IoTセキュリティ手引書 小型機器編の解説

2023年3月1日

一般社団法人 セキュアIoTプラットフォーム協議会
仕様検討部会 座長
豊島 大朗

IoTセキュリティ手引書の目的

目的

本書では、IoT機器のセキュリティ対策で必要となる項目について、国際的な標準規格として、国際電気標準会議（IEC）が開発した産業システムにおけるセキュリティ規格であるIEC62443のうち産業機器開発向けの規格であるIEC62443-4と米国立標準技術研究所（NIST）が発行する「非連邦政府組織およびシステムにおける管理対象非機密情報（CUI）の保護」を目的としたSP800-171rev.2を基準に解釈と差異を取りまとめるものとしました。

本協議会では様々な分野の会員の方々から、それぞれの分野で必要と考えられるIoTセキュリティの課題と対応策について意見を収集してきました。これらの意見を集約するにあたり、網羅性の観点からIEC62443-4とSP800-171を基準とし、項目の検証を行いました。

CUI: Controlled Unclassified Information

小型機器編の目的

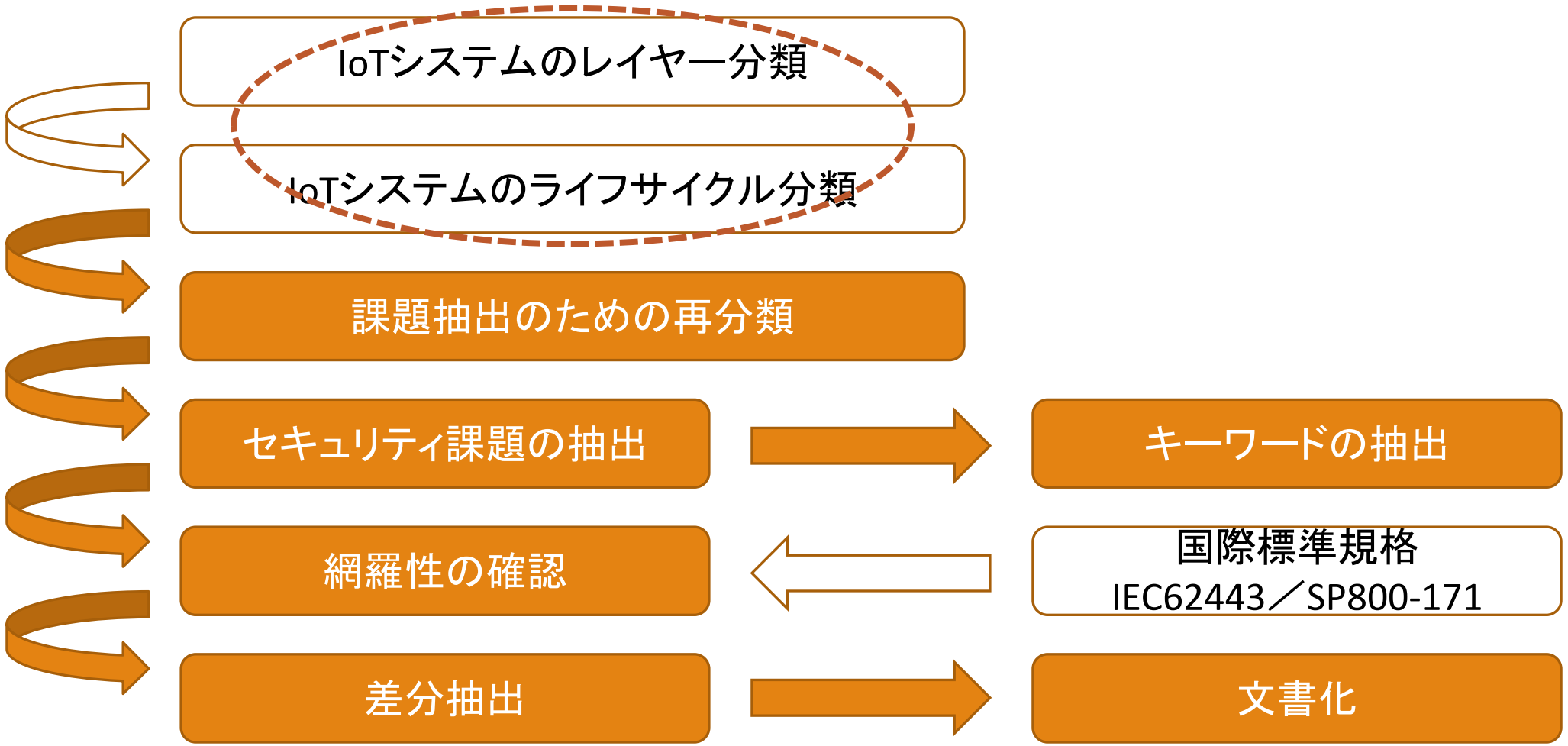
目的

　IoTセキュリティ手引書では、それぞれに実績を持たれた様々な企業からセキュリティ対策を収集し整理しました。これらは一つ一つが実績をもった有益な情報ではあります。一方で、レベル感に違いがあり実際の機器への適用に難があると考えました。

