CSA Japan Summit 2021

～大阪・関西万博に向けたスマートシティIT基盤や運用について考える～

CCDS ストラテジックアドバイザー
　スマートシティWG（旧：Trusted Data連携WG）　主査
株式会社OZ1 代表取締役
大阪府 スマートシティ戦略 スーパーアドバイザー
エストニア日本商工会議所 理事

江川　将偉

「2020年活動状況」

～より良いガイドライン整備に向けて～

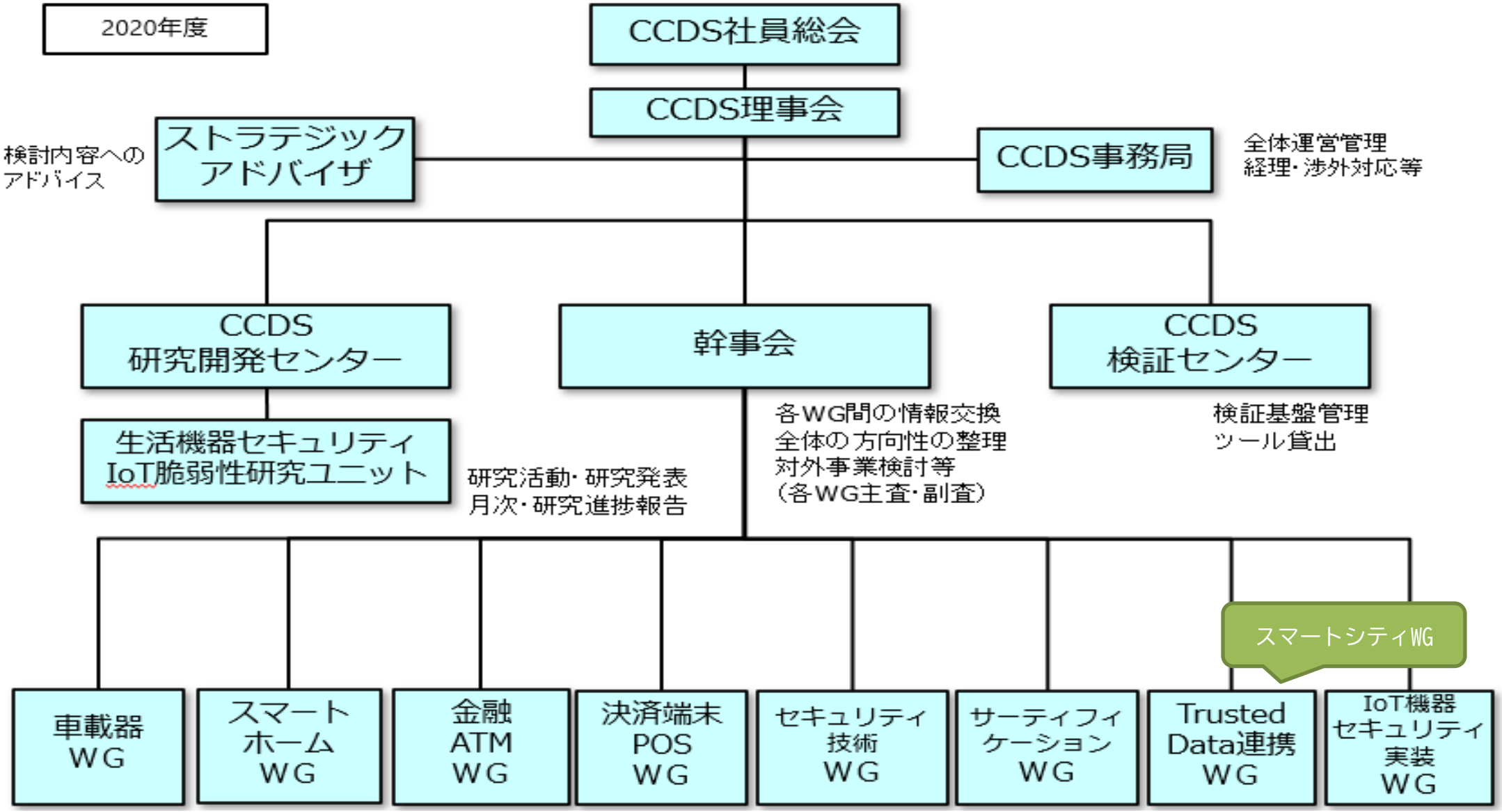
CCDSの概要

- 名称：一般社団法人 重要生活機器連携セキュリティ協議会
  - 英名：Connected Consumer Device Security council (CCDS)
- 設立：2014年10月6日
- 会長：徳田英幸（情報通信研究機構　理事長、慶応大学 名誉教授）
- 代表理事：荻野 司（情報セキュリティ大学院大学　客員教授）
- 理事：後藤厚宏（情報セキュリティ大学院大学 学長、SIP：PD）
  松本 勉（横浜国立大学先端科学高等研究院 教授）

- 会員数：216（正会員以上：61、一般会員：120、学術系：18、協賛:17）(2020年11月)

- 主な事業：
  1. 生活機器の各分野におけるセキュリティに関する国内外の動向調査、内外諸団体との交流・協力
  2. 生活機器の安全と安心を両立するセキュリティ技術の開発
  3. セキュリティ設計プロセスの開発や検証方法のガイドラインの開発、策定および国際標準化の推進
  4. 生活機器の検証環境の整備・運用管理及び検証事業、セキュリティに関する人材育成や広報・普及啓発活動等

協議会組織



IoTセキュリティを取り巻く各国の動向

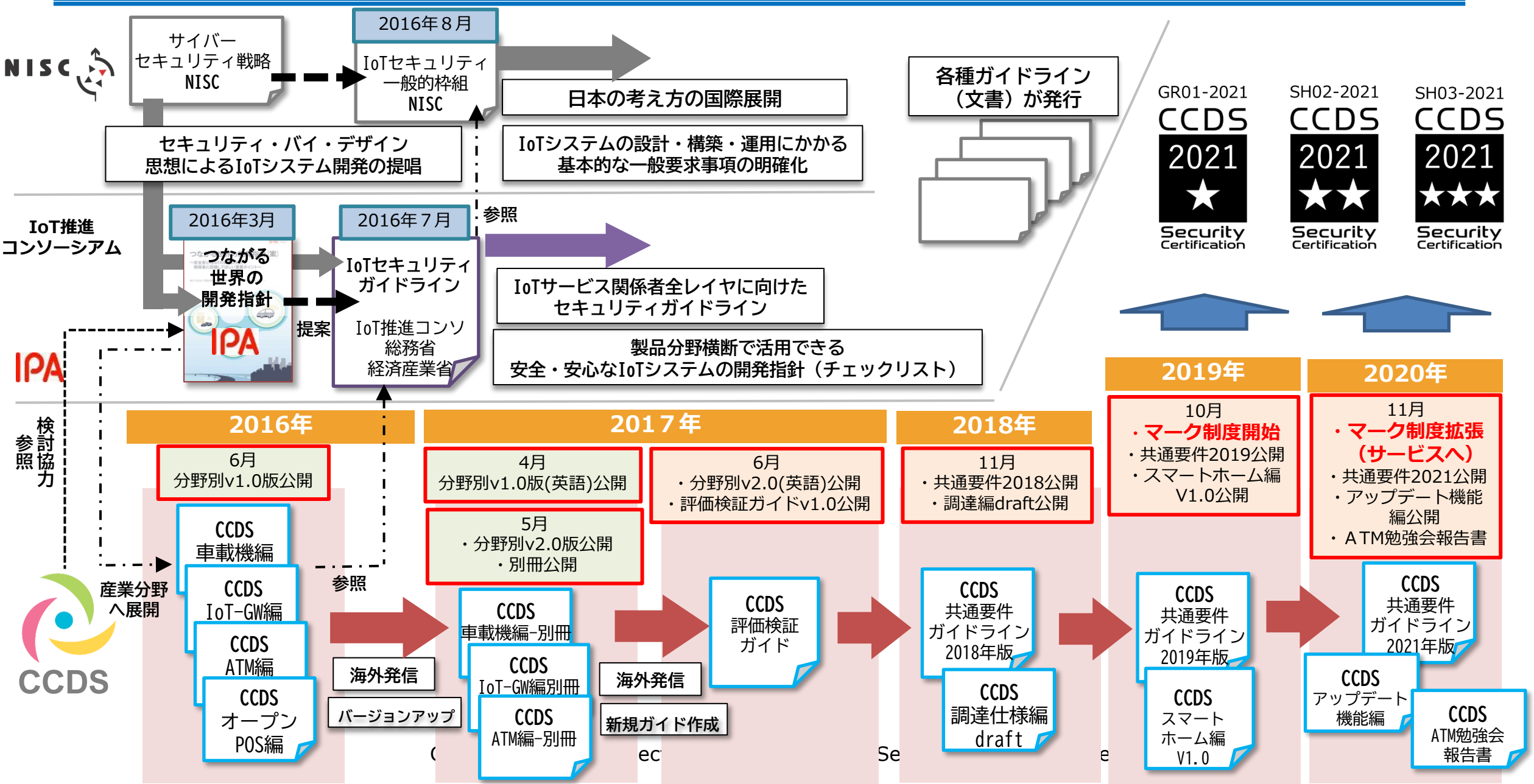
ガイドライン提案加速

法規制に向けて

	2014年	2015年	2016年	2017年	2018年	2019年	2020年
日本	11月 **サイバーセキュリティ基本法** サイバーセキュリティを推進するための基本理念や国の責務等を定めた情報セキュリティ戦略の基盤となる法律	12月 **サイバーセキュリティ経営ガイドライン** 企業経営者を対象に対策を推進するためのリーダーシップのとりかたについてガイドラインを策定	7月 **IoTセキュリティガイドライン** IoTセキュリティに関する指針と一般利用者のためのルールを策定	5月 **改正個人情報保護法施行** 個人情報の取扱いに関するルールが10年ぶりに改正され施行された 5月 **医療情報システムの安全管理に関するガイドライン第5版** 医療機関等を対象とするサイバー攻撃やIoT等の新技術への対応として改定	6月 **技適にセキュリティ要件追加提案** マルウェアの感染によりIoT機器がボットネット化しないための要件を追加 11月 **技適へのセキュリティ要件追加パブコメ**		4月 **技術適合要件施行**
米国	2月 **サイバーセキュリティフレームワーク公表** NISTがサーバーセキュリティ対策の全体像を示すフレームワークを公表			8月 **IoT Cybersecurity Act 2017法案提出** IoT製品の政府調達条件を規定 12月 **改訂版**	2月 **NISTIR8200 (Draft)公表** 5つのユースケースに対するIoTサイバーセキュリティの目的、リスク、脅威の分析、国際標準化状況を整理した 8月-2019年4月 **サイバー・フィジカル・セキュリティ対策フレームワークを策定** 9月 **米国加州でIoTセキュリティ法成立**	3月 **IoT Cybersecurity Improvement Act 2019法案提出**	3末 **連邦政府調達に適切な管理推奨事項を明確化(NIST)** NISTIR 8259DRAFT 1月 **加州SB327施行**
EU				9月 **サイバーセキュリティ認証フレームワーク導入検討を公表** 11月 **ENISAがIoTのベースラインセキュリティ推奨事項を発表**	5月 **EU一般データ保護規則(GDPR)施行** EU加盟28カ国およびアイスランド、リヒテンシュタイン、ノルウェー）の個人データ保護を目的とした管理規則 10月 **英政府コンシューマIoT向けセキュリティ行動規範13箇条**	2018/5-2019/2 **ETSI TS 103 645 Cyber Security for Consumer IoT**	

近年、IoTセキュリティに関連する法規制、ガイドラインなどが各国から出されており、これらへ対応していかないとビジネスに影響を及ぼしつつある。

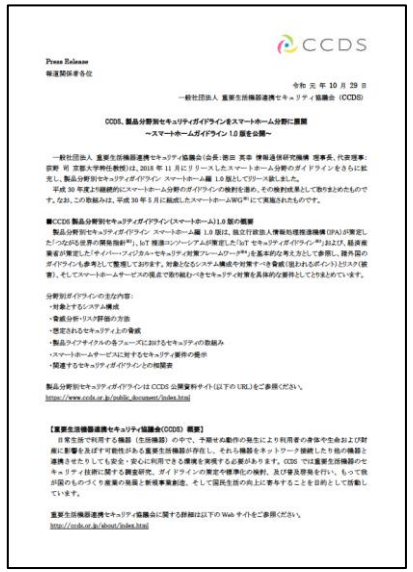
CCDS　IoTセキュリティガイドライン整備状況



この1年間で発行した報告書・ガイドライン

- 「IoT 機器セキュリティ実装ガイドライン～ソフトウェア更新機能～第 1.0 版」
- 「IoT 分野共通セキュリティ要件ガイドライン 2021 年版」
- 「自動預け払い機関連システムにおける物理・サイバー攻撃の対策検討ポイント 」
- 「IoT 分野共通セキュリティ要件ガイドライン2019 年度版11 要件における解説編」
- 「スマートホームガイドライン 1.0 版」

CCDS　幹事会員・正会員により積極的に活動を実施しています。



Press Release
報道関係者各位

令和 元 年 10 月 29 日
一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）

CCDS、製品分野別セキュリティガイドラインをスマートホーム分野に展開
～スマートホームガイドライン 1.0 版を公開～

一般社団法人 重要生活機器連携セキュリティ協議会（会長：渋谷 英幸 情報通信研究機構 理事長、代表理事：萩野 司 京都大学特任教授）は、2018 年 11 月にリリースしたスマートホーム分野のガイドラインをさらに拡充し、製品分野別セキュリティガイドライン スマートホーム編 1.0 版としてリリース致しました。

平成 30 年度より継続的にスマートホーム分野のガイドラインの検討を進め、その検討成果としてお届けしたものです。なお、この取組みは、平成 30 年 5 月に組織したスマートホームWG[※1] にて実施されたものです。

■CCDS 製品分野別セキュリティガイドライン（スマートホーム）1.0 版の概要

製品分野別セキュリティガイドライン スマートホーム編 1.0 版は、独立行政法人 情報処理推進機構（IPA）が策定した「つながる世界の開発指針[※2]」、IoT 推進コンソーシアムが策定した「IoT セキュリティガイドライン[※3]」および、経済産業省が策定した「サイバー・フィジカル・セキュリティ対策フレームワーク[※4]」を基本的な考え方として参照し、諸外国のガイドラインも参考にして整理しております。対象となるシステム構成や対策すべき脅威（狙われるポイント）とリスク（被害）、そしてスマートホームサービスの視点で取り組むべきセキュリティ対策を具体的な要件として作成しています。

分野別ガイドラインの主な内容：
・対象とするシステム構成
・脅威分析・リスク評価の方法
・想定されるセキュリティ上の脅威
・製品ライフサイクルの各フェーズにおけるセキュリティの取組み
・スマートホームサービスに対するセキュリティ要件の提示
・関連するセキュリティガイドラインとの関係表

製品分野別セキュリティガイドラインは CCDS 公開資料サイト（以下の URL）をご参照ください。
https://www.ccds.or.jp/public_document/index.html

【重要生活機器連携セキュリティ協議会(CCDS) 概要】
日常生活で利用する機器（生活機器）の中で、予期せぬ動作の発生により利用者の身体や生命および財産に影響を及ぼす可能性がある重要生活機器が存在し、それら機器をネットワーク接続したり他の機器と連携させたりしても安全・安心に利用できる環境を実現する必要があります。CCDS では重要生活機器のセキュリティ技術に関する調査研究、ガイドラインの策定を標準化の検討、及び普及啓発を行い、もって我が国のものづくり産業の発展と新規事業創造、そして国民生活の向上に寄与することを目的として活動しています。

重要生活機器連携セキュリティ協議会に関する詳細は以下の Web サイトをご参照ください。
https://ccds.or.jp/about/index.html

IoT 分野共通セキュリティ要件ガイドライン 2019 年度版

11 要件における解説編

生活機器を安全に利用できる社会の実現を目指して。

令和 2 年 10 月 16 日
一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）

「自動預け払い機関連システムにおける物理・サイバー攻撃の対策検討ポイント」の
金融関係者向け提言

一般社団法人 重要生活機器連携セキュリティ協議会（CCDS、会長：渋谷 英幸 情報通信研究機構 理事長、代表理事：萩野 司 情報セキュリティ大学院大学特任教授）は、2019 年 8 月から 2020 年 10 月に掛けて、「金融サービス浮上を持つ ATM 攻撃リスク勉強会」を開催いたしました。この度、議論の成果を「自動預け払い機関連システムにおける物理・サイバー攻撃の対策検討ポイント」として文書にまとめ、金融機関等ほにめとする金融関係者に成果文書を開示いたします。

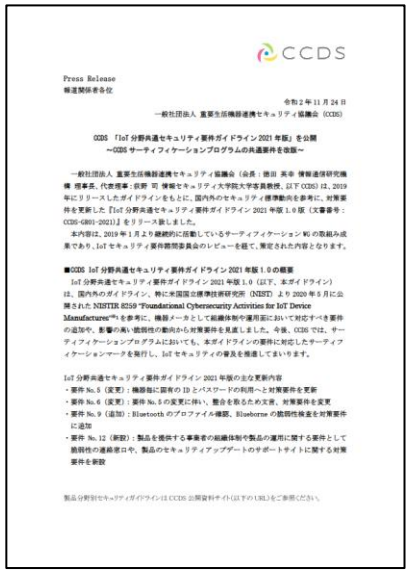
無人店舗を含む金融機関店舗や店舗外 ATM 等では、特定の条件が揃ったときに、外部からの物理的接触を通じた設定系システムへの侵入と、サイバー攻撃の可能性が指摘されています。海外では脆弱なシステムの中間サーバを狙い取られ、13 億円以上の被害を出した ATM 不正出金事例があり、国内でも同様なリスク対策を考慮する必要があります。

そこで、そのリスクと対策ポイントを議論すべく、関係有識者にご参加いただき、上記の勉強会を開催いたしました。ご参加いただいた関係有識者として、金融業界団体、大手銀行、地方銀行、システム情報会社、機器提供ベンダ、セキュリティベンダ、学術関係者の他、オブザーバとして行政機関の方にもご参加いただきました。

成果文書では、中小金融機関の導入しやすさも配慮した、想定セキュリティ対策ポイントをまとめています。対象システムは、金融機関店舗や店舗外の自動預け払い機(ATM)含む無人端末、無人端末が接続されるサーバ、端末とサーバをつなぐネットワーク機器からなる無人端末システムです。

中小金融機関でも活用しやすいよう、対策立案に向けた分析や評価の手順及び、推奨対策例を紹介しています。また、金融機関、システム情報ベンダ、機器提供ベンダが、推奨対策例を更に理解しやすいよう、対策実装具体例とその達成基準例をチェックリスト形式で表現した別紙を、CCDS 金融 ATM WG より個別に提供する予定です。

お問い合わせ：一般社団法人 重要生活機器連携セキュリティ協議会　金融 ATM WG
主査　緒方 日佐男
〒141-0021 東京都品川区上大崎２－１２－１ 野田ビル 3F
TEL：03-6455-7193　E-MAIL: ccds-sec@ccds.or.jp



Press Release
報道関係者各位

令和 2 年 11 月 24 日
一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）

CCDS「IoT 分野共通セキュリティ要件ガイドライン 2021 年版」を公開
～CCDS サーティフィケーションプログラムの共通要件を改版～

一般社団法人 重要生活機器連携セキュリティ協議会（会長：渋谷 英幸 情報通信研究機構 理事長、代表理事：萩野 司 情報セキュリティ大学院大学客員教授、以下 CCDS）は、2019 年に リリースしたガイドラインをもとに、国内外のセキュリティ標準動向を参考に、対策要件を更新した「IoT 分野共通セキュリティ要件ガイドライン 2021 年版（文書番号：CCDS-GR01-2021）」をリリース致しました。

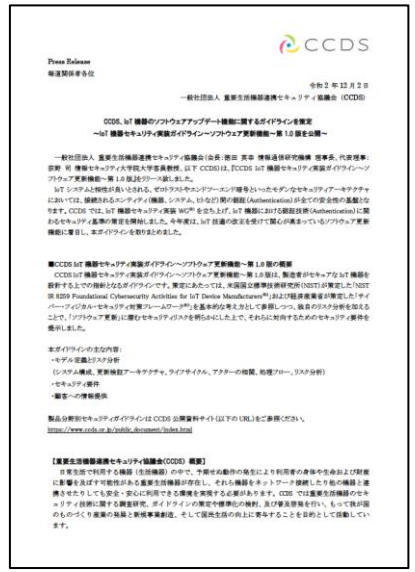
本内容は、2019 年 1 月より継続的に活動しているサーティフィケーション WG の取組み成果であり、IoT セキュリティ要件開発委員会のレビューを経て、策定された内容となります。

■CCDS IoT 分野共通セキュリティ要件ガイドライン 2021 年版 1.0 の概要

IoT 分野共通セキュリティ要件ガイドライン 2021 年版 1.0（以下、本ガイドライン）は、国内外のガイドライン、特に米国国立標準技術研究所（NIST）より 2020 年 5 月に公開された NISTIR 8259 "Foundational Cybersecurity Activities for IoT Device Manufacturers"[※1] を参考に、機器メーカとして組織体制や運用面において対応すべき要件の追加や、影響の高い脆弱性の動向から対策要件を見直しました。今後、CCDS では、サーティフィケーションプログラムにおいても、本ガイドラインの要件に対応したサーティフィケーションマークを発行し、IoT セキュリティの普及を推進してまいります。

IoT 分野共通セキュリティ要件ガイドライン 2021 年版の主な更新内容
・要件 No.5（変更）：機器毎に固有の ID とパスワードの利用へと対策要件を更新
・要件 No.6（変更）：要件 No.5 の変更に伴い、整合を取るため文言、対策要件を変更
・要件 No.9（追加）：Bluetooth のプロファイル機能、Blueborne の脆弱性検査を対策要件に追加
・要件 No.12（新設）：製品を提供する事業者の組織体制や製品の運用に関する要件として脆弱性の連絡窓口や、製品のセキュリティアップデートのサポートサイトに関する対策要件を新設

製品分野別セキュリティガイドラインは CCDS 公開資料サイト（以下の URL）をご参照ください。



Press Release
報道関係者各位

令和 2 年 12 月 2 日
一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）

CCDS、IoT 機器のソフトウェアアップデート機能に関するガイドラインを策定
～IoT 機器セキュリティ実装ガイドライン～ソフトウェア更新機能～第 1.0 版を公開～

一般社団法人 重要生活機器連携セキュリティ協議会（会長：渋谷 英幸 情報通信研究機構 理事長、代表理事：萩野 司 情報セキュリティ大学院大学客員教授、以下 CCDS）は、「CCDS IoT 機器セキュリティ実装ガイドライン～ソフトウェア更新機能～第 1.0 版」をリリース致しました。

IoT システムと相性が良いとされる、ゼロトラストやエンドツーエンド暗号といったモダンなセキュリティ・アーキテクチャにおいては、接続されるエンティティ（機器、システム、ひと）間の相互（Authentication）が全ての安全性の基盤となります。CCDS では、IoT 機器セキュリティ実装 WG[※] を立ち上げ、IoT 機器における相互認証（Authentication）に関わるセキュリティ基準の策定を開始しました。今年度は、IoT 技術の変化を受けて開心が高まっているソフトウェア更新機能に着目し、本ガイドラインを取りまとめました。

■CCDS IoT 機器セキュリティ実装ガイドライン～ソフトウェア更新機能～第 1.0 版の概要

CCDS IoT 機器セキュリティ実装ガイドライン～ソフトウェア更新機能～第 1.0 版は、製造者がセキュアな IoT 機器を設計するとての指針となるガイドラインです。策定にあたっては、米国国立標準技術研究所（NIST）が策定した「NIST IR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers[※1]」および経済産業省が策定した「サイバー・フィジカル・セキュリティ対策フレームワーク[※2]」を基本的な考え方として参照しつつ、独自のリスク分析を加えることで、「ソフトウェア更新」に潜むセキュリティリスクを明らかにした上で、それらに対向するためのセキュリティ要件を提示しました。

本ガイドラインの主な内容：
・モデル定義とリスク分析
（システム構成、更新機能アーキテクチャ、ライフサイクル、アクターの相関、処理フロー、リスク分析）
・セキュリティ要件
・留意への情報提供

製品分野別セキュリティガイドラインは CCDS 公開資料サイト（以下の URL）をご参照ください。
https://www.ccds.or.jp/public_document/index.html

