資料３

# スマートシティセキュリティガイドライン（第1.0版）の概要

令和２年11月

総務省　サイバーセキュリティ統括官室

# スマートシティにおけるセキュリティの検討の枠組み



■ スマートシティのセキュリティ確保の在り方について、多様な関係者間で一定の共通認識の醸成が必要。
■ **総務省において有識者の意見を取り入れつつ、スマートシティ推進におけるセキュリティの考え方や、セキュリティ対策を整理した「スマートシティセキュリティガイドライン（第1.0版）」を作成し、公表。（令和２年10月）**

## 政府全体の取組

### アーキテクチャ検討会議【官】

（事務局：内閣府、座長：越塚登　東京大学教授）

スマートシティの構成要素やその関係性を示した**「スマートシティリファレンスアーキテクチャ」を整理**し、**ホワイトペーパーを公表。(令和２年３月)**

検討の内容を共有 ⇩ ⇧ 事務局オブザーバ出席

### スマートシティ官民連携プラットフォーム【官民】

（令和元年８月８日設置）

（事務局：内閣府、国土交通省、**総務省**、経済産業省）

**目的**：官民が一体となって全国各地のスマートシティの取組を推進

**会員**：スマートシティ関連事業実施団体　等
（コンソーシアム・協議会(78)、地方公共団体(113)、企業・大学・研究機関等(356)、関係府省(11)、経済団体(2)）
（数字は令和元年12月末時点）

**＜活動内容＞**

- スマートシティ関連事業の効果的な推進・重点支援
- **分科会（※）の開催**（令和元年11月時点で８個）
- 企業、大学・研究機関、地方公共団体等の間のマッチング等支援
- 国内外への普及促進活動

## 総務省の取組（セキュリティ関連）

### スマートシティのセキュリティの検討

- 左記で整理した**「スマートシティリファレンスアーキテクチャ」を踏まえ**、**スマートシティのセキュリティの在り方**について検討する調査研究を実施、当調査研究の成果を反映した**ガイドラインを作成**。

