スマートシティ IoT における
セキュリティ要件の提言

オープンガバメント・コンソーシアム

サイバーセキュリティ分科会

スマートシティ IoT におけるセキュリティ検討 WG

2017 年 7 月

はじめに

平成 28 年の「世界最先端 IT 国家創造宣言」では、「一億総活躍」「地方創生」「国土強靭化」などの諸問題の解決に IT を利活用する取り組みの強化が謳われている中、現在は、家電、事務機器、医療機器、自動車、産業機器など、様々な「モノ」が繋がる「モノのインターネット(IoT)」が急速に広まりつつある。IoT により、我々の生活は増々便利になっていくが、また、IoT 機器から収集されるデータ類を利活用することで、新たな産業の創出等、更なる経済発展も期待される。

そのような状況で、自治体等が提供する IoT システムやサービスから成る「スマートシティ」の取り組みは世界の各地で始まっているところであるが、さらに促進していくためには、サイバー攻撃によるプライバシーへの侵害等を想定した、セキュリティ対策が喫緊の課題である。

そのため、今般、OGC サイバーセキュリティ分科会にて「スマートシティ IoT セキュリティ検討ワーキンググループ」を立ち上げ、セキュリティ要件を提言としてまとめたので、今後のサービスの創出に役立てて頂きたい。

一般社団法人オープンガバメント・コンソーシアム
会長　須藤 修　東京大学大学院情報学環教授

目次

1　要旨

都市の様々な情報を収集し、その情報を利活用することにより、市民の健康促進や環境に優しい都市作り等を実現するスマートシティ IoT は、これからの都市計画・運営に必須である。しかし、利便性の一方で、そのようなネットワークで接続されたシステムは、サイバー攻撃のリスクにさらされている。

サイバー攻撃に関して、一般的な IoT のセキュリティ課題は様々な報告書で取り上げられているが、スマートシティ IoT についての分析は行われていない。安全なスマートシティ IoT を実現するために、本 WG では、国内外のスマートシティ IoT のプロジェクトを分析し、スマートシティ IoT のセキュリティ課題と、複数の IoT システムが連携した際のセキュリティ課題を整理した。それらの課題を解決し、安全なスマートシティを実現するために、技術面・運用面のセキュリティ要件に基づいた以下の提言を行う。

個々の IoT システムにおけるセキュリティ要件

- IoT 機器の成りすまし、改ざんに対する防止・検知・除去機能をシステムとして具備すること
- データ漏えい、改ざんの防止機能、データトレーサビリティ機能をシステムとして具備すること

複数システム連携時におけるセキュリティ要件

- システム間の認証連携やデータトレーサビリティ、システム横断的なアクセス制御の仕組みを具備すること
- システム横断的なシステムモニタリング機能、セキュリティ運用・監視体制をもつこと

2　国内外の動向調査・分析と、日本のスマートシティ IoT の定義

2.1　　スマートシティ IoT の定義

スマートシティは様々な定義がされているが、基本的には ICT を用いて都市を効率化することである。「米国におけるスマートシティに関する取り組みの現状」[1]では、スマートシティの種類を以下の８種類に分類している。

- 行政サービス
- 交通システム
- スマートヘルス
- セキュリティ
- スマートビル
- スマートエネルギー
- インフラ
- ネットワーク基盤

スマートシティは多岐に渡るため、本報告書では、自治体が提供する IoT システムやサービスを対象とし、運営主体が自治体ではない IoT は対象外とする。例えば、産業制御システム、スマートメーター、車車間通信などは対象外とする。

2.2　　スマートシティの事例

2.2.1　　アルゼンチン・ティグレ市

アルゼンチンのティグレ市は、大規模な不動産ブームによって、過去 20 年で人口が大幅に増えている。また、娯楽産業（ミュージアム・テーマパーク・カジノ等）が発達しており、国内外から観光客が訪れている。このような状況の中、治安の維持は大きな課題であった。

ティグレ市と NEC は、2013 年に覚書を締結し、パブリックセーフティに関する技術を導入している。具体的には、街中に 640 台のカメラを設置し、事件や事故を防止するプロジェクト[2]が進められている。これらのカメラからの画像を用いて、顔認識による行方不明者や犯罪者の捜索や、行動検知技術による不審者（徘徊者）の検知やバイクの二人乗り検知を行っている。これらの情報は、専用のオペレーションセンタと危機管理室に集約されるため、都市の状況の把握や情報の共有が容易になっている(図 1)。

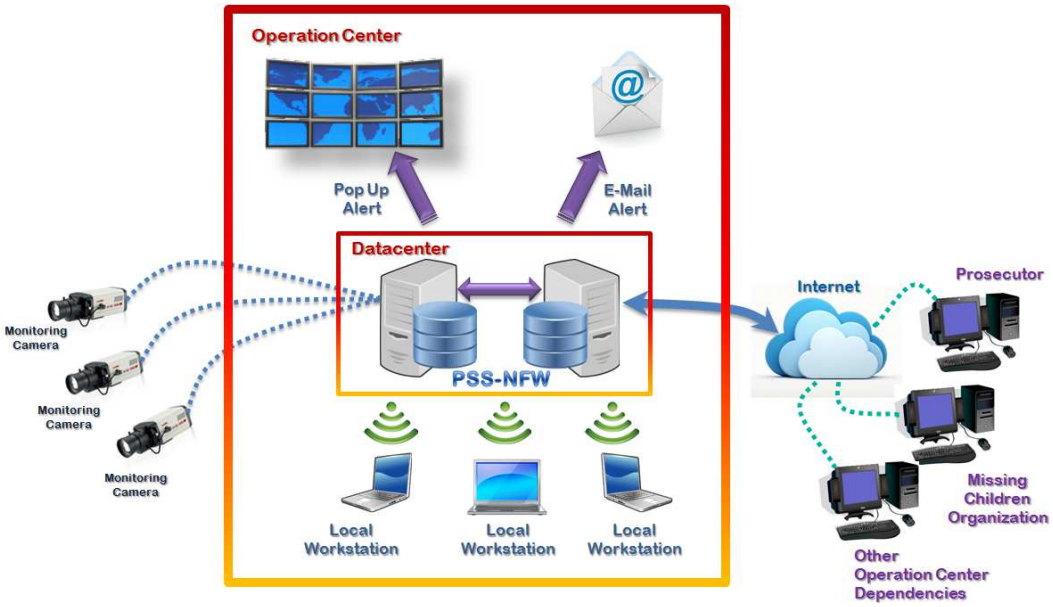
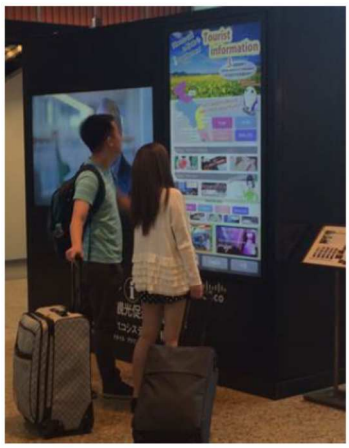


図 1　ティグレ市のシステムの概略[2]

2.2.2　京都府

2015 年 5 月、京都府とシスコシステムズは、スマートシティ推進のため協力協定を締結した。現在、ICT 技術を活用し、エネルギー・交通・ヘルスケア・セキュリティ・観光・雇用・政策等に関する課題を解決するための地域社会作りを推進している。

京都府においては効率的なスマートシティ構築を図るため、現在、都市の課題や実現したい機能などをとりまとめた「スマートシティ基本計画（ICT マスタープラン）」を策定中である。これに先立ち、2016 年度には京都府、JR 西日本及びシスコシステムズにより実証実験が実施された。この実験においては、観光客向けの情報提供手段として、各国言語で投稿された SNS を収集・選択・配信するインタラクティブなデジタルサイネージや、多言語（英語、中国語、日本語）対応のバーチャルコンシェルジュ[6]が活用された(図 2)。今後は街灯をネットワークで結び、センサーや防犯カメラなどを併設し、遠隔制御を行うことで、省エネや情報ターミナル化を実現する「スマートライティング」の実証実験を実施する予定である。



Connected Tourism
(左：サイネージ、
右：タッチパネルサイネージ
@京都駅SUVACO)

バーチャルコンシェルジュ
(@京都駅インフォメーションセンタ)

図 2　京都のバーチャルコンシェルジュ[10]

2.2.3　　会津若松市

情報通信技術（ICI・IoT）や環境技術などを活用し、健康や福祉、教育、防災、エネルギー、交通、環境といった市民生活を取り巻く様々な分野の結びつきを深め、効率化・高度化していくことにより、将来に向けて、持続力と回復力のある力強い地域社会と市民の皆様が安心して快適に生活できるまちづくりを行う取組「スマートシティ会津若松」を掲げ、HEMS（省エネ）、ヘルスケア、観光などのスマートシティ事業を通じた地域再生計画[3][4][5]が進められている(図 3、図 4)。

図 3　会津若松スマートシティ計画全体[5]

アナリティクス人材育成とアナリティクス産業分野（アナリティクスを活用した実証プロジェクトの総体）に関し、ＩＣＴに強みを持つ会津大学を中心としつつ、会津若松市（行政）が産官学の総合的な協力体制をコーディネートする地域一丸となった体制により、アナリティクス人材育成と実証プロジェクトを実施（①）している。その成果としての新事業・新ビジネス・新技術の創出とアナリティクスによる地域産業の高度化・高付加価値化（産業×ＩＣＴとの融合）（②）を断続的に発生させていく取り組みを推進している。①においては、「地域実データの収集（センサーネットワークが整備された街等）・利活用のための基盤環境の整備」し、会津大学を中心とし「アナリティクス人材の育成・教育を実施」するとともに、「産官学の実証プロジェクトの誘致」を推進し、多種多様な実データを利用した実践的な人材育成、実証成果の展開に取り組んでいる。②においては、実証事業の成果やアナリティクス人材を活用し、地域における各産業分野の高度化・高付加価値化を推進している。また、各取組実施においては共通のスマートシティ OS プラットフォーム上で事業実施を推進している。

