における管理責任等の範囲に関する理解の齟齬等に起因して、情報セキュリティ

事象の発見や対応切り分けに支障が出やすい。この課題を克服するために、技術的対策の適用及びクラウド事業者と供給者間の管理責任等の分担範囲の明確化が求められる。

以上の環境整備を前提として、その上で、内部組織に限らず、クラウド利用者や供給者が先に情報セキュリティ事象を発見した場合であっても、情報セキュリティ事象の情報を早期にクラウド事業者に集約できる体制を構築することが求められる。

１６.１.４　情報セキュリティ事象の評価及び決定

発生した情報セキュリティ事象を、情報セキュリティインシデントに分類することで、対応を本格化させ、クラウド利用者への連絡も起動させる。したがって、判断ミスを抑え、対応や連絡の速やかな実施を確保するため、情報セキュリティインシデントの分類基準を確立することが求められる。

１６.１.７　証拠の収集

情報セキュリティインシデントの事後対応において、以下に示すような場合は、懲戒処置及び法的処置のための証拠収集・保全が必要になる。

(a) クラウド事業者自身の法順守を争う場合
(b) 内部組織や委託先の要員の不正を問う場合
(c) クラウド利用者の順法が問われ証拠がクラウドサービス上に存在する場合　等

このような場合には、以下に示す不都合な事象への対応が課題となる。

(a) 訴訟への発展を予見できず証拠を破壊してしまう事象
(b) 証拠の収集と保全に係る知識不足のため裁判で証拠として採用されない事象
(c) 共用された媒体・資源からの証拠の収集・保全プロセスにおける無関係な他のクラウド利用者の記録の破損や情報の漏えいの発生
(d) 複数の司法権を跨がってデータ格納を行う場合の、海外の司法官憲等による提出命令（特定のクラウド利用者の犯罪等によるもの）、クラウドサービス提供に供する記録媒体等の差押え（クラウド事業者の不正によるもの）　等

これらの不都合な事象に対応するため、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用することが求められる。クラウド利用者による、証拠として利用できる情報へのアクセス手順（要請・許諾・課金等）を確立することもこれに含まれる。

クラウド事業者自身の法順守を争う場合には、知的財産権や個人情報の保護等が論点となる場合が多いが、クラウド利用者の順法が問われ証拠がクラウドサービス上に存在する場合は、監督官庁が定める業法を始めとして、不正アクセス防止法、各種刑法等、多様な法制度が対象になる。

１７ 事業継続マネジメントにおける情報セキュリティの側面

１７.２　冗長性

多数のクラウド利用者がクラウドサービスを利用しているため、クラウドサービスの停止は大規模かつ広範囲に影響を及ぼす。このため、サービス停止の影響は、単に可用性の低下に伴う SLA 違反による利用料の返還に留まらず、当該サービスやその提供元であるクラウド事業者の社会的信頼を失墜させる事態に陥る可能性も存在している。このため、クラウドサービス提供のための情報処理施設の可用性確保は、最優先事項として取り組むことが求められる。

１７.２.１　情報処理施設の可用性

クラウドサービスに、仮想化機能やサービス機能以外に ID 管理サービス等の単一障害点が存在していると、その機能が停止することにより、サービス全体が停止してしまうおそれがある。このため、クラウドサービス提供のための情報処理施設の単一障害点を特定し、確実に冗長化を実施することが求められる。

１８ 順守

１８.１　法的及び契約上の要求事項の順守

クラウドサービスにおいては、越境サービスを行うことにより、サービス対象となる国が複数にわたるケースがあり、これに伴い複数の国による法規制が適用されることにより、サービス提供の完全性が損なわれ、あるいは不測の対応を求められるおそれがある。

また、他国の供給者が提供するサービスと連携してクラウドサービスを提供する場合には、契約に係る紛争に対する適用法が異なることで、クラウドサービス提供の継続が困難となるおそれがある。

１８.１.１　適用法令及び契約上の要求事項の特定

複数国のクラウド利用者に対してクラウドサービスを提供する場合には、それぞれの国における適用法や司法権の管轄などが異なるため、クラウド利用者においてクラウドサービスの利用が継続できないリスクが生じる。また、複数の国等に存在する資源を用いてクラウドサービスを提供する場合、適用法令の違いから、クラウド事業者が当該資源の存在する国の法令違反を疑われ、当該国の司法官憲等による記録媒体の差押え等によって、サービス提供ができない状態に陥るおそれがある。

さらに、ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、適用法令の違いから、海外の供給者が当該国の法令違反を疑われ、当該国の司法官憲等による記録媒体の差押え等を受けることによって、サービス提供の継続が困難になるおそれがある。

１８.１.２　知的財産権

複数国のクラウド利用者に対してクラウドサービスを提供する場合に、適用される知的財産法が異なることにより、クラウド利用者が不測の損害を被るおそれがある。具体的には、著作権法の適用の違いに伴う保護範囲の違いや、営業秘密等の取扱いの違い等に基づくリスクが存在する。

また、情報サービスの提供に供するライセンスを複数国の資源において利用している場合には、ライセンスの範囲やサポート等の契約内容に差異が生じるおそれがある。

１８.１.３　記録の保護

クラウドサービスにおいて、サービス提供に供する資源やサービスが海外にある場合には、我が国とは異なる法令が適用され、クラウド事業者や供給者が法令違反を問われて記録媒体の不測の差押えを受けることでクラウドサービスの提供が停止することや、クラウド利用者の一部が法令違反を問われて預託情報の提出命令を受けることで無関係なクラウド利用者の預託情報までが提出されたりすることが発生しうる。

１８.１.４　プライバシー及び個人を特定できる情報（PII）の保護

複数国のクラウド利用者に対してクラウドサービスを提供する場合や、複数国の資源やサービスを利用してクラウドサービスを提供する場合に、クラウドサービスに供される個人情報保護法制が国や地域によって異なることから生じるリスクが存在しており、これに対する管理策が求められる。

１８.１.５　暗号化機能に対する規制

提供するクラウドサービスにおいて、サービスに供される情報等に対して、情報セキュリティマネジメントの観点から暗号化措置を講じることがある。しかし、複数国のクラウド利用者に対してサービスを提供する場合や、複数国の資源やサービスを利用してサービスを提供する場合に、国によっては公的秩序等の観点から、暗号化通信等を禁止しているケースがあり、クラウドサービス提供における情報セキュリティマネジメント上の要求事項が満たされないおそれがある。他方、ある国において法令上の要請から暗号化措置が求められている場合は、これを達成できない事態に陥る可能性がある。

１８.２　情報セキュリティのレビュー

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、クラウド事業者が提供するサービス等に関する情報セキュリティマネジメントのレビューを実施するだけでは、目標とするサービスレベルを確保する方策としては不十分であり、ICT サプライチェーンを構成する供給者との関係でもレビューを実施することが求められる。

１８.２.１　情報セキュリティの独立したレビュー

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、クラウド事業者が提供するサービスが供給者の提供するサービス等に依存し、あるいは影響を受ける部分を有することがある。このため、クラウド事業者が提供するサービスの範囲のみについて独立したレビュー・監査等を行うだけでは、クラウドサービスを提供する上での管理として不十分となりうる。

また、アグリゲーションサービス事業者は、クラウドサービス全体に対する管理責任を有するが、供給者との間でレビュー・監査における方針に齟齬がある場合には、クラウドサービス全体として必要なレビュー・監査が行えないおそれがある。

１８.２.２　情報セキュリティのための方針群及び標準の順守

アグリゲーションサービス事業者は、サービス全体に対する管理責任を有するが、順守している情報セキュリティマネジメントのための方針群、標準類等が供給者との間で一貫しておらず、結果としてクラウドサービス全体として適切な順守が確保されないおそれがある。

１８.２.３　技術的順守のレビュー

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、提供するサービスが供給者の提供するサービス等に依存し、あるいは影響を受ける部分を有する場合には、供給者のサービス等に係る技術的な順守状況を監視することが求められるが、各供給者の機密であることを理由としてレビュー結果がクラウド事業者に提供されず、十分なレビュー等ができないおそれがある。

Annex 6 利用者接点と ICT サプライチェーンに着目した情報セキュリティ対策

クラウドサービスの提供に関わらない対策項目に対しては、ISO/IEC27002 との紐付けは行っていない。したがって、Annex 6 において、章、節番号は連続していない。

6　情報セキュリティのための組織

6.1　内部組織

6.1.1　情報セキュリティの役割及び責任

個々の情報資産の保護と特定の情報セキュリティプロセスの実施に対する責任を明確に規定し、その責任を個人に割当、責任の規定と割当について定めたことを文書化することが求められる（ISO/IEC27002:2013 6.1.1 実施の手引 a）b）c）参照）。クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) クラウド利用者の情報資産の保護と特定の情報セキュリティプロセスの実施に対する管理責任の範囲を明確に定義し、利用規約・SLA 等で明文化し、クラウド利用者の同意を得ること。PaaS の場合、提供されるサービスによって、クラウド利用者が自ら管理できる情報資産や情報セキュリティプロセスの範囲にかなり幅があるため、クラウド利用者との管理責任の分担や免責の範囲が不明確になりやすく、特に慎重に責任の範囲を定めること。なお、ICT サプライチェーンを構成してクラウドサービスを提供する場合は、供給者が規定した責任範囲を確認し、これに基づいて自らの管理責任の範囲を定義すること。

(b) クラウドサービスの提供に係るクラウド事業者の委託先管理の責任を明確に規定し、従業員に割当、文書化すること。

(c) (a)(b)の実施にあたり必要となるクラウド利用者とクラウド事業者の間及びクラウド事業者と委託先の間における情報セキュリティマネジメントの側面の調整及び管理に関する事項を、契約形態、統制、順守、情報提供の範囲、技術協力の範囲、緊急時対応の役割分担等に係る要求の観点から特定し、文書化すること。

(d) クラウド利用者と締結する SLA を保証するため、提供するサービスレベルの保証に関する供給者の責任範囲の規定に基づいて供給者を適切に選定し、この選定に従って ICT サプライチェーン全体のサービスレベルの保証に係る自らの責任範囲を定義し、文書化すること。ただし、供給者との間で、データ連携等を個別の仕組みを新たに構築して実現する場合は、分担する責任についての調整及び管理に関する事項についても、併せて文書化すること。

(e) クラウド利用者に対する説明責任の主体と詳細を明確に定めること。説明責任の遂行にあたっては、Web 等を用いた情報公開によるクラウド利用者への周知とクラウド利用者個別の情報開示の範囲を明確にし、クラウド事業者として個別対応が可能な範囲について、統制の観点からクラウド利用者に通知すること。

6.1.2 職務の分離

多数のクラウド利用者に影響を及ぼす事象（クラウド事業者での内部不正、システム誤動作・誤運用、管理用インターフェイスの悪用、DDoS/DoS 攻撃等）の発生に繋がるぜい弱性として、システム設計・構築やサービス運用・設定における人為的ミスを排除するため、クラウドサービスの提供にあたっては、実務上以下に特に注意を払うことが望ましい。

(a) サービス運用・設定の実務を行う者と認可を行う者の役割と責任を明確に分離すること。
(b) システム設計・構築を行う者と認可を行う者の役割と責任を明確に分離すること。
(c) ASP・SaaS の場合は、開発・保守の実務を行う者と運用を行う者の役割と責任を明確に分離すること。

6.2 モバイル機器及びテレワーキング

6.2.1 モバイル機器の方針

モバイル機器を業務用 ASP・SaaS で用いる場合、業務情報が危険にさらされないことを確実にするために、物理的な保護、ソフトウェアのインストール制限、OS 等のセキュリティホールへの対応、情報サービスへの接続制限、モバイル機器の事前登録、アクセス制御、暗号化、モバイル機器上のデータのバックアップ、マルウェアからの保護、遠隔操作による機器の無効化・データの消去又はロック等の情報セキュリティ対策を実施することが求められる（ISO/IEC27002:2013 6.2.1 実施の手引参照）。特に、業務用 ASP・SaaS がモバイル機器に適合した認証方法を用いたアクセス制御を確実にすることが重要である。

モバイル機器の中では、特に、近年急速に普及しているスマートフォン/タブレットに対する対策が難しくなっている。そこで以下では、業務用 ASP・SaaS においてスマートフォン/タブレットの利用が可能なサービスを提供することに焦点を絞り、実務上実施することが望ましい事項について示す。詳しくは、一般社団法人日本スマートフォンセキュリティ協会の「スマートフォンの業務クラウド利用における、端末からの業務データの情報漏洩を防ぐことを目的とした、企業のシステム管理者のための開発・運用管理ガイド スマートフォンの情報漏洩を考える」を参照されたい。

(a) クラウド利用者に対し、不正改造された、もしくは、マルウェアに感染したモバイル機器をクラウドサービスに接続させないように要求すること。
(b) クラウド利用者への運用上の要求事項も含めて、モバイル機器上で、スクリーンショット・スクリーンキャスト録画・クリップボード履歴保存・キーロガー等を実行させないための対策を講じること。
(c) クラウド利用者に配布する、モバイル機器用のクライアントアプリケーションには、キャッシュ保存機能を持たせないか、又は十分な強度の鍵長とロジックでキャッシュデータを暗号化する機能を持たせること。

(d) モバイル機器において、クラウド利用者に、一定強度以上のパスワード設定を義務付けること。また、業務用クラウドサービスへの接続時に一定強度以上のパスワードが設定されているかの有無をチェックすること。

(e) モバイル機器と業務用クラウドサービスの間の通信は十分な強度の暗号を用いて暗号化すること。

(f) クラウド利用者への運用上の要求事項も含めて、モバイル機器の業務データを他のシステムと同期させないための対策を講じること。

なお、モバイル機器上の暗号化されたデータの保護において、本人認証は非常に重要な役割を果たしている。堅牢なアルゴリズムと十分な鍵長によって暗号化されたデータであっても、本人認証が破られて「正規の利用者である」とシステムに誤認させることができれば、当該システムの制御下で暗号鍵を利用する権限を自動的に付与され、暗号化されたデータの平文を自由に見ることができる。クラウド事業者としても、本人認証に係る(d)の指針が、モバイル機器の暗号化対策において特に重要な意味を持つことを理解し、クラウド利用者の認識を高めるための措置を講じることが望ましい。

一方、モバイル機器からの業務用 ASP・SaaS 利用において、HTML5 等の先進的な Web 技術を用いる場合には、これらに特有のぜい弱性を持ち込まないための管理策を、Web サービスの開発段階から実施することが望ましい。具体的な管理策については、JPCERT/CC「HTML5 を利用した Web アプリケーションのセキュリティ問題に関する調査報告書」を参照されたい。

6.3 クラウド利用者とクラウド事業者の公平な取引を確保するための措置

6.3.1 クラウドサービスの情報セキュリティマネジメントに係る提供条件の明確化

Annex 6 6.1.1【情報セキュリティの役割及び責任】(a)(b)(c)(d)(e)参照。クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) 文書化されたクラウド事業者自身の責任範囲を、Annex 6 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(b)(f)(i)から手法を選択して、SLA 等によりクラウド利用者に明確に示すこと。

(b) クラウド利用者が自組織の求める統制を満たすにあたり、クラウド事業者が提供できる機能・サービスを、Annex 6 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(b)(f)(i)から手法を選択して、SLA 等によりクラウド利用者に明確に示すこと。

(c) (b)を実施するにあたり、クラウド利用者個別に対応可能な範囲をあらかじめ明文化しておき、この文書を用いた情報提供により、クラウド利用者の個別対応範囲がかなり限定されることを認識できるようにすること。

ICT サプライチェーンを構築してクラウドサービスを提供する場合、クラウド利用者は、アグリゲーションサービス事業者の利用規約又は複数の個別契約連携クラウド事業者の利用規約に同意することになる。複数の個別契約連携クラウド事業者の利用規約に同意する必要がある場合は、

