スマートシティセキュリティ
ガイドブック

2024年6月
総務省

はじめに

本ガイドブックの位置づけ

日本全国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
総務省は「スマートシティセキュリティガイドライン（第3.0版）」を通じて
スマートシティのセキュリティの考え方や、
ステークホルダの横断的なセキュリティ留意事項など
について整理しています。

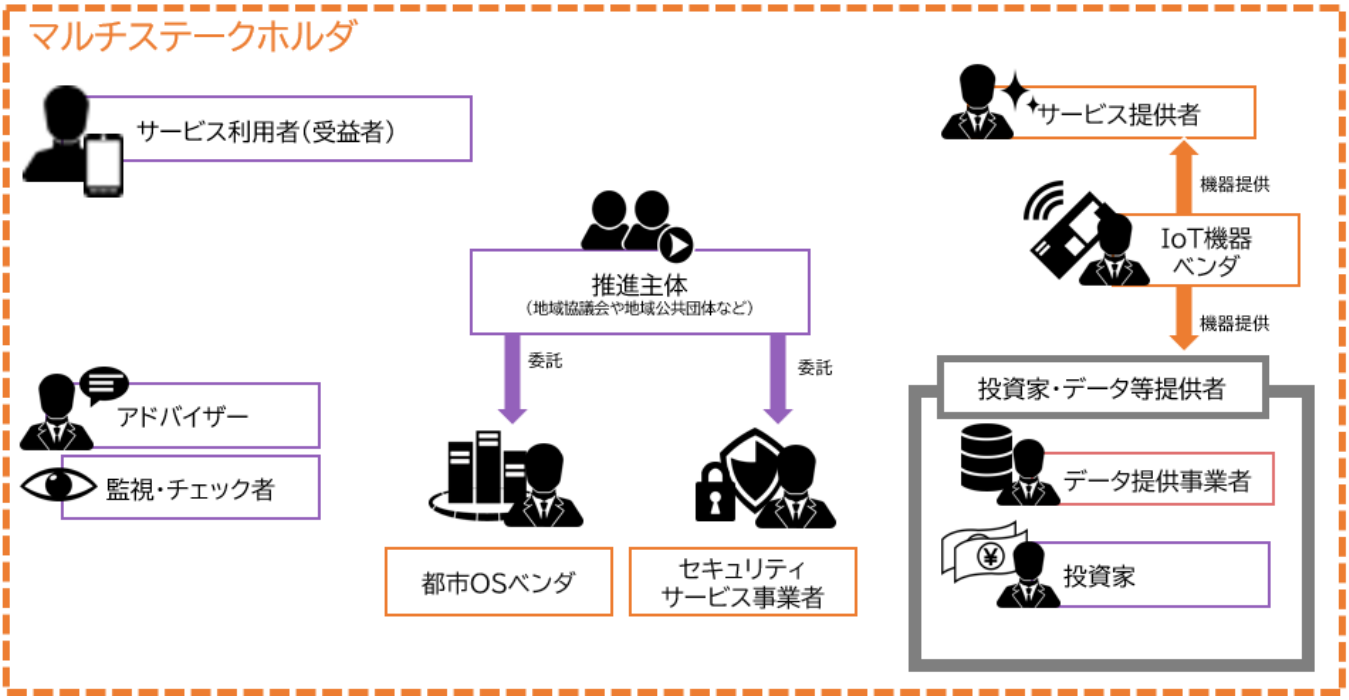
本冊子は、このガイドラインを活用しようとされる方々への
導入ガイドブックです。

対象となる読者

①
推進主体

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

本冊子では、スマートシティの関係主体間の関係性を
以下のように整理しています。
本ガイドブックを読む前に自身のスマートシティに当てはめ、
誰がどの役割を担っているかを確認しておきましょう



用語	定義
サービス利用者(受益者)	スマートシティサービス提供の対象
サービス提供者	スマートシティサービスを提供する主体
推進主体	スマートシティ全体の推進・運営に関して責任・決定権・主導権を持つ主体(地域協議会や地方公共団体など)
投資家・データ等提供者	スマートシティやスマートシティサービスの開発・運営に必要となるリソースを提供する主体
都市OSベンダ	「推進主体」からの業務委託等を請け、都市OSの構築・運用を実施する事業者
データ提供事業者	「投資家・データ等提供者」の内、IoT機器等からデータを収集し、都市OSへデータを提供する事業者の総称
IoT機器ベンダ	「データ提供事業者」や「サービス提供者」に対してIoT機器を提供する事業者
セキュリティサービス事業者	「推進主体」からの業務委託等を請け、スマートシティの全体、または一部のセキュリティ監視等のセキュリティに関するサービスを実施する事業者
マルチステークホルダ	「サービス提供者」「推進主体」「データ提供事業者」「都市OSベンダ」「セキュリティサービス事業者」「サービス利用者」などのスマートシティ推進に直接的・間接的に関与する主体の総称

もくじ

1 スマートシティセキュリティの考え方

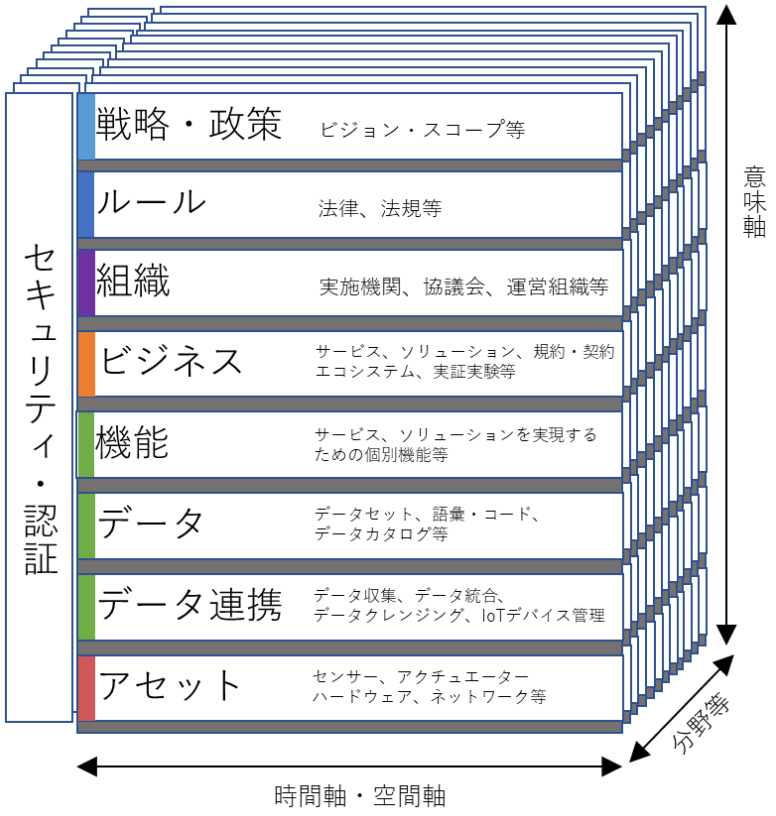
スマートシティリファレンスアーキテクチャとは？

「スマートシティリファレンスアーキテクチャ」とは、内閣府で定義されたスマートシティ推進にあたって参照すべきアーキテクチャを整理したモデルです。

スマートシティセキュリティガイドラインでは上述のアーキテクチャをベースにセキュリティの観点から「ガバナンス」「サービス」「都市OS」「アセット」の4つのカテゴリに整理しています。

各カテゴリの分類とそれを踏まえたセキュリティの考え方については、2章で詳しく解説します。

スマートシティリファレンスアーキテクチャで示されている参照すべきモデル

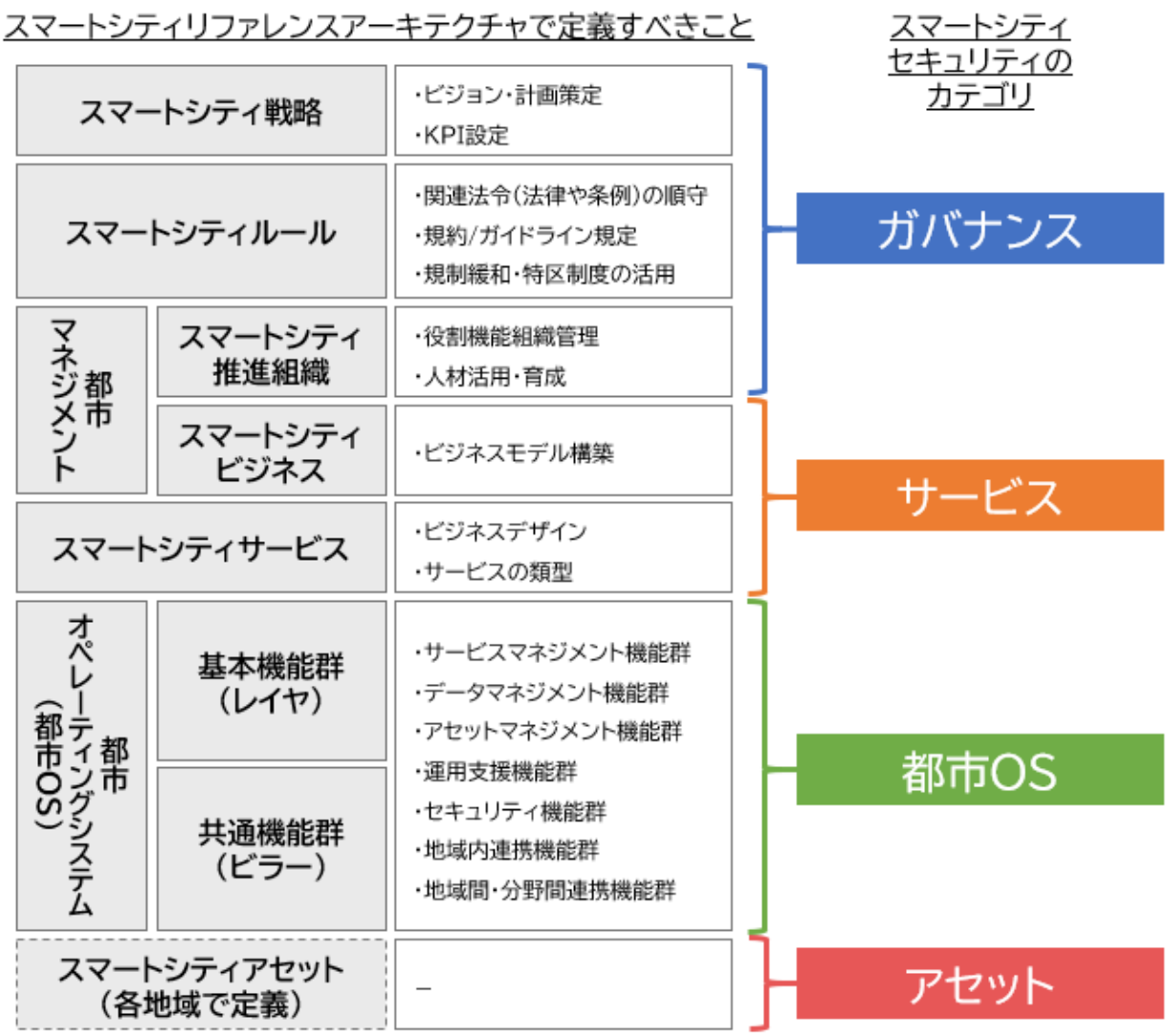


なお、スマートシティにおけるデータの種別は①「オープンデータ」②「限定公開データ」③「クローズドデータ」の3つに分類できますが、その中には、住民等のパーソナルデータも含まれます。パーソナルデータとは、個人に関係するデータであり、個人情報に加え、個人情報との境界が曖昧なものを含み、個人の属性情報、移動・行動・購買履歴データ、あるいは加工された情報や統計化された情報が含まれるため、取り扱うデータがどのデータ種別に該当するのかを踏まえ、個々のケースで適切に扱うことが求められます。

