参考資料２

スマートシティ
セキュリティガイドライン

（第 1.0 版）

2020 年 10 月

総務省

参考資料２

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・高度化する事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、関係府省庁の連携の下で取組を推進していくこととされている。

他方で、多数のセンサーやカメラ等の IoT 機器が散在し、多様なデータが流通することが想定されるスマートシティは、常にサイバー攻撃のリスクにさらされる恐れがある。また、共通のプラットフォーム上で様々なデータが流通するため、データの真正性確保や適切なデータ流通管理のための仕組みの構築等も求められる。データ管理だけでなく、スマートシティのシステム構築・運用には多様な主体が関わることから、システム全体としてのセキュリティの在り方について、関係者間で一定の共通認識を醸成することが必要となる。

しかしながら、日本国内においては、一般的な IoT システム単体におけるセキュリティについてこれまで多くの調査研究が進められており、ガイドライン等も作成されている一方で、スマートシティのセキュリティに特化した調査研究は十分でなく、ガイドライン等の共通的な指針も示されていないのが現状である。

そのため、今後、様々な地域や地方公共団体において、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、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ワーキンググループでの検討を通じて、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特有のセキュリティ留意事項などについて整理を試みた。

本ガイドラインが、スマートシティに関わるあらゆる主体がスマートシティのセキュリティの在り方について検討・議論するに当たっての参考となることを期待する。

1.2. 目的

本ガイドラインは、多様な主体が複雑に連携し、かつ様々なデータが流通するというスマートシティの特性を踏まえ、各主体が実施・検討すべきセキュリティの考え方を示しつつ、それに関連して発生することが想定される問題とその対策について示すことで、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ものである。

具体的には、本ガイドラインを通じ、各主体の連携において以下の効果が実現することを期待する。

・　本ガイドラインを参照したセキュリティ対策の実行による、スマートシティのセキュリティ、安全性、信頼性及び強靭性（レジリエンス）の確保。[1]

・　各主体間でセキュリティに対する共通認識を醸成することによる、円滑な連携を通じたセキュリティ対策の検討・実施

1.3. 対象範囲

本ガイドラインは、内閣府の戦略的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。）を前提としている。また、技術的な面だけでなく管理的な面でのセキュリティについても記載することで、スマートシティ全体としてのセキュリティが考慮できる様にしている。

本ガイドラインに記載されている考え方や問題、対策例等は、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、網羅的なものとなっていない。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。（外部の規格やガイドライン等については「5.2. 国内外のガイドライン・規格等への対応」に一部を記載する。）また、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問題や考慮すべき点について記載していることに留意する。

その他、本ガイドラインには様々なセキュリティ対策の事例が記載されているが、その対策を誰が実施すべきかについては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、個々のスマートシティごとに検討することを推奨する。

1.4. 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スマートシティ全体を統括するサービスオーナー・推進主体（地方公共団体・事業者等）

②スマートシティ事業に関わる事業者および利用者
- クラウド基盤、都市 OS 等のシステム提供者
- IoT 機器、ネットワーク機器等の機器メーカー

[1]本ガイドラインにおける「安全・安心」は、「セーフティ」・「セキュリティ」及び「リライアビリティ」を含んだ信頼性（Trustworthiness）を実現する概念であり、スマートシティライフサイクルのセーフティ、セキュリティ、リライアビリティが確保されていることである。また、NIST「CPS Framework」では、「セキュリティ」・「安全性」・「信頼性」等と並んで「強靭性（レジリエンス）」が信用性の要素になっている。

・ソフトウェア、アプリケーション等のサービス提供者
・センサーデータ、フィールドデータ等のデータ提供者　等

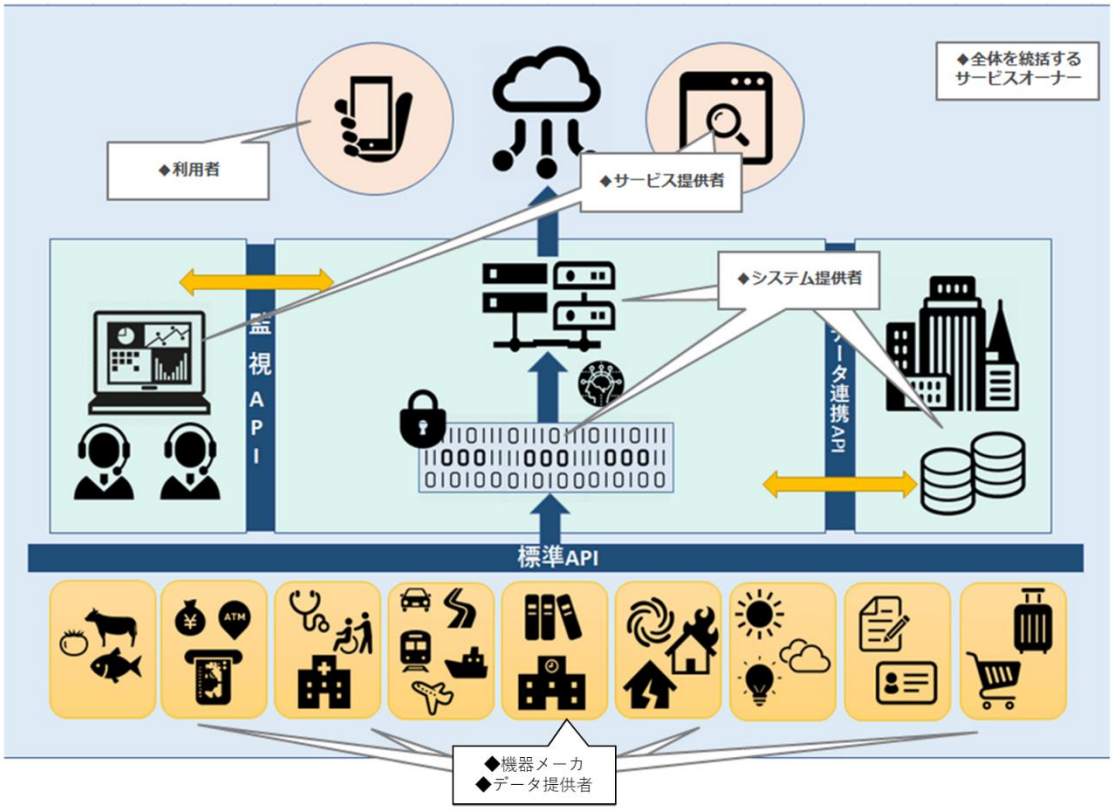


図１　想定読者のイメージ

1.5. 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．各カテゴリにおけるセキュリティ」、「４．スマートシティ特有のセキュリティ留意点」「５．セキュリティ対策要件と対策例」の５章から構成される。

・　１章においては、本ガイドラインの背景、目的、対象範囲、全体構成等を示した。

・　２章においては、スマートシティを実現するリファレンスアーキテクチャとそれに対応する形でスマートシティセキュリティの考え方を示す。

・　３章においては、２章で示した考え方に基づいて分類した各カテゴリにおいて必要とされるセキュリティ対策を示す。

・　４章においては、各カテゴリにおけるセキュリティとは別に考える必要のあるスマートシティ特有のセキュリティ留意点の観点で整理を行い、発生することが想定される問題とその対策を例示する。

・　５章においては、３章、４章の記載内容に対する分野別のユースケースや具体的な対策

例を示す。

1.6. 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。

①１章において、本ガイドラインの背景、目的、スコープ等を理解する。

②２章において、スマートシティのセキュリティに対する考え方を理解する。

③３章において、２章の考え方に基づく具体的に実施すべきセキュリティ対策について理解する。

④４章において、スマートシティの特徴及びそれを踏まえたセキュリティ留意点、リスク、対策について理解する。

⑤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、５章におけるセキュリティ対策例を参考にセキュリティ対策を選択する。

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。

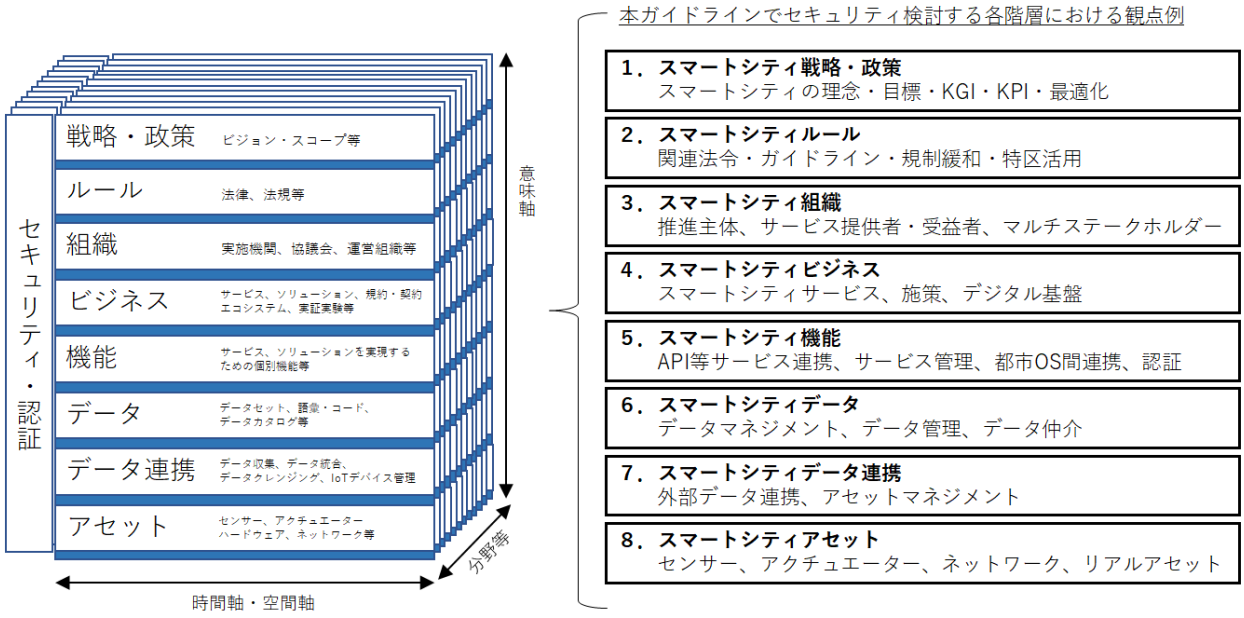


図２－１　Society5.0 のアーキテクチャとスマートシティアーキテクチャの関係

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」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の提示をしており、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がる。

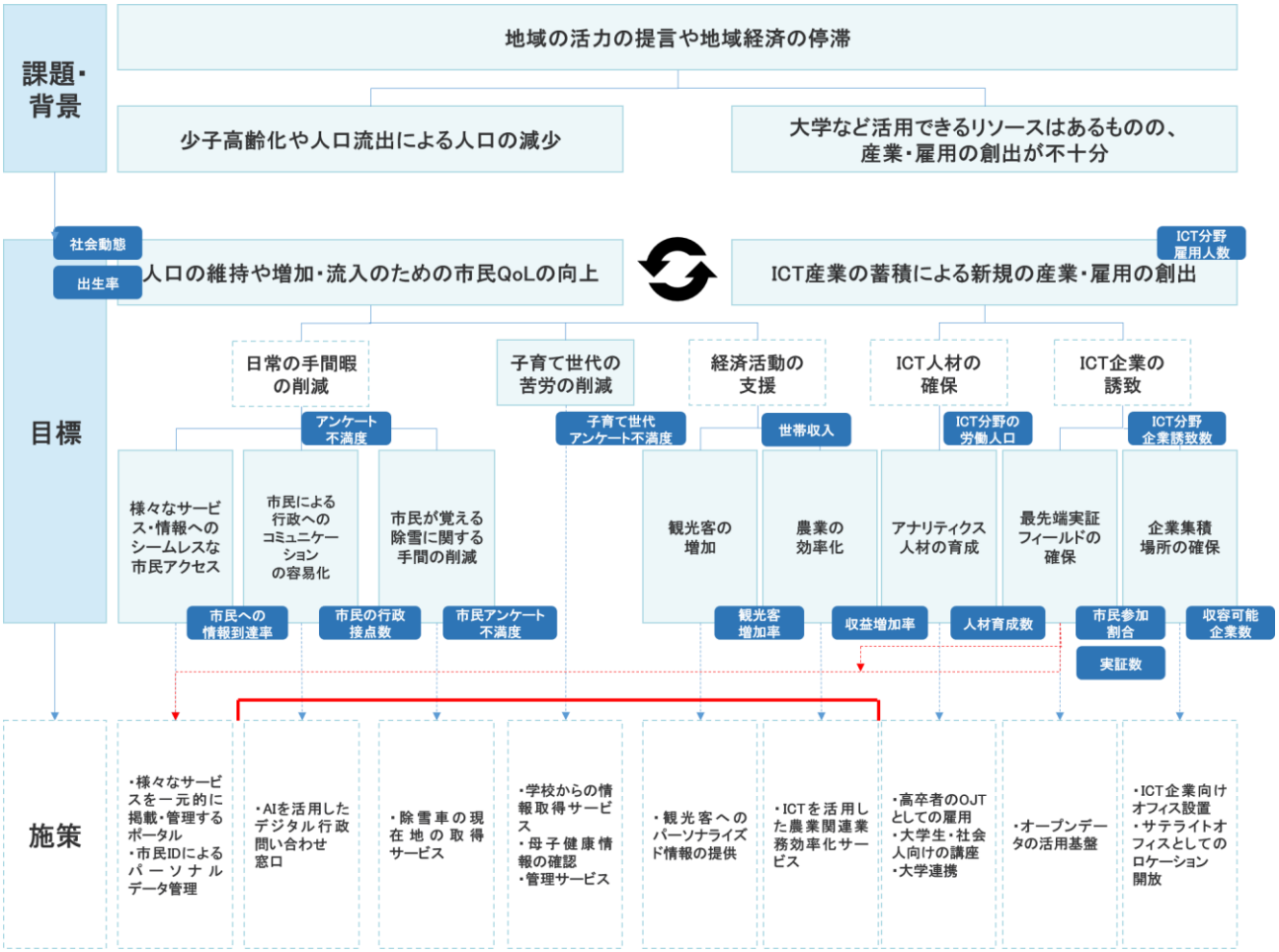


図２－２　スマートシティ戦略のイメージ

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あたっては、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。

