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３版）

２０２１年　9月

総務省

(This page is intentionally left blank.)

目次

Ⅰ．序編

Ⅰ．1．はじめに

クラウドサービスの普及及び高度化並びにIoTの実用化に伴い、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。こうした中、多くの自治体や企業が主要なシステムのオンプレミス環境からクラウド環境への移行を進めている。更に、新型コロナウイルス感染症の感染拡大及びそれに伴う人の移動の制限は多くのオフィスワーカーを一夜にしてリモートワーカーに変えただけでなく、教育現場における授業形態を対面授業からリモート授業に変えるきっかけとなっている。これらの企業等における新型コロナウイルス感染症の感染拡大への対応は、クラウドサービスが普及していなければ大きく異なっていたものと思われる。

一方、秘匿性、機密性の高い情報がインターネット上に公開されてしまうケースが後を絶たない。米国のIdentity Theft Resource Centerの調査によると、2020年には米国内で約1100件のセキュリティインシデントによって約3億件のデータが流出した[1]。IPA（独立行政法人情報処理推進機構）[2]やCSA（Cloud Security Alliance）[3]では、2020年の情報セキュリティ10大脅威の第１位に「サイバー攻撃による機密情報の漏洩」を挙げている。SOPHOS White Paper[4]（2020年7月）によると、パブリッククラウドを利用している企業の70%が過去一年にマルウェアやランサムウェアの被害を受けたと報告している。

また、クラウドサービス自体の障害も多数報告されている。2018年9月に発生したFacebookでの5000万件に及ぶアカウント情報の流出は、同社が利用者に提供しているAPI(Videoを投稿するUploader)のバグに起因している。情報流出には至らなかったが、2019年8月に発生したAWSの大規模障害は、AWSを提供する東京リージョンの4箇所あるデータセンターの一つで冷却システムに不具合が発生したため、サーバがオーバーヒートし、仮想マシンおよびストレージに障害が発生したことが原因と報告されている。

更に、CSAが情報セキュリティ10大脅威の2番目として挙げているのが、「設定ミスや不十分な変更管理」である。国内では、最近、クラウドサービスへのアクセス権限の設定不備によって、企業や個人の情報が流出したケースがある。

従来はインフラまでも含めて、クラウドサービス事業者が単独でクラウドサービスをクラウドサービス利用者に提供する形態が多かったが、現在ではインフラや実行環境などの基盤を提供するPaaS/IaaSと、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SaaSに分けて考え、SaaS事業者がPaaS/IaaSを利用してSaaSをクラウドサービス利用者に提供するなどの、クラウドサービス事業者同士が連携してクラウドサービスを提供する事例(サプライチェーンによるクラウドサービ

---

[1] 出典：「2020 in review Data Breach Report」

[2] https://www.ipa.go.jp/

[3] https://cloudsecurityalliance.org/

[4] SOPHOS 社（コンピュータセキュリティのソフトウェアおよびハードウェアを開発・提供する英国のベンダー）が発行した文書（https://www.sophos.com/en-us/labs/technical-papers.aspx）

スの提供)も急増している。

しかしながら、クラウドサービス提供形態の複雑化は、クラウドサービス事業者によるクラウドサービス全体の管理・統制を難しくする要因となり、クラウドサービス事業者とクラウドサービス利用者の責任範囲の考え方にも変化が生じている。この結果、クラウドサービス事業者とクラウドサービス利用者それぞれの責任範囲に対する認識についての齟齬が生じ、セキュリティインシデントの発生をもたらしている。

このようなクラウドサービスを取り巻く環境の変化によって生ずる課題に対応するためには、クラウドサービス事業者及びクラウドサービス利用者のそれぞれの責任範囲において、クラウドサービスを安全・安心に提供・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)を基に、ISMAP管理基準、ISO/IEC27017(2016)及びNIST SP800-53 Rev.5[5]を参照しつつ改定を行った。 なお、IoT サービスリスクへの対応方針については改定せず、「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）」と記載内容は同じである。

[5] 米国立標準技術研究所（NIST:National Institute of Standards and Technology）が公表している連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策を記載した文書

Ⅰ．2. ガイドラインの位置付け

本ガイドラインは、クラウドサービス事業者がクラウドサービスを提供する際に実施することが望ましい情報セキュリティ対策について記載している。クラウドサービス事業者が、提供するクラウドサービスの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、対策事例を提示することに努めている。クラウドサービス事業者は、取り扱うサービスの種類やデータなどを踏まえたリスク、自らの経営規模、利用できるリソース等に応じて本ガイドラインを利用することで、自ら提供するクラウドサービスに適した情報セキュリティ対策を実施することが可能である。また、クラウドサービス利用者は、クラウドサービス事業者との契約や SLA の締結において、本ガイドラインを活用することが可能である。

クラウドサービスの情報セキュリティに関する他の主たるガイドライン類として、

・政府情報システムのセキュリティ評価制度(ISMAP)管理基準(略称:ISMAP 管理基準)
・内閣サイバーセキュリティセンター（NISC）「政府機関の情報セキュリティ対策のための統一基準」(略称:政府統一基準)
・経済産業省「クラウドサービス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」

がある。

ISMAP 管理基準及び政府統一基準は、政府情報システムに求められる情報セキュリティ対策について記載されている。また、ISMAP 管理基準においては、対策の実施主体を SaaS/PaaS/IaaS 等のクラウドサービス事業者として記載している。

本ガイドラインは、地方公共団体及び民間事業者を含むあらゆる主体が利用するクラウドサービスに求められる情報セキュリティ対策を記載しており、その提供主体としては中小規模も含む SaaS/PaaS/IaaS 等の全てのクラウドサービス事業者を想定している。

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情報セキュリティ対策を網羅しており、クラウドサービス事業者が取り扱うクラウドサービスに応じて、実施すべき情報セキュリティ対策に取り組めるようにまとめている。

本ガイドラインを活用することで、以下の四つの効果が見込まれる。

1．本ガイドラインが、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規模のクラウドサービス事業者に対して、独自のリスク分析の負担を軽減し、優先的に取り組むべき対策の指針となる。
2．他のクラウドサービスと連携してサービスを提供する際、サプライチェーンを構成するクラウドサービス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．本ガイドラインが、クラウドサービス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。
4．本ガイドラインが、クラウドサービス利用者がクラウドサービスを利用するにあたって留意すべき情報セキュリティ対策の指針となる。

Ⅰ．4．ガイドラインの全体構成

本ガイドラインは、「Ⅰ．序編」「Ⅱ．共通編」「Ⅲ．SaaS 編」「Ⅳ．PaaS/IaaS 編」「Ⅴ．IoT サービスリスクへの対応方針編」「参考資料 ANNEX1～4」の六編から構成されている。クラウドサービス事業者は、取り扱うクラウドサービス[6]に応じて、必要な編を参照されたい。クラウドサービス利用者は、利用するクラウドサービスに応じて、必要な編を参照されたい。

Ⅰ．序編

本ガイドラインの目的・位置付け・利用方法、クラウドサービス事業者とクラウドサービス利用者の責任範囲、使用している用語の定義を記載している。

Ⅱ．共通編

SaaS 事業者、PaaS 事業者及び IaaS 事業者に共通して求められる情報セキュリティ対策に対する組織的な取組、情報資産の取扱い、契約や雇用における留意事項、開発や保守運用に係る対策等を取りまとめている。

Ⅲ．SaaS 編

SaaS 事業者に求められる情報セキュリティ対策を取りまとめている。

Ⅳ．PaaS/IaaS 編

PaaS/IaaS 事業者やデータセンター等の情報処理施設に求められる情報セキュリティ対策事項を取りまとめている。

Ⅴ．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取りまとめている。なお、記載内容は、「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）」と同じである。

ANNEX1　クラウドサービスのパターン

本ガイドラインでのクラウドサービスのパターン化に関する考え方を記載している。「Ⅱ．共通編」「Ⅲ．SaaS編」「Ⅳ．PaaS/IaaS編」では、このパターンに応じた【評価項目】を記載している。これらの資料についても、適宜参照されたい。

ANNEX2　対策一覧

「Ⅱ．共通編」、「Ⅲ．SaaS編」及び「Ⅳ．PaaS/IaaS編」の情報セキュリティ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のチェックリストとしても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。

---

[6] 本ガイドラインにおける SaaS、PaaS、IaaS の定義については「Ⅰ．８．用語の定義」を参照されたい。

ANNEX3　クラウド事業者が過度の責任を負わないための注意点

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、クラウドサービス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載しているので、適宜参照されたい。

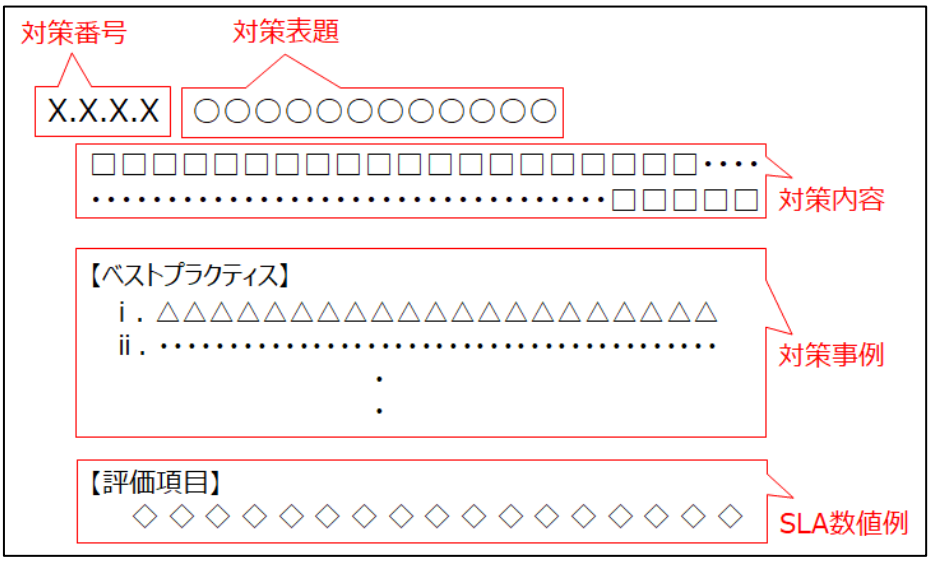
ANNEX4 【事例集】 調査テンプレートの記入例

クラウドサービス事業者の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．ガイドラインの読み方と利用方法

本ガイドラインでは、下記の記述凡例で示すように、対策内容を記載している。また、必要に応じて【ベストプラクティス】、【評価項目】及び対策参照値(SLA数値例)を付記している。なお、ベストプラクティスは、優先度の高い順で記載している。

記載凡例



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、それぞれの読者において、以下の手順に従って利用することが望ましい。

■クラウドサービス事業者(又はクラウドサービス利用者)における経営者や組織長等

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。

ⅱ. 『Ⅱ．共通編』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。

ⅲ. 『Ⅴ．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。

■SaaS事業者(又はSaaS利用者)のセキュリティ担当者・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. 自らが提供又は利用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、『Ⅱ．共通編』及び『Ⅲ．SaaS編』に基づいて対策を実施する。
「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、評価項目の対策参照値を目安とし、対策の実施レベルを判断することも可能である。

iii. 『Ⅴ．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。

■PaaS/IaaS事業者(又はPaaS/IaaS利用者)のセキュリティ担当者・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. 自らが提供又は利用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、『Ⅱ．共通編』及び『Ⅳ．PaaS/IaaS編』に基づいて対策を実施する。
「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、評価項目の対策参照値を目安とし、対策の実施レベルを判断することも可能である。

iii. 『Ⅴ．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。

なお、『Ⅱ．共通編』、『Ⅲ．SaaS編』及び『Ⅳ．PaaS/IaaS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選択し、実施されたい。

１．対策項目

クラウドサービス事業者が実施すべき情報セキュリティ対策。監査・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．対策の「基本」・「推奨」

クラウドサービスは、基幹系業務システムからソーシャルネットワーク(SNS)に至るまで多岐に渡り、様々な産業・業種で利用されている。

したがって、必要とされる情報セキュリティ対策は、クラウドサービスが取り扱う情報資産の種類と重要性、情報セキュリティに対する脅威の大きさ、情報セキュリティインシデントが発生した場合のサービス及び業務への影響度合い等によって異なる。

しかしながら、どのようなクラウドサービスでも基本的に実施することが求められる、ベースラインとも言うべき情報セキュリティ対策がある。本ガイドラインでは、このような対策を「基本」対策と称している。また、クラウドサービスでは、高い「機密性」「可用性」「完全性」が求められるサービスがある。このようなサービスでは、「基本」対策に加え、より高度な情報セキュリティ対策を実施することが望ましい場合がある。本ガイドラインでは、このような対策を「推奨」対策と称している。

・「基本」対策：クラウドサービスを提供するにあたり、基本的に実施することが求められる情報セキュリティ対策。Ⅱ章～Ⅳ章では【基本】と表記。

・「推奨」対策：より高いセキュリティレベルが求められるクラウドサービスを提供するにあたり、「基本」対策に加えて付加的に実施することが望まれる情報セキュリティ対策。Ⅱ

章～Ⅳ章では【推奨】と表記。

クラウドサービス事業者において、限られたリソースの中で、最大限の効果が発揮できるように、「基本」・「推奨」の考え方を参考に、サービスに応じて必要な情報セキュリティ対策を選択し、実施されたい。

３．ベストプラクティス

クラウドサービス事業者やクラウドサービス利用者が対策を実施するにあたっての参考となるように、具体的な実施手法や注意すべき点について、優先度の高い順に記載している。

４．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項目。SLA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

対策項目を実施する上での目安となる評価項目の値。SLAの合意数値として活用されることも想定される。

※なお、「４．評価項目」及び「５．対策参照値」については、クラウドサービスに要求されるセキュリティレベルによって異なることから、4種類のサービスパターン（詳細は「P191～193 ANNEX1　クラウドサービスのパターン」を参照）ごとに設定している。

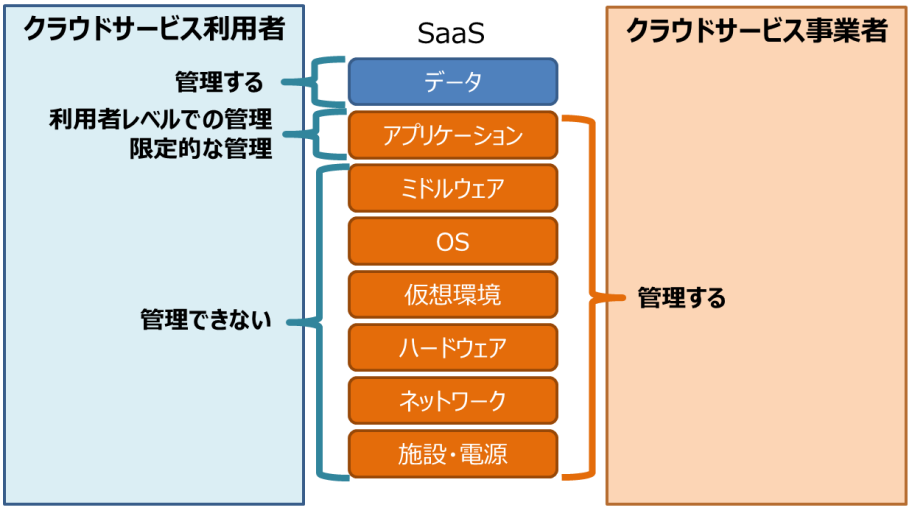
Ⅰ．6．クラウドサービス事業者とクラウドサービス利用者の責任

クラウドサービスは、組織外部での利用が前提であり、クラウドコンピューティング環境によって管理する内容も異なるため、従来のオンプレミス環境での情報セキュリティ対策に加え、クラウドコンピューティング環境特有の情報セキュリティ対策が必要となる。しかしながら、クラウドサービスを利用するにあたってのリスクに対する認識度合いによっては、機能の追加や改修などのバージョンアップ等の頻度が多いクラウドサービス特有のリスクへの対応が疎かになり、情報セキュリティ管理が不十分になりがちである。クラウドサービスのセキュリティに関する設定が十分でなかったために、意図せず、クラウドサービスで管理している機密情報を無認証状態で外部に公開してしまい、機密情報を漏洩させてしまった事例が相次いで報告されている。

クラウドサービスは市場で普及してからの歴史が長く、技術も成熟化しつつあるにもかかわらず、セキュリティインシデントが多発している要因の一つとして、クラウドサービス利用者が対応すべき情報セキュリティ対策が曖昧になっていることが挙げられる。例えば、クラウドサービス事業者は、クラウドサービスで管理する情報資産を外部からアクセスするための権限設定機能を提供し、クラウドサービス利用者は、外部からアクセスを許可するかの判断を行い、そのための権限を設定する。クラウドサービスの情報セキュリティを高めるためには、クラウドサービス事業者とクラウドサービス利用者が協力して、クラウドサービスに対する責任を共有する必要がある。この責任を共有するという考え方(責任共有モデル)を多くのクラウドサービス事業者が採用している。ただし、責任共有モデルにおけるクラウドサービス事業者とクラウドサービス利用者の責任範囲・内容は一律に決まるものではなく、クラウドサービスの内容やクラウドサービス利用条件・環境ごとに、両者で責任範囲と内容について合意し、契約で明示することが重要である。また、双方の責任範囲において、クラウドサービス利用者がセキュリティ上のリスクを判断できるように、クラウドサービス事業者はクラウドサービス利用者に対して、クラウドサービスの内容やクラウドサービス利用条件・環境等について適切に情報提供をする必要がある。

本ガイドラインでは、この責任共有モデルを採用し、各クラウドサービスモデル(SaaS/PaaS/IaaS)における責任分担の一般的な考え方を示す。この責任分担は、クラウドサービスの実装方式(パブリッククラウド、プライベートクラウド等)には依存しない。

Ⅰ．6．１．SaaS における管理と責任共有



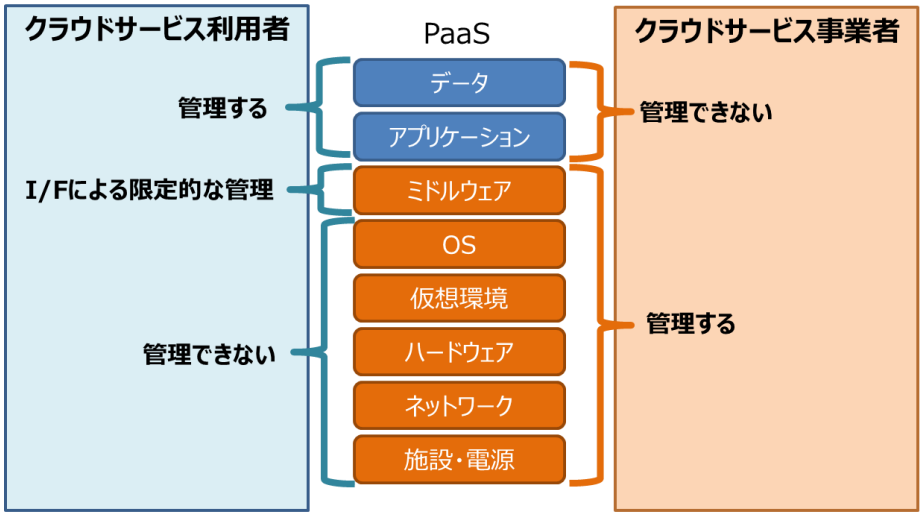
※ランタイムはミドルウェアの一部と位置付けています

SaaS を利用するクラウドサービス利用者は、クラウドサービス事業者が提供するアプリケーションを利用するためのデータやアプリケーション上で生成したデータの管理（データに対する編集・削除等の行為）をする権限と責任を有する。アカウント管理などの限定的な管理権限をクラウドサービス事業者から付与され、外部からのアクセス権限を設定する場合がある。

（注）アプリケーションのバージョンアップや機能の追加により、設定が不適切なものとなってしまい、情報漏洩に至ることが想定されるため、クラウドサービス事業者は、クラウドサービス利用者がバージョンアップによる情報セキュリティへの影響を見定めることができるよう、適切な情報提供を行う必要がある。

クラウドサービス事業者は、契約・SLA に基づくサービスをクラウドサービス利用者に提供するために、アプリケーション層以下の実装、設定、更新及び運用を管理するとともに、クラウドサービス利用者に限定的な管理権限等を提供する場合がある。

Ⅰ．6．2. PaaS における管理と責任共有



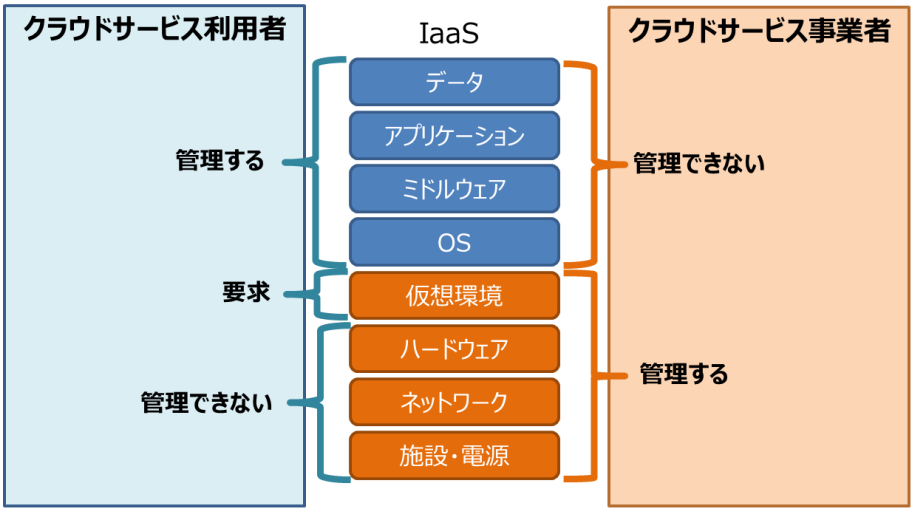
※ランタイムはミドルウェアの一部と位置付けています

PaaSを利用するクラウドサービス利用者は、クラウドサービス事業者との契約・SLAに基づいて、アプリケーションの開発、アプリケーションに対する管理を行う。クラウドサービス利用者は、クラウドサービス事業者が提供するプログラミング環境やSQL[7]等のユーティリティインターフェースを利用してミドルウェア層を利用する。また、クラウドサービス利用者は、クラウドサービス事業者が提供するセキュリティ機能（データバックアップ機能、認証機能、データ暗号化機能、ファイアウォール機能、ログ管理機能等）を正しく理解して設定する必要がある。

クラウドサービス事業者は、ミドルウェア層以下の実装、設定、更新及び運用を管理するとともに、データセンター内のネットワークインフラも管理する。

[7] SQL(Structured Query Language)はミドルウェア層にあるデータベースを操作するための言語。データベースにデータを検索、挿入、更新、削除等する際に利用する。

Ⅰ．6．3. IaaS における管理と責任共有



※ランタイムはミドルウェアの一部と位置付けています

IaaS を利用するクラウドサービス利用者は、クラウドサービス事業者との契約・SLA に基づき、ゲスト OS[8]等が動作するための仮想環境の構築と管理をクラウドサービス事業者に要求できる。クラウドサービス利用者は、仮想環境上で動作している OS を含めたすべてのソフトウェアの管理を行う。OS やミドルウェア層での障害対応や、ミドルウェアに対するパッチ適応やぜい弱性対応などは、クラウドサービス利用者の責任となる。

クラウドサービス事業者は、仮想環境層以下の実装、設定、更新及び運用を管理するとともに、データセンター内のネットワークインフラも管理する。

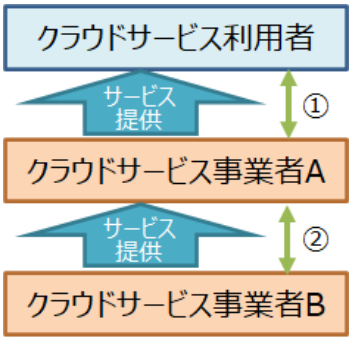
[8] 一つの物理コンピュータ上で別のコンピュータをエミュレートする仮想環境において、仮想環境で動いている OS のこと。 物理コンピュータ上で動いている OS はホスト OS と称す。例えば、Windows 上で Mac を動かす場合、ホスト OS が Windows、Mac がゲスト OS となる。ゲスト OS を動かすためには、必要な環境設定をホスト OS に施す必要がある。

Ⅰ．7．サプライチェーン

クラウドサービスの特徴の一つに、サプライチェーンが複雑になることが多いという点がある。例えば、クラウドサービス利用者が、SaaS 事業者が提供しているアプリケーションを利用している場合、クラウドサービス利用者は SaaS 事業者のアプリケーションだけを利用していると考えがちだが、SaaS 事業者は、他クラウドサービス事業者の PaaS を利用している可能性がある。このような場合、クラウドサービス利用者が SaaS 事業者にしか預けていないと考えている情報が PaaS 事業者に渡っていることがある。クラウドサービスの情報セキュリティ対策は、サプライチェーンを構成するクラウドサービス事業者（サプライチェーン事業者）も含めた対策が必要となる。また、クラウドサービスの情報セキュリティ対策のレベルは、サプライチェーンを構成する各事業者が提供するサービスの情報セキュリティ対策レベルの内、最も低いレベルとなる。したがって、クラウドサービスの情報セキュリティ対策のレベルを上げるには、サプライチェーンを構成する各事業者の責任範囲を明確にした上で、各事業者が提供するサービスの情報セキュリティ対策のレベルを上げる必要がある。

本節では、クラウドサービス利用者、クラウドサービス事業者及びサプライチェーン事業者との関係モデルを「垂直連携型」と「水平連携型」の二つのモデルに大別して、クラウドサービス利用者、クラウドサービス事業者及びサプライチェーンを構成する各事業者との役割と責任の分担[9]について記載する。

Ⅰ．7．１．垂直連携サプライチェーン１



① クラウドサービス事業者 A は、クラウドサービス利用者との契約者であることから、クラウドサービス利用者との契約に基づき、提供するクラウドサービス全体の管理責任を負う。

② クラウドサービス事業者 B は、クラウドサービス事業者 A との契約に基づきクラウドサービス事業者 B の管理責任の一部をクラウドサービス事業者 A に委譲する。クラウドサービス事業者 A

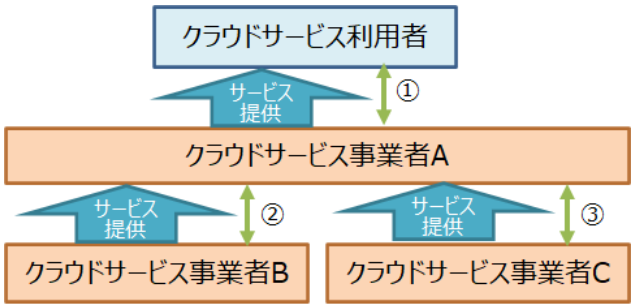
[9] クラウドサービスの提供にあたって複数のクラウドサービスが関与する場合のクラウドサービス事業者の責任に対する考え方は、NISP SP800-53 Rev.5 のサプライチェーンリスク（SR ファミリ）に準じている。

は、クラウドサービス事業者 B との契約に基づきクラウドサービス事業者 B の管理責任の一部を引き継ぐ。

提供しているクラウドサービスにおいて、クラウドサービス事業者 B の管理範囲に帰する問題が発生した場合は、クラウドサービス事業者 A とクラウドサービス事業者 B との契約に基づき、対処する。

