製品分野別セキュリティガイドライン
IoT-GW編

平成28年6月8日

CCDS セキュリティガイドラインWG
ホームGW SWG

IoT-GWガイドラインの目次構成

1.現状と課題

１．IoT-GWセキュリティの現状

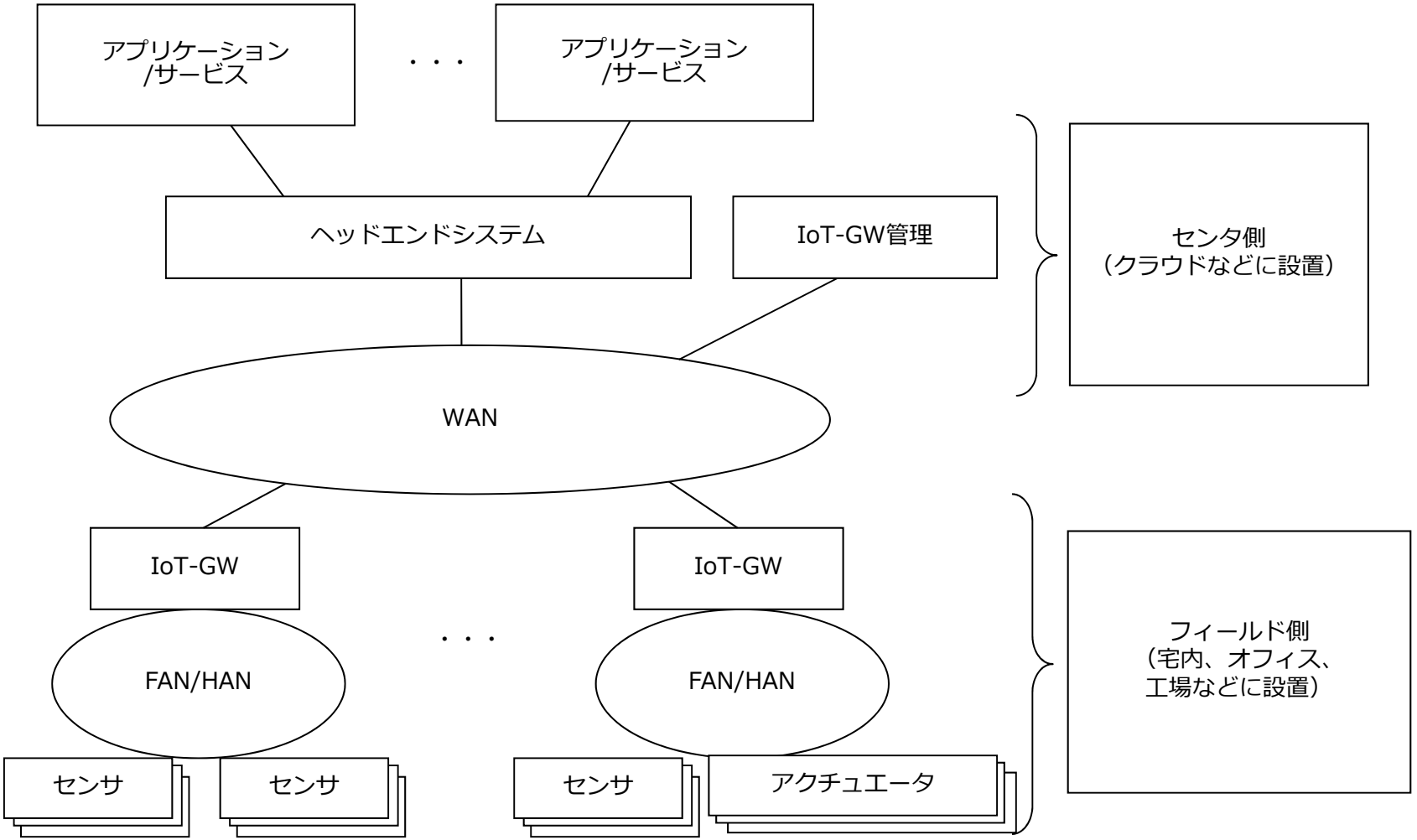
IoT（モノとインターネット）機器は、私たちにより身近なものになり、多種多様な方面で広がりを見せている。家庭内に設置したセンサをスマートフォンと連動させ、例えば遠隔で操作することを可能にすれば、家の施錠や照明、電源をコントロールすることができる。IoT機器は個人や家庭に限ったことではなく、オフィスや市街地での普及も著しく、今後はさらに増加すると想定されている。

