スマートシティ
セキュリティガイドライン

（第 3.0 版）

2024 年 6 月

総務省

目次

1. ガイドラインの背景と目的

1.1. 背景

スマートシティは、先進的技術の活用により、都市や地域の機能やサービスを効率化・高度化することで各種の課題の解決を図るとともに、快適性や利便性を含めた新たな価値を創出する取組である。「統合イノベーション戦略 2020」（令和２年７月 17 日閣議決定）では、Society5.0 の先行的実現の場としてスマートシティが位置づけられ、「デジタル田園都市国家構想総合戦略　(2023 改訂版)」（令和 5 年 12 月 26 日閣議決定）では、スマートシティは地方が目指すべき地域ビジョンのモデルの例としてあげられている。

他方で、スマートシティ内では多数のセンサーやカメラ[1]等の IoT 機器が散在し、かつ多様なデータが取り扱われるという特徴があるため、常にサイバー攻撃のリスクにさらされる恐れがある。さらに、近年のスマートシティではその地域の住民の安全に関わるサービスなど、提供されるサービスの範囲や重要性が拡大しつつあることから、安全・安心なスマートシティサービスを提供するために、スマートシティのセキュリティの実装が求められることが想定される。また、スマートシティではルール作りやシステム構築・運用などに多様な主体が関わることから、スマートシティのセキュリティを実現するためには関係者間で共通認識を醸成しつつ、適切にセキュリティ対策を実施する必要がある。

そのため、今後、地方公共団体を始めとする様々な地域において、安全・安心なスマートシティが実現できるよう、本ガイドラインでは、内閣府の戦略イノベーション創造プログラム（SIP）において定義されているスマートシティリファレンスアーキテクチャ（以下、「リファレンスアーキテクチャ」という。）を前提とした上で、学識者、自治体有識者、スマートシティ及びセキュリティに関わる ICT 企業等の有識者からなる検討会を通じて、スマートシティのセキュリティの考え方やスマートシティを実現する上で実施することが推奨されるセキュリティ対策等について整理[2]した。

本ガイドラインが、スマートシティの推進に関わるあらゆる主体において安全・安心なスマートシティを実現するにあたっての参考となることを期待する。

1.2. 目的

本ガイドラインの最終的な目標は、安全・安心なスマートシティの実現に寄与するとともにスマートシティの普及促進を図ることである。本目標を達成するためには、スマートシテ

---

[1] カメラの利活用においては、スマートシティリファレンスアーキテクチャ第 2 版(2023 年 8 月)の「＜コラム＞ 自治体による条例の制定例：加古川市における見守りカメラの運用ルール（見守りカメラの設置及び運用に関する条例)」等が参考となる。

[2] スマートシティセキュリティガイドライン 2.0 版（2021 年 6 月）はリファレンスアーキテクチャの第 1 版（2020 年 3 月）に基づくものであり、リファレンスアーキテクチャの第 2 版（2023 年 8 月）の策定を踏まえてスマートシティセキュリティガイドライン 3.0 版に改訂するものである。

ィのどこにどのようなリスクが存在し、そのリスクに対してどのような対策が必要となるかを理解する必要がある。上記を踏まえ、本ガイドラインの具体的な目的は以下のとおりである。

- ✓ スマートシティの推進に関わるあらゆる主体において、セキュリティの観点で見たスマートシティの構造を把握する
- ✓ 各関係主体が、スマートシティを構成する各要素それぞれにおけるセキュリティ上のリスク及び実施すべきセキュリティ対策を把握する
- ✓ 各関係主体が、スマートシティの特徴を踏まえたスマートシティ横断的なセキュリティ上のリスク及び実施すべきセキュリティ対策を把握する

1.3. 関係主体の定義

スマートシティでは、その推進に多様な主体が関わることから、まずは関係主体について表１－１のとおり定義する。リファレンスアーキテクチャ内で使用されている関係主体に関する用語については、基本的に同一の定義とする。一方で、リファレンスアーキテクチャ内で明確に定義されていない用語については本ガイドラインで新たに定義する。

表１－１の定義はスマートシティを推進する上で一般的と思われる体制を前提に整理している。個々のスマートシティにおいて、ここに示す定義とは異なる定義が用いられている場合や、複数の定義を満たす主体の存在が想定される場合は、適宜読み替える必要がある。

表１－１　本ガイドラインにおける関係主体の定義

用語	定義
サービス利用者（受益者）	スマートシティサービス[3]の提供の対象として、その提供ニーズを有する主体のこと。なお、提供されるサービスによっては、サービス利用者がデータを提供することもある。
サービス提供者	（サービス利用者に対して）スマートシティサービスを提供する主体。
推進主体	スマートシティ全体の推進・運営に関して責任・決定権・主導権を持つ主体。本ガイドラインにおいては地域協議会や地方公共団体などが推進主体に該当し、当推進主体から業務委託を受けるベンダ等は含まない。
投資家・データ等提供者	（時に対価を目的として）スマートシティやスマートシティサービスの開発・運営に必要となるリソースを提供する主体。
都市 OS ベンダ	「推進主体」からの業務委託等を受け、都市 OS の構築・運用を実施する事業者を指す。

[3] リファレンスアーキテクチャにおいて、スマートシティサービスは「都市 OS を通じてデータや他サービスと連携した上で利用者に提供されるもの」と定義されている。

用語	定義
データ提供事業者	「投資家・データ等提供者」の内、IoT 機器等からデータを収集し、都市 OS へデータを提供する事業者の総称を指す。
IoT 機器ベンダ	「データ提供事業者」や「サービス提供者」に対して IoT 機器を提供する事業者を指す。
セキュリティサービス事業者	「推進主体」からの業務委託等を受け、スマートシティの全体または一部のセキュリティ監視等のセキュリティに関するサービスを実施する事業者を指す。
マルチステークホルダ	「サービス提供者」「推進主体」「都市 OS ベンダ」「データ提供事業者」「IoT 機器ベンダ」「セキュリティサービス事業者」「サービス利用者」などのスマートシティ推進に直接的又は間接的に関与する主体の総称を指す。本ガイドラインでは基本的にスマートシティサービスを提供する主体の総称として使用しているが、「サービス利用者」もスマートシティを共創するマルチステークホルダの一員となる。

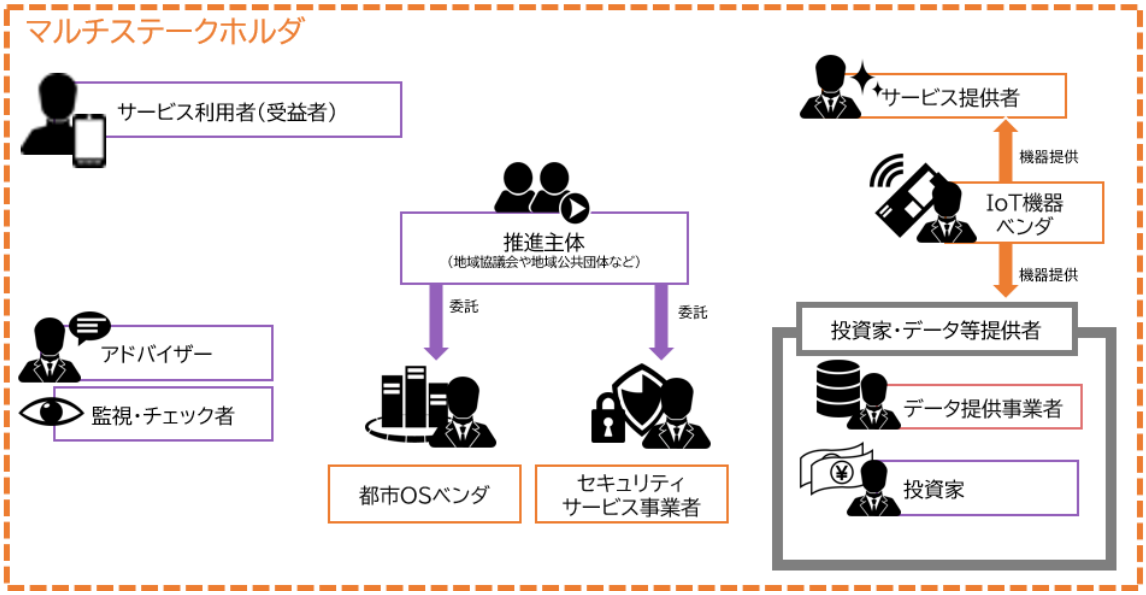


図１－１　本ガイドラインで定義する関係主体のイメージ

1.4. 対象範囲

本ガイドラインにおける対象範囲は、下記のとおりとする。

- スマートシティのセキュリティを実現する上では管理的な面と技術的な面、双方からのアプローチが必要であることから、本ガイドラインでは管理的対策、技術的対策のいずれも対象範囲として捉える
- 本ガイドラインでは基本的に、スマートシティサービスを提供する主体であるマルチステークホルダが実施すべきセキュリティ対策について言及することとする
- スマートシティで取り扱われるデータや情報は、サービスの利用範囲の拡大に伴い、オープンデータだけでなく機密性が求められる情報についても取り扱われるケースが増えていることから、本ガイドラインではオープンデータ及び機密性が求められる情報の双方に対してセキュリティを担保することを前提とし、必要と思われるセキュリティ対策等について言及する
- スマートシティでは利用者の個人情報を取り扱うケースが想定されることから、プライバシーに対する考慮が必要となるが、当然その中にはプライバシー情報のセキュリティへの考慮も含まれている。そのため、プライバシー情報のセキュリティ確保のために有用な要素（データの機密性や完全性担保などの安全管理の実施等）に関しては、本ガイドラインの対象範囲に含める
- スマートシティサービスは多種多様であり、サービスによってはその地域に住んでいる住民の安全に関わるサービスも存在する。 そのため、セキュリティ対策の不備が要因となるセーフティに関するリスクについても対象範囲に含める

なお、本ガイドラインに記載されているリスクやセキュリティ対策等は、スマートシティを構築・運用するにあたり、特に検討・実施することが推奨される事項について記載しており、網羅的な記載とはなっていない。そのため、本ガイドラインの読者においては本ガイドラインを自身が関与するスマートシティにおけるセキュリティ対策を検討するための参考としていただくとともに、必要に応じて本ガイドライン以外の国際規格やガイドライン等を参照することを推奨する。(国際規格やガイドライン等については、「3.1.1 ガバナンス」や【Appendix】A 「参照すべき法令・ガイドラインの一覧」に一部を記載する。)

また、上述の対象範囲の中で、「本ガイドラインではオープンデータ及び重要な情報の双方に対してセキュリティを担保することを前提」と言及しているが、スマートシティ内で取り扱われる情報資産に対するリスク評価や、実施するセキュリティ対策、その対策の実施主体などは、それぞれのスマートシティのサービスやビジネスの形態に大きく依存することから、スマートシティごとに検討する必要があることに留意することが求められる。

その他、スマートシティは交通や医療といった様々な分野において活用されることが想定されるが、本書においてはそれぞれの分野で共通的に発生することが想定されるリスクや実施すべきセキュリティ対策について記載していることに留意する必要がある。

1.5. 想定読者

本ガイドラインの想定する対象読者を以下に示す。

① 推進主体

本ガイドラインの主となる想定読者。スマートシティを管理・運営する主体であることから、管理的な側面でのセキュリティ検討が重要となる。また、推進主体はスマートシティ全体を把握することが望ましいことから、技術的な対策を直接実施する主体ではないとしてもスマートシティ全体におけるリスクや対策を把握することが求められる。

② サービス提供者、都市 OS ベンダ、データ提供事業者、IoT 機器ベンダ、セキュリティサービス事業者

推進主体と連携し、主に技術的なセキュリティ対策の実施が求められる主体。推進主体からの業務委託や提携を受け、それを踏まえたそれぞれの責任範囲におけるセキュリティ対策を実施することが基本となるが、他の主体と連携して対処が求められるところもあるため、幅広くセキュリティ対策について把握していることが望ましい。

1.6. 全体構成

本ガイドラインは、「１．ガイドラインの背景と目的」、「２．スマートシティセキュリティの考え方」、「３．スマートシティにおけるセキュリティ対策」、「４．セキュリティ検討のための補助コンテンツ」の４章から構成される。

- 第１章においては、本ガイドラインの背景、目的、関係主体の定義、対象範囲、全体構成等を示す。
- 第２章においては、本ガイドラインの前提となっているリファレンスアーキテクチャの構造について紹介すると共に、スマートシティのセキュリティを検討する上での構造の分類について整理し、それぞれの分類におけるセキュリティ上のリスクやセキュリティ対策の方向性を示す。
- 第３章においては、第２章で整理した分類に基づき、それぞれにおいて特に必要とされるセキュリティ対策の詳細や、具体的なセキュリティ対策の事例を記載する。
- 第４章においては、セキュリティを検討する上での補助コンテンツとして、幅広くリスクとセキュリティ対策を取りまとめた一覧表を紹介すると共に、本ガイドラインに記載されているセキュリティ対策が実施できているかを確認するためのチェックシートについて記載する。

1.7. 活用方法

上述の全体構成を踏まえた本ガイドラインの活用方法を以下に示す。

① 第１章において、本ガイドラインの背景、目的、関係主体の定義、対象範囲、全体構成等を理解する。

② 第２章において、スマートシティにおけるセキュリティ観点で見た構造の分類について理解する。また、それぞれの分類におけるリスクと対策の方向性を理解する。

③ 第３章において、それぞれの分類における具体的なセキュリティ対策について理解する。

④ 第４章において、自身が推進するスマートシティの分野や特性を踏まえたリスク分析を行った上で、リスクやセキュリティ対策の一覧表を参考に、実施すべきセキュリティ対策を検討する。また、チェックシートを活用して自身のスマートシティにおけるセキュリティ対策の網羅性をチェックする。

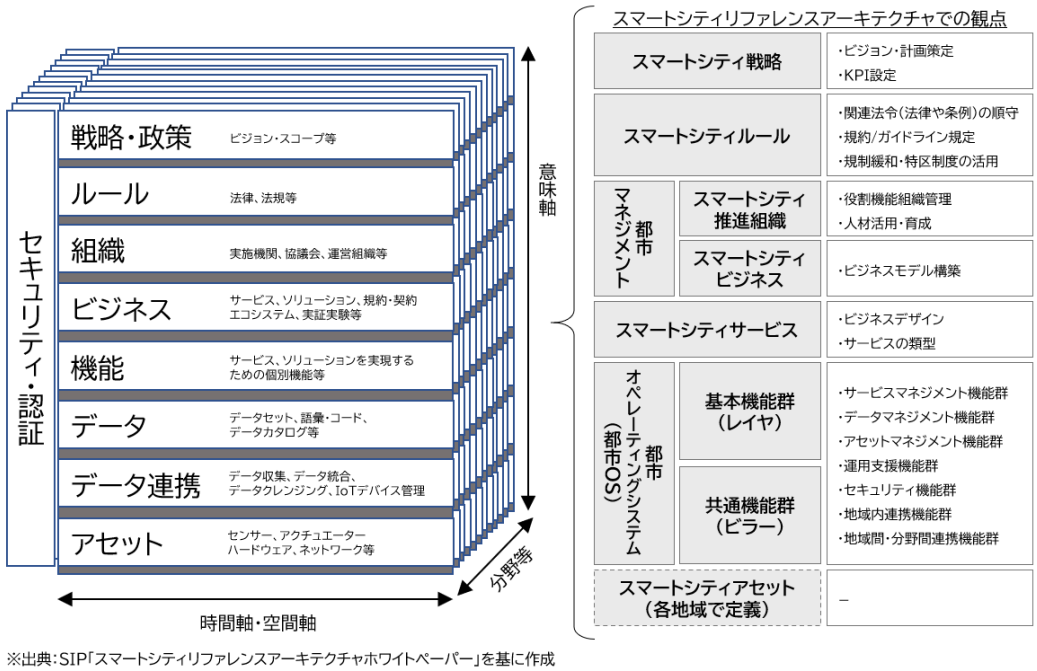
2. スマートシティセキュリティの考え方

2.1. スマートシティリファレンスアーキテクチャ

本ガイドラインは、スマートシティの推進主体をはじめとした、スマートシティに関わる各主体が、IoT 機器やデータ利活用のための基盤、サービス、データ流通等におけるセキュリティ対策を検討するものである。

スマートシティは現時点において発展途上の概念・取組であり、想定される枠組みがそれぞれのスマートシティによって異なることが想定されるため、スマートシティのセキュリティの検討にあたっては、本ガイドラインでは、内閣府で定義されたリファレンスアーキテクチャの構造を検討の前提として、セキュリティの考え方やセキュリティ対策等について整理している。

また、上記のリファレンスアーキテクチャを踏まえつつ、システムライフサイクルの中で特に重要となる企画、設計・開発、運用段階におけるセキュリティ対策に着目して整理している。



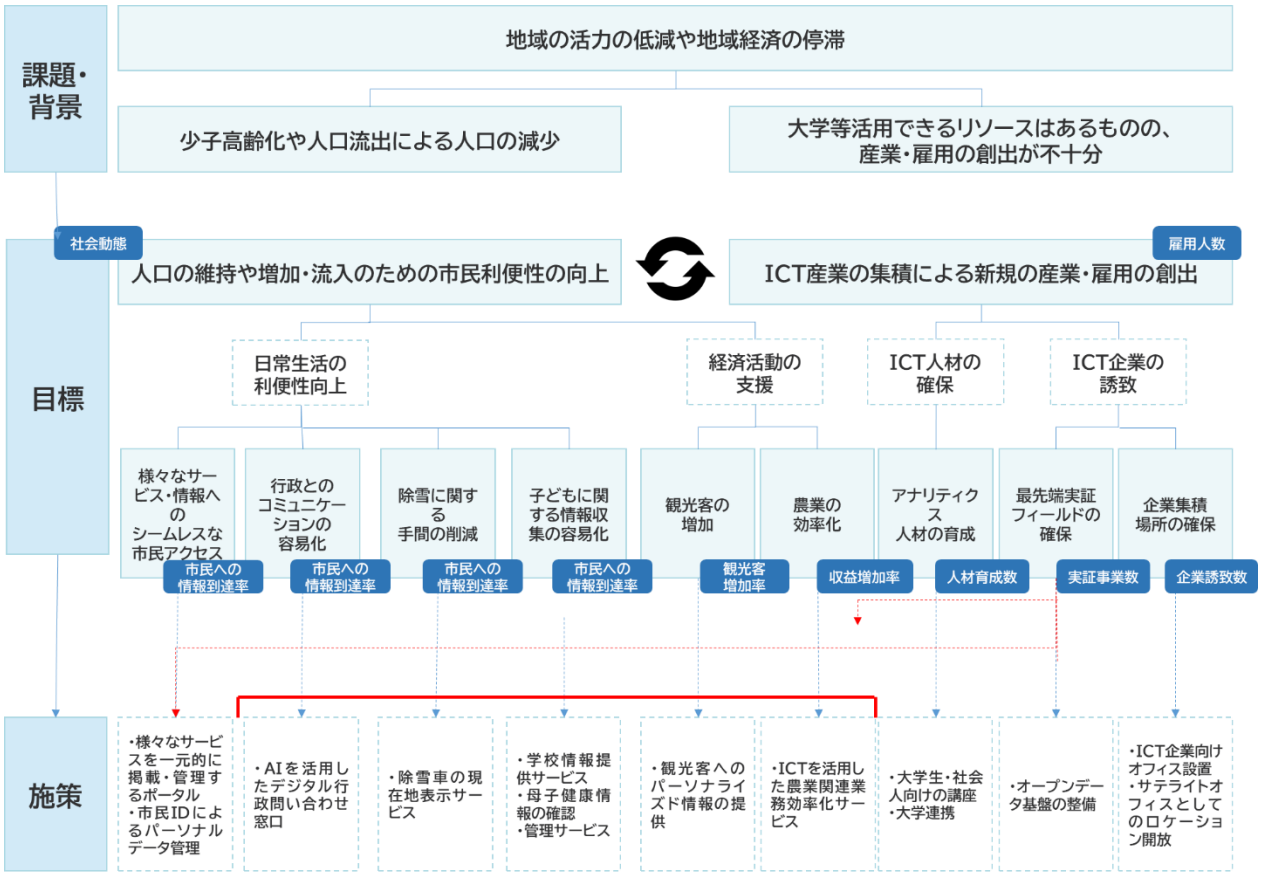
※出典：SIP「スマートシティリファレンスアーキテクチャホワイトペーパー」を基に作成

図２－１　Society5.0 リファレンスアーキテクチャとスマートシティリファレンスアーキテクチャの構成要素との関係

スマートシティのセキュリティの考え方を整理するにあたり、まずは内閣府が公表した「スマートシティリファレンスアーキテクチャホワイトペーパー[4]」に記載されているリファレンスアーキテクチャにおける各層の定義を以下に示す。

①スマートシティ戦略

スマートシティ戦略は、それぞれの地域がどのように当該地域の目標を達成するのかという道筋を描くものである。リファレンスアーキテクチャにおいては、戦略策定のフレームワークを例示しており、本フレームワークによって地域課題に基づくスマートシティの目標が階層的に整理され、施策の実施やサービス提供につなげることができる。



※出典：SIP「スマートシティリファレンスアーキテクチャホワイトペーパー」を基に作成

図２－２　スマートシティ戦略のイメージ

4 内閣府：https://www8.cao.go.jp/cstp/society5_0/smartcity/architecture.html

②スマートシティルール

スマートシティ計画を実施・運営し、様々な施策やサービス提供を実施するには、組織運営やサービス提供に関する適切なルールを各地域において策定し、運用することが重要である。スマートシティの計画においては、「関連法令」「各地域で定める規約・ガイドライン」「規制緩和・特区制度の活用、法改正」がルールの構成要素となる。

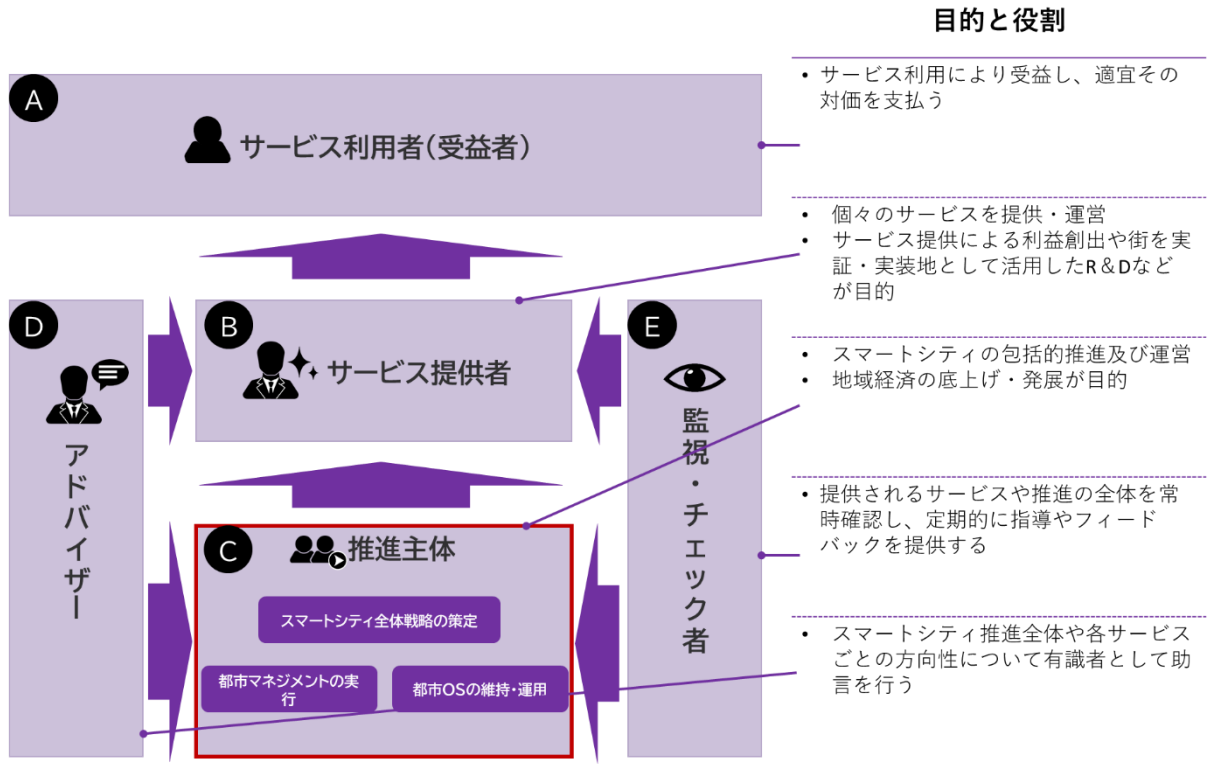
ルールの種類	内容
関連法令	スマートシティの計画を実施・運営する上で、また各施策を実施する上で順守や対応が必要となる法令 例）個人情報保護法、官民データ活用推進基本法 各分野の関連法令（モビリティ分野：道路交通法ほか）
各地域で定める規約・ガイドライン	各地域においてスマートシティの計画を実施・運営する上で、また各施策を実施する上で、地域で定める規約・ガイドライン 例）推進組織運営の規約、サービス利用に関する規約ほか
規制緩和・特区制度の活用法改正	スマートシティの施策を実施する上での、必要に応じた規制緩和や特区制度の活用・法改正

※出典：SIP「スマートシティリファレンスアーキテクチャホワイトペーパー」を基に作成

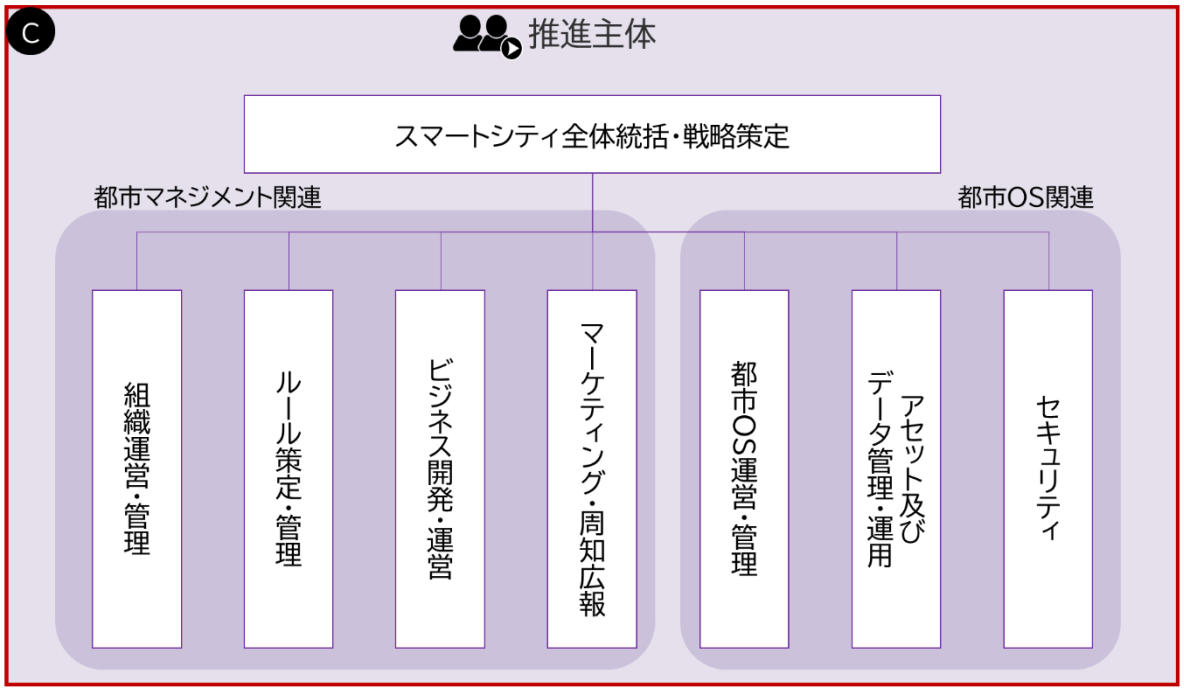
図２－３　スマートシティルールのイメージ

③　スマートシティ推進組織

スマートシティの組織は、スマートシティ全体の推進・運営に関して責任・決定権・主導権等を持つことが想定されている「推進主体」のほか、スマートシティサービスをサービス利用者に提供する「サービス提供者」をはじめとする、スマートシティの効率的な推進及び運営にあたって異なる役割を担う多くのプレイヤー（ステークホルダ）が構成要素となる。具体的なステークホルダやその関係性は図２－４を参照されたい。なお、このリファレンスアーキテクチャのステークホルダの定義を踏まえた、本ガイドラインにおける関係主体の定義は「1.3 関係主体の定義」に示したとおりである。



※アドバイザー：サービス提供者や推進主体に加わらず、外部よりアドバイスを行う主体
監視・チェック者：アドバイザーと同様に外部視点での確認を実施する主体



※出典：SIP「スマートシティリファレンスアーキテクチャホワイトペーパー」を基に作成

図２－４　スマートシティ推進組織のイメージ

④スマートシティビジネス

スマートシティにおけるビジネスは、複数のプレイヤー間で発生する、物品・サービス等の提供と金銭等の対価の支払いのやり取りに関して、構造的に理解できる「ビジネスモデル」を構築することで実現する。そして、スマートシティ全体を俯瞰したビジネスモデルを構築することで、各プレイヤーに求められる価値・対価、その他財源を明らかにでき、地域全体の持続的な運営を担保できる。

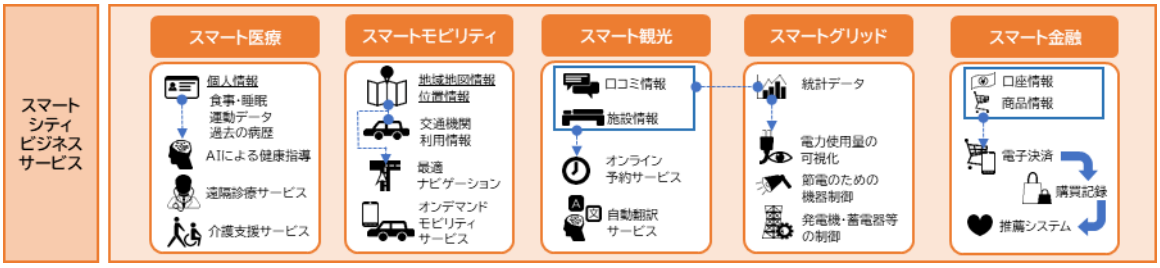


図２－５　スマートシティビジネス・サービスのイメージ

⑤スマートシティサービス

スマートシティサービスとは、都市 OS 等を活用してデータや他サービスと連携した上で利用者に提供されるものである。一般的な例としては、ウェブサイトやアプリを通じたサービス提供が挙げられる。スマートシティサービスを通じて、スマートシティ戦略に基づき特定された地域課題の解決を図る。

⑥都市オペレーティングシステム（都市 OS）

都市オペレーティングシステム（都市 OS）は、スマートシティ構築のために地域が共通的に活用する機能が集約され、様々な分野のスマートシティサービス導入を容易にするための IT システムの総称である。

スマートシティリファレンスアーキテクチャにおける都市 OS の構成要素（機能群）は、7 つの機能群で構成されており、基本機能群（レイヤ）と共通機能群（ピラー）として 2 つに分類される。基本機能群（レイヤ）は「サービスマネジメント機能群」、「データマネジメント機能群」、「アセットマネジメント機能群」の３種類で構成され、共通機能群（ピラー）は「運用支援機能群」、「セキュリティ機能群」、「地域内連携機能群」、「地域間・分野間連携機能群」の４種類で構成されている。

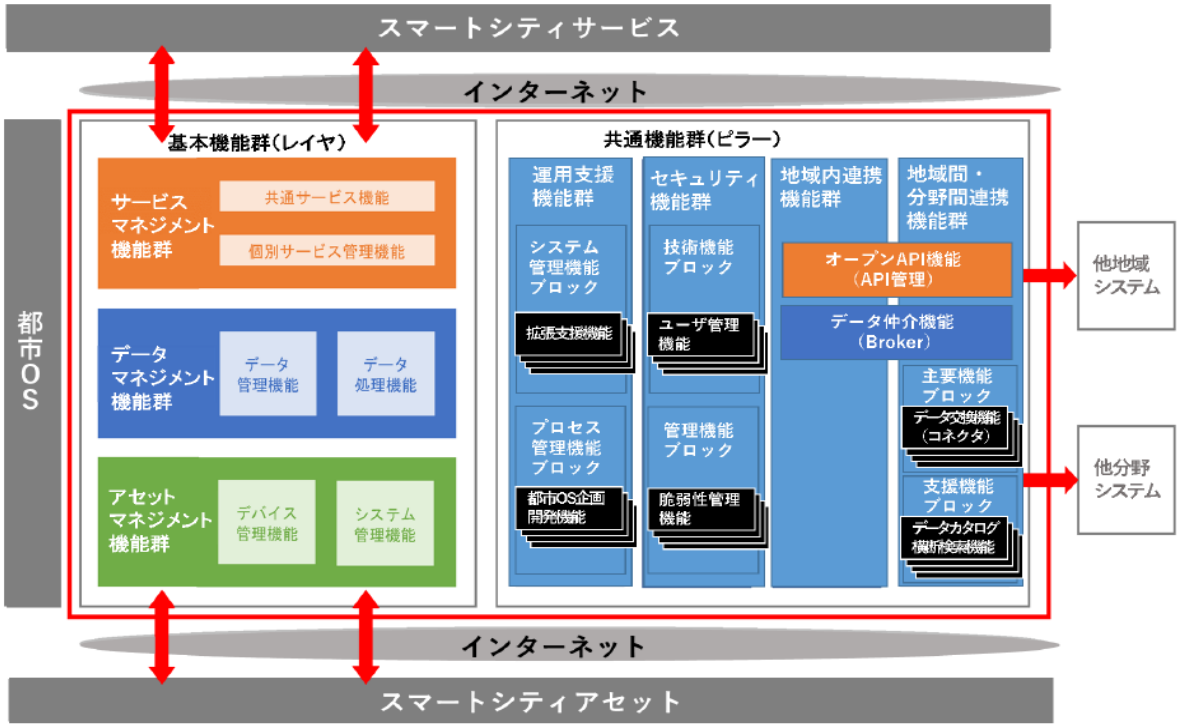


図２－６　都市 OS の機能の全体像[5]

⑦スマートシティアセット

スマートシティにおけるアセットとは、主にその都市に関連する資産や資源であり、都市 OS を通してデータ化や制御されるものである。

スマートシティアセットは、課題を解決するために必要なデータの生成を目的とし、資産や資源をデータ化するためのデバイスや、それらを都市 OS に連携するためのネットワーク、中継機器などから構成される。

生成されるデータは、様々な IoT センサーなどのセンサーデバイスから生成される河川・潮位水位などの環境データ、公共交通の運行状況データなど、様々なデータがある。

図２－７　スマートシティアセットのイメージ

[5] スマートシティリファレンスアーキテクチャ 2.0 版　P149　「図 7.2-1　スマートシティレファレンスアーキテクチャにおける都市 OS の機能の全体像」より引用

2.2. スマートシティのセキュリティ検討のアプローチ

スマートシティでは様々な主体が様々な役割を担い、それが複合的に関与しあうという特徴を有するため、セキュリティについても構造的に整理し検討することが適当である。そのため、本ガイドラインではスマートシティの構成要素をカテゴリに分け、それぞれのカテゴリにおいて確保されるべきセキュリティと、一つのスマートシティ全体や連携する複数のスマートシティ全体として確保されるべきセキュリティに分類し、それぞれの観点から考慮すべきセキュリティ上のリスクや講ずべきセキュリティ対策について記載する。

2.2.1. スマートシティの各カテゴリにおけるセキュリティ検討

スマートシティの構成要素それぞれにおいて確保されるべきセキュリティを検討するアプローチとして、リファレンスアーキテクチャで定義されている８つの層のうち、想定される脅威やリスク、講ずべきセキュリティ対策が共通化できる層をカテゴリとして分類し、整理した。具体的には、図２－９に示すように、「ガバナンス」「サービス」「都市 OS」「アセット」の４つのカテゴリに分類し、それぞれのカテゴリにおけるセキュリティ上のリスクやセキュリティの考え方、セキュリティ対策等について整理した。

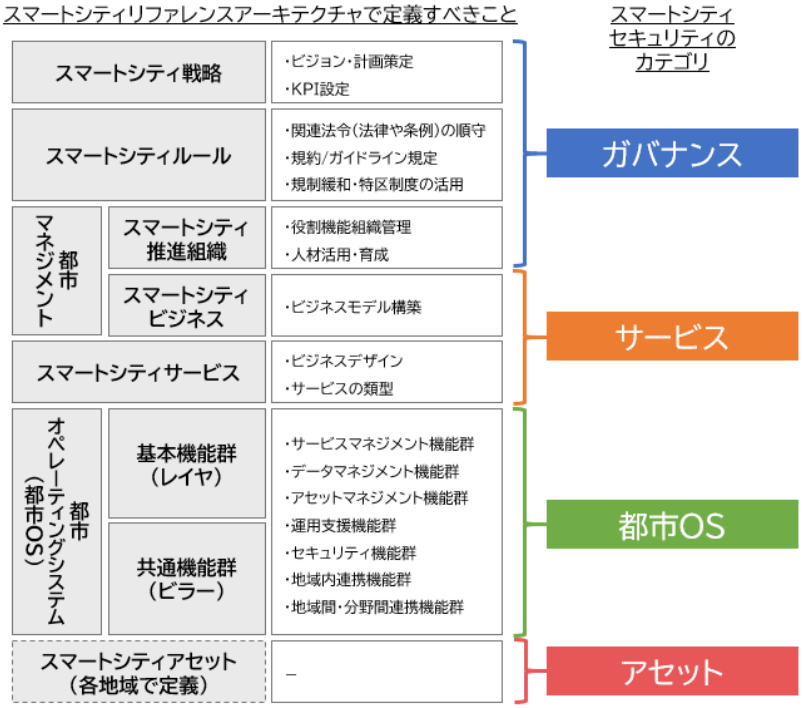


図２－８　スマートシティリファレンスアーキテクチャを踏まえたカテゴリの分類

2.2.2. スマートシティ全体におけるセキュリティ検討

本ガイドラインでは、スマートシティ全体として確保されるべきセキュリティについて、以下のとおり２つのケースについて言及する。

１つ目は、単体のスマートシティに着目し、スマートシティを構成する４つのカテゴリにまたがって対応が必要とされるセキュリティである。１つのスマートシティであっても、「推進主体」「都市 OS ベンダ」「サービス提供者」等の役割が、自治体と複数の事業者で構成されている場合、複数の主体が関連することに伴い生じるリスクがあるため、それに対するカテゴリ横断的なセキュリティの検討が必要となる。

２つ目は、スマートシティを更に俯瞰的にとらえ、単体のスマートシティ同士または自身のスマートシティと別の基盤（例えば近隣の自治体の基盤等）が接続し、機能やデータを連携する場合に対応が必要とされるセキュリティである。複数のスマートシティや基盤が連携することに伴い生じるリスクがあるため、それに対するセキュリティの検討が必要となる。

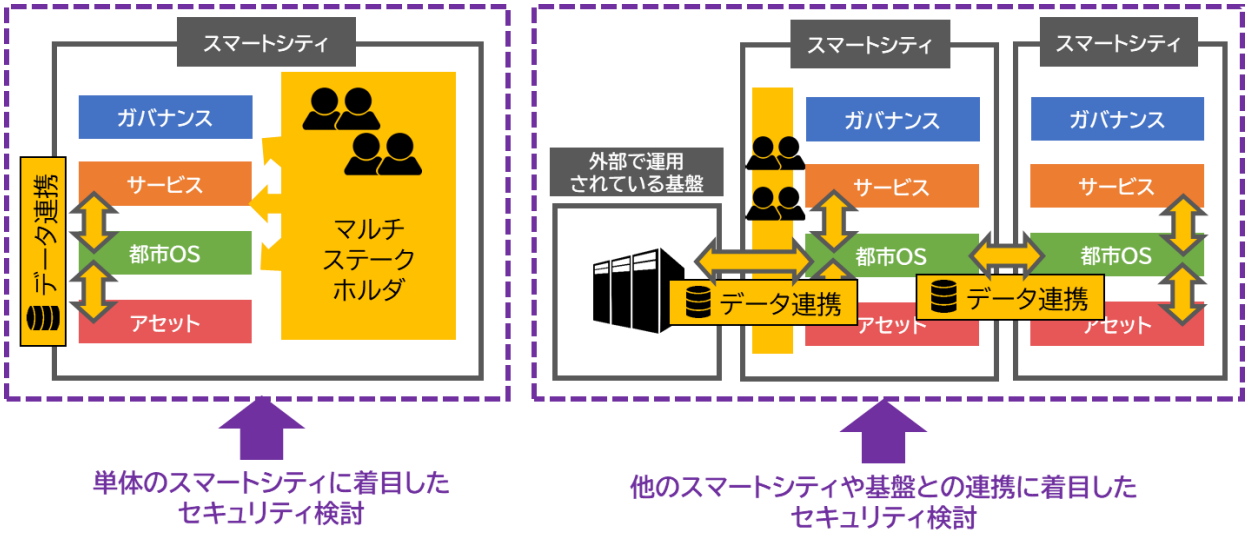


図２－９　スマートシティ全体におけるセキュリティ検討

ここで示した２つのケースのように、マルチステークホルダが複雑に関与し合うというのはスマートシティの特徴的な部分であり、その特徴を踏まえたスマートシティ特有の横断的なセキュリティの検討が必要となる。本ガイドラインでは、これら２つのケースにおいて、セキュリティ上のリスクやセキュリティの考え方、セキュリティ対策等について整理した。

2.2.3.スマートシティデータ種別

スマートシティにおけるデータの種別は①「オープンデータ」②「限定公開データ」③「クローズドデータ」の３つに分類できる。①オープンデータは政府、自治体、公共機関、民間企業などが保有するデータを公開し、営利目的、非営利目的を問わず無償で二次利用可能なルールが適用されたもの、②限定公開データはステークホルダ間で契約等に基づき限定的に開示・共有するデータ、③クローズドデータは自治体が保有する住民記録データなどであって外部に公開しない非公開データが想定される。

これらのスマートシティにおけるデータの種別の中には、住民等のパーソナルデータも含まれる。パーソナルデータは個人に関係するデータであり、個人情報に加え、個人情報との境界が曖昧なものを含む、個人の属性情報、移動・行動・購買履歴データなど個人と関連性が見出される情報であってこれを加工した情報[6]も含まれる[7]。パーソナルデータには個人情報に関する法令に従い保護・管理するものや、プライバシー保護が必要であるものがあり、情報の性質に応じて適切なセキュリティ対策が必要となる。

6 個人情報やパーソナルデータを統計化した情報が、オープンデータとされる場合がある。
7 パーソナルデータの性質に応じた取扱いについては、「DX 時代における企業のプライバシーガバナンスガイドブック ver1.3」（2023 年 4 月　総務省・経済産業省）や「パーソナルデータリファレンスアーキテクチャ」（2020 年 3 月　一般社団法人データ流通推進協議会（現データ社会推進協議会））なども参考になる。

2.3. スマートシティのセキュリティの概要

2.3.1.各カテゴリにおけるセキュリティの概要

本ガイドラインにて分類した４つのカテゴリそれぞれにおける想定されるリスクとセキュリティの考え方を以下に示す。

① ガバナンス

スマートシティ全体の取組や施策の方向性の決定、取組を継続させていくためのルールや基本方針作り、組織体制の構築等、スマートシティの在り方を決定するカテゴリである。本カテゴリで決定した内容（スマートシティを地域社会・経済においてどのように役立て、展開・拡張するか、どう管理するか等）が、他の３つのカテゴリの内容の方向性を決定づけることとなり、それはセキュリティにおいても同様となる。なお、ガバナンスカテゴリにおいて実施する対策は、スマートシティ全体の推進と管理監督の役割がある推進主体が中心・旗振り役となって検討・実施する必要がある。

ガバナンスにおいて最も重要となるのがセキュリティポリシーの策定であるが、このセキュリティポリシーが存在しない又は内容として不十分なものとなっていた場合、多様なマルチステークホルダが関与するスマートシティにおいては、マルチステークホルダ間におけるセキュリティ水準の不整合が生じることとなる。セキュリティでは「桶の理論」という考え方にもあるように、スマートシティ内でセキュリティが弱いコンポーネントが存在することで、そのコンポーネントからセキュリティインシデントが発生（水が漏れる）するリスクがあり、これは結果としてスマートシティに対する利用者からの信頼度の低下に繋がる恐れがある。