事例：A が SaaS 事業者、B が PaaS 事業者という一般的なクラウドサービス提供形態

Ⅰ．7．２．垂直連携サプライチェーン２



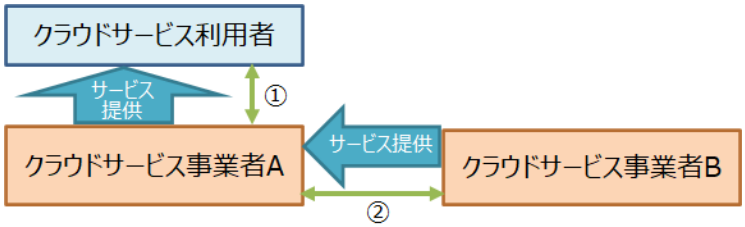
① クラウドサービス事業者 A は、クラウドサービス利用者との契約者であることから、クラウドサービス利用者との契約に基づき、提供するクラウドサービス全体の管理責任を負う。

②③ クラウドサービス事業者 B 及び C は、クラウドサービス事業者 A との契約に基づきクラウドサービス事業者 B 及び C の管理責任の一部をクラウドサービス事業者 A に委譲する。クラウドサービス事業者 A は、クラウドサービス事業者 B 及び C との契約に基づきクラウドサービス事業者 B 及び C の管理責任の一部を引き継ぐ。

クラウドサービス利用者に提供しているクラウドサービスにおいて、クラウドサービス事業者 B 又は C の管理範囲に帰する問題が発生した場合は、クラウドサービス事業者 A はクラウドサービス事業者 B 又は C との契約に基づき、対処する。

事例：A が SaaS 事業者、B 及び C が PaaS 事業者というクラウドサービス提供形態
(障害対策等で複数の PaaS を利用して、同一の SaaS サービスを提供するケース等が該当する。)

Ⅰ．7．３．水平連携サプライチェーン１



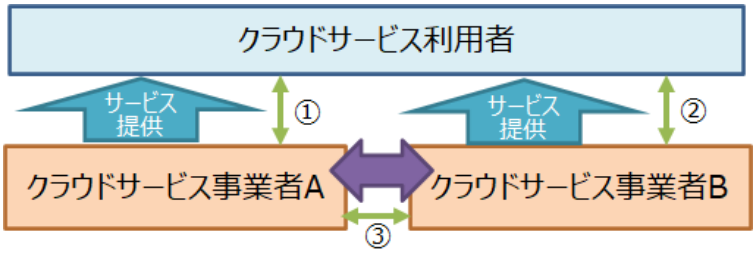
①クラウドサービス事業者 A は、クラウドサービス利用者との契約者であることから、クラウドサービス利用者との契約に基づき、提供するクラウドサービス全体の管理責任を負う。

② クラウドサービス事業者 B は、クラウドサービス事業者 A との利用契約に基づきクラウドサービスをクラウドサービス事業者 A に API 連携として提供する。 クラウドサービス事業者 B の管理責任は、クラウドサービス事業者 A との利用契約範囲内であり、その一部をクラウドサービス事業者 A に委譲することはできない。

提供しているクラウドサービスにおいて、クラウドサービス事業者 B の管理範囲に帰する問題が発生した場合は、クラウドサービス事業者 A とクラウドサービス事業者 B との契約に基づき、対処する。

事例：A 及び B が SaaS 事業者というクラウドサービス提供形態(自社の旅費申請/精算サービスに、他社の乗り換えサービスを API 連携で提供するケース等が該当する。)

Ⅰ．7．４．水平連携サプライチェーン２



①② クラウドサービス事業者A及びBは、クラウドサービス利用者との契約者であることから、クラウドサービス利用者との契約に基づき、提供するクラウドサービス全体の管理責任を負う。

③ クラウドサービス事業者A及びB間の連携部分に帰する問題が発生した場合は、クラウドサービス事業者AとB間との契約に基づき、対処する。

事例：A及びBがPaaS事業者というクラウドサービス提供形態 (A及びBもデータセンター事業者で、AとBとの間でデータ等の同期を行っているケース等が該当する。)

クラウドサービス事業者は、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クラウドサービス利用者と契約を締結することが求められる。

Ⅰ．８．用語の定義

アクセス制御(JIS Q 27000 を基に定義)

資産へのアクセスが、事業上及びセキュリティ要求事項に基づいて認可及び制限されることを確実にする手段。

暗号鍵

暗号アルゴリズムへのパラメータを構成するビット列、整数又は文字列

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。

外部組織

サプライチェーン事業者やクラウドサービス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。

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、クラウドサービス事業者とISP間、クラウドサービス事業者とサプライチェーン事業者間、クラウドサービス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。

稼働率

サービス時間帯に占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。

可用性(JIS Q 27000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。

完全性(JIS Q 27000を基に定義)

正確さ及び完全さの特性。

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。

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 “Safety aspects: Guidelines for their inclusion in standards”を参考に定義）。

機密性(JIS Q 27000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。

脅威(JIS Q 27000を基に定義)

システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。

供給者

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

（例）データ連携：クラウドサービス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サービス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。

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。

クラウドコンピューティング

共用の構成可能なコンピューティングリソース（ネットワーク、サーバ、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデル。実装モデルとして、プライベートクラウド、コミュニティクラウド、パブリッククラウド及びハイブリッドクラウドがある。

クラウドサービス

クラウドコンピューティングが提供するサービス。SaaS/PaaS/IaaSのサービスモデルがある。

クラウドサービス事業者

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。以降、事業者と略す。

クラウドサービス利用者

クラウドサービスを利用する法人又は個人。以降、利用者と略す。

クリアスクリーン

自席のコンピュータを意図せず第三者に操作されたり画面を盗み見されたりしないように対策を行うこと。

クリアデスク

離席時に書類や記録メディア、コンピュータ本体などを机の上や周辺に放置しないよう求めること

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。

コミュニティクラウド

クラウドコンピューティングは共通の関心事を持つ、複数の組織からなる特定のクラウドサービス利用者の共同体の専用使用のために提供される。クラウドコンピューティングの所有、管理及び運用は、共同体内の１つ又は複数の組織、第三者、若しくはそれらの組み合わせにより行われ、設置場所はその組織の施設内又は外部となる。

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。

サイバー脅威ハンティング機能

従来の情報セキュリティ対策では検知が難しいサイバー脅威に対し、それらのリスクが存在することを前提にネットワーク内部におけるログやプロセスを解析し、不審な振る舞いを検出することでサイバー攻撃を検知して防ぐというセキュリティ対策手法。

サーバ証明書

「通信の暗号化」「Webサイトの運営者・運営組織の実在証明」の2つの役割をもつ電子証明書で、サーバ証明書は、認証局と呼ばれる組織が発行する。

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。

サービス時間帯

契約サービス時間から定期保守時間を差し引いたもの。

サプライチェーン

クラウドサービス事業者と供給者、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、各クラウドサービス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

サプライチェーン事業者

サプライチェーンを構成する事業者。

システムコンポーネント

システムやプログラムを構成する部品で、特定の機能を単体で完結しているが、単体では使用せず、他のプログラムから呼び出されたり、他のプログラムと連結したりして使用する。

従業員

クラウドサービス事業者に所属し、当該クラウドサービス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。

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。

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。

情報資産

情報そのものだけではなく、情報を取り扱う仕組みまでを対象とするもので、書類、データだけでなく、ハードウェア、ソフトウェア、設備、ファームウェア（媒体など）、要員、文書が対象となる。

情報処理施設

クラウドサービス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。

情報セキュリティ(JIS Q 27000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。

情報セキュリティインシデント(JIS Q 27000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。

情報セキュリティ事象(JIS Q 27000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対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。

情報セキュリティ責任者

情報セキュリティ責任者は社内の情報資産に対する管理責任者で、情報セキュリティ対策の策定、指示、社内各組織への指導、情報セキュリティインシデント発生時の対応などに責任を有する。情報セキュリティ責任者は、経営陣が任命する。

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、クラウドサービス事業者の設備を防護するための機器。

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。

情報提供

情報公開、又は情報開示の実施。

ぜい弱性(JIS Q 27000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。

セキュリティ特性

情報の機密性、完全性及び可用性のこと。他に真正性、責任追跡性、否認防止及び信頼性のような特性を含めることもある。

セッション

通信の開始から終了まで。クライアントとサーバで通信を行う場合であれば、クライアントからサーバへ接続した時点でセッションが始まり、サーバから切断するとセッションが終了する。

セッション識別子

通信中の利用者が使用するセッションを識別するための固有の識別情報。

セッションのロック

ユーザが作業を中断してシステムから離れる時間が一時的であることからログアウトしたくない場合に行われる一時的なアクションのこと。なお、セッションロックは、セッションがアクティブである場合に実行され、通常はオペレーティングシステムレベルで行われる一方、アプリケーションレベルで行われる場合もある。

多要素認証

2つ以上の異なる要素の組み合わせにより、強度を高める認証方式のこと。要素は以下の3種類。

・利用者が知っている情報（例：ID・パスワードなど）
・利用者が所持している情報（例：ICカードなど）
・利用者自身の情報（例：生体情報）

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。

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。クラウドサービス事業者とクラウドサービス利用者のどちらに所属するかは問わない。

二段階認証

利用者確認時の認証を2回に分けて行う認証方式のこと。

ハイブリッドクラウド

二つ以上の異なるクラウドサービス実装モデル（プライベート、コミュニティ又はパブリック）

の組み合わせによるクラウドコンピューティングのこと。各クラウドサービス実装モデルは独立の存在であるが、標準化された、あるいは固有の技術で結合され、データとアプリケーションの移行可能性を実現している。

パブリッククラウド

広く一般の自由な利用に向けて提供されるクラウドコンピューティングのこと。クラウドコンピューティングの所有、管理及び運用は、企業組織、学術機関又は政府機関、若しくはそれらの組み合わせにより行われ、設置場所はそのクラウドプロバイダの施設内となる。

ヒープ領域

コンピュータプログラムが利用するメモリ領域の種類の一つで、実行時に任意のタイミングで確保や解放が可能なメモリ領域のこと。

秘密認証情報

パスワードや暗号鍵のこと。

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。

フォレンジック

情報セキュリティインシデント発生時に原因究明などのためにコンピュータに残された証拠を調査すること。

物理的セキュリティ境界

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。

プライベートクラウド

複数のクラウドサービス利用者から成る単一組織の専用利用のために提供されるクラウドコンピューティングのこと。クラウドコンピューティングの所有、管理及び運用は、その組織、第三者若しくはそれらの組み合わせにより行われ、設置場所はその組織の施設内又は外部となる。

ベースライン構成

特定の時点において正式に確立され、その後の変更などの基準となる構成。

ペネトレーションテスト

インターネットに接続されているコンピュータシステムのセキュリティレベルをチェックするために、意図的にサイバー攻撃を実施して、システムに侵入することが出来るぜい弱性がないか確認するテスト。

ポリシー施行

ポリシーによるネットワークトラフィックの制御方法を確認及び分析すること。ログを確認した後、ポリシールールを調整して特定のトラフィックを許可又はフィルタしたり、設定が適切でないポリシーのトラブルシューティングを行ったりする。

マルウェア

コンピュータウイルス、ワーム、トロイの木馬、スパイウェアなどの不正かつ有害な動作を行う意図で作成された「悪意のこもった」ソフトウェアの総称

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。

要配慮個人情報

不当な差別、偏見その他の不利益が生じないように取扱いに特に配慮を要する記述等が含まれる個人情報（個人情報保護法第2条第3項）。取得にあたっては、原則として、あらかじめ本人の同意が必要。人種、信条、社会的身分、病歴、前科、犯罪被害情報等のほか、障害、健康診断結果、調剤情報等も該当する。

リスク(JIS Q 27000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）。

リスクアセスメント(JIS Q 27000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。

リスク分析(JIS Q 27000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。

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。クラウドサービス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。

ASP（Application Service Provider）

本ガイドラインでは、SaaSと同定義とする。それに伴い、「ASP/SaaS」という表現を「SaaS」に統一する。

IaaS（Infrastructure as a Service）

サービスの形で提供されるインフラストラクチャ。IaaS事業者は、演算機能、ストレージ、ネットワーク他の基礎的コンピューティングリソースを配置し、クラウドサービス利用者に提

供する。

IDS･IPS（Intrusion Detection System･Intrusion Prevention System）

IDS･IPSはシステムやネットワークに対する不正行為を検出するシステム。IDSは、不正行為を検出後、指定されたアクション（例えばシステム管理者に通知するなど）を起こすものの防御措置は取らない。IPSは、検出後直ちにトラフィックを遮断するなどの防御措置を取る。

IoT（「IoTセキュリティガイドライン ver1.0」[10]を基に定義）。

情報社会のために、既存若しくは開発中の相互運用可能な情報通信技術により、物理的若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。

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。

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。

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。

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。

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。

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（クラウドサービス事業者を含む。）の対応付けを示したもの。

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。

---

[10] IoT 推進コンソーシアム、総務省、経済産業省が合同で平成 28 年 7 月に策定

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。

PaaS（Platform as a Service）

サービスの形で提供されるプラッフォーム。PaaS事業者は、クラウドのインフラストラクチャ上で、アプリケーションを開発、実装、稼働できるようにするために、ミドルウェア等を提供する。

SaaS（Software as a Service）

サービスの形で提供されるソフトウェア。SaaS事業者は、クラウドのインフラストラクチャ上で稼働するアプリケーションをクラウドサービス利用者に提供する。

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載したもの。

Ⅰ．９．参考文献

- JIS Q 27000:2019 (ISO/IEC 27000:2019)
  「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
- JIS Q 27001:2014 (ISO/IEC 27001:2013)
  「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」
- JIS Q 27002:2014 (ISO/IEC 27002:2013)
  「情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範」
- JIS Q 27017:2016 (ISO/IEC 27017:2015)
  「情報技術―セキュリティ技術―ＪＩＳ　Ｑ　２７００２に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」
- JIS X 9401：2016
  「情報技術―クラウドコンピューティング―概要及び用語」
- JIS X 9501-1：2019
  「情報技術－クラウドコンピューティング－サービスレベル合意書（ＳＬＡ）の枠組－第１部：概要及び概念」
- NIST SP800-53 Rev5
  “Security and Privacy Controls for Information Systems and Organizations”
- NIST SP800-130
  “Framework for Designing Cryptographic Key Management Systems”
- NIST SP800-144
  “Guide Lines on Security and Privacy in Public Cloud Computing”
- NIST SP800-145
  “The NIST Definition of Cloud Computing”
- NIST SP800-146
  “Cloud Computing Synopsis and Recommendations”
- 政府情報システムのセキュリティ評価制度(ISMAP)管理基準(略称:ISMAP 管理基準)
- 政府機関の情報セキュリティ対策のための統一基準（平成 30 年度版）

Ⅱ．共通編

Ⅱ．１．情報セキュリティへの組織的取組の基本方針

クラウドサービスは、クラウドサービス利用者(以降、利用者と略す)の情報資産を預かるサービスである。利用者の情報セキュリティ対策は、クラウドサービス事業者(以降、事業者と略す)の情報セキュリティ対策に大きく依存している。したがって、事業者は、利用者の情報セキュリティ対策を確実にするために、情報や機能の提供によって、利用者を支援する必要がある。

Ⅱ．１．１．組織の基本的な方針を定めた文書

【目的】

情報セキュリティに関する経営陣の方向性と姿勢を、事業上の要求事項及び関連する法令・規則に則って提示する。

Ⅱ．1．１．１．【基本】 方針の作成・承認・配布

事業者は、組織全体での情報セキュリティに関する取組についての基本的な方針、役割、責任等を定めた文書を作成し、経営陣の承認及び署名等を経て、組織内及び関係する組織に配布すること。

【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適切に公表し、通知する。
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載を含める。
   a) 情報セキュリティの定義、目的及び適用範囲
   b) 情報セキュリティの重要性についての経営陣の考え方
   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) 組織及び関連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. 基本方針を定めた文書、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。

iii. 事業者は、利用者のデータへのアクセス及び保護を考慮して、情報セキュリティ方針を拡充する。

iv. 事業者は、調査及びフォレンジックを支援するための、違反の通知及び情報共有の指針を

考慮して、情報セキュリティ方針を拡充する。

Ⅱ．1．１．２．【基本】 方針の変更

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や不適合が生じた場合（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。事業者は、経営陣の承認の下で方針の改定等を実施し、組織内及び関係する組織に通知すること。

【ベストプラクティス】

ⅰ． 事業者は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。

ⅱ． 事業者は、必要な場合には、情報セキュリティマネジメントの変更を行う。

Ⅱ．1．１．３．【推奨】 文書保護

事業者は、情報セキュリティに関する基本的な方針を定めた文書を、不正な開示による漏洩や変更等から保護すること。

Ⅱ．2．情報セキュリティのための組織

クラウドサービスの利用は、他の組織が提供するシステム環境を利用して情報処理を行うことを意味する。したがって、利用者はクラウドサービスの利用にあたっては、自らがどの範囲までの責任を負うかについて明確にする必要がある。事業者は、利用者との間で、各々の情報セキュリティの役割と責任の範囲を、利用者と合意し、契約として文書化する必要がある。

Ⅱ．2．１．内部組織

【目的】

組織内において情報セキュリティの実施及び運用を統制するための管理上の仕組みを確立する。

Ⅱ．2．１．１.【基本】 情報セキュリティ責任者

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する。更に、組織全体にわたる情報セキュリティに責任を持つ情報セキュリティ責任者を任命し、人員・資産・予算等のリソース面で積極的な支援・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、関連する役割を定める。
ii. 組織の規模によっては、取締役会などが 情報セキュリティ責任者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、内部の情報セキュリティ専門技術者又は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。
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。

Ⅱ．2．１．２.【基本】 システム一覧

情報セキュリティ責任者は、組織が保有、提供するシステム、アプリケーション及びクラウドサービスの一覧を作成し、全ての責任者を定めるとともに、個々の組織の職務記述書にセキュリティとプライバシーに関する役割と責任を記載すること。

【ベストプラクティス】

i. 個人を特定できる情報を処理するすべてのシステム、アプリケーション、クラウドサービスの一覧を作成し、維持・管理する。
ii. 情報資産の管理、バックアップ及び復元のような情報資産に関連する運用に責任をもつ当事者を定める。

Ⅱ．2．１．３．【基本】相反する職務と責任の分離

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、相反する職務及び責任範囲は、分離すること。

【ベストプラクティス】

i. 許可されていない状態又は検知されない状態で、一人で資産に対してアクセス、修正又は使用ができないようにする。

ii. 作業を始めることと、その作業を認可することとを分離する。

Ⅱ．2．１．４．【推奨】リスク管理戦略

情報セキュリティへの侵害が、業務、情報資産、個人、他の組織及びサプライチェーンへもたらす脅威に対するリスクを管理するために、組織全体の包括的なリスク管理戦略を策定する。リスク管理戦略は、定期的又はクラウドサービスの提供に係る変更が生じた場合（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。

【ベストプラクティス】

i. 個人を特定できる情報を処理する情報技術の開発又は利用する前、若しくは個人を特定できる情報の新しい収集を開始する前に、システム、アプリケーション、又はクラウドサービスがプライバシーに与える影響を評価する。

ii. システム、アプリケーション又はクラウドサービスの重要度を分析して、重要なシステムコンポーネントと機能を特定する。

iii. システムやクラウドサービスへの侵入痕跡を検索又は既存の制御を回避する脅威を検出、追跡及び妨害するサイバー脅威ハンティング機能を導入する。

Ⅱ．2．１．５．【推奨】テスト、トレーニング及びモニタリング

組織の情報システムに関連するテスト、トレーニング及びモニタリングを計画し、継続的に実施すること。また、当該計画をレビューし、組織の情報セキュリティに関する基本方針に適合しているかを確認し、必要に応じて見直しを行うこと。

Ⅱ．2．１．６．【推奨】組織内苦情管理

組織の情報セキュリティ施策とプライバシーの取組に対する従業員からの苦情、懸念又は質問を受け取り、対応するための仕組みを構築すること。

Ⅱ．2．2．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おけるセキュリティ対策を確実にする。

Ⅱ．２．２．１．【基本】モバイル機器の利用方針

モバイル機器を業務で用いることによって生じるリスクを管理するために、モバイル機器の利用方針を策定し、その方針を実施するために必要な情報セキュリティ対策を講じること。

【ベストプラクティス】

i. モバイル機器を用いる場合、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、特別な注意を払う。

ii. モバイル機器の方針には、保護されていない環境においてモバイル機器を用いた作業のリスクを考慮に入れるとともに、次の事項を考慮する。

a) モバイル機器の登録

b) 物理的保護についての要求事項

c) ソフトウェアのインストール制限

d) モバイル機器のソフトウェアのバージョン及びパッチ適用に対する要求事項

e) 情報サービスへの接続の制限

f) アクセス制御

g) 暗号化

h) マルウェアからの保護

i) 遠隔操作による機器の無効化、データの消去又はロック

j) 業務情報のバックアップ

k) ウェブサービス及びウェブアプリケーションの使用

iii. モバイル機器に格納され、処理される情報に対する認可されていないアクセス又は漏えいを防止するために、暗号技術の使用や秘密認証情報の使用を行う。

iv. モバイル機器は、紛失や盗難から、物理的に保護されること。

v. モバイル機器の盗難又は紛失の場合の対策のために、法規制、保険及び組織のセキュリティ要求事項を考慮した手順を確立する。

vi. モバイル機器を用いる要員に対する教育・訓練を計画し実施する。

Ⅱ．２．２．２．【基本】テレワーキングでの情報保護

テレワーキングでアクセス、処理及び保存する情報資産を保護するための方針を策定し、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. テレワーキングを許可する組織は、テレワーキングを行う場合の条件及び制限を定めた方針を策定し文書化する。

a) 建物及び周辺環境の物理的セキュリティを考慮に入れた、テレワーキングの場所における物理的セキュリティ

b) 次を考慮した、通信のセキュリティに関する要求事項

- 組織の内部システムへの遠隔アクセスの必要性
- 通信回線からアクセスし、通信回線を通過する情報の取扱いに慎重を要する度合い
- 内部システムの取扱いに慎重を要する度合い

c) 個人所有の装置で情報を処理及び保管できないようにする仮想デスクトップへのアクセスの提供

d) 住環境を共有する者（例えば、家族、友人）による情報資産又は資源への認可されていないアクセスの防止

e) 訪問者による装置及び情報へのアクセスに関する規則及び手引

f) 家庭のネットワークの使用及び無線ネットワークサービスの設定に関する要求事項又は制限

g) 個人所有の装置の上で開発した知的財産権に関する論争を防ぐための方針及び手順

h) 個人所有の装置へのアクセス（装置のセキュリティ検証のためのもの、又は調査期間中に行うもの）

i) 従業員又は外部の利用者が個人的に所有する装置上のクライアントソフトウェアの使用許諾について、組織が責任をもつことになる場合のソフトウェアの使用許諾契約

j) マルウェアに対する保護及びファイアウォールの要件

k) 脅威情報に応じた段階的な動的アクセス制御

ii. テレワーキングを行う場合に考慮すべき指針及び取決めには、保険の用意を含める。

iii. テレワーキングを行う場合に考慮すべき指針及び取決めには、バックアップ及び事業継続のための手順を含める。

Ⅱ．３．サプライチェーンに関する管理

事業者がサプライチェーンを構成する事業者からクラウドサービスの提供を受けて、利用者にクラウドサービスを提供する場合、利用者に提供するクラウドサービスの情報セキュリティ水準は、いずれかの事業者が提供するクラウドサービスの内の最も低い水準となる。

事業者がサプライチェーン事業者のサービスを利用して、利用者にクラウドサービスを提供する場合には、自社の情報セキュリティ水準達成のために、サプライチェーン事業者に自社が目標とする情報セキュリティ水準を提示し、各事業者の立場や環境を考慮したリスク管理を行うことが重要である。

Ⅱ．３．１．サプライチェーン事業者間の合意

【目的】

サプライチェーンの情報セキュリティと情報資産の保護を確実にする。

Ⅱ．３．１．１.【基本】 リスク対策と文書化

サプライチェーン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リスク対策及びサービスレベルを文書化するとともに、サプライチェーン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. 情報セキュリティに係る取決めをサプライチェーン事業者が確実に実施するように、契約やSLAを締結する。

Ⅱ．３．１．２.【基本】 サービスの監視

サプライチェーン事業者が提供するクラウドサービスを定常的に監視・レビューし、運用に関する記録及び報告を常に実施すること。また、定期的に監査を実施することについて、サプライチェーン事業者と合意し文書化すること。

【ベストプラクティス】

i. サプライチェーン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、ログ記録により監査できるようにする。

Ⅱ．３．１．３.【基本】 リスク評価とレビュー

サプライチェーン事業者が提供するシステム、システムコンポーネント、クラウドサービスに関連するリスクを評価及びレビューすることについて、サプライチェーン事業者と合意し文書化すること。

Ⅱ．３．１．４.【基本】 関連情報の保護

システム、システムコンポーネント、クラウドサービスに関するサプライチェーン関連の情報を保護することについて、サプライチェーン事業者と合意し文書化すること。

Ⅱ．３．１．５．【基本】 侵害通知

サプライチェーンのセキュリティ侵害に関する通知について、その手順を確立し、サプライチェーン事業者と合意し文書化すること。

Ⅱ．３．１．６．【基本】 変更管理

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に伴う、サプライチェーン事業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、手順及び対応策の保守及び改善を含む）を管理することについて、サプライチェーン事業者と合意し文書化すること。

Ⅱ．３．１．７．【推奨】 耐タンパー性と検出

システム、システムコンポーネント、クラウドサービスの改ざん防止プログラムを実装し、情報資産の完全性を保証することについて、サプライチェーン事業者と合意し文書化すること。

Ⅱ．３．１．８．【推奨】 システム又はシステムコンポーネントの検査

改ざんを検出して情報資産の完全性を保証するために、システム、システムコンポーネント又はクラウドサービスをランダムに検査することについて、サプライチェーン事業者と合意し文書化すること。

【ベストプラクティス】

i. 製品又はクラウドサービスの機能を維持するために重要な構成要素を特定する。特に重要な構成要素がサプライチェーンの外で作られる場合には注意し、検査を強化する。

ii. 重要な構成要素及びその供給元の追跡を可能とする。

Ⅱ．３．１．９．【推奨】 システムコンポーネントの信頼性

偽造されたシステムコンポーネントがシステムやクラウドサービスに侵入することを検出及び防止する手段を実装することについて、サプライチェーン事業者と合意し文書化すること。