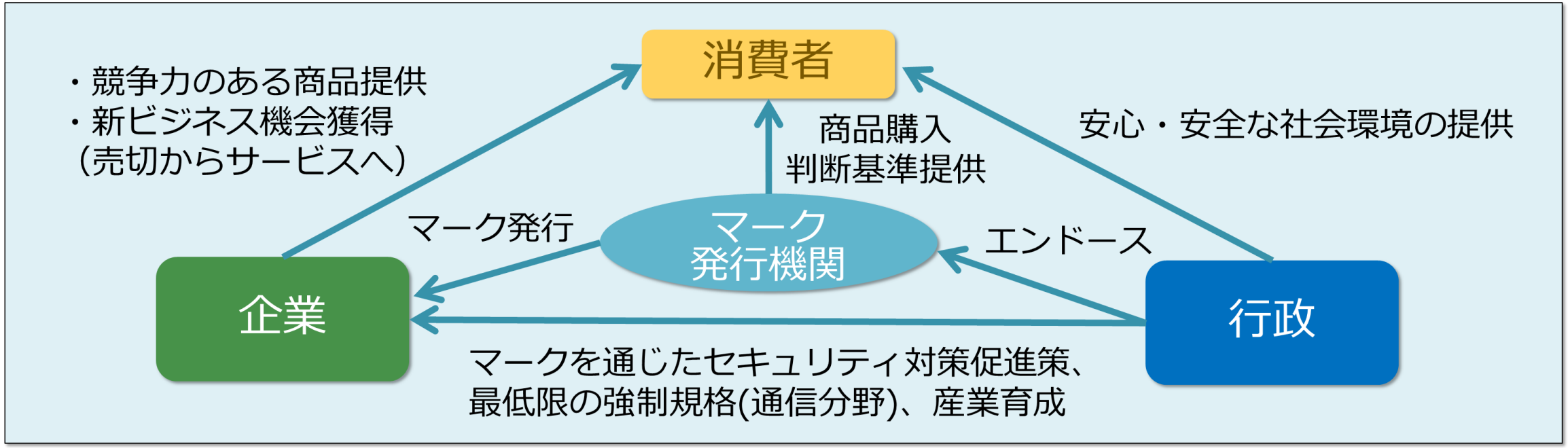
【重要生活機器連携セキュリティ協議会(CCDS) 概要】
日常生活で利用する機器（生活機器）の中で、予期せぬ動作の発生により利用者の身体や生命および財産に影響を及ぼす可能性がある重要生活機器が存在し、それら機器をネットワーク接続したり他の機器と連携させたりしても安全・安心に利用できる環境を実現する必要があります。CCDS では重要生活機器のセキュリティ技術に関する調査研究、ガイドラインの策定や標準化の検討、及び普及啓発を行い、もって我が国のものづくり産業の発展と新規事業創造、そして国民生活の向上に寄与することを目的として活動しています。

サーティフィケーションプログラム

一般社団法人
重要生活機器連携セキュリティ協議会
Connected Consumer Device Security Council （CCDS）

サーティフィケーションプログラム

CCDSサーティフィケーションのスキーム



ポイント

1.任意マーク（罰則なし）
2.自主評価と第三者評価のいずれか選択可能
3.第三者機関によるマーク付与の意味（検証結果保持と追跡可能）
4.マークの毎年更新（新規攻撃への対応）
5.セキュリティ対策の普及促進策　⇒例えば、税制優遇、助成金

IoTサイバー保険　　IoT機器＋IoTサービスを対応

ＣＣＤＳは、三井住友海上火災保険株式会社、損害保険ジャパン日本興亜株式会社、東京海上日動火災保険と連携し国内初となる「ＩｏＴ機器保険付認証制度」を構築。ＣＣＤＳがマーク付与した製品に対してサイバー保険を自動付帯します。

安心・安全なIoT機器を選択するための指標

マークによって、分野を問わず最低限守るべき要件を満たしていることが確認できるため、ユーザーがIoT機器を購入する際に選択の指標となります。

フォレンジック調査等、様々な費用・損害を保険で補償します。

原因調査

インシデントの発生またはそのおそれがある場合、迅速に調査を実施します。

その他費用損害

損害拡大防止・再発防止費用等、インシデントに起因する費用を幅広く補償します。

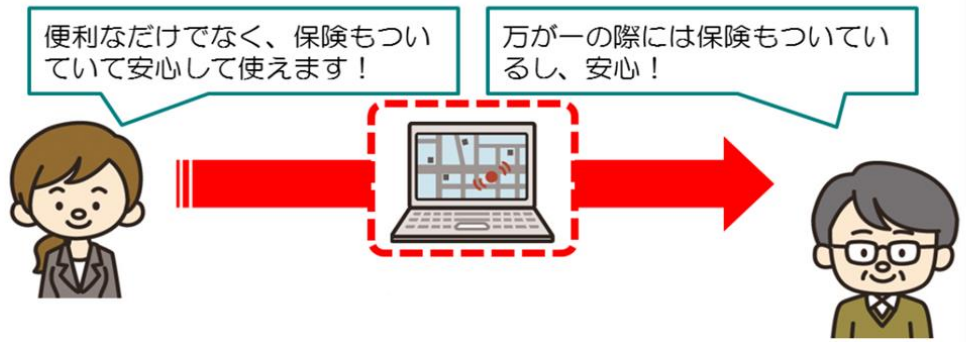
損害賠償金

メーカーに過失が発生する場合、賠償金をお支払いいたします。

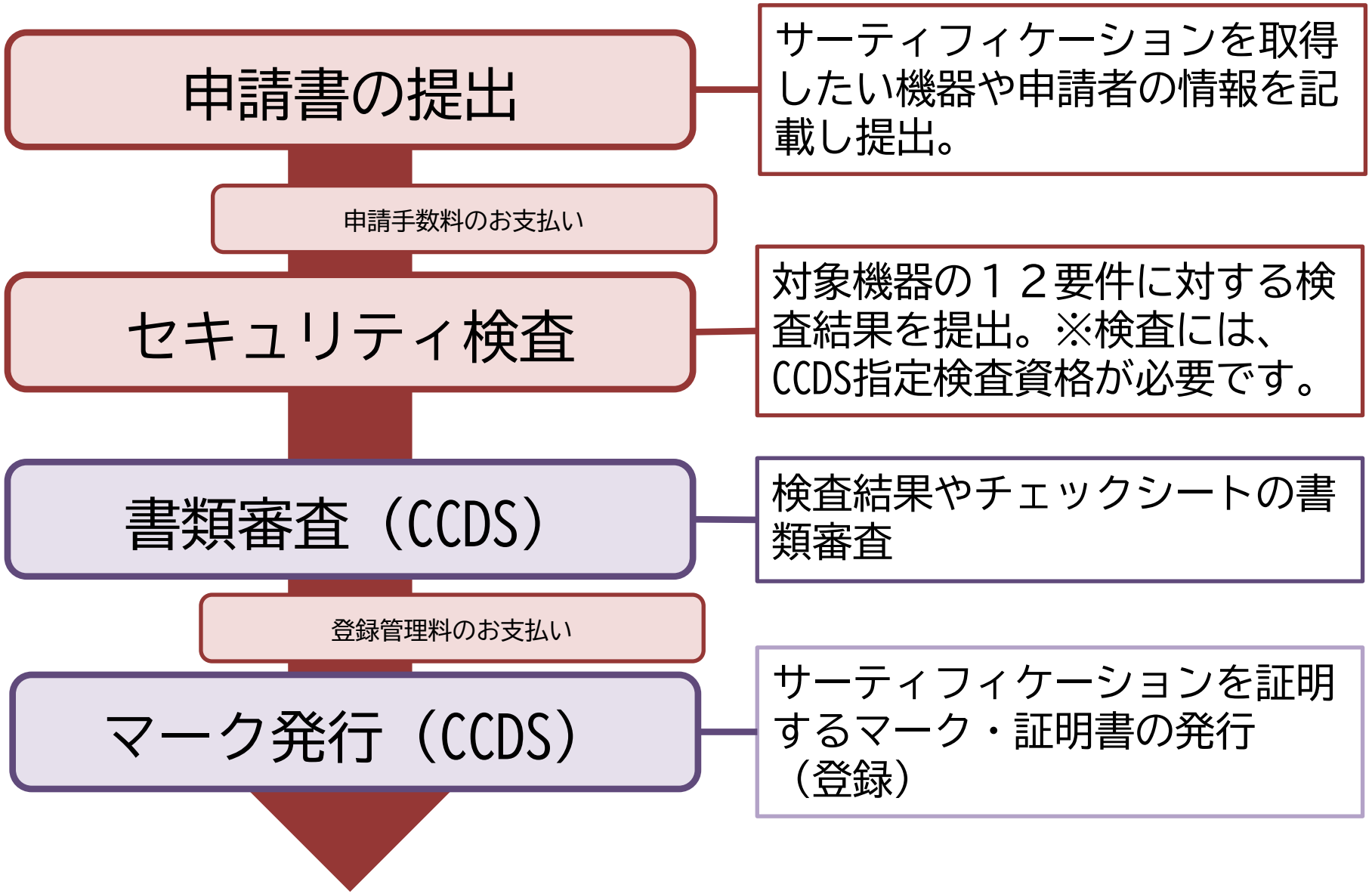
＋

事故時専門業者紹介サービス

サイバーセキュリティに関する事故が発生した際、CCDS・三井住友海上が迅速に専門業者を紹介いたします。



サーティフィケーションの申請方法

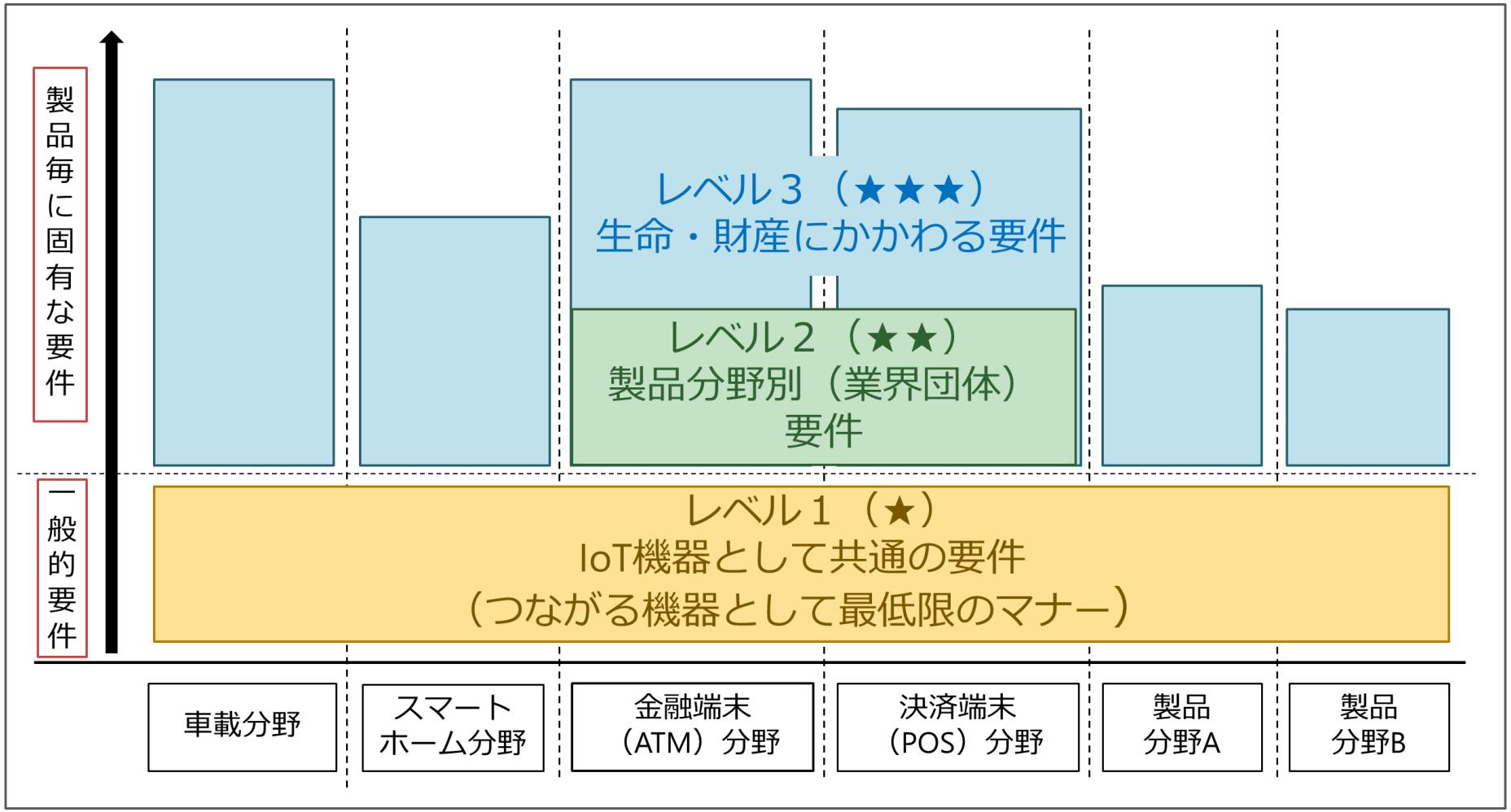


サーティフィケーションプログラム

サーティフィケーションプログラムのレベル構成

・消費者にも分かりやすいよう、★の数でセキュリティ対策のレベルを示す３階層のモデルを提示

・まずはレベル１の共通要件から、サーティフィケーションプログラムをスタートします



IoT機器が共通して守るべき、11のセキュリティ要件を定義（ミニマムな要求事項）2021年要件確定　12要件へ拡充

CCDS

① 管理画面からの侵入脅威を排除
② ID,PWを強化（一意、再設定）
③ 未使用ポートからの侵入を排除
④ アタックサーフェース
Wifi,Bluetooth,USB

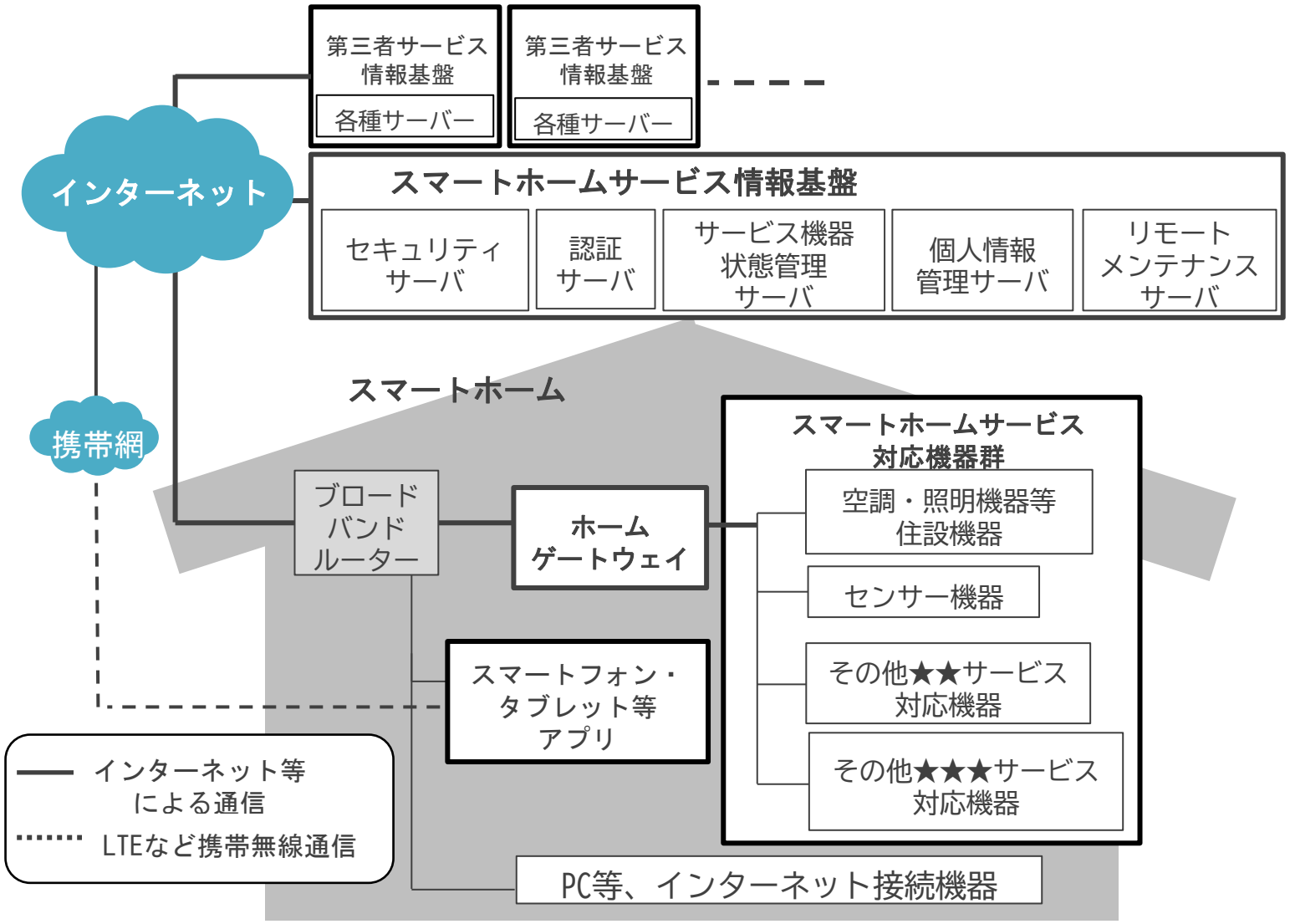
要件の粒度：
1）要件内容と合格レベルを規定

2）要件内容を規定
運用で合格レベルを規定

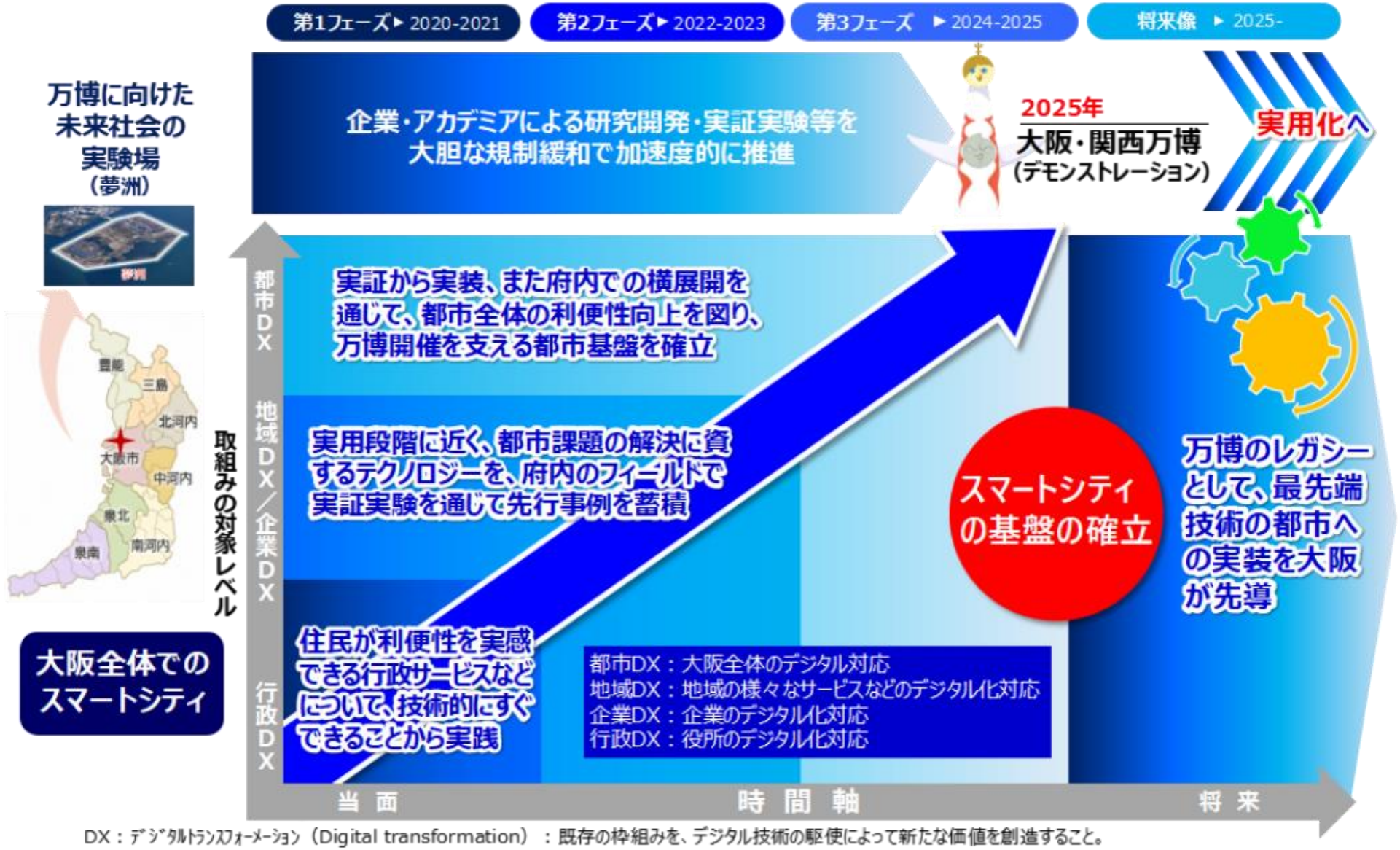
3）守るべき内容を規定
運用で合格レベルを規定

No.	サーティフィケーション要件
1	Web入力経由によるSQLインジェクションの不具合がないこと
2	Web入力経由によるクロスサイトリクエストフォージェリの不具合がないこと
3	Web入力経由によるパストラバーサルの不具合がないこと
4	未使用のTCP/UDPポートを外部より使用されないこと
5	システム運用上、必要なTCP/UDPセッションにおいて、適切な認証（機器毎にユニークなIDとパスワード）や通信アクセス制御が行われていること。
6	認証情報の設定変更が可能なこと（ハードコーディングされていないこと）
7	・利用者の設定した情報、および機器が利用中に取得した情報は、容易に消去できる機能を有すること ・情報消去後も、更新されたシステムソフトウェアは維持されること
8	Wi-Fiアライアンス推奨の最新の認証方式が装備されていること
9	・Bluetooth SIG推奨の最新のペアリング方式が装備されていること ・Bluetoothにおける不要なプロファイルを認識しないこと ・BluetoothのBlueborne脆弱性の脆弱性がないこと
10	USBについてシステム運用上、不要なクラスを認識できないこと
11	・ソフトウェア更新が可能なこと ・ソフトウェア更新された状態が電源OFF後も維持できること
12	・製品の脆弱性に関する連絡窓口があり、公開していること ・製品のセキュリティアップデートサポートサイトがあること

スマートホームのシステム構成モデル(CCDS版　モデルハウス)



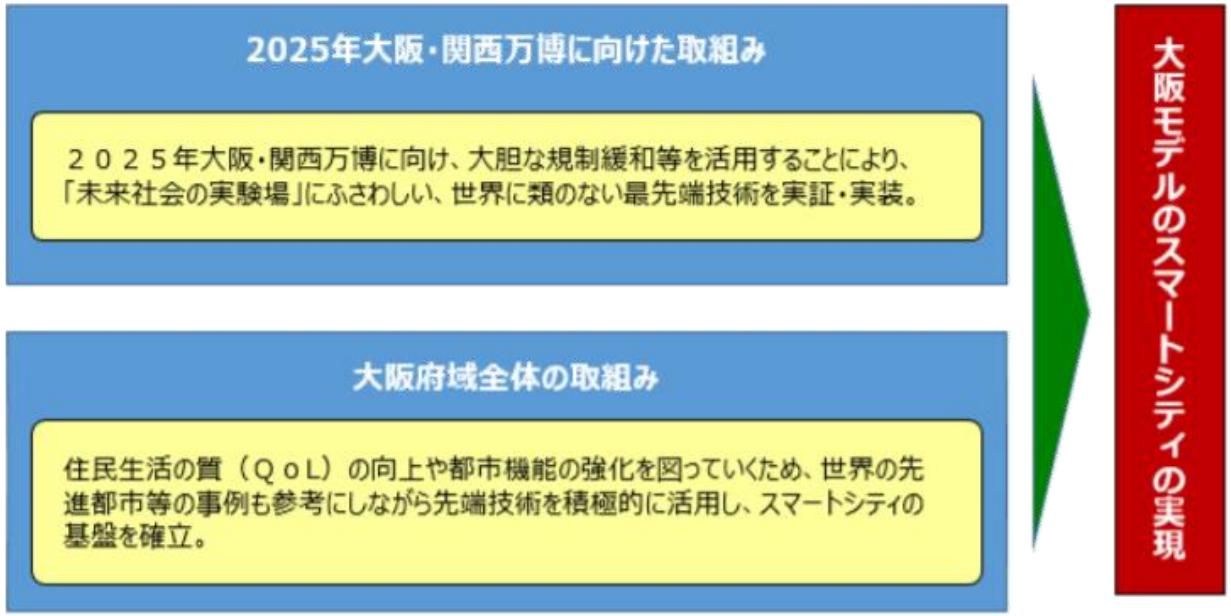
改めて、大阪・関西万博に向けて



DX：ﾃﾞｼﾞﾀﾙﾄﾗﾝｽﾌｫｰﾒｰｼｮﾝ（Digital transformation）：既存の枠組みを、デジタル技術の駆使によって新たな価値を創造すること。

大阪スマートシティ戦略 Ver.1.0

- 2050年には世界人口の約７割が都市に集中する と言われる中、世界の諸都市では、IoT、 AI、ビッグデータ等の先端技術を利用し、都市課題の解決や都市機能の効率化に活かそう とする「スマートシティ」の取組みが始まっている。 大阪府・大阪市の連携により副首都の確立・発展をめざす大阪においても、2025年大阪・ 関西万博の開催や**人口減少・超高齢社会の到来を見据え、住民の生活の質（QoL）**の向上や 都市機能の強化を図っていく上で、先端技術を活用した「スマートシティ」の実現は不可 欠である。 そのため、**最先端技術のショーケースとなる2025年大阪・関西万博を大きなインパクト**としながら、府域全体で先端技術による利便性の向上を住民に実感してもらえるような都 市をめざすため、具体的な方向性や実践的な取組みを示す「大阪スマートシティ戦略」（以 下、「本戦略」という。）を検討・策定することとした。 今般、これまで実施してきた「大阪スマートシティ戦略会議」での議論や、企業・市町 村との意見交換を踏まえ、2025年大阪・関西万博に向け、大胆な規制緩和等により、**「未来 社会の実験場」**にふさわしい、世界に類のない最先端技術を活用した取組みと、府域全体 で先端技術の利便性を住民に実感してもらえるような取組みの二つの取組みを両輪として、 大阪モデルのスマートシティを実現するための指針として、本戦略を策定した。 本戦略は、健康的な生活の確保や福祉の促進、質の高い教育や生涯学習の機会確保、安 全かつ強靭で持続可能な都市の実現といった、SDGs 1社会の実現を強力に後押しするもので もある。万博開催都市として「SDGs先進都市」をめざすためにも本戦略を推進していく。 本戦略の対象期間は、大阪・関西万博が開催される2025年頃を目途とする。 なお、本戦略は、自動運転、5Gなどの先端技術の実用化に向けた動き、戦略の取組み状 況、大阪スマートシティ戦略会議における議論などを踏まえ、今後、更新していく。