これらのリスクへの対策として、スマートシティ全体としてのセキュリティに関する統一的なポリシーを策定することが挙げられる。このポリシーで策定すべき内容としては、情報セキュリティ基本方針やセキュリティ対策基準、データ取扱い基準、インシデント対応手順等が挙げられるが、それらはスマートシティ全体のポリシーとして策定されるものであり、推進主体内のみならず、業務委託先やスマートシティサービスの提携先等においても同様に守るべきポリシーとして掲げられる。そのため、新たに接続を希望する事業者のポリシーや、対応体制などを確認する必要がある。

なお、スマートシティにおいてポリシーを策定する場合は、スマートシティ全体の構成や関係主体等を把握したうえで、リスクアセスメントを行い、ポリシーを形作っていく必要がある。その際、自身のスマートシティにおいて準拠すべき法令について考慮しつつ、自身が推進するスマートシティの特性を踏まえ、様々な省庁や団体から発出されているガイドラインを参照することが望ましい。

上記のポリシーを策定した後は、スマートシティの推進に関係する主体（マルチステークホルダ）を具体的に特定した上で、当該セキュリティポリシーに基づき、マルチステークホルダ間の責任分界点を決定し、推進主体と業務委託先やスマートシティサービスの提携先等との間での契約や規約の内容として反映することが重要となる。「サービス」「都市OS」「アセット」においては、ここで記載された内容を考慮した上で、適切なセキュリティ対策を検討、実施することが求められる。

なお、ポリシーを策定することはゴールではなく、ポリシーに従って適切なセキュリティ対策を実施することで初めてスマートシティのセキュリティを確保することができる。その観点からも、推進主体において自身のスマートシティのリスクを正確に把握し、適切にセキュリティ対策への投資を行う必要がある。

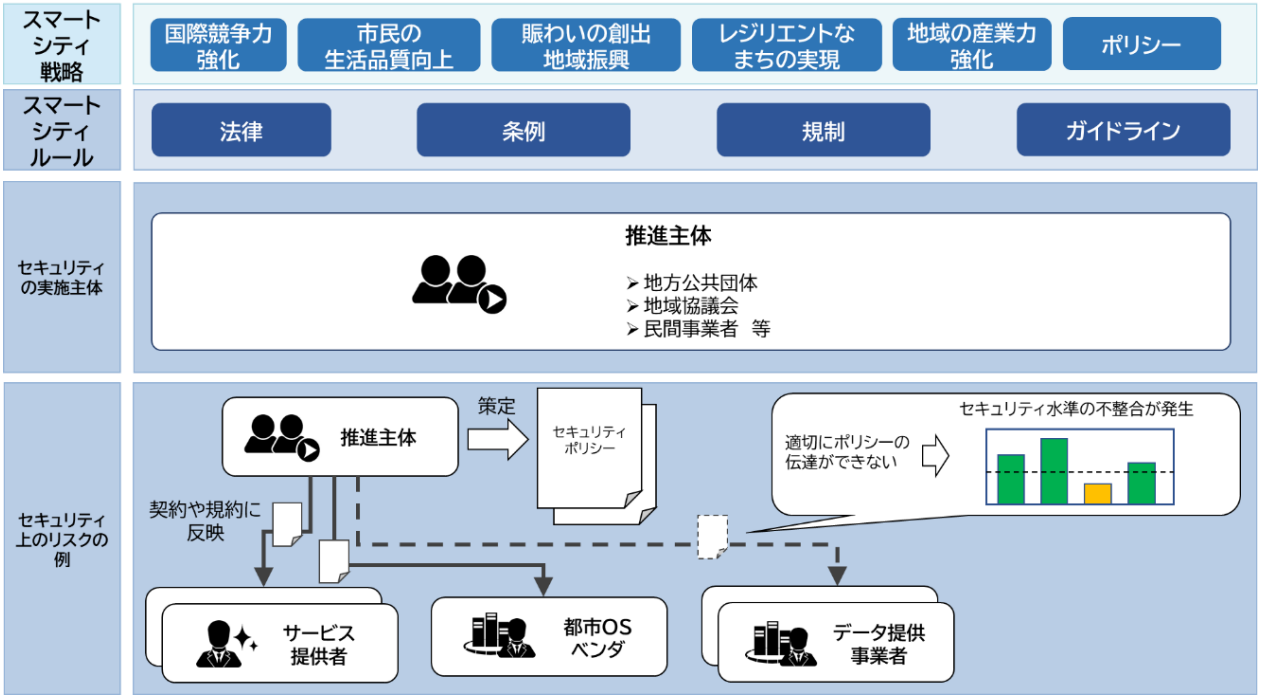


図２－１０　ガバナンスにおけるセキュリティ上のリスクのイメージ

②サービス

「サービス」とは、都市 OS を通じてデータを他サービスと連携したうえで利用者に提供されるものであり、サービスの一般的な例として、ウェブサイトやアプリを通じた利用者へのサービス提供が挙げられる。サービスのセキュリティを実施する主体はサービス提供者となる。なお、推進主体が直接サービスを提供することもあり、その場合は推進主体がサービス提供者となる。

これらのサービスはインターネット上に公開し、幅広いユーザに利用してもらうことが一般的であることから、様々なセキュリティ上のリスクが存在する。

サービスにおけるリスクの例としては、不正アクセスによる情報漏洩や分散型サービス拒否攻撃（DDoS 攻撃）等のサービス拒否攻撃によるシステム停止が挙げられる。これらの事象が一度発生すると、利用者の個人情報が外部に流出する、利用したいときにサービスが利用できないといった利用者への被害が発生する恐れがある。また、インシデントが発生したサービスの信頼性が著しく低下するだけでなく、スマートシティ全体の信頼性の低下に繋がり、全てのマルチステークホルダに対して影響が出る恐れがある。その他、脆弱性を悪用した攻撃により、ウェブサイトのコンテンツが改ざんされることによって、ウェブサイト上にマルウェアなどの不正なコンテンツが埋め込まれてしまい、ウェブサイトを閲覧した利用者のパソコンがマルウェアに感染するといったリスクも考えられる。

これらのリスクに対応するために、サービス提供者は利用者側とのインターフェースとなるウェブサイトやアプリケーションのセキュリティを適切に実装することが求められる。ウェブサイトやアプリケーションへのセキュリティ対策の例として、システムへの攻撃や侵入等を防ぐための各セキュリティ機能（アクセス制御、認証機能、セキュリティ監視等）の実装に加え、新規の脆弱性情報の把握と脆弱性への適切な対応が重要なものとして挙げられる。脆弱性への対応については、開発段階で既知の脆弱性が入りこんでいるケースも想定されるため、サービスイン前にセキュリティ検証や脆弱性診断を行い、あらかじめ適切にリスク管理を行うことを推奨する。

その他、サービス仕様が悪用されることにより、提供主体が想定しない形でサービスが利用され、不正に利益が獲得される可能性についても考慮が必要である。例えば、スマートシティサービスのアカウントを作成した際に入会特典ポイントを付与するサービスに対して、悪意のある者が実態のない大量のアカウントを新規作成し当該特典ポイントを大量取得することなどでサービス提供事業者が不利益を被るおそれもある。また、コールセンターによる本人確認時に他人になりすますことでアカウントが乗っ取られ、スマートシティで提供する行政サービスが悪用されるおそれもある。

このようにスマートシティのサービス仕様の脆弱性が悪用されるリスクに対応するために、利用者への規約・契約での不正利用の抑止を行うだけでなく、サービス特性や内容に応じて、利用者の本人確認や認証強度をどの程度必要とするかを検討し適切に設計することとなる。サービス導入時及び運用時において、類似サービスにおける不正事例を情報収集し、セキュリティの改善に繋げるとともに、有識者の知見を活用するなど多角的に精査することがセキュリティ対策として求められる。

また、有事に備え、データの暗号化やバックアップ、システムへのアクセスログなどの証跡確保のためのログの収集、検知・検出の仕組みとインシデント対応体制を構築することが考えられる。

なお、サービスのセキュリティを検討する際は、複雑・煩雑なユーザビリティとなってサービスの利便性が著しく損なわれることがないよう、バランスを考えつつ、最適なセキュリティを実装することに留意する。また、１つのスマートシティにおいて様々なサービスが提供される場合は、それぞれのサービスにおいて守るべき機能やデータ等の資産を特定し、サービス単体においてもリスクを把握した上で、適切にセキュリティ対策を決定、実施する必要がある。

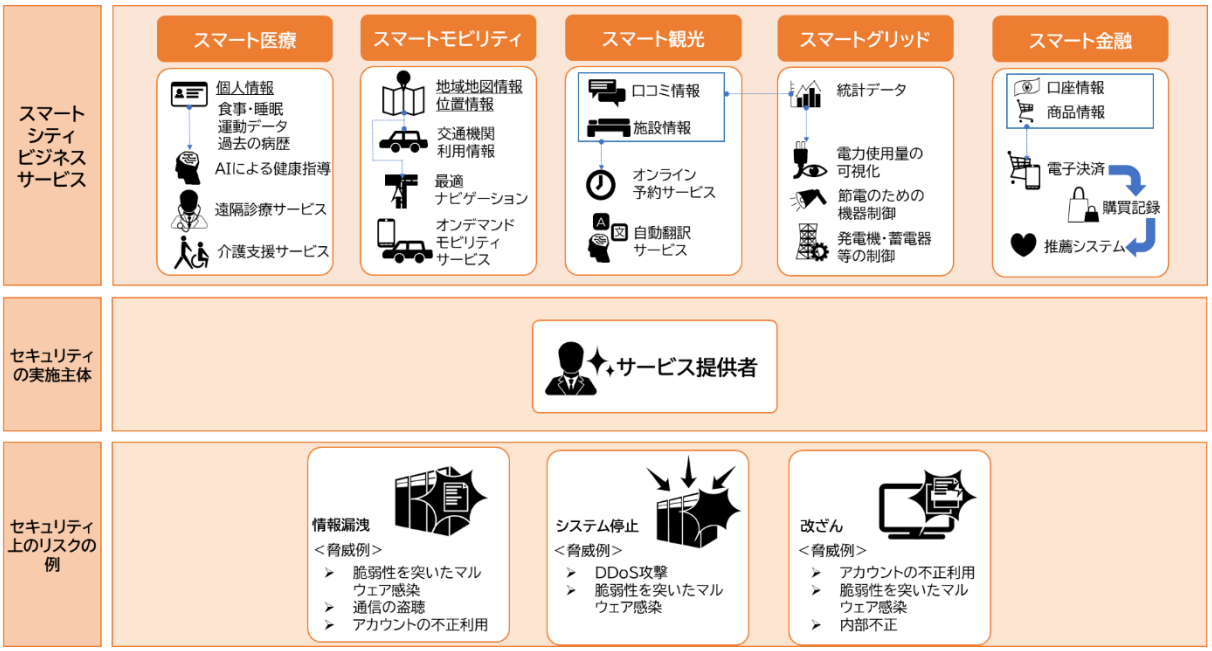


図２－１１　サービスにおけるセキュリティ上のリスクのイメージ

③都市 OS

「アセット」から収集した情報を分類、蓄積し、主に「サービス」や他の都市 OS 等へデータを提供するためのプラットフォームとしての役割を担うカテゴリである。都市 OS は基本的にクラウド基盤の活用が想定されることから、プラットフォーム単体のセキュリティとしてクラウド同士の連携やクラウドの特性を考慮したクラウドセキュリティの実装が求められる。都市 OS の構築・運用を担うのは都市 OS ベンダであり、セキュリティ対策の実施も都市 OS ベンダが中心となって実施する必要がある。

都市 OS への不特定多数のサービス利用者からのアクセスは一般的に想定されていないため、「サービス」と比較すると不正アクセス等のリスクは低くなるが、サービスやアセット、他の都市 OS などとのデータ連携のためのインターフェースは存在している。都市 OS におけるリスクの種類としては、基本的には「サービス」で挙げたリスクと同様のものが挙げられる。ただし、都市 OS はスマートシティのあらゆるサービスを提供するためのデータ連携を行う上で不可欠な基盤であり、都市 OS の機能が停止するとあらゆるサービスに影響が発生しうることから、高い可用性が求められる。また、都市 OS 内にデータを保有する

場合は、そのデータが改ざんされた場合、スマートシティサービスの品質にも影響し、最悪の場合は人命への影響が発生するリスクがある。

上記で述べたリスクへの対策としては、システムへの攻撃や侵入等を防ぐための各セキュリティ機能（アクセス制御、認証機能、セキュリティ監視等）の実装や、新規の脆弱性情報の把握と脆弱性への適切な対応が「サービス」と同じように必要となる。脆弱性への対応については、開発段階で既知の脆弱性が入りこんでいるケースも想定されるため、サービスイン前にセキュリティ検証や脆弱性診断を行い、あらかじめ対処および適切に管理することが望ましい。その他、アセットから収集したデータや都市 OS を構成するサーバ群の構成データのバックアップの取得や、データの暗号化等も必要となる。

また、都市 OS の基盤として、外部のクラウド事業者が提供する IaaS・PaaS を採用する場合は、都市 OS で求められるサービスレベルを理解し、そのサービスレベルを満たす堅牢性や可用性、信頼性が担保できるクラウドサービスを利用することが推奨される。クラウド基盤上に重要なデータを保管する場合も同様、都市 OS で求められる要件に応じて、クラウドが配置されているデータセンタ等のロケーション（リージョン）にも留意する必要がある。例えば、可用性を強く求められている場合は、ビジネス継続計画（Business Continuity Plan:BCP）や災害復旧（Disaster Recovery:DR）を考慮して地理的要素が異なるリージョンを選択してバックアップする必要がある。

なお、都市 OS に保有または都市 OS を介して扱われるデータには、オープンデータ、限定公開データ、クローズドデータなどの異なる種別や性質のものがあるため、これらの情報の種別や性質に応じ、管理基準を定めるとともに必要なセキュリティ対策を講じることが推奨される。

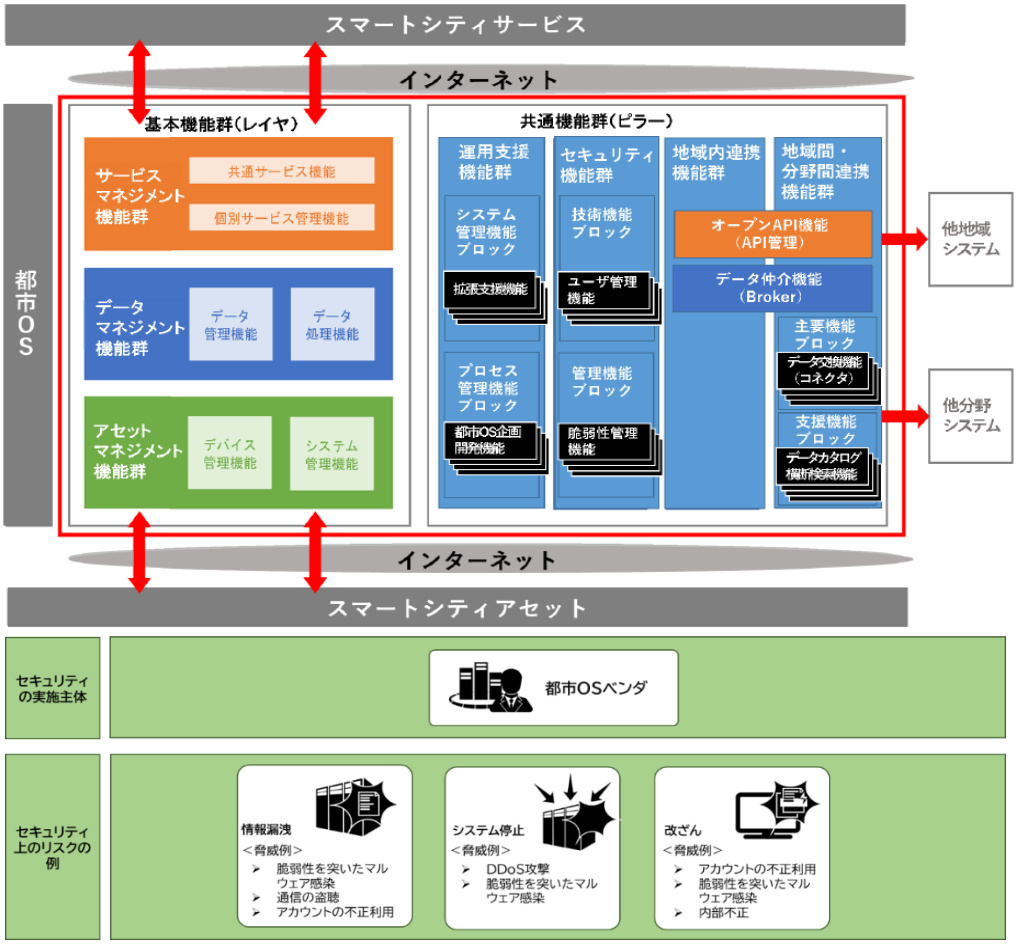


図２－１２　都市 OS におけるセキュリティ上のリスクのイメージ[8]

④アセット

課題を解決するために必要なデータを生成し、「都市 OS」へ送信するカテゴリであり、デバイス、ネットワーク、エッジコンピュータ、中継機器等から構成される。ここでは「サービス」で必要となる情報をどう収集するか、「都市 OS」にどういった形式で情報を送信するか等の検討を行う。

アセットにおける代表的なセキュリティリスクとしては、IoT 機器等のデバイス、エッジコンピュータへのマルウェア感染が挙げられる。近年では IoT 機器をマルウェア感染させ、ボット化した上で、DDoS 攻撃の踏み台とするなどの攻撃が見られている。また、これらの IoT 機器は利用者の近辺に物理的に存在することが多いという特徴があることから、物理的な破壊や不正アクセスによる停止及びデータの改ざん等もアセットにおけるリスクとして挙げられる。アセットの停止やデータの改ざんは、アセットからのデータを元にし

8 スマートシティリファレンスアーキテクチャ 2.0 版　P149　「図 7.2-1　スマートシティレファレンスアーキテクチャにおける都市 OS の機能の全体像」より引用

たサービスにも大きな影響を及ぼす可能性があり、例えば、災害対策サービスにおける水位情報や気象情報等において可用性や完全性が侵害されることで、間接的に人命に影響を及ぼす可能性があるため、非常に重大なリスクとなりうる。

上述のリスクに対応するセキュリティ対策として、課題となるのがデバイスやエッジコンピュータ、中継装置等のアセットの監視と適切な管理である。ソフトウェア等への脆弱性と同様、アセットにおいても日々脆弱性が発見、報告されているため、大量のデバイスを保有するスマートシティにおいては、それらのアセットの死活監視を行うとともに、その脆弱性情報を把握しつつアセットのバージョン情報を管理し、適切にバージョンを最新化する対応が必要となる。

また、デバイス等自体へのセキュリティも必要となる。例えば、デバイス等に直接またはネットワークを介してアクセスする際には認証機能を実装する必要があり、ネットワーク経由でデータの連携やデバイス制御などの通信が発生する場合は、通信を暗号化する必要がある。また、デバイス等で保有するデータに個人情報や秘密情報など機密性の高い情報が含まれる場合はデータの暗号化や、機器の耐タンパ性確保といった対策も必要である。さらに、物理的なセキュリティとして、センサーなどのデバイスを公共の場に設置する場合は、損壊や盗難にも留意し、モビリティなどの物理的な制御をサービスとして提供する場合は、安全性に配慮した設計・運用も必要となる。

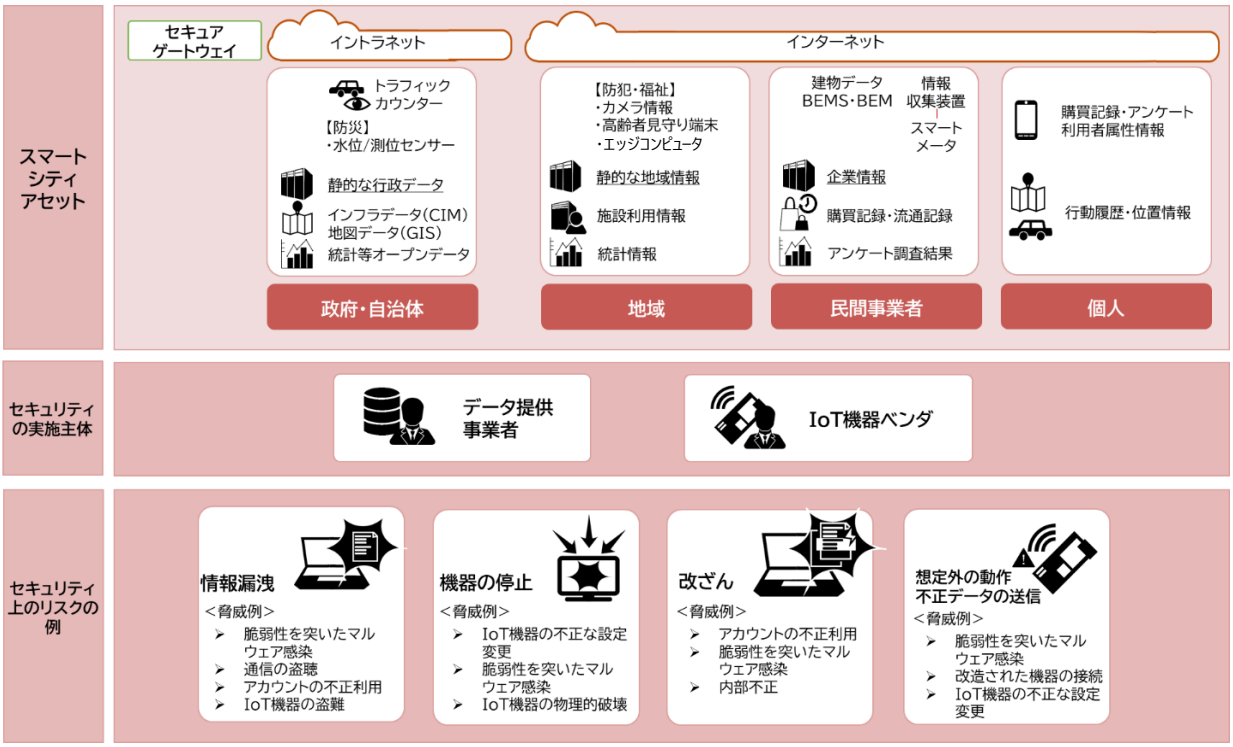


図２－１３　アセットにおけるセキュリティ上のリスクのイメージ

2.3.2.横断的なセキュリティの概要

一つのスマートシティを見てもマルチステークホルダが複雑に関与し合うことに加え、さらにスマートシティ間のデータ連携を考慮すると今後さらにステークホルダの範囲が拡大することが想定される。この広い範囲のマルチステークホルダによって、個々のカテゴリにおけるリスクに加え、新たな横断的なセキュリティ上のリスクが発生するため、そのリスクへの対策を講じることが必要となる。本ガイドラインでは横断的なセキュリティ対策を以下の 3 つの観点で整理した。

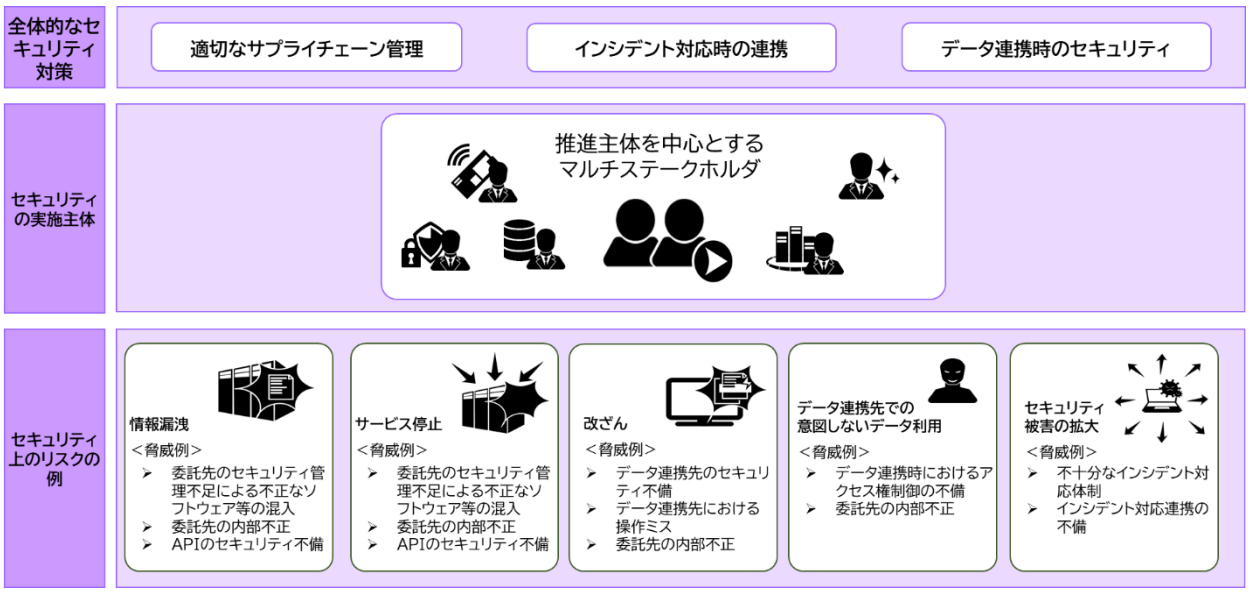


図２－１４　スマートシティ特有のセキュリティ上のリスクのイメージ

①適切なサプライチェーン[9]管理

多くのマルチステークホルダが関与することで、顕在化するのがサプライチェーン・リスクである。スマートシティでは複数の委託先や再委託先などが存在することとなるが、その委託先や再委託先におけるセキュリティ管理が不十分な場合は、委託先や再委託先に対する攻撃や内部不正によって情報漏洩やシステム／サービスの停止、データの改ざんなどに至ることがリスクの一つとして挙げられる。また、スマートシティでは多くの IoT 機器などのアセットが利用されることが想定されるが、それらの機器の供給が停止すること

9 本ガイドラインにおけるサプライチェーンとは、製造業における部品調達のような関係のみならず、クラウドサービスなど外部のデジタルサービスの利用や、API（アプリケーションプログラムインタフェース）を介したシステム同士の連携など、デジタル環境を通じた多様かつ非定型の企業間のつながりも含む（出所：2023 年 10 月　経済産業省、独立行政法人 情報処理推進機構「サイバーセキュリティ経営ガイドライン Ver 3.0」）。

により、スマートシティ全体の運用やサービスに影響が発生するというリスクも想定される。その他、IoT 機器などのアセットのみならず、システムを構成するソフトウェア等においても、開発の段階でバックドアなどの不正なプログラムを混入されることで、情報流出に至るリスクもある。

これらのリスクへの対策としては、推進主体として委託先や再委託先、提携先など、スマートシティの推進に関わるマルチステークホルダ全体を把握することが重要となり、委託先や再委託先等に対しても適切なサプライチェーン・リスクへの対策をしているかを把握することも重要となる。また、委託先や再委託先等におけるセキュリティ管理が十分であるかを確認するために、独自に作成したセキュリティに関するチェックシートを委託先に回答させ、内容を確認したり、第三者認証の取得有無を確認したりすることもサプライチェーン・リスクへの対策となる。その他、調達時の仕様書に、新たに発見された脆弱性に係るサプライチェーン先からの適切な情報提供及び対応に関する内容を含めることで、サプライチェーン全体の脆弱性を適切に把握し、対処できるようにすることも重要である。

なお、推進主体の立場からはサプライチェーン・リスクを把握する必要があるが、委託先としても同様に、再委託先や製品の供給におけるサプライチェーン・リスクへの対策を講じるとともに、委託元へ適切に情報提供することが求められる。

②インシデント対応時の連携

情報漏洩やサービスの停止などのセキュリティインシデントが発生した場合、迅速な原因究明や適切な対応を実施できないことで、上述の被害が拡大するリスクがある。特にスマートシティにおいては、マルチステークホルダが関与するという特性上、インシデント対応の統制は、一企業におけるインシデント対応と比較しても難易度が高くなるため、十分なインシデント対応体制を構築し、インシデント発生時にはマルチステークホルダ間で連携して対処することが求められる。

インシデント対応に関する具体的な対策としては、責任範囲を明確化した上で、マルチステークホルダそれぞれがセキュリティインシデントに対応できる体制を構築する必要があり、速やかな原因究明や対処等を行う上では連絡先や対応手順の整備が必要となる。また、これらの対応が適切かどうかを見直すこと、さらに、対応手順を習熟するという観点で定期的なセキュリティインシデント対応訓練・演習を実施することが望ましい。

インシデント対応の観点に加えて、レジリエンス[10]（強靭さ）を高める活動も同様に重要となる。例えば、公知情報の調査や有識者・他のスマートシティとの情報交換等を通じ、

10 【参考情報】EU サイバーレジリエンス法（CRA）
https://www.meti.go.jp/policy/netsecurity/netsecurity/CRAdraft.pdf?_fsi=OGbCBp7y
（2022 年 9 月　経済産業省）
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act（2023 年 12 月　EC）

スマートシティのサービス提供に対するリスクについて不断の検証を行い、必要とされる措置や対策、事態回復や影響極小化のための手順等を運営に取り込むなどセキュリティレベルの維持とレジリエンス強化に向けた継続的な対応が求められる。

③データ連携時のセキュリティ

スマートシティにおけるデータ連携の形としては、自都市のスマートシティ内のデータ連携だけでなく、自都市のスマートシティと他都市のスマートシティ間の連携や、自都市のスマートシティと近隣自治体や民間事業者が保有する基盤との間の連携等が考えられる。データの安全・安心に連携することがデータの利活用促進につながることから、データ連携時におけるセキュリティを検討し、対策することは非常に重要となる。このデータ連携におけるセキュリティを担保するには、データ連携先、連携元双方がセキュリティに留意することが必要となる。他スマートシティとのデータ連携時、相互承認を実施することも、より高いセキュリティレベルを求める場合に推奨される。

データ連携時にセキュリティが不十分であった場合に起こりうるリスクとしては、データ連携先のセキュリティ不備によるデータの改ざんや消失が想定される。このような事態が発生するとスマートシティの根幹であるデータが信頼・利用できなくなり、適切なサービス提供ができなくなる可能性がある。また、不正侵入によりデータのアクセス権限が不正に変更され、本来連携することのない情報が連携され、情報漏洩に至るというリスクも想定される。

そこで、データ連携時のセキュリティとして求められる対策として、まずはデータ連携先のセキュリティ体制を確認し、信頼できる連携先かどうかを評価する方法が考えられる。また、データ連携時に認証と適切なアクセス制御を課すことで、適切な宛先に適切なデータが連携されるようにする必要がある。

連携されたデータが連携先で悪用されることで、発生する被害を抑制するためにもアクセスログ等を収集し、データ追跡可能性を確保することによって透明性を担保し、データを提供しているサービス利用者が気づかない間にデータを悪用されることを抑止する仕組みの実装が必要であるほか、データの二次利用、三次利用の際のデータの信頼性を担保するためには原本性保証の確保が必要となる。また、データを悪用された場合でも被害を最小限に食い止めるという観点では、必要に応じてデータの匿名化や秘匿化を行う仕組みも導入する必要がある。

更に、インシデント発生時に、①データ連携時に適切と評価した根拠、②アクセスログなどの収集についての根拠と記録している期間等など、運用の根拠などの情報が提供できるよう、スマートシティ推進主体は運用設計することを推奨する。

その他、データ連携時はデータ連携元・連携先の API でシステム同士が接続されるため、API において標準的に求められるセキュリティ対策として通信の暗号化による盗聴の防

止や証明書を利用したデータの改ざんやなりすましの防止、アクセスログの監視・分析等を実施することが求められる。

3. スマートシティにおけるセキュリティ対策

3.1. 各カテゴリのセキュリティ対策

４つのカテゴリに分類したスマートシティの構成要素について、それぞれのカテゴリにおけるセキュリティ対策を以下に示す。

3.1.1. ガバナンス

本カテゴリは、スマートシティ全体の取組や施策の方向性の決定、ルールや基本方針の策定、組織体制の構築などがなされるカテゴリであり、セキュリティの観点からは、スマートシティ全体としてのリスクアセスメントに基づくセキュリティに関するポリシーの策定と、それらの浸透、ガバナンスの維持などがその役割として挙げられる。

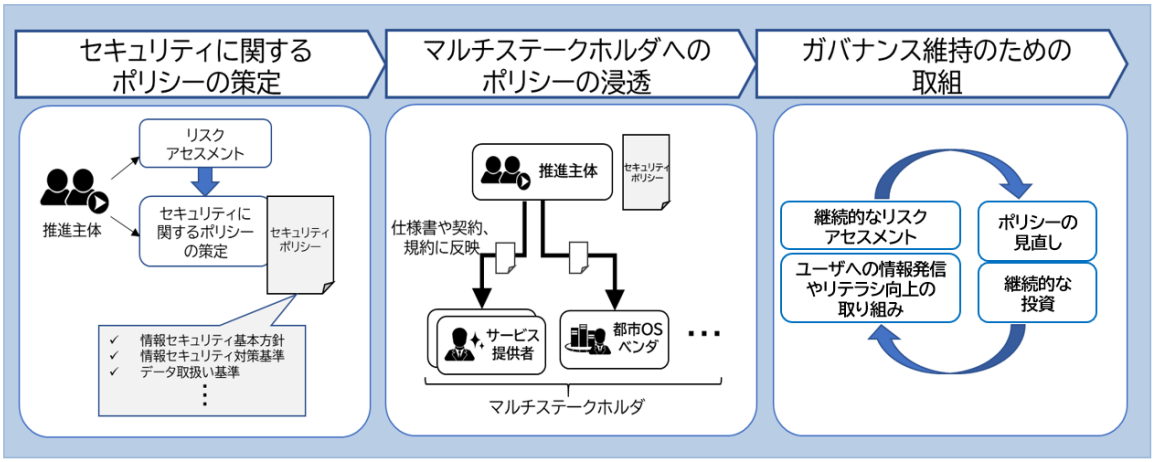


図３－１　ガバナンスにおけるセキュリティ対策のイメージ

① セキュリティに関するポリシーの策定

スマートシティ全体としてのリスクアセスメントに基づき、セキュリティに関するポリシーが策定される。セキュリティに関するポリシーとして、情報セキュリティ基本方針、セキュリティ対策基準、データ取扱い基準など、様々なものが存在するが、それぞれの内容を一つのセキュリティポリシーとして合わせて記載する、それぞれを独立して策定する、などのこれらポリシーの在り方は、策定する主体それぞれにおいて様々であるが、スマートシティ全体の管理監督の役割を負うべき推進主体が主体性を持って策定すべきものである。

これらのポリシーはスマートシティ全体として遵守すべき基本方針やポリシーとして定めるものであるが、推進主体として既に保有しているポリシーがある場合には、それぞれの推進主体の状況や維持のしやすさ等を考慮した上で、それらとの整合性も鑑みて策定す

る必要がある。ただし、既存のポリシーを参考としつつ定める場合にも、スマートシティ全体として遵守すべき基本方針やポリシーなどに準拠したレベルに統一することが必要となるため、推進主体はその整合性を確認しながら全体の策定プロセスをコントロールすることが求められる。

なお、セキュリティに関するポリシーに基づくセキュリティの推進については、推進主体以外の多様な関係組織や有識者が関わることも想定されるため、各スマートシティの状況に応じた、セキュリティ推進体制を構築することが求められる。

＜策定する内容＞
ガバナンス①-1：情報セキュリティ基本方針を策定する
ガバナンス①-2：セキュリティ対策基準を策定する
ガバナンス①-3：データ取扱い基準を策定する
ガバナンス①-4：インシデント対応手順を策定する
ガバナンス①-5：事業継続計画を策定する
ガバナンス①-6：委託先や提携先の評価基準を策定する
＜策定プロセス＞
ガバナンス①-7：リスクアセスメントを実施する
ガバナンス①-8：法令やガイドライン等との整合性を確認する
ガバナンス①-9：各種文書の作成や各活動の記録を取り共有・管理する機能を整備する

ガバナンス①-1：情報セキュリティ基本方針を策定する

策定すべきポリシーとして最も重要となるのが情報セキュリティ基本方針である。情報セキュリティ基本方針では、目的や対象範囲などの基本的な事項が記載されるほか、スマートシティ全体としてのリスクアセスメントに基づき、セキュリティ担保のための取組方針が記載されており、セキュリティに関する他のポリシーは、全てこの基本方針に従う形で作成されることとなる。

ガバナンス①-2：セキュリティ対策基準を策定する

セキュリティ対策基準は、情報セキュリティ基本方針で定められた事項を実施するために、具体的な遵守事項や判断基準等を定めるポリシーである。内容としては、組織体制や情報資産の分類・管理に関する項目のほか、管理的及び技術的なセキュリティ対策について、具体的な内容が記載される。

ガバナンス①-3：データ取扱い基準を策定する

スマートシティで取り扱われるデータは、オープンデータ、限定公開データ、クローズドデータに分類することができる。データ取扱い基準では、取り扱うデータをセキュリテ

ィやプライバシーの観点、サービスの特性を踏まえてこれらの分類に当てはめるとともに、取り扱うデータの利用目的、内容、取得方法、セキュリティ対策レベル、などの確認のほか、データの所有に関する考え方や利用権限について提供元や利用者との関係性を示す必要がある。

データ取扱い基準を策定する際は、自身のスマートシティで利活用されるデータの特性や関連する法令、その他のポリシーとの整合性に留意する。例えば、個人情報保護法で規定する「個人情報」や「要配慮個人情報」を含み、クローズドデータあるいは限定公開データを扱う場合には、それぞれ「準拠すべき法令やガイドラインをもとにしたセキュリティの要件の洗い出し。」、「サービス提供等のために複数の者がデータ取扱いを行う場合には関係者間の契約の形態（業務委託・業務提携）に基づいた、責任分界点、授受するデータに関する記録と削除に関する取り決めの明確化。」、「データを保護する責任者とデータの開示・苦情を受け付ける窓口の整理。」、「データ利用者までのデータの流れと容易照合性の確保と、関係システム・組織やデータライフサイクル毎に求めるセキュリティの要件の整理。」、「セキュリティ要件の、契約書・ポリシー・ガイドラインなど策定した文書への反映と、運用への適用。」などが考えられる。

ガバナンス①-4：インシデント対応手順を策定する

インシデント対応手順では、スマートシティにおいてサイバー攻撃や内部不正等によるセキュリティインシデントが発生した際の対応手順を定める。内容としては、インシデント対応に関与する関係主体やそれぞれの責任範囲の明確化、連絡体制や連絡先などの整備、対応における判断基準やインシデント対応フローなどが記載されることとなる。なお、市民などの利用者から見た窓口機能を担う主体である推進主体あるいは各サービス提供主体において、インシデント発生時の適切な情報発信や問合せ対応を可能とする観点から個別のインシデントの対応状況を随時把握できる枠組みを作っておくことが推奨される。

ガバナンス①-5：事業継続計画を策定する

事業継続計画はスマートシティ自身及び提供するサービスが停止した際の対応方針や手順について記載したドキュメントである。内容としては障害やセキュリティ事故等が発生した際にどの機能を優先して保護するかといった判断基準や、スマートシティ事業継続のための役割分担、対応手順などが含まれる。

ガバナンス①-6：委託先や提携先の評価基準を策定する

スマートシティでは、サービスを提供する上で、都市 OS の構築やサービス提供者との提携など、様々な主体との連携が必要となるため、委託先や提携先をセキュリティの観点から評価する基準が必要となる。詳細は「3.2.1 サプライチェーンの適切な管理」でも記載がされるが、外部委託先や提携先のセキュリティ管理体制やセキュリティに関する第三者

認証の取得有無など、外部委託を実施する際に求めるべき内容や選定条件などが記載される。

ガバナンス①-7：リスクアセスメントを実施する

上述で挙げたセキュリティに関するポリシーを策定する上で、重要となるのがリスクアセスメントである。リスクアセスメントの具体的な手法[11]としては、スマートシティの全体構成を把握するとともに、守るべき情報資産や機能（サービス）を特定し、それらの情報資産や機能、人命や健康に対して発生する可能性のある脅威[12]とその発生確率、発生した場合の影響度・深刻度を分析・評価する、という流れで実施する。リスクアセスメントをした後は、それらのリスクに対してどのように対処するかを決定する。例えば、リスクを低減・回避するためのセキュリティ対策を策定したり、リスクを受容したりといったところを決定する。

これらのリスクアセスメントのプロセスや、リスクアセスメントの結果を元にした実施すべきセキュリティ対策の策定は専門的な知見を要することから、例えば、セキュリティに知見のあるベンダや、大学・大学院の教授、弁護士などの有識者が参画する推進協議会のような場において検討するという方法もある。また、コストや取り扱うデータの特性等を考慮したうえで、リスクアセスメントの実施について、専門性を持った外部機関に委託するという方法もある。

なお、リスクアセスメントを実施する際は、それぞれのリスクアセスメントにおいて誰もが同一の基準で分析・評価ができるよう、リスク評価基準を定めておくことが望ましい。

また、セキュリティに関するリスクアセスメントだけでなく、プライバシーの観点からもプライバシー影響評価（PIA）を行い、プライバシーに関するリスクも分析・評価した上で低減・回避できるような対策を検討することが望ましい。

ガバナンス①-8：法令やガイドライン等との整合性を確認する

セキュリティに関するポリシーを策定するにあたっては、法令やガイドライン等との整合性に十分留意する必要がある。特に法令については、自身のスマートシティにおいて何の法令に遵守する必要があるかを正確に見極め、遵守できる形でポリシーを策定する必要がある。例えば、スマートシティで個人情報を取り扱う場合においては、「個人情報の保護に関する法律」等の関連法令への遵守が求められるし、EU 圏内住民の個人データを取り扱

11 一般的なリスクアセスメントの参考資料としては「NIST SP800-30　リスクアセスメントの手引き（https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025325.pdf）が参考となる。

12 人命や健康に関する脅威・リスク分析に関する記述は、一般社団法人重要生活機器連携セキュリティ協議会（CCDS）が発行する「CCDS 製品分野別セキュリティガイドライン_スマートホーム編」が参考となる。

う場合においては、EU 一般データ保護規則（GDPR）といった国外の法令への遵守も求められることとなる。

整合性を確認するには、関係法令側に大幅な変更があった場合、システムに大きな機能変更があった場合、あるいは一定期間経過毎といった契機に見直せるよう、マネジメントシステムを整備し、適切な PDCA サイクルをスパイラル的に継続することが望ましい。

また、ガイドライン類に関しては、必ず遵守することが求められるものではないが、広く一般的に参照されることが多いため、業界における基準（スタンダード）として認識されることがあり、かつ自身のスマートシティにおけるセキュリティ対策を検討する上での助けとなることから、自身のスマートシティにおける特性を理解した上で関連するガイドラインを参照することが望ましい。

これらの確認すべき法令やガイドラインの代表的なものについては、【Appendix】A「参照すべき法令・ガイドラインの一覧」において、参照することが望ましい主体や、参照するべきポイント等も含めて、一覧として表記しているので参照されたい。ただし、整理されている情報は本ガイドライン策定時点のものとなっているため、適宜インターネット上で公開されている最新の情報を参照する必要があることに留意する。

ガバナンス①-9：各種文書の作成や各活動の記録を取り共有・管理する機能を整備する

上記に列挙した様々な方針・基準・手順を全てのステークホルダに浸透させることが必要となる。更にシステムの機能変更、新たなセキュリティ脅威出現等の変化に対応するにしたがって、上記方針・基準・手順は適切な改訂が必要となる。

そのために、各種文書の作成や各活動の記録を取り、共有・管理するための体制および機能をあらかじめ整備しておく必要がある。

② マルチステークホルダへのポリシーの浸透

セキュリティに関するポリシーを策定した後は、策定したポリシーがマルチステークホルダにおいて適用されるよう、調達仕様書や契約・規約の中に適切に反映し、落とし込んでいく必要がある。本項目では、「契約や規約の中で特に反映すべき内容」に焦点を当てて記載する。なお、委託先等の評価や管理については、「3.2.1 適切なサプライチェーンの管理」において詳細を記載する。

ガバナンス②-1：ポリシーを遵守するためのセキュリティ要件を調達仕様書に反映する
ガバナンス②-2：データ取扱い基準を契約・規約に反映する
ガバナンス②-3：契約・規約で責任範囲を明確化する
ガバナンス②-4：接続を希望する事業者のセキュリティ対応レベル審査・監査
ガバナンス②-5：運営関係者に対する定期的なトレーニングを実施する