２．IoT-GWにおけるセキュリティ対策の必要性

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。現状ではセキュリティのリスクを評価する基準や規格が無いため、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。

2.IoT-GWのシステム構成–その1–

■IoT-GWシステム構成



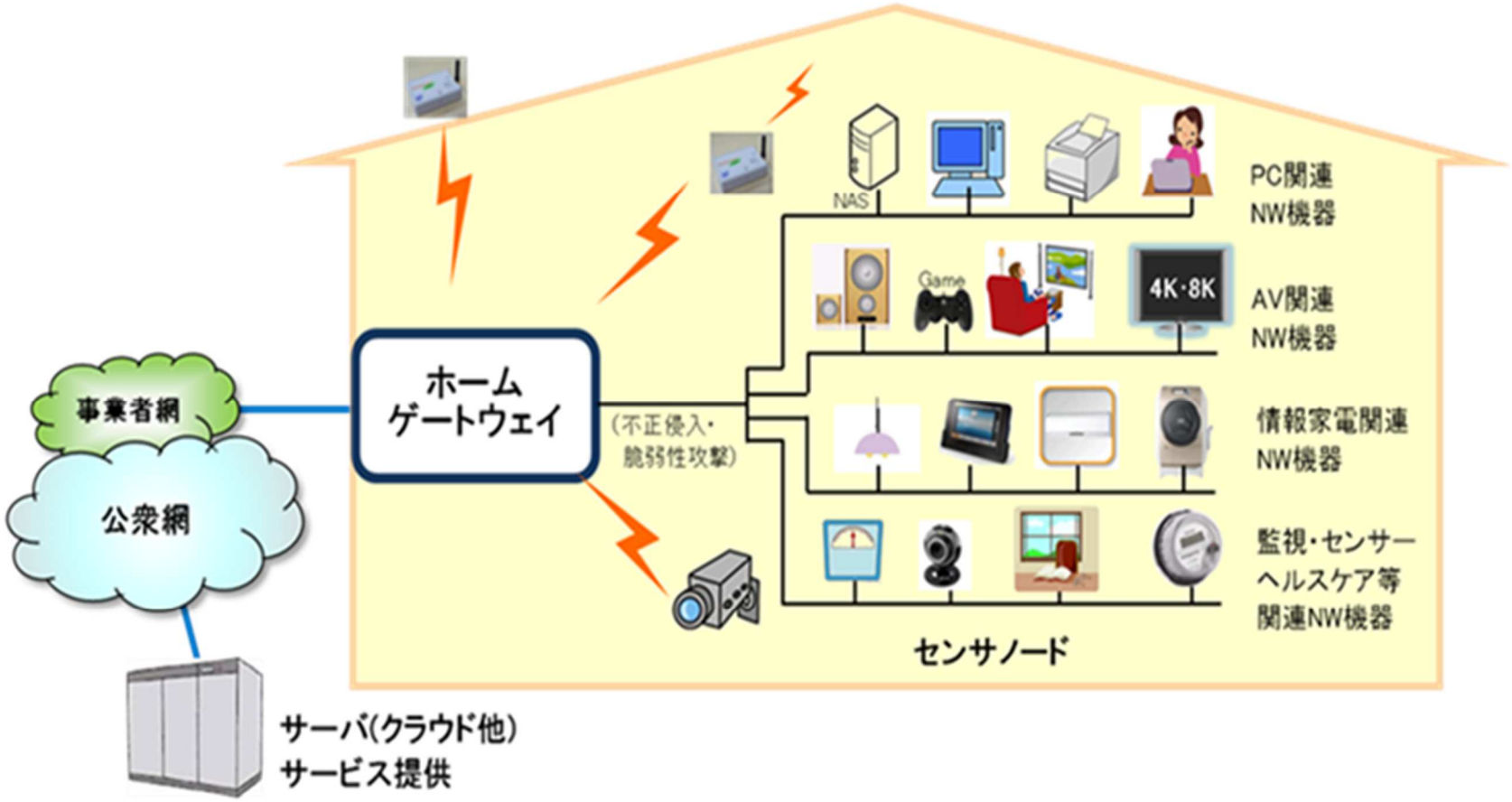
2.IoT-GWのシステム構成–その2–

■IoT-GWシステムの構成要素

項番	構成要素	機能
1	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。
2	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装置の総称である。
3	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。
4	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。
5	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装置群である。
6	IoT-GW管理	IoT-GWの機器認証や運用管理を行うサーバ装置である。
7	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。

