Computer Security Symposium 2017
23 - 25 October 2017

スマートシティ基盤のセキュリティ脅威分析と対策

森田 佑亮[†1]　濱本 亮[†1]　佐々木 貴之[†1]　三好 一徳[†1]　小林 俊輝[†1]

概要：近年，世界の様々な都市でスマートシティへの取り組みが始まり，スマートシティが高効率な社会の構築に寄与することが実証されつつある．一方，公共システムへのサイバー攻撃は世界各地で発生しており，各都市がスマートシティの取り組みを成功させるためには，セキュリティ対策が不可欠となっている．セキュリティ対策の第一歩としては，モデル化したシステムに対する脅威分析が必須である．しかし，これまでに提案されているシステムモデルは，様々な団体が独自に設けたユースケースに特化されているため，スマートシティの一般的な脅威の抽出は難しい．そのため，ユースケースに依存しない一般化されたシステムモデルが必要である．そこで本稿では，様々な標準化団体が発行しているホワイトペーパや提言を基に抽象化したスマートシティのモデルを設計する．次に，抽象化されたモデルに対してセキュリティ脅威分析を行うことで，スマートシティの一般的なセキュリティ課題の抽出を試みる．

キーワード：IoT, スマートシティ，セキュリティ脅威分析，プラットフォーム

A Security Analysis and Countermeasure for Smart City Platform

Yusuke Morita[†1]　Ryo Hamamoto[†1]　Takayuki Sasaki[†1]　Kazunori Miyoshi[†1]
Toshiki Kobayashi[†1]

Abstract: Recently, smart cities have been spread all over the world. Numerous reports show that the smart cities can contribute to realize a highly efficient society. On the other hand, cyber-attacks have been occurred in many countries. Thus, countermeasures against such attacks are inevitable to achieve the smart cities successfully. As the first step, a threat analysis for the system model of the smart city is necessary. However, since the existing system models are specific to use cases which various organizations originally assume, it was difficult to extract general threats for the smart cities. Therefore, a generalized system model which is independent from use case has been required. This paper describes the design of the generalized smart city model based on the white papers and proposals which are published by several standards bodies. General security issues of the smart cities are successfully extracted by threat analyses using the generalized model.

Keywords: IoT, Smart City, Security Analysis, Platform

1. はじめに

近年，インフラ設備から車や家電まで様々なモノが繋がる Internet of Things (IoT)が急速に広がりつつある．特に，世界各地の自治体や公益事業会社は，IoT を活用して顧客や都市の様々な情報を収集し,利活用する事により,行政，交通，産業，医療・健康，安全，インフラなどにおける資源の効率的な運用管理を促す「スマートシティ」の取り組みを始めている．しかし，スマートシティによって高効率な社会が実現可能であることが実証されつつある一方で，IoT やスマートシティを構成するシステムに対するサイバー攻撃は社会的影響の強い事例が増加傾向にある.例えば，2016 年 11 月，アメリカのサンフランシスコ市営鉄道のシステムがランサムウェアの攻撃を受け，券売機が使用不可となる事例が発生した[1]．この攻撃によってサンフランシスコ市営鉄道は乗車を無料とする対応を取り，大きな損害を被った．その他には，2015 年 12 月，ウクライナのイヴァーノ＝フランキーウシク州で電力システムが攻撃を受け数時間に及ぶ停電が発生[2]した事例や，2015 年 5 月，日本で日本年金機構の管理する個人情報の一部(約 125 万件)が，不正アクセスにより外部に流出[3]した事例などが知られている．このような公共性の高いシステムへのサイバー攻撃が出現している状況下において，スマートシティを都市基盤として定着させるためにはセキュリティ対策が不可欠である．

セキュリティ対策の立案に先立ち，システムに対してどのような脅威が存在しているのかを整理するために脅威分析を行う必要がある．脅威分析を行うには対象となるシステムのモデル化が必要となるが，スマートシティについては様々な団体が独自に想定したユースケースに特化したモデルでしかこれまで検討されていない．そのため，従来のモデルに対して脅威分析を実施しても，各ユースケースに特化した脅威の抽出しかできず，スマートシティの一般的な脅威の抽出は難しい．スマートシティにおける一般的な脅威を抽出するためには，ユースケースに依存しない一般化されたシステムモデルが必要であり，そのモデルに対する脅威分析が求められる．

