資料６－５

スマートシティセキュリティガイドラインの改定について

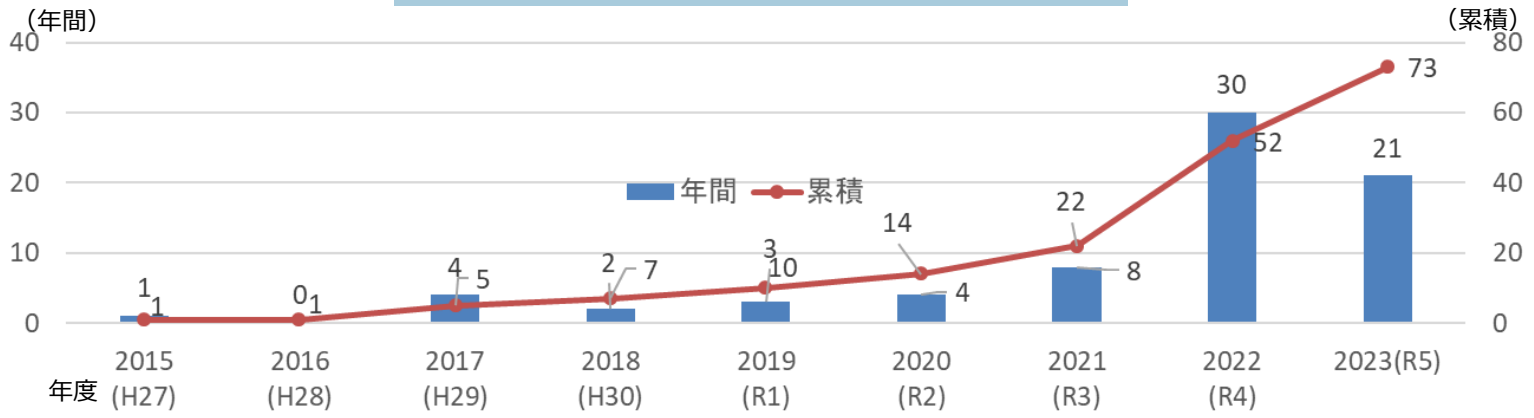
令和6年4月26日

事務局

（参考）スマートシティの普及

- 地域が抱える様々な課題（防災、セキュリティ・見守り、買物支援など）をデジタル技術やデータの活用によって解決し、地域DXや地域活性化につながるものとして、政府においてもスマートシティの実装を推進。
- 各種スマートシティサービスの基盤となる都市OS（データ連携基盤）の導入地域数について、2025年度までに100地域という政府目標がある中で、2023年度現在の導入地域数は73となっており、普及が進んでいる状況にある。

都市OSの導入地域（市町村）数の推移



年度	地方公共団体
2015年度	会津若松市
2017年度	札幌市、さいたま市、加古川市、高松市
2018年度	富山市、益田市
2019年度	伊那市、新居浜市、飯塚市
2020年度	嬬恋村、柏市、大田区、加賀市

※ 境町、秩父市は、2022年度のデジ田事業でカウントし、2023年度ではカウントしないため、2023年度は総務省施策6件＋デジ田事業15件の合計21件の見込み

年度	地方公共団体
2021年度	更別村、仙台市、つくば市、佐野市、豊能町、長崎県（全21市町）、人吉市、岐阜県（デジ田）
2022年度	江別市（デジ田）、笠間市、境町（デジ田）、前橋市（デジ田）、秩父市（デジ田）、横須賀市、鎌倉市、小田原市、朝日町（デジ田）、能美市（デジ田）、福井県（全17市町）、山梨県（デジ田）、長野県（全77市町村）、茅野市（デジ田）、浜松市（デジ田）、焼津市（デジ田）、多気町（デジ田）、京都府（デジ田）、大阪府（堺市、豊中市）、養父市（デジ田）、吉備中央町（デジ田）、西粟倉村（デジ田）、広島県（デジ田）、三次市、山口市、三豊市（デジ田）、愛媛県、松山市、福岡市、延岡市（デジ田）
2023年度	横浜市、岡崎市、有田市、熊本県（県内6市が共同利用）、南城市、（二次公募予定：境町、秩父市、すさみ町）に加えてデジ田で15団体が導入

スマートシティセキュリティガイドラインについて

■ 総務省では、スマートシティのセキュリティ確保のための指針として、多様な関係主体が講じるべきセキュリティ対策や留意事項等を記載した「スマートシティセキュリティガイドライン」を策定（令和２年10月に第1.0版を公表、令和３年６月に改定した第2.0版を公表）。