テレワーク

- ミニジョブマッチングの他、テレワーカーの生活支援のためのポータル(通称「移住者ポータル」)等のサービスを整備（総務省事業）

HEMS

- 会津若松市でオープンAPIによるHEMSを500世帯に設置（総務省、経産省事業）
- 多様なICT端末による電力の「見える化サービス」を提供

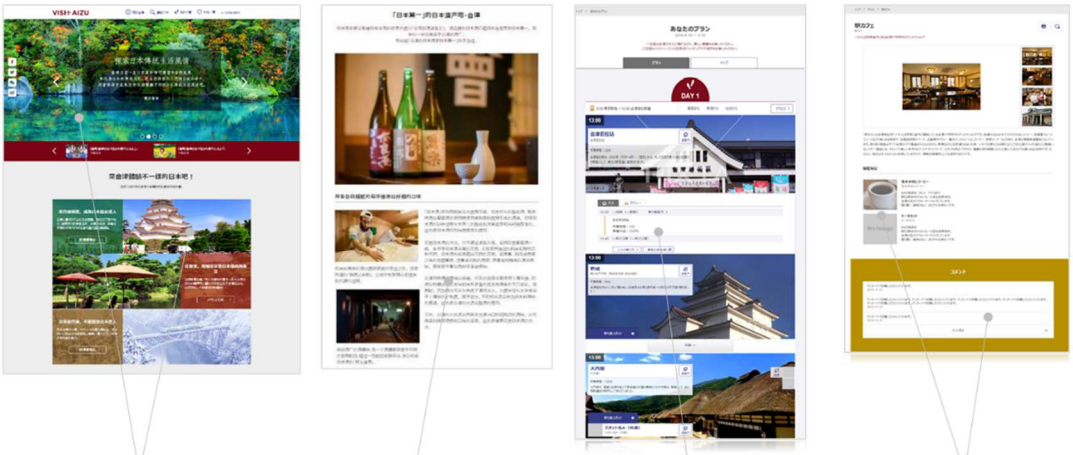
オープンデータ基盤(D4C)

- 自治体が持つデータを中心に、オープンデータの基盤を構築。この基盤上で、データのマッシュアップを行い、様々なアプリケーションを市民主導で開発

会津若松プラス

- 市民向けサービスとして、行政や民間の多様な情報源から情報を吸い上げ、ユーザの属性、嗜好性等に応じて最適なサービス、コンテンツを動的に提供するプラットフォーム事業を展開

観光事業(VISI+AIZU)



ユーザーの国籍・嗜好性にあわせたレコメンデーション
サイトを訪れたユーザーの言語設定を自動で認識し、国籍にあわせて評価の高い観光スポットを押し出す

会津の魅力を伝える深いシナリオコンテンツ
日本慣れした外国人観光客に対して、会津と他の地域との違いを打ち出した深いコンテンツを提供する

二次交通まで考慮したベストな旅行プランの提案
居住地・季節・嗜好に応じたベストな旅行プランを提案し、難点である二次交通まで詳細に解説する

店舗メニューの多言語化・観光客の生の声の収集
買うべき/食べるべきものを明確化し、消費を促す。メニューは印刷して店舗でも使用可。感想を集め、改善に活かす

会津地域における官民一体となった観光振興の推進するための仕組みとして「デジタルDMO」を実現し、誘客の強化および観光客の満足度向上を図る。また、デジタルDMOを通じて得られたデータを分析して各事業者に提供し、PDCAの仕組みを構築。

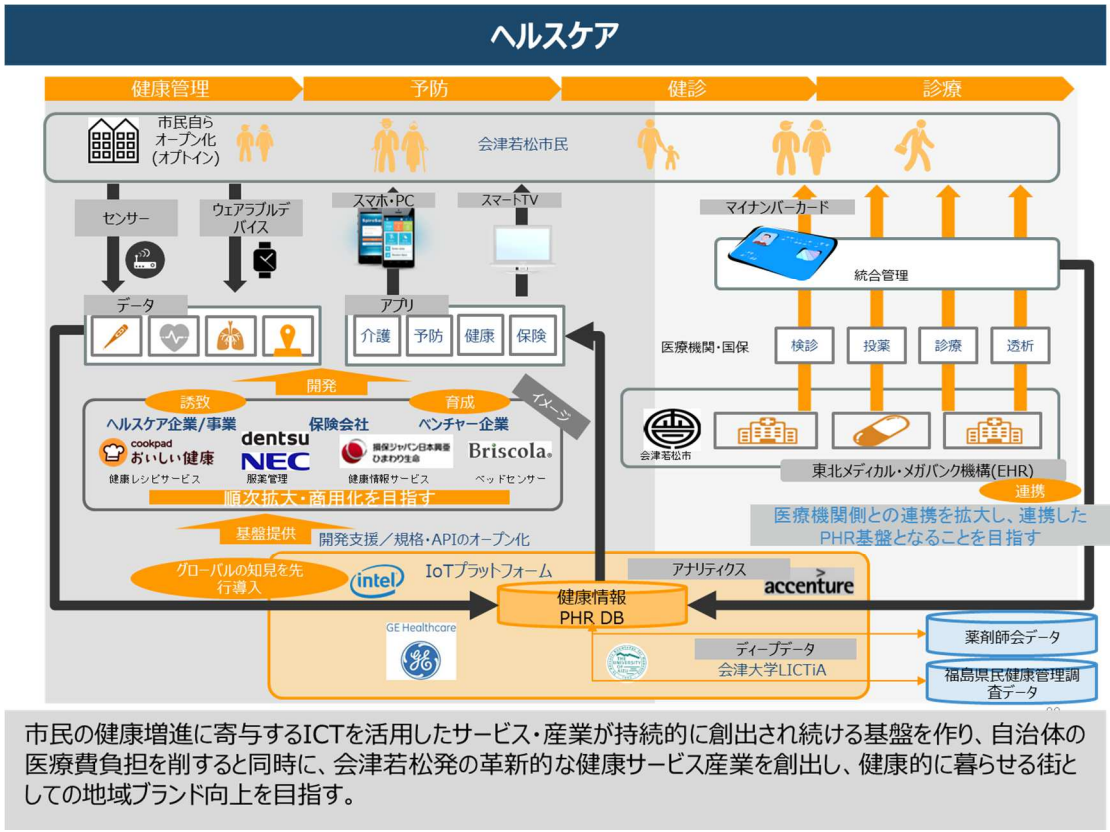


図 4　会津若松における個々の取組事例[5]

データ活用型のスマートシティとして、行政や街中のデータ等を活用し、市民データを起点としたサービス・モデル作りを推進。市の基幹データや外部の多様なサービス提供事業者とのデータ連携を行いつつ、シティズンセントリックなプラットフォームづくりを推進している(図 5)。

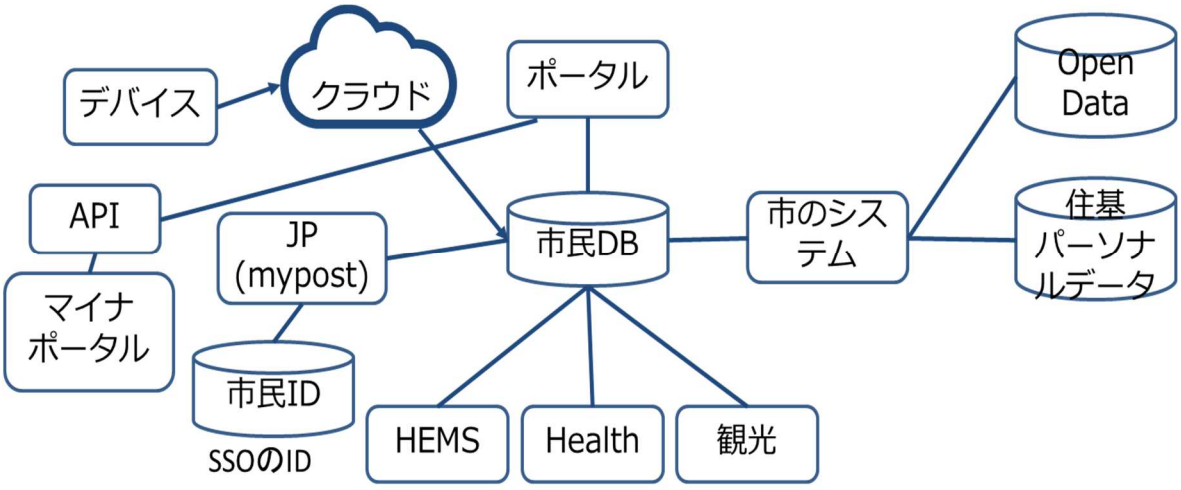


図 5 スマートシティ会津若松のシステム構成

2.2.4　エストニア

エストニアでは、電子政府を推進しており、納税や処方箋など、ID カードを用いて様々なシステムをオンラインで利用可能である。ID カードは 2002 年に導入され、人口約 130 万人に対し 125 万枚の ID カードを配布。ID カードの所有は国民の義務ともなっている。ID カード 1 枚で身分証明証、健康保険証、運転免許証、公共交通機関のチケットとしての役割を果たすほか、銀行口座へのログイン時の識別、納税、医療記録確認、選挙投票、法人登記など、ID による電子署名によって様々なサービスを使用することができる。

ID カードは生活において必需品となっており、特にインターネットバンキングや電子税務署を利用した確定申告など、100%に近い形で国民に利用されているサービスもある(図 6)。

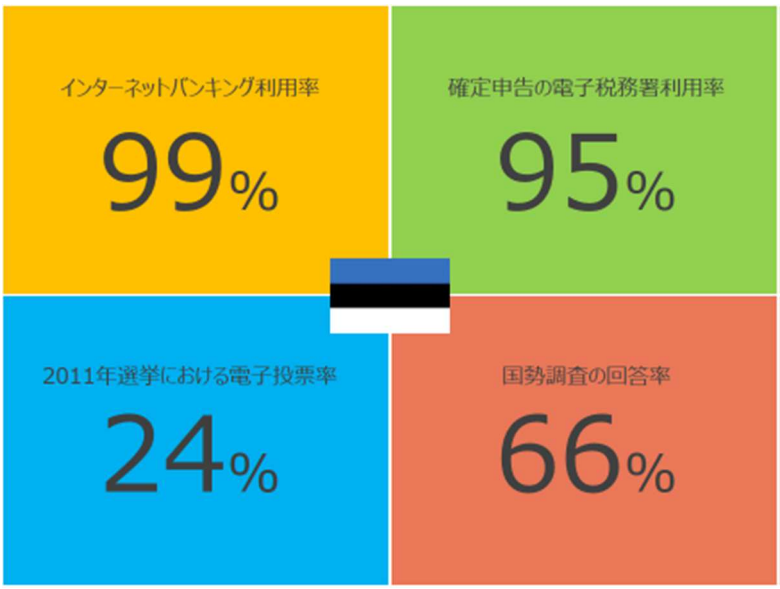


図 6 エストニアの ID カード利用度を示す指標

エストニアでは ID カードを用いたシステム利用の普及により、労働時間の削減や事務作業時間の短縮等、様々な形で効果となって表れている(図 7)。

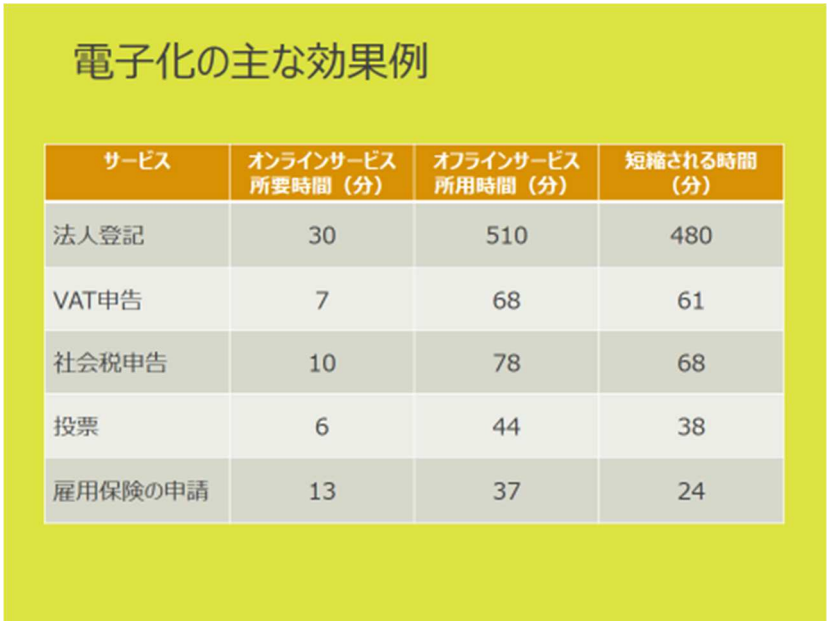


図 7 電子化の主な効果例

これらのサービスを実現するために、エストニアでは、X-ROAD と呼ばれる情報交換層で、各システムを統合している。現在では官民合わせて 2,500 種以上のサービスが X-ROAD を通じて利用できる(図 8)。