そこで本稿では，様々な標準化団体が発行しているホワ

†1 日本電気株式会社 セキュリティ研究所

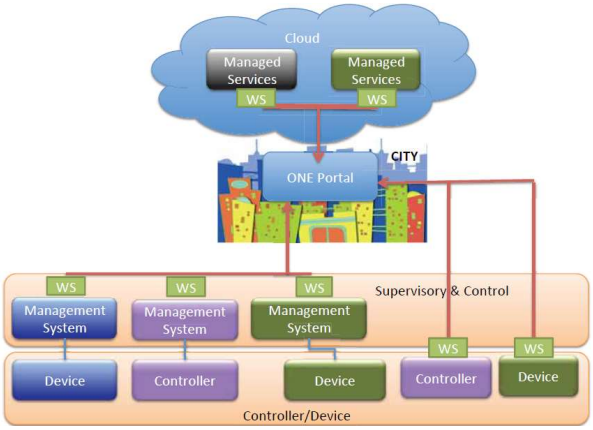

図 1　ポータルサーバを利用したスマートシティの構造[4]

イトペーパや提言を基に，特定のユースケースに依存しない抽象化されたスマートシティのシステムモデルを設計する．次に，提案するスマートシティのモデルに対してセキュリティ脅威分析を行うことで，スマートシティに対する一般的なセキュリティ課題の抽出を試みる．結果として提案するモデルを使うことでスマートシティにおける一般的な脅威を抽出することができた．

以降の章構成を示す．第 2 章では各団体が公開しているスマートシティの規格や提言についてまとめる．第 3 章では，第 2 章の規格や提言に基づいて一般的なスマートシティのモデルを提案する．第 4 章にて提案するモデルに対する脅威分析を行い，第 5 章でその分析結果を考察・議論する．第 6 章で本稿のまとめと今後の課題について述べる．

2. スマートシティの規格や提言

スマートシティの規格は，現状では標準化されておらず，様々な団体がスマートシティのホワイトペーパや提言を発表している．本章では，各標準化団体が発表した規格や提言を紹介する．

2.1 International Electrotechnical Commission

図 1 は，International Electrotechnical Commission (IEC) のホワイトペーパ[4]に記載されているスマートシティのシステムモデル例である．IEC のモデルでは，スマートシティには 2 種類のデータ流通経路が存在する．第 1 の流通経路は情報を集めるセンサーが低コストの通信モジュールを介して，都市インフラをリアルタイムに管理・分析するクラウドのアプリケーションへと送信する縦方向のフローである．これは，一般的な IoT アーキテクチャとして認識されている International Telecommunication Union (ITU) の Telecommunication Standardization Sector (ITU-T)が発行している Overview of the Internet of things[5]で示される IoT reference model (図 2)で議論されているデータ流通とほぼ同様の構成である．

第 2 の流通経路は，ONE Portal(OP)を介して異なる IoT

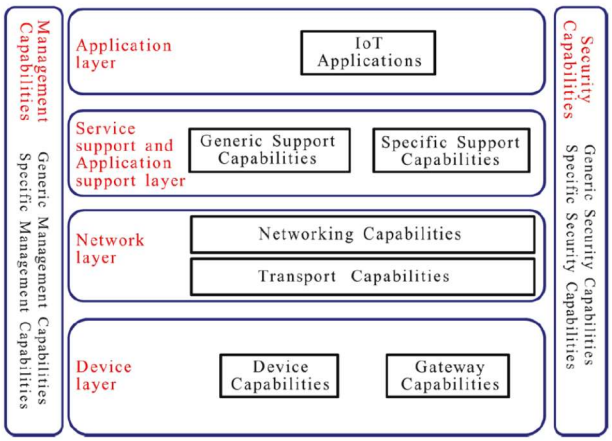

図 2　ITU-T の IoT reference model[5]

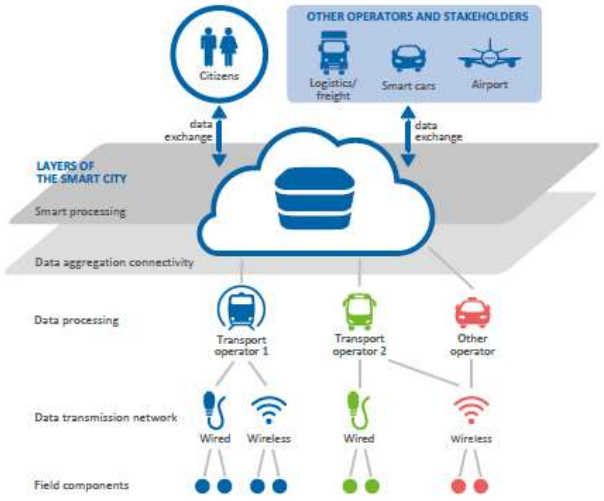

図 3　スマートシティにおける公共交通機関アーキテクチャ[6]

