別紙３

スマートシティセキュリティガイドブック

2021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」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。

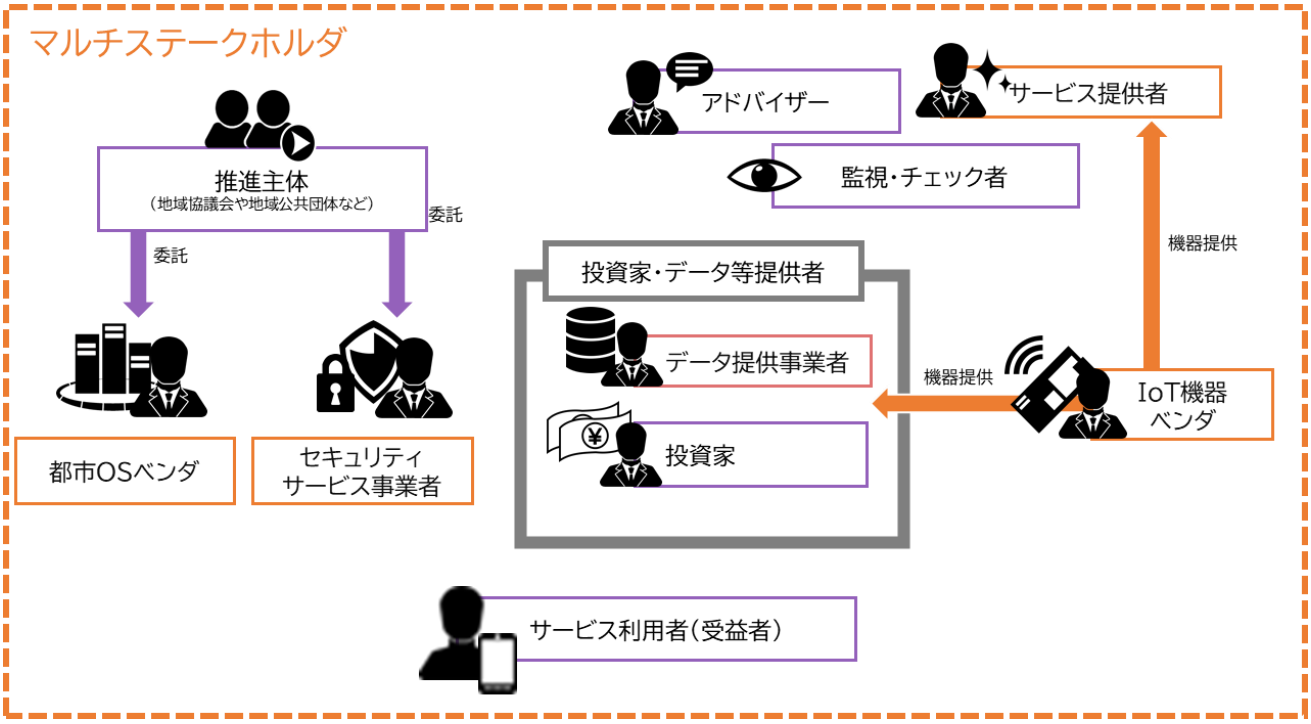
本冊子は、このガイドラインを活用しようとされる方々への
導入ガイドブックです。

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

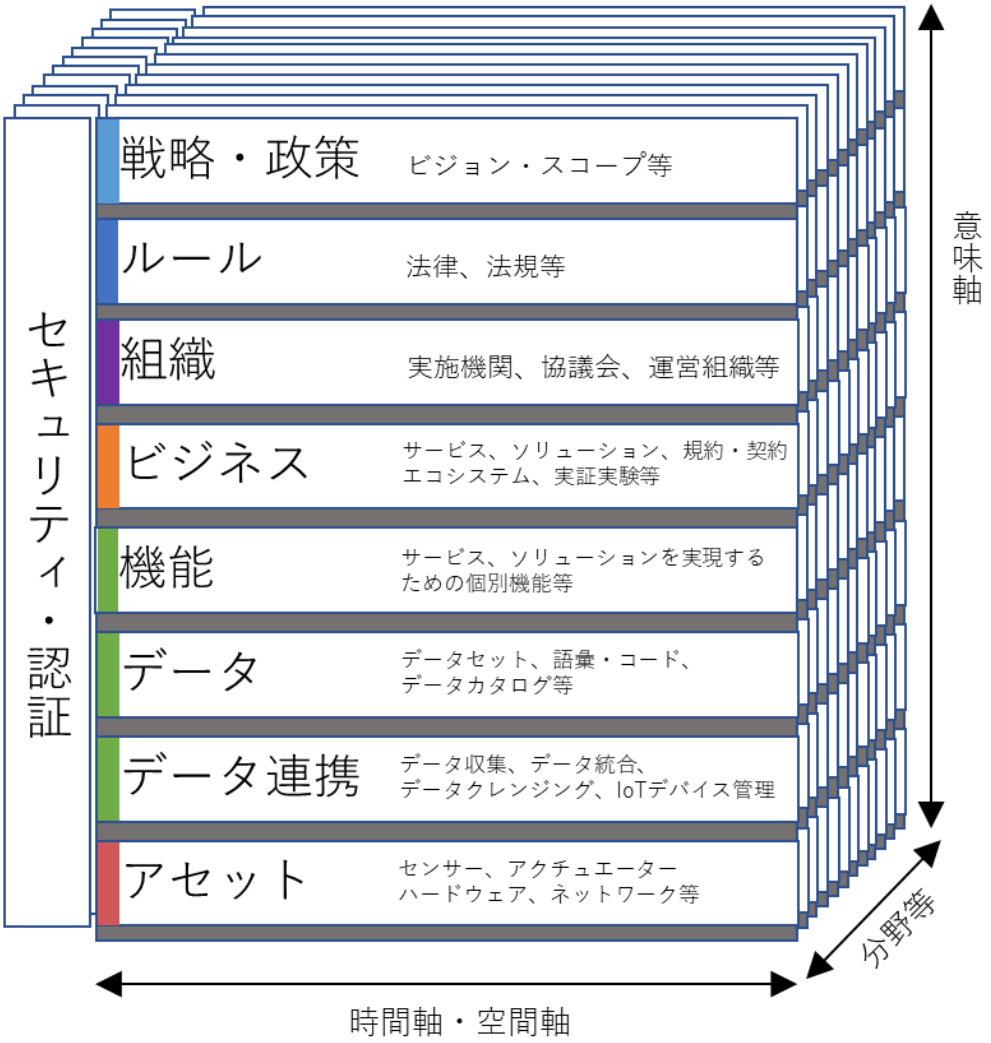
スマートシティリファレンスアーキテクチャとは？

「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。

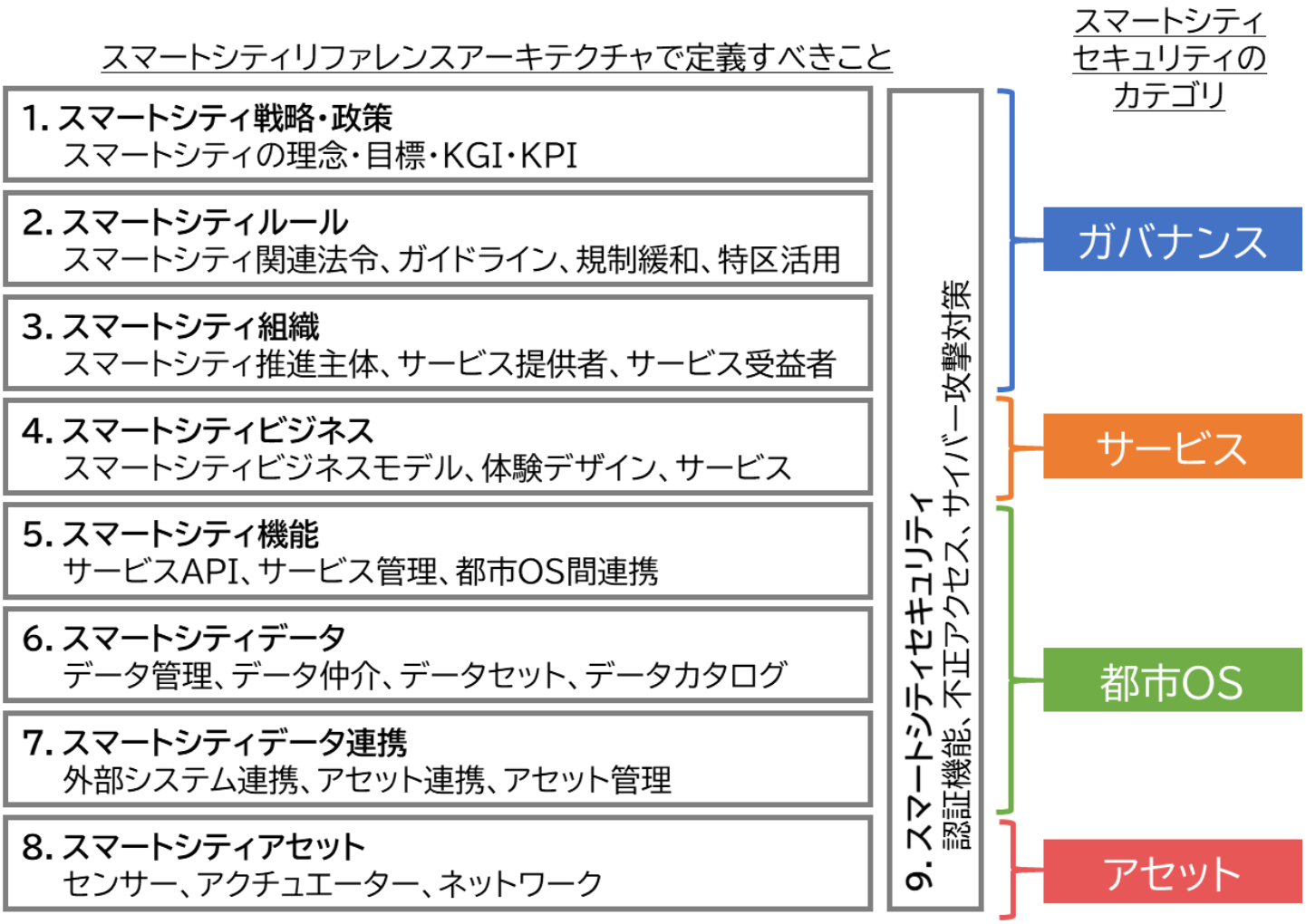
スマートシティリファレンスアーキテクチャで示されている参照すべきモデル