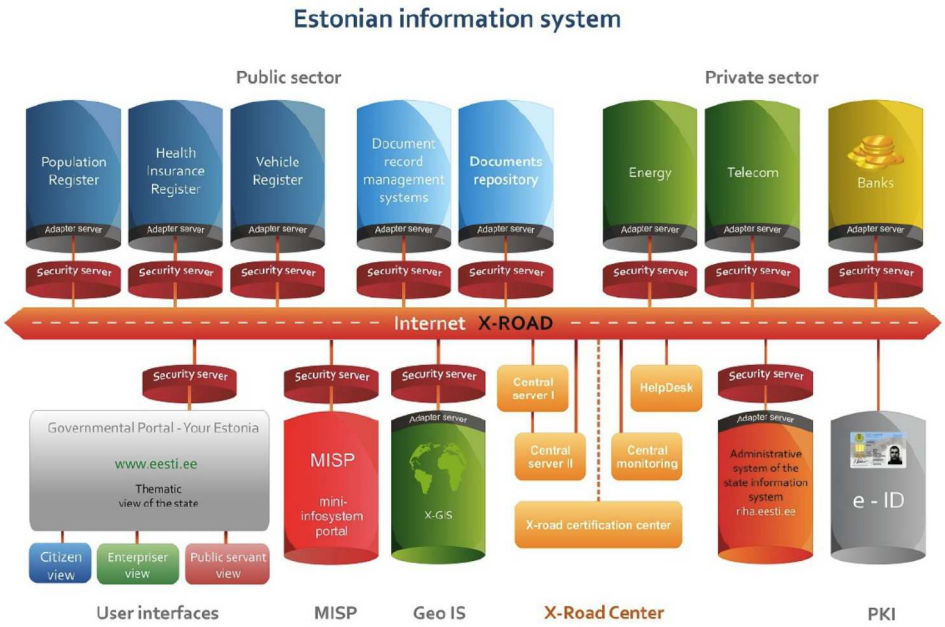


図 8 エストニアの X-ROAD[26]

X-ROAD におけるセキュリティは、各システムに接続する手前に設置されたセキュリティサーバが担っており、具体的にはブロックチェーン同様の仕組みが活用されている。

セキュリティサーバでは盗聴や改ざんからの保護のため、認証からログイン、ログイン後のアクセス先、動作等、各トランザクションを 1 秒ごとにハッシュ化しタイムスタンプと共にログとして記録している。ハッシュ及びタイムスタンプは各セキュリティサーバ上でリアルタイムに分散記録され、各サーバ間で監視を行うことで、セッションの正当性の確認及びデータ整合性の保持を実現している。

また、セキュリティオペレーションセンター（SOC）を構築し、24 時間 365 日体制でのセキュリティ監視も行っている。SOC では X-ROAD 上のセキュリティサーバ及び各ネットワーク機器のトラフィックを監視している。成り済まし等の不正な通信を検知した場合、即座に通信遮断等の対応を行うことで、漏えいを防ぐ仕組みも構築されている。

2.2.5 スペイン・サンタンデール市

スペインのサンタンデール市では、ごみの収集容器にセンサーを設置し、FIWARE[24]ベースのシステム(Cloud City Operation Center)により情報の収集と分析を行うことで、回収のタイミングと収集経路の最適化を行っている(図 9)。具体的には、以下の 2 点を実現している（NEC プレスリリース[21]から引用)。

(1) ゴミ収集容器に設置したセンサーで、集積したゴミの量をデータ化し、モバイルネットワークを介して管理センターに送信。管理センターで大型スクリーンを用いたマップにより一元管理行う。

(2) 管理センターに集められたデータを分析し、最適なゴミ収集ルートやタイミングをゴミ収集事業者に提供。清掃員はこれらの最適な収集ルートなどを、ゴミ収集車に搭載されたモニタで確認する。これにより、集積量の多いゴミ収集容器の回収を優先する、といった効率的なゴミ収集車の運用が可能である。

図 9　サンタンデールのごみ収集の最適化[15]

2.2.6　ニュージーランド・ウェリントン市

ニュージーランド・ウェリントン市は、2011 に”Wellington Towards 2040”プロジェクトを立ち上げ、ウェリントン市を、スマート、安全、そして環境に優しい都市に変えることを目標としている[22]。その目標を実現するために、NEC は、ウェリントン市に、スマートシティソリューションを提供している。具体的には、カメラを用いて車両の流れを把握し、その情報を都市開発計画や道路補修計画の立案に役立てている(図 10)。また、監視カメラの映像解析によって、反社会的な行動を検知し、適切な対処を直ちに行っている。これらの仕組みのプラットフォームとして、FIWARE ベースのシステムが構築されている。

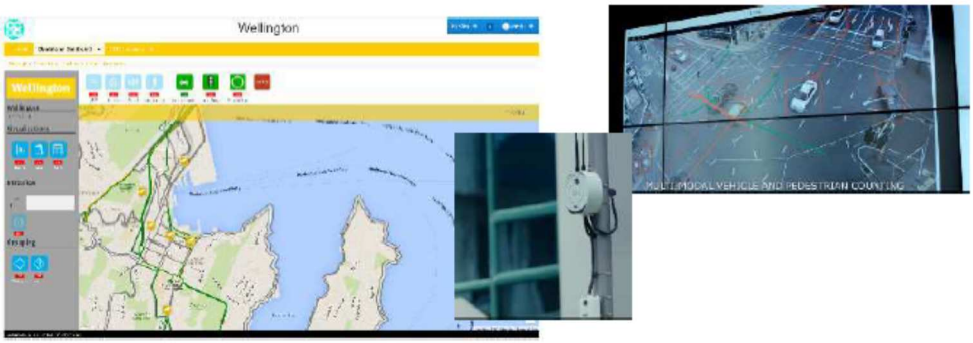


図 10　ウェリントンの交通計画策定・犯罪予兆検出[15]

2.3　　アーキテクチャ・レイヤモデルの定義

前節の事例を整理すると、アーキテクチャは、①１つのスマートシティ IoT システムの部分と、②IoT システムの連携部分に分けることができる(図 11)。以下では、それぞれの部分について、業界団体や標準化団体が発行している報告書のモデルを用いて整理する。

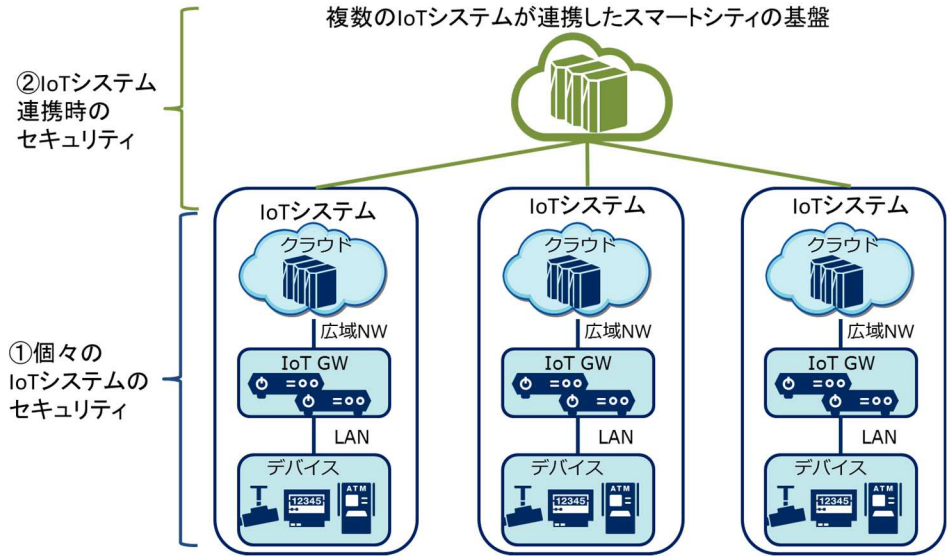


図 11 スマートシティのアーキテクチャの全体像

2.3.1　　スマートシティ IoT アーキテクチャ(単一システム)

スマートシティ IoT は、アーキテクチャのレベルで考えると、一般的な IoT のアーキテクチャと大きく変わらないと考えられる。図 12 は、ITU-T が発行している報告書(Overview of the Internet of things[20])で提案されている IoT のリファレンスモデルである。下の層から、デバイス、ネットワーク、アプリケーションのプラットフォーム、アプリケーションの 4 層に分けて整理されている。加えて、すべてのレイヤを縦断するセキュリティとマネ

ジメントのレイヤが示されている。

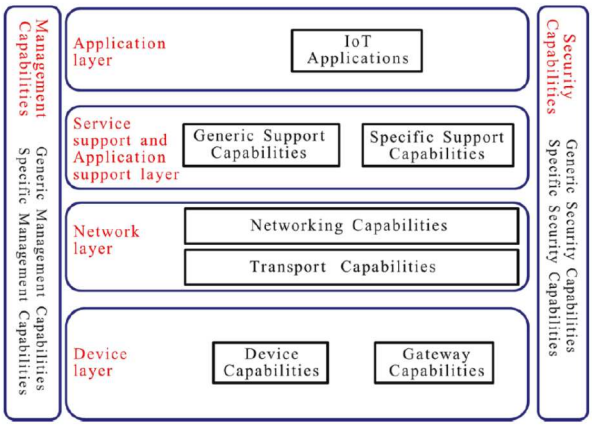


図 12　ITU-T の IoT reference model[20]

2.3.2　スマートシティ IoT のアーキテクチャ(複数のシステムの連携)

ENISA(The European Union Agency for Network and Information Security)は、公共交通機関のサイバーセキュリティの報告書[1]を発行している。主な構成要素として、Field components(デバイス)、Data transmission(ネットワーク)、クラウドに分けられている。また、報告書の中では、スマートシティの特徴として、個々のオペレータの情報を交換して統合し、全体のデータを解析することでグローバルな意思決定を可能にする点が挙げられている。