Ⅱ．３．１．１０．【基本】 システムコンポーネントの廃棄

データ、ドキュメント、ツール又はシステムコンポーネントを廃棄する方法を確立するとともに、廃棄方法についてサプライチェーン事業者と合意し文書化すること。

Ⅱ．３．２．サプライチェーン事業者の選定

【目的】

サプライチェーン事業者の情報セキュリティ対策を確実にする。

Ⅱ．３．２．１．【基本】 選定・契約

サプライチェーン事業者のリスクからクラウドサービスを保護するために、状況に応じて最も適した取得・調達・契約方法を採用すること。

【ベストプラクティス】

i. サプライチェーン事業者が提供するサービスの一部を下請負に出す場合には、サプライチェーン全体のセキュリティ要求事項を伝えるようにサプライチェーン事業者に要求する。

ii. 提供される製品が期待どおりに機能し、予期しない又は好ましくない特性を持たないという保証を得る。

Ⅱ．４．情報資産の管理

利用者は、クラウドコンピューティング環境で保持する自らのデータを情報資産として特定することが必要である。利用者のデータが情報資産としての特定から漏れると、情報資産を管理する役割や責任が不明確となり、情報セキュリティインシデントが発生するリスクが高くなる。したがって、事業者は、情報資産に対する保護の責任を明確にするために、利用者のデータ及び関連するクラウドサービス派生データを識別し、利用者と管理責任について合意する必要がある。

Ⅱ．４．１．情報資産に対する責任

【目的】

組織が取り扱う情報資産には、資産価値の低い情報資産(例えば、企業の HP に掲載されている企業の所在地や電話番号、拠点情報等)もあれば、顧客情報(個人情報含む)や製品技術情報のように価値の高い情報資産がある。組織にとって資産価値のある保護すべき情報資産を特定し、適切な保護の責任を定める。

Ⅱ．４．１．１.【基本】 管理責任者

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）を明確にした上で管理するとともに、文書化すること。

【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。

ii. 管理責任者は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。

Ⅱ．４．１．２.【基本】 事業者間の引継ぎ

クラウドサービス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。クラウドサービス利用者によるクラウドサービス選定の自由を守るため、事業者は預託された情報を他のクラウドサービスに引き継ぐか否かに関して、予め利用者と合意し、文書化すること。

【ベストプラクティス】

i. 事業者は、返却、除去及び引き継ぐ対象となる利用者の情報資産をあらかじめ特定し利用者と合意し文書化する。

ii. 引き継ぐ情報資産の真正性を確認する方法、引継ぎ方法及び引き継ぐ情報資産に対するクラウドサービ事業者の責任について、利用者と予め合意し文書化する。

Ⅱ．４．１．３．【基本】 バックアップ

情報資産、ソフトウェア及びシステムのバックアップは、利用者と合意されたバックアップ方針に従って、事業者が定期的に実施し、バックアップ内容を検査すること。また、事業者は、利用者にバックアップ機能の仕様を提供すること。

【ベストプラクティス】

i. バックアップ機能の仕様には、下記内容を含める。
   - バックアップ範囲及びスケジュール
   - 暗号化を含むバックアップ手法及びデータ書式
   - バックアップの保管場所
   - バックアップデータ保持期間
   - バックアップデータの完全性の検証手順
   - バックアップからのデータの復旧に要する手順及び時間
   - バックアップ機能の試験手順

Ⅱ．４．１．４．【推奨】 当初目的との一致

時間の経過とともに、当初の目的や提供機能の範囲外のサービス及び機能をサポートする場合があるが、情報資産の使用目的が、当初の使用目的と一致していることを確認すること。

【ベストプラクティス】

i. 情報資産の使用状況を分析することにより、潜在的な情報漏洩を特定する。

Ⅱ．４．２．情報の分類

【目的】

組織が所有する情報資産の重要性に応じて、情報資産の適切なレベルでの保護を確実にする。

Ⅱ．４．２．１．【基本】 資産目録

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、機密性や重要性の観点から情報資産を分類した上で、資産目録を作成し、維持すること。

【ベストプラクティス】

i. 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をとる。
ii. 情報資産の分類方法と各情報資産の管理責任者を定め文書化する。
iii. 情報資産の保護のレベル（機密性・完全性・可用性）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、文書化する。本ガイドラインでは、サービスパターンを以下の様に分類している。情報資産の保護レベルをこのサービスパターンに合わせるという考え方もある。

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	中	高	高
4	中	高	中

iv. 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。

Ⅱ．４．２．２．【基本】データ識別

事業者は、利用者のデータ及びクラウドサービスから派生したデータを明確に識別すること。

【ベストプラクティス】

i. 情報資産の分類結果を、従業員に対して明示する。

ii. 情報資産の分類及び保護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。

iii. 外部組織からの文書に付いている分類は、組織での定義と異なることがある。名称が同じか又は類似していたとしても、その解釈には注意を払う。

Ⅱ．４．２．３．【基本】 情報資産の取扱い

情報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。

【ベストプラクティス】

i. 情報資産の分類ごとに、安全な取扱い手順（処理・出力・保存・伝達・秘密解除・破棄等）を定める。

Ⅱ．４．３．情報セキュリティポリシーの遵守、点検及び監査

【目的】

組織が策定した情報セキュリティポリシーに基づいた情報セキュリティ対策の実行を確実にする。

Ⅱ．４．３．１．【基本】 レビュー

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に、定期的に及び脅威の変化や設定・構成変更等の状況変化に応じてレビュー及び見直しを行うこと。また、組織の情報セキュリティのための方針群及び標準に関し、システムや提供するクラウドサービスが、定めに従って技術的に遵守されていることをレビューすること。

【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。レビューは、半年ごとに実施することが望ましい。

ii. 管理責任者は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。

Ⅱ．４．３．２．【基本】 点検・監査

クラウドサービスの提供に用いるシステムが、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、定期的に検証・監査すること。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、実施すること。

【ベストプラクティス】

i. 点検・監査は、十分な技術力及び経験を持つ内部の者又は必要に応じて外部の専門家の監督の下で行う。

ii. システム、システムコンポーネント又は提供するクラウドサービスに対するセキュリティ侵害テストを組織が定めた頻度で実施する。

Ⅱ．４．４．アクセス管理

【目的】

企業や組織の情報資産及び情報処理施設へのアクセスを制限する。

Ⅱ．４．４．１．【基本】 アクセス制御方針

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。また、情報及び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。

Ⅱ．４．４．２．【基本】 アクセス制御

事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス及び利用者データへのアクセスを、利用者が制限できるようにアクセス制御を提供すること。

【ベストプラクティス】

i. クラウドサービスへのアクセスを利用者が管理出来るようにするため、事業者は、利用者に、ユーザの登録及び登録削除機能とその仕様を提供する。

ii. 利用者が、クラウドサービスへのアクセス及び利用者のデータへのアクセスを出来るようにするため、事業者は、利用者に、アクセス制御を提供する。

iii. 特権アクセス権の割当て及び利用を制限し管理するとともに、利用者の実務管理者がその役割を行えるように、利用者が特定するリスクに応じた十分に強い認証機能を事業者が提供する。

iv. 事業者は、秘密認証情報を割り当てる手順及び利用者が秘密認証情報を管理する手順(ユーザ認証手順を含む)について、利用者に情報を提供する。

Ⅱ．４．４．３．【基本】ユーティリティプログラムの使用

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(データベースの中身を強制的に書き換えることが出来る機能や一時的にポートを開放する機能等)の使用は、制限し、厳しく管理すること。また、事業者は、クラウドサービス内で利用される全てのユーティリティプログラムのための要求事項を特定すること。

Ⅱ．４．４．４．【基本】プログラムソースコードへのアクセス

プログラムソースコードへのアクセスは、制限すること。

Ⅱ．４．４．５．【基本】 アクセス制御となりすまし対策

利用者及びシステム管理者等のアクセスを管理するために、適切な認証方法、特定の場所や装置からの接続を認証する方法等によって、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. システム管理者、ネットワーク管理者、サプライチェーンの事業者等が運用・管理・保守等の目的で遠隔から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、情報セキュリティ対策に従って、適切な認証方法を利用し、なりすまし対策を行う。

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を保存する。

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認証を採用する。

【評価項目】

a. 利用者のアクセス認証方法

パターン	参考値
1	多要素認証
2	多要素認証
3	一要素認証(ID+パスワード認証)
4	一要素認証(ID+パスワード認証)

Ⅱ．４．５．構成管理

【目的】

アプリケーションやシステムの変更を体系的に扱うことで、アプリケーションやシステムの完全性を長期に渡って担保する。

Ⅱ．４．５．１．【基本】 構成管理のポリシーと手順

目的・適用範囲・役割・責任・経営コミットメント・組織間の調整・コンプライアンスを取り扱う構成管理ポリシー及び「構成管理」対応策の実施を容易にするための手順を策定し文書化すること。

Ⅱ．４．５．２．【推奨】 ベースライン構成

システムの最新のベースライン構成を把握・文書化すること。ベースライン構成には、システムコンポーネント（PC、サーバ、ネットワークコンポーネント、インストールされているソフトウェアパッケージ・OS 等の現在のバージョンとパッチ情報、設定項目等）、ネットワークの接続形態及びシステム構成内のそれらのコンポーネントの論理的な配置に関する情報を含む。

【ベストプラクティス】

i. ベースライン構成を把握するために構成管理ツールやネットワーク管理ツール等を利用する。

Ⅱ．４．５．３．【推奨】 構成変更管理

構成管理の対象となるシステムに対する変更について定めるとともに、変更内容をレビューし、セキュリティへの影響を考慮した上で変更を許可すること。また、変更に関する関連の活動を監査し、レビューすること。

【ベストプラクティス】

i. 稼働しているシステムに対して変更を実施する前に、それらの変更をテストし、結果を承認して文書化する。

ii. ベースライン構成品が一つでも不正に変更された場合には、システムの処理を停止する、選択されたシステム機能を停止する、あるいは組織の職員に警告を発する／報告する。

Ⅱ．４．５．４．【推奨】 変更に対するアクセス制限

システムに対する変更に関して、物理的／論理的なアクセス制限を定義・文書化・承認のうえ実施すること。

【ベストプラクティス】

i. ソフトウェアコンポーネントやファームウェアコンポーネントに、承認された証明書を使用した電子署名がない限りインストールを許可しない。

ii. 選択されたシステムコンポーネントと情報に対するすべての変更は、資格のある二人の個人による二重の承認を要求する。

Ⅱ．４．５．５．【推奨】 設定項目

運用上の要求事項に適合し、最も制限された運用を実現するためのセキュリティ設定に関するチェックリストを使用して、システムに導入されている製品の設定項目を把握し文書化すること。設定項目とは、システムのハードウェアコンポーネント、ソフトウェアコンポーネント又はファームウェアコンポーネントの値を変更できるパラメータのこと。

Ⅱ．４．５．６．【推奨】 ソフトウェアの使用制限

契約上の取り決めと著作権法に従ってソフトウェアと関連ドキュメントを使用するとともに、ライセンスの数によって保護されるソフトウェアと関連ドキュメントの使用をモニタリングし、それらが複製されないようにすること。

Ⅱ．４．５．７．【推奨】クラウドサービス利用者によるソフトウェアのインストール

利用者によるソフトウェアのインストールを管理するためのポリシーを確立するとともにポリシーが遵守されていることをモニタリングすること。

【ベストプラクティス】

i. 利用者がインストールしたソフトウェアが許可されていない場合、アラートを出す。

ii. ソフトウェア及びファームウェアコンポーネントをインストールする際、それらが承認されたデジタル署名がされていることを確認する。

Ⅱ．４．５．８．【推奨】 情報の場所

情報の場所と、情報が処理及び保存されるシステムコンポーネントを特定して文書化すること。また、個人を特定できる情報がどのように処理されているかについて文書化すること。

Ⅱ．５．従業員に係る情報セキュリティ

クラウドサービスには、クラウドサービス特有のリスクがある。このリスクに対応するために情報セキュリティに関する基本方針が策定され、その方針に基づく役割や責任を果たすために、情報セキュリティ対策や手順を関係者に周知する必要がある。このため、事業者及び利用者内でそれぞれの役割を担う従業員に対して、クラウドサービス特有のセキュリティに対して意識向上を図るための啓発、教育及び訓練を実施する必要がある。

Ⅱ．５．１．雇用前

【目的】

雇用予定の従業員が求められる責任を理解し、その役割の実施を確実にする。

Ⅱ．５．１．１.【基本】 雇用契約

雇用予定の従業員(就業形態に関わらず)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. 雇用条件では、次の事項を明確に記載する。
   a) 情報セキュリティに関する基本的な方針
   b) 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
   c) 従業員の法的な責任と権利
   d) 従業員が担うべき情報資産に対する責任
   e) 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

ii. 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。

Ⅱ．５．２．雇用期間中

【目的】

従業員が情報セキュリティに関して課せられた責任を認識し、その責任の遂行を確実にする。

Ⅱ．５．２．１.【基本】 教育・訓練

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．【推奨】 教育のフィードバック

組織のトレーニング結果を情報セキュリティ責任者にフィードバックすること。

Ⅱ．５．２．３．【基本】 契約違反

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。

Ⅱ．５．３．雇用の終了又は変更

【目的】

雇用の終了又は変更時に、企業若しくは組織の利益を保護する。

Ⅱ．５．３．１．【基本】アクセス権・資産の取扱い

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、モバイル機器、アクセスカード等の設備等、全ての返却を求める。
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。
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。
iv. アクセス権の削除に当たっては、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。
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。
vi. 雇用が終了又は変更となる従業員が、稼働中の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。

Ⅱ．６．情報セキュリティインシデントの管理

クラウドサービスでシステム障害などの情報セキュリティインシデントが発生した場合、利用者は業務停止等の大きな影響を被ることになる。情報セキュリティインシデントが発生した場合、サービス運用に対する影響の最小化のため、事業者と利用者は責任と役割を分担して、原因の切り分けや影響への対処を行う必要がある。事業者は、自らの責任範囲及び情報セキュリティインシデントへの対応手順等について、予め利用者と合意し、文書化しておく必要がある。

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

【目的】

情報セキュリティ事象及び情報セキュリティぜい弱性に関する情報セキュリティインシデントの管理のために、一貫性のある効果的な取組を可能にする。

Ⅱ．６．１．１．【基本】 組織内報告

全ての従業員に対し、業務において発見したあるいは疑いをもった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統括管理する組織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、報告を受けた後のインシデント対応における段階的取扱い（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）の手順を確立する。また、情報セキュリティインシデントの報告手順を全ての従業員に周知徹底する。

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。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。

iii. 全ての従業員に対し、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。

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役立てる。

Ⅱ．６．１．２．【基本】 クラウドサービス事業者とクラウドサービス利用者間の報告

事業者は、利用者が情報セキュリティ事象を事業者に報告する仕組み、事業者が情報セキュリティ事象を利用者に報告する仕組み及び利用者が報告を受けた情報セキュリティ事象の状況を追跡する仕組みを提供すること。

Ⅱ．６．１．３．【基本】 インシデントの評価と分類

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。

【ベストプラクティス】

i. 評価及び決定の結果は、以後の参照及び検証のために詳細に記録しておく。

Ⅱ．６．１．４．【基本】 フィードバック

情報セキュリティインシデントの分析及び解決から得られた知識は、情報セキュリティインシデントが将来起こる可能性又はその影響を低減するために用いること。

Ⅱ．６．１．５．【基本】 証拠の収集・取得

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。

Ⅱ．７．コンプライアンス

クラウドサービスを利用する上で、関連する法規則が複数の国や地域にわたる可能性がある。データセンターが国外にあると、日本法人の事業者と契約していても、国外の法規制の影響を受ける可能性がある。

法令順守は事業者のみならず利用者にも求められる場合がある。事業者は、クラウドサービスに適用される法域を利用者に知らせることによって、利用者が影響を受ける法令、規制や契約上の要求事項を明確にすることが必要である。

Ⅱ．７．１．法令と規則の遵守

【目的】

情報セキュリティに関連する法規制や契約上の義務に対する違反及び情報セキュリティ上の要求事項に対する違反を避ける。

Ⅱ．７．１．１.【基本】 関連法規と記録

個人情報(特に要配慮個人情報を含む)、プライバシー情報、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。また、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、法令、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、適切に管理するとともに、利用者から求められたときには提供すること。

【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。

上記の法令を遵守するにあたり、下記に示すガイドライン等を参照すること。

a) 個人情報保護法関係のガイドライン

30 の法律、ガイドライン等がある。

（参考）個人情報保護委員会

https://www.ppc.go.jp/personalinfo/legal/

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「改正著作権法第35条運用指針」等

d) e-文書法関係のガイドライン

タイムビジネス推進協議会「知的財産におけるタイムスタンプ活用ガイドライン」 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

f) 政府機関の情報セキュリティ対策のための統一基準

g) 政府情報システムのためのセキュリティ評価制度(ISMAP)

ii. クラウドサービスの提供にあたり、海外にデータセンターがある場合や海外の情報資産を扱う場合等、海外法が適用される場合があるので注意する必要がある。

iii. 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があるので注意する必要がある。

Ⅱ．７．１．２．【基本】利用可否

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にシステム及び情報処理施設を利用させないこと。

【ベストプラクティス】

i. 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システム又は情報処理施設が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。

Ⅱ．７．１．３．【基本】ソフトウェア製品

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。

【ベストプラクティス】

i. 事業者は、バックアップでのみ利用するソフトｳエア製品の使用許諾条件等についても、利用者に予め周知し、ライセンス契約違反とならないようにすること。

Ⅱ．７．１．４．【基本】不正アクセス・流出からの保護

記録は、法令、規制、契約及び事業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。また、事業者は、利用者によるクラウドサービスの利用に関連して、事業者が収集し、保存する記録の保護に関する情報を、利用者に提供すること。

【ベストプラクティス】

i. 保存した記録の暗号化又はデジタル署名に用いた暗号鍵及び暗号プログラムは、その記録類を保存している期間中に記録の復号が可能なように保管する。

ii. 電子的記憶媒体を選択する場合は将来の技術変化によって読出しができなくなることを防ぐために、保持期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確実にする手順を確立する。

Ⅱ．７．１．５．【基本】暗号化

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とともに、利用者が法令及び規制の順守をレビューできるように、事業者は実施している暗号による対応策を記載すること。

Ⅱ．８．ユーザサポートの責任

クラウドサービスで情報セキュリティインシデントが発生すると、利用者は業務上、大きな影響を被ることがある。事業者は、情報セキュリティインシデントを防止するために、また、発生した影響を最低限に止め速やかに業務が再開できるようにするために、利用者と予めクラウドサービスの保守・サポート内容について合意し、文書化しておく必要がある。

Ⅱ．８．１．利用者への責任

【目的】

利用者がクラウドサービスを安心して利用できるようにする。

Ⅱ．８．１．１.【基本】責任

クラウドサービスの提供に支障が生じた場合には、その原因がサプライチェーンの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. サプライチェーンの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、利用者の便益を最優先した方法によって実施する。事業者は、サプライチェーンの事業者との間で利用者からの故障対応要求や問合せ、作業依頼等に対する取扱手続を定め、合意した内容を文書化すること。

Ⅱ．８．１．２.【基本】 SLA

事業者自身の責任範囲をSLA 等により文書化し、利用者に明確に示すこと。

Ⅱ．８．１．３.【基本】 情報提供

クラウドサービスの新規利用/変更を計画している利用者への情報提供にあたっては、組織のガバナンス規定を順守した上で、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事業者を選定できるようにすること。

Ⅱ．８．１．４.【基本】 クラウドサービス利用者からの苦情対応

提供しているクラウドサービスに対し、利用者からの苦情、懸念又は質問を受け取り、対応するためのプロセスを構築すること。

Ⅱ．８．２．保守

【目的】

保守サポートにおいて、情報セキュリティインシデントが発生することを防止する。

Ⅱ．８．２．１．【基本】 システム保守ポリシーと手順

システム保守の目的、適用範囲、役割、責任、経営コミットメント、組織間の調整及びコンプライアンスを取り扱う保守ポリシーを策定、文書化し、関係する組織に配布すること。

Ⅱ．８．２．２．【基本】 保守管理

保守契約、保守仕様書及び要求事項に従って、保守・修理を計画、実施、文書化し、記録すること。

【ベストプラクティス】

i. 保守が現地で行われるか、遠隔で行われるかにかかわらず、すべての保守活動を確認、承認し、モニタリングする。

ii. システム又はシステムコンポーネントが施設から離れた場所で保守又は修理される場合、施設からの移動について、予め定めた明示的な承認を要求するとともに、施設からの移動に先立って、関連する媒体からすべての情報を消去し機器の無害化を実施する。

iii. 保守又は修理後に、影響を受けた可能性のあるすべてのセキュリティ対策をチェックして、それらの対策が正しく機能しているかどうかを確認すること及び保守関連情報を記録すること。

iv. 保守記録には、下記情報を含む。

① 保守日時
② 保守を実施した個人又はグループの名前
③ 付添人の名前（必要であれば）
④ 実施された保守内容
⑤ 取り外された交換されたシステムコンポーネント

Ⅱ．８．２．３．【基本】 保守ツール

システムの保守ツールを承認・管理し、モニタリングするとともに、以前の保守ツール使用状況レビューすること。

【ベストプラクティス】

i. 保守ツールの定期的なレビューにより、古くなった、サポートされていない、無関係な又は使用されなくなった保守ツールの承認を取り消す。

ii. 保守担当者が使用する保守ツールに、不適切又は不正な変更がないかを調べる。

iii. メディアをシステムで使用する前に、診断プログラム若しくはテストプログラムを利用して、メディアに悪意のあるコードがないかを確認する。

iv. 保守ツールの使用は、許可された担当者のみに制限する。

v. 特権を追加して使用する保守ツールの使用は監視する。

vi. 保守ツールに、最新のソフトウェアアップデートやパッチが適用されていることを確認する。

Ⅱ．８．２．４．【基本】 リモート保守

リモート保守及び診断を承認のうえモニタリングする。リモート保守及び診断用ツールは、組織のポリシーに沿い、かつシステムのセキュリティ計画に記載されている通りである場合のみ、使用を許可すること。また、リモート保守及び診断のためのセッションを確立する際には、厳格な認証機能を使用するのに加え、リモート保守及び診断の記録を保管すること。リモート保守が完了したら、セッションとネットワーク接続を終了すること。

Ⅱ．８．２．５．【基本】 保守要員

保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を維持すること。

Ⅱ．８．２．６．【基本】 保守要員による保守

保守要員が付添いなしで保守を行う場合、その要員が必要なアクセス権限を有することを確認すること。また、必要なアクセス権限を持たない要員による保守活動を監督するために、必要なアクセス権限と技術的能力を有する職員を指定すること。

Ⅱ．８．２．７．【基本】 タイムリーな保守

システムコンポーネントに障害が発生した場合、保守サポート契約に基づき、保守サポートを行うこと。

【ベストプラクティス】

i. 保守サポートを契約していること、保守期限が更新されているか等、保守サポートの契約内容を定期的に確認する。

ii. 保守サポート契約に基づき予防保守を実施する。

Ⅱ．９．事業継続マネジメントにおける情報セキュリティ

事業者及び利用者は、クラウドサービスに大規模障害が発生した場合に備え、バックアップデータをクラウドサービス提供地とは異なる地域に保管する等の物理的対策事項と情報セキュリティ面での対策事項を統合した事業継続計画を策定する必要がある。

Ⅱ．９．１．情報セキュリティの継続

【目的】

情報セキュリティ対策の継続を組織の事業継続マネジメントに組み込む。

Ⅱ．９．１．１．【基本】 情報セキュリティ継続計画の策定と実施

組織は、大規模災害等における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定するとともに、プロセス・手順・対策を確立、文書化し、実施、維持すること。

Ⅱ．９．１．２．【基本】 情報セキュリティ継続の検証、レビュー及び評価

情報セキュリティ継続のための対策が、大規模災害等の下で妥当かつ有効であることを確認するために、組織は、定められた間隔でこれらの対策を検証すること。

Ⅱ．９．２．緊急時対応計画

【目的】

緊急時に情報セキュリティ対策が継続されることを確実にする。

Ⅱ．９．２．１．【基本】 緊急時対応計画の策定と手順

目的・適用範囲・役割・責任・経営コミットメント、組織間の調整及びコンプライアンスを取り扱う緊急時対応計画を策定するとともに、「緊急時対応計画」の実施手順を策定・文書化し、担当組織・要員に配布すること。

緊急時対応計画には、下記項目を盛り込むこと。

1. 極めて重要なミッション／業務機能と、関連する緊急時対応要件
2. 復旧目標、復旧の優先順位及びメトリクス
3. 緊急時対応における役割、責任、割り当てられた個人と連絡先情報
4. システムの途絶又は侵害若しくは不具合が発生しても、極めて重要なミッション／業務機能を維持できるようにすること
5. 最初に計画・導入されている情報セキュリティ対策を低下させることなく、最終的にシステムを完全復旧できるようにすること

Ⅱ．９．２．２．【推奨】 緊急時対応トレーニング

システムの利用者に対して、役割と責任に応じた緊急時対応トレーニングを実施すること。

【ベストプラクティス】

i. 危機的状況において職員が効果的に対応できるよう、緊急時対応トレーニングにイベントのシミュレーションを取り入れる。

Ⅱ．９．２．３．【推奨】 緊急時対応計画のテスト

緊急時対応計画の有効性を判断して計画の欠陥を特定するために、緊急時対応計画のテストを実施すること。

【ベストプラクティス】

i. テスト方法には、実地テスト、机上テスト、チェックリストによるテスト、シミュレーション（実運用と平行した、完全な割り込み型の）テストがある。

Ⅱ．９．２．４．【推奨】 代替処理サイト

利用者とシステムバックアップ情報の保存と取得を許可するための契約を締結するとともに、代替処理サイトを確立すること。また、代替処理サイトが一次処理サイトと同等の管理機能を提供することを確認すること。

【ベストプラクティス】

i. 同じ脅威に晒されるリスクを減らすために、一次処理サイトから離れた代替処理サイトを指定する。

Ⅱ．９．２．５．【推奨】 代替処理サイトで再開

代替処理サイトを定め、利用者と合意した目標復旧時間内に、システムオペレーションを移転・再開して、極めて重要なミッション／業務機能を遂行できるようにすること。

Ⅱ．９．２．６．【推奨】 通信サービス

一次処理サイトや代替処理サイトのいずれかにおいて一次通信サービスが利用できない場合に、極めて重要なミッションや業務機能を支援する代替通信サービスを確立すること。

【ベストプラクティス】

i. 同じ脅威に晒されるリスクを減らすために、一次サービスプロバイダではないプロバイダと代替通信サービスを確立する。

Ⅱ．９．２．７．【推奨】 システムの復旧と再構成

システムの途絶、侵害、又は不具合が発生した場合に、システムを従前の状態に復旧し、再構成できるようにすること。

Ⅱ．９．２．８．【推奨】 代替通信プロトコル

利用者が、業務の継続性を維持するために組織が定めた代替通信プロトコルを使用できるようにすること。

Ⅱ．９．２．９．【推奨】 代替の情報セキュリティ対策

組織が定めた情報セキュリティ機能を実施するための主な手段が利用できない場合又は侵害された場合に、それらの情報セキュリティ機能を満たすための代替の又は補足的な情報セキュリティ対策を実装すること。

【ベストプラクティス】

i. 情報セキュリティ対策は、システム、システムコンポーネント又は情報システムサービスが提供する情報セキュリティ機能のうち、極めて重要な機能のみ実装する。

Ⅱ．１０．その他

Ⅱ．１０．１．暗号と認証

【目的】

情報資産の機密性及び完全性を保護するために、暗号を適切かつ有効に利用する。

Ⅱ．１０．１．１．【基本】 方針

情報を保護するための暗号利用に関する方針を、策定し、実施すること。

【ベストプラクティス】

i. 暗号技術は、電子政府推奨暗号リスト (CRYPTREC暗号リスト)に記載されている暗号技術を採用する。

ii. 暗号に関わる組織の方針を実施する際は、各国の規制、国境を越える暗号化された情報の流れに関する規制及び国内の制約を考慮すること。

Ⅱ．１０．１．２．【基本】 情報提供

事業者は、利用者に、事業者が処理する情報を保護するために、暗号を利用する環境に関する情報を提供すること。また、事業者は、利用者自らの暗号による保護を適用することを支援するために、事業者が提供する能力についても利用者に情報を提供すること。