ガバナンス②-1：ポリシーを遵守するためのセキュリティ要件を調達仕様書に反映する

情報セキュリティ基本方針や、セキュリティ対策基準等のセキュリティに関するポリシーに則り、セキュリティ要件を策定し、調達仕様書へ反映することでスマートシティにおいて遵守が求められるセキュリティに関するポリシーをマルチステークホルダへ浸透させることが可能となる。セキュリティ要件を策定する際は、ポリシー策定時と同様、当該委託事業におけるシステムやサービスの種類や取り扱う情報などに応じてリスクアセスメントを行い、セキュリティ要件を定めることが望ましい。セキュリティ要件に含める内容としては、提供する情報の目的外の利用禁止、情報セキュリティの管理体制の構築、情報セキュリティインシデントへの対処方法、業務において発生したインシデントの共有、推進主体が実施するステークホルダ間の情報共有機会への協力等を含めることが望ましい。なお、都市 OS の保守等、運用に関する委託を実施する場合は、脆弱性対応のためのパッチ適用やソフトウェアアップデートなどの追加で必要となるセキュリティ対策についても定めておくことを推奨する。

ガバナンス②-2：データ取扱い基準を契約・規約に反映する

スマートシティでは、データが様々なステークホルダを横断的に行き交うため、データの利活用においては情報漏洩や不正利用などのリスクが伴う。そのため、マルチステークホルダにおいてスマートシティのデータを取り扱う場合は、データ取扱い基準について明確に契約や規約[13]の中で定める必要がある。具体的には、取り扱う可能性のあるデータを明確化した上で、「ガバナンス①-3：データ取扱い基準を策定する」で定めた事項のほか、利用期間、地域、契約終了時の取扱い、分析・加工及び派生データ等の権利について契約や規約の中で定めることが望ましい。

ガバナンス②-3：契約・規約で責任範囲を明確化する

推進主体とマルチステークホルダの間のセキュリティに関する事項について、お互い責任を押しつけ合う状況を避けるために、双方の間において責任範囲について合意し、契約や規約でこれを明確に定めることが重要である。

委託先・提携先との契約において、責任範囲を明確化する観点として、システムとしての責任分界点とデータの責任分界点の２点が挙げられる。システムの責任分界点については、当該委託事業や提携事業におけるシステムの構成図をもとに、データの責任分界点については、データのフロー図や、データ取扱い基準で示されている取り扱うデータをもとに、契約の中で明確に記載されていることが望ましい。ただし、たとえ契約の間で責任範囲を明確化しても、スマートシティにおいて何らかの事案が発生した場合は、住民にスマートシティサービスを提供している立場でもある委託元側でも一定の責任を負う必要があるという点について、留意する必要がある。

13　データに関する契約については、経済産業省の「AI・データの利用に関する契約ガイドライン」等が参考となる。

なお、詳細は「3.2.2 インシデント対応時の連携」で記載されることとなるが、インシデント対応時における連携においても責任範囲を明確化するとともに実施すべき対策について記載されていると、円滑なインシデント対応が可能となる。

また、サービス利用者がスマートシティサービスを利用するケースやサービス提供者がスマートシティのオープンデータを利用するケースなどにおいては、推進主体における免責事項を規約に記載する形で責任範囲を定めることが多い。特に、サービス利用者がスマートシティサービスを利用するケースでは、その利用者のセキュリティリテラシ向上のために、推進主体において、サービスを正しく利用するためのサービス利用者への啓発活動や規約への明確かつ簡潔な記載、規約への確実な同意を求めることが重要となる。

ガバナンス②-4：接続を希望する事業者のセキュリティ対応レベル審査・監査

ガバナンス①-6 で委託先・提携先の評価基準の整備について、ガバナンス②-1 でセキュリティ要件の調達仕様書への反映について、それぞれ述べたが、実際にスマートシティに接続を希望する事業者のセキュリティ対応レベルについて、基準を満たしていることを確認したうえで接続する必要がある。そのための審査対応や、新たに基準や要件、ポリシーが変更された場合の新基準への対応状況の監査などについてあらかじめプロセスや役割を整理しておくことが必要となる。

ガバナンス②-5：運営関係者に対する定期的なトレーニングを実施する

定期的なリスクアセスメントやセキュリティポリシー、対策の見直しの結果をスマートシティの運営に適切に反映していくためには、スマートシティの運営に携わる各主体の関係者がその内容を十分に認知し、実行できる必要がある。そのための活動としてスマートシティの推進主体が、運営関係者に対して、教育や情報提供、インシデント対応時の連携等を目的としたトレーニングの定期的な実施を求めていくことが必要である。

また、スマートシティの運営には多数のステークホルダが関係しており、それぞれの主体が知見や気付きを有することが想定されることから、一方向の情報伝達や研修のようなものだけではなく、相互の持つ情報を共有・交換できるような取り組みを検討すると良い。

③　ガバナンス維持のための取組

スマートシティのセキュリティを継続的に維持・改善するためには、PDCA サイクルを回し、セキュリティのポリシーやセキュリティ対策等の見直しを継続的に行い、適切にセキュリティへの投資を続けていくことが重要となる。また、金銭的な投資のみならず、セキュリティの知見を保有する人材を確保するため、人材の育成や、適切な配置など、人的リソースへの投資もセキュリティのガバナンスを維持するうえでは重要となる。

ガバナンス③-1：継続的なリスクアセスメントの実施とセキュリティに関するポリシーの見直しを実施する
ガバナンス③-2：セキュリティ対策への適切な投資を継続的に実施する
ガバナンス③-3：ユーザに対する情報発信やリテラシ向上の取り組みを実施する

ガバナンス③-1：継続的なリスクアセスメントの実施とセキュリティに関するポリシーの見直しを実施する

ガバナンス①-8 ではリスクアセスメントの必要性について述べたが、リスクアセスメントは一度実施して終わりではなく、提供するサービスなどの変化やスマートシティで取り扱う情報の追加、新たなサイバー攻撃の発生に伴う脅威の拡大等に応じて、適切なタイミングで実施する必要がある。同時にこれらのリスクアセスメントの結果、必要とされるセキュリティ対策に変化が生まれた場合は、セキュリティ対策基準などのポリシーも定期的に変更し、常に最適な状態を維持することが重要となる。

ガバナンス③-2：セキュリティ対策への適切な投資を継続的に実施する

上述のとおり、セキュリティ対策は継続的な実施が求められることから、セキュリティ対策への適切な投資についても継続的に実施する必要がある。セキュリティインシデントへの対応として事後的に突発的なセキュリティ対策で対応することは、スマートシティの評判を落とすだけでなく、多大な費用が発生することになる。そのため、リスクアセスメントの時期を予算要求前に設定し、アセスメント結果を元に適切なセキュリティ対策を決定することで、効率的にセキュリティへの投資をしつつセキュリティの維持・向上を図ることができる。

ガバナンス③-3：ユーザに対する情報発信やリテラシ向上の取り組みを実施する

スマートシティの目的は、市民などの利用者がより便利かつ快適に過ごす・活動することができるようにすることである。そのためには、利用者自身が安心してスマートシティのメリットを最大限享受できるようにすることが望まれる。このような観点から、スマートシティのサービス内容や利用方法、運営・問合せ先について、利用者に対して分かりやすく適切な情報発信を行うなど、スマートシティに関する情報発信の充実が重要となる。

3.1.2. サービス

サービスとは、利用者がスマートシティで生み出されたメリットを享受できるように、利用者に提供されるものであり、一つのスマートシティにおいて複数のサービスがウェブアプ

リケーションといった形式で提供されることが多い。そのため、それぞれのサービスにおける守るべき機能や情報などを特定した上で、それぞれのサービスにおいてもリスクアセスメントを実施することが求められる。また、リスクアセスメント結果を踏まえ、外部からのサイバー攻撃等への対策やセキュリティインシデント発生の未然防止のための対策、インシデント発生に備えたセキュリティ対策等を講じる必要がある。

同時に気を付けなければならないのは、ユーザがサービスの仕様上の考慮不足を悪用することにより、直接または間接的に不正な利益を得る可能性があるため、機密性・完全性・可用性を中心としたセキュリティ対策のみではなく、サービス仕様に応じたセキュリティ対策を講じる必要がある点である。

その他にも、近年における機械学習等の AI 高度化に伴い、これを利用者へのより利便性の高いサービス提供のために活用するケースが将来的に増える可能性がある。AI を活用する際には、外部資料[14]を参考に、セキュリティ上の留意点を踏まえて設計・開発することを推奨する。

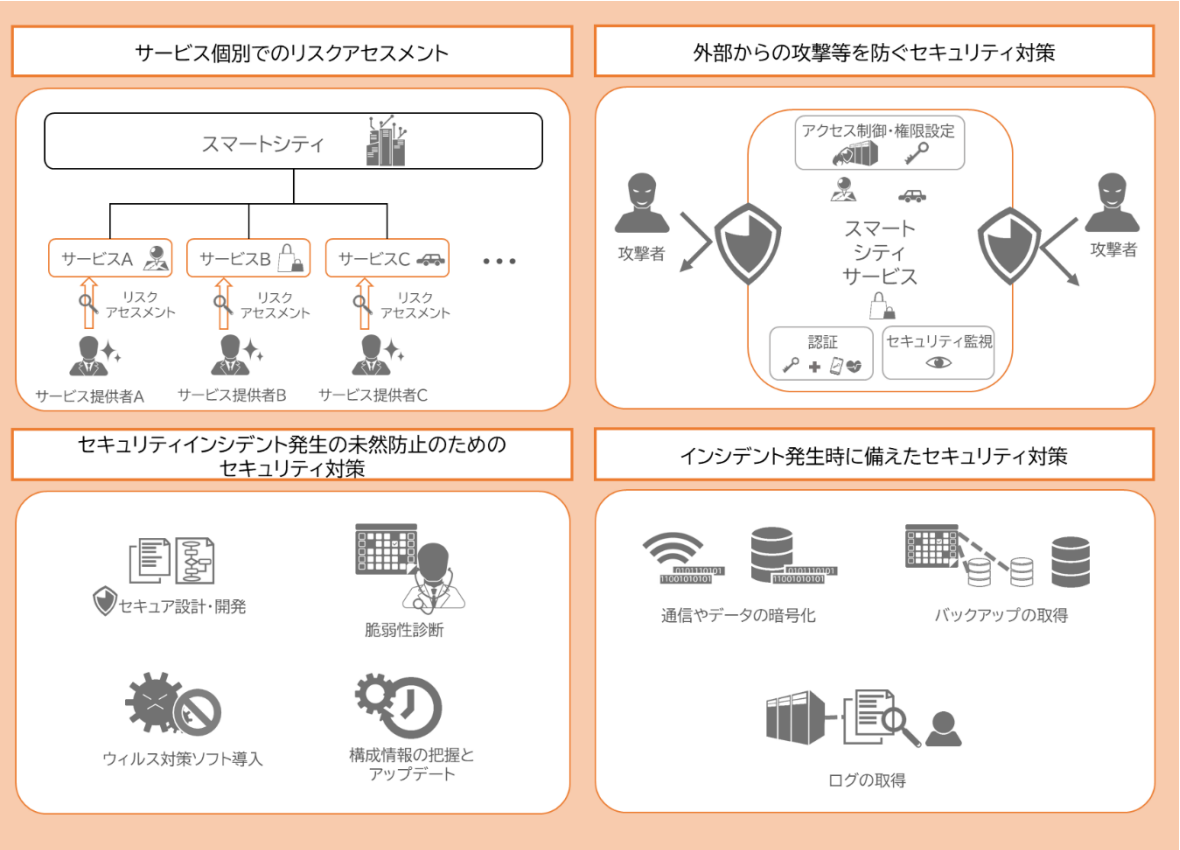


図３－２　サービスにおけるセキュリティ対策のイメージ

14 外部資料：「AI 利活用ガイドライン（2020 年 1 月 31 日、総務省情報通信政策研究所）」、「機械学習品質マネジメントガイドライン（2022 年 8 月 2 日、国立研究開発法人産業技術総合研究所）」、「AI に関する暫定的な論点整理」（2023 年 5 月 26 日、内閣府）、「AI 事業者ガイドライン（第 1.0 版）」（2024 年 4 月 19 日、総務省　経済産業省）が挙げられる。

① サービス個別でのリスクアセスメントの実施

スマートシティでは一般的に多様なサービスが提供されるが、それぞれのサービスにおいて、機能や取り扱う情報などを踏まえて求められるセキュリティの基準は異なってくる。例えば、災害対策や防犯の対策においては、可用性が重視されたセキュリティ対策、医療サービスなどでは機密性が重視されたセキュリティ対策を採用することが多い。

そこで、ガバナンスカテゴリでも実施したように、個別のサービスごとにおいてもリスクアセスメントを行い、適切なセキュリティ対策を策定していく必要がある。

サービス①：それぞれのサービスにおいてリスクアセスメントを実施する

サービスのリスクアセスメントにおいては、それぞれのサービスにおいて守るべき情報資産や機能の他、金銭的な被害や利用者の安全面など情報資産以外のリスクも含めて、予め策定したスマートシティのセキュリティに関するポリシー（リスク評価基準やデータ取扱い基準等）を踏まえて特定し、それらの情報資産や機能等に対して発生する可能性のある脅威とその発生確率、発生した場合の影響度を評価し、それらのリスクに対してどのように対処するかを決定する、といったプロセスが必要となる。実施するセキュリティ対策を検討する上では、これらのリスクアセスメントの結果を活用することが重要である。

表３－１　保護すべき情報資産の例

情報資産	説明
コンテンツ	音声、画像、動画等のマルチメディアデータ、コンテンツ利用履歴等
ユーザ情報	ユーザの個人情報（氏名/住所/電話番号/生年月日/クレジットカード番号/利用履歴・操作履歴 等）、ユーザ認証情報
機器情報	機器そのものに関する情報（機種、ID、シリアル ID 等）、機器認証情報等
ソフトウェアの状態	各ソフトウェアに固有の状態データ（動作状態、ネットワーク利用状態）等
ソフトウェアの設定	各ソフトウェアに固有の設定データ（動作設定、ネットワーク設定、権限設定、バージョン）等
ソフトウェア	OS、ミドルウェア、アプリケーション等（ファームウェアと呼ばれることもある）
設計データ内部ロジック	企画・設計フェーズで発生する仕様書・設計書の設計情報等

※出典：IPA「組込みシステムのセキュリティへの取組みガイド」を基に作成

② 外部からの攻撃等を防ぐセキュリティ対策

外部からの攻撃等を防ぐためには、企画、設計・開発段階から、様々なセキュリティ対策を実装し、運用していく必要がある。サービスにおいては、外部からの攻撃等への対策として、基本的に以下のセキュリティ対策を実装することが望ましい。

サービス②-1：サービスの不正な利用を規約・契約で抑止する
サービス②-2：サービスへのアクセス制御を実装、運用する
サービス②-3：適切な権限設定を実施し、管理する
サービス②-4：身元確認機能を実装する
サービス②-5：認証機能を実装する
サービス②-6：セキュリティ監視を実施する

サービス②-1　サービスの不正な利用を規約・契約で抑止する

サービスの不正な利用の抑止対策として、利用登録時の規約・契約での同意がある。サービスの利用開始やアカウント登録にあたり、虚偽の情報登録、第三者によるサービス利用、著作権や商標権、知財権等の侵害、プライバシー侵害、不正アクセス、不正なサービス利用、運営に支障を与える行為等の禁止事項を明確にし、また、それらが疑われる場合のアカウント停止、損害賠償等、必要な措置を取ることに対し同意取得することが必要である。

サービス②-2　サービスへのアクセス制御を実装、運用する

外部攻撃からの対策として基本となるのがアクセス制御である。サービスに関わるシステムが配置されているセグメントに外部から通信する場合は、ファイアウォール等を実装するなどし、適切なアクセス制御を実装する必要がある。例えば、IP アドレス等で通信元・通信先を制限する、プロトコルやポート番号を制限する等で、サービス提供に必要な通信以外を遮断することによって、攻撃者によるシステムへの不正なアクセスなどを防ぐことができる。なお、外部からの通信に限らず、システム内の他セグメントからの通信や同一セグメント内の通信においても適切なアクセス制御の実装は必要である点に注意する。

サービス②-3：適切な権限設定を実施し、管理する

システムや機器、データなどの情報資産へのアクセスを、必要な人や役割などに限定するために権限を設定し、管理することも基本的なセキュリティ対策の一つとなる。この権限設定・管理は外部からの攻撃への対策となるだけでなく、内部不正によるセキュリティ対策としても有効である。

権限設定・管理において特に重要となるのが管理者権限である。これを攻撃者に悪用されるとシステムの変更やログなどの改ざん、データの閲覧などができるようになってしまうことから、管理者権限の割当は最小限にするとともに、厳重に管理する必要がある。

権限管理では、システムや機器、データなどの情報資産に対してどのようなアカウントが存在し、どういった権限が割り当てられているかを管理することが重要となる。管理の方法としては、例えばアカウントや役割、権限などを整理した一覧表を作成した後、定期的に棚卸しを実施し、長期間利用されていないアカウントがないか、部署異動や退職した人の権限が残されていないか等を確認することも重要となる。

なお、サービスにおいてはサービス利用者にアカウントを割り振り、ユーザとしての権限を割り当てることがあるが、他人のデータなどにアクセスができないよう、限定的な権限付与ができる仕組みを実装し、適切に運用する必要がある。

サービス②-4：サービスの特性に応じた身元確認機能を実装する

サービスの特性に応じてサービス利用にあたっては身元確認を適切に行う。身元確認とは、本人確認と呼ばれることもある手続きであり、本人であることを前提としたサービス提供を行う場合には、当該身元の確認度合によって、サービスを提供可能かどうか判断する必要がある。サービスの特性に応じた身元確認度合いとしては例えば要求レベルの低い順に以下のようなものが想定される。

- 登録情報として自己申告を許容し、サービスとしてお客さまの登録情報の確からしさを必要としないサービス
- 機械的に大量に作成されたものではなく、個人に紐づいたことを確認した状態で提供可能なサービス
- 法規要件などで利用者を厳格に確認する必要があるサービス

例えば自己申告にあたる確認方法としては氏名やメールアドレス等の自由記述のみといった方法や顔写真付き本人確認書類の画像アップロードなどがある。個人紐づけの確認された状態としては、オンライン本人確認（eKYC）や本人確認書類の IC チップ情報の活用[15]などがあり、信頼性の高い確認手法としてはマイナンバーカードの公的個人認証の活用などが考えられる。決済機能やポイント機能、個人情報を扱うサービスにおいては、アカウント登録時にマイナンバーカードの公的個人認証サービスを利用するなど厳格な身元確認を行い、1 人が複数のアカウントを登録することを回避することが有効である。

その他、アカウントリカバリ時の身元確認は新規登録時に比べて甘くなっている場合があるため気を付ける必要がある。コールセンター等での身元確認が甘い場合に、第 3 者によるアカウントの乗っ取りが発生する可能性を考慮することが求められる。

サービス②-5：認証機能を実装する

15 例として「犯罪による収益の移転防止に関する法律(犯収法)」の第 6 条第 1 項第 1 号ホ方式、ヘ方式、ト方式による確認が挙げられる。

権限設定・管理とセットで必要となるのが、アクセスしようとしている人が適切なアクセス権限を割り当てられた本人であるかを確認するための認証機能の実装である。サービス提供者がシステムにアクセスする際や、サービス利用者がサービスにアクセスする際は、パスワードなどの知識情報を入力することによって本人であることの確認を行うことが基本的な認証の例となる。その他の認証の種類としては、所持情報（IC カード、クライアント証明書、SMS 認証[16]）、生体情報（指紋認証、静脈認証や虹彩認証）等があるが、不正アクセスやなりすましへの対策として、より高いレベルのセキュリティを実現するためには、これらの認証方法から、異なる複数の要素を組み合わせた、多要素認証を採用することが望ましい。なお、どのような認証を採用するかについては、認証を実装するシステムやサービス等の特性や重要度、アクセス元の環境に応じて適切に決定する必要がある事に留意する。また、上述の対策のほか、接続する相手のシステム・サービスのなりすましへの対策として、接続するシステム・サービス相互で公開鍵暗号技術や電子証明書等を活用し、照会することでアクセスを許可する公開鍵暗号基盤（PKI）による認証が有効となる。

シングルサインオンによる他社サービスの認証機能を利用する場合は、なりすましや大量アカウントの作成などに狙われやすく、身元確認による本人性の高さ、および、認証の強度が下がらないように仕様を検討する必要がある。

サービス②-6：セキュリティ監視を実施する

ネットワークにおけるセキュリティ監視としては、インターネットとシステムの境界に IDS（不正侵入検知システム）や IPS（不正侵入防止システム）を設置し、それを監視することによって、不正なコマンドが含まれた通信等を検知、遮断することが可能となる。同一システム内に複数のセグメントが存在する場合は、セグメント間の通信においても IDS/IPS による監視が有効な場合がある。

IDS/IPS ではアプリケーションレイヤの監視はできないため、ウェブアプリケーションのセキュリティ監視を実施する場合は WAF（Web Application Firewall）を実装することで、アプリケーションレベルで不正なコマンドを検知、遮断することが可能となる。なお、IDS/IPS 及び WAF は暗号化通信（SSL/TLS 通信）を監視できないため、暗号化通信の終端位置を考慮する等し、通信を監視できる環境を検討・構築する必要がある。

また、その他のセキュリティ対策として、DDoS 攻撃対策やウェブコンテンツ、保存されている設定ファイルやシステムデータの改ざん検知等の改ざんの検知等を必要に応じて組み合わせることで、より高度なセキュリティ監視を実現することが可能となる。

[16] SMS 認証は SMS の盗聴（予めインストールされた不正アプリやロックされていても通知時にメッセージの中身が見えてしまう、等）や SIM に対する攻撃などでパスコードを窃取される危険性があるため、SMS 認証を活用する際はこれらのリスクについて評価し、適切に対策が取れている前提で利用することが望ましい。

サービスにおけるセキュリティ監視としては、サービスへの不正ログインやプライバシー違反の監視、および、登録ユーザ自身によるサービスの不正な利用を検知・監視する仕組みの必要性についても留意すべきである。

③ セキュリティインシデント発生の未然防止のためのセキュリティ対策

サービスにおいては、外部からの攻撃等を防止するセキュリティ対策のほか、インシデントに至ることを未然に防止するセキュリティ対策として、サービスの企画・設計・開発工程から運用工程において、脆弱性が入り込まないようにするための対策や運用管理端末へのセキュリティ対策がある。

サービス③-1：サービスの企画・設計・開発工程における脆弱性を適切に管理する
サービス③-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する
サービス③-3：運用管理端末へのセキュリティ対策を実施する

サービス③-1：サービスの企画・設計・開発工程における脆弱性を適切に管理する

サービスにおけるウェブアプリケーション等を企画・設計・開発する上では、その段階からセキュア設計やセキュアコーディングを実施することによって脆弱性が入り込まないように配慮しつつ、サービスイン前に適切にセキュリティテストや脆弱性診断を実施することで、既知の脆弱性への対処が可能となる。なお、システム開発の早い段階からセキュリティを考慮した設計を行うことで、サービスイン前におけるセキュリティテストや脆弱性診断等での発見事項が少なくなり、結果として工程に手戻りが発生しなくなるため、リソースや開発コストを効率的に使用することができる。

加えて、システムの機密性・可用性・完全性だけでなく、提供するサービスや取り扱うデータに応じて、利用者の身元確認や認証強度を適切に確保していく必要がある。

サービス③-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する

脆弱性については、開発工程において対策を実施すれば完全なセキュリティが担保できるわけではなく、日々のサイバー攻撃の進化やソフトウェア等の更新に伴って新しい脆弱性が発見される。そのため、開発工程における脆弱性の適切な管理のほかに、運用フェーズにおいても新たな脆弱性がないかを把握し、それに対応する必要がある。

脆弱性を把握する手段の一つとして挙げられるのが定期的な脆弱性診断の実施である。基本的にはシステムの設定変更や新規機能の追加などがなければ、既知の脆弱性については一度確認すれば問題ないが、システムを運用する過程における設定変更などで気がつかない内に脆弱性が生じている可能性があるため、定期的な脆弱性診断を実施することを推奨する。

また、新規の脆弱性の中には緊急性の高い脆弱性が含まれることもあり、それを放置すると重大なセキュリティインシデントに至ってしまうケースもあり得る。そこで、自身のシステムで利用しているOSやミドルウェア、ソフトウェア等の構成管理情報を常に最新化して管理しつつ、新規の脆弱性情報を収集し、自身のシステムにおいて対処が必要かどうかを適宜判断し、適切なタイミングでバージョンアップやセキュリティパッチ適用などの対応を実施することが望ましい。

その他に、サービスの脆弱性を突いた事例情報を収集するとともに、自身の提供するサービスが同様の脆弱性に対処できているかを評価する仕組みを構築することが望ましい。

サービス③-3：運用管理端末へのセキュリティ対策を実施する

運用管理端末はサービス提供中の環境へ直接アクセス可能であることから、踏み台として悪用されるリスクがある。そのため、運用管理端末へのアクセス制御の実施や認証の導入はもちろん、ウイルス対策ソフトの導入や未知の不正プログラムへの対策、OS等の脆弱性への対応、運用管理端末でのシステム動作ログ等の取得といった、基本的なセキュリティ対策の実施が必要となる。

また、運用管理端末の設置場所についても、通常の執務室等、業務に関係のない者が日常的に入り込める場所ではなく、セキュリティルーム等、物理的にアクセスが制限された場所に配置することが望ましい。

④ インシデント発生時に備えたセキュリティ対策

②～③で示した対策を実施することでセキュリティインシデントが発生しないようにすることが当然望ましいが、実際はセキュリティインシデントの発生をゼロにすることは困難である。そこで、セキュリティインシデントが発生してもその被害を最小化できるよう、外部との通信やデータの暗号化、バックアップの取得、ログの取得などの対応も合わせて実施する必要がある。

サービス④-1：外部との通信やデータの暗号化を実施する
サービス④-2：定期的にバックアップを取得する
サービス④-3：証跡確保のためのログを取得する
サービス④-4：インシデント発生時のリスク軽減策を検討する

サービス④-1：外部との通信やデータの暗号化を実施する

外部との通信の内容が盗聴されたり、システム内で保有しているデータが流出したとしても、適切な強度の暗号アルゴリズムを使って通信やデータを暗号化していた場合は、解読が困難となり、被害の発生を抑止することができる。暗号化強度については、「CRYPTREC暗号リスト(電子政府推奨暗号リスト)」等で定義された十分な強度の暗号アルゴリズムを

採用することが望ましい。なお、パスワード情報など、復号が不要なデータについては、そのデータが容易に推測できないよう、ハッシュ関数を利用することが推奨される。

なお、通信の暗号化に関しては盗聴を防ぐという観点で、外部からの攻撃等を防ぐセキュリティ対策としても有効である。

サービス④-2：定期的にバックアップを取得する

システムの構成情報や、重要なデータについては、その可用性や事業継続などを考慮して、定期的にバックアップを取得することが望ましい。バックアップデータは定期的に物理的な媒体に書き出したり、災害への影響を考慮して別のロケーション（地理的に別の場所にあるデータセンタ等）に保管する等して確実に維持できるようにすることが推奨される。

サービス④-3：証跡確保のためのログを取得する

ログはセキュリティインシデントが発生した際に、原因の究明や対策の検討を行う上で必ず必要な情報となる。取得すべきログとしては、サーバ等に対するアクセスログや操作ログ、IDS や IPS 等における検知ログ、ファイアウォールにおける通信ログ等、多岐にわたるが、実際にインシデントが発生した場合は、これらのログを相関的に分析することで、攻撃内容や被害状況などを特定することが可能となる。なお、ログを相関的に分析する際は、正確に攻撃の痕跡が追えるよう、それぞれの機器において時刻同期も実施すると良い。また、システム構成が複雑化することにより複数のログを管理・監視する必要がある場合は、ログ分析基盤を導入し、ログを一元管理することで相関的な分析が可能となる。

その他、事後的にインシデントが発覚し、調査するというケースを想定し、これらのログについてはなるべく長期間保管しておくことが望ましい。また、これらのログの消失や改ざんを防ぐためにも、ログについても定期的にバックアップを取得することが推奨される。

また、不正利用と思われる操作を早期に発見するために、上記ログを元に、利用者本人に対するログインや重要操作（送金や決済、メールアドレス変更、パスワード変更等）の際のメール通知や、画面へのログイン・重要操作履歴の表示等の対策も推奨される。

サービス④-4：インシデント発生時のリスク軽減策を検討する

セキュリティインシデントが発生した際に、金銭の不正な引出しや事故等、サービス利用者に対する補償が必要となるケースに備える必要がある。そのため、セキュリティインシデントが発生した際の推進主体とサービス提供者等、ステークホルダ間における責任分界点を明示する等し、マルチステークホルダにおいてセキュリティインシデント対応体制

が構築されていることを確認する。その中で、保険加入等のリスク軽減策の対応状況についても確認、整理しておくことが望ましい。

3.1.3.都市 OS

「都市 OS」は、スマートシティのシステム全体のコアと位置づけられる部分であり、「アセット」から収集したデータを分類し、「サービス」や他の都市 OS 等へ提供する機能を果たすプラットフォームに該当する。

都市 OS は一般的にクラウド基盤の活用が想定されるため、プラットフォーム単体のセキュリティという観点から、外部からの攻撃を防ぐセキュリティ対策やセキュリティインシデントの発生を未然防止するためのセキュリティ対策など、サービスと同様のセキュリティ対策の実施が多く求められる。一方、クラウドサービスを利用することで新たに検討するべきクラウド特有の考慮事項があるため、都市 OS ベンダは十分に理解したうえで都市 OS を構築し、運用することが求められる。なお、都市 OS ではその機能としてサービス利用者に対してウェブアプリケーション等を提供することがあるが、その対策は「3.1.2. サービス」を参照されたい。

都市 OS に保有または都市 OS を介して扱われるスマートシティにおけるデータには、2.2.3 にあるようにデータ種別としてオープンデータ、限定公開データ、クローズドデータ等が想定され、個人情報に加え個人との関係性が見出されるパーソナルデータも含まれる。ガバナンス①－３に基づきこれらのデータの性質を踏まえデータ取扱い基準が策定される必要があり、都市 OS はこのデータ取扱い基準に応じたセキュリティ対策を実現するための措置を講じることが推奨される。

なお、都市 OS の機能や構成要素については、スマートシティリファレンスアーキテクチャホワイトペーパーを参照されたい。

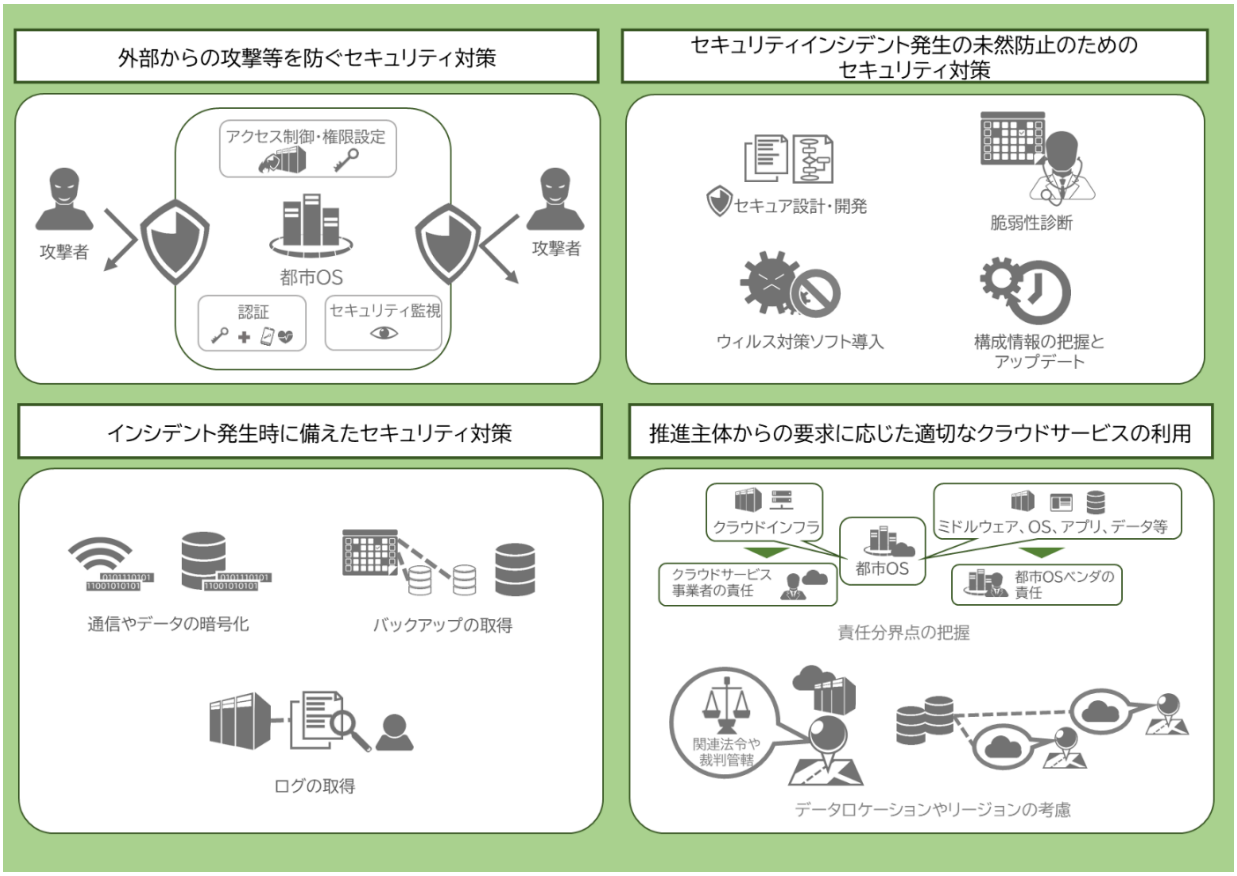


図３－３　都市 OS におけるセキュリティ対策のイメージ

① 外部からの攻撃、侵入等を防ぐセキュリティ対策

外部からの攻撃、侵入等を防ぐためには、企画・設計・開発段階から、様々なセキュリティ対策を実施し、運用していく必要がある。都市 OS においては、外部からの攻撃等への対策として、基本的に以下のセキュリティ対策を実施することが望ましい。

都市 OS①-1：都市 OS へのアクセス制御を実装、運用する
都市 OS①-2：適切な権限設定を実施し、管理する
都市 OS①-3：認証機能を実装する
都市 OS①-4：セキュリティ監視を実施する

都市 OS①-1：都市 OS へのアクセス制御を実装、運用する

外部攻撃からの対策として基本となるのがアクセス制御である。都市 OS を構成するサーバ等が配置されているセグメントに外部から通信する場合は、ファイアウォールを実装する等し、適切なアクセス制御を実装する必要がある。例えば、IP アドレス等で通信元・通信先を制限する、プロトコルやポート番号を制限する等で、サービス提供に必要な通信以外を遮断することによって、攻撃者による都市 OS への不正なアクセスなどを防ぐことがで

きる。なお、外部からの通信に限らず、システム内の他セグメントからの通信や同一セグメント内の通信においても適切なアクセス制御の実装は必要である点に注意する。

都市 OS①-2：適切な権限設定を実施し、管理する

システムや機器、データなどの情報資産へのアクセスを、必要な人や役割などに限定するために権限を設定し、管理することも基本的なセキュリティ対策の一つとなる。この権限設定・管理は外部からの攻撃への対策となるだけでなく、内部不正によるセキュリティ対策としても有効である。

権限設定・管理において特に重要となるのが管理者権限である。これを攻撃者に悪用されるとシステムの構成変更やログの改ざん、データの閲覧などができるようになってしまうことから、管理者権限の割当は最小限にするとともに、厳重に管理する必要がある。

権限管理では、システムや機器、データなどの情報資産に対してどのようなアカウントが存在し、どういった権限が割り当てられているかを管理することが重要となる。管理の方法としては、例えばアカウントや役割、権限などを整理した一覧表を作成した後、定期的に棚卸しを実施し、長期間利用されていないアカウントがないか、部署異動や退職した人の権限が残されていないか等を確認することも重要となる。

都市 OS①-3：認証機能を実装する

権限設定、管理とセットで必要となるのが、アクセスしようとしている人が適切なアクセス権限を割り当てられた本人であるかを確認するための認証機能の実装である。都市 OS の運用者が、対象システムにアクセスする際は、パスワードなどの知識情報を入力することによって本人確認を行うことが基本的な認証の例となる。その他の認証の種類としては、所持情報（IC カード、クライアント証明書、SMS 認証）、生体情報（静脈認証や虹彩認証）等があるが、不正アクセスやなりすましへの対策として、より高いレベルのセキュリティを実現するためには、これらの認証方法から異なる複数の要素を組み合わせた多要素認証を採用することが望ましい。なお、どのような認証を採用するかについては、認証を実装するシステムやサービス等の特性や重要度、アクセス元の環境に応じて適切に決定する必要がある事に留意する。また、上述の対策のほか、接続する相手のシステム・サービスのなりすましへの対策として、接続するシステム・サービス相互で暗号鍵・電子証明書等を所持し、照会することでアクセスを許可する公開鍵暗号基盤（PKI）による認証が有効となる。

都市 OS①-4：セキュリティ監視を実施する

ネットワークにおけるセキュリティ監視としては、インターネットとシステムの境界に IDS（不正侵入検知システム）や IPS（不正侵入防止システム）を設置し、それを監視することによって、不正なコマンドが含まれた通信等を検知、遮断することが可能となる。

また、その他のセキュリティ対策として、分散型サービス拒否攻撃（DDoS 攻撃）対策や保存されている設定ファイルやシステムデータの改ざん検知等を必要に応じて組み合わせることで、より高度なセキュリティ監視を実現することが可能となる。

② セキュリティインシデント発生の未然防止のためのセキュリティ対策

都市 OS においては、外部からの攻撃等を防止するセキュリティ対策のほか、インシデントに至ることを未然に防止するセキュリティ対策として、都市 OS の企画・設計・開発工程から運用工程において、脆弱性が入り込まないようにするための対策や運用管理端末へのセキュリティ対策がある。

都市 OS②-1：都市 OS の企画・設計・開発工程における脆弱性を適切に管理する
都市 OS②-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する
都市 OS②-3：運用管理端末へのセキュリティ対策を実施する

都市 OS②-1：都市 OS の企画・設計・開発工程における脆弱性を適切に管理する

都市 OS 基盤を企画・設計・開発する上では、その段階からセキュア設計やセキュアコーディングを実施することによって脆弱性が入り込まないように配慮しつつ、サービスイン前に適切にセキュリティテストや脆弱性診断を実施することで、既知の脆弱性への対処が可能となる。また、クラウド基盤のセキュリティ設計の不備にも注意を払うことに留意する。なお、システム開発の早い段階からセキュリティを考慮した設計を行うことで、サービスイン前におけるセキュリティテストや脆弱性診断等での発見事項が少なくなり、結果として工程に手戻りが発生しなくなるため、リソースや開発コストを効率的に使用することができる。

都市 OS②-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する

脆弱性とは、開発工程において対策を実施すれば完全なセキュリティが担保できるわけではなく、日々のサイバー攻撃の進化やソフトウェア等の更新に伴って新しい脆弱性が発見される。そのため、開発工程における脆弱性の適切な管理のほかに、運用フェーズにおいても新たな脆弱性がないかを把握し、それに対応する必要がある。

脆弱性を把握する手段の一つとして挙げられるのが定期的な脆弱性診断の実施である。基本的にはシステムの設定変更や新規機能の追加などがなければ、既知の脆弱性については一度確認すれば問題ないが、システムを運用する過程における設定変更などで気がつかない内に脆弱性が生じている可能性があるため、定期的な脆弱性診断を実施することを推奨する。

また、新規の脆弱性の中には緊急性の高い脆弱性が含まれることもあり、それを放置すると重大なセキュリティインシデントに至ってしまうケースもあり得る。そこで、自身の

システムで利用しているOSやミドルウェア、ソフトウェア等の構成管理情報を常に最新化して管理しつつ、新規の脆弱性情報を収集し、自身のシステムにおいて対処が必要かどうかを適宜判断し、適切なタイミングでバージョンアップやセキュリティパッチ適用などの対応を実施することが望ましい。

都市OS②-3：運用管理端末へのセキュリティ対策を実施する

運用管理端末はサービス提供中の環境へ直接アクセス可能であることから、踏み台として悪用されるリスクがある。そのため、運用管理端末へのアクセス制御の実施や認証の導入はもちろん、ウイルス対策ソフトの導入や未知の不正プログラムへの対策、OS等の脆弱性への対応、運用管理端末でのシステム動作ログ等の取得といった、基本的なセキュリティ対策の実施が必要となる。

また、運用管理端末の設置場所についても、通常の執務室等、業務に関係のない者が日常的に入り込める場所ではなく、セキュリティルーム等、物理的にアクセスが制限された場所に配置することが望ましい。

③ インシデント発生時に備えたセキュリティ対策

①～②で示した対策を実施することでセキュリティインシデントが発生しないようにすることが当然望ましいが、実際はセキュリティインシデントの発生をゼロにすることは困難である。そこで、セキュリティインシデントが発生してもその被害が最小化できるよう、外部との通信やデータの暗号化、バックアップの取得、ログの取得などの対応も合わせて実施する必要がある。

都市OS③-1：外部との通信やデータの暗号化を実施する
都市OS③-2：定期的にバックアップを取得する
都市OS③-3：証跡確保のためのログを取得する

都市OS③-1：外部との通信やデータの暗号化を実施する

外部との通信の内容が盗聴されたり、システム内で保有しているデータが流出したとしても、適切な強度の暗号アルゴリズムを使って通信やデータの暗号化をしていた場合は、解読が困難となり、被害の発生を抑止することができる。暗号化強度については、「CRYPTREC暗号リスト(電子政府推奨暗号リスト)」等で定義された十分な強度の暗号アルゴリズムを採用することが望ましい。なお、パスワード情報などの復号が不要なデータについては、そのデータが容易に推測できないよう、ハッシュ関数を利用することが望ましい。

なお、通信の暗号化に関しては盗聴を防ぐという観点で、外部からの攻撃等を防ぐセキュリティ対策としても有効である。

都市 0S③-2：定期的にバックアップを取得する

システムの構成情報や、重要なデータについては、その可用性や事業継続などを考慮して、定期的にバックアップを取得することが望ましい。バックアップデータは定期的に物理的な媒体に書き出したり、災害への影響を考慮して別のロケーション（地理的に別の場所にあるデータセンタ等）に保管する等して確実に維持できるようにすることが推奨される。

都市 0S③-3：証跡確保のためのログを取得する

ログはセキュリティインシデントが発生した際に、原因の究明や対策の検討を行う上で必ず必要な情報となる。取得すべきログとしては、サーバ等に対するアクセスログや操作ログ、IDS や IPS 等における検知ログ、ファイアウォールにおける通信ログ等、多岐にわたるが、実際にインシデントが発生した場合は、これらのログを相関的に分析することで、攻撃内容や被害状況などを特定することが可能となる。なお、ログを相関的に分析する際は、正確に攻撃の痕跡が追えるよう、それぞれの機器において時刻同期も実施すると良い。また、システム構成が複雑化することにより複数のログを管理・監視する必要がある場合は、ログ分析基盤を導入し、ログを一元管理することで相関的な分析が可能となる。

その他、事後的にインシデントが発覚し、調査するというケースを想定し、これらのログについてはなるべく長期間保管しておくことが望ましい。また、これらのログの消失や改ざんを防ぐためにも、ログについても定期的にバックアップを取得することが推奨される。

④　推進主体からの要求に応じた適切なクラウドサービスの利用

クラウドサービスはその拡張性や導入の容易さから、うまく活用すると非常に便利だが、クラウドサービス事業者から提供される IaaS/PaaS などの基盤を利用する場合は、利用者である都市 0S ベンダとクラウドサービス事業者間の責任分界点を的確に把握し、セキュリティに関する考慮漏れがないようにする必要がある。また、クラウドサービスによってはサーバが海外のデータセンタに位置することもあるため、推進主体からのデータロケーションやサービスの可用性に関する要求（SLA）を実現できるようなクラウドサービス選定やリージョンの選択などが求められる。