Figure 5 Simplified view of the ICT architecture of SCs

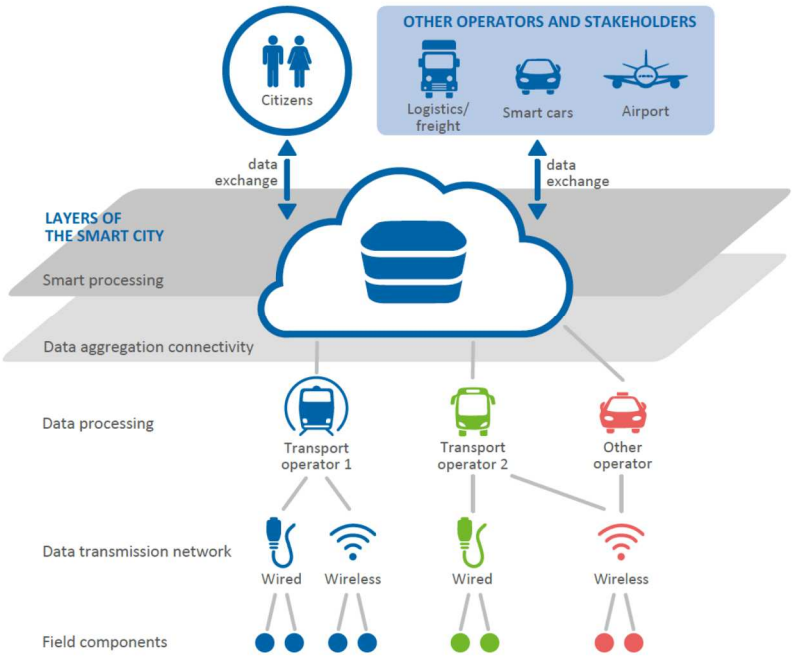


図 13　ENISA のスマートシティアーキテクチャ[8]

IEC(International Electrotechnical Commission)は、Orchestrating infrastructure for sustainable Smart Cities [13]を発行し、縦の連携(Vertical integration from sensors to management tools)と、横の連携(Horizontal integration of domains)に分けて、それぞれの連携を議論している。縦の連携のためには、情報を集めるセンサー、低コストな通信、都市インフラのリアルタイム管理システム、データ分析が必要であり、これらを通じて都市の最適化や、より良いサービスの提供が可能になるとしている。

横の連携に関して、現状では横の連携を行っているプロジェクトは少ないとしているが、地理情報システムと天気予報システムの連携や、群衆の混雑情報システムとスマート交通システムの連携を例として挙げている。また、既存のシステムとの統合について、ポータルサーバが中心となって複数のシステムを統合するアイデアを提案している。加えて、統合された都市管理プラットフォームが必要であり、トップダウンのガバナンスと、ボトムアップのイノベーションのバランスをいかに取るかが課題であると指摘している。

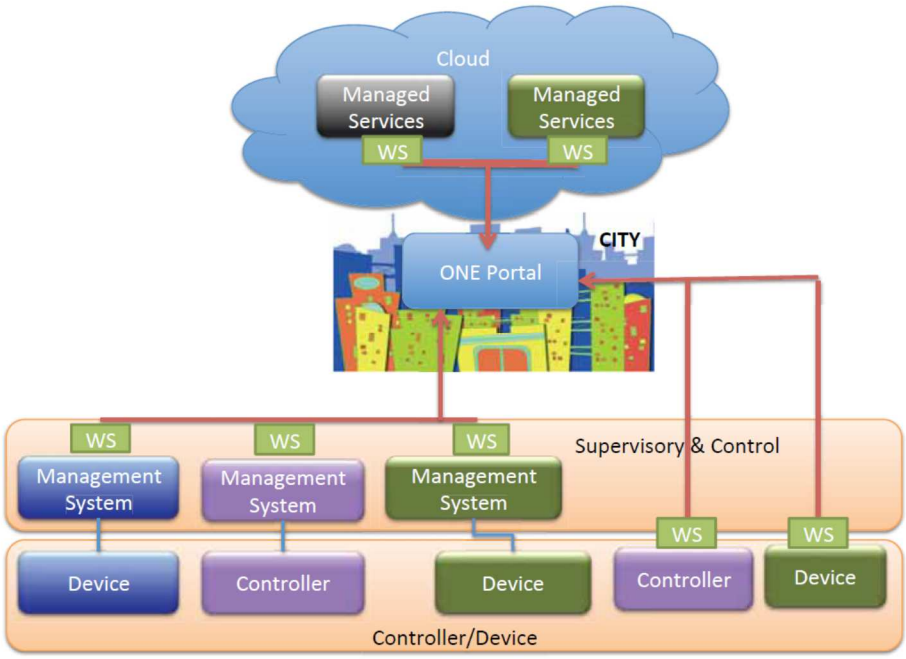


図 14 One portal structure integrated using standards[13]

BSI は、Smart city framework[14]の中で、既存のシステムの問題点として、各システムがドメインごとに垂直的に統合されており、システムがサイロ化している点を指摘している。その結果、市民や企業は、それぞれのシステムに別々にアクセスする必要がある。加えて、データはそれぞれのシステムにロックインされおり、都市の横断的なコラボレーション

を妨げている点を指摘している。

BSI の報告書では、上記の状況を改善するために、サービスやデータを連携させたモデル(図 15)を提案している。加えて、リーダシップとガバナンスについても言及しており、市当局への明確な説明、都市を横断するリーダシップチーム、ガバナンスプロセスの透明化が提案されている。

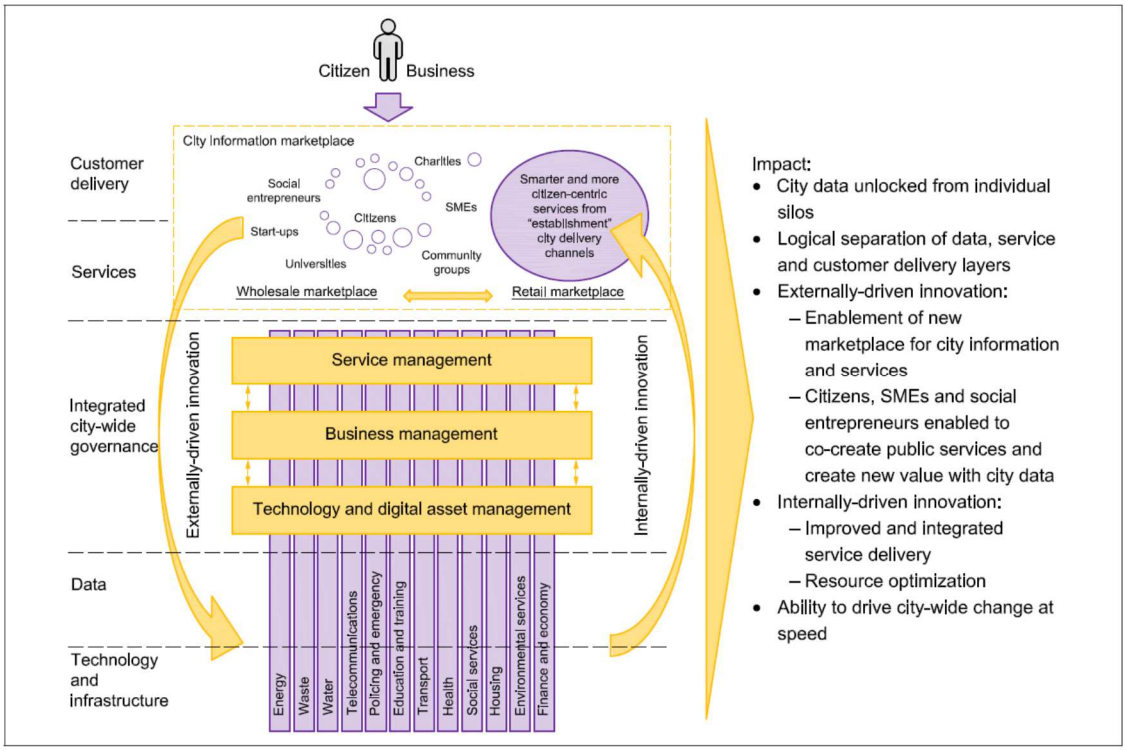


図 15 New integrated operating model[14]

2.3.2.1 システム連携のモデル

上では、個々のスマートシティ IoT システムを連携させることによる付加価値の高いサービスの提供を述べた。システムの連携は、より具体的には、次の 3 つの場合が考えられる。

- 1 つの自治体内のサービスの連携(図 16)
  - ヘルスケアサービスや省エネサービスなどのサービスが連携するモデルである。各サービスが保有しているデータを統合的に利用することにより、より価値の高いサービスが期待できる。例えば、IEC の報告書[13]では、交通情報とコンテキスト情報(天気情報、イベント情報)を組み合わせて、異なったタイムスケールでの交通情報の予測を可能とする例が示されている。
- 1 つの自治体内のオープンなサービスとクローズなシステムの連携(図 17)
  - 前のモデルの拡張であり、連携するシステムがマイナンバーカードシステムや自治体の行政システム、企業のシステムのように、機微な情報を扱う場合であ

る。そのため、より強固なセキュリティ機能や、厳格なセキュリティ運用が必要になる。

- 自治体間のシステム連携(図 18)
  - 上記の 2 つのモデルの拡張であり、各自治体のシステムが統合され、複数の自治体間でデータをやり取りする場合である。より価値のあるサービスを提供できる反面、大規模なシステムであり、また複数の事業主体が参加しているため、セキュリティ管理の難易度が高くなると考えられる。

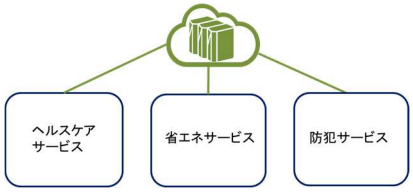


図 16　1 つの自治体内のサービス連携

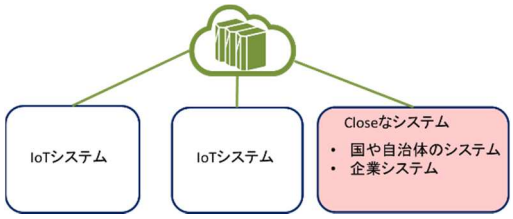


図 17　1 つの自治体内のクローズシステムとの連携

図 18　自治体間のシステム連携

2.4　セキュリティ課題抽出(単一システムの場合)

前節では、スマートシティを単一システム（縦の連携）と複数システム（横の連携）に分けて整理した。ここでは、前者の単一システムについて、ホワイトペーパや報告書を調査し、セキュリティ課題を整理する。具体的には、スマートシティ IoT のセキュリティ課題は、一般的な IoT のセキュリティ課題と、スマートシティ特有のセキュリティ課題から構成されると考えられるため、それぞれについて分析を行う。複数システムが連携する際のセキュリティ課題については、次節で述べる。