　そこで小型機器編では会員企業様が販売されている実際の機器をサンプルに置き、手引書を見直すことで実用性の高い手引き書へ進化させることを目的としています。

　このため、機器に関するドキュメントをお借りし、これの分析と解釈から始め手引書の該当する項目に対し、様々な改訂意見を集めました。

仕様検討部会　活動紹介　step 1



IoTセキュリティの検討モデル

2.1. IoT システムの階層モデル

IoT システムは「図 2-1　IoT セキュリティ総合対策モデル」の水平方向の分類に示されるように、サービス層／プラットフォーム層／ネットワーク層／デバイス層に分けられます。また、垂直方向の分類では設計・製造／サービス運用／廃棄という製品のライフサイクルにより分けられています。

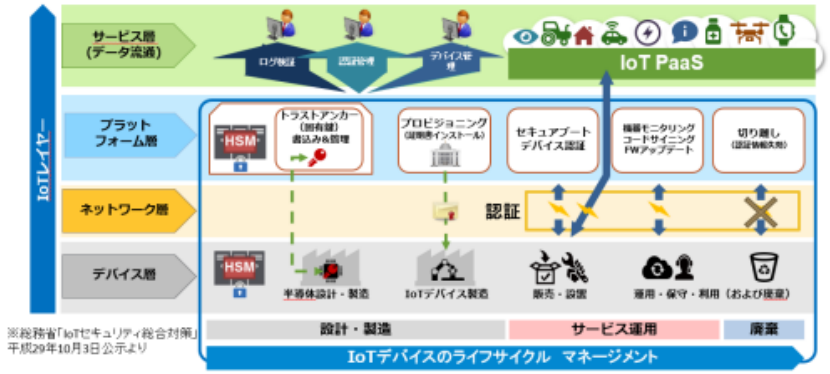


図 2-1　IoT セキュリティ総合対策モデル

機器開発における現実の役割分担を反映するため、垂直方向の分類となる、製品のライフサイクル（設計・製造／サービス運用／廃棄）を「企画」「設計」「開発」「製造」「量産」「運用」「廃棄」に細分化しました。

