製品分野別セキュリティガイドライン

IoT - GW 編

Ver. 2.0

CCDS セキュリティガイドライン WG

ホーム GW SWG

改訂履歴

版数	改訂日	改訂内容
Ver.1.0	2016/06/08	新規発行
Ver.1.01	2016/06/13	リンクエラー箇所の修正対応
Ver.2.0	2017/05/29	・設計・製造、運用保守、廃棄フェーズに項目追加 ・その他軽微な修正

目次

1 はじめに

これまで製品業界ごとにセーフティ標準は策定されてきた。一方セキュリティ標準をみると、組織運営に関する標準（ISO27001）と製品設計のセキュリティ評価・認証に関する標準（ISO15408）が策定されており、近年では、重要インフラストラクチャー（社会インフラに欠かせないプラントや施設）の制御システムを対象とした標準（IEC62443）も策定されている状況である。

IoT の普及に伴い、身の回りにある生活機器が様々なネットワーク接続機能を持つことで、製品のセキュリティ懸念は増しているが、IoT 製品やサービスには欠かせないセキュリティ標準がいまだ生活機器に対しては整備されていない状況である。

欧米の動きをみると、各業界のセーフティ標準からセキュリティ標準を検討する動きが各所にみられる。一方、日本においてもセキュリティに関する懸念は顕在化しており、検討すべき、という声は多いが、具体的検討に入っている分野はまだ少ない状況となっている。

このような状況の中で、一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）は設立された。本協議会では、生活機器セキュリティ標準の策定と、その標準に沿っていることを確認・検証した認証プログラムをセットにすることで、ユーザに安心して IoT 製品を使ってもらえる環境を整えることを目標に活動を行っている。

平成 27 年 8 月 5 日には独立行政法人 情報処理推進機構（IPA）が「つながる世界の開発指針検討 WG」を発足させ、国レベルでのセキュリティ検討がスタートした。CCDS も IPA-WG に参画し、CCDS 内でのガイドライン検討結果について提案を重ねてきた。

IPA-WG での検討結果は「つながる世界の開発指針～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント」[1]としてまとめられ平成 28 年 3 月 24 日に公表された。IPA の開発指針は分野全体をカバーする共通事項を中心にまとめられた基本的な指針となっているが、CCDS では個々の製品分野において、具体的にセキュリティをカバーした設計・開発を進めるために、本分野別ガイドラインを策定した。

IPA 発行「つながる世界の開発指針」については、下記 URL のリンク先を参照。

http://www.ipa.go.jp/sec/reports/20160324.html

1.1　IoT-GWのセキュリティの現状と課題

IoT（モノとインターネット）機器は、私達により身近なものになり、多種多様な方面で広がりを見せている。ヘルスケアおよびフィットネス分野では、ウエアラブルデバイスが取り入れられ、食生活の改善やランニングフォームのアドバイスを得ることが可能になっている。家庭内に設置したセンサをスマートフォンと連動させ、例えば遠隔で操作することを可能にすれば、家の施錠や照明、電源をコントロールすることができる。IoT 機器は個人や家庭に限ったことではなく、オフィスや市街地での普及も著しく、今後はさらに増加すると想定されている。調査会社ガートナーによると、2016 年の 64 億台から、2020 年に 208 億台に達する[2]と試算されている。

これらの IoT 機器は、インターネットに接続されていることで、様々なサービスを提供することが可能であるが、同時に、情報セキュリティの脅威にさらされている。その脅威は時に、人命をも脅かすものとなる可能性があり危惧されている。

IoT 機器が攻撃を受ける要因は利用者と提供者の二つの側面からみることができる。利用者に起因するものとしては、IoT 機器の初期設定での使用や、推測されやすいパスワードの設定、セキュリティへの知識不足などが挙げられる。提供者に起因するものとしては、初期設定で誰でもアクセスできてしまう設計や利用者のセキュリティへの知識不足の想定が不十分などである。

その背景には、セキュリティのリスクを評価する基準や規格がないことが挙げられ、これから IoT 業界が発展する上で、大きな問題となると考えられる。要因の改善を、全ての利用者に要求することは難しく、対応できることも少ない。そのため提供者は、製品提供後、機器のアップデート方法を考えるなど、開発・設計時に利用シーンへの留意も必要である
本書では IoT-GW の開発プロセスにおいて考慮する点などをガイドラインとしてまとめた。想定されるセキュリティ脅威について詳細に分析し、その脅威をどのように取り除くかを記載する。

1.2　ガイドラインの対象範囲

本書は、宅内に限らずオフィスや工場の Thing(モノ)からのデータを集約しネットワークとデータを送受信する IoT-GW を対象とし、GW 開発に際して考慮すべきセキュリティの重要ポイントについて記載する。

1.3　本書の対象者

本書は、前節で述べたようなセキュリティに対するリスクを軽減させるためのものである。IoT 機器において適切なセキュリティ対策を実施するために設計から製品リリース後までに考慮すべき設計・開発プロセスをまとめたものである。

以上のことから本書は次のような方を対象としている。

1）機器の設計を行う設計者および開発者
2）機器の設計プロジェクトの開発責任者
3）機器の設計プロジェクトの予算や人員を決定する意思決定者

1.4　略称

本書で使用されている略称について説明する。

表 1-1 略称一覧

略称	名称
API	Application Program Interface
BGA	Ball Grid Array
CCDS	Connected Consumer Device Security council
CPU	Central Processing Unit
CRYPTREC	Cryptography Research and Evaluation Committees
CVSS	Common Vulnerability Scoring System
DNS	Domain Name System
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
FBGA	Fine pitch Ball Grid Array
FIRST	Forum of Incident Response and Security Teams
GMITS	Guidelines for the Management for IT Security
ID	Identification
IoT-GW	Internet of Things-GateWay
IP	Internet Protocol
IPA	Information-technology Promotion Agency
IT	Information Technology

JTAG	Joint Test Action Group
LAN	Local Area Network
LGA	Land Grid Array
OS	Operation System
OSS	Open Source Software
OWASP	The Open Web Application Security Project
PC	Personal Computer
PPPoE	Point-to-Point Protocol over Ethernet
ROM	Read Only Memory
SNS	Social Networking Service
SQL	Structured Query Language
WAN	Wide Area Network
XSS	Cross Site Scripting

2 IoT-GW のシステム構成

2.1 IoT-GWを適用するシステムモデル

IoT-GW を適用するシステムの汎用的なモデルを図 2-1 に示す。また、各構成要素の説明を

表 2-1 に示す。本モデルでは、IoT-GW は、フィールド側に設置されたセンサやアクチュエータから物理空間上の観測データを収集し、ヘッドエンドシステムに転送する。ヘッドエンドシステムは、そのデータを蓄積し、API を介して多種のアプリケーションやサービスへのデータ配信を行う。ユースケースによっては、アプリケーションやサービスがデータ解析をした結果のフィードバックとして、アクチュエータ類の制御を行う場合もある。ヘッドエンドシステムや IoT-GW 管理は、クラウドなどのセンタ側にサーバ群として設置される。また、IoT-GW 以下の構成要素は、宅内や製造現場などのフィールド側に設置される。設置場所はユースケースによって異なる。

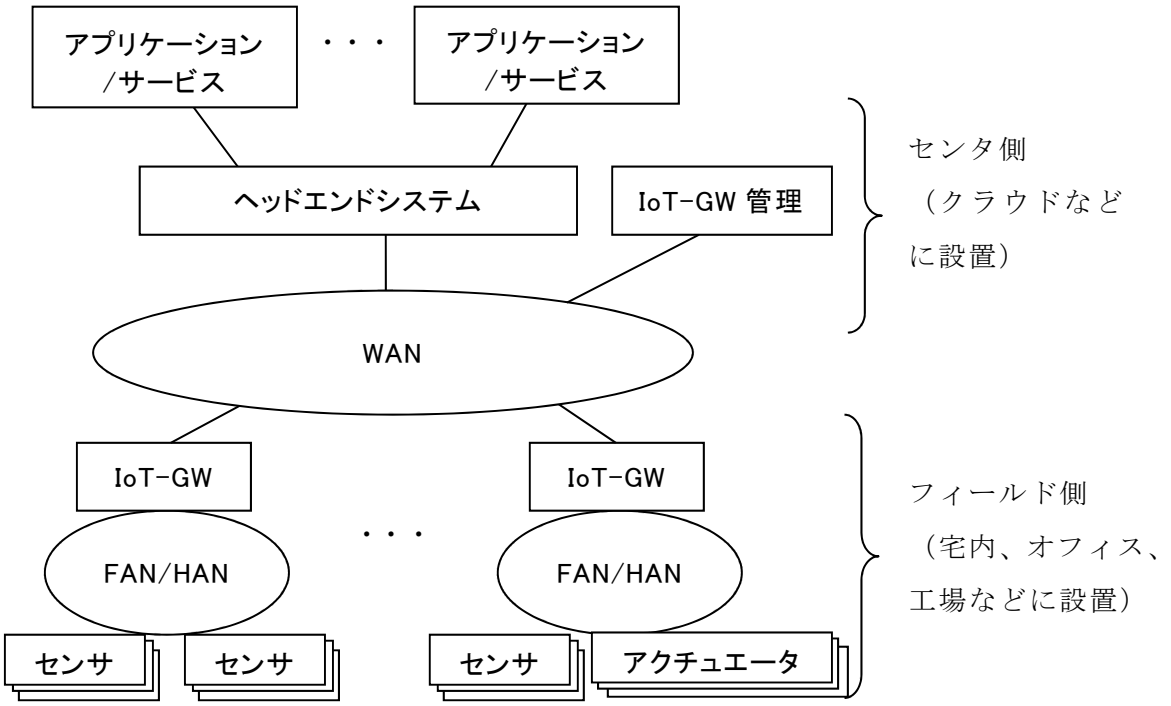

図 2-1 IoT-GW を適用するシステムモデル

表 2-1 システムモデル中の構成要素

名称	説明
センサ	人間が肉眼で識別できないものを数値化し、データ収集を行う。このデータはアプリケーション/サービスなどで使われる。
アクチュエータ	電気などのエネルギーを動力源として機械的な仕事を行う機器の総称である。
FAN/HAN	FAN：Field Area Network/HAN：Home Area Network。一般家庭、企業のオフィスや研究所、工場等のネットワークのことである。有線/無線、IP/非 IP など様々なアクセス形態が存在する。
IoT-GW	規制などの要因でインターネットに接続できない IoT 機器とインターネットを中継する機器である。
WAN	WAN：Wide Area Network。インターネット（公衆網）、広域閉域網、移動体通信網などのネットワークのことである。
ヘッドエンドシステム	データ収集および通信制御を行うサーバ機器群である。
IoT-GW 管理	IoT-GW の機器認証や運用管理を行うサーバ機器である。
アプリケーション/サービス	集計・分析した結果を他のデータベースへ蓄積し、リアルタイム通知やビジュアライゼーションなどを行う。