■ 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」に基づき、スマートシティの構成要素をセキュリティの観点から４つのカテゴリに分類し、各カテゴリごとに想定されるセキュリティ上のリスクやセキュリティ対策を記載。また、「マルチステークホルダが複雑に関与」「多様なデータの連携」といったスマートシティの特徴を踏まえ、スマートシティ特有のリスクや具体的な対策を記載。

ガイドラインの構成と主なポイント

1章　背景と目的
- 本ガイドラインの**背景、目的、関係主体の定義、対象範囲（スコープ）、全体構成**等を提示

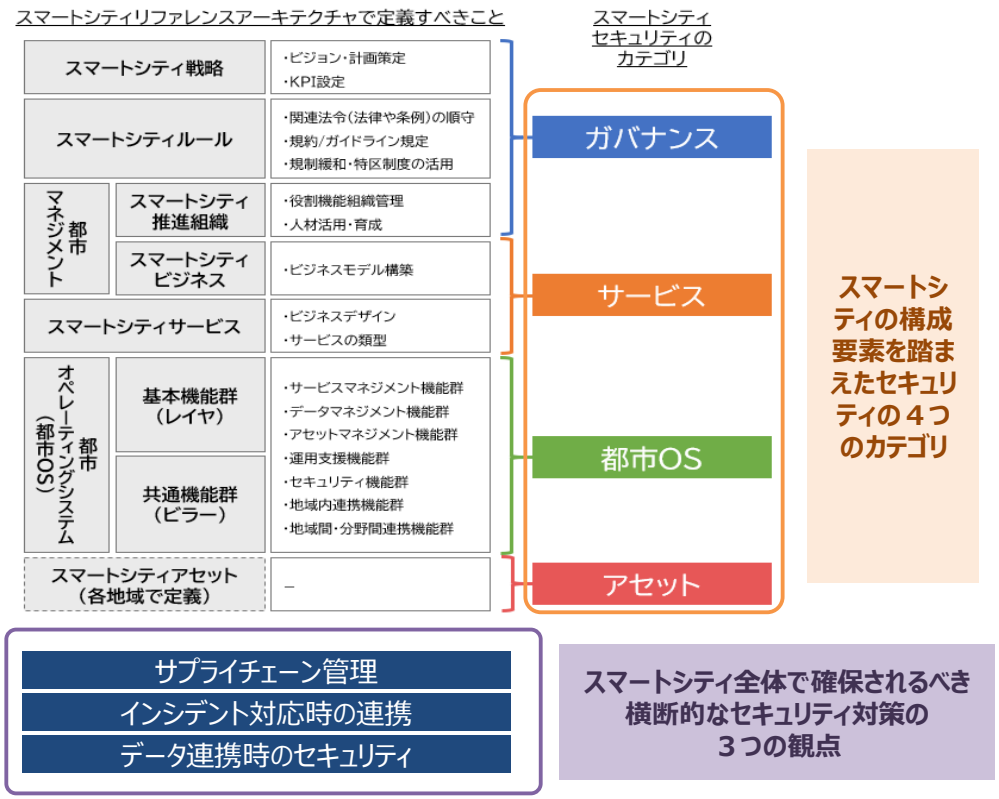
2章　スマートシティセキュリティの考え方
- スマートシティセキュリティの考え方や対策の概要等について、リファレンスアーキテクチャの構成要素を踏まえた**スマートシティセキュリティの４つのカテゴリ**や、スマートシティ全体で確保されるべき**横断的なセキュリティ対策の３つの観点**から整理

3章　セキュリティ対策
- 第2章で整理した4+3カテゴリごとに、必要な**セキュリティ対策の詳細を説明**
- スマートシティ構築・運営においてセキュリティ上、発生しうる問題点と対策を例示

