IoT 機器セキュリティ実装ガイドライン

ソフトウェア更新機能

第 1.0 版

一般社団法人 重要生活機器連携セキュリティ協議会

2020 年 12 月 1 日

要旨

本文書は、IoT（Internet of Things）機器における「ソフトウェア更新」機能の実装のためのガイドラインである。日本国内では 2020 年 4 月 1 日より「IoT 技適」が施行され、インターネットに直接つながる WEB カメラなどの一部の IoT 機器において「ソフトウェア更新」が認定を取得するための必須機能となっている。しかし、「ソフトウェア更新」の具体的な実装方法については明示されていないため、製造者にとって適切なセキュリティ要件の検討が難しい状況にある。本文書は、「ソフトウェア更新」の実装に具体的なセキュリティ要件を提示し、製造者がセキュアな IoT 機器を設計するうえでの指針となることを目標としている。

「ソフトウェア更新」機能は IoT 機器単体で完結する機能ではなく更新ファイルを提供するという「サービス」の面も含んでいるため、本文書は IoT 機器本体の実装だけでなく、IoT 機器の外部システム（更新ファイルを配信するためのサーバやネットワーク、更新ファイルの作成環境など）も含めた包括的な実装ガイドラインとなっている（ただし、あくまで IoT 機器の製造者が責任をもつ範囲にのみスコープを限定）。

本文書は、大きく分けて以下の 3 項目により構成される。

(1) 「ソフトウェア更新」の仕組みと脅威を分析するためのモデル定義とリスク分析

「ソフトウェア更新」機能のみの簡潔なモデルを定義し、システム構成、更新検証アーキテクチャ、ライフサイクル、アクターの相関、処理フローなどを図で示しながら「ソフトウェア更新」の仕組みを解説する。その後、定義したモデルに基づいて実施したリスク分析の結果を提示する。

(2) 安全な「ソフトウェア更新」を提供するためのセキュリティ要件

前記のモデル定義とリスク分析を踏まえて検討された、「ソフトウェア更新」を安全に実装するためのセキュリティ要件を提示する。各セキュリティ要件は、指標として下記の３段階にレベル分けされており、製造者が IoT 機器のユースケースに応じて必要なセキュリティ要件を選択できるよう意図されている。

［ A ］　ユースケースによらず必要となる可能性が高い要件

［ B ］　ユースケースによっては必要となり得る要件

［ C ］　より高度なセキュリティが要求される場合には追加で検討すべき要件

(3) 「ソフトウェア更新」を顧客が安全に運用するための情報提供

顧客が「ソフトウェア更新」を安全に運用するためには、製造者は前記のセキュリティ要件を満たすだけでは十分ではない。製造者は、IoT 機器のセキュリティ性能や更新サービスの提供条件など、必要な情報を顧客へ確実に提供する必要がある。「ソフトウェア更新」に関する顧客とのコミュニケーションについて製造者が検討すべき事項を一覧として提示する。

本文書の作成は、最新の国際標準に即したものとするため、米国の IoT 機器製造者向けのセキュリティ勧告である NIST.IR.8259 をベースとした（ただし、「ソフトウェア更新」という限定的な共通機能にのみ焦点を当てているため、NIST.IR.8259 全体をカバーするものではない）。また「ソフトウェア更新」に関係する業界のガイドラインなども参考にしている。国内の代表的なガイドラインについても、経済産業省が策定した CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）や IPA（独立行政法人 情報処理推進機構）が策定した「つながる世界の開発指針」を参考にしている。

また、本文書は IoT 機器単体の「ソフトウェア更新」機能にのみ焦点を当てているが、より広範な IoT システムのセキュリティ要件の検討にも役立つ内容となっている。これは「ソフトウェア更新」の仕組み自体に、外部のエンティティ（人・機器・データ）や機器内のソフトウェアなど、ほとんどのシステム要素に対する認証が含まれているためである。製造者ではなく顧客として、IoT システムを保護するためのセキュアな IoT 機器の調達を検討している場合、本文書を部分的な調達要件として参照することも可能である。

なお、本文書の利用に際しては、製造者自身が本文書の内容を製造者の提供する IoT 機器のユースケースに当てはめて修正・拡張する検討が必須であることに注意されたし。

※本文書はあくまで推奨事項をまとめたガイドラインであり、本文書への準拠に起因した如何なる損害も保障されない。

改訂履歴

版数	改訂日	改訂内容
第 1.0 版	2020/12/1	初版

目次

1. 導入

1.1 背景

本文書において IoT（Internet of Things）機器とは、物理世界と相互作用（アクチュエータまたはセンサー）をもち、インターネットに接続される機器のことを指す。IoT 機器の利用により、大規模または広範囲のシステムにおける効率的な制御・監視・管理などのサービスが実現可能となる。現在、様々な分野におけるシステム効率化のため IoT 機器の利用が拡大している（スマートシティ、スマート工場、スマートホームなど）。しかし、IoT 機器はインターネットに常時つながる性質により様々なサイバーセキュリティの脅威に晒されているのに反して、従来の PC 等に比べてセキュリティ性能が低く制限されている機器が多く、セキュリティの管理が困難であるという課題がある。近年、セキュリティの脆弱な IoT 機器が攻撃者に乗っ取られることにより、大規模な DDoS（Distributed Denial of Service）攻撃や、物理世界の工場施設で事故を起こす事件などが多発しており、深刻な社会問題となっている。

上記のような脅威を防ぐためには、IoT 機器の脆弱性を放置せず、適切な修正パッチをすぐに適用してセキュアな状態を維持できる仕組み（ソフトウェア更新）が必須となる。 このため、日本国内では「IoT 技適」（『端末設備等規則及び電気通信主任技術者規則の一部を改正する省令（平成 31 年総務省令第 12 号）』 端末設備等規則 第三十四条の十）が 2020 年 4 月 1 日より施行され、インターネットに直接つながる WEB カメラなどの一部の IoT 機器において「ソフトウェア更新」が認定を取得するための必須機能となっている。しかし、「ソフトウェア更新」の具体的な実装方法については明示されていないため、製造者にとって適切なセキュリティ要件の検討が難しい状況にある。

1.2 目標とスコープ

本文書は、「ソフトウェア更新」の実装に対して具体的なセキュリティ要件を提示し、製造者がセキュアな IoT 機器を設計するための指針となることを目標としている。

「ソフトウェア更新」機能は IoT 機器単体で完結する機能ではなく、更新ファイルの配信という「サービス」の面も含んでいるため、本文書では IoT 機器本体の実装だけでなく、IoT 機器の外部システム（更新ファイルを配信するためのサーバ、更新ファイルの作成環境など）も含めた包括的な実装ガイドラインとなっている（ただし、あくまで IoT 機器の製造者が責任をもつ範囲にのみスコープを限定）。

本文書では「ソフトウェア更新」も含めた IoT 機器の基本的セキュリティ機能の実装を対象としており、各 IoT 機器の本質的価値である物理世界との相互作用（センサまたはアクチュエータ）に関する機能については IoT 機器ごとに異なるためスコープ外としている。また、実行中のソフトウェアの信頼性を担保する機能である「セキュアブート」については、「ソフトウェア更新」と関係をもつ重要な技術ではあるが複雑なため、本文書では実装の詳細については触れず紹介の範囲に留めている。

また、本文書は IoT 機器単体の「ソフトウェア更新」機能にのみ焦点を当てているが、より広範な IoT システムのセキュリティ要件の検討にも役立つ内容となっている。これは「ソフトウェア更新」の仕組み自体に、外部のエンティティ（人・機器・データ）や機器内のソフトウェアなど、ほとんどのシステム要素に対する認証が含まれているためである。製造者ではなく顧客として、IoT システムを保護するためのセキュアな IoT 機器の調達を検討している場合、本文書を部分的な調達要件として参照することも可能である。

1.3 文書の構成

本文書は、大きく分けて以下の 3 つの項目により構成される。

(1) 「ソフトウェア更新」の仕組みと脅威を分析するためのモデル定義とリスク分析（2 章）

「ソフトウェア更新」機能のみの簡潔なモデルを定義し、システム構成、更新検証アーキテクチャ、ライフサイクル、アクターの相関、処理フローなどを図で示しながら「ソフトウェア更新」の仕組みを解説する。その後、定義したモデルに基づいて実施したリスク分析の結果を提示する。

(2) 安全な「ソフトウェア更新」を提供するためのセキュリティ要件（3 章）

前記のモデル定義とリスク分析を踏まえて検討された、「ソフトウェア更新」を安全に実装するためのセキュリティ要件を提示する。各セキュリティ要件は、指標として下記の３段階にレベル分けされており、製造者が IoT 機器のユースケースに応じて必要なセキュリティ要件を選択できるよう意図されている。

［ A ］　ユースケースによらず必要となる可能性が高い要件

［ B ］　ユースケースによっては必要となり得る要件

［ C ］　より高度なセキュリティが要求される場合には追加で検討すべき要件

(3) 「ソフトウェア更新」を顧客が安全に運用するための情報提供（4 章）

顧客が「ソフトウェア更新」を安全に運用するためには、製造者は前記のセキュリティ要件を満たすだけでは十分ではない。製造者は、IoT 機器のセキュリティ性能や更新サービスの提供条件など、必要な情報を顧客へ確実に提供する必要がある。「ソフトウェア更新」に関する顧客とのコミュニケーションについて製造者が検討すべき事項を一覧として提示する。

また、日本の IoT に関する代表的なガイドラインである CPSF への準拠を確認した結果も付録として添付している（付録 B）。

1.4 参考文献の紹介

本文書の作成は、最新の国際標準に即したものとするため、米国の IoT 機器製造者向けのセキュリティ勧告である NIST.IR.8259 をベースとした（ただし、「ソフトウェア更新」という限られた機能にのみ焦点を当てているため、NIST.IR.8259 全体をカバーするものではない）。また「ソフトウェア更新」に関係する業界のガイドラインなども参考にしている。国内の代表的なガイドラインについても、経済産業省が策定した CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）や IPA（独立行政法人 情報処理推進機構）が策定した「つながる世界の開発指針」を参考にしている。

以下、本文書の作成において参考にした文献を簡単に紹介する。

(1) NIST.IR.8259：「IoT 機器製造者の基盤的サイバーセキュリティ活動」

IoT 機器の製造者が実施すべきサイバーセキュリティの検討活動を以下の６種に分けて提示した NIST（米国標準技術研究所）の勧告。

① 想定顧客の特定と、想定ユースケースの定義

② サイバーセキュリティに関する顧客の需要と目標の調査

③ 顧客の需要と目標への対処方法の決定

④ 顧客の需要と目標への十分なサポートの計画

⑤ 顧客とのコミュニケーションへの取り組みの定義

⑥ 顧客とのコミュニケーション内容と伝達方法の決定

米議会が 2019 年に立法した「IoT Cybersecurity Improvement Act of 2019」において NIST に発行が命じられた「IoT 機器の最小要件」に相当し、米国の IoT セキュリティ標準のベースとなる文書である。今後、行政管理予算局（OMB）がこの勧告に基づいて各政府機関のガイドライン作成と定期レビューを担当し、連邦政府が調達する IoT 機器はこれらの文書（勧告とガイドライン）への準拠が要求される。

(2) NIST.IR.8259A：「IoT 機器サイバーセキュリティ性能のコアベースライン」

NIST.IR.8259 の別紙。IoT 機器に共通のサイバーセキュリティ性能を要件一覧として提示している（必須要件とはしていない）。ENISA(European Network and Information Security Agency)、GSMA(GSM Association)、IEC(International Electrotechnical Commission)など、他の標準化団体の IoT セキュリティ要件へのマッピングも提示されている。

(3) NIST.IR.8228：「IoT のサイバーセキュリティとプライバシーの管理に関する検討」

従来の IT 機器とは異なる IoT 機器特有のサイバーセキュリティとプライバシーのリスクについて周知するための文書。NIST の IoT 関連文書の基盤として位置づけられており、NIST.IR.8259 からも参照されている。

(4) NIST.IR.8267：「スマートホーム IoT 製品に対するセキュリティレビュー」

市場に流通しているスマートホーム IoT 機器のセキュリティ性能に関する NIST の調査レポート（現在、ドラフトの段階）。IoT 機器の製造者がセキュリティ向上に役立てられるような一般的な考察やプラクティス、改善案などを提示。

(5) NIST.SP.800-193：「プラットフォームファームウェアの弾力性ガイドライン」

リモート攻撃に対するプラットフォームの弾力性を実現するため、構成デバイスにおける保護・検知・復旧の仕組みと指針を示す NIST の技術文書。TPM（Trusted Platform Module）を搭載した PC などがメインのスコープであり、IoT 機器は直接の対象ではないが、「ソフトウェア更新」に関連する内容である RoT（信頼性の基盤）やファームウェア更新の仕組みについて説明されている。

(6) “TCG Guidance for Secure Update of Software and Firmware on Embedded Systems”

TPM 仕様を策定している標準化団体 TCG（Trusted Computing Group）が作成。組み込み機器におけるセキュアなソフトウェアとファームウェアの更新の実装に関するガイド資料。更新ファイルのライフサイクルや、更新エンジンを保護する仕組みなど、「ソフトウェア更新」に関する詳細な要件が提示されている。

(7) IETF draft-ietf-suit-architecture-11：「IoT のためのファームウェア更新アーキテクチャ」

インターネット技術の標準化団体 IETF（Internet Engineering Task Force）が作成。IoT 機器におけるファームウェア更新に関するガイドライン（現在、ドラフトの段階）。ファームウェアの更新を中心に検討されており、更新ファイルのファイル形式やブートローダに関する詳細な要件が提示されている。また、更新処理における更新ポリシーなどのメタデータを更新ファイルに添付するためのデータ形式を「Manifest」として提案している。

(8) CPSF：「サイバー・フィジカル・セキュリティ対策フレームワーク」

IoT により実現される「Society5.0」や「Connected Industries」における新たなサプライチェーン（バリュークリエイションプロセス）全体のセキュリティ確保を目的として、産業全体に求められるセキュリティ対策の全体像を整理したフレームワーク。経済産業省により策定された。

(9) 「つながる世界の開発指針」

IoT 製品の開発者が開発時に考慮すべきリスクと対策を 17 の指針としてまとめた開発ガイドライン。IPA（情報処理推進機構）により策定された。

※本文書の利用にあたっては、上記の文献についても適宜参照することを推奨。

1.5 用語一覧

本文書で使用される用語と定義の一覧を、表 1 に示す。

表 1　用語と定義　(50 音/アルファベット順)

用語	定義
HSM	Hardware Security Module。主にサーバにおける暗号鍵の生成・保管、暗号演算などに利用されるハードウェア。PC サーバや拡張ボードなどの形態で提供される。
IoT 機器	物理世界と相互作用（アクチュエータまたはセンサー）をもち、インターネットに接続される機器。例：WEB カメラ、ドローン、産業用ロボット、スマートスピーカーなど。
OS	Operating System。ハードウェアを抽象化し、共通 API を提供することで汎用のアプリケーション・サービスの作成・提供を可能にするソフトウェア。
RoT	Root of Trust。機器を構成するハードウェアとソフトウェアの正当性を検証する際に信頼性の基盤となる構成要素。IoT 機器に要求されるセキュリティレベルに応じて RoT の機能要件は変化する（保存、計測、検証、報告など）。
SE	Secure Element。主に決済・交通系の IC カードや携帯 SIM などに利用されている耐タンパー性セキュアコンポーネント。GlobalPlatform、GSMA、ETSI、Eurosmart などの標準化団体が仕様を策定している。
TEE	Trusted Execution Environment。主にスマホ用 CPU などに実装されている論理的に隔離されたセキュアな実行環境領域。論理的なセキュアコンポーネントだが、耐タンパー性はもたない。GlobalPlatform が仕様を策定（ARM 仕様 TrustZone が元になっている）。
TPM	Trusted Platform Module。主に PC・サーバなどで BIOS や OS の保護（セキュアブート）に利用されている耐タンパー性セキュアコンポーネント。TCG が仕様を策定している。
アップデート	更新ファイル、または更新処理を指す。可読性のため、本文書では漢字が連続して読みづらい一部の文章でのみ使用。