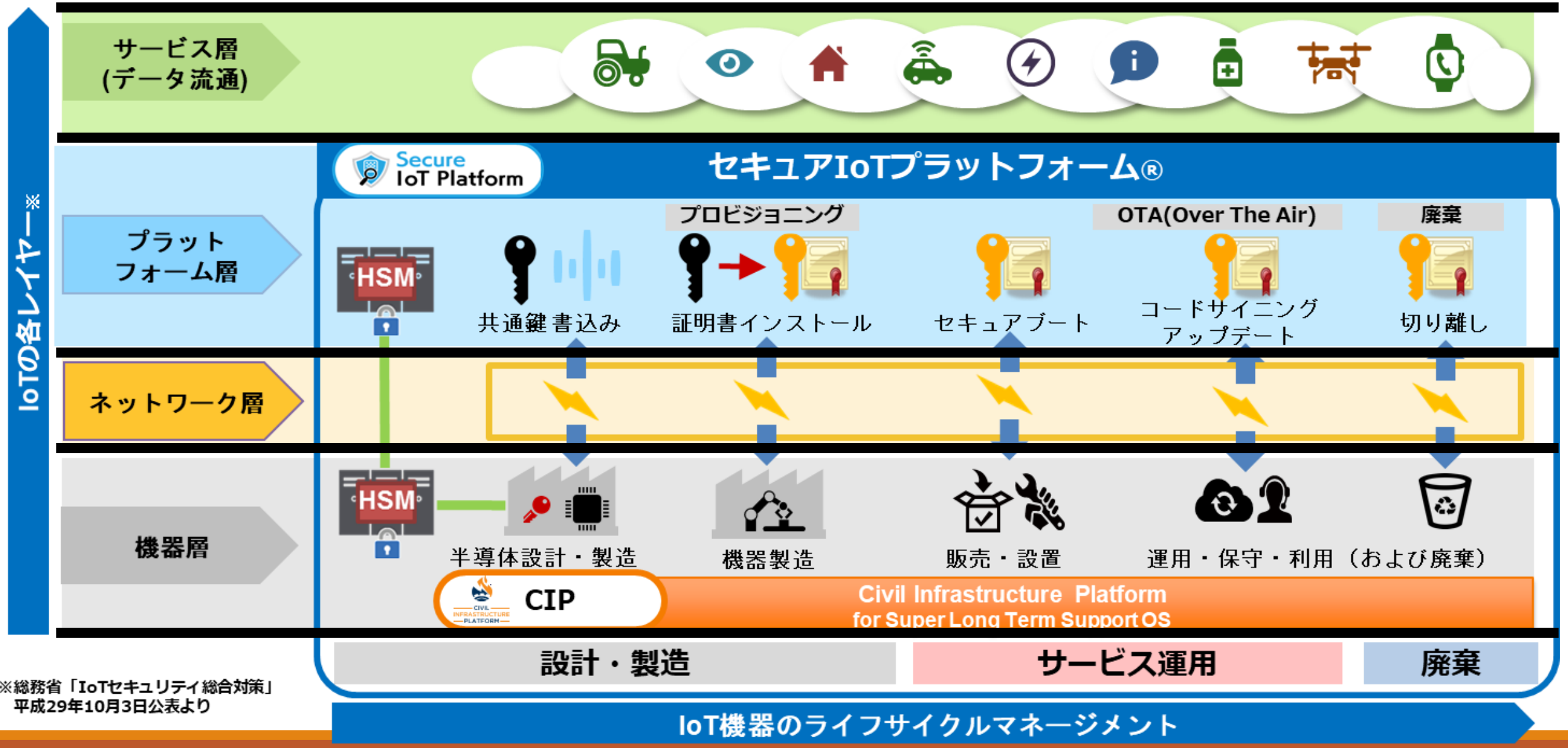
IoT セキュリティの検討モデル

IoT システムは一般的には、水平方向の分類としてサービス層／プラットフォーム層／ネットワーク層／デバイス層に分けられます。また、垂直方向の分類では設計・製造／サービス運用／廃棄という製品のライフサイクルにより分けられています。