システム間で情報をやり取りする横方向のフローである．OP は既存の各種 IoT システムを集中管理し，連携させる機能を持つ．従って，スマートシティ構築以前に存在していた IoT システムと，構築後に新たに作られた IoT システムとを統合的に運用管理できる．OP の活用例として，地理情報を管理する IoT システムと天気予報を実現する IoT システムの連携による災害警告サービスや，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による高精度なナビゲーションサービスがある．ITU-T の IoT reference model と IEC のモデルとの大きな違いは，OP による横方向のフローの存在である．以上より，IEC の提唱するスマートシティモデルは複数の一般的な IoT システムとそれらを束ねる連携部分で構成される．

2.2 The European Union Agency for Network and Information Security

The European Union Agency for Network and Information Security (ENISA) はスマートシティにおける公共交通機関のアーキテクチャモデル[6]を発表している(図 3)．ENISA で示されるアーキテクチャは Connected City (CC)と

Smart City (SC)の 2 つに分けられる．CC は図 3 の下位 3 層に，SC はその上位層に対応する．CC は Field components, Data transmission, Data processing によって構成される. Field components はセンサーやアクチュエータ等の実世界に作用するデバイスを想定しており, Data transmission は通信モジュールなどのデータ転送用のデバイス，Data processing は Field components からのデータを統合し，システムの状態を可視化する等の役割を想定している．

この構成や構成要素の機能は，2.1 節で述べた IEC の IoT アーキテクチャにおける縦方向の流通経路と同一であり，一般的な IoT アーキテクチャと大きく変わらない. つまり，CC は複数の IoT システムによって構成されていると言える．しかし，CC 内の IoT システムは，構成によっては直接別の IoT システムに情報を提供することができないケースがある．そこで SC 部分に定義された，CC 内の各 IoT システムの情報を集約あるいは交換する Data aggregation connectivity 層と各システムの情報を相関させて，システム全体としての決定を下す Smart Processing 層により，CC 内に存在する複数の IoT システムを連携させる. この構成は，IEC が議論しているスマートシティのアーキテクチャと類似点が多く，とりわけ，各 IoT システム間での情報交換および連携により有益な情報を生み出すという思想を実現するために要求される機能は同一である．

2.3 British Standards Institution

British Standards Institution (BSI) は Smart city framework [7]を発行し，電力システムや水道システム等の異なるシステム間で，サービスやデータを連携させたモデルを提案している．BSI は異なるシステムが保有するデータを統合していくことで，新たなサービスの出現や効率化イノベーションが生まれるとしている. IEC や ENISA などの提言では IoT システムを連携させることによって，高度なサービスを実現できるとしているが，この点で BSI の主張と一致している．そのため，スマートシティのアーキテクチャとしても連携部 IEC や ENISA と著しく乖離することは無いと言える．

以上，IEC，ENISA，BSI 等で議論および定義されているスマートシティのシステムモデルを参照すると，スマートシティは複数の IoT システムと，それらを接続/連携し新たな情報の生成と意思決定を下すシステムの 2 つの要素で構成されると考えられる．この点を踏まえて，次節では一般化されたスマートシティのモデルを設計する．

3. 一般化スマートシティモデルの設計

本章では，第 2 章で確認したスマートシティのシステムモデルの共通点などを基に一般化したスマートシティのシステムモデル(提案モデル)を設計する．設計は下記の手順に従う．

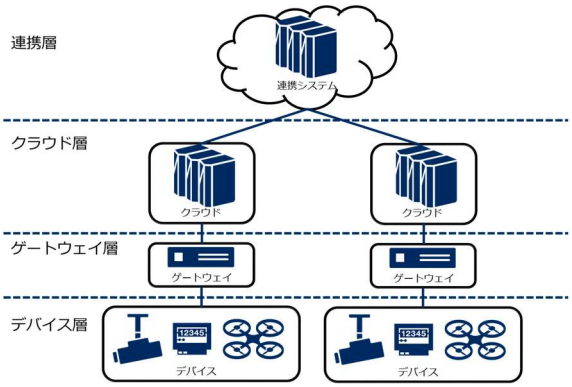

図 4　一般化したスマートシティの概念

① IEC，ENISA，BSI で示されているスマートシティのモデルから，共通点を抽出し抽象化されたスマートシティの構成要素を整理する
② ①にて整理された各構成要素の持つ役割を整理する
③ ②にて整理した役割を基に，スマートシティにおいて各構成要素に要求される機能を整理する

3.1 スマートシティの構成要素

第 2 章より，IEC，ENISA，BSI で提案されているスマートシティに以下の共通点があることが明らかになった．

(1) 複数の IoT システムを統合・連携したプラットフォームであること
(2) IoT システムの構成要素はほぼ共通しており, いずれのモデルでもデバイス/アクチュエータ，データ転送モジュール，システム管理/データ分析機能を備えること
(3) IoT システムを連携させる部分については, 構成は違うものの担う役割については複数の IoT システム間の情報交換，情報の集約，連携であること

