スマートシティIoTに求められるセキュリティ要件と技術

佐々木 貴之　森田 佑亮　小林 俊輝

要 旨

スマートシティは効率的な都市運営を実現する一方で、そのシステムがサイバー攻撃の対象となるリスクが存在します。本稿では、セキュアなスマートシティ実現に必要なセキュリティ要件と、それらを満たすために求められるセキュリティ機能について述べます。具体的には、スマートシティIoTの特徴である多様なデータが扱われている点と、機器が街中にも配置される点から、スマートシティIoTに特有のセキュリティ要件は、柔軟な情報流通制御と、IoT機器の保護であることを明らかにします。更に、各要件を満たすための実現技術（セキュアデータ流通基盤、IoT機器の改ざん検知）について説明します。

KeyWords　スマートシティ／IoT／セキュリティ

1. はじめに

スマートシティは、IoT（Internet of Things）を活用することにより効率的な運営を行うことが可能な都市であり、ユースケースとして、防災、観光、環境保護など、さまざまな適用先が検討されています。一方、IoTの導入により、都市運営のシステムがネットワークにつながるため、サイバー攻撃の対象となるリスクがあり、実際に、ハッキング可能な交通システムがあることが報告されています。このように、スマートシティのシステムが攻撃されると、都市機能が麻痺する可能性があります。また、スマートシティでは、オープンデータに加えて、個人情報などのクローズドデータも扱われるため、そのようなデータは適切に管理される必要があります。

本稿では、スマートシティを支えるIoTシステム（以下、スマートシティIoT）がどのようなセキュリティ要件を満たす必要があるかを、スマートシティIoTに特有の要件に絞って説明します。それ以外のセキュリティ要件は、ITシステムと共通しており、例えば、認証・認可、不要な通信の禁止、セキュリティの運用管理（IoT機器の管理、脆弱性やパッチの管理、インシデント対応など）が求められます。このような一般的なセキュリティ要件は、Cloud Control Matrix[1)]にまとめられています。

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IoT特有のセキュリティに関して、NECは、International Electrotechnical Commission[2)]やEuropean Union Agency for Network and Information Security[3)]が発行している文書に基づいてスマートシティの機能モデルを作成し、STRIDEと呼ばれる脅威分析手法によって脅威の洗い出しを行いました[4)]。その結果を基に、スマートシティIoTに特有のセキュリティ要件を整理したものを後述します。具体的には、スマートシティIoTの特徴である、さまざまなデータが扱われる点と、機器が街中に配置される点を基に、スマートシティIoTに特有のセキュリティ要件を明確化します。

（1）データの漏えい・改ざんの防止

スマートシティIoTの特徴として、オープンデータやクローズドデータが混在して扱われることが挙げられます。例えば、観光の情報は基本的にオープンデータですし、ヘルスケアの個人に関係する情報はクローズドデータです。また、イベント情報システムと交通管

理システムを連携させた精度の高い渋滞予測のように、さまざまなシステム間での情報の共有が予測されます。従って、そのようなさまざまなデータの種類や、多様なサービス間連携が混在する環境でも、情報の漏えいや改ざんが防止される必要があります。

(2)機器の改ざん防止・発見

通常のITシステムやスマートファクトリーのIoTは、敷地内にしか機器は配置されませんが、スマートシティIoTでは機器が街中に配置されるため、攻撃者にアクセスされやすいことが挙げられます。従って、攻撃者が機器に直接アクセスし改ざんしたり、機器を入れ替えたりするリスクあるため、改ざんされた機器や不正な機器の発見が求められます。加えて、IoT機器からクラウドまでの堅牢性が求められます。なぜなら、スマートシティIoTは、IoT機器、ゲートウェイ、サーバやPCなどから構成され、攻撃者はシステムの一番弱い部分を狙うため、システム全体の堅牢性を向上させるには、すべての機器を堅牢にする必要があるためです。

3. スマートシティに求められるセキュリティ機能

本章では、第2章で説明したスマートシティ特有のセキュリティ要件に対応するための機能について述べます。具体的には、データの漏えい・改ざん防止のためのセキュアデータ流通基盤と、改ざんされた機器の発見のための改ざん検知技術について説明します。この2つの技術がそろうことで、信頼できる基盤の上で、情報の流通を確実に制御することができ、安全なスマートシティが実現できます(**図1**)。