Ⅱ．１０．１．３．【基本】 暗号鍵の作成と管理

組織が定めた方針に従って、システム内で使用する暗号鍵を生成・配布・保管・アクセス・廃棄すること。

【ベストプラクティス】

i. 事業者は、利用者の独自の暗号による保護を支援する機能について、利用者に情報を提供する。

ii. 最適な慣行に従って、暗号アルゴリズム、鍵の長さ及び使用法を選定する。

iii. 全ての暗号鍵は、改変及び紛失から保護する。

iv. 秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護する。

v. 鍵の生成、保管及び保存のために用いられる装置は、物理的に保護する。

vi. 不適切な使用を起こりにくくするために、鍵の活性化及び非活性化の期日を定め、これによって、鍵管理の方針で定めた期間内でだけ鍵を使用できるようにする。

vii. 秘密鍵及びプライベート鍵はセキュリティを保って管理することに加え、公開鍵の真正性についても考慮する。

viii. 公開鍵を発行する認証局は、要求された信頼度を提供するために適切な対応策及び手順を備えている、認知された組織であること。

ix. 暗号サービスの外部供給者（例えば、認証局）とのサービスレベルに関する合意又は契約の内容では、賠償責任、サービスの信頼性及びサービス提供のための応答時間に関する事項を扱うこと。

Ⅱ．１０．２．開発プロセスにおけるセキュリティ

【目的】

開発のライフサイクルにおいて情報セキュリティ対策を確実にする。

Ⅱ．１０．２．１．【基本】 開発プロセスにおける情報セキュリティへの取組

プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組むこと。

【ベストプラクティス】

i. 開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。
ii. 情報セキュリティに配慮したシステムを構築するための原則を確立、文書化、維持し、全てのシステムの実装に対して適用する。
iii. 外部委託したシステム開発活動を監督、監視する。
iv. 新しいシステム及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。
v. 試験データは注意深く選定、保護、管理する。

Ⅲ. SaaS 編

Ⅲ．１．運用における情報セキュリティ

Ⅲ．１．１．運用管理

【目的】

アプリケーションやシステムの正確かつセキュリティを保った運用を確実にする。

Ⅲ．１．１．１．【基本】情報セキュリティ監視手順の策定

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。

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。

Ⅲ．１．１．２．【基本】 運用管理端末

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ファイルのウイルスチェックを行うこと。

【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は、厳しく制限する。

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。

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、従業員に周知徹底の上、違反した場合には罰則を課す。

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、完全スキャンを行う。

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。

vi. 情報セキュリティに関する情報を提供している機関（警察庁@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等の情報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。

vii. パッチは、運用管理機能への影響がないことを確認した上で適用する。

【評価項目】

a．パターンファイルの更新間隔

パターン	参考値
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 48 時間以内
4	ベンダリリースから 72 時間以内

Ⅲ．１．１．３．【基本】 稼働・障害監視

クラウドサービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行うこと。また、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。稼働停止や異常を検知した場合は、利用者に速報すること。また、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. 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。

ii. 稼働停止を検知した場合は、電子メール等で利用者に速やかに速報すること。ここで、速報先には、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。

iii. 監視の結果、クラウドサービスのレスポンスが大きく遅延した場合には、SLA 等の利用者との取決めに基づいて、利用者に速報すること。ここで、速報先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。

iv. 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。

v. 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。

【評価項目】

a. 死活監視インターバル（応答確認）

パターン	参考値
1	1 回以上／1 分
2	1 回以上／5 分
3	1 回以上／10 分
4	1　回以上／30 分

b. 稼働率

パターン	参考値
1	99.9%以上
2	99.0%以上

3	95.0%以上
4	95.0%以上

c. 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	参考値
1	5 分以内
2	10 分以内
3	20 分以内
4	30 分以内

Ⅲ．１．１．４．【基本】追加報告

クラウドサービスの提供に用いるアプリケーションに係る稼働停止、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。ここで、報告先は利用者側の管理連絡窓口のみとする。

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。

iii. 原因の分析結果や復旧の予測を含んだ報告を行う。

Ⅲ．１．１．５．【基本】 定期報告

クラウドサービスの提供に用いるアプリケーションの監視結果、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 の結果、パフォーマンス監視結果等を含める。

ii. 定期報告内容は、月単位で集計する。

【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	参考値
1	一ヵ月
2	一ヵ月
3	二ヵ月
4	三ヵ月

Ⅲ．１．１．６．【基本】 時刻同期

クラウドサービスの提供に用いるアプリケーション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. 一般財団法人日本データ通信協会のタイムビジネス認定制度や総務大臣による時刻認証業務に関する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。

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・通信機器間でも時刻同期を取ること。

iii. 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。

iv. 定期的に時刻同期の状況を確認すること。

Ⅲ．１．１．７．【基本】パスワード管理

パスワード管理システムは、対話式とすること、また、良質なパスワードとすること。パスワードの文字数等については、情報資産の機密度合いやリスクの大きさを考慮して、具体的なルールについては、組織が自主的に定めること。

【ベストプラクティス】

i. パスワード管理システムでは、利用者に自分のパスワードの選択及び変更を許可し、また、入力誤りを考慮した確認手順を組み入れる。

ii. パスワード管理システムでは、利用者に以前登録したパスワードの利用を禁止する。

Ⅲ．１．１．８．【基本】 クラウドサービスの変更管理

情報セキュリティに影響を与える組織、業務プロセス及びシステムの変更を管理すること。また、事業者は、クラウドサービス利用者の情報セキュリティに影響を与える可能性のあるクラウドサービスの変更について、利用者に情報を提供すること。

【ベストプラクティス】

i. 事業者は、下記事項についての情報を提供すること。併せて、変更開始と完了の通知を行うこと。

a. 変更内容

b. 変更予定日

c. 変更内容の技術的説明

Ⅲ．１．１．９．【基本】リソース監視

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。また、事業者は、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を監視すること。

【ベストプラクティス】

i. システムの重要度を考慮に入れて、その容量・能力に関する要求事項を特定する。
ii. 将来必要とされる容量・能力の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び予測される傾向を考慮する。
iii. 入手時間がかかるか又は費用がかかる資源については、特別な注意を払う。
iv. 情報セキュリティ又はサービスに脅威をもたらすおそれのある潜在的なボトルネック及び主要な要員への依存度合いを特定するとともに、適切な処置を立案する。

Ⅲ．１．１．１０．【基本】環境分離

開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために分離すること。

【ベストプラクティス】

i. ソフトウェアの開発から運用の段階への移行についての規則を明確に定めて文書化する。
ii. アプリケーションに対する変更は、運用システムに適用する前に試験環境又はステージング環境（運用環境に近い試験環境）で試験する。
iii. 取扱いに慎重を要するデータは、試験システムに同等の対策が備わっていない限り、その試験システム環境には複写しない。

Ⅲ．１．１．１１．【基本】マルウェア対策

マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。

【ベストプラクティス】

i. 異なる業者及び技術によるマルウェア対策ソフトウェア製品を複数利用することによって、マルウェアからの保護の有効性を高める。
ii. 緊急時手順においては、マルウェアに対する通常の対策を省略する場合があるため、マルウェアの侵入防止に向けた特段の注意を払う。
iii. マルウェアの検出及び修復ソフトウェアだけを利用するのではマルウェア対策として不十分であるため、マルウェアの侵入を防止するための運用手順を併用する。

Ⅲ．１．１．１２．【基本】イベントログの取得

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。また、事業者は、利用者に、ログ取得機能を提供すること。

【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。取得することが望ましい情報は以下のとおり。
   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) 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) システム構成の変更
g) 特権の利用
h) 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) 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。

Ⅲ．１．１．１３．【基本】 ログの保護

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。

【ベストプラクティス】

i. 情報セキュリティの監視を目的として重要イベントを特定するために、適切なメッセージを二次的ログとして自動的に複製すること又は適切なシステムユーティリティ若しくは監査ツールを用いること。

ii. システムログに含まれているデータが改ざん又は削除されると、セキュリティ上、誤った判断をする場合がある。システムログを保護するために、システム管理者の管理外にあるシステムにログを逐次複製する。

Ⅲ．１．１．１４．【基本】 作業記録

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。

【ベストプラクティス】

i. ログ編集は特定の PC からのみできるようにする。

ii. ログを編集したときにアラートが出るようにする。

Ⅲ．１．１．１５．【基本】 ソフトウェア導入

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。

【ベストプラクティス】

i. 組織はサポートのないソフトウェアを導入することについてのリスクを考慮する。

ii. ソフトウェアをアップグレードすることを決定する際には、アップグレードに対する事業上及び情報セキュリティ上の要求を考慮に入れる。

iii. ソフトウェア供給者による物理的又は論理的アクセスは、サポート目的で必要なときにのみ、管理者の承認を得て許可すること。また、その活動を監視する。

Ⅲ．１．１．１６．【基本】 技術的ぜい弱性

利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに入手すること。また、そのようなぜい弱性に組織がさらされている状況を評価すること。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。また、事業者は、提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。

【ベストプラクティス】

i. ぜい弱性の診断対象（インターフェースや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。

ii. 診断の結果、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。

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、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。

Ⅲ．１．２．システム及び情報の完全性

【目的】

アプリケーションやシステム、情報資産のセキュリティを確実にする。

Ⅲ．１．２．１．【基本】 原本性確保

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確保の手段としては、時刻認証による方法、電子署名（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ある。

Ⅲ．１．２．２．【推奨】 メモリ保護

許可されていない不正なコード実行からシステムメモリを保護するために、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. 重要なデータ領域の位置（プロセスのアドレス空間における実行ファイルの基底とライブラリ、ヒープ領域、及びスタックの位置が含まれる）を無作為に配置する「アドレス空間のランダム配置(ASLR)」機能や「実行保護(ESP)」機能を採用する。

Ⅲ．１．２．３．【基本】 セキュリティ侵害の検知

システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたり、不

適切に変更、削除されたりしたかを検知すること。

【ベストプラクティス】

i. システムコンポーネントを構成しているいくつかの関数にチェック処理を埋め込み、実行中に動的に改ざんされていなかを確認する。

ii. プログラムの流れを複雑にし、攻撃者によるソフトウェアの解析を困難にする。

Ⅲ．１．２．４．【推奨】 情報の更新

不要になった情報は削除するとともに削除したことを記録するログ情報等を残すこと。

Ⅲ．１．２．５．【推奨】 代替情報源

主要な情報源が破損しているか利用できない場合、システム又はシステムコンポーネントが重要な機能又はサービスを実行するための代替情報源を使用すること。

【ベストプラクティス】

i. 複数の入力ソースを持つことによって 1 つのソースが破損して使用できなくなった場合でも、サービス又は機能の提供を継続できること。

Ⅲ．１．２．６．【推奨】情報の断片化

一度システムに侵入されると、失われた情報を回復する方法は、通常は存在しない。組織は、情報を異なる要素に分割し、それらの要素を複数のシステム又はシステムコンポーネントと場所に分散すること。

【ベストプラクティス】

i. 断片化の程度は、情報の影響又は分類レベル、脅威インテリジェンス情報、及びデータ汚染が発生しているかどうかによって決定する。

Ⅲ．１．３．媒体の保管と廃棄

【目的】

媒体に保管された情報の許可されていない開示、変更、削除又は破壊を防止する。

Ⅲ．１．３．１．【基本】 媒体保管

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。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。

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。

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。

Ⅲ．１．３．２．【基本】 廃棄

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、当該システムの運用が完全に終結していることを確認する。

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。また、重要なデータの読み出しを不可能とすること。

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。

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。

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。

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。

Ⅲ．１．３．３．【基本】 輸送

情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。

【ベストプラクティス】

i. 輸送される情報を格納した媒体を保護するために次の事項を考慮すること。

a.信頼できる輸送機関又は運送業者を用いる。

b.認可された運送業者の一覧について、管理者の合意を得る。

c.運送業者を確認する手順を策定する。

d.輸送途中に生じるかもしれない物理的損傷から内容を保護（熱、湿気又は電磁気にさらすといった環境要因からの保護）するために、梱包を十分な強度とし、また、製造業者の仕様にも従う。

e.媒体の内容、適用された保護、輸送の責任窓口への受渡時刻及び目的地での受取り時刻の記録を特定するログを保持する。

Ⅲ．２．アプリケーション

Ⅲ．２．１．アプリケーションの情報セキュリティ対策

【目的】

アプリケーションが扱う情報資産の保護を確実にする。

Ⅲ．２．１．１.【基本】 ウイルス対策

クラウドサービスの提供に用いるアプリケーション（データ・プログラム等）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、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。

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。

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。

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。

【評価項目】

a. パターンファイルの更新間隔

パターン	参考値
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 48 時間以内
4	ベンダリリースから 72 時間以内

Ⅲ．２．１．２.【基本】 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮

公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護すること。

【ベストプラクティス】

i. 公衆ネットワークを経由するアプリケーションサービスに関する情報セキュリティには、次の事項を考慮すること。

a) 当事者が提示する自らの識別情報について、それぞれが互いに要求し合う信頼の

レベル

b) 重要な取引文書の内容の承認、その発行及びその文書への署名を誰が行うかについての認可プロセス

c) サービスの提供又は利用が認可されていることを通信業者に十分に通知していること

d) 入札手続、契約手続などにおいて、重要な文書の機密性、完全性及び発送・受領の証明、並びに契約の否認防止に関する要求事項の決定及びその実施

e) 重要な文書の完全性についての信頼のレベル

f) 秘密情報の保護に関する要求事項

g) 注文情報、支払い情報、納入先の宛名情報及び受領確認の機密性及び完全性

h) 顧客から提供された支払い情報を検証するための適切な検査の度合い

i) 不正行為を防ぐための最も適切な支払いの決済形式の選定

j) トランザクション情報の紛失又は重複の防止

k) 不正なトランザクションに関する賠償義務

l) 保険の要件

Ⅲ．２．１．３．【基本】 アプリケーションサービスのトランザクションの保護

アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護すること。

・不完全な通信

・誤った通信経路設定

・認可されていないメッセージの変更

・認可されていない開示

・認可されていないメッセージの複製又は再生

【ベストプラクティス】

i. 適宜ネットワークを分離する(開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境等)等してネットワークの完全性を保護する。

ii. 送受信・保管する情報(データ)に完全性チェックメカニズムを使用する。

Ⅲ．２．１．４．【基本】 プラットフォーム変更後のアプリケーションの技術的レビュー

プラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験すること。

Ⅲ．２．１．５．【基本】 パッケージソフトウェアの変更に対する制限

パッケージソフトウェアの変更は、必要な変更だけに限ることが望ましい。また、全ての変更を厳重に管理すること。

【ベストプラクティス】

i. 可能な限り、そして実行可能な場合には、業者が供給するパッケージソフトウェアは、変更しないで用いること。パッケージソフトウェアの変更が必要な場合は、次の事項を考慮すること。

a.組み込まれている機能及び処理の完全性が損なわれるリスク

b.業者の同意の取得

c.標準的なプログラム更新として業者から必要とする変更が得られる可能性

d.変更の結果として、将来のソフトウェアの保守に対して組織が責任を負うようになるかどうかの影響

e.用いている他のソフトウェアとの互換性

ii. 変更が必要な場合、原本のソフトウェアは保管し、指定された複製に対して変更を適用すること。

Ⅲ．２．２．データの保護

【目的】

情報資産を消失から保護する。

Ⅲ．２．２．１．【基本】 バックアップ

利用者のデータ、アプリケーション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（利用者のデータ、アプリケーション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。

【評価項目】

a. バックアップ実施インターバル

パターン	参考値
1	1回／1日
2	1回／1週間
3	1回／2週間
4	1回／1ヵ月

b. 世代バックアップ

パターン	参考値
1	5世代
2	3世代
3	2世代
4	1世代

Ⅲ．２．２．２．【基本】 バックアップ情報の完全性

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。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。

【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	参考値
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

Ⅲ．２．３．セッション管理

【目的】

アプリケーションがセッションを扱う場合、情報資産の保護を確実にする。

Ⅲ．２．３．１．【基本】 セッションのライフサイクル管理

セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。

Ⅲ．２．３．２．【基本】 セッションの真正性

通信セッションの真正性を保護すること。パケットレベルではなくセッションレベルでの通信の保護によって、通信セッションの両端で通信相手の身元及び伝送される情報の有効性に関して信頼の根拠をもたらす。

【ベストプラクティス】

i. システムは、利用者がログアウトした時点で、もしくはその他のセッションが終了した時点でセッション識別子を無効にする。

ii. システムは、ランダム化を経て、一意のセッション識別子を生成する。また、システムが生成したセッション識別子のみを認める。

Ⅲ．２．３．３．【基本】 同時セッションの制御

同時処理されるアカウントの割り当て数又はアカウントタイプの割り当て数は、システムが定めた各セッションの割り当て数まで制限すること。

Ⅲ．２．３．４．【基本】 セッションのロック

定められたアイドル時間を経過した場合又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。なお、認証手順として確立された手順を用いたユーザによってアクセスが再確立されるまで、セッションをロックすること。

【ベストプラクティス】

i. 利用者に対して1 日の作業が終わった際にシステムからログアウトすることを義務付ける。

ii. デバイスロックを介して、以前にディスプレイに表示されていた情報を一般公開の画像で隠す、若しくは、パターン非表示ディスプレイでは、スクリーンセーバーで使用されるパターンで隠す。

Ⅳ. PaaS/IaaS 編

Ⅳ．１．運用における情報セキュリティ

Ⅳ．１．１．運用管理

【目的】

クラウドサービスの正確かつセキュリティを保った運用を確実にする。

Ⅳ．１．１．１.【基本】情報セキュリティ監視手順の策定

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管理機能を持つアプリケーション、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。

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。

Ⅳ．１．１．２.【基本】 運用管理端末

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ファイルのウイルスチェックを行うこと。

【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。

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。

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た上で、違反した場合には罰則を課すこと。

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、完全スキャンを行うこと。

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。

vi. 情報セキュリティに関する情報を提供している機関（警察庁@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。

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。

【評価項目】

a. パターンファイルの更新間隔

パターン	参考値
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 48 時間以内
4	ベンダリリースから 72 時間以内

Ⅳ．１．１．３．【基本】 稼働・障害監視

クラウドサービスの提供に用いる管理機能を持つアプリケーション、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、障害監視、パフォーマンス監視を行うこと。稼働停止や異常を検知した場合は、利用者に速報すること。また。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. 監視対象機器のサービス稼働状態の監視を行うための方法（ping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。
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。
iii. 稼働停止を検知した場合は、電子メール等で利用者に速やかに速報する。ここで、速報先には、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。
iv. 監視の結果、クラウドサービスのレスポンスが大きく低下した場合には、SLA 等の利用者との取決めに基づいて、利用者に速報する。ここで、速報は利用者側の管理連絡窓口のみとする。
v. 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。
vi. 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。

【評価項目】

a. 死活監視インターバル（応答確認）

パターン	参考値
1	1回以上／1 分
2	1回以上／5 分
3	1回以上／10 分
4	1回以上／30 分

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	参考値
1	5 分以内
2	10 分以内
3	20 分以内
4	30 分以内

Ⅳ．１．１．４．【基本】追加報告

クラウドサービスの提供に用いる管理機能を持つアプリケーション、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クラウドサービス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。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。

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。

iii. 原因の分析結果や復旧の予測を含んだ報告を行う。

Ⅳ．１．１．５．【基本】 定期報告

クラウドサービスの提供に用いる管理機能を持つアプリケーション、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 の結果、パフォーマンス監視結果等を含める。

ii. 定期報告内容は、月単位で集計する。

【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	参考値
1	一ヵ月
2	一ヵ月
3	二ヵ月
4	三ヵ月

Ⅳ．１．１．６．【基本】 時刻同期

クラウドサービスの提供に用いる管理機能を持つアプリケーション、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. 一般財団法人日本データ通信協会のタイムビジネス認定制度や総務大臣による時刻認証業務に関する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。

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。

iii. 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。

iv. 定期的に時刻同期の状況を確認する。

Ⅳ．１．１．７．【基本】パスワード管理

パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとすること。

【ベストプラクティス】

i. パスワード管理システムでは、利用者に自分のパスワードの選択及び変更を許可し、また、入力誤りを考慮した確認手順を組み入れる。

ii. パスワード管理システムでは、利用者に以前登録したパスワードの利用を禁止する。

Ⅳ．１．１．８．【基本】 クラウドサービスの変更管理

情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更を管理すること。また、事業者は、クラウドサービスに悪影響を与える可能性のあるクラウドサービスの変更について、利用者に情報を提供すること。

【ベストプラクティス】

i. 事業者は、下記事項についての情報を提供すること。併せて、変更開始と完了の通知を行うこと。

a. 変更内容

b. 変更予定日

c. 変更内容の技術的説明

Ⅳ．１．１．９．【基本】リソース監視

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。また、事業者は、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を監視すること。

【ベストプラクティス】

i. システムの重要度を考慮に入れて、その容量・能力に関する要求事項を特定する。

ii. 将来必要とされる容量・能力の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び予測される傾向を考慮する。

iii. 入手時間がかかるか又は費用がかかる資源については、特別な注意を払う。

iv. 情報セキュリティ又はサービスに脅威をもたらすおそれのある潜在的なボトルネック及び主要な要員への依存度合いを特定するとともに、適切な処置を立案する。

Ⅳ．１．１．１０．【基本】環境分離

開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離すること。

【ベストプラクティス】

i. ソフトウェアの開発から運用の段階への移行についての規則は明確に定めて文書化する。
ii. 運用システムに対する変更は、運用システムに適用する前に試験環境又はステージング環境（運用環境に近い試験環境）で試験を行う。
iii. 取扱いに慎重を要するデータは、試験システムに同等の対策が備わっていない限り、その試験システム環境には複写しない。

Ⅳ．１．１．１１．【基本】マルウェア対策

マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。

【ベストプラクティス】

i. 異なる業者及び技術によるマルウェアからの対策ソフトウェア製品を複数利用することによって、マルウェアからの保護の有効性を高める。
ii. 緊急時手順においては、マルウェアに対する通常の対策を省略する場合があるため、マルウェアの侵入防止に向けた特段の注意を払う。
iii. マルウェアの検出及び修復ソフトウェアだけを利用するのではマルウェア対策として不十分であるため、マルウェアの侵入を防止するための運用手順を併用する。
iv. システムやクラウドサービスへの侵入痕跡を検索又は既存の制御を回避する脅威を検出、追跡及び妨害するサイバー脅威ハンティング機能を導入する。

Ⅳ．１．１．１２．【基本】イベントログの取得

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。また、事業者は、利用者に、ログ取得機能を提供すること。

【ベストプラクティス】

i. クラウドサービス利用者の利用状況、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。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) 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) システム構成の変更
g) 特権の利用
h) 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) 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。

Ⅳ．１．１．１３．【基本】 ログの保護

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。

【ベストプラクティス】

i. 情報セキュリティの監視を目的として重要イベントを特定するために、有意なメッセージを二次的ログとして自動的に複製すること又は適切なシステムユーティリティ若しくは監査ツールを用いること。

ii. システムログに含まれているデータが改ざん又は削除されると、セキュリティ上、誤った判断をする場合がある。システムログを保護するために、システム管理者の管理外にあるシステムにログを逐次複製すること。

Ⅳ．１．１．１４．【基本】 作業記録

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。

【ベストプラクティス】

i. ログ編集は特定の PC からのみできるようにすること。

ii. ログを編集したときにアラートが出るようにすること。

Ⅳ．１．１．１５．【基本】 ソフトウェア導入

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。

【ベストプラクティス】

i. 組織はサポートのないソフトウェアを導入することのリスクを考慮する。

ii. ソフトウェアをアップグレードすることを決定する際には、アップグレードに対する事業上及びセキュリティ上の要求を考慮に入れる。

iii. ソフトウェア供給者による物理的又は論理的アクセスは、サポート目的で必要なときにのみ、管理者の承認を得て許可すること。また、活動を監視すること。

Ⅳ．１．１．１６．【基本】 技術的ぜい弱性

利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに獲得すること。また、そのようなぜい弱性に組織がさらされている状況を評価すること。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。また、事業者は、提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。

【ベストプラクティス】

i. ぜい弱性の診断対象（インターフェースや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。
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。
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。

Ⅳ．１．２．システム及び情報の完全性

【目的】

システムや情報資産のセキュリティを確実にする。

Ⅳ．１．２．１．【基本】 原本性確保

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確保の手段としては、時刻認証による方法、電子署名（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。

Ⅳ．１．２．２．【推奨】 メモリ保護

許可されていないコードの実行からメモリを保護するための、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. 重要なデータ領域の位置（プロセスのアドレス空間におけるファイルの基底とライブラリ、ヒープ領域及びスタックの位置が含まれる）を無作為に配置する「アドレス空間のランダム配置(ASLR)」機能や「実行保護(ESP)」機能を採用する。

Ⅳ．１．２．３．【基本】 セキュリティ侵害の検知

システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたか、不適切に削除されたかを判断すること。

【ベストプラクティス】

i. システムコンポーネントを構成しているいくつかの関数にチェック処理を埋め込み、実行中に動的に改ざんされていいなかを確認する。

ii. プログラムの流れを複雑にし、攻撃者によるソフトウェアの解析を困難にする。

Ⅳ．１．２．４．【推奨】 情報の更新

不要になった情報は削除するとともに削除したことを記録するログ情報等を残すこと。

Ⅳ．１．２．５．【推奨】 代替情報源

主要な情報源が破損しているか利用できない場合、システム又はシステムコンポーネントが重要な機能又はサービスを実行するための代替情報源を使用すること。

【ベストプラクティス】

i. 複数の入力ソースを持つことによって 1 つのソースが破損して使用できなくなった場合でも、サービス又は機能の提供を継続できること。

Ⅳ．１．２．６．【推奨】情報の断片化

一度システムに侵入されると、失われた情報を回復する方法は、通常は存在しない。組織は、情報を異なる要素に断片化し、それらの要素を複数のシステム又はシステムコンポーネントと場所に分散すること。

【ベストプラクティス】

i. 断片化の程度は、情報の影響又は分類レベル、脅威インテリジェンス情報及びデータ汚染が発生しているかどうかによって決定する。

Ⅳ．１．３．媒体の保管と廃棄

【目的】

媒体に保管された情報の許可されていない開示、変更、削除又は破壊を防止する。

Ⅳ．１．３．１．【基本】 媒体保管

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。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。

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。

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。

Ⅳ．１．３．２.【基本】 廃棄

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、当該システムの運用が完全に終結していることを確認する。

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。内部の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。

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。

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。

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。

Ⅳ．１．３．３.【基本】 輸送

情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。

【ベストプラクティス】

i. 輸送される情報を格納した媒体を保護するために次の事項を考慮すること。

a.信頼できる輸送機関又は運送業者を用いる。

b.認可された運送業者の一覧について、管理者の合意を得る。

c.運送業者を確認する手順を策定する。

d.輸送途中に生じるかもしれない物理的損傷から内容を保護（熱、湿気又は電磁気にさらすといった環境要因からの保護等）するために、梱包を十分な強度とし、また製造業者の仕様にも従う。

e.媒体の内容、適用された保護、輸送の責任窓口への受渡時刻及び目的地での受取り時刻の記録を特定するログを保持する。

Ⅳ．２．プラットフォーム、サーバ・ストレージ

Ⅳ．２．１．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.