2.2 IoT-GWで実現されるサービス・ユースケース

IoT-GW を適用するシステムによって実現されるサービス・ユースケースは多岐にわたる。本項では、IoT-GW を適用するシステムのリスクを分析する上で、主要なユースケースとして以下の 4 つを説明する。

2.2.1 ユースケース１：ホームゲートウェイ

本ユースケースにおいて、ホームゲートウェイは、屋内や宅内の状態を見える化し、また屋内や宅内に設置された家電等の機器を制御する機能を具備した機器である。ホームゲートウェイを使用したシステム構成の一例を図 2-2 に示す。屋内や宅内に配備されたセンサ類から、温度、湿度、照度、消費電力などのデータを収集し、統計処理を施してユーザに対して見える化を行う。将来的なサービスとしては、収集したデータを用いて、センタ側から空調や照明設備の最適制御を行うことも考えられる。

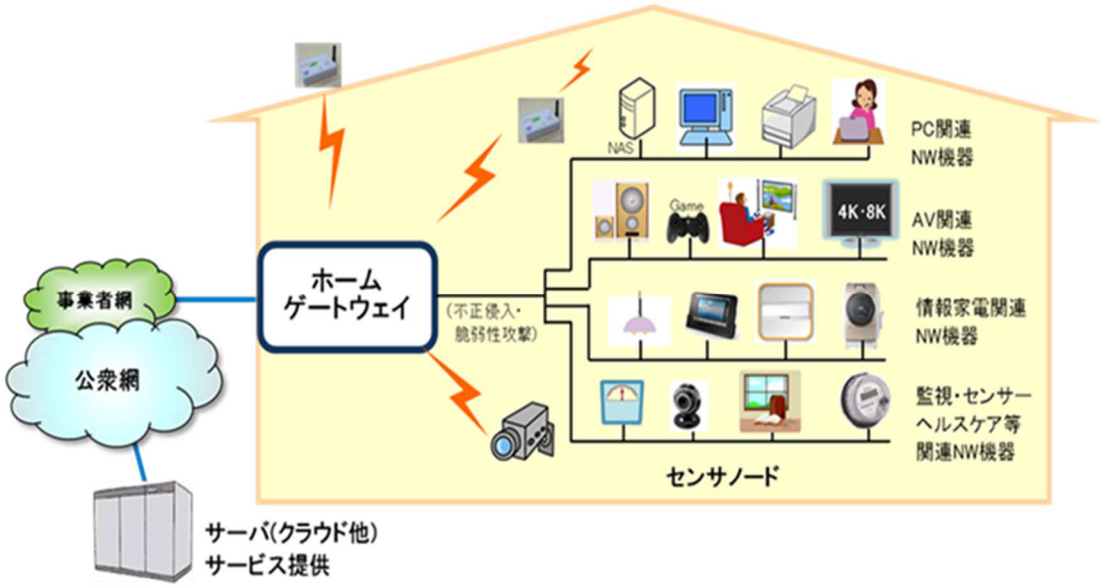

図 2-2 ホームゲートウェイ

2.2.2 ユースケース 2：スマートメンテナンス

スマートメンテナンスは、公共設備･インフラ等の劣化度合いを見える化し、最適なメンテナンス時期を評価し、メンテナンスコストを削減することを目的としたユースケースである。スマートメンテナンスのシステム構成の一例を図 2-3 に示す。例えばガスタービン発電設備の場合には、タービン、圧縮機、ボイラ、ポンプなどの設備をセンサやマシンデータ（信号）から観測し、設備劣化度合いを推定可能なデータを収集する。収集したデータから、設備劣化度合いを評価し、保守・点検の目安値に到達しているかどうか（あるいは、いつ到達するか）を判定する。この他にも、鉄道設備の保守などを取り扱うユースケースもある。

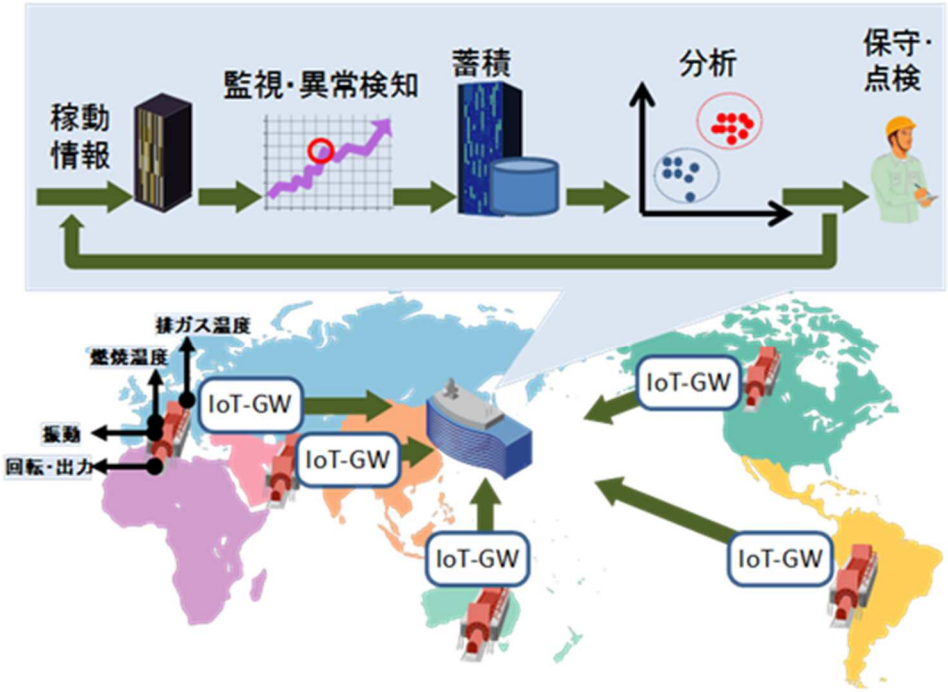

図 2-3 スマートメンテナンス

2.2.3 ユースケース 3：サプライチェーン管理および生産ライン最適化

サプライチェーン管理および生産ライン最適化は、需要に応じた最適部品発注、生産ライン組替、部品中間材の工場内配送、物流状況のモニタリングなどを目的としたユースケースである。サプライチェーン管理および生産ライン最適化のシステム構成の一例を図 2-4 に示す。各サプライヤにおける部品・中間財在庫情報、顧客・市場需要情報、サプライヤ供給能力情報、現状の生産状況をデータとして収集する。収集したデータを解析して、少し先の将来にわたってサプライチェーン全体が最適化されるように、発注部材・発注先・発注量、需要に応じた生産ライン切り替え計画、工場内在庫・輸送計画などを行う。将来的には、工場内配送（ベルトコンベアやフォークリフトなど)、生産ラインへのプログラム配信などの遠隔制御も考えられる。

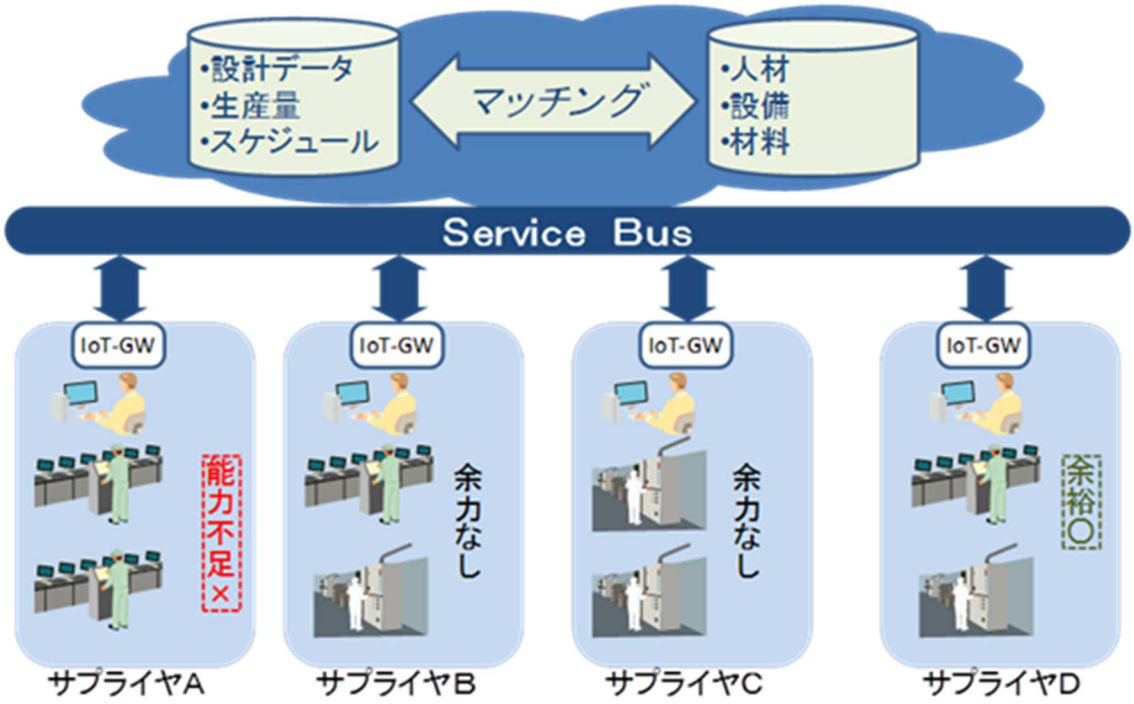

図 2-4 サプライチェーン管理および生産ライン最適化

2.2.4 ユースケース 4：映像監視

映像監視は、設置されたカメラ等からの映像データを自動解析することよって、市街地・駅・施設等での安全確保を目的としたユースケースである。映像監視のシステム構成の一例を図 2-5 に示す。カメラの映像データ、映像記録のトリガとなる通過検出センサのデータを収集し、不審者検出、証拠記録、検索のためのタグ付けなどを行う。また、遠隔からカメラの向きと ON/OFF 制御も行う。

映像監視のユースケースでは、カメラ自身が直接 WAN や LAN に接続する形態もあるが、ここでは IoT-GW を導入し、より大規模にカメラを設置する形態を想定する。