スマートシティのセキュリティ検討のアプローチ

スマートシティ全体として確保するべきセキュリティについて
2つのケースを考えましょう。

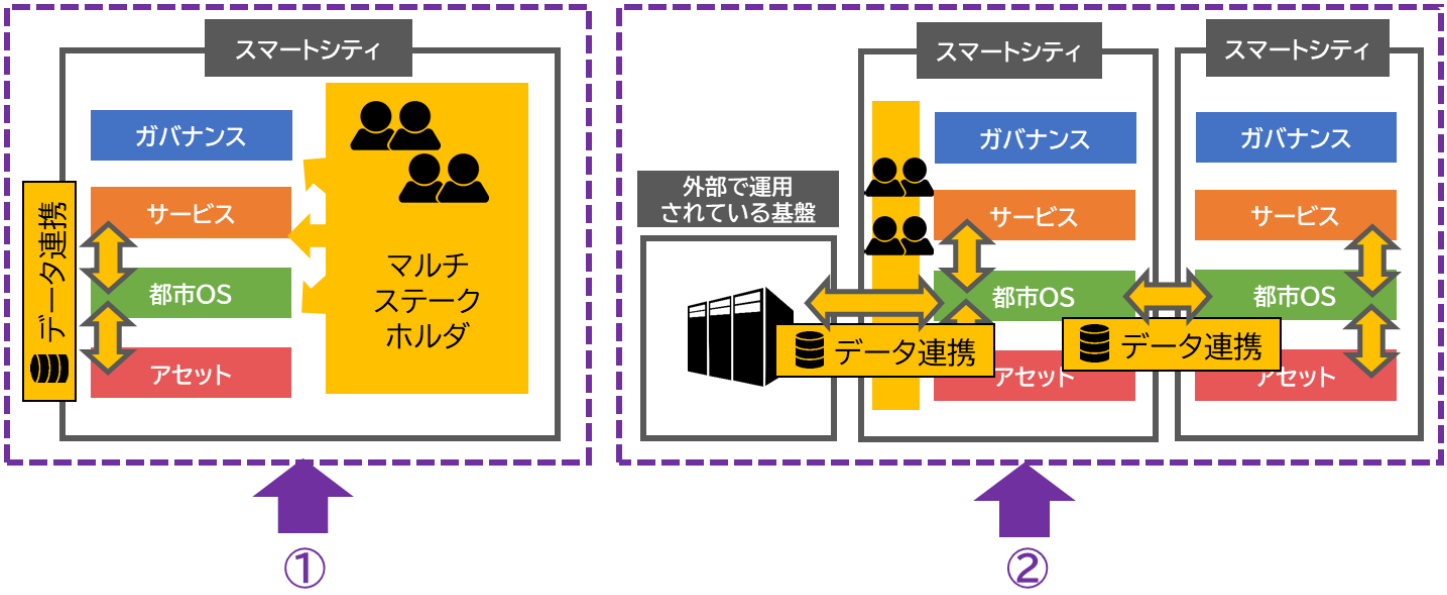
Case 1：各カテゴリにおけるセキュリティ検討



カテゴリごとの視点

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モデルをセキュリティの観点で4つのカテゴリに分類し、各カテゴリおけるセキュリティ上のリスクや対策のポイントを検討します。

Case　2：スマートシティ全体におけるセキュリティ検討



全体的な視点

スマートシティを俯瞰的にとらえ、**①単体のスマートシティ内でカテゴリ横断的に必要となるセキュリティ**及び**②単体のスマートシティ同士または自身のスマートシティと別の基盤（例えば近隣の自治体の基盤等）が接続する場合に必要となるセキュリティ**について検討します。

Check!

多様な事業者（マルチステークホルダ）が複雑に関与し合うというのはスマートシティの特徴的な部分であり、その特徴を踏まえたスマートシティの横断的なセキュリティ検討が必要となります。

本冊子では、これら2つのケースにおいて、セキュリティ上のリスクや対策のポイント、対策例について整理しました。

ガイドラインをどう使いますか？

地域課題解決や地域の経済活性化に、IoTを活用したスマートシティを構築できたらいいなあ！

「スマートシティセキュリティガイドライン」を参照すると良いのよ！使い方を確認しましょう！

色々なデータが流通するスマートシティではセキュリティも考えないといけないよ。安全・安心なスマートシティを実現するには何を注意したらいいのかな？

☑ 各カテゴリのセキュリティ対策を確認しましょう

ガバナンス

推進主体

都市OS

都市OSベンダ

サービス

サービス提供者

アセット

IoT機器ベンダ

データ提供事業者

ガバナンスを構築しよう

スマートシティ全体で一貫性のあるセキュリティを実現するためにも、軸となるセキュリティに関するポリシーを作りましょう。

セキュアなサービスを提供しよう

セキュアな都市OS（プラットフォーム）を準備しよう

スマートシティを実現する上でサービスや都市OSはなくてはならないものです。しっかりとセキュリティを考えて構築・運用をしましょう。
特に、スマートシティサービスの根幹とも言えるデータに対するセキュリティや、継続して利用できるシステム作りが重要となります。

機器やデータを保護しよう

スマートシティではデータが全てのサービスの元となります。データが安全に収集できるようにすることも大切です。

☑ マルチステークホルダで連携して対応が必要となるセキュリティ対策を確認しましょう

スマートシティの推進は様々な主体が関与しているため、推進主体を中心に**全てのステークホルダ**において考慮が必要となる**横断的なセキュリティ対策**が存在します！

- 適切にサプライチェーンを管理しよう
- インシデント対応時の連携に向けた準備しよう
- データ連携時のセキュリティを確保しよう

2 スマートシティにおけるセキュリティ対策

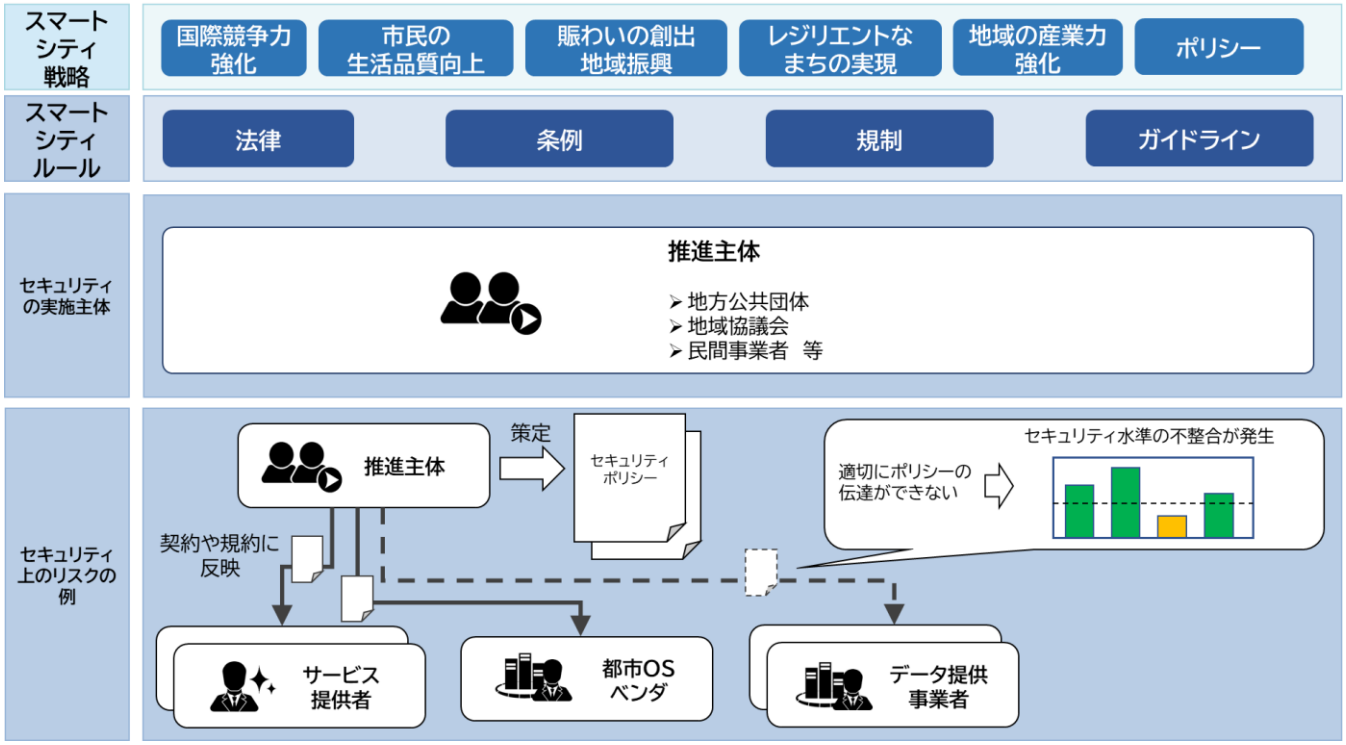
ガバナンスを構築しよう

「ガバナンス」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**等、スマートシティの在り方を決定するカテゴリです。

このカテゴリにおいて実施する対策は、**スマートシティ全体の推進と管理監督の役割がある推進主体（自治体または推進協議会等）**が主体性をもって検討・実施すべき項目です。

代表的なセキュリティ上のリスク

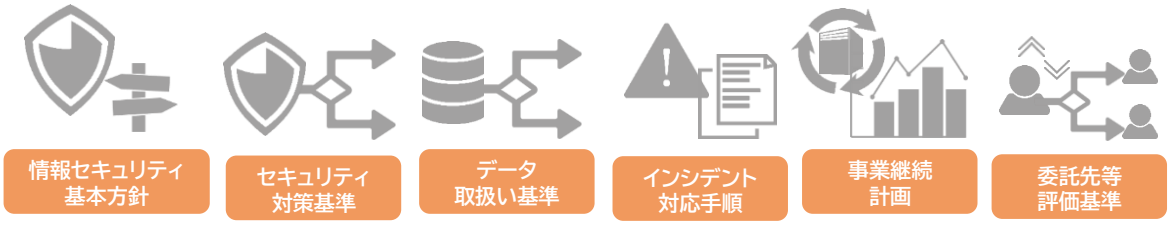
- マルチステークホルダ間におけるセキュリティ水準の不整合が発生し、セキュリティが弱いコンポーネントが発生する
- 上述のコンポーネントでセキュリティインシデントが発生することでスマートシティに対する利用者からの信頼度が低下する