【目的】

プラットフォーム、サーバやストレージに保管された情報の許可されていない開示、変更、削除又は破壊を防止する。

Ⅳ．２．１．１.【基本】 ウイルス対策

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、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。

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。

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。

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。

【評価項目】

a. パターンファイルの更新間隔

パターン	参考値
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 48 時間以内
4	ベンダリリースから 72 時間以内

Ⅳ．２．２．プラットフォーム、サーバ・ストレージの運用・管理

【目的】

プラットフォーム、サーバやストレージの正確かつセキュリティを保った運用を確実にする。

Ⅳ．２．２．１．【基本】 可用性

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、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。

【評価項目】

a．クラウドサービスの稼働率

パターン	参考値
1	99.9%以上
2	99.0%以上
3	95.0%以上
4	95.0%以上

Ⅳ．２．２．２．【基本】 リソース

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、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。

ii. 定期的にプラットフォーム、サーバ・ストレージの利用状況を監視する。

【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	参考値
1	サービス提供期間＋10 年間
2	サービス提供期間＋5 年間
3	サービス提供期間＋1 年間
4	サービス提供期間

Ⅳ．２．３．データの保護

【目的】

情報資産を消失から保護する。

Ⅳ．２．３．１．【基本】 バックアップ

利用者のサーバ・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。

【評価項目】

a. バックアップ実施インターバル

パターン	参考値
1	1回／1日
2	1回／1週間
3	1回／2週間
4	1回／1ヵ月

b. 世代バックアップ

パターン	参考値
1	5世代
2	3世代
3	2世代
4	1世代

Ⅳ．２．３．２．【基本】 バックアップ情報の完全性

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。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。

【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	参考値
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

Ⅳ．３．ネットワーク

Ⅳ．３．１．ネットワークにおける情報セキュリティ対策

【目的】

ネットワークにおける情報の保護及び情報処理施設の保護を確実にする。

Ⅳ．３．１．１.【基本】 ネットワーク構成

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. クラウドサービス利用者、システム等の管理者、サプライチェーン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。
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。
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。

Ⅳ．３．１．２.【基本】 管理者の権限

情報セキュリティ責任者は、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、システム管理者及びネットワーク管理者に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。
ii. 特に、システム管理者及びネットワーク管理者に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。
iii. 管理者権限の割当一覧を作成して管理する。
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。

Ⅳ．３．１．３.【基本】 不正アクセス防止

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。

【ベストプラクティス】

i. 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。

ii. 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。

Ⅳ．３．１．４．【基本】 パケット検知

不正な通過パケットを自動的に発見、若しくは遮断する措置を講じること。

【ベストプラクティス】

i. 不正アクセスを検出するには、IDS/IPS 等を導入する。

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。

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する。

Ⅳ．３．１．５．【基本】 実施基準

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。

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. 管理者とサプライチェーン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。

iii. 管理者間又は管理者とサプライチェーン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。

Ⅳ．３．１．６．【基本】 通信の暗号化

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。

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(CRYPTREC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を利用する。

Ⅳ．３．１．７．【基本】 サーバ証明書

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。

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。

Ⅳ．３．１．８．【基本】 情報セキュリティ特性

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. 事業者と ISP 間、事業者の保守管理用、事業者とサプライチェーン事業者間ごとに、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。

ii. 提供するクラウドサービスに利用者が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。

Ⅳ．３．１．９．【基本】 障害監視

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. 事業者とISP 間、事業者の保守管理用、事業者とサプライチェーン事業者間等、それぞれの外部ネットワークごとに管理責任者を設置する。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。

【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	参考値
1	5 分以内
2	10 分以内
3	20 分以内
4	30 分以内

Ⅳ．３．１．１０．【推奨】 クロス・ドメイン・ポリシーの実施

論理的に接続するセキュリティドメインの物理インターフェイスやネットワークインターフェイス間にポリシー施行メカニズムを実装すること。

【ベストプラクティス】

i. 論理ポリシー施行メカニズムの場合、ポリシー施行メカニズムをバイパスする機能を防ぐために、インターフェイス間に論理パスを作成することを避ける。

ii. 物理ポリシー施行メカニズムの場合、セキュリティドメインに侵入する論理的な秘密チャネルの存在を排除するために、ポリシー施行の物理的な実装によって物理的な分離を行う。

Ⅳ．３．１．１１．【推奨】統制管理のための代替通信パス

指揮統制のために代替通信パスを確立すること。

【ベストプラクティス】

i. 意思決定者が不在の場合に代替の意思決定者を指定し、その行動の範囲と制限を確立するなど、指揮統制の目的で代替の通信パスを確立することによって、インシデント中に組織が運用を継続し、適切な行動をとる。

Ⅳ．３．１．１２．【推奨】検出機器の再配置

攻撃者が目標を達成する能力を妨げるために、センサー又は監視機能を新しい場所に再配置すること。

【ベストプラクティス】

i. 攻撃者を混乱させるために、組織が取得した脅威情報に基づいて、センサー又は監視機能を新しい位置に配置する、又はランダムに再配置を行う。

Ⅳ．３．１．１３．【推奨】ハードウェア/ソフトウェアによる分離とポリシーの施行

セキュリティドメイン間にハードウェア/ソフトウェアによる分離とポリシーの適用メカニズムを実装すること。

Ⅳ．３．１．１４．【推奨】ハードウェアベースの書き込み保護

システムファームウェアコンポーネントにハードウェアベースの書き込み保護を採用すること。

Ⅳ．３．２．情報の転送

【目的】

組織の内部及び外部に転送した情報の保護を確実にする。

Ⅳ．３．２．１．【基本】 情報転送の方針及び手順

あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び対策を備えること。

Ⅳ．３．２．２．【基本】 情報転送に関する合意

組織と外部関係者との間で、業務情報のセキュリティを保った転送について、合意すること。

Ⅳ．３．２．３．【基本】 秘密保持契約又は守秘義務契約

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。

Ⅳ．３．３．セッション管理

【目的】

システムがセッションを扱う場合、情報資産の保護を確実にする。

Ⅳ．３．３．１．【基本】 セッションのライフサイクル管理

セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。

Ⅳ．３．３．２．【基本】 セッションの真正性

システムは、通信セッションの真正性を保護すること。

【ベストプラクティス】

i. システムは、利用者がログアウトした時点で、もしくはその他のセッションが終了した時点でセッション識別子を無効にする。

ii. システムは、ランダム化を経て、一意のセッション識別子を生成する。また、システムが生成したセッション識別子のみを認める。。

Ⅳ．３．３．３．【基本】 同時セッションの制御

同時処理されるアカウントの割り当て数又はアカウントタイプの割り当て数は、システムが定めた各セッションの割り当て数まで制限すること。

Ⅳ．３．３．４．【基本】 セッションのロック

定められたアイドル時間を経過した場合又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。なお、認証手順として確立された手順を用いたユーザによってアクセスが再確立されるまで、セッションをロックすること。

【ベストプラクティス】

i. 利用者に対して1 日の作業が終わった際にシステムからログアウトすることを義務付ける。

ii. デバイスロックを介して、以前にディスプレイに表示されていた情報を一般公開の画像で隠す、若しくは、パターン非表示ディスプレイでは、スクリーンセーバーで使用されるパターンで隠すこと。

Ⅳ．４．建物、電源(空調等)

Ⅳ．４．１．建物の災害対策

【目的】

情報処理施設に預託されている情報資産の損失、損傷、劣化を防止するとともに提供サービスへの影響を防止する。

Ⅳ．４．１．１.【基本】 建物

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、物理的及び環境上の危険を考慮して、システムが存在する施設の場所を計画すること。また、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。
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。
iii. サーバルームは建物の２階以上に設置すること。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。

Ⅳ．４．１．２.【基本】 電源

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。
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。

Ⅳ．４．１．３.【基本】 空調

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。
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。

Ⅳ．４．２．火災、雷、静電気からシステムを防護するための対策

【目的】

情報処理機器の障害による情報資産の損失、損傷、劣化を防止するとともに提供サービスへの影響を防止する。

Ⅳ．４．２．１．【基本】 汚損対策

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不活性ガス又はハロゲンガスを用いた消火設備である。

【評価項目】

a．汚損対策の実施

パターン	参考値
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	汚損対策消火設備（ガス系消火設備等）の使用
4	汚損対策消火設備（ガス系消火設備等）の使用

Ⅳ．４．２．２．【基本】 火災対策

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。

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。

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。

Ⅳ．４．２．３．【基本】 雷対策

情報処理施設に雷が直撃した場合及び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. 情報処理施設には避雷針を設置する。

ii. 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[11]を設置する。

iii. 情報処理施設は等電位化（全ての接地の一本化）を行う。

Ⅳ．４．２．４．【基本】 静電気対策

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。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。

Ⅳ．４．２．５．【基本】 緊急遮断

緊急時に、システム又は個々のシステムコンポーネントの電源を遮断できる機能を提供するとともに、緊急時に電源を遮断する機能が、不正に起動されないようにすること。

Ⅳ．４．２．６．【基本】 非常用電源

一次電源が失われた場合に、長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意すること。

Ⅳ．４．２．７．【基本】 非常用照明

停電が発生した場合や、電力が途絶えた場合に作動し、施設内の非常口と避難経路を照らす自動非常用照明をシステムに導入し、維持すること。

Ⅳ．４．２．８．【推奨】 電磁パルス保護対策

システム及びシステムコンポーネントの電磁パルス損傷に対して保護対策を講じること。

Ⅳ．４．３．装置の対策

【目的】

情報資産の損失、損傷、盗難、劣化を防止し、業務に対する妨害を阻止する。

Ⅳ．４．３．１．【基本】 サポートユーティリティ

装置は、サポートユーティリティの不具合による、停電、その他の故障から保護すること。サポートユー

[11] Constant Voltage Constant Frequency の略。停電時などに安定的に交流電流を供給するための無停電電源装置。

ティリティ（電気、通信サービス、給水、ガス、下水、換気、空調等）は、次の条件を満たすこと。

a) 装置の製造業者の仕様及び地域の法的要求事項に適合している。

b) 事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を定期的に評価する。

c) 適切に機能することを確実にするために定期的に検査及び試験する。

d) 必要であれば不具合を検知するための警報装置を取り付ける。

e) 必要であれば物理的な経路が異なる複数の供給元を確保する。

Ⅳ．４．３．２．【基本】 ケーブル配線のセキュリティ

データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護すること。

【ベストプラクティス】

i. 情報処理施設に接続する電源ケーブル及び通信回線は、可能な場合、地下に埋設するか、若しくはこれに代わる十分な保護手段を施す。

ii. 干渉を防止するために、電源ケーブルは通信ケーブルから隔離する。

Ⅳ．４．３．３．【基本】 装置の保守

装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守すること。

【ベストプラクティス】

i. 装置は供給者の推奨する間隔及び仕様に従って保守する。

ii. 認可された保守要員だけが装置の修理及び手入れを実施する。

iii. 故障と思われるもの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持する。

Ⅳ．４．３．４．【基本】 資産の移動

装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さないこと。

Ⅳ．４．３．５．【基本】 構外にある装置及び情報資産のセキュリティ

構外にある情報資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、 セキュリティを適用すること。

【ベストプラクティス】

i. 情報を保管及び処理する装置を組織の構外で用いる場合は，管理層の認可を得る。

Ⅳ．４．３．６．【基本】 装置のセキュリティを保った処分又は再利用

記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを全て消去していること、若しくはセキュリティを保って上書きしているこ

とを検証すること。事業者は、装置のセキュリティを保った処分又は再利用を行うための取決めについて、利用者と合意していること。

【ベストプラクティス】

i. 秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊するか、その情報を消去若しくは上書きする。

ii. 消去又は上書きには、標準的な消去又は初期化の機能を利用するより、消磁[12]や暗号化消去等の手法で元の情報を復元不可能な状態にするための技術を利用する。

Ⅳ．４．３．７．【基本】 無人状態にあるクラウドサービス利用者装置

利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にすること。

【ベストプラクティス】

i. 無人状態にある装置の保護を実施する責任と同様、その装置を保護するための情報セキュリティ要求事項及び手順についても、利用者に認識させること。

Ⅳ．４．３．８．【基本】 クリアデスク・クリアスクリーン方針

書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用すること。

Ⅳ．４．４．建物の情報セキュリティ対策

【目的】

情報処理施設に対する許可されていない物理アクセス、損傷及び妨害を防止する。

Ⅳ．４．４．１．【基本】 オフィス、部屋及び施設のセキュリティ

オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用すること。

Ⅳ．４．４．２．【基本】 セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関する手順を設計し、適用すること。

Ⅳ．４．４．３．【基本】 入退室記録

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の手順書と記録を作成し、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。

[12] 強力な磁場をかけることで、ハードディスク内のデータを破壊する行為のこと。

ii. 個人の資格確認による入退室管理を行う。

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。

【評価項目】

a. 入退室記録の保存

パターン	参考値
1	10 年以上
2	5 年以上
3	5 年以上
4	3 年以上

Ⅳ．４．４．４．【基本】 監視カメラ

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。

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。

iii. 監視カメラは用途に応じて十分な解像度を持つこと。

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。

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。

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。

【評価項目】

a. 監視カメラの稼働時間

パターン	参考値
1	365 日24 時間
2	365 日24 時間
3	365 日24 時間
4	365 日24 時間

b. 監視映像保存期間

パターン	参考値
1	6ヵ月
2	6ヵ月
3	3ヵ月

4	1ヵ月

Ⅳ．４．４．５．【基本】 破壊対策ドア

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。

Ⅳ．４．４．６．【基本】 警備員

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。

Ⅳ．４．４．７．【基本】 鍵管理

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。

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。

Ⅳ．４．４．８．【基本】 受渡場所

荷物の受渡場所などの立寄り場所及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理すること。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から可能な限り離すこと。

この対策の実施にあたっては，次の事項を考慮すること。

a) 建物外部からの受渡場所へのアクセスは、識別及び認可された要員に制限する。

b) 受渡場所は、配達要員が建物の他の場所にアクセスすることなく荷積み及び荷降ろしできるようにする。

c) 受渡場所の外部扉は、内部の扉が開いているときには情報セキュリティを保つ。

d) 入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないかを検査する。

e) 入荷物は、事業所へ持ち込むときに資産の管理手順に従って登録する。

f) 可能な場合には、入荷と出荷とは物理的に分離した場所で扱う。

g) 入荷物は輸送中に開封された痕跡がないかを検査する。開封の痕跡が見つかった場合には直ちにセキュリティ要員に報告する。

Ⅳ．４．４．９．【基本】 搬入と搬出

施設に搬入・搬出されるシステムコンポーネントに対して許可・未許可、モニタリング及び管理を行い、それらについての記録を保管すること。

Ⅴ．IoT サービスリスクへの対応方針編

Ⅴ．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、ガイドライン公表後、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、本ガイドラインに新たに第Ⅴ部を追加し、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。

第Ⅴ部では 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。

Ⅴ．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[13]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．８．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．８．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。

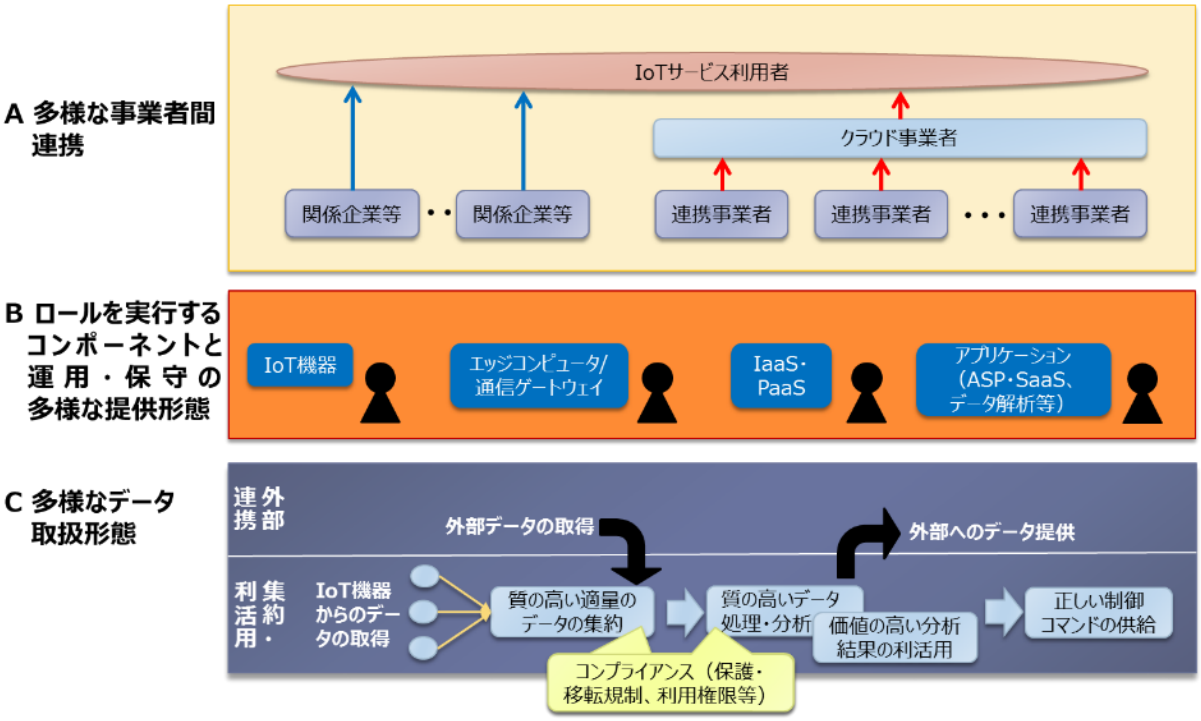
[13] 消費者に付加価値サービスを提供するために IoT サービスを利用する企業等も多い。

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 7 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。

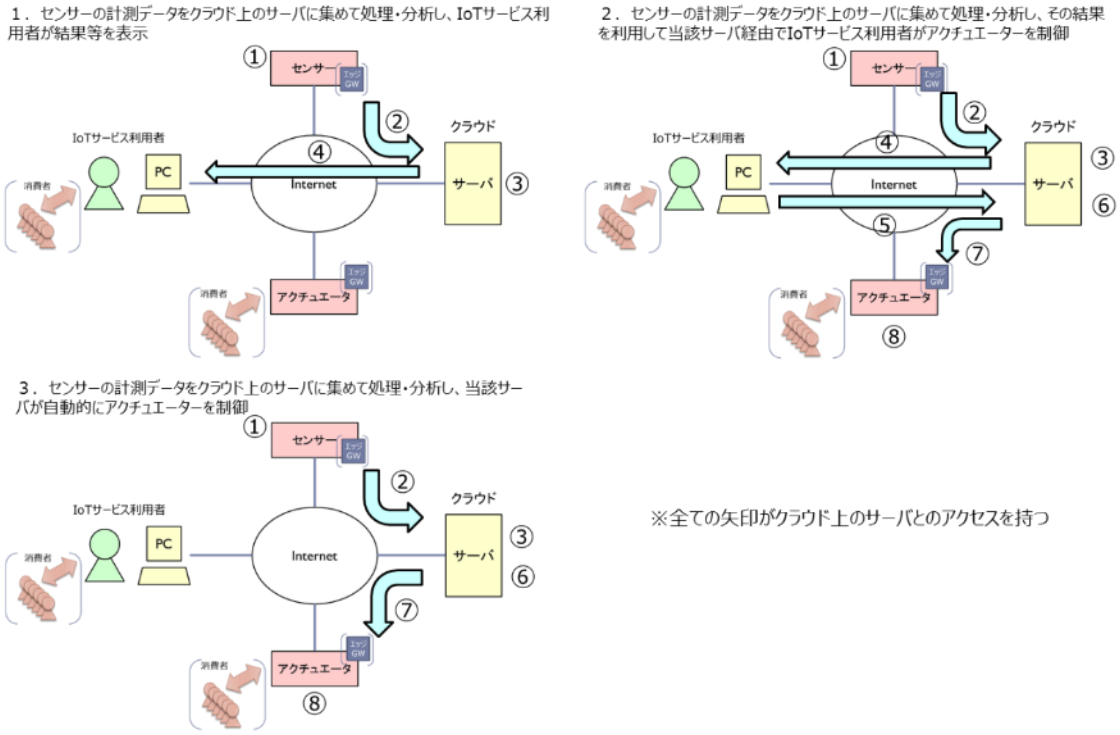
図表 7　IoT サービスを特徴付ける三つの観点



Ⅴ．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８参照）。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８　IoT サービスの三つの構造



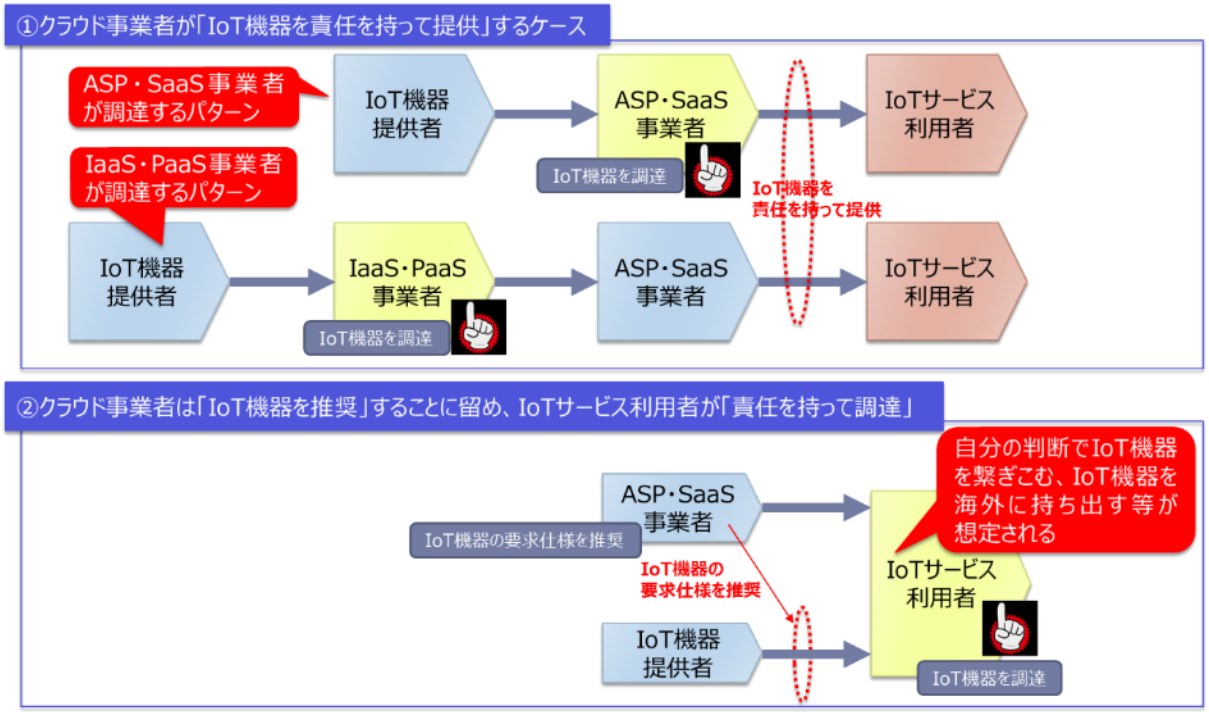
＜クラウド事業者及び連携事業者が果たす IoT サービス運用上の役割（Ⅴ．２．１．１（イ）参照）＞

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９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９　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）



Ⅴ．１．３．IoT サービスにおいて重視すべきリスク

図表７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　<u>【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</u>（Ⅴ．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　<u>【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</u>（Ⅴ．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（Ⅴ．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[14]」「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

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、ANNEX3 に取りまとめている。

Ⅴ．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 V.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（Ⅴ．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

[14] 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。

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（Ｖ．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（Ｖ．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

Ｖ．１．５．第Ｖ部の活用方法

第Ｖ部は、IoT サービスを提供している又は提供を検討/計画しているクラウド事業者が読むのに適している。「Ｖ．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Ｖ部は、以下の順で読み進めることを推奨する。

① まず「Ｖ．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Ｖ部の活用方法等の概略を理解する。

② 次に、「Ｖ．２．」の前半を読み、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「Ｖ．２．」の後半を読み進むことを推奨する。

③ さらに「Ｖ．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。

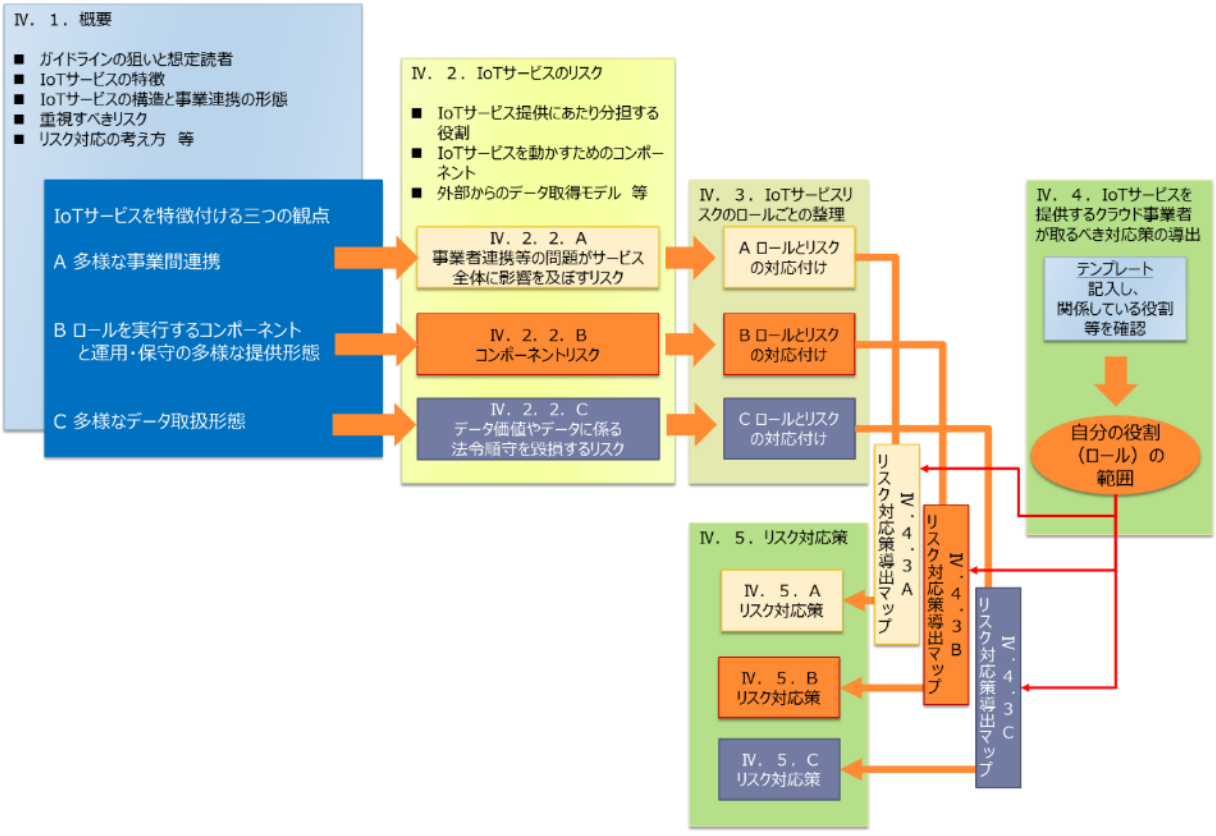
④ 以上の準備をした上で「Ｖ．４．１．」、「Ｖ．４．２．」を読み、IoT サービス提供にあたりクラウド事業者が関わりを持つ役割を整理し、「Ｖ．４．３．」の「ロール（＝役割）ごと