3.1 データの漏えい・改ざんの防止を行うセキュアデータ流通基盤

スマートシティの基盤の1つとして、欧州で開発されたFIWARE(ファイウェア)があります。FIWAREは、Generic Enabler(GE)と呼ばれるコンポーネントの集まりであり、情報収集用のGEや解析用のGEなどを組み合わせて、スマートシティの基盤を構築することが可能です。セキュリティのGEも用意されており、アクセスを監視・遮断するWilma、セキュリティポリシーを基にアクセス可否の判定を行うAuthZForce、ユーザー認証を行うKeyRockがGEとして用意されています。しかし、これらのGEを用いたアクセス制御機構のフレームワークが用意されているだけであり、実際に上記GEを用いて情報の流通を制御するには、ユースケースに基づいてアクセス制御のモデルを検討し、XACMLと呼ばれる言語を用いてセキュリティポリシーを記述し、更にアクセス制御に用いるデータを格納するデータベースなどの用意が必要であり、簡単に使用することはできませんでした。

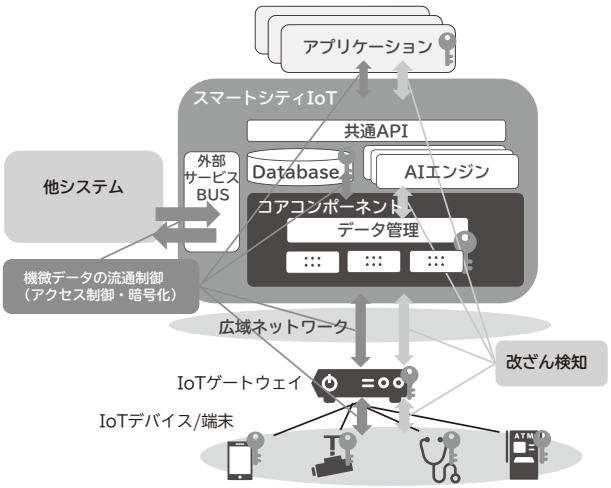


図1　スマートシティに求められるセキュリティ機能

NECは、この課題を解決するために、スマートシティの情報流通のユースケースを網羅し、かつ、簡単に使用できるセキュアデータ流通基盤を開発しました。このセキュアデータ流通基盤は、ユーザーとデータに属性を割り当て、その属性関係に基づいてアクセス制御を行うことで、情報の流通を制御します。具体的には、スマートシティのユースケースを分析し、防災や観光などのドメイン、所属部門、役職(セキュリティレベル)など、スマートシティの情報流通の制御に必要な属性を洗い出しました。これらの属性を、ユーザーやデータに割り当てるだけで、簡単に情報の流通制御を行うことができます。例えば、**図2**のように、機密データを特定の役職の人にしか開示しないようにしたり(セキュリティレベル属性による制御:灰色線)、クローズド情報を市役所内のみで共有したり(所属の属性による制御:破線)、オープン情報を市民の方にも公開したり(黒線)と、情報の種類によって柔軟な流通範囲の制御が可能です。