大阪スマートシティパートナーズフォーラム

ABOUT US 大阪スマートシティパートナーズフォーラムとは

大阪スマートシティパートナーズフォーラムは“大阪モデル”のスマートシティ実現に向けて、企業やシビックテック、府内市町村、大学等と連携し、地域・社会課題を解決していく「公民共同エコシステム」として令和2年8月に設立。(約350の企業・団体が参画)

団体概要

目的

企業やシビックテック、府内市町村、大学等と連携した“大阪モデル”のスマートシティの実現に向けた取組みの推進

事業内容

社会課題の見える化、コーディネート／ワークショップ・セミナー開催／情報発信　ほか

会員種別／会員資格

法人会員：企業など営利を目的とする団体

個人会員：法人会員に務める役員又は社員、個人事業主

特別賛助会員：経済団体

賛助会員：地方自治体、大学、研究機関など営利を目的としない団体

- 2020年8月設立
- 366団体
  （2021年4月現在）
- ６課題（＋1課題）
  - 16社が企業連携して取り組み中

大阪スマートシティパートナーズフォーラム

OSPFプロジェクト進捗状況

分野	プロジェクト内容	企業	市町村	進捗
スマートヘルスシティ	スマートヘルスプラットフォーム	デロイトトーマツグループ	堺市	令和3年度早期実証開始
高齢者にやさしいまちづくり	リビングラボ構想	EY新日本有限責任監査法人	泉大津市	令和3年度早期実証開始
	『共助』社会の構築		池田市・大阪府	令和3年度早期実証開始
	シニア向けスマートサービス	大阪ガス株式会社	大阪府	令和3年秋頃実証開始
	"地域コミュニティ"による課題解決	関西電力株式会社	河内長野市	令和3年度実証開始
	地域包括ケアシステム	株式会社日立製作所	募集中	-
	買物弱者支援	三井住友海上火災保険株式会社	富田林市	令和3年度早期実証開始
子育てしやすいまちづくり	可視化による保育の質向上	EY新日本有限責任監査法人	募集中	-
	見守りサービス	NECネッツエスアイ株式会社	門真市、堺市	令和3年度早期実証開始
	子育て支援施設の見える化	日本マイクロソフト株式会社	門真市	令和3年度早期実証開始
	リトルエストニア（北欧文化とスマートシティサービス）	NECネッツエスアイ株式会社、株式会社NTTドコモ、株式会社021、関西電力株式会社、三井住友海上火災保険株式会社	豊能町	令和3年度早期実証開始（豊能町との事業連携協定締結済み）
移動がスムーズなまちづくり	オンデマンド交通・交通渋滞緩和	アクセンチュア株式会社	-	-
	パーソナルモビリティ・AIオンデマンドバス	株式会社NTTドコモ	河内長野市	令和2年度 一部実証実施 令和3年度 継続し実証実施予定
	AIオンデマンド・モビリティポート	損害保険ジャパン株式会社／大日本印刷株式会社	-	-
	オンデマンド交通	パナソニックシステムソリューションズジャパン株式会社	-	-
インバウンド・観光の再生	バーチャルオンラインツアー・ライブコマース	凸版印刷株式会社	泉州エリア、藤井寺市	令和3年度実証開始
	観光行動データ利活用	日本電気株式会社	泉佐野市	令和3年度早期実証開始
大阪ものづくり2.0	基幹システムシェアリング	ソフトバンク株式会社	枚方市、八尾市、東大阪市	令和3年度早期実証開始

令和2年度プロジェクト分野

プロジェクト参加市町村（令和3年3月時点）

総括	大阪府／OSPF事務局／江川　将偉 氏（大阪府スマートシティ戦略スーパーアドバイザー）					
分野	スマートヘルスシティ	高齢者にやさしいまちづくり	子育てしやすいまちづくり	移動がスムーズなまちづくり	インバウンド・観光の再生	大阪ものづくり2.0
コーディネーター	Deloitte. デロイトトーマツ	EY / Daigas Group / 関西電力 power with heart / HITACHI Inspire the Next / MS&AD 三井住友海上	EY / NEC NECネッツエスアイ株式会社 / Microsoft	accenture / SOMPO 損保ジャパン / DNP / docomo / Panasonic BUSINESS	TOPPAN / Orchestrating a brighter world / NEC	SoftBank

会員企業・団体

連携してシームレスな
スマートシティへ

CCDSは賛助会員
CCDS代表理事　荻野はOSPF企画運営委員

2020年度スマートシティに対する取組み@OSPF(大阪スマートシティパートナーズフォーラム)

自治体の課題の整理方法

スマートシティの作り方概論

自治体(豊能町)の進め方例

提案資料作成例
自治体と企業の組立方法

IT基盤(簡単に行政サービス開発)
コミュニケーションI/Fを作る

豊能町での事例発表
誰でも始められるスマートシティ

CCDS　スマートシティへのアプローチ

スマートシティWGのアクティビティ

2021年4月 新設スマートシティWG　（活動趣意）

■概要：

（TrustedData連携からスマートシティWGへの変更）

スマートシティは、「IoT（Internet of Things：モノのインターネット）の先端技術を用いて、基礎インフラと生活インフラ・サービスを効率的に管理・運営し、環境に配慮しながら、人々の生活の質を高め、継続的な経済発展を目的とした新しい都市」であり、社会基盤になるIoTや個人データなどサービスを行う為に色々なデータを活用しながらサービスの構築がなされます。

スマートシティWGでは、安心・安全な街づくりに貢献すべく、以下ガイドラインの作成するものとします。

・産業別データ連携基盤の利用ガイドライン

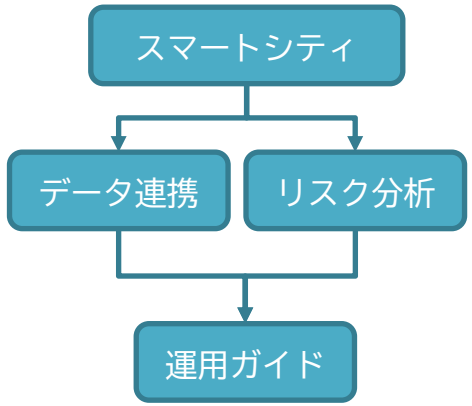
・スマートシティのデータ層（サイバー層）におけるリスクアセスメントガイドライン

■活動内容：

1）スマートシティサービスにおける情報の共有

2）産業別データ連携基盤の整理及び利用ガイドラインの作成　　（可能であれば、運用ガイドライン）

3）スマートシティにおけるリスクアセスメントガイドラインの作成



■本年度ゴール：

ガイドラインの方針の構築。翌年度からガイドラインを作成する検証期間

■参加者：

・主査：江川 将偉（CCDS/OZ1）、副査：検討中

・メンバー：三井住友海上、損保ジャパン、セイコーソリューションズ、帝国データバンク、電通国際、トレンドマイクロ、Trustdock、日立グループ（日立キャピタル）、関電グループ（オプテージ）、NEC、NECネッツエスアイ、凸版印刷、両備システムズ、コムソル、フューチャーアクセス、千葉銀行、りそな銀行、大阪府、横浜市、市原市、市川市、エストニア大使館（エンタープライズオブエストニア）、公立校大学大阪、神奈川大学、慶応義塾大学　など

・メンバー募集の有無：募集あり

簡単にまとめると・・・

「自治体がスマートシティ始めるのに、IT基盤（データ連携基盤・都市OS）どう選んだらいい？」

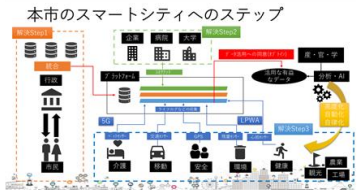
「IT基盤どうやって運用するの？　安全性は？」　のガイドライン

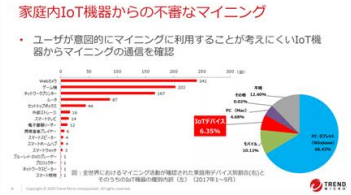
TrustData連携WG2020年度アクティビティ

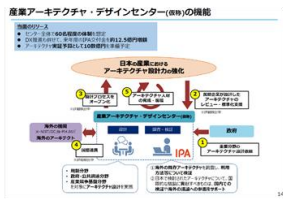
- **第一回**
  - サービス　日立キャピタル　Life as a Service　（スマートホーム）
  - セキュリティ・技術　OZ1　データ連携例（エストニア）＋データ連携技術説明（X-Road/FIWARE）
- **第二回**
  - サービス　市原市　スマートシティ デジタルコミュニケーション基盤の構築に向けた取組
  - セキュリティ・技術　トレンドマイクロ　いえなかに関するIoT関連ソリューションについて
- **第三回**
  - サービス　エストニア大使館　電子立国エストニアと日本での取組について
  - セキュリティ・技術　帝国データバンク　トラストサービスについて（CA/eシール）
  - オブザーバー　情報処理推進機構　産業アーキテクチャ・デザインセンター取組の狙いについて
- **第四回**
  - サービス　ビットキー　Bitkey Platformについて（スマートロック）
  - セキュリティ・技術　TRSUTDOCK　オンラインにおける身元確認について（eKYC）
  - 告知　大阪府　大阪スマートシティパートナーズフォーラム（OSPF）8月25日スタートお知らせ
- **第五回**
  - サービス　OZ1　エストニアヘルスケアサービス　Viveo/Helmes紹介
  - TDWG　大阪府/OZ1　大阪OSPFの取組み（案）案内、スマートシティフィールドとしての活用検討
- **第六回**
  - 続・大阪スマートシティパートナーズフォーラムの進め方と自治体の課題を検討
  - CCDSで取り組む安全なデータ連携の基礎作りを相談

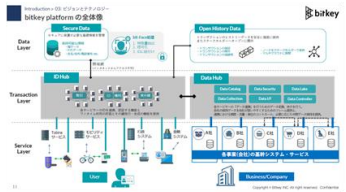
TrustData連携WG2020年度アクティビティ

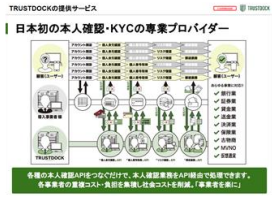
- **第七回**
  - ・大阪スマートシティパートナーズフォーラムOSPFの進捗サマリー
    ・＊スマートシティの基礎になるデータ連携基盤（一部都市OS)の仕様＊＊
    ・＊スマートシティのオペレーション分析に関して＊＊
    ・各省庁（総務省、経産省、内閣府など）や外部協議会とのタッチポイント
- **第八回**
  - ・OSPFの進捗・豊能町PJ進捗
  - ・OSPF/CCDSでのデータ連携勉強会検討
  - ・ガイドラインの取組み進捗
- **第九回**
  - ・OSPFの進捗
  - ・豊能町PJ進捗
  - ・OSPFのデータ連携勉強会
  - ・ガイドラインの取組み進捗
  - ・トラストサービスUpdate（帝国データバンク）
- **第十回**
  - ・OSPF（大阪スマートシティ）の進捗
  - １月25日開催　まちづくりのコンセプトセミナーについて
  - （江川分作りかけの資料先出）
  - 今回自治体と企業との文化の違いやコンセプトを考える
    意味提案書の見え方などを話します。
  - ・スマートシティの調達基準や考え方　by荻野さん 30分程度
  - 大阪を踏まえてスマートシティのサービスにおける
  - 調達基準や監査基準の考え方をシェアします。
  - ＊OSPF参加企業は基準作りする上の準備として検討
  - ＊参加自治体は、自治体でどのように考えればよいのかの参考
  - ・NoCode
- **第十一回**
  - OSPFの進捗
    ・イベント関連（NoCodeイベントなど）
    ・豊能町の進捗
    来年度の取組み
    ・ワーキング名変更
    ・取組み内容説明











現在の展開

OSAKA SMARTCITY PARTNERS FORUM

- 大阪スマートシティパートナーズフォーラム
  企画運営委員に荻野 司就任
  （大阪府スマートシティ戦略 スーパーアドバイザーにTDWG主査江川が就任）
- 大阪府をフィールドにスマートシティでデータ連携をベースに検証をスタート
- CCDSを介して、他府県とも連携しながら大阪に留まらず展開

- 繋がるモノやサービスの可視化、データの在り方などフィールドから
  可視化させセキュリティや安全な連携のガイドラインを作成し始めます。

ガイドラインサンプル

JP-Link 利用事業者ガイドライン

2021 年 xx 月発行

一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）
Trusted Data 連携ワーキンググループ

目次

1. はじめに

1.1 ガイドライン策定の背景・目的

1.1.1 スマートシティにおける JP-Link の位置付け

Society5.0 の考え方に基づくデータ駆動型のスマートシティを実現するためには、市民や IoT 製品などから収集したデータや、行政の持つオープンデータを分野横断的に連携するプラットフォームが必要不可欠である。内閣府の「スマートシティリファレンスアーキテクチャ」においても、スマートシティの基礎プラットフォームとして都市オペレーティングシステム（以下、「都市 OS」）を定義し、その要件として「相互運用（つながる）」、「データ流通（ながれる）」、「拡張容易（つづけられる）」としている。

重要生活機器連携セキュリティ協議会（以下、CCDS）では、2020 年 4 月に Trusted Data 連携ワーキンググループ（以下、TDWG）を立ち上げ、スマートシティをフィールドに、サイバー空間におけるデータ連携サービス、セキュリティの検討とガイドライン化、サービスを活用したエコシステムの検討を行っている。TDWG では都市 OS の基本アーキテクチャとして、ヒトをつなぐ ID システム、組織をつなぐデータ連携基盤、モノをつなぐ IoT 基盤の 3 つを定義し、それぞれが連携し作用することで市民、組織に付加価値の高いサービスを提供するとしている。本ガイドラインで説明する「JP-Link」とは、このうちのデータ連携基盤を指し、CCDS/TDWG の幹事企業である株式会社 OZ1 が、エストニアの情報連携基盤である X-Road をベースに開発したデータ連携プラットフォームである。X-Road は参加した自治体/企業が容易に接続可能で、組織間のデータ連携をセキュアに行える基盤である。X-Road はスマートシティリファレンスアーキテクチャ内でも EU の代表的な取り組みとして紹介されており、都市 OS のプラットフォームとして有用な基盤である。なお、JP-Link はその用途を都市 OS に限定するものでは無い。分野横断的にセキュアにデータ連携を行う要件があればどの分野においても活用可能である。

本ガイドラインは JP-Link 利用を前提に、JP-Link の概要、利用組織がどのようにビジネスを考えれば良いのか、参加資格と導入運用保守、セキュリティの考え方を纏めたものである。

図 1-1 (暫定図)都市 OS における JP-Link の位置付け

1.2 ガイドラインの構成と想定読者

本ガイドラインでは JP-Link サービスを活用し、利用者に新たな付加価値サービスを提供する事業者を対象としている。

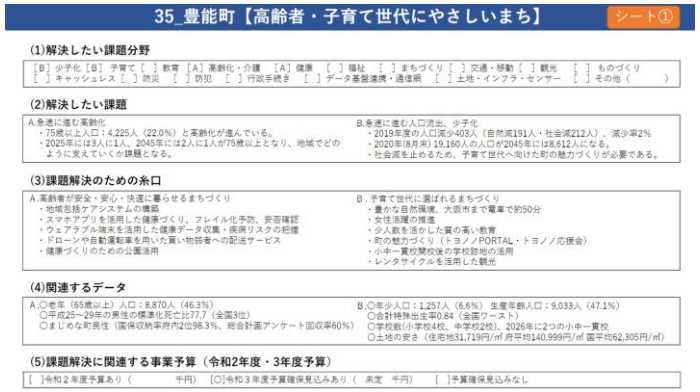
特定の技術に偏ったので現状未公開

スマートシティWGアクティビティについて（説明用資料）

サービス（豊能町をサンプリング）
IT基盤
リスクアセスメント

スーパーアドバイザープロジェクトとして豊能町のスマートシティをモデリン

元の課題：人口減による過疎化


35_豊能町【高齢者・子育て世代にやさしいまち】 シート①

(1)解決したい課題分野

[B] 少子化 [B] 子育て [ ] 教育 [A] 高齢化・介護 [A] 健康 [ ] 福祉 [ ] まちづくり [ ] 交通・移動 [ ] 観光 [ ] ものづくり [ ] キャッシュレス [ ] 防災 [ ] 防犯 [ ] 行政手続き [ ] データ基盤連携・通信網 [ ] 土地・インフラ・センサー [ ] その他 ( )

(2)解決したい課題

A.急速に進む高齢化
・75歳以上人口：4,225人（22.0%）と高齢化が進んでいる。
・2025年には3人に1人、2045年には2人に1人が75歳以上となり、地域でどのように変えていくか課題となる。

B.急速に進む人口流出、少子化
・2019年度の人口減少403人（自然減191人・社会減212人）、減少率2%
・2020年(8月末)19,160人の人口が2045年には8,612人になる。
・社会減を止めるため、子育て世代へ向けた町の魅力づくりが必要である。

(3)課題解決のための糸口

A.高齢者が安全・安心・快適に暮らせるまちづくり
・地域包括ケアシステムの構築
・スマホアプリを活用した健康づくり、フレイル化予防、安否確認
・ウェアラブル端末を活用した健康データ収集・病気リスクの把握
・ドローンや自動運転車を用いた買い物弱者への配送サービス
・健康づくりのための公園活用

B.子育て世代に選ばれるまちづくり
・豊かな自然環境、大阪市まで電車で約50分
・女性活躍の推進
・少人数を活かした質の高い教育
・町の魅力づくり（トヨノ/PORTAL・トヨノ応援金）
・小中一貫校開校後の学校跡地の活用
・レンタサイクルを活用した観光

(4)関連するデータ

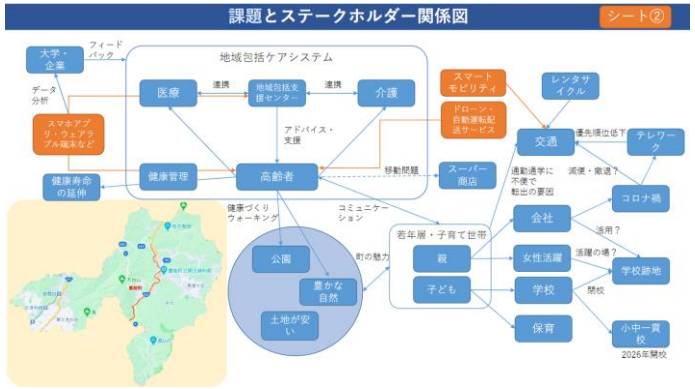
A.○老年（65歳以上）人口：8,870人（46.3%）
○平成25～29年の男性の標準化死亡比77.7（全国3位）
○まじめな町民性（国保収納率府内位98.3%、総合計画アンケート回収率60%）

B.○年少人口：1,257人（6.6%） 生産年齢人口：9,033人（47.1%）
○合計特殊出生率0.84（全国ワースト）
○学校数(小学校4校、中学校2校)、2026年に2つの小中一貫校
○土地の安さ（住宅地31,719円/㎡ 府平均140,999円/㎡ 国平均62,305円/㎡）

(5)課題解決に関連する事業予算（令和2年度・3年度予算）

[ ]令和２年度予算あり（ 千円） [○]令和３年度予算確保見込みあり（ 未定 千円） [ ]予算確保見込みなし

高齢化対策と移動の問題



根本課題

急速に進む人口流出と少子高齢化
・2020年(7月末)は19,174人の人口が2045年には8,612人になる。
・人口流出と共に少子高齢化も進み、2045年には町内のおよそ2人に1人が高齢者になる。

基本目標（自治体の課題を読みながら考える）

豊能町の進む高齢化と人口減少を軽減させるため、**人口流入による地域の活性化**
活性化による高齢者の支援を基本します。また豊能町の最大を強みを生かした街づくりを考えます。

豊能町の最大の強み

1．自然の豊かさ　町の9割が「緑」
2．大阪市街地からのアクセスの良さ。大阪駅から妙見口60分（東京で言う八王子高尾さん観光）
3．高齢者が元気（農家も多い。）

豊能町の弱み

1．人口流出　若者世代が町外に流出
2．町の強みが見え辛い
3．町内の移動手段

環境変化を捉える

コロナ禍で、個人の趣味嗜好の変化を捉える！
キャンプ・グランピングでの自然との遊びやリモートワークでの働き方改革を活用！

POINT

豊能町の財務力は900位くらい(1800自治体中)で、平均に近い自治体です。
豊能町がスマートシティ化できるかは、日本全体がスマートシティに進めるかの大きな課題

財務力調べアパマンショップのWebより

街の資産を有効に活用して、街全体の活性化を目指す

関係者みんなで街の在り方を考え、デジタル先進国の北欧文化を含めて取組み

リモートワーク環境充実西地区
（市街地へのアクセスもできる街）

ネットワーク環境	NEC NECネッツエスアイ株式会社
リモートオフィス	NEC NECネッツエスアイ株式会社
地域交流サービス	NEC NECネッツエスアイ株式会社
デジタル教育	MS&AD 三井住友海上
買い物支援	MS&AD 三井住友海上
子供見守り	NEC NECネッツエスアイ株式会社
高齢者見守り	関西電力 power with heart
シェアモビリティ	docomo

町内住民8割が西地区

移動手段

北欧体験ができる東地区
（リラックスを中心とした街づくり）

北欧文化を学び
住民とも一緒に街づくりを
考える

ネットワーク環境	NEC NECネッツエスアイ株式会社
文化交流サービス	豊能町
デジタル教育	MS&AD 三井住友海上
買い物支援	MS&AD 三井住友海上 / 関西電力 power with heart
（子供見守り）	NEC NECネッツエスアイ株式会社
（高齢者見守り）	関西電力 power with heart / NEC NECネッツエスアイ株式会社
体験サービス	豊能町
まつりイベント	豊能町
地域電力	関西電力 power with heart
行政効率化	RESONA

リモートワーク環境と生活環境の改善を図り
都心部への転出を抑制し、都心部へ流出した人を
「UJIターン」を図りながら西地区の活性化を図ります

自然豊かな環境を北欧文化を
取り込みながら豊能文化を再
構築

都会の疲れを癒す街

色々なサービスで地域の活性
化やコミュニティを構築

西地区　**東地区**

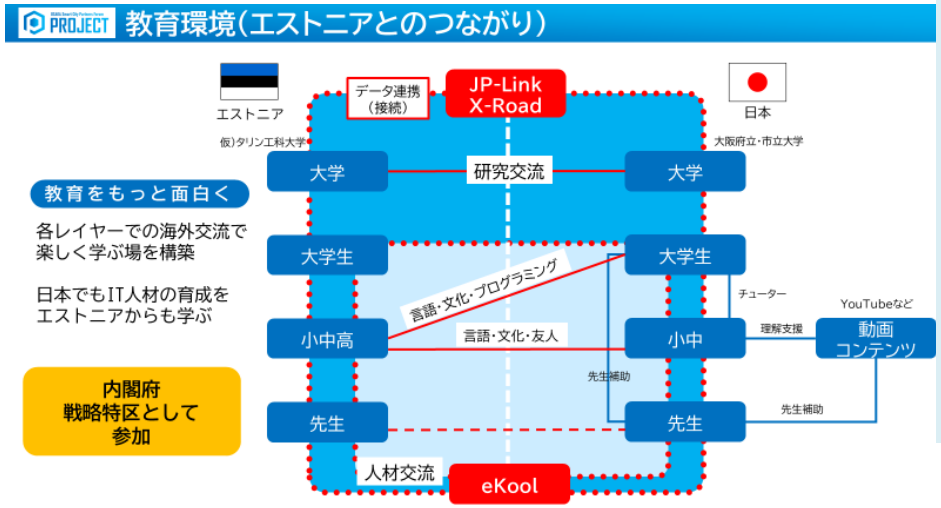
街のインフルエンサー

豊能町の主になる教育（GIGAスクール環境を活用し教育を豊かに）

北欧（エストニア）の教育環境を参考に豊能町でできる事を考える
5-10年先のスマートシティを支える為にも教育は非常に重要

OECDのPISAテストでのエストニアの位置づけ

		Mean reading score in PISA 2018	Coverage Index 3: Coverage of 15-year-old population	Strength: Percentage of variance in reading performance explained by ESCS[1] (R^2)	Difference between advantaged[2] and disadvantaged students in reading	Percentage of disadvantaged students who are academically resilient[3]
		Mean		%	Score dif.	%
	OECD average	487	m	12.0	89	11
中華圏	B-S-J-Z (China)	555	0.81	12.6	82	12
中華圏	Singapore	549	0.95	13.2	104	10
中華圏	Macao (China)	525	0.88	1.7	31	20
中華圏	Hong Kong (China)	524	0.98	5.1	59	16
エストニア	Estonia	523	0.93	6.2	61	16
	Canada	520	0.86	6.7	68	14
	Finland	520	0.96	9.2	79	13
	Ireland	518	0.96	10.7	75	13
	Korea	514	0.88	8.0	75	13
	Poland	512	0.90	11.6	90	11
	Sweden	506	0.86	10.7	89	11
	New Zealand	506	0.89	12.9	96	12
	United States	505	0.86	12.0	99	10
	United Kingdom	504	0.85	9.3	80	14
日本	Japan	504	0.91	8.0	72	12
	Australia	503	0.89	10.1	89	13
	Chinese Taipei	503	0.92	11.4	89	12
	Denmark	501	0.88	9.9	78	12
	Norway	499	0.91	7.5	73	12
	Germany	498	0.99	17.2	113	10
	Slovenia	495	0.98	12.1	80	12
	Belgium	493	0.94	17.2	109	9
	France	493	0.91	17.5	107	10