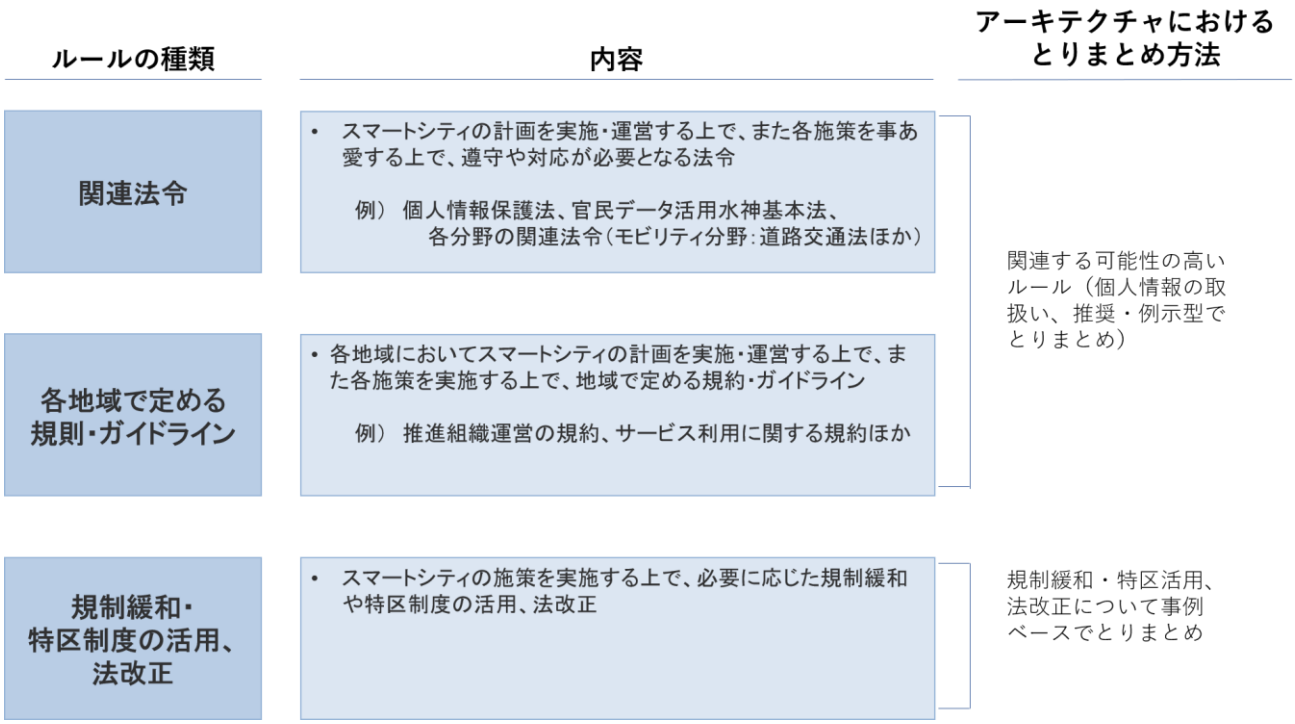
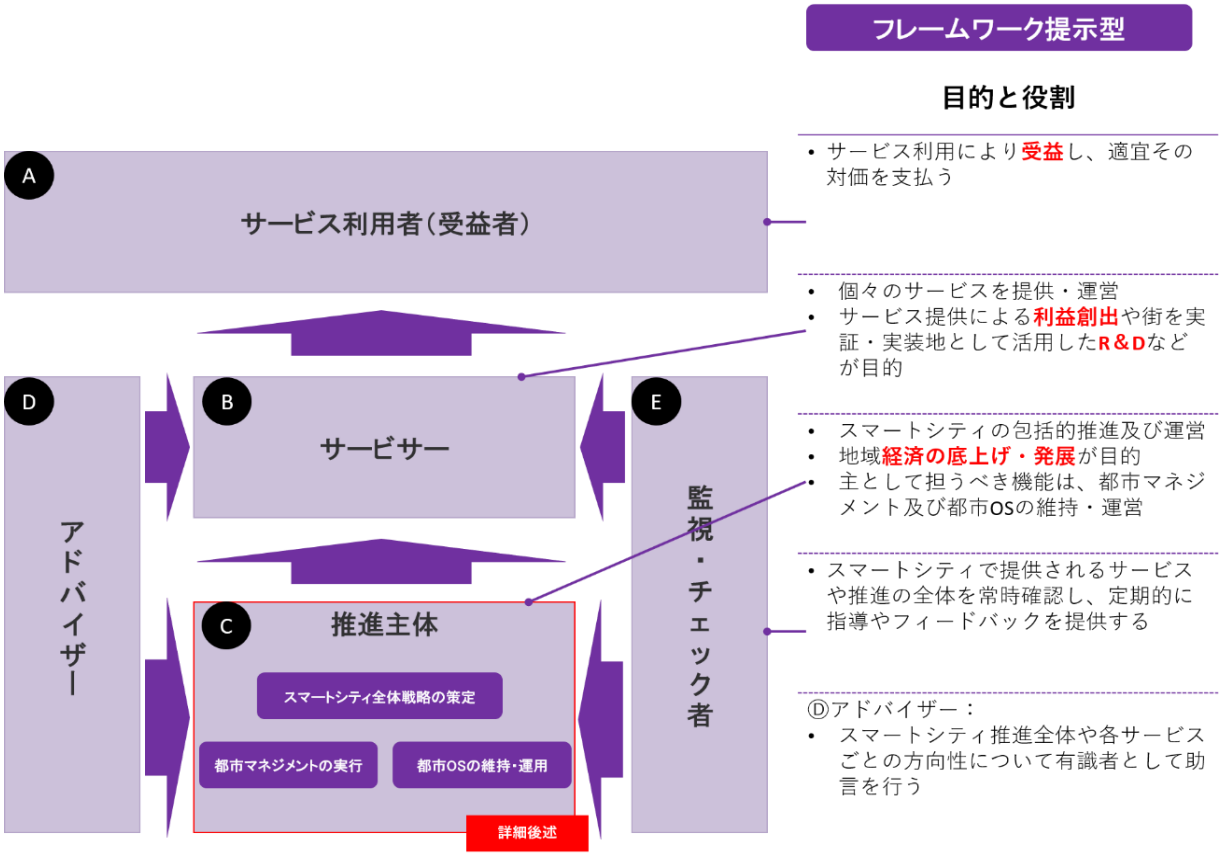


図２－３　スマートシティルールのイメージ

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[2]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ーヤー（ステークホルダー）が構成要素となる。具体的なステークホルダーやその関係性は図２－４を参照されたい。なお、当ガイドラインにおいては、表中のステークホルダーの内、サービス利用者（受益者）を除くスマートシティを推進・運営する主体を「マルチステークホルダー」と呼ぶこととする。

2 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。



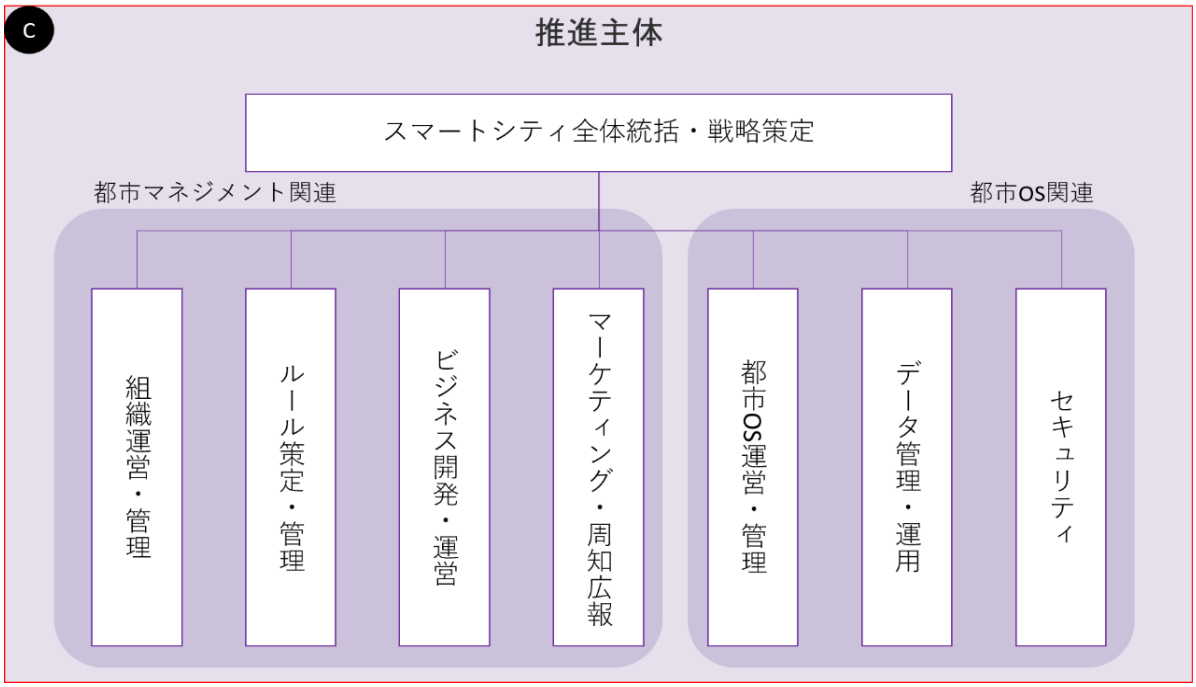


図２－４　スマートシティ組織のイメージ

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、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を構造的に示す「ビジネスモデル」と利用者のニーズに合ったサービスを提供する「体験デザイン」、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する「サービス」で構成される。「サービス」の一般的な例としては、ウェブサイトやアプリを通じた形が挙げられる。

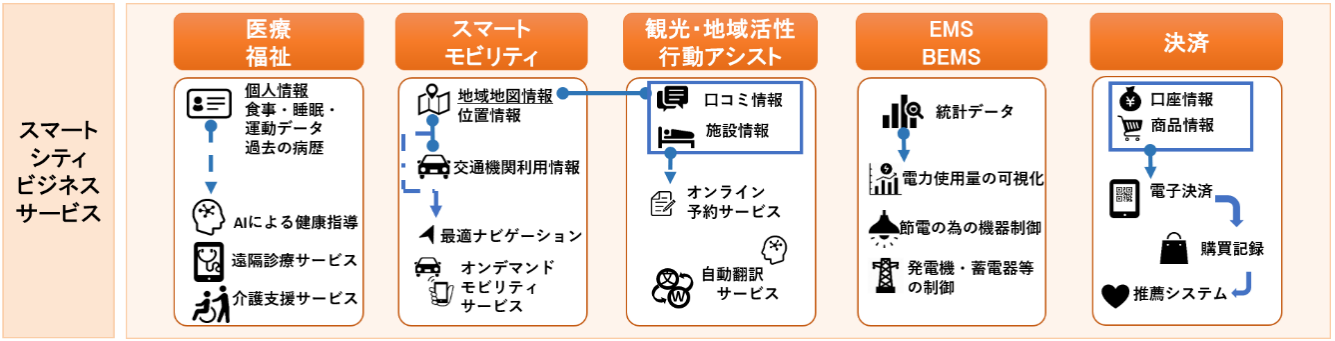


図２－５　スマートシティビジネス・サービスのイメージ

⑤スマートシティ機能

スマートシティ機能は、都市 OS 上で動作する各種スマートシティサービスが、都市 OS や他のスマートシティサービスと連携するための「サービス連携」や、都市 OS の利用者や、都市 OS と連携するアプリケーションや他システムに対して、都市 OS が用途に応じて認証情報を提供する「認証」、都市 OS と連携するスマートシティサービスを管理し、適切に運用するための「サービスマネジメント」が構成要素となる。

⑥スマートシティデータ

スマートシティデータは、都市 OS に保存・蓄積するデータの管理、及び単一都市・複数都市や他システムに分散されたデータを仲介する「データマネジメント」が構成要素となる。

⑦スマートシティデータ連携

スマートシティデータ連携は、データの収集、及び接続するスマートシティアセットや他システムの登録・削除等の管理と、スマートシティアセットへの制御を実行する「アセットマネジメント」、スマートシティアセットや他システムとのインタフェースを管理し、データモデルやプロトコルの差異を吸収しデータ処理、データ伝送する「外部データ連携」の二つが構成要素となる。

※なお、このスマートシティ機能、スマートシティデータ、スマートシティデータ連携の 3 層を総じて「都市 OS」と呼び、この都市 OS は、スマートシティの実施、運営にあたりそ

のシステムの核となるものであり、スマートシティを実現しようとする地域が共通的に活用する機能が集約され、スマートシティで導入する様々な分野のサービスの導入を容易にさせることを実現する IT システムである。

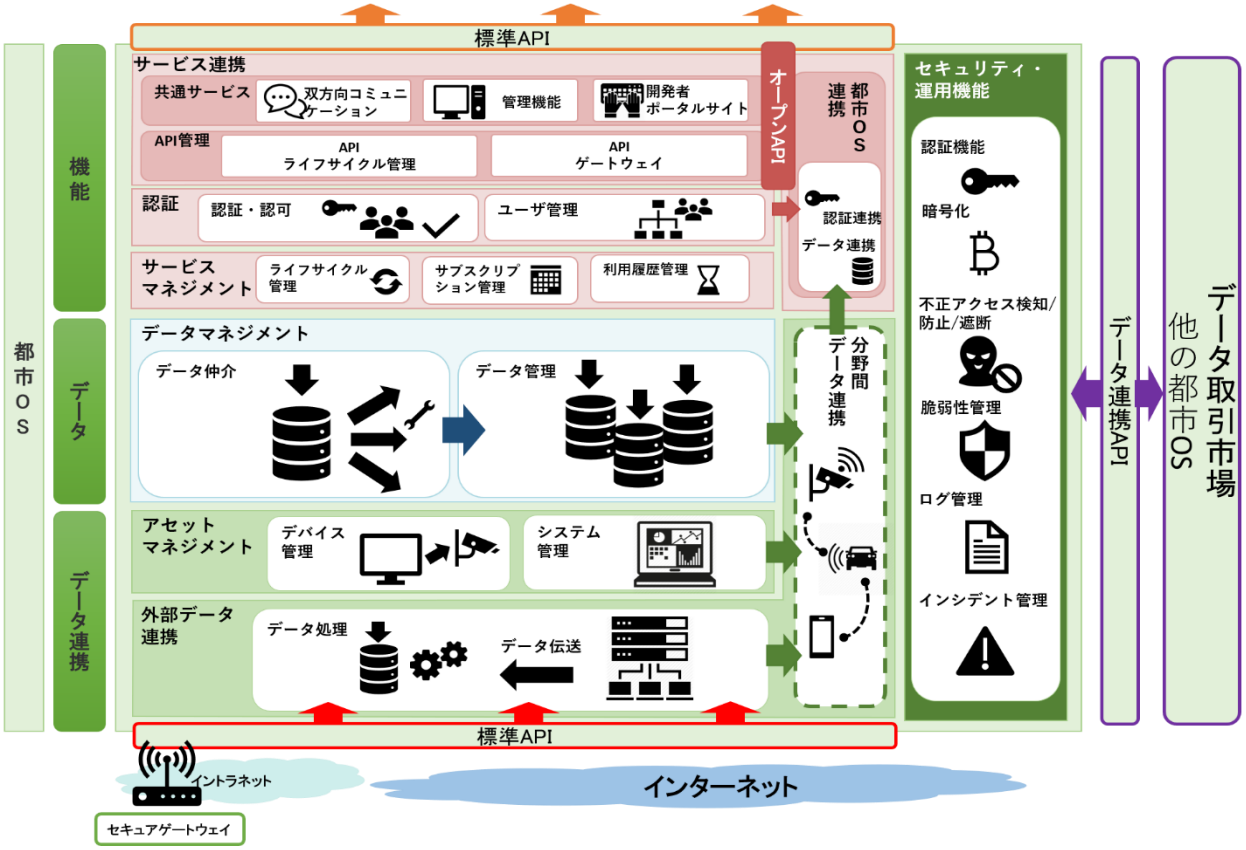


図２－６　都市 0S のイメージ

⑧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 0S 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 0S 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。