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。

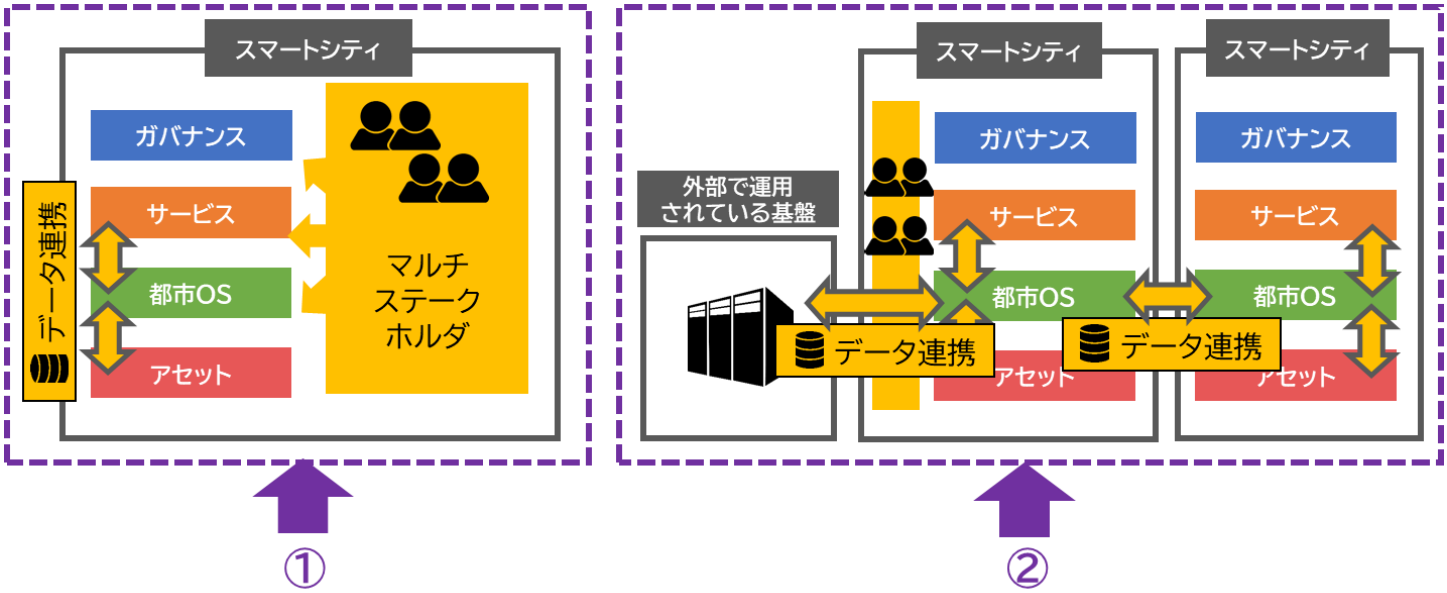
Case 1：各カテゴリにおけるセキュリティ検討



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特有のセキュリティの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な**スマートシティ特有のセキュリティ対策**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

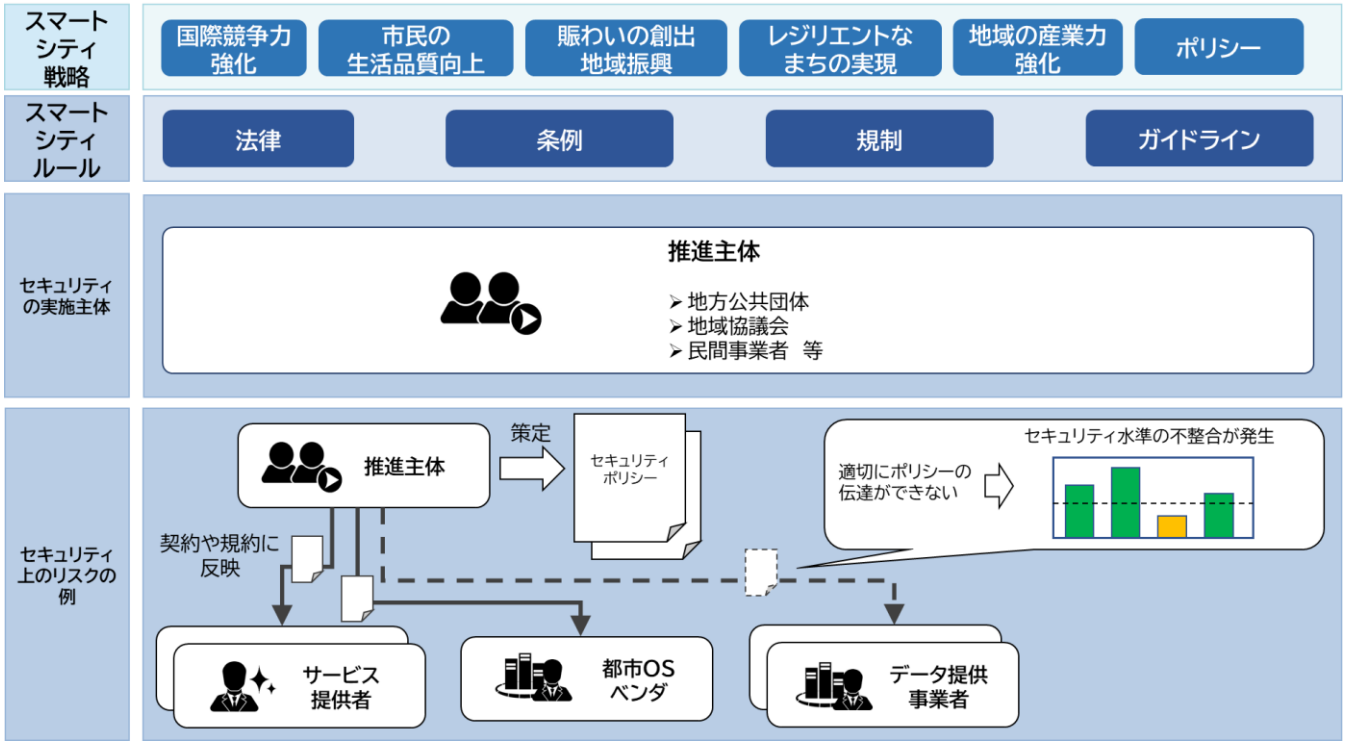
ガバナンスを構築しよう

「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管理や推進を執り行う推進主体**が中心となって検討・実施されることが多いです。