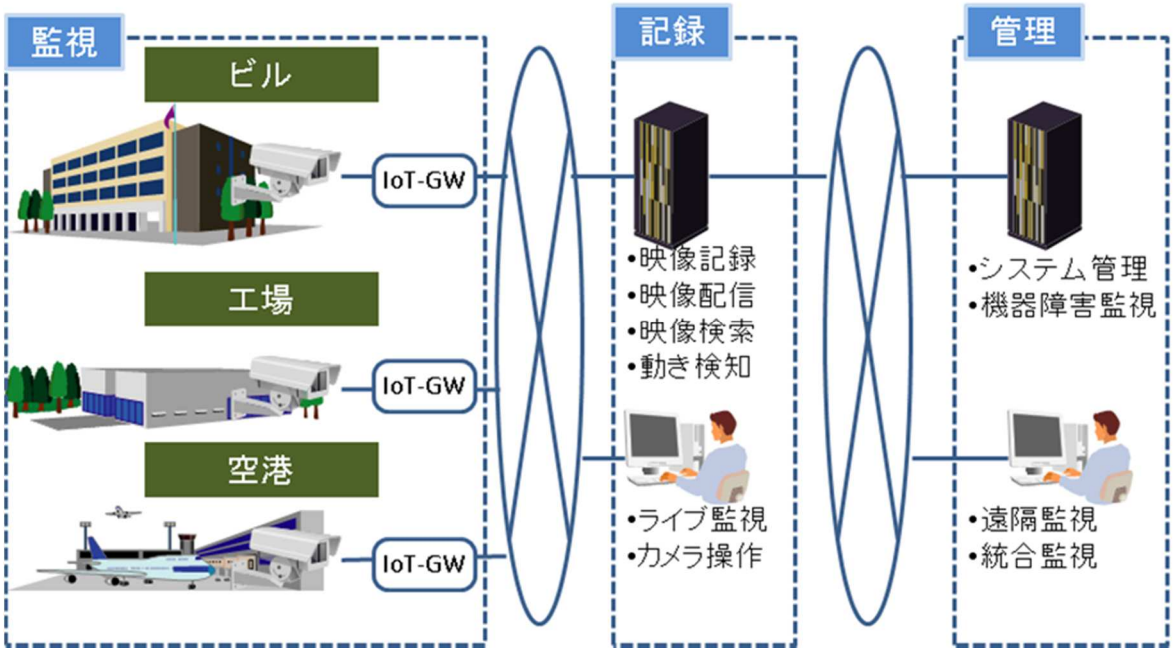

図 2-5 映像監視

2.3　保護すべき資産、考慮すべき影響

2.1 節の図 2-1 IoT-GW を適用するシステムモデルにおいて、IoT-GW を適用するシステムモデルを示した。このシステムモデルは、下記に列挙するように大きく 4 部分に分類できる。IoT では、これらの各部分は同一の組織の場合もあれば、別々の組織によって運用管理される場合もあり、全体として大きなシステムを構成するところに特徴がある。

- エンドポイント（IoT-GW、FAN/HAN、センサ、アクチュエータ）
- ネットワーク（WAN）
- サーバ（ヘッドエンドシステム、IoT-GW 管理）
- サービス（アプリケーション/サービス）

上記各部分には、一般的な情報システムと同様に、サービスやプロセスを実行する端末、機密情報、個人情報などの保護すべき資産が含まれる。一方、IoT においては、エンドポイントで収集するデータが各部分を流通する形になる。IoT では、エコシステム全体を通して、この流通データを保護すべき資産として扱う必要がある。

また、対象とするシステムモデルでは、実世界に物理的に影響を及ぼすアクチュエータが存在する。これが暴走した際には人命に関わる可能性もある。

したがって、脅威を評価する上では、システムそのものへの影響だけでなく、その周りに存在するものへの影響、すなわち、他企業・他組織への影響、人命への影響、社会への影響も考慮に入れる必要がある。表 2-2 に各ユースケースにおける保護すべき資産と想定被害・影響の例を示す。

表 2-2 各ユースケースにおける保護すべき資産と想定被害・影響例

ユースケース	保護すべき資産	想定被害・影響
ホームゲートウェイ	・個人情報 ・金融資産データ ・設定情報 ・ログ情報 ・ネットワーク	・乗っ取りによる攻撃への踏み台 ・金融資産の損失 ・なりすまし ・通信の停止
スマートメンテナンス	・センサ情報 ・生産設備 ・インフラ ・人命 ・ネットワーク	・発電設備の破壊・停止 ・停電による生産設備の破壊や停止、インフラの停止 ・停電による人命に関わる重大被害 ・通信の停止

サプライチェーン管理 および生産ライン最適化	・センサ情報 ・制御システム情報 ・生産設備 ・インフラ ・人命 ・工場内環境 ・ネットワーク	・データ取得が不可能となることによる本来機能の低下および精度の低下 ・設備停止、生産過剰/不足、不良品発生 ・生産設備の破壊や停止、インフラの停止、生産ロボットの暴走等の人命に関わる動作を引き起こす可能性 ・通信の停止
映像監視	・映像データ ・センサ情報 ・カメラ制御情報 ・個人情報 ・ネットワーク、	・監視カメラから得られるデータに対し、なりすまし等で誤ったデータ（例：通行人の数を過大に評価したデータ）を注入、2 次利用するユーザ（例：ナビサービス、マーケティング情報など）が誤った情報に基づいてサービスを提供 ・カメラの乗っ取り等によるプライバシーの侵害 ・通信の停止

3 想定されるセキュリティ上の脅威

IT セキュリティと IoT セキュリティの関係の概念図を図 3-1 に示す。IT セキュリティとは、既存の一般的な情報システムにおけるセキュリティのことである。IT セキュリティと IoT セキュリティでは、セキュリティ対策として重なり合う領域が多く存在する。一方で、2.1 節で述べたように、対象とする IoT のシステムでは、異なる種別の機器が接続されており、これまでの情報システムとは大きく異なる部分も存在する。したがって、本章では IoT セキュリティとして新たに考慮しなければならない領域に着目し、IoT-GW を適用したシステムにおいて想定されるセキュリティ上の脅威について説明する。

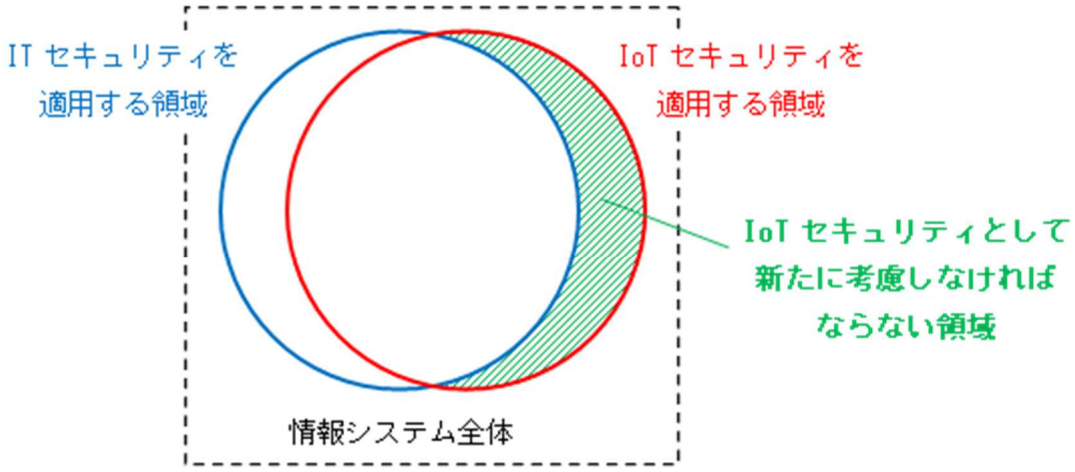

図 3-1 IT セキュリティと IoT セキュリティの関係

3.1 ネットワーク対応機器への攻撃事例

ネットワーク対応機器を狙った攻撃が年々増加しているが、過去の脅威事例から IoT-GW に関するものを紹介する。

(1) ホームルータへの不正な設定変更による偽 DNS サーバの参照[3]

2012 年 3 月にブラジルで行われた 2012 FIRST Symposium, Sao Paulo で、IoT-GW の脆弱性を悪用した攻撃事例が公開された。ブラジルで一般的に使用されている IoT-GW の脆弱性を利用し、管理者権限のパスワードを変更した上で、攻撃者の用意した DNS サーバを参照するように設定を書き換える攻撃である。攻撃者の DNS は偽の応答を返すため、利用者は偽サイトに誘導され、セキュリティソフトを無効化されるマルウェアをインストールさせられるなどして、機密情報を詐取される被害が発生している。

(2) ブロードバンドルータ脆弱性悪用事例

2012 年 5 月 16 日に無線 LAN ブロードバンドルータの一部にセキュリティ脆弱性があると情報が公開された。この無線 LAN ブロードバンドルータを使用すると利用者が設定した PPPoE の認証 ID およびパスワードが平文で保存されるため外部から取得される可能性があった。2012 年 5 月 24 日には、この脆弱性を改修したファームウェアが公開されたが、その後も被害が発生している。インターネット上で頻発している会員サービスサイトへのリスト型アクセス攻撃に、本脆弱性を持つブロードバンドルータから取得したインターネット接続 ID およびパスワードを使用したなりすまし接続がされた。その結果、攻撃インフラとして使用されている事象や詐取元利用者の契約情報の変更による金銭的被害などの発生が判明している。

(3) ペースメーカへのハッキング事例[4]

2012 年 10 月、Barnady Jack 氏が BreakPoint security conference 2012 でペースメーカへのハッキングについて発表し、ハッキング実演のデモ映像を流した。このデモ映像では、ノート PC を用いて、15m 以内のペースメーカに対し 830 ボルトの電流を流せることを実演した。ワイヤレストランスミッタ（送信機）をリバースエンジニアリングすることで、脆弱性を発見し、本デモ映像で利用している。本脆弱性では機器を制御するための情報を、特別なコマンドで引き出せるというものである。この他にも、ペースメーカとの無線通信に使われている機器に、不正なファームウェアをアップロードすれば、大量のペースメーカに同時攻撃することも可能であるとしている。

上記で紹介した以外にも多くの事象が発生しているが、IoT 機器を狙った攻撃には、新しいものだけではなくサーバやパソコン等と類似しているものも多くあるため、今後もサーバやパソコン等と同様の被害を受ける機器が増加することが見込まれる。サーバやパソコン等の脅威については IPA から情報セキュリティ 10 大脅威[5]という資料が発信されている。情報セキュリティ 10 大脅威には、その年で社会影響の大きかったセキュリティ上の脅威がランキング形式でまとめられている。表 3-1 に過去 3 年分の情報セキュリティ 10 大脅威についてまとめた。これらの脅威については、IoT 機器に対しても注意が必要である。

IoT 機器の脅威については、OWASP（The Open Web Application Security Project）[6]というプロジェクトにより紹介されている。このプロジェクトでは主に Web アプリケーションのセキュリティリスクに重点をおいた活動を行っており、Web アプリケーション脆弱性診断ツールなども提供している。誰でも適切な情報に基づく判断を行えるように、セキュリティを取り巻く状況の可視化やリスクへの対応について公開している。表 3-2 には、OWASP によって公開されている IoT の 10 大セキュリティリスク[7]についてまとめた。

