2F-03

実機を用いたスマートシティのリスク評価

金尾 幸香†
パーソルプロセス&テクノロジー株式会社 †
満永 拓邦‡ 松田 亘‡ 藤本 万里子‡
東京大学 ‡

概要：近年、あらゆるモノがネットにつながる「IoT」技術の普及が進み、更には、IoT を活用した生活空間である「スマートシティ」の概念も広く知られるようになった。例えば、スマートフォンアプリでの鍵の開錠や電源スイッチの入り切りなど、サイバー空間と我々の生活はより密接に連携していくと考えられる。しかし、IoT 機器の利用用途拡大の一方で、サイバー攻撃のリスクも増大している。本研究は、市販 IoT 機器をスマートシティで利用するシナリオを策定し、IoT 機器のセキュリティテストを実施する。そして、テスト結果が生活にどのような影響をもたらすかリスク評価を行う。

1. はじめに

1.1 IoT とは

IoT（Internet of Things）はネットワークに接続されたモノを表し、IoT 機器は家電量販店等で広く販売されている。OS の多くに Linux が採用され、通信方式は TCP/IP・BLE（Bluetooth Low Energy）[1]・ZigBee[2]等が使われている。IoT のセキュリティについては様々な組織からガイドラインが公開されているが、多くの IoT 機器は可用性重視でセキュリティに関連する機密性は考慮されていないことが多い。一方で IoT 製品は安価で使用用途が特化しており、セキュリティに詳しくない人も使用する可能性が高い。本稿では機器利用における生活への影響を明らかにするため、スマートシティでの IoT 機器の利用を想定したセキュリティテストを実施する。

1.2 スマートシティ

スマートシティは、IoT の活用で生活インフラを効率化して人々がより快適に暮らすことができる都市であり、2018 年の国土交通省のレポート[3]では、スマートシティが実現した社会は、ICT 技術の進展で生活者がリアルタイムに情報の収集と共有が出来るようになるため、物理的・時間的な制約から解放され、個人の生活の質（QOL）を高められると述べられている。

例えば、高松市の「スマートシティたかまつ」プロジェクト[4]では IoT の活用で地域サービスのデータ連携を行う共通プラットフォームを構築している。例として、交通分野では車内に搭載したドライブレコーダの記録をクラウド上の共通基盤にて収集し、分析することでヒヤリハット発生地点の特定を行う。そして、分析したデータを行政や市民が活用することで地域課題の解決を目指している。

2 スマートシティの想定モデル

本稿では、IoT 機器を利用したスマートシティにおける生活を想定する。想定モデルとして、多くの利用者に身近な事例である「通勤」時の IoT 利用を取り上げる。図 1 では、家を出るときにスマートフォンで(1)電球の入り切りと(2)家の鍵の開け閉めを行う。その後、(3)ドローンで空から交通整理された道路を車で走り交通整理（走行速度・交通量計測等）、その様子は(4)ドライブレコーダで撮影され、ドライブレコーダの WEB インタフェースにアクセスして閲覧する。また、スマートフォンにおける(1)～(4)の通信内容は次の通りである。(1)LED 電球と BLE 通信を行う(2)Wi-Fi でホームゲートウェイへ接続し、ホームゲートウェイから ZigBee 通信で鍵と接続する。(3) (4)機器自体がアクセスポイントとなっており、機器との間で Wi-Fi 通信を行う。なお、(3)は WEB インタフェースを持っており、機器接続中はブラウザからのアクセスが可能である。

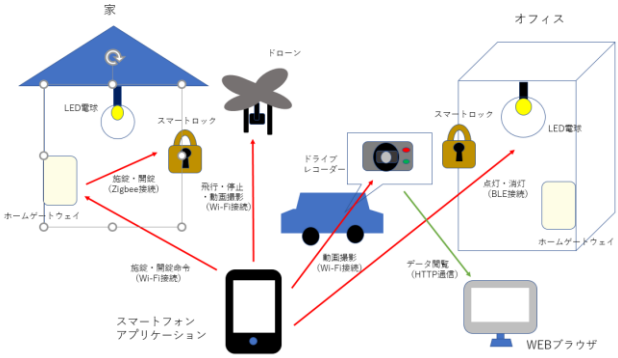

図 1 スマートシティでの IoT 製品利用イメージ

Risk assessment of IoT devices using in smart city
† Sachika Kanao, Persol Process & Technorogy CO. LTD.
‡ Takuho Mitsunaga, The University of Tokyo
‡ Wataru Matsuda, The University of Tokyo
‡ Mariko Fujimoto, The University of Tokyo