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「Ⅴ．５．」に記載）を特定する。（図表９、図表 10 参照）

⑤ 対応策の具体的な内容は「Ⅴ．５．」に列挙されている。「Ⅴ．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、「Ⅴ．５．」は必要な箇所のみ読むことで足りるはずである。

第Ⅴ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 10 参照）。「Ⅴ．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 10 第Ⅴ部の活用方法（概要）



図表 10 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 11 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 11 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 11 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： V．4．3．X → 「リスク対応策導出マップ」の記載箇所

図表 11 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 サービスを特徴づける三つの観点		
		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 サービス提供の環境を整備・維持するロール（103ページ参照）	a 利用者契約	**実行 →対応策V.4.3.A**		
	b 機器等提供	委託先全体のガバナンス維持のための管理	**提供 →対応策 V.4.3.B ①**	データ監視・保全への協力の委託管理
	c 機器等推奨		**推奨 →対応策 V.4.3.B ②**	
	d 構成管理	**実行**		
	e 契約管理	**→対応策V.4.3.A**	**委託 →対応策 V.4.3.B ③**	**委託 →対応策 V.4.3.C ②**
	f データ監視・保全	ロール実行の委託管理		**主導 →対応策 V.4.3.C ①**
（イ）IoT サービスを実際に動かすためのロール（106ページ参照）	a 計測		**実行 →対応策V.4.3.B ④**	
	b ローカル伝送			
	・・・			
	k 駆動			

Ｖ．１．６．IoT セキュリティガイドライン[15]との関係

第Ｖ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Ｖ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Ｖ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載との整合性を維持するように配慮している。

[15] IoT 推進コンソーシアム、総務省、経済産業省が平成 28 年 7 月にバージョン 1.0 を公表

Ⅴ．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、ANNEX3 において解説する。

Ⅴ．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

Ⅴ．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 12 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 12　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 14 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、準備した機器等について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 9 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 機器について責任を持って提供」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 9 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（Ⅴ．４．３．B、Ⅴ．5．B 参照）。

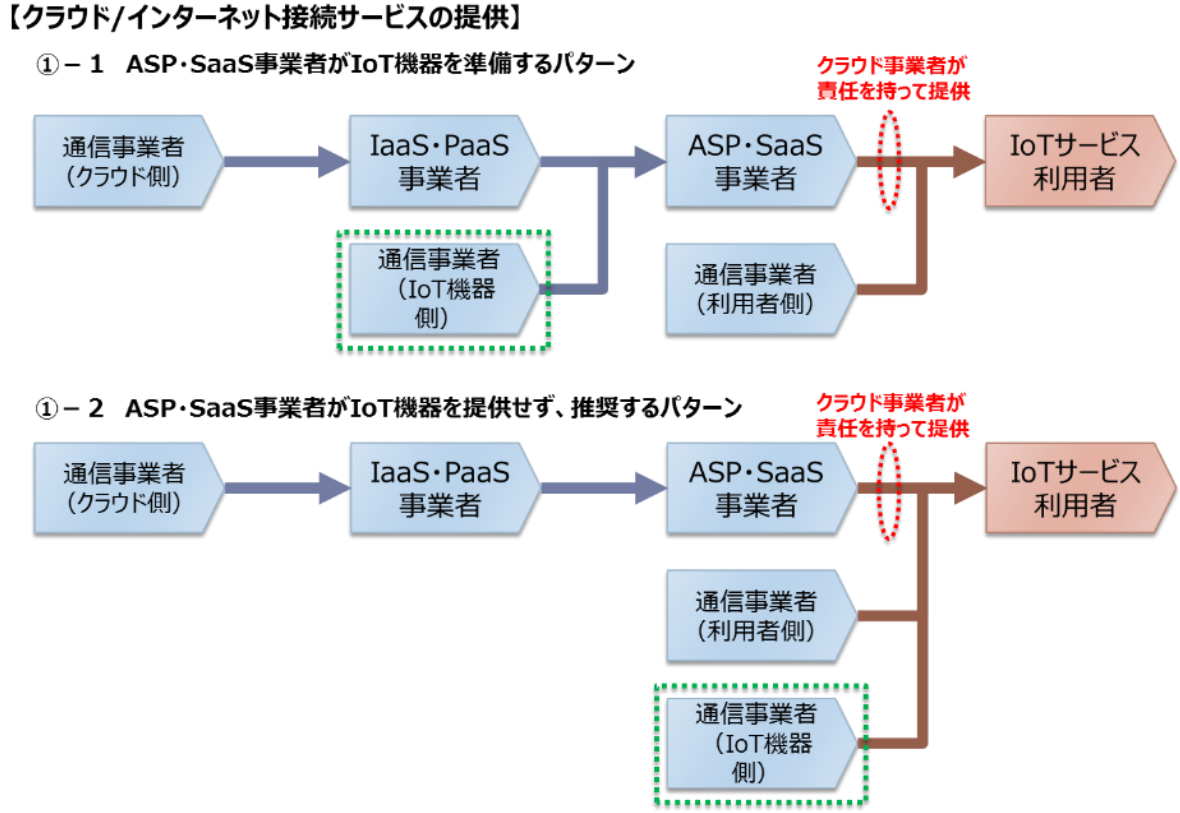
「**b** 機器等提供」のロールについては、クラウド事業者は IoT サービスを特徴付ける以下の主要コンポーネントの提供責任についても考えておく必要がある。

- 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 13 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[16]/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（Ⅴ．４．３．B、Ⅴ．５．B 参照）。

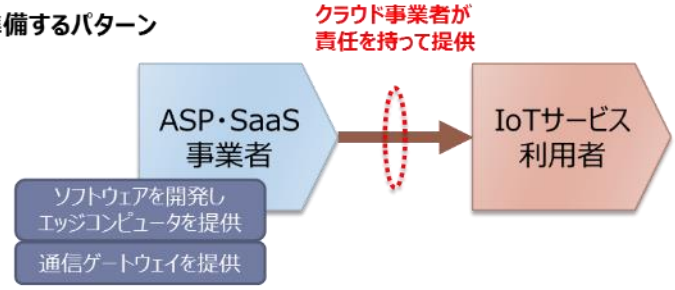
図表 13　IoT 機器以外の主要コンポーネントの準備・提供の現状



[16] 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】

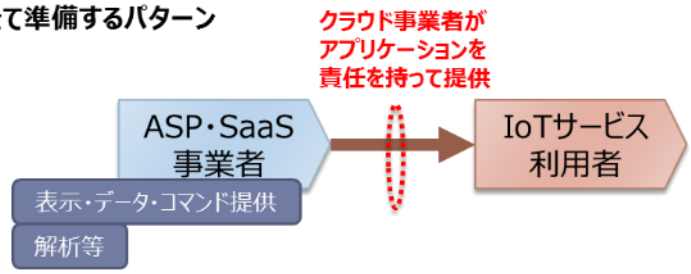
②－１　ASP・SaaS事業者が全て準備するパターン



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

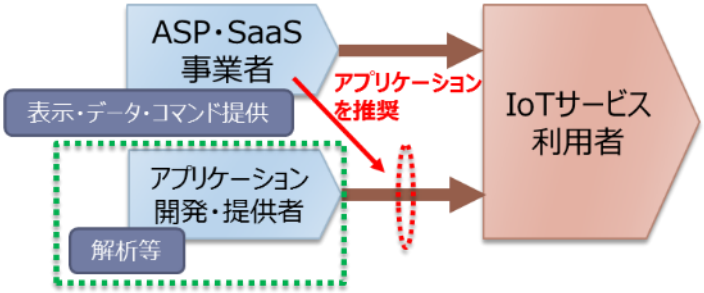
【アプリケーションの提供（表示・データ・コマンド提供、解析等）】

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 サービスを実際に動かすため、「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 14 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 15 参照）。

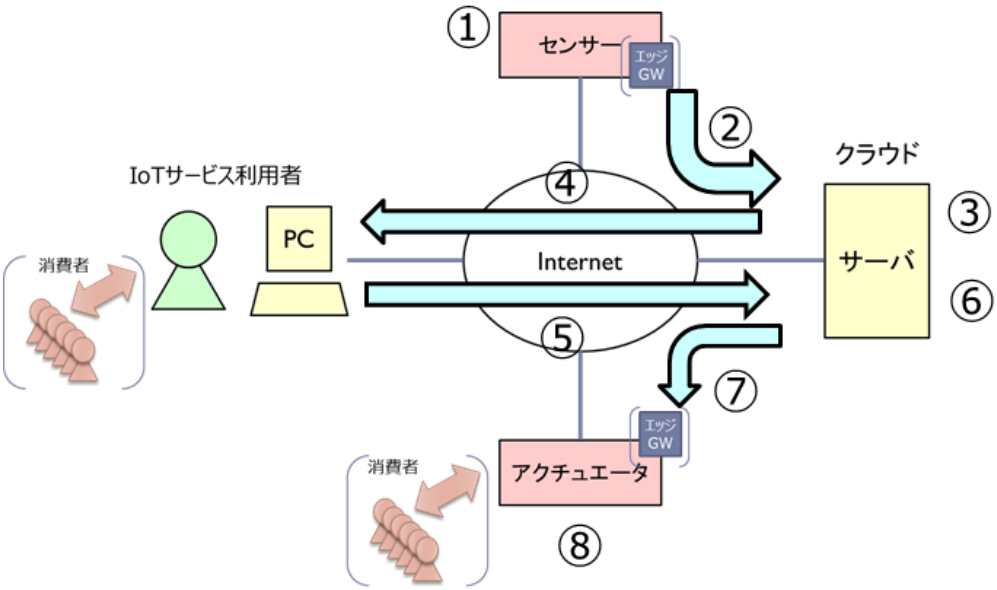
図表 14　IoT サービスを実行するためのロールの定義

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

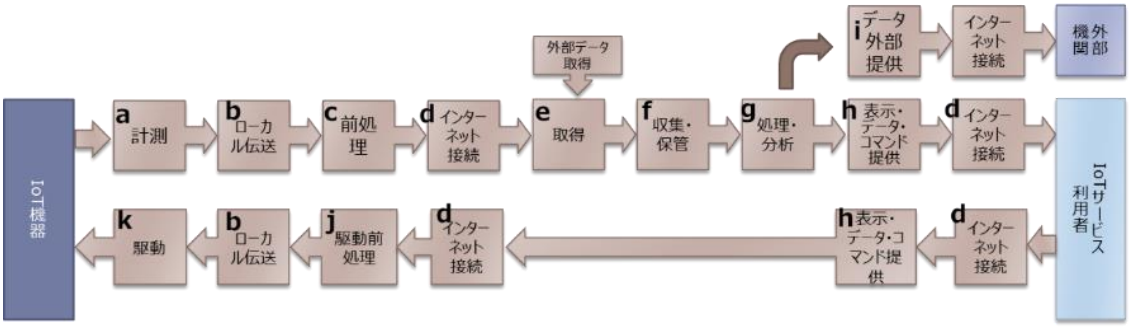
*下図中の番号を対応付けている

図表 15 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。

（V．４．３．C、V．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）

Ⅴ．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 16 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 17 に「ロールとコンポーネントの対応」を示した。

図表 16 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 17 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

Ⅴ．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、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
	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 が繋がる	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
		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	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

マンド提供、データ解析等）	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
		価値の高い、あるいは保護対象となるレベルのデータの海外流出	価値が高い等の我が国の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

Ⅴ．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、Ⅴ．２．２．A～Ⅴ．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。その結果を以下に示す。

A 多様な事業者連携（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
		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
		セキュリティリスク	ぜい弱性が残るリスク

	エッジコンピュータ		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

Ⅴ．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

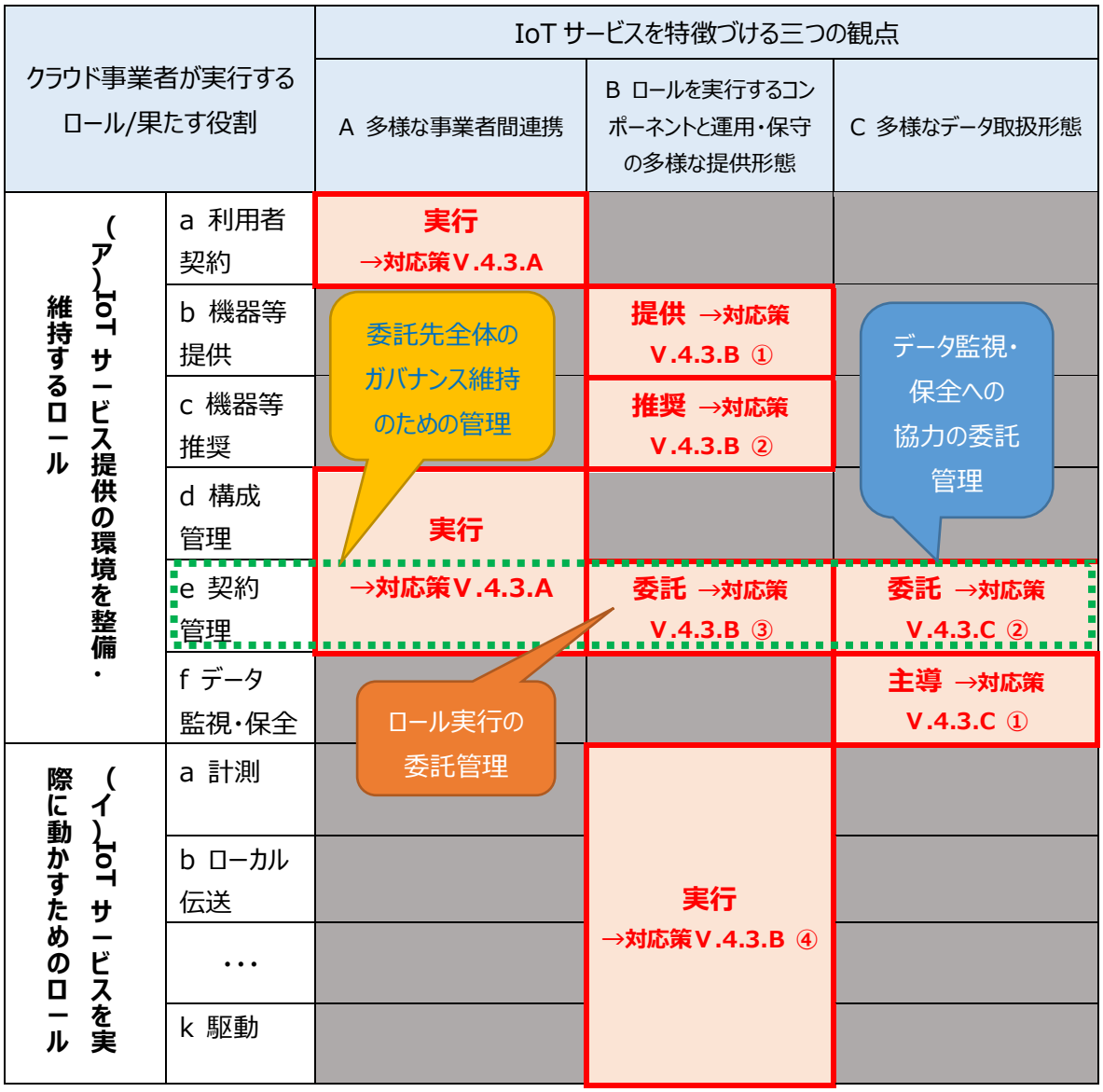
Ⅴ．４．１．対応策導出の流れ

Ⅴ．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Ⅴ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（Ⅴ．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 18（再掲）に取りまとめた。

凡例： Ⅴ.4.3.X → 「リスク対応策導出マップ」の記載箇所

図表 18 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－



Ｖ．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 19 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 19　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><td rowspan="2">クラウド事業者が実行するロール/果たす役割</td><td rowspan="2" colspan="2">調査項目</td><td colspan="3">クラウド事業者の責任範囲（記入欄）　※○×を記入する</td></tr>
<tr><td>A 多様な事業者連携</td><td>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</td><td>C 多様なデータ取扱形態</td></tr>
<tr><td rowspan="10">（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/ローカルコンピュータ</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>組込みアプリケーション</td><td></td><td></td></tr>
<tr><td>LAN</td><td></td><td></td></tr>
<tr><td>エッジコンピュータ</td><td></td><td></td></tr>
<tr><td>通信 GW</td><td></td><td></td></tr>
<tr><td>IaaS/PaaS</td><td></td><td></td></tr>
<tr><td>アプリケーション（データ解析）</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）</td><td></td><td></td></tr>
</table>

<table>
<tr><td rowspan="15"></td><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/ローカルコンピュータ</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>エッジコンピュータ</td><td></td><td></td></tr>
<tr><td>通信 GW</td><td></td><td></td></tr>
<tr><td>IaaS/PaaS</td><td></td><td></td></tr>
<tr><td>アプリケーション（データ解析）</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="10">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="9">事業連携先に委託するロール</td><td>a 計測</td><td></td><td rowspan="9">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></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>クラウド事業者がデータ内容を見る場合○</td></tr>
<tr><td rowspan="11">（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="11">クラウド事業者が自らロールを実行するか</td><td></td><td rowspan="11">クラウド事業者が自ら実行するロールに○</td><td></td></tr>
<tr><td>b ローカル伝送</td><td></td><td></td></tr>
<tr><td>c 前処理</td><td></td><td></td></tr>
<tr><td>d インターネット接続</td><td></td><td></td></tr>
<tr><td>e 取得</td><td></td><td></td></tr>
<tr><td>f 収集・保管</td><td></td><td></td></tr>
<tr><td>g 処理・分析</td><td></td><td></td></tr>
<tr><td>h 表示・データ・コマンド提供</td><td></td><td></td></tr>
<tr><td>i データ外部提供</td><td></td><td></td></tr>
<tr><td>j 駆動前処理</td><td></td><td></td></tr>
<tr><td>k 駆動</td><td></td><td></td></tr>
</table>

Ｖ．４．１．３．対応策導出の流れ

「Ｖ．４．１．１．」、「Ｖ．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 19 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 18、図表 20、Ｖ．４．３．参照）
③ 第 5 章の対応策一覧から、「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（Ｖ．５．A～Ｖ．５．C を参照）

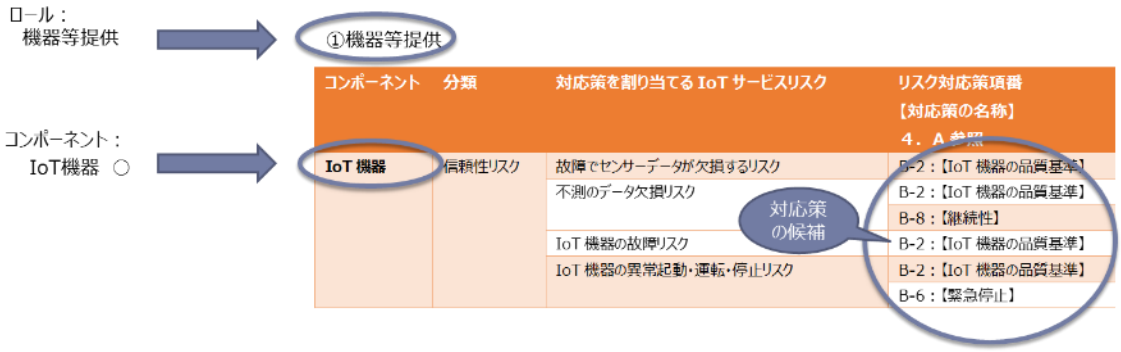
図表 20 リスク対応策導出マップの見方（1/3）

<table>
<tr><th colspan="2" 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="12">（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="5">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 rowspan="6">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 21 (3/3)参照）</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></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><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 21 (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 rowspan="4" colspan="2">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 21 リスク対応策導出マップの見方（2/3）

【B の機器等提供（V．4．3．B ①）】

※機器等推奨（V．4．3．B ②）も同じ図表形式



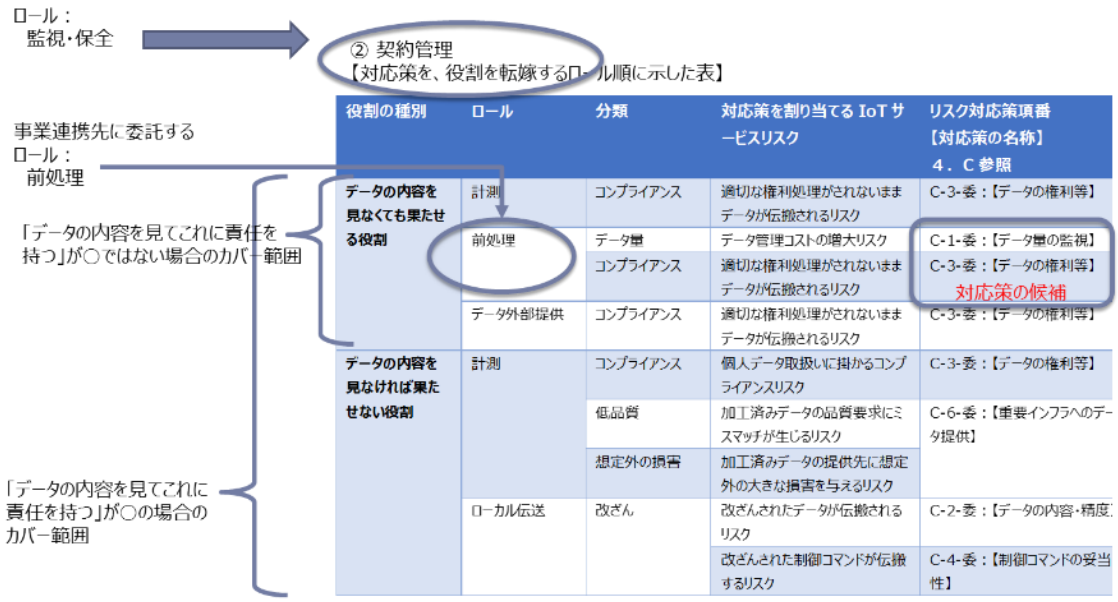
【B の契約管理（V．4．3．B ③）】

※IoT サービスを実際に動かすためのロール（V．4．3．B ④）も同じ図表形式

【C のデータ監視･保全（V．4．3．C ①）】

図表 21 リスク対応策導出マップの見方（3/3）

【C の契約管理（Ⅴ．４．３．C ②）】



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】４．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】
	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	計測	コンプライアンス	個人データ取扱いに掛か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】

（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。（Ⅴ．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）Ⅴ．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。

Ⅴ．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 22 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 ANNEX4 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 22 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 22　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/ローカルコンピュータ		○	
			組込みアプリケーション		×	
			LAN		○	
			エッジコンピュータ		○	
			通信 GW		○	
			IaaS/PaaS		○	
			アプリケーション（データ解析）		○	
			アプリケーション（表示・データ・コマンド提供）		○	
	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 GW		×	
			IaaS/PaaS		×	

			アプリケーション（データ解析）		×	
	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				○	

Ⅴ．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】Ⅴ．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、165 ページの 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】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。（Ⅴ．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】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。（Ⅴ．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）Ⅴ．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。

Ⅴ．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 多様な事業者連携

クラウド事業者が、多様な事業者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、又は、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、又は、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、又は、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】 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	❑ 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 ❑ 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が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組、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（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）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】 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 ❑ 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（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）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	❑ 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

		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	❑ 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 ❑ 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	❑ 制御コマンド提供の問題点の是正を主導する ❑ 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】	❑ 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】 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-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

参考資料

ANNEX1 クラウドサービスのパターン

クラウドサービス事業者が提供するサービスは、基幹系業務システムからソーシャルネットワーク(SNS)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。

本ガイドラインでは、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４パターンに分類している。また、この分類を基に各編での対策項目をパターン化している。

１．パターン化の考え方

「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１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】

完全性への要求は「高」いが、機密性・可用性への要求は「中」程度のサービス

【パターン 4】

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

図表１ 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	中	高	高
4	中	高	中

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】

クラウドサービスでは、利用者は、サービスを利用するために何らかの個人識別情報(アカウント ID 等)を利用する。また、クラウドサービス事業者は、この個人識別情報と利用者に関する情報を結びつけ、個人情報として利用者を管理している。よって、クラウドサービスでは個人情報を扱うことを前提に、機密性への要求度を判断する。

以下の情報資産を扱う場合には、機密性への要求は「高」い。

(1)特定個人情報

マイナンバーを内容に含む個人情報（行政手続における特定の個人を識別するための番号の利用等に関する法律第 2 条第 8 項）。

(2)要配慮個人情報

不当な差別、偏見その他の不利益が生じないように取扱いに特に配慮を要する記述等が含まれる個人情報（個人情報保護法第 2 条第 3 項）。取得にあたっては、あらかじめ本人の同意が必要。

(3)機密性 3 情報

政府機関の情報セキュリティ対策のための統一基準(平成 30 年度版)で定められた秘密情報。行政文書等で秘密情報に該当する情報資産。

以下の情報資産を扱う場合には、機密性への要求は「中」程度。

(1)個人情報

個人情報保護法第 2 条第 1 項に定める個人情報

(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】

クラウドサービス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、利用者の事業継続に多大な影響を与えるものと考える。また、クラウドサービス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利用者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、クラウドサービス事業者においては、そのサービス種別にかかわらず、完全性への要求は「高」いと考える。

【可用性への要求】

(1)可用性への要求が「高」程度のサービス

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

サービスが停止することで、利用者の業務に支障を来たし、場合によっては、経済的損失が生じるおそれのあるサービス

２．典型的サービスのパターン分類

上記に基づき、典型的なクラウドサービスについて、その特性を考慮してパターンごとに分類した結果が、図表 2 である。

図表 2　パターンごとのサービス種別

パターン	サービス種別
1	認証支援、勘定系支援、遠隔医療支援、福祉・介護業務支援
2	人事業務支援、e ラーニング
3	経理業務支援、電子商取引、営業支援、顧客管理、配送計画、倉庫管理、賃貸物件管理
4	ビッグデータ分析支援、コンテンツ配信、コミュニケーションツール、情報共有サービス

なお、図表 2 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 2 で分類されているパターンにそぐわない場合、図表 2 中に存在しない場合、等は、「1．パターンの考え方」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。