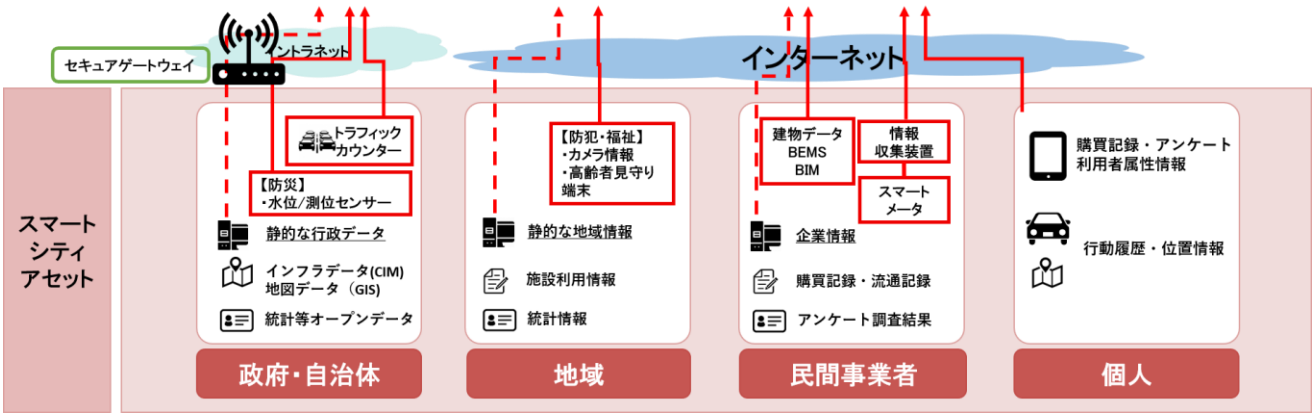


図２－７　スマートシティアセットのイメージ

2.2. スマートシティのセキュリティ検討のアプローチ

本ガイドラインでは、スマートシティの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、そのセキュリティ対策が共通化できる層をカテゴリとして整理した。具体的には、図２－８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対策のポイントと対策例について整理した。

なお、もう一つの観点として、この４つのカテゴリは管理的側面と技術的側面という２つに分類することも可能であり、両方のアプローチからセキュリティを検討することでスマートシティ全体としてのセキュリティ担保を実現することが可能となる。

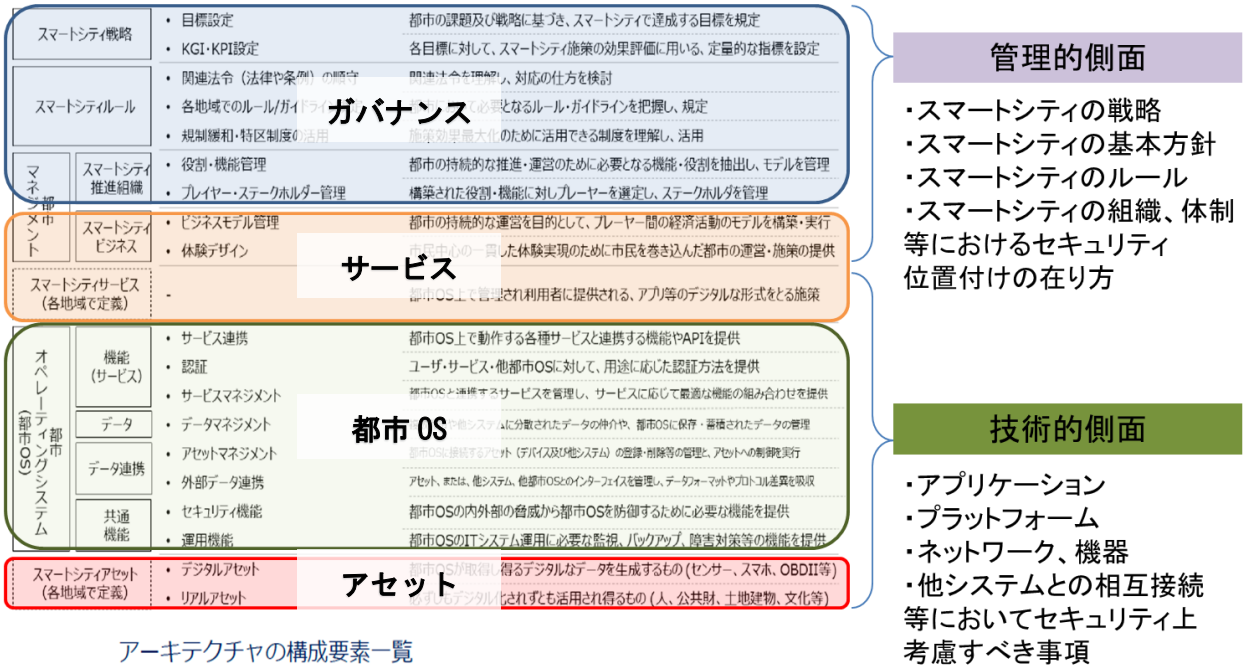


図２－８　スマートシティリファレンスアーキテクチャを踏まえたカテゴリ分け

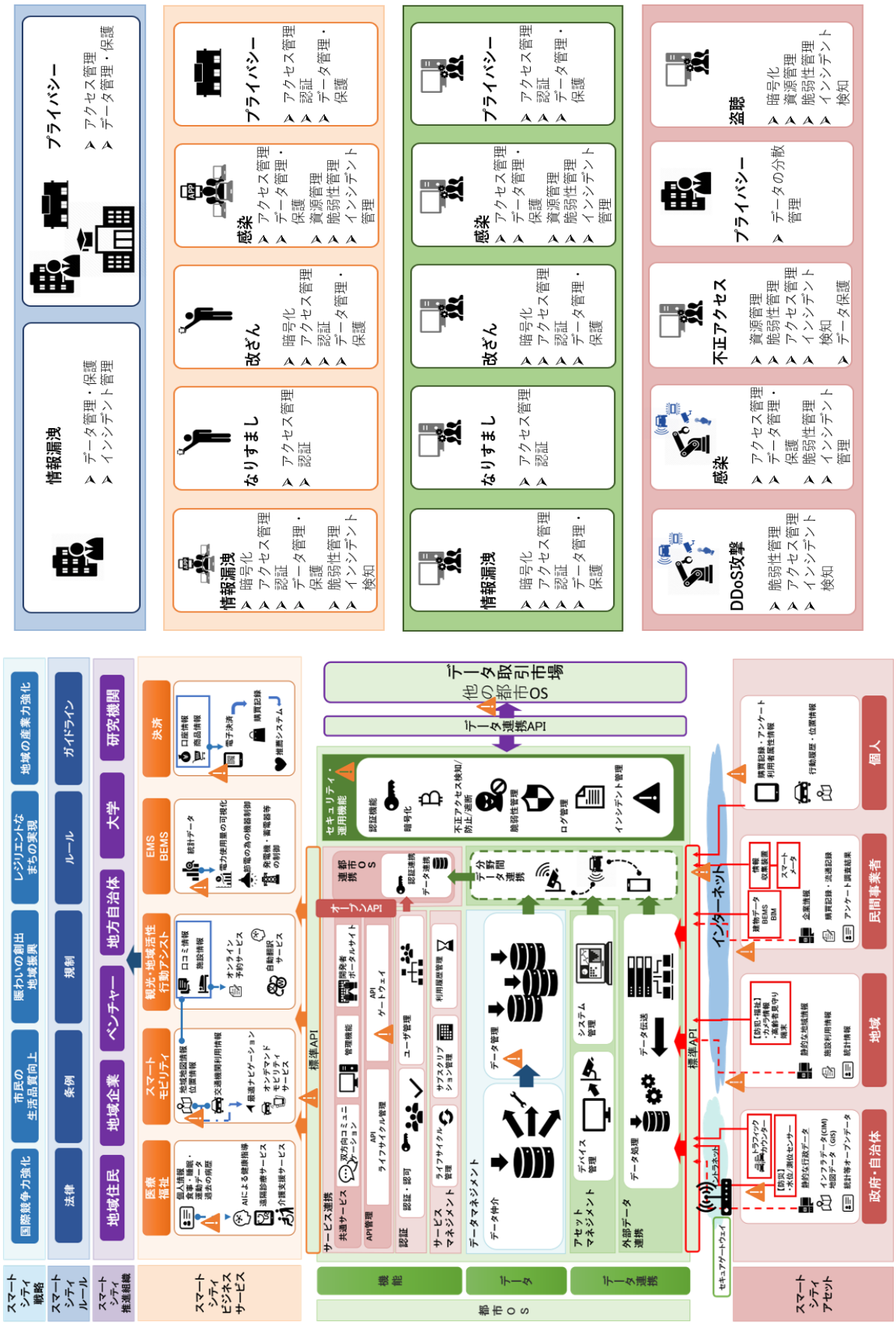


図２－９　各カテゴリにおける脅威とセキュリティ対策例

2.3. 各カテゴリにおけるセキュリティの考え方（概要）

本ガイドラインにて整理した４つのカテゴリにおける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・拡張していくか、どう管理していくか等）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。

大きな運営方針についてはもちろんだが、セキュリティの観点でも、スマートシティ全体としてどのようなセキュリティポリシーを策定するか、求めるべきセキュリティ基準はどうあるべきか、どういった組織体制で運営するか等について、マルチステークホルダー間で共通認識として策定をすることが重要となる。

スマートシティにおけるルールを策定する場合は、個人情報保護法、官民データ活用推進基本法、EU 一般データ保護規則（GDPR）といった国内外の法令や、それぞれの分野における業法やガイドラインを考慮することに留意する。

また、スマートシティをサービスとして継続するためのビジネス継続計画（BCP）についてもマルチステークホルダー間で協議を行い、基本方針やそれぞれの役割、対応手順などについて決定しておくことが望ましい。

②サービス

「ガバナンス」で決めた方向性をサービスに落とし込むカテゴリであり、ここでサービスやビジネスモデルが定義される。セキュリティの観点からは、定義されたサービスを踏まえ、守るべき機能や資産（ファシリティやデータ）を特定することが重要となる。また、ビジネスモデルが定義されることで、マルチステークホルダー間の関係性が明らかになるため、そのモデルを元にセキュリティに関する責任分界点について決定することが重要となる。「都市 OS」「アセット」においては、ここで決めら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。

また、「サービス」においては、利用者にウェブサイトやアプリを通じてサービス提供されるケースがあるが、その場合はここでユーザとの接点が生じることから、それらアプリのセキュリティについても検討し、実装することが求められる。

なお、上述のビジネスモデルに関しては、スマートシティを運営していく上で徐々に形が変わっていくことが想定されるため、その変化するビジネスモデルに応じてセキュリティの在り方も都度検討する必要がある。また、アプリ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。

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一般的なクラウドセキュリティの対策（認証管理、アクセス制御、データの保護、システムやセキュリティの監視、脆弱性管理等）が求められる。

都市 OS は「サービス」、「アセット」や他の都市 OS などの外部システムと接続点を持ち、多様なデータの流通が発生することから、都市 OS 外との通信を行う上で暗号化や安全なプロトコルを利用することについても留意する必要がある。

また、都市 OS のプラットフォームとして、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 が求めるサービスレベルについてよく検討したうえで、そのサービスレベルを満たすだけの堅牢性や可用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。

なお、都市 OS 内における分野を超えたデータ連携や、他の都市 OS と連携した際のデータの管理の在り方に関しては、まだ国内における実証や議論が十分でないことから、今後、当ガイドラインを改定する際に記載を検討・反映していく。

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、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。

提供するサービスによって IoT 機器や取り扱うデータなどが多様化されることが想定されるため、全ての機器に対して共通のセキュリティ対策を期待することが困難であるが、全てのデータの根源ともなることから、完全性が比較的重視されるカテゴリでもある。そのため、機器の異常を検知することや、機器を物理的に保護すること、インターネットを経由して外部と通信をする際は暗号化を行うこと等が求められる。

なお、完全性以外の観点では、取り扱うデータに個人情報などの秘匿性の高い情報が含まれる場合、機密性にも十分留意する必要があるし、アクチュエータの制御等、物理的に大きな影響を与えるようなサービスの場合は人命保護の観点から可用性にも留意する必要がある。

3. 各カテゴリにおけるセキュリティ

3.1. 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ものであり、セキュリティの文脈では、スマートシティ全体としてのセキュリティに関する取組方針・基本方針などのポリシーの策定、平時のセキュリティ対策や有事のセキュリティ対処のルール化、セキュリティ対応組織の構築などが挙げられる。

＜ポイント＞

① リスクアセスメント、及びデータライフサイクルを考慮した、自組織およびサプライチェーンに係るセキュリティに関する基本方針を定めると共に、セキュリティ対策基準、責任範囲、リスク許容水準等を整備し、マルチステークホルダー間で適宜共有する。

② 自組織におけるセキュリティ上の役割と責任、情報の管理体制および共有方法等を整備する。

③ 個人情報保護法、官民データ活用推進基本法、GDPR 等の国内外の法令や、それぞれの分野における業法や業界ガイドラインを考慮したルールを整備する。

④ スマートシティ提供を継続する上で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およびレジリエンス（回復）を検討する。

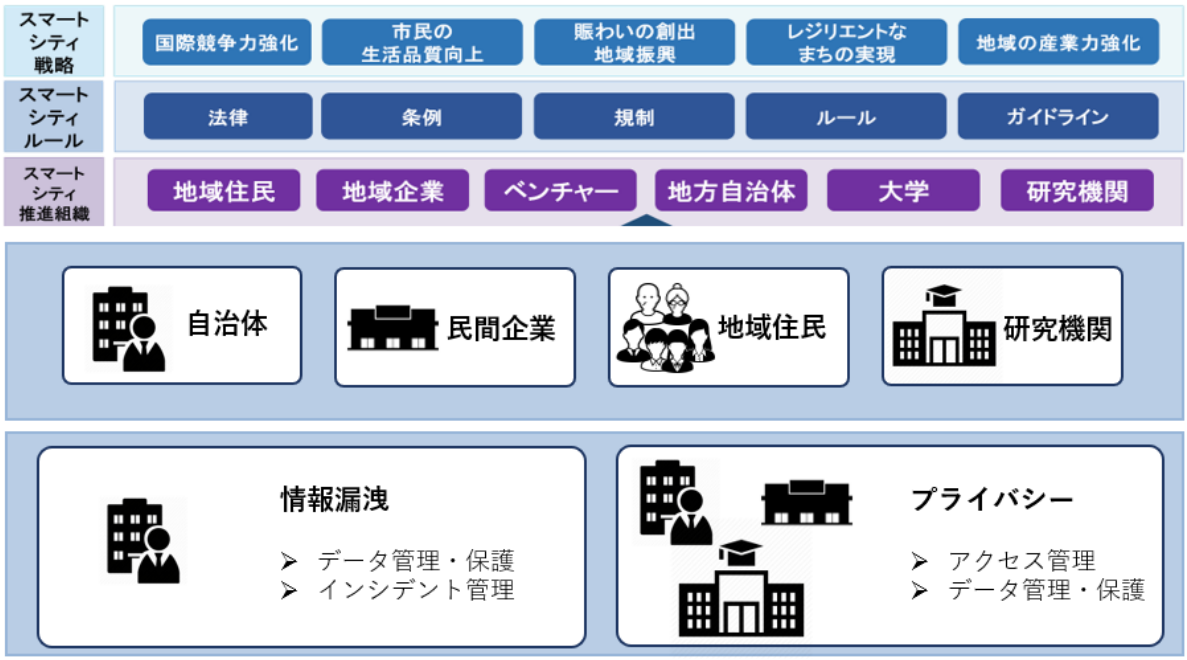


図３－１　ガバナンスのイメージ図

＜対策例＞

①リスクアセスメント及びデータライフサイクルを考慮した、自組織およびサプライチェーンに係るセキュリティに関する基本方針を定めると共に、セキュリティ対策基準、責任範囲、リスク許容水準等を整備し、マルチステークホルダー間で適宜共有する。