エストニアと豊能町でも交流を

サービスを行う効果

効果の在り方
想定される効果や今までの事例で関係者が理解できる情報

【エストニアの環境】
デジタル先進国エストニア活用
・デジタル教育（GIGAスクール）
既に導入し20年近くの経験
・デジタル教育の結果PISAテストでNo1
・利用しているツールの概要

【期待される効果】
・導入すれば街の教育も良くなる
・学生がIT教育されるとIT人材も増える
・スマートシティのサービスを開発する
人材も増える

GIGAスクール環境を活用した教育を豊かに

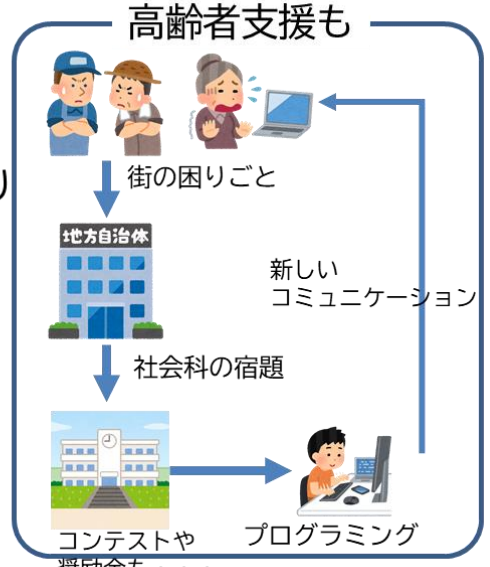
GIGAスクールの環境を豊かに、街づくりにも貢献を

ドローンプログラミング

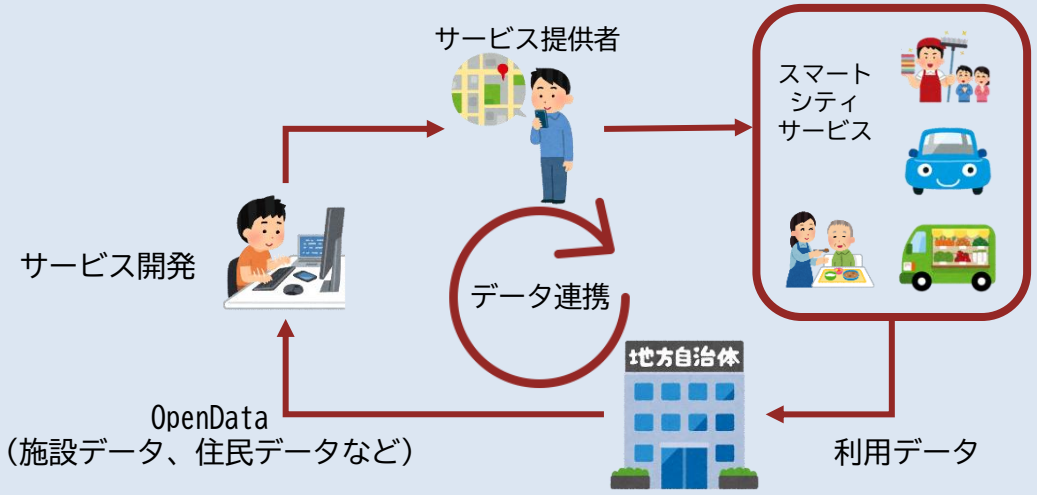
NoCodeプログラミング

プログラミング教育も色々と用意してＩＴ活用人材も
スマートシティを維持する上でもＩＴ人材は重要

子供たちと
作る街づくり



NoCodeを活用して、街の課題を住民と一緒にデザインする



アプリ例

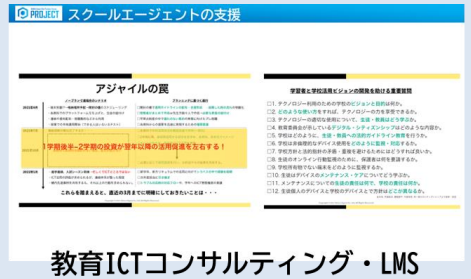
- 街の手の空いた人が高齢者支援
  - 家事代行
  - 買い物代行
  - 介護支援
- アスマイルなどと連携してヘルスケアアプリ
- 農業の支援アプリ（農機具シェア、人材マッチング）
- 交通アプリ（シェア型移動サービス）

- 自治体と一緒にデジタル行政サービス

GIGAスクールを
国内企業も支援

デジタル教科書

教育コンテンツ配信サービス



教育ICTコンサルティング・LMS

教育ICT＋先生の教え方など情報交換

組み入れるサービスを検討

各企業同士も連携してサービスの拡張を

子育てしやすい

NEC
NECネッツエスアイ株式会社
IoT機器（LPWAやカメラなど）を活用した子供の見守り

MS&AD 三井住友海上（OZ1）
GIGAスクール環境における教育内容の拡充（海外との交流）

高齢者にやさしい

MS&AD 三井住友海上
買い物支援サービス（移動販売、宅配BOXなど）

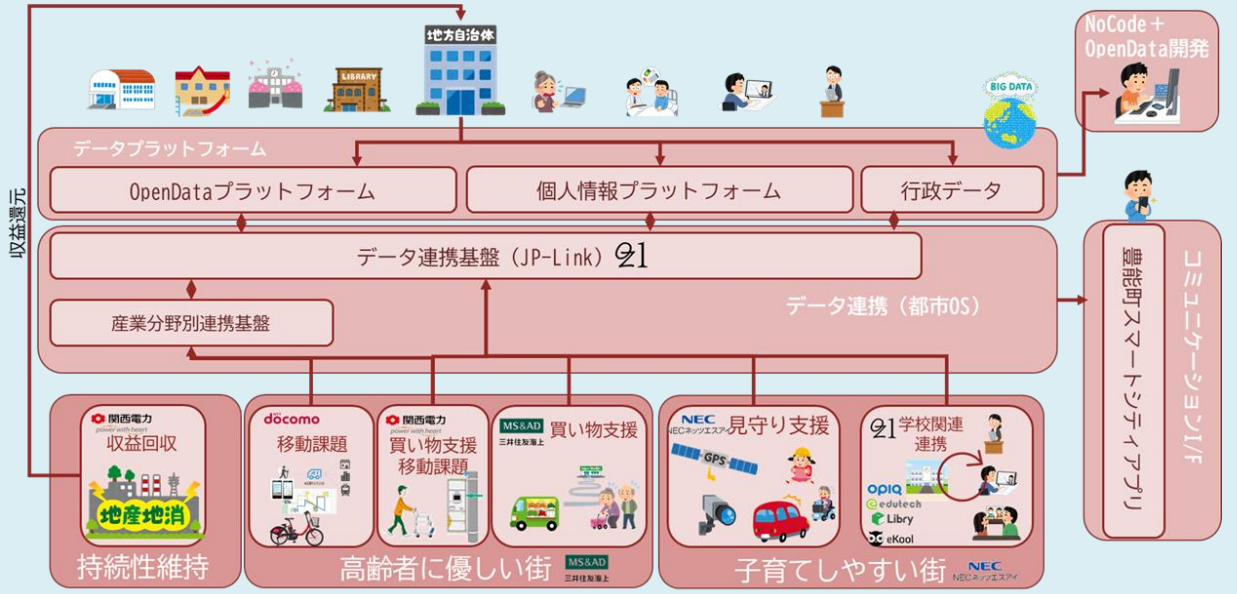
関西電力 power with heart
買い物支援サービス（宅配BOXなど）

移動がスムーズ

関西電力 power with heart
電動ゴルフカートなど利用や独自交通サービスの提供

docomo
AIオンデマンドシステム、シェア電動自転車の提供

データ連携基盤活用
企業とサービス・データ活用しシームレスなサービスへ



（その他企業や団体も参加しやすい環境を構築）

全体取り纏め
スーパーアドバイザー　江川
教育改革・省庁調整
OZ1　江川
海外交流
OSPF運営委員　須原

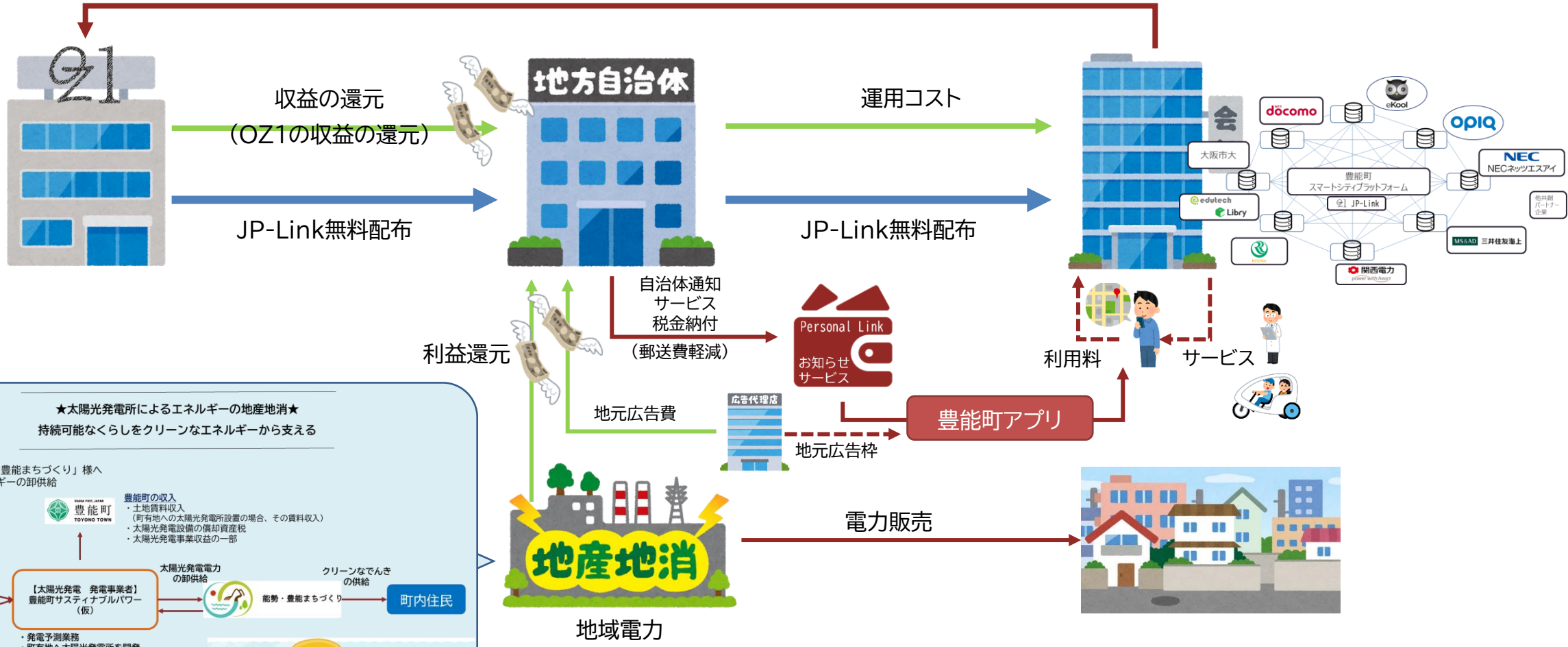
現在24企業・団体の参加し、豊能町のスマートシティ化を検討

持続可能なエコシステム（収益の地産地消）→　地域電力（関西電力）＋データ連携（OZ1）

持続可能なエコシステム（収益の地産地消）

地域エネルギーやデータ利用での収益を自治体に還元し、スマートシティサービスの維持

JP-Link利用料（アクセスした分だけ）



始めの設備費は、ふるさと納税・クラウドファンディングなど活用

全体のスケジュール

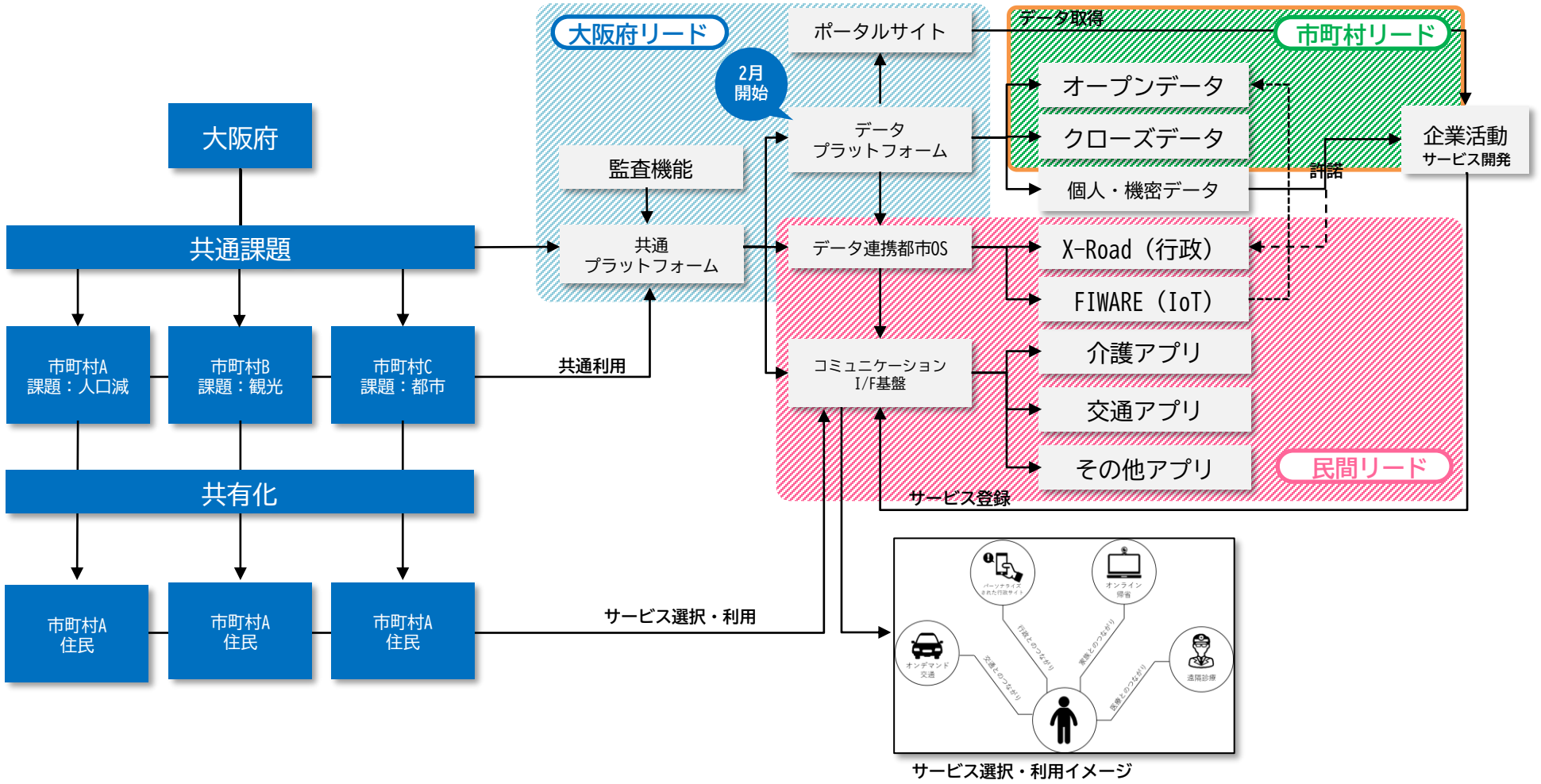
項目		3				4				5				6				7				8				9				10				11			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
街づくり	東地区	リーダー声がけ			Estonia説明	イベント段取り				北欧・エストニア文化 浸透イベント																								とよのまつり			
				電力関連調査						地域電力検討								クラウドファンディング				費用検討															
	西地区	高齢者・子育て政策検討＆調査								実装段取（見守・買い物支援）								一部実装								実装・検証											
														住民ヒアリング モニター住民募集																							
	全体					特区申請準備＆助成金検討								特区申請												予算概算要求								とよのまつり			
														移動問題検討																				のせでんアートライン			
	ITインフラ環境			要件・環境調査						WBS作成								実装・検証								アプリ・データ環境調整											
						豊能データ整理（Opendata等）								サービス検討				サービス整理				テストアプリ				豊能アプリ（スーパーアプリ）				アプリ随時強化更新							
						行政サービスデジタル化検討																																	
										企業サービス整理																													
														運用体制検討								運用チーム・検証								維持管理							
教育環境	GIGA	GIGA準備				開封	ITツール慣れ							カリキュラム準備				環境準備								現場フォロー											
	エストニア教育													現場状況把握								交流先検討				一部交流											
														eKool準備																							
	大学生支援					NoCodeトレーニング												学生交流準備				一部交流															
														ボランティアorバイト募集																							
	他校交流																																				
	他自治体交流					市原市																															

*特区例：制限として紙の教科書無償配布（文部科学省）、住民の配送における費用（国土交通省）、外国人医師の診療（厚生労働省）など→特区で規制緩和

IT基盤

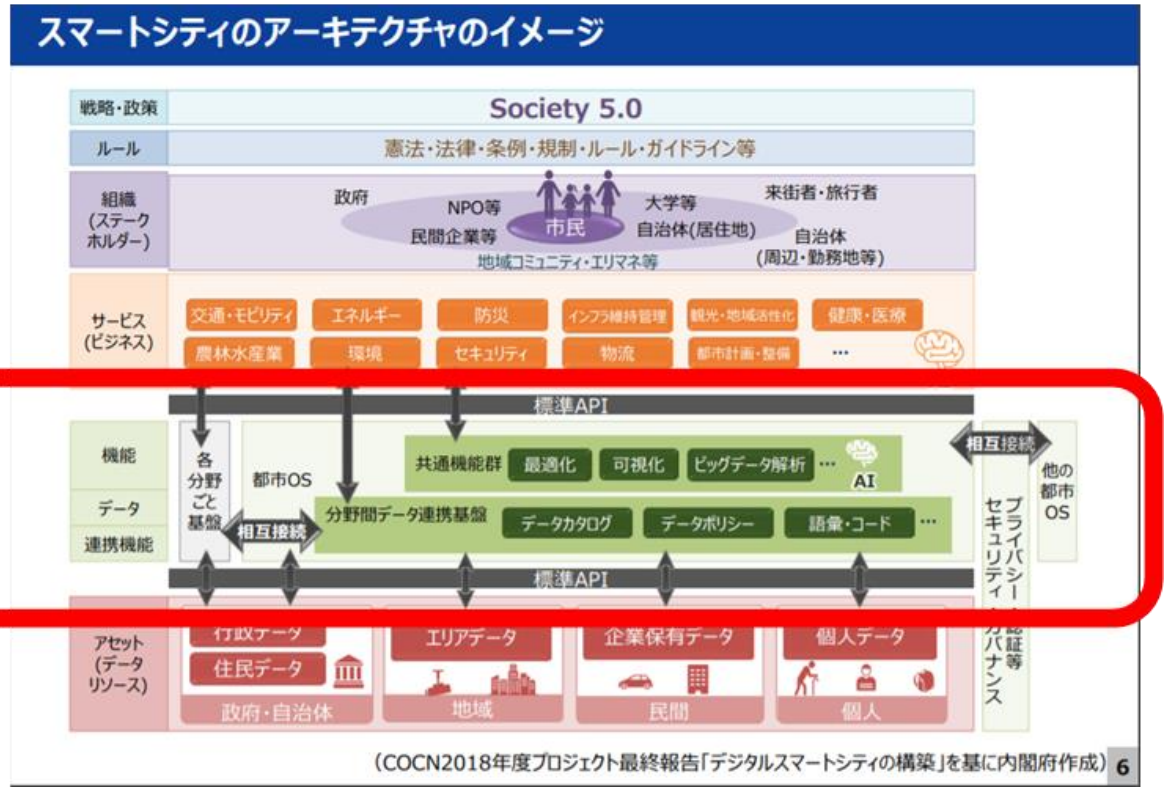
OSPFでのIT共通プラットフォームのガイドライン

- スマートシティはITだけでは、成立しない。オペレーション・ガバナンスが重要
- データ連携を順に追って構築し、各社と調整が大切



日本が想定するサービス・データ連携の在り方

標準APIを持ち全てのサービスを繋ぎ、データを管理・仲介する事でデータの売買も可能な新しいサービス
このサービスを**都市OS**と位置づけております。
スーパーシティ・スマートシティで都市OSは非常に重要な役割になります。



スーパーもスマートも都市OS上に構築されている

スマートシティを運営する組織体にも
データ連携基盤（都市ＯＳ）を組織する体制（オペレーション）

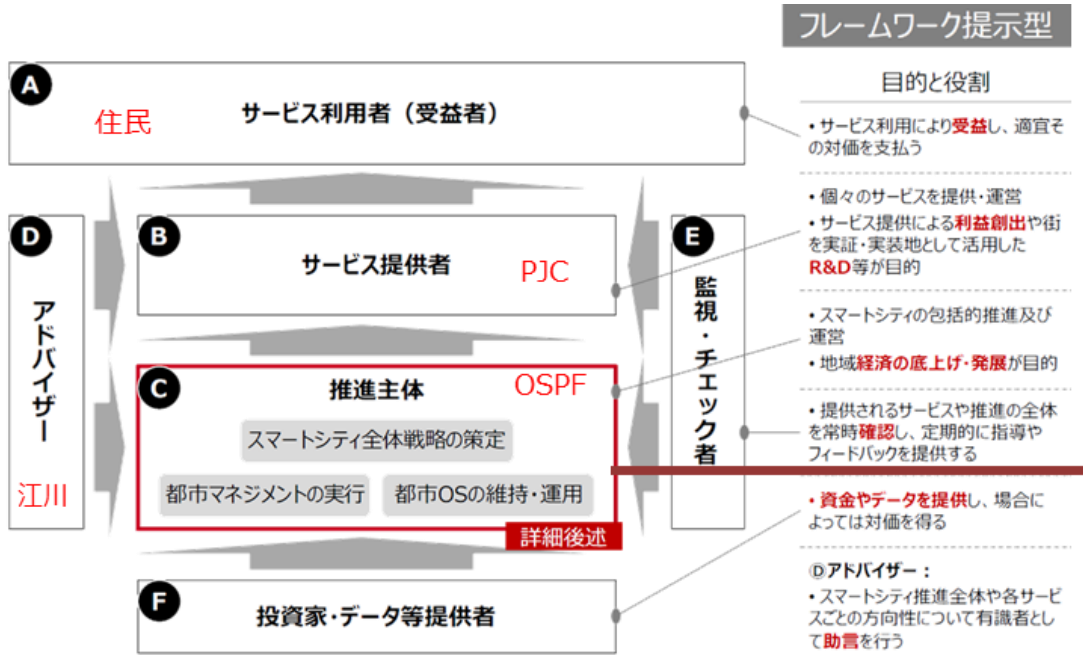


図 5.1-1　スマートシティにおけるステークホルダーの種類

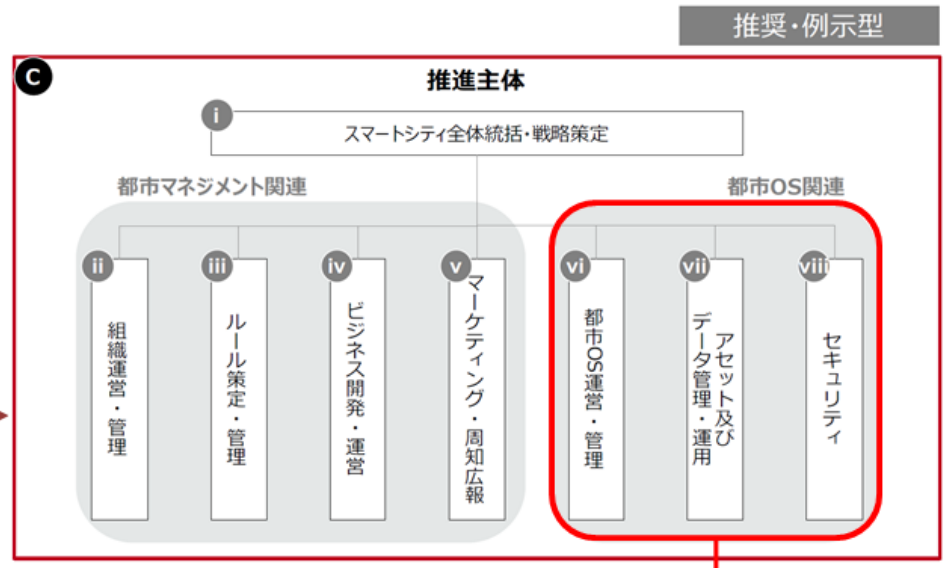
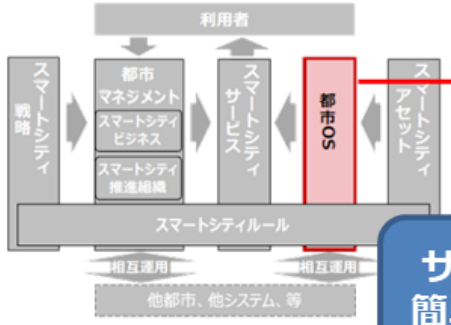