表 3-1 情報セキュリティ 10 大脅威　2014・2015・2016

順位	2014 年	2015 年	2016 年
1 位	標的型メールを用いた組織へのスパイ･諜報活動	インターネットバンキングやクレジットカード情報の不正利用	インターネットバンキングやクレジットカード情報の不正利用
2 位	不正ログイン･不正利用	内部不正による情報漏えい	標的型攻撃による情報流出
3 位	Web サイトの改ざん	標的型攻撃による諜報活動	ランサムウェアを使った詐欺・恐喝
4 位	Web サービスからのユーザ情報の漏えい	Web サービスへの不正ログイン	Web サービスからの個人情報の窃取
5 位	オンラインバンキングからの不正送金	Web サービスからの顧客情報の窃取	Web サービスへの不正ログイン
6 位	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ	Web サイトの改ざん
7 位	SNS への軽率な情報公開	Web サイトの改ざん	審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ
8 位	紛失や設定不備による情報漏えい	インターネット基盤技術を悪用した攻撃	内部不正による情報漏えい
9 位	ウィルスを使った詐欺・恐喝	脆弱性公表に伴う攻撃	巧妙・悪質化するワンクリック請求
10 位	サービス妨害	悪意のあるスマートフォンアプリ	対策情報の公開に伴い公知となる脆弱性の悪用増加

表 3-2 OWASP による IoT10 大セキュリティリスク

項番	英タイトル	日本語タイトル
1	Insecure Web Interface	セキュリティが確保されていない Web インタフェース
2	Insufficient Authentication/Authorization	不十分な認証
3	Insecure Network Services	セキュリティが確保されていないネットワークサービス
4	Lack of Transport Encryption	暗号化されていない通信路
5	Privacy Concerns	プライバシーに関する懸念
6	Insecure Cloud Interface	セキュリティが確保されていないクラウドインタフェース

7	Insecure Mobile Interface	セキュリティが確保されていないモバイルインタフェース
8	Insufficient Security Configurability	不十分なセキュリティ設定
9	Insecure Software/Firmware	セキュリティが確保されていないソフトウェア/ファームウェア
10	Poor Physical Security	物理的セキュリティの脆弱さ

3.2　IoT-GWを適用したシステムの特徴・課題

2.2 節で説明したユースケースおよび 3.1 節で説明した脅威事例を基に、IoT-GW を適用したシステムにおける特徴、課題を抽出した。IoT-GW を適用したシステムの課題について以下に示す。

(1) フィールド側にガバナンスがなく、機器・端末に対する脅威が大きい。

機器・端末が所有者または利用者の物理的管理範囲外に配置されている、または攻撃者が物理的に容易に侵入可能な場所に配置されている場合がある。

(2) フィールド側に設置される機器・端末が安価なため、高価なセキュリティ対策が困難。

フィールド側に設置される機器・端末に許容されるコストが低いため、十分な強度の暗号化やファイアウォール等のセキュリティ対策機能を搭載、設置することが困難である場合がある。

(3) フィールド側にアクチュエータが接続されている。

センサによる計測だけでなく、制御対象となるアクチュエータや、制御システムのコントローラがネットワーク的に繋がっているため、各機器に対して脆弱性をついた攻撃や、不正アクセスが実行された場合、重大な影響・被害(人命や社会的混乱)に繋がる場合がある。

(4) 長期使用を前提としたシステムでは更新が難しい。

社会インフラや産業システムは 10 年を超えて使用されることが多いため、サポート期間が切れたソフトウェアを使い続けざるを得ない状況や、一度稼働させるとシステムの更新が難しい場合がある。仮に脆弱性が発見された場合、未対策の状態が続いてしまう可能性がある。

(5) 組織間における全体最適化により、特定のデータへの依存度が高まる。

IoT 適用の目的の 1 つはビッグデータを用いた全体最適化である。そのため、組織間でのデータ共有と利活用が進展し、各組織が保持するインフラやシステムにおけるデータへの依存度が高くなることが予想される。標的型の攻撃や、悪意のある人間が作成したプログラムによって、解析されてしまう機会が増加する。

3.3　IoT-GWを適用したシステムにおいて想定されるセキュリティ上の脅威

IoT-GW を適用したシステムにいて想定されるセキュリティ上の脅威・リスク項目について、上記の特徴・課題から抽出した 10 項目を以下に示す。

(1) センサの停止により、データ取得が不可能となる。【脅威番号①】

センサの盗難、故障・電源断、DoS 攻撃、自然災害などの要因によって、センサが停止状態になりデータ取得が不可能となり、精度や品質の低下といった影響が出る。例えば、スマートメンテナンスのユースケースでは、温度や回転数などのデータが欠落することによって保守・点検の品質が下がってしまう。

(2) センサの不正改造などにより、不正データの送信が行われる。【脅威番号②】

フィールド上のセンサが、内部の人間や、悪意のある第三者に物理的に不正改造されたり、偽造センサが設置されたりすることにより、不正データの送信やデータの改造が行われ、アプリケーション/サービスに影響が出る。例えば、サプライチェーン管理および生産ライン最適化のユースケースでは、設備停止・生産過剰/不足、不良品発生などの影響が考えられる。

(3) センサが乗っ取られることにより、DoS 攻撃へ加担する。【脅威番号③】

センサが乗っ取られることによって、他の機器に対してリクエスト要求や帯域占有などの DoS 攻撃が発生する。例えば、映像監視のユースケースでは、他の機器のデータ収集阻害を引き起こす。センサ個々では能力は低く、大きなトラヒックも発生できないが、設置されている台数が脅威となる場合もある。

(4) 生産設備の破壊や停止、インフラの停止、人命に関わる動作が誘発される。【脅威番号④】

アクチュエータや制御対象のコントローラが乗っ取られることにより、工場などの生産設備の破壊や停止、発電所・上下水道などのインフラの停止・危険の発生、車両やロボットの暴走などの人命に関わる動作が誘発される。例えば、サプライチェーン管理および生産ライン最適化のユースケースでは、外部からコントローラを乗っ取られ、ロボットアームを暴走させられ、周りの作業員に影響が出ることが考えられる。

(5) ネットワークからエンドポイント機器が攻撃される。【脅威番号⑤】

これまでネットワーク接続が想定されていなかった機器がネットワークに接続されるた

め、不正アクセス、乗っ取り、DoS などの攻撃が容易に実行される。機器の処理能力やネットワーク帯域が小さいため、DoS 攻撃を受けるとすぐに被害が出る。例えば、スマートメンテナンスのユースケースでは、トンネル壁面、山岳部雨量センサへの攻撃で列車運行に障害が出る可能性がある。

(6) 攻撃者が FAN/HAN へ物理的に侵入して攻撃する。【脅威番号⑥】

フィールド上のネットワークである工場や宅内の FAN/HAN に、不正な機器を物理的に接続されることでセキュリティが侵害される。例えば、ホームゲートウェイのユースケースでは、不正に改造された中古品による家電やゲートウェイを使用することによって、ネットワーク側への攻撃や個人情報の搾取が可能となる。

(7) センサからサーバへのデータ送信により処理負荷や消費電力を増加させる。【脅威番号⑦】

大量のセンサからの同時刻データ送信によって、データ自体は正常であっても、サーバの処理負荷・消費電力の急増、さらにはサーバダウンを引き起こす。例えば、映像監視のユースケースでは、大量のカメラから同時に映像データを流すように仕組まれると、サーバの処理が間に合わなくなり、開発者やシステム設計者の意図した通りに動作しなくなる可能性がある。

(8) エンドポイント機器の暗号強度不足によりデータ盗難が発生する。【脅威番号⑧】

センサなどのエンドポイント機器の処理能力や消費電力の制約によって、高度な暗号化が実施できない場合、通信傍受などを防止できない。例えば、サプライチェーン管理および生産ライン最適化のユースケースでは、工場内制御システムのコンポーネントでは生産に影響を与えるものは極力排除される傾向にあるため、暗号処理の強度が不足することが懸念される。

(9) 誤データが注入され、伝搬される。【脅威番号⑨】

誤データを注入したり、一部のデータを削除・改変したりすることで、データベース上にも誤データが残り、誤った統計データを生成され、社会に誤った情報発信が行われる。例えば、サプライチェーン管理および生産ライン最適化のユースケースでは、センサから得られるデータに対し、なりすまし等で誤ったデータ（例：生産台数を過大評価したデータ）を注入され、2 次利用するサプライチェーンが誤った情報に基づいて製造工程を決定してしまう。また、オープンデータなど公共性のある情報資産は、機密性はないが、社会に

与える影響が大きくなる可能性がある。

(10) 更新が困難なシステムの脆弱性をついた攻撃をされる。【脅威番号⑩】

社会インフラや製造ラインなど、システムに脆弱性があり、攻撃を受けた場合にも、システム運用やサービスを継続させる必要がある。システム可用性を優先することにより脆弱性対処が遅れ、その脆弱性をついた攻撃をされることが懸念される。例えば、サプライチェーン管理および生産ライン最適化のユースケースでは、製造ラインを止められず、攻撃や脆弱性を放置することが考えられる。

今回、10 のセキュリティ上の脅威を抽出したが、技術の進歩とともに脅威・課題も増えてゆくためその時々で見直しが重要である。

4 開発のフェーズとセキュリティの取組み

4.1 ライフサイクルにおけるフェーズの定義

製品の開発フェーズは、大きく「製品企画」、「設計・製造」、「評価」、「運用保守」、「廃棄」の 5 フェーズに分類される。提供する製品において十分なセキュリティを確保するには各フェーズにおいて十分な対策を施し、製品のセキュリティ品質を確実なものとするべきである。

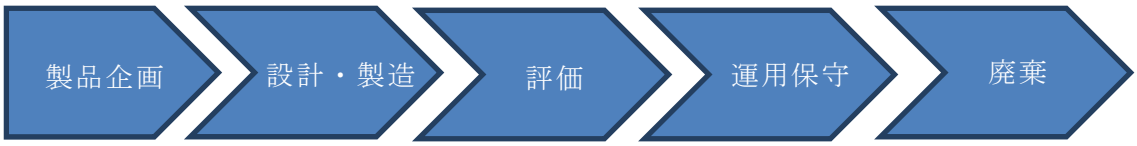

図 4-1 ライフサイクルにおけるフェーズ

表 4-1 フェーズの定義

フェーズ	説明
製品企画	製品のコンセプト、予算、要件定義の策定を行う。
設計・製造	企画フェーズの要件定義を受けて設計・実装・製造を行う。
評価	製造された製品の正当性の評価を行う。
運用保守	所有者（利用者）に販売され、利用者が使用している期間に、インシデントへの対応、整備、サービス等を行う。
廃棄	所有者が廃棄手続きを行う。