機器開発における現実の役割分担を反映するため、垂直方向の分類となる、製品のライフサイクルを「企画」「設計」「開発」「製造」「量産」「運用」「廃棄」に細分化しそれぞれのフェーズでのセキュリティ対策を収集しました。

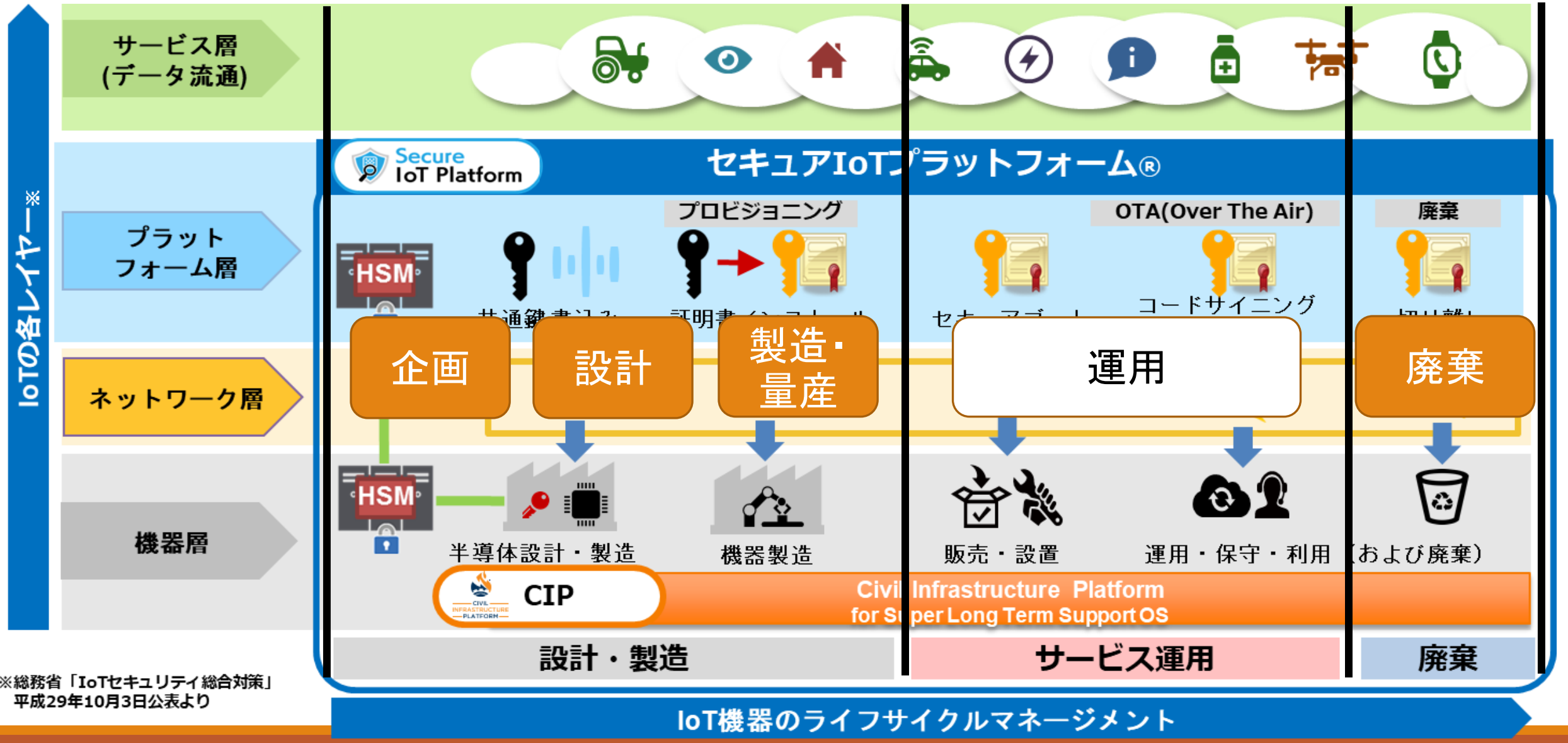
小型機器での検討を加味したところ「企画」「設計」「開発」「製造」「販売」「設置」「運用」「廃棄」へ再分類することとしました。