情報セキュリティマネジメントに係る責任範囲の構造が複雑化し、その分担が不明確になりやすいため、個別契約連携クラウド事業者としても特別な注意を払う必要がある。

6.3.2　利用者接点とサプライチェーンにおける情報提供・共有

クラウドサービスの新規利用/乗り換え利用を目論むクラウド利用者への情報提供にあたっては、自組織のガバナンス規定を順守するために、クラウド利用者が、必要な統制機能及び能力を有しているクラウドサービス及びこれを提供するクラウド事業者を選定できることが求められる。この目的で提供される情報を以下に例示する。

- クラウドサービスが保証又は努力目標とするサービスレベル（SLA 文書の内容を公開する例も見られる）
  - 故障回復時刻、故障通知時刻
  - サービス提供時間、ヘルプデスク提供時間
  - サービス稼働率、平均応答時間
  - 情報セキュリティ対策・設備の措置、ログ記録、サービス継続のための措置、バックアップ、暗号化に対応できるサービスの範囲
- 取得した認証
- 監査済み言明書、言明に対する監査報告書（その他関連する監査報告書）

また、これらの情報をクラウド利用者に提供する手段を以下に例示する。

- Web による一般公開
- 利用者個別の要請に基づく情報開示

上述した提供手段によりクラウド利用者に情報提供を行うにあたっては、実務上以下を実施することが望ましい。

(a) クラウドサービスの比較 Web サイト（例：クラウドサービス情報開示認定サイト https://www.fmmc.or.jp/cloud-nintei/）を活用し、クラウドサービスに係る情報を一般公開することを検討すること。

(b) 提供しているクラウドサービスのサービスレベルの保証値又は努力目標を、Web 等による一般向けの情報公開システムにより、情報公開すること。また、取得した認証（情報セキュリティ対策実施に関するもの、内部統制監査に関するもの等）を一覧できる形式で情報公開すること。

(c) 監査済みの「情報セキュリティ対策の設計・実装・運用に係る言明書」がある場合は、(b)の一般向け情報公開システムを用いて情報公開すること[31] [32]。

クラウドサービス提供段階では、クラウド利用者に限定し、必要とする情報を提供する。この目的で提供される情報を以下に例示する。

- クラウド利用者のサービス利用状況
- クラウド利用者が預託された情報の取扱い状況
- 日常の連絡
- 緊急時の連絡・報告
- 現在の稼働状況
- サービス達成状況（障害発生履歴の情報公開を含む）
- クラウド利用者からの問合せ件数や内容
- 操作マニュアル・FAQ
- クラウド事業者のセキュリティ管理に係る内部統制保証報告書（IT 実 7 号、SOC2 等）
- クラウド事業者の内部統制保証報告書[33]（監保実 86 号、ISAE3402/SSAE16 等）
- クラウド利用者の要請に基づく個別開示情報

また、これらの情報をクラウド利用者に提供するための、クラウド利用者に限定した手段を以下に例示する。

- 管理ツールを利用した情報照会機能
- 利用者限定 Web による情報公開（ログイン認証付きの Web サイト）
- 電子メール・FAX
- 利用者個別の要請に基づく情報開示

[31] 特定非営利活動法人日本セキュリティ監査協会（JASA）では、クラウドセキュリティ推進協議会（JCISPA）において、クラウド情報セキュリティ監査制度の検討を進めており、その中で言明要件の検討も実施しているので、参考にされたい。

[32] クラウド利用者の要請により、クラウド事業者のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制確保状況を、合理的な水準で保証することを企図した「クラウド事業者のセキュリティ管理に係る内部統制保証報告書」（IT 実 7 号、SOC2 等）の情報開示を求められることが増えてきている。この場合は NDA を締結した上で情報開示することも選択肢となる。

[33] クラウド事業者が、クラウド利用者の財務報告に関連する業務サービスを提供する場合に限定される。

上述した提供手段によりクラウド利用者に情報提供を行うにあたっては、実務上以下を実施することが望ましい。

(d) クラウドサービスの情報セキュリティに関する窓口（ヘルプデスク等）を分かりやすく公開すること。

(e) クラウド利用者からの個別要求に基づき、NDA を締結して、個別の情報開示を行うにあたり、その窓口をできる限りワンストップ化すること。また、個別の情報開示におけるクラウド利用者のコンタクト窓口を特定し、管理すること。

(f) ログイン認証付き Web サイトでは、日常の都度の連絡（計画的サービス停止/定期保守、バージョンアップ、マニュアル類の最新版公開の案内など）、サービス達成状況（サービス稼働率、平均応答時間、サポートサービス応答率等）又は障害発生履歴、現在の稼働状況、利用者からの問合せ件数/内容などの情報公開を検討すること。

(g) 管理ツールでは、クラウド利用者のサービス利用状況（ログイン実績、利用時間、利用ログ提供等）、クラウド利用者から預託された情報の保守取扱い実績などの情報照会機能を検討すること。

(h) 電子メール・FAX では、緊急時の連絡・報告（クラウドサービス内で発生した情報セキュリティインシデントについての情報：障害発生/復旧時刻・障害経過の通知、障害内容・原因・対処等に係る事後報告等）の情報提供を検討すること。

(i) クラウド利用者からの個別要求に基づき、NDA を締結して、個別の情報開示（例：クラウド利用者が希望する種別のインシデント履歴、第三者機関による監査・ぜい弱性検査レポート、クラウド利用者から預託されたデータ・利用ログ記録等の保存場所等）を行う場合は、クラウド利用者にとっての知るメリットとクラウド事業者にとっての情報開示のデメリット（業務負荷の増大も含む）のトレードオフを検討すること。
代替案として、監査済み言明書の公開や、NDA を締結した上での「クラウド事業者のセキュリティ管理に係る内部統制保証報告書」（IT 実 7 号、SOC2 等）、「クラウド事業者の内部統制保証報告書[34]」（監保実 86 号、ISAE3402/SSAE16 等）など、対策の実施状況に関する言明や内部統制の有効性についての合理的な水準の保証を企図した報告書を、クラウド利用者に開示すること。

緊急時の連絡・報告の情報提供については、さらに実務上以下を実施することが望ましい。

(j) クラウド利用者に影響を及ぼす情報セキュリティインシデントの発生後、その情報を適切に設定された時間以内に、(h)の手法により、クラウド利用者に通知すること。その後も、適

[34] 情報セキュリティマネジメントの全般をカバーするものではないことを、クラウド利用者に伝えることが望ましい。

切な時間間隔で情報の通知を続け、クラウド利用者が受領した情報を追跡できるようにすること。

(k) クラウド利用者に一斉周知する情報は、Annex６ 16.1.4【情報セキュリティ事象の評価及び決定】(d)に従って提供すること。

(l) クラウド利用者によって発見された情報セキュリティインシデントの情報の受付窓口を設置し、利用者に分かりやすく示すこと。

(m) 正確な情報を相互に交換するため、緊急時の情報提供と情報受付に係る供給者の規定を確認し、これに基づいて情報セキュリティインシデントの情報を ICT サプライチェーンで共有するための連絡体制を構築すること。

(n) (m)で構築した連絡体制に基づき、ICT サプライチェーンを構成するクラウド事業者は、情報セキュリティインシデントの際のコンタクト窓口を設置すること。

(o) 個別契約連携クラウドサービスを提供する場合は、クラウド利用者の便益を考慮し、個別契約連携クラウド事業者間の情報共有を積極的に行うこと。

個別契約連携クラウドサービスを提供する場合は、クラウド利用者に対する情報提供は、各個別契約連携クラウド事業者が個別に行うことになるため、各々が提供する情報に不整合や質や早さの違いが生じ、結果としてクラウド利用者の不信を招くおそれがある。このため、個別契約連携クラウド事業者間の情報提供に係る役割分担（例：情報提供窓口の一本化等）を定め、クラウド利用者の同意を得ることが望ましい。

8　資産の管理

8.1 資産に対する責任

8.1.1　資産目録

クラウド利用者は、情報のライフサイクル（作成、処理、保管、送信、削除及び破棄を含む）に関連したクラウド利用者の情報を特定し、その重要度と業務上の価値を自ら判定し、資産目録として記録・維持（正確かつ最新に保つ）する（ISO/IEC 27002:2013 8.1.1 実施の手引 参照）。クラウド利用者のこの作業を支援するため、クラウド利用者から預託された情報について、実務上以下を実施することが望ましい。

(a) クラウド利用者から預託された情報と、クラウドサービスを運用するための内部情報を、別の資産として分類すること。

(b) 仮想化資源を用いてクラウドサービスを提供している場合は、仮想化資源をラベル付けすること。

(c) (a)(b)等に係るクラウドサービスの特性に基づき、管理水準が異なる預託情報をクラウド利用者が分類するために必要な情報を、Annex 6　6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(i)の手法に基づき、SLA に記載して同意した範囲内でクラウド利用者に提供すること。

8.1.2　資産の管理責任

クラウド利用者が作成し管理する目録の中の各々の預託情報が保存されるクラウド事業者の情報処理施設等（仮想化資源を含む）のそれぞれについて、個別に管理ポリシーと管理水準に関する情報を、Annex 6　6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(i)の手法に基づいてクラウド利用者に提供し、クラウド利用者が適切なサービスを選択できるように支援することが望ましい。

なお、クラウド利用者から個別に委託を受けた場合等を除いては、預託情報の内容を一切利用・開示しないことを管理ポリシーに明示することが望ましい。

8.1.5　クラウド利用者から預託された情報の返却

クラウド利用者がクラウドサービスの利用を終了するにあたり、預託されていた情報をクラウド利用者が取り扱うことができる書式で返却することに加え、有料であるかどうかも含めてその対応方針をクラウド利用者に情報提供し、クラウド利用者が自らのポリシーに沿う返却方法を提供できるクラウド事業者及びサービスを選定できるようにすることが求められる。

また、クラウドサービスの利用終了後に、クラウドサービスに供する情報処理施設等から預託された情報が漏洩しないように、情報を二度と取り出せないようにすることが求められる。

さらに、これらの実施方針がクラウド利用者に周知されることが求められる。

上記を実現するため、実務上以下を実施することが望ましい。

(a) 個々のクラウド利用者の預託情報を、特定して抽出するための措置を講じること。
(b) Annex 6　13.2.2【情報転送に関する合意】(e)の事前合意に基づき、預託された情報をクラウド利用者又はその指示によって他のクラウド事業者が取り扱うことができる形式で、クラウド利用者に返却すること。
(c) (b)の対応が有料である場合は、その旨をクラウド利用者に周知すること。
(d) クラウドサービスの利用終了後に、預託された情報を二度と取り出せないように消去又は破壊すること。
(e) (b)(d)を実現する方法について、クラウド事業者又はクラウドサービスを選定するにあたり参考にできるような形で、クラウド利用者（潜在利用者を含む）に情報提供すること。
(f) (e)について詳細な情報の開示を求められた場合には、Annex 6　6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(i)の手法に従って情報開示することを検討すること。

8.2 情報分類

8.2.1　情報の分類

クラウド利用者から預託された情報を、提供するクラウドサービスごとに分類し、その分類に応じた情報セキュリティマネジメントを実施するとともに、クラウド利用者からの求めがあった場合に、その分類ごとの情報セキュリティマネジメントの実施状況を情報開示しうる状況にしておくため、実務上以下を実施することが望ましい。

(a) 複数のクラウドサービスを提供している場合には、提供するサービスに応じてクラウド利用者からの預託情報の分類を行うこと。
(b) (a)の各分類に対し、対応しているクラウドサービスの種類に応じて、預託情報の価値、重要性等を定義すること。
(c) 各々のクラウドサービスの提供において、クラウド利用者からの預託情報を、(b)の定義を踏まえて管理すること。
(d) クラウドサービスの提供にあたり、仮想化された資源を利用している場合は、クラウド利用者からの預託情報を明確に分類できる措置を施すこと。

8.2.3 資産の取扱い

複数のクラウド利用者から預託を受け、返却が必要となる情報を誤って情報漏えいしないよう、それぞれのクラウド利用者から預託を受けた情報を明確に分離して管理できる措置を講じることが望ましい。具体的には、実務上以下を実施することが望ましい。

(a) クラウド利用者から預託を受けた情報については、それぞれを容易に分離できるような措置を講じること。
(b) 仮想化された資源を用いて預託を受けた情報を管理する場合には、各クラウド利用者から預託された情報を特定できるような措置を講じること。

9 アクセス制御

9.1 アクセス制御に対する業務上の要求事項

9.1.1 アクセス制御方針

クラウドサービス提供にかかるクラウド利用者のアクセス制御について、クラウド事業者と供給者の間で依存関係がある場合には、クラウド事業者と供給者の間でアクセス制御の方針に齟齬が生じて、アクセス制御に支障を来すおそれがある。その可能性を低減するため、導入しているアクセス制御に係る方針を事前に確認し、クラウド事業者が求める方針を満足できる供給者を適切に選定することが求められる。また、供給者が規定する、アクセス制御に関する技術的対応に係る役割と責任の範囲を事前に確認し、供給者を適切に選定することで、ICT サプライチェーンにおいて、アクセス制御に関し必要な技術的対応を確保することが望ましい。

具体的には、クラウドサービスの提供にあたり、実務上以下を実施することが望ましい。

(a) アクセス制御サービスを提供している情報処理施設等の冗長化を行うこと。
(b) ソフトウェア更新時の切り替え試験を徹底して行うこと。
(c) 運用上の設定を行う者とそれを認可する者を分離すること。
(d) 運用手順書のレビューを徹底し、その品質を向上させること。
(e) クラウド利用者が、提供されるクラウドサービスにおいて実施可能なアクセス制御機能を、判断し選択できるようにするため、クラウド利用者から個別に要請を受けた場合は、Annex 6 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(i)に従い、アクセス制御方針について以下の情報の提供を検討すること。
    - クラウド利用者に付与するアクセス制御権限及び内部統制が機能した権限付与プロセス
    - 導入している ID 管理のフレームワーク（シングル・サイン・オン等の ID 連携を組み込む能力があるか、等）
    - 認証の強度（認証対象とする要素及び数、各要素における技術的・運用的な措置による堅牢性等）

- シングル・サイン・オン等の ID 連携への対応状況

(f) シングル・サイン・オンや ID 連携を実施する場合は、管理責任と役割の範囲、技術的対応のための仕様、運用規約・手順等について供給者の規定を確認し、これに基づいて、ICT サプライチェーンにおける自らの管理責任と役割の範囲を定義するとともに、供給者との連携を実現できる仕様、運用規約、手順等を定めることで、必要な技術的対応を確保すること。ただし、連携するにあたり、供給者との間で特定個別の仕組みを新たに構築する場合は、役割や責任の分担、技術的対応のための取決め等についても個別に明確化し、文書化すること。

なお、個別契約連携クラウドサービスの形態でサービス提供している場合は、クラウド利用者が自らの管理責任の範囲を定義するにあたり、個別契約連携クラウド事業者が規定する管理責任の範囲を一つひとつ確認する必要がある。この確認プロセスは、通常のクラウド利用者対クラウド事業者の場合よりも複雑であるので、責任の所在に係るクラウド利用者の理解が不明確になる課題が生じうるため、特に注意を要する。

(g) クラウド利用者から個別に要請を受けた場合は、シングル・サイン・オンや ID 連携の実現と運用に係る技術情報等を、Annex 6　6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(i)に従って提供することを検討すること。

9.1.2　ネットワーク及びネットワークサービスへのアクセス

クラウド事業者がネットワーク及びネットワークサービスのアクセス制御を適正に実施しないことにより、上述のように二つの問題が生じる。一つめの問題は第三者による不正アクセスが生じ、クラウド利用者のデータの盗聴、情報漏えい、システムの改ざん、破壊等が生じうることである。二つめの問題は、クラウド利用者に対するアクセス制御が適切に行われないことにより、他のクラウド利用者のデータ等に対する不正なアクセス、システム等の改ざん、破壊等、また、許可されていないサービスへのアクセス等が生じうることである。さらに、クラウド利用者が本来利用できるサービスを適切に利用できないことなども想定される。

これらの問題に対処するため、クラウドサービスに供するネットワーク及びネットワークサービスに対して、第三者による不正アクセスを防止するとともに、クラウド利用者の適正な利用を確保するためのアクセス制御に係る措置を講じることが求められる。具体的には、実務上以下を実施することが望ましい。

