つながる世界における脅威と脆弱性検討のポイント

IPA 技術本部 セキュリティセンター
情報セキュリティ技術ラボラトリー ラボラトリー長
金野　千里

様々な物がネットにつながることで、利便性の飛躍的な向上やサービス利用形態の質的な変革が期待されるが、そうした世界を実現するには、セキュリティ上の課題を解決していかなければならない。本稿では脅威とセキュリティ対策の概要と、基本的な課題である脆弱性への対応について解説する。

1 はじめに

様々な物がネットにつながることで、利便性の向上やサービスの質の変化を生む、IoT と呼ばれている世界が開けていくが、その反面、セキュリティ上の課題が大きくクローズアップされてくる。図 1 に IoT の世界の全体イメージを示す。

IPA では、組込みシステム [1]、情報家電 [2]、制御システム [3]、自動車 [4]、医療機器 [5] などの個々の分野において、システムやサービスの形態の急速な変化を考慮し、セキュリティ上の脅威の調査と対策のガイドの策定を行ってきている。それぞれの分野における各論については、公開物を参照いただきたい。

本稿では、つながる世界 IoT 全般に対して、脅威と対応の全体概要と脆弱性の対応について解説する。

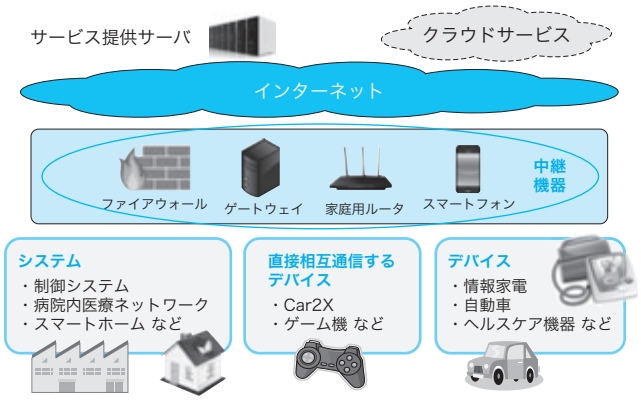

図 1　IoT の全体像

2 課題

IoT を情報の流れと構成からみると、Things（「物」：デバイスや機器やシステムなど）が、ネットワークと接続し、それを介して情報のやり取りをし、「物」に対しては情報やサービスが提供されるが、やり取りする相手は「物」同士であったり、他のシステムであったりする。また、「物」が所有している情報がネットワークを介してバックにあるシステムやクラウドサービスに収集され、様々な利用がなされ、それにより新たに生成された情報が再び「物」にフィードバックされたりする。

これは、例えば「物」をパソコンに置き換えてみれば、一般的なインターネットシステムと構造的には何ら変わることがあるわけではない。従って、脅威としては、パソコンと同様のことを想定することになり、対策はこれまで情報セキュリティで培われてきた技術を活用することになる。ただ、IoT の描く世界では、以下のような固有の様々な課題が存在しており、それらが対応を困難にしている。

(1) ネットにつながる脅威をこれまで考慮していなかった分野の機器の接続が想定される
(2) 生命にかかわる機器やシステムがつながることが想定される
(3) 「物」同士が、無線などで自律的につながることが想定される
(4) 「物」のコストの観点から、セキュリティ対策が省かれることが想定される
(5) ネットを介して収集される情報の用途は、「物」側では制御が困難であり、バックにあるシステムやクラウドサービス側での管理範囲となる
(6) つながる世界を広げていくためには、「物」同士の技術的（通信プロトコル、暗号、認証など）、

及びビジネス的な約束事が不可欠となってくる

この内、(1) ～ (4) は、「物」におけるセキュリティ対策を「物」を開発する側が考えることになるが、(5)(6) は様々な分野の事業者の連携や業界基準、あるいは個人情報やプライバシー情報の取り扱いなどにおいては制度や規制が必要になってくるものと考えられる。IoT の世界におけるセキュリティは、「物」単体やその製造者による管理にとどまらず、「物」と接続して情報をやり取りするサービス側のセキュリティ（とくに収集情報の取り扱い範囲と管理など）も絡んでくるため、問題を難しくしている。

以下では、この「物」におけるセキュリティ対策について述べる。

3 脅威とセキュリティ対策の概要

ネットにつながる「物」としては、主な脅威と攻撃は以下となる：

(a) 不正アクセス
(b) つながる「物」やサービスシステムの成りすまし
(c) ウイルス感染
(d) 通信情報の盗聴、改ざん

これらに引き続いて、情報の改ざんや漏えい、誤動作などが発生しうるが、攻撃の上流にあるこれらをいかに抑止するのかが対策の基本となる。

その対策としては、技術的には一般のパソコンと変わることなく、

① 脆弱性対策 〈(a) (c) (d)〉
② ウイルス対策 〈(c)〉
③ 認証（つながる相手の特定）〈(a) (b)〉
④ 使うサービスの特定 〈(a) (c)〉
⑤ 通信路暗号（盗聴の防止）〈(d)〉
⑥ 情報の完全性の保証（やり取りされる情報の改ざんの防止）〈(d)〉

などが挙げられる。

これらを具体的に決めるためには、「物」に実装されるコンピュータリソースやかけられるコストの問題、要求されるセキュリティレベルなどを勘案して定めていくことになる。更に、「物」のつながる世界の範囲やその世界のビジネスの管理主体（サービスやシステムの運営管理元）にも依存してくる。これらが、IoT の世界のセキュリティの検討を進める上での大きな隘路であり、個々のつながる世界ごとに議論が必要となってくるところである。

次節では、この中で、「物」を作る側にとって、とくに重要となり、共通で基本的なセキュリティ上の課題である脆弱性への対応について、説明する。

4 脆弱性への対応

情報システムにおける脆弱性への対応は、以下の２ステップから成る：

【開発時】：開発段階で脆弱性を極力埋め込まない、残留させないようにする。これには、上流から、以下の対応を実施することになる：

① 脆弱性を作り込まない
　セキュアプログラミング技術の適用やコーディング規約（例えば ESCR[6] など）の利用
② 既知の脆弱性を解消する
　用いるソフトウェア部品（フリーウェアを含む）に、既知の脆弱性がないか脆弱性対策情報データベース JVN-iPedia の活用（下記 (1) で紹介）
③ 残留している脆弱性を検出し解消する
　出荷前の脆弱性検査として、各種のテスト（既知の脆弱性検査、ソースコード検査、ファジング [7] による未知の脆弱性検出）ツールの活用

【運用時】：利用開始後に、新たに報告される脆弱性に対して、「物」の開発者（提供者）は脆弱性対策情報（パッチなど）の作成と、「物」の利用者への通知、更にその対策情報を「物」に適用する手段が必要となる。そのためには、「物」の開発者側には、これらを実施できる仕組みと組織体制の整備が期待されることになる。

この脆弱性への対応を支援するため、IPA では脆弱性対策情報を提供するデータベースと、脆弱性の早期解消を促進する制度を運用している。

(1) 脆弱性対策情報データベース：JVN iPedia（http://jvndb.jvn.jp/）

これまで報告された脆弱性対策情報のデータベースとその利用機能（例えば製品名やバージョンで該当する脆弱性をすべて検索する機能など）を合わせて広く一般に公開しているのが、図２に示す JVN iPedia である。現

2015 年第 3 四半期の登録件数

	情報の収集元	登録件数	累計件数
日本語版	国内製品開発者	0 件	168 件
	JVN	326 件	5,722 件
	NVD	1,435 件	50,585 件
	計	1,761 件	56,475 件
英語版	国内製品開発者	0 件	168 件
	JVN	53 件	1,113 件
	計	53 件	1,281 件

図２　脆弱性対策情報データベース

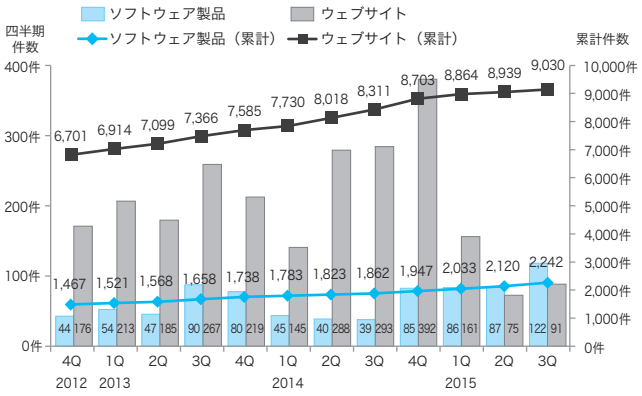

図３　脆弱性の届出状況

在、56,000 件以上の国内外のソフトウェアの脆弱性対策情報が蓄積されている。従って本データベースを、「物」の【開発時】の②における業務に活用することや、【運用時】においては、新たに登録された脆弱性の有無や対策情報の収集に活用することが可能である。

(2)　脆弱性届出制度（https://www.ipa.go.jp/security/vuln/report/index.html）

ソフトウェア製品やウェブサイトに脆弱性を発見した場合、それを IPA に届け出て、当該ソフトウェアの開発者（提供者）やウェブサイト運営事業者に、脆弱性対策対応を促し、ソフトウェア製品に対しては対策情報が用意されたら、その情報を広く周知する役割を果たしているのが、「情報セキュリティ早期警戒パートナーシップ」制度である。対策情報の用意された脆弱性は、(1) のデータベースにも登録される。この制度における脆弱性の届出状況を図３に示すが、年々、新たに発見された多数の脆弱性が届け出られており、対象製品には家電やホームルータなども含まれている。今後これまで以上に、IoT にかかわる製品の届け出が増えてくるものと推測される。

■ IoT における課題

上記ではこれまでの情報システムに対する脆弱性への対応手順にそって説明したが、パソコンのように新たに発見された脆弱性を解消する手順や利用者のリテラシーが確立していない IoT という新しい分野で、これらに対応していくには開発者側の脆弱性に対する対応体制の整備、脆弱性対策を「物」に適用する手段と利用者の対応など、２節で述べた様々な課題を背景に、解決していく必要がある。

例えばその典型的な例として、今年は、自動車のインターネット接続サービスの口から脆弱性を突いて侵入され自動車が遠隔操作できてしまうという問題が表面化し、大きなニュースとなった。その対応に USB で修正プログラムを対象車種のオーナーに送付して実施してもらうことから、リコールでの対応にまで発展した。これは、２節 (2) で述べた課題が背景にあるからである。また、利用者が特定される「物」であればこうした対応も考えられるが、民生品として広く販売されたものとなると、その脆弱性対応は、ネット経由で自動的にできることなどが、市場の要請としては求められることが想定される。

5　おわりに

技術的につながる世界が広がっていくことで、様々な利便性の向上とサービスや利用形態の質の変革が期待されているが、真にその発展を実現していくためには、セキュリティの保証が不可欠となってくる。そのためには、個々の「物」へのセキュリティの実装と運用はもとより、業界横断や異業種との連携の下で共にセキュリティや情報を運用管理する規約や基準などの約束事が重要となってくるものと考えられる。

【参考文献】

[1] 組込みシステムのセキュリティへの取組みガイド , http://www.ipa.go.jp/security/fy20/reports/emb_app/index.html
[2] 情報家電におけるセキュリティ対策　検討報告書 , http://www.ipa.go.jp/security/fy22/reports/electronic/index.html
[3] 制御システムの情報セキュリティ動向に関する調査 , http://www.ipa.go.jp/security/fy22/reports/ics_sec/index.html
[4] 自動車の情報セキュリティ動向に関する調査 , http://www.ipa.go.jp/security/fy22/reports/emb_car/index.html
[5] 医療機器における情報セキュリティに関する調査 , https://www.ipa.go.jp/security/fy25/reports/medi_sec/index.html
[6] 組込みソフトウェア開発向け コーディング作法ガイド , https://www.ipa.go.jp/sec/publish/tn13-001.html
[7] 脆弱性対策：ファジング活用の手引き , http://www.ipa.go.jp/security/vuln/fuzzing.html