図 5.1-3　推進主体の担うべき機能例



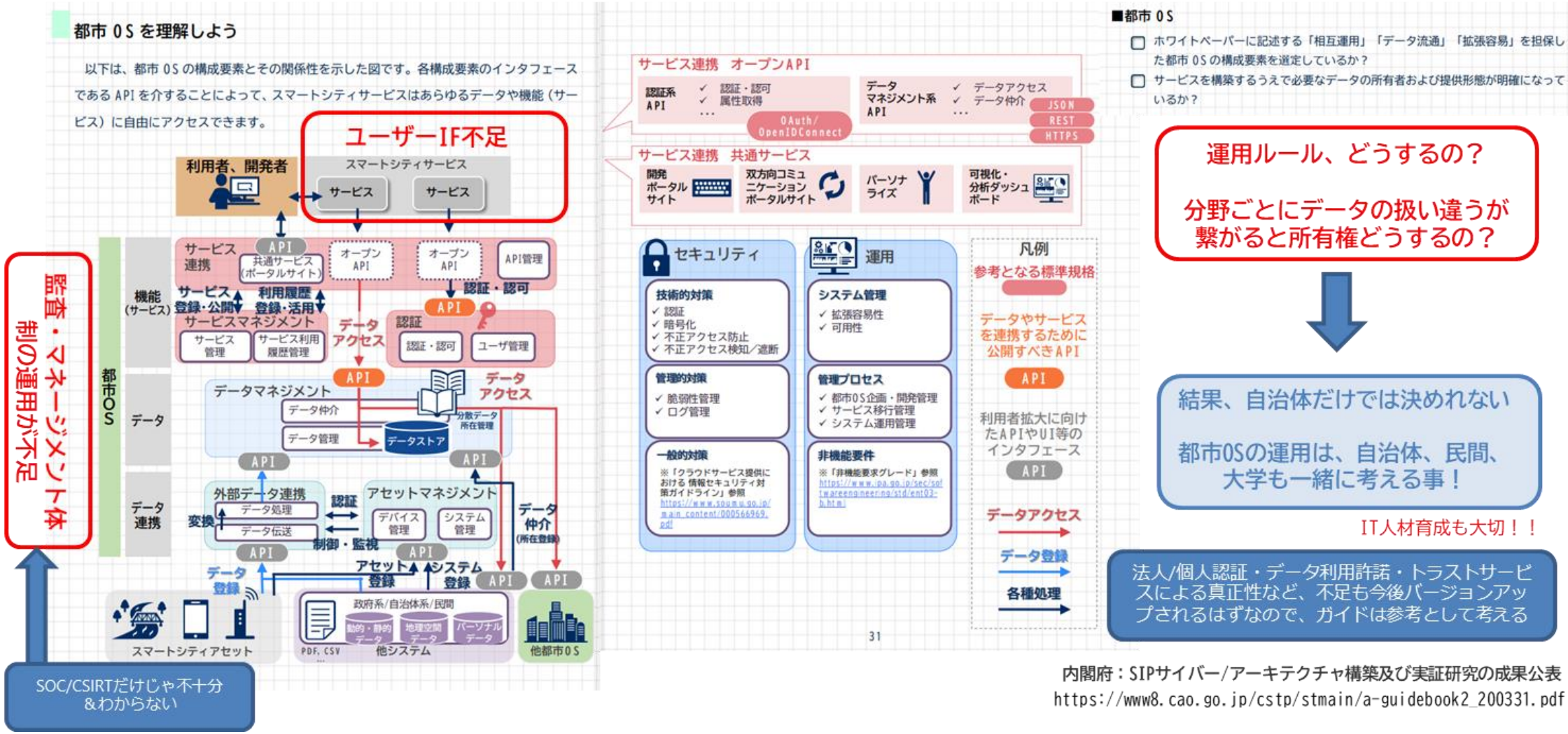
都市OSの見え方は、記載者により場所は変わるが
都市OSは独立して記載されております。

**サービスも都市OSに関わり、共にルールにも関わるので
簡単に割り切れない組織をどのように組むのかも今後検討**

出展：内閣府SIPより江川追記

データ連携のガイドラインを考えていく

都市OSの概略と考えていくべきポイント



内閣府：SIPサイバー/アーキテクチャ構築及び実証研究の成果公表
https://www8.cao.go.jp/cstp/stmain/a-guidebook2_200331.pdf

産業分野ごとに使われ方の違うデータ連携基盤

X-Road/IDの領域

- 法人間/個人間のデータ連携
- 監査証跡の確保
- 個人の許諾ベースの情報活用

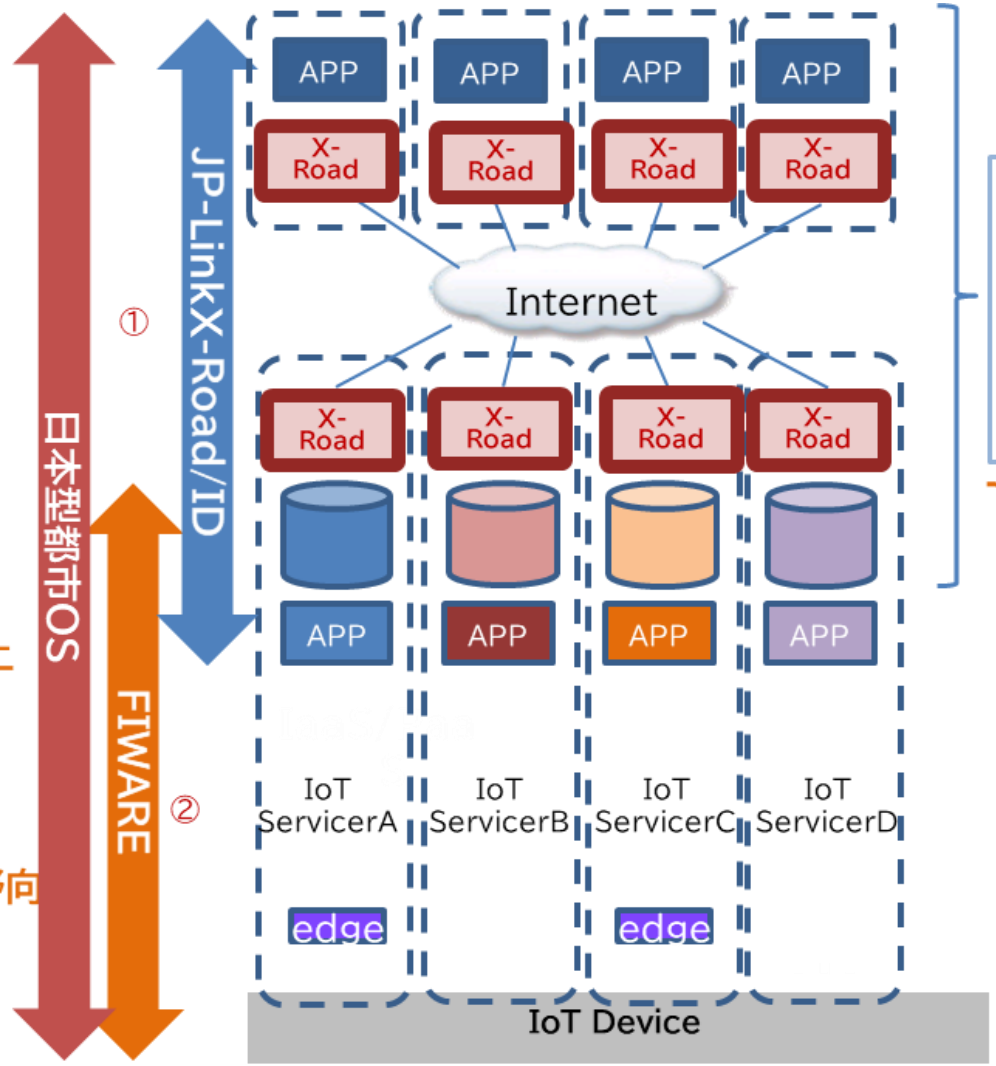
FIWAREの領域

- IoTサービスプラットフォーム
- IoT領域の標準化からStart
- IoTシステム開発の生産性向上
- IoT Systemの相互運用性
- データ収集・蓄積・仲介

Context Broker

＋

データモデルをターゲットした分野向けに準備



・X-Roadは組織データやデータベースをPtoPで共有する基盤

・オープンソースで汎用性が高く住民サービスを構築する際に使われる手法

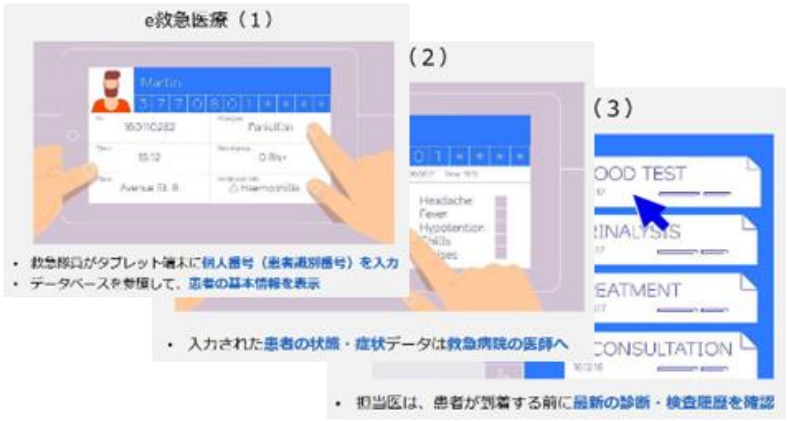
・FIWAREはIoTのためのデータ共有の基盤
・柔軟性の高いデータモデルで統合管理が可能

データの流通を可能にするために、標準的なデータモデルと、オープンな共通APIを準備

各モジュールを組み合わせて開発が可能

出展：OZ1技術説明資料より

用途によるデータ連携基盤のサービス例



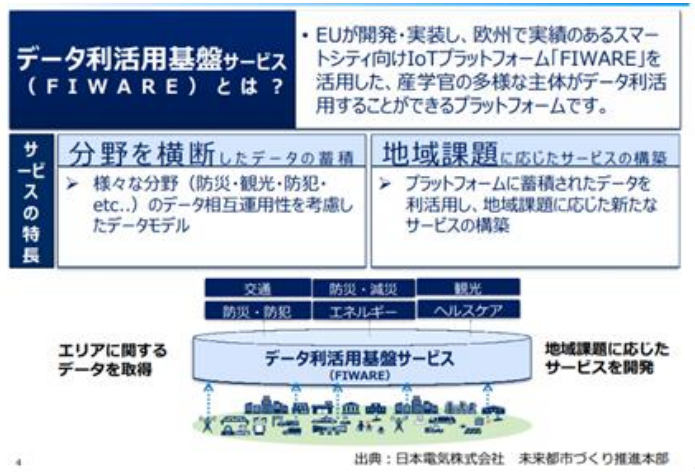
①

住民サービス
X-Road

利用目的が違うので
共存を検討

都市開発
FIWARE

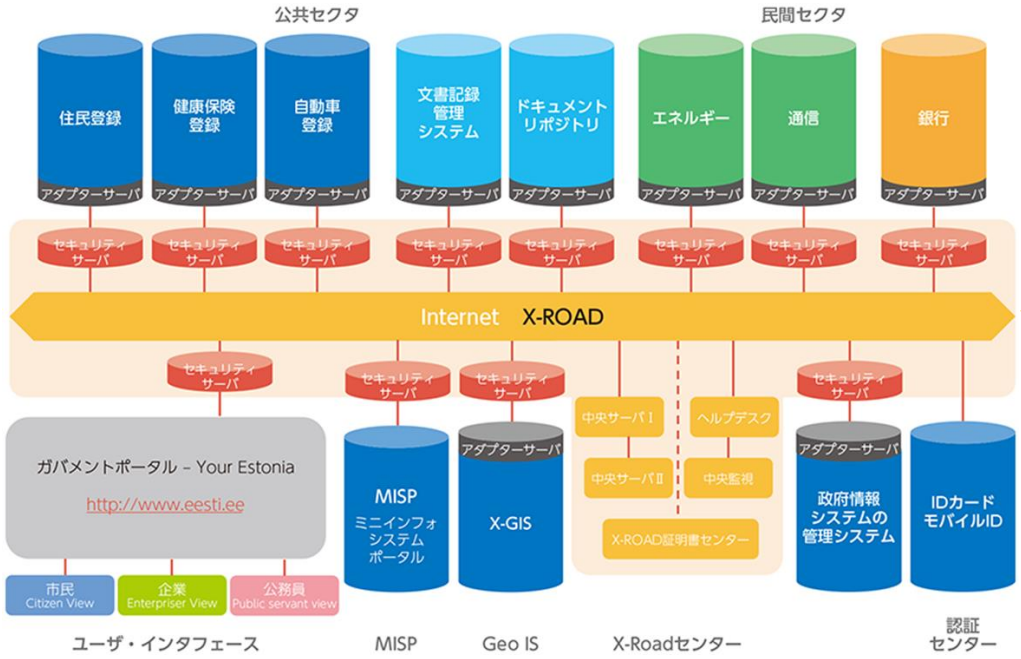
②

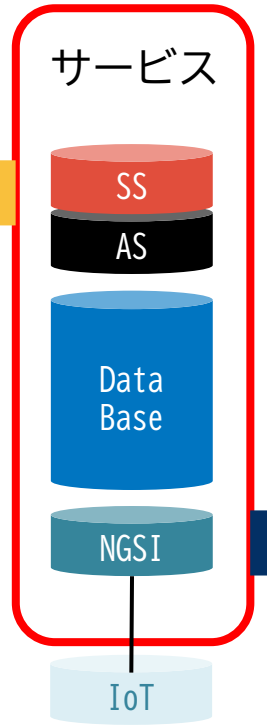


出展：OZ1技術説明資料より

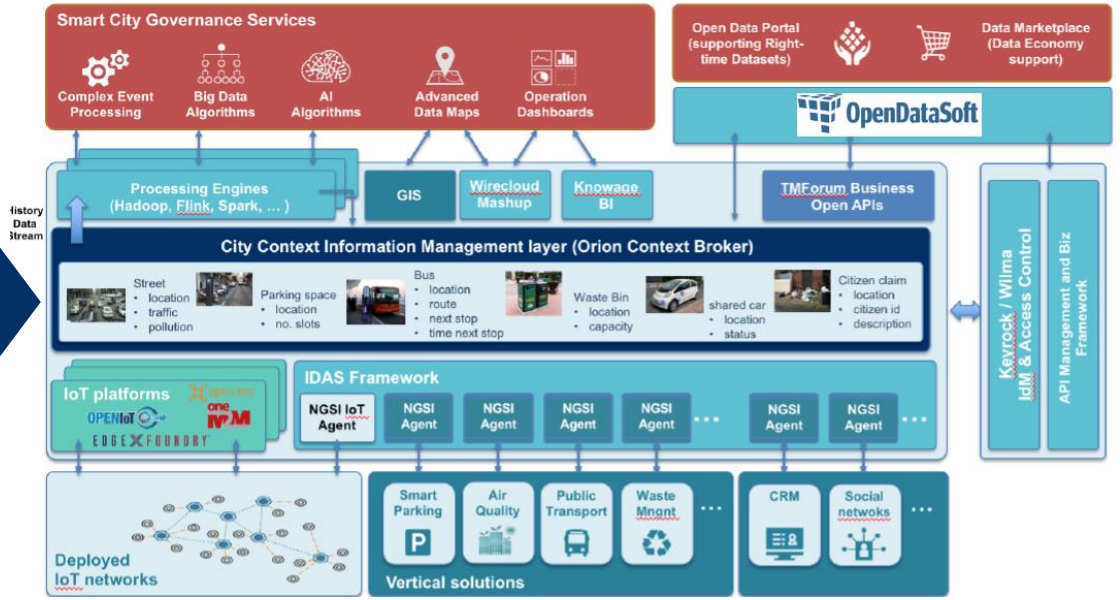
混在するデータ連携基盤は共存できる可能性を模索

サービス上で、複数のデータ連携基盤は共存可能（CPU/メモリの物理リソースは掛かります。）
何を介してデータを連携させるかはサービスの状況次第





FIWAREはContext Broker（データ仲介）が入り
データコントロールを行う。誰が管理するかを
考えて、運用を行う形式が取れる。
Context Broker中心に新しいビジネス策定が可能。

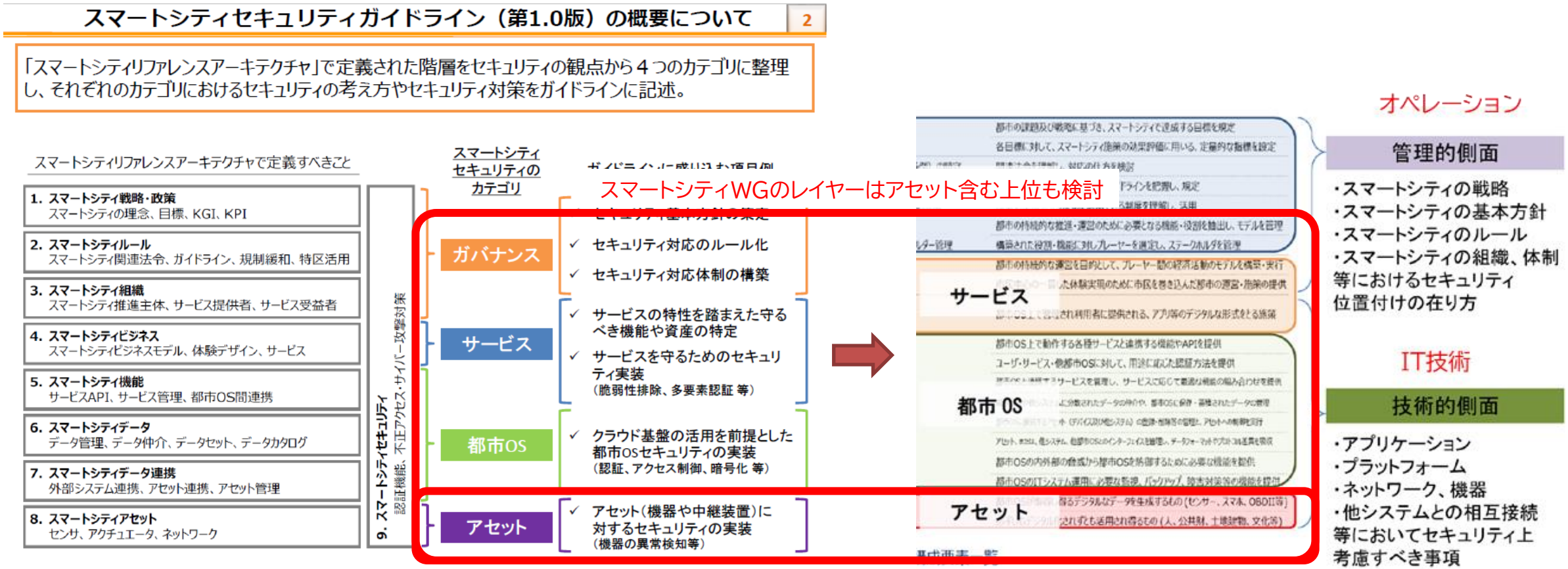


X-Roadは企業間をP to Pで繋ぐモジュール
で、データコントロールは個人の許諾による。
個人が情報を提供することで、新しいビジネス策定

出典：OZ1技術説明資料より

リスクマネージメントにおいて

スマートシティガイドラインもオペレーションと技術に分けて



CCDSのその他ワーキングはアセットが中心でセキュリティの議論を行っております

スマートシティガイドラインも参照しながら

スマートシティ特有の留意点について

3

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

都市OSには色々な団体が参加

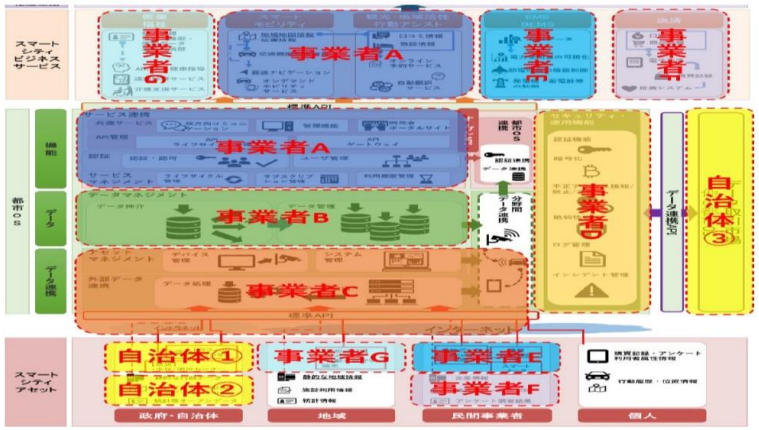


図４－１　マルチステークホルダーのイメージ

パトロール　監査

図４－４　ＳＯＣ／ＣＳＩＲＴの設置

IoTから決済・個人情報まで対応できる組織

自治体で考える領域としては非常に幅広く難しい

日・EUのトラストサービスに関する制度比較

スマートシティをスタートする上でも足りない法律や規制も色々と

4. トラストサービスを巡る状況

4

		ヒト	組織	モノ
【日本】	送信元の確認	電子署名 【電子署名法】	制度無し 日本のこの部分の未定義が課題	制度無し
	非改ざんの確認	タイムスタンプ（民間の認定スキーム）		

		ヒト	組織	モノ
【EU】	送信元の確認	【eIDAS規則】 電子署名	eシール	ウェブサイト認証
		eデリバリー		
	非改ざんの確認	タイムスタンプ		

＜参考3＞ eIDASの概要

7

○ EUでは、電子取引における確実性を確保し、市民、企業の経済活動の効率化を促進するため、2016年7月にeIDAS（electronic Identification and Authentication Services）規則を発効し、トラストサービスに関して包括的に規定

○ パーソナルデータについては、EUがGDPRを制定することにより、国際的なプライバシー保護の潮流をリード。トラストサービスについても、eIDAS規則を発効し、包括的な法的枠組みの整備を先行。

EUにおけるトラストサービスのイメージ

電子署名
○ 自然人が電磁的に記録した情報について、その自然人が作成したことを示すもの

タイムスタンプ
○ 電子データが、ある時刻に存在していたこととその時刻以降に改ざんされていないことを示すもの

ウェブサイト認証
○ ウェブサイトが真正で正当な主体により管理されていることを示すもの

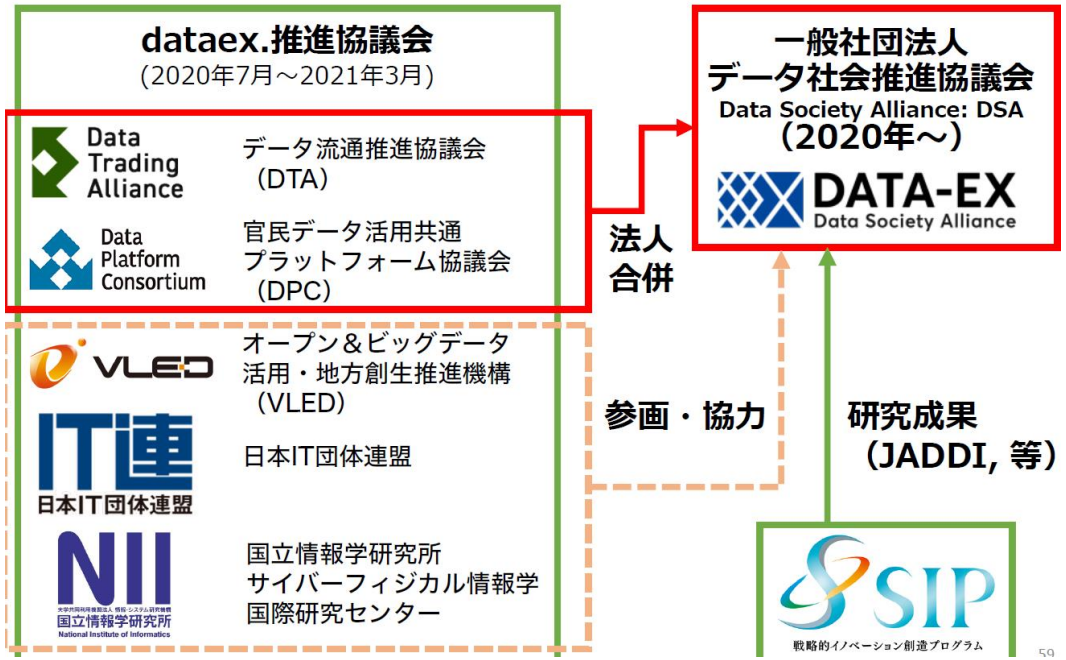
eシール
○ 文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの

eデリバリー
○ データの送受信の証明も含め、データ送信の取扱いに関する証拠を提供するもの

出典:トラストサービスに関する総務省の取組　2019/11/13
10月25日(金)「トラストサービスシンポジウム2019秋@大阪」総務省サイバーセキュリティ統括官室 赤阪晋介参事官による講演の取りまとめ
https://www.dekyo.or.jp/info/2019/11/security/14314/