ガバナンスにおけるセキュリティ対策のポイント

① セキュリティに関するポリシーの策定

セキュリティに関するポリシーは多岐にわたり存在します。これらのポリシーの在り方は、策定する主体によって様々ですが、以下の内容を含めたポリシーを策定してください。



なお、ポリシーを策定するにあたっては、以下のプロセスが重要となります。

1. リスクアセスメントの実施
2. 法令やガイドライン等との整合性の確認

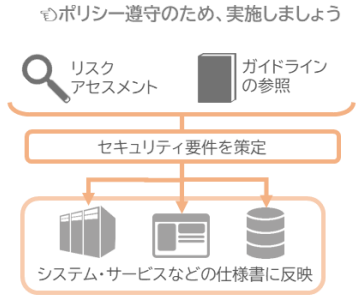
②マルチステークホルダへのポリシーの浸透

委託契約等、契約関係にあるものについては、以下について契約上明確に記載し遵守を求めるようにしましょう。

また、推進主体の役割として、新たに接続を希望する事業者のポリシーや、対応体制などを確認しましょう。

1. セキュリティ要件を調達仕様書に反映

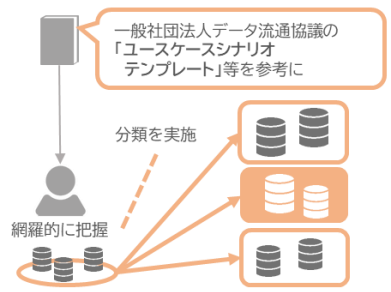
当該委託事業において



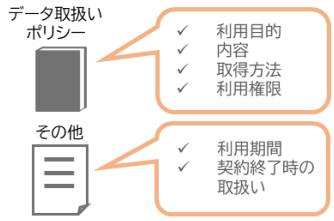
運用に関する委託を実施するとき

2. データ取扱い基準を契約・規約に反映

取り扱う可能性のあるデータを明確化

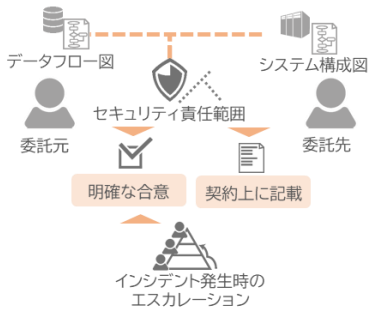


データの取り扱い方を決める

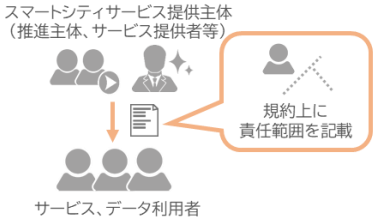


3. 契約・規約で責任範囲を明確化

マルチステークホルダ間での責任範囲の明確化



利用者との間の責任範囲の明確化



③ガバナンス維持のための取組

ガバナンスを改善・維持していきましょう。

そのために、継続的にリスクアセスメントを実施し、セキュリティのポリシーやセキュリティ対策等の見直しを行い、適切にセキュリティへの投資を続けていくことが重要です。

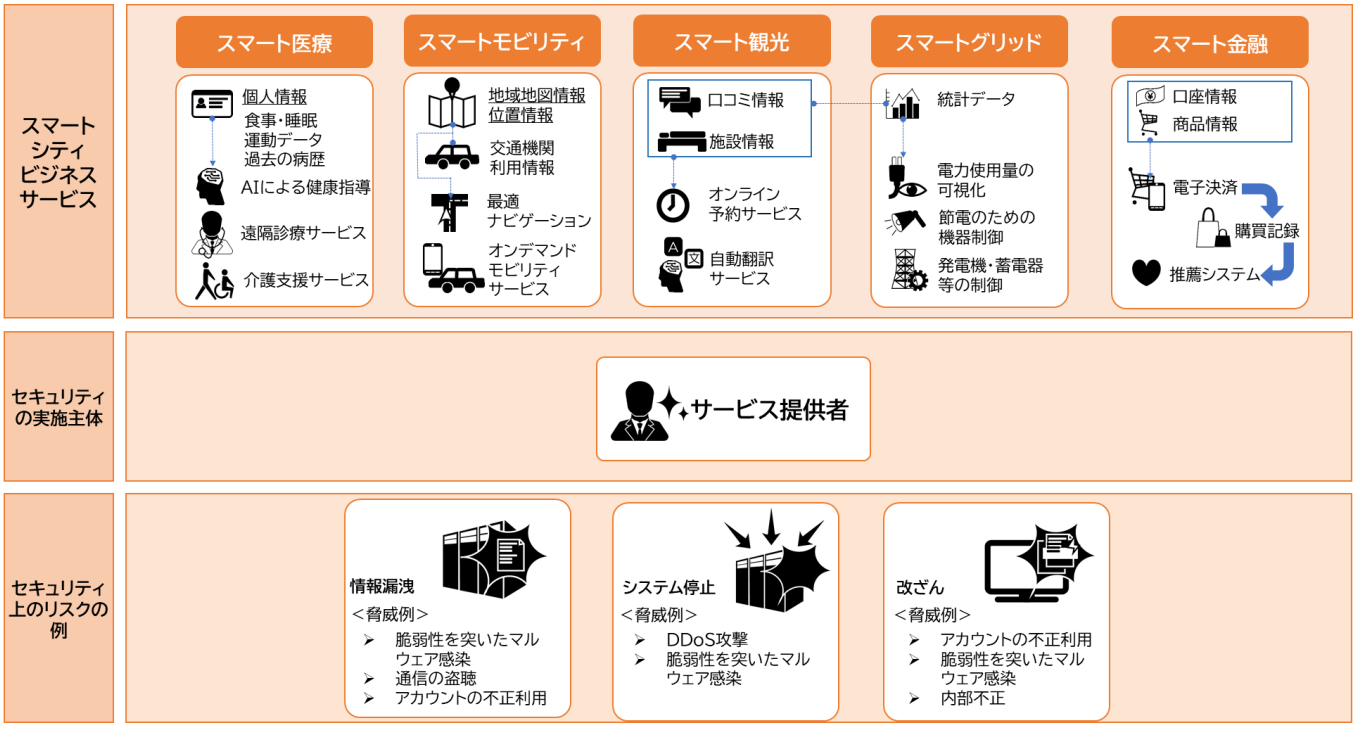
セキュアなサービスを提供しよう

「サービス」とは、スマートシティのサービス利用者が、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、**ウェブサイトやアプリ**を通じて利用者に提供されます。