4.2 各フェーズにおけるセキュリティ取組み

前節で概説したライフサイクルの各フェーズおいて実施すべきセキュリティへの取組みを説明する。

4.2.1 製品企画フェーズ

製品のセキュリティ品質を確保するには、より上位からのセキュリティ設計が必要となる。ここでは製品企画におけるセキュリティ品質の確保について述べる。

表 4-2 製品企画フェーズでのセキュリティ取組み

項番	項目	内容
1	保護すべき資産および脅威の特定とリスク分析	製品を開発するに当たり、市場ニーズや顧客要求に基づき企画した製品について、概要、製品の想定利用環境、想定前提条件、保護すべきデータ、保護すべきデータと人的環境のマッピング、想定する脅威、類似製品で知られる既知問題などの要素を元に保護すべき資産および脅威の特定を行う。具体的分析例は 5 章を参照のこと。 ポイントとしては機器が取り扱うデータにどのような脅威が存在するか、例えば、他者への攻撃の踏み台にされてしまう、といった「取り扱うデータ以外の脅威」等を明確にし、それら脅威に対して設計や運用で対策を行う必要がある。 特定した保護すべき資産と、脅威を考慮し、5 章で後述するようなリスク分析評価方法によりリスク分析を行い、設計および運用にて対策を施す。
2	セキュリティ要件の抽出	上記項番 1「 保護すべき資産および脅威の特定とリスク分析」の内容同様、製品概要、製品の想定利用環境等を考慮し、製品として考慮すべきセキュリティ要件の抽出を行い、次フェーズの設計・製造にて実装を行う。具体的なセキュリティ要件としては以下の例が挙げられるが、開発する機器により過不足があると思われるので、開発者にて十分に検討する必要がある。 ・機密情報の流出防止 ・障害復旧 ・踏み台攻撃への対策 ・アラート機能（攻撃を受けた、不正侵入を受けた等） ・ロギング機能 ・サービス機能 ・ハードウェアに対する直接的な攻撃対策 ・サイドチャネルアタックへの対策 ・機密情報の廃棄機能
3	企業組織としての対応	組織においては情報セキュリティ方針を定め、その方針に基づいた情報セキュリティ規則を定義し、情報セキュリティ対策を講じる。 情報セキュリティ規則例 ・管理規定の構成と位置づけ ・管理体制と責務 ・教育、点検の実施

4.2.2 設計・製造フェーズ

4.2.1 で実施したリスク分析、セキュリティ要件の抽出結果を基に、対策を設計・製造フェーズで実装する。

表 4-3 設計・製造フェーズでのセキュリティ取組み

項番	項目	内容
1	開発プラットフォーム選定	(1) 既知の脆弱性の確認 ・開発する製品に取り込む OS、boot プログラムやアプリケーションプログラムとそのバージョンについて既知のセキュリティ脆弱性問題が存在しないことを確認する。 ・開発する製品で使用する CPU にセキュリティ脆弱性問題が存在しないことを確認する。 (2) 認証や情報保護に使用する暗号技術に関する技術動向の確認 ・日本においては CRYPTREC が提供している報告書があり、認証や情報保護に暗号技術を利用している組込みシステムを開発する際に参照できる。 ・海外においては各国の取り決めがあるため、各国の暗号基準を参照する必要がある。
2	セキュリティ機能の実装	セキュリティ要件の定義に従い、機器にセキュリティ要件を担保するための機能を実装する。 表 4-2 の項番 2 で挙げたセキュリティ要件に対する対策例を以下に示す。 (1) 機密情報の流出防止 ・機密度に応じた暗号アルゴリズムの採用 ・暗号化メモリなどの採用 ・アクセス制御の実装 ・不要なサービスの無効化 ・リムーバブルメディア自動実行の無効化 ・他者が推定しにくいパスワード設定 ・パスワードの連続試行の防止 ・適切なアカウント権限の付与 ・パスワード情報の保護 ・ファイル共有の無効化 ・ファイルへのアクセス権設定 ・ログの取得 ・不正アクセスの監視

		・NAT 機能の実装 ・ファイアウォール機能の実装 (2) 障害復旧 ・障害検出と通知機能 ・ログの取得 ・設定情報の 2 面化 (3) 踏み台攻撃への対策 ・特定期間内での多すぎるパケットデータの受信検出 ・特定期間内での多すぎるパスワード誤入力検出 ・ポートスキャン検出 ・想定外の大きいサイズのパケットデータの受信検出 ・不正操作の抑止 ・ping に対して reply を送信しない仕様もしくは、reply を送信したとしても rate limit を設定 ・脆弱性の伝播を防ぐために機器内のデータをサンドボックス化 (4) アラート機能（攻撃を受けた、不正侵入を受けた等） ・攻撃を受けた場合のランプ等を利用したユーザ通知 ・ユーザによるポート開放など脆弱性に繋がる操作への警告表示 ・取扱説明書などへ使い方によって考えられるリスク、脅威の表示 (5) ロギング機能 ・機器に対して不正アクセスがあったときの、時刻、Source IP アドレス、ポート番号、プロトコルの種類等の記録 ・機器のユーザによる認証ログ記録機能の実装是非の決定。ユーザ ID、ログイン回数、ログインエラー回数、時刻等 ・上記ログを残すために必要な分だけの機器内メモリ容量の検討 (6) 保守機能 ・保守者と一般利用者で管理画面を区別 ・保守者と一般利用者で権限を分ける認証の実施 ・デバッグ機能等の不要な機能の削除 ・脆弱性対策のための遠隔プログラムアップデート機能 ・ユーザへプログラムアップデートを促すための製品の管理画面やランプ表示による最新プログラムの有無の表示 ・初期化(工場出荷状態に戻す)機能 ・データの初期化を確実に実現できるよう、対象記憶媒体の特性

		を考慮した(Flash ROM であればウェアリングレベル)完全消去機能の実装 ※データの浄化方法については NIST SP 800-88 Guidelines for Media Sanitization[13]等を参照
3	使用するプロトコルのリスク検討	一般的に IoT-GW においては使用されるプロトコルは仕様が標準化または公開されているものがあり、標準化されているがゆえに攻撃者から狙われやすい。設計段階において、使用するプロトコルとそのプロトコルに関する脆弱性、影響を抽出してその対策を設計・製造時に実装する必要がある。付録 1 に使用するプロトコルと脆弱性、影響をリストアップした一例を示す。このような形で使用しているプロトコルと脆弱性、影響をまとめることで、既知の脆弱性への対策点が明確になり、網羅性が上がる。
4	ソフトウェア実装	(1) セキュアプログラミング セキュアプログラミングとは攻撃者やマルウェアなどの攻撃に耐えられる、堅牢なプログラムを書くことである。攻撃の脅威をあらかじめ想定し、たとえプログラムが意図しないデータを受け取ったとしても、意図した通り正しく動作するプログラムを書くことである。 製品開発においてセキュリティ脆弱性問題の作り込みを防止するためには、セキュアプログラミングを実施する必要がある。具体的なセキュアプログラミング手法については、IPA が発行する「IPA セキュア・プログラミング講座」があり、これらは IPA のホームページから参照できるので、実際のプログラミングで実践するとよい。 (2) OS に実装されているセキュリティ機能の活用 OS にも独自にセキュリティを考慮した機能が盛り込まれている。例えば、プログラムをロードする度にアドレス空間をランダム化し、仮に脆弱性があったとしても、脅威度を下げる ASLR(Address Space Layout Randomization)がある。 これらの機能を使用できるか、積極的に検討するべきである。
5	ハードウェア実装	(1) ハードウェアに対する物理的な攻撃への対策 ハードウェアに対する物理的な攻撃への対策としては以下のような方法がある。 ・プロービングによるデータ解析を難しくするために、リファレンス回路を丸ごとコピーした部品実装、層構成、配置配線を行わない、また BGA、FBGA、LGA などのプロービングしにくい実装方法が必要となる部品を使用する。さらに、重要な信号線は表層配線とせずに内層配線とする。 ・JTAG などのデバッグポートや診断ポートは製品開発時に実装されることが多いが、製品リリース時にはデバッグポートを

		露出しないようにする。 ・使用している CPU のアドレスマップ、レジスタの内容を CPU のデータシートから容易に入手されることを防ぐために実装する CPU の品名表示を消去する。 （どんな部品を使用しているか不明であれば、レジスタ設定などを変更不可） ・機器の持ち去りを防ぐためにワイヤーロックをかけることができる穴を実装する。 ・いたずら防止ネジを使用する。 ・筐体開封防止のために、セキュリティラベルを使用する。 ・筐体開封検知機能を具備する。（開封を検知したら、メモリの中身を消去） ・容易に開封できない構造にする。 ・金属カバーでシールドする。 (2) サイドチャネル攻撃への対策 サイドチェネル攻撃への対策としては以下のような方法がある。 ・サイドチャネル情報（消費電力や漏えい電磁波）を隠蔽または遮蔽する。 これらは代表的なハードウェア実装の対策であり、開発する製品によってはさらに対策が必要な場合もある。
6	開発の外部委託における取組み	外部委託先へ､以下のような発注元の設計ルールや基準を明示し、そのルールに従ってもらうべきである。[11]、[12] (1) 外部委託に関する基準類の整備 外部委託に関する次のような基準類や手続き、体制を整備する。 ・外部委託の対象としてよい範囲や、委託先によるアクセスを認める情報資産の範囲を判断する基準 ・委託先の選定手続き、選定基準および委託先が備えるべき要件に関する基準 ・委託業務に関して情報セキュリティが侵害された場合の対処手順 ・委託先の情報セキュリティ対策の実施状況を確認するための評価基準 (2) 委託先の選定 事前に定めた委託先の選定手続き、選定基準、委託先が備えるべき要件に関する基準に基づき、委託先を選定する。委託先候補には、事前に次のことを伝達する。 ・委託業務遂行に関して委託先が実施するべき情報セキュリティ対策の内容

		・委託業務に関して情報セキュリティが侵害された場合の対処手順 ・委託先の情報セキュリティ対策の実施状況を確認すること、および、確認の結果、情報セキュリティ対策が不十分である場合の対処手順 (3) 委託先との契約 委託先との契約書には、一般的に次のことを記載する。 ・外部委託の対象となる情報および情報システムの範囲 ・機密情報の取扱いと管理に関する取り決め ・守秘義務や契約違反時の措置 ・再委託に関する取り決め、契約終了時の情報の返却・破棄 ・情報セキュリティ事件・事故の際の対応手順 ・情報セキュリティ対策の履行が不十分である場合の対処手順 ・委託業務の作業に携わる者の特定とそれ以外の者による作業の禁止 ・情報セキュリティ監査を受け入れること ・提供されるサービスレベルに関する取り決め (4) 委託先の監督 委託後は、必要に応じて適宜委託先を監督する。主な監督内容は以下の通り。 ・要求するセキュリティレベル達成のために、委託業務の担当者が実施する具体的な取組み内容 ・委託業務は、双方合意した作業者のみにより行われていることの確認 ・情報セキュリティ監査などによる情報セキュリティ対策実施状況の確認 (5) その他 その他の取組み内容は以下の通り。 ・委託先に提供する情報は必要最低限とし、情報提供に当たっては、不要部分のマスキングや暗号化など安全な受渡方法を用い、情報提供の記録を保存する。 ・外部委託契約の継続に当たっては、選定手続き、選定基準、委託先が備えるべき要件に基づき、その都度審査する。 ・契約終了時には、業務委託に際して提供した情報や情報システムの返却または破棄を確認する。