IoTシステムのレイヤー分類



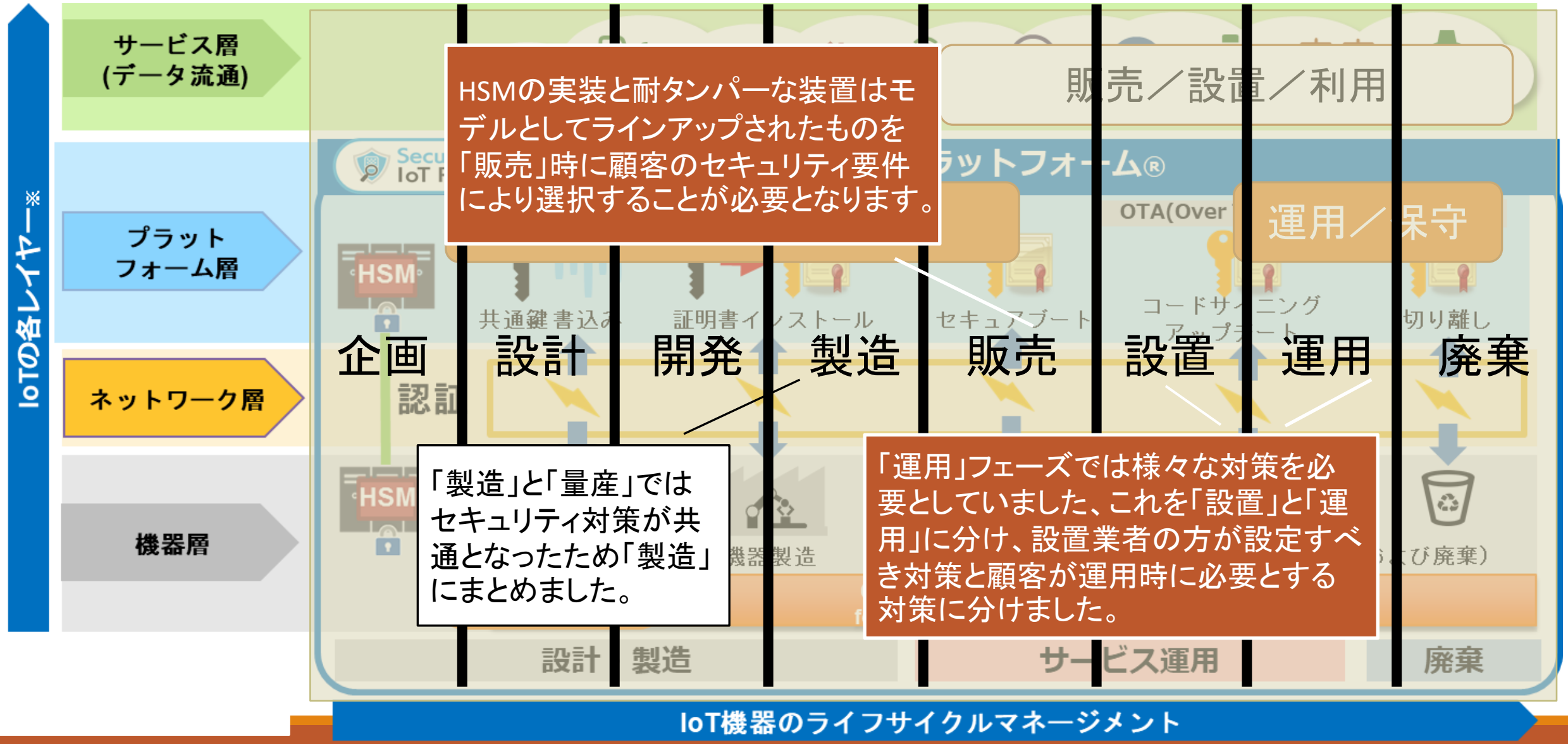
※総務省「IoTセキュリティ総合対策」
平成29年10月3日公表より

IoTシステムのレイヤー分類



※総務省「IoTセキュリティ総合対策」
平成29年10月3日公表より

IoTシステム（小型機器）のライフサイクル分類



販売時のセキュリティ課題

国際基準のセキュリティ要件

「コンポーネントが依存する認証子は、ハードウェアメカニズムによって保護されなければならない。」

※IEC62443-4-2　CR1.5　認証機構管理
　付則１　認証機のハードウェアセキュリティ　より

「支援インフラへの物理的アクセスを管理するために使用される管理策には、たとえば、鍵がかかった配線用ボックス、分離したまたは鍵がかかった予備ジャック、導管やケーブルトレイによる配線の保護、および、通信傍受センサーなどがある。