そこで，これらのシステム連携機能を 1 つの層として定義する事でスマートシティのモデルを抽象化(一般化)する．一般化したスマートシティの概念を図 4 に示す．

以降，より抽象化した表現を行うために，便宜上デバイス/アクチュエータが存在する層をデバイス層, データ転送モジュールが存在する層をゲートウェイ層，システム管理/データ分析などを行う層をクラウド層，各 IoT システム間の情報交換や情報の集約および連携を行う層を連携層と呼ぶ. 一般化したスマートシティのモデルはこれら 4 つの層によって定義される．

3.2 各層の役割

ここでは, 3.1 節で定義した層が担う役割について整理する(表 1).

デバイス層はデータ収集や実世界に作用する役割を担い，ゲートウェイ層は複数デバイスからのデータ収集とク

表 1　各層の役割

層	役割
連携層	IoT システム間の情報交換，情報の集約，連携.
クラウド層	システム管理，データ分析.
ゲートウェイ層	複数デバイスからのデータ収集と転送.
デバイス層	データ収集，物理的な動作.

表 2　各層に要求される機能

層	機能
連携層	IoT システム間の情報の授受, IoT システムから受信した情報の蓄積, 複数 IoT システムの情報を基にした情報の生成
クラウド層	情報の蓄積/加工/表示, IoT システムの操作
ゲートウェイ層	複数デバイスとの接続，データ転送
デバイス層	感知，計測，運動

ラウド・デバイスへのデータ転送を行う．クラウド層はデバイス層からのデータに基づいたシステム管理やデータ分析を行う．連携層は，前節でも触れた通り IoT システム間の情報交換・集約・連携という役割を担う．

3.3　各層に要求される機能

本節では，各層を構成する機能について整理する(表 2)．デバイス層は，データ収集と物理的な動作を担うため，感知，計測，運動の機能が必要となる．ゲートウェイ層は，複数デバイスからのデータ収集と転送を担うため，複数デバイスとの接続，複数プロトコルの解釈，データ転送の機能が要求される．クラウド層は，デバイスで取得したデータの分析とシステム管理を担うため，情報の蓄積，情報の加工，情報の表示，IoT システムの制御といった機能が要求される．連携層は，IoT システム間の情報交換，情報の集約，連携といった役割を持つため，IoT システム間の情報の授受，複数の IoT システムからの情報の蓄積，複数 IoT システムの情報を基にした情報の生成といった機能が要求される．

4.　脅威分析

本章では，第 3 章で作成したスマートシティのシステムモデルを用いて脅威分析を行い一般的なスマートシティにおける脅威の抽出を試みる．

4.1　脅威分析の手法

脅威分析とは，対象システムに存在する脅威を抽出することである．脅威分析の手法としては，セキュリティ要件から脅威を導出する方法や Microsoft が提唱する STRIDE*

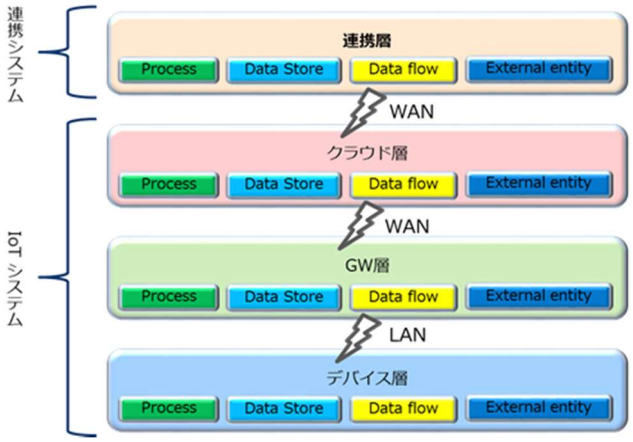

図 5　各層の構成イメージ

脅威モデル[8]などが知られている．前者はシステム内で守るべき資産と，その資産を操作するアクターを明確にしなければならないため，今回の一般的なスマートシティモデルに対する脅威分析では不向きである．そのため，本稿では STRIDE 脅威モデルを使用した脅威分析を行う．STRIDE 脅威モデルによる具体的な脅威分析手法として STRIDE per Element，STRIDE per Interaction が知られている[9]．

2 つの分析手法は共に，システム内を流通するデータの流れを把握するためのデータフロー図を使用して脅威分析を行う．一方，STRIDE per Element がデータフロー図内のコンポーネント毎に脅威を検討する手法であるのに対して，STRIDE per Interaction はコンポーネント間の相互作用に着目して脅威を検討する手法である点が異なる．STRIDE per Element は STRIDE per Interaction に比べて，短時間かつ正確に脅威を抽出する事が可能である[10]ため，本稿では STRIDE per Element を採用する．