(a) クラウドサービスの提供に供するネットワーク及びネットワークサービスについては、クラウド利用者を認証した後のみ内部的なネットワーク等にアクセスできる等の適正なアクセス制御の措置を講じること。

(b) クラウドサービスを利用できる対象者を限定している場合（例：国内からクラウドサービスを利用するクラウド利用者に限定）は、アクセス元サーバに対する認証を行う、または、

許可されたクラウド利用者以外からのアクセスを制限する等、第三者からの不要なアクセスを排除する措置を講じること。

(c) クラウドサービスの提供に供するネットワーク及びネットワークサービスで利用するネットワーク機器等におけるぜい弱性について定期的に確認するほか、ぜい弱性が露見した場合には速やかに対応できる措置を講じること。

(d) 供給者と連携してクラウドサービスを提供するために用いるネットワーク及びネットワークサービスについて、連携するクラウド事業者と供給者の間で必要なアクセス制御措置について確認し、これを実施すること。

(e) クラウド利用者による不正なネットワーク及びネットワークサービスの利用がないことを、アクセス制御の設定を確認すること、あるいはクラウド利用者の内部的なネットワーク等のアクセス状況を監視すること等を定期的に行うことにより確認すること。

9.2 利用者アクセスの管理

9.2.3 特権的アクセス権の管理

特権的アクセス権を保護するため、特権的アクセス権を有する特権ユーザに対し、多要素認証技術を適用した認証を行う等の強力な認証機能を提供することが望ましい。これと同時に、Annex 6 9.4.4【特権的なユーティリティプログラムの使用】(a)(b)(c)(d)(e)を確実に実施し、特権的なユーティリティプログラムの監視と保護を強化することが望ましい。

9.2.4 利用者の秘密認証情報の管理

クラウド利用者のユーザ（個人）が、クラウドサービスが要求する強度の秘密認証情報の割当てを実行できる仕組みを確実に提供することが求められる。

また、秘密認証情報に関する管理情報をクラウド利用者に提供することによって、クラウド利用者がクラウドサービスの提供機能の利用判断をしやすくするため、上記を実現するための手順や秘密認証情報の割当て手順に係る情報を、Annex 6 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(b)(f)(i)から手法を選択してクラウド利用者に情報提供することが望ましい。

シングル・サイン・オンや ID 連携を行う場合は、秘密認証情報をクラウド事業者と供給者の間で共有することから、当該情報の管理元からの情報漏えいは、クラウド事業者及び供給者に幅広く影響を及ぼす。このため、秘密認証情報の管理元は、当該情報の情報セキュリティに格別の注意を払うことが求められる。

なお、クラウド事業者が導入すべき正式な管理手続として参考となるものに、Payment Card Industry(PCI)データセキュリティ基準の要件 8 などがある。

９.４　システム及びアプリケーションのアクセス制御

９.４.１　情報へのアクセス制限

第三者からの不正アクセスを防止するため、情報及びアプリケーション機能に対して、第三者による不要なアクセスを防止する措置を講じる必要がある。また、クラウド利用者に対しても、適正な情報及びアプリケーション機能に対するアクセス制御のための措置を講じることが求められる。さらに、クラウド利用者に対するぜい弱性の周知、管理責任の範囲に係るクラウド利用者の同意などの措置も求められる。具体的には、実務上以下を実施することが望ましい。

(a) クラウドサービスの提供に係る情報及びアプリケーション機能へのアクセス制御について、自社が提供するシステム・プログラム等におけるぜい弱性を定期的に確認するほか、利用する OS、ミドルウェア等におけるぜい弱性に関する情報及び対応策を確認し、必要な措置を講じること。

(b) クラウドサービスの提供において供給者と連携する際に、その供給者が提供するアクセス制御に依存している場合は、供給者の選定にあたり同意したアクセス制御に係る方針に基づいて供給者が実施する措置を確認し、課題が存在する場合は具体的な対応策を要求して、これを実施させること。

(c) 不要なアクセス権限の設定、必要なアクセス権限設定の遺漏等が生じないように、クラウド利用者が利用可能な情報、システム等とクラウド利用者の ID との関係を定期的にレビューする等の措置を講じること。

(d) アグリゲーションサービス事業者は、供給者が提供するサービスへのアクセス制御も含めた措置を講じること。

(e) クラウドサービスを利用するのに必要なクラウド利用者側の環境（利用する Web ブラウザ、OS、その他のアプリケーション、デバイス等）のぜい弱性に関する情報収集を行い、クラウド利用者に対して必要な情報の提供、対応措置の依頼等の措置を講じること。

(f) クラウド利用者側のシステム/ネットワーク環境におけるアクセス制御に係るぜい弱性が原因となって、クラウド利用者からの預託情報に損害等が発生した場合の、クラウド事業者の免責等について、クラウド利用者とあらかじめ同意しておくこと。

(g) クラウドサービスを利用するのに必要なクラウド利用者の認証に係る情報の漏えいについて、特にフィッシングやマルウェアなどに関する情報収集を行い、クラウド利用者に対して必要な情報の提供、対応措置の依頼等の措置を講じること。

(h) 認証に係る情報がクラウド利用者から漏えいしたことにより、クラウド利用者からの預託情報に損害等が生じた場合のクラウド事業者の免責等について、クラウド利用者とあらかじめ同意しておくこと。

さらに、クラウド事業者が提供するアクセス制御の範囲と、クラウド利用者が利用可能なアクセス制御機能に基づいて、クラウド利用者がクラウドサービス選択の判断をできるようにするため、アクセ

ス制御方針に係る以下の内容を、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(b)(f)(i)から手法を選択してクラウド利用者に情報提供することが望ましい。

(a) 情報アクセス制御手法
(b) アクセス可能な範囲、粒度
(c) 権限管理者、権限付与・変更手順

また、クラウドサービスを提供するために供給者のクラウドサービスを利用している場合は、クラウド利用者の ID 管理の利便性を向上させるサービス機能等に係る以下の情報を、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(b)(f)(i)から手法を選択してクラウド利用者に情報提供することが望ましい。

(d) シングル・サイン・オン・メカニズムへの対応状況
(e) ID 連携管理の有無

シングル・サイン・オンや ID 連携を実施する場合は、管理責任と役割の範囲、技術的対応のための仕様、運用規約・手順等について供給者の規定を確認し、これに基づいて、ICT サプライチェーンにおける自らの管理責任と役割の範囲を定義するとともに、供給者との連携を実現できる仕様、運用規約、手順等を定めることで、必要な技術的対応を確保すること。ただし、連携するにあたり、供給者との間で特定個別の仕組みを新たに構築する場合は、役割や責任の分担、技術的対応のための取決め等についても個別に明確化し、文書化すること。

なお、個別契約連携クラウドサービスの形態である場合は、クラウド利用者が自らの管理責任の範囲を定義するにあたり、個別契約連携クラウド事業者が規定する管理責任の範囲を一つひとつ確認する必要がある。この確認プロセスは、通常のクラウド利用者対クラウド事業者の場合よりも複雑であるので、責任の所在に係るクラウド利用者の理解が不明確になる課題が生じうるため、特に注意を要する。

９.４.４ 特権的なユーティリティプログラムの使用

クラウドサービスがネットワークを通じて提供される性格を有するものであることから、第三者による特権的ユーティリティプログラムへの不正アクセスを防止するための措置を講じる必要がある。

また、クラウド事業者内部での特権的ユーティリティプログラムの管理に加え、クラウドサービスの提供を目的とするクラウド利用者に対して、サービス提供に必要な範囲で特権的ユーティリティプログラムを利用できるようにする際には、クラウド事業者及び供給者が提供するサービスへの不正アクセスにより、システムの改ざんや破壊、情報資産の盗聴や漏えい等が生じないようにするための措置を講じる必要がある。なお、ICT サプライチェーンを構築している場合には、Annex６ 15.２【供給者のサービス提供の管理】の措置を併せて講じることが望ましい。

さらに、エンドユーザ（組織）の管理者に対して、クラウドサービス利用の管理に関する特権的なユーティリティを利用できるようにする際には、クラウド利用者による他のクラウド利用者の預託情報への不正アクセスにより、他のクラウド利用者からの預託情報の改ざん、破壊、盗聴、漏えい等が生じないようにするための措置を講じる必要がある。

具体的には主要なシステムと業務用ソフトウェアによる制御を無効にすることのできる特権的ユーティリティプログラム等については、以下の対応策を講じることが望ましい。

(a) 特権的ユーティリティプログラム等を外部からの攻撃にさらされにくい環境に隔離すること。
(b) 特権的ユーティリティプログラム等へのアクセス状況を定期的にレビューし、不正なアクセスの監視を行うこと。
(c) クラウドサービスの提供を目的とするクラウド利用者が特権的ユーティリティプログラムを利用できるように権限を付与する場合には、特権的ユーティリティプログラムのアクセス権限及び権限付与・変更手順等を文書化すること。また、アクセス権限付与に関する証跡を記録し、不要なアクセス権限の設定がないかを、定期的なレビューにより確認すること。
(d) クラウドサービスの提供を目的とするクラウド利用者が特権的ユーティリティプログラムを利用する場合には、当該クラウド利用者に対しても特権的ユーティリティプログラムの利用に関する監視を求め、必要があればこれに関する情報の提供を求めること。
(e) エンドユーザ（組織）の管理者に対して、サービス利用の管理に関する特権的なユーティリティプログラムを利用できるようにする場合には、当該プログラムを通じて、他のクラウド利用者の預託情報へのアクセスがなされていないかを、定期的なレビューにより確認すること。

９.５　仮想化されたクラウドサービスのアクセス制御

９.５.１　仮想化資源の分離の確実な実施

仮想化された資源を用いてクラウドサービスを提供するクラウド事業者は、ソフトウェアの分離機能の技術的ぜい弱性を管理するとともに、クラウド利用者がクラウドサービス上にインストールするソフトウェアに起因する脅威も考慮して、仮想化マシンによるクラウド利用者の利用環境の分離（テナント分離）が適切に実施されるための措置を講じる必要がある。具体的には以下の対応策を講じることが望ましい。

(a) 仮想化マシンを構成するのに用いるソフトウェアのぜい弱性について定期的に確認を行い、技術的ぜい弱性が露見した場合には、適切な措置を講じること。

(b) IaaS・PaaS の場合は、クラウド利用者がクラウドサービス上にインストールしたソフトウェアに潜在するマルウェア等のリスクについても考慮すること。具体的には、ソフトウェアのインストールや変更に係る履歴を取る等の対策により、情報セキュリティ事象が当該インストールソフトウェアに起因するものであることを切り分けられるようにしておくこと[35]。

(c) 仮想化されたアプリケーション、OS、ストレージ、ネットワークについて、テナント間の分離及びテナントとクラウド事業者の内部管理の間の分離を確実に行うこと。また、分離された資源に対するアクセス制御を確実にするための措置を講じること。

[35] クラウド利用者に IaaS で仮想環境を提供し、この環境をクラウド利用者が自らの責任で運用している場合は、クラウド利用者によるソフトウェアのインストールや変更に係る履歴を、クラウド事業者が取得する権限を有していない場合がある。この場合は、(b)項の指針は適用されない。

１０ 暗号

１０.１　暗号による管理策

１０.１.１　暗号による管理策の利用方針

暗号による管理策の利用方針は、クラウドサービスにおいて、暗号を用いて保管又は伝送される情報の機密性確保/完全性・真正性の検証、アクセス制御における認証、否認防止等を行う範囲をどこまでとするか、これをどの程度の管理レベルで実施するか（ISO/IEC 27002:2013 10.1.1 実施の手引参照）によって定まる。クラウドサービス提供においては、クラウド利用者が暗号化に関し、自らが求める要求レベルを確保したクラウドサービスを確実に選択できるようにするため、実務上以下を実施することが望ましい。

(a) 暗号化に対応しているサービスを、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(b)(f) から手法を選択して、クラウド利用者に情報公開すること。また、暗号化されていないクラウドサービスについては、暗号化を代替する機能がある場合は、同じ手法を用いて、これをクラウド利用者に情報公開すること。

(b) クラウドサービスにおいて、保管又は伝送される情報の機密性確保/完全性・真正性の検証、アクセス制御における認証、否認防止等について、暗号化を適用する範囲を明確にし、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(i)に従って、クラウド利用者に情報開示すること。

(c) (b)を実施するにあたり、外部組織とクラウド事業者の間で転送する情報と長期間保存するクラウド利用者の情報（バックアップ等）の取扱いについて、特に留意すること。

(d) 暗号による管理策の運用実態について、クラウド利用者から個別に情報開示を要求された場合は、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(i)に基づいて情報開示することを検討すること。

１０.１.２　鍵管理

一般に、暗号鍵には使用期日を定め、そのライフサイクル全体で（生成→保管→保存→読出し→配布→使用停止→破壊）改変・漏洩・紛失から保護する必要がある。ここで、暗号アルゴリズム、鍵の長さ及びその使用法は、最適な慣行に従って選定する。公開鍵の真正性は認証局により確保することが望ましく、認証局との間では、賠償責任・サービスの信頼性・サービス提供の応答時間を含む契約又はSLAを締結することが望ましい（ISO/IEC 27002:2013 10.1.2 実施の手引参照）。これに加えて、クラウドサービス提供においては、実務上以下を実施することが望ましい。

(a) クラウド利用者に対し、暗号化の強度（鍵タイプ、暗号アルゴリズム、鍵の長さ）と鍵管理徹底の実態（例：鍵管理システムの仕様、推奨する鍵管理手順）を明確に示すため、個別の情報開示や監査済み言明書の公開により（Annex６ 6.3.2【利用者接

点とサプライチェーンにおける情報提供・共有】(c)(i)参照）、クラウド利用者に情報提供すること。

(b) クラウド利用者が、クラウドサービスに預託した情報の暗号化に用いる鍵を、個別に管理できるツールを提供すること。

１２　運用のセキュリティ

１２.１　運用の手順及び責任

１２.１.１　操作手順書

クラウド利用者が、クラウドサービスの情報セキュリティ関連機能（例：ログイン認証機能）の操作手順書を作成し、エンドユーザ（個人）に徹底することを支援することが望ましい。このため、クラウド利用者に対し、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(f)(i)から手法を選択して、操作手順書作成に必要な情報を提供することが望ましい。また、不明点の解消機能として、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(d)に基づいて FAQ や問合せ窓口を提供することが望ましい。

１２.１.２　変更管理

クラウドサービスに供するシステムに対して、第三者、あるいはクラウド利用者及びクラウド事業者の特権ユーザによる不正なプログラムの改ざん、変更、破壊等が生じないようにするため、あるいは生じた場合に、可及的速やかに発見できるようにするため、実務上以下を実施することが望ましい。

(a) クラウドサービスに供するシステムに関するプログラムは、安全に隔離された資源において管理を行うこと。

(b) クラウドサービスに供するシステムの変更のために、特権を利用する場合には、その利用を管理できるよう、手順を作成し、記録を作成すること。

(c) クラウドサービスに供するシステムのプログラム変更等について、必要なログ等を取得し、変更管理の状況について定期的にレビューを行うこと。

(d) 仮想化されたデバイス（サーバ、ネットワーク、ストレージ等）の導入・変更・削除、クラウドサービスの停止、バックアップ＆リストア等にあたっては、その障害がクラウドサービスを提供する資産に復旧できない損害を与えるおそれがあることから、その手順を文書化し、実務運用者と実施判断者の両方に徹底すること。

(e) アグリゲーションサービスを提供している場合は、供給者が提供するクラウドサービスの変更についても、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(f)(i)から手法を選択し、クラウド利用者に情報提供すること。

上記に加えて、クラウドサービスに供するシステムの変更を行う際に、誤ったプログラムのリリースや削除、破壊などを防止し、また、誤ったシステム変更が行われた場合に、可及的に速やかにサービスを復旧できるようにするために、以下の対応策を行うことが望ましい。