サービスのセキュリティを実施する主体は**サービス提供者**となります。

代表的なセキュリティ上のリスク

- 不正アクセスによる情報漏洩
- DDoS攻撃等のサービス拒否攻撃によるシステム停止
- 改ざんされたサービスを利用した人のパソコンがマルウェアに感染する　等



サービスにおけるセキュリティ対策のポイント

①サービス個別でのリスクアセスメントの実施

1. 情報資産・システムに対するアセスメント

1. 個別のサービス単位で
守るべき情報資産や機能を特定

2. 脅威とその発生確率、影響度を
評価し、対処を決定する

以下の情報資産を保護しましょう

・コンテンツ
・ユーザ情報
・機器情報
・ソフトウェアの状態
・ソフトウェアの設定
・ソフトウェア
・設計データ内部ロジック

2. サービス仕様の脆弱性に対するアセスメント

1. 要件定義等の上流工程で
不正利用のシナリオを想定する

2. シナリオをベースに仕様上の脆弱
性が無いか精査し対策を策定する

サービス仕様の脆弱性を分析・評価し、下記のような対策を講じましょう

・サービス不正利用の規約・契約による抑止
・身元確認の実装
・サービス特性に応じた認証の強化

②外部からの攻撃等を防ぐセキュリティ対策

企画、設計・開発段階から、以下のようなセキュリティ設定を行いましょう。

1. 規約・契約での抑止

禁止事項の明確化

違反時の措置の事前同意取得

2. サービスへのアクセス制御 実装・運用

ファイアウォールの実装

3. 適切な権限設定の実施・管理

適切な権限付与ができる仕組みを実装

アクセス情報の最新化と確認

4. 身元確認機能の実装

自己申告による身元確認

顔写真付き本人確認書類の画像 アップロード

個人紐づけ確認された状態の身元確認

顔写真付き本人確認書類の画像＋容貌の画像 アップロード

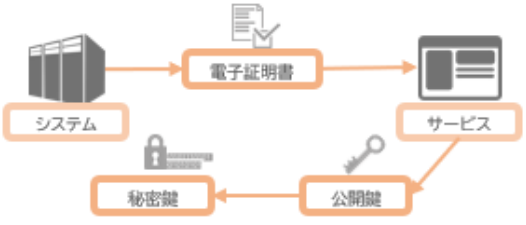
厳格な身元確認

マイナンバーカードの公的個人認証サービスを利用

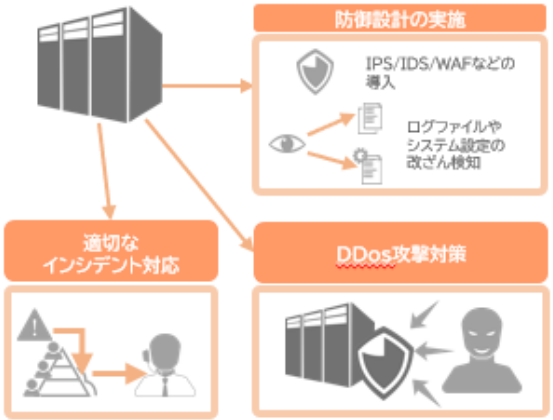
5. 認証機能の実装

多要素認証を採用

システム・サービス間の相互認証

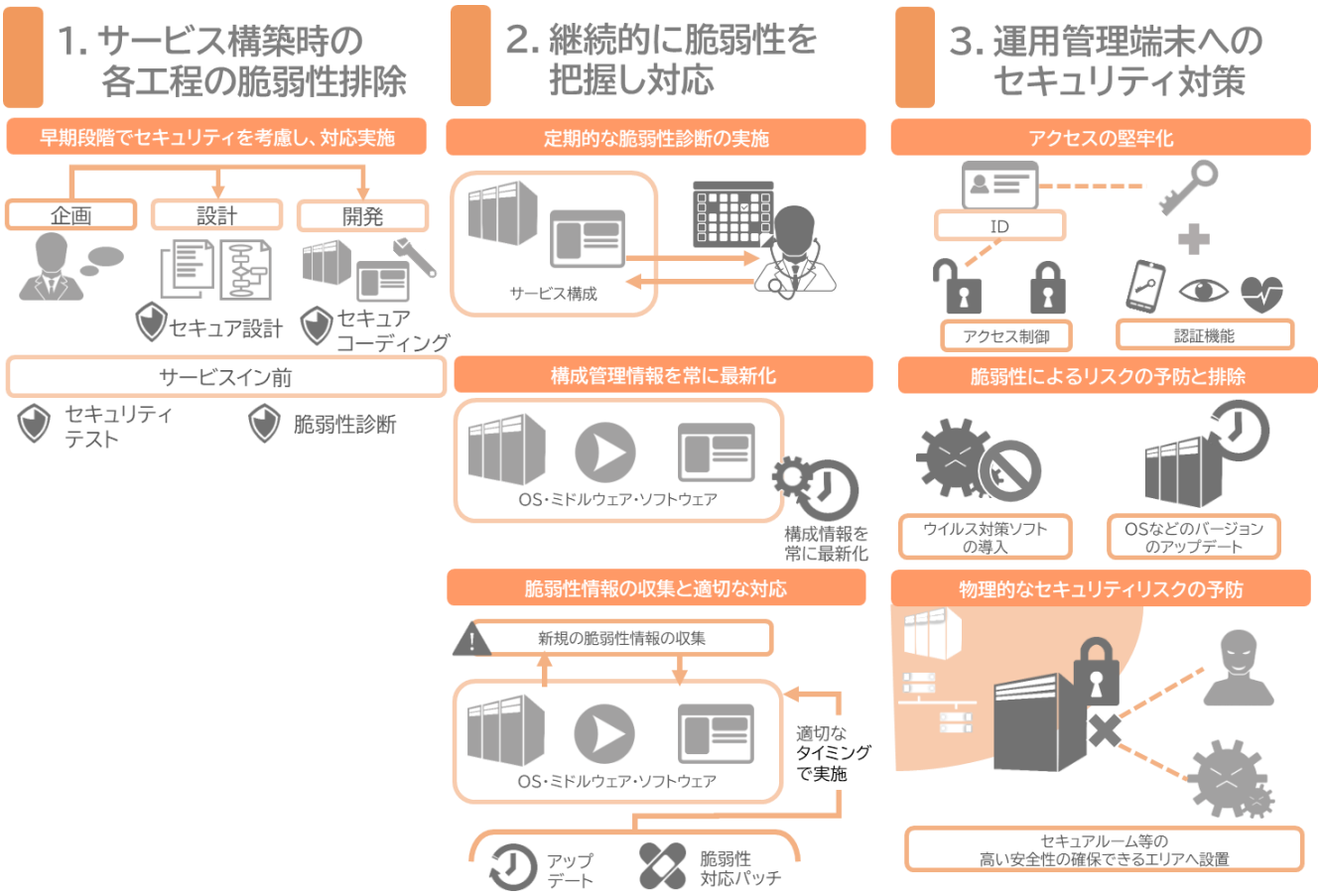


6. セキュリティ監視の実施



③セキュリティインシデント発生の未然防止のためのセキュリティ対策

セキュリティインシデントを未然に防ぐためには、以下対策が効果的です。

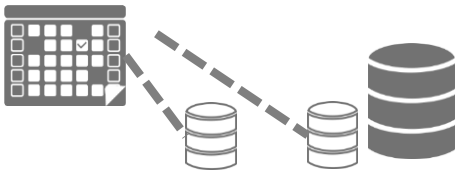


④インシデント発生時に備えたセキュリティ対策

仮にインシデントが発生した場合でも、以下の対応を実施することでサービスへの影響を最小限に抑える事ができます。

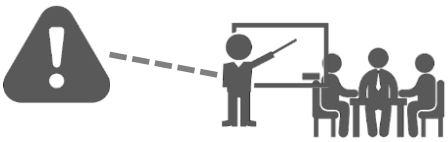
1. 外部との通信やデータの暗号化

2. 定期的なバックアップの取得



3. 証跡確保のためのログの取得

4. インシデント発生時のリスク軽減策を検討



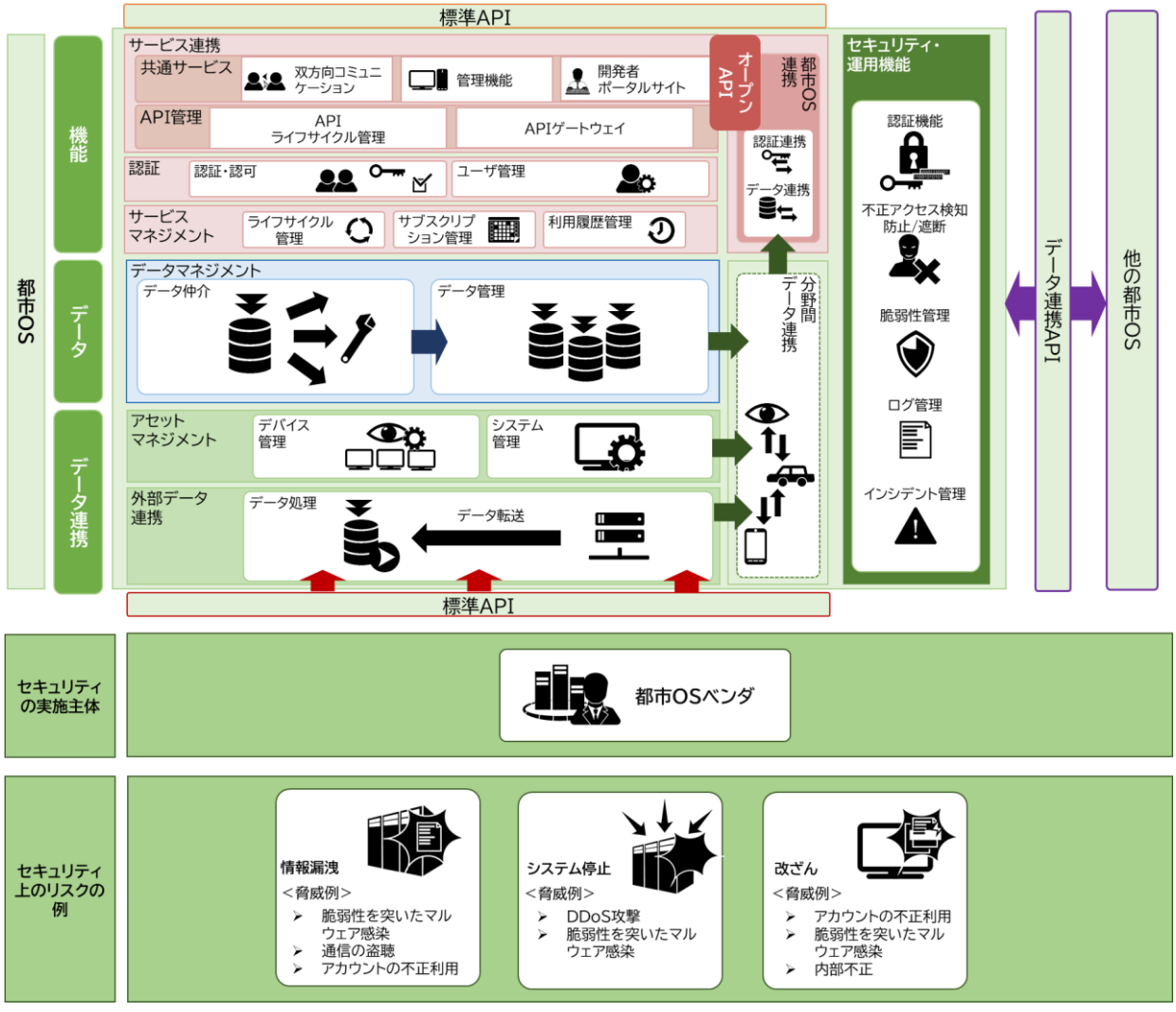
セキュアな都市OS（プラットフォーム）を準備しよう

「都市OS」は、「アセット」から収集したデータを分類・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す。

都市OSの構築・運用を担うのは**都市OSベンダ**であり、セキュリティ対策の実施も都市OSベンダが中心となって実施する必要があります。

代表的なセキュリティリスク

- 不正アクセスによる情報漏洩
- サービス停止やデータの改ざんによる、サービスや人命への影響
- クラウドサービス事業者と利用者の間の曖昧な責任分界によるセキュリティ事故の発生



都市OSにおけるセキュリティ対策のポイント

①外部からの攻撃、侵入等を防ぐセキュリティ対策

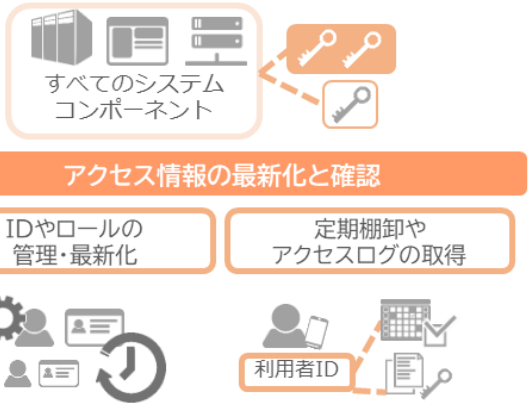
企画、設計・開発段階から、以下のようなセキュリティ設定を行いましょう。

1. 都市OSへのアクセス制御の実装・運用

ファイアウォールの実装

2. 適切な権限設定の実施・管理

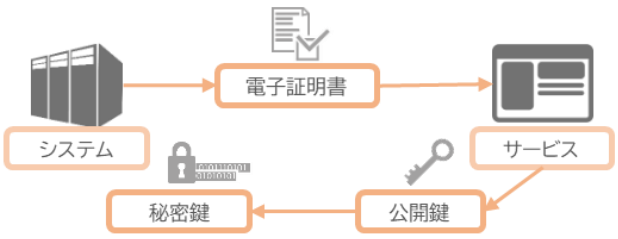
適切な権限付与ができる仕組みを実装



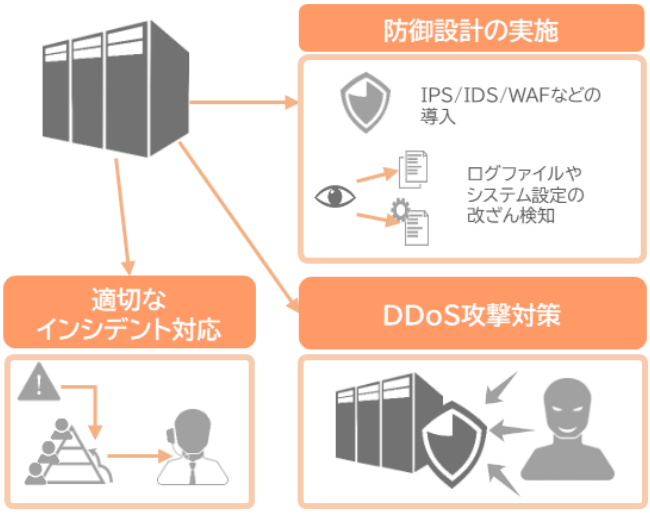
3. 認証機能の実装

多要素認証を採用

システム間の相互認証



4. セキュリティ監視の実施



以下の②、③における対策のポイントは「サービス」の③、④と同一となります。
P10を参照してください。

②セキュリティインシデント発生の未然防止のためのセキュリティ対策

③インシデント発生時に備えたセキュリティ対策

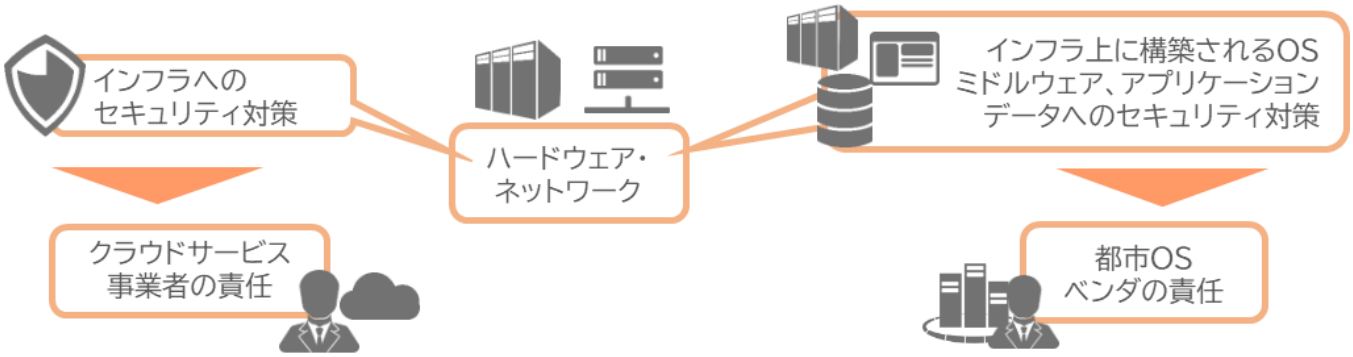
④推進主体からの要求に応じた適切なクラウドサービスの利用

クラウド上で都市OSを構築している場合は、以下のポイントを押さえて、セキュリティ対策をとりましょう。

1. クラウドサービスにおける責任分界点の把握

責任分界点をきちんと把握することで、都市OSベンダ（クラウドサービス利用者）として実施すべきセキュリティ対策が明確になります。

例：IaaS上に都市OSを構築している場合



2. データロケーションに関する要求事項への対応

クラウドの設置場所（リージョン）によってデータの取り扱いに関連する法令が異なる可能性があります。データの取扱いに関するトラブルを未然に防ぐために、以下を確認しておきましょう。