検討の内容を共有 ⇩ ⇧ フィードバック

### スマートシティセキュリティ・セーフティ分科会

（令和２年１月活動開始）

（事務局：**総務省**、(株)ラック、(一社)オープンガバメント・コンソーシアム）

**目的**：スマートシティにおいて実現される様々な機能・サービス・機器などについて、セキュリティやセーフティを確保しつつ、実装していくための方策について検討する。

**メンバー**：13者（令和２年２月時点）

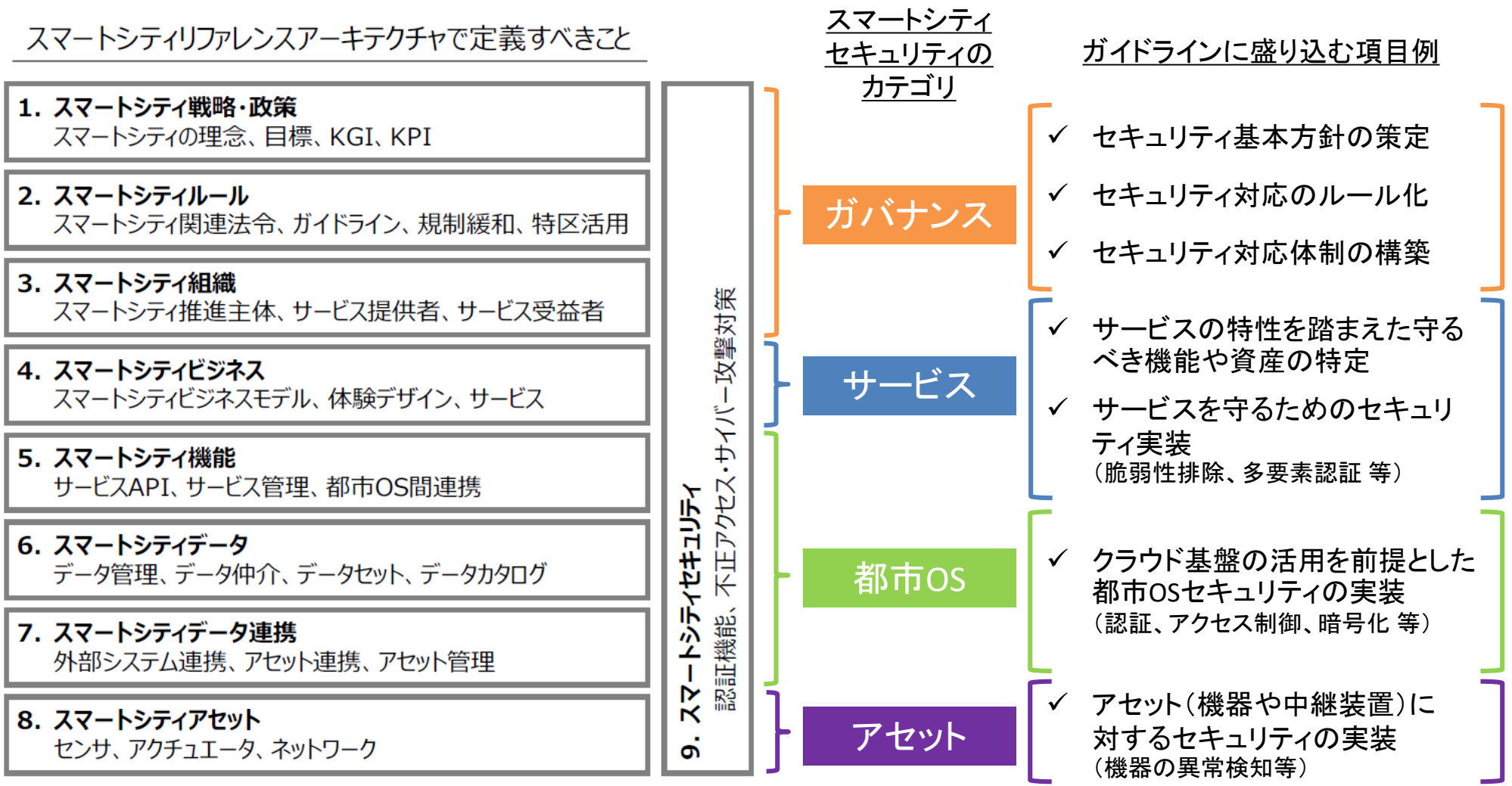
**総務省**、(株)ラック、(一社)オープンガバメント・コンソーシアムのほか、地方公共団体、印刷会社、機器メーカ、損害保険会社、不動産デベロッパー、セキュリティベンダー　など

今後、本分科会と連携し、ガイドラインのさらなるブラッシュアップ作業を進めていく予定

# スマートシティセキュリティガイドライン（第1.0版）の概要について



「スマートシティリファレンスアーキテクチャ」で定義された階層をセキュリティの観点から４つのカテゴリに整理し、それぞれのカテゴリにおけるセキュリティの考え方やセキュリティ対策をガイドラインに記述。



# スマートシティ特有の留意点について



スマートシティ特有の構造に関連して、特有のセキュリティ留意点を記載し、それぞれの留意点について、起こりうる問題や対策の方向性などをガイドラインにて整理。

## 留意点①　マルチステークホルダー間の連携

＜起こりうる問題（例）＞

- ✓ データ取扱いポリシーの不整合による、本来公開すべきでない情報の公開
- ✓ セキュリティ対応・連携体制が整備されていないことによる、インシデント発生時の原因究明遅延、被害拡大

＜対策の方向性＞

- ✓ スマートシティで流通するデータの把握とデータ取扱いポリシーの策定
- ✓ マルチステークホルダー間の責任分界点の明確化・対応体制の整備
- ✓ 上記2点の共通認識化

## 留意点②　データやサービスの信頼性の担保

＜起こりうる問題（例）＞

- ✓ 特定のコンポーネントにおけるスマートシティで取り扱われるデータの改ざん
- ✓ サプライチェーン（再委託先や再々委託先等）における情報漏洩
- ✓ 上記インシデントの発生によるスマートシティ全体の利用者からの信頼低下