STRIDE 脅威モデルによる脅威分析は下記の 2 つの手順で脅威を抽出する．

(1) システムやアプリケーションをコンポーネントなどで構成されるデータフロー図で記述する

(2) 記述したデータフロー図内の各コンポーネント等に対し STRIDE の 6 つの観点で脅威を特定する

以下，4.2 節でデータフロー図を作成し，4.3 節でその構成要素である各コンポーネントについて説明する．

4.2　データフロー図の作成

各層の構成イメージを図 5 に示す．データフロー図を作成するにあたり，一般化したスマートシティのモデルでは，そのシステムを構成するコンポーネントについても抽象度の高い表現を採用する必要がある．そのため，データフロー図の各コンポーネントについて具体的な表現を避け，Process，Data flow，Data store，External entity といったデ

* STRIDE は，Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege の頭文字である

表 3　コンポーネント間のデータフローの有無

Destination \ Source	Process	Data store	External entity
Process	—	○	○
Data store	○	—	○
External entity	○	○	—

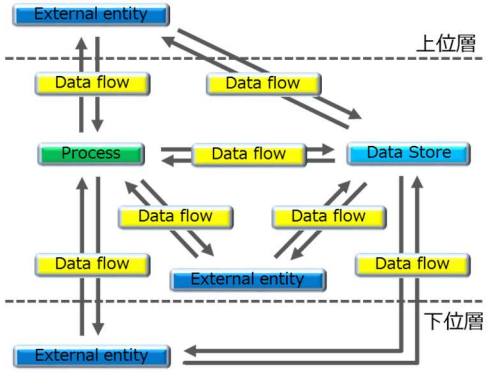

図 6　各層のデータフロー図

ータフロー図で用いられる表現をそのまま採用することとする．ここで，Process はデータの入力を受け，加工等の処理を施した後，結果を出力するコンポーネントを指し，Data Flow はコンポーネント間でやり取りするデータを指す．また，Data Store は情報を一時的または長期的に保持するコンポーネントを指す．External entity は，外部に存在するシステムなどの実体を指し，代表例としてコンポーネントを取り巻く環境や他の層のコンポーネント，オペレータからの入力を含む．

通常，データフロー図は，システムの入出力やコンポーネント間のデータフローが固定されたものを表現する際に記述する．しかし今回は，対象が一般化された(抽象度の高い)スマートシティのモデルであるため，その抽象度を下げることなくシステムの入出力やコンポーネント間のデータフローについて網羅的に表現することが望ましい．そこで，Process，Data store，External entity の 3 種類のコンポーネントのうち，2 つのコンポーネントの間を流れる全ての Data Flow を整理すると，表 3 に示す 6 通りとなる．

なお，簡略化のために Process - Process 間のデータフローについては，それら複数の Process を 1 つの Process と見なしてデータフローが存在しないものとした．また，Data store - Data store 間のデータフローも同様に，それら複数の Data store を 1 つの Data Store と見なすことで，データフローは発生しないとしている．External entity - External entity 間で発生するデータフローは全て対象のシステム外で発生している事象のため今回の脅威分析では除外した．

以上，表 3 に示したコンポーネント間のデータフローの有無と，他の層のコンポーネントを External entity とした表現した場合に各層のデータフロー図は図 7 のように表現することができる．

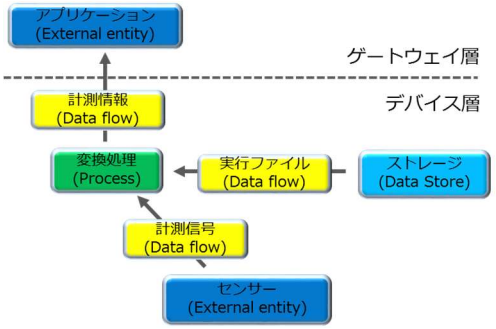

図 7　機能に従ったコンポーネントの定義例

4.3 各層におけるコンポーネントの意味付け

第 3 章で述べた通り，一般化したスマートシティを構成する各層は，層毎に担う役割と機能が異なるため，作成したデータフロー図の各コンポーネントは同一の名称であっても，各層でそれぞれ異なる存在である．そのため，脅威分析を行うにあたっては，各コンポーネントが何を意味するかを意味付ける必要がある．