クラウドの設置場所

設置環境における関連法令

有事の際の裁判管轄等

3. 複数リージョン選択による可用性の担保

災害等によるシステム停止等への対応として行いましょう。

異なるリージョンへのデータ保存

BCP環境の構築

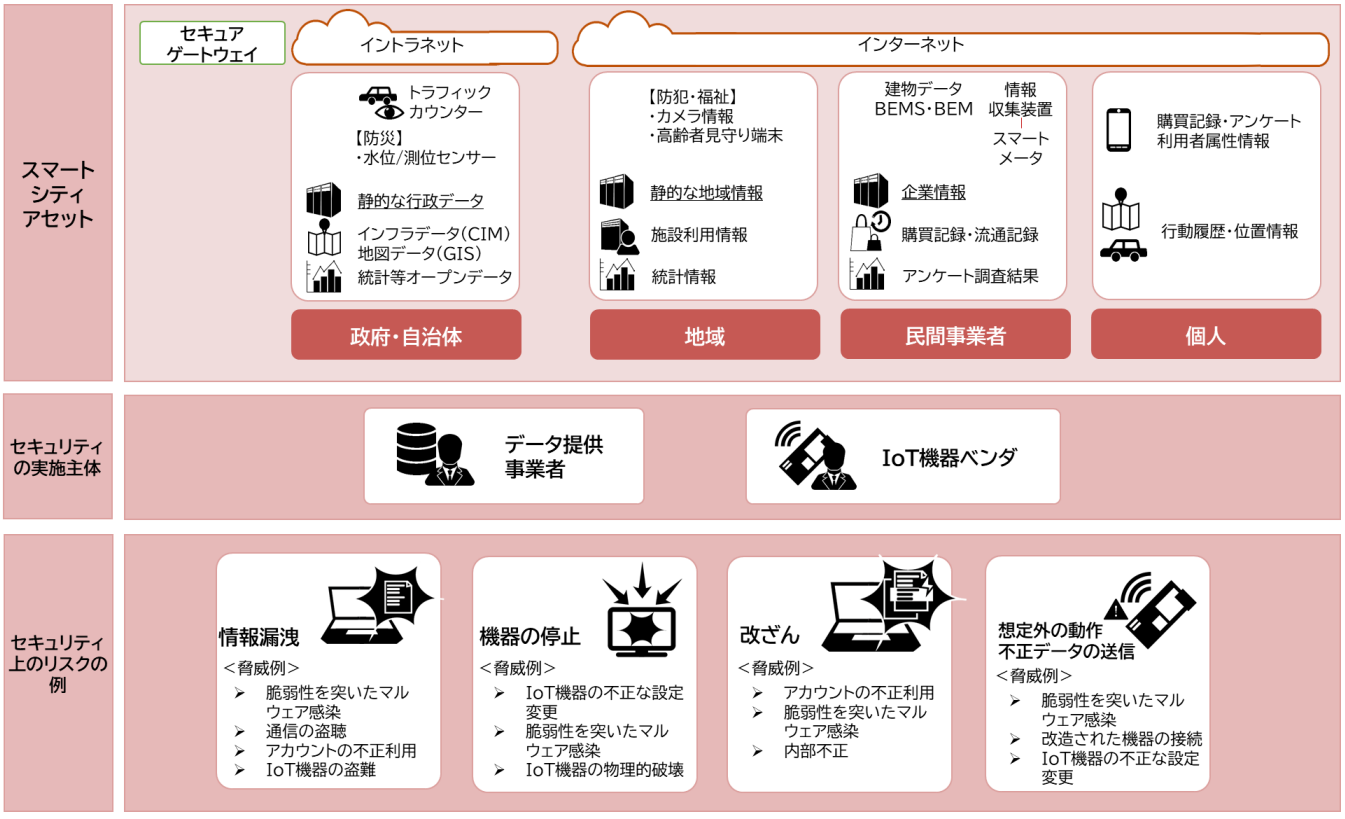
機器やデータを保護しよう

「アセット」は、地域の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**するカテゴリです。

デバイス、ネットワーク、中継機器等でのセキュリティの検討が必要です。

代表的なセキュリティ上のリスク

- IoT機器等のデバイスへのマルウェア感染
- 物理的な破壊や不正アクセスによる停止やデータの改ざん　等



アセットにおけるセキュリティ対策のポイント

①アセットの監視・管理

アセットが正常に稼働しているか（正確なデータが収集できているか）どうかは、スマートシティで提供するサービスの信頼性に影響する重要なポイントとなります。
以下のポイントでアセットの監視・管理を行いましょう。

1. アセットの監視・管理

・アセットの死活監視、効率的な管理

2. 新規の脆弱性情報の把握、及びファームウェア、ソフトウェア等のバージョンアップ

・重大な脆弱性が発生した場合の速やかな対応

②アセットそのものへのセキュリティ対策

アセット自体に関しても、以下のセキュリティ対策を守りましょう

1. 外部との通信や、保有するデータの暗号化

・アセットから都市OSへデータを送信する際の通信を暗号化しよう。
・アセットが保有するデータを暗号化しよう。

2. 認証機能

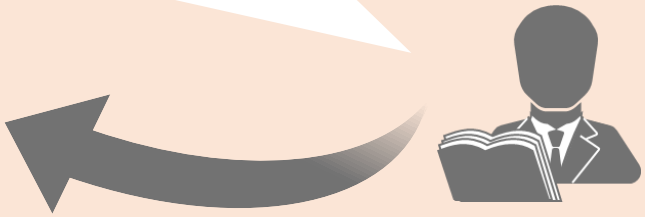
・アセットにアクセスする際に、パスワードを容易に推測ができないように設定し、セキュリティを高めよう。
・監視カメラ等のプライバシーが関わるアセットの場合には、認証を強化しよう。
また、IoT等に付帯するWebサービスの認証強度にも注意しよう。

3. 物理的なセキュリティ

・物理機器を手の届かない場所や、関係者以外による物理的なアクセスを制限した場所で設置しましょう。
また、何らかの誤動作が起きたとしても人命の影響が発生しないように、安全側（セーフ側）に倒れるようなフェイルセーフを考慮した設計をする必要があります。

スマートシティの4つのカテゴリにおける
セキュリティ対策については以上となります。

次頁より、横断的なセキュリティ対策について
ご説明いたします。

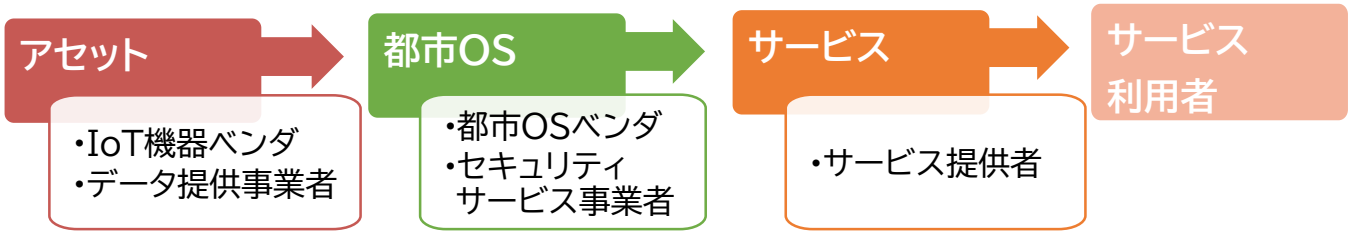


3 横断的なセキュリティ対策

サプライチェーン全体を管理しよう

サプライチェーン管理

データの流れ



スマートシティのサプライチェーンでは、それぞれのサービスや基盤を支える委託・再委託先や、様々な機器・ソフトウェアを供給する事業者など、多くの関係者が複雑に関与しており、サイバー攻撃の起点が拡大することで発生する被害の影響範囲が広くなることが懸念されます。

これらの対策として、以下のポイントを踏まえて、適切にサプライチェーン管理を行いましょう。

①サプライチェーン全体のリスクを管理・把握する

スマートシティに関わっているマルチステークホルダ全体を把握する

<u>スマートシティ推進主体</u>は

- スマートシティ全体のセキュリティに対する一義的な責任主体となり、業務委託先や業務提携先等の関係事業者との間の共通認識醸成と役割分担整理を実行することを推奨する
  - 業務委託先に対して推進主体はデータの取扱いを中心に業務委託先役務全体の責任を負う
  - 業務提携先に対して推進主体はデータの取扱いを中心に業務提携先役務に関しての責任は負わない

<u>業務委託先や業務提携先</u>は

- 推進主体がサプライチェーンを管理・把握できるようにするための適切な情報提供を行う
- 再委託先や利用している製品・ソフトウェア等の情報の適切な管理・把握を行う

②業務委託先や業務提携先のセキュリティ管理体制を評価する

業務委託先や業務提携先のセキュリティ体制の評価

- セキュリティチェックシートに回答してもらい、その回答を持って委託先のセキュリティを評価する
- ISO/IEC 27001等のセキュリティに関する第三者認証の取得状況を確認し、評価する

契約期間中においても定期的に評価を行い、不十分な点があれば改善を求める

③サプライチェーン全体の脆弱性情報を適切に把握し、対応する

継続的な脆弱性への対応が期待できるソフトウェアやハードウェア等を選定する

- 脆弱性への対応体制が十分なIoT機器のメーカ
- 継続的なサポートが保証されるような機器

脆弱性情報を適切に把握し、迅速に対処する

推進主体は

- サプライチェーン間の契約や、調達時の仕様に含める内容として、「脆弱性情報を適切に提供し、対応する」ことを記載する

業務委託先・業務提携先側は

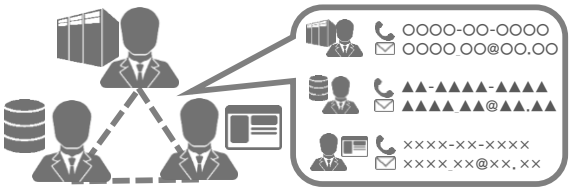
- 自身が構築・運用している基盤やサービスなどを構成するソフトウェアやハードウェアなどを適切に管理する
- 公開情報や脆弱性情報配信サービスなどから脆弱性情報を収集・把握し、それらの脆弱性がスマートシティサービスに与える影響などを判断した上で、委託元と連携して迅速に脆弱性に対処する
- なお、損害賠償等金銭的な負担が生じる場合の求償関係は業務委託先・業務提携先との契約によることになる

インシデント対応時の連携に向けた準備をしよう

スマートシティ内でセキュリティインシデントが発生した際に、被害が拡大することを防ぐため、スマートシティに関与するマルチステークホルダが能動的に連携し、対応を図ることが重要です。

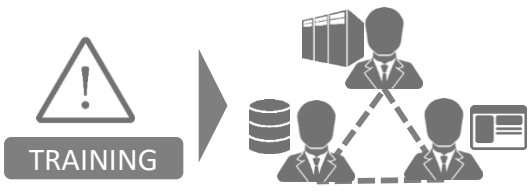
また、利用者・市民に向けた適切な情報発信と利用者からの問い合わせを受け付ける窓口の情報等を明確にするなどのコミュニケーション施策も同様に重要な取り組みとなります。

①責任範囲を明確にしたセキュリティインシデント対応体制を構築する



②連絡窓口を整備し、マルチステークホルダ間で共有する

③スマートシティ全体及び各マルチステークホルダにおけるセキュリティインシデント対応手順の整備と事象解析・復旧に必要な情報を事前に整理しておく



④定期的にセキュリティインシデント対応訓練・演習を実施する
また、最新の脅威やインシデント事例なども定期的に収集し関係者間で共有する

データ連携時のセキュリティを確保しよう

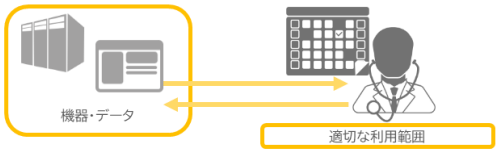
スマートシティのデータ連携においては、各事業者等におけるAPIを介してデータ連携が行われるが、適切でセキュアなデータ連携が行われるように、その認証・制御についてはデータ連携基盤で実施されることが多い。