用語	定義
インストール	ソフトウェアのプログラムや設定が保存されている機器内のデータ領域に対して更新イメージのデータを上書きし、ソフトウェアの動作を変更する処理。
管理者	機器の管理に責任をもつ担当者。顧客自身か、または顧客によって委任される。
権限エンティティ	機器の機能にアクセスする権限を認可されたエンティティ（人、機器、サービス、アプリケーションなど）。
攻撃者	ソフトウェア更新システムの脆弱性を利用して IoT 機器の改ざん・乗っ取りなどを実行し、他のアクターの利益を損なうことを企図するアクター。
更新イメージ	更新ファイルから復号・展開された平文状態のインストール用データ。ソフトウェアまたはファームウェアなどのメモリ領域に上書きされることでソフトウェア更新が達成される。
更新エンジン	更新処理に必要なプログラム群を備え、更新処理全体を担当するソフトウェア。「ソフトウェア更新」のセキュリティ向上のため、コンパクトかつセキュアに設計されることが望ましい。
更新処理	機器内で実行されるソフトウェア更新の処理。更新ファイルの検証、復号、インストール、インストール結果の検証などが含まれる。
更新ファイル	ソフトウェア更新に利用するため、サーバやネットワークを通して配信されるデータ。機密性や完全性を保証するため、データ形式にはハッシュまたは署名付きの暗号化などが利用される。更新ファイルのインストールは、ハッシュまたは署名の検証ののち、更新イメージへの復号・展開を経由して実行される。
更新ファイルサーバ	製造者からアップロードされた更新ファイルを保管・配信するサーバ。
顧客	機器の購入者。
自動更新	機器が自動でソフトウェア更新を実行する機能。
セキュアコンポーネント	機器の機密情報の保存・管理や暗号演算などの機能をもつセキュアな構成要素（SE、TEE、TPM など）。セキュリティ領域の保護に利用され、RoT の役割を担うために必要なセキュリティ機能をもつ。
セキュアブート	ソフトウェアの正当性を保証するためセキュアに設計された起動プロセス。ソフトウェア／ファームウェアの読み込み時に実行される処理の内容によって、計測ブート（ハッシュの記録のみ）、検証ブート（ハッシュや署名の検証、実行の可否判断）などに分類される。
セキュリティ領域	クリティカルなコードや鍵などの保護されるべきデータが保存される領域。
ソフトウェア	機器を構成する要素のうち、論理的な構成要素（ハードウェアの動作や演算処理を定義するプログラムデータ）を指す概念。ハードウェアの対義語。
ソフトウェア更新	機器を構成しているソフトウェアの更新機能。本文書では、IoT 機器が外部の更新ファイルサーバから更新ファイルをダウンロードしてメモリに格納し、更新ファイルのインストールを実施する機能を指す。更新ファイルの検証によるインストール可否の判断や、インストール結果の検証とその報告などの処理も含む。
耐タンパー性	外部からの物理的な手段による攻撃に対し、ハードウェアが耐性をもっている状態。たとえば内部メモリへの直接アクセス、電磁波などを計測して解析するサイドチャネル攻撃、外乱注入による出力の変化を解析するフォールト攻撃などの攻撃に対する防衛策がハードウェアに実装されている状態を意味する。
ハードウェア	機器を構成する要素のうち、物理的な構成要素（機械、装置、設備など）を指す概念。ソフトウェアの対義語。
ファースト更新エンジン	「ソフトウェア更新」において最初に実行される更新エンジン。大規模なソフトウェアの更新などで複数の更新エンジンが存在する場合を想定した概念。

用語	定義
ファームウェア	ソフトウェアの一種。OS の下で動作し、機器のハードウェア機能を直接制御するソフトウェア。機器の起動時には、ブートローダにより OS よりも先にロードされる。
ブートローダ	機器の起動時に最初に実行され、ファームウェアをロードするソフトウェア。
報告エンジン	IoT 機器にインストールされているソフトウェアの正当性検証結果を外部エンティティに報告するための機能を備えたソフトウェア。更新エンジンと同様、コンパクトかつセキュアに設計されることが望ましい。
ロールバック	ソフトウェア更新に問題が生じた場合などに、ソフトウェアを以前の状態に戻す機能。

2.　モデル定義とリスク分析

本章では、「ソフトウェア更新」機能のみに絞った簡潔なモデルを定義する。システム構成、更新検証アーキテクチャ、ライフサイクル、アクターの相関、処理フローなどを図で示しながら、「ソフトウェア更新」の一般的な仕組みを解説していく。その後、定義したモデルを対象にリスク分析を実施した結果を提示する。

2.1　システム構成

IoT 機器の「ソフトウェア更新」に関係する要素のみを抽象化したモデルを定義した。本文書における「ソフトウェア更新」システムの構成を以下の図 1 に示す。なお、図 1 において赤点線で示した「製造者の責任範囲」は本文書のスコープを示すものではないことに注意されたし（「ソフトウェア更新」機能を実装する IoT 機器のセキュリティが本文書のスコープ）。

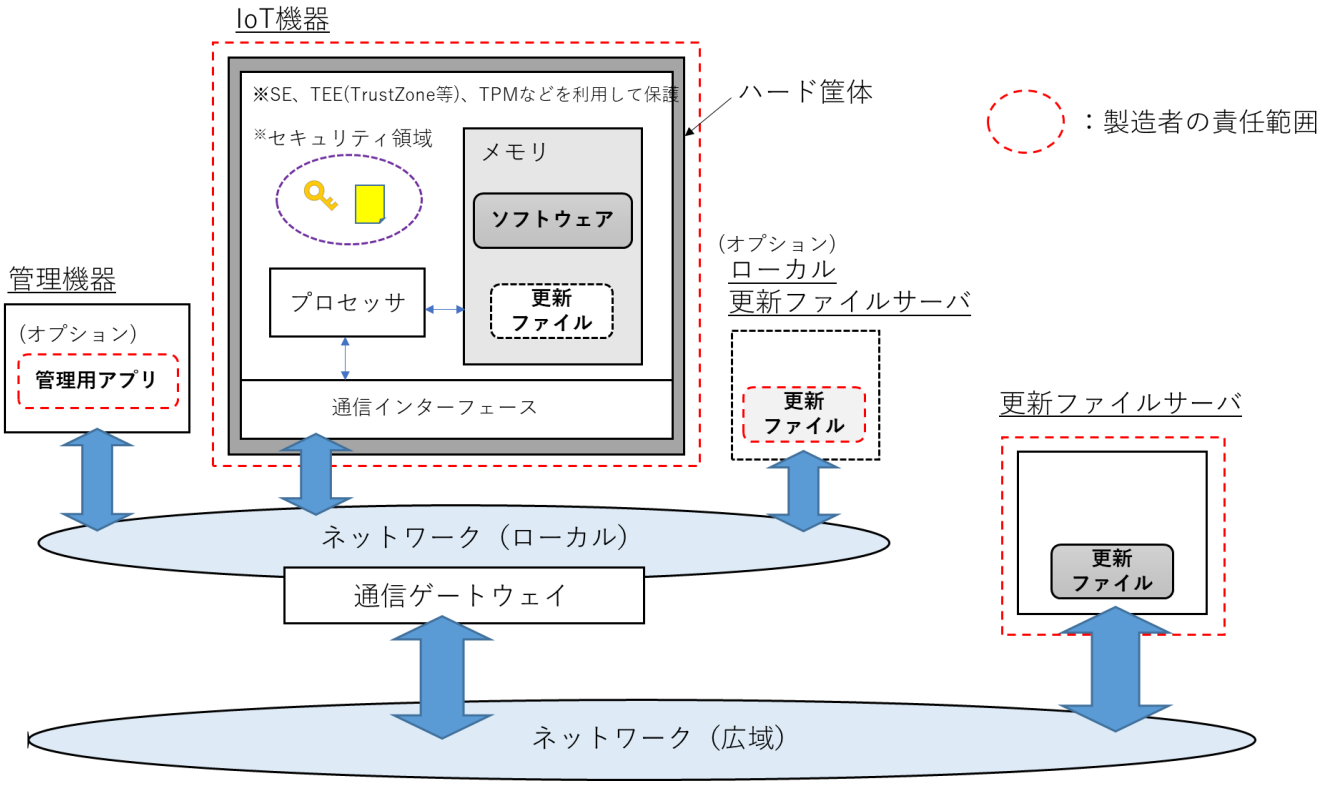

図 1　システム構成図

システム構成の各要素の説明を以下に記述する。

(1)　IoT 機器

ハード筐体、通信インターフェース、プロセッサ、メモリ、セキュリティ領域をもつ。外部の更新ファイルサーバから更新ファイルをダウンロードしてメモリに保存したのち、更新ファイルのインストールを実施する。

(2) メモリ

「ソフトウェア更新」の対象となるソフトウェアとファームウェア、ダウンロードされた更新ファイル、更新ファイルから復号・展開された更新イメージなどが保存される記憶装置。記憶装置の構成は機器によって多用なバリエーションが存在するため、本文書においては集約された単一の抽象的メモリとして表現する。

(3) セキュリティ領域

「ソフトウェア更新」に必要な鍵や証明書など、保護されるべきデータが保存される領域。IoT 機器の実装によってはセキュリティ領域がメモリ上に存在する場合もあるが、攻撃者による不正なアクセスから保護するためには、セキュリティ領域が通常のデータ領域から論理的または物理的に隔離された設計・実装が必要となる。このため、セキュリティ領域を保護する手段として、セキュアコンポーネント（SE、TEE、TPM など）を利用する場合がある。

(4) プロセッサ

メモリとセキュリティ領域にアクセスし、更新ファイルの検証、更新ファイルのインストール、インストール結果の検証などを実行するメインの処理装置。

(5) ハード筐体

IoT 機器を構成する回路基板などのハードウェア部品を固定し、保護する筐体。IoT 機器が設置される環境の脅威に応じた適切な保護性能が求められる（防塵、防水、攻撃者による開封検知や持ち去りの防止ロックなど）。

(6) 更新ファイルサーバ

製造者によりアップロードされた更新ファイルを保持し、IoT 機器からのダウンロード要求に応じて更新ファイルを配信するサーバ。「ソフトウェア更新」サービスを安定的に提供するため、製造者は更新ファイルサーバの運用に責任をもつ。ただし、運用の業務を外部のサービス事業者に委託することは可能（コストとセキュリティを検討した場合、自前でのファイルサーバの立ち上げ・運用の代わりに既存のサービス事業者を利用することは有力な選択肢になり得る）。IoT 機器の管理ポリシーによっては、更新ファイルはローカル更新ファイルサーバを経由して間接的に配信される場合がある。ただし、ローカル更新ファイルサーバは IoT 機器の管理者によって運用されるため、製造者の責任範囲には含まれない。

(7) ネットワーク（ローカル）

IoT 機器が直接接続するネットワーク（LAN）。IoT 機器が直接に WAN またはインターネットに接続している場合には、ネットワーク（広域）と同一の場合もある。

(8) ネットワーク（広域）

更新ファイルサーバが接続する広域のネットワーク（WAN またはインターネット）。

(9) 通信インターフェース

IoT 機器が外部の機器と通信するためのインターフェース。

(10) 通信ゲートウェイ

ネットワーク（ローカル）とネットワーク（広域）間の通信を制御する装置（LAN ルータなど）。IoT 機器の処理性能が低いユースケース（センサネットワークなど）では、接続する IoT 機器の「ソフトウェア更新」処理の一部（暗号演算、データバックアップなど）を通信ゲートウェイが担当する場合がある。

(11) 管理機器

IoT 機器の「ソフトウェア更新」を設定・管理するための機器（PC、スマホ、タブレットなど）。図 1 ではネットワーク（ローカル）に接続しているが、ネットワーク（広域）から接続して管理する場合や、通信ゲートウェイを通さずに IoT 機器と直接通信（Wi-Fi、Bluetooth など）で接続して管理する場合もあり得る。管理機器で使用する管理用アプリケーションなどのソフトウェアを製造者が提供する場合、このソフトウェアは製造者の責任範囲となる。また、IoT 機器の管理者ではなく製造者が各 IoT 機器の「ソフトウェア更新」を中央管理する場合、管理機器の運用も製造者の責任範囲となる。

2.2 更新検証アーキテクチャ

「ソフトウェア更新」の正当性を保証するために必要な IoT 機器内部の検証機能のアーキテクチャを以下の図 2 に示す。

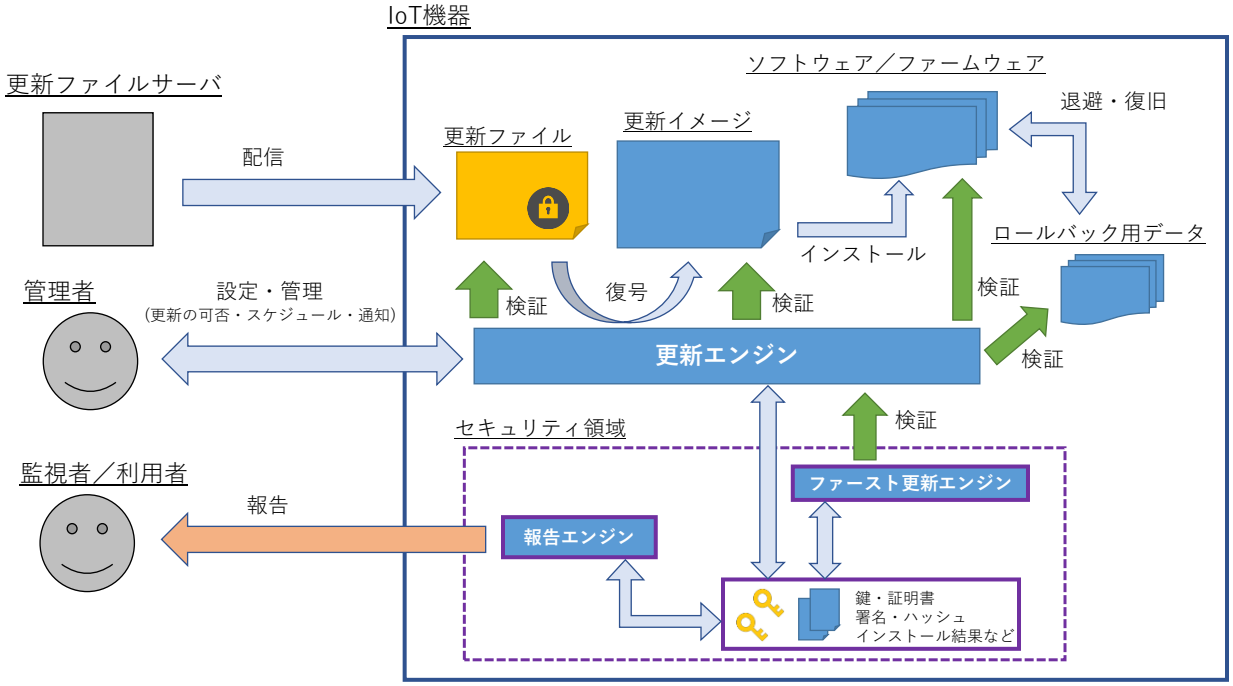

図 2　更新検証アーキテクチャ

(1) 更新ファイルと関連データ

「ソフトウェア更新」のプロセスにおいてメモリに展開されるデータ（ダウンロードした更新ファイル、更新イメージ、ソフトウェア／ファームウェア、ロールバック用データなど）の全てが正当性の検証対象となる。

(2) 更新エンジン

「ソフトウェア更新」を実行する「更新エンジン」それ自体もメモリに保存されたプログラムデータであるため、メモリ上の「更新エンジン」も更新ファイルと同様に正当性の検証対象となる。本文書で

は、「ソフトウェア更新」において最初に実行され、他の「更新エンジン」の更新と検証を担当する「更新エンジン」のことを「ファースト更新エンジン」と定義する。「ファースト更新エンジン」はクリティカルなコードであるため、「ソフトウェア更新」において使用される鍵や証明書などと同様にセキュリティ領域に保存され、保護される必要がある。

「ソフトウェア更新」における更新エンジンの連鎖的な検証アーキテクチャは、「セキュアブート」におけるブートローダの検証アーキテクチャと同様の仕組みであり、技術的な共通点が多い。とくにファームウェアの更新においては、機器の再起動を要求される場合が多く、更新エンジンが「セキュアブート」におけるブートローダと同一の機能になることもある。

(3) 報告エンジン

IoT 機器の正当性に関する情報（ソフトウェアやハードウェアの構成、インストールの検証結果、機器の ID、証明書など）を外部のエンティティに報告するプログラム（報告エンジン）もまた、ファースト更新エンジンと同様にセキュリティ領域に保存され、保護される必要がある。