2.4.1　一般的な IoT のセキュリティ課題

ENISA のレポート[9]とトレンドマイクロのレポート[10]からセキュリティ課題を抽出し

た。ENISA は、 運用や組織の課題について述べており、トレンドマイクロのレポートは技術的な課題についてまとめている。

① 運用や組織の課題

ENISA は、Cyber Security and Resilience of Intelligent Public Transport[9]の中で、以下の点を挙げている。

- Challenge 1: Difficulties to integrate security for safety
  - 公共交通事業者は、安全性(Safety)を重要視する傾向があり、サイバーセキュリティのコンセプトの理解が難しい場合がある。
- Challenge 2: Inadequate importance and spending being afforded to cyber security
  - サイバーセキュリティの重要度(優先度)が十分ではない。また、脅威に対抗するための予算も不足している。
- Challenge 3: Inadequate checking for countermeasures
  - 多くの交通機関は、対策の有効性を評価していない。その結果、どの対策が効果的か・効果が薄いかという知見が欠けている。
- Challenge 4: Unwillingness to collaborate and exchange information on cyber security
  - 交通機関は、サイバーセキュリティの情報交換を、他の事業者と行うことに対して消極的である。
- Challenge 5: Slow phasing out of legacy systems
  - レガシーシステムの存在が弱点となっている。レガシーシステムのセキュリティは物理的な脅威への対策が主な目的であり、ネットワークで繋がっているシステムへの対応が遅れている。
- Challenge 6: Inadequate data exchange between IPT and Smart Cities operators
  - 公共交通機関と他のスマートシティの事業者のデータ交換は、制限されていたり、連携されていなかったり、その場しのぎであったりする。また、複数のステークホルダーが関連する統合されたシステムにおいて、誰がそれぞれのコンポーネントのセキュリティについて責任を持つかが曖昧となっている。
- Challenge 7: Weak situational awareness of cyber threats
  - 交通のシステムが相互接続になる等、変化が速いので、脅威の全体像の知見を得ることが難しい。
- Challenge 8: Resistance to security adoption
  - 有効ではないと考えられている対策が実施されている場合や、逆に、有効と考えている対策が実施されていない場合がある。これは、「言われたからやる」という受け身の文化のためである。

② 技術的なセキュリティ課題

トレンドマイクロは、IoT セキュリティガイドライン[10]を発行し、以下の課題を挙げている。

- ハードウェアの制約とコスト要因
  - IoT デバイスは、IT 機器に比べ、ハードウェアリソースが非常に限られたものであることが多く、また製造コストの制約もあるため、セキュリティ機能そのもの実装が非常に困難な場合がある。そのため、現状では、通信の暗号化等も実施されていないことが非常に多く、攻撃に脆弱な状況である。
- ハードウェアへの不正侵入とデバイス ID
  - IoT デバイスは容易に入手可能であるため、解析等を行うこと自体も非常に容易である。クラウドへの接続時には固有のデバイス ID を利用しているケースなどもあるが、容易に解析が可能な場合、デバイス ID の偽造等も非常に容易となるため、クラウドへの不正接続なども発生しうる。
- システムに対するセキュリティパッチ適用の問題
  - オープンソースライブラリを利用している機器はこれまでも潜在的な脆弱性を持っていたが、従来はインターネットに接続していないことによって攻撃を受けていなかっただけである。問題のあるライブラリなどをアップデートすることなくインターネットに接続することは、非常に大きなリスクとなる。そのため、FOTA（Firmware Over the Air）による脆弱性の対策が重要な解決策となる。

2.4.2 スマートシティ IoT 特有のセキュリティ課題

次に、スマートシティ IoT 特有のセキュリティ課題を分析する。ここでは、システムや機器と、その上で扱われるデータの特性に注目して分析を行った。

- システム・機器の要素
  - デバイスや IoT ゲートウェイに、物理的にアクセスされやすい。工場、農業などの IoT は敷地内だけだが、スマートシティは町中にセンサーが配置されるためである。
  - 影響範囲が大きい。都市を運営するインフラの一部であるため、システムダウンや乗っ取りが発生した場合、被害が大きい。例えば、2016 年 11 月に、サンフランシスコ市営鉄道のシステムが攻撃され、精算機が稼働しなくなり、運賃を無料とすることを余儀なくされた。この攻撃による市民への被害は大きくなかったものの、攻撃の対象によっては、より大きな被害を及ぼす可能性がある。
- データの要素
  - センサー・カメラ等が収集する情報は機微な情報（privacy-sensitive）な場合がある。例えば、産業競争力懇談会の報告「IoT 時代におけるプライバシーと イノベーションの両立」[16]では、情報管理だけではなく、自己情報のコントロー

ルなどの必要性が述べられている。

- １つのシステムの上で、様々なデータを扱う。例えば、機密レベルの違いがあり、Open なデータと機密データを１つのシステムで扱う場合がある。エストニアの例では、プライバシー情報である健康情報も情報交換基盤である X-ROAD で取り扱われている。その際、市民が自身の健康情報について、アクセス権を設定することで、開示先を詳細に決めることができるようになっている。

2.5 複数のシステムが連携する際のセキュリティ課題

上では、1 つのスマートシティ IoT システムのセキュリティ課題を述べた。次に、それらのシステムが連携した場合のセキュリティ課題について分析する。具体的には、2.3.2 で述べたように、複数のスマートシティサービスが連携し、より価値の高いサービスを提供する場合のセキュリティ課題を考える。その際、以下の点が課題として挙げられる。各課題の解決策については、4 章で詳しく述べる。

- 複数のシステムで ID・パスワードや鍵・証明書が個別に管理されることによって、管理の不備が生じるリスクがある。一般的な解決方法は、認証連携のメカニズムや PKI を構築することである。詳しくは、次章で述べる。
- 他のシステムに渡した情報が漏えいするリスクがある。具体的には、あるシステムが他のシステムに情報を渡した際、その情報をどのようにコントロールするかという課題がある。一般的な解決方法は、システム横断的な情報流通管理やトレースバック機能を備えることである。
- 複数のシステムの情報を統合して分析すると、より詳細な行動の把握が可能となり、サービス利用者のプライバシーが侵害される可能性が指摘されている[17]。
- インシデント発生時に、複数のシステムのログを解析する必要があるため、インシデントへの対応が遅れるリスクがある。また、それぞれのサービスで運営主体が異なるために情報の共有が円滑に進まないリスクや、リーダシップの欠如による対応の遅れのリスクがある。

3　スマートシティ IoT に必要とされるセキュリティ要件

本章では、前章でまとめたスマートシティ IoT のセキュリティ課題を基にスマートシティ IoT に必要とされるセキュリティ要件をまとめる。

3.1　　脅威を防ぐために必要な技術要件の検討

ここでは、IoT のセキュリティ要件を一般的な IoT とスマートシティ IoT に分けて分析する。具体的には、一般的な IoT のセキュリティ要件をトレンドマイクロ、McAfee、シマンテックの報告書を基に分析し、スマートシティ特有のセキュリティ要件を 2.2 で示したスマートシティの事例と 2.4.2 で示したスマートシティ特有の課題を基に分析する。

3.1.1　　一般的な IoT のセキュリティ要件

セキュリティベンダーが発行しているレポートを分析し、IoT システムのセキュリティ要件を抽出する。セキュリティ要件は、フェーズごとに分類し、機器の初期化時・起動時、運用時、アップデート時の要件に分けることができる。また、アーキテクチャに注目し、IoT 特有のデバイスの観点からセキュリティ要件を整理することもできる。以下では、それぞれの分析の例として、トレンドマイクロ、マカフィー、シマンテックの報告書の要点を述べる。

3.1.1.1　　トレンドマイクロ

トレンドマイクロのレポート[10]では、IoT のライフサイクルにおいて、それぞれのステップでどのようなセキュリティ機能が必要かをまとめている。

- 起動時
  - セキュアブート
- 初期化時
  - AAA 保護　（認証（Authentication）、認可（Authorization）、アカウンティング（Accounting））
    - ✧ システムの暗号化
    - ✧ 初期設定のパスワードの変更をエンドユーザに求める
  - 鍵/証明書の保護
    - ✧ KMS（Key Management System、鍵管理システム）や CMS（Certificate Management System、証明書管理システム）の利用
    - ✧ TPM（トラステッドプラットフォームモジュール）の利用
  - 通信の保護
    - ✧ デバイス間、デバイス/インターネット間、デバイス/ユーザインターフェース間（モバイルアプリ/ウェブアプリ経由）の通信を暗号化
  - ID の保護
    - ✧ ID 偽造（なりすまし）を防ぐために、通信対象の認証の実施
- 運用時（稼働時）
  - AAA 保護

✧ 管理用、開発用アカウントの削除

- 監視

✧ 異常データの検出機能を実装し、異常時にクラウド等に警告を送付

- 完全性チェック
- リスク管理

✧ FOTA（Firmware Over the Air）によるセキュリティパッチ適用までの間のリスク軽減策の策定

● アップデート時

- セキュアな FOTA（Firmware Over the Air）

3.1.1.2 McAfee

IoT におけるセキュリティ要件として、ポイントソリューションによる保護だけでなく、システム全体の監視やレジリエンスの考え方を導入し、レジリエンスを実現するため、エッジデバイス、ネットワーク、ログ監視を組み合わせ、エンド・ツー・エンドでのセキュリティ実装が重要である。また、様々な利用用途・環境が考えられるため、サイバーの観点だけでなく、物理的な観点でもセキュリティを確保する必要があり、ハードウェアとソフトウェアの両面で網羅的にセキュリティ機能を実装する必要がある[27]。

● エッジデバイスのセキュリティの考え方

- セキュリティ監視との連携を実現するため、セキュリティログ収集機能を実装
- 耐性は高く、運用負荷は極小化するため、ホワイトリスト型のセキュリティ対策を導入
- ハードウェアセキュリティ（信頼できる実行環境、デバイス認証、セキュアなブート・メモリ・ストレージ）
- 脆弱性が発見される事態を見据えた運用体制の構築

● 通信ネットワークのセキュリティの考え方

- 通信プロトコルおよびコマンドのホワイトリストの実装
- 暗号化や認証の導入による秘匿性とシステムの可用性のバランスを熟考
- セキュリティ監視との連携を実現するため、セキュリティログ収集機能を実装

● セキュリティログ監視の考え方

- エッジデバイス、ネットワーク、クラウドのセキュリティログを SIEM に可能な限り収集し、いつもと違う事象が発生していないかを監視（可視化による平常時との乖離の分析、相関分析ルールによる異常事象の検知）
- 複数拠点に点在する全てのデバイスやネットワークのセキュリティを一元的に監視し、見える化
- 状況認識（Situational Awareness）を活かしてレジリエンスを実現
- インシデント検知をトリガーにして対応を自動化し、迅速な復旧を支援

● セキュリティ管理の考え方

- エッジデバイスのセキュリティポリシーを単一のコンソールで一元管理する
- 膨大な数の IoT デバイスを管理するためのスケーラビリティとパフォーマンスに加えて、様々なセキュリティ機能を一括して取り扱える管理性
- デバイスに対して様々なアクション（隔離やアップデートなど）を迅速に実施し、レジリエンスを実現