※SP800-171　3.10　物理的保護
　3.10.2　組織のシステムの物理的施設および支援インフラを保護し、監視する。　より

販売時の課題

左記の要件は、HSM（Hardware Security Module）の実装と鍵付きのケースによる保護で要件を満たすことができるが、装置が対応している場合、多くの場合セキュリティ対応モデルとして販売されており、顧客によるセキュリティ対応モデルの選択が対応策となってくる。

メーカ側としては、販売時に機器を導入するシステムがどのようなセキュリティ基準への対応が必要かを把握し、必要であればセキュリティ対応モデルを薦めることが重要となってくる。

設置時・運用時のセキュリティ課題

設置時のセキュリティ課題

　コンシューマ機器ではユーザが実施する場合もあるが、小型機器では設置業者が必要な設定を（最低限の範囲で）実施する場合が一般的である。ここでは、運用に耐えうる以下のようなセキュリティ機能が有効となるよう設定を合わせて実施する必要がある。

- CR1.2　ID認証
- CR1.5　初期認証機能
- CR1.7　パスワード強度
- CR1.11　認証ロック機能
- CR3.2　マルウェア対策

など・・・

※いずれも　IEC62443-4-2　のセキュリティ要件

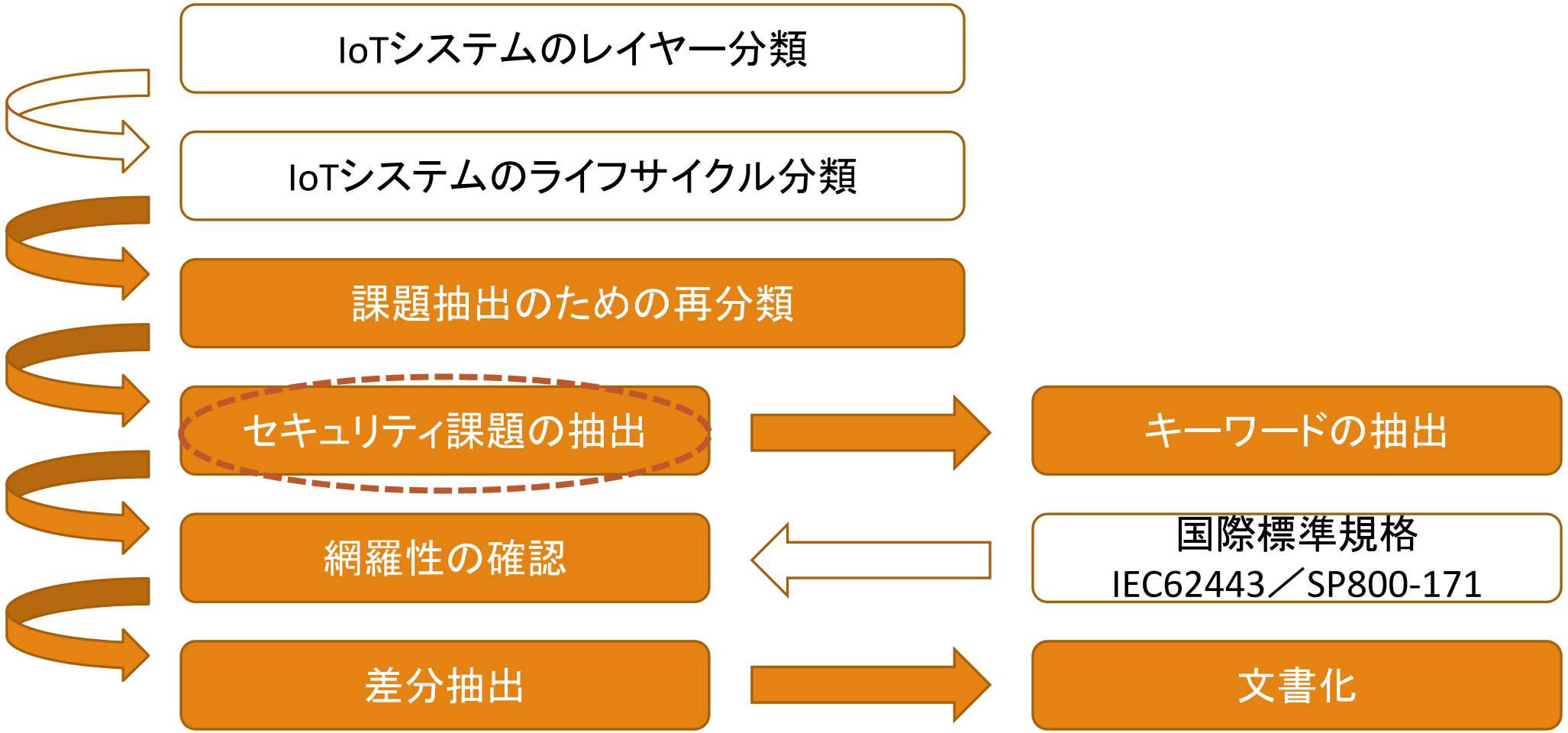
運用時のセキュリティ課題

　運用時には、設置時に設定したセキュリティ機能の有効性を維持する必要がある。
　例えばID認証であれば、移動や退職などにより担当者が変更となった場合、国際基準では旧担当者のIDを削除し新たな担当者にIDを発行することが望ましいとなっている。場合によってはユーザIDに有効期限を設け、これを超過し更新がない場合、認証ロック機能によって旧IDの不正利用へ対応することも可能ではあるが、タイムラグを考慮し不要なIDは速やかに削除することが望ましい。