2.3 ライフサイクル

「ソフトウェア更新」を実装する IoT 機器のライフサイクルを以下の図 3 に示す。

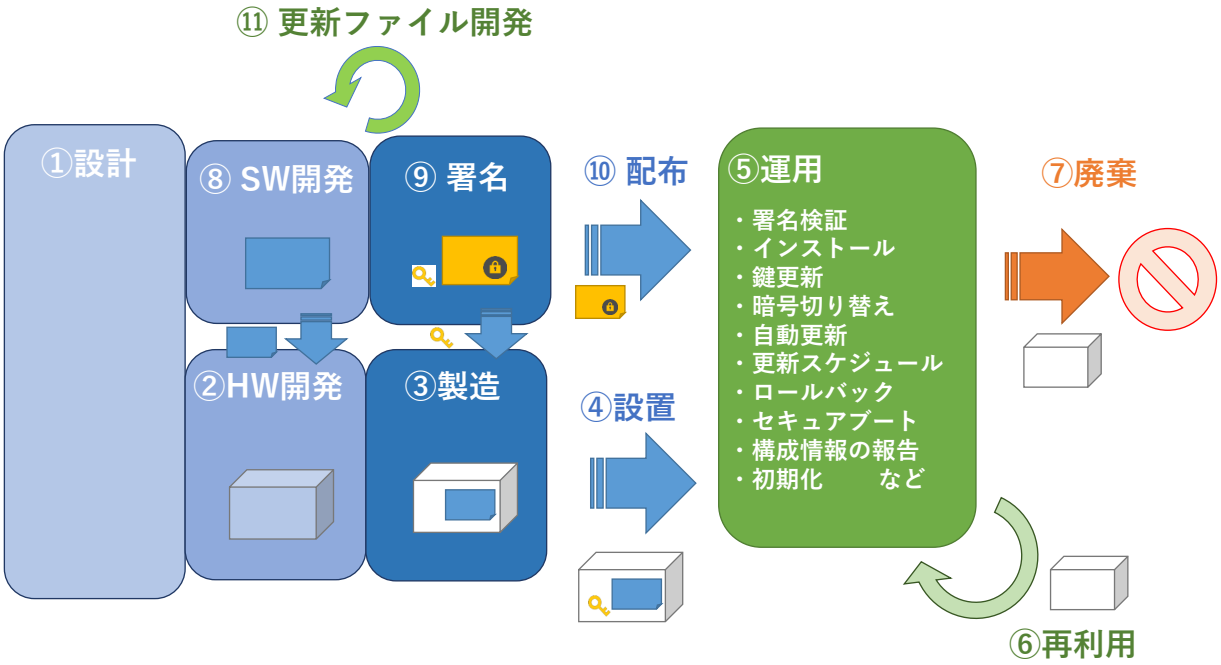

図 3　ライフサイクル

図 3 のように、「ソフトウェア更新」を実装する IoT 機器ではハードウェアとソフトウェアが異なるライフサイクルの流れをもつため、それぞれのライフサイクルを別個のものとして検討する必要がある。図 3 で示したライフサイクルの各フェーズに対する説明を以下に列記する。

① **設計**：

IoT 機器の設計仕様をアウトプットするまでのフェーズ（本文書では顧客へのヒアリングや要件定義などの過程も含める）。想定する顧客のセキュリティ要求を満たすため、IoT 機器のユースケースに応じたセキュリティ対策を設計フェーズから検討する必要がある。

② **HW 開発**：

設計仕様をインプットとして IoT 機器を構成するハードウェアを開発するフェーズ（デバッグなどの動作テストも含める）。SW 開発フェーズと並行して進められる。

③ **製造**：

開発が完了した IoT 機器を工場生産ラインで製造するフェーズ。「ソフトウェア更新」の実装のため、更新ファイルの署名を検証するための鍵の書き込みが必要。

④ **設置**：

製造が完了した IoT 機器を配送し、設置者（顧客自身もしくはシステムインテグレータなど）によって IoT 機器の使用環境へ設置されるフェーズ。

⑤ **運用**：

設置された IoT 機器が顧客によって運用されるフェーズ。

⑥ **再利用**：

IoT 機器の管理者や利用者が変更された場合に、IoT 機器の設定を初期化して再利用するフェーズ。

⑦ **廃棄**：

IoT 機器が顧客によって廃棄対象として処分されるフェーズ。

⑧ **SW 開発**：

IoT 機器を構成するソフトウェアを開発するフェーズ。HW 開発フェーズと並行して進められる。

⑨ **署名**：

SW 開発からアウトプットされたソフトウェア（更新イメージ）に対して署名を生成・付与し、更新ファイルの作成を実施するフェーズ。

⑩ **配布**：

署名ファイルを配布するフェーズ。更新ファイルサーバを運用し、更新ファイルのアップロードとダウンロードのサービスを提供する。

⑪ **更新ファイル開発**：

リリース後に判明した不具合や脆弱性への対応または機能追加のため、更新ファイルを開発するフェーズ。⑧と⑨のフェーズの繰り返しにより実施される。

2.4 アクターの相関

「ソフトウェア更新」に関与するアクターの関係を説明するため、アクターの相関図を以下の図 4 に示す。

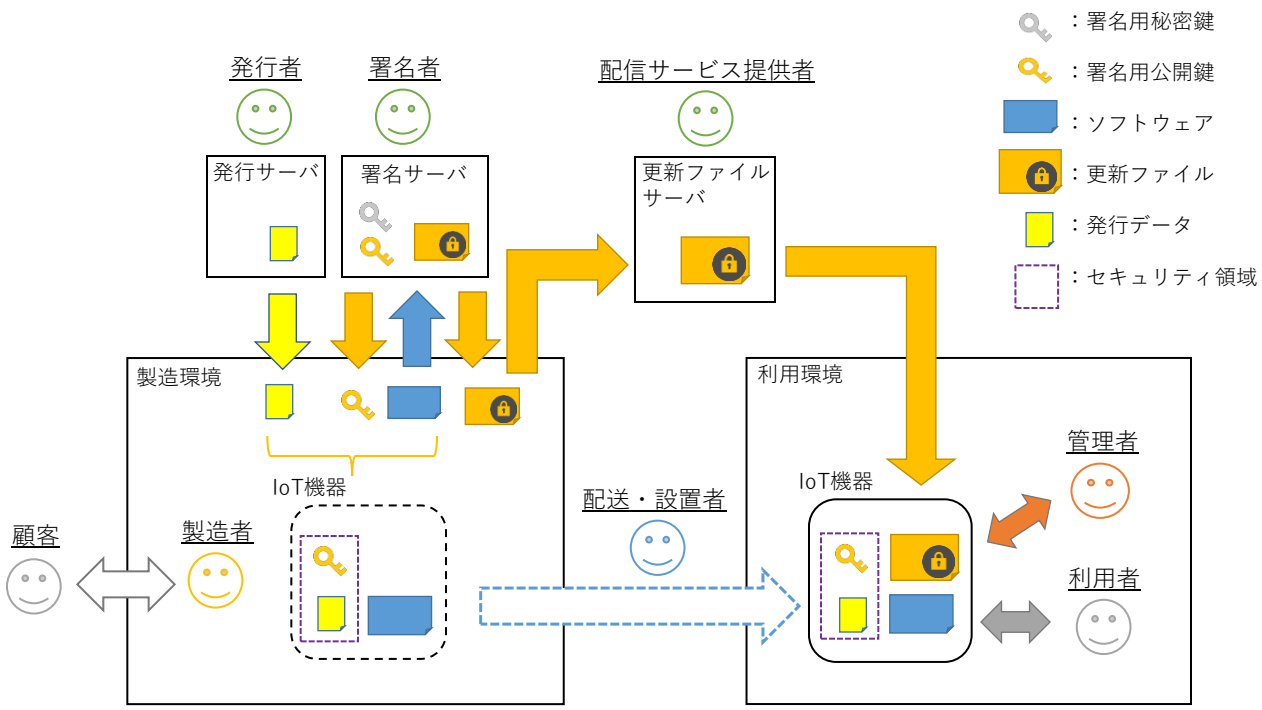

図 4　アクターの相関図

図 4 の各アクターに対する説明を以下に列記する。なお、本文書におけるアクターは役割の分類を示すために細分化したものであり、１人のアクターが複数の役割を兼ねることも想定されている。

① **顧客**：

製造者との契約（売買・賃貸など）を通して、IoT 機器と更新ファイル配信サービスなどの提供を受けるアクター。利用者や管理者を兼ねる場合がある。

② **製造者**：

IoT 機器の製造者であり、IoT 機器のハードウェア組み立て、ソフトウェアの書き込み、発行データ（ユニークな ID や鍵、証明書などの機密データ）の書き込み、署名用公開鍵の書込み、更新ファイルのアップロードを担当するアクター。「ソフトウェア更新」の運用に必要な各サーバの要件（発行サーバと署名サーバは高いセキュリティ、更新ファイルサーバは高い可用性が要求される）を製造者自身でまかなうことが困難な場合、各サーバの運営を信頼できる外部のアクター（発行者、署名者、配信サービス提供者）に委託する場合がある。また、IoT 機器へのセキュアなデータ書き込み環境の確保が困難な場合、機密データのセキュリティ領域への書き込み業務も発行者に外部委託する場合がある。

③ **発行者**：

IoT 機器に対する発行データ（ユニークな ID や鍵、証明書などの機密データ）の生成を担当するアクター。また、製造者に機密データの書き込み業務の委託を受けた場合には、セキュリティ領域への発行データと署名用公開鍵の書き込みも担当する。IoT 機器のハッキング・なりすましを防ぐため、発行データは厳重に保護・管理される必要がある。

④ **署名者**：

アップロードされたソフトウェア（更新イメージ）に対して、更新ファイルの作成（署名の生成・付与と暗号化）を担当する。更新ファイルの改ざんを防ぐため、署名生成に用いられる秘密鍵は厳重に保護・管理される必要がある。

⑤ **配信サービス提供者**：

更新ファイルの配信サービス提供者。更新ファイルサーバをロバストに運用する責任をもつ。

⑥ **配送・設置者**：

IoT 機器の出荷から設置に至るまでのロジスティクスを担当するアクター。配送業者、小売販売業者、システムインテグレータなどを含む。

⑦ **管理者**：

設置された IoT 機器に対して「ソフトウェア更新」の管理権限をもつアクター。顧客に委託された第三者（システムインテグレータなど）でない場合には、顧客または製造者が兼ねる。

⑧ **利用者**：

設置された IoT 機器に対して「ソフトウェア更新」の管理権限をもたず、IoT 機器の提供するサービスを利用するアクター。末端のユーザや監視エンティティなどを含む。顧客や管理者が兼ねる場合もある。

2.5 処理フロー

「ソフトウェア更新」に関する IoT 機器外部の処理の流れを説明するため、処理フローの例を提示する。IoT 機器のユースケースによって様々な処理フローが考えられるが、ここではコンシューマ IoT 機器を想定した簡潔な処理フロー、産業用 IoT 機器を想定した高度な処理フローの 2 つの例を提示する。