スマートシティIT基盤に関与している団体

データ連携・標準化を考える団体



セキュリティを考える団体

CSA cloud security alliance SM

CSAJC Japan Chapter cloud security alliance SM

クラウドシステム

CCDS 一般社団法人 重要生活機器連携セキュリティ協議会
Connected Consumer Device Security Council

IoT機器中心

セキュリティ運用の再考

＜ポイント＞

① リスクアセスメント、及びデータライフサイクルを考慮した、自組織およびサプライチェーンに係るセキュリティに関する基本方針を定めると共に、セキュリティ対策基準、責任範囲、リスク許容水準等を整備し、マルチステークホルダー間で適宜共有する。

② 自組織におけるセキュリティ上の役割と責任、情報の管理体制および共有方法等を整備する。

③ 個人情報保護法、官民データ活用推進基本法、GDPR 等の国内外の法令や、それぞれの分野における業法や業界ガイドラインを考慮したルールを整備する。

④ スマートシティ提供を継続する上で自組織及び関係する他組織における依存関係と重要な機能およびレジリエンス（回復）を検討する。

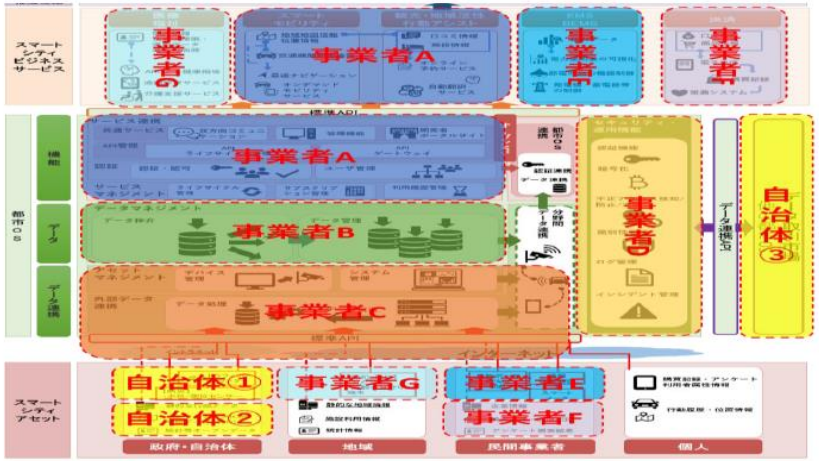
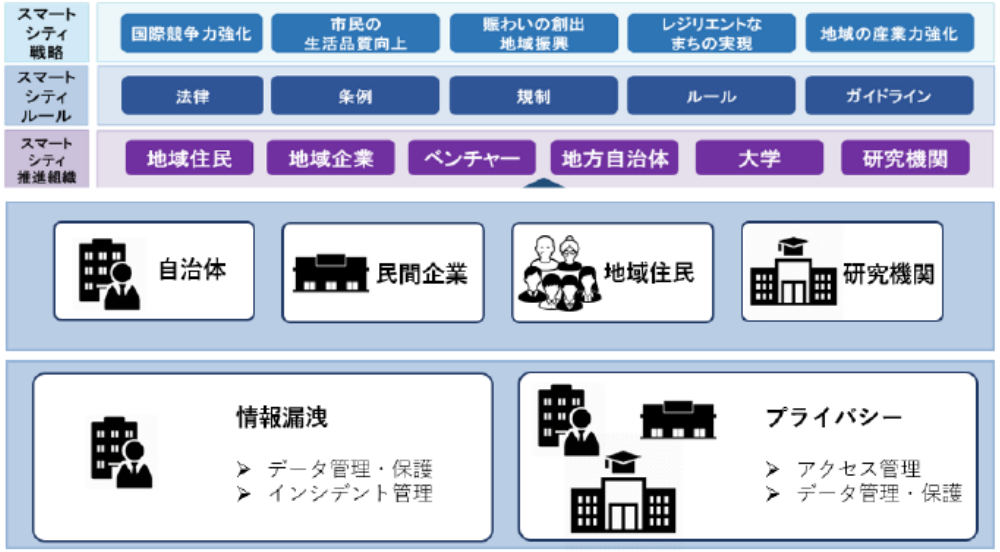


図４－１　マルチステークホルダーのイメージ

仕分けを行いルールやセキュリティ・管理が必要



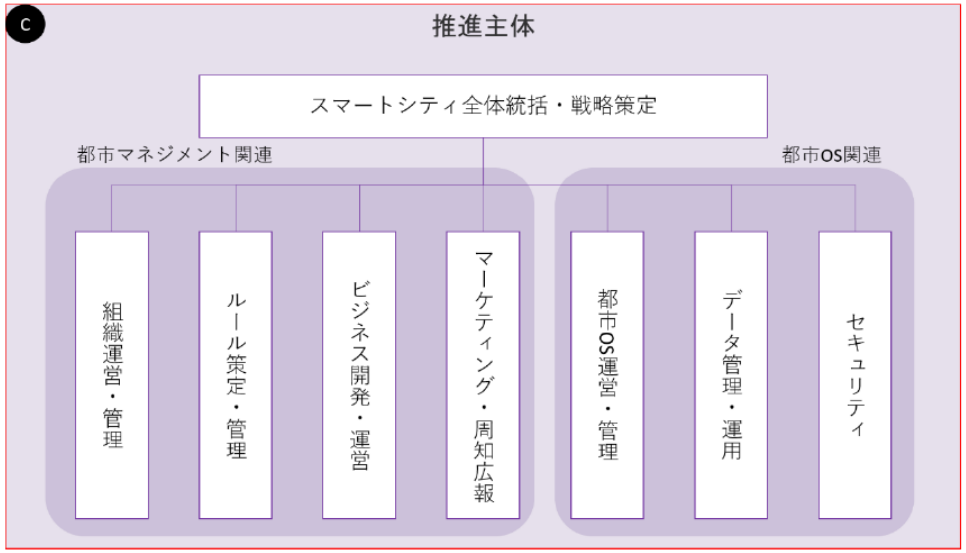
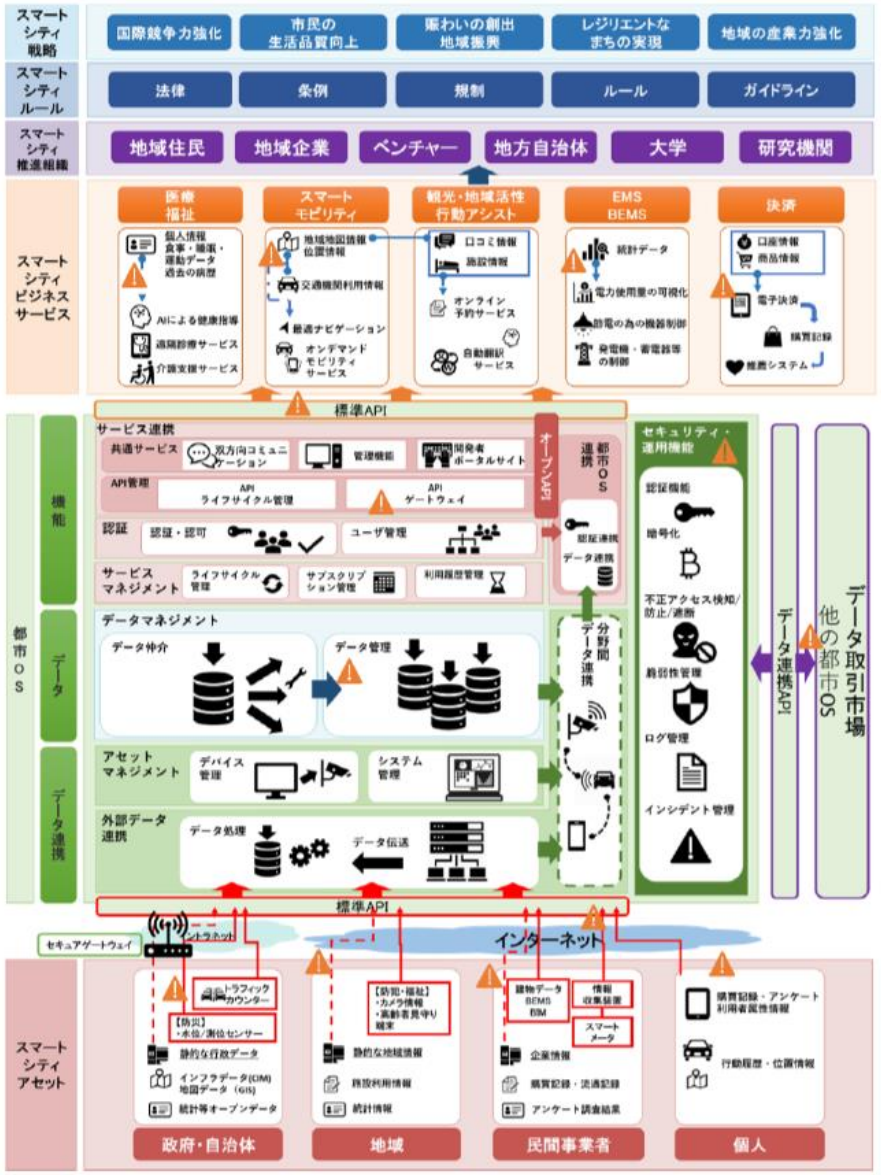


図２－４　スマートシティ組織のイメージ

46

起こりうるサイバーリスク



SOC/SIRTのみでは解決しない

・脅威・脆弱性・運用などリスクも複雑に絡まり整理が困難

↓

スマートシティの責任

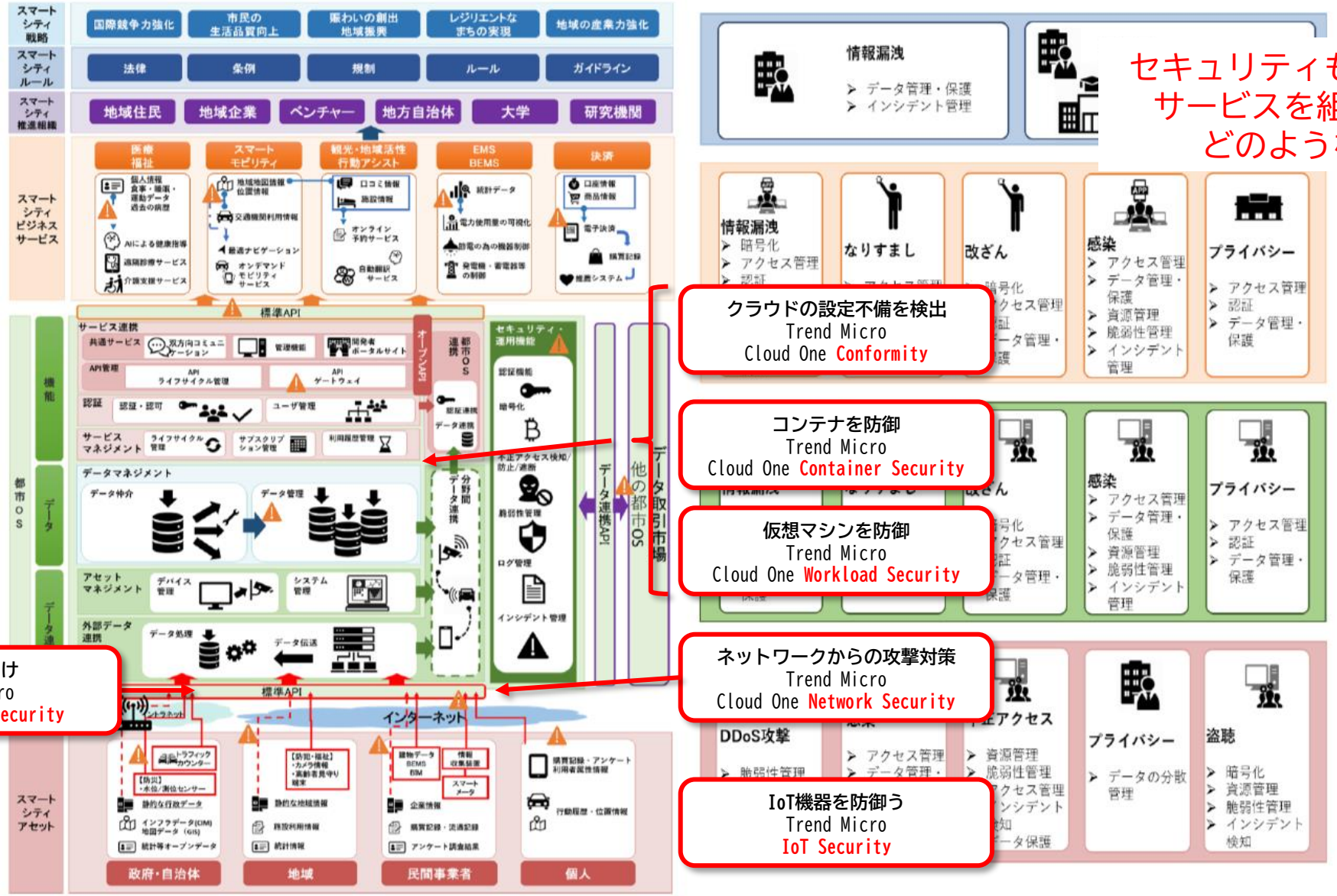
↓

自治体の責任

↓

誰が考えられるの？

セキュリティ対策例（トレンドマイクロ）



セキュリティも1社じゃなく複数のサービスを組み合わせて使うがどのようなサービスが？

クラウドの設定不備を検出
Trend Micro
Cloud One Conformity

コンテナを防御
Trend Micro
Cloud One Container Security

仮想マシンを防御
Trend Micro
Cloud One Workload Security

ネットワークからの攻撃対策
Trend Micro
Cloud One Network Security

IoT機器を防御う
Trend Micro
IoT Security

Local 5G向け
Trend Micro
Moble Network Security

48

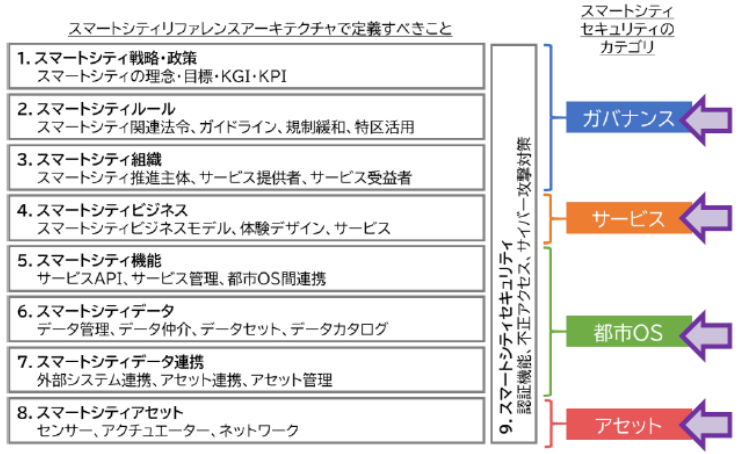
スマートシティセキュリティガイドラインver2

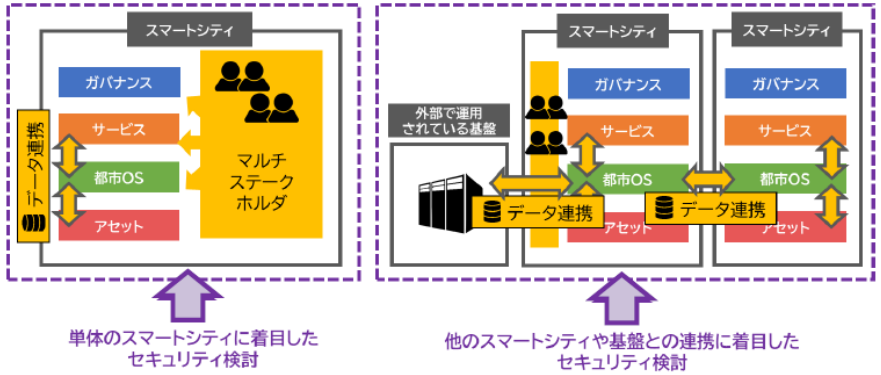
スマートシティセキュリティガイドライン（第2.0版）の概要について　別添1

■「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。





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

4/26にv2がリリース
パブリックコメント募集中

スマートシティセキュリティガイドラインver2

- 法令やセキュリティ上のリスク一覧なども色々と記載されてます

スマートシティセキュリティ導入チェックシート

カテゴリ１ ガバナンス

① セキュリティに関するポリシーの策定

ガバナンス①-1：情報セキュリティ基本方針を策定する
- □ 目的や対象範囲など基本的な事項のほか、セキュリティを担保するための取組方針が記載された情報セキュリティ基本方針を策定する

ガバナンス①-2：セキュリティ対策基準を策定する
- □ 組織体制や情報資産の分類・管理に関する項目のほか、管理的及び技術的なセキュリティ対策等について具体的な遵守事項や判断基準等を定めたセキュリティ対策基準を策定する

ガバナンス①-3：データ取扱い基準を策定する
- □ スマートシティで取り扱われるデータを分類するとともに、適切なデータの取扱いに関する事項や、法令等への対応等を定めたデータ取扱い基準を策定する

ガバナンス①-4：インシデント対応手順を策定する
- □ インシデント対応に関与する関係主体やそれぞれの責任範囲の明確化、連絡体制や連絡先などの整備、対応における判断基準やインシデント対応フロー等のインシデント対応手順を策定する

ガバナンス①-5：事業継続計画を策定する
- □ 障害やセキュリティ事故等が発生した際にどの機能を優先して保護するかといった判断基準や、スマートシティ事業継続のための役割分担、対応手順等を定めた事業継続計画を策定する

ガバナンス①-6：委託先や提携先の評価基準を策定する
- □ セキュリティ管理体制やセキュリティに関する第三者認証の取得有無等、外部委託等を実施する際に求めるべき内容や選定条件などを定めた評価基準を策定する

ガバナンス①-7：リスクアセスメントを実施する
- □ スマートシティの全体構成や守るべき機能や情報資産を踏まえ、リスク評価を実施する

ガバナンス①-8：法令やガイドライン等との整合性を確認する
- □ スマートシティのセキュリティに関するポリシー策定時に、自身のスマートシティにおいて遵守することが求められる法令を把握する。また、それらの法令が遵守できる形でガイドラインを参考としながらポリシーを策定する。

カテゴリ２ サービス

① サービス個別でのリスクアセスメントの実施

サービス①-1：それぞれのサービスにおいてリスクアセスメントを実施する
- □ 個々のサービスにおいて守るべき情報資産や機能を特定した上で、リスクアセスメントを実施する

② 外部からの攻撃等を防ぐセキュリティ対策

サービス②-1：サービスへのアクセス制御を実装、運用する
- □ 外部からサービスに関わるシステムに通信をする場合は、ファイアウォール等を実装し、適切なアクセス制御を実装する

サービス②-2：適切な権限設定を実施し、管理する
- □ 必要な人や役割などに限定した権限設定を行い、アカウントの一覧表を作成し、定期的に棚卸しするなどして適切に管理する

サービス②-3：認証機能を実装する
- □ アクセスした人が本人であるかを確認するための認証機能を実装する

サービス②-4：セキュリティ監視を実施する
- □ IDS や IPS、WAF などを設置し、外部からの不正なコマンドが含まれた通信等のシステムへのサイバー攻撃を監視する

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

サービス③-1：サービスの企画・設計・開発工程における脆弱性を排除する
- □ セキュア設計やセキュアコーディング、サービスイン前のセキュリティテストや脆弱性診断などによってサービスの企画・設計・開発工程における脆弱性を排除する

サービス③-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する
- □ 定期的な脆弱性診断の実施や、継続的な脆弱性情報の収集によって自システムの脆弱性を把握しつつ、構成情報を適切に管理し、それらの情報を元に適切にバージョンアップやセキュリティパッチの適用等の対策を実施する

サービス③-3：運用管理端末へのセキュリティ対策を実施する
- □ システムへ直接アクセスが可能な運用管理端末は、当該端末へのアクセス制御と認証の導入をした上で、ウィルス対策ソフトの導入、OS 等の脆弱性への対応、物理的なアクセス制限等の対策を実施する

カテゴリ３ 都市 OS

① セキュリティに関するポリシーの策定

都市 OS①-1：都市 OS へのアクセス制御を実装、運用する
- □ 外部から都市 OS に関わるシステムに通信をする場合は、ファイアウォール等を実装し、適切なアクセス制御を実装する

都市 OS①-2：適切な権限設定を実施し、管理する
- □ 必要な人や役割などに限定した権限設定を行い、アカウントの一覧表を作成し、定期的に棚卸しするなどして適切に管理する

都市 OS①-3：認証機能を実装する
- □ アクセスした人が本人であるかを確認するための認証機能を実装する

都市 OS①-4：セキュリティ監視を実施する
- □ IDS や IPS を設置し、不正なコマンドが含まれた通信等のシステムへのサイバー攻撃を監視する

② セキュリティに関するポリシーの策定

都市 OS②-1：都市 OS の企画・設計・開発工程における脆弱性を排除する
- □ 都市 OS を構成するシステムの企画・設計・開発等の各段階においてセキュリティを検討・実施する

都市 OS②-2：脆弱性診断や情報収集等で継続的に脆弱性を把握し、対応する
- □ 定期的な脆弱性診断の実施や、継続的な脆弱性情報の収集によって自システムの脆弱性を把握しつつ、構成情報を適切に管理し、それらの情報を元に適切にバージョンアップやセキュリティパッチの適用等の対策を実施する

都市 OS②-3：運用管理端末へのセキュリティ対策を実施する
- □ システムへ直接アクセスが可能な運用管理端末は、当該端末へのアクセス制御と認証の導入をした上で、ウィルス対策ソフトの導入、OS 等の脆弱性への対応、物理的なアクセス制限等の対策を実施する

③ インシデント発生時に備えたセキュリティ対策

都市 OS③-1：外部との通信やデータの暗号化を実施する
- □ 外部との通信やシステムに保存されるデータは十分な強度の暗号アルゴリズムで暗号化を実施する

都市 OS③-2：定期的にバックアップを取得する
- □ システムの構成情報や重要なデータは定期的にバックアップし、災害や復旧を踏まえた保管を行う

カテゴリ４ アセット

① アセットの監視・管理

アセット①-1：アセットの監視・管理を実施する
- □ アセットの死活監視をしたうえで、バージョン情報などの基本的な情報を管理する

アセット①-2：新規の脆弱性情報を把握し、ファームウェア、ソフトウェア等のバージョンアップを適切に実施する
- □ アセットの脆弱性情報を継続的に収集・把握し、適切なタイミングでバージョンアップの対応を行う

② アセットそのものへのセキュリティ対策

アセット②-1：外部との通信や、保有するデータを暗号化する
- □ アセットと外部との通信やアセットで保有するデータは十分な強度の暗号アルゴリズムで暗号化を実施する

アセット②-2：認証機能を実装する
- □ アセットにアクセスする際の認証機能を実装する。パスワードは工場出荷状態でのデフォルトパスワードや容易なパスワードを避け、サービス利用者側でデバイス管理をする場合は、適切なパスワードの設定や管理などの注意喚起をする

アセット②-3：物理的なセキュリティ対策を実施する
- □ デバイスに対する物理的な破壊や盗難からの保護対策を行う。誤動作が起きたとしても人命への影響が発生しないよう、フェイルセーフを考慮した設計をする。また、デバイスを廃棄する場合は物理的に破壊するなど情報漏洩対策を実施する