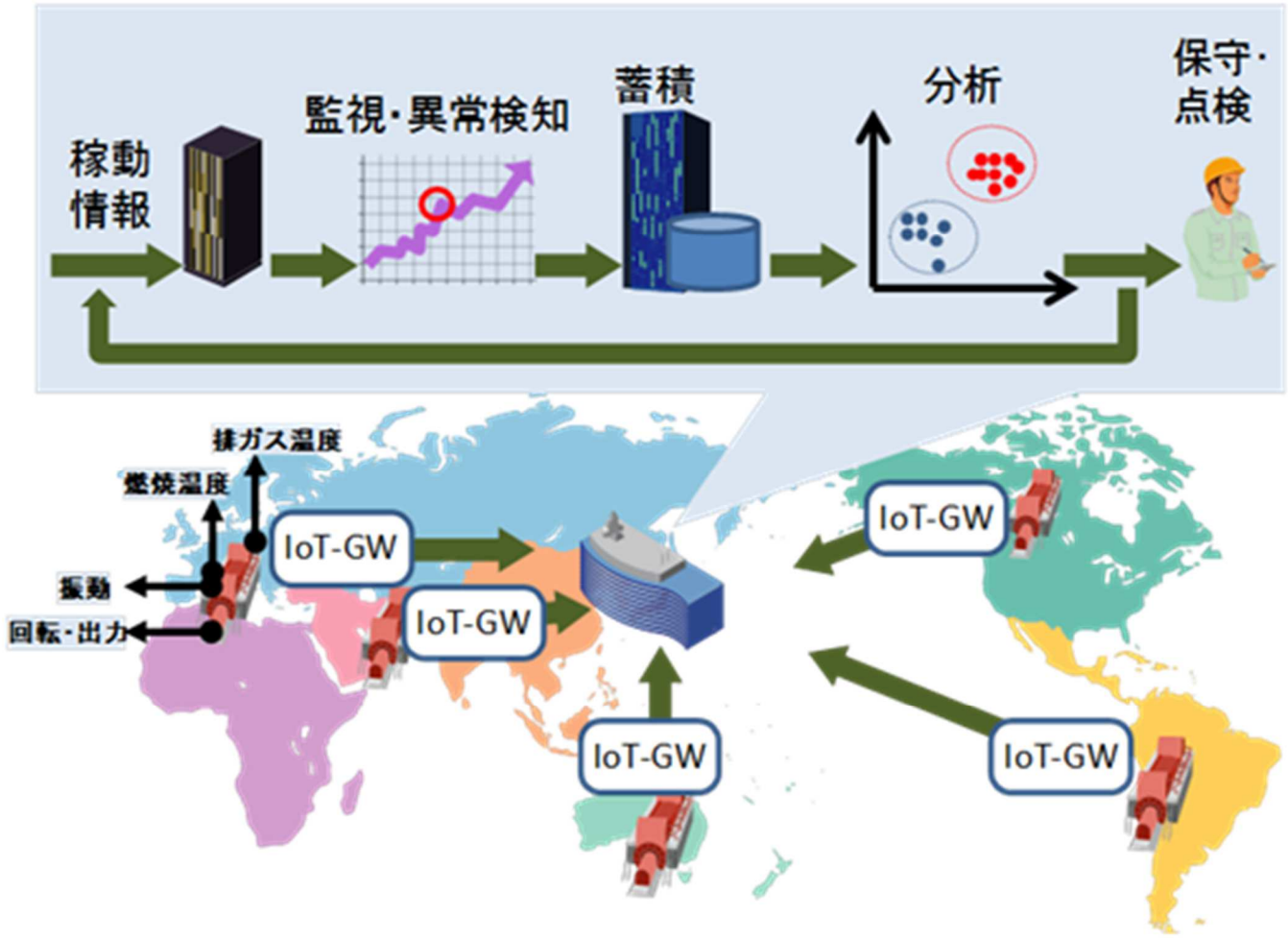
3.IoT-GWのサービスユースケース-その1-

■ホームゲートウェイ



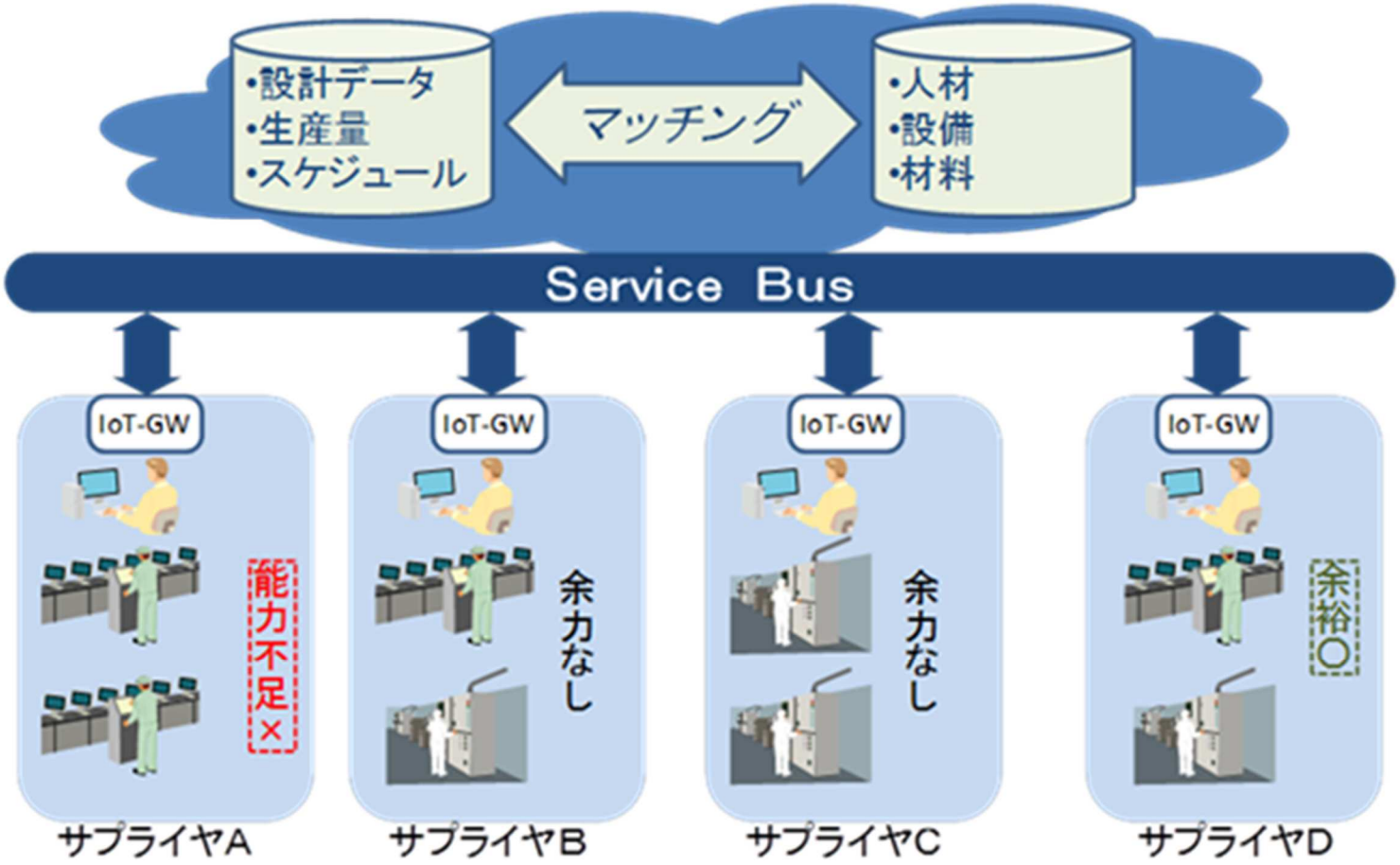