データ連携における対策のポイント

①データ連携元・連携先のセキュリティ体制の確認・評価

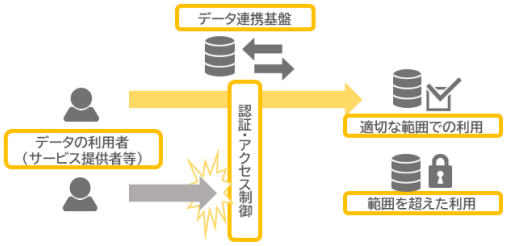
連携元・連携先組織でのセキュリティマネジメントを確認する

機器やサービスの信頼性を評価する



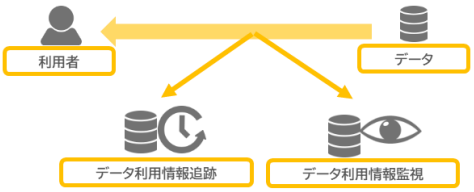
②データ提供事業者・サービス提供者等の認証と適切なアクセス制御

データ連携基盤を介して認証したうえで、適切なアクセス制御を実装する



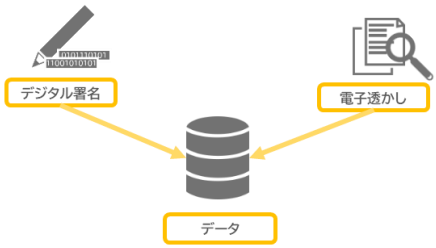
③データの追跡可能性を確保しデータ利用の透明性を担保する

データの利用状況の監視・追跡の機能を設け、データの追跡可能性を確保する



④データの原本性保証を確保しデータの信頼性を担保する

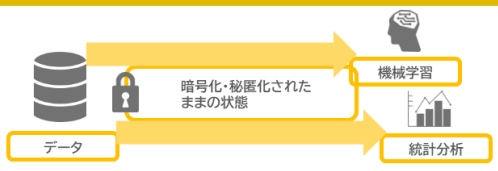
デジタル署名、電子透かしなどを活用し、データの原本性を確保する



⑤必要性に応じたデータの匿名化・秘匿化

データから個人特定ができないよう匿名加工を行う

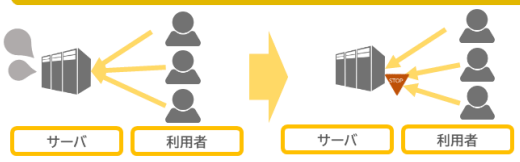
データに暗号化・秘匿化を施したまま利用を行う



⑥ APIにおけるセキュリティの確保

TLSを用いた認証や通信の暗号化

サーバへの負荷を考慮し適した機能を実装する



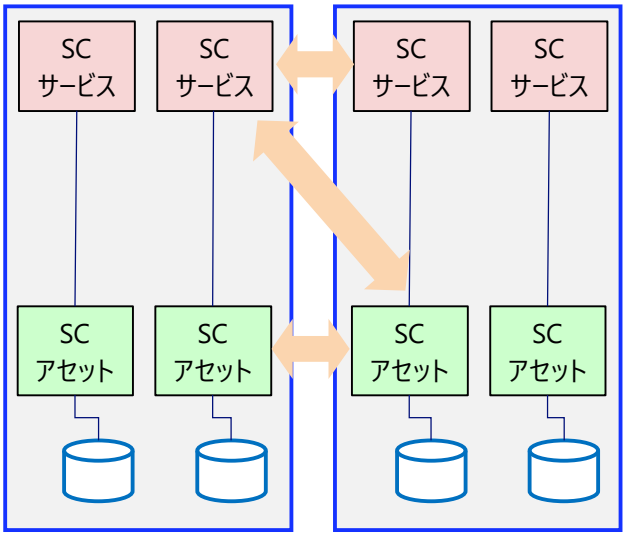
データ連携時のパターン毎の特徴を理解しよう

他の都市・地域とのデータ連携を実施する場合のパターンは主に4パターンが考えられる。
それぞれのデータ連携パターンには、特徴があるため、理解した上で選択することが最適解である。

データ連携パターン毎の特徴

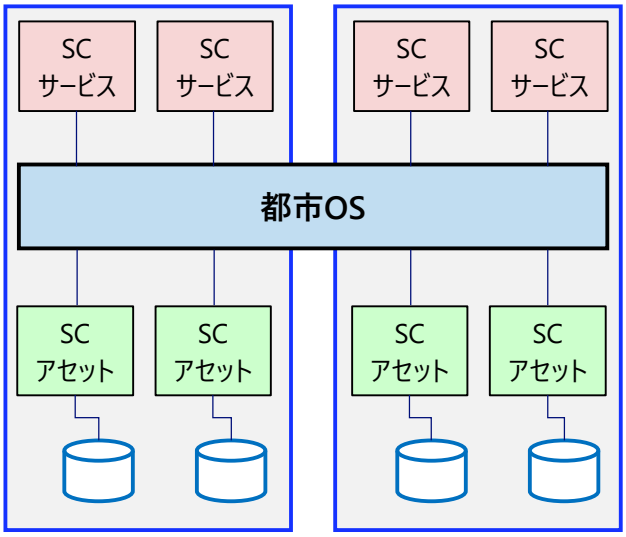
①個別連携型（都市OS支援なし）

都市OS 等による支援がなく、個々のステークホルダーが、他の都市が提供するスマートシティの機能を直接利用する方法



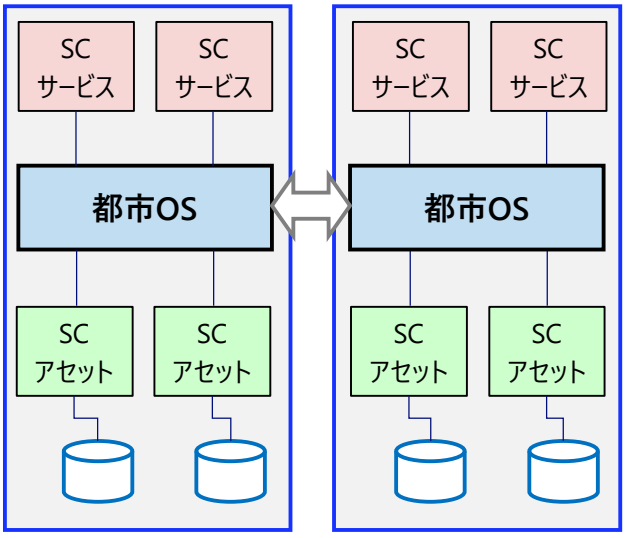
②都市OS共有型（集中型連携）

広域の複数の都市・地域で、共通の都市OSを共有する密結合型の連携方式



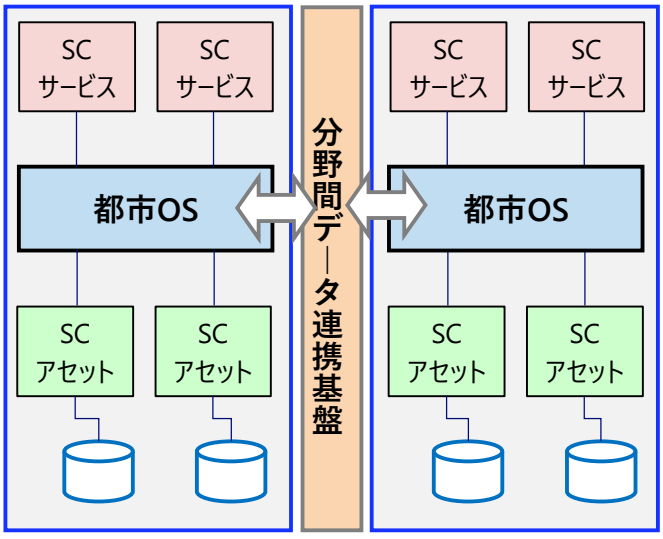
③都市OS連携型（分散型連携）

個々の都市・地域で導入した個々の都市OSとの間でAPIを介した疎結合型の連携方式



④連携基盤利用型（連邦型連携）

分野間データ連携基盤がハブとなり、個々の都市・地域で導入した個々の都市OSがこのハブと接続することで、間接的に都市・地域間が連携される方式



4 事例紹介

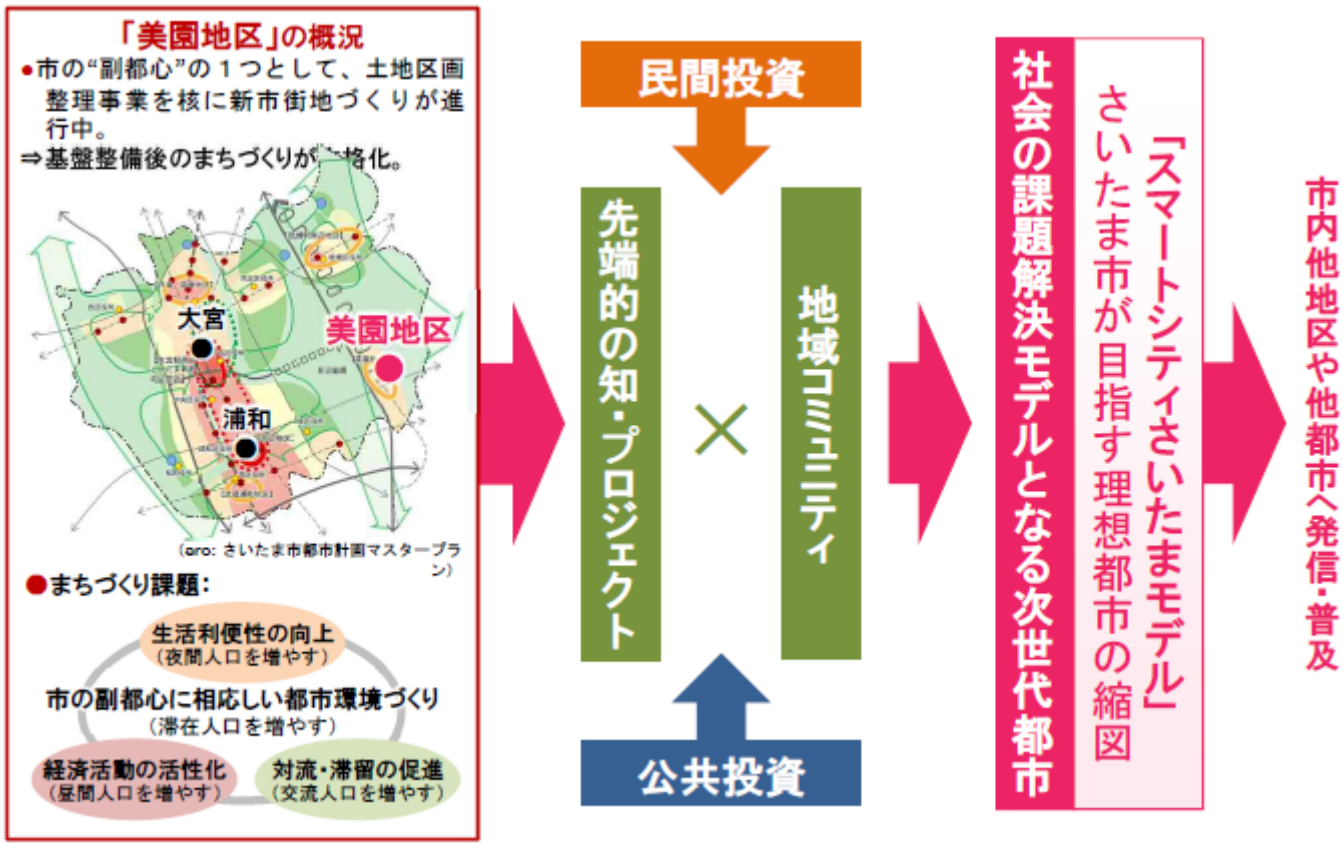
「公民＋学」連携により構成されたガバナンス ◎さいたま市

さいたま市の副都心の一つに位置づけられ、大規模な都市開発の進む「美園地区」において、次世代のまちづくり方策の構想・実践に向けて、住民・地権者・民間事業者・行政機関・専門家など本地区で活動する多様な個人・組織等が協働・連携しながら、地域課題解決に取り組むためのまちづくり拠点施設**「アーバンデザインセンターみその（略称：UDCMi）」**が2015年より運営されています。

主にソフト分野の調査検討・企画調整・事業化を行う**「美園タウンマネジメント協会」**と、主としてハード分野の検討・協議調整を行う**「みその都市デザイン協議会」**の、2つのまちづくり連携組織がUDCMiを拠点に活動を進めています。