(f) クラウドサービスに供するシステムに関するプログラムの変更手順を明確に定め、変更後の確認を、変更した者以外の者が行う等、変更に対するチェック体制を構築すること。

(g) クラウドサービスに供するシステムの変更を行うにあたり、システムにおける直前の構成管理を明らかにし、変更結果から元の構成に戻すことができるように必要なバックアップを取る等の対応を行うこと。

１２.１.３　容量・能力の管理

サービス提供にあたり、第三者からの攻撃やクラウド利用者の不正な資源の利用が生じないようにするために、以下の対応策を講じることが望ましい。

(a) クラウドサービスに供するシステムで使用される資源の容量・能力等に不足が生じないように、状況に応じて必要な措置を講じるため、資源を常時監視すること。

(b) 外部からの攻撃や、利用者による不正な資源の利用により、サービス提供に必要な資源が枯渇する危険性が生じた場合には、それらを遮断、分離、停止できる対応策を講じること。

(c) 他のクラウド利用者に対するサービスを阻害するような資源の利用をした場合にサービス利用凍結を含めた措置を行う旨の資源の利用に関する同意を、クラウド利用者から得るほか、クラウド利用者が過大な資源の占有を行わないようにするための対策を講じること。

(d) クラウド利用者がクラウドサービスの資源逼迫状況や兆候を把握し、そのリスク管理等に役立てるため、資源の使用率や停止している資源の状況等を Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(f)(g)から手法を選択し、情報提供すること。

また、クラウドサービスの提供にあたり、必要な容量・能力を十分かつ効率的に確保するため、以下の対応策を講じることが望ましい。

(e) 資源確保の予測を的確に行えるようにするため、最適な資源配分を行う仕組みの有効性と運用設定の妥当性を定期的にレビューすること。

(f) クラウド利用者が要求する論理資源を十分に割り当てるため、物理資源使用の限界を超えた論理資源の総和を設定すること。この際、論理資源の総和が物理資源を超過するような資源の割当は、物理資源の最繁時の同時使用率を考慮して行うこと。

(g) 運用者向けの手順書のレビューにおいて、容量及び能力が設計時の想定を超えた場合の対応手順（仮想資源の再配置のためのライブマイグレーション及び仮想ネットワークの変更手順等）が確実に行われるようにすること。

１２.２　マルウェアからの保護

１２.２.１ マルウェアに対する管理策

クラウドサービスに供する情報処理施設等へのマルウェアの感染を防止し、あるいは感染後、二次的な被害の発生（情報の漏えい、クラウド利用者への感染等）を防止するための措置を講じる必要がある。また、感染後、サービス再開に向けた必要な対応策を講じる必要がある。具体的には、実務上以下を実施することが望ましい。

(a) クラウドサービスに供する情報処理施設等に侵入したマルウェアのスキャン及び検出を毎日実施するほか、第三者からの攻撃等が生じた場合等のマルウェアへの感染が疑われる情報セキュリティ事象が生じた場合にも、マルウェアのスキャン及び検出を速やかに行うこと。また、これに必要な情報収集を日常的に行うこと。

(b) クラウドサービスに供する情報処理施設等に対するマルウェアの感染が認められた場合には、速やかなマルウェアの駆除、外部ネットワークとクラウド事業者が管理するクラウド利用者の預託データとの分離等の、二次的な被害の発生を防止するための措置を講じること。

(c) クラウド利用者の情報処理施設等でマルウェア感染の可能性が生じた場合には、クラウドサービスに供する情報処理施設等においても、速やかにマルウェア検出のための措置を講じること。

(d) マルウェア感染に伴いクラウドサービスが停止した場合には、速やかにクラウド利用者に対してその事実を示すとともに、クラウド利用者の情報処理施設等のマルウェア感染の確認を促す等の措置を講じること。また、クラウド利用者に対し、必要に応じて、被害状況、サービスの復旧見込み等についての情報を、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(h)の手法によって提供すること。

(e) アグリゲーションサービス事業者は、提供するクラウドサービスの ICT サプライチェーンの一部の情報処理施設等にマルウェアの感染が認められた場合であっても、影響範囲が確認できるまで、ICT サプライチェーン全体で(b)(c)の措置を講じること。その上で原因が特定され、影響範囲が明確になった段階で、ICT サプライチェーンにおいてクラウド利用者に影響が及ばない措置（駆除あるいは隔離等）を講じたうえで、サービスの提供を再開すること。

さらに、自社のサービス利用に供するクラウド利用者の情報処理施設等を攻撃対象としたマルウェアへの感染を防ぐため、以下の対応策を講じることが望ましい。

(f) 自社のサービス利用に供するクラウド利用者の情報処理施設等を攻撃対象としたマルウェアに関する情報を日常的に収集し、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(f)の手法により、クラウド利用者に提供すること。

(g) マルウェアが伝送されてくる等、特定のクラウド利用者がマルウェアに感染した兆候を検知した場合は、その事実をクラウド利用者に通知するとともに、必要があれば当該利用者のクラウドサービス利用を一時停止できるよう、契約上及び技術上の措置を講じること。

１２.３　バックアップ

１２.３.１　　情報のバックアップ

クラウド事業者が取得するバックアップについて、特定のクラウド利用者の預託データの提出命令等が生じた場合でも、クラウドサービスのサービスレベルを保証したままクラウドサービスの利用を継続できるようにするため、実務上以下を実施することが望ましい。

(a) クラウド事業者が取得するバックアップのうち、クラウドサービス提供に不可欠な設定などに関するデータのバックアップと、クラウド利用者の預託データのバックアップを分離すること。

(b) クラウド利用者の預託データのバックアップにおいて、個々のクラウド利用者の預託データを特定できる、あるいは検索可能な措置を講じること。

(c) 特定のクラウド利用者の預託データの提出等がなされた場合でも、(b)によりその対象を最小限の範囲に限定することで、無関係なクラウド利用者の預託データのバックアップが、不当に情報漏洩しないような措置を講じること。

１２.４　ログ取得及び監視

１２.４.１　イベントログ取得

供給者が必要なイベント等のログを取得し、取得したログを保持することを確保する必要がある。このため、供給者の選定にあたっては、イベントログの範囲、内容、粒度等について、供給者の規定がクラウド事業者の要求を満足していることを事前に確認することが求められる。このため、実務上以下を実施することが望ましい。

(a) 脅威として監視すべきイベント等を定め、これに基づいて、クラウドサービスとして取得するイベントログの範囲、内容、粒度等を定めること。
(b) (a)で定めた取得するログの範囲、内容、粒度等について、供給者の利用規約、SLA等の規定を確認し、クラウド事業者の要求を満足できる供給者を選定すること。

また、アグリゲーションサービスを提供する場合には、アグリゲーションサービス事業者が主導し、供給者との間で、取得するログの範囲、内容、粒度等に関して一貫したポリシーを適用するために、実務上以下を実施することが望ましい。

(c) アグリゲーションサービス事業者は、供給者との間で、取得できるログの範囲、内容、粒度等について情報を共有すること。
(d) アグリゲーションサービス事業者は、供給者のイベントログ取得ポリシーを確認し、これを踏まえて ICT サプライチェーン全体で、統一して適用するイベントログ取得ポリシーの範囲を明示・調整すること。

１２.４.２　ログ情報の保護

クラウド利用者や特権ユーザによる不正アクセスや外部からの攻撃等からログ情報を保護することが求められる。また、クラウドサービス提供にあたっては、一部のクラウド利用者や特権ユーザの犯罪行為等に伴う記録媒体の提出命令、クラウド利用者等による不正な行為への対応のためのログ記録の提出命令等により、提供するサービスの停止等が生じないための措置を講じることが求められる。具体的には、実務上以下を実施することが望ましい。

(a) 適切なアクセス制御、資源の分離等の保護対策を適用し、ログ情報の記録の削除や、改ざん、ログ取得設定の変更などを防止すること。
(b) 一部のクラウド利用者等の犯罪行為等に伴う記録媒体の提出命令等によるサービス停止を防ぐため、ログ情報のバックアップを作成するとともに、ログ情報をエンドユーザ（個人）/特権ユーザ単位に管理できる措置を講じること。
(c) アグリゲーションサービス事業者は、供給者のログ情報の保護ポリシーを確認し、ICT サプライチェーン全体で統一して適用できるポリシーの範囲を明らかにすること。

１２.４.３ 実務管理者及び運用担当者の作業ログ

クラウド事業者の実務管理者や運用担当者の特権利用及びクラウド利用者の特権利用について、連携する供給者が提供する管理機能等を利用する場合も含めて監視できるようにする必要がある。このため、供給者の選定にあたっては、取得するログで対象とするイベントの範囲やその詳細事項について、供給者の規定がクラウド事業者の要求を満足していることを事前に確認することが求められる。また、特権の悪用から保護する措置の一環として、取得したログに対する適切な保護対策を講じるとともに、定期的なレビューを行う必要がある。これらの措置を確実にするため、以下の対応策を講じることが望ましい。

(a) クラウド利用者の特権利用に基づく資源利用に係るログを特権ユーザ単位で取得し、管理者による不正行為に対する措置を講じられるようにすること。また、クラウド事業者においても同様に特権利用のログを特権ユーザ単位で取得し、クラウド利用者とクラウド事業者の特権利用のログを突合することによって、クラウド利用者とクラウド事業者の適正な運用責任の分担を検証できるようにすること。

(b) システムのぜい弱性、サービス管理のためのアプリケーションなどのぜい弱性を利用した管理用インターフェイスの悪用を防ぐため、管理アプリケーションに対する利用状況やそのためのプログラム等の構成管理状況のログを取得し、監視等の措置を講じること。

(c) (a)(b)の求めに応じて定めるログ取得方針について、供給者の規定を確認し、クラウド事業者の要求を満足できる供給者を選定すること。

(d) 取得した特権利用に関するログについて、発生したイベントの妥当性等を検証し、あるいは不正なアクセスの可能性を分析するなど、適切なレビューを行うための措置を講じること。

さらに、アグリゲーションサービス事業者は、クラウドサービス全体に対する監視が求められることから、サービス提供のための ICT サプライチェーン全体で適用できるログ取得・保護方針の範囲を明らかにすることが求められる。具体的には、以下の対応策を講じることが望ましい。

(e) アグリゲーションサービス事業者は、供給者のログ取得及び記録保護等に関するポリシーを確認し、ICT サプライチェーン全体で一貫して適用できるポリシーの範囲を明らかにすること。

(f) アグリゲーションサービス事業者は、ICT サプライチェーン全体でどのようなログ情報を一貫して取得できるのかを確認し、クラウド事業者と供給者間で突合が可能なログ情報の範囲を明らかにすること。

１２.５　運用ソフトウェアの管理

１２.５.１　運用システムに関わるソフトウェアの導入

クラウドサービス上に、クラウド利用者が供するソフトウェアのインストールを行うことができる資源を提供する場合、当該ソフトウェアの悪意ある動作に対応するため、以下の対応策を実施することが望ましい。

(a) 情報セキュリティマネジメントの観点から必要である場合には、クラウド利用者がクラウドサービス上にインストールできるソフトウェアの範囲に制限を設け、クラウド利用者と同意すること。

(b) クラウド利用者がクラウドサービス上にインストールしたソフトウェアにより、クラウドサービスに情報セキュリティマネジメント上のぜい弱性が生じた場合には、当該クラウド利用者が利用する資源を隔離して、安全にサービスを提供できるような措置を講じること。

(c) クラウド利用者がクラウドサービス上にインストールしたソフトウェアにより、クラウドサービスに情報セキュリティマネジメント上のぜい弱性が生じたため、安全なサービスの提供が継続できない場合には、速やかにクラウドサービスの全部又は一部を停止する等の措置を講じること。

(d) 利用規約等によって、クラウド利用者の運用により、マルウェアに感染したソフトウェアをクラウドサービス上にインストールさせないことを求めること。

(e) クラウド利用者がインストールしたソフトウェアに起因して、他のクラウド利用者に影響を及ぼすような情報セキュリティ事象が発生した場合に、その原因を切り分けられるように、クラウド利用者によるソフトウェアのアップロード及び変更の履歴を保持すること。

１２.６ 技術的ぜい弱性管理

１２.６.１ 技術的ぜい弱性の管理

一般には、技術的ぜい弱性管理のためには、適切な IT 資産管理による完全な資産目録の維持、管理のための役割と責任の確立、情報の収集、技術的ぜい弱性が発見された際の処置選択の判断及び処置実施に係る対応プロセスの確立、監査ログの保持、対応プロセスの有効性の監視・評価等を行う必要がある（ISO/IEC 27002:2013 12.6.1 実施の手引参照）。また、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) クラウドサービスとその資源に適用される技術的ぜい弱性管理についての情報を、Annex 6 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(f)(i)から適切な手法を選択して、クラウド利用者に提供すること。
(b) ISO/IEC 27002:2013 の 12.6.1 の実践の規範が示すポイントを実現する手法についても、(a)と併せてクラウド利用者に情報提供することを検討すること。
(c) クラウド事業者が実施する技術的ぜい弱性の同定作業に伴い、計画的なサービス停止が発生する場合は、Annex６ 6.3.2【利用者接点とサプライチェーンにおける情報提供・共有】(f)に従って、クラウド利用者に事前に情報公開すること。
(d) 個別のクラウド利用者に係る技術的ぜい弱性情報を、他のクラウド利用者に提供しないこと。

１２.７ 情報システムの監査に対する考慮事項

１２.７.１ 情報システムの監査に対する管理策

クラウドサービスの監査については、最小限の点検によって管理策の十分性を確認できるような対応策を講じて、運用業務プロセスの中断リスクを最小限にすることが望ましい。また、クラウド事業者の負担を軽減し、クラウドサービス中断リスクを低減するため、クラウド利用者からの個別の監査対応要請を減ずるための措置を講じることが求められる。具体的には、実務上以下を実施することが望ましい。

(a) クラウドサービスの監査について方針を定め、監査を定期的に実施する、監査対象となる資源とサービス提供に係る情報資産等の分類を適切に行い、監査対象を明確にし、最小限の監査により、管理策の十分性を確認できるようにする等、効果的な監査を実施できるようにする措置を講じること。
(b) クラウド利用者からの個別の監査対応要請を少なくするために、監査済み言明書の公開、監査報告書（クラウド事業者のセキュリティ管理に係る内部統制保証報告書（IT

実 7 号、SOC2 等）等）の情報開示、その他必要な情報の開示、認証の取得等、クラウド利用者が行う監査対応を簡素化するための措置を講じること[36]。

また、財務報告に関連する場合に限定されるが、クラウド利用者は、日本公認会計士協会の監査・保証実務委員会実務指針第 86 号又は米国公認会計士協会（AICPA）の米国保証業務基準書第 16 号（SSAE16）に基づく監査を受けているクラウド事業者を優先的に選択する場合がある。このような場合には、これらの基準/指針に基づくクラウド事業者の内部統制保証報告書を、NDA を締結した上で情報開示することによっても、クラウド利用者が行う情報システム監査対応の簡素化に貢献できることが多く、検討に値する。

１３　通信のセキュリティ

１３.１ ネットワークセキュリティ管理

１３.１.４仮想ネットワークにおいて重視すべきぜい弱性

仮想ネットワークを構築してクラウドサービスを提供する場合には、仮想ネットワークの管理ミスを防止し、オンプレミスから移行するクラウド利用者に対する移行中の悪意の攻撃にも留意するため、実務上以下を実施することが望ましい。

(a) クラウドサービスの提供にあたり、仮想ネットワークを新たに構築する場合は、物理ネットワーク構成との対応関係が明確になるように仮想ネットワークを構成すること。
(b) 仮想ネットワークの運用設定方針と設定承認方針を、物理ネットワークの運用経験とノウハウに基づいて実施しやすい形で定義し、文書化すること。
(c) PaaS/IaaS を提供している場合は、クラウド利用者の構内設備をクラウドサービスに移行させる際に、仮想/物理ネットワークの再構成、移行、試験運用のプロセスで悪意の攻撃を受けないように、クラウド利用者にセキュリティ管理の徹底を助言すること。