コンポーネントの意味付けは，第 3 章で定義した各層の機能を図 6 のデータフロー図に当てはめることによって行う．例えば，デバイス層はデータ収集や物理的な動作を行うことを役割としているため，感知，計測，運動といった機能を備えていると考えられる．さらに，計測という機能を例に，図 6 のデータフロー図に当てはめると，デバイス層の Process，Data store，data flow，External entity および上位層は図 7 に示すデータフロー図で表現できる．図 7 は，ストレージから読み出された実行ファイルで変換処理が動き出し，センサーが生成した計測信号を変換処理により計測情報に変換してゲートウェイ層に送信する手順を表現している．

以上，4.2 節および 4.3 節の手順を各層の機能数分だけ繰り返すことで，システム全体のデータフロー図を作成し，STRIDE 脅威モデルを用いた脅威分析を行う．

5. 脅威分析結果

脅威分析の結果の正当性を検証するためには，既存の分析結果との比較が必要である．筆者らの知る限り，本稿はスマートシティに関する脅威分析を行った初めての論文であるため，比較すべき対象は存在しない．しかし，スマートシティは

1) 複数の IoT システム層と，

2) それらを接続/連携し新たな情報の生成と意思決定を下す連携システム層，

の 2 つの要素で構成されることが，第 2 章での検証の結果明らかになっており，1)の一般的な IoT システムについては既に IPA[10]などが脅威分析を行っている．そこで本稿で

は，1)の IoT システム層について詳細な脅威分析を行い，2)の連携システム層については簡単に述べるに留める．連携システム層，および IoT システム層と連携システム層とを併せた詳細な脅威分析は今後の課題とする．

IoT システム層の各層に対して行った脅威分析の結果をそれぞれ表 4，表 5，表 6 に示す．まず，各層で共通した脅威として，システム管理者(保守者)へのなりすましや，システム内の通信に対する盗聴・改竄，システムのコンポーネントやネットワークへの DoS 攻撃などが挙げられる．これらの脅威例は，IPA が発行している IoT 開発におけるセキュリティ設計の手引き[11]などでも指摘されている脅威であり，一般化したスマートシティのモデルを使用して脅威分析を行った場合でも同様の脅威を抽出する事ができた．

次に，IoT システム層の各層に特徴的な脅威について説明する．

(1) デバイス層：デバイス層における脅威の特徴は，物理的な脅威が多い点である．これは，デバイス層がデータ収集や実世界に作用する機能を持つという特徴が要因にある．デバイスが現実世界に影響を与えることができるということは，攻撃者の視点に立つと対象のデバイスに物理的にアクセスしやすいことになる．そのため通常の IT システムに比べて物理的に攻撃を受ける可能性が高くなる．また，一方で攻撃者が行った攻撃の結果，デバイスのアクチュエータが不正な動作をする場合，現実世界に影響を与える．例えば車や医療機器へのハッキングは，人命に多大な影響を与える．デバイス層への攻撃を防ぐためには，デバイスへの物理的なアクセスの制限と，不正デバイスがシステム内で動作しない仕組みを検討する必要がある．

(2) ゲートウェイ層：ゲートウェイ層における特徴的な脅威は，物理的なネットワークの遮断である．IoT システムでは，ゲートウェイがデバイスと LAN で接続されるケースも容易に考えられるが，この場合はゲートウェイも攻撃者から物理的にアクセスする事が比較的容易な環境に置かれる可能性が高い．その場合はケーブルの切断など物理的にネットワークを遮断される可能性がある．また，物理的にゲートウェイを差し替える，直接的にゲートウェイを操作される，といった可能性もある．さらに，ゲートウェイが管理しているネットワーク(WAN/LAN)に着目すると，キャリアによって管理され，かつ複数経路(3G/LTE など)によって冗長化されている WAN に比べて LAN はその信頼度は低く，攻撃を受けやすいことも脅威である．これらの脅威に対応するためには，デバイス層と同じく物理的なアクセスを制限する事に加え，通信経路の冗長化が必要である．

(3) クラウド層：クラウド層の特徴的な脅威は，IoT システムの管理情報やサービスで使用する情報の漏洩や改竄である．クラウド層は IoT システムの中でも重要な情報(システム設定や IoT システムを制御するための情報)を保持するため，ゲートウェイ層やデバイス層以上に情報の管理を徹底する必要がある．特にこれらの脅威は連携層との通信でその影響が強く現れる．例えば，連携する正規の外部サービスに成り済ましてクラウド層の情報にアクセスされ，情報を改竄されることは容易に想定できる．また，外部からクラウドのサーバに対して大量のトラヒックを送ることで DoS 攻撃が発生する可能性もある．さらに，正規の外部サービスとして取得した情報を不正に外部に流出される可能性もある．クラウド層の情報を保護するためには，上位層に当たる連携層に対して，アクセス制御や情報の流通先を制限する技術が必要となる．