各ガイドー覧

【Appendix】A　参照すべき法令・ガイドラインの一覧

項番	法令・ガイドライン名称	概要	発行主体	特に参考することが望ましい主体	特に参照することが求められるケース	セキュリティに関する条文・項目	セキュリティ対策を検討する上での参考となるポイント
1	個人情報の保護に関する法律	個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。	-	スマートシティの推進に関わる全ての主体	個人情報を取り扱う場合	・第十九条（データ内容の正確性の確保等） ・第二十条（安全管理措置） ・第二十一条（従業者の監督） ・第二十二条（委託先の監督） ・第二十三条（第三者提供の制限）	個人情報の定義や個人情報取扱事業者が行うべき従業員や委託先の監督について記載されているため、個人情報を取り扱う場合に参照する。
2	不正競争防止法	事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与することを目的とする。	-	スマートシティの推進に関わる全ての主体	営業秘密情報を取り扱う場合	・第十条（秘密保持命令）	不正競争防止法によって禁止される行為、不正競争行為に対しての是正方法が記載されているため、営業秘密情報を取り扱う場合に参照する。
3	官民データ活用推進基本法	官民データの適正かつ効果的な活用の推進に関し、基本理念を定め、国、地方公共団体及び事業者の責務を明らかにし、並びに官民データ活用推進基本計画の策定その他官民データ活用の推進に関する施策の基本となる事項を定めるとともに、官民データ活用推進戦略会議を設置することにより、官民データ活用の推進に関する施策を総合的かつ効果的に推進し、もって国民が安全で安心して暮らせる社会及び快適な生活環境の実現に寄与することを目的とする。	-	スマートシティの推進に関わる全ての主体	官民データを取り扱う場合	・第十条（手続における情報通信の技術の利用等） ・第十一条（国及び地方公共団体等が保有する官民データの容易な利用等） ・第十二条（個人の関与の下での多様な主体による官民データの適正な活用） ・第十三条（個人の関与の下での多様な主体による官民データの適正な活用）	官民データの定義や、官民データを活用していくための基本的施策について記載されているため、官民データを取り扱う場合に参照する。
4	サイバーセキュリティ基本法	サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。	-	スマートシティの推進に関わる全ての主体	-	・第十三条（国の行政機関等におけるサイバーセキュリティの確保） ・第十四条（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進） ・第十五条（民間事業者及び教育研究機関等の自発的な取組の促進）	サイバーセキュリティについて、基本理念、各主体の責務、戦略、施策について記載されている。
5	サイバー・フィジカル・セキュリティ対策フレームワーク	サイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」、様々なつながりによって新たな付加価値を創出する「Connected Industries」における新たなサプライチェーン全体のサイバーセキュリティ確保を目的とする	経済産業省	スマートシティの推進に関わる全ての主体	サービスや都市OSやがクラウドで構築されている場合	第Ⅱ部 ポリシー：リスク源の洗い出しと対策要件の特定 2．リスク源と対策要件の対応関係	「企業間のつながり」「フィジカル空間とサイバー空間のつながり」「サイバー空間におけるつながり」の三層に分類して考える三層構造モデルの定義、及びモデルに基づいたリスクアセスメント、リスクへの対策について記載されている。

【Appendix】B　セキュリティ上のリスク一覧

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	・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 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 CPS.IP-10 CPS.MA-1 CPS.MA-2 CPS.RA-2 CPS.CM-6 CPS.CM-7 CPS.SC-12
（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	・通信路が適切に保護されていない	CPS.DS-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	・早期にセキュリティ上の異常を素早く検知し、対処するような仕組みが自組織のシステムに実装されていない	CPS.AE-1 CPS.CM-1 CPS.CM-5 CPS.RP-1 CPS.PT-1
（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	・サイバー空間との通信開始時に、通信相手を識別・認証していない	CPS.AC-1 CPS.AC-3 CPS.AC-4 CPS.AC-8 CPS.AC-9
（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	・通信相手のエンドポイントから送信されるデータをフィルタリングする仕組みが導入・運用されていない	CPS.CM-3 CPS.CM-4
（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情報を契約前、契約後に確認していない	CPS.SC-2 CPS.SC-3 CPS.SC-4 CPS.SC-6 CPS.SC-7 CPS.SC-8 CPS.SC-12 CPS.SC-13 CPS.SC-14
（監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗難等の後）改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施されたIoT機器によるネットワーク接続・悪意を持った自組織内外のヒトによる不正改ざん・センサーの測定値、閾値、設定の改ざん	・利用している機器に耐タンパー性がなく、物理的な改ざんを防げない	CPS.DS-8
（監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗難等の後）改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施されたIoT機器によるネットワーク接続・悪意を持った自組織内外のヒトによる不正改ざん・センサーの測定値、閾値、設定の改ざん	・定期的に接続機器の完全性を検証していない	CPS.DS-10 CPS.DS-12
（監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗難等の後）改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施されたIoT機器によるネットワーク接続・悪意を持った自組織内外のヒトによる不正改ざん・センサーの測定値、閾値、設定の改ざん	・不正な機器がネットワークに接続されたことを適切に検知できない。	CPS.AM-1 CPS.CM-6
（監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗難等の後）改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する	・盗難等により不正な改造を施されたIoT機器によるネットワーク接続・悪意を持った自組織内外のヒトによる不正改ざん・センサーの測定値、閾値、設定の改ざん	・IoT機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない	CPS.AC-2 CPS.CM-2 CPS.IP-5 CPS.PT-2

【Appendix】C　セキュリティ対策一覧

セキュリティカテゴリ	対策要件ID	対策要件	リファレンスアーキテクチャ
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 サービス 都市OS 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 サービス 都市OS 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 都市OS 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 都市OS 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 サービス 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、想定されるリスクも考慮して、信頼性の高い認証方式（例：二つ以上の認証機能を組み合わせた多要素認証）を採用する	サービス 都市OS
	CPS.AC-7	・データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する（例：開発・テスト環境と実運用環境、IoT機器を含む環境と組織内の他の環境）等してネットワークの完全性を保護する	サービス 都市OS アセット
	CPS.AC-8	・IoT機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ（ヒト／モノ／システム等）との通信に限定する	サービス 都市OS アセット
	CPS.AC-9	・IoT機器やユーザによる構成要素（モノ／システム等）への論理的なアクセスを、取引のリスク（個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク）に見合う形で認証・認可する	サービス 都市OS アセット
AE:異変とイベント	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する	ガバナンス サービス 都市OS アセット
	CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える	ガバナンス
	CPS.AE-3	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する	ガバナンス 都市OS
	CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する	ガバナンス
	CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める	ガバナンス
AM:資産管理	CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する	サービス 都市OS アセット
	CPS.AM-2	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める	ガバナンス サービス 都市OS
	CPS.AM-3	・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する	ガバナンス サービス
	CPS.AM-4	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する	ガバナンス

どこから手を付けるか？→スマートシティのサービスと対比して、重要度の高いものから対応

リスクマネージメントとアセスメント(重要度の高さ)

情報セキュリティ

脅威・脆弱性・データのアセットにより、対策が変ります。
すべてにセキュリティコストを掛けると、コスト面でも運用面でもシステムが使えないものになります。

各分野を整理し、適切にセキュリティ対策を考え、運用していく事でスマートシティの安全性が担保されるのでは？

4.1.2 リスクアセスメント

4.1.1 で示したモデル化された開発対象となる IoT 機器・システムに対してセーフティ、セキュリティの観点からリスクアセスメントを行う必要がある。図 4-1 は、「つながる世界の開発指針」で示しているリスクアセスメント（守るべきものの洗い出し～リスク評価）の手順である。

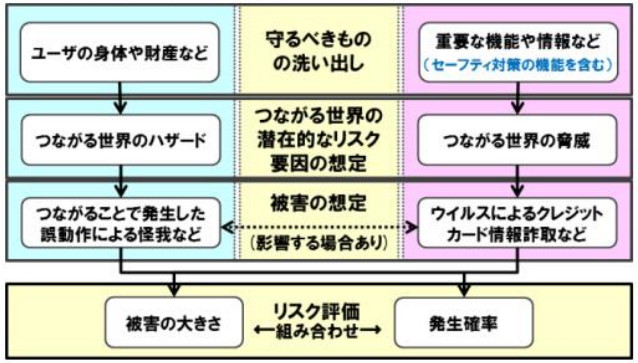


図 4-1 リスクアセスメントの手順

	ケース	ニーズ	機器	CCDS的考え方
レベル4	人命に関わるケース：緊急災害／防犯／見守り	安全（防犯、防災） 安心（見守り、健康）	電子錠・センサー （人感・開閉etc）	レベル3
レベル3	財産に関わるケース：緊急災害／防犯／節電/エコ	省エネ（エネルギー）	HEMS ガスメーターetc	レベル2
レベル2	快適性に関わるケース：空調／日よけ／湿度	快適性 （暑さ寒さ、静けさ、換気）	家電・センサー （温湿度、照度etc）	CCDS共通要件レベル1
レベル1	エンターテイメントに関わるケース：ゲーム／AV機器／趣味	利便性 （生活・趣味）	家電・ゲーム 趣味用品etc	CCDS共通要件レベル1

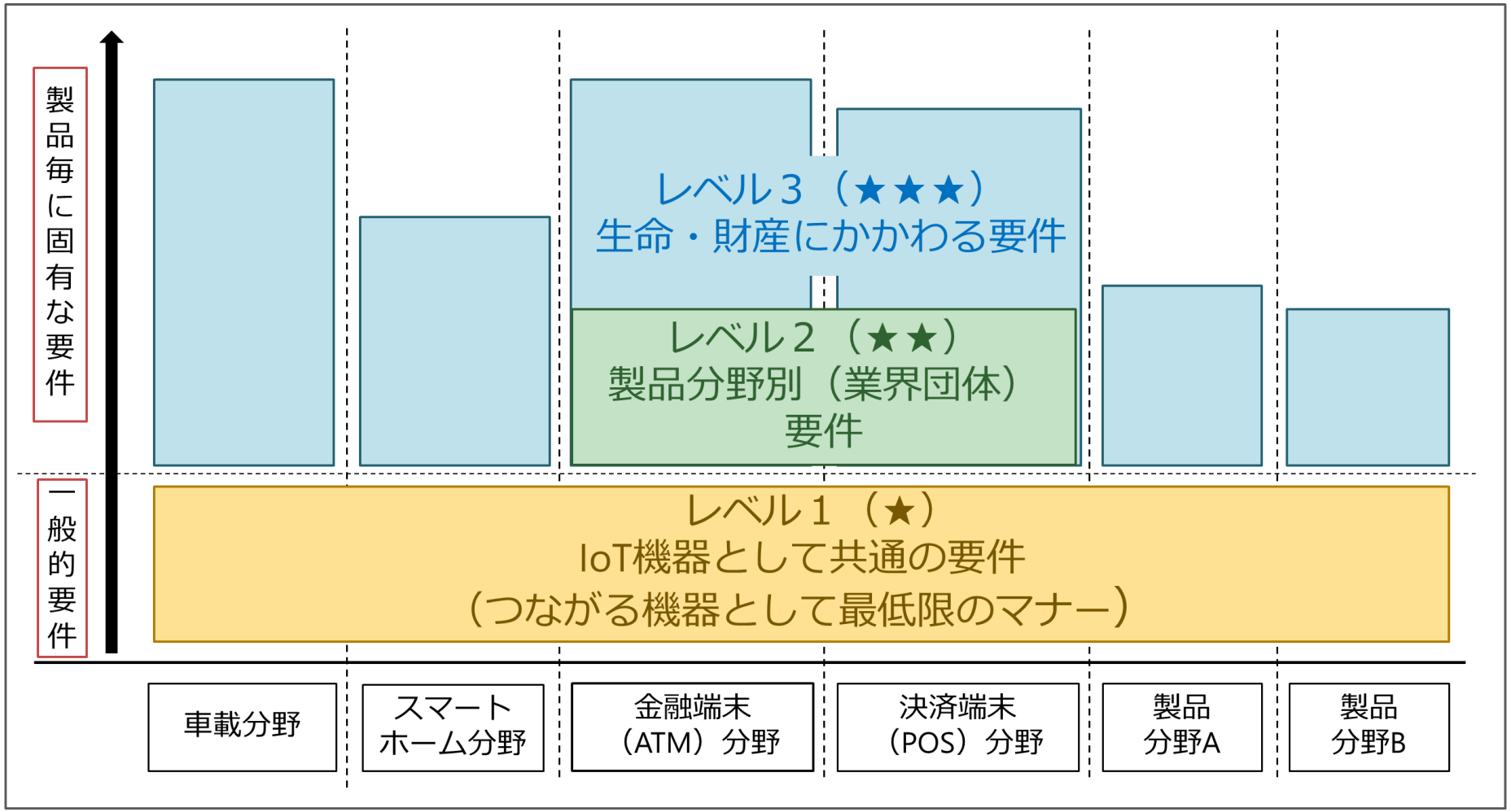
※（参考）「つながる世界の開発指針」の実践に向けた手引き(IPA)

サーティフィケーションプログラム

サーティフィケーションプログラムのレベル構成

・消費者にも分かりやすいよう、★の数でセキュリティ対策のレベルを示す３階層のモデルを提示

・まずはレベル１の共通要件から、サーティフィケーションプログラムをスタートします



「通信キャリアやサービサー視点から見たIoTセキュリティ要件」

1．ヒトの管理

・オペレーターの本人性・信頼性を確認する手段
・オペレーションミスを早期発見する手段
・オペレーターの不正行為を早期発見する手段

2．エンドデバイス（センサー**/アクチュエーター**）**の管理**

・個体の信頼性確認**/すり替え検知をする手段**
・**CPU・メモリー・電源などの状態を確認する手段**
・エンドデバイスの動作が平常か異常かを見分ける手段
・機器の個体差や故障による誤差・異常値を補正する手段

3．制御システムの管理

・接続されている装置の構成を把握する手段
・接続対象機器の脆弱性を調べる手段
・脆弱性のある装置を監視し攻撃から守る手段
・設定値の正常**/異常を検知する手段**
・ソフトウェアのバージョンを把握する手段
・多様なプロトコルを理解し通信内容を解析する手段
・危険な制御コマンド**/パラメータ設定を検知する手段**
・異常検知・解析のための通信ログ・動作ログを収集する手段

4．通信端末（**IoTゲートウェー**）**の管理**

・接続を要求するデバイスの信頼性を確認する手段
・通信端末の型式やバージョンを把握する手段
・通信端末のセキュリティホールを調べる手段
・**SIM/eSIMの信頼性を確認し認証する手段**
・ソフトの脆弱性やバグを発見する手段
・ソフトウェアを強制的に更新できる手段
・ハードの故障を早期発見する手段
・設定変更・改造・差換えを検知する手段
・盗難・紛失を検知する手段
・怪しいデバイスの接続を拒否**/強制切断する手段**

5．ネットワークの管理

・大量のデバイスを同時に接続し通信させる手段
・回線の契約者・利用者を正しく登録・変更する手段
・通信量（トラフィック）の集中を防ぎ分散する手段
・トラフィック輻輳時に不急の通信を規制できる手段
・重要なデータを確実に伝送し保存できる手段
・データの送信エラーや損失を検知し再送する手段
・誤送信や迷惑送信を防ぐ手段
・不審な通信を遮断する手段

6．システム全体の管理

・どの国**/地域の安全基準を適用すべきかを決める手段**
・システム構築プロセスの安全を確認する手段
・システム運用プロセスの安全を確認する手段
・システム構成の最新状態を正確に把握する手段
・システムの動作が平常か異常かを見分ける手段
・システムの稼動状態を利用者**/運用者に見せる手段**
・システムの異常を検知し原因を推定し切り分ける手段
・セキュリティ管理サービスレベルに応じて利用料金を変えられる手段
・システムに対する既知の攻撃を発見し、対処策を提案する手段
・システムに対する未知の攻撃を検知し、原因と対策を推定する手段

7．1 異常（不具合・事件事故・災害）発生時の対策

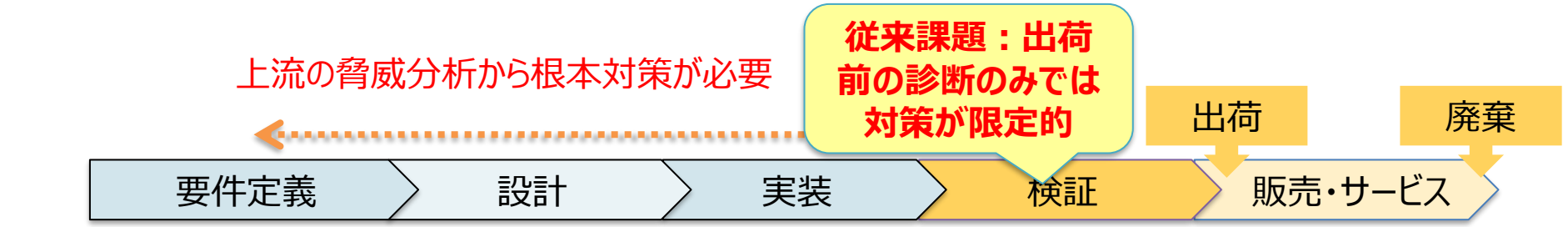
・異常が発生した箇所（ハード**/ソフト/データ**）**を特定する手段**
・原因解析に必要なデータをアナリストに見せる手段
・異常発生の原因を解析・推定する手段
・異常を放置した場合の被害を想定・算定する手段
・発生事象と推定原因を運用者や利用者へ知らせる手段
・サイバー攻撃発生時に犯人を追跡する手段
・マルウェアの拡大・蔓延を最小限にとどめる手段
・妨害パケットを遮断する手段
・通信ゲートウェーを強制的に停止**/再起動する手段**

7．2 異常（不具合・事件事故・災害）発生時の対策

・国**/地域の安全基準に応じて必要な対処法を判断する手段**
・異常発生の状況を政府や関係機関に報告する手段
・事件発生時に警察や軍に開示してよい情報の範囲を決める手段
・被害に対する賠償の責任者を明確にする手段
・セキュリティ対策済ソフトを端末に自動配布・実装する手段

セキュリティ開発プロセスと活動イメージ

Security by Designに基づき、要件定義～保守までセキュリティ品質を確保
→ 製品ライフサイクル全般で脆弱性排除、セキュリティ対策にかかるコストを削減



方針	混入防止（脆弱性を作りこまない）			検出除去（脆弱性を検知し除去）	保守・改修（出荷後の対応）
対応	**脅威分析、** 脅威分析ツール	**脆弱性分析、** セキュリティアーキ設計・機能開発	**セキュアコーディング対応、ハードウェア攻撃対策、** 組込み対応セキュリティ機能群	**脆弱性評価、** 脆弱性診断	インシデント対応 SIRTコンサル

太字は製造時のセキュリティ対策基準の対応項目

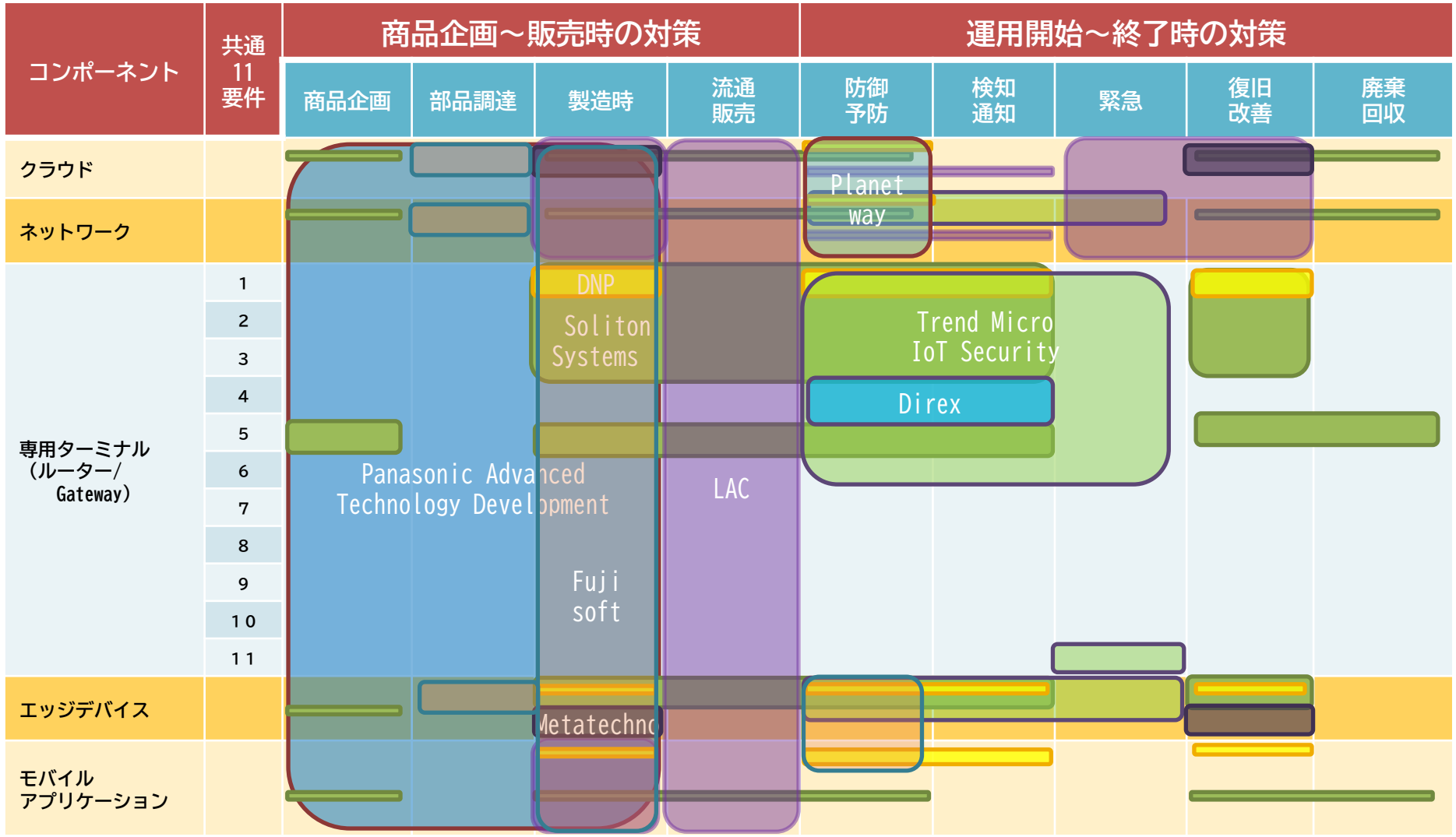
想定される脅威の抽出

- STRIDEにCCDSで脅威を追加したモデル

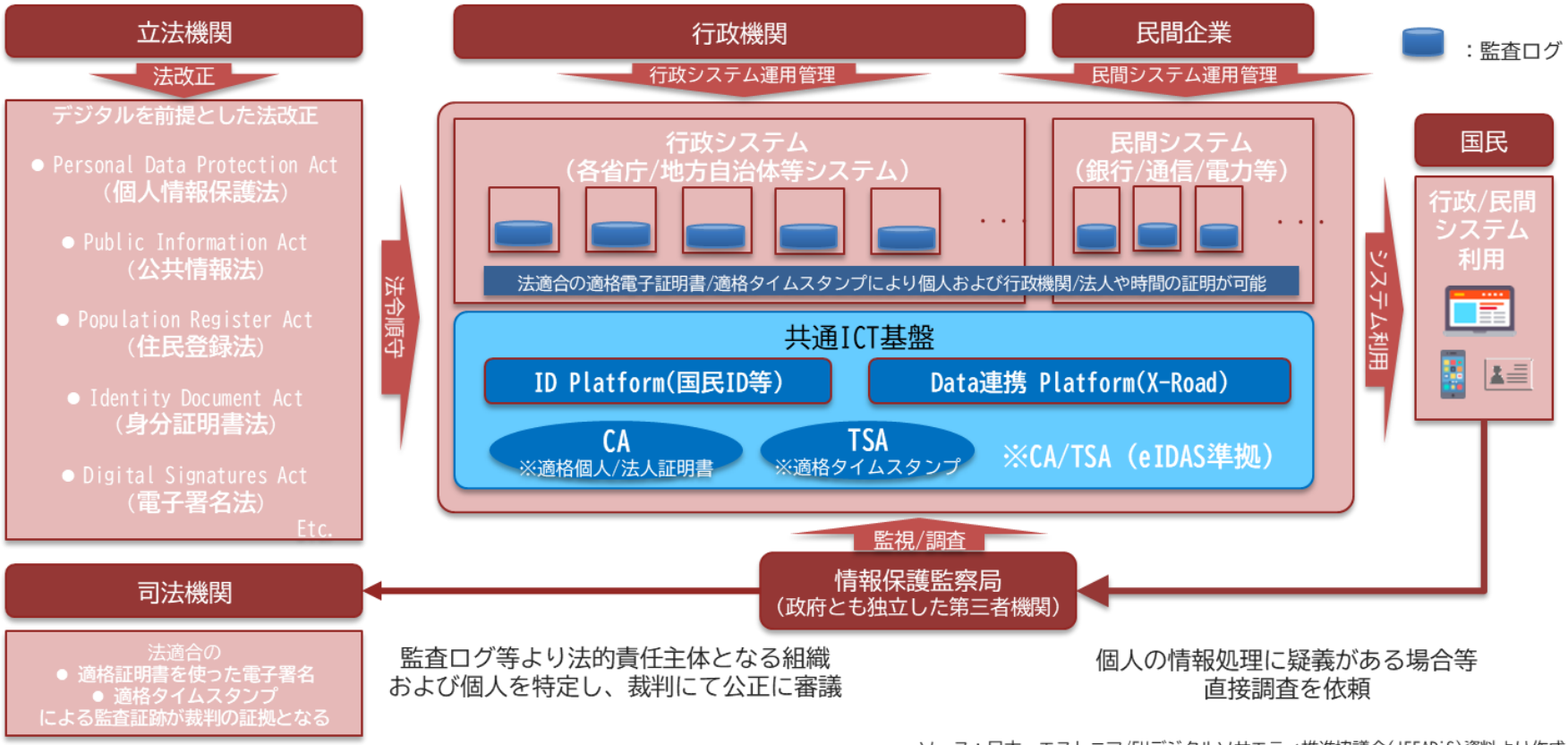
脅威名称	英語表記	説明
なりすまし（偽装）	Spoofing	コンピューターに対し、他のユーザーや機器を装うこと
データの改ざん	Tampering with Data	権限なしでデータを改ざんし、データの完全性を失わせること
否認	Repudiation	ユーザーがあるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
情報の暴露(漏洩)	Informal Disclosure	アクセス権限を持たない個人に情報が公開されること
サービス不能(DoS)	Denial of Service	正規のユーザがサーバやサービスにアクセスできないこと ※(D)DoS攻撃やジャミングによるサービス妨害など
権限の昇格	Elevation of Privilege	権限のないユーザーがアクセス権限を得ること
不正アクセス	Unauthorized access	アクセス権限を持たない者にアクセスされること
マルウェア感染	Malware infection	他の機器への汚染源になる。ランサムウェアなどにより業務妨害を受けること
踏み台	Stepping stone attack	他の機器へ不正アクセス等を行う際の中継地点として使用されること
不正改造(HW/SW)	Tampering with device	不正（違法）なハード、ソフトウェアの改造により、内部データを抜き取ったり、脆弱性の要因を組み込まれること
未知の脆弱性	Unknown Vulnerabilities	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性のこと