１３.２ 情報の転送

１３.２.２　情報転送に関する合意

供給者との間で適用できるデータ転送に係る標準的な規格・仕様、クラウドサービス内又は外部とのデータ連携における暗号化・資源の隔離、クラウド利用者のユーザ ID 窃取に対する措置、クラウド利用者から預託された情報の返却に係るデータ規格・仕様等について、供給者が可能な対応範囲をクラウド事業者の要求水準まで引き上げ、クラウド利用者からも必要な同意を獲得す

[36] 特定非営利活動法人日本セキュリティ監査協会（JASA）では、クラウドセキュリティ推進協議会（JCISPA）において、クラウド情報セキュリティ監査制度の検討を進めており、その中で言明要件の検討も実施しているので、参考にされたい。

ることにより、データ連携や預託情報の返却に係る情報転送を確実かつ安全に実施できるようにすることが求められる。このため、実務上以下を実施することが望ましい。

(a) ICT サプライチェーンを構成してクラウドサービスを提供する場合には、クラウドサービスの提供におけるデータ転送に係る方針、標準的な規格・仕様等及びこれに対する保守方針等について、供給者の規定を事前に確認し、データ転送が確実かつ安全に実施できる供給者を選定すること。ただし、特定の供給者との間で個別の方法によりデータ転送を行う場合には、方針、規格・仕様、保守方針等について、個別の調整と合意が求められる。

(b) ICT サプライチェーンを構成してクラウドサービスを提供する場合には、供給者のサービスが停止した場合のデータ転送の安全確保等に係る措置を講じること。

(c) クラウドサービス内又は外部とのデータ連携を行うにあたり、暗号化・資源の隔離等の、情報転送を確実かつ安全に実施できる措置を講じること。

(d) フィッシング対策等の秘密認証情報窃盗への対応及びクラウド利用者への注意喚起を行うことにより、クラウド利用者からの ID 等の秘密認証情報の転送の安全を確保するための措置を講じること。

(e) クラウドサービスの利用終了時に、預託された情報を安全かつ完全な形で返却するために、情報転送のためのデータ規格、仕様等について、事前にクラウド利用者からの同意を得ること。

１３.２.４ 秘密保持契約又は守秘義務契約

複数国の資源やサービスを利用してクラウドサービス提供する場合に、契約締結を行う他国の供給者との機密保持契約等の順守が確保されるために必要な対応策を講じる必要がある。具体的には、実務上以下を実施することが望ましい。

(a) 複数国の資源やサービスを利用してクラウドサービス提供する場合に、機密保持契約等の順守に必要となる、裁判管轄や適用法に関する規定、損害賠償の約定、担保措置等の措置が講じられていることを事前に確認した上で、他国の供給者との秘密保持契約、守秘義務契約の締結を行うこと。

１５ 供給者関係

１５.１ 供給者関係における情報セキュリティ

１５.１.１供給者関係のための情報セキュリティの方針

クラウドサービスを連携して提供するにあたっては、情報セキュリティマネジメント措置を講じる範囲や対策に係る方針について明確に規定し、その規定がクラウド事業者の要求を満足する水準を確保している供給者を選定することが求められる。サービス提供における資源、運用に関する基本的な方針についても明らかにすることで、サービス提供の継続性を維持し、あるいは不正な管理対応を未然に防止することが期待できる。これらの対応を図るために、実務上、以下のような対応を行うことが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、情報セキュリティマネジメントに関する基本的な方針等に関し、情報セキュリティポリシー等の適用範囲と内容について明確にすること。また、ICT サプライチェーンを構成して提供されるクラウドサービスに必要な技術的仕様、サービスレベル、運用手順等について明確にすること。さらに、これらにつき、利用規約、SLA 等で明記し、同意を行うことが可能な供給者を選定すること。ただし、データ連携等のため、特定の供給者と個別の仕組みを新たに構築して対応する範囲に限っては、情報セキュリティポリシー等の適用範囲と内容、サービス提供に必要な技術的仕様、サービスレベル、運用手順等について当該供給者と調整し、明確にすることが求められる。

(b) ICT サプライチェーンを構成して提供されるクラウドサービスについて、サービス提供における情報セキュリティマネジメントの要求事項に係る責任の所在を、クラウド利用者に対して明確に示し、あるいは責任が分散している場合には、その旨を明示すること。

(c) クラウド事業者及び供給者以外が提供するサービスを、クラウド利用者がクラウドサービスと併せて利用する場合、クラウド事業者及び供給者以外が提供するサービスに係る情報セキュリティマネジメント上の要求事項についての、クラウド利用者の管理責任の範囲やクラウド事業者・供給者の免責の範囲、運用方針等を明確にし、利用規約等を通じてクラウド利用者の同意を得ること。

(d) ICT サプライチェーンを構成して提供されるクラウドサービスに適用する証跡の記録・管理に関する方針等を明確に定めること。また、これについて、利用規約、SLA 等で明記し、同意を行うことが可能な供給者を選定すること。さらに、クラウド事業者と供給者との間でのサービス接続において生じる証跡の記録等に係る管理責任等の範囲について、供給者が明示する規定を確認して同意し、これに基づいて自らの責任等の範囲を明確に定義した上で、必要な措置を講じること。ただし、データ連携等のため、特定の供給者と個別の仕組みを新たに構築して対応する範囲に限っては、証跡の記録・管理に関する方針及びサービス接続において生じる証跡の記録等に係る管理責任等の範囲について、当該供給者と調整し、明確にすることが求められる。

１５.１.３　ICT サプライチェーン

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、一部の供給者が提供するサービスにおいて情報セキュリティマネジメントに係る要求事項が満たされないことを防止するために、供給者の利用規約、SLA 等の規定により情報セキュリティマネジメントに関する要求事項への対応状況を確認し、クラウド事業者の要求を満足できる供給者を選定することが求められる。具体的には、実務上以下を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、サービス継続に必要な情報セキュリティマネジメント要求事項に関し、供給者の利用規約、SLA 等の規定によりその対応状況を確認し、全ての要求を満足できる供給者を選定すること。ただし、データ連携等のため、特定の供給者と個別の仕組みを新たに構築して対応する範囲に限っては、当該供給者との間で調整・合意を行うことが求められる。

(b) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、クラウド事業者と供給者の間でクラウドサービスの接続に関する情報セキュリティマネジメント上のリスクを明確にし、その管理策を具体的に定めること。
また、これらの管理策の実施に係る供給者の管理責任の内容・範囲及び役割について利用規約、SLA 等で明記して同意できる供給者を選定し、その同意に基づいて自らの管理責任を定義すること。ただし、データ連携等のため、特定の供給者と個別の仕組みを新たに構築して対応する範囲に限っては、当該供給者との間で調整・合意を行うことが求められる。

１５.２ 供給者のサービス提供の管理

１５.２.１供給者のサービス提供の監視及びレビュー

ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、供給者と連携する事項に関して、情報セキュリティマネジメントにおけるぜい弱性を監視・レビューするとともに、供給者においてぜい弱性が生じた場合でも、クラウド事業者が提供するサービスが被る影響を最小限に抑える措置を講じることが求められる。

また、アグリゲーションサービスの場合には、クラウドサービス提供に影響を及ぼす供給者のサービスレベル低下を未然に防止し、あるいは円滑なサービス回復を実現するため、ICT サプライチェーンの全ての供給者のサービス提供状況を監視することが求められる。

これらの対応を図るために、実務上、以下を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、供給者が自ら提供するサービスについて、情報セキュリティマネジメントに係る要求事項の実施状況の管理及びレビュー実施に関し、利用規約、SLA 等でどのように規定しているかを確認し、クラウド事業者が求める水準でレビューを実施できる供給者を選定すること。

(b) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、クラウド事業者は、供給者のサービスと連携する事項（データ、インターフェース等）について、情報セキュリティマネジメントに係るぜい弱性を監視・レビューするとともに、供給者においてぜい弱性が生じた場合でも、クラウド事業者が提供するサービスが被る影響を最小限とする措置を講じること。

(c) アグリゲーションサービス事業者は、提供するクラウドサービス全体についての監視、レビュー、監査実施に対する責任を果たすこと。ただし、この責任は、供給者に対し、外部監査人による「クラウド事業者のセキュリティ管理に係る内部統制保証報告書」の提供を求めることで代替が可能であり、これによってアグリゲーションサービス事業者の管理統制業務の負担を軽減することができる。

１５.２.２供給者のサービス提供の変更に対する管理

ICT サプライチェーンを構成して提供されるクラウドサービスでは、一部の供給者のサービスの変更に起因して、他の供給者が提供するサービスや、クラウド事業者が提供するサービス全体に、不測の障害等が生じないようにするための管理策を取ることが求められる。

特にアグリゲーションサービス事業者においては、一部の供給者におけるサービスの変更が、アグリゲーションサービス全体に影響を生じさせないように管理する責任があるため、その管理策が求められる。具体的には、実務上以下を実施することが望ましい。

(a) アグリゲーションサービス事業者は、ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、供給者が提供するサービスの変更に伴う影響範囲等について事前に把握し、他の供給者が提供するサービスに不測の障害等を生じないように、必要な情報を提供すること。

(b) アグリゲーションサービス事業者は、一部の供給者が行う変更に関する管理を行い、クラウドサービス全体として変更に伴う影響を最小限にするための対応策を講じること。

１６　情報セキュリティインシデント管理

１６.１　情報セキュリティインシデントの管理及びその改善

１６.１.２　情報セキュリティ事象の報告

資産管理の責任をもれなく個人に割り当て、これらの責任者に対し、報告すべき情報セキュリティ事象の内容、その明確な連絡先（時機を失しない対応ができることが望ましい。）及び可能な限り速やかな報告の実施を徹底する。ここで、報告すべき情報セキュリティ事象の内容には、効果のないセキュリティ管理策、情報の完全性・機密性・可用性に関する期待に対する違反、人的ミス、個別方針又は指針の不順守、物理的セキュリティの取決めに対する違反、管理されていない

システム変更、ソフトウェア又はハードウェアの誤動作、アクセス違反が含まれる（ISO/IEC 27002:2013 16.1.2 実施の手引 a）-h)参照）。

また、情報セキュリティ事象の報告書式を定め、事象の発見者は、この書式に従って重要事項を詳細に記録し、直ちにあらかじめ定められた連絡先に報告することが望ましい。

また、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) ガバナンスの実態が異なるクラウド事業者と供給者間で、クラウドサービス提供におけるそれぞれの管理責任等の範囲を明確に設定すること。
(b) クラウド利用者や供給者に対しても、クラウドサービスにおける情報セキュリティ事象の速やかな報告手順とその連絡先を認識させておくこと。
(c) クラウドサービスにおける情報セキュリティ事象を、クラウド利用者から受け付ける窓口を設置して周知し、情報セキュリティ事象に係る速やかな情報集約に努めること。
(d) ICT サプライチェーンの中で、情報セキュリティ事象の連絡を伝播させる連絡経路を、管理責任の分担と一体で明確にし、訓練によって正しく連絡を伝播できることを確認すること。

なお、個別契約連携クラウドサービスの形態である場合は、緊急時における役割分担等が曖昧になっていると、クラウド利用者からの情報セキュリティ事象の報告が適切な個別契約連携クラウド事業者に通報されない事態が生じる。これに対処するため、個別契約連携クラウド事業者間での情報共有の仕組みを強化する、クラウド利用者に対する窓口を一本化する等の対策を行うことが望ましい。

１６.１.４　情報セキュリティ事象の評価及び決定

クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) クラウドサービス提供における重大な情報セキュリティインシデントの明確な分類基準を定め、この基準を用いて情報セキュリティ事象を評価し、その事象を情報セキュリティインシデントに分類するかを決定すること。
(b) 情報セキュリティインシデントへの分類の判断において、クラウド利用者との間で認識の違いが生じると、情報提供に不満を感じる等の理由から、情報セキュリティインシデント対応に係るクラウド利用者からの信頼感を阻害するおそれがあるため、分類基準を明確に定めることに加えて、必要に応じてクラウド利用者と SLA を締結すること。
(c) 情報セキュリティインシデントの形態、規模及び費用を定量化して監視できるようにする仕組みを備えること。また、この仕組みを活用し、情報セキュリティインシデントの分類基準の妥当性をレビューし、必要に応じて改善を加えること。
(d) 情報セキュリティインシデントの事実関係、復旧/回復措置、復旧見込、影響範囲等の情報を、クラウド利用者に提示すること。情報提供の方法については、Annex６ 6.3.2

【利用者接点とサプライチェーンにおける情報提供・共有】(h)に基づくこととし、情報提供のタイミングは、随時又は一定間隔とすること。また、この方針に従って、必要に応じてクラウド利用者と SLA を締結すること。

１６.１.７　証拠の収集

懲戒措置及び法的処置のために証拠を取り扱う場合は、組織内部の手順を定めてこれに従うことが望ましい。

まず、証拠として利用できる情報は特定し、文書化しておく。証拠として利用できる情報は、紙文書として得られる情報、仮想マシンから得られる情報、ネットワークから得られる情報、SIEM から得られる情報、IPS から得られる情報等に分類される。

証拠となる情報の取扱いはその種別（紙文書、コンピュータ媒体上の情報）により異なるため、それぞれについてフォレンジック（収集・保存・保全）の手順（保存期間も含む）を定めておくことが望ましい。特に、コンピュータ媒体上の情報を取り扱う場合は、フォレンジックの知識に基づく専門性の高い手順を適用する必要があるため、その事象が訴訟に発展するかどうか判然としない場合は、早めに弁護士、警察、フォレンジックの専門家等に相談し、助言を求めることが望ましい。また、可能であれば、フォレンジック情報が供給されるインターフェイスと API を把握しておき、コンピテンシーが高い人物からフォレンジック実務の支援を受けることが望ましい[37]。

さらに、クラウドサービスの提供にあたっては、以下に示す技術の実装を検討するとともに、実務上以下を実施することが望ましい。

(a) 可能であれば、複数のクラウド利用者で共用された媒体・資源へのフォレンジック調査中に、証拠の収集・保存・保全に無関係な他のクラウド利用者の記録の破損等の二次的な資産の損害を防止できる技術を適用すること。
(b) 可能であれば、複数のクラウド利用者で共用された媒体・資源へのフォレンジック調査中に、証拠の収集・保存・保全に無関係な他のクラウド利用者の機微情報を保護できる技術を適用すること。
(c) クラウド利用者が行う証拠収集の制限事項について定義し、クラウド利用者と合意すること。
(d) クラウド利用者が、証拠として利用できる情報へのアクセスを要請し、その許諾を得るための手順をクラウド利用者と合意すること。このアクセスに費用や料金が発生する場合は、それを文書化してクラウド利用者に示すこと。

[37] クラウド環境におけるフォレンジックは、技術的な困難さがあり、また実務上経済的な負担も少なくない。

(e) クラウドサービスにおいて、司法権を跨るデータ格納を行う場合は、各国の法制度を考慮するとともに、その情報をクラウド利用者にも提供し、この情報に基づいてクラウド利用者が自らデータ格納を行う国等を選択できる仕組みを提供すること。

１７ 事業継続マネジメントにおける情報セキュリティの側面

１７.２　冗長性

１７.２.１情報処理施設の可用性

情報処理施設の可用性を保証するためには、情報処理施設の十分な冗長性を確保した上で、障害時には運用系から冗長系への切り替えを確実に行うことが求められる。運用系から冗長系への切り替えを確実にするためには、切り替えが意図どおりに動作することを定期的に確認することが望ましい。

さらに、クラウドサービスの提供にあたっては、実務上以下を実施することが望ましい。

(a) ID 管理サービス、課金サービスなどの基幹機能において、単一障害点となっているものを特定し、十分な冗長性と障害時の円滑な切り替えを確保すること。
(b) 仮想化機能やサービス管理機能において、単一障害点となっている機能を特定し、十分な冗長化、障害時の円滑な切り替え、情報処理施設の管理単位分割等の対策を講じること。
(c) 情報処理施設やネットワークにおいて、単一障害点となっている設備を特定し、十分な冗長性と障害時の円滑な切り替えを確保すること。
(d) 障害の連鎖を食い止める防護機構を組み込むこと。