代表的なセキュリティ上のリスク

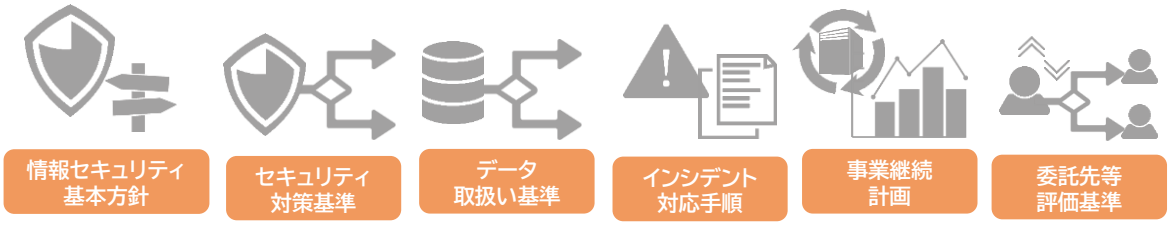
- マルチステークホルダ間におけるセキュリティ水準の不整合が発生し、セキュリティが弱いコンポーネントが発生する
- 上述のコンポーネントでセキュリティインシデントが発生することでスマートシティに対する利用者からの信頼度が低下する



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。

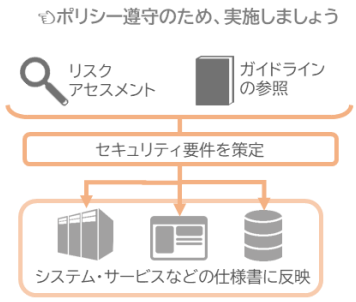
1. リスクアセスメントの実施
2. 法令やガイドライン等との整合性の確認

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。

1. セキュリティ要件を調達仕様書に反映

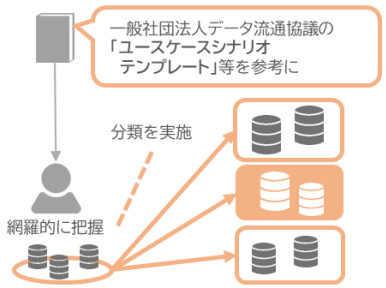
当該委託事業において



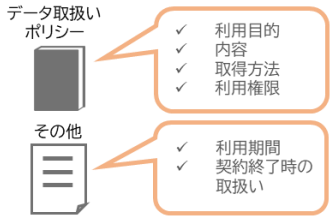
運用に関する委託を実施するとき

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

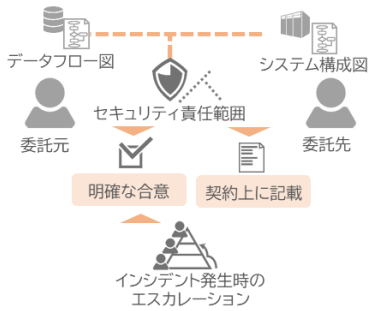


データの取り扱い方を決める

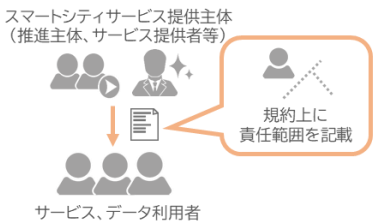


3. 契約・規約で責任範囲を明確化

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。

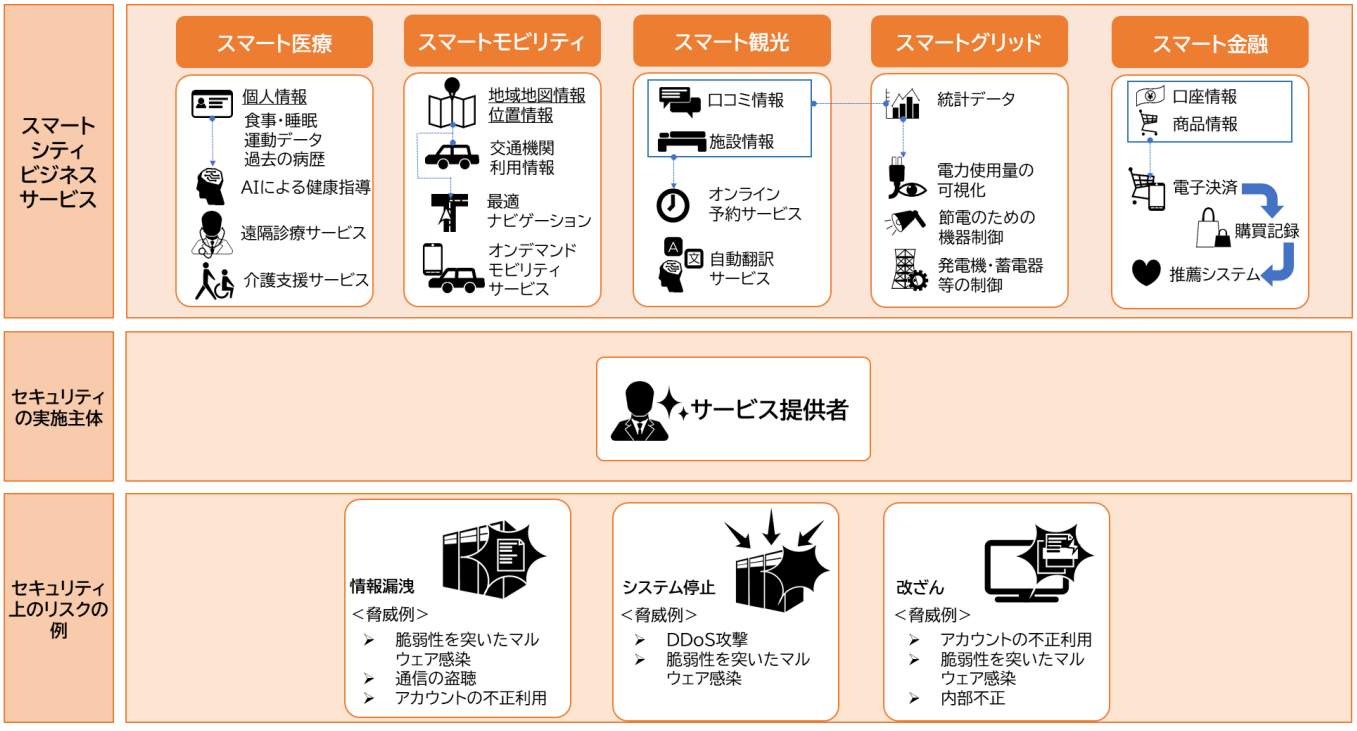
セキュアなサービスを提供しよう

「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. 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。