3.IoT-GWのサービスユースケース-その2-

■スマートメンテナンス



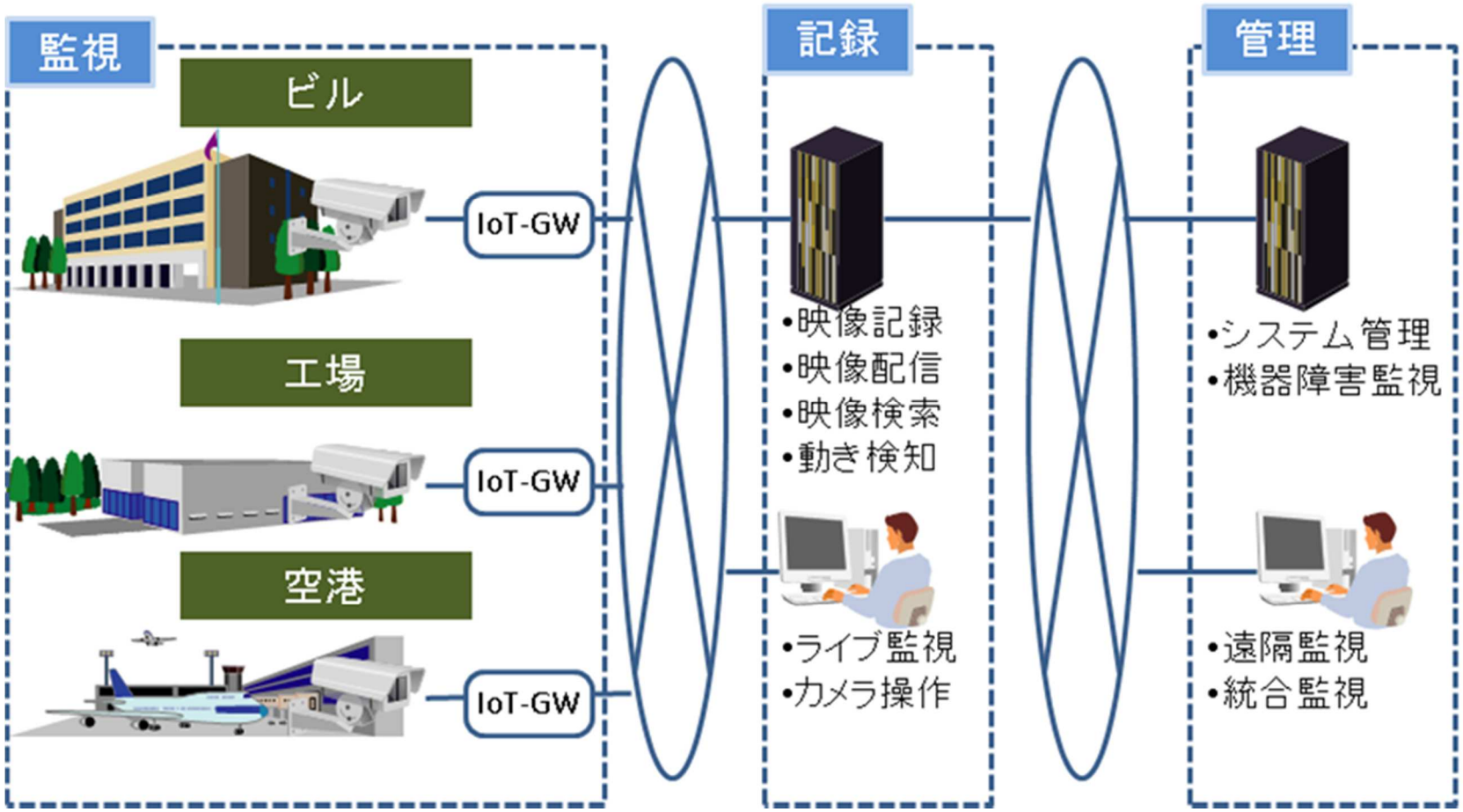
3.IoT-GWのサービスユースケース–その3–

■サプライチェーン管理および生産ライン最適化