なお、クラウドサービスを広域災害から防護する観点からは、以下を実施することも推奨される。

(e) クラウドサービスを広域災害から防護するため、データセンタを地理的に離れた複数の地域に設置することにより、(a)～(c)の対策を補完すること。
(f) 広域災害の発生に際しては、クラウドサービスの継続を優先するか、情報セキュリティ対策の確保を優先するかについての方針を定め、クラウド利用者の同意を得ること。

１８ 順守

１８.１　法的及び契約上の要求事項の順守

１８.１.１　適用法令及び契約上の要求事項の特定

クラウドサービスにおいては、特に国際間でサービス提供される場合に、適用される法令が国によって異なることによって、サービス提供の継続や、クラウド利用者のサービス利用の継続が困難になることがある。具体的には、実務上以下を実施することが望ましい。

(a) 複数国のクラウド利用者に対してサービス提供を行う、または、複数国の資源やサービスを利用してサービス提供を行うクラウド事業者は、サービス対象や利用資源が越境することによってクラウドサービスに生じうる、適用法の違いによるリスクを事前に把握すること。

(b) 複数国の資源やサービスを利用してサービス提供を行うクラウド事業者は、当該資源やサービスが存在する国において適用される法令等に係るリスクに対して、サービス提供上必要な措置を講じること。

(c) クラウド利用者が、クラウドサービスの海外における脅威を正しく認識し、これに基づいて預託する情報の範囲と情報の保存国を適切に選択する責任を果たせるように、その判断を情報提供等により支援できる範囲を明示して支援し、クラウド利用者の正確な判断を促進すること。

なお、適用法令及び契約上の要求事項の特定という観点では、利用規約や SLA 等における一般的な契約上の要求事項に加えて、クラウド利用者から預託された情報の契約終了時の取扱いに係る要求事項等も考慮する必要がある。これらについては、総務省、経済産業省等から ＩＴ アウトソーシングや SLA 等に係るガイドラインが公表されているので、こちらを参照されたい。

１８.１.２　知的財産権

複数国のクラウド利用者に対してクラウドサービスを提供する場合や、複数国の資源やサービスを利用してクラウドサービスを提供する場合に生じうる、知的財産法の違いに伴うリスクを明確にし、必要な措置を講じることが求められる。また、情報サービス利用に供するライセンスの範囲についての紛争に伴うサービス停止等が生じないようにするための管理が求められる。このため、実務上以下を実施することが望ましい。

(a) 複数国のクラウド利用者に対してサービス提供するクラウド事業者は、クラウドサービス利用において供するクラウド利用者の知的財産情報の権利に対し、国による知的財産保護法上の保護範囲の違いに起因して生じうるリスクを明らかにすること。

(b) 複数国のクラウド利用者に対してサービス提供するクラウド事業者は、クラウドサービスの提供にあたって利用する知的財産権の取り扱いについて、複数国でサービス提供することによって生じるリスクを把握し、必要な対策を講じること。

(c) クラウド利用者が、クラウドサービスの海外における脅威を正しく認識し、これに基づいて預託する情報の範囲と情報の保存国を適切に選択する責任を果たせるように、その判断を情報提供等により支援できる範囲を明示して支援し、クラウド利用者の正確な判断を促進すること。

１８.１.３　記録の保護

他国の資源やサービスを利用してクラウドサービスの提供を行うクラウド事業者は、他国の我が国とは異なる法令の適用によって、クラウド事業者、供給者又は一部のクラウド利用者が当該国の法令違反を疑われ、その結果遂行される不測の差押えや提出命令によって、クラウドサービス提供の停止や無関係なクラウド利用者の預託情報の流出を発生させるおそれがある。そこで、実務上、以下の対応策を実施することが望ましい。

(a) 他国の資源やサービスを利用してクラウドサービスを提供するクラウド事業者は、他国において自身又は供給者が法令違反を疑われ、当該国の司法官憲等の不測の差押えを受けた場合であっても、クラウドサービスが停止しないように、国境を越えたバックアップを行う等の必要な措置を講じること。

(b) 他国の資源やサービスを利用してクラウドサービスを提供するクラウド事業者は、一部のクラウド利用者による法令違反の疑いにより、他国の司法官憲等から当該利用者の預託情報の提出命令を受けた場合であっても、無関係なクラウド利用者の預託情報が一緒に流出しないように、預託情報を容易に分離できる等の必要な措置を講じること。

１８.１.４　プライバシー及び個人を特定できる情報（PII）の保護

複数国のクラウド利用者に対してクラウドサービスを提供する場合や、複数国の資源やサービスを利用してクラウドサービスを提供する場合に、複数の国や地域における個人情報保護法制の違いなどに基づく、情報セキュリティマネジメントに関する要求事項の違いに対応する管理策を講じる必要がある。具体的には、実務上以下の対応策を実施することが望ましい。

(a) 複数国のクラウド利用者に対してクラウドサービスを提供するクラウド事業者、あるいは複数国の資源・サービス等を利用するクラウド事業者は、クラウド利用者の資源が存在する各国の法制に基づく個人情報保護に必要な取扱いについて事前に把握し、必要な対策を講じること。

(b) クラウド利用者が、クラウドサービスの海外における脅威を正しく認識し、これに基づいて預託する個人情報の範囲と個人情報の保存国を適切に選択する責任を果たせるように、その判断を情報提供等により支援できる範囲を明示して支援し、クラウド利用者の正確な判断を促進すること。

なお、クラウドサービスにおける PII の安全な取扱いについては、ISO/IEC27018 が策定されている。

１８.１.５　暗号化機能に対する規制

複数国のクラウド利用者に対してクラウドサービスを提供する場合や、複数国の資源やサービスを利用してクラウドサービスを提供する場合、複数の国や地域における暗号化措置に対する規制等の違いに基づく、情報セキュリティマネジメントに係る要求事項の違いに対応する管理策を行う必要がある。具体的には、実務上以下の対応策を実施することが望ましい。

(a) 複数国のクラウド利用者に対してクラウドサービスを提供するクラウド事業者、あるいは他国の資源、サービス等を利用するクラウド事業者は、クラウド利用者や資源が存在する各国における暗号利用に係る法律上の必要性、あるいは制約等について把握し、クラウドサービスの提供に際しての必要な対策を講じること。

１８.２　情報セキュリティのレビュー

１８.２.１　情報セキュリティの独立したレビュー

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、クラウド事業者が提供するサービスが供給者の提供するサービス等に依存し、あるいは影響を受ける部分を有する場合には、供給者が提供するサービスにおける情報セキュリティマネジメント上の課題等を監視できる対応策を講じることが求められる。また、アグリゲーションサービス事業者は、クラウドサービス全体に対する管理責任を果たすのに必要なレビュー・監査等を実施できる対応策を講じることが求められる。具体的には、実務上以下の対応策を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、提供するサービスが供給者の提供するサービス等に依存し、あるいは影響を受ける部分を有する場合には、供給者が行う独立したレビュー・監査結果等を入手し、その結果をクラウド事業者が行う独立したレビュー・監査に反映させる等の措置を講じること。

(b) アグリゲーションサービス事業者は、供給者が行う独立したレビュー・監査の実施方針について把握し、必要な調整を行うことで、ICT サプライチェーン全体においてレビュー・監査等に係る一貫した方針の適用が必要な範囲を明確にし、これを適用するための措置を講じること。

１８.２.２　情報セキュリティのための方針群及び標準の順守

アグリゲーションサービス事業者は、サービス全体に対する管理責任を果たすために、クラウドサービス全体として適切な情報セキュリティマネジメントのための方針群、標準類等が順守されているかを定期的にレビューすることが求められる。具体的には、実務上以下を実施することが望ましい。

(a) アグリゲーションサービス事業者は、供給者が行う情報セキュリティマネジメントのための方針群、標準類等の順守に係る定期的なレビュー結果を入手し、必要な調整を行うことで、ICT サプライチェーン全体において一貫した定期的レビューを行う範囲を明確にし、各供給者にこれを実施させるための措置を講じること。

１８.２.３　技術的順守のレビュー

ICT サプライチェーンを構成して提供されるクラウドサービスにおいて、供給者のサービス等に係る技術的な順守状況のレビュー結果等を入手する際に、十分な情報等の提供を受けるための措置を講じる必要がある。具体的には、実務上以下を実施することが望ましい。

(a) ICT サプライチェーンを構成して提供されるクラウドサービスにおいては、供給者のサービス等に係る技術的な順守状況のレビュー結果等を入手する際に、機密的な内容が含まれる場合には、クラウド事業者と供給者の間で機密保持契約の締結等、必要な措置を講じること。

Annex 7 クラウド事業者が過度の責任を負わないための注意点

１．IoT 機器のコンポーネントリスクの処理戦略

クラウド事業者が IoT サービスを提供するにあたり、リスク対応の観点から実務上最も重要な選択となるのは、IoT 機器の高いコンポーネントリスクをどのように処理するかである。例えば、人に危害を及ぼすモノのリスクはクラウド事業者にとって未経験であり、多額の賠償責任にどのように備えるかのノウハウも十分ではない。

クラウド事業者が IoT 機器を自ら提供しようとすると、そのコンポーネントリスクを自ら処理して機器を提供することになるため、事業リスクは高い。しかし、多数必要となる IoT 機器を自ら提供できれば大きな事業収益を得ることができる。他方、クラウド事業者が IoT 機器の提供は行わず、推奨に留める場合、IoT 機器のコンポーネントリスクの処理を IoT サービス利用者に移転することとなるため、事業リスクは大きく低減される。しかし、IoT 機器のリース等で得られる事業収益は手放すことになる（図表６参照）。

クラウド事業者が取りうる二つの対極的なリスク処理戦略（①IoT 機器を自ら提供する、②IoT 機器は推奨に留め提供しない）について具体的な理解を助けるため、ユースケースを例示しておく。

【想定例：ハウス栽培向け IoT サービスの開発　－**IoT 機器を自ら提供するケース**】

＜概要＞

1 年を通してハウス栽培の省力化と高品質生産を実現するため、ハウス内の環境データ（温度・湿度、日射量、土壌内の温度・水分量、CO_2 濃度等）を計測して見える化するとともに、集約した環境データの分析結果に基づいて照明、加湿器、暖房機等を遠隔制御する IoT サービスを開発する。

＜事業主体＝IoT サービス利用者との契約者＞

ASP・SaaS 事業者

＜IoT サービス利用者＞

ハウス栽培を行う農家、アグリ事業者等

＜事業連携を図る他の事業者等＞

IoT 機器（センサー、アクチュエータ）のベンダー、IaaS 事業者、IoT 機器運用保守の委託先等

＜IoT 機器の種別＞

センサー：温湿度計、土壌センサー、CO_2 濃度計等

アクチュエータ：照明、加湿器、暖房機及びこれらの遠隔制御装置

＜生じうる事業リスク＞

ハウス栽培中の植物の損害（売り物にならなくなる）に対し、賠償を求められるリスク

＜事業収入＞

センサーとアクチュエータの販売/リース料及び保守料、計測データを分析して見える化する ASP・SaaS の利用料、データ分析結果に基づきアクチュエータを遠隔制御（制御コマンドを提供）する ASP・SaaS の利用料等

＜IoT 機器の提供形態＞

本ケースでは、センサー/アクチュエータの信頼性向上、情報セキュリティ対策等の技術的対策により、事業リスクを十分に低く抑えられるものと期待できる。このため、事業収入を優先し、IoT 機器は自ら提供することを選択する。

＜データ解析アプリケーション＞

ハウス内の環境を分析するデータ解析アプリケーションは、外部の専門研究所と共同開発して使用する。

＜データの品質（精度、欠損等）/可用性/持続性の確保体制＞

ASP・SaaS 事業者が IoT サービス設計時にあらかじめ定めた基準に従って IoT 機器を選定・調達。センサーについては較正を、アクチュエータについては保守を定期的に実施。事業者連携にあたり、全体が協力して IoT 機器の構成管理を実施。

【想定例： 生体/位置情報の計測に基づく労災防止ソリューションの開発 **－IoT 機器の推奨に留め、提供はしないケース**】

＜概要＞

製造ラインの作業者がウェアラブルデバイスを装着して生体/位置情報を計測し、作業者の健康状態・疲労度・位置を分析評価することで、ラインのロボットアームの駆動範囲や当該作業者による制御操作可能範囲を自動的に限定し、作業者を労働事故と操作ミスから守る IoT サービスを開発する。

＜事業主体＝IoT サービス利用者との契約者＞

ASP・SaaS 事業者

＜IoT サービス利用者＞

製造ラインを稼動させる製造業企業

＜事業連携を図る他の事業者等＞

IoT 機器（ウェアラブルデバイス、産業用ロボット/機械）のベンダー、IaaS 事業者

※IoT 機器の運用・保守は IoT サービス利用者の責任で実施

＜IoT 機器の種別＞

センサー：体温、心拍、活動量、血圧等

アクチュエータ：製造ライン（ロボットアーム、制御用コンピュータ等）

＜生じうる事業リスク＞

種々の原因に伴う不適切な制御による労災事故の発生と作業者の死傷

＜事業収入＞

計測データを分析して見える化する ASP・SaaS の利用料、データ分析結果に基づきラインのロボットやコンピュータの制御コマンドを提供する ASP・SaaS の利用料等

＜IoT 機器の提供形態＞

本ケースでは、センサー故障やこれに伴う不適切な制御コマンドの提供、ロボットアームの誤動作等により、ロボットアームが作業者を死傷させるリスクがあり、その責任を自社だけで担うことが難しいと判断される。このため、IoT 機器についてはベンダーや機種の推奨しか行わない。

＜データ解析アプリケーション＞

作業者の健康状態・疲労度・位置を分析評価するデータ解析アプリケーションは自ら保持しているので、データ解析アプリケーションを使用する。

＜データの品質（精度、欠損等）/可用性/持続性の確保体制＞

ASP・SaaS 事業者が IoT サービス設計時にあらかじめ定めた基準に従ってセンサーを選定・推奨。ASP・SaaS 事業者が、クラウド上でデータを取得した際に、その品質（精度、欠損の有無）を、常時自動的に確認。

２．モノのリスクと責任分担の基本

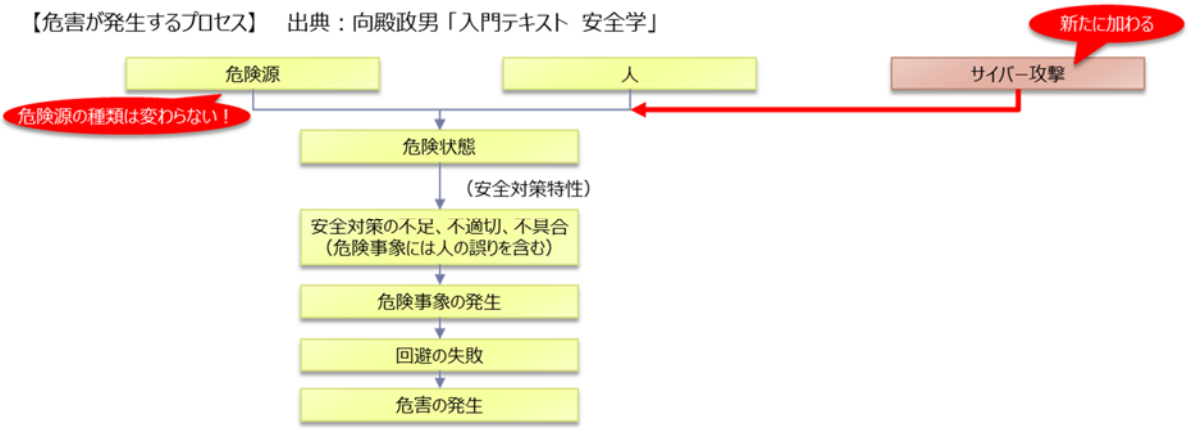
モノのリスクは、クラウドサービスでは見ることがなかった IoT サービスに特徴的なものである。IoT 機器へのサイバー攻撃によって、以下の二つのリスク（以下「セーフティリスク」という。）のどちらか一つでも発現しうる場合は、モノの安全の国際標準に従ったリスク対応が必要になる。