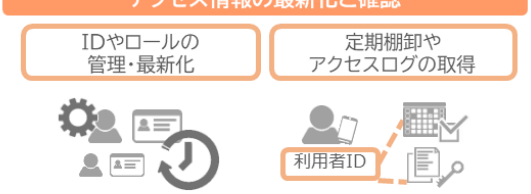
1. サービスへのアクセス制御実装・運用

ファイアウォールの実装

2. 適切な権限設定の実施・管理

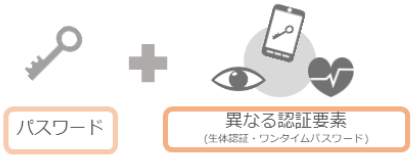
適切な権限付与ができる仕組みを実装

アクセス情報の最新化と確認

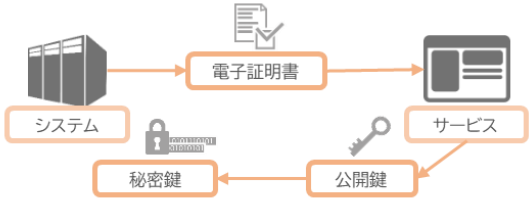


3. 認証機能の実装

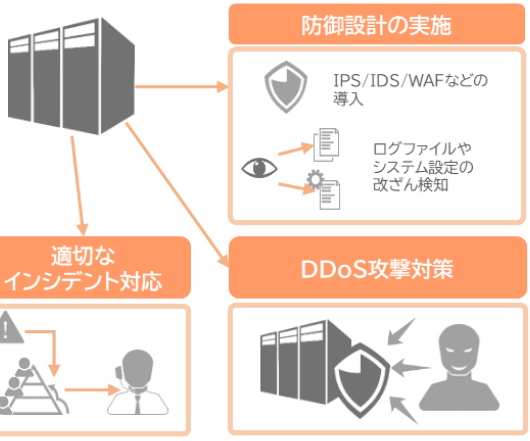
多要素認証を採用



システム・サービス間の相互認証

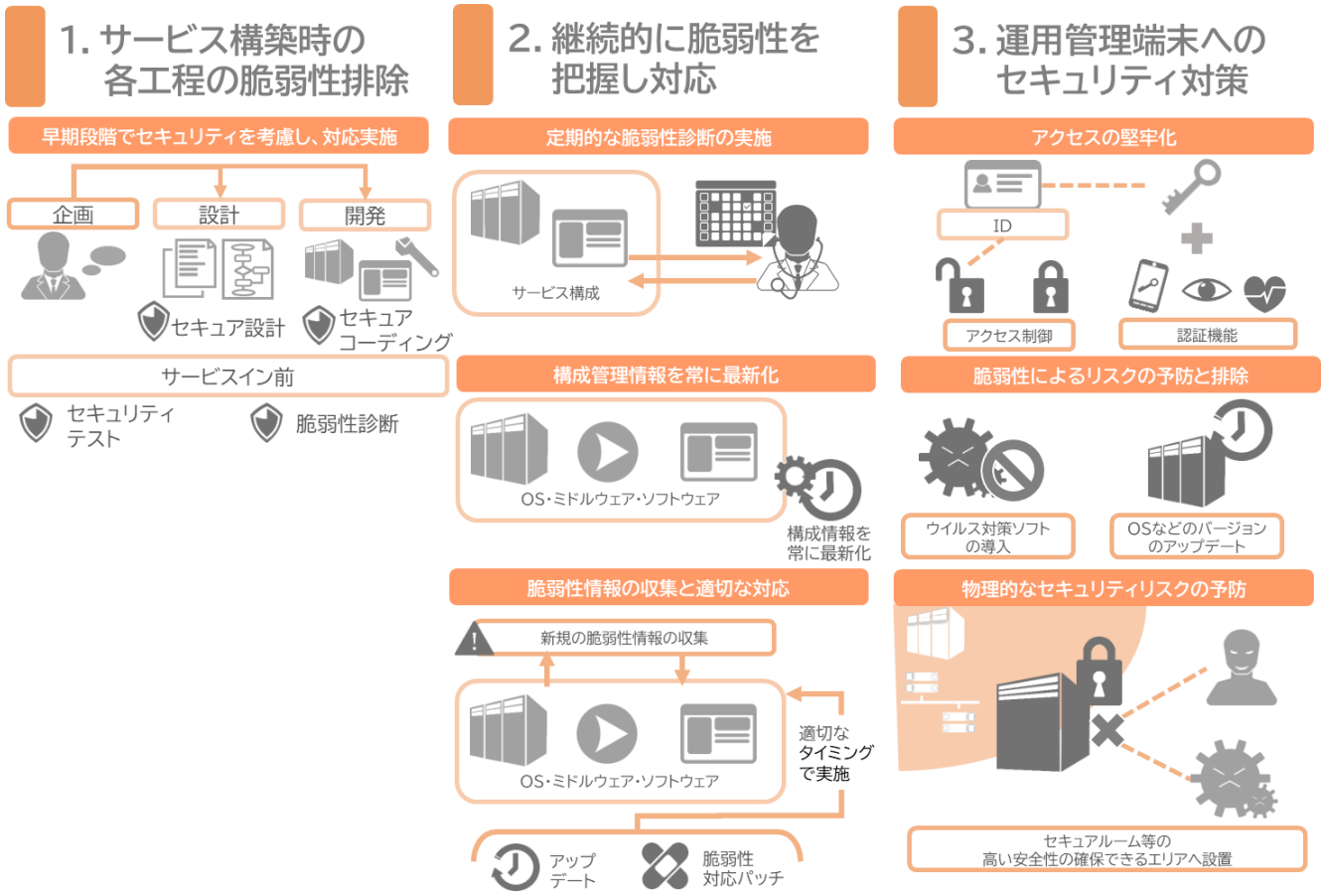


4. セキュリティ監視の実施



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。

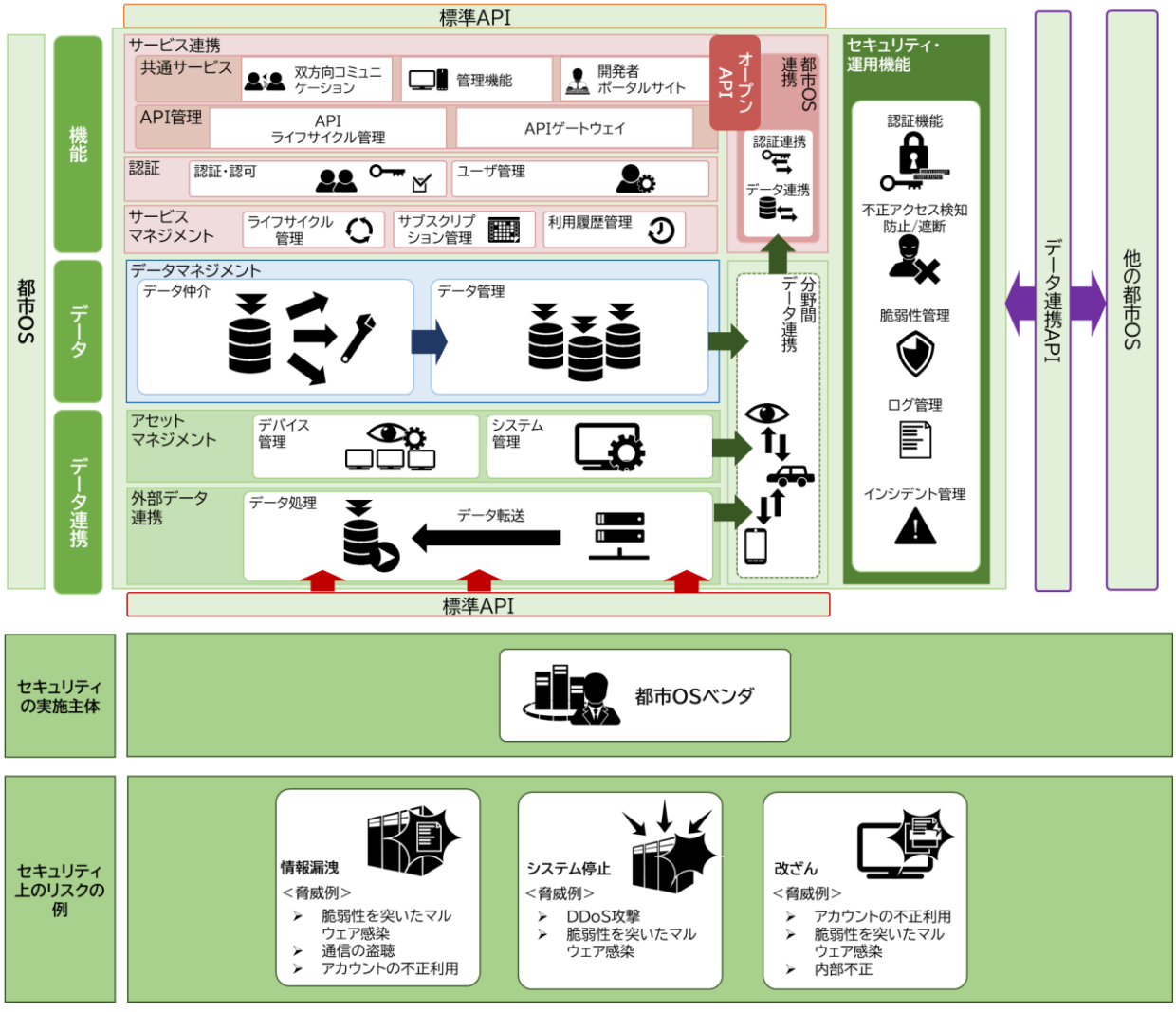
セキュアな都市OS（プラットフォーム）を準備しよう

「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。

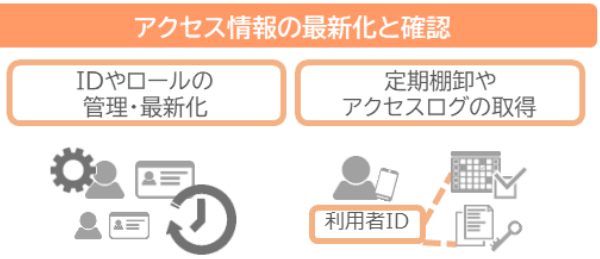
1. 都市OSへのアクセス制御の実装・運用

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

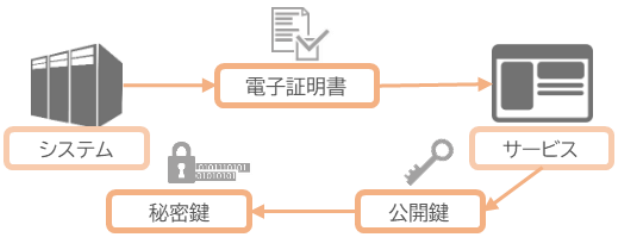
アクセス情報の最新化と確認



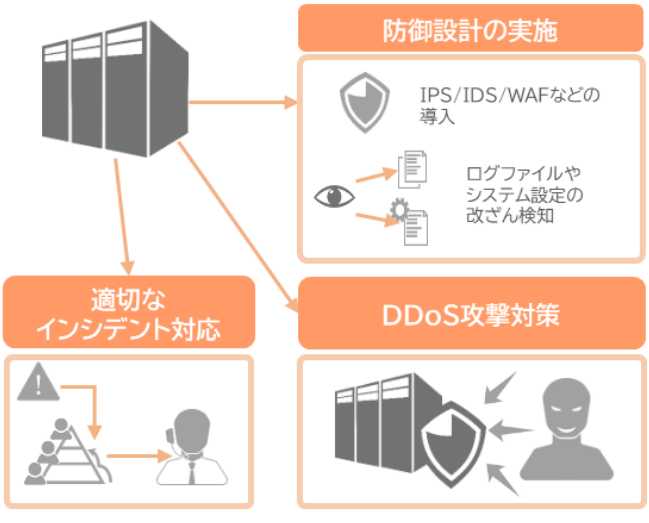