CCDS会員企業 セキュリティ技術を提供

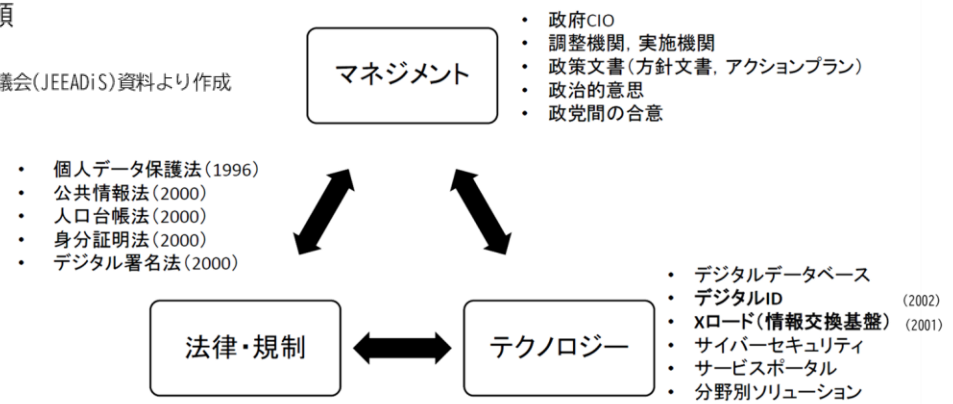
CCDSの各企業が提供している技術マッピング



スマートシティ参照するエストニアICTのガバナンス体制



ソース：日本・エストニア/EUデジタルソサエティ推進協議会(JEEADiS)資料より作成

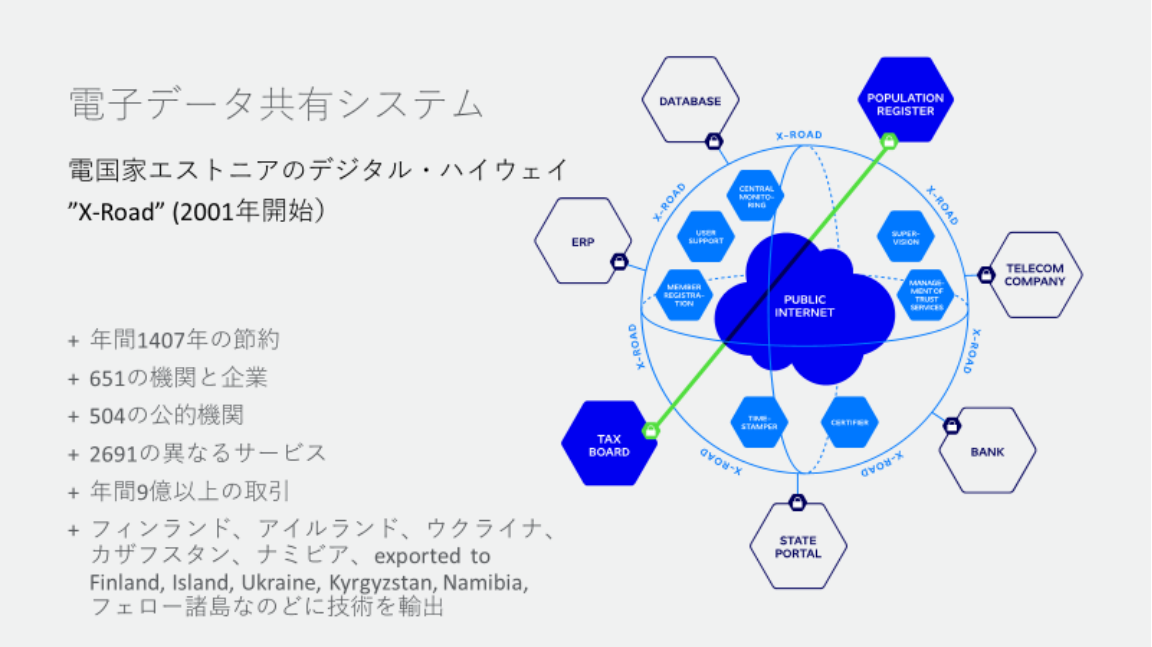


ポストエストニアの勘違い

エストニアは国民IDとX-Road(データ連携基盤)から成り立つデジタル国家として有名ですが、、、

お金のある自治体の解決方法

エストニアみたいな国民IDがあれば全てが出来る、マイナンバーカードもそうなれば、マイナンバーカードは難しい、「自治体IDを作ろう」と言う動きが・・・



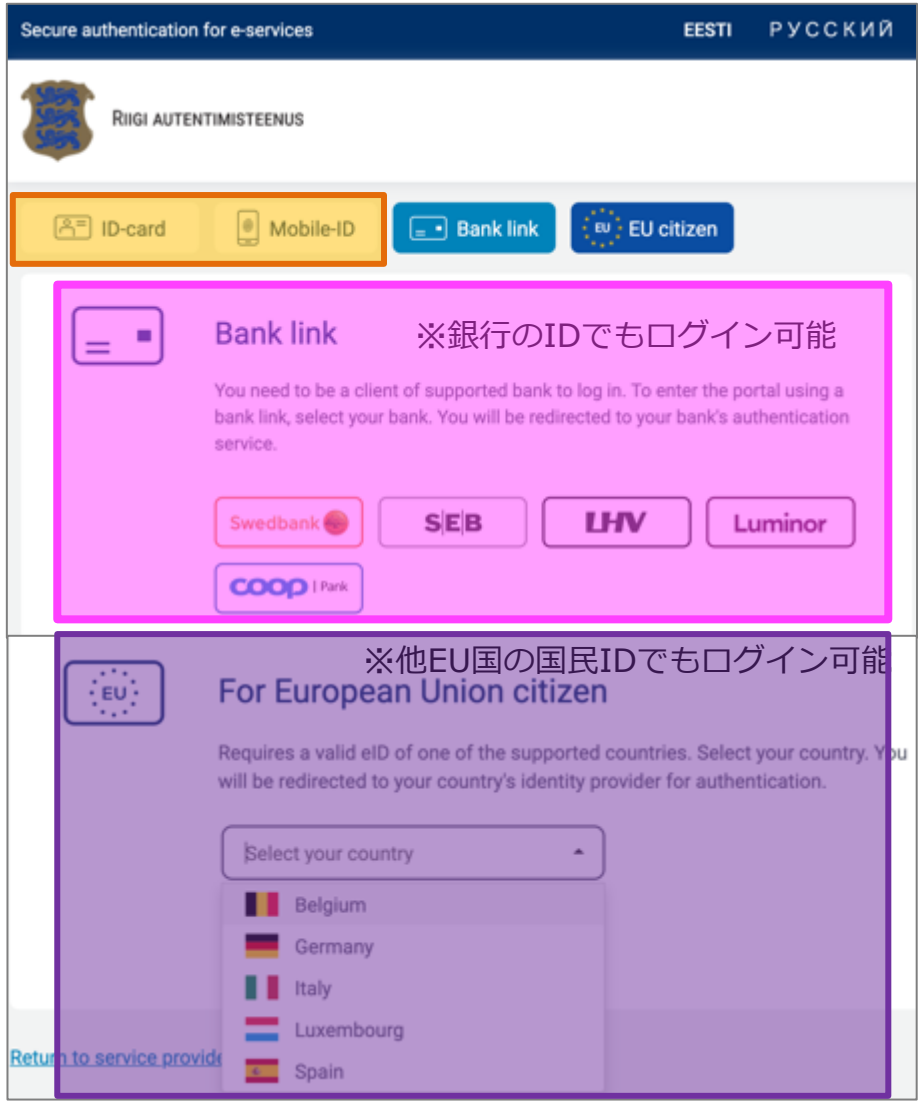
エストニアは国民IDとX-Road(データ連携基盤)が対になり構成されている点は非常に強力なシステムですが、利用は必ずしも国民IDではない！

如何に**本人確認済みIDを信頼の源泉**にするかである。エストニアではマルチIDが基本です

X-Roadは超汎用APIで一度インストールするとP to Pでデータベースを繋げる良いサービスだが、IoT機器には入らない(Xeon 2GHzクラス必要)

エストニア マルチID認証の事例（行政機関）

国民ポータルログイン画面

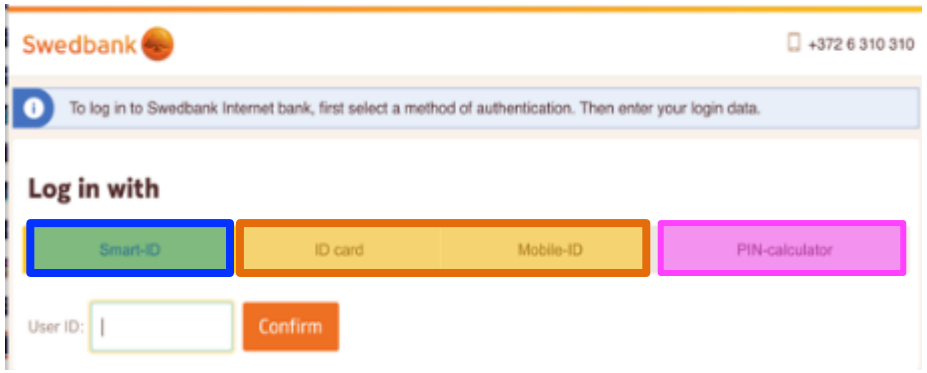


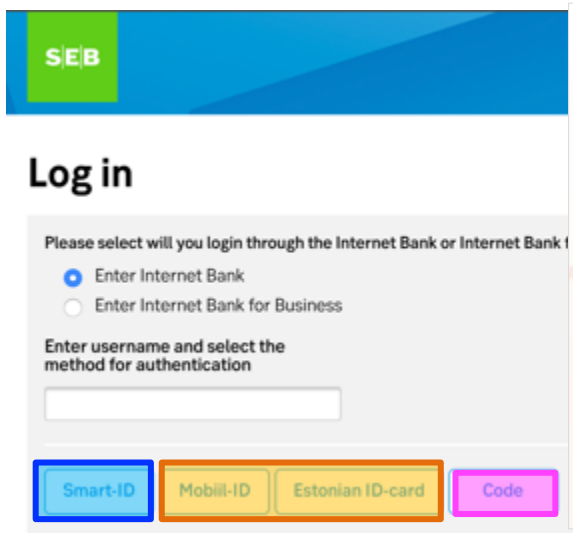
e-Tax ログイン画面

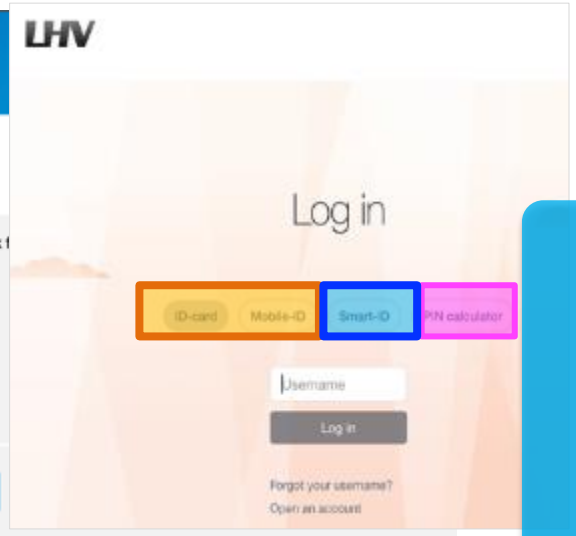
60

エストニア　マルチID認証の事例（民間企業）

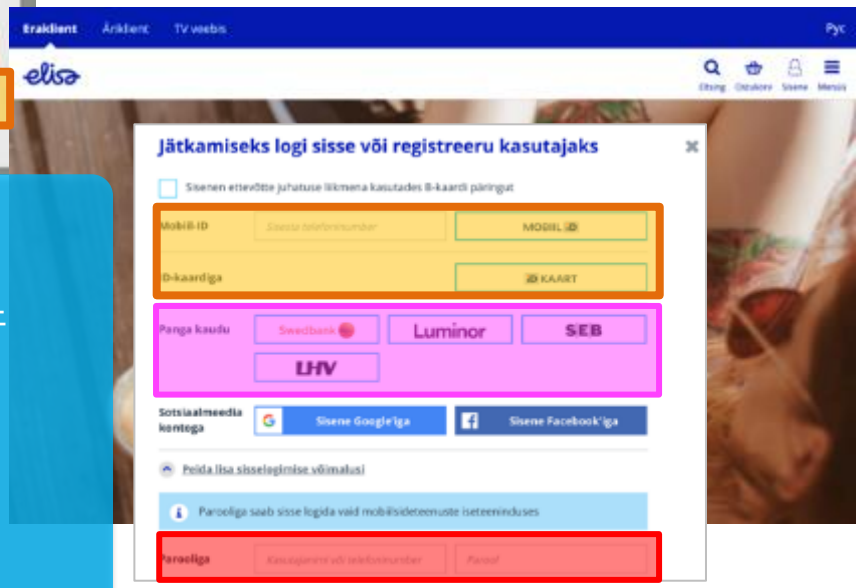
銀行 ログイン画面







通信会社 ログイン画面



政府発行の国民ID

Smart-ID:民間発行のユニバーサルID

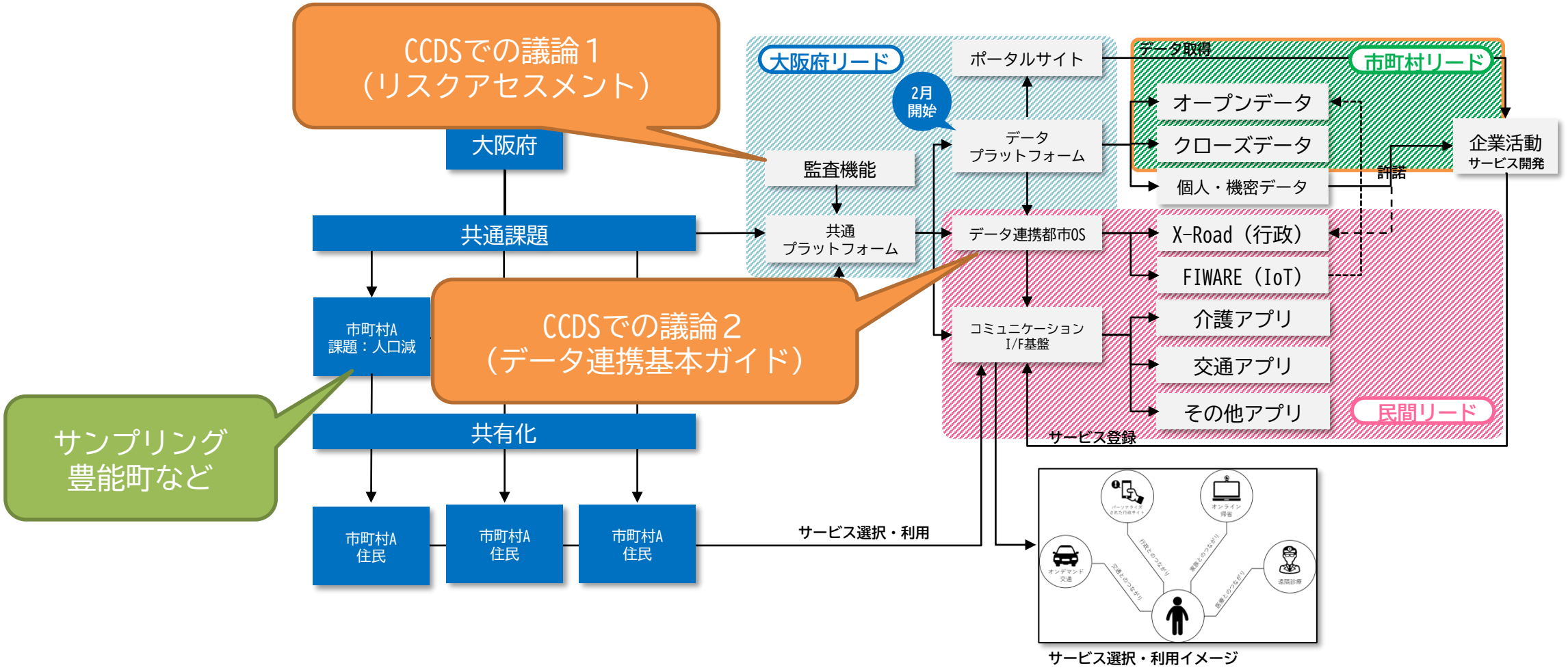
銀行のID

独自ID

61

改めてスマートシティWGの活動

多くの自治体にはIT専任者がいなかったり、部署が無かったりします。
各省庁からも色々なガイドは出るが、読んでも何からすれば、どうすればが分かりにくく、スマートシティが遠く感じられます
スマートシティWGは、省庁のガイドラインで分かりずらい部分を整理して、運用できるように組み上げて行きたいと思います



IT基盤を考える

一番ファンクションが複雑な分野はデータ連携基盤

その他データ連携基盤保有企業

富士通：Virtuora DX
　　Human Bridge（医療）
東芝：ifLink
TIS:　FIWARE
富士ソフト：FIWARE＋X-Road
HULFT：DataSpider
ユニシス：　Dot to Dot

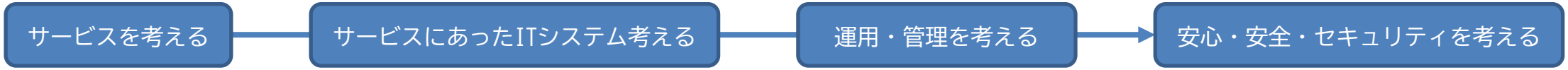
以外にも色々な企業が参加・・・

都市OS　CISCO　HITACHI Inspire the Next　NTT西日本　NEC　FUJITSU　uhuru　OBAYASHI　ITbook　HEROZ JAPAN　データ連携基盤　SmartDrive　MULTISOUP　Nefrock　MORGENROT　DASSAULT SYSTEMES　21　JTB

データ連携比較

自治体サービス側がどのようなIT基盤を用意すればよいのか分かりやすく整理(ガイド)をする為に

企業側の視点より利用者側の視点で分かるように作成



提供元企業	OZ1	NTT	Hitachi	NEC	Panasonic	Fujitsu
製品名						
製品区分						
許諾ベースの個人情報						
許諾操作						
データの扱い						
データ可用性						
リアルタイムデータ						
API						
スケーラビリティ						

データの種類と着手の容易度

着手の容易度

① 【行政】のオープンデータの徹底 → 企業等が自主的に利用

② 【行政】の都市系データ(クローズ含む)の利活用
③ 【民間】の都市系データとの連携強化(掛け合わせ)
④ 【個人】の情報を含む全データ利活用(データポータビリティ)

大学、研究機関、企業等と何らかの契約を結び、サービスに繋げる

リアルタイムデータ

		人に関するデータ		都市に関するデータ		
行政のデータ	① オープンデータ	【統計データ】 ・世帯、人口、年齢 ・出生、死亡、婚姻 ・健康、衛生、福祉 ・収入、貯蓄、消費 ・治安、防災、災害 ・観光、外国人　等	【調査結果データ】 ・人口動態調査 ・景気動向調査 ・学力テスト調査 ・健康状況調査 ・生活保護調査 ・住民アンケート　等	【記録データ】 ・インフラ老朽化 ・パーソントリップ ・住宅・土地調査 ・公共施設、観光施設 ・避難所、無線LAN ・ハザードデータ　等	【リアルタイムデータ】 ・河川防災情報 ・防災カメラ ・道路渋滞情報 ・環境観測データ ・天候データ　等	行政努力 ※多くは公表済
	クローズデータ	【生データ／個人情報データ】 ・上記の統計や調査の生データ(元データ) ※公表を前提としていないデータ ・住民からの申請、相談、問い合わせデータ ・保健所、児童相談、生活保護等の対応データ ・健診データ、レセプトデータ、感染症データ　等		【生データ】 ・上記記録データの生データ(元データ) ※公表を前提としていないデータ	【リアルタイムデータ】 ・水道・下水道利用 ・消防・救急位置 ・交通管制データ ・公用車GPS ・公用車ドラレコ	規制緩和
個人のデータ 民間のデータ		【記録データ】 ・健康データ ⇒電カルテ、お薬手帳 ・経済活動データ ⇒売上、雇用 ・金融データ ⇒預貯金、資産	【リアルタイムデータ】 ・健康データ ⇒バイタルデータ ・移動データ ⇒渋滞、位置情報 ・購買データ ⇒POSデータ	【記録データ】 ・デジタルマップ ・駅・商業施設情報 ・観光文化情報 ・イベント情報 ・ビルメンテナンスデータ	【リアルタイムデータ】 ・GPS情報 ・モバイル空間統計 ・公共交通位置情報 ・防犯カメラ(民) ・センサー情報	個人情報

② ③

自治体が持つ公的データの代表例

人・企業系

【個人の身体に関するデータ】

種別	分野	内容
健診系	乳幼児健診	身長、体重、胸囲、頭囲、心音、反応 等
	学校健診	身長、体重、視力・聴力、尿、歯、栄養 等
	後期高齢者健診	問診、血圧、身長、体重、BMI、血液 等
	特定健診	既往歴、BMI、血圧、血液、指導レベル 等
医療系	レセプトデータ	傷病、医学管理、投薬、注射、検査 等
	電子カルテ	病名、処置、手術、投薬、検査、画像 等
	臨床検査データ	血液、血清、尿、腎機能、内分泌 等
介護系	要介護認定	身体機能、生活機能、認知機能 等
	介護記録	食事、移動、排せつ、就寝、サービス利用 等
	介護レセプト	サービス内容、回数、医療、特定疾患 等

【自治体に記録(蓄積)されるデータ】

種別	分野	内容
窓口	総合相談	相談先の問い、苦情、通報、各種相談 等
	行政手続き	マイナンバー、住民票、引っ越し、水道 等
	社会福祉相談	高齢介護、児童相談、生活保護、雇用 等
統計	基幹統計	国勢調査、経済センサス、住宅土地統計 等
	健康医療	公衆衛生、健康づくり、福祉計画 等
	産業・企業	観光統計、景況観測、消費者指数 等

都市・モノ系

【まち系データ】

種別	分野	内容
インフラ	道路	交通量、信号、道路構造、老朽化 等
	河川	水位(センサー)、流量、高低、整備 等
	公園	施設、駐車場、利用形態、利用状況 等
	水道・下水道	使用量(センサー)、使用頻度、老朽化 等
土地	都市計画	区域区分、用途地域、建蔽率、容積率 等
	地図	デジタルMAP、ハザードMAP、観光MAP等
	地価	地価公示、路線価、固定資産税評価額 等
建物	住宅	種別、構造、規模、密集市街地、老朽化 等
	公共施設	種別、構造、利用頻度、付属物、老朽化 等
	商業施設	種別、構造、交通接続、利用状況 等

【安全・安心系データ】

種別	分野	内容
防犯	防犯カメラ	街頭カメラ、施設カメラ、ドラレコ 等
	防犯情報	ひったくり、不審者、痴漢、自転車盗 等
	刑法犯認知	空き巣、傷害、暴行、強盗、殺人 等
防災	防災情報	震度、津波、洪水、土砂、避難所 等
	災害予知情報	台風、津波、雨量、土砂、洪水、竜巻 等
	消防・救急情報	火災状況、救急状況、救命状況 等

ご清聴ありがとうございました。

一緒にガイド検討頂ける企業は随時募集中です