都市 OS④-1：クラウドサービスの利用者と提供事業者間の責任分界点を把握する
都市 OS④-2：データロケーションに関する推進主体からの要求事項に対応する
都市 OS④-3：複数リージョン選択等により、可用性を担保する

都市 0S④－1：クラウドサービスの利用者と提供事業者間の責任分界点を把握する

IaaS/PaaS などのクラウド基盤を利用するにあたっては、クラウドサービス利用における契約や規約の中で示されている責任分界点について正確に把握し、都市 OS ベンダとして実施すべきセキュリティ対策を理解し、実施する必要がある。例えば、IaaS を利用する場合、ハードウェアやネットワークなどへのセキュリティ対策はクラウドサービス事業者の責任範囲となるが、そのインフラ上に構築される OS、ミドルウェア、アプリケーション、データなどへのセキュリティ対策は利用者側（都市 OS ベンダ側）の責任範囲となる。

都市 OS④－2：データロケーションに関する推進主体からの要求事項に対応する

クラウドの設置場所（リージョン）により、国外の法令に基づいてデータの取扱いが求められるなど、クラウド上に保存しているデータ（特に機密データ）の取扱いに関連する法令が国内とは異なる可能性がある。そのため、都市 OS 上で取り扱うデータの種類を理解した上で、クラウドの設置場所及び設置環境において適用される関連法令や裁判管轄等を確認し、推進主体からの要求事項に対応できているかを確認することが重要である。

都市 OS④－3：複数リージョン選択等により、可用性を担保する

クラウドを利用する利点の一つとして、柔軟に冗長性を組むことができ、可用性を担保できることが挙げられる。例えば「都市 OS③-2」でも述べたバックアップを取得していれば、クラウド上で容易に環境の復元が可能となり、システムに致命的な障害が発生した場合でも速やかな復旧が可能となる。一つのリージョンしか選択していなかった場合、そのリージョンで障害が発生してしまうことで都市 OS の停止に至る可能性があるため、より高い可用性を実現するためには複数のリージョンを選択する必要がある。また、災害復旧（DR）の観点からも、地理的に分離された拠点にシステムやデータの冗長化やバックアップをすることが望ましい。

3.1.4.アセット

「アセット」はサイバー領域がフィジカル領域と接点を持つ領域であり、地域課題解決のために必要なデータを生成し、「都市 OS」へ送信するカテゴリである。ここでは、IoT 機器などのデバイスや、「都市 OS」にデータを流通させるためのネットワーク、中継機器等のセキュリティについて考慮する必要がある。これらのデバイスは大量に設置されることが想定されるため、効率的に監視・管理し、適切なセキュリティ対策を実施できるようにする必要があ

る。また、必要性に応じ、デバイスへのセキュリティ機能を予め実装できるよう、設計や機器選定の段階からセキュリティについて考慮することが望ましい。

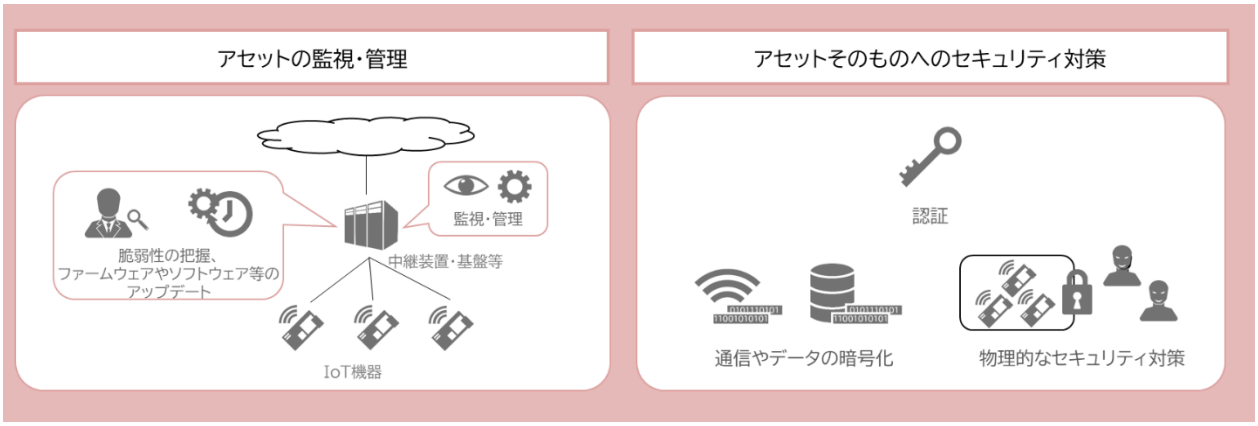


図３－４　アセットにおけるセキュリティ対策のイメージ

① アセットの監視・管理

アセットで収集されるデータは様々なサービスで活用されることから、正確なデータを途切れることなく収集することがアセットでは求められる。また、ソフトウェア等と同じように、アセットにおいても日常的に脆弱性が発見され、それを悪用された攻撃が発生する可能性もある。そのため、アセットの監視・管理をしつつ、新規の脆弱性への対応などを継続的に実施することがアセットでは求められる。

アセット①-1：アセットの監視・管理を実施する アセット①-2：新規の脆弱性情報を把握し、ファームウェア、ソフトウェア等のバージョンアップを適切に実施する

アセット①－1：アセットの監視・管理を実施する

まずは正しいアセットが接続されているかを確認することが必要となる。確認できないアセットはスマートシティのネットワークへのアクセスを拒否するなど、切り離す必要がある。確認は、ネットワークアドレス、ハードウェア識別子、アセット名、所有者などの情報を用いる方法や、クライアント証明書などセキュリティ技術を用いて不正なアセットなどのなりすましを検知する方法など、アセットの重要度に応じて確認方法を選択することが望ましい。

その後、アセットで異常が発生していることが検知できるように、アセットの死活監視を実施することが必要となる。また、アセットのバージョン情報などの基本的な情報は管理しておくことが求められる。アセットは将来的に大量のデバイスが接続されることから、手作業での管理ではなく機械的な管理をする等、効率的に管理するための機能を実装

することが望ましい。さらに不正なアセットの接続や不正なデータの監視を行うことが推奨される。

アセット①-2：新規の脆弱性情報を把握し、ファームウェア、ソフトウェア等のバージョンアップを適切に実施する

アセットにおいても、OS やソフトウェア等と同様、日常的に脆弱性が発見されている。新規の脆弱性が発見された場合は、その脆弱性がスマートシティに与える影響について評価した上で、適切なタイミングでバージョンアップの対応を行うことが重要となる。IoT 機器に直ちに影響を及ぼすような脆弱性が発見された場合には、迅速にこれらの対応を実施する必要があることから、リモートで一斉に IoT 機器をバージョンアップする機能を実装するという方法もある。その際に、管理アクセスの経路の制限や認証強度の強化を十分に考慮することが必要である。

② アセットそのものへのセキュリティ対策

アセットへのセキュリティとしては、①で述べた全体的な管理・監視に関する内容以外にも、アセットそのもの、特に IoT 機器等のデバイスへのセキュリティ対策が非常に重要となる。アセットそのものへのセキュリティ対策としては、通信やデータの暗号化、認証機能の実装のほか、物理的なセキュリティ対策も考慮が必要となる。

アセット②-1：外部との通信や、保有するデータを暗号化する
アセット②-2：認証機能を実装する
アセット②-3：物理的なセキュリティ対策を実施する

アセット②-1：外部との通信や、保有するデータを暗号化する

アセットから都市 OS へのデータ連携等、インターネットを経由して外部との通信が発生する場合は、通信の暗号化を実施することで、盗聴を防止することができる。また、アセットで保有するデータに、例えばヘルスケア情報等の重要な情報が含まれる場合は、それらのデータを暗号化することも重要である。暗号化強度については、「CRYPTREC 暗号リスト(電子政府推奨暗号リスト)」等で定義された十分な強度の暗号アルゴリズムを採用することが望ましい。さらに、アセット内でデータを保有する際には、機器の耐タンパ性を確保する等によって、不正にデータが取得できないように対策する必要がある。

なお、機能や性能の制限によって IoT 機器で十分なセキュリティ機能が実装できない場合は、IoT 機器の通信を束ねる中継装置（セキュアゲートウェイ）において対策するという方法もある。

アセット②-2：認証機能を実装する

アセットの設定を悪意のある第三者に変更されないためにも、アセットにアクセスする際は ID／パスワード等による認証機能を実装することが重要である。そのためにはデバイスの設計段階からセキュリティの考慮が必要となる場合がある。そして、パスワードは工場出荷状態で他のアセットと同一とならないように考慮する必要があるし、そのパスワードも容易に推測ができないように、十分な桁数や英数字や記号、大文字小文字などを混ぜたものにする必要がある。また、監視カメラ等のプライバシーが関わるアセットの場合には、十分な認証強化が推奨される。さらに IoT 等に付帯する Web サービスの脆弱性が狙われることもあり、認証強度に注意が必要であることも留意されたい。

そして、サービス利用者側でデバイスを管理する場合は、サービス利用者に適切なパスワードの設定や管理などの注意喚起をすることも必要となる。

アセット②-3：物理的なセキュリティ対策を実施する

センサーなどのスマートシティのデータ収集のためのデバイスは、公共空間などに設置されることが多いことから、破壊や盗難などの物理的なリスクのための対策として、物理的なセキュリティ対策を可能な限り実施することが求められる。例えば、関係者以外が立ち入ることができないよう物理的なアクセスが制限された領域にデバイスを設置する等がある。

また、サービスによってはモビリティなどの物理的な制御を行うデバイスが設置されることもある。その場合は、何らかの誤動作が起きたとしても人命の影響が発生しないように、安全側（セーフ側）に倒れる、いわゆるフェイルセーフを考慮して設計する必要がある。

その他の物理的なセキュリティとして、デバイスの廃棄に際してもセキュリティを考慮する必要がある。具体的には、廃棄した機器から情報が盗み出されないようにデバイスを廃棄する際は記録媒体部分を物理的に破壊するなど、適切な方法でデータの読み出しができないように処理する必要がある。

3.2. 横断的なセキュリティ対策

Society5.0 の先行的実現の場としてのスマートシティは、将来的に高度にネットワーク化されたサプライチェーンに様々な主体が参加するような状況が想定される。その場合、一主体が取り組むセキュリティ対策だけではスマートシティ全体のセキュリティを確保していくことに限界がある。これまでに挙げてきた各主体による能動的なセキュリティ対策の実施のほか、適切なサプライチェーン管理による信頼性の確保やインシデントの発生に備えた体制整備、その対応における連携など、より幅広い視点で対策を検討・実施することが望ましい。また、スマートシティでは新たな価値を創出するためにデータ連携も積極的に進めて行く必要があり、データ連携時のセキュリティも求められていくこととなる 。

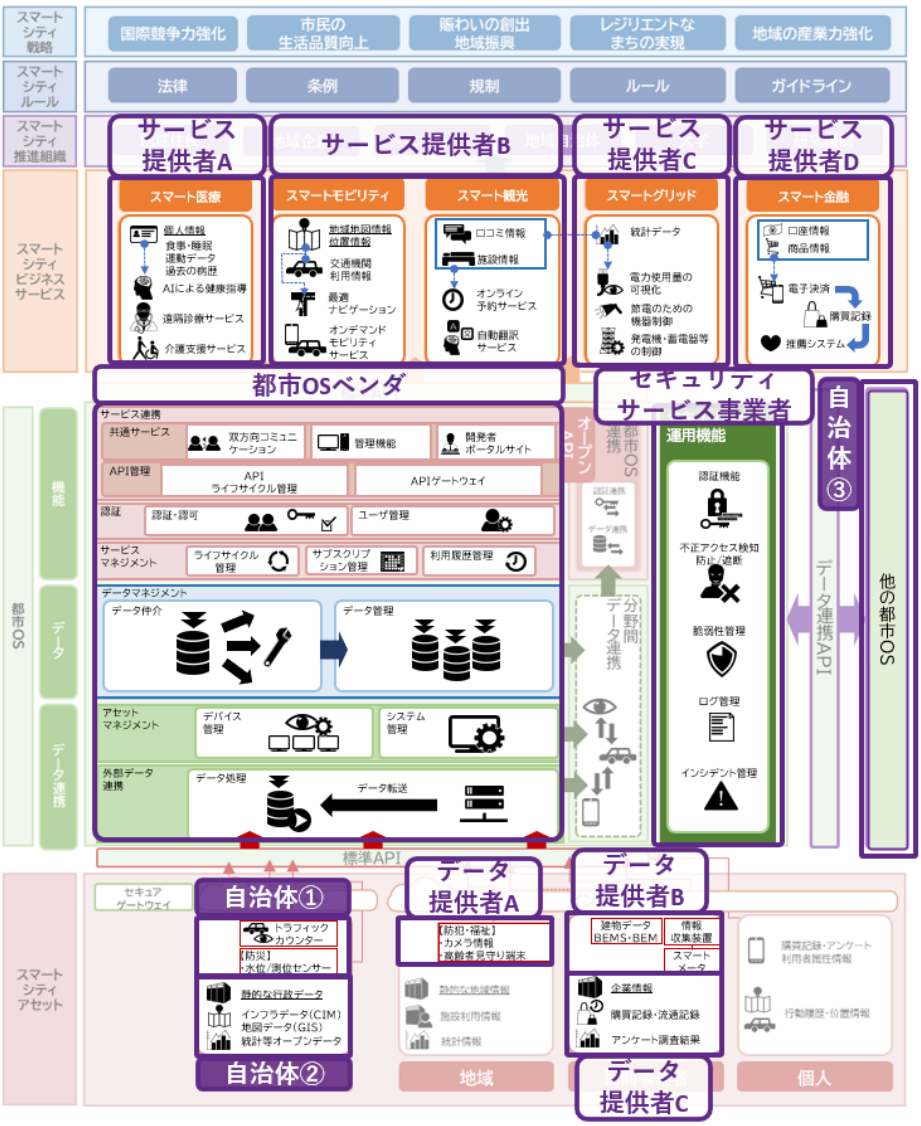


図３－５　マルチステークホルダが関与するスマートシティのイメージ

3.2.1.サプライチェーン管理

マルチステークホルダが複雑に関与するスマートシティで発生する問題点の一つとして、サプライチェーンの拡大によるサイバー攻撃の起点の拡大や、発生する被害の影響範囲が広がることが挙げられる。これらの対策として、推進主体においてスマートシティの委託先や再委託先などのサプライチェーン全体を管理・把握する必要がある。また、委託先等のセキュリティ管理体制を評価することにより、サプライチェーンにおいて一定レベル以上のセキュリティが担保できていることを確認することができる。サプライチェーン先に脆弱性が存在することで、そこが侵入口となり、スマートシティ全体へ影響を及ぼすことも考えられるため、サプライチェーン全体の脆弱性情報を把握できるようにしておくこともサプライチェーン・リスクへの対策となる。なお、セキュリティインシデント発生時に利用者やサービス提供者の立場から見ると障害の切り分けなどは難しいため、スマートシティの推進主体がスマートシティ全体のセキュリティに対する一義的な責任主体となり、サービス提供者や機器ベンダ等の関係事業者との間の共通認識醸成と役割分担整理を実行することを推奨する。

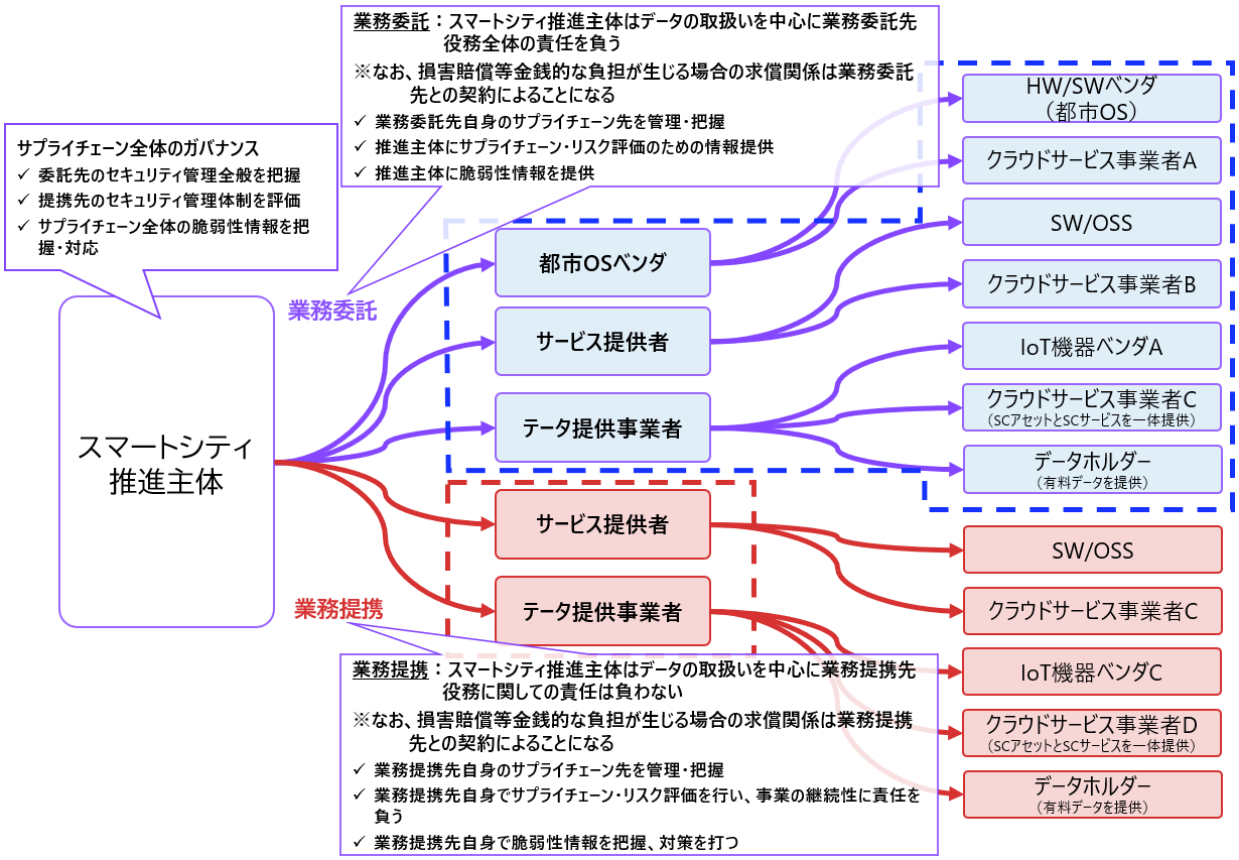


図３－６　サプライチェーンにおける責任分界点

- **スマートシティ推進主体はステークホルダ毎の責任分界点を明確にする。**
  ✓業務委託の場合、スマートシティ推進主体はデータの取扱いを中心に業務委託先役務全体の責任を負う。
  ✓業務提携の場合、スマートシティ推進主体はデータの取扱いを中心に業務提携先役務に関しての責任は負わない。
  ✓スマートシティ全体のガバナンスは、スマートシティ推進主体が責任を負う。
  ※なお、損害賠償等金銭的な負担が生じる場合の求償関係は業務委託先・提携先との契約によることになる。

- サプライチェーン①：サプライチェーン全体のリスクを管理・把握する
- サプライチェーン②：委託先／提携先のセキュリティ管理体制を評価する
- サプライチェーン③：サプライチェーン全体の脆弱性情報を適切に把握し、対応する
- サプライチェーン④：推進主体はステークホルダ毎の責任分界点を明確にする

サプライチェーン①：サプライチェーン全体のリスクを管理・把握する

スマートシティにおけるマルチステークホルダは、都市 OS ベンダやサービス提供者だけでなく、データ提供事業者や IoT 機器ベンダ等、非常に多岐にわたる。また、都市 OS ベンダやサービス提供者においても事業の一部を委託（再委託）しているケースは十分に想定される。そこで、推進主体としては、まずはスマートシティに関わっているマルチステークホルダ全体を把握することが重要となる。

ただし、推進主体が委託先や再委託先などで利用される全てのオープンソースソフトウェア（OSS）を含むソフトウェアやハードウェアを把握し、管理するのは困難であることから、推進主体としては、委託先に対して、委託事業におけるサプライチェーン・リスクへの対応のための管理体制の整備を求めるといった現実的な対策を中心に検討する必要がある。

サプライチェーン・リスクへの対策を検討する上では、「ガバナンス」や「サービス」のカテゴリにも記載があるように、サプライチェーン・リスクのアセスメントを実施してシステムのライフサイクルそれぞれの工程で求められる対策を考え、実施していく必要がある。具体的には、調達するシステムにおける機能や取り扱う情報の特性に応じた脅威を踏まえてサプライチェーン・リスクを特定し、そのリスクへの対策を検討していく、という流れとなる。

なお、本節で記載した対策は推進主体の視点で記載しているが、推進主体から見てサプライチェーン先である都市 OS ベンダやサービス提供者などの委託先等においては、推進主体がサプライチェーンを管理・把握できるようにするための適切な情報提供が求められる。また、委託先等においてもそのサプライチェーン先（再委託先や利用している製品・OSS を含むソフトウェア等の情報）の適切な管理・把握が求められることとなることに留意する。

サプライチェーン②：委託先／提携先のセキュリティ管理体制を評価する

スマートシティの基盤である都市 OS やサービス利用者に提供するサービス等を構築し運用する上では複数の事業者と委託契約を結び、委託事業として進めて行くことが想定される。ここで、委託先の情報セキュリティ管理が不適切だった場合、委託先による情報漏えい等が懸念される。そのため、委託先の選定時や契約期間中などにおいて委託先のセキュ

リティ管理・対応の体制を評価することが一つのサプライチェーン・リスクへの対策となる。

委託先のセキュリティ体制の評価にあたっては、委託先に実施を求めるセキュリティ管理体制について記載したセキュリティチェックシートに委託先に回答してもらい、その回答をもって委託先のセキュリティを評価する方法のほか、ISO/IEC 27001 等のセキュリティに関する基準に適合していることの第三者認証の取得状況による評価などが考えられる。また、これらを組み合わせて実施することで、より委託先のセキュリティ体制を正確に評価することが可能となる。なお、契約期間中においても定期的にセキュリティ体制について確認・評価し、不十分な点があれば改善を求めることが望ましい。

サプライチェーン③：サプライチェーン全体の脆弱性情報を適切に把握し、対応する

スマートシティでは、そのサービスを提供するためのサーバやネットワーク機器などのハードウェアや利用されているソフトウェア、ミドルウェア、データ収集・サービス提供のための IoT 機器などのデバイスなど、非常に多岐にわたるソフトウェア、ハードウェアの上で成り立っている。スマートシティを運用する中では、これらのソフトウェアやハードウェアの脆弱性が発見されることは容易に想定されるため、推進主体においてはその脆弱性情報を適切に把握[17]し、対応できるようにしておく必要がある。

まず重要になるのが、継続的な脆弱性への対応が期待できるソフトウェアやハードウェア等を選定することである。例えば調達する IoT 機器のメーカにおける脆弱性への対応体制が不十分だった場合は、重大な脆弱性が公開されてから修正プログラムが作成されるまで、機器を停止せざるを得ない事態に陥る可能性がある。また、サポートが 1 年以内に終了することが分かっているような機器を調達した場合、1 年後以降で重大な脆弱性が発見された時に脆弱性が残留することになってしまい、当該製品の利用を停止せざるを得ない事態となる。そのため、脆弱性が発見された場合に直ちにセキュリティパッチなどをリリースできるだけのサポート体制が整っており、かつ継続的なサポートが保障されている製品やソフトウェア等を選定することが望ましい。

加えて、サプライチェーンにおける関係者間の契約や、調達時の仕様に含める内容として、これらの脆弱性情報を委託元に適切に提供し、対応するといった記載を盛り込むことが望ましい。都市 OS ベンダやサービス提供者等の委託先・提携先側としては、自身が構築・運用している基盤やサービスなどを構成するソフトウェアやハードウェアなどを適切に管理するとともに、公開情報や脆弱性情報配信サービスなどから脆弱性情報を収集・把握し、それらの脆弱性がスマートシティサービスに与える影響などを判断した上で、委託元と連携して迅速に脆弱性に対処することが求められる。

17 ソフトウェアやハードウェア等の構成管理にあたっては、以下のドキュメントが参考となる。
- 内閣サイバーセキュリティセンター（NISC）「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」
- 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」

サプライチェーン④：推進主体はステークホルダ毎の責任分界点を明確にする

スマートシティ推進主体とステークホルダ間の契約形態によって、責任分界点が異なる。業務委託の場合は、推進主体が委託先の提供するサービス等に対して全責任を負う。一方、業務提携の場合は、業務提携先であるステークホルダが業務提携に基づき提供するスマートシティサービスの責任を負う。ただし、スマートシティ全体のガバナンスは、スマートシティ推進主体が責任を負う。

また、推進主体・業務委託先・業務提携先の責任分界点を整理したうえで、マルチステークホルダすべてがスマートシティ全体の責任分界点を理解するように努めることが重要である。

3.2.2.インシデント対応時の連携

一つのスマートシティを見たときに、そのスマートシティ内のとあるコンポーネントでセキュリティインシデントが発生した場合、様々なマルチステークホルダが関与するスマートシティにおいては、その影響はスマートシティ全体に及ぶ。そこでマルチステークホルダ間連携が不十分だったり、お互いのシステムの責任分界点が共通認識となっていなかったりした場合、インシデントへの対応が遅れて被害が拡大する恐れがある。そこで、スマートシティにおけるレジリエンス（強靭さ）を確保するためには、事前に責任範囲を明確にしたセキュリティインシデント対応体制を構築し、各主体においてインシデント発生時の連絡窓口を整備し、連絡先をマルチステークホルダ間で相互共有することが重要となる。同時に各主体が所有するインシデントの解析・復旧に必要な情報の洗い出しと相互連携フローについても、ステークホルダ間で整理・規定しておくことが望ましい。そのうえで、 それぞれのインシデント対応に従事する者が円滑に対応できるようにスマートシティ全体及び各マルチステークホルダにおけるインシデント対応手順を整備することが重要となる。また、これらの対応の実効性を確認する、または対応習熟のための定期的なセキュリティインシデント対応訓練・演習も必要となる。

一方、インシデントが発生した際には、利用者（市民）へのフォローアップや適切な情報発信も重要な取り組みであり、例えば問い合わせなどを受け付ける窓口機能を担う主体・連絡先等を明確にし、日ごろから利用者が確認できるよう情報を公開しておくことなどが望ましい。

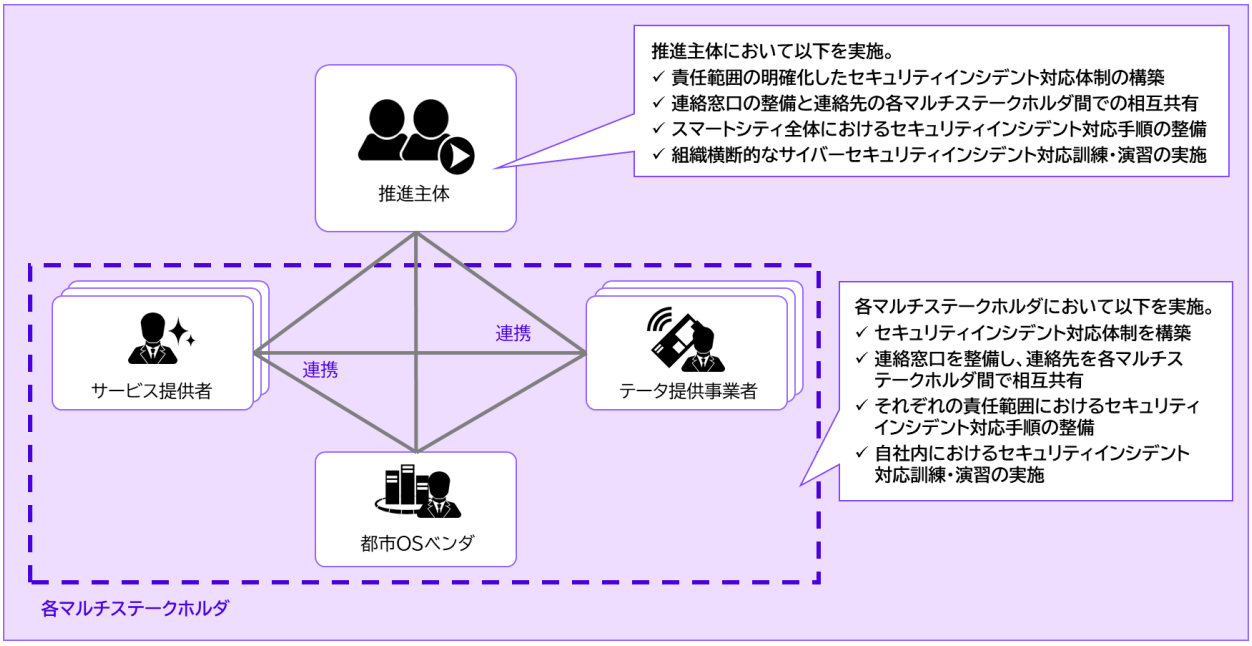


図３－７　インシデント対応時の連携におけるセキュリティ対策のイメージ

インシデント対応①：責任範囲を明確にしたセキュリティインシデント対応体制を構築する
インシデント対応②：連絡窓口を整備し、マルチステークホルダ間で相互に共有する
インシデント対応③：スマートシティ全体及び各マルチステークホルダにおけるセキュリティインシデント対応手順を整備する
インシデント対応④：定期的にセキュリティインシデント対応訓練・演習を実施する
インシデント対応⑤：新たな脅威やインシデント事例などの情報を収集・分析する

インシデント対応①：責任範囲を明確にしたセキュリティインシデント対応体制を構築する

セキュリティインシデントが発生した際に、即座にインシデント対応を実施できるよう、推進主体をはじめ、マルチステークホルダにおけるセキュリティインシデント対応のための体制を構築することは必要不可欠である。推進主体においてはデータの流通等を踏まえたスマートシティに関与するステークホルダやシステムなどの全体像を把握した上で、委託契約などで明確化した責任分界を元に、セキュリティインシデントが発生した際の対応に関する責任分界点を明示する等し、全てのマルチステークホルダにおいてセキュリティインシデント対応体制が構築されていることを確認する必要がある。

インシデント対応②：連絡窓口を整備し、マルチステークホルダ間で相互に共有する

実際にスマートシティにおいてセキュリティインシデントが発生した際は、マルチステークホルダで連携して対処する必要がある。即座にインシデント対応連携が開始できるように、各マルチステークホルダの連絡体制や緊急連絡先を予め整備し、マルチステークホルダで相互に共有することが重要となる。また、それぞれのマルチステークホルダ内においてもインシデント対応に関する部門や経営者／CISO 等への連絡が発生する可能性があることから、その連絡先も事前に整備しておく必要がある。さらに、インシデントが発生した場合に備え、主管官庁や警察などの公的機関、JPCERT/CC など、対外的に連絡をとる可能性がある連絡先についても予め把握しておくことが望ましい。

インシデント対応③：スマートシティ全体及び各マルチステークホルダにおけるインシデント対応手順を整備する

セキュリティインシデントの発生に備え、予めどのような判断の下で誰がどのようなオペレーションを実施するのかを決めておき、また、連絡や報告のフォーマットなども準備し、インシデント対応手順としてまとめておくことで、有事の際に円滑にインシデント対応を行うことができる。特に重大なセキュリティインシデントにおいては経営者による意志決定が必要になるケースが想定されるため、セキュリティインシデントの内容や被害状況について速やかに把握し、整理して報告できるようにするための手順やフォーマットを整備しておくことを推奨する。

推進主体においては事前に整理している責任分界点に基づいて、マルチステークホルダ間の連携を含めたスマートシティ全体としての対応手順を整備すると同時に、各ステークホルダが所有するインシデント対応に資するログなどの情報を把握しておくことが求められる。そして、これらの手順・情報に沿う形で、各ステークホルダが、自らの対応手順の整備や、解析・分析すべき情報、提供・共有すべき情報をあらかじめ整理しておくことが望ましい。

インシデント対応④：定期的なセキュリティインシデント対応訓練・演習を実施する

インシデント対応①～③で整備した体制や対応手順等をミスなく、円滑に実施できるようにするためにはセキュリティインシデント対応訓練を定期的に実施することが重要となる。この対応訓練では、自組織内における対処手順や復旧手順の浸透のほか、自組織内や組織外との各種連絡による連携対応の習熟などを図ることができる。また、今整備している対応手順が適切かどうか、といった対応手順の検証や課題を抽出するためのインシデント対応演習を実施することも有効となる。

なお、訓練・演習の種類としては、実機を用い、実践的な内容を含む「実機訓練」のほか、状況付与を元にどう判断、対応するかを検証するロールプレイングやシミュレーションなどの「机上演習」などがあり、その訓練・演習を行う目的に応じて適切なものを選択することが望ましい。例えば、簡単に連絡のフローが適切かを確認したいだけの場合は、

簡易的に机上で状況付与に応じた連絡対応のシミュレーションを行うなどで検証することが可能である。

これらの訓練や演習は、各マルチステークホルダの組織内において実施するだけでなく、スマートシティ全体として連携したインシデント対応が実施できることを確認・検証するために、インシデント対応の統制を行う推進主体が中心となり、マルチステークホルダが同時に参加する訓練・演習を実施することが望ましい。また、セキュリティ推進体制による定期的な内部（相互）監査等も有効である。

インシデント対応⑤：新たな脅威やインシデント事例などの情報を収集・分析する

スマートシティを構成する要素はインターネット技術を多く活用することから、インシデント対応体制関係者はスマートシティを含むインターネットに関連する新たな脅威、攻撃手法、脆弱性、およびセキュリティに関するベストプラクティスに関する情報等を収集し、インシデント対応体制内で共有・学習する。そのうえで、既存のインシデント対応手順や役割・責任分担、連携フロー、対応訓練・演習メニュー等の見直しを行うことでインシデント対応能力を高めスマートシティのレジリエンスを強化する。

情報の収集方法としては、公知情報の収集等に加え、有識者からのアドバイスや、他のスマートシティとの情報交換、外部団体活動への参加等も有効であり、日ごろからそういった情報に触れられるコミュニケーションパスを構築しておくことが望ましい。

3.2.3.データ連携時のセキュリティ

Society 5.0 を具現化するスマートシティでは、国、地方公共団体、民間などで散在するデータを連携させ、分野・組織を越えたデータ活用とサービス提供を可能とするため、データ分散方式[18]に代表されるデータ連携基盤の実装が想定される。

データ連携においては、機能や管理するデータ等を他のサービスやアプリケーションから呼び出して利用するための接続仕様である API におけるセキュリティの確保だけではなく、データ連携時のデータ連携元、連携先のセキュリティ態勢を評価するなどで信頼性を確保しつつ、データに対する適切なアクセス制御を付与するなど、データ連携する際の対策を検討・実施することが望ましい。

データ流通・連携を行う場合、セキュリティの観点から、都市 OS の有無にかかわらず、以下に示す 6 つの事項のうち該当する部分の点検を行う必要がある。

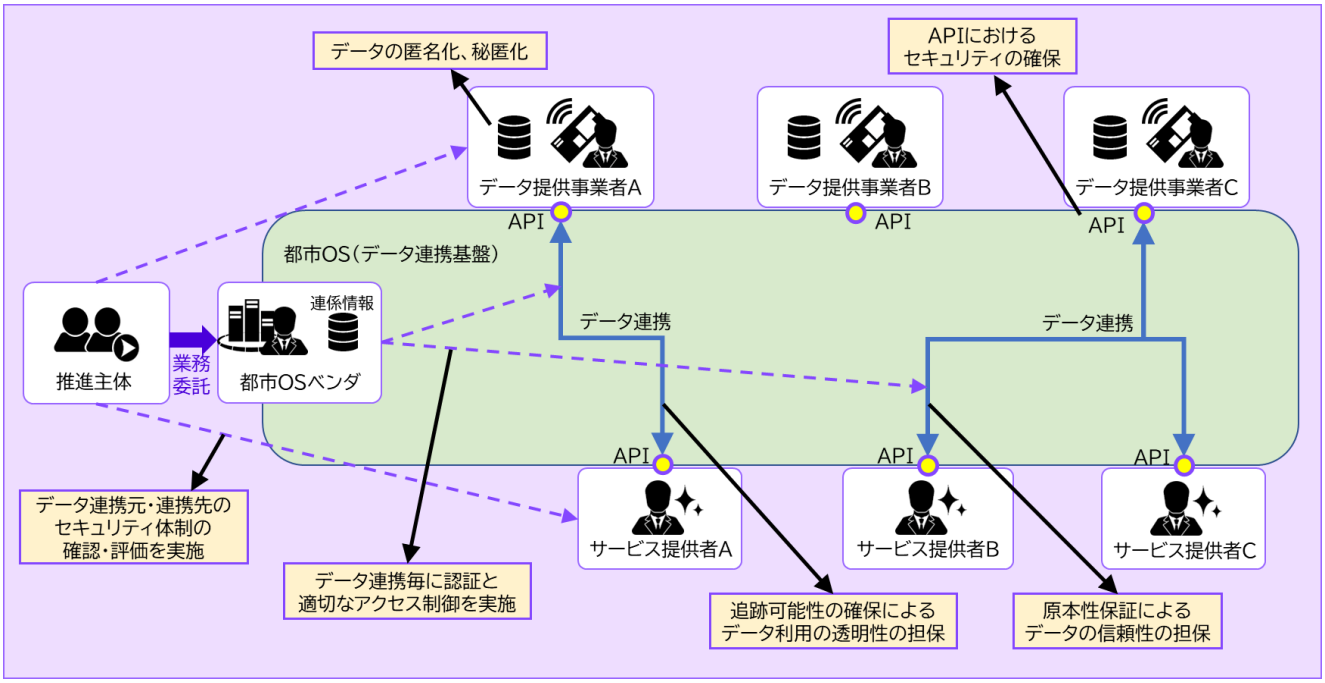


図３－８　データ連携時におけるセキュリティ対策のイメージ
（分野別データ連係基盤を用いた連携基盤利用型の場合）

18 都市 OS にデータを蓄積せず、都市 OS は分散されたデータの所在情報を管理し、利用者からデータアクセスがあった場合は、この所在情報を利用してデータの仲介を行う方式。

データ連携①：データ連携元・連携先のセキュリティ体制の確認・評価を実施する
データ連携②：データ提供事業者・サービス提供者等の認証・認可と適切なアクセス制御を実施する
データ連携③：データの追跡可能性の確保によるデータ利用の透明性を担保する
データ連携④：データの原本性保証によるデータの信頼性を担保する
データ連携⑤：必要性に応じたデータの匿名化・秘匿化を実施する
データ連携⑥：API におけるセキュリティ（機密性・完全性・可用性・真正性）を確保する

データ連携①：データ連携元・連携先のセキュリティ体制の確認・評価を実施する

スマートシティでは、データ連携元から連携先まで多様な主体が連続的に関わりを持ち、データ連携が行われるが、安全・安心にデータ連携を行う上では連携元・連携先による信頼の連鎖が重要となる。そこで、推進主体がデータ提供事業者等のデータ連携元、サービス提供者等のデータ連携先のセキュリティマネジメントを確認することによって、接続される機器、サービス等が自身の定めるセキュリティに関する要求事項を満たしているかを確認することができる。

連携元・連携先のセキュリティマネジメントの確認方法としては、「3.2.1. 適切なサプライチェーン管理」の②で記載したチェックシートや第三者認証の有無等によって、連携先のセキュリティ管理体制を評価することで、接続されるシステムや機器、サービス等の一定レベルの信頼性の担保を行うことが可能となる。チェックシートで確認すべき項目については、本章で記載している対策全般を目安にスマートシティのデータ連携において必要な対策を選定し、連携先に要求すると良い。

データ連携②：データ提供事業者・サービス提供者等の認証・認可と適切なアクセス制御を実施する

データ提供事業者とサービス提供者の間でデータ連携を行う場合、双方の API を通じて連携を行うこととなるが、適切なデータ連携の要求元が適切なデータだけを取得することができるように、連携するデータの内容、個人情報の利用に関する同意内容などに沿った利用目的等に合わせ、データ提供事業者及びサービス提供者をデータ連携基盤を介して認証したうえで、適切なアクセス制御を行うことが重要となる。

データ提供事業者、サービス提供者の認証では、API キーや、アクセストークンを使用した OAuth 2.0、OpenID Connect1.0[19]による認証等、適切な認証手法を選択し、連携元、連携先を認証する必要がある。また、認証を行った後は、データの要求元（データの利用者）の情報を踏まえ、アクセスしたいデータの内容や当該データのユーザからの許諾（個

19 サービスのリソース（情報）にアクセスする際に、アクセストークンを利用させることで、部分的な情報にだけアクセスを許可する仕様を OAuth 2.0 と呼ぶ。OpenID は OAuth 2.0 の拡張で、ID 認証もあわせてできるようにした仕様を指す。

人がデータを提供することに同意しているか）の状況など、細かい条件に応じて、必要最小限のアクセスを許可するアクセス制御を実施する必要がある。

データ連携③：データの追跡可能性の確保によるデータ利用の透明性を担保する

サービス利用者の個人情報等の重要なデータを連携する場合、データ利用の透明性が担保できていないと、自身が提供したデータが、知らぬ間に自身の想定しない用途で利用されてしまう等が起こりうるため、情報流出と実質的に同じ状況となってしまうことが懸念される。そこで、住民やデータ提供元において、そのデータがどのように扱われているかを把握できるよう、データの利用状況の監視や適切な追跡・開示を可能とする仕組みを設け、追跡可能性を確保することでデータ利用の透明性を担保することが重要となる。

追跡可能性の確保の方法としては、データ利用で生じるアクセスログやシステムログを取得し分析・監視することで、データの利用流通を把握することが可能となる。なお、これらのログは、情報流出等のセキュリティインシデントが発生した場合においてもインシデントの発生元を特定することが可能になることから、インシデント対応においても有効である。

データ連携④：データの原本性保証によるデータの信頼性を担保する

今後、データ連携が加速し、多くのサービス提供者によるデータの利用や他のデータ連携基盤との連携によるデータの利活用など、様々な場面でのデータの利用が進む場合、利用先においてデータが加工されてしまったり、データの定義が誤って設定されてしまうことで、データの信頼性が担保できず、最終的にスマートシティで提供するサービスに影響が出てしまうことが想定される。そこで、データを提供するサービス利用者やデータ提供事業者、サービス提供者等が安心してデータを提供・利用するためにはデータの原本性保証[20]の確保が重要となる。

原本性保証を実現する方法としては、デジタル署名・ｅシール、電子透かしなどの技術を活用したものがある。また、データを利用する際は、ストアドプロシージャ[21]を通すことで不用意なデータ操作によるデータの改ざんや破壊などを防ぐことが可能になる。

データ連携⑤：必要性に応じたデータの匿名化・秘匿化を実施する

データを連携する際に、提供先に不必要なデータを連携してしまった場合、意図しないデータが連携先に渡る形で情報が漏えいし、また、そのデータが更に悪用されるリスクが生じることとなる。そのため、データを提供する個人がそれを要望する場合等の必要性に応じて、個人を特定できてしまう情報の削除や、個人を特定不可能な情報に変更するデー

20 原本性保証とは、原本（オリジナル）から改ざんされていないことを保証することである。
21 データベースの処理において、データの検索やコピーなど一連の処理をまとめた手続を持つプログラムのこと。