4章　補助コンテンツ
- ガイドラインに記載されている**セキュリティ対策の実施状況を確認するためのチェックシート**を記載

付録
- 参照情報として、法令等の一覧や、ユースケースイメージ、サービス観点の脅威事例等を記載

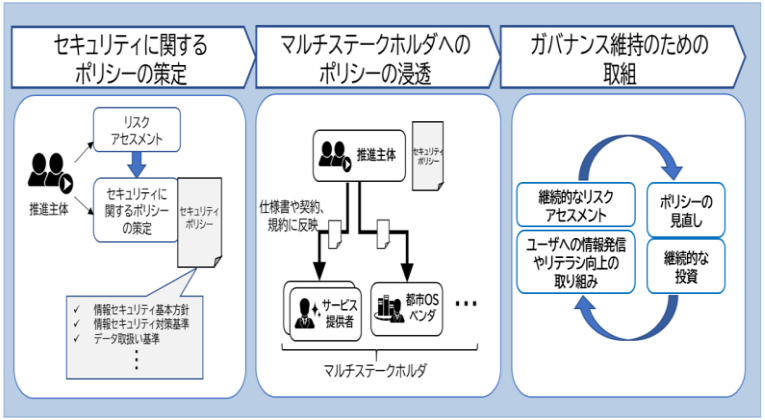
対策カテゴリの考え方



ガイドラインの概要①（スマートシティセキュリティのカテゴリ毎の対策）

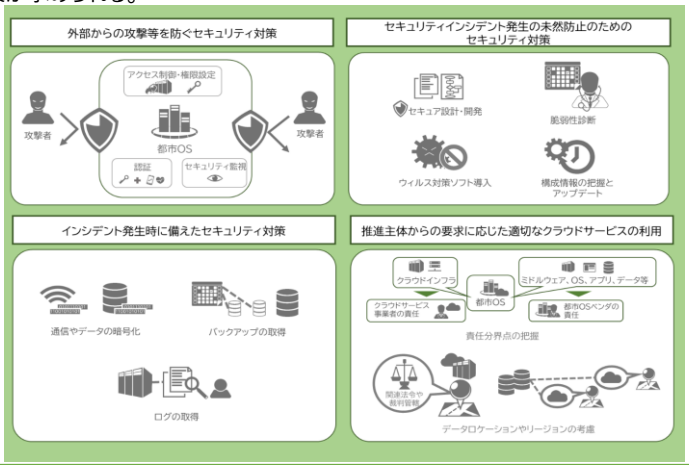
ガバナンス

スマートシティ全体の取組や施策の方向性の決定、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ことから、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、その浸透、ガバナンスの維持などが必要となる。



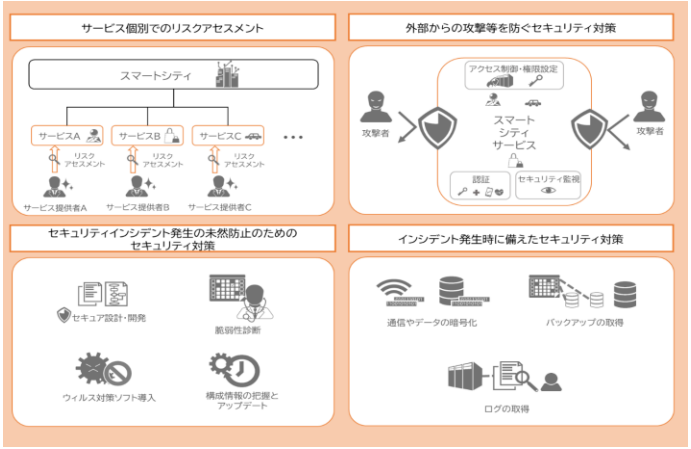
都市OS

スマートシティのシステム全体のコアと位置づけられ、「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ものであるため、サービスと同様のセキュリティ対策の実施や、都市OSがクラウド基盤を活用することからクラウドサービス特有の対策が求められる。



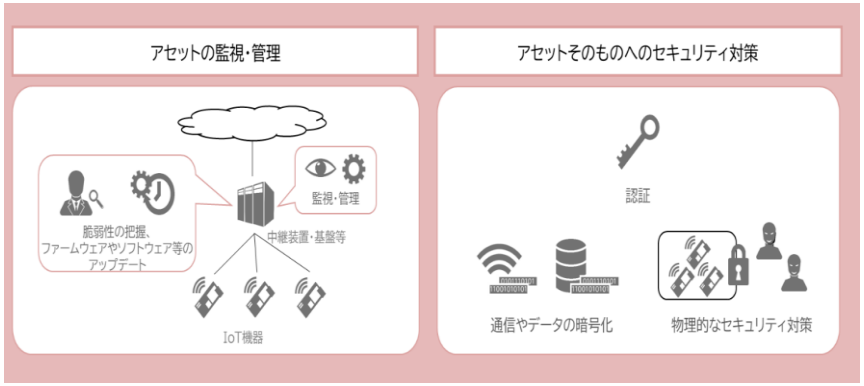
サービス

利用者がスマートシティで産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で複数のサービスが提供されることが多いことから、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した上で、その結果を踏まえた対策を講じる必要がある。