① 人に物理的障害又は健康障害を生じる

② 人の環境を阻害する

セーフティリスクがあるにもかかわらず、サイバー攻撃による危害の発生を食い止める設計（図表 Annex7- 1 参照）がなされていない、または、それでも残留してしまうセーフティリスクについて開示していない IoT 機器の使用は推奨しない。リスク回避を重視する場合は、セーフティリスクがある IoT 機器は初めから使用しない、または、自らがこのような IoT 機器を提供するリスクを負わない（IoT サービス利用者に選定・調達を委ねることでリスクを移転する）という判断もありうる。

図表 Annex7- 1　サイバー攻撃によって危害が発生するプロセス



どうしても、セーフティリスクがある IoT 機器を使用する場合は、IoT 機器ベンダーと協力してサイバー攻撃を対象としたセーフティバイデザインに取り組み、残留しうるセーフティリスクを十分に理解しておくべきである。また、サイバー攻撃により、IoT 機器ベンダーが開示していない残留セーフティリスクが発現した場合は、クラウド側は責任を負わないように、あらかじめ契約で定めておくことが望ましい。

３．クラウド事業者が把握できていない「繋がり」

クラウド事業者が IoT 機器の提供は行わず、推奨に留める場合は、IoT 機器の調達や配置は IoT サービス利用者に任せることが多くなる。このケースでは IoT サービス利用者の裁量が大きくなり、IoT サービス利用者が、IoT サービス提供者であるクラウド事業者が把握していない IoT 機器を繋いでしまいやすくなる。この中に、セーフティリスクが残るものや重要性が高いものが含まれていると、クラウド事業者は想定外の高リスクを抱え込むことになる。

また、工場内などでは、IoT サービス利用者が IoT 機器を調達・配置する場合、利用者がエッジコンピュータを FA ベンダー等から導入することも多い。この場合、クラウド事業者の統制がエッジコンピュータまで及ばないことで、クラウド事業者が「偽者のエッジコンピュータ」に接続させられてしまうリスクが生じてくる。これもクラウド事業者にとっては重大なリスクであるといえる。

一方、IoT サービスでは、外部機関の希望するデータ書式/データ内容に加工された「加工済みデータ」を当該外部機関に提供することがあり、今後はさらに活性化することが見込まれる。また、外部提供されたデータがさらに転得されることも想定される。この際に、外部提供されたデータが、クラウド事業者に把握されることなく知らないうちに、重要性の高い用途（重要インフラ、医療等）に組み込まれていたりすると、不測の高いリスクを背負うことになってしまう。

このように、IoT サービスの場合、サービス提供者であるクラウド事業者が把握できていない「繋がり」により、知らないうちに高リスクを抱えてしまう場合があるので、十分な注意を要する。

４．クラウド事業者が把握できていない「責任分担の空白」

IoT サービスの提供においては、サービス提供主体であるクラウド事業者を中心として、連携事業者や IoT サービス利用者が役割を分担し、この役割に則してサービス提供責任を分担している。しかし、この責任分担にあいまいな所があり、IoT サービスの提供構造の中に「責任分担の空白」が生じていると、事故発生時に、サービス提供主体であるクラウド事業者が「空白部分の責任」を抱えざるを得なくなることが想定される。これによって不測の高いリスクが生じる場合があるため、クラウド事業者は、サービス提供開始以前に十分な対策を取っておく必要がある。

Annex 8【事例集】調査テンプレートの記入例

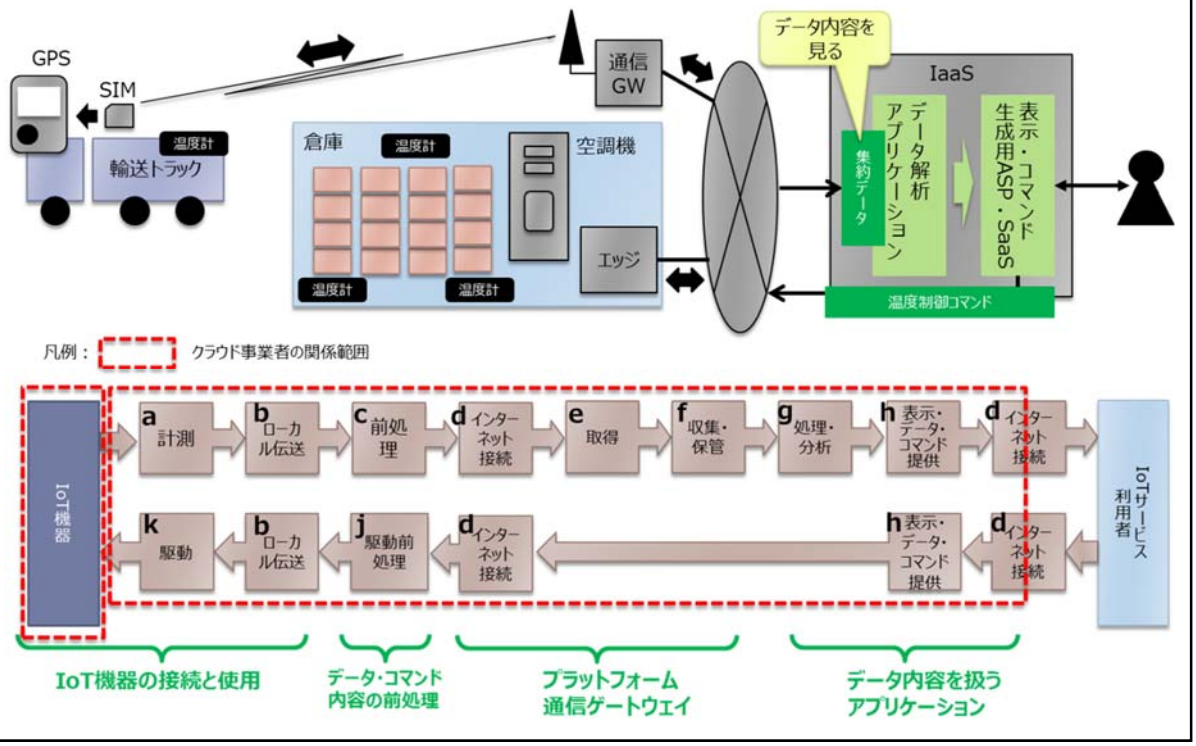
クラウド事業者が自ら提供する IoT サービスにおいて、どこまでが自らの責任範囲であるかを把握するために、図表 16 の調査テンプレートを活用することができる。ここでは、特徴の異なる六つの IoT サービスを事例として、「Ⅳ．４．１．２．クラウド事業者の責任範囲の把握」の図表 16 の記入例を提示する。

【取り上げる事例】

事例番号	事例の名称	業種	IoT サービスを提供する際の構造（図表５参照）	
			番号	構造の概要
1	運送車・倉庫温度監視・制御サービス	物流	2	センサーの計測データをクラウド上のサーバに集めて処理・分析し、その結果を利用して当該サーバ経由で IoT サービス利用者がアクチュエータを制御
2	不動産向け映像クラウド	不動産業	1	センサーの計測データをクラウド上のサーバに集めて処理・分析し、IoT サービス利用者が結果等を表示
3	工作機械の遠隔状態監視	製造業		
4	スマートメーターからのデータ集約	電力		
5	認知症対応型 IoT サービス	介護		
6	ハウス環境の遠隔自動制御	農業	3	センサーの計測データをクラウド上のサーバに集めて処理・分析し、当該サーバが自動的にアクチュエータを制御

事例１．運送車･倉庫温度監視･制御サービス

クール宅配便のような温度管理の要件が厳しい物流形態に対し、一括して温度を監視･制御するサービスを提供する。全てのロールがクラウド事業者の責任範囲である。



【調査テンプレートの記入例】

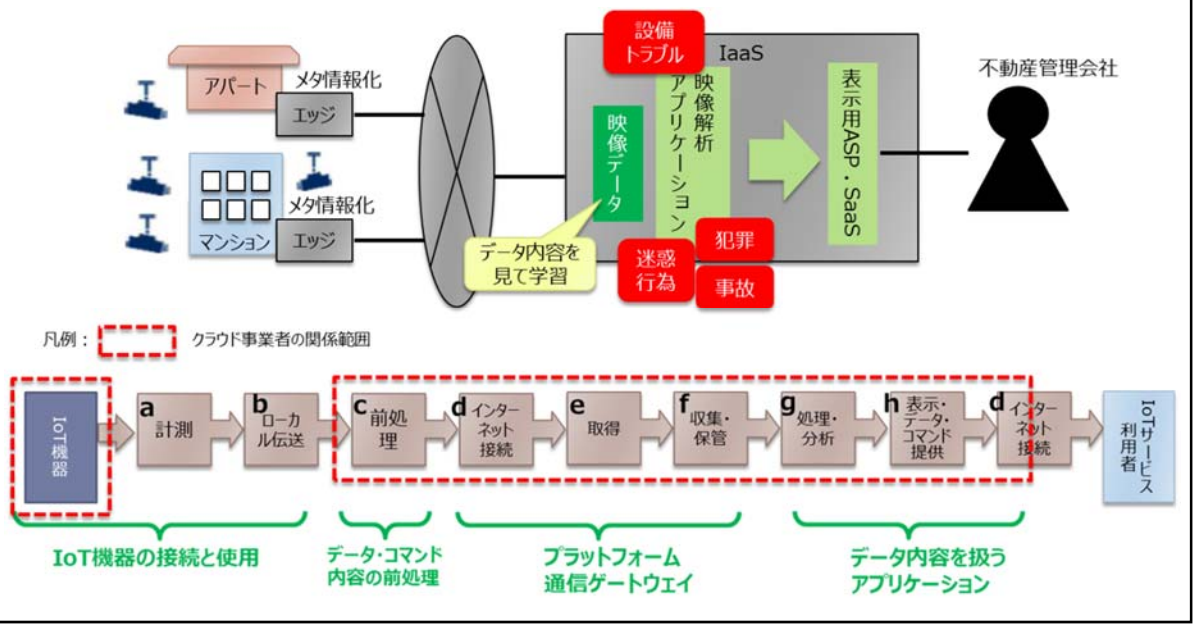
クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者間連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器		○	
			LAN		○	
			ローカルコンピュータ		○	
			エッジコンピュータ		○	
			通信ゲートウェイ		○	
			WAN		○	
			クラウド		○	
			組込みアプリケーション		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		○	
	c 機器等推奨（クラウド事業者以外が機器を提供する場合）	推奨するコンポーネント	IoT 機器		×	
			ローカルコンピュータ		×	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			クラウド		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	
	d 構成管理	全てのクラウド事業者が該当する		○		
	e 契約管理	全てのクラウド事業者が該当する		○		
		データ内容を見てこれに責任を持つ				○
		事業連携先に委託するロール	a 計測		×	×
			b ローカル伝送		×	× *データ内容を見ない場合は記入不要
			c 前処理		×	×
			d インターネット接続		○	○ *データ内容を見ない場合は記入不要
			e 取得		×	×
			f 収集・保管		×	×
			g 処理・分析		×	×
			h 表示・データ・コマンド提供		×	×
			i データ外部提供		× （提供なし）	×

			j 駆動前処理		×	× *データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				○
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			○	
	b ローカル伝送				○	
	c 前処理				○	
	d インターネット接続				×	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				○	
	h 表示・データ・コマンド提供				○	
	i データ外部提供				× （提供なし）	
	j 駆動前処理				○	
	k 駆動				○	

（注）外部データの取得はない

事例２．不動産向け映像クラウド

管理している不動産の監視映像を分析し、設備トラブル・犯罪・迷惑行為・事故等の発生を自動的に検知し、その状況を不動産管理会社に提供するサービスを提供する。不動産会社が監視カメラを用意し、計測・ローカル伝送のロールの責任を持つ。クラウド事業者は、制御に関わりのないその他のロールを責任範囲とする。



【調査テンプレートの記入例】

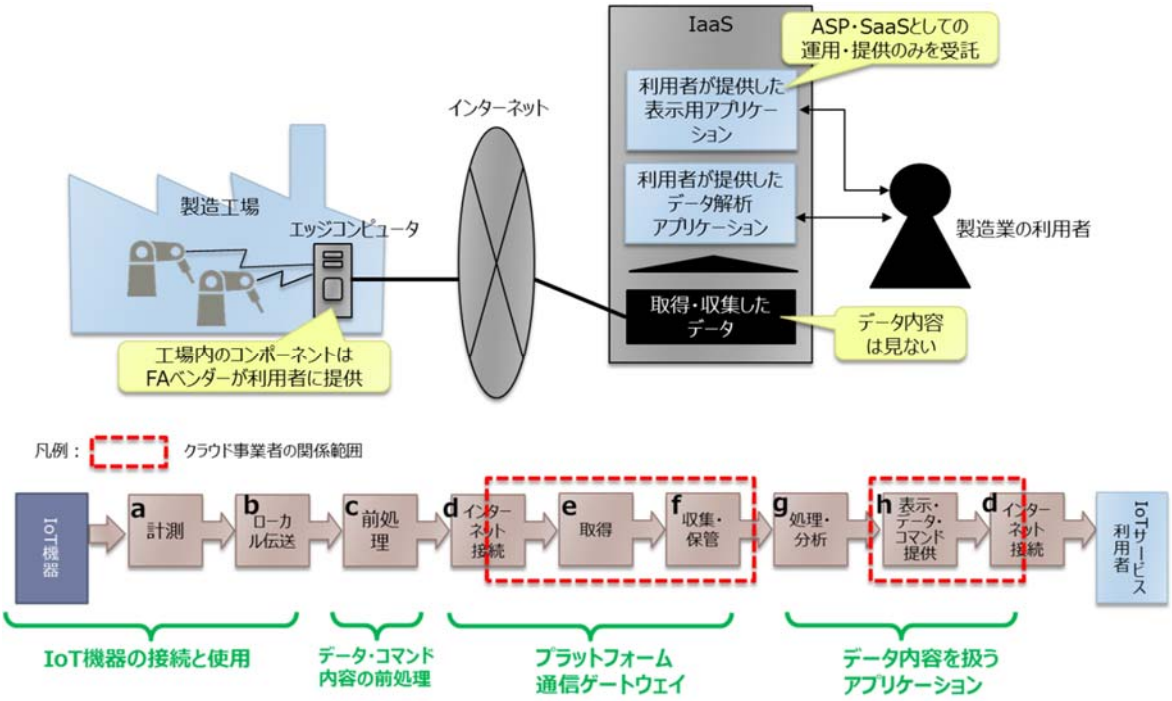
クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者間連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器		×	
			LAN		×	
			ローカルコンピュータ		×	
			エッジコンピュータ		○	
			通信ゲートウェイ		×	
			WAN		○	
			クラウド		○	
			組込みアプリケーション		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		○	
	c 機器等推奨（クラウド事業者以外が機器を提供する場合）	推奨するコンポーネント	IoT 機器		○	
			ローカルコンピュータ		○	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			クラウド		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	
	d 構成管理	全てのクラウド事業者が該当する		○		
	e 契約管理	全てのクラウド事業者が該当する		○		
		データ内容を見てこれに責任を持つ				○
		事業連携先に委託するロール	a 計測		×	×
			b ローカル伝送		×	× *データ内容を見ない場合は記入不要
			c 前処理		○	○
			d インターネット接続		○	○ *データ内容を見ない場合は記入不要
			e 取得		×	×
			f 収集・保管		×	×
			g 処理・分析		×	×
			h 表示・データ・コマンド提供		×	×
			i データ外部提供		× （提供なし）	×

			j 駆動前処理		×	× *データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				○
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			×	
	b ローカル伝送				×	
	c 前処理				×	
	d インターネット接続				×	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				○	
	h 表示・データ・コマンド提供				○	
	i データ外部提供				× （提供なし）	
	j 駆動前処理				×	
	k 駆動				×	