スマートシティの実施・運営にあたり、想定されるセキュリティリスク、またそのリスクが引き起こす影響を評価し、どのような対応をするか、どのようなセキュリティ対策を実施するかを検討する。この一連の作業をリスクアセスメントといい、そのセキュリティ対策は自組織だけでなくサプライチェーンに係る様々な組織においても、その役割や責任範囲を明確化したうえで取り組む必要がある。

また、セキュリティ対策内容を検討する際には、取り扱うデータのデータライフサイクルを考慮したうえで、サプライチェーンを含めたセキュリティポリシーや基準の整備を行う必要がある。例えば、委託先との間での役割や情報取扱いに関する責任範囲を明確化した契約文書を作成し、事前に双方が同意した上で取り組みを進めることや、スマートシティの取組におけるセキュリティ上のリスクを洗い出し、必要となる対策を検討することなどが考えられる。

②自組織におけるセキュリティ上の役割と責任、情報の管理体制および共有方法等を整備する。

「サービス」、及び「都市 OS」で提供されるシステムにおいて、自組織がどのような対応をするのかを事前に明確化しておくことで、有事の際に対策が後手に回り被害の影響が大きくなる可能性を低減する。

また、スマートシティの取り組みにおいては、多くの関係者が存在し、かつ、複雑な関係となっているため、情報の管理や共有方法を整備し、マルチステークホルダー間で理解する必要がある。例えば、自組織及び関係する他組織における役割（最高情報セキュリティ責任者や統括情報セキュリティ責任者等の設置）や情報取扱いに関する責任範囲を明確化した契約文書を作成し、事前に双方が同意した上で取り組みを進める。

③個人情報保護法、官民データ活用推進基本法、GDPR 等の国内外の法令や、それぞれの分野における業法や業界ガイドラインを考慮したルールを整備する。

自組織内で考案したルールやセキュリティ対策のみを実施する場合、本来対策すべき観点が漏れていたり、対策内容が不十分となったりする可能性がある。そのため、国内外の法令上や、業界標準となるようなセキュリティガイドライン等を考慮した上で、最低限のルールやセキュリティ対策を策定する必要がある。

セキュリティ対策を検討する上で、考慮することが推奨される法令やガイドライン等を以下に例示する。

－個人情報保護法

－不正競争防止法
－官民データ活用推進基本法
－サイバー・フィジカル・セキュリティ対策フレームワーク
－IoT セキュリティガイドライン
－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
－EU 一般データ保護規則（GDPR）

④スマートシティ提供を継続する上で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およびレジリエンス（回復）を検討する。

スマートシティを運用していく上で、システムの異常や外部からの不正アクセス、情報漏洩などのインシデントが発生した際に、自組織及び関係する他組織が適切に対応し、早急なサービスの復旧を行うことが重要である。

また、レジリエンス(回復)を行うにあたり、異常や障害が発生した対象における重要度や、他組織、他システムとの依存関係を事前に整理することで、最適な対応を行うことが可能となる。例えば、スマートシティを構成する各システムや機能、機器、取り扱う情報等の重要度やリスクの大きさを整理することで、インシデント発生時の判断ミスを抑え、速やかなインシデント対応や情報連携を実現することができる。

3.2. サービス

本カテゴリは、「ガバナンス」で決めた方向性をサービスに落とし込むカテゴリであり、サービス・ビジネスモデルの定義や、サービス提供のためのアプリケーションの在り方について検討がなされる。

サービスやビジネスモデルごとに重要度や取り扱う情報が異なるため、当該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、それらを適切に守るためのセキュリティ対策を講じる必要がある。

＜ポイント＞

① 提供するサービス等について、守るべき本来機能や情報等を特定する。
② 企画、設計・開発段階で、サービスのコンテンツ改ざんやサービスに対する不正なコマンド入力等に関する脆弱性を排除する
③ アプリケーションに対する不正なコマンドやリクエスト等を確認または監視する。

参考資料２

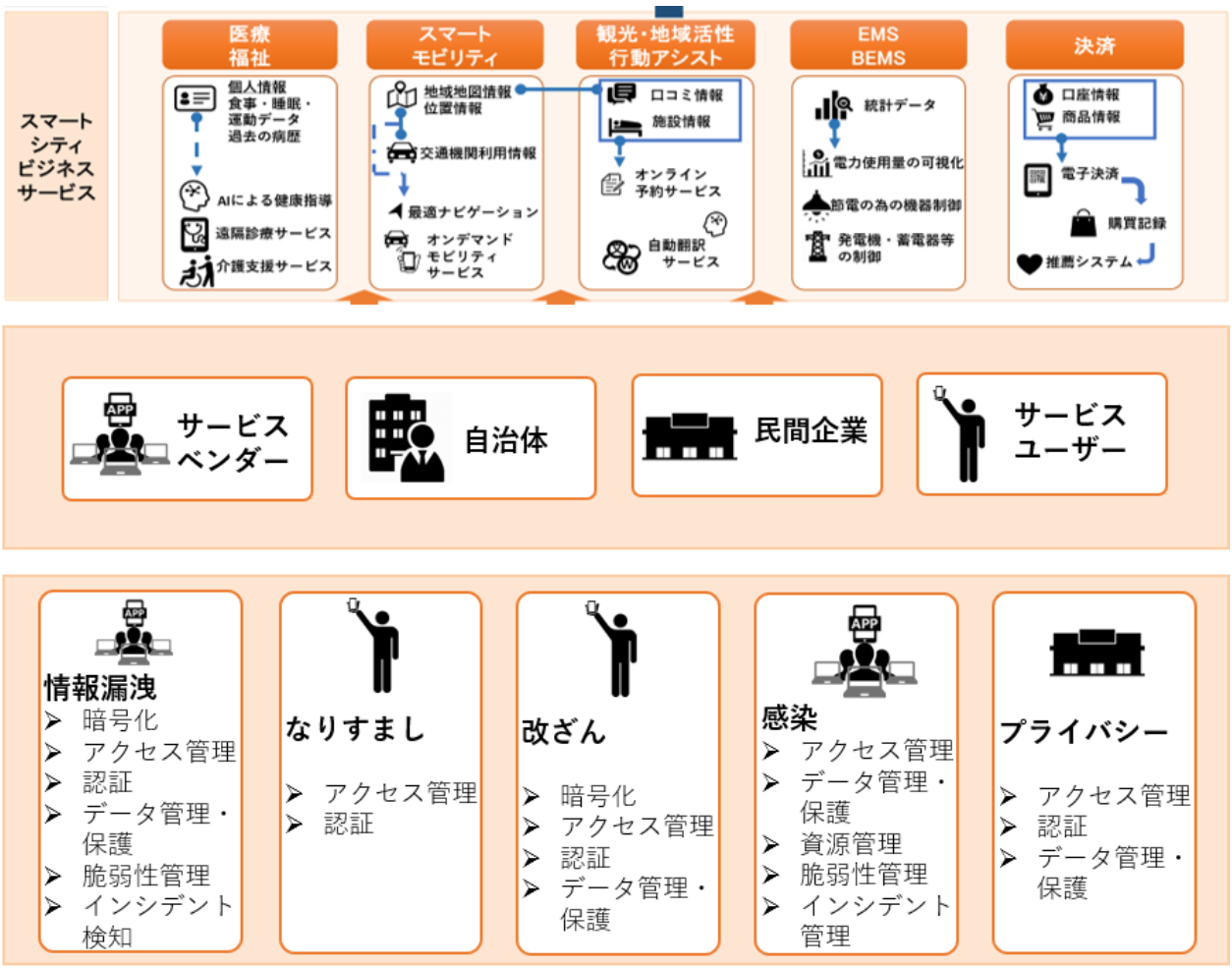


図３－２　サービスのイメージ図

＜検討イメージ＞

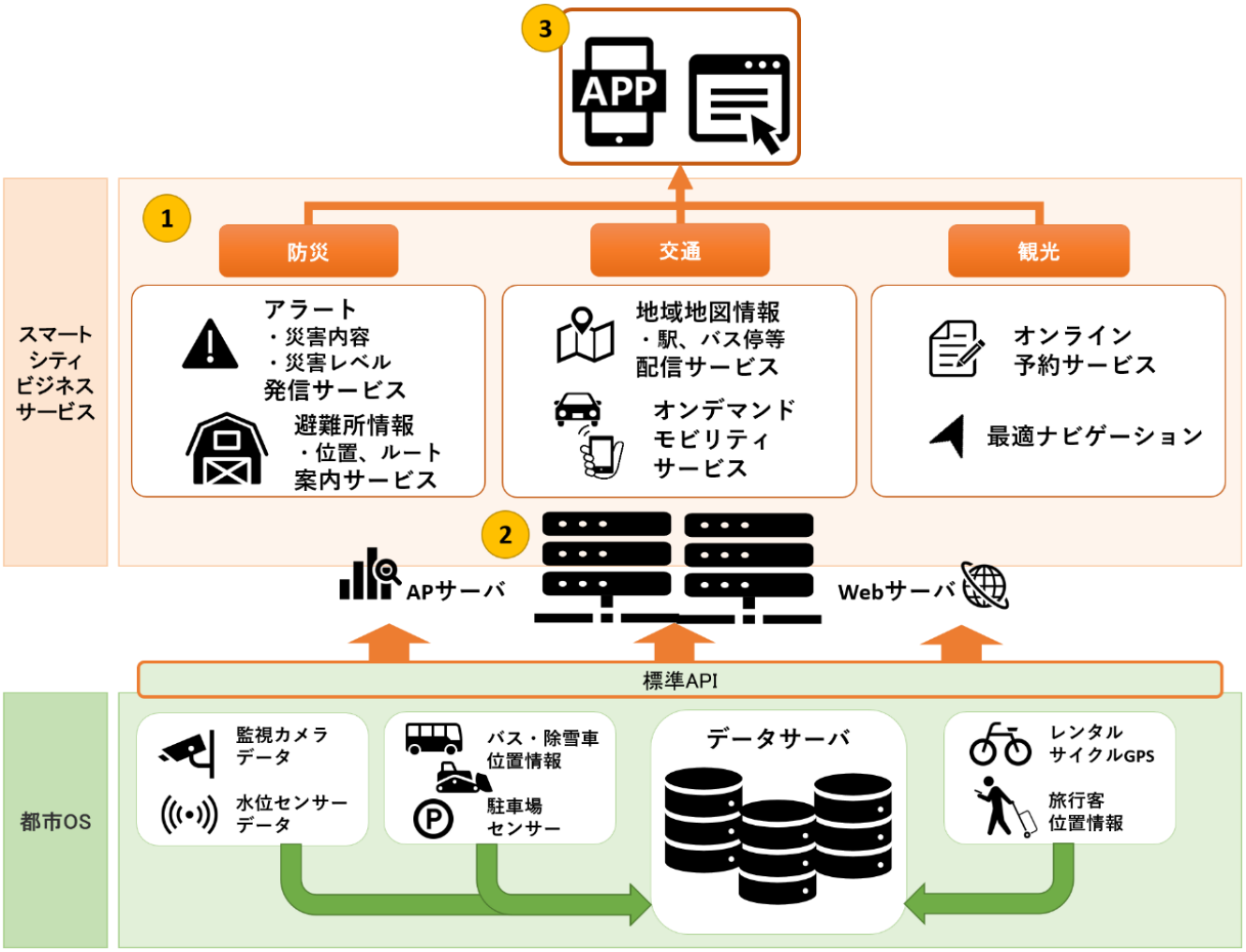


図３－３　「サービス」のセキュリティ対策検討イメージ

＜対策例＞

① 提供するサービス等について、守るべき本来機能や情報等を特定する。

「サービス」のカテゴリで提供される機能（通信、表示、データ、制御コマンド）や情報（プライバシーを含む個人情報、所有する設計情報等）を洗い出す。なお、情報資産の漏えい・改ざん以外のセキュリティの脅威として、スマートシティのサービスを踏み台やボットとして他のシステム等への攻撃に利用されるリスクや、提供するサービス自体を不正操作されるリスクがある。

表３－１　組込みシステムで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（商用コンテンツ利用時の著作権管理データおよびプライベートコンテンツ等）、コンテンツ利用履歴（コンテンツ利用履歴も保護することが重要）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等）、ユーザ認証情報、利用履歴等
機器情報	情報家電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ガイド」を基に作成

②企画、設計・開発段階で、サービスのコンテンツ改ざんやサービスに対する不正なコマンド入力等に関する脆弱性を排除する

１．安全・安心な設計の検証・評価

前項で記載したサービスのカテゴリにおける様々なアプリケーションなどの提供において守るべき機能や情報等の特定に対し、安全・安心対策のレベルに応じた検証・評価を行う。検証・評価にあたっては、各業界における様々な規格や基準の要求事項や、第三者認証などの客観的な評価も活用可能である。

２．認証機能の導入

サービス利用者を制限する必要がある場合など、サービス利用前に利用者の本人確認認証を行う必要がある。不正アクセスやなりすましへの対策として、知識情報（識別子、パスワード）、所持情報（IC カード、クライアント証明書、SMS 認証）、生体情報（静脈認証や光彩認証）による認証等があるが、セキュリティを高めるためには、これらの中から複数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。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・電子証明書等を使用した認証が重要となる。

３．初期設定

スマートシティサービスの提供者として、導入・接続にあたりパスワードの設定・管理や、不要なサービス・ポートの停止、アクセス制御の適用、ソフトウェアのアップデートを実施する等、適切な初期設定に留意する。

４．暗号化

外部への情報漏洩を防止するため、サービスのカテゴリにおけるアプリケーションなどで保持するデータやインターネットを経由する外部との通信を暗号化する。その際、暗号機能の適用にあたっては、「CRYPTREC 暗号リスト(電子政府推奨暗号リスト)」などで定義される適切な強度の暗号アルゴリズム、ハッシュ関数を採用する。

③アプリケーションに対する不正なコマンドやリクエスト等を確認または監視する。

アプリケーションにおける不具合や攻撃などによる異常な動作が発生した場合、影響の拡大を防ぐためにまず異常な状態を検知できるようにする必要がある。例えば、利用者からの入力を受け付けるようなサービスの場合、通信の中に、サービスに対して想定外の影響を与える不正なコマンドが含まれていないかを確認する必要がある。