ANNEX2 対策一覧

項番	対策項目	対策内容	区分
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	**方針の作成・承認・配布**	クラウドサービス事業者は、組織全体での情報セキュリティに関する取組についての基本的な方針、役割、責任等を定めた文書を作成し、経営陣の承認及び署名等を経て、組織内及び関係する組織に配布すること。	基本
Ⅱ．１．１．２	**方針の変更**	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や不適合が生じた場合（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。事業者は、経営陣の承認の下で方針の改定等を実施し、組織内及び関係する組織に通知すること。	基本
Ⅱ．１．１．３	**文書保護**	事業者は、情報セキュリティに関する基本的な方針を定めた文書を、不正な開示や変更から保護すること。	推奨
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	**情報セキュリティ責任者**	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する。更に、組織全体にわたる情報セキュリティに責任を持つ情報セキュリティ責任者を任命し、人員・資産・予算等のリソース面で積極的な支援・支持を行うこと。	基本
Ⅱ．２．１．２	**システム一覧**	情報セキュリティ責任者は、組織が保有、提供するシステム、アプリケーション及びクラウドサービスの一覧を作成し、全ての責任者を定めるとともに、個々の組織の職務記述書にセキュリティとプライバシーに関する役割と責任を記載すること。	基本

Ⅱ．２．１．３	**相反する職務と責任の分離**	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、相反する職務及び責任範囲は、分離すること。	基本
Ⅱ．２．１．４	**リスク管理戦略**	情報セキュリティへの侵害が、業務、資産、個人、他の組織及びサプライチェーンへもたらす脅威に対するリスクを管理するために、組織全体の包括的なリスク管理戦略を策定する。リスク管理戦略は、定期的又はクラウドサービスの提供に係る変更が生じた場合（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。	推奨
Ⅱ．２．１．５	**テスト、トレーニング及び監視**	組織全体にわたって実施されるセキュリティテスト、プライバシーテスト、トレーニングを監視すること。	推奨
Ⅱ．２．１．６	**組織内苦情管理**	組織のセキュリティ施策とプライバシーの取組に対する従業員からの苦情、懸念又は質問を受け取り、対応するための仕組みを構築すること。	推奨
Ⅱ．２．２．モバイル機器及びテレワーキング			
Ⅱ．２．２．１	**モバイル機器の利用方針**	モバイル機器を業務で用いることによって生じるリスクを管理するために、モバイル機器の利用方針を策定し、その方針を実施するために必要な情報セキュリティ対策を講じること。	基本
Ⅱ．２．２．２	**テレワーキングでの情報保護**	テレワーキングでアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施すること。	基本
Ⅱ．３．サプライチェーンに関する管理			
Ⅱ．３．１．サプライチェーン事業者間の合意			
Ⅱ．３．１．１	**リスク対策と文書化**	サプライチェーン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リスク対策及びサービスレベルを文書化するとともに、サプライチェーン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	**サービスの監視**	サプライチェーン事業者が提供するクラウドサービスを定常的に監視・レビューし、運用に関する記録及び報告を常に実施すること。また、定期的に監査を実施することについて、サプライチェーン事業者と合意し文書化すること。	基本
Ⅱ．３．１．３	**リスク評価とレビュー**	サプライチェーン事業者が提供するシステム、システムコンポーネント、クラウドサービスに関連するサプライチェーン関連のリスクを評価及びレビューすることについて、サプライチェーン事業者と合意し文書化すること。	基本
Ⅱ．３．１．４	**関連情報の保護**	システム、システムコンポーネント、クラウドサービスに関するサプライチェーン関連情報を保護することについて、サプライチェーン事業者と合意し文書化すること。	基本
Ⅱ．３．１．５	**侵害通知**	サプライチェーンのセキュリティ侵害に関する通知について手順を確立し、サプライチェーン事業者と合意し文書化する。	基本
Ⅱ．３．１．６	**変更管理**	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に伴う、サプライチェーン事業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、手順及び対応策の保守及び改善を含む）を管理することについて、サプライチェーン事業者と合意し文書化すること。	基本
Ⅱ．３．１．７	**耐タンパー性と検出**	システム、システムコンポーネント、クラウドサービスの改ざん防止プログラムを実装することについて、サプライチェーン事業者と合意し文書化すること。	推奨
Ⅱ．３．１．８	**システム又はシステムコンポーネントの検査**	改ざんを検出するために、システム、システムコンポーネント又はクラウドサービスをランダムに検査することについて、サプライチェーン事業者と合意し文書化すること。	推奨
Ⅱ．３．１．９	**システムコンポーネントの信頼性**	偽造システムコンポーネントがシステムやクラウドサービスに侵入することを検出及び防止する手段を実装することについて、サプライチェーン事業者と合意し文書化すること。	推奨
Ⅱ．３．１．１０	**システムコンポーネントの廃棄**	データ、ドキュメント、ツール、又はシステムコンポーネントを破棄する方法を確立するとともに、廃棄方法についてサプライチェーン事業者と合意し文書化すること。	基本

Ⅱ．３．２．サプライチェーン事業者の選定			
Ⅱ．３．２．１．	**選定・契約**	サプライチェーン事業者のリスクからクラウドサービスを保護するために、状況に応じて最も適した取得・調達・契約方法を採用すること。	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．	**管理責任者**	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）を明確にした上で管理するとともに、文書化すること。	基本
Ⅱ．４．１．２．	**事業者間の引継ぎ**	クラウドサービス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。クラウドサービス利用者によるクラウドサービス選定の自由を守るため、事業者は預託された情報を他のクラウドサービスに引き継ぐか否かに関して、予め利用者と合意し、文書化すること。	基本
Ⅱ．４．１．３．	**バックアップ**	情報、ソフトウェア及びシステムのバックアップは、利用者と合意されたバックアップ方針に従って、事業者が定期的に実施し、バックアップ内容を検査すること。また、事業者は、利用者にバックアップ機能の仕様を提供すること。	基本
Ⅱ．４．１．４．	**当初目的との一致**	時間の経過とともに、当初の目的や提供機能の範囲外のサービス及び機能をサポートする場合があるが、情報資産が当初の目的と一致して使用されていることを確認すること。	推奨
Ⅱ．４．２．情報の分類			
Ⅱ．４．２．１．	**資産目録**	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、機密性や重要性の観点から情報資産を分類した上で、資産目録を作成し、維持すること。	基本

Ⅱ．４．２．２．	**データ識別**	事業者は、利用者のデータ及びクラウドサービスから派生したデータを明確に識別すること。	基本
Ⅱ．４．２．３．	**情報資産の取扱い**	情報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。	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．	**レビュー**	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に、定期的にレビュー及び見直しを行うこと。また、組織の情報セキュリティのための方針群及び標準に関し、システムや提供するクラウドサービスが、定めに従って技術的に順守されていることをレビューすること。	基本
Ⅱ．４．３．２．	**点検･監査**	クラウドサービスの提供に用いるシステムが、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、定期的に検証・監査すること。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、実施すること。	基本
Ⅱ．４．４．アクセス管理			
Ⅱ．４．４．１．	**アクセス制御方針**	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。また、情報及び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。	基本
Ⅱ．４．４．２．	**アクセス制御**	事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス及び利用者データへのアクセスを、利用者が制限できるようにアクセス制御を提供すること。	基本
Ⅱ．４．４．３．	**ユーティリティプログラムの使用**	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(データベースの中身を強制的に書き換えることが出来る機能や一時的にポートを開放する機能等)の使用は、制限し、厳しく管理すること。また、事業者は、ク	基本

		ラウドサービス内で利用される全てのユーティリティプログラムのための要求事項を特定すること。	
Ⅱ．４．４．４．	**プログラムソースコードへのアクセス**	プログラムソースコードへのアクセスは、制限すること。	基本
Ⅱ．４．４．５．	**アクセス制御となりすまし対策**	利用者及びシステム管理者等のアクセスを管理するために、適切な認証方法、特定の場所や装置からの接続を認証する方法等によって、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。	基本
Ⅱ．４．５．構成管理			
Ⅱ．４．５．１．	**構成管理のポリシーと手順**	目的・適用範囲・役割・責任・経営コミットメント・組織間の調整・コンプライアンスを取り扱う構成管理ポリシー及び構成管理ポリシーと関連する対応策の実施手順を策定・文書化すること。	基本
Ⅱ．４．５．２．	**ベースライン構成**	システムの最新のベースライン構成、システムコンポーネント一覧を把握・文書化すること。	推奨
Ⅱ．４．５．３．	**構成変更管理**	構成管理の対象となるシステムに対する変更について定めるとともに、変更内容をレビューし、セキュリティへの影響を考慮した上で変更を許可すること。また、変更に関する関連の活動を監査し、レビューすること。	推奨
Ⅱ．４．５．４．	**変更に対するアクセス制限**	システムに対する変更に関して、物理的／論理的なアクセス制限を定義・文書化・承認のうえ実施すること。	推奨
Ⅱ．４．５．５．	**設定項目**	運用上の要求事項に適合し、最も制限された運用を実現するためのセキュリティ設定に関するチェックリストを使用して、システムに導入されている製品の設定項目を把握し文書化すること。	推奨

Ⅱ．４．５．６．	**ソフトウェアの使用制限**	契約上の取り決めと著作権法に従ってソフトウェアと関連ドキュメントを使用するとともに、ライセンスの数によって保護されるソフトウェアと関連ドキュメントの使用をモニタリングし、それらが複製されないようにすること	推奨
Ⅱ．４．５．７．	**クラウドサービス利用者によるソフトウェアのインストール**	利用者によるソフトウェアのインストールを管理するためのポリシーを確立するとともにポリシーが遵守されていることをモニタリングすること。	推奨
Ⅱ．４．５．８．	**情報の場所**	情報の場所と、情報が処理及び保存されるシステムコンポーネントを特定して文書化すること。また、個人を特定できる情報がどのように処理されているかについて文書化すること。	推奨
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．	**雇用契約**	雇用予定の従業員(就業形態に関わらず)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．	**教育・訓練**	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．	**教育のフィードバック**	組織のトレーニング結果を情報セキュリティ責任者にフィードバックすること。	推奨
Ⅱ．５．２．３．	**契約違反**	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．	**アクセス権・資産の取扱い**	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．	**組織内報告**	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．６．１．２．	**クラウドサービス事業者とクラウドサービス利用者間の報告**	事業者は、利用者が情報セキュリティ事象を事業者に報告する仕組み、事業者が情報セキュリティ事象を利用者に報告する仕組み及び利用者が報告を受けた情報セキュリティ事象の状況を追跡する仕組みを提供すること。	基本
Ⅱ．６．１．３．	**インシデントの評価と分類**	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。	基本
Ⅱ．６．１．４．	**フィードバック**	情報セキュリティインシデントの分析及び解決から得られた知識は、情報セキュリティインシデントが将来起こる可能性又はその影響を低減するために用いること。	基本
Ⅱ．６．１．５．	**証拠の収集・取得**	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。	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．	**関連法規と記録**	個人情報、要配慮個人情報、プライバシー情報、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。また、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、法令、契約及び情報セキュリテ	基本

		ィポリシー等の要求事項に従って、適切に管理するとともに、利用者から求められたときには提供すること。	
Ⅱ．７．１．２．	**利用可否**	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にシステム及び情報処理施設を利用させないこと。	基本
Ⅱ．７．１．３．	**ソフトウェア製品**	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。	基本
Ⅱ．７．１．４．	**不正アクセス・流出からの保護**	記録は、法令、規制、契約及び事業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。また、事業者は、利用者によるクラウドサービスの利用に関連して、事業者が収集し、保存する記録の保護に関する情報を、利用者に提供すること。	基本
Ⅱ．７．１．５．	**暗号化**	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とともに、利用者が法令及び規制の順守をレビューできるようにするために、事業者は実施している暗号による対応策を記載すること。	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．	**責任**	クラウドサービスの提供に支障が生じた場合には、その原因がサプライチェーンの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
Ⅱ．８．１．２．	**SLA**	事業者自身の責任範囲を SLA 等により文書化し、クラウド利用者に明確に示すこと。	基本
Ⅱ．８．１．３．	**情報提供**	クラウドサービスの新規利用/変更を計画しているクラウド利用者への情報提供にあたっては、組織のガバナンス規定を順守した上で、クラウド利用者が、必要な統制	基本

		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事業者を選定できるようにすること。	
Ⅱ．８．１．４．	**クラウドサービス利用者からの苦情対応**		基本
Ⅱ．８．２．保守			
Ⅱ．８．２．１．	**システム保守ポリシーと手順**	システム保守の目的、適用範囲、役割、責任、経営コミットメント、組織間の調整及び保守ポリシーを策定、文書化し、関係する組織に配布すること。	基本
Ⅱ．８．２．２．	**保守管理**	保守契約、保守仕様書及び要求事項に従って、保守・修理を計画、実施、文書化し、記録をレビューすること。	基本
Ⅱ．８．２．３．	**保守ツール**	システムの保守ツールを承認・管理し、モニタリングするとともに、以前の保守ツール使用状況レビューすること。	基本
Ⅱ．８．２．４．	**リモート保守**	リモート保守及び診断を承認のうえモニタリングする。リモート保守及び診断用ツールは、組織のポリシーに沿い、かつシステムのセキュリティ計画に記載されている通りである場合のみ、使用を許可すること。また、リモート保守及び診断のためのセッションを確立する際には、厳格な認証機能を使用するのに加え、リモート保守及び診断の記録を保管すること。リモート保守が完了したら、セッションとネットワーク接続を終了すること。	基本
Ⅱ．８．２．５．	**保守要員**	保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を維持すること。	基本
Ⅱ．８．２．６．	**保守要員による保守**	保守要員が付添いなしで保守を行う場合、その要員が必要なアクセス権限を有することを確認すること。また、必要なアクセス権限を持たない要員による保守活動を監督するために、必要なアクセス権限と技術的能力を有する職員を指定すること。	基本
Ⅱ．８．２．７．	**タイムリーな保守**	システムコンポーネントに障害が発生した場合、保守サポート契約に基づき、保守サポートを行うこと。	基本

Ⅱ．９．事業継続マネジメントにおける情報セキュリティ			
Ⅱ．９．１．情報セキュリティの継続			
Ⅱ．９．１．１．	**情報セキュリティ継続計画の策定と実施**	組織は、大規模災害等における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定するとともに、プロセス・手順・対策を確立、文書化し、実施、維持すること。	基本
Ⅱ．９．１．２．	**情報セキュリティ継続の検証、レビュー及び評価**	情報セキュリティ継続のための対策が、大規模災害等の下で妥当かつ有効であることを確認するために、組織は、定められた間隔でこれらの対策を検証すること。	基本
Ⅱ．９．２．緊急時対応計画			
Ⅱ．９．２．１．	**緊急時対応計画の策定と手順**	目的・適用範囲・役割・責任・経営コミットメント、組織間の調整及びコンプライアンスを取り扱う緊急時対応計画を策定するとともに、「緊急時対応計画」の実施手順を策定・文書化すること。	基本
Ⅱ．９．２．２．	**緊急時対応トレーニング**	利用者に対して、役割と責任に応じた緊急時対応トレーニングを実施すること。	推奨
Ⅱ．９．２．３．	**緊急時対応計画のテスト**	緊急時対応計画の有効性を判断して計画の欠陥を特定するために、緊急時対応計画のテストを実施すること。	推奨
Ⅱ．９．２．４．	**代替処理サイト**	利用者とシステムバックアップ情報の保存と取得を許可するための契約を締結するとともに、代替処理サイトを確立すること。また、代替処理サイトがプライマリサイトと同等の管理機能を提供することを確認すること。	推奨
Ⅱ．９．２．５．	**代替処理サイトで再開**	代替処理サイトを定め、利用者と合意した目標復旧時間内に、システムオペレーションを移転・再開して、極めて重要なミッション／業務機能を遂行できるようにすること。	推奨
Ⅱ．９．２．６．	**通信サービス**	一次処理サイトや代替処理サイトのいずれかにおいて一次通信サービスが利用できない場合に、極めて重要なミッションや業務機能を支援する代替通信サービスを確立すること。	推奨

Ⅱ．９．２．７．	**システムの復旧と再構成**	システムの途絶、侵害、又は不具合が発生した場合に、システムを従前の状態に復旧し、再構成できるようにすること。	推奨
Ⅱ．９．２．８．	**代替通信プロトコル**	利用者が、業務の継続性を維持するために組織が定めた代替通信プロトコルを使用できるようにすること。	推奨
Ⅱ．９．２．９．	**代替のセキュリティ対策**	組織が定めたセキュリティ機能を実施するための主な手段が利用できない場合、又は侵害された場合に、それらのセキュリティ機能を満たすための代替の、又は補助的なセキュリティ対策を実装すること。	推奨
Ⅱ．１０．その他			
Ⅱ．１０．１．暗号と認証			
Ⅱ．１０．１．１．	**方針**	情報を保護するための暗号利用に関する方針を、策定し、実施すること。	基本
Ⅱ．１０．１．２．	**情報提供**	事業者は、利用者に、事業者が処理する情報を保護するために、暗号を利用する環境に関する情報を提供すること。また、事業者は、利用者自らの暗号による保護を適用することを支援するために、事業者が提供する能力についても利用者に情報を提供すること。	基本
Ⅱ．１０．１．３．	**暗号鍵の作成と管理**	組織が定めた方針に従って、システム内で使用する暗号鍵を生成・配布・保管・アクセス・廃棄すること。	基本
Ⅱ．１０．２．開発プロセスにおけるセキュリティ			
Ⅱ．１０．２．１．	**開発プロセスにおける情報セキュリティへの取組**	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。	基本
Ⅲ．１．運用における情報セキュリティ			
Ⅲ．１．１．運用管理			
Ⅲ．１．１．１．	**情報セキュリティ監視手順の策定**	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の運	基本

		用・管理に関する手順書を作成すること。	
Ⅲ．１．１．２．	**運用管理端末**	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ファイルのウイルスチェックを行うこと。	基本
Ⅲ．１．１．３．	**稼働・障害監視**	クラウドサービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行うこと。稼働停止や異常を検知した場合は、クラウドサービス利用者に速報すること。また、結果を評価・総括して、管理責任者に報告すること。	基本
Ⅲ．１．１．４．	**追加報告**	クラウドサービスの提供に用いるアプリケーションに係る稼働停止、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クラウドサービス利用者に対して行うこと。	基本
Ⅲ．１．１．５．	**定期報告**	クラウドサービスの提供に用いるアプリケーションの監視結果、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。	基本
Ⅲ．１．１．６．	**時刻同期**	クラウドサービスの提供に用いるアプリケーションの時刻同期の方法を規定し、実施すること。	基本
Ⅲ．１．１．７．	**パスワード管理**	パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にすること。	基本
Ⅲ．１．１．８．	**クラウドサービスの変更管理**	情報セキュリティに影響を与える組織、業務プロセス及びシステムの変更を管理すること。また、事業者は、クラウドサービスに影響を与える可能性のあるクラウドサービスの変更について、利用者に情報を提供すること。	基本
Ⅲ．１．１．９．	**リソース監視**	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。また、事業者は、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を	基本

		監視すること。	
Ⅲ．１．１．１０．	**環境分離**	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために分離すること。	基本
Ⅲ．１．１．１１．	**マルウェア対策**	マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。	基本
Ⅲ．１．１．１２．	**イベントログの取得**	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。また、事業者は、利用者に、ログ取得機能を提供すること。	基本
Ⅲ．１．１．１３．	**ログの保護**	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。	基本
Ⅲ．１．１．１４．	**作業記録**	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。	基本
Ⅲ．１．１．１５．	**ソフトウェア導入**	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。	基本
Ⅲ．１．１．１６．	**技術的ぜい弱性**	利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに獲得すること。.また、そのようなぜい弱性に組織がさらされている状況を評価すること。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。また、事業者は、提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。	基本
Ⅲ．１．２．システム及び情報の完全性			
Ⅲ．１．２．１．	**原本性確保**	電子データの原本性確保を行うこと。	基本
Ⅲ．１．２．２．	**メモリ保護**	許可されていない不正なコード実行からシステムメモリを保護するために、セキュリティ対策を実施すること。	推奨
Ⅲ．１．２．３．	**セキュリティ侵害の検知**	システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたり、不適切に変更、削除されたりしたかを検知すること。	基本
Ⅲ．１．２．４．	**情報の更新**	不要になった情報は削除すること。	推奨

Ⅲ．１．２．５．	**代替情報源**	主要な情報源が破損しているか利用できない場合、システム又はシステムコンポーネントが重要な機能又はサービスを実行するための代替情報源を使用すること。	推奨
Ⅲ．１．２．６．	**情報の断片化**	一度システムに侵入されると、失われた情報を回復する方法は、通常は存在しない。組織は、情報を異なる要素に分割し、それらの要素を複数のシステム又はシステムコンポーネントと場所に分散すること。	推奨
Ⅲ．１．３．媒体の保管と廃棄			
Ⅲ．１．３．１．	**媒体保管**	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。	基本
Ⅲ．１．３．２．	**廃棄**	機器及び媒体を正式な手順に基づいて廃棄すること。	基本
Ⅲ．１．３．３．	**輸送**	情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。	基本
Ⅲ．２．アプリケーション			
Ⅲ．２．１．アプリケーションの情報セキュリティ対策			
Ⅲ．２．１．１．	**ウイルス対策**	クラウドサービスの提供に用いるアプリケーション（データ・プログラム等）についてウイルス等に対する対策を講じること。	基本
Ⅲ．２．１．２．	**公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮**	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護すること。	基本
Ⅲ．２．１．３．	**アプリケーションサービスのトランザクションの保護**	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、 保護すること。 ・不完全な通信 ・誤った通信経路設定 ・認可されていないメッセージの変更 ・認可されていない開示	基本

		・認可されていないメッセージの複製又は再生	
Ⅲ．２．１．４．	**プラットフォーム変更後のアプリケーションの技術的レビュー**	プラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験すること。	基本
Ⅲ．２．１．５．	**パッケージソフトウェアの変更に対する制限**	パッケージソフトウェアの変更は、必要な変更だけに限ることが望ましい。また、全ての変更を厳重に管理すること。	基本
Ⅲ．２．２．データの保護			
Ⅲ．２．２．１．	**バックアップ**	利用者のデータ、アプリケーション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。	基本
Ⅲ．２．２．２．	**バックアップ情報の完全性**	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。	基本
Ⅲ．２．３．セッション管理			
Ⅲ．２．３．１．	**セッションのライフサイクル管理**	セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。	基本
Ⅲ．２．３．２．	**セッションの真正性**	通信セッションの真正性を保護すること。	基本
Ⅲ．２．３．３．	**同時セッションの制御**	同時処理されるアカウントの割り当て数、又はアカウントタイプの割り当て数は、システムが定めた各セッションの割り当て数まで制限すること。	基本
Ⅲ．２．３．４．	**セッションのロック**	定められたアイドル時間を経過した場合、又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。	基本
Ⅳ．１．運用における情報セキュリティ			
Ⅳ．１．１．運用管理			
Ⅳ．１．１．１．	**情報セキュリティ監視手順の策定**	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、通信機器の運用・管理に関する手順書を作成すること。	基本

Ⅳ．１．１．２．	**運用管理端末**	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ファイルのウイルスチェックを行うこと。	基本
Ⅳ．１．１．３．	**稼働・障害監視**	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、通信機器の稼働監視、障害監視、パフォーマンス監視を行うこと。稼働停止や異常を検知した場合は、利用者に速報すること。また。結果を評価・総括して、管理責任者に報告すること。	基本
Ⅳ．１．１．４．	**追加報告**	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クラウドサービス利用者に対して行うこと。	基本
Ⅳ．１．１．５．	**定期報告**	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。	基本
Ⅳ．１．１．６．	**時刻同期**	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、通信機器の時刻同期の方法を規定し、実施すること。	基本
Ⅳ．１．１．７．	**パスワード管理**	パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとすること。	基本
Ⅳ．１．１．８．	**クラウドサービスの変更管理**	情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更を管理すること。また、事業者は、クラウドサービスに悪影響を与える可能性のあるクラウドサービスの変更について、利用者に情報を提供すること。	基本
Ⅳ．１．１．９．	**リソース監視**	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。また、事業者は、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を監視すること。	基本

Ⅳ．１．１．１０．	**環境分離**	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離すること。	基本
Ⅳ．１．１．１１．	**マルウェア対策**	マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。	基本
Ⅳ．１．１．１２．	**イベントログの取得**	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。また、事業者は、利用者に、ログ取得機能を提供すること。	基本
Ⅳ．１．１．１３．	**ログの保護**	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。	基本
Ⅳ．１．１．１４．	**作業記録**	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。	基本
Ⅳ．１．１．１５．	**ソフトウェア導入**	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。	基本
Ⅳ．１．１．１６．	**技術的ぜい弱性**	利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに獲得すること。.また、そのようなぜい弱性に組織がさらされている状況を評価すること。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。また、事業者は、提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。	基本
Ⅳ．１．２．システム及び情報の完全性			
Ⅳ．１．２．１．	**原本性確保**	電子データの原本性確保を行うこと。	基本
Ⅳ．１．２．２．	**メモリ保護**	許可されていないコードの実行からメモリを保護するための、セキュリティ対策を実施すること。	推奨
Ⅳ．１．２．３．	**セキュリティ侵害の検知**	システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたか、不適切に削除されたかを判断すること。	基本
Ⅳ．１．２．４．	**情報の更新**	不要になった情報は削除すること。	推奨

Ⅳ．１．２．５．	**代替情報源**	主要な情報源が破損しているか利用できない場合、システム又はシステムコンポーネントが重要な機能又はサービスを実行するための代替情報源を使用すること。	推奨
Ⅳ．１．２．６．	**情報の断片化**	一度システムに侵入されると、失われた情報を回復する方法は、通常は存在しない。組織は、情報を異なる要素に断片化し、それらの要素を複数のシステム又はシステムコンポーネントと場所に分散すること。	推奨
Ⅳ．１．３．媒体の保管と廃棄			
Ⅳ．１．３．１．	**媒体保管**	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。	基本
Ⅳ．１．３．２．	**廃棄**	機器及び媒体を正式な手順に基づいて廃棄すること。	基本
Ⅳ．１．３．３．	**輸送**	情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。	基本
Ⅳ．２．プラットフォーム、サーバ・ストレージ			
Ⅳ．２．１．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.			
Ⅳ．２．１．１．	**ウイルス対策**	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・ストレージについてウイルス等に対する対策を講じること。	基本
Ⅳ．２．２．プラットフォーム、サーバ・ストレージの運用・管理			
Ⅳ．２．２．１．	**可用性**	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、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。	基本
Ⅳ．２．２．２．	**リソース**	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。	基本
Ⅳ．２．３．データの保護			

Ⅳ．２．３．１．	**バックアップ**	利用者のサーバ・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。	基本
Ⅳ．２．３．２．	**バックアップ情報の完全性**	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。	基本
Ⅳ．３．ネットワーク			
Ⅳ．３．１．ネットワークにおける情報セキュリティ対策			
Ⅳ．３．１．１．	**ネットワーク構成**	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。	基本
Ⅳ．３．１．２．	**管理者の権限**	情報セキュリティ責任者は、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。	基本
Ⅳ．３．１．3.	**不正アクセス防止**	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。	基本
Ⅳ．３．１．4.	**パケット検知**	不正な通過パケットを自動的に発見、若しくは遮断する措置を講じること。	基本
Ⅳ．３．１．5.	**実施基準**	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。	基本
Ⅳ．３．１．6.	**通信の暗号化**	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。	基本
Ⅳ．３．１．7.	**サーバ証明書**	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。	基本