	(1)LED 電球	(2)スマートロック	(3)ドローン	(4)ドライブレコーダ
用途	家庭・オフィスの照明	自家用車の運転記録	交通整理（走行速度・交通量計測等）	家庭・オフィスの入退室
通信方式	Bluetooth Low Energy(BLE)	ZigBee	Wi-Fi	Wi-Fi
（1）通信の盗聴	可能	可能	可能	可能
（2）暗号通信の解読	暗号化無	可能 (ZigBee の仕様)	暗号化無	暗号化無
（3）リプレイ攻撃[5]	可能	不可	可能	可能
その他		大量の通信パケットを送ると鍵が操作不能となる		Wi-Fi パスワードが製品 HP 上で公開されている
影響	遠隔の第三者による電球の入り切り	遠隔の第三者による機器操作の把握	任意の操作（墜落）	WEB 上のデータの削除および改ざん

表 1　IoT 機器へのセキュリティテスト内容および結果

3. スマートシティを構成する IoT 機器に対するセキュリティテストおよび結果

2 章で述べたスマートシティ内の各 IoT 機器に対して、以下に記載する攻撃の可否についてセキュリティテストを行った。

（1）通信の盗聴
IoT 機器とコントローラ（スマートフォンアプリなど）間で行われる通信を盗聴する

（2）暗号通信の解読
盗聴した通信が暗号化されていた場合に解読する

（3）リプレイ攻撃[5]
盗聴した通信内容を第三者が対象機器に再送することで不正な操作を引き起こす

セキュリティテストの内容と結果は表 1 の通りである。各機器の製品名は、影響について検証中のため伏せる。テストの内容は各機器に対してそれぞれ、通信の盗聴・暗号通信の解読・リプレイ攻撃[5]の可否を検証した。

結果については、4 製品とも通信の盗聴が可能であり、LED 電球・ドローン・ドライブレコーダの 3 製品でリプレイ攻撃が可能であった。また、スマートロックは通信が暗号化されていたが、ZigBee の仕様上、鍵共有方法に問題があるため暗号通信の解読が可能であった。検証した事項以外にドライブレコーダは製品ホームページにパスワードが公開されており、パスワード認証によるアクセスポイントへの接続が可能であった。スマートロックについては施錠・開錠のリプレイ攻撃を行う事は不可であったが、スマートロックに対して大量の通信パケットを送った際に、ロックがスマートフォンアプリの操作に反応しない状態となった。

4. 考察

3 章の結果より、通信方式にかかわらずテスト内容の各項目について容易に実行できることが分かった。テスト結果から考えられる影響として、リプレイ攻撃が成功した 3 製品は、第三者による操作が可能であるため、利用者の意図しない動作や、物理的な事故を引き起こす可能性がある。加えて、スマートロックについてもスマートフォンアプリの操作に反応しない場合には開錠・施錠のタイミングを第三者に知られるなどの犯罪行為につながる可能性が考えられる。

IoT 製品は利用者の生活に深く密接しており、物理的攻撃も可能であるため、攻撃が実行されたら広範囲かつ大きな影響をもたらすことが予想される。そのため、スマートシティにおいても IoT を用いた利用者の生活の向上を考えるとともに、アクセス制御やパスワード設定などセキュリティ面を意識して信頼できる製品を導入する事が重要であると考える。

参考文献

[1] C. Gomez, J. Oller, J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology", Sensors, vol. 12, no. 9, pp. 11734-11753 (2012)
[2]zigbee alliance
https://www.zigbee.org/(参照 2019-01-09)
[3] 国土交通省　スマートシティの実現に向けて
http://www.mlit.go.jp/common/001249774.pdf(参照 2019-01-08)
[4]総務省　「スマートシティたかまつ」プロジェクトの推進について
http://www.soumu.go.jp/main_content/000563390.pdf（参照 2019-01-09)
[5] IPA RFC の「セキュリティについての考慮事項」についての文章を書くためのガイドライン 3.3.1.リプレイ攻撃
https://www.ipa.go.jp/security/rfc/RFC3552JA.html(参照 2019-01-10)