3.1.1.3 シマンテック

シマンテックは、IoT（モノのインターネット）の 参照アーキテクチャ[11]で、以下のセキュリティ要件を挙げている。

● 通信の保護

● デバイスの保護

✧コードの保護

✧ホストベースの保護

● デバイスの管理

✧構成のアップデート

✧セキュリティ分析のためのセキュリティコンテンツとセキュリティ測定データの管理

✧適切なシステム機能のための測定データと制御の管理

✧診断と修復

✧NAC（Network Access Control）認証情報の管理

✧権限などの管理

● システムの理解

✧デバイスが依然として信頼できるかどうか は、最終的には評価ベースなどの他のサービスや「モノのディレクトリ」によって判断する必要がある。このディレクトリでは各デバイスや IoT システムに関するセキュリティ情報を追跡できるだけでなく、デバイスやシステムが相互に付与する権限や資格も追跡可能である必要がある。

3.1.2 スマートシティ IoT 特有のセキュリティ要件

スマートシティ特有のセキュリティ課題として、2.4.2 で、物理的にアクセスされやすい点と、機微な情報を扱う点を挙げた。これらの課題に対処するために、以下の機能が必要である。

● システムの堅牢性

【要件１】機器の成りすまし防止・発見：システムを安全に保つためには、システムが正しい機器で構成されている必要がある。そのため、機器の差し替え

や、不正な機器が設置された場合に、それを検知し、取り除く必要がある。

【要件２】機器の改ざん防止・発見：不正な機器の設置だけではなく、正規の機器が攻撃者によって改ざんされる可能性がある。具体的には、アプリケーションや OS の改ざんや、よりレイヤが低いファームウェアの改ざんが考えられる。これらの改ざんされた機器を検出し、システムを健全に保てることが望ましい。また、IoT デバイスが攻撃者に乗っ取られた場合、IoT デバイスからスマートシティ IoT プラットフォームに対して何らかの攻撃(DoS や、不正侵入)が行われることも想定される。このような乗っ取られた機器や改ざんされた機器からの攻撃は、認証や認可によるアクセス制御では防ぐことができないため、機器の振舞いの監視が求められる。

【要件３】ハードウェアからクラウドまで(end-to-end) の堅牢性：上記の 2 点は、機器単独の真正性の担保には有効であるが、システム全体の真正性を担保するためには、システム全体の監視が必要である。具体的には、中央集権的アプローチで検証サーバがすべての構成要素の真正性を検証する方式や、分散的アプローチで機器同士が互いに検証する方式が考えられる。

- データの管理

【要件４】漏えい・改ざんの防止：前項の対策でシステムの堅牢性は担保されるため、そのシステム上でデータを適切に扱うことにより、データの安全性(完全性と機密性)を保証することができる。具体的には、データに対して適切なアクセス権を設定し、あらかじめ定められた人・機器・ソフトウェアコンポーネントのみがデータにアクセスできるような制御が求められる。加えて、データの属性(データの生成場所、処理履歴、プライバシーのレベルなど)に基づいてアクセス制御できることが望ましい。また、様々なデータのアクセス権を簡単に管理する仕組み(例えば、RBAC(Role-Based Access Control)など)が使用可能であることが望ましい。

【要件５】トレーサビリティ：セキュリティインシデントの解析や、機微な情報が適切に扱われているかを監査するためには、データの生成から消滅までのライフサイクルがトレースできる必要がある。

3.1.2.1 日本特有の要件

- **マイナンバーカードとの連携**
  - マイナンバーカードは、税・社会保障・災害対策の行政手続での利用が予定されている[18]。特に、防災は、スマートシティ IoT のユースケースの１つであり、この分野でマイナンバーカードとの連携の可能性がある。その際は、マイナンバーカードのセキュリティ運用ルールに準拠する必要がある。詳細な要件は、本報告書の対象外とする。
- **法的な課題**

- カメラ画像や医療データなどの個人情報に関わるデータは、個人情報保護法に基づいた運用が必要である。詳細な要件は、本報告書の対象外とする。

4　複数のスマートシティシステムが連携する際の要件

本章では、2.5 で述べたスマートシティ IoT システムが連携する際のセキュリティ課題に基づいて、連携基盤が備えるべきセキュリティ機能の要件について述べる。

4.1　　複数システム連携のためのアーキテクチャ

セキュリティ要件を検討する前に、システムのアーキテクチャを整理する。エストニアの X-ROAD を基にスマートシティ IoT のシステム連携のアーキテクチャを考えると、図 19 のような構成になると考えられる。具体的には、個々のシステムの上位にデータ連携のための IoT システム連携基盤が配置され、各システムはこの基盤を通じて連携を行う。また、IoT システム連携基盤はシステム連携 IF を備え、異なるシステム間で相互参照するための共通フォーマットによって、提供側と活用側の橋渡しを行う。

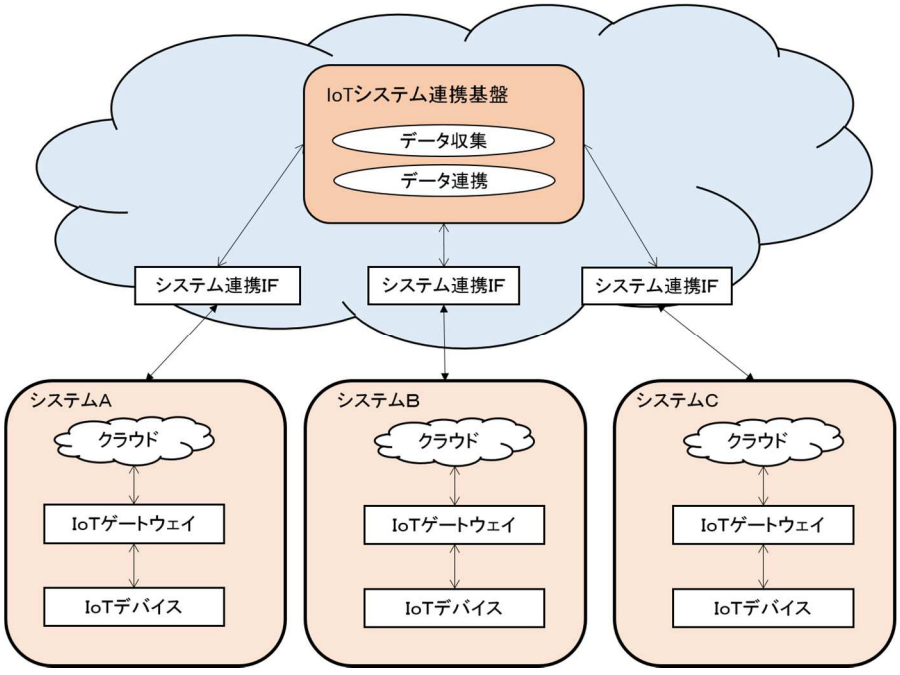


図 19　複数システム連携のアーキテクチャ

4.2 セキュリティ要件

次に、2.5 で述べた複数のスマートシティ IoT システムが連携した時の課題を解決するために必要なセキュリティ要件を、上記のシステム連携アーキテクチャを基に述べる。

【要件６】認証連携

- 複数のシステムで ID・パスワードや鍵・証明書の管理が分散することによる管理の不備やコストの増加という課題を解決する必要がある。そのためには、各システムが持つ ID 管理サーバ間の認証連携や、各システムから利用可能な PKI を構築する必要がある。
- その際、認証局の設置場所や、証明書が失効した時の処理の手順を決める必要があるが、それらは未解決の課題であり、更なる検討が必要である。
- 本人確認をより確実に行う必要がある場合には、公的個人認証サービスの利用も検討するべきである。

【要件７】他のシステムから渡された情報の保護

- 情報漏えいや情報の目的外利用などを防止するために、他のシステムから渡された情報に対し、権限のない者がアクセスできないようにすることが求められる。その際、前項の認証連携の仕組みと連動して、アクセス制御の仕組みが動作することが望ましい。
- 連携しているシステムへの情報の受け渡しにおいて、情報の漏えいや改ざんがされないよう、セキュアな通信手段を用いることが求められる。
- 万一情報が漏えいした際に、その被害を防止するために受け渡す情報は暗号化することが望ましい。

【要件８】プライバシー侵害リスクの最小化

- 各システムから収集した複数のデータを組み合わせることよって、個人の特定などができてしまうリスクがあるため、サービスを実現する上で提供する情報に留意する必要がある。
- 匿名化によってプライバシーを保護することも重要であるが、匿名化の具体的な方法はユースケースやデータ依存であるため、本報告書の対象外とする。

【要件９(技術面)】システム横断的なインシデント対応

- セキュリティインシデント発生時、システム間で不正な活動が行われている場合であっても、迅速な対応を行う必要がある。そのために、システム横断的な情報トレーサビリティ機能を備えることが望ましい。具体的には、複数システムに跨ったログ取得、および、複数システムを横断的に監視する機能を備えているこ

とが望ましい。

4.3 セキュリティ運用体制の要件

システムを堅牢に保つためには、セキュリティ機能の導入だけでは不十分であり、その機能が正しく運用される必要がある。以下では、システム連携時の運用体制の要件を述べる。

【要件９(運用面)】システム横断的なセキュリティ運用

IT のセキュリティ運用では、Computer Security Incident Response Team(CSIRT)が脆弱性発見時や攻撃検出時にインシデント対応を行う。その対応を迅速に行うために、事前に対応フローを決めておくことが一般的である。例えば、JPCERT が発行している「インシデント対応マニュアルの作成について」[12]では、インシデントの定義や、責任を持つ部署・担当者の明確化、全体の統括を行う部署またはチームの定義が、マニュアルに記載されている必要があるとしている。スマートシティ IoT においても、同様の運用体制や責任分担の明確化が必要であると考えられる。また、CISRT 発足の際には、組織対応力ベンチマーク[23]などの指標に基づいて、対応力が十分であるかを評価することが望ましい。

また、セキュリティ運用のための費用に関して、現状では横断的なセキュリティ運用をする場合の費用負担が整理できていない。それを解決するために、横断的なセキュリティ管理の運用費用については、国からの補助のほか、連携するシステム全体で負担するなど、継続して検討すべきである。例えば、BSI のレポート[14]では、予算も単一のシステムごとではなく、スマートシティ全体の予算を立てること“**setting holistic and flexible budgets**, with a focus on value for money beyond standard departmental boundaries”を提案している。

5　スマートシティ IoT 基盤の実装例

本章では、スマートシティ IoT を実現するプラットフォームの一例として、導入実績のある FIWARE[7]を分析し、不足しているセキュリティ機能の洗い出しを行う。

5.1　FIWARE

欧州では、EU が投資を行い、スマートシティ IoT 基盤である FIWARE を開発している。FIWARE のホームページ[24]によると、そのコミュニティは、７５以上の都市や１０００社以上のスタートアップに広がっており、欧州では非常に実績のあるスマートシティ IoT 基盤である(図 20)。2.2 で紹介したサンタンデール市やウェリントン市も FIWARE ベースのシステムを採用している。