4.2.3 評価フェーズ

4.2.2 に記載されているセキュリティ対策がとられ、機器に脆弱性がないかどうかを評価フェーズで確認する。

表 4-4 評価フェーズでのセキュリティ取組み

項番	項目	内容
1	脆弱性の検証	(1) 脆弱性の検証 脆弱性は仕様の不備や、セキュアプログラミングを行わないことなどによって潜在的に作り込まれてしまう。脆弱性検証作業を人間が手作業で行うことは大変困難であり、脆弱性検証ツールを使用することによって、網羅的、効率的に脆弱性の点検を行うことができる。 表 4-5 に OSS として提供されているツールの一部を記載する。これら全てを使用することで脆弱性検証の網羅性をあげることができると考える。いずれのツールも OSS であり、新たな脆弱性に OSS 開発コミュニティが対応してくれるため、開発者にとって導入のメリットがあると考える。また CCDS としても今後表 4-5 に挙げた OSS を利用したツールを開発し提供する予定である。 なお、IoT-GW においては下部に繋がる機器へのアクセスを防ぐという観点から、開いているポートや稼動サービスの探索を行うネットワーク、サーバの脆弱性の点検を優先的にツールを使用して検証する必要がある。(例 OpenVAS) (2) 脆弱性検証のタイミング 脆弱性検証は開発時や製品出荷前の評価段階で実行されるべきであるが、脆弱性は日々増えていくので運用後においても定期的に検証を実施する必要がある。 (3) 脆弱性検証項目 IoT-GW で一般的に使用されるプロトコルとその脆弱性の一例を付録 1 に示す。これら脆弱性に関してツールを使用して検証を行う必要がある。 (4) 脆弱性検証の留意事項 ・ツールが正しく動作していることを確認すること。 ・ツールが出力する結果レポート等を確認し、脆弱性の有無について検証を行う。結果の中には 脆弱性の疑いのあるもの、システムの使い方によっては発生する可能性のあるものをレポートとして表示されることがある。その場合、その内容を確認して、脆弱性か否かを判断する必要がある。

表 4-5 脆弱性検証ツール一覧

項番	種類	ツール名	目的
1	ファジングツール	Sulley	対象ソフトウェアの脆弱性の有無をチェックする。 予測不可能な入力データを与えることで意図的に例外を発生させ、その例外の挙動を確認することで脆弱性をチェックする。
2	ネットワーク脆弱性検査	OpenVAS	IoT-GW に導入されているソフトウェアのバージョンや設定、構成などを確認して、それらの脆弱性の有無をチェックする。
3	Web アプリ脆弱性検査	OWASP ZAP	Web サーバ/アプリケーションの脆弱性の有無をチェックする。 検査対象機器に導入されている Web サーバ機能に対してリクエストを送信して、XSS や SQL/Command Injection などの脆弱性をチェックする。
4	パケット生成	Ostinato	不正パケット受信時の振る舞いを確認するため、不正パケットデータを作成、IoT-GW に対して送信する。 DoS 攻撃などを想定して、高負荷時の振る舞いを確認するため、大量の IP パケットを送信、負荷をかける。
5	Web リクエスト生成	Gatling	DoS 攻撃などを想定して、高負荷時の振る舞いを確認する。 対象となる Web アプリケーションに対して条件(リクエスト数/秒、利用者の挙動（画面入力、画面遷移など）) を指定して負荷をかける。

4.2.4 運用保守フェーズ

製品のセキュリティ品質を確保するには、製品そのものへの対策だけではなく製品リリース後のセキュリティ品質維持も重要である。ここでは運用保守フェーズにおけるセキュリティ品質の確保について述べる。

表 4-6 運用保守フェーズでのセキュリティ取組み

項番	項目	内容
1	最新の脆弱性への対応	(1)最新の脆弱性への対応 使用している OS、boot プログラム、アプリケーションに脆弱性がないかどうかを、以下に挙げる脆弱性関連情報を常にウォッチし、関連する脆弱性の場合、プログラムのアップデートを実施する。 ・CVE(Common Vulnerabilities and Exposures) ・NVD(National Vulnerability Database) ・JVN(Japan Vulnerability Notes) ・JVN iPedia ・OSVDB(Open Source Vulnerability Database)
2	企業､組織としての対応	・脆弱性が発見された場合、自社の HP、電子メール等によるユーザへの脆弱性の通知、注意喚起の実施 ・ユーザあるいは項番 1 で挙げた脆弱性関連情報を取扱う機関から情報を受け取るための窓口の設置と、その情報をいち早く開発者に伝える体制の構築 ・脆弱性が発見され、開発者に情報が伝わった後、「誰が」、「どのように」対応するかを事前に決定しておく ・脆弱性の影響度、波及性の確認や対策の修正プログラム作成等に向けた対応フローの策定 ・上流工程での再発防止の仕掛け構築 ・開発者が会社を辞めてしまった後、機密情報の持出しを行わないよう労務契約書へ明記
3	機器利用期限	・今現在十分と考えられているアルゴリズムや鍵長も、将来的には不十分になる可能性があり、ユーザへある時点で機器利用の停止を推奨することを検討する ・利用期間が長いと想定される IoT-GW においては、ベンダーとして保守期間を明確化し、マニュアルや HP 上でユーザに周知する

4	啓蒙活動	・デフォルトパスワードからパスワード変更を行うように取扱説明書等で促す ・直接ネットワークにつながるため、設定をひとつ間違えると機器が危険に晒されるというということを取扱説明書等で周知する ・機器の能力、どんなことができ、それらが悪用された場合どのようなリスクにつながるかを周知する
5	運用方法の提案	・保護されたネットワーク内に機器を配置するなど、システム全体として脅威から防御するということを周知する ・機器として具備しているがユーザとして使用しない機能(例えば、UPnP、無線 LAN、PPP、IPv6 等)は OFF にすることを促す ・無線 LAN は SSID やパスワードによる制限だけではなく、MAC アドレスフィルタリングにより意図しない接続を防ぐよう周知する

4.2.5 廃棄フェーズ

IoT-GW は様々なデータを扱うため、中には重要なデータも含まれることがある。それらのデータは多くの場合、ネットワーク側へ転送され現在は機器の中には保存されていないことがほとんどであるが、中には扱うデータを記憶するためのストレージを搭載している機器も登場しており、機器を廃棄する場合には注意が必要である。ここでは廃棄フェーズにおけるセキュリティ品質の確保について述べる。

表 4-7 廃棄フェーズでのセキュリティ取組み

項番	項目	内容
1	機器廃棄方法の周知	・機器内にデータが残留したまま廃棄することで想定される脅威、リスクを取扱説明書等で明示 ・廃棄時には機器の設定やメモリ内のデータを初期化(工場出荷状態)することを取扱説明書等で推奨する ・破壊し廃棄することを推奨する場合には、各自治体の規則に従って廃棄処分する旨を取扱説明書等でユーザに周知する ・廃棄する場合は、リユースされないようにきちんと破壊されたことを確認するよう取扱説明書等で推奨する

5 リスク分析・評価

安心安全な IoT 機器を設計開発する場合、実施すべきセキュリティ対策方針を定めるため、システムで想定される脅威を抽出してリスク分析を行う必要がある。国際標準規格 ISO/IEC TR 13335-3 (GMITS part3)[10]の指針によれば、リスク値は、資産価値×脅威の基準値×脆弱性の基準値×発生頻度の基準値によって計算できる。脅威の影響度合いなどはユースケースごとに異なるため、上記の基準値をユースケースに応じて独自に設定し、リスクの分析・評価を行うこともできる。

ここでは ISO/IEC TR 13335-3 をベースとした、簡易的なリスク分析の方法を紹介する。大きなリスク分析の流れはの図 5-1 リスク分析手順通りとなる。

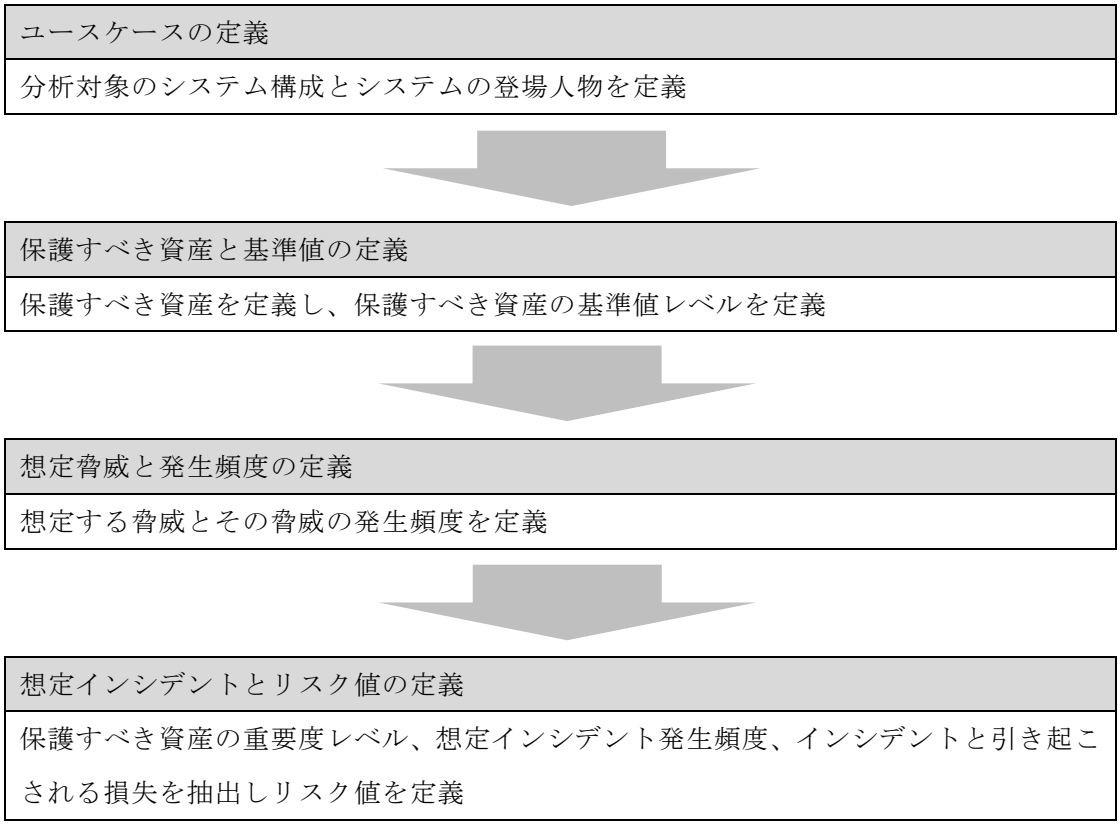

図 5-1 リスク分析手順

5.1 ユースケースの定義

IoT の世界においてはユースケース間でリスク項目に大きな差異がある。ユースケースごとに関連する IoT セキュリティの特徴・課題やリスク項目は異なるため、ユースケースのグルーピングは困難である。そのため、個別のユースケースを丁寧に評価していくことが大事である。本書では 2.2 項で示したように、4 つのユースケースを例に定義すること