3. 認証機能の実装

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

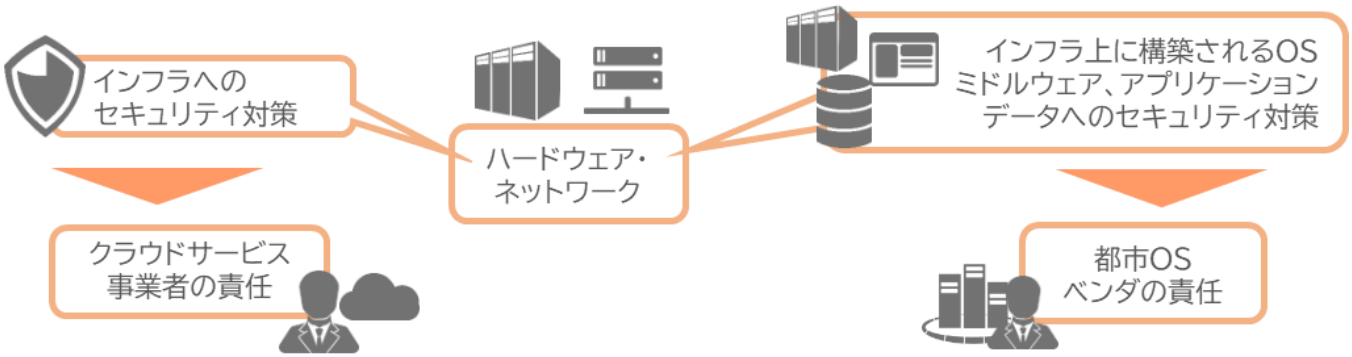
④推進主体からの要求に応じた適切なクラウドサービスの利用

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

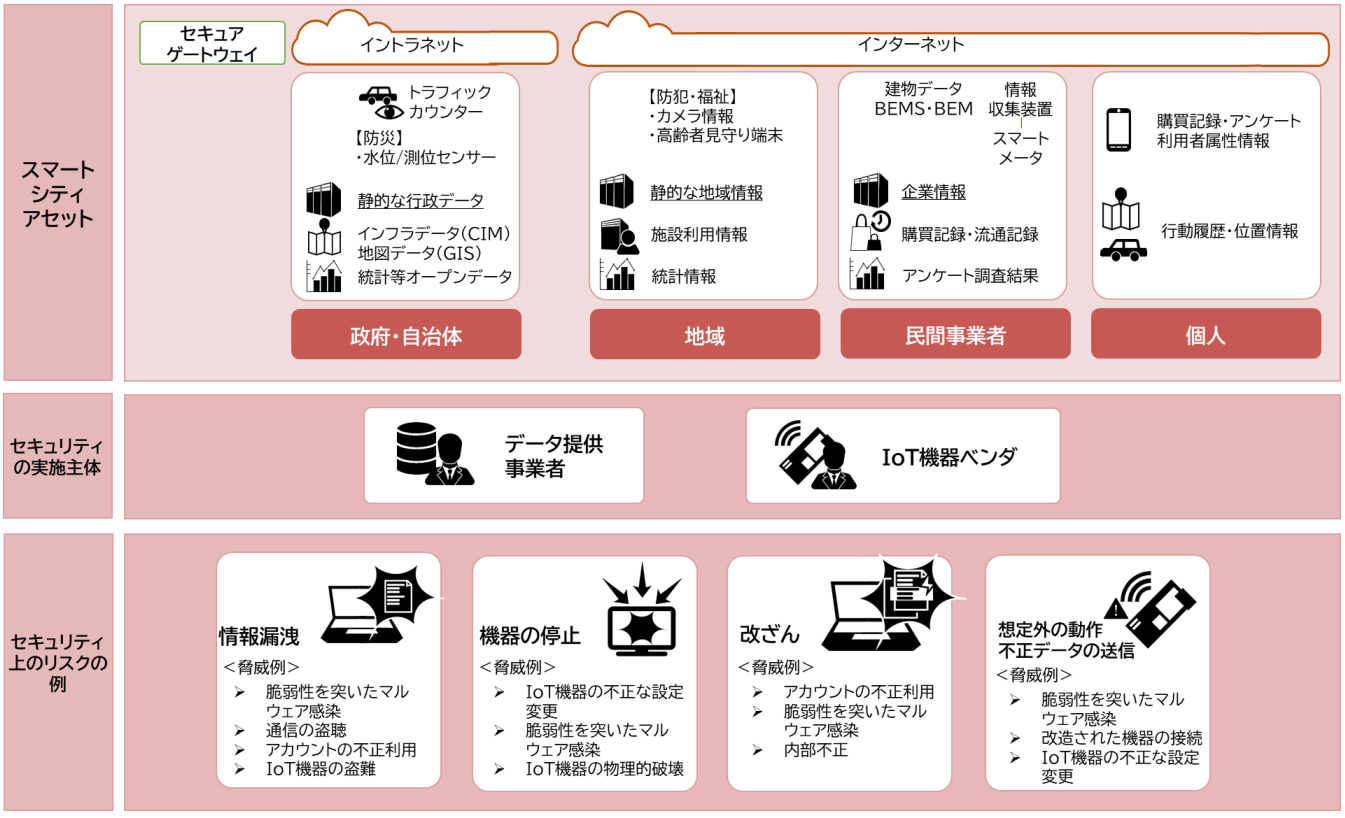
機器やデータを保護しよう

「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

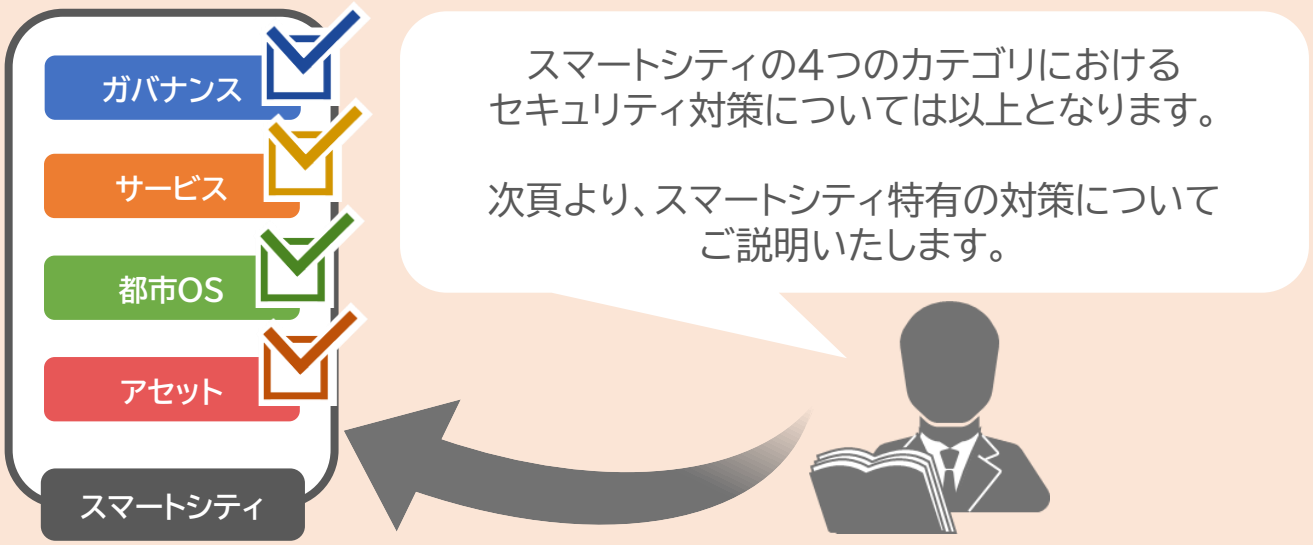
・アセットから都市OSへデータを送信する際の通信を暗号化しよう。
・アセットが保有するデータを暗号かしよう。

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。

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。

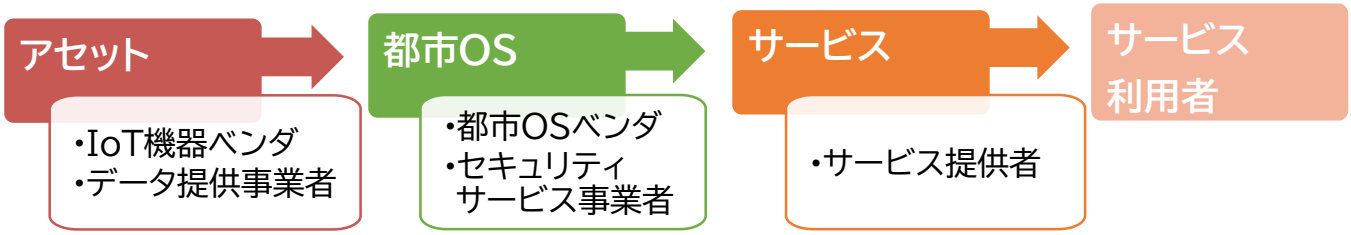


3 スマートシティ特有のセキュリティ対策

サプライチェーン全体を管理しよう

スマートシティ特有のサプライチェーン

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>推進主体</u>は
- 委託先に対して、委託事業におけるサプライチェーン・リスクに対応するための管理体制の整備を求める