3.IoT-GWのサービスユースケース-その4-

■映像監視



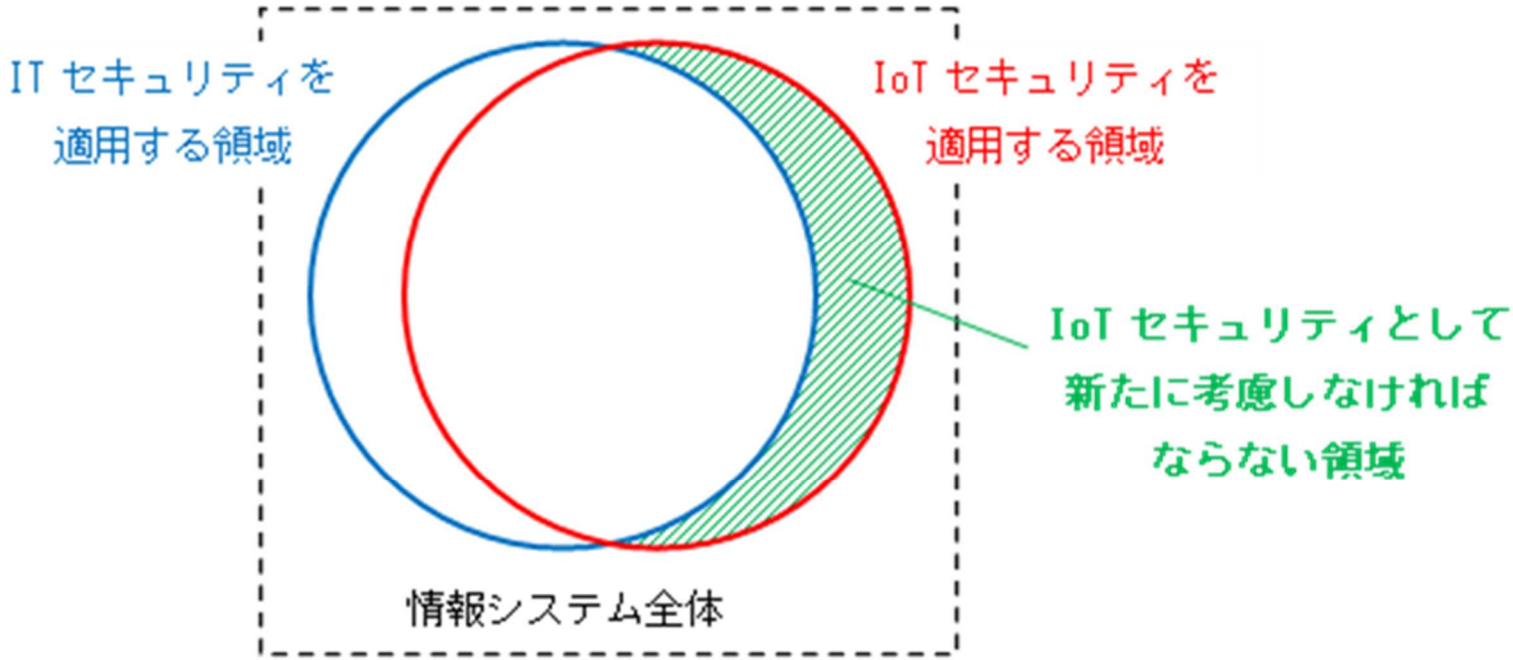
4.保護すべき資産、考慮すべき影響

■保護すべき資産、考慮すべき影響

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 ・停電による人命にかかわる重大被害 ・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 ・カメラののっとり等によるプライバシーの侵害 ・通信の停止