タ処理を用いる等により、個人が特定されないデータに加工する匿名化や秘匿化を実施し、連携するデータを制限する必要がある。

匿名化・秘匿化した上でデータの連携を行う場合は、データ提供元において責任をもって匿名化・秘匿化の処理を行うことが重要となる。

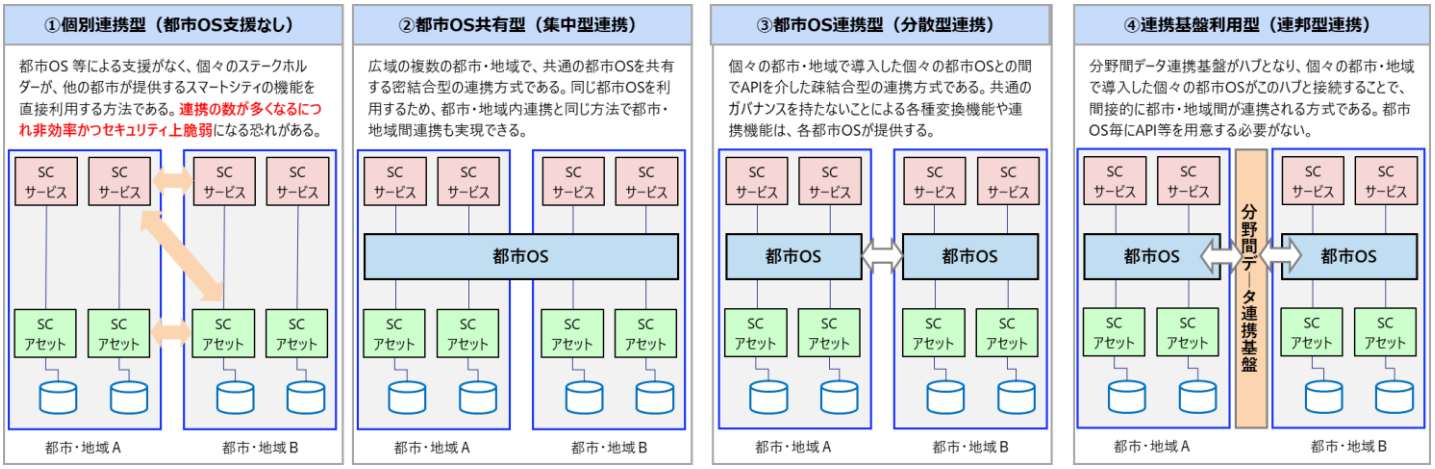
データ連携⑥：API におけるセキュリティ（機密性・完全性・可用性・真正性）を確保する

データ提供事業者が管理するデータ等をサービス提供者等が呼び出して利用する場合、API を介したデータ連携が発生するため、API におけるセキュリティを確保することが重要となる。

API の利用においては、データ連携②に記載したデータ提供事業者及びサービス提供者それぞれを認証し、アクセス制御を実施する機能を実装するほか、TLS[22]を用いた認証や通信の暗号化によって機密性、完全性及び真正性[23]の確保が必要となる。また、可用性の観点からは、API 利用者ごとにアクセスする時間や回数、取得するデータに制限を設けるなど、API の利用制限を設けることでサーバへの負荷を軽減するセキュリティ対策も必要となる。さらに、他のサービスの API を呼び出す場合、自身のスマートシティとは別のドメインへのアクセスとなるケースがあり、その場合はクロスドメインの通信を許可する必要がある。その際、ドメインを超えたデータリソースへのデータ連携を制御する CORS（Cross Origin Resource Sharing）を設定することでセキュリティを担保しながら API 連携を図ることが可能となる。

他の都市・地域とのデータ連携を実施する場合のパターンは主に以下の４パターンが考えられる。スマートシティ開発の初期段階では、「個別連携型」都市 OS 支援なしのパターンも考えられるが、連携先の増加に伴い連携時の効率性の低下と、セキュリティ上の脆弱さが露呈するため、都市 OS による支援を推奨する。

22 Transport Layer Security の略。インターネット上で通信データを暗号化するための技術。公開鍵認証基盤（PKI:Public Key Infrastructure）の技術が利用されており、電子署名や相手認証などを通じて機密性や完全性、真正性の担保が可能となる。
23 真正性とは、アクセス者などのエンティティがなりすましでない（本物である）ことを明確にすることである。



出所）内閣府「スマートシティリファレンスアーキテクチャ（ホワイトペーパー）第２版」
「7.1.2 都市・地域「内」連携と都市・地域「間」連携」を元に作成

図３－９　データ連携を実施する場合のパターン

都市 OS におけるデータ流通方式毎（蓄積型・分散型）の特徴は、以下のとおりである。

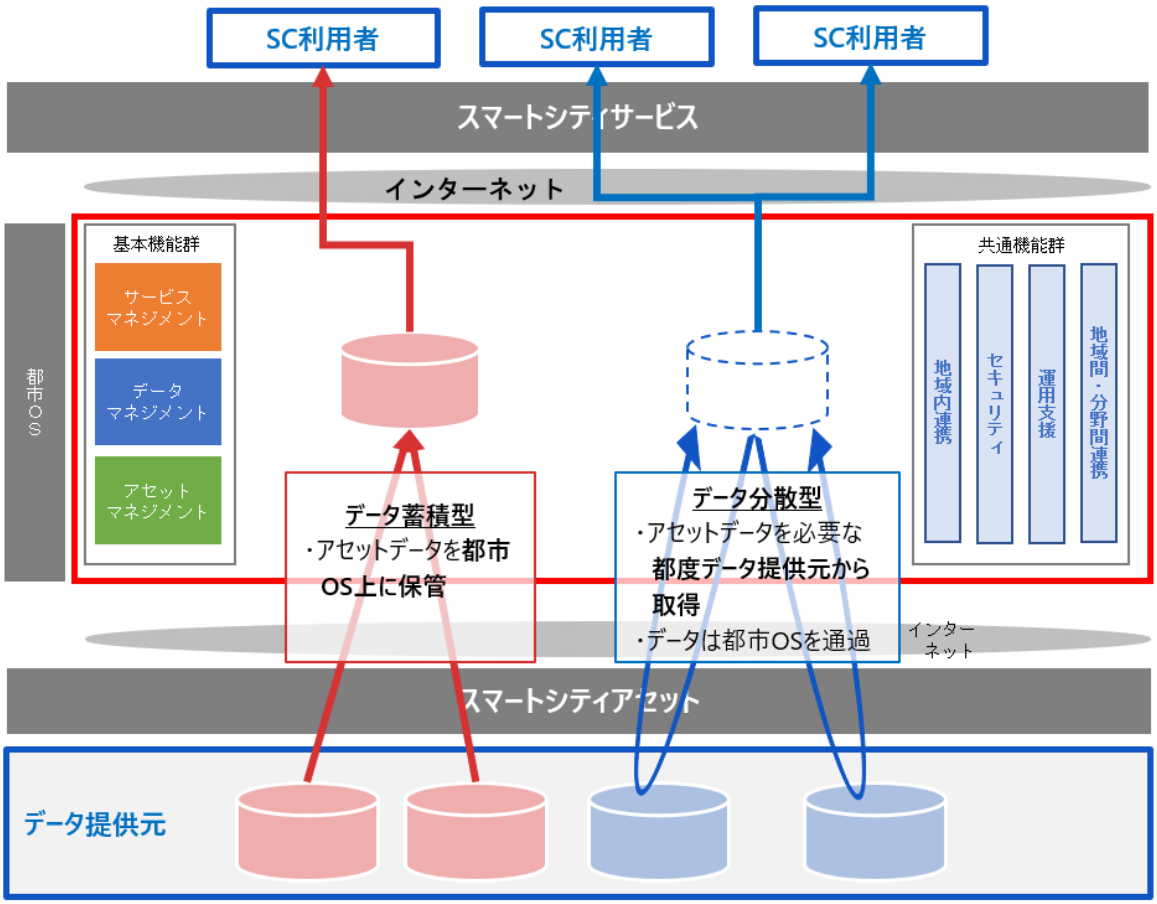


図３－１０　都市 OS におけるデータ流通方式毎（蓄積型・分散型）の特徴

データ蓄積型

主に頻繁にデータに更新が無いもしくは、オープンデータ系は、データ提供元のデータを都市 OS 内に蓄積し、スマートシティサービス生成に活用する。

データ分散型

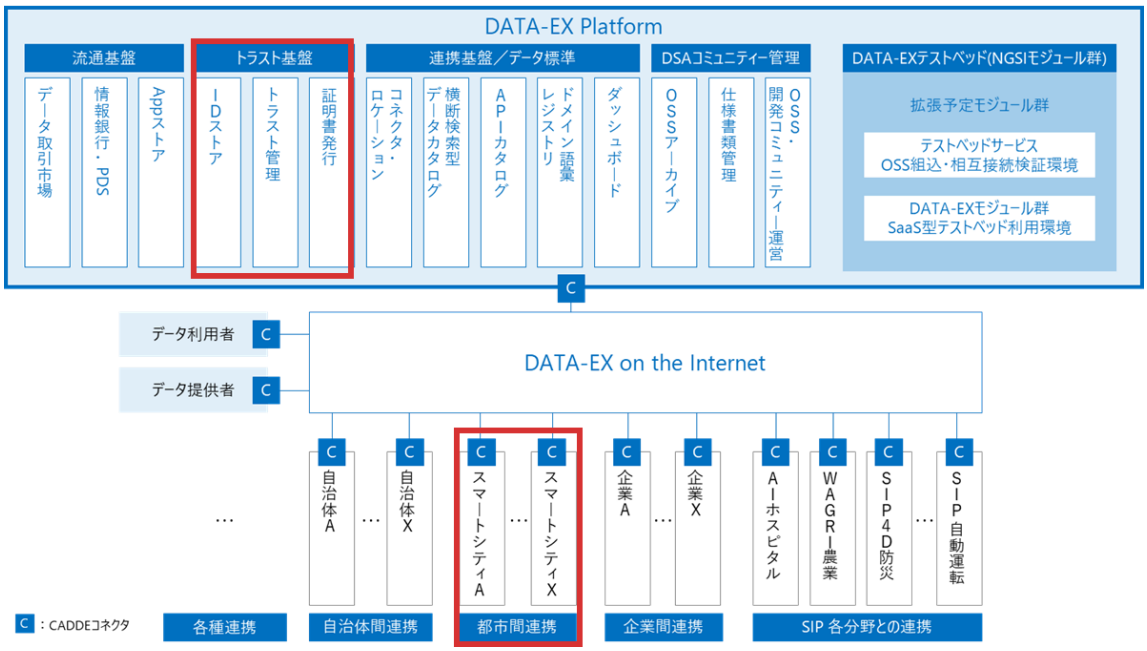
主に頻繁にデータに更新が有るもしくは、機微な情報（個人情報等）を取り扱う場合は、データ提供元のロケーション情報（URL 等）のみを保持し、必要な都度データ提供元から必要なデータを取得し、スマートシティサービス生成に活用する。

なお、取得したデータは、履歴を取得することが出来るため都市 OS を通過する設計（パススルー）が望ましい。

コラム

■ 現在、DSA（Data Society Alliance：一般社団法人データ社会推進協議会）において、**連携基盤利用型（連邦型連携）**の利用を可能とする分野間データ連係基盤（DATA-EX）の実証実験、開発を実施している。**DATAーEX を介することで異なるスマートシティ間のデータ連携を可能**にすることが期待できる。さらに、誰がどのようなデータを持っているか横断的に検索することが出来る。

■ データ連携時のセキュリティ機能としては、「データ提供者・利用者の真正性」、「データの完全性を保証する機能」、「国際連携機能」などを提供する予定である。



出所）DSA：DATA-EX 分野間データ連携基盤の将来展望と開発環境（https://data-society-alliance.org/data-ex/）

3.3. スマートシティで起こりうる問題事象と対策例

横断的なセキュリティ対策について、理解を促進できるように本節ではスマートシティで起こりうる問題事象について記述するとともに、セキュリティ対策例を 3.2 節で記載したセキュリティ対策と関連付ける形で記述している。セキュリティ対策例は全てのスマートシティにおいて基本的に実装されることが望ましい「標準対策」と、高いセキュリティレベルが求められるスマートシティにおいて付加的に実装されることが望ましい「推奨対策」で分けて記載している。なお、「3.1.1 ガバナンス」で記載したセキュリティ対策でも、横断的なセキュリティ対策と言えるものが含まれていることから、一部のセキュリティ対策については「3.1.1 ガバナンス」からも抜粋している。

3.3.1.セキュリティ管理体制に関する問題

起こりうる問題

ケース：スマートシティシステム全体が把握できないことによって生じる問題

推進主体においてサービス提供者にシステム構築・運用を委託しているが、その再委託、再々委託が存在するケースがある。その場合、再委託先等に対して、推進主体からのセキュリティやシステムに対する要求が十分に伝わっておらず、講じられるセキュリティ対策が脆弱なものとなってしまうことがある。その結果、再委託先のシステムで利用しているソフトウェアにおいて重大な脆弱性が存在し、その脆弱性が悪用されて情報流出等の問題が発生する等によって、スマートシティ全体としての利用者からの信頼が失われてしまう可能性がある。

セキュリティ対策例

標準対策

① 推進主体はスマートシティの推進に関与している委託先や再委託先等のサプライチェーンを把握し、スマートシティ全体の管理を行う。【サプライチェーン①】

② 推進主体において把握が困難な再委託先等やソフトウェア、製品などがある場合は、委託先にサプライチェーン・リスクへの対応のための管理体制を要求し、その管理体制を確認する。【サプライチェーン①】

③ 推進主体は、サプライチェーンを含めた連携する事業者のセキュリティレベルを把握する。【サプライチェーン②】【データ連携①】
- 連携する事業者に実施を求めるセキュリティ管理体制について記載したセキュリティチェックシートの活用
- ISO/IEC 27001 等のセキュリティに関する第三者認証の取得状況の確認

④　脆弱性への対応について、あらかじめ委託契約などに盛り込み、対応する主体と対応する内容を明確にしておく。【サプライチェーン③】

3.3.2.マルチステークホルダ間の責任分界に関する問題

起こりうる問題

ケース：不明確な責任分界点によって生じる問題

推進主体とその他のスマートシティ事業に関わる事業者（ベンダー等）との間で、サービスについて契約を行う場合、その契約内容が不十分だった場合、例えば情報の流出が発覚した際、推進主体と契約先の事業者がどちらの責任で対応するかが不明確となってしまうケースがある。その結果、対応を取りまとめる組織が不在となり、状況把握に時間がかかってしまい、対策が遅れて被害が拡大することがある。また、推進主体とサービス提供者の間でスマートシティサービスについての契約を行い、有事の対応を取りまとめる組織を決めていた場合でも、サービス提供者とその委託先（推進主体から見た再委託先）との契約において、どちらの責任で対応するかを定めていないと、事案対処の主管組織において十分な情報収集ができず、状況把握ができないというケースも考えられる。その場合、結果として、対策検討に時間がかかり、被害が拡大することもあり得る。

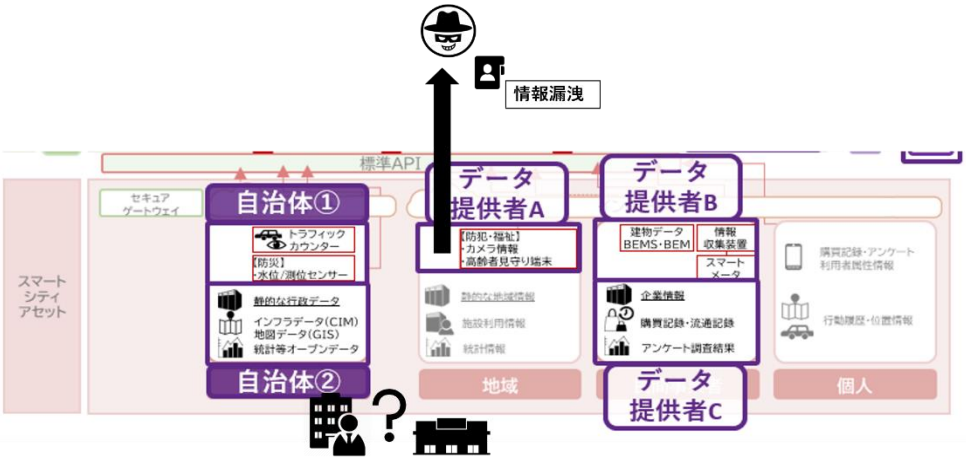


図３－１１　不明確な責任分界点によって生じる問題

セキュリティ対策例

標準対策

①　システムや機能の責任分界点を明確にした構成図や体制図を整備し、スマートシティを構成するシステム全体の繋がりを理解・把握し、スマートシティに関する契約や規約の中で責任範囲を明確化する。【ガバナンス②-1～ガバナンス②-3】【サプライチェーン①】【インシデント対応①】

② 継続的にリスクアセスメントを実施し、ポリシーの見直しを行うとともに、契約や規約の内容の見直しを行う。【ガバナンス③-1】

3.3.3.マルチステークホルダにおけるセキュリティポリシーに関する問題

起こりうる問題

ケース①：マルチステークホルダ間でセキュリティ管理水準が異なることで生じる問題

マルチステークホルダのうち、ソフトウェア、アプリケーション等のサービス提供者のセキュリティ管理体制が脆弱だった場合、別サービス経由で都市 OS への不正ログイン等が発覚しても、サービス提供者においてサービスを構成するシステムへのアクセス状況に関する情報収集が遅延する。その結果、原因究明が遅れて被害が拡大する場合がある。

また、マルチステークホルダ間でのセキュリティ対応体制にばらつきがある場合、例えばスマートシティで取り扱っている情報の改ざんが発覚し、都市 OS ベンダが都市 OS における事案調査に必要となる情報の収集や原因調査をしていたとしても、サービス提供者が情報収集・調査等の対応をしていなければ、調査に向けた情報が不十分となる。その結果、スマートシティで流通しているデータの信頼性が損なわれる状態が継続し、最終的に提供されるサービスの品質に影響することが考えられる。また、推進主体として被害状況の把握ができず、適切にサービス利用者に対して情報発信ができなくなってしまうため、サービス利用者からのスマートシティ全体に対する信頼を失ってしまうこともあり得る。

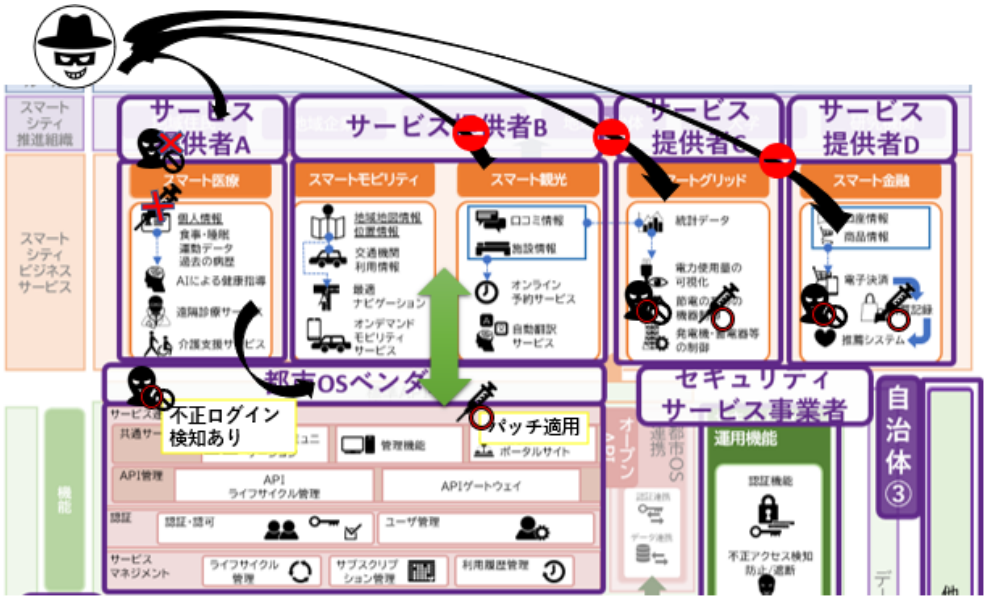


図３－１２　マルチステークホルダ間でセキュリティ管理水準が異なることで生じる問題

ケース②：マルチステークホルダにおける不明確な役割分担によって生じる問題

マルチステークホルダ間の役割分担が不明確な場合、スマートシティ内で流通するデータが改ざんされていることが発覚しても、それぞれのコンポーネントを担当する事業者間の情報連携や、それぞれにおける調査対応が不十分となり、事案の被害状況や発生原因を特定することができず、結果として原因究明が遅れ、データの提供や機能停止等、スマートシティの運営に影響が発生することがある。

セキュリティ対策例

標準対策

① 推進主体が、スマートシティ全体、もしくはスマートシティで提供するサービスごとに、連携する事業者（ベンダ等）を把握し、スマートシティのインシデント対応体制を整理し、マルチステークホルダ間で共有する。【インシデント対応①】

② 全てのマルチステークホルダに対して有事における連絡窓口を設置させ、連絡先をマルチステークホルダ間で共有する。【インシデント対応②】

③ 推進主体において、スマートシティ全体におけるセキュリティインシデント対応手順を整備する。また、都市 OS ベンダやサービス提供者等の事業者は予め決められている責任分界を踏まえ、スマートシティ全体におけるセキュリティインシデント対応手順に沿って、システム・サービス障害時の障害切り分けや復旧のための手順、セキュリティインシデント発生時のシステム・サービスの停止・復旧のための手順、原因調査手順等が含まれたセキュリティインシデント対応手順を整備する。【インシデント対応③】

④ 有事の際に円滑にマルチステークホルダ間で連携しながらインシデント対応が実施できるよう、推進主体が中心となり、マルチステークホルダがプレイヤーとなるインシデント対応演習を実施する。【インシデント対応④】

推奨対策

① 推進主体が中心となり、スマートシティ全体を対象とする SOC／CSIRT 等の組織を作り、マルチステークホルダ間での円滑な連携体制を構築する。【インシデント対応①】

② SOC での監視の状況や CSIRT が収集した脅威情報等を踏まえたリスクアセスメントを行い、新たな対策を検討する等、能動的なセキュリティ対策を図る。【ガバナンス③-1】

補足

SOC／CSIRT における状況把握、情報収集、インシデント対応統制等の協働体制について

スマートシティにおいて、重大なセキュリティ事故の発生や事故発生時の被害拡大を防ぐためには、ログの監視・分析などを行い、セキュリティインシデントを迅速に検知し、即時に対応できるようにしておくことが推奨される。また、事故発生予防の観点から、日常的に情報収集を行い、計画的かつ定常的なセキュリティ対応を行う事が望ましい。それを実現するためにも、組織横断的なセキュリティ対応機能を具備する SOC／CSIRT の設置が推奨される。

SOC／CSIRT のあり方については、それぞれのスマートシティのビジネスモデルによって様々なケースが想定されるが、例えば推進主体が主導で対応するケース、都市 OS ベンダが主導で対応するケースなどが想定される。

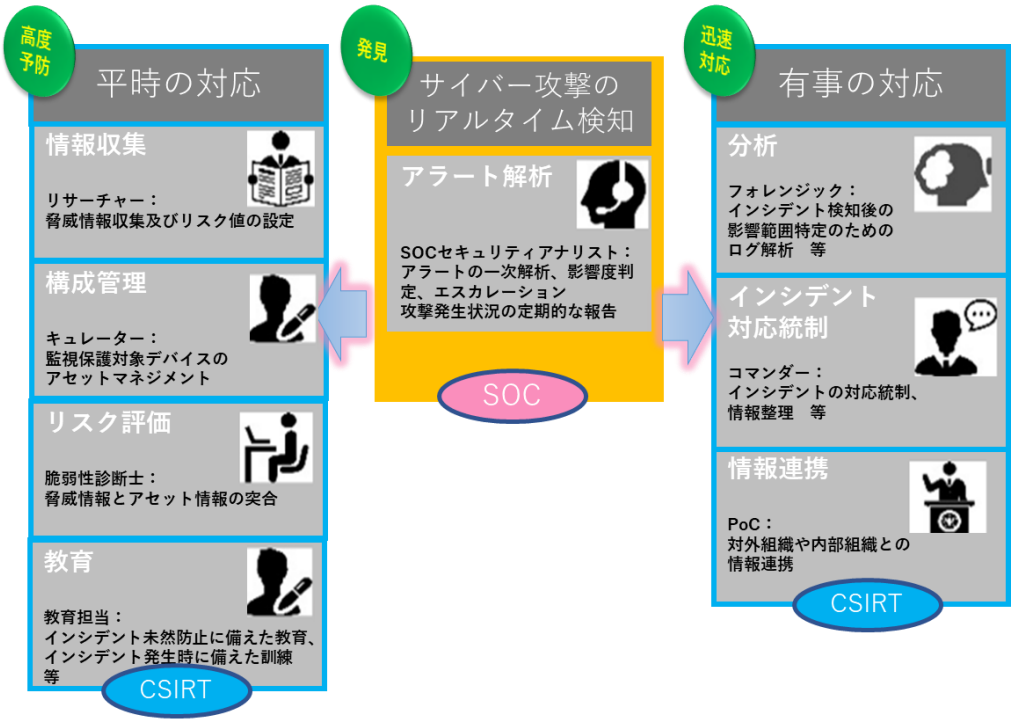


図３－１３　SOC／CSIRT の主な役割

＜想定される SOC／CSIRT の役割＞

SOC

- サイバー攻撃の検知/通知

CSIRT

- 平時の対応（情報収集・分析・共有、構成情報管理、インシデント未然防止のための教育　等）
- 有事の対応（インシデント対応統制、ログの分析又はその支援、内外との情報連携等）

3.3.4.マルチステークホルダにおけるデータ管理ポリシーに関する問題

起こりうる問題

ケース：データの利用目的、権限、範囲が不明確なことから生じる問題

データの利用や他のデータ連携基盤との連携によるデータの利活用など、様々な場面でのデータの利用が進むスマートシティでは、マルチステークホルダ間の契約においてデータの利用目的、権限が明確に定められていない場合、本来権利を有さない者に利用される又は目的外の利用が行われるといったケースが想定される。例えば、推進主体と契約したサービス提供者が、クローズドデータを利用したサービスの提供を開始する際、そのサービスにおいて契約に記載されている本来の利用目的の範囲外でデータが利用されてしまった場合、推進主体とサービス提供者間における契約違反やデータを提供している個人のプライバシー侵害等が発生する可能性がある。

セキュリティ対策例

標準対策

① 推進主体は、アクセスログやシステムログ等のログデータを活用し、スマートシティ全体で流通するデータの利用状況（誰がいつどのデータにアクセスして何に利用したか等）を把握する。【データ連携③】

② 利用目的、提供範囲、提供項目等、データを提供するサービス利用者との同意内容に応じたデータの連携・アクセス制御を適切に行う。【データ連携②】

③ 契約や規約の中でスマートシティ内で取り扱われるデータの取扱い基準（利用目的、内容、取得方法、データの所有者等）を明確化し、マルチステークホルダとの間で共通認識とする。【ガバナンス①-3】

④ スマートシティで連携するデータについて、スマートシティサービス提供において不要な場合は個人情報等の匿名化・秘匿化を行う。【データ連携⑤】

推奨対策

① トラストサービス／ブロックチェーン等の技術を活用した、追跡可能なシステム構成及びそれに準じたセキュリティ設計を検討する。【データ連携③】

3.3.5.データの連携先の拡大に関する問題

起こりうる問題

ケース①：データ連携が適切に制御されないことにより生じる問題

個人やデータ提供事業者から、提供されるデータの利用目的、内容について同意を得た上で、データ提供事業者、サービス利用者間のデータ連携における認証・アクセス制御を都市 OS で設定するが、データの流通がより拡大した場合、分野や地域を越えたデータ連携が行われ、データの連携元・連携先が拡大することが想定される。この場合、新たな連携先へのデータ連携にあたっては、同意が行われたデータ単位での適切なアクセス制御が重要となるが、連携先が増える度に手動でのアクセス制御のメンテナンスを実施していた場合、連携の遅れや、煩雑な設定変更作業の発生に伴う設定ミスなどによって同意されていないデータの連携や情報の流出など意図しない連携につながる可能性がある。

ケース②：データ連携におけるセキュリティ対策が適切に講じられていないことで生じる問題

データ連携の際、都市 OS に接続する者に対する認証の未実施や認証強度の弱い認証、暗号強度が弱い暗号アルゴリズムによる通信の暗号化が、悪意のある者による盗聴や情報漏えいにつながる可能性がある。また、複数のコンピュータから大量のデータ連携要求などによりサーバの負荷がかかりシステム停止やスマートシティサービスの中断につながる可能性がある。

セキュリティ対策例

標準対策

① データ連携先と接続する際に、独自のセキュリティチェックシートや第三者認証の取得有無を確認し、連携先のセキュリティ体制の確認・評価を実施する。【データ連携①】

② データ連携をする場合は、データ提供事業者及びデータへアクセスする主体の認証を適切に行う。【データ連携②】

③ 利用目的、提供範囲、提供項目等、データを提供するサービス利用者との同意内容に応じたデータの連携・アクセス制御を適切に行う。【データ連携②】

④ データ連携先が増えた場合は、都度データを提供する住民の同意をとったうえで連携を行う。オプトアウト方式をとる場合では、個人情報保護法による届出など適切な手続を行う。【データ連携②】

⑤ 通信の暗号化を実装する。また、API の利用者ごとに 1 日のアクセス回数の制限など、極度にシステムリソースを消費する動作を制限し、可用性を担保する。【データ連携⑥】

推奨対策

① データ連携先が連続的に増えることを想定し、都市 OS 上に設置されるポータルサイトやアプリケーションなどにおいて、データを提供するサービス利用者からの追加同意の仕組みを整える。【データ連携②】

② データ項目単位や、新たな連携先に対する提供について同意が行われたデータ単位でのシステムによる動的なアクセス制御を行う。【データ連携②】
（例）推奨対策①とシステム連動し、同意された内容を条件の一つとしつつ、連携先、連携元の情報等の複合的な条件に従いアクセスポリシーを決定し動的にアクセス権を制御する仕組み

コラム：海外のスマートシティ事例

■シンガポールのスマートネイション

・シンガポールは、2014 年より国を挙げて「スマートネイション（スマートな国家）」イニシアチブに取り組んでいる。スマートネイションとは、デジタル技術とデータを活用して国全体をスマートシティ化し、「より良い暮らし、より多くの機会、より強固なコミュニティ」を実現しようとする構想である。2017 年には関連する部局の統合により、政府横断的な取り組みを取りまとめる組織として、首相府直下にスマートネイション・デジタル政府グループ（SNDGG）が設立された。

・2018 年：保健省管轄下の公的医療グループ・シングヘルスのデータベースがサイバー攻撃を受け、約 150 万人分の個人情報が流出したと発表した。サイバー攻撃を受けたシングヘルスは、シンガポール最大の公的医療グループである。流出した情報は、シングヘルスが運営する専門医療施設と診療所を訪れた外来患者約 150 万人分の個人情報で、名前、身分証明番号、住所、生年月日などの情報が不正にアクセスされ、コピーされた。また、このうち約 16 万人分については処方された薬の情報も流出した。

・SNDGG は政府のシステムを見直し、対応策を導入するまではスマート国家構想に基づく一部プロジェクトを中断する方針を明らかにした。なお、一時的な中断であって、首相は「安全性を確保したスマート国家を構築していく必要がある」としている。

出所：2018 年 7 月、JETRO、https://www.jetro.go.jp/biznews/2018/07/2a683a939c59d0db.html
2019 年 8 月、日本総研、https://www.jri.co.jp/page.jsp?id=34979

4. セキュリティ検討のための補助コンテンツ

これまで、スマートシティの構築・運用におけるセキュリティの考え方や、サプライチェーンを含めたスマートシティの推進・運営に携わる関係主体において実施すべきセキュリティ対策を整理してきた。

第４章では、スマートシティを構築・運用する上で考慮すべきセキュリティ上のリスクの一覧や、検討すべきセキュリティ対策の一覧、セキュリティ対策に漏れがないかを確認するためのチェックシートなど、補助的に利用できるコンテンツについて紹介する。

4.1. セキュリティ対策一覧

スマートシティを推進する上で、想定されるセキュリティ上のリスクを幅広くまとめたものを【Appendix】B「セキュリティ上のリスク一覧」、それらのリスクを踏まえたセキュリティ対策をまとめたものを【Appendix】C「セキュリティ対策一覧」に示す。これらの【Appendix】は、自身のスマートシティにおいてセキュリティ対策を検討する上での補助的なコンテンツとして活用することが可能である、具体的な活用の手順を以下に記載する。

① 自身が実現しようとしているスマートシティシステム、サービスにおいて、守るべき機能や資産（データ）を特定する。

② 特定した機能や資産をふまえ、自身のスマートシティシステム、サービスにおいて想定されるセキュリティ上のリスクを導出する。

③ 【Appendix】B「セキュリティ上のリスク一覧」から該当するリスクを抽出し、それに対応する【対策要件 ID】を確認する。

④ 【対策要件 ID】を基に、対策の具体的な内容を【Appendix】C「セキュリティ対策一覧」から導出する。

以下に、ユースケースを用いた例を示す。また、「防災」「医療・福祉」「決済」「交通」「観光」の５分野におけるリスク特定とセキュリティ対策検討の例を【Appendix】D「各分野におけるリスク特定とセキュリティ対策検討のイメージ」に示す。

その他に、スマートシティと連携され得るサービスにおいて、考慮すべきリスクと対策例を脅威事例として【Appendix】E「サービス観点の脅威事例」に記載する。

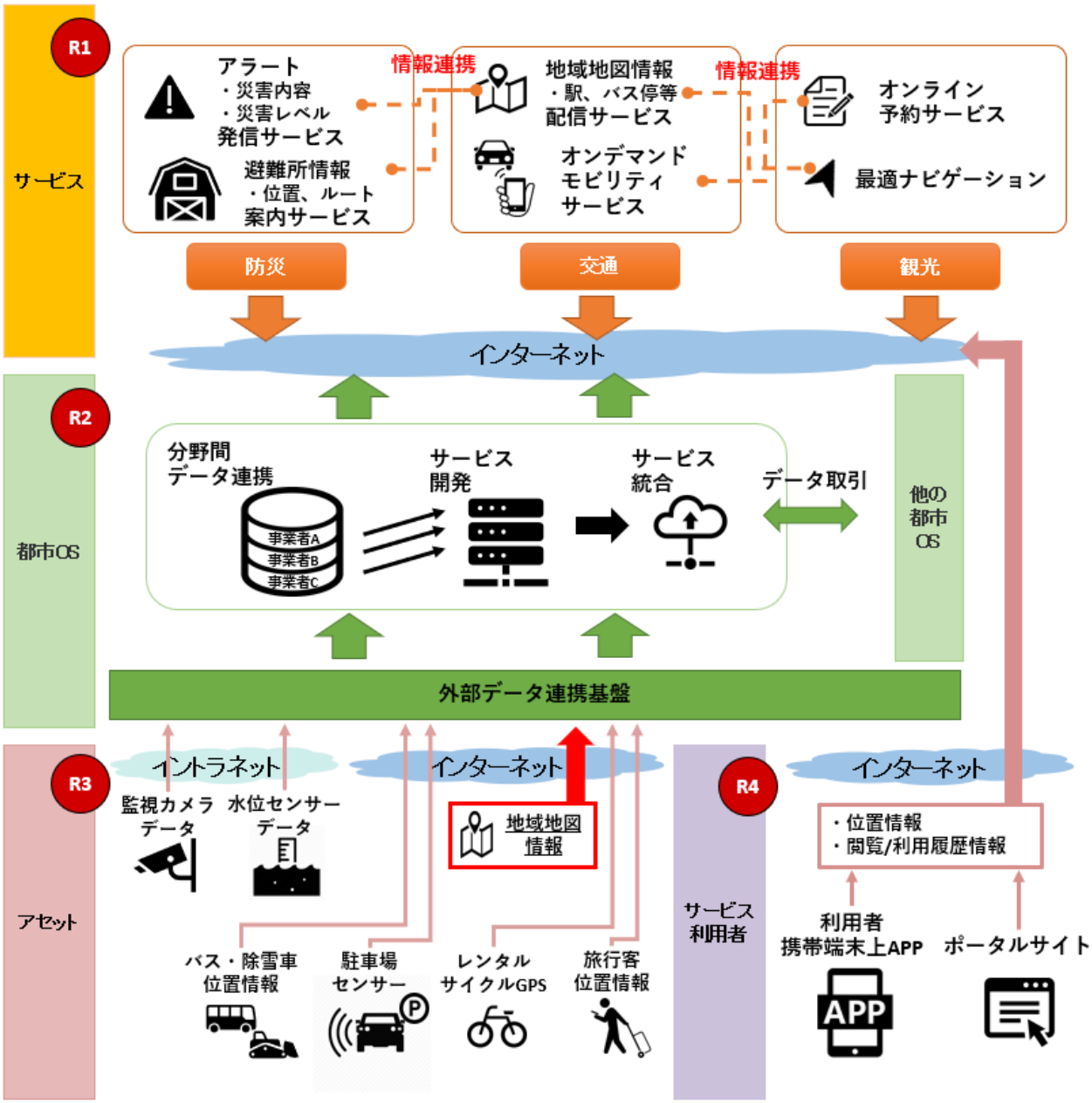


図４－１　スマートシティのユースケース

表４－１　リスク例

リスク箇所	リスク概要	対策番号
R1	なりすましによる不正の受信	CPS.AC-1、CPS.AC-3、CPS.AC-4、CPS.AC-8、CPS.AC-9、CPS.IP-2、CPS.IP-10、CPS.MA-1、CPS.MA-2、CPS.RA-2、CPS.CM-6、CPS.CM-7
	サービス拒否攻撃、ランサムウェアへの感染等によるシステムが停止する	CPS.RA-1、CPS.RA-3、CPS.RA-4、CPS.RA-5、CPS.RA-6、CPS.RM-2、CPS.DS-6、CPS.DS-7
	自組織の保護すべきデータが改ざんされる	CPS.AC-7、CPS.AC-9、CPS.DS-2、CPS.DS-3、CPS.DS-4、CPS.DS-11
	不正なエンティティによる許容範囲外のインプットデータ・マルウェアによる制御信号の改ざん	CPS.RA-4、CPS.RA-6
R2	自組織で管理している（データ保管）領域から関係する他組織の保護すべきデータが漏えいする	CPS.AC-1、CPS.AC-5、CPS.AC-6、CPS.AC-9、CPS.GV-3
	データ加工・分析システムが誤動作することで、適切でない分析結果が出力される	CPS.CM-3、CPS.CM-4
R3	改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信が発生する	CPS.AC-1、CPS.AE-1、CPS.AM-1、CPS.AM-5、CPS.CM-5、CPS.CM-6、CPS.DS-8、CPS.SC-4
	不正なエンティティによる許容範囲外のインプットデータ・マルウェアによる制御信号の改ざん	CPS.CM-3、CPS.AE-1、CPS.CM-1、CPS.CM-5、CPS.PT-1、CPS.RP-1
	IoT機器内部への不正アクセス	CPS.IP-1、CPS.PT-2、CPS.DS-15、CPS.RA-4、CPS.RA-6、CPS.SC-4
	IoT機器におけるセキュリティ上の脆弱性を利用したネットワーク上の通信の盗聴	CPS.AC-1、CPS.AE-1、CPS.AM-1、CPS.AM-5、CPS.CM-5、CPS.CM-6
R4	（なりすまし等をした）ソシキ/ヒト/モノ等から不適切なデータを受信する	CPS.DS-3、CPS.AC-1、CPS.AC-3、CPS.AC-4、CPS.AC-8、CPS.AC-9

本ガイドラインでは、スマートシティリファレンスアーキテクチャを前提とし、スマートシティ全体におけるセキュリティの考え方や想定されるリスク、セキュリティ対策について整理しているが、これらの整理を行う上では、その他のガイドライン等も参考としている。

例えば、スマートシティアセットにおける IoT 機器などのアセットにおいてセキュリティ対策を検討するにあたっては、IoT 推進コンソーシアムが公表している「IoT セキュリティガイドライン」を参照するとともに、当該ガイドラインとの記述の整合性を維持するように配慮している。その他、参考としている資料として、「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」や「NIST SP800-53」、「NIST SP800-171」、「サイバー・フィジカル・セキュリティ対策フレームワーク」等が挙げられ、【Appendix】B「セキュリティ上のリスク一覧」や【Appendix】C「セキュリティ対策一覧」もこれらのガイドラインを参考として作成している。

自身が検討しようとしているセキュリティの内容やレベル感、粒度などを踏まえ、本ガイドラインや【Appendix】を活用しつつ、加えて本ガイドラインが参考としている上述のガイドライン等を適宜参照することで、自身が推進するスマートシティセキュリティの実装に資することを期待する。

	サイバー・フィジカル・セキュリティ対策フレームワークでの該当対策要件		参照ガイドライン					
			NIST Cybersecurity Framework Ver 1.1	NIST SP 800-171.53	ISO/IEC 27001:2022（付属書A）	ISO/IEC 27017:2015	IoTセキュリティガイドライン Ver 1.0	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）
ガバナンス	CPS. AC-1, 2, 5 CPS. AE-1~5 CPS. AM-2~7 CPS. AN-1~3 CPS. AT-1~3 CPS. BE-1~3 CPS. CM-1, 2, 6 CPS. CO-1~3 CPS. DP-1~4	CPS. DS-1, 11, 13~15 CPS. GV-1~4 CPS. IM-1, 2 CPS. IP-1, 3, 7~10 CPS. MI-1 CPS. PT-1 CPS. RA-1~3, 5, 6 CPS. RM-1, 2 CPS. RP-1~3 CPS. SC-1~11	◎	○	◎	○	◎	○
サービス	CPS. AC-1~9 CPS. AE-1 CPS. AM-1~3, 5 CPS. CM-1~7 CPS. DS-2~11, 13 CPS. GV-3	CPS. IP-1, 2, 4~6, 10 CPS. MA-1, 2 CPS. PT-1, 2 CPS. RA-1, 2, 4, 6 CPS. RP-1, 4 CPS. SC-3, 4, 8	○	○			○	○
都市OS	CPS. AC-1~9 CPS. AE-1, 3 CPS. AM-1, 2, 5 CPS. CM-1~7 CPS. DP-4 CPS. DS-1~13 CPS. GV-3	CPS. IP-1, 2, 4~6, 10 CPS. MA-1, 2 CPS. PT-2, 3 CPS. RA-1~6 CPS. RM-2 CPS. RP-1 CPS. SC-3, 4, 8	○	○	○	◎	○	◎
アセット	CPS. AC-1~4 CPS. AC-7~9 CPS. AE-1 CPS. AM-1, 5 CPS. CM-2, 3, 5~7 CPS. DS-3, 6~8, 10, 11, 13, 15	CPS. IP-1, 2, 4~6 CPS. MA-1~3 CPS. PT-2 CPS. RA-4, 6 CPS. SC-3, 4, 8	○	○			◎	◎

図４－２　本ガイドラインと主に参照したガイドラインの対応関係

4.2. スマートシティセキュリティ導入チェックシート

第３章において、スマートシティにおける具体的なセキュリティ対策について記載しているが、スマートシティ全体のセキュリティを担保する上では考慮漏れがないように対応することが求められる。

そこで、本節において、第３章に記載されている内容を元に作成した、「スマートシティセキュリティ導入チェックシート」を示す。推進主体においては包括的なスマートシティのセキュリティを検討する上で、セキュリティ検討の考慮漏れがないように本チェックシート全体を参照することが望ましい。また、都市 OS ベンダやサービス提供者、データ提供事業者などの各カテゴリのセキュリティ対策を主で担当する主体においては、自身のカテゴリにおけるセキュリティ対策をチェックするとともに、横断的なセキュリティ対策についてチェックすることで、考慮漏れなくセキュリティ検討を行うことが可能となる。

なお、本ガイドラインの第３章で記載されているセキュリティ対策は完全に網羅的なものではなく、分野を限定せずあらゆるスマートシティにおいて基本的に実施が求められるセキュリティ対策を取りまとめたものとなっている。そのため、それぞれのスマートシティで提供するサービスの内容や提供形態、取り扱う情報等に応じて、追加のセキュリティ対策が必要となることは十分に考えられる。つまり、本セキュリティチェックシートを全て遵守できていれば、あらゆるセキュリティインシデントの発生を防ぐことができるわけではないことに留意されたい。

スマートシティセキュリティ導入チェックシート

カテゴリ１　ガバナンス

① セキュリティに関するポリシーの策定

ガバナンス①-1：情報セキュリティ基本方針を策定する

☐ 目的や対象範囲など基本的な事項のほか、セキュリティを担保するための取組方針が記載された情報セキュリティ基本方針を策定する

ガバナンス①-2：セキュリティ対策基準を策定する

☐ 組織体制や情報資産の分類・管理に関する項目のほか、管理的及び技術的なセキュリティ対策等について具体的な遵守事項や判断基準等を定めたセキュリティ対策基準を策定する

ガバナンス①-3：データ取扱い基準を策定する

☐ スマートシティで取り扱われるデータを分類するとともに、適切なデータの取扱いに関する事項や、法令等への対応等を定めたデータ取扱い基準を策定する

ガバナンス①-4：インシデント対応手順を策定する

☐ インシデント対応に関与する関係主体やそれぞれの責任範囲の明確化、連絡体制や連絡先などの整備、対応における判断基準やインシデント対応フロー等のインシデント対応手順を策定する

ガバナンス①-5：事業継続計画を策定する

☐ 障害やセキュリティ事故等が発生した際にどの機能を優先して保護するかといった判断基準や、スマートシティ事業継続のための役割分担、対応手順等を定めた事業継続計画を策定する