コンシューマ IoT 機器を想定した簡潔な処理フローの例

【特徴】

① 登場するアクターは製造者、配信サービス提供者、利用者の３名。

② 発行サーバと署名サーバの運用を外部に委託せず、製造者自身が発行者と署名者の役割を兼ねている。

③ 利用者が顧客と設置者と管理者を兼ねている。

④ 更新ファイルのインストールは、利用者の自己判断によって実行される。

上記の特徴をもつ処理フローの例を以下の図 5～7 に示す。

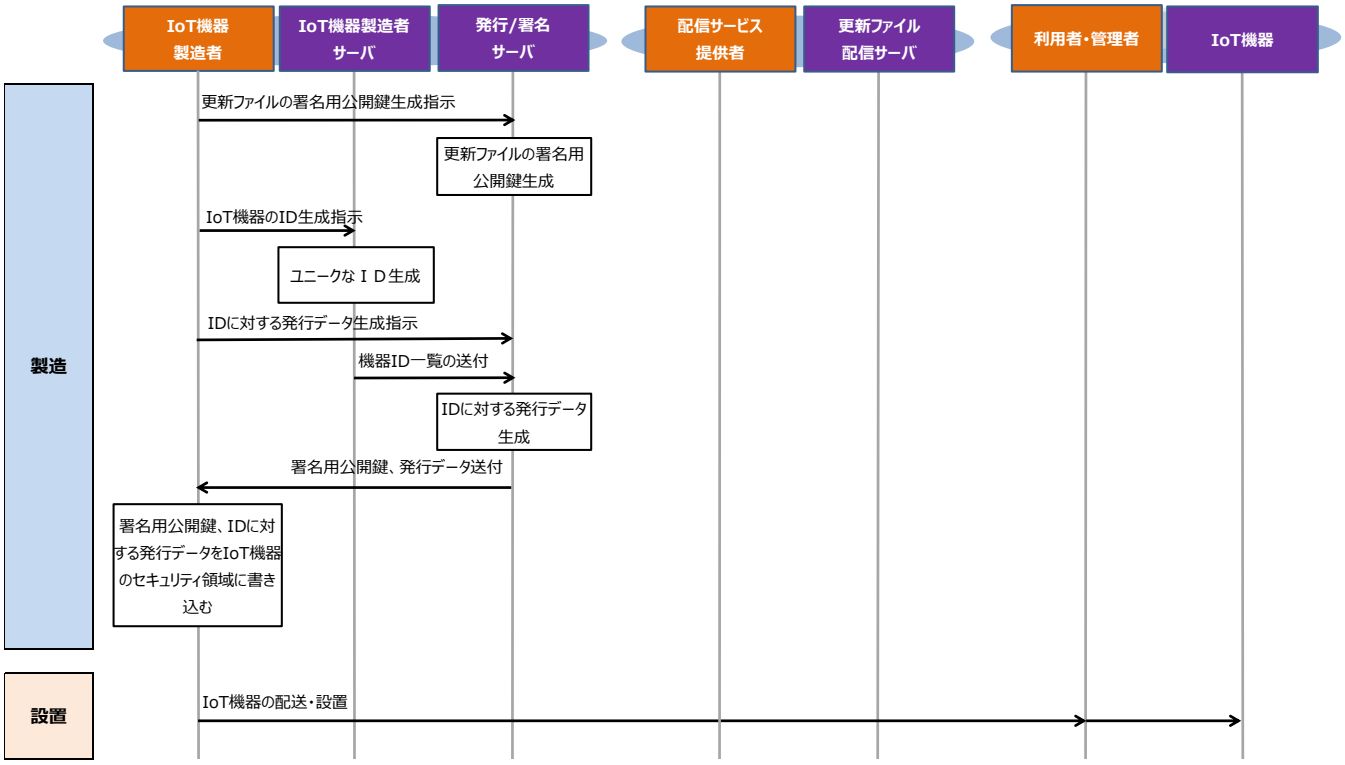

図５　製造から設置までの処理フロー（簡潔な処理フロー）

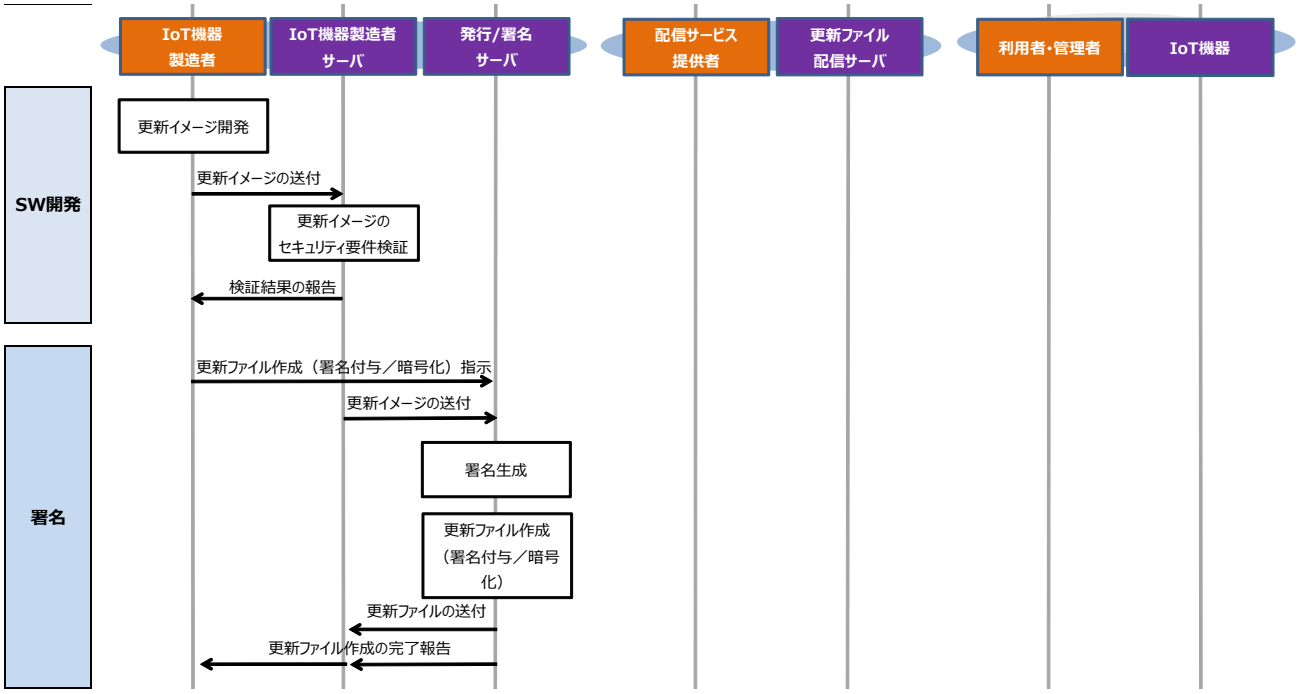

図６　SW 開発から署名までの処理フロー（簡潔な処理フロー）

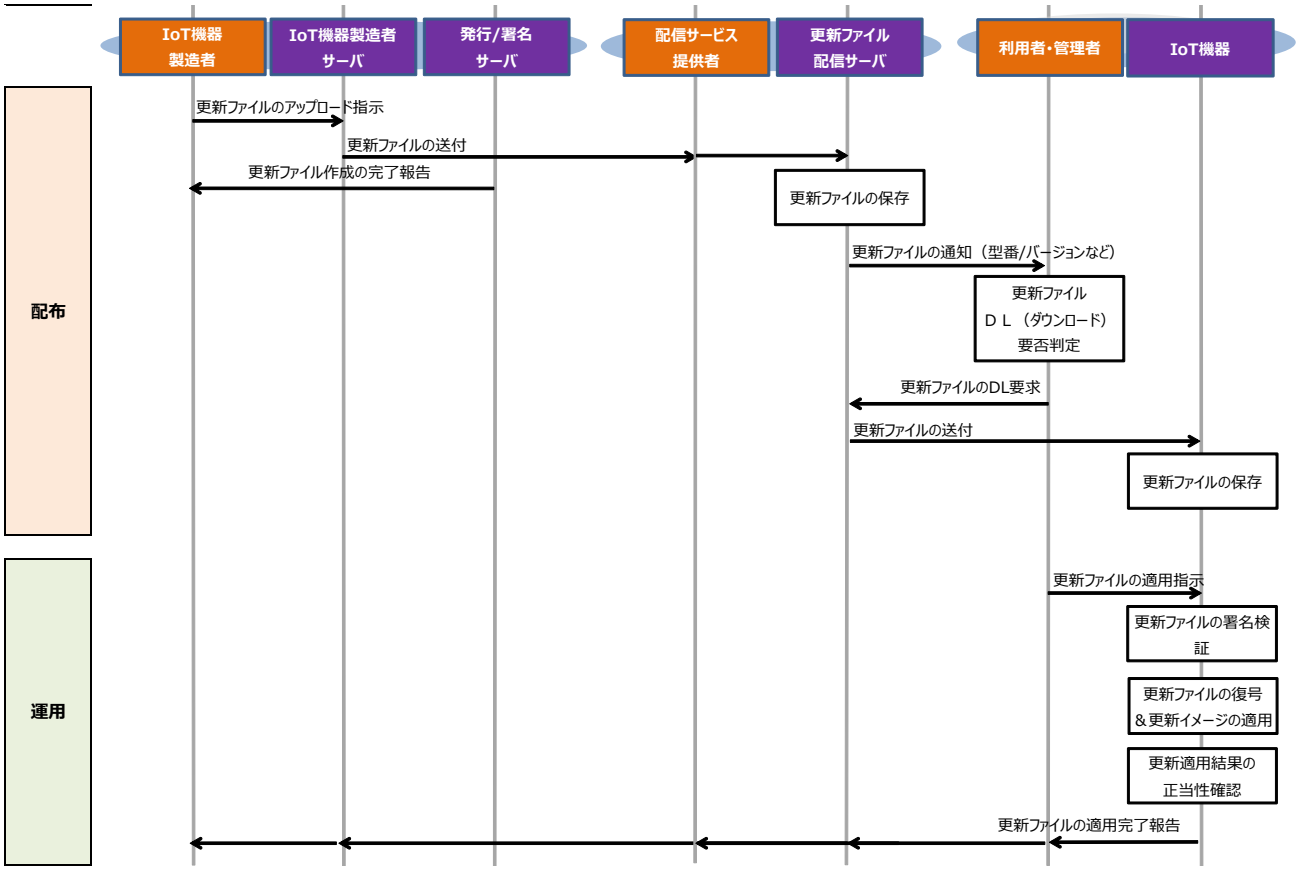

図７　配布から運用までの処理フロー（簡潔な処理フロー）

産業用 IoT 機器を想定した高度な処理フローの例

【特徴】

① 登場するアクターは製造者、配信サービス提供者、管理者、利用者の 4 名。

② 管理者が配送･設置者を兼ねている（工場におけるシステムインテグレータを想定）。

③ 更新ファイルは、管理者が管理するローカル更新サーバを経由して IoT 機器にダウンロードされる（工場内のネットワークを想定）。

④ 更新ファイルのインストールは、利用者の要求に対して管理者が可否を判断することによって実行される。

上記の特徴をもつ処理フローの例を以下の図 8～10 に示す。

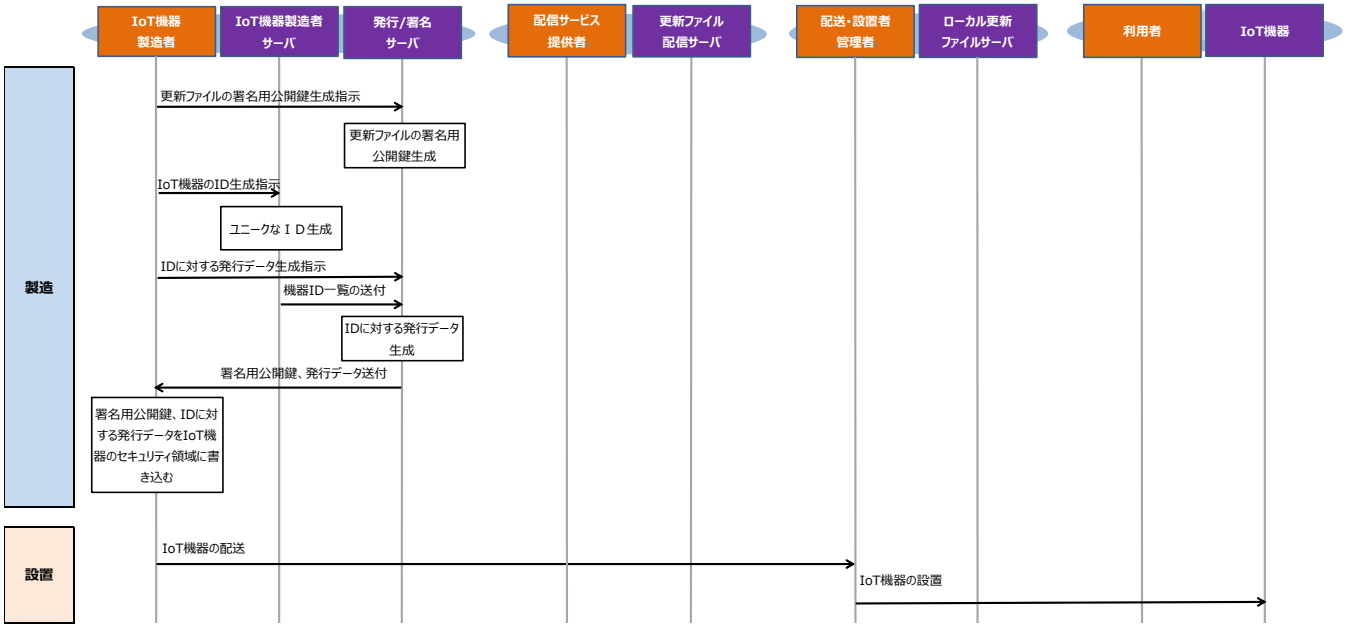

図 8　製造から設置までの処理フロー（高度な処理フロー）

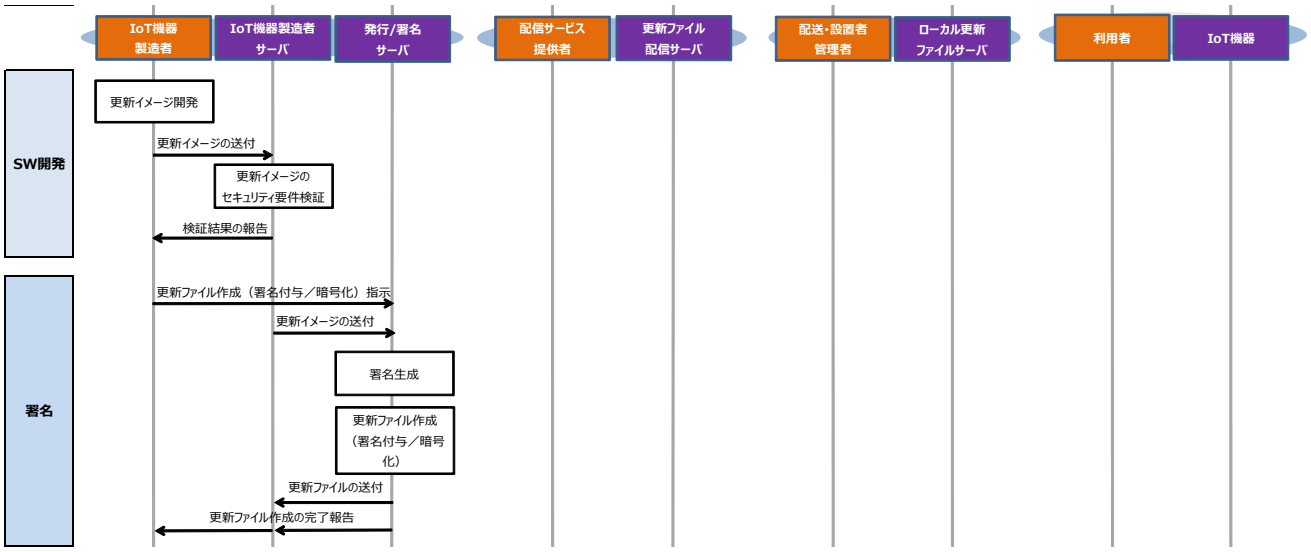

図 9　SW 開発から署名までの処理フロー（高度な処理フロー）

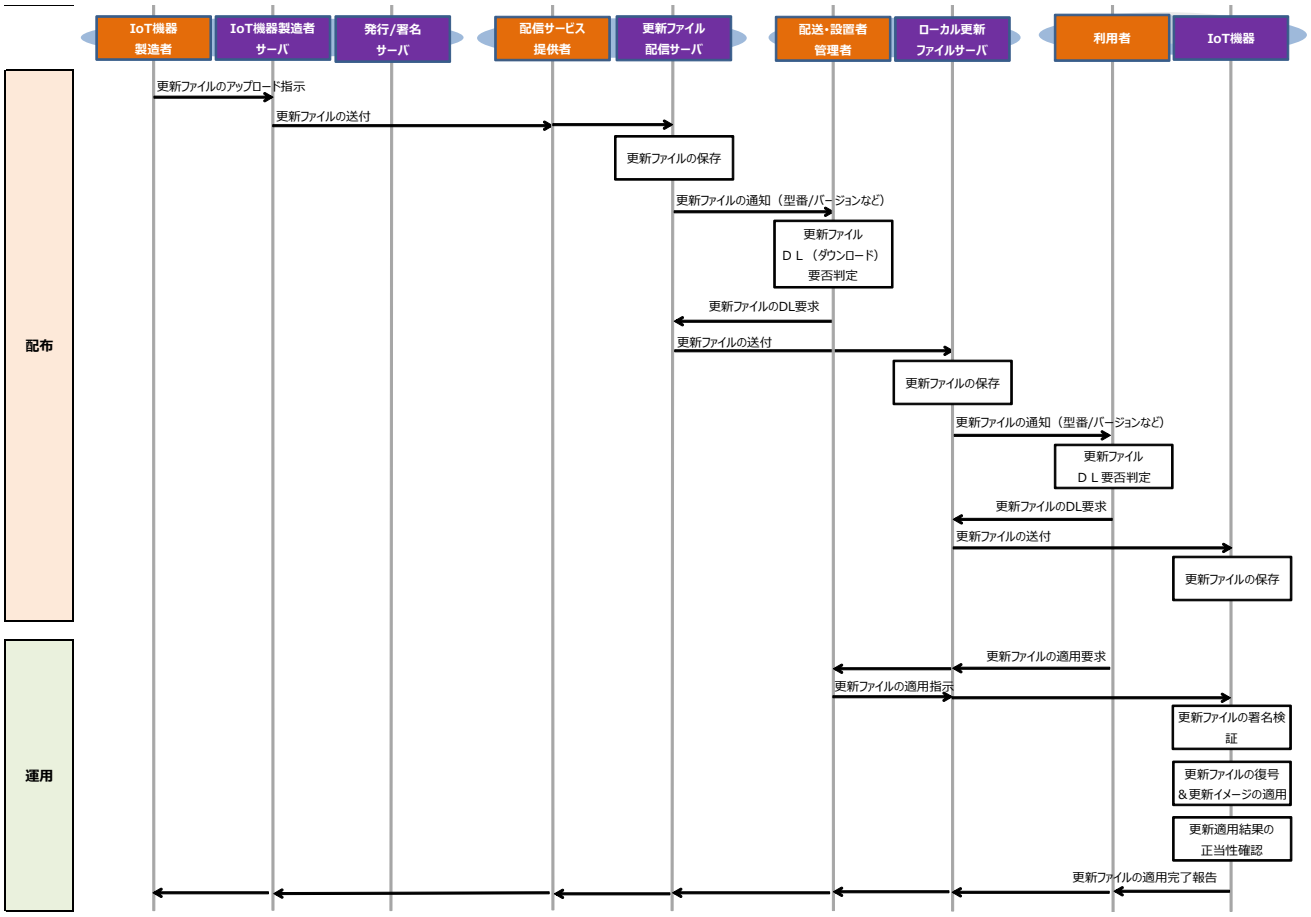

図 10　配布から運用までの処理フロー（高度な処理フロー）

2.6 リスク分析

前節までに定義されたモデルを対象に「ソフトウェア更新」のリスク分析を実施した結果を以下に示す。

(1) リスク分析の実施手順

① ライフサイクルの各フェーズに対し、脅威と脆弱性を抽出。

② 抽出された脅威と脆弱性の対応関係を整理。

③ 次章で実施されたセキュリティ要件の検討の結果をフィードバックして修正。

(2) リスク分析の結果

下記の表 2 に示す。なお、次章で解説するセキュリティ要件との対応を示すため、右端の列に識別子を表示している。

表 2 リスク分析結果

ライフサイクル	リスク分析		セキュリティ要件識別子
	脅威	脆弱性	
製造	製造環境における鍵や証明書情報が漏洩	開発時に使用した鍵や証明書が利用可能な状態で出荷している	HLC01
		機密情報を書き込む製造環境のセキュリティ対策が不十分（入退室管理、ネットワーク隔離、生産管理サーバのセキュリティ対策など）	HLC02
	部外者が製造スタッフになりすます	製造環境への入退室管理が十分なされていない	ORG08
	通信路にて、データが盗聴・改ざんされる	古いアルゴリズムや短い鍵長の鍵を使用している	STS07
	機器内のデータが改ざんされる	古いアルゴリズムや短い鍵長の鍵を使用している	STS07
設置	配送過程における第三者による機密情報の解析、改ざん、機器のすり替え	機密情報の解析、改ざんが容易な設計になっている	HLC03
	初期設定が適正に実施されず、脆弱なセキュリティ状態のまま設置される	設置時の初期設定におけるセキュアでない PC の使用、担当者のスキル不足	HLC04
		設置時の初期設定において、自動化ツールがない	HLC05
SW 開発／署名	新規の脆弱性を利用した攻撃を受け、不正に利用される	新しく発見された脆弱性への対応を怠り、放置している	ORG01
	未対策のソフトウェアの脆弱性が悪用され、不正に利用される	セキュリティを事前に考慮(セキュリティ・バイ・デザイン)した開発が行われず、リスク分析と対策が不十分	ORG02
		第三者によるレビューや監査を受けていないため、リスク分析と対策が不十分	ORG04