「退職や異動などの人事処理中、およびその後において、CUI を含む組織のシステムが保護されていることを確実にする。」

※SP800-171　3.9　要員のセキュリティ　3.9.2　より

仕様検討部会　活動紹介　step 3

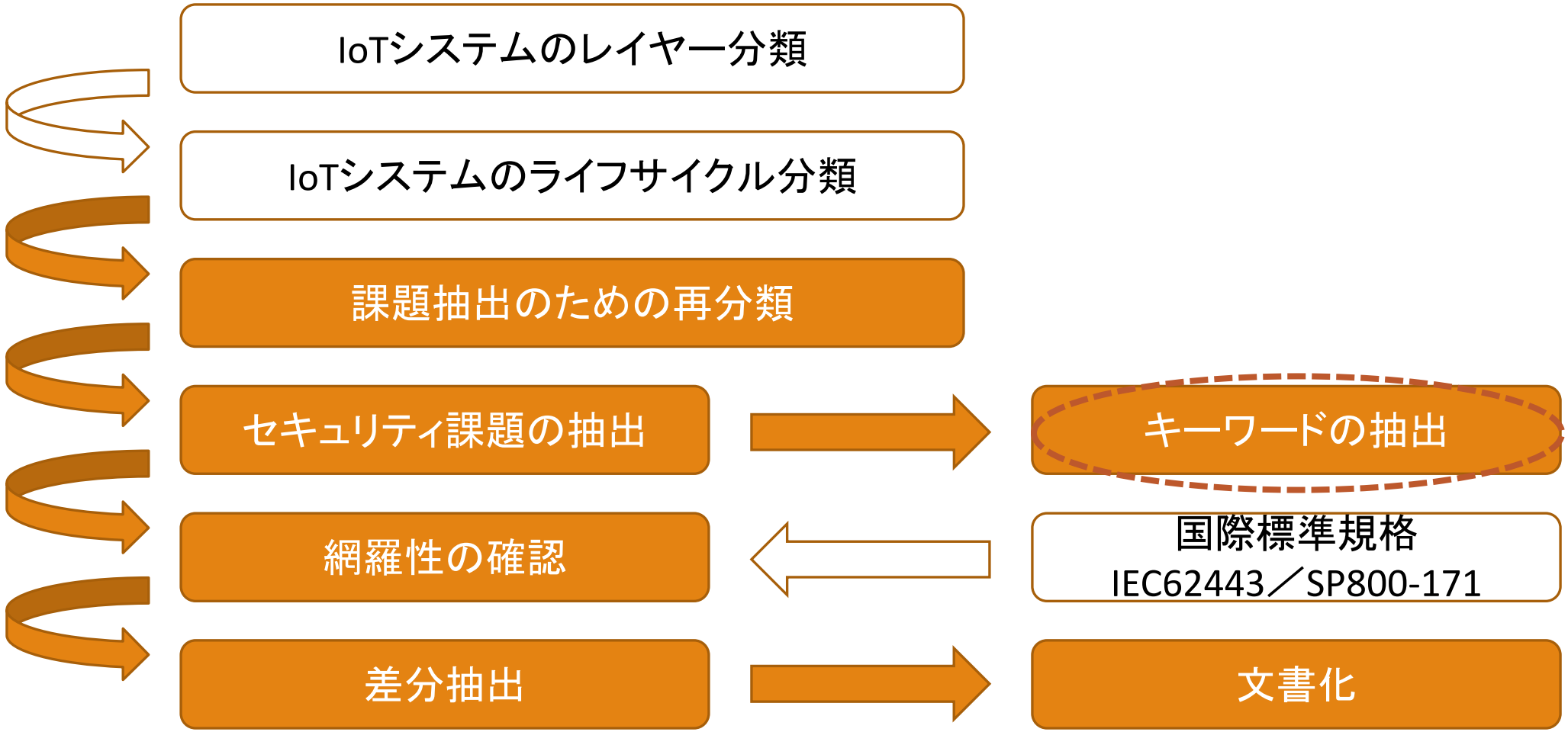


セキュリティ課題の抽出（S/W設計フェーズの例）

項番	脅威のカテゴリ		基準（対策）
1	セキュリティアーキテクチャ設計		セキュリティデータや処理をどのように守るか、破られた場合も被害を最小限にするための分散化をどのように考えるかをシステム全体のアーキテクチャとして設計する。
2	セキュリティ機能設計	ユーザ認証	一度設定をしておくと、パスワードを入力せずにログインできる自動ログインログファイルに改ざん防止、削除防止を施すこと
		アクセ	許可テーブルを引き、認証ユーザが許可を得ているコンテ
		セッシ	以上アイドル状態にあればセッションタイムアウトとし、セッションを破棄しログアウトすること。
		URLパラメータ	URL パラメータにユーザID やパスワードなどの秘密情報を格納しないこと。
		文字列処理	クロスサイトスクリプティング(XSS)対策。
		サイトデザイン	入力フォームのある画面はhttpsであること。
		ログ	ログファイルに改ざん防止、削除防止を施す。
3	セキュアコーディングガイド定義		セキュアなコーディングを行うためのルールや指針を定義。CERT CやCWEなど引用元を定義し、引用元がない場合は独自定義する。

課題自体に大きな変更はありませんが、文章の体裁とそれぞれの課題をどのフェーズで対策するかは再度見直しています。

仕様検討部会　活動紹介　step 4



IoTセキュリティ用語

4. 付録 A　IOT セキュリティ用語

- CDN
- 正式名称：Content Delivery Network、Web コンテンツを最適に配信する分散されたサーバープラットフォーム。エンドユーザーのコンテンツ要求ごとに、最適な位置の CDN サーバーをマップし、そのサーバーにキャッシュされたファイルを用いてリクエストに応答する。物理的に近いネットワークでエンドユーザーのリクエストに応答することで、コンテンツサーバーのトラフィックをオフロードしてウェブの応答性を高めることが出来る。
- CSRF
  - Cross-Site Request Forgeries の略、Web サイトの脆弱性をついた攻撃の一種
- DDoS 攻撃等
  - 正式名称：Distributed Denial of Service attack、トラフィックの増大によるネットワークの遅延、サーバやサイトへのアクセス不能等を目的とした攻撃手法のひとつであり、大量のマシンから 1 つのサービスに、一斉に DoS 攻撃を仕掛ける方法を指す。
- 協調分散型 DoS 攻撃
  - 攻撃者が大量のマシン(踏み台)を不正に乗っ取った上で、それらのマシンから一斉に DoS 攻撃をしかける攻撃手法
- 分散反射型 DoS 攻撃
  - 攻撃者が攻撃対象のマシンになりすまして大量のマシンに何らかのリクエストを一斉に送信する攻撃手法。攻撃対象のマシンはリクエストを受け取ったマシンから、大量の返答が集中することで、高負荷がかかることになる。

IoTセキュリティ用語

　課題抽出の過程で、それぞれの業界により微妙に用語の用法が異なる、もしくは専門用語がそもそも異なることに気づき、協議会各位の相互理解のために集めた課題の中から、キーワードを抜き出し、これにそれぞれ得意な分野について解説を入れていただき、IoTセキュリティ用語集として加えました。

　この用語集は付録Aの形で、本手引書に添付していましたが、ISOの慣習に習い「用語と定義」の章を設け、略語については移動します。

国際標準におけるIoTセキュリティ用語

SP 800-171 Revision 2　　非連邦政府のシステムおよび組織における管理対象非機密情報の保護

付属書 B

用語解説

共通用語および定義

付属書 B では、「SP 800-171」で使われるセキュリティに関する専門用語の定義を定める。本用語解説で特段の定義がある場合を除いて、本出版物で使われるすべての用語は、CNSS 指令 4009『米国国家情報保証用語解説』CNSS Instruction 4009, に含まれる定義に一致する。