ガバナンス①-6：委託先や提携先の評価基準を策定する

☐ セキュリティ管理体制やセキュリティに関する第三者認証の取得有無等、外部委託等を実施する際に求めるべき内容や選定条件などを定めた評価基準を策定する

ガバナンス①-7：リスクアセスメントを実施する

☐ スマートシティの全体構成や守るべき機能や情報資産を踏まえ、リスク評価を実施する

ガバナンス①-8：法令やガイドライン等との整合性を確認する

☐ スマートシティのセキュリティに関するポリシー策定時に、自身のスマートシティにおいて遵守することが求められる法令を把握する。また、それらの法令が遵守できる形でガイドラインを参考としながらポリシーを策定する

ガバナンス①-9：各種文書の作成や各活動の記録を取り共有・管理する機能を整備する

☐ 様々な方針・基準・手順をステークホルダに浸透させ、必要な文書改訂とそれらを共有・管理するための体制および機能を整備する

② マルチステークホルダへのポリシーの浸透

ガバナンス②-1：ポリシーを遵守するためのセキュリティ要件を調達仕様書に反映する

- □ セキュリティに関するポリシーに則り、情報セキュリティの管理体制の構築やセキュリティインシデントへの対処などのセキュリティ要件を調達仕様書に反映させる

ガバナンス②-2：データ取扱い基準を契約・規約に反映する

- □ データの流通や利活用における取扱いについて、データ取扱い基準で定めた内容を委託先や提携先との契約・規約に反映する

ガバナンス②-3：契約・規約で責任範囲を明確化する

- □ システムの責任分界点とデータの責任分界点を委託先や提携先との契約・規約の中で明確化する

ガバナンス②-4：接続を希望する事業者のセキュリティ対応レベル審査・監査

- □ スマートシティに接続を希望する事業者のセキュリティ対応レベルを評価するために、事前にプロセスや役割を整理する

ガバナンス②-5：運営関係者に対する定期的なトレーニングを実施する

- □ スマートシティの運営関係者に対する教育や情報提供を目的としたトレーニングを定期的に実施する

③ ガバナンス維持のための取組

ガバナンス③-1：継続的なリスクアセスメントの実施とセキュリティに関するポリシーの見直しを実施する

- □ 提供するサービスの変化や脅威の拡大等に応じ、継続的にリスクアセスメントを実施し、セキュリティに関するポリシーの見直しを実施する

ガバナンス③-2：セキュリティ対策への適切な投資を継続的に実施する

- □ セキュリティの維持・向上を図るため、セキュリティ対策への適切な投資を継続的に実施する

ガバナンス③-3：ユーザに対する情報発信やリテラシ向上の取り組みを実施する

- □ 利用者に対して適切な情報発信の場や、IT リテラシのトレーニング機会を設けるなどの取り組みを、検討・実施する

カテゴリ２ サービス

① サービス個別でのリスクアセスメントの実施

サービス①-1：それぞれのサービスにおいてリスクアセスメントを実施する

- □ 個々のサービスにおいて守るべき情報資産や機能を特定した上で、リスクアセスメントを実施する

② 外部からの攻撃等を防ぐセキュリティ対策

サービス②-1：サービスの不正な利用を規約・契約で抑止する

- □ サービスの利用開始やアカウント登録時に、運営に支障を与える行為等の禁止事項を明確にし、それらが疑われる場合にはアカウント停止、損害賠償等の必要な措置を取ることに対し同意取得をする

サービス②-2：サービスへのアクセス制御を実装、運用する

- □ 外部からサービスに関わるシステムに通信をする場合は、ファイアウォール等を実装し、適切なアクセス制御を実装する

サービス②-3：適切な権限設定を実施し、管理する

- □ 必要な人や役割などに限定した権限設定を行い、アカウントの一覧表を作成し、定期的に棚卸しするなどして適切に管理する

サービス②-4：身元確認機能を実装する

- □ サービス利用登録時や必要なタイミングで身元確認を適切に行い、サービスを提供可能か判断する

サービス②-5：認証機能を実装する

- □ アクセスした人が本人であるかを確認するための認証機能を実装する

サービス②-6：セキュリティ監視を実施する

- □ IDS や IPS、WAF などを設置し、外部からの不正なコマンドが含まれた通信等のシステムへのサイバー攻撃を監視する

③ セキュリティインシデント発生の未然防止のためのセキュリティ対策

サービス③-1：サービスの企画・設計・開発工程における脆弱性を適切に管理する

- □ セキュア設計やセキュアコーディング、サービスイン前のセキュリティテストや脆弱性診断などによってサービスの企画・設計・開発工程における脆弱性を適切に管理する

サービス③-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する

□　定期的な脆弱性診断の実施や、継続的な脆弱性情報の収集によって自システムの脆弱性を把握しつつ、構成情報を適切に管理し、それらの情報を元に適切にバージョンアップやセキュリティパッチの適用等の対策を実施する

サービス③-3：運用管理端末へのセキュリティ対策を実施する

□　システムへ直接アクセスが可能な運用管理端末は、当該端末へのアクセス制御と認証の導入をした上で、ウイルス対策ソフトの導入、OS 等の脆弱性への対応、物理的なアクセス制限等の対策を実施する

④ インシデント発生時に備えたセキュリティ対策

サービス④-1：外部との通信やデータの暗号化を実施する

□　外部との通信やシステムに保存されるデータは十分な強度の暗号アルゴリズムで暗号化を実施する

サービス④-2：定期的にバックアップを取得する

□　システムの構成情報や重要なデータは定期的にバックアップし、災害や復旧を踏まえた保管を行う

サービス④-3：証跡確保のためのログを取得する

□　証跡を確保するための様々なログを取得し、適切に保管する

サービス④-4：インシデント発生時のリスク軽減策を検討する

□　セキュリティインシデントが発生に備え、セキュリティインシデント対応体制が構築されていることを確認する

カテゴリ３ 都市 OS

① 外部からの攻撃、侵入等を防ぐセキュリティ対策

都市 OS①-1：都市 OS へのアクセス制御を実装、運用する

- □ 外部から都市 OS に関わるシステムに通信をする場合は、ファイアウォール等を実装し、適切なアクセス制御を実装する

都市 OS①-2：適切な権限設定を実施し、管理する

- □ 必要な人や役割などに限定した権限設定を行い、アカウントの一覧表を作成し、定期的に棚卸しするなどして適切に管理する

都市 OS①-3：認証機能を実装する

- □ アクセスした人が本人であるかを確認するための認証機能を実装する

都市 OS①-4：セキュリティ監視を実施する

- □ IDS や IPS を設置し、不正なコマンドが含まれた通信等のシステムへのサイバー攻撃を監視する

② セキュリティインシデント発生の未然防止のためのセキュリティ対策

都市 OS②-1：都市 OS の企画・設計・開発工程における脆弱性を適切に管理する

- □ 都市 OS を構成するシステムの企画・設計・開発等の各段階においてセキュリティを検討・実施する

都市 OS②-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する

- □ 定期的な脆弱性診断の実施や、継続的な脆弱性情報の収集によって自システムの脆弱性を把握しつつ、構成情報を適切に管理し、それらの情報を元に適切にバージョンアップやセキュリティパッチの適用等の対策を実施する

都市 OS②-3：運用管理端末へのセキュリティ対策を実施する

- □ システムへ直接アクセスが可能な運用管理端末は、当該端末へのアクセス制御と認証の導入をした上で、ウイルス対策ソフトの導入、OS 等の脆弱性への対応、物理的なアクセス制限等の対策を実施する

③ インシデント発生時に備えたセキュリティ対策

都市 OS③-1：外部との通信やデータの暗号化を実施する

- □ 外部との通信やシステムに保存されるデータは十分な強度の暗号アルゴリズムで暗号化を実施する

都市 OS③-2：定期的にバックアップを取得する

- □ システムの構成情報や重要なデータは定期的にバックアップし、災害や復旧を踏まえた保管を行う

都市 OS③-3：証跡確保のためのログを取得する

☐ 証跡を確保するための様々なログを取得し、適切に保管する

④ 推進主体からの要求に応じた適切なクラウドサービスの利用

都市 OS④-1：クラウドサービスの利用者と提供事業者間の責任分界点を把握する

☐ クラウド基盤として IaaS/PaaS を利用する場合、責任分界点について正確に把握し、それに応じたセキュリティ対策を実施する

都市 OS④-2：データロケーションに関する推進主体からの要求事項に対応する

☐ クラウド基盤を利用する場合、都市 OS 上で取り扱うデータの種類や適用される法令を理解した上で、クラウドの設置場所（リージョン）に関する推進主体からの要求事項に対応できているかを確認し利用する

都市 OS④-3：複数リージョン選択等により、可用性を担保する

☐ クラウド基盤を利用する場合、障害や復旧の観点から複数リージョンの選択を検討する

カテゴリ４ アセット

① アセットの監視・管理

アセット①-1：アセットの監視・管理を実施する

- ☐ アセットの死活監視をしたうえで、バージョン情報などの基本的な情報を管理する

アセット①-2：新規の脆弱性情報を把握し、ファームウェア、ソフトウェア等のバージョンアップを適切に実施する

- ☐ アセットの脆弱性情報を継続的に収集・把握し、適切なタイミングでバージョンアップの対応を行う

② アセットそのものへのセキュリティ対策

アセット②-1：外部との通信や、保有するデータを暗号化する

- ☐ アセットと外部との通信やアセットで保有するデータは十分な強度の暗号アルゴリズムで暗号化を実施する

アセット②-2：認証機能を実装する

- ☐ アセットにアクセスする際の認証機能を実装する。パスワードは工場出荷状態でのデフォルトパスワードや容易なパスワードを避け、サービス利用者側でデバイス管理をする場合は、適切なパスワードの設定や管理などの注意喚起をする

アセット②-3：物理的なセキュリティ対策を実施する

- ☐ デバイスに対する物理的な破壊や盗難からの保護対策を行う。誤動作が起きたとしても人命への影響が発生しないよう、フェイルセーフを考慮した設計をする。また、デバイスを廃棄する場合は物理的に破壊するなど情報漏洩対策を実施する

横断的なセキュリティ対策

1　適切なサプライチェーン管理

サプライチェーン①：サプライチェーン全体のリスクを管理・把握する

□　スマートシティ全体における、委託先・再委託先も含めたマルチステークホルダ全体のサプライチェーン・リスク（委託先等の立地する場所の法的環境等による影響や供給安定性に対するリスクを含む）を把握し、そのリスクへの対策を検討する
※委託先等においては、上述のサプライチェーン・リスクへの対策を検討しつつ、委託元に対して適切な情報提供を実施する

サプライチェーン②：委託先／提携先のセキュリティ管理体制を評価する

□　チェックシートや第三者認証の取得状況などを活用し、委託先のセキュリティ管理体制を評価する。契約期間中においても継続的に確認・評価し、不十分な点があれば改善を求める

サプライチェーン③：サプライチェーン全体の脆弱性情報を適切に把握し、対応する

□　継続的な脆弱性への対応が期待できるソフトウェアやハードウェアを選定するとともに、サプライチェーン間の契約や、調達時の仕様に脆弱性情報を適切に提供し、対応するといった記載を盛り込むことで、脆弱性情報を適切に把握し、対応できるようにする

サプライチェーン④：提携主体はステークホルダ毎の責任分界点を明確にする

□　推進主体とステークホルダ間の契約形態（業務委託・業務提携など）によって責任を追う先が異なるため、提供するサービス等の責任範囲を明確にする

2　インシデント対応時の連携

インシデント対応①:責任範囲を明確にしたセキュリティインシデント対応体制を構築する

□　セキュリティインシデントが発生した際の対応に関する責任分界点を明示したセキュリティインシデント対応体制を構築する

インシデント対応②：連絡窓口を整備し、マルチステークホルダ間で相互に共有する

□　セキュリティインシデントの発生に備え、マルチステークホルダ間の連絡体制や緊急連絡先を予め把握・整備し、共有する

インシデント対応③：スマートシティ全体及び各マルチステークホルダにおけるインシデント対応手順を整備する

□　セキュリティインシデントが発生に備え、それぞれのマルチステークホルダ内及びスマートシティ全体としてのインシデント対応手順を整備する

インシデント対応④：定期的にセキュリティインシデント対応訓練・演習を実施する

- □ インシデント対応手順や自組織内、組織外との連携対応の習熟などを目的とした、インシデント対応訓練・演習を実施する

インシデント対応⑤：新たな脅威やインシデント事例などの情報収集・分析する

- □ レジリエンス強化のため、インシデント対応関係者は新たな脅威やインシデント事例などを情報収集し共有・学習を行い、既存の対応手順などの見直しを行う

3　データ連携時のセキュリティ

データ連携①：データ連携元・連携先のセキュリティ体制の確認・評価を実施する

- □ データの連携元・連携先組織のセキュリティマネジメントを、チェックシートや第三者認証の有無等を活用して確認し、評価する

データ連携②：データ提供事業者・サービス提供者等の認証と適切なアクセス制御を実施する

- □ 連携するデータの内容や個人情報の同意内容に沿った利用目的等を踏まえ、認証と適切なアクセス制御の付与することで適切なデータ連携を行う

データ連携③：データの追跡可能性を確保しデータ利用の透明性を担保する

- □ データ利用で生じるアクセスログやシステムログを取得し、分析・監視することで、データの追跡可能性を確保し、データ利用の透明性を担保する。

データ連携④：データの原本性保証を確保しデータの信頼性を担保する

- □ デジタル署名、電子透かしなど技術を活用し、原本性保証を確保することでデータの信頼性を担保する

データ連携⑤：必要性に応じたデータの匿名化・秘匿化を実施する

- □ データを提供する個人がそれを要望する場合等、必要性に応じてデータの提供元において匿名化・秘匿化の処理を行う

データ連携⑥：API におけるセキュリティ（機密性・完全性・可用性・真正性）を確保する

- □ API の利用では認証や通信の暗号化、公開鍵暗号基盤の利用、サーバへの負荷対策、クロスドメインの通信を許可するなど、API におけるセキュリティを考慮する

【Appendix】A　参照すべき法令・ガイドラインの一覧

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
1	法律・法令（国内）	個人情報の保護に関する法律（令和五年法律第四十七号による改正）	個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。	－	スマートシティの推進に関わる全ての主体	個人情報を取り扱う場合	・第十八条（利用目的による制限） ・第二十二条（データ内容の正確性の確保等） ・第二十三条（安全管理措置） ・第二十四条（従業者の監督） ・第二十五条（委託先の監督） ・第二十六条（漏えい等の報告等） ・第二十七条（第三者提供の制限） ・第二十八条（外国にある第三者への提供の制限） ・第二十九条（第三者提供に係る記録の作成等） ・第三十条（第三者提供を受ける際の確認等） ・第三十一条（個人関連情報の第三者提供の制限等） ・第三十二条（保有個人データに関する事項の公表等） ・第三十三条（開示） ・第三十四条（訂正等） ・第三十五条（利用停止等） ・第三十七条（開示等の請求等に応じる手続） ・第四十一条（仮名加工情報の作成等） ・第五十七条（適用除外） ・第七十一条（外国にある第三者への提供の制限）	個人情報の定義や個人情報取扱事業者が行うべき従業員や委託先の監督について記載されているため、個人情報を取り扱う場合に参照する。
2		不正競争防止法	事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与することを目的とする。	－	スマートシティの推進に関わる全ての主体	営業秘密情報を取り扱う場合	・第十条（秘密保持命令）	不正競争防止法によって禁止される行為、不正競争行為に対しての是正方法が記載されているため、営業秘密情報を取り扱う場合に参照する。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
3	法律・法令（国内）	官民データ活用推進基本法	官民データの適正かつ効果的な活用の推進に関し、基本理念を定め、国、地方公共団体及び事業者の責務を明らかにし、並びに官民データ活用推進基本計画の策定その他官民データ活用の推進に関する施策の基本となる事項を定めるとともに、官民データ活用推進戦略会議を設置することにより、官民データ活用の推進に関する施策を総合的かつ効果的に推進し、もって国民が安全で安心して暮らせる社会及び快適な生活環境の実現に寄与することを目的とする。	-	スマートシティの推進に関わる全ての主体	官民データを取り扱う場合	・第十条（手続における情報通信の技術の利用等） ・第十一条（国及び地方公共団体等が保有する官民データの容易な利用等） ・第十二条（個人の関与の下での多様な主体による官民データの適正な活用） ・第十三条（個人の関与の下での多様な主体による官民データの適正な活用）	官民データの定義や、官民データを活用していくための基本的施策について記載されているため、官民データを取り扱う場合に参照する。
4		サイバーセキュリティ基本法	サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。	-	スマートシティの推進に関わる全ての主体	-	・第十三条（国の行政機関等におけるサイバーセキュリティの確保） ・第十四条（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進） ・第十五条（民間事業者及び教育研究機関等の自発的な取組の促進）	サイバーセキュリティについて、基本理念、各主体の責務、戦略、施策について記載されている。
5		電波法（令和四年法律第七十号による改正）	電波の公平且つ能率的な利用を確保することによって、公共の福祉を増進することを目的とする。	-	スマートシティの推進に関わる全ての主体	同法で定められた基準を満たす無線通信を利用する場合	・第五十九条（秘密の保護） ・第百九条（罰則）	通信の秘密の保護について記載されているため、同法で定められた基準を満たす無線通信（ローカル５G等）利用する場合に参照する。なお、ローカル５Gを利活用する際は免許の取得が必要となる。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
6	ガイドライン（国内）	サイバー・フィジカル・セキュリティ対策フレームワーク	サイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」、様々なつながりによって新たな付加価値を創出する「Connected Industries」における新たなサプライチェーン全体のサイバーセキュリティ確保を目的とする	経済産業省	スマートシティの推進に関わる全ての主体	サービスや都市OS等がクラウドで構築されている場合	第Ⅱ部 ポリシー：リスク源の洗い出しと対策要件の特定 ２．リスク源と対策要件の対応関係	「企業間のつながり」「フィジカル空間とサイバー空間のつながり」「サイバー空間におけるつながり」の三層に分類して考える三層構造モデルの定義、及び本モデルに基づいたリスクアセスメント、リスクへの対策について記載されている。
7		パーソナルデータリファレンスアーキテクチャ	パーソナルデータを扱う全ての事業者、ステークホルダが、ビジネスモデルや内部統制などのシステム設計を行うためのガイドとなる設計書。	データ流通推進協議会 （※資料の発行元は上述の通りだが、同団体は2021年1月に「データ社会推進協議会」に改名されている）	スマートシティの推進に関わる全ての主体	パーソナルデータを取り扱う場合	・第6章 トラストサービスの概要と現状 ・第8章 リファレンスアーキテクチャ本体（設計部）	パーソナルデータの定義や、パーソナルデータ取扱事業者がアーキテクチャを設計する際のガイドが記載されているため、パーソナルデータを取り扱う場合に参照する。
8		政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）	国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している基準群。	内閣サイバーセキュリティセンター（NISC）	推進主体	-	・第2部 情報セキュリティ対策の基本的枠組み ・第3部 情報の取扱い ・第4部 外部委託 ・第5部 情報システムのライフサイ クル ・第6部 情報システムの構成要素 ・第7部 情報システムのセキュリティ要件 ・第8部 情報システムの利用	行政機関等にて求められるサイバーセキュリティに関する対策の基準が記載されている。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
9	ガイドライン（国内）	地方公共団体における情報セキュリティポリシーに関するガイドライン（令和5年3月版）	各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したガイドライン。	総務省	推進主体	地方公共団体としてスマートシティを推進する場合	・第 3 編 地方公共団体における情報セキュリティポリシー（解説） ・第4編 地方公共団体におけるクラウド利用等に関する特則（例文・解説）	各地方公共団体がセキュリティポリシーを策定・見直しする際のポイント等が記載されている。 令和5年3月版の改定では、元々あったISO27001で規定されているものとほぼ同等の対策基準に加えて、クラウドサービス利用におけるセキュリティの考え方、情報資産の廃棄・返却におけるポイントが加筆されている。
10		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	クラウド利用者の視点から JIS Q 27002（実践のための規範）の各管理策を再考し、クラウドコンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として，作成したガイドライン。	経済産業省	推進主体	クラウドサービスを利用のための管理を行う場合	・5 セキュリティ基本方針 ・6 情報セキュリティのための組織 ・7 資産の管理 ・8 人的資源のセキュリティ ・9 物理的及び管理的セキュリティ ・10 通信及び運用管理 ・11 アクセス制御 ・12 情報システムの取得、開発及び保守 ・13 情報セキュリティインシデントの管理及びその改善 ・14 事業継続管理 ・15 遵守	クラウドサービスを利用する際のリスク対応のための、目的、管理策、クラウド利用者のための実施の手引、そしてクラウド事業者の実施が望まれる事項について記載されている。
11		MaaS 関連データの連携に関するガイドライン Ver.3.0	MaaSに関連するデータの連携が円滑に行われることを目的として、各地域等のMaaSにおいて、関係者がデータ連携を行うにあたって参照すべき事項が整理されたガイドライン。	国土交通省	スマートシティの推進に関わる全ての主体	該当分野に関連するスマートシティサービスを提供する場合	・６．データ連携を行う上でのルール	MaaS に関連するプレイヤーがそれぞれの立場からデータ連携を行う際に留意すべき下記のような事項について記載されている。 ・移動関連データの取扱い ・個人情報・プライバシー保護対策 ・セキュリティ対策・不正利用対策、他

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
12	ガイドライン（国内）	電力制御システムセキュリティガイドライン	電力制御システム等のサイバーセキュリティ確保を目的として，電気事業者が実施すべきセキュリティ対策の要求事項について規定したガイドライン。	経済産業省	スマートシティの推進に関わる全ての主体	該当分野に関連するスマートシティサービスを提供する場合	・第4章 セキュリティ管理 ・第5章 設備・システムのセキュリティ ・第6章 運用・管理のセキュリティ ・第7章 セキュリティ事故の対応	電気事業者が実施すべきセキュリティ対策の要求事項について記載されている。
13		医療情報システムの安全管理に関するガイドライン第6.0版	医療情報システムの導入を検討若しくは決定する立場にある管理者等が、医療情報システムの安全管理や e-文書法への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したガイドライン。	厚生労働省	スマートシティの推進に関わる全ての主体	該当分野に関連するスマートシティサービスを提供する場合	全般	医療情報システムの安全管理や e-文書法への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものである。
14		ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第2版	エレベーターや空調など多くの制御系機器を有するビル分野に関して、ビルシステムに関するサイバーセキュリティの確保を目的に、そのサイバーセキュリティ対策の着眼点や具体的対策要件を体系的に整理したガイドライン。	経済産業省	スマートシティの推進に関わる全ての主体	該当分野に関連するスマートシティサービスを提供する場合	・3. ビルシステムにおけるサイバーセキュリティ対策の考え方 ・4. ビルシステムにおけるリスクと対応ポリシー	ビルシステムに対して考えられる脅威について、場所ごと、機器ごとに分類し、それぞれの場所や機器について考えられるインシデント、リスク源、その対策要件をポリシーレベルで記載されている。
15		安全なウェブサイトの作り方 改訂第7版	IPA が届出を受けたソフトウェア製品およびウェブアプリケーションの脆弱性関連情報に基づいて、特にウェブサイトやウェブアプリケーションについて、届出件数の多かった脆弱性や攻撃による影響度が大きい脆弱性を取り上げ、その根本的な解決策と、保険的な対策を示している。また、ウェブサイト全体の安全性を向上するための取り組みや、ウェブアプリケーション開発者が陥りやすい失敗例を紹介している。	情報処理推進機構（IPA）	サービス提供者	サービスとしてウェブアプリケーションを利用する場合	1．ウェブアプリケーションのセキュリティ実装 2．ウェブサイトの安全性向上のための取り組み	ウェブアプリケーションの脆弱性についての根本的解決策と保険的な対策、そしてウェブサイト全体の安全性を向上させるための取り組みについて記載されている。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
16	ガイドライン（国内）	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	クラウド事業者がクラウドサービスを提供する際に実施すべき情報セキュリティ対策のガイドラインであり、クラウド事業者が提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として、可能な限り分かりやすくかつ具体的な対策項目が提示されたガイドライン。	総務省	都市OSベンダ	サービスや都市OS等がクラウドで構築されている場合	・Ⅴ．４．３．リスク対応策導出マップ	クラウドの管理的及び物理的対策、IoTサービスと連携する場合におけるリスクとその対応方針に関連して、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について記載されている。
17		クラウドサービス提供・利用における適切な設定に関するガイドライン	クラウドサービス利用において設定不備に起因する情報漏えい等のインシデントを抑止・防止するため、クラウドサービス利用側、提供側それぞれで実施することが望ましい対策について記載したもの。	総務省	サービス提供者、データ提供事業者	サービスや都市OS等がクラウドで構築されている場合。	・Ⅱ．１．１　クラウドサービスにおける典型的なセキュリティ設定項目と設定不備があった場合のリスク ・Ⅲ．３．１　クラウドセキュリティに係る設定項目の確認	クラウドサービス利用側に求められる対策、および、クラウドサービス提供側に求められる対策として、設定不備の抑止・防止のための具体的な対策やベストプラクティスについて検討する際に参照する。
18		情報信託機能の認定に係る指針 Ver3.0	情報信託機能を提供する「情報銀行」について、民間の団体等による任意の認定の仕組みを有効に機能させるためのもので、消費者個人を起点としたデータの流通や消費者からの信頼性確保に主眼を置いて作成された指針。	情報信託機能の認定スキームの在り方に関する検討会	都市OSベンダ	情報銀行の認定を検討する場合	・Ⅲ情報信託機能の認定基準 １事業者の適格性 ２情報セキュリティ・プライバシー保護 ３ガバナンス体制 ４事業内容	情報銀行の定義、認定基準及び、認定スキームについて記載されており、情報銀行の認定を検討する場合に参照する。 2023年7月公表の最新版Ver3.0では、健康・医療分野の要配慮個人情報の取扱いに係る要件等を盛り込んでいる。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
19	ガイドライン（国内）	IoTセキュリティガイドライン	IoT 機器やシステム、サービスの供給者及び利用者を対象として、サイバー攻撃などによる新たなリスクが、モノの安全や、個人情報や技術情報などの重要情報の保護に影響を与える可能性があることを認識したうえで、IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめたガイドライン。	IoT推進コンソーシアム、総務省、経済産業省	データ提供事業者、IoT機器ベンダ	IoT機器を用いて、データ収集を行う場合。	第2 章 IoT セキュリティ対策の5つの指針	IoT特有の性質とセキュリティ対策の必要性を踏まえて、IoT機器やシステム、サービスについて、その関係者がセキュリティ確保の観点から求められる基本的な取組について記載されている。
20		CCDS製品分野別セキュリティガイドライン_スマートホーム編	本書では、下記の関連ガイドラインを参考に、スマートホーム分野としての必要可否を検討した上でセキュリティ要件の定義を行う。 - IoT推進コンソーシアム「IoTセキュリティガイドライン」 - 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」 - 英国「Code of Practice for consumer IoT security」 - 米国カリフォルニア州「接続される機器のセキュリティ法」(Senate Bill No.327 CHAPTER886)	重要生活機器連携セキュリティ協議会（CCDS）	データ提供事業者、IoT機器ベンダ	IoT機器を用いて、データ収集を行う場合。	全般	スマートホーム分野に特化し、IoT機器のセキュリティに関する脅威・リスク分析とそれを踏まえたセキュリティ対策（セキュリティ要件）について記載されている。
21		カメラ画像利活用ガイドブックver3.0	IoTの普及に伴い、データ利活用が増加する一方、プライバシーとデータセキュリティの懸念も高まっている。特にカメラ画像の扱いに注意が必要で、個人情報保護法を遵守し、適切なコミュニケーションが重要。事業者にプライバシー保護と信頼関係の強化を奨励している。	・経済産業省 ・総務省	・サービス提供者 ・データ提供事業者 ・IoT機器ベンダ	カメラ画像の利活用を検討する場合	・4.配慮事項	個人情報保護法等関係法令を遵守し、カメラ画像の利活用を検討する場合に参照する。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
22	ガイドライン（国内）	犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について	駅、空港等の不特定多数の者が出入りする大規模施設において、個人情報取扱事業者（主に民間事業者）が顔識別機能付きカメラシステムを導入・利用する際の留意する点等について、以下3点を柱として整理。 ・肖像権・プライバシーに関する留意点 ・個人情報保護法上の留意点 ・事業者の自主的な取組として考えられる事項	・個人情報保護委員会	・サービス提供者 ・データ提供事業者 ・IoT機器ベンダ	個人情報取扱事業者が顔識別機能付きカメラシステムを導入する場合	・第4章 肖像権・プライバシーに関する留意点 ・第5章 顔識別機能付きカメラシステムを利用する際の個人情報保護法上の留意点	個人情報保護法の遵守や肖像権・プライバシー侵害を生じさせないための観点から少なくとも留意するべき点や、被撮影者や社会から理解を得るために自主的に取り組むべき事項について整理されており、個人情報取扱事業者が顔識別機能付きカメラシステムを導入する場合に参照する。
23		DX時代における企業のプライバシーガバナンスガイドブックver1.3	Society 5.0構想においてデータ活用によるイノベーション促進や新規事業に取り組む企業・関連企業に、プライバシーガバナンスの構築と信頼の獲得に役立つステップを提供する。また、個人情報保護法の改正に加え、パーソナルデータの利活用に焦点を当てている。	・経済産業省 ・総務省	・サービス提供者 ・データ提供事業者	パーソナルデータを利活用している企業や、そのような企業と取引をしているベンダー企業である場合。	・3.経営者が取り組むべき三要件 ・4.プライバシーガバナンスの重要項目	パーソナルデータを利活用して、消費者へ製品・サービス等を提供する中で、消費者のプライバシーへの配慮を消費者から直接要請される可能性のある企業や、そのような企業と取引をしているベンダー企業等である場合に参照する。
24		民間PHR事業者による健診等情報の取扱いに関する基本的指針	安全、安心な民間PHR（Personal Health Record）サービスの利活用の促進に向けて、健診等情報を取り扱う事業者によるPHRの適正な利活用が効率的かつ効果的に実施されることを目的として、PHRサービスを提供する事業者が遵守すべき事項を示すもの。	・経済産業省 ・総務省 ・厚生労働省	・サービス提供者 ・データ提供事業者	適正なPHRの利活用を促進するための遵守事項を確認する場合。	・2.情報セキュリティ対策 ・3.個人情報の適切な取扱い ・4.健診等情報の保存及び管理並びに相互運用性の確保	要配慮個人情報である健診等情報を取り扱うこととなるサービスを提供する民間事業者が法規制により遵守を求められている事項に加えて、適正なPHRの利活用を促進するために遵守することが必要と考えられる事項を確認する場合に参照する。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
25	ガイドライン（国内）	スマートシティデータガバナンスガイドライン―スマートシティ実装におけるデータ利活用の考え方―	スマートシティにおいて、ICTやデータ活用を先行させるのではなく、「人間中心」の本来の価値を創出できるよう、スマートシティの推進におけるデータガバナンスの考え方をとりまとめたもの。スマートシティにおけるデータの取扱いに関するルールを定め、これに基づき適切な利活用をコントロールする仕組みであり、それ自体が市民や社会の意識や認識との差異が生じないようにするプロセスを内包することで、適切なスマートシティの推進に貢献する。	東京大学未来ビジョン研究センター 教授/データガバナンス研究ユニット 渡部俊也 株式会社日立コンサルティング ディレクター 美馬正司	スマートシティ推進組織	データ活用してスマートシティサービスを提供する場合	・2.3 スマートシティの推進組織 ・3.5. トラストの考え方 ・3.6. DFFT ・5.3. リスク分析 ・5.4. ルールの設計 ・参考資料 プライバシーリスクの内容	スマートシティ推進組織が多様なステークホルダに対するデータガバナンスを効かせる場合の、考え方やプロセスについて検討する際に参照する。 特に、スマートシティ推進組織がガバナンスを効かせる際に必要な機能について整理されている。
26		IOTセキュリティ手引書	IoT機器のセキュリティ対策に対して、国際的なセキュリティ標準規格として、国際電気標準会議（IEC）が開発した産業システムにおけるセキュリティ規格であるIEC62443のうち産業機器開発者向けの規格であるIEC62443-4と米国立標準技術研究所（NIST）が発行する「非連邦政府組織およびシステムにおける管理対象非機密情報CUIの保護」を目的としたSP800-171rev.2を基準に、業界基準の解釈と国際標準の差異を取りまとめたもの。	一般社団法人セキュアIoTプラットフォーム協議会 セキュリティ仕様検討部会	IoTクラウドサービス事業者、IoTクライアントデバイス製造事業者、およびこれらの機能を活用しカスタマーへトータルのサービスとして供給する事業者	IoT機器を活用してスマートシティサービスを提供する場合	2.1 IoT システムの階層モデル 3.1 企画フェーズ 3.2 アーキテクチャ設計フェーズ 3.3 ハードウェア設計フェーズ 3.4 S/W 設計フェーズ	スマートシティアセットのデータ収集用IoT機器の企画～設計～選定～製造～調達～運用～破棄（リサイクル含む）の各フェーズにおけるセキュリティ対策項目を検討する際に参照する。
27		FIPS140-3を取り巻く環境に対する考察	米国標準技術研究所（NIST：National Institute of Standards and Technology）が制定した、暗号モジュールに関する標準規格FIPS140-3に着目し、米国政府の動きや民間の取組みをまとめた考察。	一般社団法人セキュアIoTプラットフォーム協議会 理事長 辻井重男	暗号モジュールの安全な設計、実装、運用に関連する開発者向け。	コンピュータおよび電気通信システムにおいて機密情報を保護するための暗号モジュールとして、またセンサーからクラウドサービスにおける安全なデータ伝送を行う上に遵守する国際標準規格。	-	FIPS140-3はIoT機器等のハードウェアだけでなく、システム全体やクラウドサービスにも対応が必要。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
28	ガイドライン（国内）	2022年海外における「スマートシティ×プロジェクト」に関する網羅的な調査	36か国を中心に、海外における「スマートシティ×プロジェクト（公開事例）」の網羅的な調査を実施（200件）	未来トレンド研究機構	スマートシティにこれから主体的に取り組もうとする自治体や企業 スマートシティ関連のサービスを提供しようと考えている全ての企業	日本にはないスマートシティサービスのメカニズムの解明 日本国内の法律や規制によって実現できないスマートシティサービスのメリットやサービスモデルの研究	2-37. 海外・スマートシティプロジェクト＜北米分野×ヒューストン：消防ドローンによる安全管理×Huston Smart City of the Future＞ 2-38. 海外・スマートシティプロジェクト＜北米分野×ヒューストン：洪水検知センサによるリアルタイム通知×Huston Smart City of the Future＞	日本にはないスマートシティサービスにおけるセキュリティリスクの把握と、予見されるリスク対策立案に有効であることが期待される。
29		スマートシティリファレンスアーキテクチャ（ホワイトペーパー）（第2版）	スマートシティのアーキテクチャ（設計思想、設計方法、実現方式等）を各主体が決定していく際に参照するもの（リファレンスアーキテクチャ）。	戦略的イノベーション創造プログラム（ＳＩＰ）第2期ビッグデータ・AIを活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究事業	「スマートシティに主体的に取り組む自治体、企業、地域協議会・エリアマネジメント団体」 「スマートシティ関連のサービスを提供する企業」「スマートシティの推進に関わる国やアカデミア」	スマートシティに主体的に取り組もうとする場合	4. スマートシティルール 5. 都市マネジメント 7. 都市OS 8. スマートシティアセットと他システム	都市OSのアーキテクチャの構成要素として「セキュリティ」があり、「技術機能ブロック」「管理機能ブロック」から構成されている。 ・技術機能ブロック：認証、暗号化、不正アクセス防止など ・管理機能ブロック：教育、ルール、セキュリティ監査など
30		スマートシティリファレンスアーキテクチャの使い方（導入ガイドブック）（第2版）	スマートシティリファレンスアーキテクチャ（ホワイトペーパー）を理解し活用しやすくするため、図などを用いながら平易な解説に努めたもの。	内閣府	スマートシティにこれから主体的に取り組もうとする自治体や企業 スマートシティ関連のサービスを提供しようと考えている全ての企業 日本のスマートシティの在り方に関して検討を行う国、企業やアカデミア	スマートシティに主体的に取り組もうとする場合	第3章 スマートシティアーキテクチャのつかい方 必要なルールを確認、整備しよう 誰がどんな役割を果たすべきか整理しよう 都市OS（データとAPI）を準備しよう	セキュリティを含む、スマートシティを検討する上で必要な項目をチェックすることが出来る。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
31	ガイドライン（国内）	スマートシティガイドブック（第２版）	スマートシティに取り組む地方公共団体、協議会等の取組を支援するため、先行してスマートシティに取り組む地域における成功・失敗体験等を踏まえつつ、スマートシティの意義・必要性、導入効果、及びその進め方等についてガイドブックとしてとりまとめたもの。	内閣府・総務省・経済産業省・国土交通省 スマートシティ官民連携プラットフォーム事務局	主に、これからスマートシティの取り組みを始めようとする地方公共団体の首長、職員等を想定するほか、地方公共団体のパートナーとなるべき民間企業・大学等の担当者など	スマートシティに主体的に取り組もうとする場合	２－２．スマートシティを進める上でのポイントと対応の考え方 ・推進主体における実行力の強化 ・プロジェクトを牽引し、調整する組織・人材の確保 ・推進主体のガバナンスの明確化 ・データ取り扱いルールの明確化 ・都市 OS の導入	スマートシティの国内事例から、セキュリティ面での施策を確認することが出来る。 レジリエンス（回復力）について触れられており、有事の際の最適な対応について記載されている。
32		分野間データ連携基盤「CADDE」に係る主要機能の外部仕様書	分野・組織を超えたデータ連携を実現する分野間データ連携基盤「CADDE」の普及促進を最終的な目的として、CADDE に係る主要機能の外部仕様を示すもの	「分野間データ連携基盤技術の社会実装に向けた外部仕様書の作成・公開および相互接続性実証」プロジェクトの受託事業者（日本電気株式会社、大学共同利用機関法人情報・システム研究機構国立情報学研究所、株式会社日立製作所）	CADDE へ参加するデータ提供者やデータ利用者、CADDE に接続するサービスを提供する者、CADDE モジュールの機能等を強化して、OSS や製品ソフトウェアとしてリリースを行う者、CADDE の外部仕様（API 仕様）を参考にして新たなデータ連携基盤の仕様を策定する者	CADDE を利用する場合、CADDE を参考に新たなデータ連携基盤の使用を策定する場合	全般	外部に位置する都市 OS 間のデータやスマートシティサービスを連携する際に必要な支援サービスについて記載されている。 特にセキュリティに関しては、認証許可・契約管理・証明書登録・ロケーション管理などの機能に関して記載されている。
33		ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 Ver. 1.0	ソフトウェア管理に向けた SBOM の作成・共有・運用・管理に関する様々な課題の解決するために、SBOM に関する基本的な情報を提供し、ソフトウェアサプライヤーにおける一連の SBOM 導入に向けたプロセスを示す手引き。	・経済産業省	・サービス提供者 ・データ提供事業者	ソフトウェアを利活用した製品・サービスの安全・安心を担保するために、利活用するソフトウェアの脆弱性の管理が求められる場合。	・6. SBOM 運用・管理フェーズにおける実施事項・認識しておくべきポイント	企業における効率的・効果的な SBOM 導入を支援するために、各フェーズにおける主な実施事項や SBOM 導入に当たって認識しておくべきポイントについて記載されている。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
34	ガイドライン（国内）	EU サイバーレジリエンス法（草案概要）	EU が 2025 年後半の適用を目指すサイバーセキュリティ規制。例外を除き、デジタル要素を備えたすべての製品が対象。SOM 作成や更新プログラム提供等、セキュリティ要件への適合が求められる。	・経済産業省	・サービス提供者 ・データ提供事業者 ・IoT 機器ベンダ	デジタル製品（デジタル要素を備えた製品で、デバイスやネットワークに直接的／間接的に接続されるものを含む）を開発・展開する場合。	・製造業者の義務（10 条） ・製造業者の報告義務（11 条） ・全てのデジタル製品に求められるセキュリティ特性要件（附属書 I）	デジタル製品を市場に出す際の製造業者の義務や、インシデント確認時の報告義務について確認する際に参照する。
35		データ連携基盤に求められる互換性・安全性・プライバシーに関する事項	スーパーシティやスマートシティ等に関するガイドライン等で示されているデータ連携基盤に求められる事項について、①相互運用性の確保（互換性）、②セキュリティ対策（安全性）、③プライバシー対策の観点から整理している。	・内閣府	・サービス提供者 ・データ提供事業者	データ連携基盤を構築する場合。	・（参考）求められる事項一覧 ② セキュリティ対策（安全性） －1. システム要件 －2. ガバナンス要件 ③ プライバシー対策 －1. 個人情報保護法令の確実な遵守 －2. 法令遵守に加えて求められる事項	スーパーシティやスマートシティ等に関するガイドライン等にて示されているデータ連携基盤におけるセキュリティ対策の要求事項が整理して提示されている。
36		行政手続におけるオンラインによる本人確認の手法に関するガイドライン	デジタル・ガバメント実行計画に基づき、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」を見直し、各種行政手続きをデジタル化する際に必要となるオンラインでの本人確認に対する考え方及び手法をまとめたもの。	・デジタル庁	・サービス提供者 ・データ提供事業者	本人確認が必要な行政手続のうち、個人・法人等と政府との間の申請・届出等のオンライン手続きをする場合。	全般	個人および法人別に、オンラインによる本人確認が求められる際の要件が整理されており、手法例や実現できること・特徴を確認することができる。
37		民間事業者向けデジタル本人確認ガイドライン第 1.0 版	自社サービスの特徴に応じた本人確認手法を選択するためのガイドブックとして以下を記載。 ①本人確認の導入・選択に必要な基礎知識のまとめ ②本人確認手法の特徴の整理 ③マイナンバーカードや本人確認をめぐる最新動向等の紹介	・デジタル庁	・サービス提供者 ・データ提供事業者	本人確認が導入されるサービスを構築する場合。	全般	既存の身元確認手法の課題を解決する、事業者・ユーザ負担を軽減する中間的な手法について紹介されている。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
38	ガイドライン（国内）	データ品質管理ガイドブック	データが利用に適していることを確認し、データ利用者のニーズを満たすために、データに品質管理技術を適用する活動の計画、実装、および制御	・デジタル庁	データを管理または利用する組織や個人全般	データ品質の向上を目指す場合や、データ品質に問題や課題が発生した場合、データ連携やデータ共有を行う場合、データガバナンスの構築時	2．3 データの評価 2．5 データ管理プロセスの評価	データの品質を管理するに当たり、セキュリティ面での考慮が必要であることが記述されている。
39	法律・法令（海外）	一般データ保護規則（GDPR）	「EU 基本権憲章」において保障されている、個人データの保護に対する権利という基本的人権の保護を目的とし、欧州経済領域（EEA）の個人データの処理、および個人データを EEA から第三国に移転するために満たすべき法的要件を規定した法律。	-	スマートシティの推進に関わる全ての主体	EEA 域内の個人データを取り扱う場合	・第 5 条 個人データの取扱いと関連する基本原則 ・第 24 条 管理者の責任 ・第 32 条 取扱いの安全性	個人情報取扱事業者としての義務等が記載されているため、EEA 域内の個人データを取り扱う場合に参照する。
40	ガイドライン（海外）	NIST SP 800-53	連邦政府組織に対するセキュリティ管理策、およびプライバシー管理策を合わせて提示する文書であるとともに、さまざまな脅威からミッション・機能・イメージ・評判・業務・資産・個人・他組織・国家を保護するために管理策を選択するプロセスを提示する文書。	米国国立標準技術研究所（NIST）	スマートシティの推進に関わる全ての主体	組織内のセキュリティを向上させる場合	全般	プライバシー管理、及びセキュリティ管理について網羅的に記載されているため、セキュリティ向上を施策する場合に参照する。
41		ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements	情報セキュリティマネジメントシステム（ISMS）を確立し、実施し、維持し、継続的に改善するための要求事項を提供することを目的として作成された国際規格。ISMS は，リスクマネジメントプロセスを適用することによって情報の機密性，完全性及び可用性を維持し，かつ，リスクを適切に管理しているという信頼を利害関係者に与える。	国際標準化機構	スマートシティの推進に関わる全ての主体	組織内のセキュリティを向上させる場合	全般	保護すべき各情報資産に対して機密性、完全性、可用性についてのセキュリティ対策がバランスよく記載されているため、セキュリティ向上を施策する場合に参照する。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
42	ガイドライン（海外）	ISO/IEC 27017	クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針を提示する国際規格。	国際標準化機構	スマートシティの推進に関わる全ての主体	クラウドサービスに関するリスク低減を考える場合	全般	ISO27001に加えクラウドサービスのセキュリティ対策について記載されているため、クラウドサービスに関するリスク低減を考える場合に参照する。
43		ISO/IEC 62443-4	制御システムセキュリティ標準の国際規格。 そのうち、IEC62443-4は「概要」「ポリシー、手順」「システム」「コンポーネント」のうちの「コンポーネント」という構成要素に該当する。	・国際標準化機構（ISO）	制御関連製品の製品供給者（機器のサプライヤー）	IoT機器を用いて、データ収集を行う場合。	第2章 IoT セキュリティ対策の5つの指針	IoT特有の性質とセキュリティ対策の必要性を踏まえて、IoT機器やシステム、サービスについて、機器のサプライヤーがセキュリティ確保の観点から求められる対策について記載されている。
44		Cybersecurity Best Practices for Smart Cities	スマートシティは悪意のあるサイバー攻撃者にとって魅力的なターゲットであり、完全に安全なテクノロジーソリューションは存在しない。このガイダンスは、コミュニティがスマートシティテクノロジーを導入する際に、効率とイノベーションとサイバーセキュリティ、プライバシー保護、国家安全保障のバランスを取るための推奨事項を提供する。	・米国サイバーセキュリティ・インフラストラクチャーエージェンシー（CISA） ・米国国家安全保障局（NSA） ・米国連邦捜査局（FBI） ・イギリス国立サイバーセキュリティセンター（NCSC-UK） ・カナダサイバーセキュリティセンター（CCCS） ・ニュージーランド国立サイバーセキュリティセンター（NCSC-NZ）	・スマートシティの推進に関わる全ての主体	特定のサイバーセキュリティ要件に合わせてベストプラクティスを実装する場合	全般	組織がインフラストラクチャシステムの安全かつ確実な運用、国民の個人データの保護、政府および企業の機密データのセキュリティを確保するために、特定のサイバーセキュリティ要件に合わせてベストプラクティスを実装する場合に参照する。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
45	ガイドライン（海外）	ISO/IEC TS 27570:2021 Privacy protection – Privacy guidelines for smart cities	スマートシティにおけるプライバシー保護に関する国際的なガイドライン。スマートシティプロジェクトやイニシアティブにおいてプライバシーを守るための指針を提供し、個人情報の収集、処理、保護に関するベストプラクティスを示している。スマートシティのデータ利活用に伴うプライバシーの課題に対処し、市民の権利とプライバシーを守るための枠組みを提供している。	・国際標準化機構（ISO） ・国際電気標準会議（IEC）	・スマートシティの推進に関わる全ての主体	スマートシティ環境でサービスを提供する場合。	全般	以下の観点の指針を提供している。 ・スマートシティエコシステムのプライバシー保護。 ・市民の利益のために標準がグルーバルレベルや組織レベルでどのように活用できるか。 ・スマートシティエコシステムのプライバシー保護のためのプロセス。 公共及び民間企業、政府機関、および非営利団体を含む、スマートシティ環境でサービスを提供するあらゆる種類と規模の組織に適用される。
46		NIST SP800-63-4	デジタルアイデンティティのセキュリティガイダンス。オンライン認証、アイデンティティ管理、パスワードセキュリティ、多要素認証、生体認証、プライバシー保護などに関する技術的な指針を提供し、デジタルアイデンティティのセキュリティ向上に有用。	・アメリカ合衆国国立標準技術研究所（NIST）	・サービス提供者 ・データ提供事業者	外部ユーザーとやり取りする組織サービスを取り扱う場合。	全般	公共サービスにアクセスする市民やコラボレーションスペースにアクセスする民間セクターのパートナーなど、外部ユーザーとやり取りする組織サービスを取り扱う場合に参照する。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
47	ガイドライン（海外）	ISO 37120:2018 持続可能な都市及びコミュニティー都市サービス及び生活の質の指標 Sustainable cities and communities -- Indicators for city services and quality of life	ISO37120は、2014年5月に国際標準化機構（ISO）が「維持可能な共同体の発展－都市サービス及びQoL（クオリティ・オブ・ライフ）に関する指標として認定した国際標準。都市サービスと生活の質の指標であり、19分野、111項目の指標で構成。	World Council on City Data（WCCD）が作成し、国際標準化機構（ISO）が認定した国際標準	都市インフラ設計や都市サービス設計を行う行政向け。	持続可能な都市及びコミュニティー都市サービス及び生活の質の指標	10章：ガバナンス（Governance） 15章：安全（Safety） 18:通信、技術革新（Telecommunication）	他都市と比較して低い数値が検出された分野・項目を脆弱な部位と意識し、重点的に強化する施策のプライオリティ付けに役立つ。
48		ISO 37122:2019 持続可能な都市及びコミュニティースマートシティの指標 Sustainable cities and communities -- Indicators for smart cities	ISO37122は、2019年5月に公開された、スマートシティ指標規格であり、ISO37120の補助規格。 スマートシティの政策、計画、プロジェクトを分析するための指標であり、19分野、80項目の指標で構成。	World Council on City Data（WCCD）が作成し、国際標準化機構（ISO）が認定した国際標準	都市インフラ設計や都市サービス設計を行う行政向け。	持続可能な都市及びコミュニティースマートシティの指標	6章：ガバナンス（Governance） ・市の非緊急照会システムを通じて行われた問合せに対する平均応答時間 ・都市のITインフラストラクチャの平均ダウンタイム 11章：安全（Safty） ・デジタル監視カメラでカバーされている市街地の割合	他都市と比較して低い数値が検出された分野・項目を脆弱な部位と意識し、重点的に強化する施策のプライオリティ付けに役立つ。
49		ISO 37123:2019 持続可能な都市およびコミュニティー回復力のある都市 Sustainable cities and communities -- Indicators for resilie	ISO37122は、2019年12月に公開された、レジリエントシティ指標規格であり、ISO37120の補助規格。 都市のレジリエンスに関する指標の定義と算出方法などを定めた規格。都市が直面するリスクを把握し、リスクへの脆弱（ぜいじゃく）性を特定して対策立案に役立つ規格。	World Council on City Data（WCCD）が作成し、国際標準化機構（ISO）が認定した国際標準	都市、自治体、地方政府などの防災・復興担当者。	持続可能な都市およびコミュニティー回復力のある都市	10章：ガバナンス（Governance） ・市の電子データのうち、安全で遠隔地にバックアップ保管されているデータの割合 ・事業継続計画を文書化している主要サービス提供者の割合 15章：安全（Safty） ・マルチハザード早期警報システムがカバーする市人口の割合 18章：テレコミュニケーション（Telecommunication） ・災害発生時に信頼できる専門通信技術を備えた緊急対応要員の割合 19章：交通（Transportation） ・避難経路の数	他都市と比較して低い数値が検出された分野・項目を脆弱な部位と意識し、重点的に強化する施策のプライオリティ付けに役立つ。