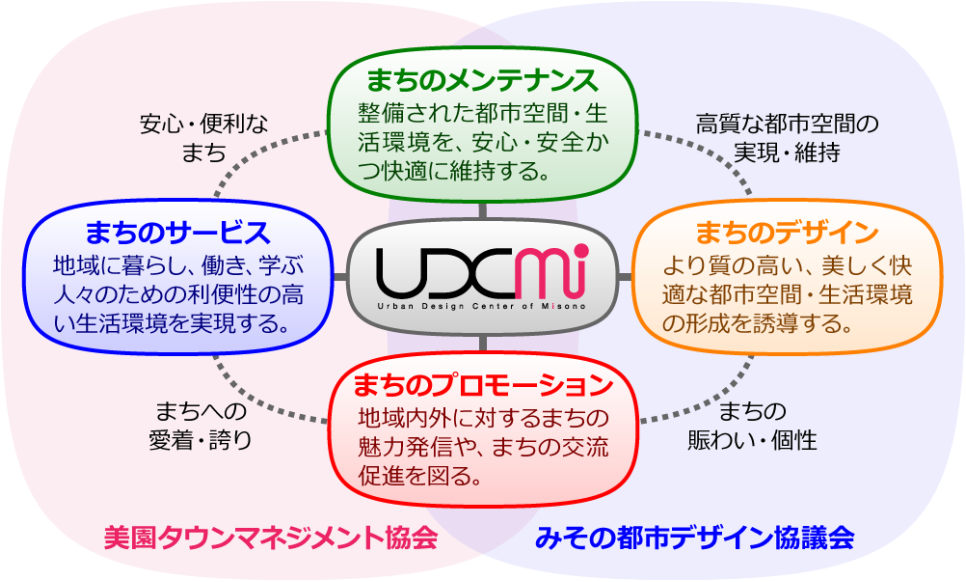
協会事務局である**（一社）美園タウンマネジメント**では、個人情報について適切な保護措置を講ずる体制を整備してます。さらに、昨今の情報銀行の動向注視しながら、データ取扱いに関するポリシーも議論が進んでいます 。

美園タウンマネジメント協会体制



事業内容

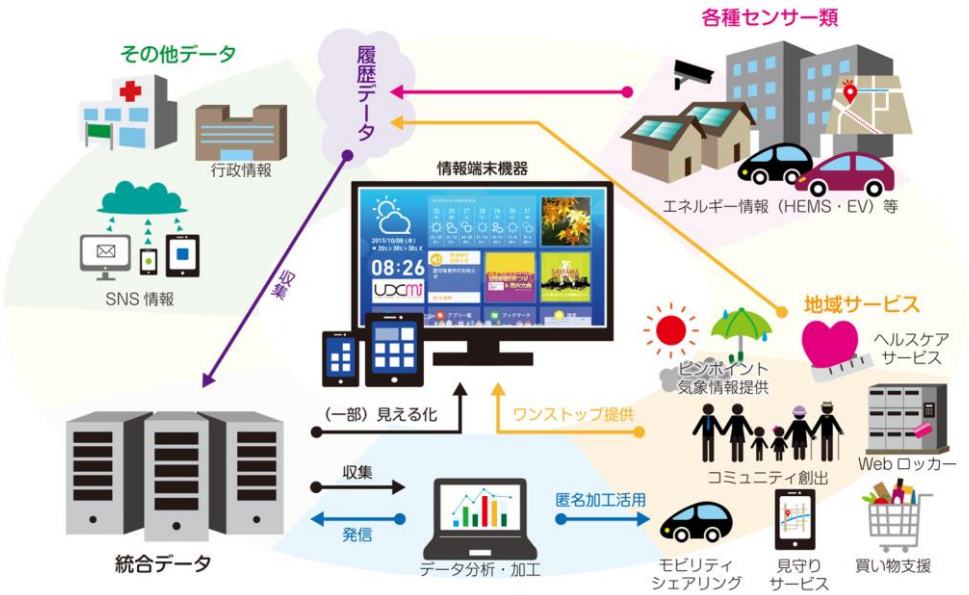
UDCMiという“場”を介して、「デザインマネジメント」・「メンテナンスマネジメント」・「サービスマネジメント」・「プロモーションマネジメント」の各分野に亘るプロジェクトの企画立案・試行的実践（社会実験）・まちへの実装化（事業化）等を促進させ、地区まちづくりに係る各者の連携・役割分担に基づく持続可能な地域マネジメント体制の構築を図っています。



さいたま市の「統合データプラットフォーム」についての取組み

美園地区では、子育て世代を中心とした居住人口の急増に伴い、多様化するライフスタイルやニーズに応じて、住民一人ひとりに合わせた地域サービスの充実が、まちづくり課題の一つとなっています。

地域サービスを取り巻く環境を見ると、IoT・AI・ビッグデータ等のIT技術の目覚ましい進歩により暮らしの利便性が増した一方で、それら技術を通じて収集される**パーソナルデータの扱い方を巡る議論**も、国内外で本格化しています。

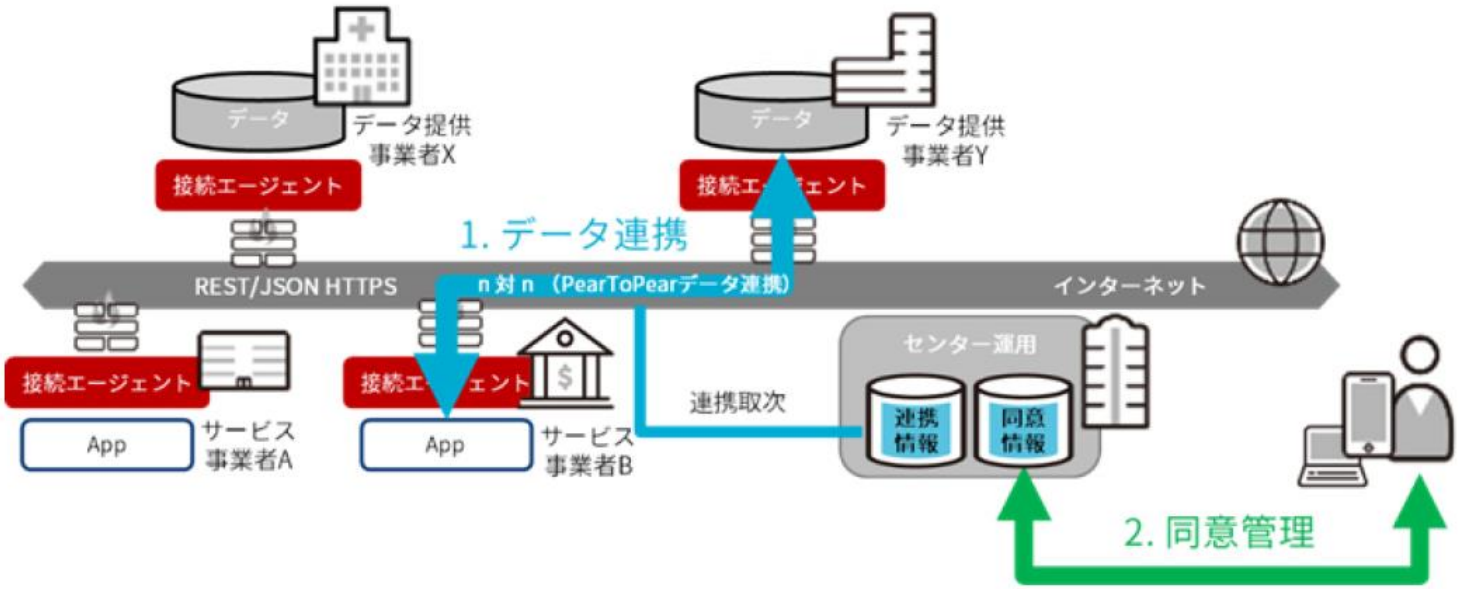


こうした社会情勢も踏まえ、個人のプライバシーを守ったデータの安心・安全な管理を研究してきた慶應義塾大学西宏章教授の協力のもと、2015年より「共通プラットフォームさいたま版」の開発を、美園タウンマネジメント協会の重点施策の1つとして進めてきました。

パーソナルデータを安心・安全に取り扱うための動的なアクセス制御
◎柏の葉スマートシティ

三井不動産株式会社、BIPROGY株式会社は、生活者が所有するパーソナルデータを、本人の意思に基づき、安心・安全に業種・業界を横断して流通させることを可能とするプラットフォーム**「Dot to Dot」**を共同で開発しました

Dot to Dotの特徴

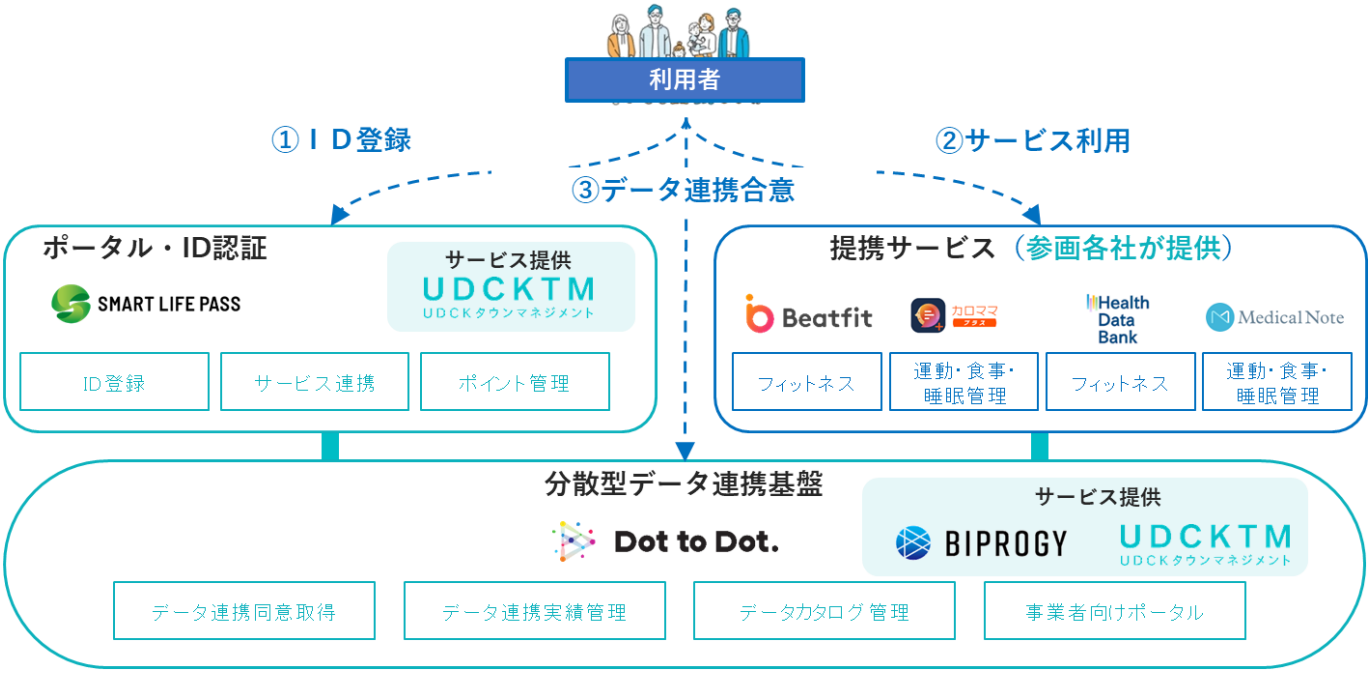


「Dot to Dot」は、生活者が所有するパーソナルデータの活用の意思決定権利は個人にあるという**「データの個人主権」**と、事業者が責任をもって自社サービスのデータ管理を行い、必要なときのみ他の事業者とデータを連携する**「分散型データ管理」**の2つの理念に基づき開発されたプラットフォームです。