3.3. 都市 OS

本カテゴリは、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」から収集した情報を分類、蓄積し、「サービス」や他の都市 OS へデータを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 は原則として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いう観点から、一般的なクラウドセキュリティの対策を実施することが求められている。その他、都市 OS 内部でのデータ流通の確保や、取り扱っているデータの保護が求められるほか、他のカテゴリとの接続点において、障害の少ない構築／運用とデータ保護のためのセキュリティ対策の検討・実施が本カテゴリで求められる役割となる。

＜ポイント＞

① インターネットを経由する外部との通信は暗号化する。
② 外部から都市 OS への通信は、適切なアクセス制御を実装する。
③ 都市 OS の保守・運用者によるアクセスは、本人確認のための認証を行う。
④ 個人情報などの重要な情報を保存している場合は、暗号化して保存する、不要な情報は削除する等、適切に管理する。
⑤ サーバ OS やミドルウェア、ソフトウェア等のバージョンを最新状態に保つ。
⑥ システムの状態を監視し、システムに異常が発生したことを検知する。
⑦ 機器の状態を監視し、機器に異常が発生したことを検知する。

参考資料２

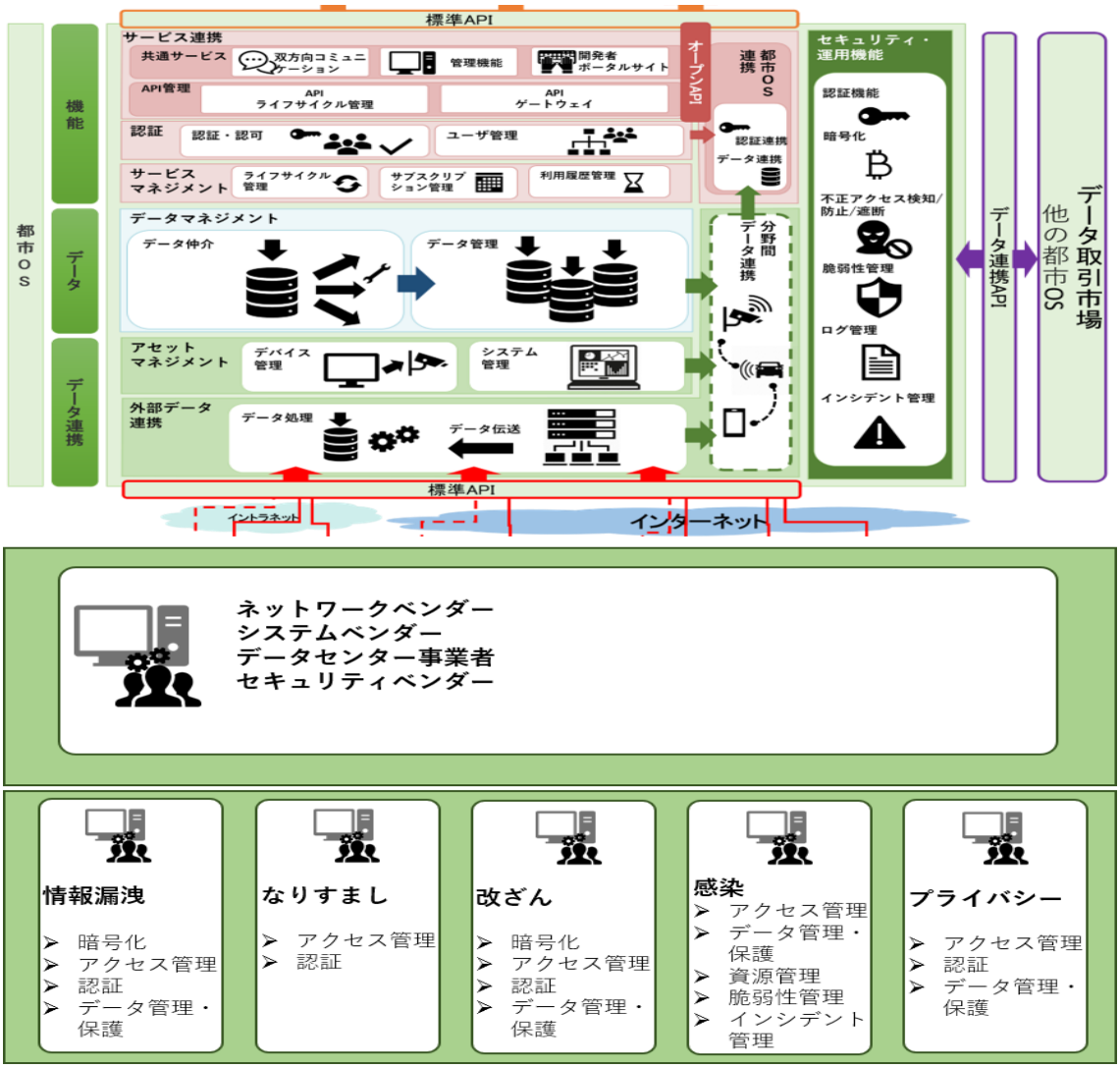


図３－４　都市 OS のイメージ図

＜検討イメージ＞

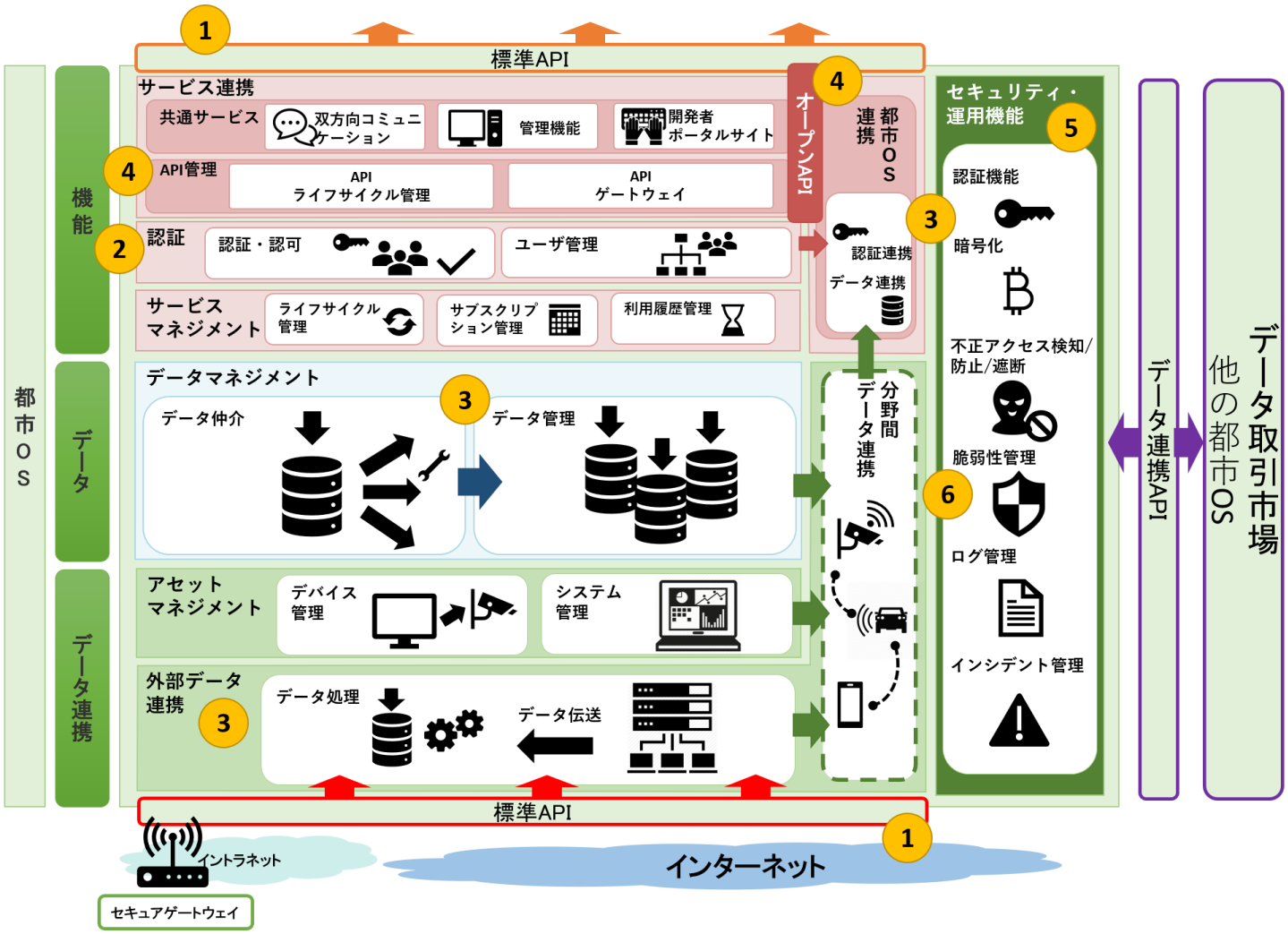


図３－５　「都市 OS」のセキュリティ対策検討イメージ

＜対策例＞

①　インターネットを経由する外部との通信は暗号化する。

インターネットを経由する外部ネットワークとの通信の場合は、悪意のある人物に盗聴されたり、通信データを改ざんされたりする可能性があるため、API によるデータ連携、サービスやアセットとの通信を暗号化する必要がある。

②　外部から都市 OS への通信は、適切なアクセス制御を実装する。

都市 OS に対する不正侵入や脆弱性を悪用したサイバー攻撃を防ぐためには、第三者が容易に都市 OS にアクセスできないように、適切なアクセス制御を実装する必要がある。例えば、通信元・通信先を限定する、不要なサービスやポートの利用を停止する等により、必要最低限なアクセスに限定することが重要となる。

③ 都市 OS の保守・運用者によるアクセスは、本人確認のための認証を行う。

都市 OS へアクセス可能な人物を一意に特定するための認証の仕組みを導入する。なお、認証の種類として知識情報（識別子、パスワード）、所持情報（IC カード、クライアント証明書、SMS 認証）、生体情報（静脈認証や光彩認証）による認証等があるが、セキュリティを高めるためには、これらの中から複数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。

④ 個人情報などの重要な情報を保存している場合は、暗号化して保存する、不要な情報は削除する等、適切に管理する。

個人情報などの重要な情報を保存している場合は、基本的にはその情報にアクセスできる人物を制限し、適切に制御する必要がある。

しかし、物理的に持ち出されたり、不正にアクセスされたりするリスクも完全に排除できないことから、都市 OS 内にそういった情報を保存する際にはデータを暗号化して保存する必要がある。暗号化をする際は、AES128bit 以上や、SHA-256bit 以上など「CRYPTREC 暗号リスト(電子政府推奨暗号リスト)」で定義されている安全な暗号化プロトコルによる暗号化を行う。

⑤ サーバ OS やミドルウェア、ソフトウェア等のバージョンを最新状態に保つ。

サーバ OS やミドルウェア、ソフトウェアは、日々脆弱性が発見され、その脆弱性への対策を行ったパッチがベンダから公開されている。

悪意を持った人物による不正アクセスや脆弱性を突いた攻撃からシステムを保護するために、サーバ OS やミドルウェア、ソフトウェアのバージョンを適宜アップデートし最新化する必要がある。また、サーバ OS やミドルウェア、ソフトウェアの提供ベンダから配信される脆弱性情報を継続的に収集し、必要に応じてパッチ適用等の対応をする。

⑥ システムの状態を監視し、システムに異常が発生したことを検知する。

システムの障害のみならず、不正アクセスや改ざん、不正プログラムの混入、データ破壊といった、システムへのサイバー攻撃によるシステム異常の発生に備え、その異常を発見するための機能を実装することが重要となる。

影響範囲の拡大を防ぎ、システムを早く回復させるために、システムの重要性やシステムに異常が発生した際に想定されるリスクの大きさに従って適切に監視を行う必要がある。

・　システムの状態を監視し、システムエラーや想定外の事象などの異常が発生したことに気がつくようにする。
・　システムの異常を検知した際に、適切に対応することができるよう、初動から事態収束までの運用・管理手順を作成し、必要に応じて適宜評価や見直しを行う。

⑦ 機器の状態を監視し、機器に異常が発生したことを検知する。

リファレンスアーキテクチャでは、都市 OS の機能の一つにアセットマネジメントが定義されており、機器の状態監視も都市 OS に求められる役割の一つとなる。

機器への不正アクセスや盗難、故障など、機器に異常が発生した際には、その異常に気付けることが重要である。そのためには、影響範囲の拡大を防ぎ、サービスを早急に回復させるために、機器の重要性や機器に異常が発生した際に想定されるリスクの大きさに従い、適切に監視を行う必要がある。

・　機器の状態を監視し、機器のエラーや想定外の事象などの異常が発生したことに気付けるようにする。
・　機器の異常を検知した際に、適切に対応することができるよう、初動から事態収束までの運用管理手順を作成し、必要に応じて適宜評価や見直しを行う

3.4. アセット

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、物理的なデバイスや、「都市 OS」にデータを流通させるためのネットワークや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。