図 20　FIWARE のコミュニティマップ[24]

FIWARE は、Generic Enabler (GE)と呼ばれるソフトウェアコンポーネントの集まりであり、開発者は必要な機能を提供する GE を組み合わせることによって、システムを構築することができる(図 21)。具体的には、ユーザインターフェース、クラウド基盤、認証等のセキュリティ、データ処理・管理などの機能を提供する GE が提供されている。また、各モジュールが連携するために、インターフェースの標準として NGSI を採用している。

セキュリティに関しては、ID 管理を行う KeyRock、セキュリティポリシーの強制を行う Wilma、ポリシーに基づいたアクセス可否の判定を行う AuthZForce が、GE として用意されている。

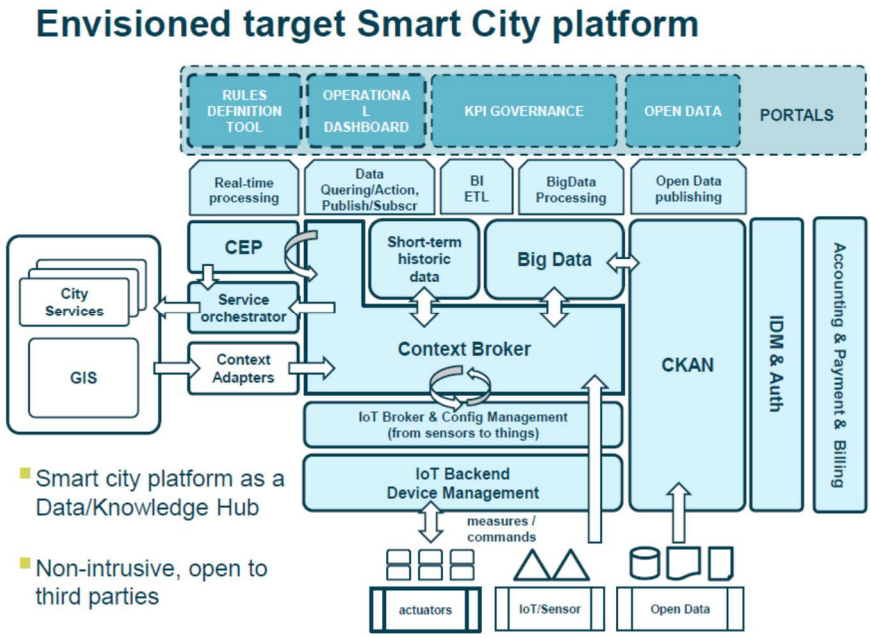


図 21　FIWARE のアーキテクチャ[25]

5.2　セキュリティ要件の分析

次に、FIWARE が 3 章と 4 章で挙げたセキュリティ要件を満たしているかを検証する。

5.2.1　1 つの IoT システム内のセキュリティ要件

- システムの真正性検証、不正デバイス排除（要件 1～3）
  - 上で述べたように、FIWARE のセキュリティ機能は、認証・認可によるアクセス制御を備えている。従って、不正なデバイスがシステムに接続しようとしても、認証によって防ぐことができる。しかし、認証は OAuth[1] 2.0 のトークンを基に行われており、デバイスにアクセス可能な攻撃者が、このトークンを盗み出した場合、デバイスの成りすましが可能となるリスクが残存している。同様に、アプリケーション・OS・ファームウェアが改ざんされた場合でも、それを検知する仕組みを FIWARE は備えていない。
- データの漏えい・改ざん防止（要件 4）
  - FIWARE は、Policy Enforcement Point(PEP)である Wilma によってコンポーネントの API 呼び出しをフックし、認証を行う KeyRock と Policy Decision Point(PDP)である AuthZForce とを組み合わせることによって、認証・認可によるアクセス制御を行うことができる。具体的には、アクセス

[1] OAuth 2.0 は、本来は認可のためのプロトコルであるが、FIWARE では認証のために用いている。

制御は、API の呼び出し者(Subject)、API(Object)、Put/Get などの API の操作(Action)によってアクセス可否が判定される。よって、データベースからの NGSI を用いた情報読み出しの制限など、基本的なデータ流通制御が可能である。しかし、データの履歴などの属性に基づいた制御の機能は備えておらず、1 つのシステム上で様々なデータを扱うためには、機能が不十分である。

- データのトレーサビリティ（要件５）
  - FIWARE には、データの生成から消滅までを包括的にトレースする機能は備わっていない。

5.2.2 システム連携時のセキュリティ要件

- 認証・認可の連携（要件６）
  - FIWARE の ID 管理コンポーネントである KeyRock は、OAuth 2.0 をサポートしている。しかし、特定の ID 管理サーバで認証が行われるような実装になっており、そのままでは対応できない。
  - FIWARE は、認可の問い合わせのフォーマットとして XACML を採用している。XACML はポリシー記述言語であり、複数システム間の連携までは規定していない。
- 他のプラットフォームから渡された情報の保護（要件７）
  - データがシステムから外に出る際のアクセス制御は、FIWARE 標準の認証・認可機能で可能である。しかし、複数システムの連携のためのセキュリティ機能、例えば、複数システム横断的なトレースバック等の機能は備えていない。
- プライバシー保護（要件８）
  - データを FIWARE 外に送る際の匿名化については、標準のコンポーネントとしては採用されていない。どのように匿名化するかはデータ依存であり、サービスごとに適切な匿名化方法を実装する必要がある。従って、具体的な要件は、本報告書の対象外とする。
- システム横断的なモニタリング（要件９）
  - FIWARE の GE には、連携したシステム全体をモニタリングする機能を提供するコンポーネントは無い。

5.3 日本のスマートシティ IoT 基盤に求められるセキュリティ機能

5.3.1 １つの IoT システム内のセキュリティ機能

日本のスマートシティ IoT 基盤は、プラットフォームを堅牢にするための真正性検証機能と、プラットフォーム上のデータの流通を制御するためのデータ流通制御機能を備えることが望ましい。これにより、不正なデバイスが存在しない健全なプラットフォームの上で、

確実に情報流通を制御することができ、情報の不正利用や漏えいを無くすことができる。また、真正性の検証について、スマートシティ IoT では、攻撃者がデバイスに直接アクセスする可能性が高いことから、例えば、 Trusted Platform Module(TPM)や、Trusted Execution Environment(TEE)などのようなセキュリティハードウェアを利用した真正性確認の導入が考えられる。

加えて、システムが正常に動作しているかをモニタリングし、異常があれば対処・復旧を行う SOC (Security Operation Center)を構築し、インシデントに迅速に対応できるスマートシティ運用の実現が求められる。スマートシティ IoT は、デバイスの数や種類が多いという特徴があり、今までのような人手による状況把握や分析は難しいと考えられるため、自動化技術や機械学習技術の導入などが考えられる。また、インシデントへの迅速な対応や復旧のために、分析のフェーズだけではなく、状況把握・分析・対処の一連の流れが自動化されることが望ましい。

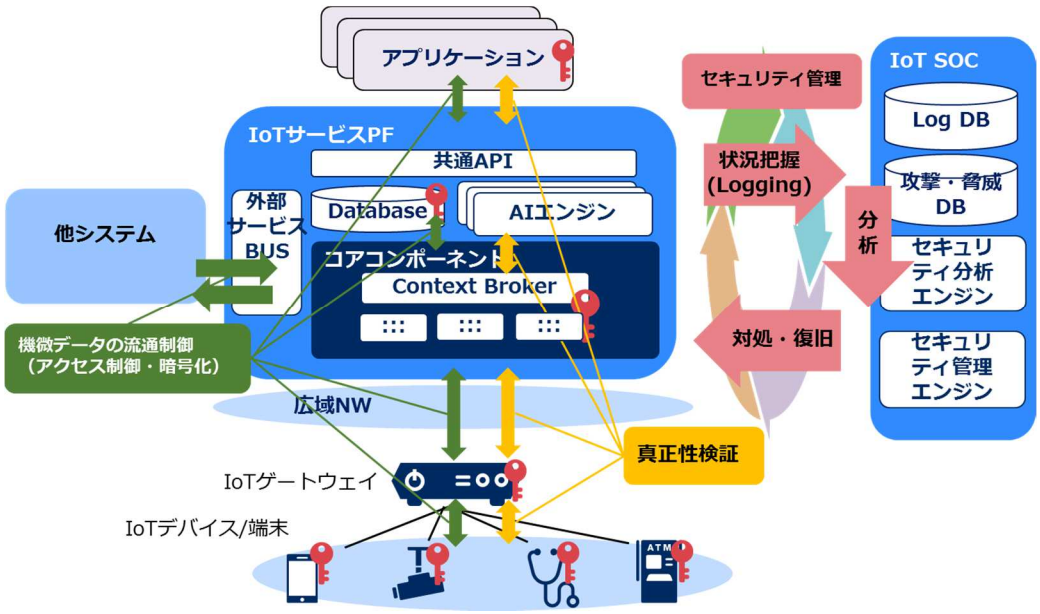


図 22　日本のスマートシティ IoT のセキュリティ機能

5.3.2　システム連携時のセキュリティ機能

日本のスマートシティ IoT では、ドメインを超えたデータ流通を実現し、新たなサービスを創出することが目的の 1 つである(図 23、図 24)。ドメインを超えたデータ流通では、4 章で述べたように、以下のセキュリティ機能が必要である。

- 複数システム間の認証連携
  - 複数のシステムを統合する際、それぞれのシステムが ID 管理機能を持つ場合は、認証の連携が必要になる。FIWARE の標準は、OAuth 2.0 と XACML を用いて認証と認可を行っているが、それらを拡張することによる認証連携が考え

られる。

- 複数システム横断的なアクセス制御と情報のトレースバック
  - 単一システムでの情報流通制御でも述べたように、機微なデータは、その生成から消滅まで、一貫して管理されることが望ましい。この要件は、複数のシステムの場合であっても同様である。すなわち、情報が他のシステムに渡った後でも、その情報を扱うべきソフトウェアコンポーネントやユーザのみがその情報にアクセスできるように制御されることが望ましい。また、情報の生成元のシステムと、情報を渡した先のシステムの情報のトレースログを突合せ、データのトレースバックをシステム横断的に行う必要がある。
- 複数のシステムのインシデントレスポンスと、それを支える運用体制
  - 4.3 でも述べたように、JPCERT/CC では、「インシデント対応マニュアルの作成について」[12]の中で、インシデントに対応する人及び組織の明確化の必要性を述べている。スマートシティ IoT においても、インシデント発生時に全体の統括を行うチームが必要である。組織横断的なインシデントハンドリングは、一般的な IT でも取り組みが始まりつつあり、スマートシティ IoT ではどのような体制になるべきかを、今後検討する必要がある。