- サプライチェーン・リスクのアセスメントを実施して、それぞれの工程で求められる対策を検討し、実施する

<u>委託先</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委託先のセキュリティ管理体制を評価する

委託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

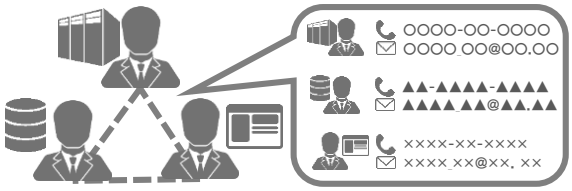
委託先・提携先側は

- 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

インシデント対応時の連携に向けた準備をしよう

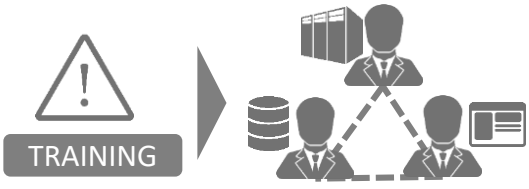
スマートシティ内でセキュリティインシデントが発生した際に、被害が拡大することを防ぐため、スマートシティに関与するマルチステークホルダが能動的に連携し、対応を図ることが重要です。

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を整備する



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

データ連携時のセキュリティを確保しよう

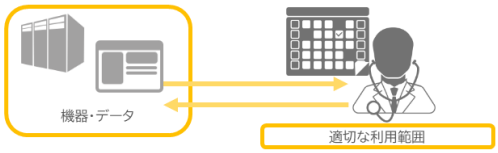
スマートシティのデータ連携においては、各事業者等におけるAPIを介してデータ連携が行われるが、適切でセキュアなデータ連携が行われるように、その認証・制御についてはデータ連携基盤で実施されることが多い。