ライフサイクル	リスク分析		セキュリティ要件識別子
	脅威	脆弱性	
	マルウェアや脆弱性の仕込まれたライブラリ等を使用してしまい、不正に利用される	信頼性の低いツールやライブラリを無条件に信用して利用している	ORG03
		外部から調達したツールやライブラリの安全性について検証していない	ORG06
	ソフトウェアの脆弱性への対応の遅れにより、不正に利用される	製品リリース後のインシデント発生に対応するための組織体制（ISMS など）が不十分	ORG05
		第三者のセキュリティチェックは行っていない	ORG07
	部外者が開発スタッフになりすます	開発環境への入退室管理が十分なされていない	ORG08
	開発環境から設計情報が漏洩	マルウェアの感染やソーシャルハッキングなどを防ぐための開発環境・開発プロセスの整備、開発スタッフの教育が不十分	UPC09
	コードの脆弱性をついた攻撃がなされる	セキュリティ要件に適合しない脆弱なコードを見過ごしたままリリースしている	UPC10
	偽造された署名により、不正なソフトウェアをインストールされる	署名生成・付与の環境へのアクセスが容易なため、署名用秘密鍵が漏洩	UPC11
	通信路にて、データが盗聴・改ざんされる	古いアルゴリズムや短い鍵長の鍵を使用している	STS07
	機器内の廃棄済みデータが盗聴される	機器内のデータを適切に消去する機能がない	STS08
	機器内のデータが改ざんされる	古いアルゴリズムや短い鍵長の鍵を使用している	STS07
配布／運用	運用中の IoT 機器を個体識別できず、管理不能に陥る	製品リリース後、各 IoT 機器をユニークに識別する手段がない	STS01
			STS02
		多数の機器を管理するためのアセット管理ツールが用意されていない	STS03
	脆弱性への対応のため、IoT 機器の物理的な交換を余儀なくされる	IoT 機器にソフトウェア更新機能がない	STS04
		IoT 機器に暗号の設定を変更する機能がない	STS09
	攻撃者により脆弱なセキュリティ状態に設定を変更され、不正に利用される	設定変更機能へのアクセスが制限されていない	STS05
	脆弱なセキュリティ状態を修正できず、不正に利用され続ける	セキュアな設定に修復する機能がない	STS06
	通信路にて、データが盗聴・改ざんされる	古いアルゴリズムや短い鍵長の鍵を使用している	STS07
	機器内の廃棄済みデータが盗聴される	機器内のデータを適切に消去する機能がない	STS08
	機器内のデータが改ざんされる	古いアルゴリズムや短い鍵長の鍵を使用している	STS07

ライフサイクル	リスク分析		セキュリティ要件識別子
	脅威	脆弱性	
	機器内のデータを改ざんされたIoT機器を復旧できない	データをバックアップする機能がない	STS10
	開放する必要のないインターフェースを攻撃者に利用され、IoT機器の可用性とセキュリティが損なわれる	機器のコア機能には不要なポートやスイッチなどを禁止する機能がない	STS11
	ネットワークインターフェースを不正利用され、データが盗聴・改ざんされる	ネットワークインターフェースへのアクセスを制限する機能がない	STS12
	総当り攻撃によってアカウントを乗っ取られ、不正に利用される	過剰な認証トライ(攻撃)に対して、試行回数に応じた措置（アカウントのロックや禁止、ディレイなど）を実行する機能がない	STS13
	論理的アクセスの偽装を識別できず、不正に利用される	論理的アクセスを試行する各ユーザ、機器、プロセスをユニークに識別する機能がない	STS14
		論理的アクセスを試行する各ユーザ、機器、プロセスを認証する機能がない	STS15
	IoT機器への直接の物理的攻撃により、IoT機器のデータが盗難・改ざんされ、不正に利用される。または破損・破壊される	物理的なセキュリティ対策を実施していない	STS16
	ソフトウェアの脆弱性への対策や機能修正を実施できず、IoT機器のセキュリティと可用性を維持できない	IoT機器のソフトウェアを更新する機能がない	UPE01
	ソフトウェア更新によってクリティカルな業務に悪影響が出た場合に復旧できない	IoT機器のソフトウェアを更新前の状態に戻す機能(ロールバック機能)がない	UPE02
	攻撃者によってソフトウェアを脆弱なバージョンにロールバックされ、IoT機器の可用性とセキュリティが損なわれる	ロールバック機能の許可権限を管理する機能がない	UPE03
	管理者の意図しないソフトウェア更新が実施され、IoT機器の可用性とセキュリティが損なわれる	ソフトウェア更新の許可権限を管理する機能がない	UPE04
		ソフトウェア更新の有効／無効を切り替えられない	UPE05
		ソフトウェア更新を要求するIoT機器に対して、個体ごとに認証して許可する仕組みがない	UPD08
		利用者によるIoT機器のアップデート操作に対して、管理者が上書きする機能がない	UPD11
		更新ファイルの仕様にシーケンシャルなバージョン番号が含まれておらず、古いバージョンの更新ファイルのインストールを防ぐ機能がない	UPC02

ライフサイクル	リスク分析		セキュリティ要件識別子
	脅威	脆弱性	
	ソフトウェア更新の機能仕様が顧客の要件に適合しないため、IoT 機器の可用性とセキュリティが損なわれる	リモートでのソフトウェア更新の実行を自動／手動で切り替えられない	UPE06
		顧客の要件に合わせて更新通知を設定できない	UPE07
		ソフトウェア更新の実施タイミングをスケジュール管理する機能がない	UPE08
		冗長システムを構成するために必要な機能がない	UPE09
		更新ファイルサーバがトリガーを出す自動ソフトウェア更新に対し、IoT 機器の管理者が更新スケジュールを設定できない	UPD05
	TOCTTOU 攻撃などにより権限状態を偽装され、不正に利用される	ソフトウェア更新処理中の操作が禁止されていない	UPE10
	不正な更新ファイルをインストールすることにより、IoT 機器の可用性とセキュリティが損なわれる	更新ファイルの正当性をインストール前に検証する機能がない	UPE11
		更新ファイルの正当性検証などで利用される暗号演算の保護が不十分	UPE12
		更新ファイルの仕様に正当性検証のための署名が含まれておらず、署名検証のプロセスがない	UPC01
	ソフトウェア更新に失敗した状態で放置され、IoT 機器の可用性とセキュリティが損なわれる	ソフトウェア更新の失敗を検知する機能がない	UPE13
		更新ファイルファイルサーバから各 IoT 機器のソフトウェア更新の結果を追跡する手段がない	UPD09
		更新ファイルファイルサーバから各 IoT 機器のソフトウェア更新の結果を追跡する手段がない	UPD10
	ソフトウェア更新の失敗によってクリティカルな業務に悪影響が出た場合に復旧できない	ソフトウェア更新を失敗した状態から回復する機能がない	UPE14
	更新エンジンが改ざんされることで不正な更新ファイルのインストールが可能となり、不正に利用される	更新エンジンがハードウェアレベルで保護されていない	UPE15
		更新エンジンの検証と報告の機能がハードウェアレベルで保護されていない	UPE17
	IoT 機器内のクリティカルなコードや鍵が漏洩し、不正に利用される	クリティカルなコードと鍵がハードウェアレベルで保護されていない	UPE16
	署名用の鍵が脆弱化し、署名を偽造されることで不正な更新ファイルをインストールされ、IoT 機器の可用性とセキュリティが損なわれる	署名に使用する鍵と証明書を、開発時とリリース時で分けていない	UPC03
		製造出荷された製品が、開発時の鍵で生成された署名を付与された更新ファイルを受け入れる設定になっている	UPC04

ライフサイクル	リスク分析		セキュリティ要件識別子
	脅威	脆弱性	
		脆弱なパッチや漏洩した鍵の廃棄プロセスが設計されておらず、無効化できない	UPC05
		鍵の有効期限を管理し、使用開始や廃棄を行うスケジューリング機能がない	UPC06
		適切な強度の署名鍵が選択されていない	UPC07
		公開鍵基盤において信頼性を保証する基であるべき CA の選択が不適切	UPC08
	最新の更新ファイルが適用されず古いバージョンのままの IoT 機器が増え続けることにより、攻撃者のターゲットとなる脆弱な IoT 機器も膨大な数になり、不正利用のリスクが高まる	集中管理されたスケーラブルな自動ソフトウェア更新機能がない	UPD01
	更新ファイルサーバの可用性の低下によりソフトウェア更新を利用できなくなり、IoT 機器の可用性とセキュリティが損なわれる	多数の IoT 機器からの更新ファイルのダウンロードに対して、ネットワークとサーバの容量をオーバーさせないための仕組みが適切に設計されていない	UPD02
		非効率または脆弱な配布システムのために管理タスクが増大し、管理者が IoT 機器のソフトウェア更新を適切に管理できない	UPD04
		更新ファイル配布サービスの実装において、サービス拒否攻撃を検知して防御する機能がない	UPD06
	更新ファイルサーバへの不正アクセスにより、更新ファイルを盗難・改ざんされる	更新ファイルサーバへのアクセスが保護されていない	UPD03
	更新ファイルサーバの通信鍵の漏洩によって更新ファイルが盗聴・改ざんされ、IoT 機器の可用性とセキュリティが損なわれる	更新ファイルサーバの通信鍵がハードウェアレベルで保護されていない	UPD07
	IoT 機器のセキュリティ状態を監視できないために脆弱性や攻撃が放置され、不正に利用される	IoT 機器のセキュリティ状態を報告する機能がない	SSS01
		IoT 機器のセキュリティ状態の変化を検出する機能がない	SSS02
	IoT 機器のセキュリティ状態が盗聴・改ざんされ、不正に利用される	IoT 機器のセキュリティ状態インジケータへのアクセスが制限されていない	SSS03
		IoT 機器のセキュリティ状態の編集が機器モニターのみに制限されていない	SSS04

ライフサイクル	リスク分析		セキュリティ要件識別子
	脅威	脆弱性	
	インシデント分析に必要なログ情報の不足によってインシデントへの対応が遅れ、IoT 機器の可用性とセキュリティが損なわれる	IoT 機器のセキュリティ状態の情報を他の機器に提供する機能がない	SSS05
	ソフトウェアのバージョンや更新ファイルの適用状態を把握できないために脆弱性の有無を判定できず、IoT 機器の信頼性が損なわれる	IoT 機器のソフトウェアのバージョンや更新ファイルの適用状態を設定管理できない	SSS06
		外部から IoT 機器のソフトウェアのバージョンや更新ファイルの適用状態を検証する機能がない	SSS07
再利用／廃棄	再利用フェーズにおける機密情報、個人情報の漏洩	機密情報、個人情報の初期化機能、または耐タンパー性の不足	HLC06
	廃棄フェーズにおける機密情報、個人情報の漏洩	機密情報、個人情報の初期化機能、機器の動作停止機能、または耐タンパー性の不足	HLC07

3. セキュリティ要件

本章では、2.6 節のリスク分析の結果を受け、「ソフトウェア更新」実装のためのセキュリティ要件を検討し、整理した結果を表 3 に提示する。

本文書におけるセキュリティ要件の大分類は以下の 7 項目である。

(1) 組織の体制
(2) 基本セキュリティ
(3) 更新処理の実行
(4) 更新ファイルの作成
(5) 更新ファイルの配布
(6) セキュリティ状態検知
(7) HW ライフサイクル

※本文書は「ソフトウェア更新」に焦点を当てているため、「ソフトウェア更新」のようなシステムの動的変化に関係しないセキュリティ機能を「基本セキュリティ」として分けて分類している。

本文書における各セキュリティ要件は、製造者が IoT 機器に必要なセキュリティ要件をユースケースに応じて検討するための目安として利用するため、以下の３段階にレベル分けされている。

［ A ］ ユースケースによらず必要となる可能性が高い要件
［ B ］ ユースケースによっては必要となり得る要件
［ C ］ より高度なセキュリティが要求される場合には追加で検討すべき要件

※A 要件については、NIST.IR.8259A で提示されている共通サイバーセキュリティ性能（Common cyber-security capabilities）に準拠している。

※A～C のレベルはセキュリティレベルの認証基準ではなく、実装検討の目安としてのレベル分けである。本章のセキュリティ要件は、あくまで製造者自身が各自のユースケースに応じたセキュリティ要件を検討するための材料であり、すべてのセキュリティ要件への準拠を指示するものではない。

表 3　「ソフトウェア更新」実装のためのセキュリティ要件

大分類	分類	セキュリティ要件	識別子	補足説明
組織の体制	製造者の組織体制			• 「オンライン更新」をサービスとして継続的に提供するために、組織全体としてのセキュリティ改善活動の継続が推奨される。 • 設計時だけでなく、メンテナスにおいても脅威分析の更新と適切な対策の選択が推奨される。 • 開発において使用されるツール類の信頼性が将来的なリスクの発生に影響するため、使用するツール類は慎重に選択することが推奨される。
	B	継続的なセキュリティ改善活動（新しい脅威への対応など）の実施	ORG01	
		設計段階とメンテナス時における脅威分析と対策の実施	ORG02	
		信頼できる開発環境（ツール・言語・アルゴリズム・プロトコル・ライブラリ）の使用	ORG03	
	C	第三者によるセキュリティレビュー、セキュリティ監査認証の実施	ORG04	
		ロバストなインシデント対応プロセスの整備、ISMS の設置	ORG05	
		利用している外部ツールライブラリのセキュリティ解析の実施	ORG06	
		侵入テスト、ストレステスト、動的解析（ファジングなど）、静的解析の実施	ORG07	
		職員に対する高度な本人認証（ID カード、多要素認証など）の利用	ORG08	
基本セキュリティ	機器の識別と管理			• ユニークな論理 ID は通常のデバイス管理や監視において他の機器との識別に利用される。ID による一貫した識別のため、ID が不変であることが要求される場合もある。ID がそのままデバイス認証などに利用される場合もあるが、用途に即した適切な ID の選択方法を検討する必要がある（ID の長さ、生成アルゴリズムなど）。 • 物理 ID は論理 ID が使えないタイミング（設置、廃棄、故障時など）において機器の識別手段として利用可能。 • ユニークではない追加の論理 ID が必要になる場合もある（機器の用途を示す ID など）。
	A	機器へのユニークな論理 ID の付与	STS01	
		機器へのユニークな物理 ID の付与	STS02	
	B	アセット管理システムを利用して機器を管理できる	STS03	
	機器の設定変更			• 権限エンティティは、様々な理由（サイバーセキュリティ、相互運用性、プライバシーなど）から IoT 機器の設定を変更しようとする可能性がある。権限エンティティの
	A	機器のソフトウェアとファームウェアの設定を変更できる	STS04	
		機器の設定変更を権限エンティティにのみ許可する	STS05	

大分類	分類	セキュリティ要件	識別子	補足説明
		権限エンティティによって、権限エンティティの定義するセキュアな設定に機器を修復できる	STS06	要求に適合させるため、設定変更の機能が必要になる。 • IoT 機器は多かれ少なかれ設定機能に依存しており、攻撃者が狙うポイントとなっている。そのため、非権限エンティティによる設定変更を禁止する機能や、攻撃された場合にはセキュアな設定に修復する機能が必要となる。 • 非権限エンティティは様々な動機（不正なアクセス、機器の誤作動、機器の周辺環境の観察など）から IoT 機器の設定を変更しようとする可能性がある。
	機器のデータ保護			• 非権限エンティティによるデータへのアクセスや誤用を防ぐため、機密性を適切に保護する機能が必要となる。 • 廃棄されたデータへのアクセスを防ぐため、全てのエンティティからアクセスできないようにする機能が必要となる。 • 権限エンティティが要求するセキュリティレベルを満たすため、データ保護機能の設定を変更する機能が必要となる。
	A	機器が保存または送信するデータの機密性と完全性を保護するため、安全性が実証されている暗号モジュールと標準の暗号アルゴリズムを使用する （脆弱な古い TLS などを使わない）	STS07	
		機器内の全てのデータに対して、権限エンティティが適切な消去（全エンティティからのアクセス不能化）を実行できる （内部ストレージ初期化における暗号化データに対応した暗号鍵の破棄、など）	STS08	
		権限エンティティが機器のデータ保護機能の設定を変更できる （暗号の種類や鍵長など）	STS09	
	B	データ可用性を支援するため、機器がセキュアバックアップの機構を備える	STS10	
	機器のアクセス制御			• インターフェースへのアクセスを制限することは、IoT 機器に対する攻撃手段を減らし、悪用される機会を少なくすることにつながる。 • IoT 機器の状態によって、部分的または完全にインターフェースへのアクセス制限するような実装もあり得る。たとえば、IoT 機器がセキュアオンボーディング（ネットワーク経由の自動初期設定）のスキ
	A	機器のコア機能に必要でないインターフェース（機器本体／ネットワーク）を、論理的または物理的に禁止できる （危険なポートの禁止、屋外使用機器におけるリセットボタンの禁止など）	STS11	
		機器の各ネットワークインターフェースへの論理的アクセスを制限できる（デバイス認証、ユーザ認証など）	STS12	