（注）外部データの取得はない

事例３．工作機械の遠隔状態監視

工作機械の各種データを計測し、状態監視保全を支援するサービスを提供する。製造工場内のコンポーネントは FA ベンダーが提供し、データ内容についても FA ベンダーが責任を持つ。したがって、クラウド事業者はデータ内容は見ず、ストレージ提供と、利用者が開発した表示用アプリケーションの、ASP・SaaS としての運用・提供のみを請け負う。



【調査テンプレートの記入例】

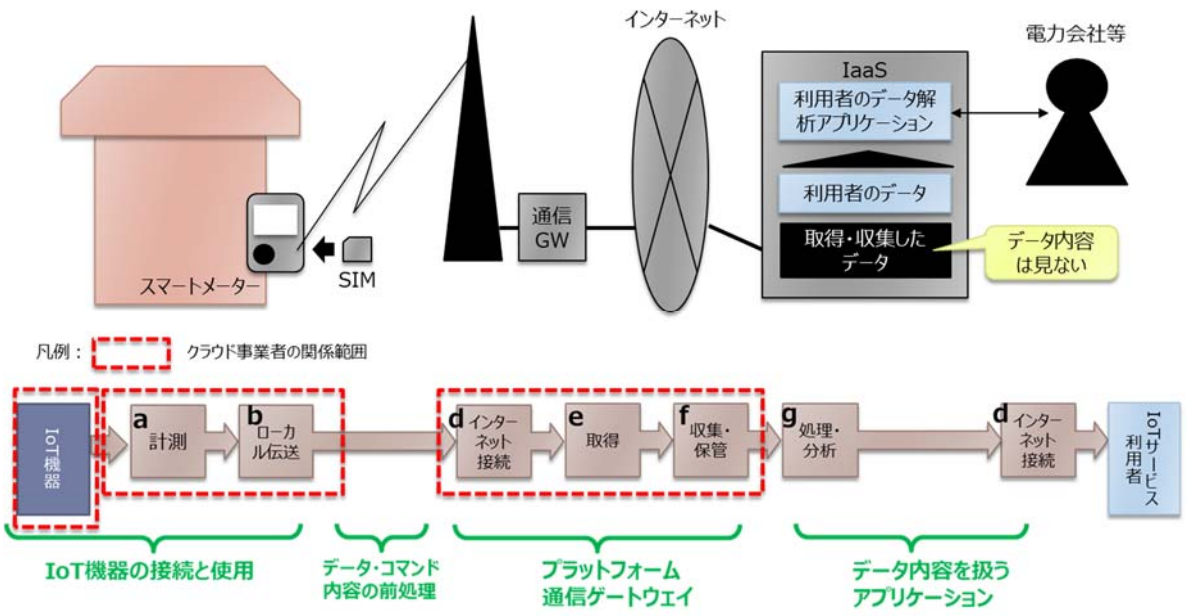
クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者間連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器		×	
			LAN		×	
			ローカルコンピュータ		×	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			WAN		×	
			クラウド		○	
			組込みアプリケーション		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	
	c 機器等推奨（クラウド事業者以外が機器を提供する場合）	推奨するコンポーネント	IoT 機器		×	
			ローカルコンピュータ		×	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			クラウド		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	
	d 構成管理	全てのクラウド事業者が該当する		○		
	e 契約管理	全てのクラウド事業者が該当する		○		
		データ内容を見てこれに責任を持つ				×
		事業連携先に委託するロール	a 計測		×	×
			b ローカル伝送		×	*データ内容を見ない場合は記入不要
			c 前処理		×	×
			d インターネット接続		○	*データ内容を見ない場合は記入不要
			e 取得		×	×
			f 収集・保管		×	×
			g 処理・分析		×	×
			h 表示・データ・コマンド提供		×	×
			i データ外部提供		×（提供なし）	×

			j 駆動前処理		×	*データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				×
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			×	
	b ローカル伝送				×	
	c 前処理				×	
	d インターネット接続				×	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				×	
	h 表示・データ・コマンド提供				○	
	i データ外部提供				× （提供なし）	
	j 駆動前処理				×	
	k 駆動				×	

（注）外部データの取得はない

事例４．スマートメーターからのデータ集約

スマートメーターの計測データを収集してストレージに保管し、電力会社が利用できるようにするサービスである。クラウド事業者は、SIM スロットを持つスマートメーターと SIM を一体的に提供するとともに、モバイル通信路と安全なインターネット伝送を提供し、収集したデータをストレージに蓄積する。電力会社は、自分でデータ解析アプリケーションを用意し、蓄積されたデータを利活用する。



【調査テンプレートの記入例】

クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者間連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器		×	
			LAN		○	
			ローカルコンピュータ		×	
			エッジコンピュータ		×	
			通信ゲートウェイ		○	
			WAN		○	
			クラウド		○	
			組込みアプリケーション		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	
	c 機器等推奨（クラウド事業者以外が機器を提供する場合）	推奨するコンポーネント	IoT 機器		○	
			ローカルコンピュータ		○	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			クラウド		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	
	d 構成管理	全てのクラウド事業者が該当する		○		
	e 契約管理	全てのクラウド事業者が該当する		○		
		データ内容を見てこれに責任を持つ				×
		事業連携先に委託するロール	a 計測		×	×
			b ローカル伝送		×	*データ内容を見ない場合は記入不要
			c 前処理		×	×
			d インターネット接続		×	*データ内容を見ない場合は記入不要
			e 取得		×	×
			f 収集・保管		×	×
			g 処理・分析		×	×
			h 表示・データ・コマンド提供		×	×
			i データ外部提供		×（提供なし）	×

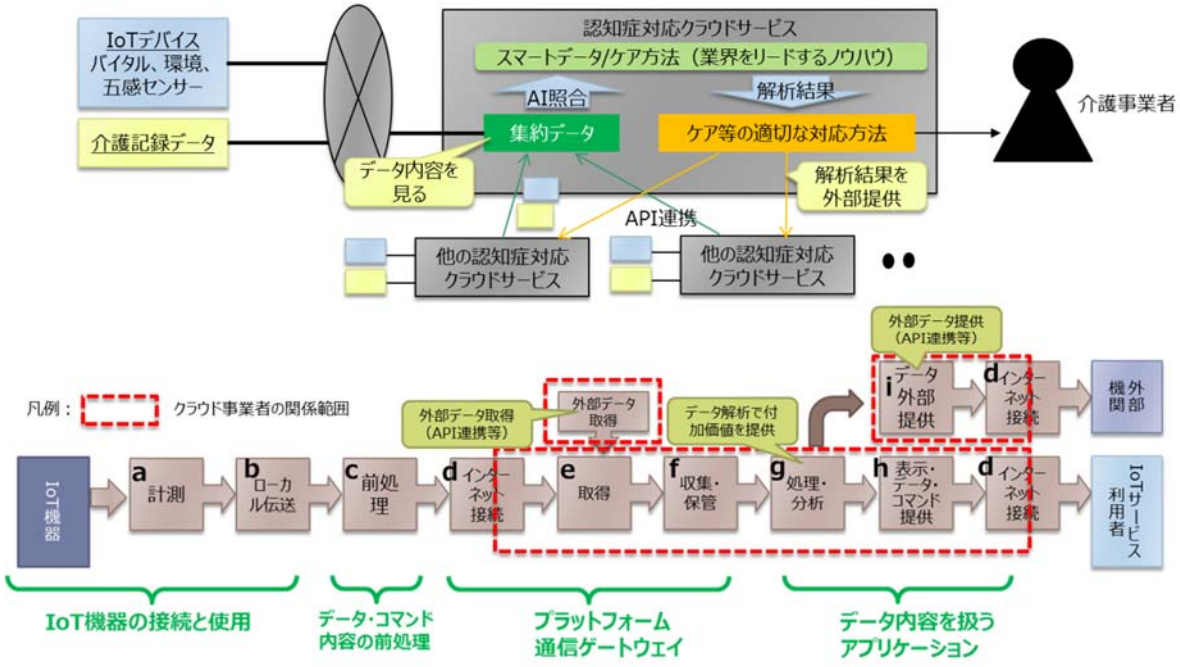
			j 駆動前処理		×	*データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				×
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			×	
	b ローカル伝送				○	
	c 前処理				×	
	d インターネット接続				○	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				×	
	h 表示・データ・コマンド提供				×	
	i データ外部提供				× （提供なし）	
	j 駆動前処理				×	
	k 駆動				×	

（注）外部データの取得はない

事例５．認知症対応型 IoT サービス

業界をリードする認知症対応のための「スマートデータ/ケア方法」の DB を持ち、介護事業者が送付してきた計測データ（バイタル、環境、五感センサー）と介護記録データを、この DB を用いて解析することで、介護事業者に対し、ケア等の適切な対応方法を提供する。データ内容はもちろん見ている。計測、ローカル伝送のロールは介護事業者の責任範囲であり、クラウド事業者は、取得、収集・保管、処理・分析、表示・データ・コマンド提供、データ外部提供等のロールの責任を負う。

また、クラウド事業者は、スマートデータ/ケア方法 DB を活かし、同業他社の外部データを取得して解析を受託し、解析結果としてケア等の適切な対応方法を提供するサービスも同時に提供する。



【調査テンプレートの記入例】

クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者間連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器		×	
			LAN		×	
			ローカルコンピュータ		×	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			WAN		○	
			クラウド		○	
			組込みアプリケーション		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		○	
	c 機器等推奨（クラウド事業者以外が機器を提供する場合）	推奨するコンポーネント	IoT 機器		○	
			ローカルコンピュータ		○	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			クラウド		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	
	d 構成管理	全てのクラウド事業者が該当する		○		
	e 契約管理	全てのクラウド事業者が該当する		○		
		データ内容を見てこれに責任を持つ				○
		事業連携先に委託するロール	a 計測		×	×
			b ローカル伝送		×	× *データ内容を見ない場合は記入不要
			c 前処理		×	×
			d インターネット接続		○	○ *データ内容を見ない場合は記入不要
			e 取得		×	×
			f 収集・保管		×	×
			g 処理・分析		×	×
			h 表示・データ・コマンド提供		×	×
			i データ外部提供		×	×
			j 駆動前処理		×	×

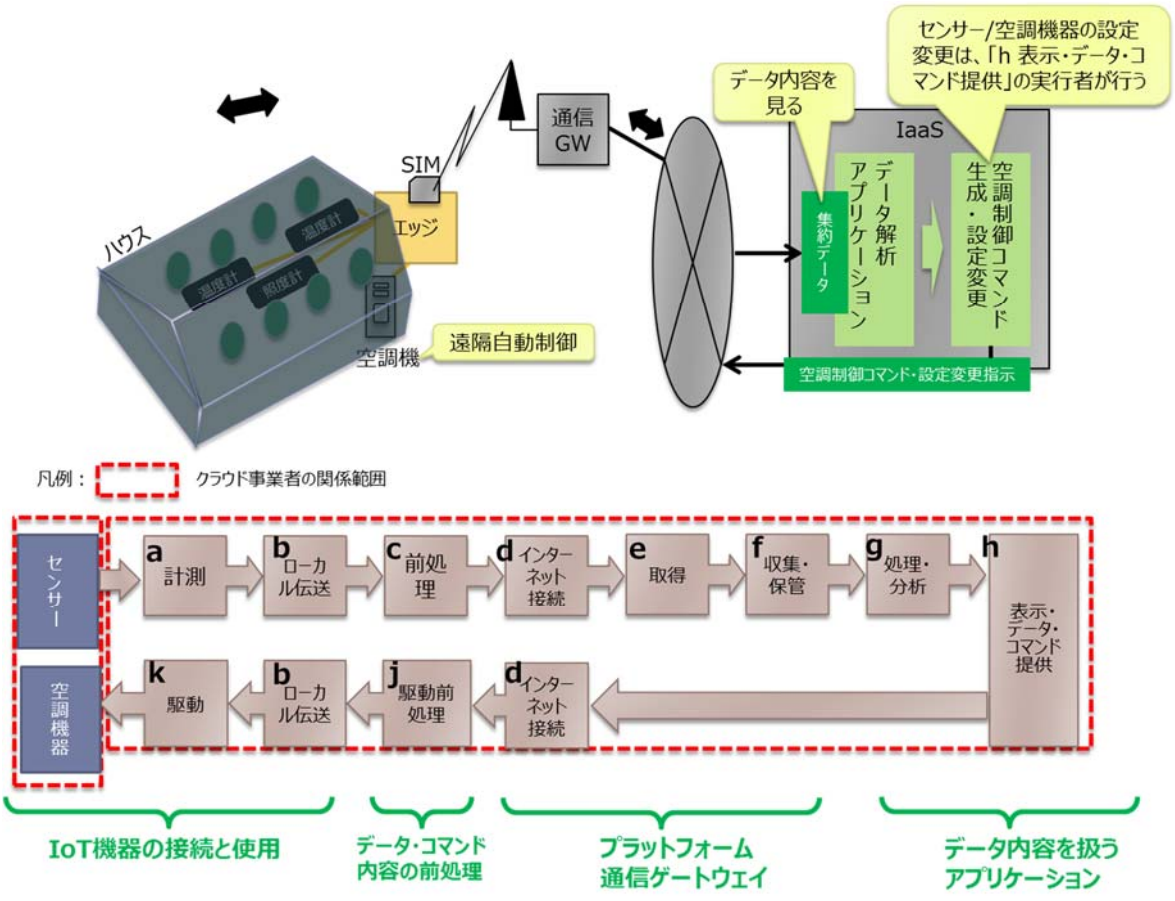
						*データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				○
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			×	
	b ローカル伝送				×	
	c 前処理				×	
	d インターネット接続				×	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				○	
	h 表示・データ・コマンド提供				○	
	i データ外部提供				○	
	j 駆動前処理				×	
	k 駆動				×	

（注）「取得」のロールで、外部データからデータを取得している

事例６．ハウス環境の遠隔自動制御

管理を請け負っている圃場のハウス環境に設置したセンサー（温度計、湿度計、照度計、CO_2 濃度計等）でハウス環境を遠隔から 24 時間自動監視。取得した計測データを分析・処理し、温度・湿度・照度・CO_2 濃度を一定に保つように空調機・照明等を自動制御する。クラウド事業者は全てのロールの実行に責任を持ち、計測データの内容を見てデータ品質を維持する。また、センサー/空調機等の動作設定を行い、適切な自動制御を確保・維持する。

なお、計測データの「ローカル伝送」には、クラウド事業者が（モバイル通信事業者と契約して）提供するモバイル通信を用いる。



【調査テンプレートの記入例】

クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者間連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器		○	
			LAN		○	
			ローカルコンピュータ		○	
			エッジコンピュータ		○	
			通信ゲートウェイ		×	
			WAN		○	
			クラウド		○	
			組込みアプリケーション		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		○	
	c 機器等推奨（クラウド事業者以外が機器を提供する場合）	推奨するコンポーネント	IoT 機器		×	
			ローカルコンピュータ		×	
			エッジコンピュータ		×	
			通信ゲートウェイ		×	
			クラウド		×	
			アプリケーション（表示・データ・コマンド提供、データ解析等）		×	
	d 構成管理	全てのクラウド事業者が該当する		○		
	e 契約管理	全てのクラウド事業者が該当する		○		
		データ内容を見てこれに責任を持つ				○
		事業連携先に委託するロール	a 計測		×	×
			b ローカル伝送		○	○ *データ内容を見ない場合は記入不要
			c 前処理		×	×
			d インターネット接続		○	○ *データ内容を見ない場合は記入不要
			e 取得		×	×
			f 収集・保管		×	×
			g 処理・分析		×	×
			h 表示・データ・コマンド提供		×	×
			i データ外部提供		× （提供なし）	×

			j 駆動前処理		×	× *データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				○
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			○	
	b ローカル伝送				×	
	c 前処理				○	
	d インターネット接続				×	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				○	
	h 表示・データ・コマンド提供				○	
	i データ外部提供				× （提供なし）	
	j 駆動前処理				○	
	k 駆動				○	

（注）外部データの取得はない