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

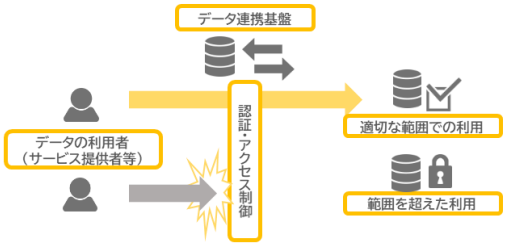
連携元・連携先組織でのセキュリティマネジメントを確認する

機器やサービスの信頼性を評価する



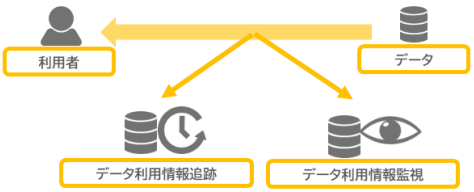
②データ提供事業者・サービス提供者等の認証と適切なアクセス制御

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



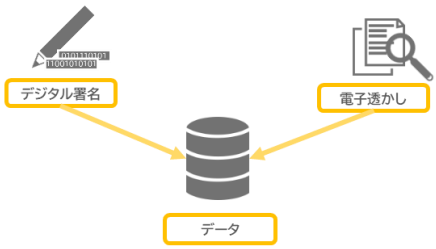
③データの追跡可能性を確保しデータ利用の透明性を担保する

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

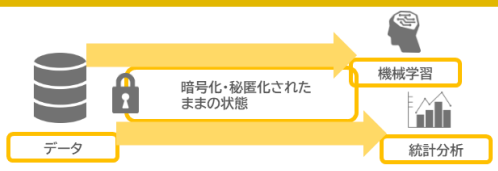
デジタル署名、電子透かしなどを活用し、データの原本性を確保する



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

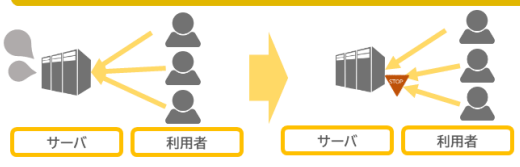
データに暗号化・秘匿化を施したまま利用を行う



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



4 事例紹介

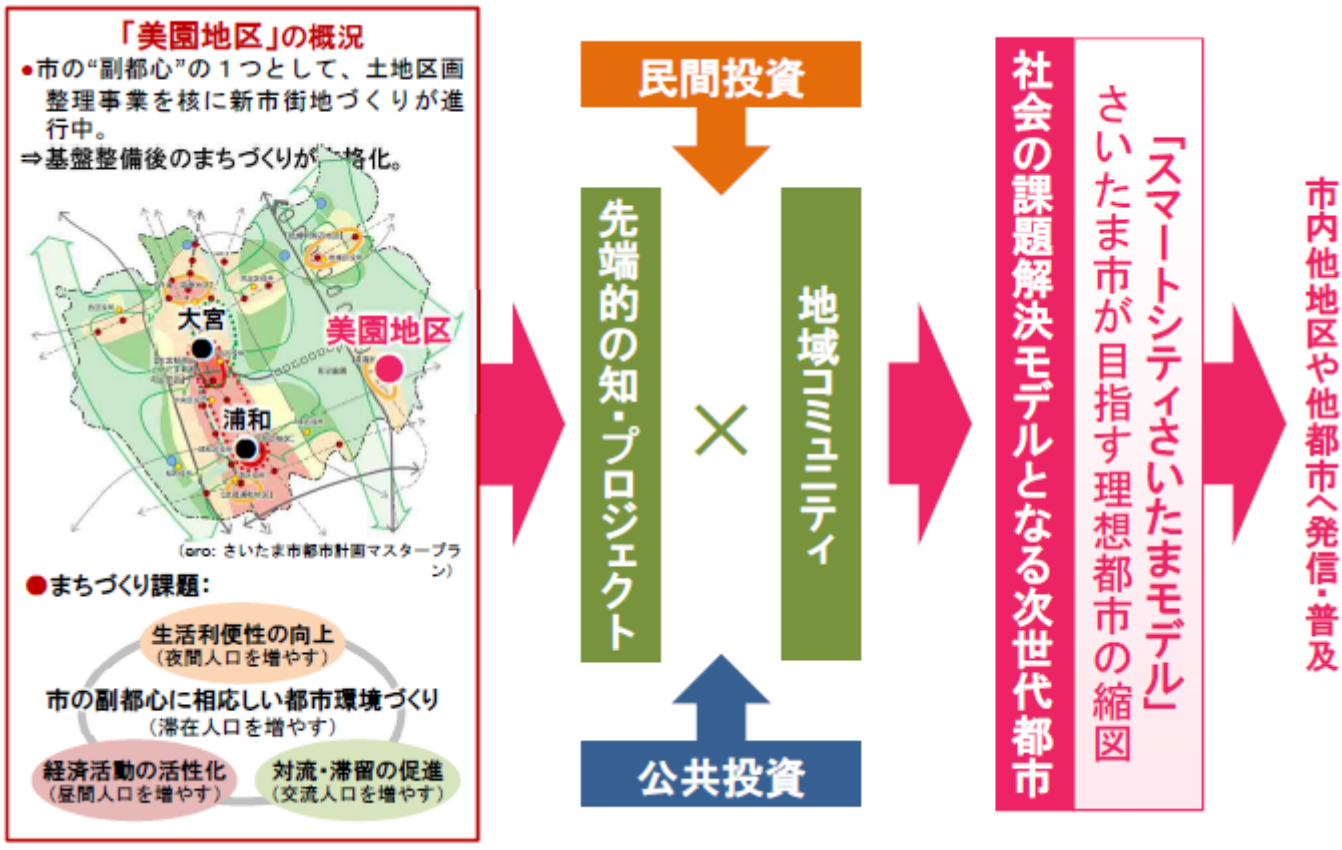
「公民＋学」連携により構成されたガバナンス ◎さいたま市

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。

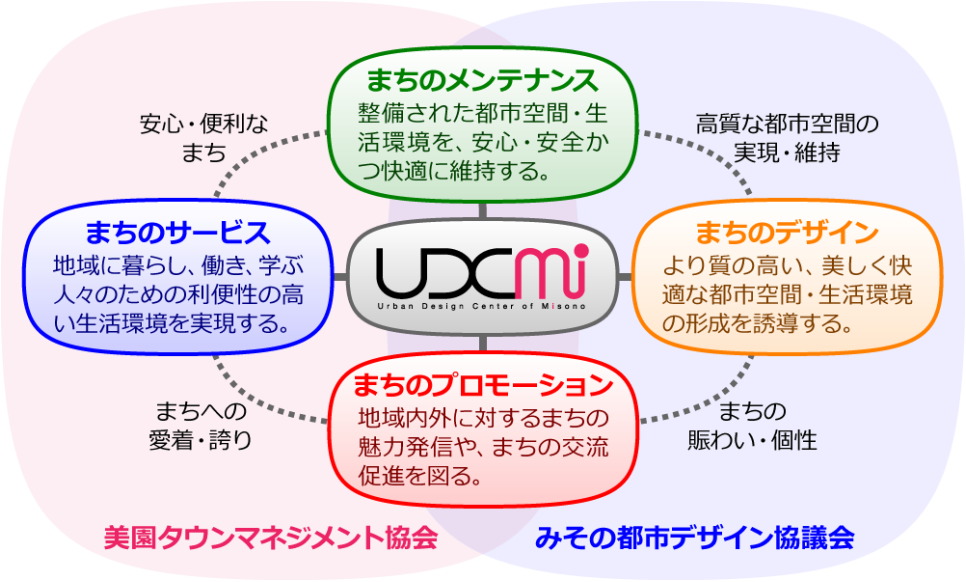
協会事務局である**（一社）美園タウンマネジメント**では**プライバシーマーク**を取得し、個人情報について適切な保護措置を講ずる体制を整備してます。さらに、昨今の情報銀行の動向注視しながら、データ取扱いに関するポリシーも議論が進んでいます 。

美園タウンマネジメント協会体制



事業内容

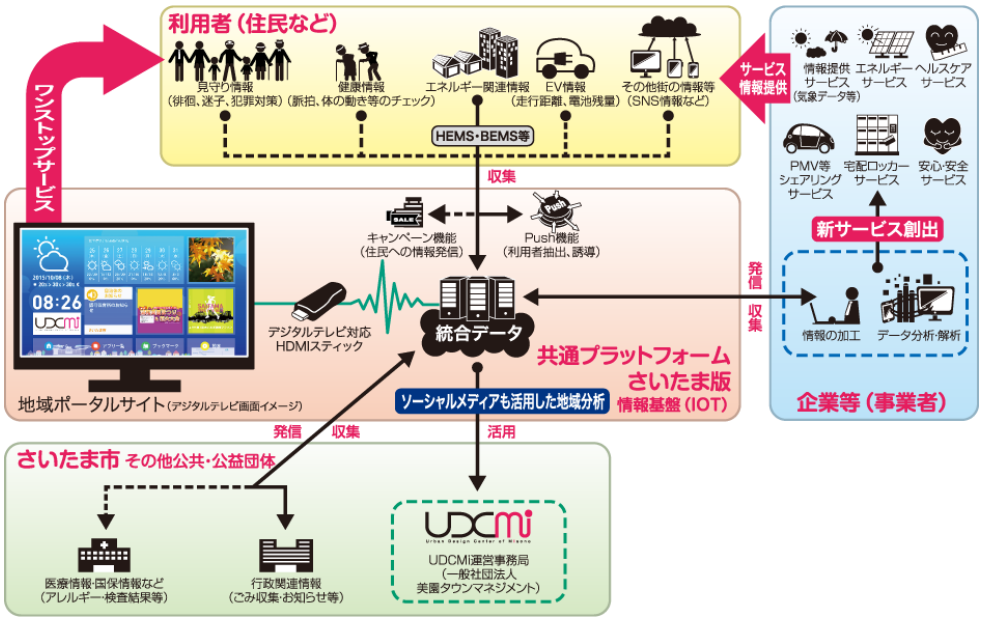
UDCMiという“場”を介して、「デザインマネジメント」・「メンテナンスマネジメント」・「サービスマネジメント」・「プロモーションマネジメント」の各分野に亘るプロジェクトの企画立案・試行的実践（社会実験）・まちへの実装化（事業化）等を促進させ、地区まちづくりに係る各者の連携・役割分担に基づく持続可能な地域マネジメント体制の構築を図っています。