項番	カテゴリ	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
		nt cities						
50	ガイドライン（海外）	Cybersecurity Labeling Program	家庭に持ち込まれているテクノロジーが合理的に安全であるという安心感を消費者に提供し、通信に対するリスクを防ぐために、消費者にわかりやすくアクセス可能な情報を提供する自主的なサイバーセキュリティラベルプログラムを提案。	・米国連邦通信委員会（FCC）	・IoT機器ベンダ	無線インターフェースを備えたIoTデバイスを利活用した製品・サービスを展開する場合。	全般	セキュリティ対策が施されているコンシューマーデバイスに関する認証制度であり、スマートシティ上で活用するIoT製品などの安全性を確認することが出来る。
51		ISO/IEC 23751(Data sharing agreement (DSA) Framework)	クラウドコンピューティングと分散プラットフォームにおける、データ共有合意（DSA）の枠組みを示した規格	・国際標準化機構（ISO）	データを共有する複数組織	データを複数組織で共有するケースにおいて、それによって生じる様々なタスクや課題を整理するケース	・（参考）求められる事項一覧 ② セキュリティ対策（安全性） －1. システム要件 －2. ガバナンス要件	データを複数組織で共有するケースにおいて、タスクや課題を整理するための勘所を提示し、時間とコストを削減する一助となる。

【Appendix】B　セキュリティ上のリスク一覧

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
(なりすまし等をした)ソシキ/ヒト/モノ等から不適切なデータを受信する	・不正な組織/ヒト/モノ/システムによる正規エンティティへのなりすまし・改ざん等された正規なモノ/システムからの適切でないデータの受信	・自組織の保護すべきデータのセキュリティ上の扱いについて、外部委託先の担当者が十分に認識していない	CPS.AT-2 CPS.AT-3
		・データを収集・分析等するシステムにおいて、対処すべき脆弱性が放置されている	CPS.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.RA-2 CPS.CM-6 CPS.CM-7 CPS.SC-12
		・通信路が適切に保護されていない	CPS.DS-3
		・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みが自組織のシステムに実装されていない	CPS.AE-1 CPS.CM-1 CPS.CM-5 CPS.RP-1 CPS.PT-1
		・サイバー空間との通信開始時に、通信相手を識別・認証していない	CPS.AC-1 CPS.AC-3 CPS.AC-4 CPS.AC-8 CPS.AC-9
		・通信相手のエンドポイントから送信されるデータをフィルタリングする仕組みが導入・運用されていない	CPS.CM-3 CPS.CM-4
		・データ送信元となるデータの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14
(監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗難等の後)改ざんされた IoT 機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施された IoT 機器によるネットワーク接続・悪意を持った自組織内外のヒトによる不正改ざん・センサーの測定値、閾値、設定の改ざん	・利用している機器に耐タンパー性がなく、物理的な改ざんを防げない	CPS.DS-8
		・定期的に接続機器の完全性を検証していない	CPS.DS-10 CPS.DS-12
		・不正な機器がネットワークに接続されたことを適切に検知できない。	CPS.AM-1 CPS.CM-6
		・IoT 機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	CPS.AC-2 CPS.CM-2 CPS.IP-5 CPS.PT-2

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
(監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗難等の後)改ざんされた IoT 機器がネットワーク接続され、故障や正確でないデータの送信等が発生する（再掲）	・盗難等により不正な改造を施された IoT 機器によるネットワーク接続・悪意を持った自組織内外のヒトによる不正改ざん・センサーの測定値、閾値、設定の改ざん（再掲）	・IoT 機器の廃棄時に、データを削除（または読み取りできない状態に）する手順がない	CPS.IP-6
		・自組織の情報システムや産業用制御システムに接続している機器の状態を把握できていない	CPS.AM-1 CPS.CM-6 CPS.IP-1
		・自組織内外のヒトによる IoT 機器に対する物理的な不正行為を防げない	CPS.AC-2 CPS.CM-2 CPS.SC-5
サービス拒否攻撃、ランサムウェアへの感染等により、自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバ等の電算機器、通信機器等に対するサービス拒否攻撃・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・妨害電波の発信	・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	CPS.AM-6 CPS.BE-2 CPS.IP-3 CPS.SC-1 CPS.SC-2 CPS.SC-12 CPS.SC-13 CPS.SC-14
		・自身が関わりうるセーフティやセキュリティに関わるリスクに対して十分な認識を有していない	CPS.AT-1 CPS.AT-3
		・ヒトに関わるセーフティやセキュリティに関係するリスクに対するガバナンスが十分でない	CPS.SC-8 CPS.IP-9
		・情報システムや産業用制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理（例：資産の棚卸し、モニタリング）されていない	CPS.AC-1 CPS.AE-1 CPS.AM-1 CPS.AM-5 CPS.CM-5 CPS.CM-6
		・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	CPS.RA-1 CPS.RA-3 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.RM-2
		・IoT、サーバ等に対する通信を適切に制御していない	CPS.CM-1 CPS.PT-2
		・IoT、サーバ等に対する物理的な妨害（例：妨害電波）に対処できていない	CPS.AC-2 CPS.CM-2 CPS.IP-5
		・IoT 機器を含むシステムに十なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	CPS.DS-6 CPS.DS-7
		・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	CPS.GV-1 CPS.GV-4 CPS.IP-7 CPS.RM-1 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-10 CPS.SC-11 CPS.SC-12 CPS.SC-13 CPS.SC-14

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する	・システムを構成するサーバ等の電算機器、通信機器等に対するサービス拒否攻撃・妨害電波の発信	・データの収集先、加工・分析等の依頼先の組織の信頼を契約前、契約後に確認していない	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14
		・IoT 機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	CPS.DS-6 CPS.DS-7 CPS.IP-4
		・IoT 機器の停止を検知した後の対応手順が定義されていない	CPS.RP-1
サイバー空間におけるデータ保護を規定する法規制等への違反が発生する	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・データ保管エリアに対する不正なエンティティの物理的な侵入・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし	・保護すべきデータの管理に関する組織内の責任が明確でない	CPS.AM-6
		・対応が必要なデータ保護に関する法規制等を十分に認識してない	CPS.GV-3 CPS.SC-13
		・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない	CPS.AT-1 CPS.AT-3
		・データの取扱いについて、必要なプロシージャを規定していない	CPS.GV-3
		・データの取扱いについて、必要なプロシージャを満たしているかを確認していない	CPS.DS-14
		・複数の組織、システム等に個人情報等が分散して所在している	CPS.SC-3 CPS.SC-6
		自組織で扱うデータの保護が必要な特定の種類のデータであることが識別されていない	CPS.DS-1
データが IoT 機器・サイバー空間間の通信路上で改ざんされる	・通信系路上でデータを改ざんする中間者攻撃等	・機器を調達する際、改ざん検知機能及び改ざん防止機能を実装しているかを確認していない	CPS.DS-15 CPS.SC-4
データ加工・分析システムが誤動作することで、適切でない分析結果が出力される	・データ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・データ加工・分析システムに対する攻撃コードを含んだ許容範囲外のインプットデータ	・データを加工・分析する組織、システム等の安全性・信頼性を契約前、契約後に確認していない	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
データ加工・分析システムが誤動作することで、適切でない分析結果が出力される（再掲）	・データ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・データ加工・分析システムに対する攻撃コードを含んだ許容範囲外のインプットデータ（再掲）	・データを加工・分析するシステムにおいて、セキュアでない設定がなされている	CPS.CM-6 CPS.CM-7 CPS.IP-1 CPS.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.PT-2 CPS.RA-2
		・システム上でデータが十分に保護されていない	CPS.DS-2 CPS.DS-3 CPS.DS-4
		インプットとなるデータを十分に確認していない	CPS.CM-3 CPS.CM-4
		・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	CPS.AE-1 CPS.CM-1 CPS.CM-5 CPS.PT-1 CPS.RP-1
遠隔から IoT 機器を管理するシステムに不正アクセスされ、IoT 機器に不正な入力をされ、事前に想定されていない動作をする	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし・IoT 機器を管理するシステムから IoT 機器への不正なコマンド送信	・IoT 機器を管理するシステムのセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない	CPS.CM-6 CPS.SC-12
		・システム管理権限に対するアクセス制御が十分でない	CPS.AC-5 CPS.AC-6
		・システムにおいて対処すべき脆弱性が適切に対処されていない	CPS.CM-6 CPS.CM-7 CPS.IP-2 CPS.MA-1 CPS.MA-2 CPS.RA-2 CPS.SC-12
		・IoT 機器の誤動作を検知した後の対応手順が定義されていない	CPS.RP-1
関係する他組織で管理している(データ加工分析)領域から自組織の保護すべきデータが漏えいする	・他組織の管理するデータ加工分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・他組織の管理するデータ加工分析エリアに対する不正なエンティティの物理的な侵入窃取した ID、パスワード等を利用した正規ユーザへのなりすまし・他組織のエンティティによる保護すべきデータの適切でない持出行為	・データを加工・分析する組織、システム等の安全性・信頼性を契約前、契約後に確認していない	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
関係する他組織で管理している(データ加工・分析)領域から自組織の保護すべきデータが漏えいする（再掲）	・他組織の管理するデータ加工・分析システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・他組織の管理するデータ加工・分析エリアに対する不正なエンティティの物理的な侵入・窃取したID、パスワード等を利用した正規ユーザへのなりすまし・他組織のエンティティによる保護すべきデータの適切でない持出行為（再掲）	・データの加工・分析を委託する組織における要員の信頼性を契約前、契約後に確認していない	CPS.SC-5
		・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	CPS.SC-3 CPS.SC-6
		・データを保管する組織、システム等の安全性を契約前、契約後に確認していない	CPS.SC-2 CPS.SC-3 CPS.SC-6 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14
		・データの加工を委託する組織における要員の信頼性を契約前、契約後に確認していない	CPS.SC-5
		・セキュリティ水準が統一されていない複数の組織、システム等に自組織の保護すべき情報が分散して所在している	CPS.SC-3 CPS.SC-6
関係する他組織で使用中の自組織の保護すべきデータが改ざんされる	・窃取したID、パスワード等を利用した正規ユーザへのなりすまし・通信系路上でデータを改ざんする中間者攻撃等	・通信路上でデータが十分に保護されていない	CPS.DS-3 CPS.DS-4
		・使用中のデータに改ざんを検知するメカニズムがない	CPS.DS-11
		・保管中のデータに改ざんを検知するメカニズムがない	CPS.DS-11
関係する他組織のセキュリティインシデントにより自組織が適切に事業継続できない	All threats	・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	CPS.AE-1 CPS.AM-4 CPS.AM-5 CPS.CM-5 CPS.CM-6
		・自組織と他組織(サプライヤ等)とのフィジカル空間における連携状況および責任分界を把握していない	CPS.AM-7 CPS.BE-1 CPS.BE-3 CPS.RM-1
		・自組織のヒトが他組織のセキュリティ事象発生時に適切なアクションを取ることができない	CPS.AT-1 CPS.AT-3 CPS.RP-2
		・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	CPS.RP-2
計測機能に対する物理的な不正行為により、正確でないデータの送信等が発生する	・悪意を持った自組織内外のヒトによる計測機能に対する不正行為	・IoT機器を調達する際、調達製品が計測セキュリティを考慮しているものかを確認していない	CPS.SC-4 CPS.SC-6 CPS.DS-15
		・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	CPS.AC-2 CPS.CM-2 CPS.IP-5

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
攻撃の有無に関わらず、データを取り扱うシステムが停止する	・品質や信頼性の低いシステムによるサービス提供	・サービスサプライヤに対して、組織、システム等の信頼性を契約前、契約後に確認していない	CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14
		・IoT 機器を含むシステムに十分なリソース(処理能力、通信帯域、ストレージ容量)が確保されていない	CPS.DS-6 CPS.DS-7 CPS.IP-4
		・サービスサプライヤに対して、組織、システム等の信頼性を契約前、契約後に確認していない	CPS.SC-2
正規のユーザになりすまして IoT 機器内部に不正アクセスされ、事前に想定されていない動作をする	・窃取した ID 等を利用した正規ホストへのなりすまし・セキュリティが実装されていない脆弱なプロトコルを悪用した不正アクセス	・ネットワークの適正利用を確認していない	CPS.AE-1 CPS.CM-1 CPS.PT-1
		・セキュリティの観点において強度が十分でない設定(パスワード、ポート等)がなされている	CPS.IP-1 CPS.PT-2
		・通信相手に対するアクセス制御が十分でない	CPS.AC-4 CPS.AC-7 CPS.AC-8 CPS.AC-9
		・IoT 機器のセキュリティ設定手順が定められていない	CPS.IP-1
		・IoT 機器の誤動作を検知した後の対応手順が定義されていない	CPS.RP-1
正常動作・異常動作に関わらず、安全に支障をきたすような動作をする	・不正なエンティティによるコマンドインジェクション攻撃・サイバー空間からの許容範囲外のインプットデータ・マルウェアによる制御信号の改ざん	・機器を調達する際、安全性を実装しているかを確認していない	CPS.PT-3 CPS.RA-4 CPS.SC-4 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14
		・インプットされたデータを検証する仕組みが無い	CPS.CM-3
		・稼動するシステムとして、安全計装が考慮されていない。	CPS.RA-4 CPS.RA-6
		・安全に支障をきたしうる機器等の兆候を発見した際のプロシージャが定められていない	CPS.RP-1
製品・サービスの提供チャネルでセキュリティ事象が発生し、機器の破損等の意図しない品質劣化が生じる	・悪意を持った自組織内外のヒトによる不正改ざん・正規の機器を模した偽造品の挿入	・製品・サービスの調達時に、調達品の適格性を確認するプロシージャが存在しない	CPS.DS-11 CPS.DS-12 CPS.DS-13
		・製品・サービスを調達する際、それが信頼できるものかを確認していない	CPS.SC-3 CPS.SC-4 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14
		・自組織の調達に関わる要員が、調達にセキュリティリスクを十分に認識していない	CPS.AT-1
		・調達する製品・サービスが十分な物理的保護を実施されていない	CPS.DS-8 CPS.SC-4

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
脆弱性を悪用して IoT 機器内部に不正アクセスされ、事前に想定されていない動作をする	・攻撃ツール等を利用した IoT 機器におけるセキュリティ上の脆弱性を利用したマルウェア感染	・利用している IoT 機器に関わる脆弱性情報、脅威情報を収集・分析し、適切に対応していない	CPS.MA-1 CPS.MA-2 CPS.MA-3 CPS.SC-12
		・利用している IoT 機器が十分なセキュリティ機能を実装していない	CPS.DS-15 CPS.RA-4 CPS.RA-6 CPS.SC-4
		・情報システムや産業用制御システムに接続している自組織の IoT 機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない	CPS.AM-1
		・調達時に、適切なレベルのセキュリティ機能が実装されているかを確認するプロシージャがない	CPS.DS-15 CPS.RA-4 CPS.RA-6 CPS.SC-4
		・IoT 機器の誤動作を検知した後の対応手順が定義されていない	CPS.RP-1 CPS.SC-14
		・情報システムや産業用制御システムに接続している自組織の IoT 機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない	CPS.CM-6 CPS.IP-1 CPS.IP-2 CPS.SC-12
		・利用している IoT 機器に関わる脆弱性情報、脅威情報を収集・分析し、適切に対応していない。	CPS.IP-7 CPS.IP-8 CPS.IP-10 CPS.RA-2 CPS.SC-12
品質や信頼性の低い IoT 機器がネットワーク接続され、故障や正確でないデータの送信、想定していない通信先へのデータ送信等が発生する	・品質や信頼性の低い IoT 機器のネットワーク接続・正規の機器を模した偽造品の挿入	・IoT 機器を調達する際、調達製品が信頼できるものかを確認していない	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14
		・運用時に IoT 機器やソフトウェアが正規品である（改ざんされていない）ことを確認していない	CPS.DS-13
		・不正な機器によるネットワーク接続（有線あるいは無線）を防止できない	CPS.AC-2 CPS.AC-3 CPS.CM-6
		・組織外部への不正な通信を適切に検知し、遮断する等の対応ができない	CPS.DS-9 CPS.CM-1 CPS.CM-6
		・サイバー空間および正規の機器に接続する機器が正規のものかを確認する仕組みが実装されていない	CPS.AC-1 CPS.DS-13
		・IoT 機器を調達する際に、調達製品が信頼できるものかを確認するプロシージャがない	CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8
法制度等で規定されている水準のセキュリティ対策を実装できない	All threats	・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを策定・運用していない	CPS.DP-2 CPS.GV-2 CPS.SC-13
		・遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを遵守していない	CPS.AT-1 CPS.SC-13
		・法制度等で一定の保護を義務付けられている種のモノが、要求される水準の保護を適用されていない	CPS.GV-2
		・法制度等で一定の保護を義務付けられている種のシステムが、要求される水準の保護を適用されていない	CPS.GV-2

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
法制度等で規定されている水準のセキュリティ対策を実装できない（再掲）	All threats（再掲）	・組織内で規定されているプロシージャが関連する法規制等を遵守するような内容となっていない	CPS.GV-2
		・法制度等で一定の保護を義務付けられている種のデータが、要求される水準の保護を適用されていない	CPS.GV-2
一部の関係者だけで共有する秘匿性の高いデータのセキュリ ティ要求が設定・対応されていない	・データ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・データ保管エリアに対する不正なエンティティの物理的な侵入・正規ユーザによる内部不正・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし	・対応が必要なデータ保護に関する法規制等を十分に認識してない	CPS.GV-3 CPS.SC-13
		・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない	CPS.AT-1 CPS.AT-3
		・データの取扱いについて、必要なプロシージャを規定していない	CPS.GV-3
		・データの取扱いについて、必要なプロシージャを満たしているかを確認していない	CPS.DS-14
		・データを扱うシステムにおいてデータの秘匿性に応じた設計がなされていない	CPS.AC-7 CPS.AC-9 CPS.DS-2
		・複数の組織、システム等に個人情報等が分散して所在している	CPS.SC-3 CPS.SC-6
		・自組織で扱うデータの保護が必要な特定の種類のデータであることが識別されていない	CPS.DS-1

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
自組織で管理している(データ保管)領域から関係する他組織の保護すべきデータが漏えいする	・他組織の管理するデータ保管システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・他組織の管理するデータ保管エリアに対する不正なエンティティの物理的侵入・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし・自組織における悪意あるエンティティによる保護すべきデータの持出し	・自組織のシステムにおいて、対処すべき脆弱性が放置されている	CPS.CM-6 CPS.CM-7 CPS.SC-12
		保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	CPS.AC-1 CPS.AC-5 CPS.AC-6 CPS.AC-9 CPS.GV-3
		・IoT 機器、サーバ等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	CPS.AC-2 CPS.IP-5 CPS.PT-2 CPS.CM-2
		・保護すべきデータの管理に関する組織内の責任が明確でない	CPS.AM-6
		・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	CPS.AE-1 CPS.CM-1 CPS.CM-5 CPS.PT-1 CPS.RP-1
		・他組織から管理を委託されるデータの機密区分および必要なセキュリティ対策について確認するプロシージャがない	CPS.DS-1
		・他組織から管理を委託されているデータの保護に係る区分が明確になっていない	CPS.GV-3
		・定められた機密区分に沿った情報の保護が実装されていない	CPS.AC-7 CPS.SC-6
		・関係する他組織の保護すべきデータを格納するシステムにおいて、セキュアでない設定がなされている	CPS.IP-1
		・定められた機密区分に沿った情報の保護が実装されていない	CPS.DS-2 CPS.DS-3 CPS.DS-4 CPS.DS-5 CPS.DS-9
		・関係する他組織の保護すべきデータを格納するシステムにおいて、セキュアでない設定がなされている	CPS.PT-2
		・自組織のシステムにおいて、対処すべき脆弱性が放置されている	CPS.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.RA-2

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
自組織で管理している領域から保護すべきデータが漏えいする	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・入力確認の不備を突いたインジェクション攻撃(例：SQL インジェクション、 XSS)・ネットワーク上の通信の盗聴・保護が必要なエリアに対する不正なヒトの物理的な侵入・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし・正規ユーザによる内部不正	・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	CPS.AM-6 CPS.SC-12
		・モノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	CPS.AC-1 CPS.AE-1 CPS.AM-1 CPS.AM-5 CPS.CM-5 CPS.CM-6
		・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	CPS.RA-1 CPS.RA-3 CPS.RA-4 CPS.RA-5
		・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	CPS.BE-2
		・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	CPS.RA-6 CPS.RM-2
		・自組織のシステムにおいて、対処すべき脆弱性が放置されている	CPS.CM-6 CPS.CM-7 CPS.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.RA-2 CPS.SC-12
		・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている	CPS.IP-1 CPS.PT-2
		・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	CPS.SC-1
		・保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	CPS.GV-3 CPS.AC-1 CPS.AC-5 CPS.AC-6 CPS.AC-9
		・IoT 機器、サーバ等の設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	CPS.AC-2 CPS.CM-2 CPS.IP-5 CPS.PT-2
		・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	CPS.SC-2

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
自組織で管理している領域から保護すべきデータが漏えいする（再掲）	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・入力確認の不備を突いたインジェクション攻撃(例：SQL インジェクション、 XSS)・ネットワーク上の通信の盗聴・保護が必要なエリアに対する不正なヒトの物理的な侵入・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし・正規ユーザによる内部不正（再掲）	・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない	CPS.AE-1 CPS.CM-1 CPS.CM-3 CPS.CM-5 CPS.PT-1 CPS.RP-1
		・自組織で管理しているデータの保護に係る区分が明確になっていない	CPS.GV-3
		・定められた機密区分に沿った情報の保護が実装されていない	CPS.DS-2 CPS.DS-3 CPS.SC-6
		・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	CPS.IP-3
		・定められた機密区分に沿った情報の保護が実装されていない	CPS.DS-4 CPS.DS-5 CPS.DS-9
		・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	CPS.GV-1 CPS.GV-4
		・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	CPS.RM-1 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.IP-7 CPS.SC-10 CPS.SC-11
		・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	CPS.AT-1
		・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	CPS.AT-3
		・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	CPS.SC-5 CPS.IP-9

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
自組織で管理している領域において保護すべきデータが改ざんされる	・窃取した ID、パスワード等を利用した正規ユーザへのなりすまし・通信系路上でデータを改ざんする中間者攻撃等・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染・正規ユーザによる内部不正・保護が必要なエリアに対する不正なヒトの物理的な侵入・保護が必要なデータを扱う媒体の物理的な破壊	・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	CPS.SC-7 CPS.SC-10 CPS.SC-11 CPS.IP-7
		・通信路及び通信路上のデータが十分に保護されていない	CPS.DS-3 CPS.DS-4
		・取り扱うデータに改ざんを検知するメカニズムがない	CPS.DS-11
		・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	CPS.AM-6 CPS.BE-2 CPS.IP-3 CPS.SC-1 CPS.SC-2
		・自身が関わりうるセキュリティやセーフティに関係するリスクに対して十分な認識を有していない	CPS.AT-1 CPS.AT-3
		・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	CPS.IP-9 CPS.SC-5
		・情報システムや産業用制御システムを構成しているモノのセキュリティ状況やネットワーク接続状況が適切に管理(例 ：資産の棚卸し、モニタリング)されていない	CPS.AC-1 CPS.AE-1 CPS.AM-1 CPS.AM-5 CPS.CM-5 CPS.CM-6
		・自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない	CPS.RA-1 CPS.RA-3 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.RM-2
		・保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている	CPS.IP-1 CPS.PT-2
		・保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	CPS.AC-1 CPS.AC-5 CPS.AC-6 CPS.AC-9 CPS.GV-3
		・早期にネットワーク上での異常(例 ：なりすまし、 メッセージの改ざん)を素早く検知し、対処するような仕組みがシステムに実装されていない	CPS.AE-3 CPS.CM-3 CPS.DP-4
		・セキュリティに関わるリスクマネジメントの適切な手順が確立していない	CPS.GV-1 CPS.GV-4 CPS.RM-1 CPS.SC-3 CPS.SC-4 CPS.SC-6

想定されるセキュリティインシデント	リスク源		対策要件 ID
	脅威	脆弱性	
自組織のセキュリティインシデントにより関係する他組織が適切に事業継続できない	All threats	・自組織のモノ/システム/データのサイバー空間における他組織との連携状況を把握していない	CPS.AE-1 CPS.AM-4 CPS.AM-5 CPS.CM-5 CPS.CM-6
		・自組織と他組織(サプライヤ等)とのフィジカル空間における連携状況および責任分界を把握していない	CPS.AM-7 CPS.BE-1 CPS.BE-3 CPS.RM-1
		・他組織のヒトが自組織のセキュリティ事象発生時に適切なアクションを取ることができない	CPS.AT-2 CPS.AT-3 CPS.RP-2 CPS.SC-9
		・セキュリティ事象による被害を受けたモノ(製品)・サービスが生じる	CPS.RP-4
		・自組織が提供する/されるモノ(製品)に関する記録(例:製造日/識別ナンバー/提供先)が保持されていない	CPS.AM-2 CPS.AM-3
		・関係する他組織と連携したセキュリティ事象対応手順が策定されていない	CPS.AE-4 CPS.RP-2
自組織のセキュリティインシデントにより自組織が適切に事業継続できない	All threats	・セキュリティインシデントに的確に対応するための体制が構築されていない	CPS.IM-1 CPS.IM-2
		・セキュリティインシデント発生時に適切なアクションを取ることができない	CPS.AT-1 CPS.AT-3 CPS.RP-1
		・セキュリティインシデントにより被害を受けた自組織の事業の範囲(製品等)を特定することができない	CPS.AM-2 CPS.AM-3 CPS.AN-1
		・セキュリティインシデントを適切に検知するための機器等が導入されていないか、あるいは正しく運用されていない	CPS.AE-3 CPS.CM-1
		・セキュリティ事象を的確に検知するための体制が構築されていない	CPS.AE-2 CPS.RA-2 CPS.AE-2 CPS.DP-1 CPS.DP-2 CPS.DP-3 CPS.DP-4 CPS.RA-2
		・自組織におけるセキュリティインシデントへの対応手順が策定されていない	CPS.AE-5 CPS.AN-1 CPS.AN-2 CPS.AN-3 CPS.MI-1 CPS.RP-1
		・事業継続計画にセキュリティインシデントが位置づけられておらず、セキュリティインシデント発生時に自組織の事業継続に支障が生じる	CPS.CO-1 CPS.CO-2 CPS.RP-3 CPS.CO-3 CPS.SC-14
		・セキュリティインシデント発生時に事業を継続するために必要なデータが、適切に準備されていない、又は準備されているが適切に機能しない	CPS.AT-1 CPS.AT-2 CPS.IP-4 CPS.RP-3

【Appendix】C　セキュリティ対策一覧

セキュリティカテゴリ	対策要件ID	対策要件	リファレンスアーキテクチャ
AC:アクセスコントロール	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する	ガバナンス サービス 都市OS アセット
	CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する	ガバナンス サービス 都市OS アセット
	CPS.AC-3	・無線接続先（ユーザやIoT機器、サーバ等）を正しく認証する	サービス 都市OS アセット
	CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ	サービス 都市OS アセット
	CPS.AC-5	・職務及び責任範囲（例：ユーザ／システム管理者)を適切に分離する	ガバナンス サービス 都市OS
	CPS.AC-6	・特権を持つユーザのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する	サービス 都市OS
	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：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）等してネットワークの完全性を保護する	サービス 都市OS アセット
	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する	サービス 都市OS アセット
	CPS.AC-9	・IoT機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する	サービス 都市OS アセット
AE:異変とイベント	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する	ガバナンス サービス 都市OS アセット
	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える	ガバナンス
	CPS.AE-3	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する	ガバナンス 都市OS
	CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する	ガバナンス
	CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める	ガバナンス
AM:資産管理	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する	サービス 都市OS アセット
	CPS.AM-2	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める	ガバナンス サービス 都市OS
	CPS.AM-3	・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する	ガバナンス サービス
	CPS.AM-4	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する	ガバナンス

セキュリティカテゴリ	対策要件ID	対策要件	リファレンスアーキテクチャ
	CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する	ガバナンス サービス 都市OS アセット
	CPS.AM-6	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する	ガバナンス
	CPS.AM-7	・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める	ガバナンス
AN:分析	CPS.AN-1	・セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する	ガバナンス
	CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレンジックを実施する	ガバナンス
	CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する	ガバナンス
AT:意識向上及びトレーニング	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する	ガバナンス
	CPS.AT-2	・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する	ガバナンス
	CPS.AT-3	・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する	ガバナンス
BE:ビジネス環境	CPS.BE-1	・サプライチェーンにおいて、自組織が担う役割を特定し共有する	ガバナンス
	CPS.BE-2	・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤ、第三者プロバイダ等を含む）に共有する	ガバナンス
	CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する	ガバナンス
CM:セキュリティの継続的なモニタリング	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する	ガバナンス サービス 都市OS
	CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する	ガバナンス サービス 都市OS アセット
	CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する。・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する	サービス 都市OS アセット
	CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する	サービス
	CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする	アセット サービス 都市OS アセット
	CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する	ガバナンス サービス 都市OS アセット
	CPS.CM-7	・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する	サービス 都市OS アセット
CO:伝達	CPS.CO-1	・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する	ガバナンス

セキュリティカテゴリ	対策要件ID	対策要件	リファレンスアーキテクチャ
	CPS.CO-2	・事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける	ガバナンス
	CPS.CO-3	・復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける	ガバナンス
DP:検知プロセス	CPS.DP-1	・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする	ガバナンス
	CPS.DP-2	・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する	ガバナンス
	CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する	ガバナンス
	CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する	ガバナンス 都市OS
DS:データセキュリティ	CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取決める	ガバナンス 都市OS
	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する	サービス 都市OS
	CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	サービス 都市OS アセット
	CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する	サービス 都市OS
	CPS.DS-5	・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する	サービス 都市OS
	CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する	サービス 都市OS アセット
	CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う	サービス 都市OS アセット
	CPS.DS-8	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する	アセット
	CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する	サービス 都市OS
	CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する	サービス 都市OS アセット
	CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する	ガバナンス サービス 都市OS アセット
	CPS.DS-12	・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する	都市OS アセット
	CPS.DS-13	・IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する	ガバナンス サービス 都市OS アセット
	CPS.DS-14	・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する	ガバナンス
	CPS.DS-15	・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する	ガバナンス アセット
GV:ガバナンス	CPS.GV-1	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする	ガバナンス
	CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する	ガバナンス
	CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う	ガバナンス サービス 都市OS
	CPS.GV-4	・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う	ガバナンス

セキュリティカテゴリ	対策要件ID	対策要件	リファレンスアーキテクチャ
IM:改善	CPS.IM-1	・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する	ガバナンス
	CPS.IM-2	・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急事対応計画を継続的に改善する	ガバナンス
IP:情報保護プロセス・手順	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する	ガバナンス サービス 都市OS アセット
	CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する	サービス 都市OS アセット
	CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する	ガバナンス
	CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする	サービス 都市OS アセット
	CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する	サービス 都市OS アセット
	CPS.IP-6	・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする	サービス 都市OS アセット
	CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する	ガバナンス
	CPS.IP-8	・保護技術の有効性について、適切なパートナーとの間で情報を共有する	ガバナンス
	CPS.IP-9	・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める	ガバナンス
	CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する	ガバナンス サービス 都市OS
MA:保守	CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する	サービス 都市OS アセット
	CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する	サービス 都市OS アセット
	CPS.MA-3	・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する	アセット
MI:低減(Mitigation)	CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う	ガバナンス
PT:保護技術	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする	ガバナンス サービス
	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする	サービス 都市OS アセット
	CPS.PT-3	・ネットワークにつながることを踏まえた安全性を実装するIoT機器を導入する	都市OS
RA:リスク評価	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する	ガバナンス サービス 都市OS
	CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する	ガバナンス サービス 都市OS
	CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する	ガバナンス 都市OS
	CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する	サービス 都市OS アセット

セキュリティカテゴリ	対策要件ID	対策要件	リファレンスアーキテクチャ
	CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する	ガバナンス 都市OS
	CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する	ガバナンス サービス 都市OS アセット
RM:リスク管理戦略	CPS.RM-1	・自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例 ：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例 ：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する	ガバナンス
	CPS.RM-2	・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する	ガバナンス 都市OS
RP:インシデント対応計画	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する	ガバナンス サービス 都市OS
	CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する	ガバナンス
	CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける	ガバナンス
	CPS.RP-4	・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う	サービス
SC:サプライチェーン・リスク管理	CPS.SC-1	・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する	ガバナンス
	CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する	ガバナンス
	CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する	ガバナンス サービス 都市OS アセット
	CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する	ガバナンス サービス 都市OS アセット
	CPS.SC-5	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する	ガバナンス
	CPS.SC-6	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	ガバナンス
	CPS.SC-7	・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する	ガバナンス
	CPS.SC-8	・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする	ガバナンス サービス 都市OS アセット
	CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う	ガバナンス
	CPS.SC-10	・取引先等の関係する他組織との契約が終了する際（例 ：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する	ガバナンス

セキュリティカテゴリ	対策要件ID	対策要件	リファレンスアーキテクチャ
	CPS.SC-11	・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する	ガバナンス
	CPS.SC-12	・製品等の供給元にて、脆弱性関連情報の取扱いについてのポリシーが策定、公表されており、脆弱性情報を収集する体制の確保及び調整機関と情報交換を行うための窓口が設置されていること、脆弱性が発見された場合、速やかに脆弱性検証を行い、対策方法を作成する体制が整備され、発見された脆弱性の概要や作成した対策方法を速やかに通知し、必要な技術的情報を提供する体制が整備されていることを確認し、製品等の供給元から脆弱性情報の適切な通知及び情報提供を受ける運用体制を整備する 〃	ガバナンス サービス 都市OS アセット〃
	CPS.SC-13	・製品等の供給元が本社等の立地する場所の法的環境等により開発供給の適切性が影響を受けない理由を確認し、製品等の供給元の法的環境等による影響を排除する	ガバナンス サービス 都市OS アセット〃
	CPS.SC-14	・製品等の供給元における開発供給の拠点及びその供給能力、製品等の供給安定性に対するリスクとその対応の考え方、製品等の供給にて他社製品を使用している場合、サプライヤーリストが存在し、保守及び管理の方針が策定されていること、BCPが策定されていることを通じて製品等の供給安定性が確保されていることを確認する	ガバナンス サービス 都市OS アセット〃

セキュリティ対策一覧（カテゴリ毎）

カテゴリ	対策区分	対策要件ID	対策要件
ガバナンス	AC:アクセスコントロール	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する
		CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する
		CPS.AC-5	・職務及び責任範囲（例：ユーザ／システム管理者）を適切に分離する
	AE:異変とイベント	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する
		CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える
		CPS.AE-3	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する
		CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する
		CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める
	AM:資産管理	CPS.AM-2	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める
		CPS.AM-3	・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する
		CPS.AM-4	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する
		CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する
		CPS.AM-6	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する
		CPS.AM-7	・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める
	AN:分析	CPS.AN-1	・セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレンジックを実施する
		CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する
	AT:意識向上及びトレーニング	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する
		CPS.AT-2	・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する
		CPS.AT-3	・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する
	BE:ビジネス環境	CPS.BE-1	・サプライチェーンにおいて、自組織が担う役割を特定し共有する
		CPS.BE-2	・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤ、第三者プロバイダ等を含む）に共有する
		CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する
	CM:セキュリティの継続的なモニタリング	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する
		CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する
		CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する
	CO:伝達	CPS.CO-1	・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する
		CPS.CO-2	・事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける
		CPS.CO-3	・復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける
	DP:検知プロセス	CPS.DP-1	・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.DP-2	・監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する
		CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する
		CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する
	DS:データセキュリティ	CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取決める
		CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する
		CPS.DS-13	・IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する
		CPS.DS-14	・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する
		CPS.DS-15	・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する
	GV:ガバナンス	CPS.GV-1	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする
		CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する
		CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う
		CPS.GV-4	・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う
	IM:改善	CPS.IM-1	・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する
		CPS.IM-2	・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急事対応計画を継続的に改善する
	IP:情報保護プロセス・手順	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する
		CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する
		CPS.IP-8	・保護技術の有効性について、適切なパートナーとの間で情報を共有する
		CPS.IP-9	・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例 ：アクセス権限の無効化、従業員に対する審査）を含める
		CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する
	MI:低減(Mitigation)	CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う
	PT:保護技術	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする
	RA:リスク評価	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する
		CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する
		CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する
		CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する
		CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する
	RM:リスク管理戦略	CPS.RM-1	・自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例 ：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例 ：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する
		CPS.RM-2	・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する
	RP:インシデント対応計画	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する
		CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける
	SC:サプライチェーン・リスク管理	CPS.SC-1	・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する
		CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する
		CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する
		CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する
		CPS.SC-5	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する
		CPS.SC-6	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。
		CPS.SC-7	・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する
		CPS.SC-8	・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする
		CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う
		CPS.SC-10	・取引先等の関係する他組織との契約が終了する際（例：契約期間の満了、サポートの終了）に実施すべきプロシージャを策定し、運用する
		CPS.SC-11	・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する
		CPS.SC-12	・製品等の供給元にて、脆弱性関連情報の取扱いについてのポリシーが策定、公表されており、脆弱性情報を収集する体制の確保及び調整機関と情報交換を行うための窓口が設置されていること、脆弱性が発見された場合、速やかに脆弱性検証を行い、対策方法を作成する体制が整備され、発見された脆弱性の概要や作成した対策方法を速やかに通知し、必要な技術的情報を提供する体制が整備されていることを確認し、製品等の供給元から脆弱性情報の適切な通知及び情報提供を受ける運用体制を整備する
		CPS.SC-13	・製品等の供給元が本社等の立地する場所の法的環境等により開発供給の適切性が影響を受けない理由を確認し、製品等の供給元の法的環境等による影響を排除する
		CPS.SC-14	・製品等の供給元における開発供給の拠点及びその供給能力、製品等の供給安定性に対するリスクとその対応の考え方、製品等の供給にて他社製品を使用している場合、サプライヤーリストが存在し、保守及び管理の方針が策定されていること、BCP が策定されていることを通じて製品等の供給安定性が確保されていることを確認する