3.2 通信のセキュリティ:軽量認証暗号

データの改ざん防止のためには、前述した情報の流通

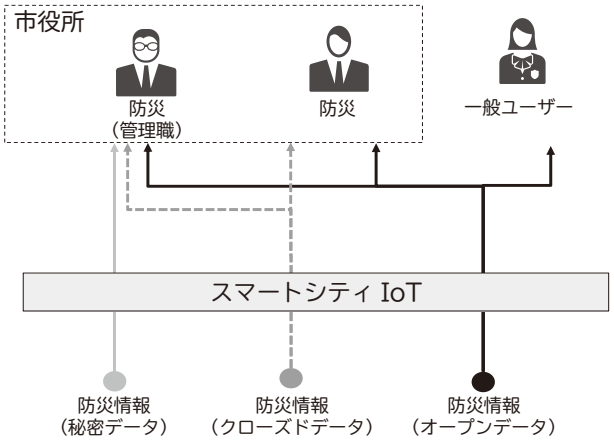


図２　スマートシティにおける情報流通の例

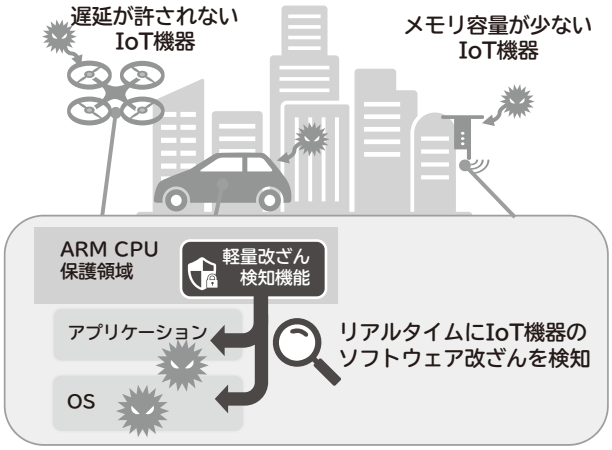


図３　軽量改ざん検知技術

制御に加えて、機器から情報を収集する際にも、データは保護される必要があります。このためには通信の暗号化が有効ですが、IoT機器はパソコンと比較して、CPU速度やメモリ量に制限があるため、IoT機器に暗号化機能を搭載することができない場合があります。NECはこの課題を解決するために、軽量暗号TWINE[5]を開発しています。これにより、メモリ量が小さいIoT機器の通信内容を暗号によって保護することが可能です。加えて、OTR（Offset Two-Round）認証暗号方式を使用することにより、暗号化と改ざん検知を一度に行うことが可能です。

3.3 機器の改ざん防止・発見のための改ざん検知技術

第２章で述べたように、サイバー攻撃からより強固にIoT機器を保護するためには、末端のIoT機器のセキュリティが重要になります。しかし、第３章２節でも説明したように、IoT機器のCPU速度やメモリ量の制約から、セキュリティ対策を導入できない場合がありました。NECは、この課題を解決するために、CPU性能やメモリ容量が十分ではないIoT機器にも適用できる軽量な改ざん検知技術を開発しました[6]（**図３**）。本技術では、ARM Cortex-Mのメモリ保護機能TrustZoneを用いて、実行コードの改ざん検知機能を4kBと軽量に実装しています。機器に送られる制御命令を監視し、その命令に対応した機能の実行コードのみをリアルタイムに検査することで、IoT機器への影響を最小限にしており、遅延が許容されないIoT機器にも適用可能です。本技術は、検知に絞ることで軽量実装を実現しており、改ざんの防止はできませんが、検知後に素早く隔離や復旧などの対処を行うことができます。

4. 都市間連携時のセキュリティ

より良いサービスを提供するために、複数の都市が連携することが考えられます。例えば、災害時には、複数の都市が道路情報を交換することで、救援物資を被災地まで素早く届けることができます。複数の都市のスマートシティIoTが連携し、情報を交換する場合には、第２章で説明した単一の都市のスマートシティIoTのセキュリティ要件に加えて、以下のセキュリティ要件を満たす必要があります。

（1）認証連携

ある都市のユーザーが、他の都市のサービスを受ける場合や、データを参照したい場合には、ユーザー認証の連携が必要になります。

（2）他のシステムから渡された情報の保護

自都市の基盤で生成した情報だけではなく、他の都市の基盤で生成され、連携サービスのために渡された情報も適切に管理される必要があります。

（3）システム横断的なインシデント対応

複数の都市の基盤が連携して動作するときには、インシデント対応も複数の基盤をまたがって行う必要があり、この作業を効率的に行う仕組みが求められます。

これらのうち、（1）認証連携は、SAMLやOpenID Connectなどの標準的なプロトコルがありますが、（2）

他のシステムから渡された情報の保護や、(3) システム横断的なインシデント対応は、標準化された技術や運用方法はありません。今後、スマートシティが発展するにつれ、このような技術が求められると考えており、技術開発を進めていく予定です。