で、分析対象のシステム構成を定義し、保護すべき情報資産を定義することとした。

5.2　保護すべき資産と重要度の定義

保護すべき資産は前項で定義したユースケースから導き出す必要があり、IoT 機器が扱う情報の種類、IoT 機器自体の機能、あるいは IoT 機器本体等様々な面から想定する必要がある。作業のポイントとしては製品全体を把握している設計者が，保護すべき資産を漏れなく洗い出す必要がある。表 5-1 はホームゲートウェイをユースケースとした場合の保護すべき情報資産の例である。また、図 5-2 にシステム構成を示す。

表 5-1 ホームゲートウェイをユースケースとした保護すべき資産例

保護すべき資産 (想定被害)	要因となるセキュリティ脅威
個人情報	・エンドポイント機器の暗号強度不足によりデータ盗難が発生する。 ・ネットワークからエンドポイント機器が攻撃される。
金融資産データ	・エンドポイント機器の暗号強度不足によりデータ盗難が発生する。 ・ネットワークからエンドポイント機器が攻撃される。
設定情報	・エンドポイント機器の暗号強度不足によりデータ盗難が発生する。 ・ネットワークからエンドポイント機器が攻撃される。
ログ情報	・エンドポイント機器の暗号強度不足によりデータ盗難が発生する。 ・ネットワークからエンドポイント機器が攻撃される。
セキュリティ情報 (電子証明書、暗号鍵)	・エンドポイント機器の暗号強度不足によりデータ盗難が発生する。 ・ネットワークからエンドポイント機器が攻撃される。
ホームゲートウェイ本体	・攻撃者が FAN/HAN へ物理的に侵入して攻撃する。

※ホームゲートウェイのユースケース

有線 LAN：PC(ネットサーフィン、ネットバンキング、ネット株取引)

無線 LAN：PC、スマホ、ポータブルゲーム

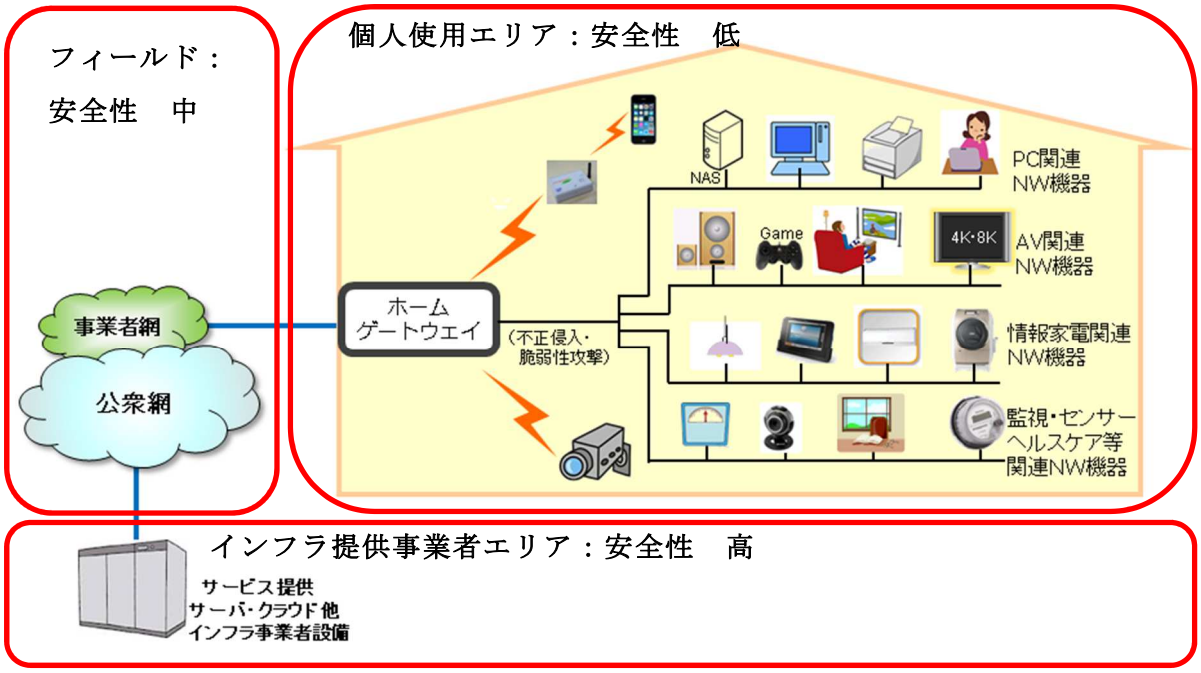

図 5-2 ホームゲートウェイをユースケースとした場合のシステム構成

次に保護すべき情報資産の重要度を定義する。使用する重要度の指標として表 5-2 は各ユースケースにおいて保護すべき情報資産の重要度を NIST IR7628 の重要度基準をベースに定義の策定を行った内容である。

表 5-2 保護すべき資産の重要度定義

	重要度基準		
	3(影響が重大、深刻)	2(影響が大きい)	1(影響が少ない)
機密性 (Confidentiality)	漏えいした場合に、利用者のプライバシーが侵害されるか、システムが重大な脅威にさらされる情報	左記以外の情報で、システムで恒常的に利用され、漏えいにより一定期間、脅威が発生する情報	左記以外の情報で、漏えいしても一時的且つ軽微な脅威にしかならない情報
完全性 (Integrity)	改ざんされた場合に、不正な課金が発生するか、端末制御に影響し、物理的損害が発生する可能性がある情報	左記以外の情報で、改ざんされると一定期間、利用・運営に支障をきたす情報	左記以外の情報で、改ざんされても軽微な障害しか発生しない情報
可用性 (Availability)	情報を扱うシステムの可用性が完全に損なわれる情報	情報を扱うシステムの可用性が一定期間にわたり損なわれる情報	情報を扱うシステムの可用性が一時的且つごく一部、損なわれる情報

表 5-3、表 5-4 は表 5-2 を用いてホームゲートウェイをユースケースとした場合の、ホームゲートウェイが扱う資産をピックアップしそれらが保護すべき資産すべきかどうかを判定した一例である。これらのように保護すべき資産の重要度の定義を行う。ここでは重要度が 2 以上となっている情報、物理資産を保護対象と定義した。

表 5-3 ホームゲートウェイにおける情報資産の重要度定義例

No.	情報資産	機密性(C)	完全性(I)	可用性(A)	保護対象?
1	個人情報	3	3	2	Yes
2	金融資産データ	3	3	2	Yes
3	設定情報	3	3	2	Yes
4	ログ情報	2	2	1	Yes
5	セキュリティ情報 (電子証明書、暗号鍵)	3	2	2	Yes

表 5-4 ホームゲートウェイにおける保護すべき情報資産の重要度定義例

No.	物理資産	生成、保持する情報資産 No.	機密性(C)	完全性(I)	可用性(A)	保護対象?
6	ホームゲートウェイ本体	1,2,3,4,5	3	3	3	Yes

5.3 想定脅威と発生頻度の定義

3.3 節において一例として挙げた想定されるセキュリティ上の脅威が、どの程度の頻度で発生するかを考慮することがリスク分析では必要になる。本書では機器を長期使用するという IoT 特有の事情を考慮し発生頻度を表 5-5 に示す 4 段階に分類した。

表 5-5 想定脅威の発生頻度定義

発生頻度	1：（極小）	2：（小）	3：（中）	4：（多）
	10 年に 1 回以上	5 年に 1 回以上	2 年に 1 回以上	1 年に 1 回以上

5.4 想定インシデントとリスク値の定義

ここではホームゲートウェイをユースケースの一例とし、脅威分析より想定インシデントを抽出し、インシデントにおける重要度と発生頻度を用いてリスク計算した一例の結果を表 5-6 に示す。ここで算出されるリスク値はあくまで相対評価であるため、後述する CVSS のようにある一定のスコア以上であれば危険であるというような判断は難しいが、製品企画段階

で実施することで設計・製造フェーズにおいて取り組まなければならないセキュリティ対策方針が明確になると考える。

表 5-6 想定インシデントとリスク値の結果

インシデント	引き起こされる損失	想定脅威※	関連資産	重要度			発生頻度	リスク値
				C	I	A		
GW 破損・停止	公衆網との通信途絶	⑤DoS 攻撃 ⑥改造、破壊	2,6	―	―	3	2	6
GW 内 情報の漏えい	公衆網－GW 間 情報の漏えい	⑤設定値改変 ⑩不正ファームウェア書き込み ⑨なりすまし機器利用 ⑩ウィルス感染 ⑧通信データの傍受	1-6	3	―	―	4	12
GW の 誤動作	公衆網－GW 間 情報の改ざん	⑤設定値改変 ⑩不正ファームウェア書き込み ⑨なりすまし機器利用 ⑩ウィルス感染 ⑧通信データの傍受	1-6	―	3	3	3	27

※3.3 節の脅威番号を示す。

以上の通り、簡易的にリスク分析を行う手法を示したが、情報システムに対するリスクの分析・評価手法は多数存在する。代表的な手法は、ETSI TS 102 165-1[8]や CVSS v3.0[9]である。両評価手法の概要と課題について以下に説明する。

5.5 ETSIの評価手法

ETSI TS 102 165-1 は、欧州電気通信標準化機構 ETSI（European Telecommunications Standards Institute）によって策定された、通信を伴う情報システム向けのリスク分析・評価手法である。システムにおいて発覚した脆弱性のリスクを評価、運用管理者が脆弱性対策の優先順を意思決定するのに活用することを目的とする。攻撃の頻度（攻撃に要する時間、攻撃者のスキル、必要なシステム知識、攻撃の機会、攻撃に必要な設備の評価より算出）と、攻撃の影響度（資産への影響、攻撃の強度の評価より算出）の積算により、リスクをスコアリングする。ETSI TS 102 165-1 は、攻撃の頻度×影響度によるシンプルな評価手法であると