大分類	分類	セキュリティ要件	識別子	補足説明
		機器への過剰な回数の認証トライに対して、機器がアカウントのロックや禁止、ディレイなどの措置を実行でき、それぞれの有効／無効や閾値を設定できる	STS13	ームに則る場合、正規の手順でプロビジョニングされていない状態では全てのネットワークインターフェースが制限される。 • 論理的アクセスを試行するエンティティを一意に識別し、認証することは不正なアクセスの防止や、インシデントの分析に役立つ。
	B	機器への論理的アクセスを試行する各ユーザ、各機器、各プロセスを、機器がユニークに識別できる	STS14	
		機器への論理的アクセスを試行する各ユーザ、各機器、各プロセスを、機器が正当に認証できる　(弱いパスワード要件の禁止、認証機能のない UPnP の禁止など)	STS15	
		機器に対する無許可の開封や改ざんを防ぐための適切な物理セキュリティをもつ （物理アクセスの制限、開封防止シールや耐タンパー筐体の使用など)	STS16	
アップデート実行	更新の実行と管理			• IoT 機器から脆弱性を除去し、攻撃者によって機器が悪用される可能性を低減するため、ソフトウェアを更新できる機能が必要となる。 • 更新機能は、IoT 機器の運用上の問題（可用性、信頼性、速度など）の修正のためにも有用である。 • IoT 機器への直接制御による手動更新か、または IoT 機器自身による自動更新か、権限エンティティによって必要とする更新機能のタイプは異なる。 • クリティカルな業務で IoT 機器を利用する組織においては、ソフトウェア更新による意図しない悪影響に対処するため、ロールバック機能を必要とする場合がある。一方、組織によってはロールバック操作によって脆弱なバージョンになってしまうリスクを排除するため、ロールバックを禁止したい場合がある。 • クリティカルな業務で利用される IoT 機器においては可用性の確保が
	A	機器のソフトウェアを更新できる	UPE01	
		更新されたソフトウェアを機器がロールバックできる	UPE02	
		権限エンティティにのみ機器がロールバックを許可する　(ロールバック攻撃への対策)	UPE03	
		権限エンティティにのみ機器が更新の実行を許可する	UPE04	
		機器のソフトウェア更新機能の有効／無効を設定できる	UPE05	
		機器のソフトウェア更新の実行開始を自動／手動に設定できる	UPE06	
		機器の更新通知に関する設定を変更できる　(更新が利用可能になった際の通知の有効／無効化、通知の送信先の設定機能など)	UPE07	
	B	更新による可用性リスクを管理するため、機器の更新スケジュールを調整できる	UPE08	
		管理者が冗長システムを構成するために必要な機能を機器が備えている （従来版の機器から更新版の機器への切り替えトリガーへの対応など)	UPE09	

大分類	分類	セキュリティ要件	識別子	補足説明
	C	設計段階で予期されていない操作によって発生し得るセキュリティ認証の競合状態（TOCTTOU など）と、それを利用した攻撃を防ぐため、機器のセキュリティに関連した操作は排他的に処理されるように設計する（アップデート中の他の操作の禁止など）	UPE10	重要になるため、運用に影響が出ない時間帯を狙った更新のスケジューリングや、冗長システムの構成を検討する必要がある。
	更新ファイルの保護と検証			• 更新ファイルの改ざんによる攻撃を防ぐため、インストール前に更新ファイルの正当性を検証する機能の実装が推奨される。 • 正当性の検証プロセス（署名検証、MAC 照合など）はセキュアな環境での実行が推奨される。 • 更新ファイルを保護するため、暗号演算をセキュアな環境で実行することが追加対策として検討できる。
	A	インストール前に、更新ファイルの正当性（製造者の意図した状態で配信されたか否か）を機器が検証できる（署名者、完全性、適格性、その他権限などを確認）	UPE11	
	C	機器が暗号演算にセキュアコンポーネントを利用できる（更新ファイルの署名検証・復号など）	UPE12	
	更新した結果の検証と復旧			• 更新失敗の主な原因としては、不正な更新ファイル、電源断、ハードウェア故障などが考えられる。 • ファームウェアの更新に失敗した場合でも起動でき、更新結果の検証が可能となる設計が必要。 • 更新失敗からの回復手段として、ロールバック処理の実行は最低限のオプションとして推奨される。
	B	機器が更新失敗を検知できる （セキュアコンポーネントによる検証も可）	UPE13	
		機器が更新失敗から回復できる（ロールバックの実行、中断したインストールの再開など）	UPE14	
	更新エンジンの保護と検証			• 更新ファイルを処理するプロセスのデータを保護するため、最初に呼び出される更新エンジン（ファースト更新エンジン）をセキュアなハードウェアで保護する実装が推奨される。 • IoT 機器にとってクリティカルなコードと鍵のセキュアコンポーネントへの保存を追加対策として検討できる。 • 外部に更新エンジンの正当性を報告するため、SE や TPM などのセキュアなハードウェアを利用した検証と報告の機能が追加対策として検討できる。
	B	機器のファースト更新エンジンをハードウェアで保護できる（耐タンパー性セキュアコンポーネントなど）	UPE15	
	C	機器のクリティカルなコードと鍵をハードウェアで保護できる（耐タンパー性セキュアコンポーネントなど）	UPE16	
		機器の更新エンジンと報告エンジンをハードウェアで保護できる（耐タンパー性セキュアコンポーネントなど）	UPE17	
アップデート作成	セキュアなアップデート署名			• 更新ファイルの機密性と完全性を確保するため、更新ファイルへの信頼できる署名の付与が推奨される。
	B	更新ファイルへの署名付与	UPC01	
		更新ファイルへのシーケンシャルなバージョン番号の付与	UPC02	

大分類	分類	セキュリティ要件	識別子	補足説明
		更新ファイルの開発時とリリース時では異なる署名用の鍵と証明書を使用	UPC03	• セキュアな更新ファイルの作成において署名付与は最も重要なプロセスであり、攻撃者による更新ファイルの改ざんを防ぐため慎重に設計・実装される必要がある。 • ロールバック攻撃を防ぐため、更新ファイルにはシーケンシャルなバージョン番号の付与が推奨される。 • 開発環境から漏洩した鍵と証明書が悪用されるのを防ぐため、開発時とリリース時で分けることが推奨される。 • 適切な使用期間で暗号鍵を使用開始し、廃棄するためのスケジューリング機能の実装が推奨される。 • 公開鍵基盤による署名は CA の信頼性をセキュリティ基盤としているため、利用する CA は慎重に吟味する必要がある。
		製造出荷される機器がリリース時の鍵のみ受け入れることを確認	UPC04	
		脆弱なパッチや漏洩した鍵の廃棄プロセスをあらかじめ設計し、機器がアップデートを実行する際は事前に廃棄情報を確認できるようにする	UPC05	
		鍵のスケジューリング（廃棄・失効に合わせた更新プロセス）を設計し、機器が鍵を更新できるようにする	UPC06	
		適切な強度の署名鍵を選択する　（秘密鍵が危殆化した場合に備え、順番付きリストもしくは階層構造をもつ公開鍵の利用）	UPC07	
		署名プロセスで信頼を置く対象（CA など）を慎重に吟味する	UPC08	
	セキュアな開発			• 攻撃者によるハッキング（マルウェア・標的型攻撃など）を受けて設計情報などが漏洩するのを防ぐため、セキュアな開発環境と開発プロセスの整備、スタッフのセキュリティ教育などが推奨される。
	B	セキュアな開発環境（SW/HW）・開発プロセス・開発スタッフを整備	UPC09	
		リリース前にセキュリティ要件適合性チェックを実施　（コード脆弱性解析など）	UPC10	
	C	リリース時の署名生成環境の保護（署名用秘密鍵を HSM に保存、専用の隔離されたオフライン環境、厳重なアクセス制限、複数パーティによる認証の要求など）	UPC11	
アップデート配布	ロバストな配布			• 膨大な数の IoT 機器をスケーラブルに管理するために、自動ソフトウェア更新機能の実装が推奨される。特にコンシューマ向けなどの、顧客によるセキュアな管理が難しく製造者が一元的に管理するような IoT 機器においては自動更新のモデルが適している。 • 更新ファイルのダウンロードには通常大きな通信量が発生するため、ネットワークとサーバを圧迫しない仕組みの設計が推奨される。
	B	最新アップデートを広く普及させるため、機器がソフトウェア更新を自動で実行できる	UPD01	
		更新ファイルの通信によってネットワークとサーバの容量をオーバーさせないための仕組みを検討する　（ロードバランサーの追加、更新ファイルの小サイズ化など）	UPD02	
		更新ファイルサーバへのアクセス保護（ユーザ認証、通信の暗号化など）	UPD03	
		更新ファイルサーバの管理タスクを減らすため、既存の実績ある配信システムの採用を検討する	UPD04	

大分類	分類	セキュリティ要件	識別子	補足説明
		更新ファイルサーバから機器の自動更新のスケジュールを設定できる	UPD05	
		更新ファイルサーバまたは関連する配布機構へのサービス拒否攻撃の検知と防御	UPD06	
	C	更新ファイルサーバの通信鍵をハードウェアで保護できる　(HSM など)	UPD07	
		アップデートリクエスト承認のため、更新ファイルサーバが機器を個体認証できる	UPD08	
		機器の管理者が更新ファイルのインストール結果を確認するための追跡手段の用意	UPD09	
		更新ファイルのインストールに失敗した機器の管理者へのインストール結果の通知	UPD10	
		利用者からのアップデート操作に対して、管理者による操作の上書きを許可する	UPD11	
セキュリティ状態検知	サイバーセキュリティ状態の検知			• サイバーセキュリティ状態の検知は、セキュリティ攻撃の調査、不正使用の特定、運用上の特定問題の解決などの達成を支援する。 • サイバーセキュリティ状態は、IoT 機器の利用される文脈によって必要とされる情報や目標が変化する。IoT 機器内のイベントに関連したキャプチャ情報とログ記録を、IoT 機器の外部に保持されたレコードに保存する機能などは実装の一例として考えられる。また、外部の監視システムへの信号送信だけでなく、IoT 機器自身のインターフェースによる警報発令なども考えられる。
	A	機器が自身のサイバーセキュリティ状態を報告できる （運転状態、ウィルススキャン結果、ブート時の完全性チェック結果など、顧客にとって扱いやすい形式で表現されたセキュリティ情報が対象）	SSS01	
		機器が自身のサイバーセキュリティ状態が、想定された状態なのか、または劣化した状態なのかを識別できる	SSS02	
		権限エンティティにのみ閲覧を許可するため、機器の状態インジケータへのアクセスを機器が制限できる	SSS03	
		機器のサイバーセキュリティ状態の整備に責任を持つエンティティ以外には、サイバーセキュリティ状態の編集を禁止する	SSS04	
		機器のサイバーセキュリティ状態の情報を他の機器（イベント/状態のログサーバーなど）に提供できる　（インシデント分析活動の支援）	SSS05	
	ソフトウェア構成の管理			• 複数のモジュールやソフトウェアの組み合わせとして構成される IoT 機器において、各ファームウェア／ソフトウェアのバージョン情報やパッチ／更新の適用状態を管理
	B	機器が自身のソフトウェアのバージョンや更新ファイルの適用状態を設定管理する能力をもつ。または外部の管理システムとインターフェースで通信することで同様の能力を得られる	SSS06	

大分類	分類	セキュリティ要件	識別子	補足説明
		機器が外部からの脆弱性スキャンに対応できる能力をもつ。または、組み込みの脆弱性検知と報告の能力をもつ（ファームウェア／ソフトウェアのバージョンを検証・管理するための計測ブートや、検証結果の報告など）	SSS07	することは、脆弱性の有無を検知するために重要な機能である。 • 外部からの脆弱性スキャンに対して報告の正当性を保証するためには、IoT 機器内に信頼の基盤となる HW（耐タンパー性セキュアコンポーネントなど）が必要になる。
HW ライフサイクル	セキュアな製造プロセス			• ソフトウェア開発時に使用された鍵や証明書は流出による悪用のリスクがあるため、リリース用の鍵と証明書のみを書き込む必要がある。 • 製造時の機密情報の書き込みにおける漏洩や改ざんなどのリスクを防ぐためには、セキュリティ工場の整備が必要となる（セキュリティゲートの設置、入退場の厳格管理、工場施設の機密性強化、ネットワークの隔離、機密情報管理用サーバの設置など）。 • セキュア工場の整備にコストをかけられない場合、耐タンパー性セキュアコンポーネントの利用によって機密情報の書き込みと管理を外部に委託することも可能（外部業者によって機密情報が書き込まれた耐タンパー性セキュアコンポーネントを調達して組み込み、セキュアでない工場での機密情報の書き込みを避ける、など）。
	B	製造時の機器への書き込みにおいては、ソフトウェア開発時に使用した鍵と証明書を使用せず、必ずリリース用の鍵と証明書のみを機器に書き込む	HLC01	
	C	製造時の機密情報の書込み環境の保護（セキュア工場の整備、または耐タンパー性セキュアコンポーネントを利用した外部委託など）	HLC02	
	セキュアな設置プロセス			• 出荷後に納入先まで配送される過程において、機器内の機密情報の解析・改ざん、もしくは盗聴用チップの埋込などを実施される危険性を防ぐため、適切な追跡管理や身元確認などの対策が必要となる。製造在庫をストックする倉庫がある場合には、倉庫のセキュリティにも同様に対策が必要。
	C	機器が配送される過程における改ざんとすり替えの防止 （出荷から荷受けまでの追跡管理、納入業者の身元確認、開封防止シールなど）	HLC03	
		機器が設置される際の初期設定におけるセキュリティ保護 （設定用端末のウィルス検査、設置作業員のセキュリティ教育など）	HLC04	

大分類	分類	セキュリティ要件	識別子	補足説明
		機器が設置される際の初期設定の自動化 （リモートプロピジョニング機能など）	HLC05	• 開封防止シールなどによって耐タンパー性を確保する対策も有効である。 • 設置時の初期設定は機器のセキュリティにおいてクリティカルなポイントであり、様々な攻撃（感染マルウェアによる盗聴、電磁波によるテンペスト攻撃、ソーシャルエンジニアリングなど）の危険性が高いため、適切な対策が必要（設定 PC のウィルス検査や設定スタッフのセキュリティ教育など）となる。 • 機器自身がリモートの管理サーバにアクセスして自動で初期設定を実施する機能（リモートプロピジョニング）も有効である。
	セキュアな再利用プロセス			• 機密情報と個人情報が漏洩するリスクを防ぐため、適切な初期化機能が必要。 • 適切な再利用プロセスが実施されなかった場合（初期化の失敗など）の予防策として、保護すべき情報をあらかじめ耐タンパー性セキュアコンポーネントに保存し、漏洩を防ぐ。
	C	機器が再利用される際の機密情報と個人情報の保護 （初期化機能、耐タンパー性セキュアコンポーネントの利用など）	HLC06	
	セキュアな廃棄プロセス			• 機密情報と個人情報が漏洩するリスクや廃棄済み機器が再利用されるリスクを防ぐため、適切な初期化機能と動作停止機能が必要。 • 適切な廃棄プロセスが実施されなかった場合（完全消去に失敗、廃棄業者の横流しなど）の予防策として、保護すべき情報をあらかじめ耐タンパー性をもつセキュアメモリやセキュアコンポーネントに保存し、漏洩を防ぐ。
	C	機器が廃棄される際の機密情報と個人情報の保護 （初期化機能、動作停止機能、耐タンパー性セキュアコンポーネントの利用など）	HLC07	

4. 顧客への情報提供

顧客が「ソフトウェア更新」を安全に運用するためには、製造者は前章のセキュリティ要件を満たすだけでは十分ではない。製造者は、IoT 機器のセキュリティ性能や更新サービスの提供条件など、必要な情報を顧客へ確実に提供する必要がある。本章では、「ソフトウェア更新」に関する顧客とのコミュニケーションについて製造者が検討すべき事項を一覧として提示する。

4.1 顧客とのコミュニケーション方法

サイバーセキュリティ情報の提供においては、様々な顧客で異なる、それぞれの需要やリソースに応じたアプローチが必要となる。顧客とのコミュニケーション方法を決める際に検討すべき事項を以下に列挙する。

(1) 使用する用語

たとえば、機器の利用がホーム用途の場合には利用者の技術的知識が少ないため使用できる用語が限定されるが、IT セキュリティに知見のあるシステム管理者による利用が想定される場合には CVE 番号などの専門用語の使用が望ましい。

(2) 情報量

情報量が多すぎる場合、顧客が必要な情報を探すのを妨げることになるが、情報量が少ないことも望ましくない。ただし、公開することで負の影響が予想されるような情報（対処できていない新しい脆弱性など）の場合には、その限りでない。