最後に連携システム層での特徴的な脅威を簡単に述べる．連携システム層では管理者の異なるシステムを連携させるため，連携相手の悪意ある行動が，スマートシティを運用する際に致命的な影響を発生させる．この対策として，連携システム層では管理者の異なるシステムが提供する情報やシステムそのものの検証機構が必要である．

以上，本稿で提案したモデルを脅威分析することで，IPA が述べている各層に共通的な脅威だけでなく，各層での特徴的な脅威も抽出できた．したがって，提案モデルは一般的なスマートシティの IoT システム部分の脅威分析に有効であると考える．

6. おわりに

世界中の様々な都市でスマートシティへの取り組みが検討され始めている．スマートシティによって人々の生活の利便性が向上することが実証されつつあるが，その一方で，強固なセキュリティ対策が不可欠である．セキュリティ対策の第一歩として，モデル化したシステムに対する脅威分析が必須であるが，これまでに提案されているスマートシティのシステムモデルは，様々な団体が独自に設けたユースケースに特化されているため，スマートシティの一般的な脅威の抽出は困難であった．

そこで本稿では，様々な標準化団体が発行しているホワイトペーパや提言をもとに，大きく IoT システムと連携システムの 2 つのシステムで構成される一般化スマートシティのモデルを設計した．次に，抽象化されたモデルに対してセキュリティ脅威分析を行うことで，スマートシティの一般的なセキュリティ課題の抽出を試みた．設計したモデルを脅威分析した結果，IoT システム部分については IPA が述べている各層共通的な脅威に加え，各層で特徴的であった脅威も抽出できていることを確認した．今後は，連携

システム部分で抽出した脅威の妥当性を検証し，本モデルの有効性を確認する必要がある．

参考文献

[1] Krebs on security, “San Francisco Rail System Hacker Hacked", https://krebsonsecurity.com/2016/11/san-Francisco-rail-system-hacker-hacked/, cited 2017.

[2] McAfee Blog, “ウクライナのサイバー攻撃が示す本当の脅威”, http://blogs.mcafee.jp/mcafeeblog/2016/01/post-748a.html, cited 2017.

[3] 内閣サイバーセキュリティセンター サイバーセキュリティ戦略本部, “日本年金機構における個人情報流出事案に関する原因究明調査結果”, https://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf, cited 2017.

[4] IEC, “Orchestrating infrastructure for sustainable Smart Cities”, http://www.iec.ch/whitepaper/pdf/iecWP-smartcities-LR-en.pdf, cited 2017.

[5] ITU-T, "Overview of the Internet of things", http://www.itu.int/rec/T-REC-Y.2060-201206-I, cited 2017.

[6] ENISA, “Architecture model of the transport sector in Smart Cities”, https://www.enisa.europa.eu/publications/smart-cities-architecture-model, cited 2017.

[7] BSI, “Smart city framework – Guide customer service to establishing strategies for smart cities and communities”, http://shop.bsigroup.com/upload/267775/PAS%20181%20(2014).pdf, cited 2017.

[8] A. Shostack, "STRIDE approach", http://blogs.microsoft.com/cybertrust/2007/09/11/stride-chart/, cited 2017.

[9] A. Shostack, “Threat Modeling: Designing for Security”, Wiley, 2014.

[10] 株式会社 FRRI, “Monthly Research 「STRIDE の変化形およびセキュリティ要件で導き出す脅威分析手法」”, http://www.ffri.jp/blog/2016/960/2016-11-11.htm.

[11] IPA, https://www.ipa.go.jp/, cited 2017.

[12] IPA, "IoT 開発におけるセキュリティ設計の手引き", https://www.ipa.go.jp/files/000052459.pdf, cited 2017.

表 4 クラウド層に対する脅威分析結果

Cloud Layer	S (spoofing)	T (Tampering)	R (Repudiation)	I (Information Disclosure)	D (DoS)	E (Elevation privilege)
Process	正規アプリケーションに成り済ます － 不正に情報を受信 － 不正に情報を配信 － 不正なプログラムの実行 － 不正な応答の返却	情報の改竄 － 設定ファイルの書き換え － プログラムの改竄(差し替え) － メモリの情報を改竄	操作・情報の否認 － 設定変更の否認 － 実行状況の否認 － ログの削除・変更	情報の流出 － 設定ファイルの流出 － ログ情報の流出 － 内外部から取得した情報の不正な配布	負荷の上昇・プログラムを停止 － 処理能力の著しい低下や処理の中断。	プログラムの脆弱性を突き、権限を取得
Data store	－	情報の改竄 － 管理用データベースの改竄 － サービス用データベースの改竄 － 課金情報の改竄	操作・情報の否認 － 設定変更の否認 － 実行状況の否認 － ログの削除・変更	情報の流出 － 管理用情報の流出 － サービス用情報の流出 － アカウント情報の流出	負荷の上昇・プログラムを停止 － DBへの要求不可。無応答。	－
Data flow	－	通信をフックし、改竄 － 入出力/操作/要求・応答など、各種情報の改竄	－	通信をフックし、盗聴 － 入出力/操作/要求・応答など、各種情報を不正に取得	ネットワーク負荷の上昇/通信の遮断/改竄 － ネットワーク負荷の上昇による転送遅延の発生 － ネットワーク負荷の上昇に起因した情報の消失 － 通信をフックされる事による通信の遮断や改竄	－
External entity	管理者、正規ユーザ、正規サービスに成り済ます － 管理者に成り済ました操作の実行 － 正規ユーザに成り済まし不正に利用 － 他人に成り済ました操作の実行 － 正規の外部サービスとして接続	－	操作・情報の否認 － 設定変更の否認 － 実行状況の否認 － ログの削除・変更	－	－	－