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。

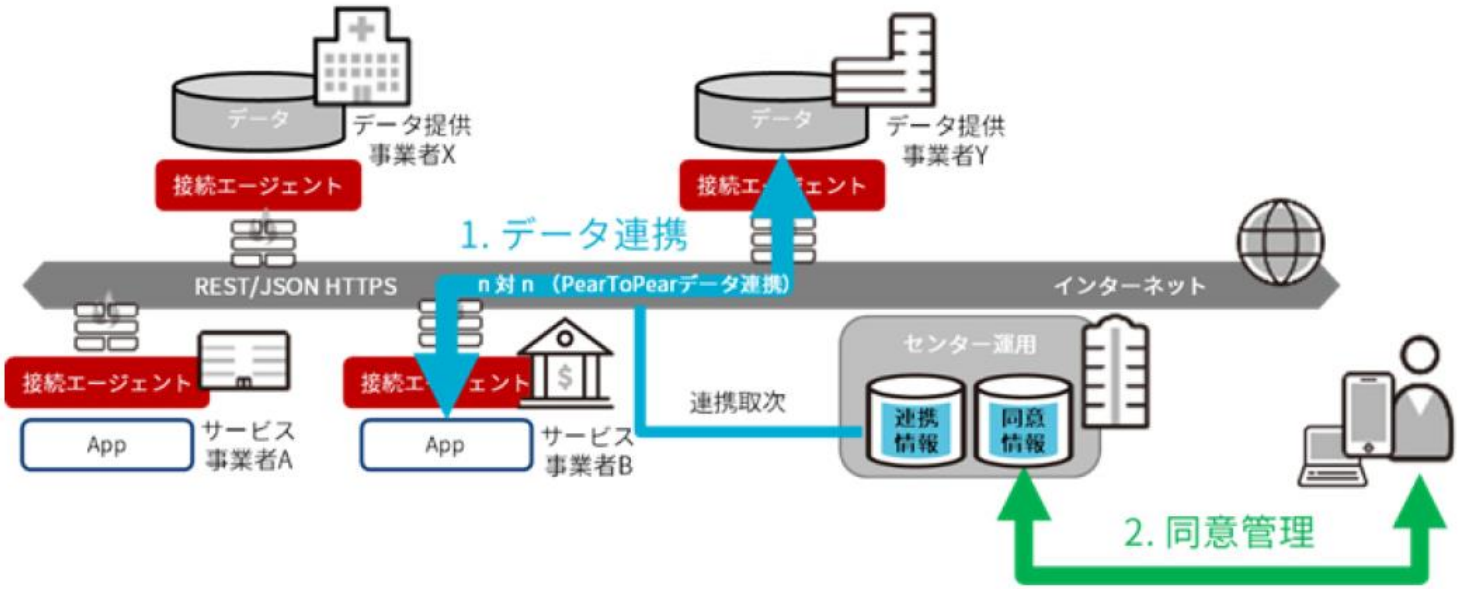


こうした社会情勢も踏まえ、個人のプライバシーを守ったデータの安心・安全な管理を研究してきた慶應義塾大学西宏章教授の協力のもと、2015年より「共通プラットフォームさいたま版」の開発を、美園タウンマネジメント協会の重点施策の1つとして進めてきました。

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、日本ユニシス株式会社は、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

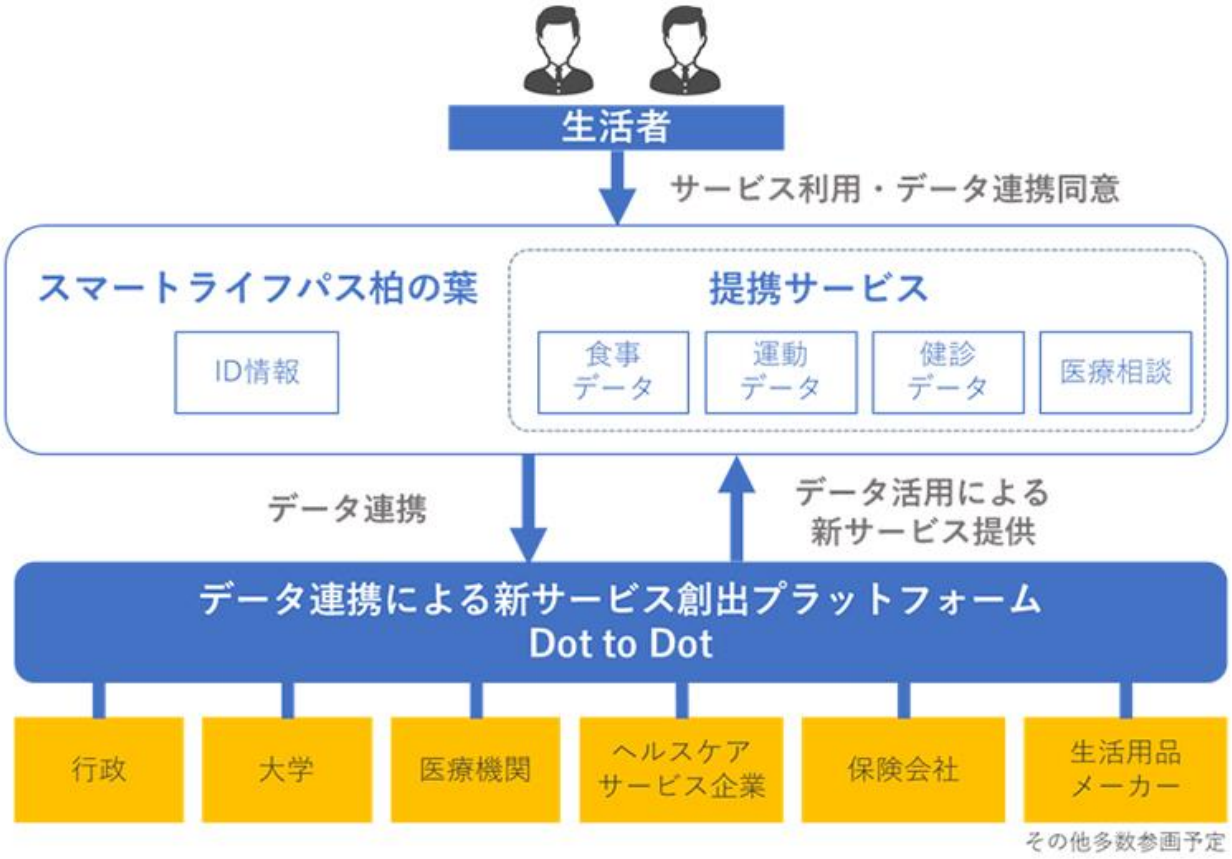


「Dot to Dot」は、生活者が所有するパーソナルデータの活用の意思決定権利は個人にあるという**「データの個人主権」**と、事業者が責任をもって自社サービスのデータ管理を行い、必要なときのみ他の事業者とデータを連携する**「分散型データ管理」**の2つの理念に基づき開発されたプラットフォームです。

■ **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柏の葉」



「スマートライフパス柏の葉」は、柏の葉の住民であればどなたでも登録できるポータルサイトです。登録すると、様々なヘルスケアサービスを利用することができます。
　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柏の葉」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。
　「スマートライフパス柏の葉」では、今後もサービス連携する企業を増やしていきながら、生活者の生活利便性の向上を目指していきます。