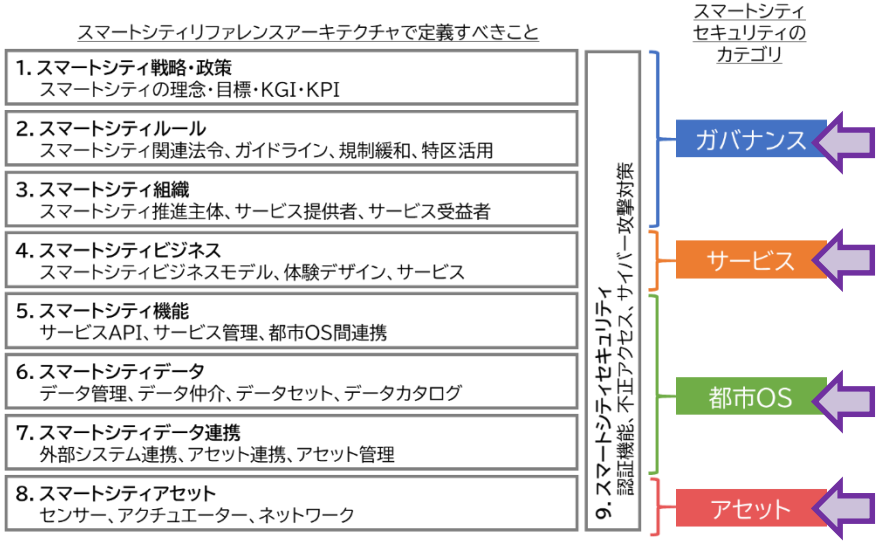
スマートシティセキュリティガイドライン（第2.0版）の概要について

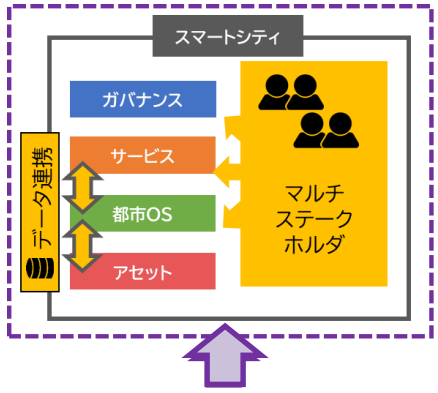
別添1

■「スマートシティセキュリティガイドライン」は、スマートシティの推進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示したもの。令和２年10月に第1.0版を公表した後、内容のブラッシュアップを進め、令和３年４月に改定案(第2.0版の案)を作成。

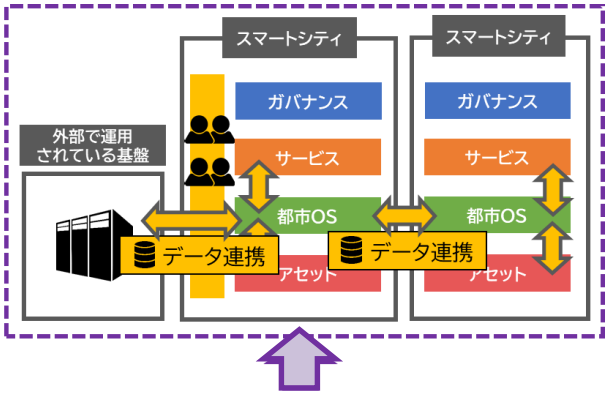
■ガイドラインでは、スマートシティの構成要素(※)をセキュリティの観点から４つのカテゴリ（＝ガバナンス、サービス、都市OS、アセット）に分類し、各カテゴリごとに想定されるセキュリティ上のリスクやセキュリティ対策を記載。（※:「スマートシティリファレンスアーキテクチャ」で定義されている各階層）

■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セキュリティ対策を３つに分類して（＝適切なサプライチェーン管理、インシデント対応時の連携、データ連携時のセキュリティ確保）、リスクや具体的な対策を記載。





単体のスマートシティに着目したセキュリティ検討



他のスマートシティや基盤との連携に着目したセキュリティ検討

上述の４つのカテゴリそれぞれにおけるリスクやセキュリティ対策を記載

ガバナンス
- ✓ セキュリティに関するポリシー策定
- ✓ マルチステークホルダへのポリシー浸透
- ✓ ガバナンス維持のための取組

サービス
- ✓ それぞれのサービスにおけるリスクアセスメント
- ✓ 外部からの攻撃等を防ぐセキュリティ対策
- ✓ インシデント発生防止のためのセキュリティ対策
- ✓ インシデント発生時に備えたセキュリティ対策

都市OS
- ✓ 外部からの攻撃等を防ぐセキュリティ対策
- ✓ インシデント発生防止のためのセキュリティ対策
- ✓ インシデント発生時に備えたセキュリティ対策
- ✓ 適切なクラウドサービスの利用

アセット
- ✓ アセットの監視・管理
- ✓ アセットそのものへのセキュリティ対策

スマートシティの特徴を踏まえ、スマートシティ特有のセキュリティ対策として以下の３つに分類し、それぞれにおけるリスクやセキュリティ対策を記載

適切なサプライチェーン管理
- ✓ サプライチェーン全体のリスク・脆弱性情報の管理・把握
- ✓ 委託先のセキュリティ管理体制評価

インシデント対応時の連携
- ✓ インシデント対応体制の構築
- ✓ インシデント対応手順の整備
- ✓ インシデント対応訓練・演習の実施

データ連携時のセキュリティ
- ✓ データ連携元・連携先のセキュリティ管理体制評価
- ✓ 認証とアクセス制御の実施
- ✓ データ利用時の透明性、信頼性の担保、匿名化・秘匿化
- ✓ APIのセキュリティ確保

■ その他、補助コンテンツとしてスマートシティセキュリティ導入チェックシートやリスク一覧、セキュリティ対策一覧などを掲載