カテゴリ	対策区分	対策要件ID	対策要件
サービス	AC:アクセスコントロール	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する
		CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する
		CPS.AC-3	・無線接続先（ユーザやIoT機器、サーバ等）を正しく認証する
		CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ
		CPS.AC-5	・職務及び責任範囲（例 ：ユーザ／システム管理者)を適切に分離する
		CPS.AC-6	・特権を持つユーザのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例 ：二つ以上の認証機能を組み合わせた多要素認証）を採用する
		CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例 ：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）等してネットワークの完全性を保護する
		CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する
		CPS.AC-9	・IoT機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する
	AE:異変とイベント	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する
	AM:資産管理	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例 ：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する
		CPS.AM-2	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める
		CPS.AM-3	・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する
		CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する
	CM:セキュリティの継続的なモニタリング	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する
		CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する。・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する
		CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する
		CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする
		CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する
		CPS.CM-7	・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する
	DS:データセキュリティ	CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する
		CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する
		CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する
		CPS.DS-5	・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する
		CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する
		CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う
		CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する
		CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する
		CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.DS-13	・IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する
	GV:ガバナンス	CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う
	IP:情報保護プロセス・手順	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する
		CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する
		CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする
		CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する
		CPS.IP-6	・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする
		CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する
	MA:保守	CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する
		CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する
	PT:保護技術	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする
		CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする
	RA:リスク評価	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する
		CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する
		CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する
	RP:インシデント対応計画	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する
		CPS.RP-4	・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して適切な対応を行う
	SC:サプライチェーン・リスク管理	CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する
		CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する
		CPS.SC-8	・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする
		CPS.SC-12	・製品等の供給元にて、脆弱性関連情報の取扱いについてのポリシーが策定、公表されており、脆弱性情報を収集する体制の確保及び調整機関と情報交換を行うための窓口が設置されていること、脆弱性が発見された場合、速やかに脆弱性検証を行い、対策方法を作成する体制が整備され、発見された脆弱性の概要や作成した対策方法を速やかに通知し、必要な技術的情報を提供する体制が整備されていることを確認し、製品等の供給元から脆弱性情報の適切な通知及び情報提供を受ける運用体制を整備する
		CPS.SC-13	・製品等の供給元が本社等の立地する場所の法的環境等により開発供給の適切性が影響を受けない理由を確認し、製品等の供給元の法的環境等による影響を排除する
		CPS.SC-14	・製品等の供給元における開発供給の拠点及びその供給能力、製品等の供給安定性に対するリスクとその対応の考え方、製品等の供給にて他社製品を使用している場合、サプライヤーリストが存在し、保守及び管理の方針が策定されていること、BCP が策定されていることを通じて製品等の供給安定性が確保されていることを確認する
都市 OS	AC:アクセスコントロール	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する
		CPS.AC-2	・IoT 機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する
		CPS.AC-3	・無線接続先（ユーザや IoT 機器、サーバ等）を正しく認証する
		CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT 機器、サーバ等に対する不正ログインを防ぐ
		CPS.AC-5	・職務及び責任範囲（例 ：ユーザ／システム管理者)を適切に分離する
		CPS.AC-6	・特権を持つユーザのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式（例 ：二つ以上の認証機能を組み合わせた多要素認証）を採用する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例 ：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）等してネットワークの完全性を保護する
		CPS.AC-8	・IoT 機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する
		CPS.AC-9	・IoT 機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する
	AE:異変とイベント	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する
		CPS.AE-3	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する
	AM:資産管理	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例 ：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する
		CPS.AM-2	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める
		CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する
	CM:セキュリティの継続的なモニタリング	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する
		CPS.CM-2	・IoT 機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する
		CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する
		CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする
		CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する
		CPS.CM-7	・自組織の管理している IoT 機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する
	DP:検知プロセス	CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する

カテゴリ	対策区分	対策要件ID	対策要件
	DS:データセキュリティ	CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取決める
		CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する
		CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する
		CPS.DS-12	・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する
		CPS.DS-13	・IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する
		CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する
		CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する
		CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する
		CPS.DS-5	・送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する
		CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する
		CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う
		CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する
	GV:ガバナンス	CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う
	IP:情報保護プロセス・手順	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する
		CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする
		CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する
		CPS.IP-6	・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする
		CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する
	MA:保守	CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する
		CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する
	PT:保護技術	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする
		CPS.PT-3	・ネットワークにつながることを踏まえた安全性を実装するIoT機器を導入する
	RA:リスク評価	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する
		CPS.RA-2	・セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する
		CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する
		CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する
		CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する
		CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する
	RM:リスク管理戦略	CPS.RM-2	・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する

カテゴリ	対策区分	対策要件ID	対策要件
	RP:インシデント対応計画	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する
	SC:サプライチェーン・リスク管理	CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する
		CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する
		CPS.SC-8	・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする
		CPS.SC-12	・製品等の供給元にて、脆弱性関連情報の取扱いについてのポリシーが策定、公表されており、脆弱性情報を収集する体制の確保及び調整機関と情報交換を行うための窓口が設置されていること、脆弱性が発見された場合、速やかに脆弱性検証を行い、対策方法を作成する体制が整備され、発見された脆弱性の概要や作成した対策方法を速やかに通知し、必要な技術的情報を提供する体制が整備されていることを確認し、製品等の供給元から脆弱性情報の適切な通知及び情報提供を受ける運用体制を整備する
		CPS.SC-13	・製品等の供給元が本社等の立地する場所の法的環境等により開発供給の適切性が影響を受けない理由を確認し、製品等の供給元の法的環境等による影響を排除する
		CPS.SC-14	・製品等の供給元における開発供給の拠点及びその供給能力、製品等の供給安定性に対するリスクとその対応の考え方、製品等の供給にて他社製品を使用している場合、サプライヤーリストが存在し、保守及び管理の方針が策定されていること、BCPが策定されていることを通じて製品等の供給安定性が確保されていることを確認する
アセット	AC:アクセスコントロール	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する
		CPS.AC-2	・IoT機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する
		CPS.AC-3	・無線接続先（ユーザやIoT機器、サーバ等）を正しく認証する
		CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT機器、サーバ等に対する不正ログインを防ぐ
		CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：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）等してネットワークの完全性を保護する
		CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する
		CPS.AC-9	・IoT機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する
	AE:異変とイベント	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する

カテゴリ	対策区分	対策要件ID	対策要件
	AM:資産管理	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する
		CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する
	CM:セキュリティの継続的なモニタリング	CPS.CM-2	・IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する
		CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行うIoT機器を導入する。・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する
		CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする
		CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする
		CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する
		CPS.CM-7	・自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する
	DS:データセキュリティ	CPS.DS-3	・IoT機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する
		CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する
		CPS.DS-7	・IoT機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う
		CPS.DS-8	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する
		CPS.DS-10	・IoT機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する
		CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する
		CPS.DS-12	・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する

カテゴリ	対策区分	対策要件ID	対策要件
		CPS.DS-13	・IoT機器やソフトウェアが正規品であることを定期的（起動時等）に確認する
		CPS.DS-15	・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する
	IP:情報保護プロセス・手順	CPS.IP-1	・IoT機器、サーバ等の初期設定手順（パスワード等）及び設定変更管理プロセスを導入し、運用する
		CPS.IP-2	・IoT機器、サーバ等の導入後に、追加するソフトウェアを制限する
		CPS.IP-4	・構成要素（IoT機器、通信機器、回線等）に対し、定期的なシステムバックアップを実施し、テストする
		CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織のIoT機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する
		CPS.IP-6	・IoT機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規IoT機器、サーバ等を一意に識別するID（識別子）や重要情報（秘密鍵、電子証明書等）を削除又は読み取りできない状態にする
	MA:保守	CPS.MA-1	・IoT機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する
		CPS.MA-2	・自組織のIoT機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する
		CPS.MA-3	・可能であれば、遠隔地からの操作によってソフトウェア（OS、ドライバ、アプリケーション）を一括して更新するリモートアップデートの仕組みを備えたIoT機器を導入する
	PT:保護技術	CPS.PT-2	・IoT機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする
	RA:リスク評価	CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する
		CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する
	SC:サプライチェーン・リスク管理	CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する
		CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する

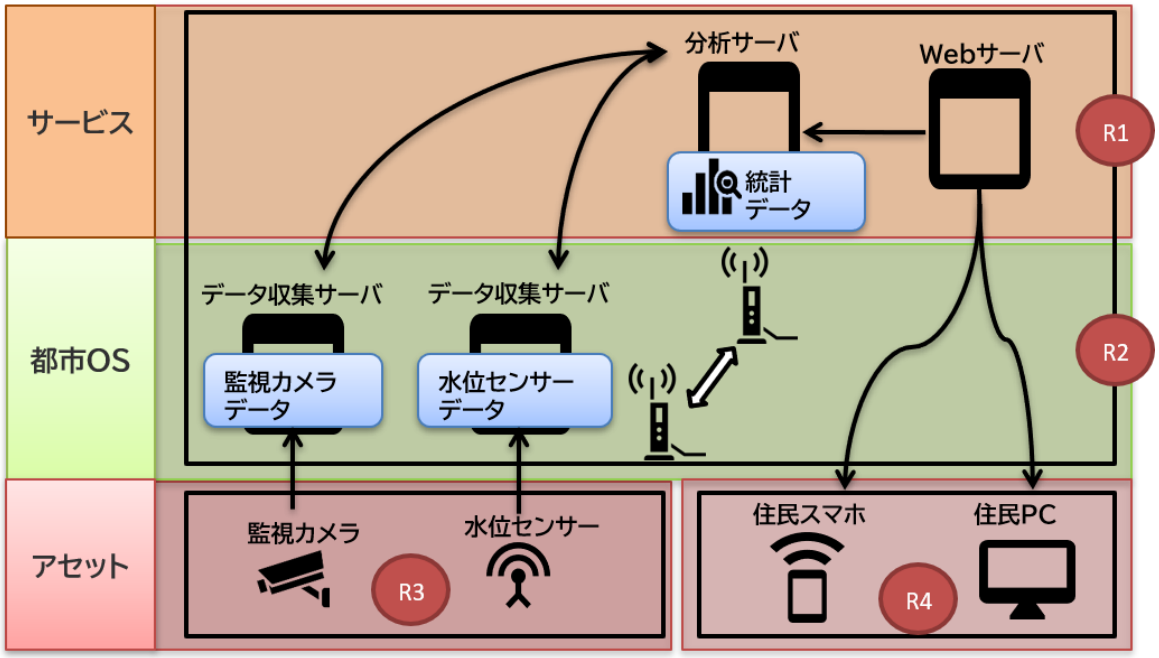
カテゴリ	対策区分	対策要件ID	対策要件
		CPS.SC-8	・自組織が関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報（データ）を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする
		CPS.SC-12	・製品等の供給元にて、脆弱性関連情報の取扱いについてのポリシーが策定、公表されており、脆弱性情報を収集する体制の確保及び調整機関と情報交換を行うための窓口が設置されていること、脆弱性が発見された場合、速やかに脆弱性検証を行い、対策方法を作成する体制が整備され、発見された脆弱性の概要や作成した対策方法を速やかに通知し、必要な技術的情報を提供する体制が整備されていることを確認し、製品等の供給元から脆弱性情報の適切な通知及び情報提供を受ける運用体制を整備する
		CPS.SC-13	・製品等の供給元が本社等の立地する場所の法的環境等により開発供給の適切性が影響を受けない理由を確認し、製品等の供給元の法的環境等による影響を排除する
		CPS.SC-14	・製品等の供給元における開発供給の拠点及びその供給能力、製品等の供給安定性に対するリスクとその対応の考え方、製品等の供給にて他社製品を使用している場合、サプライヤーリストが存在し、保守及び管理の方針が策定されていること、BCP が策定されていることを通じて製品等の供給安定性が確保されていることを確認する

【Appendix】D　各分野におけるリスク特定とセキュリティ対策検討のイメージ

防災イメージ

【ユースケース例】

・水位センサーや防犯カメラで、洪水・土砂崩れ・河川氾濫の先行情報を取得し、適切な場所での防犯措置や住民に避難誘導を展開する等、対策をとる。



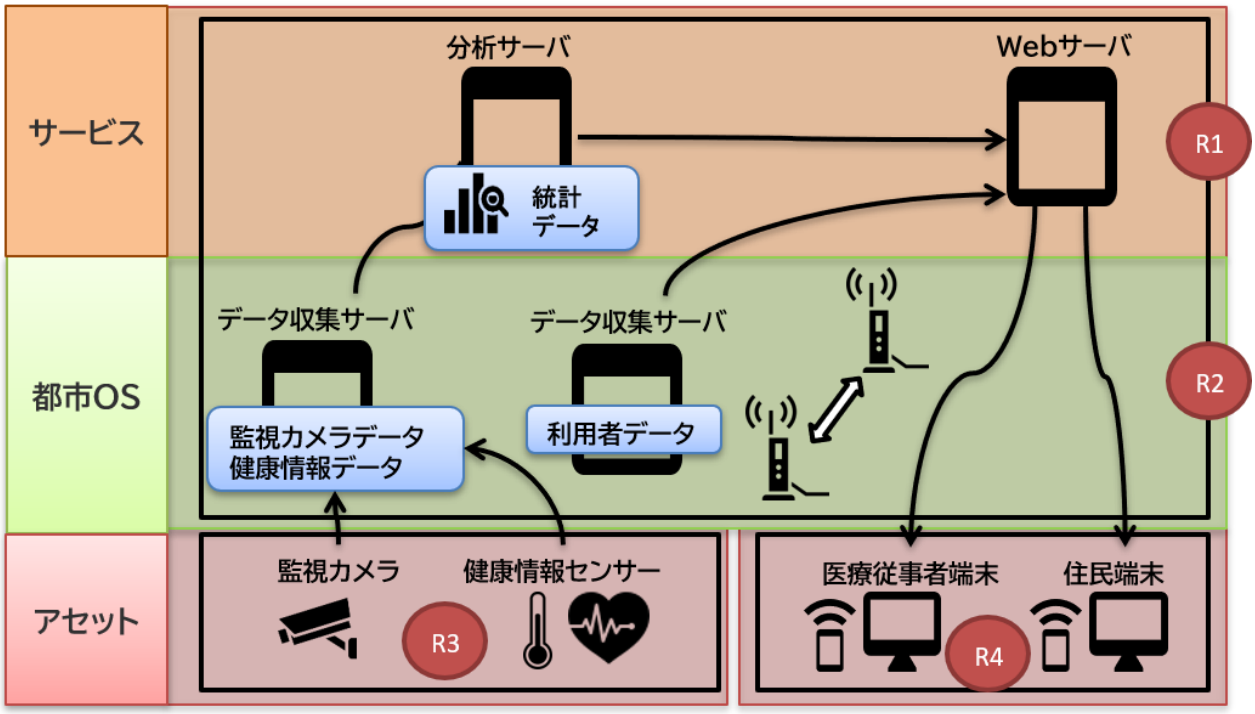
リスク箇所	リスク概要	対策番号
R1	なりすましによる不正の受信	CPS.AC-1, CPS.AC-3, CPS.AC-4, CPS.AC-8, CPS.AC-9, CPS.IP-2, CPS.IP-10, CPS.MA-1, CPS.MA-2, CPS.RA-2, CPS.CM-6, CPS.CM-7
	サービス拒否攻撃、ランサムウェアへの感染等によるシステムが停止する	CPS.RA-1、CPS.RA-3、CPS.RA-4、CPS.RA-5、CPS.RA-6、CPS.RM-2、CPS.DS-6、CPS.DS-7
	自組織の保護すべきデータが改ざんされる	CPS.AC-7、CPS.AC-9、CPS.DS-2、CPS.DS-3、CPS.DS-4、CPS.DS-11
	不正なエンティティによる許容範囲外のインプットデータ・マルウェアによる制御信号の改ざん	CPS.RA-4、CPS.RA-6
R2	自組織で管理している（データ保管）領域から関係する他組織の保護すべきデータが漏えいする	CPS.AC-1、CPS.AC-5、CPS.AC-6、CPS.AC-9、CPS.GV-3
	データ加工・分析システムが誤動作することで、適切でない分析結果が出力される	CPS.CM-3、CPS.CM-4
R3	改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信が発生する	CPS.AC-1、CPS.AE-1、CPS.AM-1、CPS.AM-5、CPS.CM-5、CPS.CM-6、CPS.DS-8、CPS.SC-4
	不正なエンティティによる許容範囲外のインプットデータ・マルウェアによる制御信号の改ざん	CPS.CM-3、CPS.AE-1、CPS.CM-1、CPS.CM-5、CPS.PT-1、CPS.RP-1
	IoT機器内部への不正アクセス	CPS.IP-1、CPS.PT-2、CPS.DS-15、CPS.RA-4、CPS.RA-6、CPS.SC-4
	IoT機器におけるセキュリティ上の脆弱性を利用したネットワーク上の通信の盗聴	CPS.AC-1、CPS.AE-1、CPS.AM-1、CPS.AM-5、CPS.CM-5、CPS.CM-6
R4	（なりすまし等をした）ソシキ/ヒト/モノ等から不適切なデータを受信する	CPS.DS-3、CPS.AC-1、CPS.AC-3、CPS.AC-4、CPS.AC-8、CPS.AC-9

図 A－１：各層におけるリスクと対応する経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」の対策要件 ID

医療・福祉イメージ

【ユースケース例】

・高齢者や患者の健康情報を収集、蓄積することで、医者や家族が患者の健康情報を常に把握可能とする。

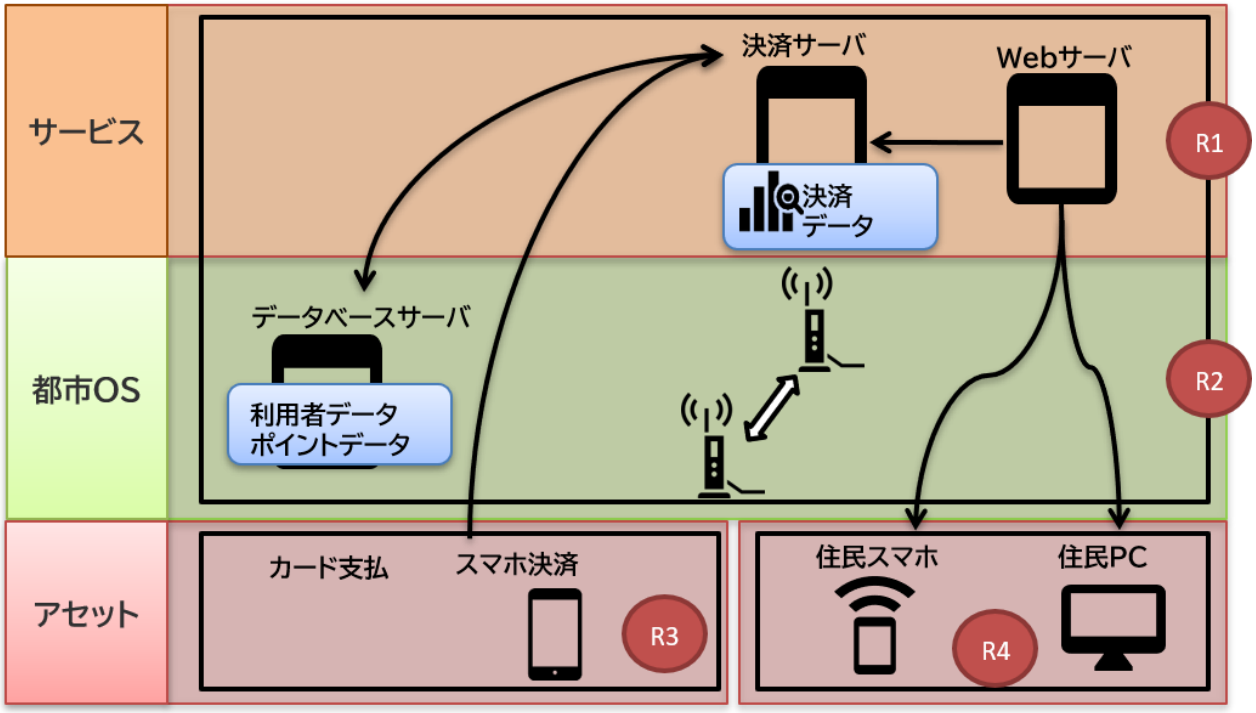


リスク箇所・リスク概要・対策番号の一覧については、前掲の「防災イメージ」の項を参照。

決済イメージ

【ユースケース例】

・地域通貨や自治体ポイントによる決済を可能とする。利用者は Web サービスから自身の取得ポイントや利用状況を確認可能とする。



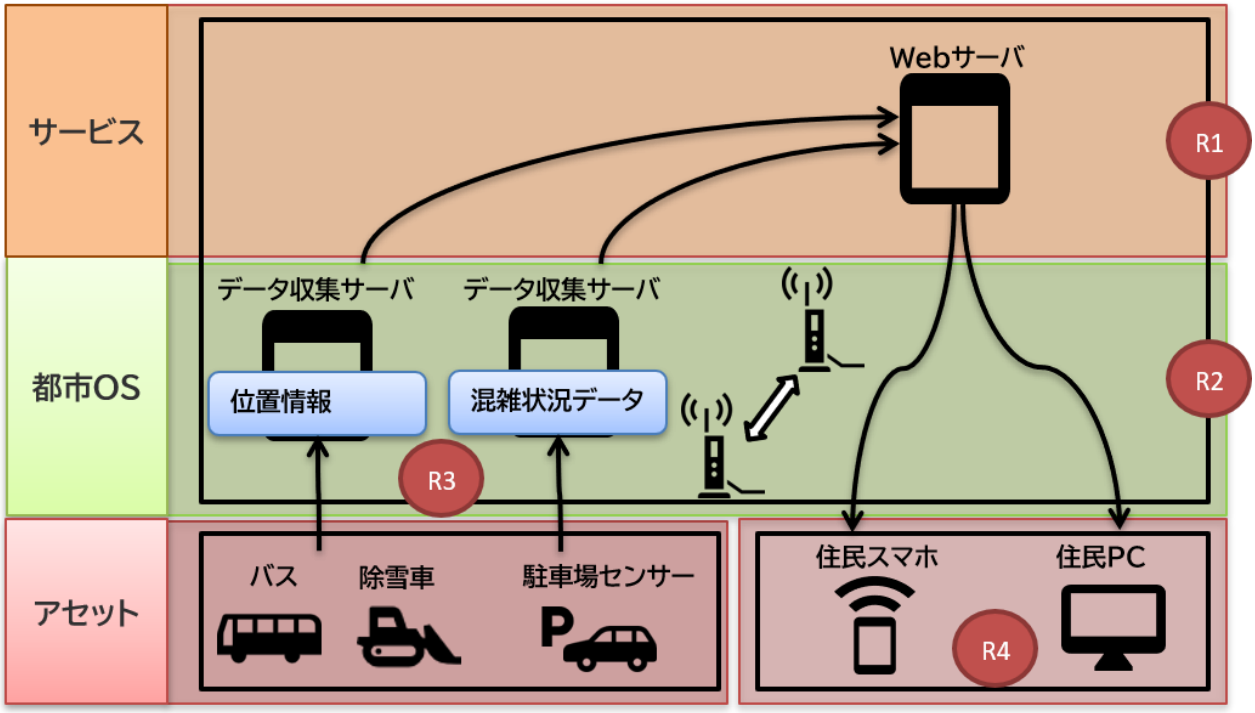
リスク箇所・リスク概要・対策番号の一覧については、前掲の「防災イメージ」の項を参照。

交通イメージ

【ユースケース例】

・バスや除雪車の位置情報を取得し、住民や観光客に配信することで交通機関の利用促進を行う。

また、駐車場の利用状況を配信することで、住民や観光客の利用を促す。

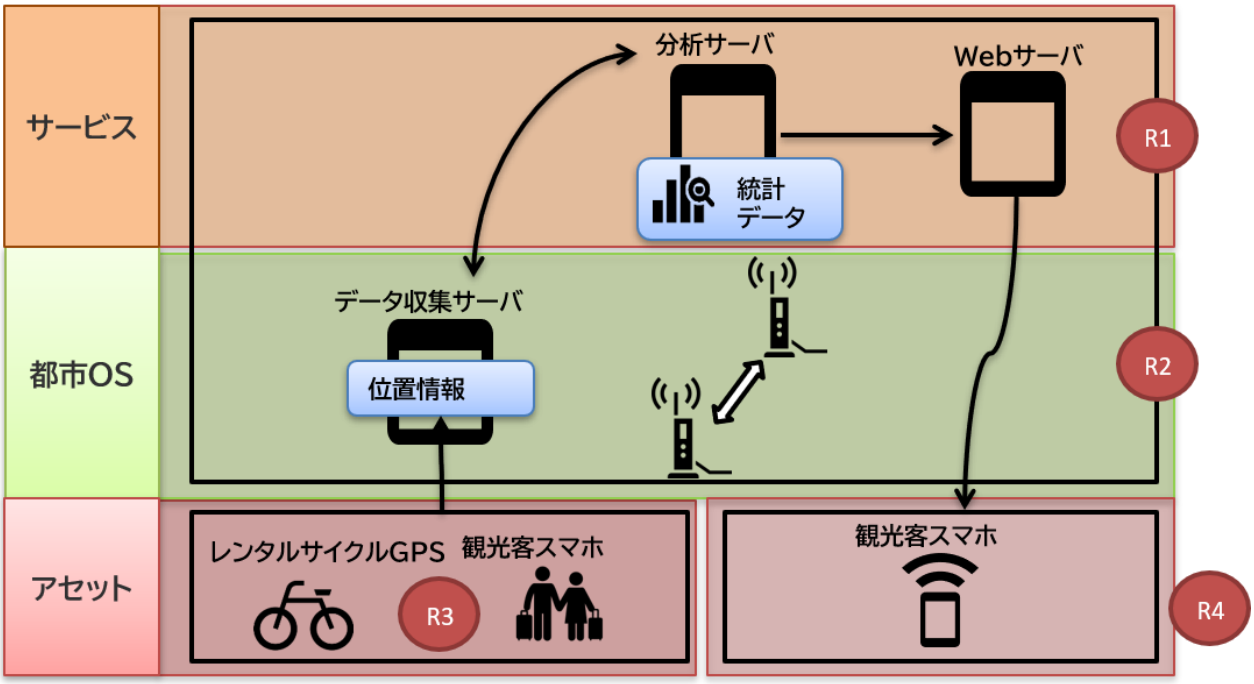


リスク箇所・リスク概要・対策番号の一覧については、前掲の「防災イメージ」の項を参照。

観光イメージ

【ユースケース例】

・観光客向けのレンタルサイクルに GPS を搭載し、観光客の行動情報を取得することで観光地にいる観光客へ適切な観光情報を配信する。



リスク箇所・リスク概要・対策番号の一覧については、前掲の「防災イメージ」の項を参照。

【Appendix】E　サービス観点の脅威事例

リスクシナリオ１：決済系 不正ログインによる保険証画像の窃取

■ シナリオ

・ 決済系のアプリ等で悪意を持ったユーザが、第三者の銀行口座を登録し、サービスにおいて、アカウントの所有者ではない第三者への支払いの押し付けが発生。

■ 脆弱性

・ アカウント作成時の認証強度が弱く、不正な第三者の銀行口座とアカウントの紐付けを許容してしまう

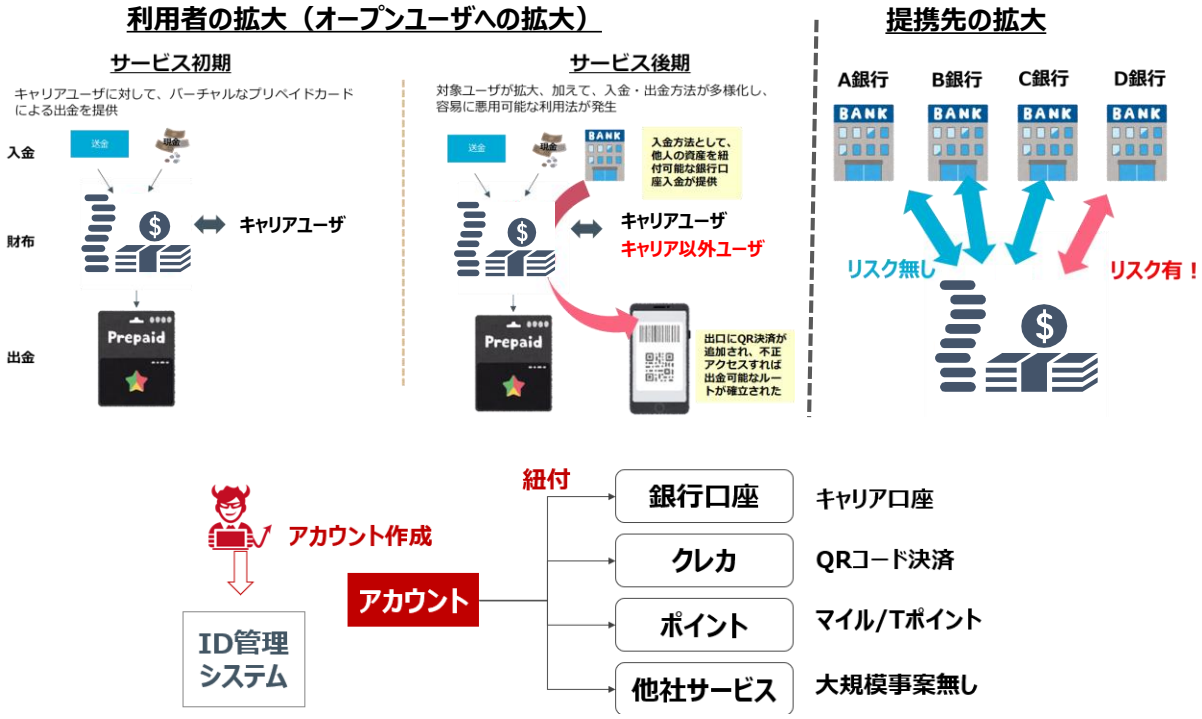
想定されるインシデント例

■ 概要

・ QR コード決済等のアプリで、悪意を持ったユーザがアカウント作成後、支払で銀行口座と紐づける際に、何らかの手段で取得した第三者の銀行口座と紐づける。
　決済時には商品を取得したユーザとは別のユーザの銀行口座から引き落とされるため、金銭的被害の発生が想定される。

■ 経緯

・ 悪意あるユーザが、銀行口座情報（銀行・支店・口座番号・暗証番号等）を不正入手
・ 悪意あるユーザが、QR コード決済等の決済アプリでアカウントを新規開設
・ 悪意あるユーザが、決済アプリのアカウントと、不正入手した銀行口座の紐づけに成功する（紐づけ時の認証強度が弱いと成功してしまう）
・ 悪意あるユーザが店舗に行き、高額の商品を購入し、別ルートで転売する
・ 銀行口座引落しは、不正窃取された銀行口座の持ち主から引落される



■　原因

・　一部銀行で、銀行口座登録時の認証の強度が弱い（口座番号と 4 桁暗証番号のみ）

■　対策例

【予防的対策（特定・防御）】

・　銀行口座等登録時に、認証を高いレベルで行うこと。【サービス②-5】

・　銀行口座情報について銀行で提供する情報との一致確認を検討すること。
【サービス②-4】

・　銀行口座紐付け前に、外部（銀行等）で提供する認証機能を呼び出すこと。
【サービス②-5】

・　連続した登録エラーに対し、アカウントロックを検討すること。
【サービス②-5】

【発見的対策（検知・対応・復旧）】

・　不正利用検知の仕組みを導入すること。【サービス③-1】
（同一口座の複数アカウント登録など）

・　利用時に本人に通知する仕組みの導入（ご利用時の即時メール等）。【サービス④-3】

・　不正利用に関する通報を受け付ける窓口・体制を用意すること。
【インシデント対応②】

リスクシナリオ２：決済系 多重申込等による不正ポイント獲得

■ シナリオ

・ サービス利用により、何らかの予約/キャンセル・何らかの購入/返品等を繰り返すことで、サービス側が意図しない形でポイント等の利益を得る。

■ 脆弱性

・ キャンペーンのポイント付与上限チェックの不備
（アカウント登録時の身元確認が弱い、１人で多重にアカウント登録可能、キャンペーン申込取消時のポイントクリア漏れなど、のサービス仕様不備）

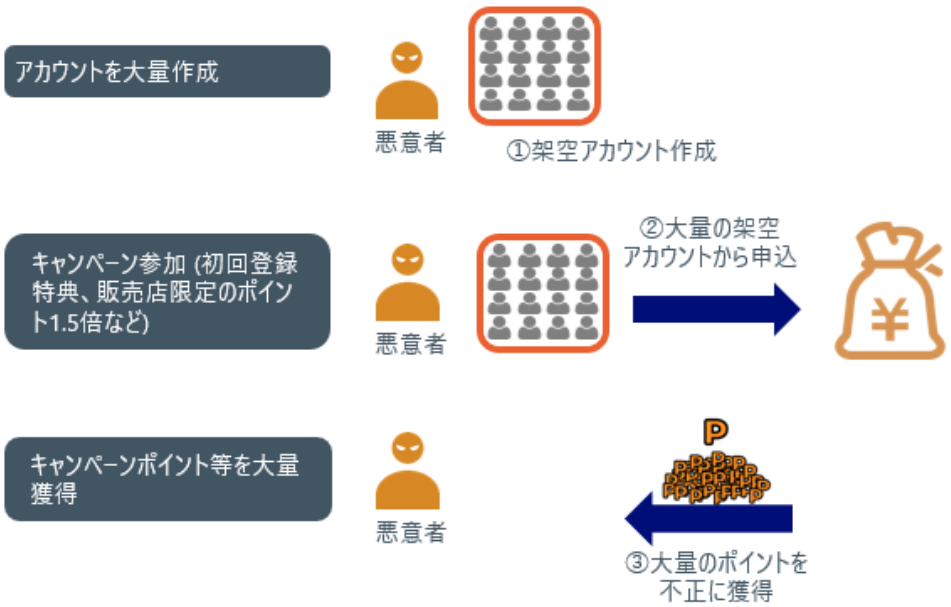
想定されるインシデント例

■ 概要

・ 決済系のアプリ等で、悪意を持ったユーザがアカウントを多重登録（1 人で何件も登録）や、キャンペーンへ多重申込等をすることで、不正にポイントを大量獲得する。

■ 経緯

・ 悪意あるユーザが、キャンペーンのポイント付与上限チェックの不備を発見
（1 人で多重にアカウント登録可能、キャンペーン申込取消時のポイントクリア漏れなど、のサービス仕様不備）
・ 悪意あるユーザが、アカウントを大量作成
・ 悪意あるユーザが、各アカウントからキャンペーンに申込み、ポイントを取得
・ 悪意あるユーザが、キャンペーンに申込取消→再申込を繰り返し、ポイントを取得
・ 悪意あるユーザが、不正取得したポイントで商品を購入し、転売して利益を得る



■　原因

・　アカウント登録時の身元確認が弱い等の理由で、多重登録ができてしまう

・　キャンペーン申込取消時のポイント取消仕様等に不備があり、ポイント増殖ができてしまう

■　対策例

【予防的対策（特定・防御）】

・　アカウント登録時の身元確認を高いレベルで行うこと。【サービス②-4】
（アカウント作成時に１人１アカウントの制限を検討すること）

・　サービスの利用規約の禁止事項に不正利用に関する記述を定義すること。
【サービス②-1】

・　不正利用のリスクの観点を考慮したインセンティブ設計を行うこと。【サービス①】
（アカウント再登録によるインセンティブ獲得や、ポイント即時付与・利用後の返品など）

【発見的対策（検知・対応・復旧）】

・　不正利用の検知の仕組みを用意すること。【サービス③-1】
（同一アカウントでの大量獲得、複数回獲得など）

・　インセンティブ不正取得時の対応手順を整備すること。【インシデント対応③】

リスクシナリオ３：医療系 不正ログインによる保険証画像の窃取

■ シナリオ

・ 悪意ある第三者によるサービスのマイページへの不正ログイン
・ ログイン後、保険証画像を窃取される
・ 偽造保険証を利用し、被害者名義の借り入れによる金銭の不正取得

■ 脆弱性

・ サービスにおける本人確認に利用可能な証明書類画像へアクセスの際の、認証強度が低い。

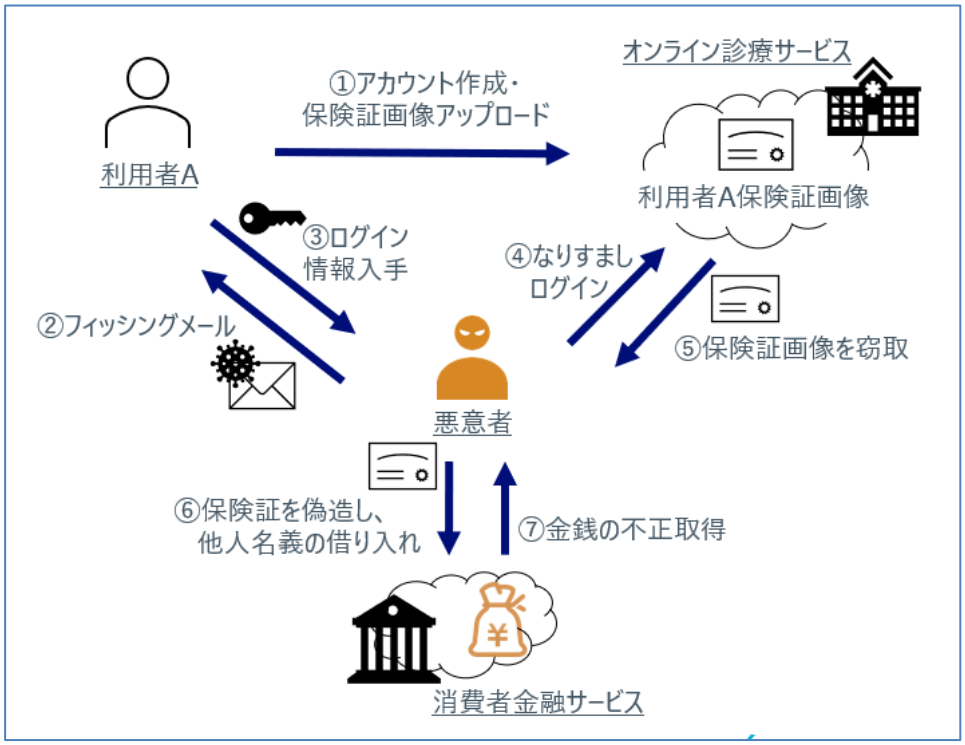
想定されるインシデント例

■ 概要

・ オンライン診療サービスに登録された保険証画像が、キャッシングの本人確認に不正利用され、金銭的被害の発生が想定される

■ 経緯

・ 悪意ある第三者がフィッシングメールにてログイン情報を不正入手
・ 不正入手したログイン情報によりオンライン診療サービスへログイン
・ ログイン後、アップロードされている保険証画像を窃取
・ 窃取した保険証画像を用い、保険証を偽造
・ 偽造保険証を利用し、他人名義の借り入れによる金銭の不正取得



■　原因

・　ログイン後、保険証画像が参照可能なサービス仕様となっている

・　当該サービスへのログイン時、ユーザ認証の強度が低い

■　対策例

【予防的対策（特定・防御）】

・　マイページへのログイン時における多要素認証の実装による認証強化【サービス②-5】

・　重要情報アクセス時の 2 段階認証の実装による認証強化【サービス②-5】

・　アップロード完了後の保険証画像は、閲覧不可の仕様にする【サービス③-1】

【発見的対策（検知・対応・復旧）】

・　マイページログイン時のログ表示および通知【サービス④-3】

・　重要情報アクセス時のログ表示および通知【サービス④-3】

リスクシナリオ４：交通系 デジタルスタンプラリー不正参加

■ シナリオ

・ デジタルスタンプラリーにおいて、悪意ある参加者が GPS 偽装等の不正な手段でスタンプを取得し、容易に景品獲得できる

・ 複数回のスタンプラリー参加が容易にできる仕組みとなっている場合、同一人物による繰り返しの景品獲得が可能

■ 脆弱性

・ スタンプ取得の条件が GPS による位置情報のみであった

・ cookie のみで同一人物による複数回の参加を制限していた

想定されるインシデント例

■ 概要

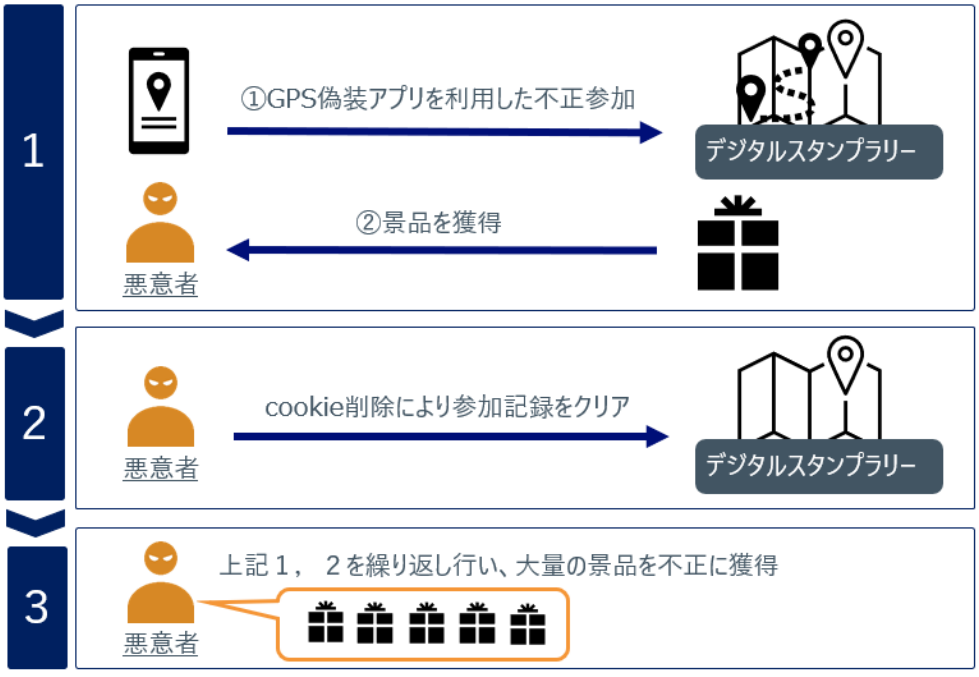
・ デジタルスタンプラリーにて、悪意ある参加者が、GPS 偽装による景品の不正獲得を繰り返し行った

■ 経緯

・ デジタルスタンプラリーにて、悪意ある参加者が GPS の位置情報を操作できるアプリを用いて不正にスタンプを取得し、景品を獲得

・ ブラウザの cookie にて参加記録が保存される仕組みのため、cookie を削除して参加記録をクリア

・ 上記操作を繰り返し行い、大量の景品を不正に獲得する



■ 原因

・ スタンプ取得の条件が GPS による位置情報のみであった

・ 同一人物による複数回の参加を制限する仕組みが甘かった

■ 対策例

【予防的対策（特定・防御）】

・ スタンプ取得条件を GPS 位置情報＋QR コード読み取り等の複数条件とする不正対策を行う【サービス③-1】

・ 複数回の参加を防止するため、アカウント発行による参加を前提条件とする【サービス③-1】

・ 複数回の参加防止の強化策として、マイナンバー等による身元確認を条件とする【サービス②-4】

・ サービス利用規約の禁止事項に不正利用に関する記述を定義し、不正を抑止する【サービス②-1】

・ 不正獲得されることを視野に入れた景品選定を行い、不正目的での参加を抑制する【サービス①】

【発見的対策（検知・対応・復旧）】

・ 不正利用者を自動検出する仕組みの導入を検討する【サービス③-1】

・ インセンティブ不正取得時の対応手順を整備する【インシデント対応③】