＜ポイント＞

① 機器のファームウェアやソフトウェアのバージョンを最新状態に保つ。
② インターネットを経由する外部との通信は暗号化する。
③ 機器を物理的に保護する。

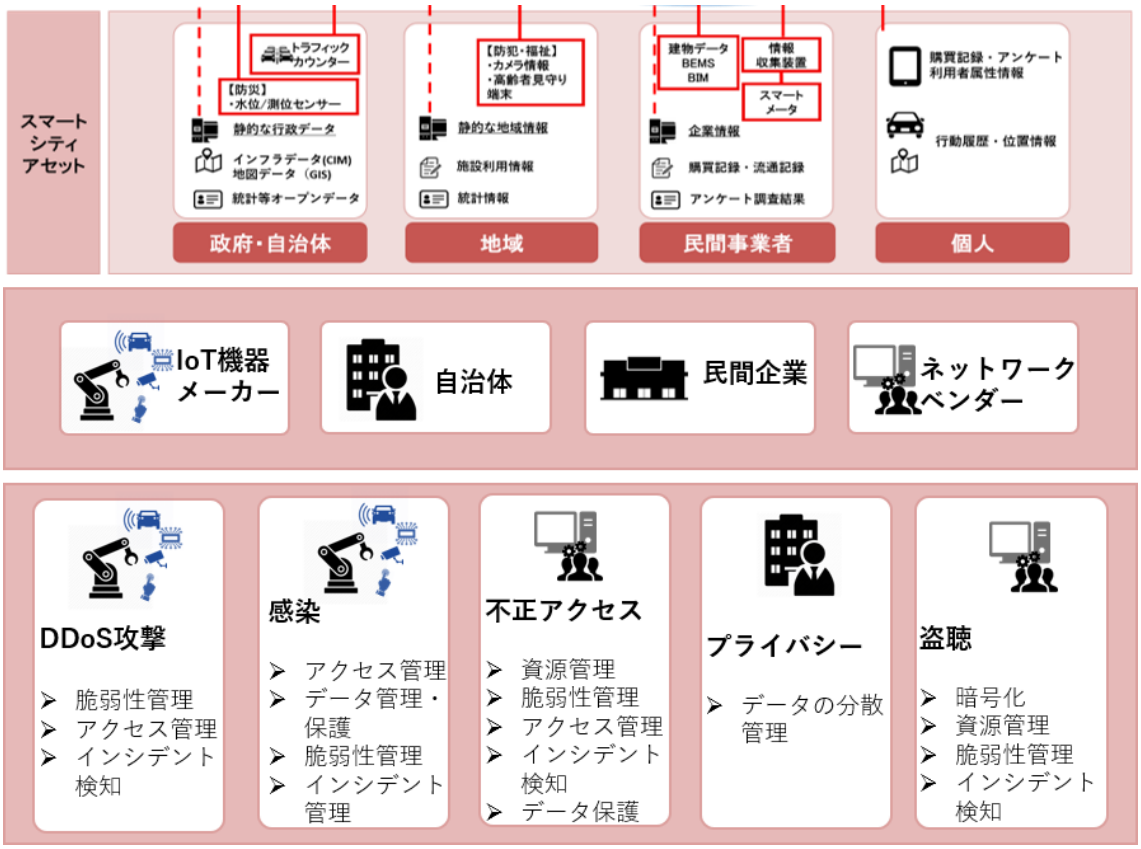


図３－６　アセットのイメージ図

＜検討イメージ＞

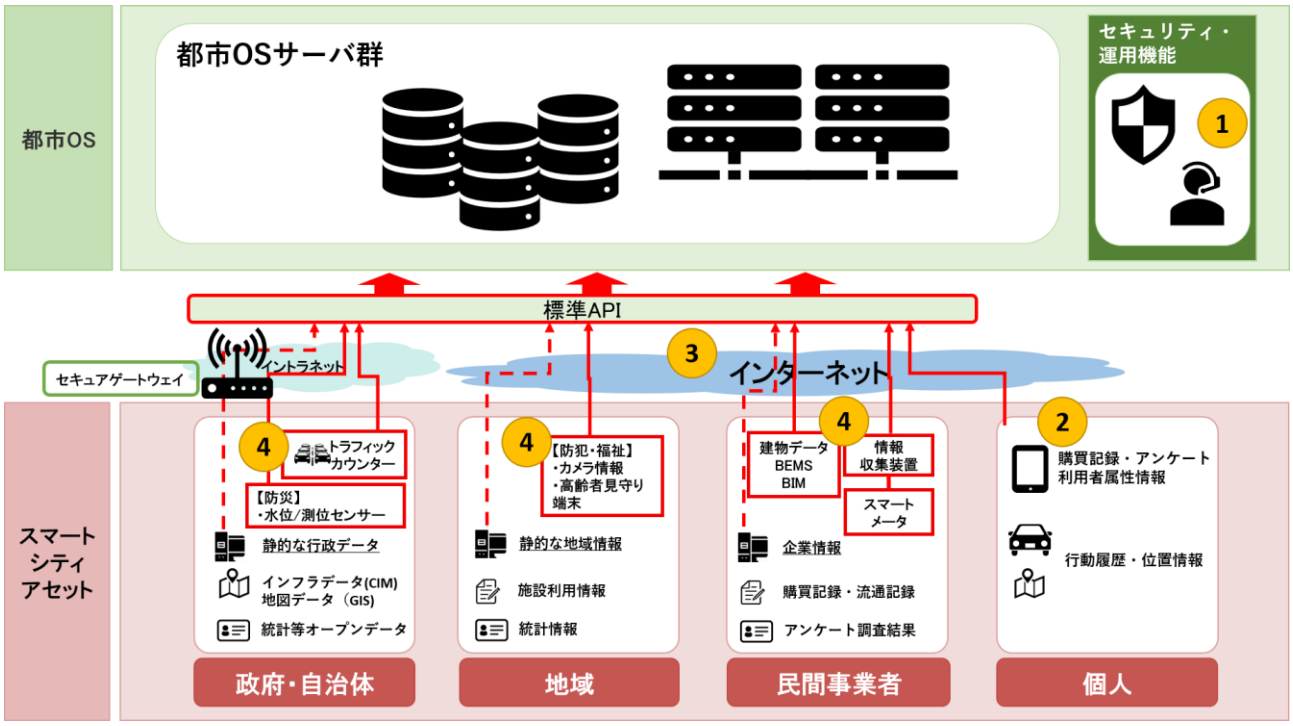


図３－７　「アセット」のセキュリティ対策検討イメージ

＜対策例＞

①IoT 機器や中継装置のファームウェアやソフトウェアのバージョンを最新状態に保つ。

IoT 機器や中継装置は、日々脆弱性が発見され、その脆弱性への対策を行ったパッチがベンダから公開されている。悪意を持った人物による不正アクセスや脆弱性を突いた攻撃から機器類を保護するために、IoT 機器や中継装置のファームウェアやソフトウェアのバージョンは適宜アップデートし、最新化する必要がある。また、IoT 機器や中継装置の提供ベンダから配信される脆弱性情報を継続的に収集し、必要に応じて最新化する。

②インターネットを経由する外部との通信は暗号化する。

IoT 機器で収集されたデータは、インターネットを経由して「都市 OS」へ集められるが、その経路上において、悪意のある人物に盗聴されたり、通信データを改ざんされたりする可能性があるため、「都市 OS」との通信を暗号化する必要がある。

③機器を物理的に保護する。

IoT 機器は、サービスによっては、持ち歩いて利用したり、家庭や公共空間などに設置されたりするケースが存在する。そういった状況においては、悪意のある第三者によって機器

が盗難されたり、利用者紛失した機器が第三者によって不正操作されるなど、物理的な攻撃を受ける危険性がある。

また、廃棄した機器から情報が漏えいしたり、不正なソフトウェアを組み込んだ機器が中古販売されたりする可能性がある。そのため、外部からの機器への不正なアクセスは物理的に保護する必要がある。

- 家庭や公共機関などに設置された機器は、関係者以外による物理的なアクセスを制限する。
- 機器が物理的に破壊される等の故障などの異常が発生した場合に検知できるように、機器の状態を監視する。

＜補足＞

なお、上記のポイントで挙げた①～③は主に運用段階における具体例を挙げているが、企画、設計・開発段階においては、①～③に関する機能を保有するアセットを調達・導入することに留意する。

4. スマートシティ特有のセキュリティ留意点

4.1. セキュリティ留意点とセキュリティ対策

4.1.1. マルチステークホルダー間の連携

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、動的に構成される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、一企業が取り組むセキュリティ対策だけで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は限界がある。そのため、企画・設計、開発、運用などのスマートシティのライフサイクルの各段階において、推進主体が中心となって、マルチステークホルダー間で十分に連携し、企画、設計・開発段階における製品やサービスのセキュリティ対策の実施や運用段階における能動的なセキュリティ対策の実施、インシデントの発生を想定した対応体制の整備など、幅広い領域で対策を検討・実施することが望ましい。

マルチステークホルダー間の連携をする上で、特に留意すべき点を以下に挙げる。

① セキュリティに関する共通のポリシーを策定する
② マルチステークホルダー間の責任分界点を明確化し、スマートシティ全体としての対応体制を整備する
③ ①、②について、マルチステークホルダー間で連携し、共通認識のものとする

以下で、上記それぞれの留意点について、簡単に解説する。

① セキュリティに関する共通のポリシーを策定する

セキュリティに関するポリシーの例として、セキュリティ管理基準やデータ取扱いに関するポリシー、リスク判断の基準などが挙げられるが、例えばデータの取扱い基準が異なることにより、一方の組織で公開すべきでないとしていた情報が、別の組織において公開されてしまうと言ったケースが考えられる。また、リスク判断の基準が異なることで、一方の組織で問題無しと判断していたところ、別の組織において大きな問題となっている可能性が考えられる。こういった状況を防ぐために、予めマルチステークホルダー間で話し合い、スマートシティ全体としての、共通のポリシーを策定することが望ましい。

② マルチステークホルダー間の責任分界点を明確化し、スマートシティ全体としての対応体制を整備する

マルチステークホルダーが関与することによって発生する問題点として、責任分界点があいまいになってしまうケースが挙げられる。例えば、スマートシティの運用において何

かしらの問題が発生したときに、その問題をどの組織が事象の把握を行い、どの組織が対応を行うか、といった取決めが事前に決められていないと、行き当たりばったりの対応となってしまい、結果としてスマートシティ機能の持続的提供や、セキュリティ強度やサービスレベルの維持、円滑なインシデント対応に支障が発生する可能性がある。こちらについてもあらかじめマルチステークホルダー間で話し合い、責任分界点及びそれぞれの役割を明確化し、平時・有時における協働体制を構築しておくことで、こういった事象に対して速やかに対応できるようになる。

③ ①、②について、マルチステークホルダー間で連携し、共通認識のものとする

マルチステークホルダーが関与することによって生じる問題を解消する上で最も重要となるのが、①、②の内容について、マルチステークホルダー間で共通認識とすることである。こういったポリシーや責任分界点、対応体制といった内容は、一つの組織で決定するものではなく、マルチステークホルダー間で話し合い、それぞれの組織が共通的に認識することで始めて意味があるものとなる。スマートシティのビジネスモデルにも依るが、一般的にはスマートシティの推進主体を中心に協議の場を持ち、スマートシティ全体の方向性として共通認識の下、定めていくことが望ましい。

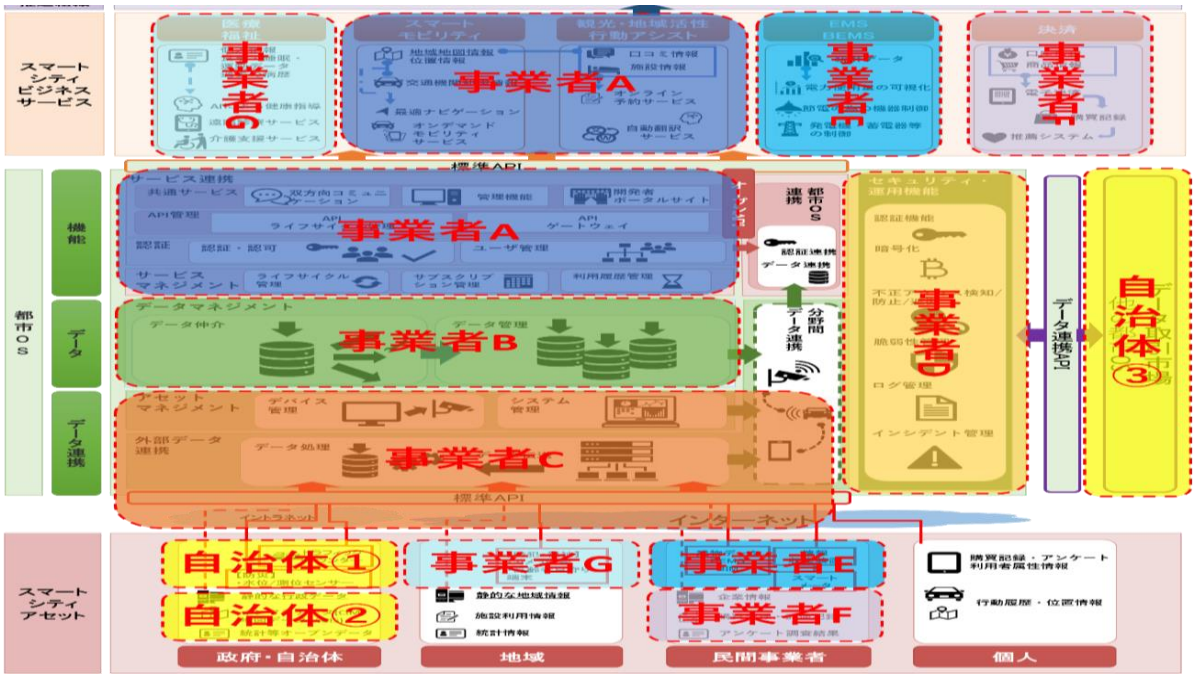


図４－１　マルチステークホルダーのイメージ

4.1.2. データやサービスの信頼性の担保

スマートシティとしてもう一つの留意すべき事項として、データやサービスの信頼性の担保が挙げられる。多様な事業者が複雑に関わるスマートシティにおいては、組織の信頼性、データの信頼性など、信頼性が低いコンポーネントの存在により、スマートシティ全

体のサービスレベルが低下されるだけで無く、最悪の場合はシステム・サービスの停止や情報漏洩等に繋がり、結果としてスマートシティサービスとしての信頼が損なわれてしまうことになる。

そのため、適切なサプライチェーン管理による組織の信頼性担保のほか、機器やプラットフォームなどのコンポーネント間のデータ流通において、電子証明書の利用などにより、完全性・真正性の担保を実現し、サービスとしての信頼性を担保する必要がある。

また、特定のコンポーネントや組織に閉じた問題への対処とならないよう、スマートシティサービスを守るための SOC／CSIRT を構築し、リアルタイムでサイバー攻撃やセキュリティインシデントの発生状況を把握し、マルチステークホルダーに情報共有を行い、これらの事象に対し推進主体を中心にマルチステークホルダー間で連携して対処して行くことが望ましい。

4.2. 想定されるリスクとセキュリティ対策例

① マルチステークホルダー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ー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ーのうち、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、管理システムへの不正ログイン等が発覚しても、サービス提供者によ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ー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 ベンダーが都市 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、原因究明が遅れる可能性がある。その結果として、スマートシティ全体を統括するサービスオーナーや推進主体への状況報告が遅れ、ユーザのスマートシティ全体に対する信頼を失うという事もあり得る。

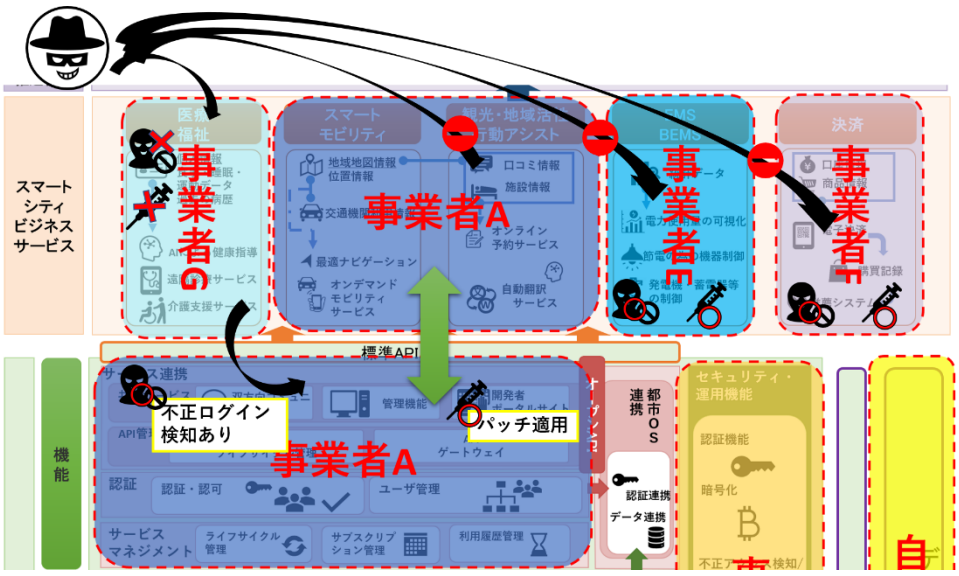


図４－２　マルチステークホルダー間でセキュリティ管理水準が異なることで生じる問題

ケース②：マルチステークホルダー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ー間の役割分担が不明確な場合、情報の改ざんが発覚したとしても、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事がある。