5. むすび

スマートシティによる安定した都市運営を行うためには、サイバー攻撃に対処できなければなりません。本稿では、スマートシティIoTに求められるセキュリティ要件を明確にし、その要件を満たすために求められるセキュリティ技術を紹介しました。今後、スマートシティIoTのセキュリティを担保するための技術開発と社会実装を通じて、安全・安心な社会を実現していきます。

参考文献

1) 日本クラウドセキュリティアライアンス（CSAジャパン）：CCMワーキンググループ
http://www.cloudsecurityalliance.jp/ccm_wg.html
2) International Electrotechnical Commission
http://www.iec.ch/
3) European Union Agency for Network and Information Security
https://www.enisa.europa.eu/
4) 森田 佑亮 、濱本 亮 、佐々木 貴之 、三好 一徳 、小林 俊輝：スマートシティ基盤のセキュリティ脅威分析と対策，コンピュータセキュリティシンポジウム2017論文集，2017.10
5) 岡村 利彦：IoTにおける多様なデバイスに適用可能な軽量暗号，NEC技報，Vol.70 No.1，pp.64-67，2017.9
https://jpn.nec.com/techrep/journal/g17/n01/170114.html
6) NECプレスリリース：NEC、工場における末端のIoT機器にも適用可能な4キロバイトの軽量改ざん検知技術を開発，2018.4
https://jpn.nec.com/press/201804/20180402_01.html

執筆者プロフィール

佐々木 貴之
セキュリティ研究所
主任研究員

森田 佑亮
セキュリティ研究所

小林 俊輝
セキュリティ研究所

関連URL

IoTデバイス向け軽量改ざん検知技術
https://jpn.nec.com/rd/technologies/falsification_find/index.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.71 No.1　データを活用した持続可能な都市経営特集

データを活用した持続可能な都市経営特集によせて
データ利活用型スマートシティの始動

◇ 特集論文

データを活用した都市経営のビジョン
世界のデータ利活用型スマートシティ開発動向
持続可能な社会に向けた都市経営へのパラダイムシフト

データ利活用型スマートシティの実証・実装事例
データを活用した都市経営の海外事例
FIWAREを活用したスマートシティ向け共通プラットフォームの構築（高松市事例）
豊島区における「群衆行動解析技術」を活用した総合防災システム
訪日外国人向けのおもてなしサービスの高度化と地域活性化への取り組み事例
自治体データ活用事例 ～財務・子育て・地域振興などのさまざまなデータ活用～

シティマネジメント技術
データ利活用型都市経営を実現する情報プラットフォーム：FIWARE
FogFlow：クラウドとエッジを通じたIoTサービスのオーケストレーション
スマートシティIoTに求められるセキュリティ要件と技術
欧州におけるスマートシティとSociety 5.0の実現へ向けての標準化の動向
都市評価指標標準とその活用

地域共創
地域共創基盤としての「スマートシティたかまつ推進協議会」
枠を超えた共創活動「せとうちDMO」の立ち上げ
包括連携協定による地域共創
「新たな行政サービス共創研究会」が創るこれからのあたりまえ

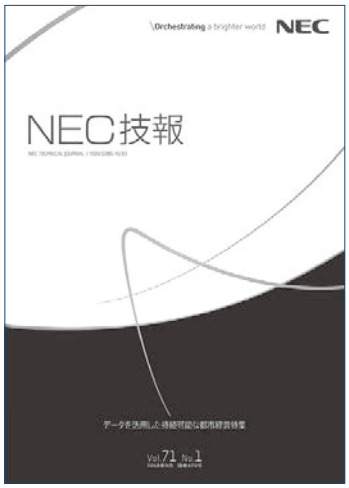
◇普通論文

スピン流熱電変換 ～インフォマティクスを活用した材料開発と適用領域～
NanoBridge-FPGAによるIoTデバイスの低電力・高性能化
IoTデバイス応用に向けたナノカーボンの材料開発
Hyperledger Fabric 1.0を用いた金融領域におけるブロックチェーン技術検証

◇ NEC Information

C&Cユーザーフォーラム＆iEXPO2017　Orchestrating a brighter world
基調講演
展示会報告

NEWS
2017年度C&C賞表彰式開催



Vol.71 No.1
（2018年9月）

特集TOP