■ **個人主権によるデータ連携**
- 利用者は流通・利用される自身のパーソナルデータの内容や目的を理解し、価値を感じた利用ケースのみに同意することができます。同意の要件は個人情報保護法に準拠しています。
- 利用者は一度同意した内容に対し、同意期限の変更や取り消しを行うことができます。また、自身のデータがいつ・どこに連携されたか確認できます。

■ **分散管理によるセキュアなデータ連携**
- 事業者間のデータ連携時は、データ送信元の身元やデータの正しさが「Dot to Dot」により保証され、安全性の高いデータ連携を実現します。
- データ連携は事業者間で直接行われるため、「Dot to Dot」が流通するデータを取得することはありません。

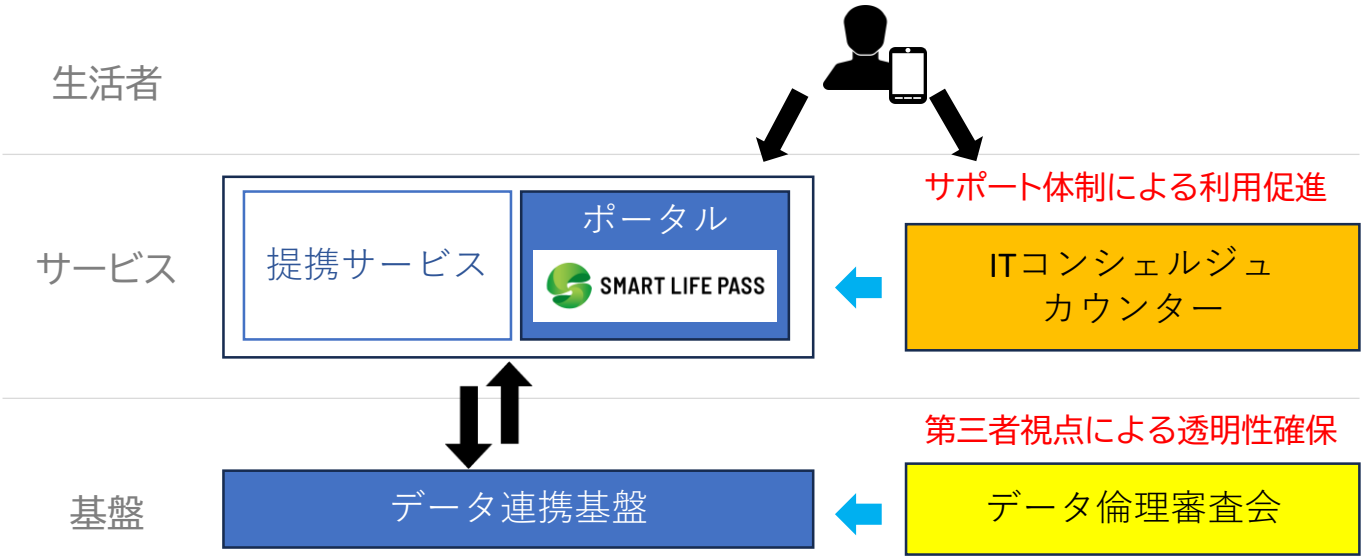
サービス例:
生活をより豊かにするためのポータルサイト「スマートライフパス」



「スマートライフパス」は、生活を豊かにするサービスを利用できるポータルサイトです。登録すると、様々な提携サービスを利用することができます。登録手続きにおける本人確認には、オンライン上で完結する仕組み（eKYC）が導入されており、利用者の負担を軽減する工夫がされています。このeKYCでは、マイナンバーカードによる公的個人認証サービス（JPKI）を含め、各種公的身分証明書が利用可能です。
スマートライフパスでは様々な提携サービスを提供しており、上記の本人確認情報を基に指定されたエリアでは利用者が無償でサービスを利用できます。サービスはそれぞれの運用企業が自社の責任で提供しています。

また、これまで情報管理上の問題からサービス間でのデータ提供ができず、複数のサービスを利用する際はそれぞれのサービスに自身のパーソナルデータの入力が必要でした。「スマートライフパス」では、「Dot to Dot」を活用することで、提携サービス間におけるパーソナルデータ連携が可能となり、利用者の煩雑なデータ入力・手続きを省略することができます。なお、パーソナルデータは、生活者の方の同意がないと連携はされません。このように適切な権限管理を実現し、必要な先に必要な情報だけを連携し、連携するデータの透明性を実際に確保しています。

組織・体制



「スマートライフパス」は、生活者がより豊かな生活をするためのサービスであり、一人でも多くの方に利用してもらうことに意義があります。一方で、サービス利用にはスマートフォンの使用が必須となりますが、スマートフォンの操作に不慣れな方もいらっしゃいます。ITの利用が障壁となるため、それを解決し、利用促進となる施策として、対面型窓口である「ITコンシェルジュカウンター」を2拠点設けています。

対面型の窓口を設置することで、オンラインでの相談が難しい利用者に対して手厚いサポート体制を提供することができます。また、スマートフォンの紛失や盗難、アカウントパスワードを忘れてしまった場合等の相談も可能で、セキュリティ面でのフォローにも役立っています。このITコンシェルジュカウンターにより、誰もが便利で安心して使えるサービス運営が行われています。

柏の葉スマートシティでは、利用者本人の意思に基づき、パーソナルデータがデータ連携基盤を通じて提携サービス間に連携されることで、既存サービスの改善、新たなサービスの開発等に役立てられています。

一方で、パーソナルデータの運用に関しては、適切に行われる必要があります。柏の葉スマートシティにおけるデータ連携基盤の管理は、委託先の事業者により適切に行われています。しかしながら、パーソナルデータの運用が事業者任せになってしまうことは、透明性確保の観点が不十分です。そこで、第三者視点でデータの取り扱いに関して評価する組織として**「データ倫理審査会」**が設置されています。

データ倫理審査会は、データの運用に関して、柏の葉におけるデータ利活用の指針である「データ倫理原則」や法令、ガイドライン等が遵守され、適切な運営がされているかを審議し、また必要に応じて助言を行う第三者機関です。データ倫理審査会により、パーソナルデータの利活用に関する透明性が確保され、安心できるデータ連携基盤の運営が行われています。

安心・安全なデジタルIDとデータガバナンスの取組
◎前橋市

共助型未来都市を支える「デジタルID」と「官民連携会社」

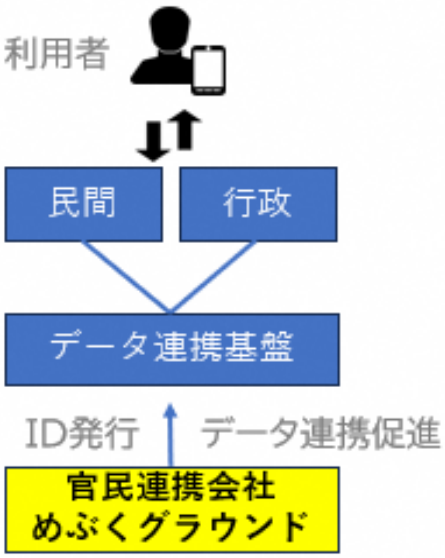
前橋は市民によって育まれる共助型未来都市、一人ひとりがWell-Beingでいられる街をめざして、リアル/デジタル両面でのまちづくりを推進しています。

共助型未来都市において求められる要件として、以下の要件が求められています。

- 本人の同意に基づいて、市民・民間サービス・公的サービスとつながる安心・安全な仕組み
- 個人情報を含むデータの取り扱いに対するガバナンスと透明性の確保
- 暮らしのあらゆる局面の課題解決と様々な領域での自己実現に邁進できるようなパーソナライズサービスの提供

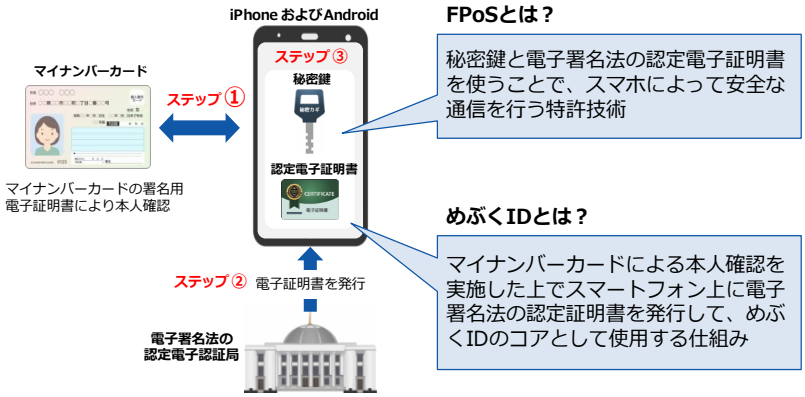
これらを実現するため、「めぶくID」を開発し、管理運用を行う「めぶくグラウンド株式会社」を官民で連携して設立しました。

「めぶくグラウンド」は共助による豊かで人に優しい社会の構築に向けたデータ提供者の意思と利益を守る役割として「データガバナンス委員会」を設置し、データ保護に関する各種討議や、意思決定を行っています。 また、不適切なデータ利用防止策として、各関連事業者とデータ保護に関する罰則規定を含めた契約を締結し、スマートシティ全体でデータ保護に取組む意識を醸成しています。



「めぶくID」は、利便性と安心・安全なスマートシティサービスの提供を目的としたデジタルIDです。マイナンバーカードによる本人確認を実施した上で、FPoS（FinTech Platform over SIM）技術を用いて秘密鍵と電子署名法の認定電子証明書を使うことで、スマホによって安全な通信を実現する技術を導入し、かつ電子署名法の認定電子証明書をデジタルIDとして活用することにより、法的裏付けをもったIDとして利用者のデータを安心・安全に守ることができます。

また、医療・福祉、教育、公共交通といったさまざまな公益、準公共、民間サービスにおいて、本人性、真正性、利便性、自己主権の4つの重要な観点を確保しながら、「めぶくID」自体は個人データを所有せず個人情報を流通させないデータ連携を実現することができます。



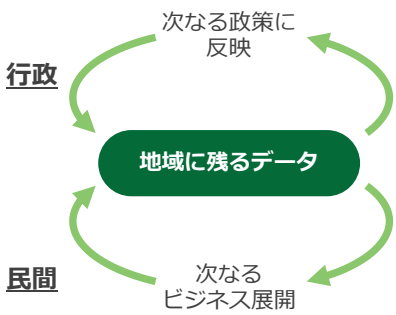
自身の意志に基づいたデータ連携 「ダイナミックオプトイン」

めぶくIDのシステム面では各サービスへのパーソナルデータのデータ連携には、利用規約で対象・目的を明示した上で、「めぶくアプリ」の中で利用者のデータ連携の同意取得（オプトイン）を制御可能とした「ダイナミックオプトイン」機能を実装し、パーソナルデータの自己主権を確保する仕組みを提供しています。
ダイナミックオプトインは利用者がいつでも、自由なタイミングでデータ連携の同意許諾を制御することができるため、自身の意志に基づいたデータ連携を実現しています。
また、オプトイン取得時には、電子署名法の認定電子証明書による電子署名を実施しており、法的裏付けをもったオプトインを取得することができます。
その他にも、パーソナルデータは分散型のデータ連携方式をとり、データ連携基盤には保存しない方針とすることで、基盤環境におけるデータ保護のリスク低減を図っています。

「めぶくID」を活用した安心・安全な電子地域通貨「めぶくPay」

めぶくIDを活用した電子地域通貨「めぶくPay」を提供しています。地域の決済データをめぶくIDで安心・安全にデータ連携を行い、データを地域に残すことで、行政による次なる政策への反映、民間企業による次なるビジネス展開等への活用を想定しています。

地域に残るデータの活用に関しては、データガバナンス委員会にてそのあり方を議論しながら、地域経済の活性化を目指します。



データ活用に関しては、めぶくグラウンドのデータガバナンス委員会で議論しながら進める。