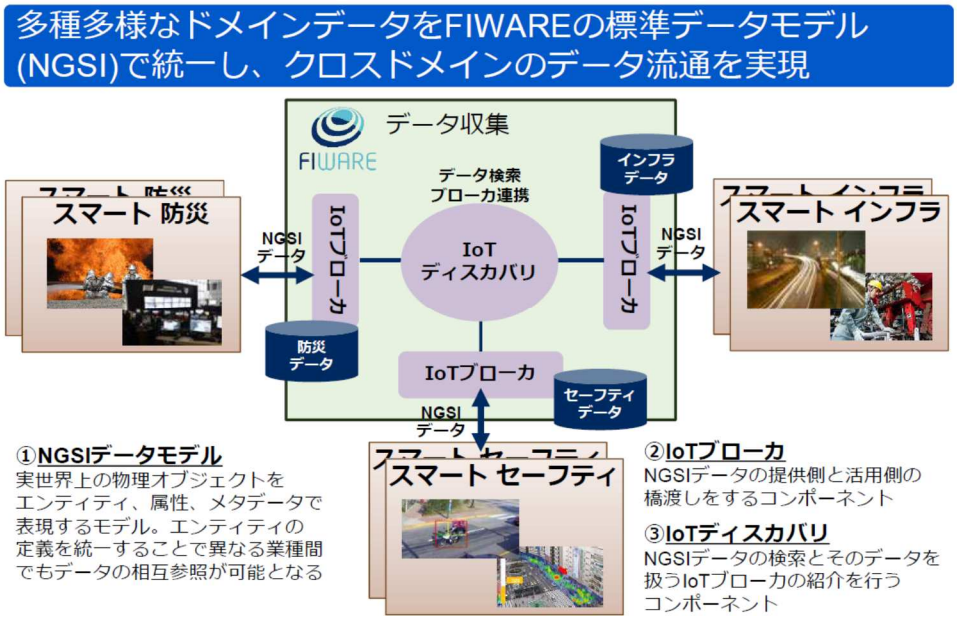


図 23　クロスドメインのデータ流通[15]

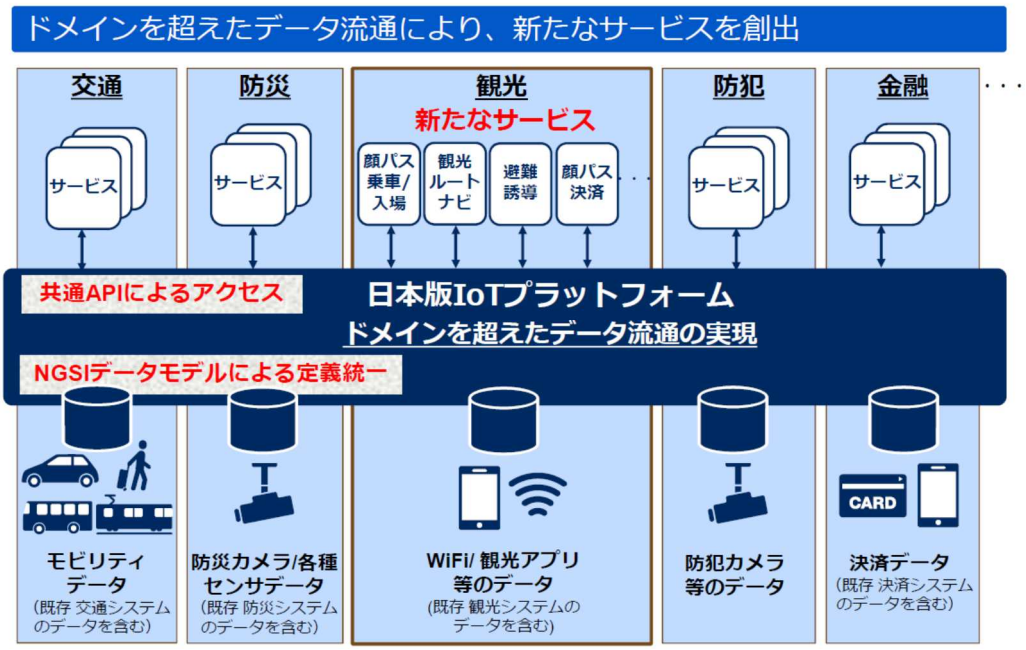


図 24　ドメインを超えたデータ流通による新サービスの創出[15]

6　まとめと提言

上の分析に基づき、安全なスマートシティを実現するために、以下の要件を提言する。

個々の IoT システムにおけるセキュリティ要件

スマートシティ IoT では、IoT 機器が町中に配置されるため、不正な物理的アクセスの脅威にさらされている。更に、システムの正常な動作の保障と、機微な情報を安全に活用するために、データの保護が必要である。従って、以下の 2 点を提言する

- IoT 機器の成りすまし、改ざんに対する防止・検知・除去機能をシステムとして具備すること【要件１～３】
- データ漏えい、改ざんの防止機能、データトレーサビリティ機能をシステムとして具備すること【要件４、５】

複数システム連携時におけるセキュリティ要件

複数のシステム間で情報が流通する際には、情報漏えいリスクや、運用主体が複数組織にまたがることによるセキュリティ運用の課題がある。従って、以下の 2 点を提言する。

- システム間の認証連携やデータトレーサビリティ、システム横断的なアクセス制御の仕組みを具備すること【要件６～８】
- システム横断的なシステムモニタリング機能、セキュリティ運用・監視体制をもつこと【要件９】

WG メンバー

谷本　哲郎	アクセンチュア株式会社
下堀　昌広	インテル株式会社
片山　智	シスコシステムズ合同会社
佐々木　淳一	シスコシステムズ合同会社
池田　昭雄	株式会社シマンテック
桜井　重宣	株式会社シマンテック
金田　智史	株式会社シマンテック
和歌　宏享	トレンドマイクロ株式会社
萩原　健太	トレンドマイクロ株式会社
辻　秀典	ネットワンシステムズ株式会社
石井　保弘	ネットワンシステムズ株式会社
宇野　誠	マカフィー株式会社
田室　秀行	マカフィー株式会社
山田　淳史	マカフィー株式会社
佐々木　弘志	マカフィー株式会社
岩野　圭一郎	新日鉄住金ソリューションズ株式会社
青山　修二	一般社団法人オープンガバメント・コンソーシアム
立道　豊典	日本電気株式会社
藤田　範人　(座長)	日本電気株式会社
石倉　禎志	日本電気株式会社
佐々木　貴之	日本電気株式会社
岩隈　聖子	日本電気株式会社
荒尾　千秋	日本電気株式会社

参考文献

[1] 米国におけるスマートシティに関する取り組みの現状
https://www.ipa.go.jp/files/000048357.pdf

[2] Jorge Vargas, Daniel Bergonzelli, アルゼンチン ティグレ市の 未来を守るビデオ解析ソリューション, NEC 技報 Vol.67 No.1（2014 年 11 月）
http://jpn.nec.com/techrep/journal/g14/n01/pdf/140116.pdf

[3] 会津若松市,「スマートシティ会津若松」の実現に向けた取組について
http://www.city.aizuwakamatsu.fukushima.jp/docs/2013101500018/

[4] 会津若松市, スマートシティ会津若松 ～ICT を活用した様々な取組～
https://ogc.or.jp/wp/wp-content/uploads/2016/02/6-2_Panel_MrMurai.pdf

[5] 会津若松市 IoT ヘルスケアプラットフォーム事業、会津地域スマートシティ推進協議会、 http://www.midika-iot.jp/wp-content/uploads/2016/07/④会津若松スマートウェルネスシティ IoT ヘルスケアプラットフォーム事業.pdf

[6] シスコシステムズ合同会社, スマートシティの事例
http://www.soumu.go.jp/main_content/000447791.pdf

[7] FIWARE, https://www.fiware.org/

[8] ENISA, Cyber security for Smart Cities, 2016
https://www.enisa.europa.eu/publications/smart-cities-architecture-model

[9] ENISA, Cyber Security and Resilience of Intelligent Public Transport, 2016
https://www.enisa.europa.eu/publications/good-practices-recommendations

[10] トレンドマイクロ株式会社, IoT セキュリティガイドライン － デバイスライフサイクルの概要 －, 2016
https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=214

[11] 株式会社シマンテック, IoT の参照アーキテクチャ
https://www.symantec.com/content/ja/jp/enterprise/white_papers/iot-brochure-final-sr-101515-jp-w.pdf

[12] JPCERT/CC, インシデント対応マニュアルの作成について
https://www.jpcert.or.jp/csirt_material/build_phase.html

[13] IEC, Orchestrating infrastructure for sustainable Smart Cities
http://www.iec.ch/whitepaper/pdf/iecWP-smartcities-LR-en.pdf

[14] Smart city framework – Guide customer service to establishing strategies for smart cities and communities, BSI Standards Publication
http://shop.bsigroup.com/upload/267775/PAS%20181%20(2014).pdf

[15] 日本電気株式会社, スマートシティを実現する IoT プラットフォーム FIWARE について
http://www.soumu.go.jp/main_content/000449824.pdf

[16] 産業競争力懇談会 ２０１５年度 プロジェクト 最終報告、IoT 時代におけるプライバシーと イノベーションの両立、http://www.cocn.jp/thema84-L.pdf
[17] 高橋克巳、匿名化技術の現状について
http://www.kantei.go.jp/jp/singi/it2/pd/wg/dai1/siryou2_3.pdf
[18] 経済産業省 情報プロジェクト室、マイナンバー制度の 民間活用について
http://www.meti.go.jp/policy/it_policy/id_renkei/150917_1_METI.pdf
[19] 総務省、公的個人認証サービスの利活用推進に向けた取組
http://asist.ssr.titech.ac.jp/wp-content/uploads/a6c8b0d62ef7351360d0afb931331eed.pdf
[20] ITU-T、Overview of the Internet of things、
http://www.itu.int/rec/T-REC-Y.2060-201206-I
[21] NEC、プレスリリース、スペイン サンタンデール市におけるゴミ収集管理サービスの高度化事業に参画、http://jpn.nec.com/press/201410/20141006_03.html
[22] NEC, Wellington City Council
http://www.nec.com/en/case/wellington/index.html
[23] オープンガバメント・コンソーシアム、組織対応力ベンチマーク
https://ogc.or.jp/wp/wp-content/uploads/2015/06/benchmark_checksheet_detail_pdf.pdf
https://ogc.or.jp/wp/wp-content/uploads/2015/06/benchmark_commentary_Ver.1.0.pdf
[24] FIWARE、https://www.fiware.org/
[25] Juanjo Hierro, BigData for Smart Cities: FI-WARE and FI-Lab proposition,
https://bscw.fi-ppp.eu/pub/bscw.cgi/d69198/Session05_5%20Hierro.pdf
[26] Estonian Information Systems's Authority, X-Road
https://www.ria.ee/public/x_tee/xRoadOverview.pdf
[27] McAfee, Secure IoT Devices to Protect Against Attacks,
https://www.mcafee.com/ca/resources/solution-briefs/sb-quarterly-threats-mar-2017-1.pdf