アセット

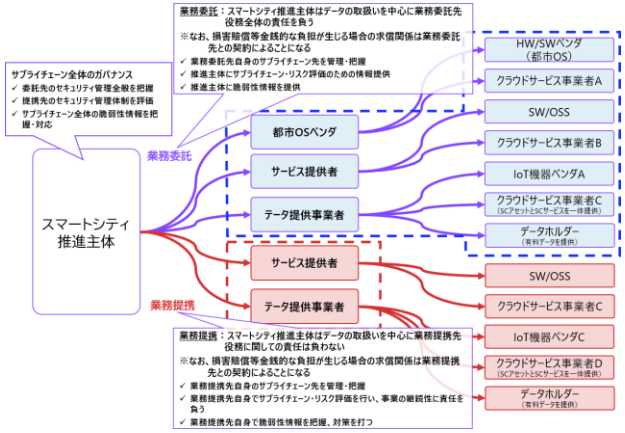
サイバー領域がフィジカル領域と接点を持つ領域であり、地域課題解決のために必要なデータを生成し、「都市OS」へ送信するカテゴリであることから、データを収集・流通するためのデバイスの効率的な監視・管理や、デバイスへのセキュリティ対策が求められる。



ガイドラインの概要②（横断的なセキュリティ対策）

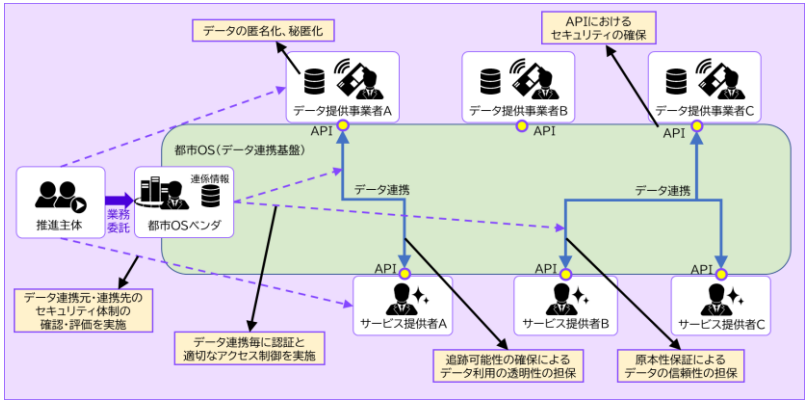
サプライチェーン管理

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。



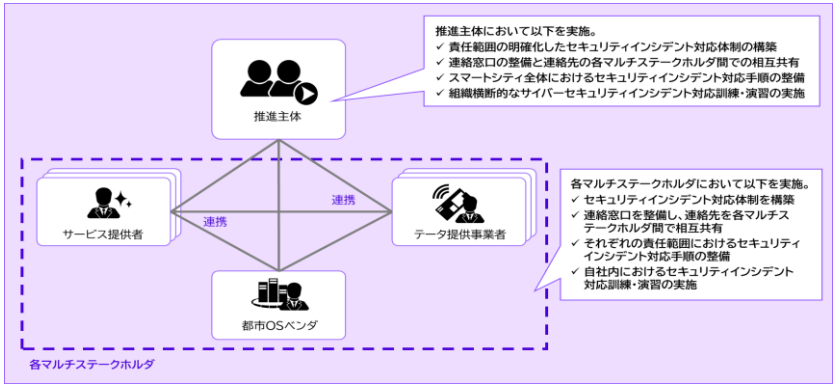
データ連携時のセキュリティ

データ連携において、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、都市OSの有無にかかわらず、データ連携元・連携先の信頼性確保やデータに対する適切なアクセス制御など、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。