表 5　ゲートウェイ層に対する脅威分析結果

GW Layer	S (spoofing)	T (Tampering)	R (Repudiation)	I (Information Disclosure)	D (DoS)	E (Elevation privilege)
Process	正規アプリケーションに成り済ます －不正に情報を受信 －不正に情報を配信 －不正なプログラムの実行 －不正な応答の返却	情報の改竄 －設定ファイルの書き換え －プログラムの改竄(差し替え) －メモリの情報を改竄	操作・情報の否認 －設定変更の否認 －実行状況の否認 －ログの削除・変更	情報の流出 －設定ファイルの流出 －ログ情報の流出 －内外部から取得した情報の不正な配布	負荷の上昇・プログラムを停止 －処理能力の著しい低下。処理の中断。 －物理的なネットワークの遮断	プログラムの脆弱性を突き、権限を取得 HWの脆弱性を突き、権限を取得
Data Store	－	情報の改竄 －不揮発性メモリ内の情報を改竄	操作・情報の否認 －設定変更の否認 －実行状況の否認 －ログの削除・変更	情報の流出 －アカウント情報の流出	ストレージコンポーネントの破壊	－
Data Flow	－	通信をフックし、改竄 －入出力/操作/要求・応答など、各種情報の改竄	－	通信をフックし、盗聴 －入出力/操作/要求・応答など、各種情報を不正に取得	ネットワーク負荷の上昇/通信の遮断/改竄 －ネットワーク負荷の上昇による転送遅延の発生 －ネットワーク負荷の上昇に起因した情報の消失 －通信をフックされる事による通信の遮断や改竄	－
External Entity	管理者に成り済ます。 －管理者に成り済ました操作の実行 －不正GWへの差し替え －GWに対する直接的な操作	－	操作・情報の否認 －設定変更の否認 －実行状況の否認 －ログの削除・変更	－	－	－

表 6　デバイス層に対する脅威分析結果

Device Layer	S (spoofing)	T (Tampering)	R (Repudiation)	I (Information Disclosure)	D (DoS)	E (Elevation privilege)
Process	正規アプリケーションに成り済ます －不正な情報の配信 －不正なプログラムの実行 －不正な動作 －不正な応答の返却	情報の改竄 －設定ファイルの書き換え －プログラムの改竄(差し替え) －メモリの情報を改竄	操作・情報の否認 －設定変更の否認 －実行状況の否認 －ログの削除・変更	情報の流出 －設定ファイルの流出 －ログ情報の流出 －内外部から取得した情報の不正な配布	負荷の上昇・プログラムの停止、意図的な環境の改変 －処理能力の著しい低下。処理の中断。 －環境を変化させる事による情報収集の妨害 －物理的なネットワークの遮断	プログラムの脆弱性を突き、権限を取得 HWの脆弱性を突き、権限を取得
Data Store	－	情報の改竄 －不揮発性メモリ内の情報を改竄	操作・情報の否認 －設定変更の否認 －実行状況の否認 －ログの削除・変更	情報の流出 －アカウント情報の流出	ストレージコンポーネントの破壊	－
Data Flow	－	通信をフックし、改竄 －入出力/操作/要求・応答など、各種情報の改竄	－	通信をフックし、盗聴 －入出力/操作/要求・応答など、各種情報を不正に取得	ネットワーク負荷の上昇/通信の遮断/改竄 －ネットワーク負荷の上昇による転送遅延の発生 －ネットワーク負荷の上昇に起因した情報の消失 －通信をフックされる事による通信の遮断や改竄	－
External Entity	管理者に成り済ます －管理者に成り済ました操作の実行 －不正デバイスへの差し替え －デバイスに対する直接的な操作	－	操作・情報の否認 －設定変更の否認 －実行状況の否認 －ログの削除・変更	－	－	－