(3) 情報提供の場所と手段

１つまたは複数の物理的／論理的な提供場所。例：ユーザマニュアル、サービス利用規約、その他の文書、ウェブサイト、E メール、IoT 機器自身とその関連アプリ、など。顧客が必要なときにすぐアクセスできると利便性が高い。

(4) 情報の完全性を検証する手段

いくつかの提供方法（E メールなど）においては、提供された情報が正当なものかどうか顧客が判定したい場合がある（ソーシャルエンジニアリングへの対策）。

(5) 顧客から製造者への通信手段

必要な情報（利用機器のアップデートなど）を確認するための問い合わせや、問題事項（脆弱性など）についての報告など、顧客から製造者への通信の需要があり得る。顧客から製造者への通信チャンネルは、顧客やその他（セキュリティ調査員など）からの利用を保証するため、機能・可用性・有効性について製造者によってテストされる必要がある。

4.2 コミュニケーション内容の例

製造者が顧客に伝達する情報の例を以下に列挙する。

(1) サイバーセキュリティのリスクに関する前提事項

サイバーセキュリティのリスクに関して、製造者の想定との差異について顧客が把握するため、以下のような情報が有益である。

① 想定する顧客

② 想定する利用方法（特定の利用方法や、特定のシステム内での利用などの依存要素）

③ 想定利用環境（公衆での利用可否、他の機器との連携の必要性、ネットワークの帯域やレイテンシなど）

④ 製造者と顧客、その他の責任の分担（各セキュリティ機能やタスクに対して責任をもつパーティの明確化）

(2) 想定しているサポート期間とライフスパン

機器のサポート期間やライフスパンについての情報提供は、顧客が機器のライフサイクル全体を通したサイバーセキュリティリスクへの対策を計画するうえで有益である。以下のような情報の提供が考えられる。

① 機器のサポート期間の長さ（更新ファイルや技術サポートの提供期間）

② 機器の保守期限と廃棄プロセス（保守終了の半年前の通知など）

③ サポート終了時や保守終了時においても機器が保持できる機能

④ セキュリティ問題の可能性（ソフトウェア脆弱性など）について顧客が製造者に報告する手段

例）電話番号、メアド、Web フォームなど。

⑤ 公式サポート終了後でもセキュリティを維持する手段

例）製造者が廃業した場合に製品コードをオープンソースとして公開し、コミュニティにサポートを託すなど。

(3) 機器の構成と性能

機器のハードウェア、ソフトウェア、サービス、データ型などの情報提供は、顧客が機器のサイバーセキュリティをよく理解して管理するうえで有益である（特に、顧客自身が機器のサイバーセキュリティ管理を実質的に担当する場合）。以下のような情報の提供が考えられる。

① 一般的サイバーセキュリティについて顧客が必要とする情報（インストール、ハードニングを含む設定、利用、管理、メンテナンス、廃棄など）

例）安全にネットワークにつなぐ方法、設定オプションがサイバーセキュリティにどのような影響を与えるか、既知の危険な利用方法の警告など。

② セキュリティ設定をデフォルトよりも厳しくした場合の潜在的影響

③ 機器の内部ソフトウェアに関連するインベントリ関連情報（バージョン、パッチ状態、既知の脆弱性など）と、顧客が最新インベントリへのアクセスする手段

④ 機器のハードウェア、ソフトウェア、サービスに関して顧客が必要とする情報

例）機器の IoT ソフトウェアの開発元、機器のプロセッサの製造元、機器が使用するクラウドベースサービスの提供者など

⑤　顧客が適切で安全な運用をするために必要な機器の特性情報とその提供方法

例）Web サイト、または標準化された機器間通信プロトコル（機器の利用意図などの情報は機器自身に提供させた方がスケーラブル）など。

⑥　機器が実施可能な機能（サイバーセキュリティ以外も含む）

例）遠隔システムへのデータ転送、マイク、カメラによる録音、録画など。

⑦　機器が収集するデータ型と、各データにアクセス可能なパーティの識別

例）クラウドに保存された位置情報や音声コマンドなどのデータが他の目的で使用される可能性について顧客が把握できるか、など。

⑧　機器に対してアクセス権または制御権をもつすべてのパーティの識別（製造者含む）

例）製造者の代理として、第三者が機器のソフトウェアや設定に対してリモート更新などの技術サポートを提供する場合、など。

(4) ソフトウェア更新

①　アップデートの提供時期（定期的なのか単発的なのか）

②　どのようなときにアップデートが発行されるか（不具合の修正、脆弱性への対策など）

③　アップデートの配信方法、更新／インストール通知の有無

④　アップデートの実行に責任をもつエンティティ（顧客、製造者、第三者）と　顧客による委任の可否

⑤　顧客がアップデートの検証と信頼性証明をする方法（ハッシュ比較、コード署名検証、または製造者提供ソフトウェアによる検証と信頼性証明など）

⑥　各アップデートに提供されるべき情報（エラー修正、機能変更・追加などの更新内容、インストールによって起こりうる影響など）

(5) 再利用と廃棄

①　他者に機器の所有権を譲渡する場合、機器内のユーザや設定情報または関連システム（機器に利用されるクラウドサービスなど）を相手にアクセスさせないために必要な手順

②　機器を使用不可能な状態にする方法

(6) サイバーセキュリティ性能

①　提供可能な技術的サイバーセキュリティ性能（機器自身、または関連機器、もしくは製造者のサービスやシステムにより提供される）

②　製造者（または代理となる第三者）のサービスによる非技術的なサイバーセキュリティ性能（顧客にとって有益な情報）

③　顧客自身による提供が必要または検討されるサイバーセキュリティ性能（インターネットからの直接アクセスを防ぐためのネットワークベースのセキュリティ制御や、機器の設定や実装が要件に適合しているかの監査の実施など）

④　各サイバーセキュリティ性能のリスクへの影響

5. 参考文献

(1) NIST

https://csrc.nist.gov/publications/detail/nistir/8259/final

https://csrc.nist.gov/publications/detail/nistir/8228/final

https://csrc.nist.gov/publications/detail/nistir/8267/draft

https://csrc.nist.gov/publications/detail/sp/800-193/final

(2) TCG

https://trustedcomputinggroup.org/resource/tcg-guidance-for-secure-update-of-software-and-firmware-on-embedded-systems/

(3) IETF

https://datatracker.ietf.org/doc/draft-ietf-suit-architecture/

(4) CPSF

https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

(5) IPA

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

https://www.ipa.go.jp/sec/reports/20180322.html

添付 A.　耐タンパー性セキュアコンポーネントを利用した実装例

「耐タンパー性セキュアコンポーネント」とは、外部からの物理的な手段による攻撃に対して耐性をもち、機器の機密情報の保存・管理や暗号演算などの機能をもつセキュアな構成要素である。具体的には、SE や TPM などのセキュリティチップを指し、提供形態は組み込み用のチップ形状や、交換可能なカード形状などが存在する。

本章では、IoT 機器の「ソフトウェア更新」に対して「耐タンパー性セキュアコンポーネント」を利用した実装例を紹介する。

A.1　利用のメリット

本文書で提示したリスク分析結果（表 2）とセキュリティ要件（表 3）のうち、「耐タンパー性セキュアコンポーネント」によって対応が可能な項目は、以下の表 4 に示す 8 項目である。

表 4「耐タンパー性セキュアコンポーネント」によって対応が可能なリスク分析結果とセキュリティ要件

項目	リスク分析結果（表 2 より抜粋）			セキュリティ要件（表 3 より抜粋）
	ライフサイクル	脅威	脆弱性	
①	配布／運用	不正な更新ファイルをインストールすることにより、IoT 機器の可用性とセキュリティが損なわれる	更新ファイルの正当性検証などで利用される暗号演算の保護が不十分	セキュアコンポーネントによる暗号演算（更新ファイルの署名検証・復号など）
②		ソフトウェア更新に失敗した状態で放置され、IoT 機器の可用性とセキュリティが損なわれる	ソフトウェア更新の失敗を検知する機能がない	更新失敗の検知（セキュアコンポーネントによる検証も可）
③		更新エンジンが改ざんされることで不正な更新ファイルのインストールが可能となり、不正に利用される	更新エンジンがハードウェアレベルで保護されていない	起点となる更新エンジンのハードウェアによる保護（耐タンパー性セキュアコンポーネントなど）
④		IoT 機器内のクリティカルなコードや鍵が漏洩し、不正に利用される	クリティカルなコードと鍵がハードウェアレベルで保護されていない	ハードウェアによるクリティカルなコードと鍵の保護（耐タンパー性セキュアコンポーネントなど）
⑤		更新エンジンが改ざんされることで不正な更新ファイルのインストールが可能となり、不正に利用される	更新エンジンの検証と報告の機能がハードウェアレベルで保護されていない	ハードウェアによる更新エンジンと報告エンジンの保護（耐タンパー性セキュアコンポーネントなど）
⑥	再利用／廃棄	再利用フェーズにおける機密情報、個人情報の漏洩	機密情報、個人情報の初期化機能、または耐タンパー性の不足	再利用時の機密情報と個人情報の保護（初期化機能、耐タンパー性セキュアコンポーネントの利用など）

⑦		廃棄フェーズにおける機密情報、個人情報の漏洩	機密情報、個人情報の初期化機能、機器の動作停止機能、または耐タンパー性の不足	廃棄時の機密情報と個人情報の保護 （初期化機能、動作停止機能、耐タンパー性セキュアコンポーネントの利用など）
⑧	製造	製造環境における鍵や証明書情報が漏洩	機密情報を書き込む製造環境のセキュリティ対策が不十分（入退室管理、ネットワーク隔離、生産管理サーバのセキュリティ対策など）	製造時の機密情報の書込み環境の保護 （セキュリティ工場の整備、または耐タンパー性セキュアコンポーネントを利用した外部委託など）

上記のうち、⑧とそれ以外ではセキュリティ要件への対応方法が異なっているため、以下に説明する。

A) IoT 機器が「耐タンパー性セキュアコンポーネント」の機能（セキュアな暗号演算、耐タンパー性など）を利用することでセキュリティ要件に対応できる。(①～⑦)

B) IoT 機器が「耐タンパー性セキュアコンポーネント」の機能を利用していることを前提にしつつ、「耐タンパー性セキュアコンポーネント」をセキュアな記憶媒体としても利用し、機密情報の書き込みと管理を外部業者やチップメーカー（セキュアな環境をもつ）に委託することによってセキュリティ要件に対応できる。(⑧)

セキュアな IoT 機器を製造する上で、⑧に対応するようなセキュアな書き込み環境（セキュア工場）を製造者が自前で整備することは多大なコスト（物理的にセキュアな製造サイトの準備、厳格な入退室管理システムの導入、他の製造ラインから隔離されたサーバとネットワークの構築、機密情報を扱う人員のセキュリティ教育など）が必要となるため、上記 B のような「耐タンパー性セキュアコンポーネント」を利用した書き込み工程のアウトソーシングは、コストの面で効果的である。

A.2 利用における検討事項

IoT 機器の要件に適合した「耐タンパー性セキュアコンポーネント」の選定においては、以下のような項目が検討事項となる。

(1) 提供形態（IC カード、組み込み用チップなど）
(2) 通信インターフェース（ISO/IEC7816、SPI、I2C など）
(3) プロセッサの処理性能
(4) メモリのサイズと書き換え寿命
(5) サポートする暗号機能の種類
(6) 取得済みのセキュリティ認証
(7) 電気特性（対応する電圧、消費電力など）

(8)　熱や静電気、衝撃などの物理耐性

(9)　「耐タンパー性セキュアコンポーネント」のベンダーが提供するサポート（開発支援など）

(10)　「耐タンパー性セキュアコンポーネント」のベンダーが提供するサービス（鍵や発行データの生成と管理、書き込みの代行など）

「耐タンパー性セキュアコンポーネント」は高度なセキュリティをもち専門性の高い部材であるため、選定にあたっては IoT 機器の要件をベンダーに共有して、適切なサポートを得ることが推奨される。また、「耐タンパー性セキュアコンポーネント」のベンダーはセキュア工場を保有していることが多いため、前節の B のような書き込み工程のアウトソーシングの委託先としても合理的である。

A.3　処理フローの例

発行データと署名用公開鍵の生成と書き込み、更新ファイルの作成を「耐タンパー性セキュアコンポーネント」のベンダーに外部委託（発行者と署名者の役割をベンダーに委託）した場合の処理フローの例を以下の図 11～13 に示す（図 11～13 の発行者/署名者がベンダーに相当）。2.5 節の「産業用 IoT 機器を想定した高度な処理フロー」との差分を赤枠で示した。