インシデント対応時の連携

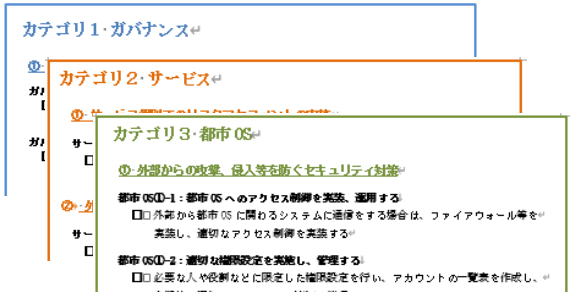
セキュリティインシデントが発生した場合、様々なマルチステークホルダが関与するスマートシティにおいては、その影響はスマートシティ全体に及ぶ。そこでマルチステークホルダ間連携が不十分だったり、お互いのシステムの責任分界点が共通認識となっていなかったりした場合、インシデントへの対応が遅れて被害が拡大するおそれがある。そのため、インシデント対応体制の構築や連絡窓口、インシデント対応手順の整備等の事前準備と実効性の確認が重要となる。



ガイドラインの概要③（セキュリティ対策の推進）

- 内閣府のスマートシティのアーキテクチャの検討状況を踏まえるなど、政府全体のスマートシティの取組と連動する形でスマートシティセキュリティガイドラインについて検討を実施。
- 本ガイドラインを有効に活用できるよう、「スマートシティセキュリティ導入チェックシート」や「スマートシティセキュリティガイドブック」といった補助コンテンツも同時に公表。
- 政府のスマートシティ関連事業において、「スマートシティセキュリティ導入チェックシート」を応募書類の一部として位置付けるなど、関係省庁等と連携しながら、スマートシティにおけるセキュリティ対策の積極的な実施を促進。

わかりやすい補助コンテンツの提供



スマートシティセキュリティ導入チェックシート

- セキュリティ対策の検討にあたって、考慮漏れがないよう、ガイドラインに記載されている対策をまとめたチェックシート

スマートシティセキュリティガイドブック

- ガイドラインの内容を要約しつつ図を多用して説明し、誰でも短時間でガイドラインの全容を把握できるようにしたガイドブック
- 実際のスマートシティでの好事例も紹介

関係省庁等との連携

内閣府「スーパーシティ型国家戦略特区」

- 「スーパーシティ等における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」において、セキュリティガイドラインを参照

内閣府「スマートシティリファレンスアーキテクチャ」

- セキュリティ機能部分について、セキュリティガイドラインを参照

内閣府・総務省等「スマートシティ関連事業」

- 合同で公募を行う政府事業*の応募様式の中に「スマートシティセキュリティ導入チェックシート」を位置づけ

***令和６年度対象事業**

1．未来技術社会実装事業（内閣府 地方創生推進事務局）
2．地域課題解決のためのスマートシティ推進事業（総務省）
3．地域新 MaaS 創出推進事業（経済産業省）
4．共創・MaaS 実証プロジェクト（日本版 MaaS 推進・支援事業）（国土交通省）
5．スマートシティ実装化支援事業（国土交通省）

ガイドラインの見直しの実施

- スマートシティセキュリティガイドラインについては、スマートシティを取り巻く環境の変化等を踏まえて、適時見直しを行ってきたところ。
- 今般、ガイドラインにおいて前提としているスマートシティリファレンスアーキテクチャの第２版の公表（令和５年８月）や、事例調査の結果等も踏まえ、ガイドライン等の見直しを実施。
- 現在、改定案の意見募集を実施しており（令和６年４月26日～５月27日）、令和６年夏までを目処に、「スマートシティセキュリティガイドライン（第3.0版）」を公表予定。

第3.0版での主な改定のポイント

- スマートシティリファレンスアーキテクチャの改定内容に従い、アーキテクチャ図やカテゴリの分類図を更新。
- スマートシティのセキュリティ検討のアプローチとして、スマートシティにおいて扱われるデータ種別の記載を新設し、オープンデータ／限定公開データ／クローズドデータの3つの分類とそれぞれの概要を説明した上で、パーソナルデータなどプライバシー保護が求められるデータもあることから、情報の性質に応じた適切なセキュリティ対策が必要となる旨を提示。
- サプライチェーン管理の観点で、スマートシティ推進主体とステークホルダー間の契約形態による責任分界の考え方を新たに整理した上で、利用者等との間ではスマートシティの推進主体が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ー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。
- データ連携時のセキュリティにおいて、スマートシティリファレンスアーキテクチャの第2版の内容も踏まえて、都市・地域間連携時の想定される実施パターンを提示するのと合わせて、都市OSにおける２つのデータ流通方式（蓄積型・分散型）の特徴を整理し、それぞれについてセキュリティの観点から望ましいパターンについても記載。
- その他、改定に伴い、読み手における読みやすさの観点で形式等を修正。