Ⅳ．３．１．８.	**情報セキュリティ特性**	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。	基本
Ⅳ．３．１．９.	**障害監視**	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。	基本
Ⅳ．３．１．１０.	**クロス･ドメイン･ポリシーの実施**	論理的に接続するセキュリティドメインの物理インターフェイスやネットワークインターフェイス間にポリシー施行メカニズムを実装すること。	推奨
Ⅳ．３．１．１１.	**統制管理のための代替通信パス**	指揮統制のために代替通信パスを確立すること。	推奨
Ⅳ．３．１．１２.	**検出機器の再配置**	攻撃者が目標を達成する能力を妨げるために、センサー又は監視機能を新しい場所に再配置すること。	推奨
Ⅳ．３．１．１３.	**ハードウェア/ソフトウェアによる分離とポリシーの施行**	セキュリティドメイン間にハードウェア/ソフトウェアによる分離とポリシーの適用メカニズムを実装すること。	推奨
Ⅳ．３．１．１４.	**ハードウェアベースの書き込み保護**	システムファームウェアコンポーネントにハードウェアベースの書き込み保護を採用すること。	推奨
Ⅳ．３．２．情報の転送			
Ⅳ．３．２．１.	**情報転送の方針及び手順**	あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び対策を備えること。	基本
Ⅳ．３．２．２.	**情報転送に関する合意**	組織と外部関係者との間で、業務情報のセキュリティを保った転送について、合意すること。	基本
Ⅳ．３．２．３.	**秘密保持契約又は守秘義務契約**	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。	基本
Ⅳ．３．３．セッション管理			
Ⅳ．３．３．１.	**セッションのライフサイクル管理**	セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。	基本

Ⅳ．３．３．２．	セッションの真正性	システムは、通信セッションの真正性を保護すること。	基本
Ⅳ．３．３．３．	同時セッションの制御	同時処理されるアカウントの割り当て数、又はアカウントタイプの割り当て数は、システムが定めた各セッションの割り当て数まで制限すること。	基本
Ⅳ．３．３．４．	セッションのロック	定められたアイドル時間を経過した場合　又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。	基本
Ⅳ．４．建物、電源(空調等)			
Ⅳ．４．１．建物の災害対策			
Ⅳ．４．１．１．	建物	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、物理的及び環境上の危険を考慮して、システムが存在する施設の場所を計画すること。また、地震・水害に対する対策が行われていること。	基本
Ⅳ．４．１．２．	電源	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。	基本
Ⅳ．４．１．３．	空調	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。	基本
Ⅳ．４．２．火災、雷、静電気からシステムを防護するための対策			
Ⅳ．４．２．１．	汚損対策	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。	基本

Ⅳ．４．２．２．	**火災対策**	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。	基本
Ⅳ．４．２．３．	**雷対策**	情報処理施設に雷が直撃した場合及び誘導雷が発生した場合を想定した対策を講じること。	基本
Ⅳ．４．２．４．	**静電気対策**	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システムについて、作業に伴う静電気対策を講じること。	基本
Ⅳ．４．２．５．	**緊急遮断**	緊急時に、システム又は個々のシステムコンポーネントの電源を遮断できる機能を提供するとともに、緊急時に電源を遮断する機能が、不正に起動されないようにすること>	基本
Ⅳ．４．２．６．	**非常用電源**	一次電源が失われた場合に、長期間使用可能な代替電源への切り替えを支援する、短期無停電電源装置を用意すること。	基本
Ⅳ．４．２．７．	**非常用照明**	停電が発生した場合や、電力が途絶えた場合に作動し、施設内の非常口と避難経路を照らす自動非常用照明をシステムに導入し、維持すること。	基本
Ⅳ．４．２．８．	**電磁パルス保護対策**	システム及びシステムコンポーネントの電磁パルス損傷に対して保護対策を講じること。	推奨
Ⅳ．４．３．装置の対策			
Ⅳ．４．３．１．	**サポートユーティリティ**	装置は、サポートユーティリティの不具合による、停電、その他の故障から保護すること。	基本
Ⅳ．４．３．２．	**ケーブル配線のセキュリティ**	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護すること。	基本
Ⅳ．４．３．３．	**装置の保守**	装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守すること。	基本

Ⅳ．４．３．４．	**資産の移動**	装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さないこと。	基本
Ⅳ．４．３．５．	**構外にある装置及び情報資産のセキュリティ**	構外にある情報資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、 セキュリティを適用すること。	基本
Ⅳ．４．３．６．	**装置のセキュリティを保った処分又は再利用**	記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを全て消去していること、若しくはセキュリティを保って上書きしていることを検証すること。	基本
Ⅳ．４．３．7．	**無人状態にあるクラウドサービス利用者装置**	利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にすること。	基本
Ⅳ．４．３．8．	**クリアデスク・クリアスクリーン方針**	書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用すること。	基本
Ⅳ．４．４．建物の情報セキュリティ対策			
Ⅳ．４．４．１．	**オフィス、部屋及び施設のセキュリティ**	オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用すること。	基本
Ⅳ．４．４．２．	**セキュリティを保つべき領域での作業**	セキュリティを保つべき領域での作業に関する手順を設計し、適用すること。	基本
Ⅳ．４．４．３．	**入退室記録**	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の手順書と記録を作成し、適切な期間保存すること。	基本
Ⅳ．４．４．４．	**監視カメラ**	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。	基本
Ⅳ．４．４．５．	**破壊対策ドア**	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。	基本
Ⅳ．４．４．６．	**警備員**	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。	基本
Ⅳ．４．４．７．	**鍵管理**	サーバルームやラックの鍵管理を行うこと。	基本

Ⅳ．４．４．８．	**受渡場所**	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理すること。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から可能な限り離すこと。	基本
Ⅳ．４．４．９．	**搬入と搬出**	施設に搬入・搬出されるシステムコンポーネントに対して許可・未許可、モニタリング、及び管理を行い、それらについての記録を保管すること。	基本

ANNEX3 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９参照）。

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

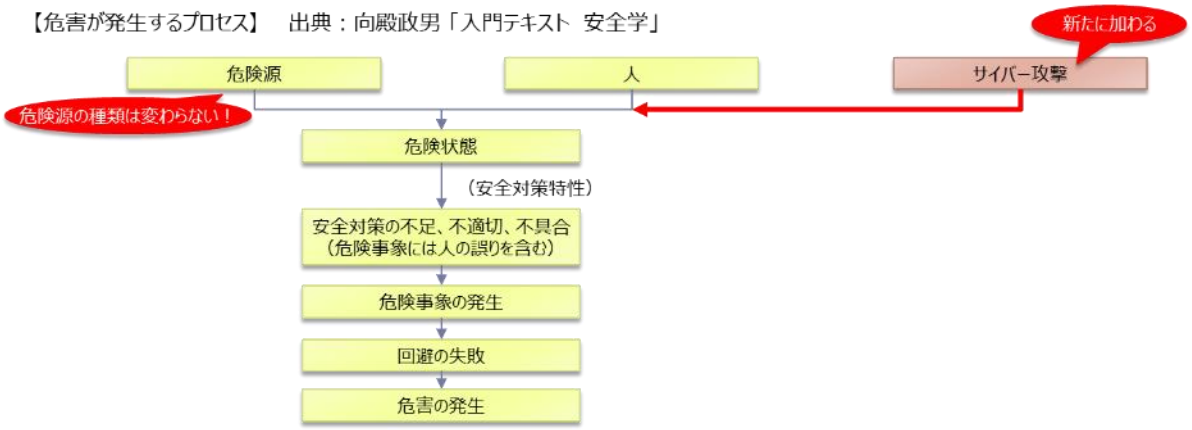
モノのリスクは、クラウドサービスでは見ることがなかった IoT サービスに特徴的なものである。IoT 機器へのサイバー攻撃によって、以下の二つのリスク（以下「セーフティリスク」という。）のどちらか一つでも発現しうる場合は、モノの安全の国際標準に従ったリスク対応が必要になる。

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 ANNEX3- 1 参照）がなされていない、又は、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、又は、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 ANNEX3- 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組、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。

ANNEX4【事例集】調査テンプレートの記入例

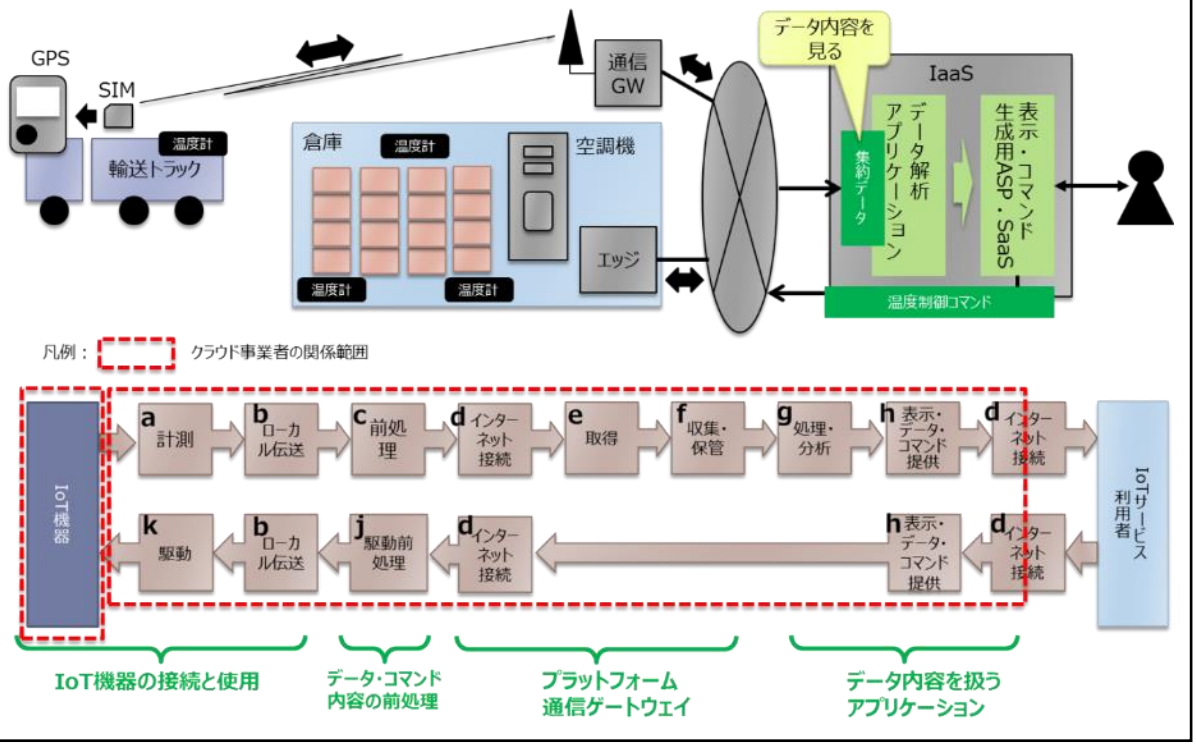
クラウド事業者が自ら提供する IoT サービスにおいて、どこまでが自らの責任範囲であるかを把握するために、図表 19 の調査テンプレートを活用することができる。ここでは、特徴の異なる六つの IoT サービスを事例として、「Ⅴ．４．１．２クラウド事業者の責任範囲の把握」の図表 19 の記入例を提示する。

【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８参照）	
			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】

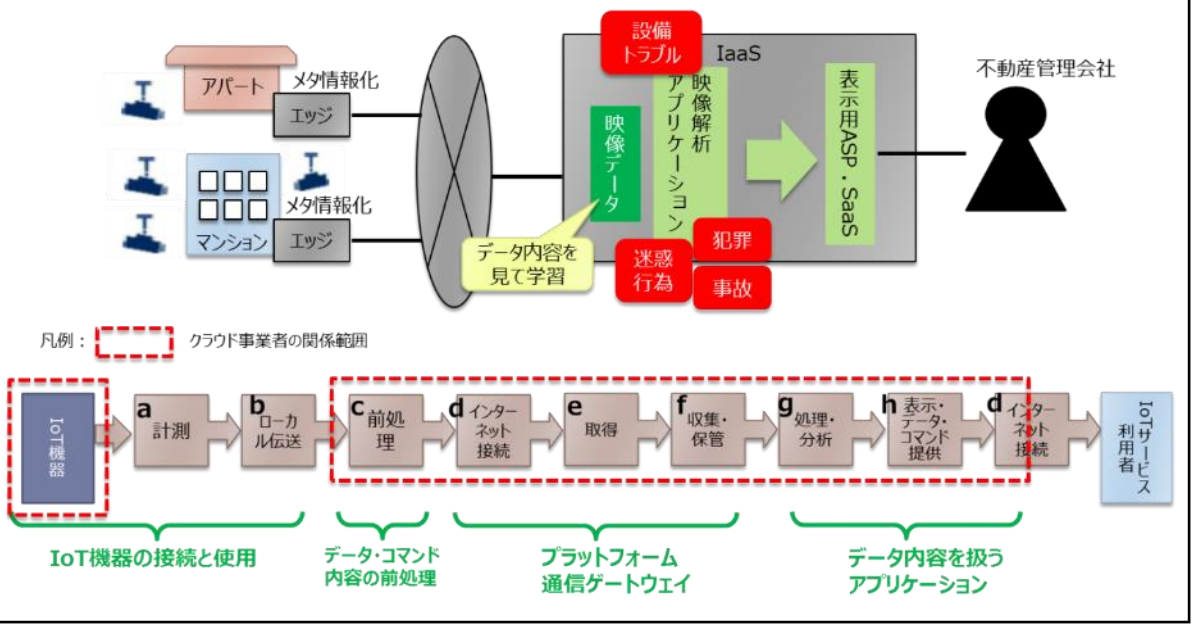
クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器/ローカルコンピュータ		○	
			組込みアプリケーション		×	
			LAN		○	
			エッジコンピュータ		○	
			通信 GW		○	
		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

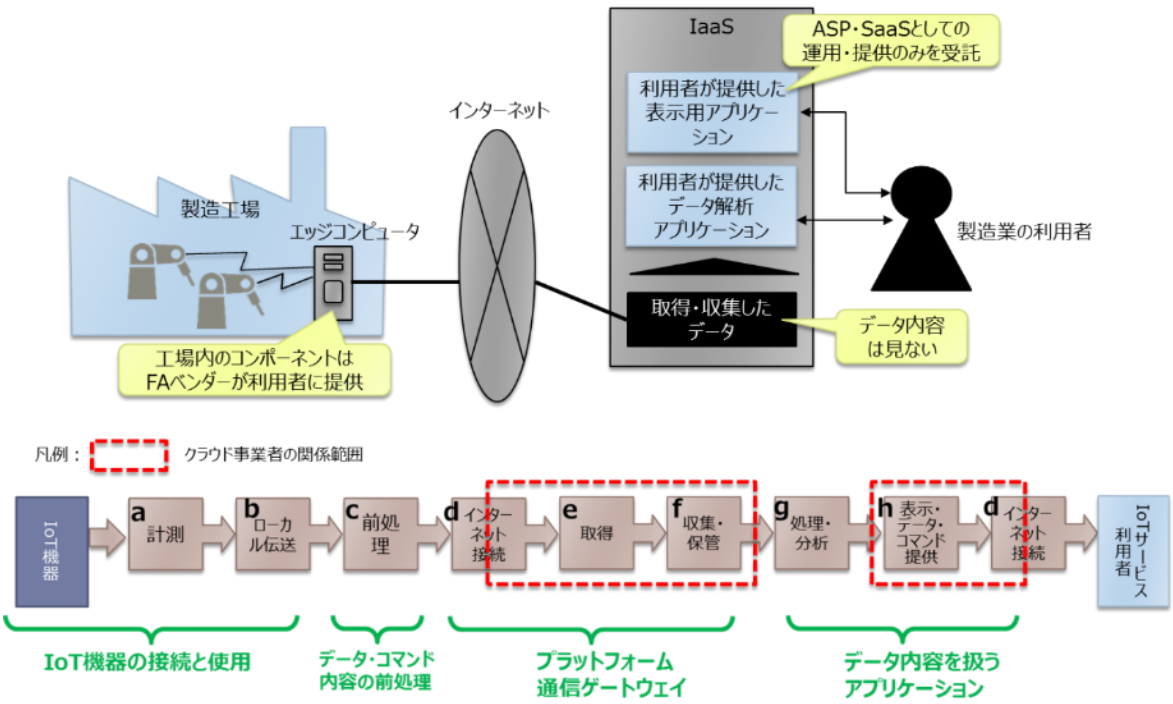
クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器/ローカルコンピュータ		×	
			組込みアプリケーション		×	
			LAN		×	
			エッジコンピュータ		○	
			通信 GW		×	
		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

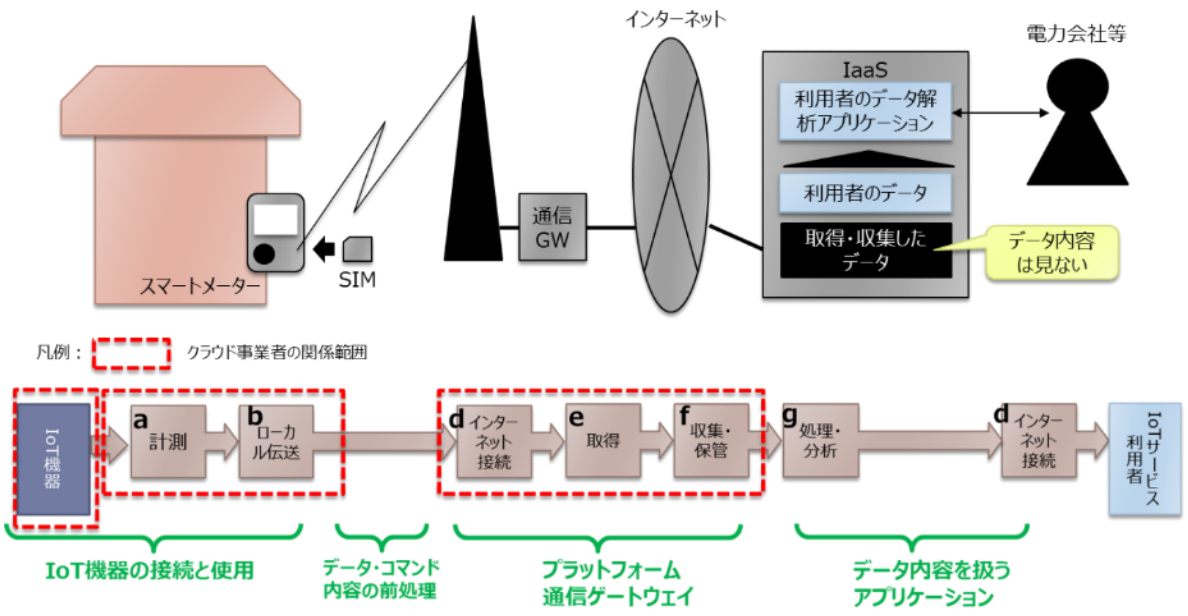
クラウド事業者が実行するロール/果たす役割		調査項目		クラウド事業者の責任範囲（記入欄） ※○×を記入する		
				A 多様な事業者連携	B ロールを実行するコンポーネントと運用・保守の多様な提供形態	C 多様なデータ取扱形態
（ア）IoTサービスの提供環境を整備・維持するロール	a 利用者契約	全てのクラウド事業者が該当する		○		
	b 機器等提供（クラウド事業者が自ら機器を提供する場合）	提供するコンポーネント	IoT 機器/ローカルコンピュータ		×	
			組込みアプリケーション		×	
			LAN		×	
			エッジコンピュータ		×	
			通信 GW		×	
		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

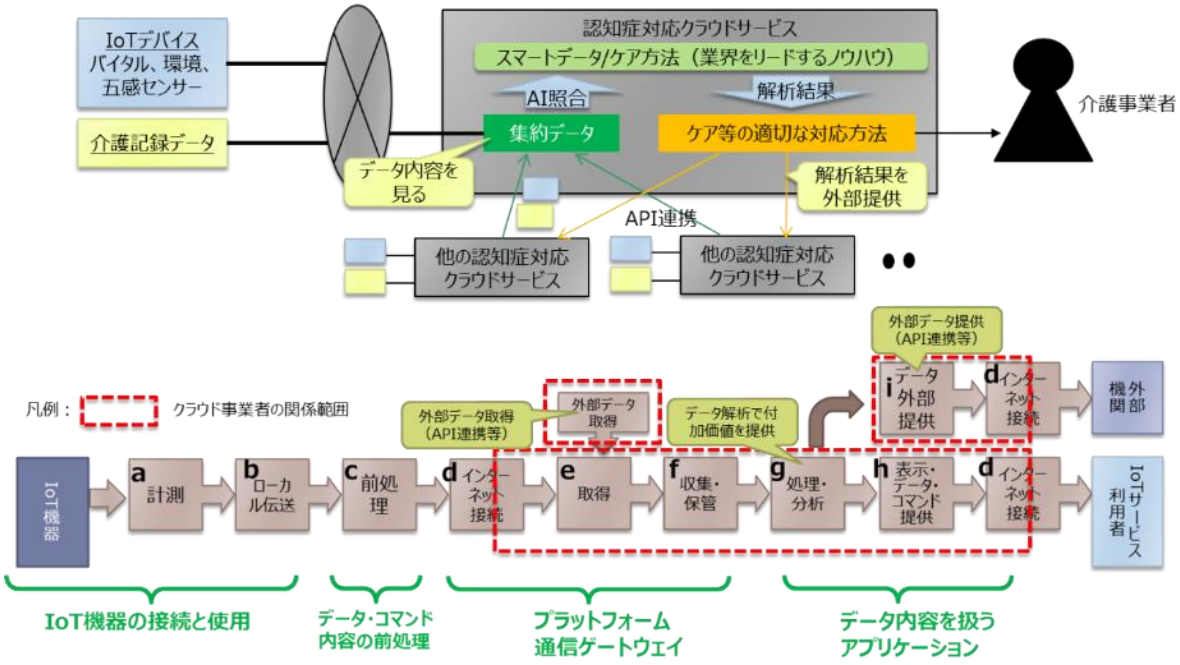
					（提供なし）	
			j 駆動前処理		×	*データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				×
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			×	
	b ローカル伝送				○	
	c 前処理				×	
	d インターネット接続				○	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				×	
	h 表示・データ・コマンド提供				×	
	i データ外部提供				× （提供なし）	
	j 駆動前処理				×	
	k 駆動				×	

（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/ローカルコンピュータ		×	
			組込みアプリケーション		×	
			LAN		×	
			エッジコンピュータ		×	
			通信 GW		×	
			IaaS/PaaS		○	
			アプリケーション（データ解析）		○	
			アプリケーション（表示・データ・コマンド提供）		○	
	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 GW		×	
			IaaS/PaaS		×	
			アプリケーション（データ解析）		×	
	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		×	×

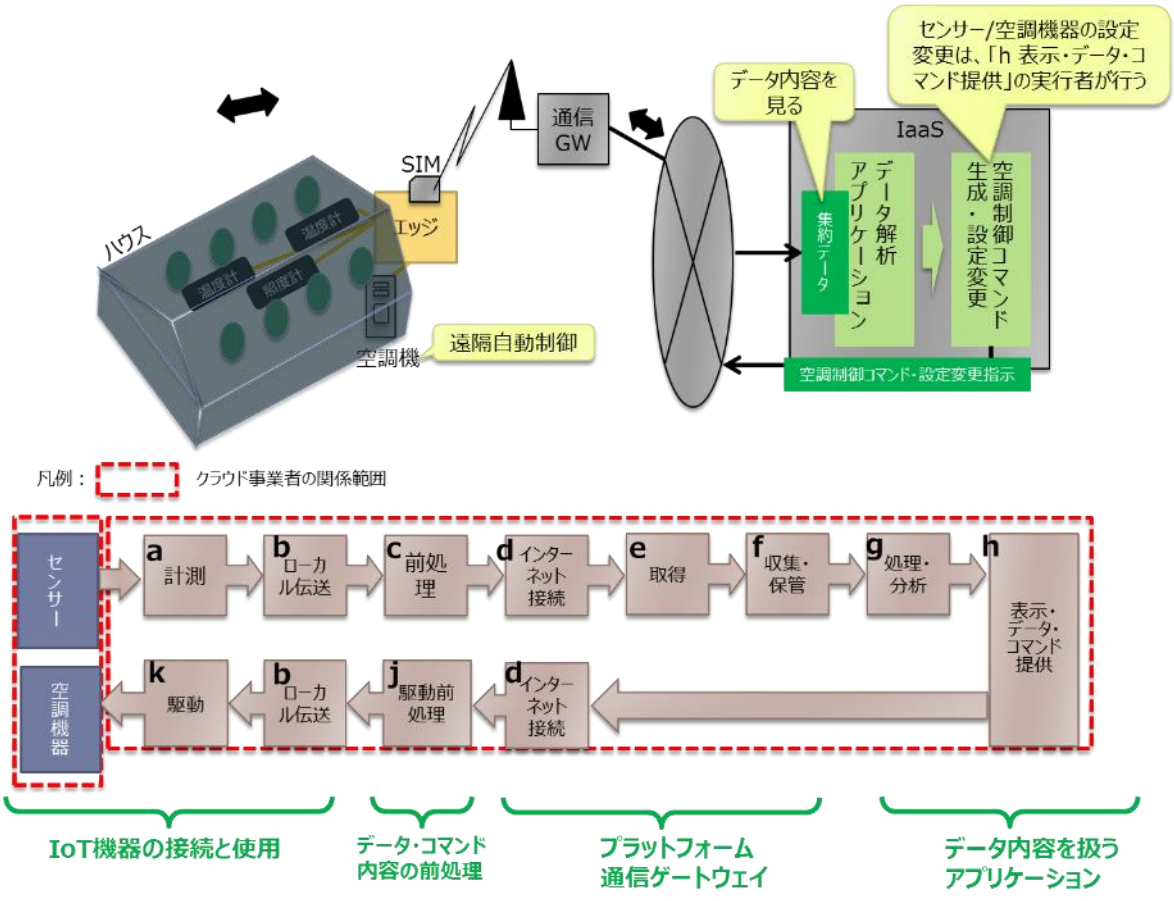
			j 駆動前処理		×	× *データ内容を見ない場合は記入不要
			k 駆動		×	
	f データ監視・保全	データ内容を見てこれに責任を持つ				○
（イ）IoTサービスを実行するためのロール	a 計測	クラウド事業者が自らロールを実行するか			×	
	b ローカル伝送				×	
	c 前処理				×	
	d インターネット接続				×	
	e 取得				○	
	f 収集・保管				○	
	g 処理・分析				○	
	h 表示・データ・コマンド提供				○	
	i データ外部提供				○	
	j 駆動前処理				×	
	k 駆動				×	

（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/ローカルコンピュータ		○	
			組込みアプリケーション		×	
			LAN		○	
			エッジコンピュータ		○	
			通信 GW		×	
			IaaS/PaaS		○	
			アプリケーション（データ解析）		○	
			アプリケーション（表示・データ・コマンド提供）		○	
	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 GW		×	
			IaaS/PaaS		×	
			アプリケーション（データ解析）		×	
	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