参考資料２

セキュリティ対策例

必須対策

① 全体を統括するサービスオーナーや推進主体等、主管者を定める。
② 主管者が、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（ベンダー等）を把握し、マルチステークホルダー間で共有する。
③ 全てのマルチステークホルダーに有事における連絡窓口を設置させ、それをマルチステークホルダー間で共有する。
④ ベンダー等のシステム・サービス提供者が、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、原因調査手順等を整備する。

推奨対策

① 主管者が、全てのマルチステークホルダーのセキュリティレベルを把握する。
・各事業者におけるリスク分析結果の把握
・各事業者におけるシステム障害やセキュリティ事故発生時の対応体制の把握
・リスク分析結果や対応体制等把握の定期的な更新
② 主管者が中心となり、スマートシティに関連する SOC／CSIRT 等の組織を作り、マルチステークホルダー間での円滑な連携体制を構築する。
③ SOC／CSIRT において、継続的に脅威情報等を収集し、それを活用した能動的なセキュリティ対策を図る。

② マルチステークホルダー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、守秘義務契約も併せて締結するが、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事がある。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のベンダーとの契約において、どちらの責任で対応するかを定めていないと、結局、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、被害が拡大する事もあり得る。

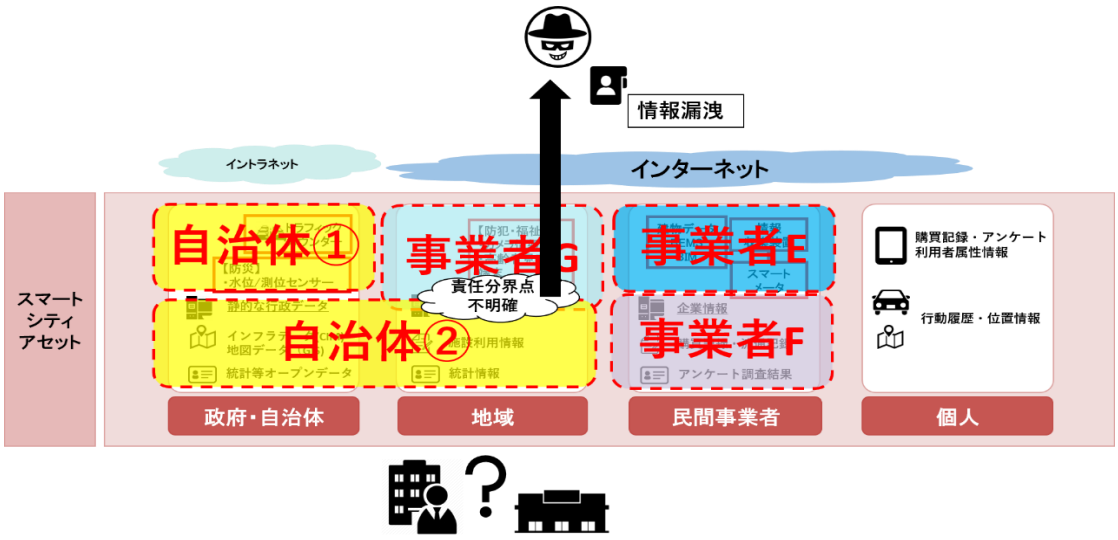


図４－３　不明確な責任分界点によって生じる問題

セキュリティ対策例

必須対策

① それぞれのマルチステークホルダー間におけるスマートシティに関する契約時に、取り扱う情報、機能、運用方法、責任範囲等について明確にし、合意する。

② ①で合意した内容を定期的に確認し、見直しを行う。

推奨対策

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する。

② 推進主体において構成図、体制図等を確認し、管理上空白となる箇所がないことを確認する。

③ マルチステークホルダー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①：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

マルチステークホルダー間の契約で、都市 OS に蓄積されているデータの利用目的、権限、利用範囲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、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、主管者である推進主体と契約したサービス提供者が、すでに都市 OS に蓄積されている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、そのサービスが本来の利用目的を超える範囲でのサービスだった場合、サービス提供者が不正にクローズドデータを活用して利益を上げることとなり、最終的に訴訟問題に発展する可能性がある。

ケース②：データの制限・取扱いが不明確なことから生じる問題

すでに都市 OS に蓄積されているデータを利用して、例えば位置情報サービスの提供を開始する際、取り扱うデータに非識別加工情報として扱われるデータ（オープンデータ）だけでなく、位置情報や本人認証情報などのデータ（クローズデータ）が含まれている場合、個人が特定できる情報が漏洩してしまう恐れがある。

セキュリティ対策例

必須対策

①スマートシティの情報主管者（推進主体やサービスオーナー等）が、スマートシティ全体で創出、流通される全てのデータを把握し、一覧化する。
②スマートシティ内で取り扱われるデータの利用目的、権限、利用範囲、データの所有者を明確化し、全てのマルチステークホルダーの間で合意する。
③②で合意した内容を定期的に確認し、見直しをする。
④データを公開する場合には、利用範囲やデータの所有者を明確に表示する。

推奨対策

①特定のサービスを提供するためのシステムのサービスイン前に、それぞれのマルチステークホルダーが必要なデータのみへアクセスできる設計になっているかを確認する。
②都市 OS が収集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となる個人情報等のクローズドデータを除去し、無害化を行う。
③都市 OS が収集するデータについて、個人が特定できないよう情報をグループ化する等し、統計データとして取り扱う。
④システムへのアクセスの監視・分析を行う。
⑤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（トレーサビリティが担保されている）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。

④ 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

主管者（サービスオーナーや推進主体）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、再々委託先に対して、主管者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、脆弱なセキュリティ対策が取られてしまうことがある。その結果、再々委託先で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

必須対策

①全体を統括するサービスオーナーや推進主体等、主管者を決める。

②主管者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、データの流れと連携しているシステムを把握するとともに、再委託や再々委託等を含めたサプライチェーンについても把握し、スマートシティシステム全体の管理を行う。

推奨対策

① 主管者が、サプライチェーンを含めた連携事業者のセキュリティレベルを把握する。
- ・各事業者におけるリスク分析結果の把握
- ・各事業者におけるシステム障害時やセキュリティ事故発生時の対応体制の把握
- ・リスク分析結果や対応体制等把握の定期的な更新

② 主管者が中心となり、スマートシティに関連する SOC／CSIRT 等の組織を作り、マルチステークホルダー間での円滑な連携体制を構築する。

③ 主管者主体で、セキュリティインシデント対応訓練を実施し、対策遅延ポイントやセキュリティ対策が不十分なポイントを把握し、改善に向けた活動を行う。

＜例＞
- ・再委託、再々委託等を含めたサプライチェーン管理体制の見直し
- ・それぞれのマルチステークホルダーのリスク及びセキュリティ対策状況の明確化
- ・セキュリティインシデント発生時のマルチステークホルダー間の連絡窓口、体制の整備
- ・事案発生時の情報連携手法やサービス復旧に向けた対応手順の整備
- ・定期的なセキュリティインシデント対応訓練の実施

参考資料２

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などの協働体制について

スマートシティにおいて確保すべきセキュリティ上の要素の例は以下となる。

・スマートシティのシステム内の重要な情報の漏洩防止
・システムへの不正侵入の防止
・IoT 機器自体の完全性・信頼性の担保
・IoT 機器から送られるアセット（データ）の真正性の担保
・コンポーネント間の通信の完全性及び真正性の担保

これらを確保し、重大なセキュリティ事故の発生を防ぐため、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、即時で対応できる様になることが推奨される。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、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。

図４－４　ＳＯＣ／ＣＳＩＲＴの設置

＜想定される SOC／CSIRT の役割＞

SOC

・　脅威の検知/通知
・　インシデントの検知/通知

CSIRT

・　事前対応（情報収集、構成管理、リスク評価）
・　事後対応（相関分析、インシデント対処）
・　情報連携

5. セキュリティ対策要件の例示

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。

５章では、セキュリティ対策の観点・リスクに対して、スマートシティの推進主体やシステム構築・運用等に関わる各主体が実装すべきセキュリティ対策一覧を示し、選択の一助とすることを目的としている。

なお、セキュリティ対策一覧で整理した対策例は、あくまで対策の一例を示すものであり、国内外の様々なガイドライン等や他の実装を何ら否定するものではなく、各主体におけるシステムの重要度やリスク、セキュリティ対策を導入・運用する際の相対的コスト等の観点を考慮してセキュリティ対策一覧を参考に適切なセキュリティ対策を検討することが推奨される。

5.1. セキュリティ対策一覧

スマートシティを提供する推進主体やシステム構築・運用等に関わる各主体が実装すべきセキュリティ対策について、以下の順で検討することを推奨する。

①３章、４章において、スマートシティにおけるセキュリティの考え方や代表的なセキュリティ対策について理解する。

②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。

③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、サービスにおいて発生することが想定されるリスク（想定されるインシデントや脅威、脆弱性）を導出する。

④添付 A「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。

⑤【対策要件 ID】を基に、対策の具体的な内容を添付 B「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。

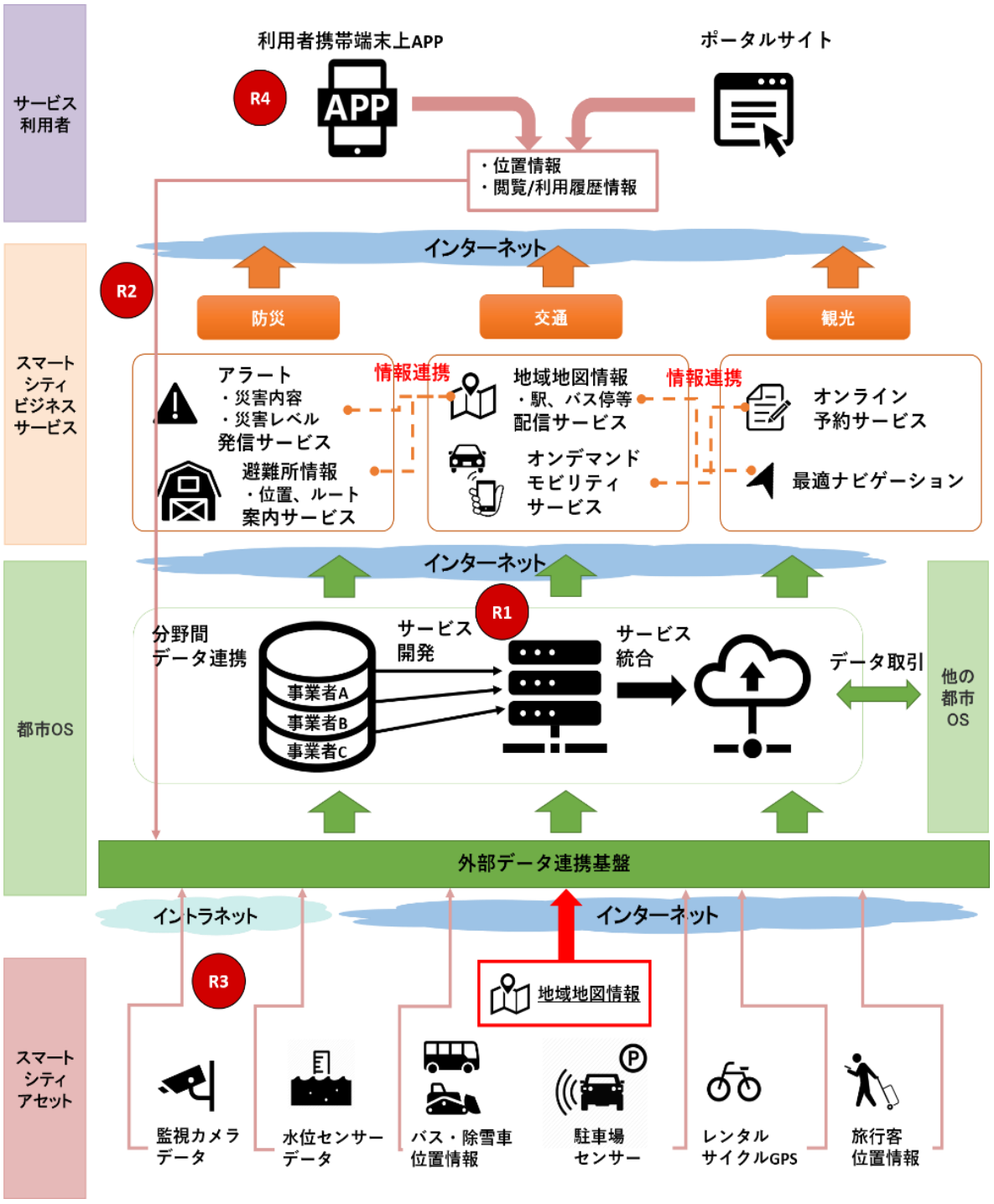


図５－１　スマートシティのユースケース

参考資料２

表５－１　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洩する	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

5.2. 国内外のガイドライン・規格等への対応

本ガイドラインでは、スマートシティ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。

一方、スマートシティアセットにおける IoT 機器等、各個のセキュリティ対策の検討を行うにあたっては、IoT 機器のライフサイクル（方針、分析、設計、構築・接続、運用・保守）に焦点を当て IoT 機器のリスクとその対応について体系的に示すガイドライン「IoT セキュリティガイドライン」がある。

本ガイドラインでは、IoT 機器リスクへの対応策として「IoT セキュリティガイドライン」における観点を参考にするとともに、「IoT セキュリティガイドライン」等の記述との整合性を維持するように配慮している。また、スマートシティにおいてアプリケーションやシステム等を提供する上で必要とされるセキュリティ対策例を、添付 B「セキュリティ対策一覧」で挙げているが、この一覧は「クラウドサービス提供における情報セキュリティ対策ガイドライン」や「NIST SP800-171」、「NIST SP800-53」、「サイバー・フィジカル・セキュリティ対策フレームワーク」等のガイドラインを参照しているため、本対策要件を実装することで、間接的に国際規格等に準拠することに通ずる。本ガイドラインにおいて記載したスマートシティにおいて重視するべきセキュリティ観点と、本対策例を組み合わせ、より高度なセキュリティの実装に資することを期待する。