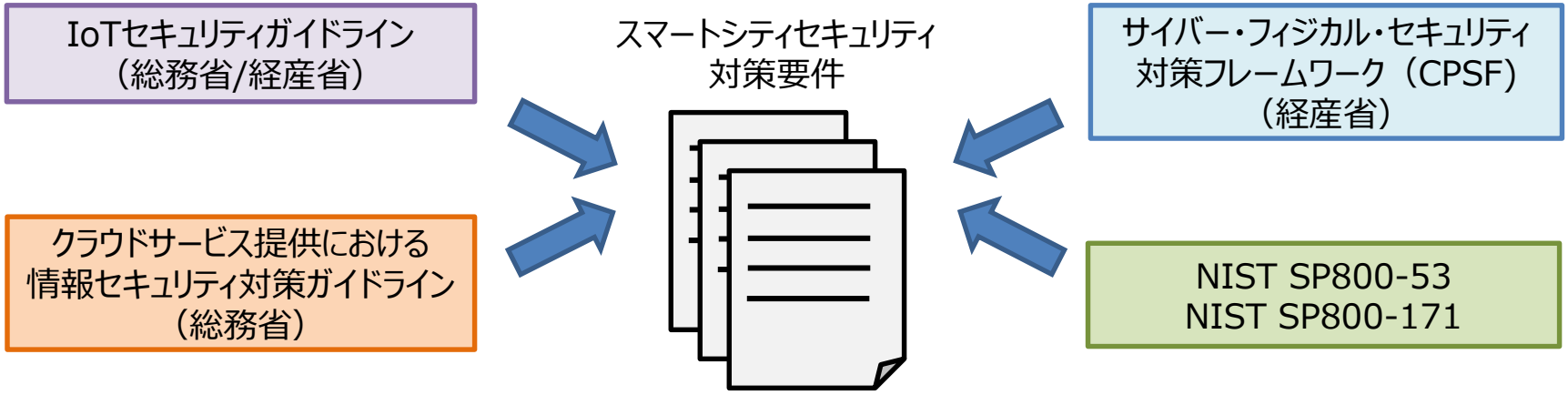
＜対策の方向性＞

- ✓ 各事業者のセキュリティ管理水準の一元的把握
- ✓ 推進主体等のスマートシティ全体を統括する主管者による、サプライチェーンの把握と管理
- ✓ SOC/CSIRTの設置によるセキュリティ監視、インシデント対応の統制やインシデント発生の予防

# セキュリティ対策要件の例示



- ガイドライン内でスマートシティにおいて想定されるセキュリティリスクと、それに対するセキュリティ対策を例示
- 本対策例は外部のガイドラインやドキュメントを参照しつつ作成
- 対策例の利用法としては、スマートシティを推進するマルチステークホルダーにおいて、自身が構築・運用するスマートシティのリスク把握や、取るべきセキュリティ対策を考える上での参考としてもらうことを想定




## 想定されるリスクの表

| 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<br>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<br>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<br>CPS.IP-10<br>CPS.MA-1<br>CPS.MA-2<br>CPS.RA-2<br>CPS.CM-6<br>CPS.CM-7 |
| (なりすまし等をした)ソシキ/ヒト/モ | ・不正な組織/ヒト/モノ/システムによる正規 | ・通信路が適切に保護されていない | CPS.DS-3 |

## リスクに対するセキュリティ対策

| カテゴリ | 対策要件 ID | 対策要件 | リファレンス<br>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<br>サービス<br>都市 OS<br>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<br>サービス<br>都市 OS<br>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<br>都市 OS<br>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<br>都市 OS<br>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<br>サービス<br>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、 | 都市 OS |

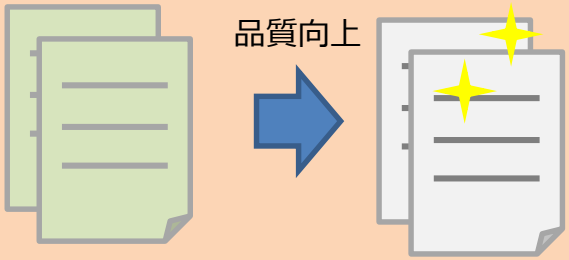
# 今後の予定

今後、ガイドラインの品質向上及び幅広いユーザ利便の向上を図り、本ガイドラインの普及を促進していく。

## １．ガイドラインの品質向上

■ ガイドライン改定（考慮点の追加・構成の変更等）

例）・都市OS間を相互接続した際のセキュリティ
・各カテゴリの接続点（API）におけるセキュリティ
・各分野において準拠すべき法令への言及




## ２．ユーザ利便の向上

■ 幅広いユーザへの当ガイドラインの普及啓発を目的とした付属資料の作成

例）・チェックリストやガイドブックの検討・作成


前述の「スマートシティセキュリティ・セーフティ分科会」における検討をはじめ、国内外から幅広く意見を取り入れつつ、上記の施策を推進していく。