5.IoTセキュリティの適用領域

ITセキュリティとIoTセキュリティで重なり合わない領域 = IoTセキュリティ検討範囲



6.IoT-GW適用システムの特徴と課題

IoT-GW適用システムの特徴と課題	
1	フィールド側にガバナンスが無く、機器・端末に対する脅威が大きい。
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。
3	フィールド側にアクチュエータが接続されている。
4	長期使用を前提としたシステムでは更新が難しい。
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。

7. IoT-GW適用システムで想定される脅威

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	
1	センサの停止により、データ取得が不可能となる。
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。
3	センサが乗っ取られることにより、DoS攻撃へ加担する。
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。
5	ネットワークからエンドポイント機器が攻撃される。
6	攻撃者がFAN/HANへ物理的に侵入して攻撃する。
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。
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。
9	誤データが注入され、伝搬される。
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。

8.製品ライフサイクルのフェーズ

■製品ライフサイクルにおける５つのフェーズ

フェーズ	説明
製品企画フェーズ	製品のコンセプト、予算、要件定義の策定を行う。
設計・製造フェーズ	企画フェーズの要件定義を受けて設計・実装・製造を行う。
評価フェーズ	製造された製品の正当性の評価を行う。
運用フェーズ	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。
廃棄フェーズ	所有者が廃棄手続きを行う。

9.各フェーズの取組み–その1–

各フェーズにおけるセキュリティの取組みを以下に示す。

■製品企画フェーズ

	項目	内容
1	保護すべき資産及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。 ポイントとしては装置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、前章で述べた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「 保護すべき資産及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、開発する装置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

9.各フェーズの取組み–その2–

■製品企画フェーズ（続き）

	項目	内容
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

9.各フェーズの取組み–その3–

■設計・製造フェーズ

	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、装置にセキュリティ要件を担保するための機能を実装する。 製品企画フェーズの項番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

9.各フェーズの取組み–その4–

■設計・製造フェーズ（続き）

	項目	内容
	セキュリティ機能の実装（続き）	(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 (4) アラート機能（攻撃を受けた、不正侵入を受けた等） • 攻撃を受けたことのユーザ通知 • 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 • 装置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装置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の区別 • 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

9.各フェーズの取組み–その5–

■設計・製造フェーズ（続き）

	項目	内容
	セキュリティ機能の実装（続き）	・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
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のセキュリティ実装の活用 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。

9.各フェーズの取組み–その6–

■設計・製造フェーズ（続き）

	項目	内容
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） • 装置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。

9.各フェーズの取組み–その7–

■設計・製造フェーズ（続き）

	項目	内容
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。 (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

9.各フェーズの取組み–その8–

■設計・製造フェーズ（続き）

	項目	内容
	開発の外部委託における取組み （続き）	• 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。

9.各フェーズの取組み–その9–

■評価フェーズ

	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こまれてしまう。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。 「11. 脆弱性検証ツール一覧」にOSSとして提供されているツールの一部を記載する。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。 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。

9.各フェーズの取組み–その10–

■運用フェーズ

	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 Vulnerabilitied 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しかけ仕掛構築

■廃棄フェーズ

	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

11.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。

12. リスク分析・評価–その1–

■ISO/IEC TR 13335-3によるリスク分析の流れ

ユースケースの定義

分析対象のシステム構成とシステムの登場人物を定義

保護すべき資産と基準値の定義

保護すべき資産を定義し、保護すべき資産の基準値レベルを定義

想定脅威と発生頻度の定義

想定する脅威とその脅威の発生頻度を定義

想定インシデントとリスク値の定義

保護すべき資産の重要度レベル、想定インシデント発生頻度、
インシデントと引き起こされる損失を抽出しリスク値を定義

12. リスク分析・評価–その2–

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

ETSIの評価手法

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。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

CVSSの評価手法

■分析・評価システムの課題

・ISO/IEC TR 13335-3と比較し、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。
・同様に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。

12. まとめ

■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。

付録

■使用するプロトコルと脆弱性、影響のリストアップ例－その1－

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。

付録

■使用するプロトコルと脆弱性、影響のリストアップ例－その2－

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
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。