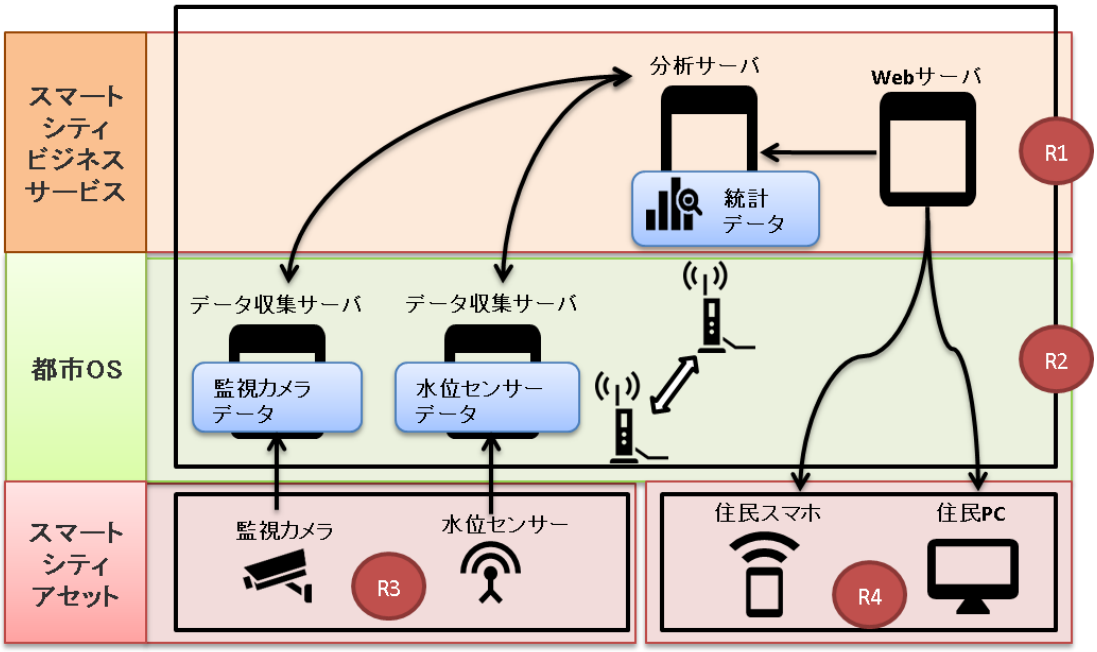
表５－２　参照ガイドライン

	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 27001:2013（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）（案）
スマートシティガバナンス・マネジメント	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	◎	○	◎	○	◎	○
スマートシティサービス・ビジネス	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	○	○			○	○
スマートシティ都市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	○	○	○	◎	○	◎
スマートシティアセット	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	○	○			◎	◎

（参考）ユースケース（「防災」、「交通」、「観光」、「医療」、「決済」）における考慮

防災イメージ

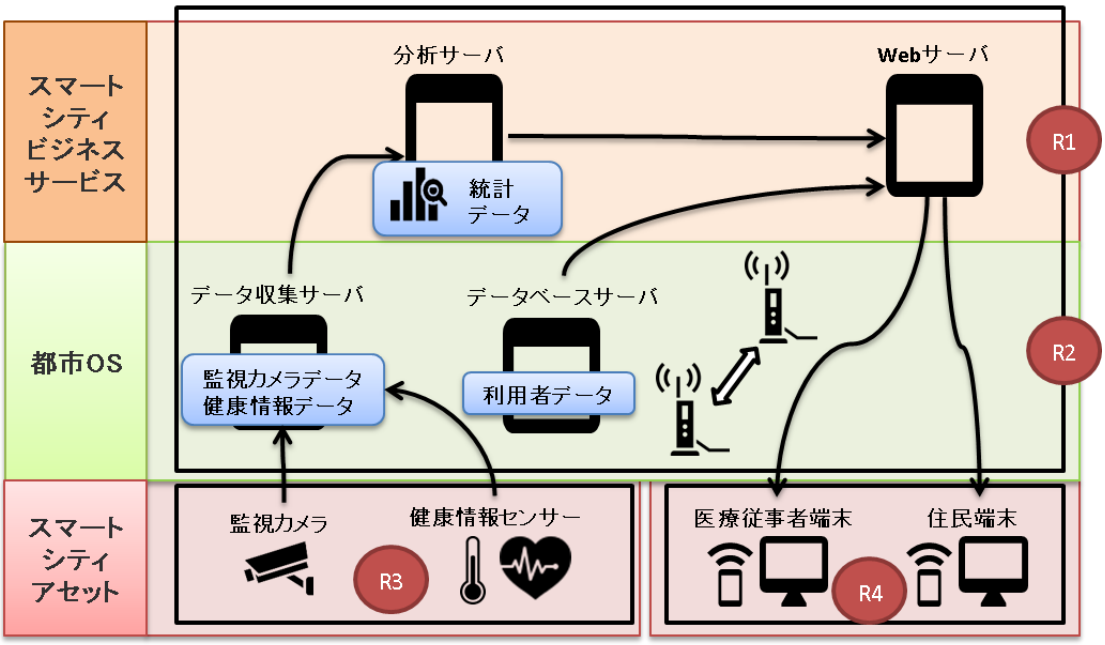
【ユースケース例】
・水位センサーや防犯カメラで、洪水・土砂崩れ・河川氾濫の先行情報を取得し、
適切な場所での防災措置や住民に避難誘導を展開するなど、対策をとる。



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データの受信	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り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洩する	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等が発生する	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

医療・福祉イメージ

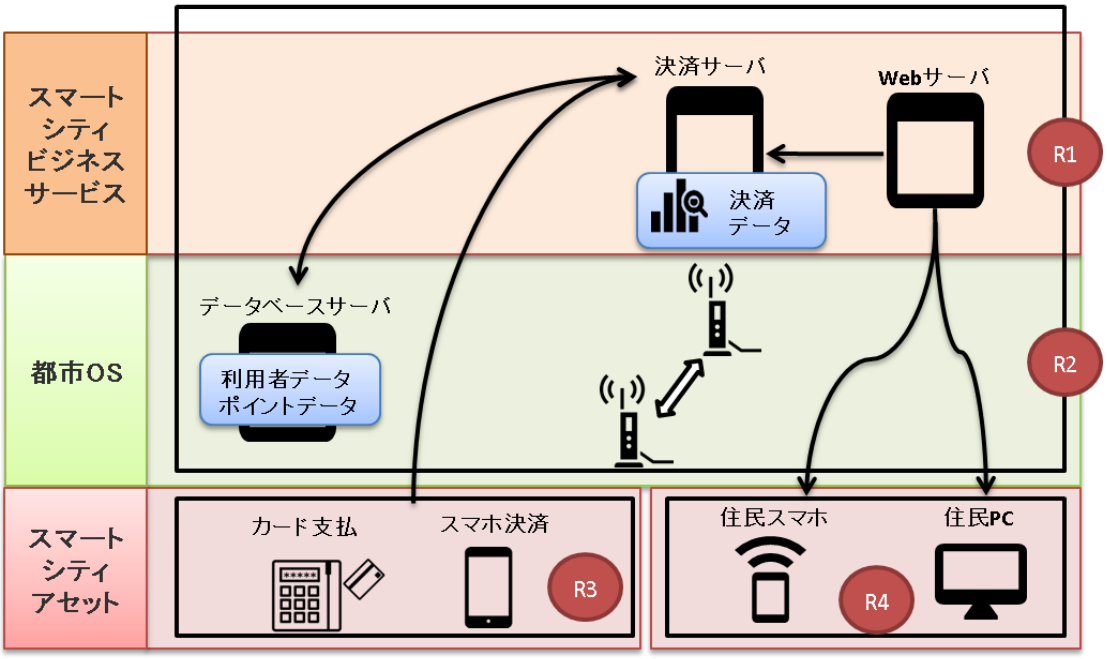
【ユースケース例】
・高齢者や患者の健康情報を収集、蓄積することで、医者や家族が患者の健康情報を常に把握可能とする。



リスク箇所	リスク概要	対策番号
R1	なりすましによる不正データの受信	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り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洩する	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等が発生する	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

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
R1	なりすましによる不正データの受信	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り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洩する	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等が発生する	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

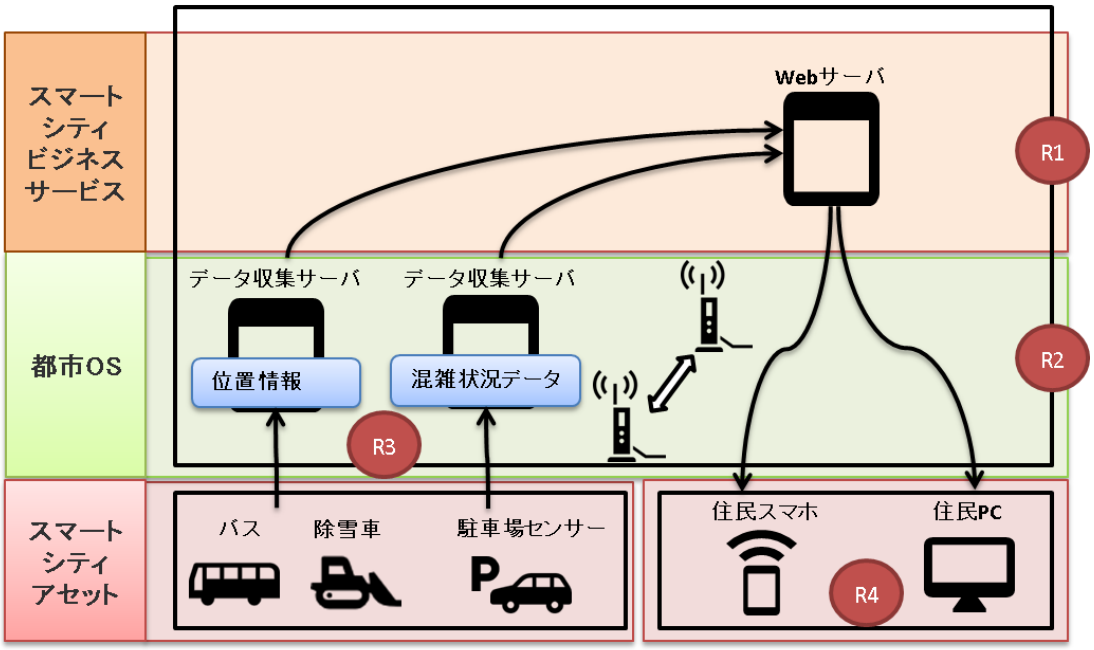
参考資料２

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。

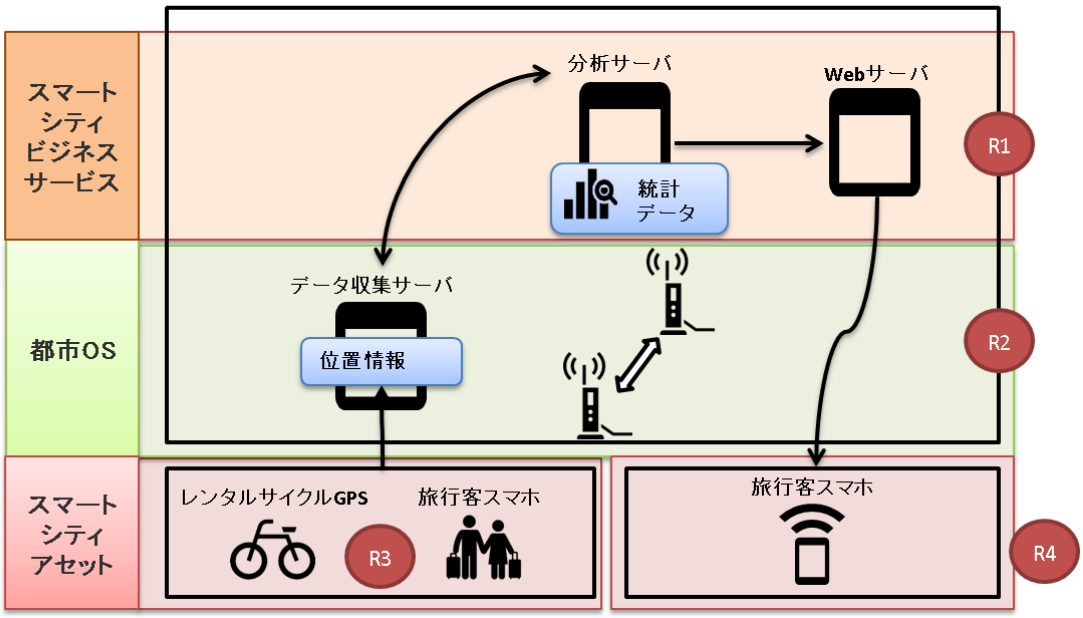
また、駐車場の利用状況を配信することで、住民や観光客の利用を促す。



リスク箇所	リスク概要	対策番号
R1	なりすましによる不正データの受信	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り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洩する	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等が発生する	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

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
R1	なりすましによる不正データの受信	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り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洩する	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等が発生する	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

添付A　「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	・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-7 CPS.SC-8
(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
(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	・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
(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	・通信路が適切に保護されていない	CPS.DS-3
(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	・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
(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	・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
(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	・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
(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	・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
(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
(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	・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
(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	・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
(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	・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

(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	・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
(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	・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
(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	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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	・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

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
サービス拒否攻撃等により、IoT 機器や通信機器等の機能が停止する	・IoT システムを構成する IoT 機器、通信機器等に対するサービス拒否攻撃	・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
サービス拒否攻撃等により、IoT 機器や通信機器等の機能が停止する	・IoT システムを構成する IoT 機器、通信機器等に対するサービス拒否攻撃	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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	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
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-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8

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
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	・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
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	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
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	・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
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	・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
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	・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
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)領域から自織の保護すべきデータが漏洩する	・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
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洩する	・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

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洩する	・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	・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
関係する他組織で管理している(データ保管)領域から自組織の保護すべきデータが漏洩する	・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	・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
関係する他組織で管理している(データ保管)領域から自組織の保護すべきデータが漏洩する	・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	・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
関係する他組織で管理している(データ保管)領域から自組織の保護すべきデータが漏洩する	・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	・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
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	・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
関係する他組織で保管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	・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
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	・自組織と他組織(サプライヤー等)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
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	・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
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

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ーに対して、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
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	・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
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ーに対して、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
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	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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

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
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	・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 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
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	・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
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	・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
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	・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
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.IP-7 CPS.IP-8 CPS.IP-10 CPS.RA-2
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
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	・・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
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	・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
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	・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
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	・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
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
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遵守していない	CPS.AT-1
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	・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	・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
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	・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	・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
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	・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
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	・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
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	・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
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	・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
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	・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
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	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
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洩する	・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
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洩する	・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	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

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洩する	・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	・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
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洩する	・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	・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
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洩する	・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	・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.CM-2
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洩する	・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	・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
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洩する	・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	・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
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洩する	・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	・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
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洩する	・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	・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

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洩する	・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	・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
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洩する	・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	・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
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洩する	・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	・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洩する	・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.IP-2 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.RA-2
自組織で管理している領域から保護すべきデータが漏洩する	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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

自組織で管理している領域から保護すべきデータが漏洩する	・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.BE-2
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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.SC-1
自組織で管理している領域から保護すべきデータが漏洩する	・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	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
自組織で管理している領域から保護すべきデータが漏洩する	・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	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

自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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.SC-2
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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.IP-3
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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

自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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.IP-7 CPS.SC-10 CPS.SC-11
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
自組織で管理している領域から保護すべきデータが漏洩する	・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	・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
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

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	・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
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	・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
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	・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	・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
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	・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
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	・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	・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

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	・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
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	・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
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	・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
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.GV-1 CPS.GV-4 CPS.RM-1 CPS.SC-3 CPS.SC-4 CPS.SC-6
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	・自組織と他組織(サプライヤー等)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	・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
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	・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
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	・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
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
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

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
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
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	・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
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	・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
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.RA-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	・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-3
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
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.DP-1 CPS.DP-2 CPS.DP-3 CPS.DP-4 CPS.RA-2

参考資料２

添付 B　「セキュリティ対策一覧」

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

	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（サプライヤー、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
	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
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
	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
	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