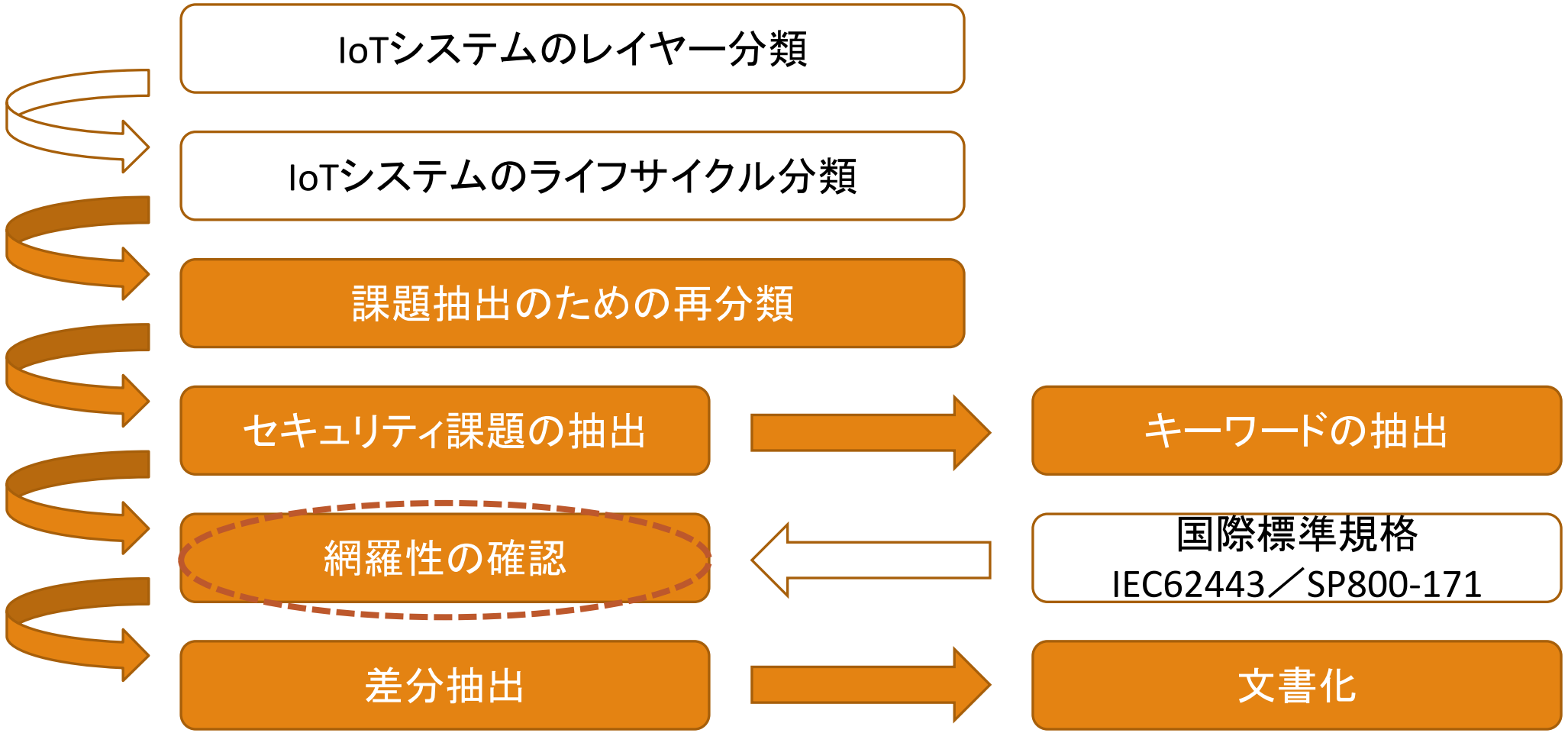
agency （政府機関） [OMB A-130]	行政機関または部局、軍事部局、連邦政府法人、連邦政府が管理する法人、または連邦政府の行政機関にあるその他の施設、または独立した規制機関。
assessment （評価）	*Security Control Assessment*（セキュリティ管理策評価）を参照のこと。
assessor	*Security Control Assessor*（セキュリティ管理策評価者）を

国際標準のセキュリティ用語

　左は「SP800-171rev.2」の「付属書 B」にある用語解説の章です。ここにあるように、IoTセキュリティに関する用語は独特のものがあり、同様に「IEC62443-4-2」では「3章 用語、定義、略語、頭字語、慣用句」となっており、これら用語の理解からはじめることで本文を読まれた時の理解が進むと思います。

　特に「SP800-171」ではCUI（Controlled Unclassified Information）情報を取り扱う場合の標準となっており、日本語では「管理対象非機密情報」と訳されていますが、これは同標準のもととなっている「SP800-53」が「Federal Information」日本語では「連邦政府情報」のセキュリティ対策の基準であるため、連邦政府情報から見ると非機密情報でありながら管理対象となる情報を指しています。

仕様検討部会　活動紹介　step 5



仕様検討部会　活動紹介　new steps


セキュア IoT プラットフォーム協議会

IOT セキュリティ手引書

小型機器編

セキュリティ仕様検討部会

2022 年 6 月 15 日　版

2023 年 3 月 1 日　改訂

手引書改訂

本書では、国際標準として IEC62443 を活用しました。2021年度では国際標準として米国のセキュリティ標準規格である NIST SP800 に目を向け、特に SP800-171 を中心とした検証を実施しました。

本年度では「小型機器編」を作成し、開発者の方がより具体的に対策を打てるよう再編中です。

さらにIoTセキュリティ用語集については「フェーズ別索引」を含めカテゴリ分けを実施し、産業機器に対するセキュリティ対策を理解いただくための一助となれるよう、さらなる改訂を予定しています。