言える。

5.6　CVSSの評価手法

CVSS v3.0 は、国際的なセキュリティチームの連合である FIRST(Forum of Incident Response and Security Teams）によって管理される、情報システムの脆弱性に対するオープンで汎用的な評価手法である。ETSI TS 102 165-1 と同様に、システムにおいて発覚した脆弱性のリスクを評価、運用管理者が脆弱性対策の優先順を意思決定するのに活用することを目的とする。基本評価基準として、攻撃元区分、攻撃条件の複雑さ、必要な特権レベル、ユーザ関与レベル、スコープ、機密性（情報漏えい）への影響、完全性（情報改ざん）への影響、可用性（業務停止）への影響を評価し、決められた計算式によって評価値を算出する。上記基本評価基準に加え、現状評価基準、環境評価基準も計算し、総合的にリスクをスコアリングする。CVSS v3.0 は、脆弱性の危険度を詳細に評価可能であると言える。

5.7　分析・評価システムの課題

今回 5.1 節～5.4 節で説明した手法と比較して、ETSI、CVSS の評価手法は、システム構築前でのリスク評価を想定して開発されたものではないため、いくつかのパラメータの評価がシステム構築前では難しい。また、2.3 節で述べたような人命や社会への影響については考慮されない。既存の評価手法を用いる場合は、上記の課題を加味した上で使用する必要がある。既存の手法を使うにしても、組織で蓄積したノウハウを元に独自の手法を使うにしても、ユースケースに応じて使いやすいものを選択するなどの使い分けが必要である。

6 まとめ

6.1 IPA作成の「つながる世界の開発指針」との関係

本書は IPA が先行して公開している「つながる世界の開発指針」を詳細化した内容になっている。「つながる世界の開発指針」の 17 指針と本書の対応に示す。

表 6-1 つながる世界の開発指針と本書の対応

「つながる世界の開発指針」			本書での対応箇所	
大項目		指針	章番号	概要
方針	つながる世界の安全安心に企業として取り組む	指針1 安全安心の基本方針を策定する	4.2.1	製品企画フェーズ項番3:施策として情報セキュリティ方針について記載。
		指針2 安全安心のための体制・人材を見直す	4.2.1	製品企画フェーズ項番3:施策として情報セキュリティ方針について記載。
			4.2.4	運用フェーズ2:施策として組織の体制について記載。
		指針3 内部不正やミスに備える	4.2.2	設計・製造フェーズ項番6:施策として開発時の外部委託における取り組みについて記載。
分析	つながる世界のリスクを認識する	指針4 守るべきものを特定する	2	2章：実施例としてシステム構成を定義し、各ユースケースにおける保護すべき資産をリストアップ。
			4.2.1	製品企画フェーズ項番1,2:施策としてリスク分析について記載。
			5	5章:実施例としてリスク分析の中で保護すべき資産について記載。
		指針5 つながることによるリスクを想定する	2	2章：実施例として各ユースケースにおける被害・影響をリストアップ。
			3.3	3.3:想定されるセキュリティ上のリスク例について記載。
			4.2.1	製品企画フェーズ項番1,2:施策としてリスク分析について記載。
			5	5章:ユースケースにおけるリスク例について記載。
		指針6 つながりで波及するリスクを想定する	(同上)	指針5と同一。
		指針7 物理的なリスクを認識する	4.2.1	製品企画フェーズ項番1,2:施策としてリスク分析について記載。
			4.2.2	設計・製造フェーズ項番5:施策として物理的な攻撃に対する対策について記載。
			5	5章:ユースケースにおける物理的リスク例について記載。
設計	守るべきものを守る設計を考える	指針8 個々でも全体でも守れる設計をする	4.2.2	設計・製造フェーズ項番2,5:施策としてセキュリティ機能の実装について記載。
		指針9 つながる相手に迷惑をかけない設計をする	4.2.2	設計・製造フェーズ項番2:施策として迷惑をかけないための機能について記載。
		指針10 安全安心を実現する設計の整合性をとる	4.2.1	製品企画フェーズ項番1,2:施策として安心安全を実現するための脅威の抽出について記載。
			4.2.2	設計・製造フェーズ項番1,2,3,4,5:施策として抽出した脅威に対する対策について記載。
		指針11 不特定の相手とつなげられても安全安心を確保できる設計をする	4.2.2	設計・製造フェーズ項番3:施策として相手との通信に使用するプロトコルについて記載。
		指針12 安全安心を実現する設計の検証・評価を行う	4.2.3	評価フェーズ1:施策として設計に問題がないかを確認する評価について記載。
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける	4.2.2	設計・製造フェーズ項番2:自装置の状態を記録するためのロギング機能について記載。
		指針14 時間が経っても安全安心を維持する機能を設ける	4.2.2	設計・製造フェーズ項番2:施策としてプログラムアップデート機能実装について記載。
			4.2.4	運用フェーズ項番1:施策としてプログラムのアップデートに関して記載。
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する	4.2.4	運用フェーズ項番1,2:施策として最新の脆弱性への対応と、組織の対応内容について記載。
		指針16 出荷後の関係事業者に守って　もらいたいことを伝える	4.2.4	運用フェーズ項番1,2:施策として出荷後組織がとるべき体制について記載。
			4.2. 5	廃棄フェーズ項番1:施策として廃棄時のリスク表示について記載。
		指針17 つながることによるリスクを一般利用者に知ってもらう	4.2.2	設計・製造フェーズ項番2:施策として取扱説明書へのリスク、脅威の表示について記載。

6.2　まとめ

本書は IoT-GW 分野を対象としたセキュリティガイドラインとして作成したが、想定される脅威やライフサイクルにおけるセキュリティの取組みなど、他の分野でも応用できるところがあると考えられる。様々な製品の開発プロセスにおいてセキュリティ対策を考慮するに当たり、本ガイドラインを積極的に活用して欲しい。

今後は、更なる内容の充実化や、本ガイドラインをベースとした機器の認証・認定制度の確立を図ってゆく。

付録

付録1： 使用するプロトコルと脆弱性、影響のリストアップ例

項番	プロトコル	想定される脅威	想定される脅威の例	想定される影響
1	IPv4	サービス拒否	フラグメントパケットの再構築時にシステムがクラッシュする問題（Teardrop Attack）	データが重複するフラグメントパケットを正常に処理できないというTCP/IP の実装上の問題を保持していた場合、システムのクラッシュやリブート、ハングアップといった事象が発生し、結果としてサービス不能状態に陥る。
2	ICMP	サービス拒否	パケット再構築時にバッファが溢れる問題（Ping of death）	大量にフラグメント化された ICMP を再構築する際にバッファが溢れシステムクラッシュ、リブートなどが起きる。
3	TCP	なりすまし	TCP の初期シーケンス番号予測の問題	送信元を偽造した IP アドレスから受信ホストにパケットを受信、処理を行わせることが可能になる。
4		サービス拒否	SYN パケットにサーバ資源が占有される問題（SYN Flood Attack）	SYN パケットを受信により、TCP 接続を確立するための接続情報を格納するコネクションバックログ等のリソースが枯渇し、新たに接続を受け入れられなくなる。
5	UDP	サービス拒否	UDP ヘッダの長さフィールド不正	不正なパケット処理時にOS、システムをクラッシュするなどの影響がある。
6	HTTP	情報漏えい	コマンド/コード/クエリの注入に基づく攻撃（Attacks Based on Command, Code, or Query Injection）	SQL インジェクションや任意コマンド実行により、情報搾取(個人・組織)が発生する。

7	HTTP	サービス拒否	プロトコルの要素長を利用した攻撃（ Protocol Element Length）	http ヘッダ部のパーサ部脆弱性をつくような長い文字列を送信することで、帯域圧迫等によりサービス不能となる。
8	HTTPS/TLS	なりすまし	証明書と認証の不備	信頼のない CA 局を登録した場合、正規の証明書であることを保証できない。
9		情報漏えい	匿名鍵交換の利用	サーバ、クライアント共に匿名の認証モードを利用する場合、本質的に中間者攻撃を受けやすい。中間者攻撃により情報搾取される。
10		サービス拒否	バージョンロールバック攻撃	SSL2.0 にフォールバックして、ハンドシェイクを開始することで、SSL2.0 の未対処の脆弱性を利用して攻撃する。攻撃の結果、サービス不能となる。
11	CoAP	サービス拒否	プロトコルパーサと URI 処理	複雑なパーサや URI 処理コードの実装不備を攻撃され、リモートノードをクラッシュさせられる。
12		サービス拒否	アンプ攻撃	CoAP サーバは一般的に、要求パケットよりも大きい応答パケットを応答する。大量の要求パケットに対して、増幅された応答パケットにより帯域圧迫によりサービス不能。
13	FTP	改ざん	Anonymous FTP	ファイルアクセス制御が不完全なため、匿名ユーザがすべてのファイルを読んだり、ファイル作成できてしまう。

14	FTP	情報漏えい	不正ログイン	ログイン ID、パスワードをデフォルトのまま放置、パスワード無し、類推されやすいパスワードの利用により不正にログインされる。その結果、ファイルの書き換え、マルウェアの配布、情報漏えい、ボットネット化が行われる。
15		特権昇格	ブルートフォース攻撃	（並行セッションによる）ブルートフォース攻撃によって、特権ユーザのパスワードが特定される。

引用/参考文献

[1] つながる世界の開発指針　～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント～、独立行政法人情報処理推進機構　技術本部　ソフトウェア高信頼化センター

https://www.ipa.go.jp/files/000051411.pdf

[2] ガートナーの調査

http://www.gartner.com/newsroom/id/3165317

[3] ホームルータへの不正な設定変更による偽 DNS サーバの参照

https://sect.iij.ad.jp/d/2012/06/148528.html

[4] ペースメーカへのハッキング事例

https://www.ipa.go.jp/files/000038223.pdf

[5] 情報セキュリティ 10 大脅威

https://www.ipa.go.jp/security/vuln/10threats2016.html

https://www.ipa.go.jp/files/000045039.pdf

https://www.ipa.go.jp/files/000037151.pdf

[6] OWASP Internet of Things Project

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014

[7] IoT のセキュリティリスク Top 10

https://devcentral.f5.com/articles/iot-top-10

[8] ETSI TS 102 165-1: “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis,” V4.2.3 (2011-03).

[9] CVSS v3.0: “Common Vulnerability Scoring System v3.0: Specification Document V1.7.

[10] ISO/IEC TR 13335-3 (GMITS part3): ″Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security.″

[11] アウトソーシングに関する情報セキュリティ対策ガイダンス

http://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf

[12] 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書
http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0303.pdf

[13] NIST Special Publication 800-88 Guidelines for Media Sanitization
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf