トピックス

IoTの普及に伴うPSIRTの必要性
―飛躍的に重要性を増すサイバー脅威への対応―

IoTの普及により、インターネットに常時接続される機器が加速度的に増えている。このいわゆるコネクティッド化に伴い、従来型のITシステムと同様にサイバー攻撃を受けるリスクが増大することから、製品の情報セキュリティインシデント対応を主体となって行うPSIRTが必要である。その活動内容や態勢整備時の留意点を紹介する。

NRIセキュアテクノロジーズ
マネジメントコンサルティング部
副主任セキュリティコンサルタント
西　俊祐（にし　しゅんすけ）
専門は情報セキュリティ全般に関するコンサルティング

NRIセキュアテクノロジーズ
マネジメントコンサルティング部
上級セキュリティコンサルタント
熊白　浩丈（くましろ　ひろたけ）
専門は情報セキュリティ全般に関するコンサルティング

問題化するIoTの脆弱（ぜいじゃく）性

“IoT”、もはやこの言葉を説明する必要はないだろう。家電、自動車、スマートメーター、スマートフォンを媒体とした各種アプリ、決済用端末などがネットワークにつながることで、飛躍的に社会の在り方を変えつつあるのはご承知の通りである。そしてIoTの普及とともに、「自動車がリモートから不正に操作された」「家庭用のWebカメラから室内の画像が流出した」など、それらに組み込まれているソフトウェアの脆弱性を突くセキュリティ事故の発生や研究機関からの発表が、毎日のようにニュースをにぎわせている（表1参照）。

表1　セキュリティ事故または脆弱性の事例

発生年月	概要
2013年8月	米国において、Webカメラの脆弱性を利用した著名人の盗撮被害が発生した。
2015年7月	米国大手自動車メーカーの車両において、ブレーキやエンジンなどの遠隔操作が可能となる脆弱性が公表された。
2016年1月	ロシアのWebサイトで、初期パスワードを変更していない、またパスワードの設定されていない監視カメラの映像が公開された。
2016年9月	米国大手自動車メーカーの車両において、ブレーキやドアの施解錠などの遠隔操作が可能となる脆弱性が公表された。

出所）各種報道および各社発表資料より作成

コネクティッド化された各種機器の安全性を脅かすサイバー攻撃に対して、今、企業としての防衛が求められているが、どのように対策を進めるべきだろうか。

日進月歩で変わり続けるIoTの世界では、開発着手からマーケットインまでのサイクルが短い。また、既製のソフトウェアやOSS（Open Source Software）を活用して、コストを抑制するとともに、開発期間を短縮しているものもある。そのため、利用状況やユーザーの行動に対して、十二分に想定したテストが行えない場合もある。

IoTにおいても、通常のIT製品と同様に、不具合（脆弱性）の多くは初期に発生し、次第に収束していくが、製品の成熟期にハッカーや研究者がセキュリティ上の脆弱性を見いだすことがある。またマーケットインから時間がたつと、新たな攻撃手法の出現や、実装している既製のソフトウェアのサポートアウトなどにより、十分な対策をとることが難しくなることも考慮しておかなければなら

ない。

設計・製造時に意図していない動きや結果をもたらすセキュリティの脆弱性は、製品の欠陥である。しかしながら、設計・開発当時の状況から、製品の専門家として必要十分な注意を払っていたとしても、見つけきれない・防ぎきれないセキュリティの脆弱性が発生してしまうのは、IoT製品としては逃れようがない。OSSや既製のソフトウェアを搭載している場合はなおさらである。

そのため、自動車業界で定められている「リコール」「改善対策」や「サービスキャンペーン」（保安基準に該当しない不具合対策の一種）のように、セキュリティの脆弱性が引き起こす影響によって、どのように対処するべきか、結果の重大性に応じた対応の方向性を取り決めておき、態勢を整えておくことが重要である。

PSIRTの必要性

CSIRT（Computer Security Incident Response Team）は、この5年間で、国をはじめ、多くの企業・団体などで整備が進み、すでに一般的な用語として定着している。組織によって定義や守備範囲は異なるが、主に自社や自グループのPCやサーバーなどのIT機器や自社ホームページなどに対するサイバー攻撃への対応、リスクマネジメント（リスクの特定・評価・対処）に主眼を置いたレスポンス・エンティティ（態勢）である。

一方、PSIRT（Product Security Incident Response Team）とは、自社が製造または販売した製品、構成部品、成果物、サービス、ソリューションに存在する「セキュリティの脆弱性」に関わるリスクマネジメントに主眼を置いたレスポンス・エンティティのことをいう。

PSIRTは、ソフトウェアプロダクトメーカーを中心に整備が進められてきており、決して新しい概念ではない。しかし、これまで情報セキュリティ事故やセキュリティの脆弱性と関わりが薄かった製品メーカーも、ソフトウェアやインターネットとのインターフェース、それらを実装した製品すなわちIoTを市場投入するようになり、差し迫った情報セキュリティの脅威に直面する機会が出てきている。そのため、PSIRTの整備を急ぐ必要性が高まっている。

またPSIRTの管理領域となり得る製品は、その特性が多様であることから、ITにおけるシステムとは異なり、共通のベストプラクティスの定義が難しいという特徴がある。そのためいろいろなガイドラインについては、産業別に策定される方向性が予想される。よって、産業ごとに、関連する省庁や団体の動向を注視する必要がある。しかし、産業によらずPSIRTで行う製品の脆弱性管理の仕組みそのものは、共通かつ、不可欠なものである。

PSIRTの活動内容

では、PSIRTの活動とは具体的にどういうものであろうか。いろいろな活動があるが、以下の3点が重要ではないかと考える。

1点目は、自社製品に重大な脆弱性を有するものがあるかを、早期に検知する役割であ

る。これについては、脆弱性の情報を集約した「脆弱性情報データベース」の活用がある。例えば、アメリカ国立標準技術研修所（National Institute of Standards and Technology）が管理をしているNVD（National Vulnerability Database）や、日本ではJVN（Japan Vulnerability Notes）があり、他にもOSSに特化した商用の脆弱性情報データベースがある。こうしたデータベースと、自社の製品の構成情報をマッチングし、該当するものがあるかを確認する。すでにこうした取り組みを進めている企業では、インテリジェンス情報（アンダーグラウンドでの交換情報や海外のコミュニティ、学会における発表など）まで収集対象を広げているところもある。

2点目は、自社の製品に該当する脆弱性があった場合の対応である。影響の大きさを評価・分析し、影響が大きいものから優先順位をつけ（トリアージ）、製造部門や品質管理部門（脆弱性の修復策または回避方法の策定）、広報部門（脆弱性情報の公開）と密に連携して対応を進めることである。

3点目はステークホルダーとのつながりを管理することである。コミュニケーションチャネル（社内製造系部門の窓口、広報・法務・人事などコーポレート部門の窓口、脆弱性の発見者、サプライチェーン上の関係者、外部セキュリティベンダー、所轄省庁）を事前にまとめておき、有事の際にはPSIRTの主導で、各コミュニケーションチャネルと機動的な対応を行えるようにしておくことが重要である。そのためにも可能な限り手順を定め、日頃から訓練や連携を欠かさないことである。

PSIRT態勢整備の留意点

次にPSIRT態勢の整備において、留意すべき点を3つ紹介する。

①製品仕様に応じた情報収集態勢の整備

PSIRTが管理対象とするIoT機器の特性として、PCやサーバーなどのIT機器と異なるのは、製品はOSSや独自開発したソフトウェアなど、製品仕様に応じた柔軟性の高いソフトウェアを利用していることが多いということである。特にOSSについては、製品のリリースサイクルの高速化および価格競争力の確保のために利活用が進んでおり、今後もその傾向は継続することが予測されている。そのため、製品仕様に応じた情報収集態勢の整備がポイントとなる。

②DevSecOpsの考慮

「DevSecOps」とは、「DevOps」に「セキュリティ」を加えた考え方である。元になっている「DevOps」は開発者と運用者が密に連携して、品質を確保しつつ、システム開発のスピードを速めることを目的とした開発スタイルである。

具体的には要件定義、設計、実装、テスト、リリース、運用の各工程においてセキュリティ上の脆弱性を組み込んでしまうリスクを低減するため、各工程に応じたセキュリティ対策をプロセスに組み込むことを指す。例えば、設計段階で国際規格ISO/IEC15408、2016年に策定された「IoTセキュリティガイドライン ver1.0」（経済産業省）などのセキュリティ関連のガイドラインを用いてのアセスメントや、実証・テスト段階で静的・動的なセキュリティ診断を行うな

どの対策が挙げられる。

なお、ITシステム開発においての運用者とは主にシステム運用者を想定しているが、製品の場合は、製品供給元の企業の運用者の場合もあれば、消費者または研究者、製品供給先の企業が運用者となる場合もある。ただ、共通して重要なことは、運用者が発見した問題が開発者にフィードバックされることであり、その仕組みを整備することである。仕組みの構築には国際規格ISO/IEC29147、ISO/IEC30111などのガイドラインが参考となる。

製品のセキュリティ水準を底上げし、インシデント発生の可能性そのものを低減する仕組み作りについても、「DevSecOps」の考え方を開発時の標準プロセスに組み込み、製造部門に啓発するといったことは、態勢整備における欠かせない検討事項である。

③マーケットイン後のサポート

IT機器の場合、社内やデータセンターなどで対象の集中管理が可能である。一方で製品については、マーケットイン後、管理対象が消費者のもとに分散的に存在することから、セキュリティパッチの適用や、脆弱性の影響を回避、低減する設定の変更をどのように行うのかといった方針や手段について、製品特性を十分に考慮し、製品個別に定める必要がある。またIT機器においてはソフトウェアがサポートアウトした際に、リプレースなどで対応が可能であるが、製品については同様の手段がとれない。そのため、人命などの安全性に関連する製品は最重要として、自社の業績に多大な影響を及ぼす主力製品はより上位になど、自社の製品ポートフォリオにおける位置付けや製品特性を踏まえて、製品個別の対応フローを定めることが重要となる。

PSIRTに求められる人員

PSIRTとして製品セキュリティを確保するためには、セキュリティ全般の知識および製品知識の両方を備えた人員がその活動をハンドリングすることが理想である。しかしながら現実論として、その両方を備えた人員は極めて少なく、確保は困難である。製品部門におけるエース級の担当者をPSIRT担当者とするという選択肢も考えられるが、製造現場への影響が大きく、事業力の低下につながる可能性があって得策ではない。

現実的な選択肢として、セキュリティ全般知識を有したPSIRT担当者と製品知識を有した製造担当者が相互に補完しながら、製品セキュリティを管理することが考えられる。しかしながら価値観・文化の相違から、セキュリティ知識を有するPSIRT担当者がセキュリティの原理原則にのっとった要求や判断をする一方、製品担当者は安全性や可用性を重視する傾向があるケースも多く見受けられる。密なコミュニケーションを通じて相互理解を深め、共に脅威に向き合うことが重要だと考える。

セキュリティ人材の不足が叫ばれるなか、中長期的な要員育成は不可欠であるが、短期的にはセキュリティの専門能力を有する外部パートナーの活用が有効となる場合もある。ただし、この場合も、専門性に加えてコミュニケーション能力を重視すべきであることは上述のとおりである。■