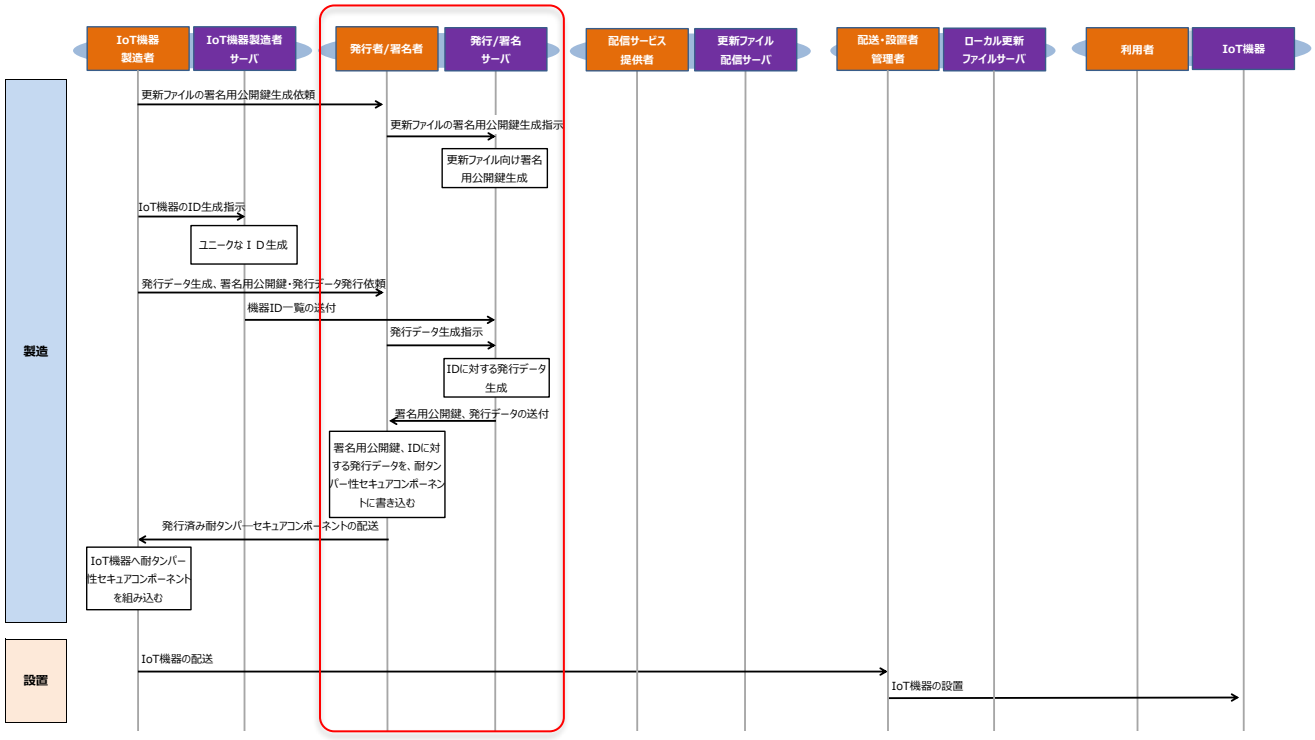

図 11　製造から設置フェーズまでの処理フロー（耐タンパー性セキュアコンポーネントの利用例）

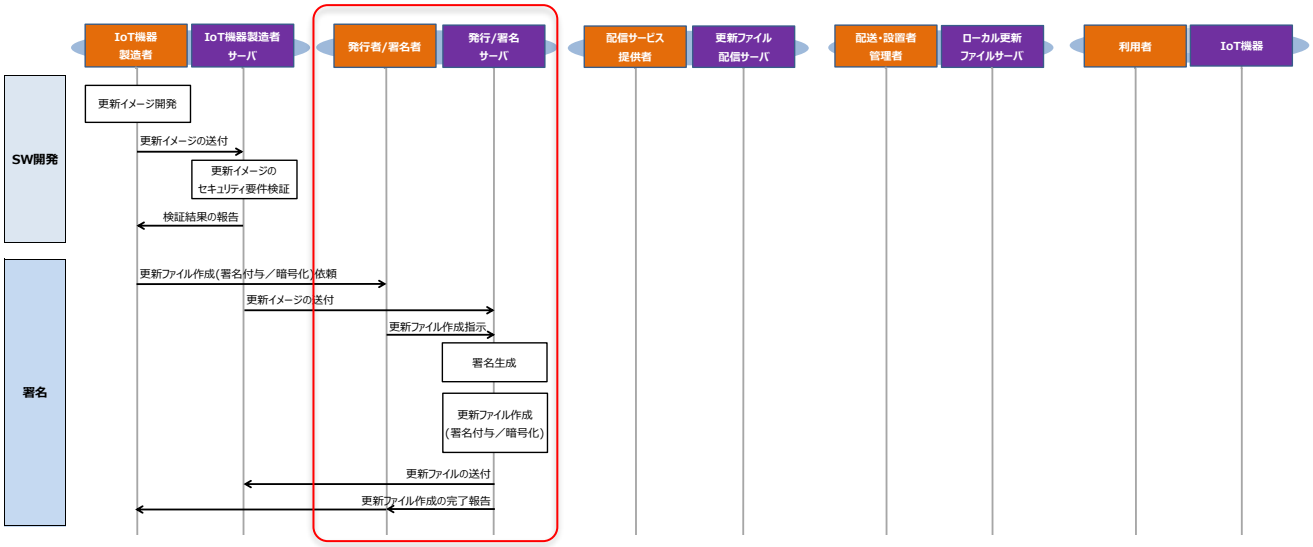

図 12　配布から運用フェーズまでの処理フロー（耐タンパー性セキュアコンポーネントの利用例）

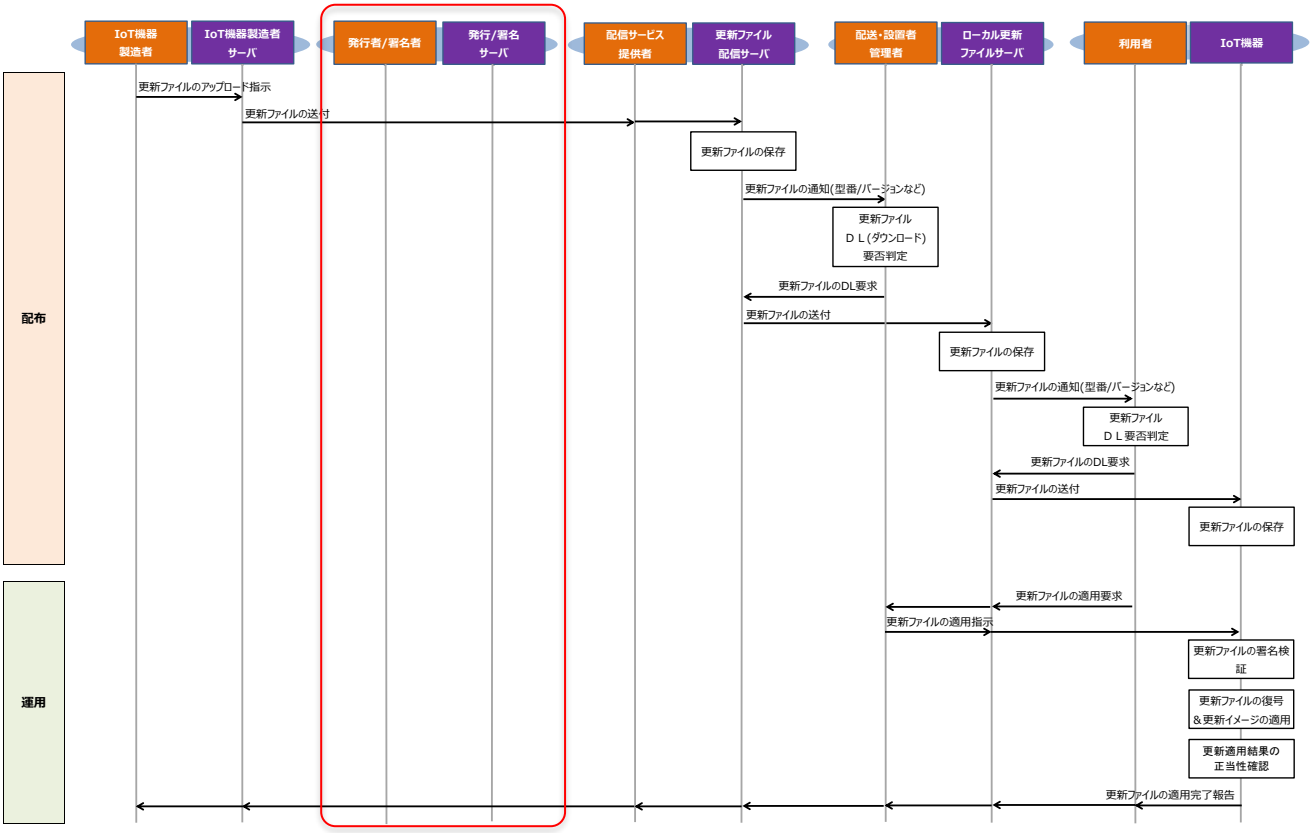

図 13　配布から運用フェーズまでの処理フロー（耐タンパー性セキュアコンポーネントの利用例）

添付 B.　CPSF との対応表

表 5 CPSF との対応表

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
3.1	資産管理	CPS.AM-1	・システムを構成するハードウェ ア、ソフトウェア及びその管理情報(例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報)の一覧を作成し、適切に管理する。)	STS01 STS02 STS03 ORG05 ORG08
		CPS.AM-2	・自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。	STS03
		CPS.AM-3	・重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。	STS03
		CPS.AM-4	・組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。	ORG03 ORG04 ORG05
		CPS.AM-5	・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	ORG03 ORG04 ORG05 ORG08
		CPS.AM-6	・リソース（例：モノ、、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	ORG05
		CPS.AM-7	・自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。	ORG05
3.2	ビジネス環境	CPS.BE-1	・サプライチェーンにおいて、自組織が担う役割を特定し共有する。	なし
		CPS.BE-2	・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者(サプライヤー、第三者プロバイダ等を含む)に共有する。	ORG05
		CPS.BE-3	・自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	なし
3.3	ガバナンス	CPS.GV-1	・セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	ORG05

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
		CPS.GV-2	・個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。	ORG05
		CPS.GV-3	・各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。	ORG05
		CPS.GV-4	・セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	ORG05
3.4	リスク評価	CPS.RA-1	・自組織の資産の脆弱性を特定し、対応する資産とともに一覧を文書化する。	ORG05
		CPS.RA-2	・セキュリティ対策組織(SOC/CSIRT)は、組織の内部及び外部の情報源(内部テスト、セキュリティ情報、セキュリティ研究者等)から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	ORG01 ORG04 ORG05
		CPS.RA-3	・自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	ORG05
		CPS.RA-4	・構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。	ORG02 ORG04 ORG05 UPC09 UPC10
			・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	ORG02 ORG04 ORG05
		CPS.RA-5	・リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	ORG01 ORG02
		CPS.RA-6	・リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。	ORG02 ORG04 ORG05
			・IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	ORG02 ORG04 ORG05

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
3.5	リスク管理戦略	CPS.RM-1	・自組織内におけるセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織(例：業務委託先)の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	ORG04 ORG05
		CPS.RM-2	・リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	なし
3.6	サプライチェーンリスク管理	CPS.SC-1	・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	なし
		CPS.SC-2	・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	ORG05
		CPS.SC-3	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	ORG05
		CPS.SC-4	・外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。	ORG05
		CPS.SC-5	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	なし
		CPS.SC-6	・取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	ORG05
		CPS.SC-7	・取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	ORG05
		CPS.SC-8	・自組織が、関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	ORG05

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
		CPS.SC-9	・サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	ORG05
		CPS.SC-10	・取引先等の関係する他組織との契約が終了する際(例：契約期間の満了、サポートの終了)に実施すべきプロシージャを策定し、運用する。	ORG05 HLC07
		CPS.SC-11	・サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	ORG05
3.7	アイデンティティ管理、認証及びアクセス制御	CPS.AC-1	・承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	ORG05 ORG08 STS01 STS02 STS03
		CPS.AC-2	・IoT 機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	ORG05 ORG08 STS16
		CPS.AC-3	・無線接続先(ユーザーや IoT 機器、サーバ等)を正しく認証する。	STS12 STS15
		CPS.AC-4	・一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT 機器、サーバ等に対する不正ログインを防ぐ。	STS13
		CPS.AC-5	・職務及び責任範囲(例：ユーザー/システム管理者)を適切に分離する。	STS05 STS14
		CPS.AC-6	・特権を持つユーザのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式(例：二つ以上の認証機能を組み合わせた多要素認証)を採用する。)	ORG08
		CPS.AC-7	・データフロー制御ポリシーを定 め、それに従って適宜ネットワークを分離する (例：開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する。	STS07
		CPS.AC-8	・IoT 機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ(ヒト/モノ/システム等)との通信に限定する。	STS07 STS12

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
		CPS.AC-9	・IoT 機器やユーザによる構成要素(モノ/システム等)への論理的なアクセスを、取引のリスク(個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク)に見合う形で認証・認可する。	STS12 STS15
3.8	意識向上及びトレーニング	CPS.AT-1	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	ORG05
		CPS.AT-2	・自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練（トレーニング）、セキュリティ教育を実施し、その記録を管理する。	ORG05
		CPS.AT-3	・自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	ORG05
3.9	データセキュリティ	CPS.DS-1	・組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。	なし
		CPS.DS-2	・情報を適切な強度の方式で暗号化して保管する。	STS07
		CPS.DS-3	・IoT 機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	UPD03
		CPS.DS-4	・情報を送受信する際に、情報そのものを暗号化して送受信する。	STS07
		CPS.DS-5	・送受信データ、保管データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。	UPC03 UPC04 UPC06
		CPS.DS-6	・サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適 切に保護し、攻撃による影響を最小限にできるよう、構成要素にお いて十分なリソース(例：ヒト、モノ、システム)を確保する。	UPD06
		CPS.DS-7	・IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や 無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェ アの更新を行う。	UPD02

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
		CPS.DS-8	・保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	STS16 HLS02 UPE12 UPE15 UPE16 UPE17
		CPS.DS-9	・自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	UPD03 UPD08
		CPS.DS-10	・IoT 機器、サーバ等にて稼動するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。	UPE11 UPC01
		CPS.DS-11	・送受信・保管する情報に完全性チェックメカニズムを使用する。	STS07 UPE11 UPC01
		CPS.DS-12	・ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。	SSS06 SSS07
		CPS.DS-13	・IoT 機器やソフトウェアが正規品であることを定期的(起動時等)に確認する。	SSS06 SSS07
		CPS.DS-14	・データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する。	HLC01-07
		CPS.DS-15	・計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。	なし
3.10	情報を保護するためのプロセス及び手順	CPS.IP-1	・IoT 機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	STS03
		CPS.IP-2	・IoT 機器、サーバ等の導入後に、追加するソフトウェアを制限する。	STS04 STS05
		CPS.IP-3	・システムを管理するためのシステム開発ライフサイクルを導入する。	HLC01-07
		CPS.IP-4	・構成要素(IoT 機器、通信機器、回線等)に対し、定期的なシステムバックアップを実施し、テストする。	STS10
		CPS.IP-5	・無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	なし

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
		CPS.IP-6	・IoT 機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規 IoT 機器、サーバ等を一意に識別する ID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする。	HLC07
		CPS.IP-7	・セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視／測定／評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	ORG01 ORG05
		CPS.IP-8	・保護技術の有効性について、適切なパートナーとの間で情報を共有する。	なし
		CPS.IP-9	・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	ORG01 ORG05
		CPS.IP-10	・脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	ORG01 ORG05
3.11	保守	CPS.MA-1	・IoT 機器、サーバ等のセキュリティ上重要なアップデート等を、必要 なタイミングに管理されたツールを利用して適切に履歴を記録しつつ 実施する。	SSS06 SSS07
			・可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライ バ、アプリケーション)を一括して更新するリモートアップデートの仕組 みを備えた IoT 機器を導入する。	UPD01-11
		CPS.MA-2	・自組織の IoT 機器、サーバ等に対する遠隔保守を、適用先のモ ノ、システムのオーナー部門による承認を得 て、ログを記録し、不正ア クセスを防げる形で実施する。	UPE04
3.12	保護技術	CPS.PT-1	・セキュリティインシデントを適切に検知するため、監査記録／ログ記 録の対象を決定、文書化し、そうした記録を実施して、レビューする。	SSS06 SSS07
		CPS.PT-2	・IoT 機器、サーバ等の本体に対して、不要なネットワークポート、 USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバ等の機能を必要最小限とする。	STS11-16
		CPS.PT-3	・ネットワークにつながることを踏まえた安全性を実装する IoT 機器を導入する。	なし

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
3.13	異変とイベント	CPS.AE-1	・ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	ORG03 ORG05
		CPS.AE-2	・セキュリティ管理責任者を任命し、セキュリティ対策組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	ORG01 ORG02 ORG04 ORG05
		CPS.AE-3	・セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	ORG01 ORG02 ORG04 ORG05
		CPS.AE-4	・関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	ORG01 ORG02 ORG04 ORG05
		CPS.AE-5	・セキュリティ事象の危険度の判定基準を定める。	ORG02
3.14	セキュリティの継続的なモニタリング	CPS.CM-1	・組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	ORG01 ORG02 ORG04 ORG05
		CPS.CM-2	・IoT 機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	STS11-16
		CPS.CM-3	・指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。	なし
			・サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	ORG01 ORG02 SSS01-05
		CPS.CM-4	・サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	ORG01 ORG02 SSS01-05
		CPS.CM-5	・セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。	ORG01 ORG02 SSS01-05
		CPS.CM-6	・機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	ORG01 ORG02 SSS01-05

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
		CPS.CM-7	・自組織の管理している IoT 機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	ORG01 ORG02 SSS01-05
3.15	検知プロセス	CPS.DP-1	・セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知 における自組織とサービスプロバイダが担う役割と負う責任を明確 にする。	ORG01 ORG02
		CPS.DP-2	・監視業務では、地域毎に適用される法令、通達や業界標準等に準 拠して、セキュリティ事象を検知する。	ORG05
		CPS.DP-3	・監視業務として、セキュリティ事象を検知する機能が意図したとおり に動作するかどうかを定期的にテストし、妥当性を検証する。	ORG07
		CPS.DP-4	・セキュリティ事象の検知プロセスを継続的に改善する。	ORG01
3.16	対応計画	CPS.RP-1	・セキュリティインシデント発生後の対応の内容や優先順位、対策範 囲を明確にするため、インシデントを検知した後の組織／ヒト／モノ／ システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義 し、実装する。	ORG01 ORG02 ORG05
		CPS.RP-2	・セキュリティ運用プロセスにおいて、取引先等の関係する他組織と の連携について手順と役割分担を定め、運用する。	ORG01 ORG02 ORG05
		CPS.RP-3	・自然災害時における対応方針及び対応手順を定めている事業継続 計画又は緊急時対応計画の中にセキュリティインシデントを位置づ ける。	ORG01 ORG02 ORG05
		CPS.RP-4	・セキュリティインシデント発生時に被害を受けた設備にて生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ(製品)に対して適切な対応を行う。	ORG01 ORG02 ORG05
3.17	伝達	CPS.CO-1	・セキュリティインシデント発生後の情報公表時のルールを策定し、運用する。	ORG01 ORG02 ORG05
		CPS.CO-2	・事業継続計画又は緊急時対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	ORG01 ORG02 ORG05

サイバー・フィジカル・セキュリティ対策フレームワーク				本ガイドライン
章	カテゴリ	対応要件 ID	対応要件	セキュリティ要件 ID
		CPS.CO-3	・復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急時対応計画の中に位置づける。	ORG01 ORG02 ORG05
3.18	分析	CPS.AN-1	・セキュリティインシデントの全容と、推測される攻撃者の意図から、 自組織及び関係する他組織を含む社会全体への影響を把握する。	ORG01 ORG02 ORG05
		CPS.AN-2	・セキュリティインシデント発生後に、デジタルフォレンジックを実施 する。	ORG01 ORG02 ORG05
		CPS.AN-3	・検知されたセキュリティインシデントの情報は、セキュリティに関する 影響度の大小や侵入経路等で分類し、保管する。	ORG01 ORG02 ORG05
3.19	低減	CPS.MI-1	・セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。	ORG01 ORG02 ORG05
3.20	改善	CPS.IM-1	・セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。	ORG01 ORG02 ORG05
		CPS.IM-2	・セキュリティインシデントへの対応から教訓を導き出し、事業継続計画又は緊急時対応計画を継続的に改善する。	ORG01 ORG02 ORG05

以上