解説！「IoTセキュリティ手引書 Ver2.0」

2022年3月

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


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

セキュリティ仕様検討部会

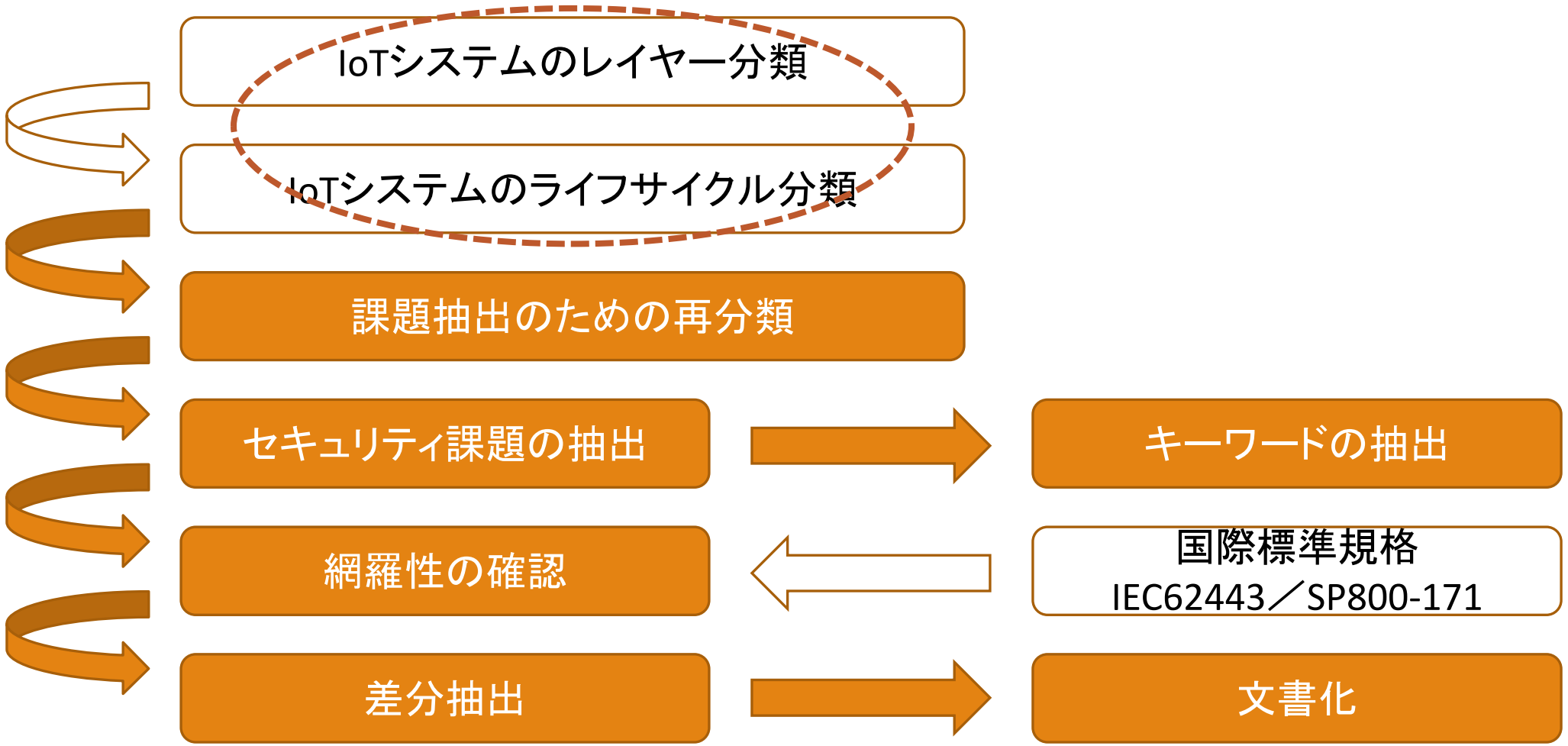
2020年10月21日　初版
2021年11月 1日　改訂（予定）

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者向けの規格である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す。

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。

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。

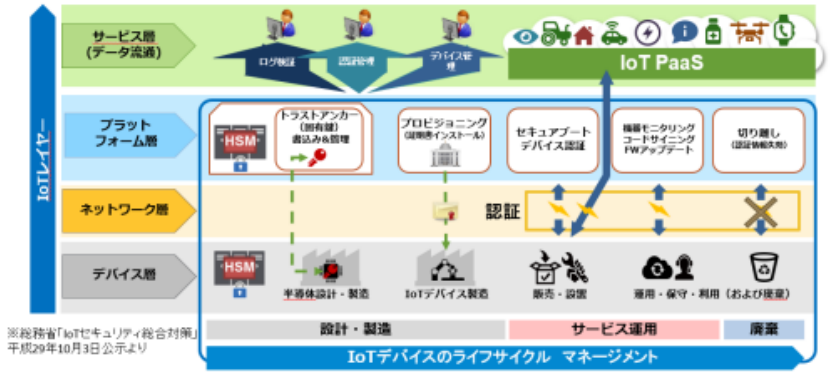


図 2-1　IoT セキュリティ総合対策モデル

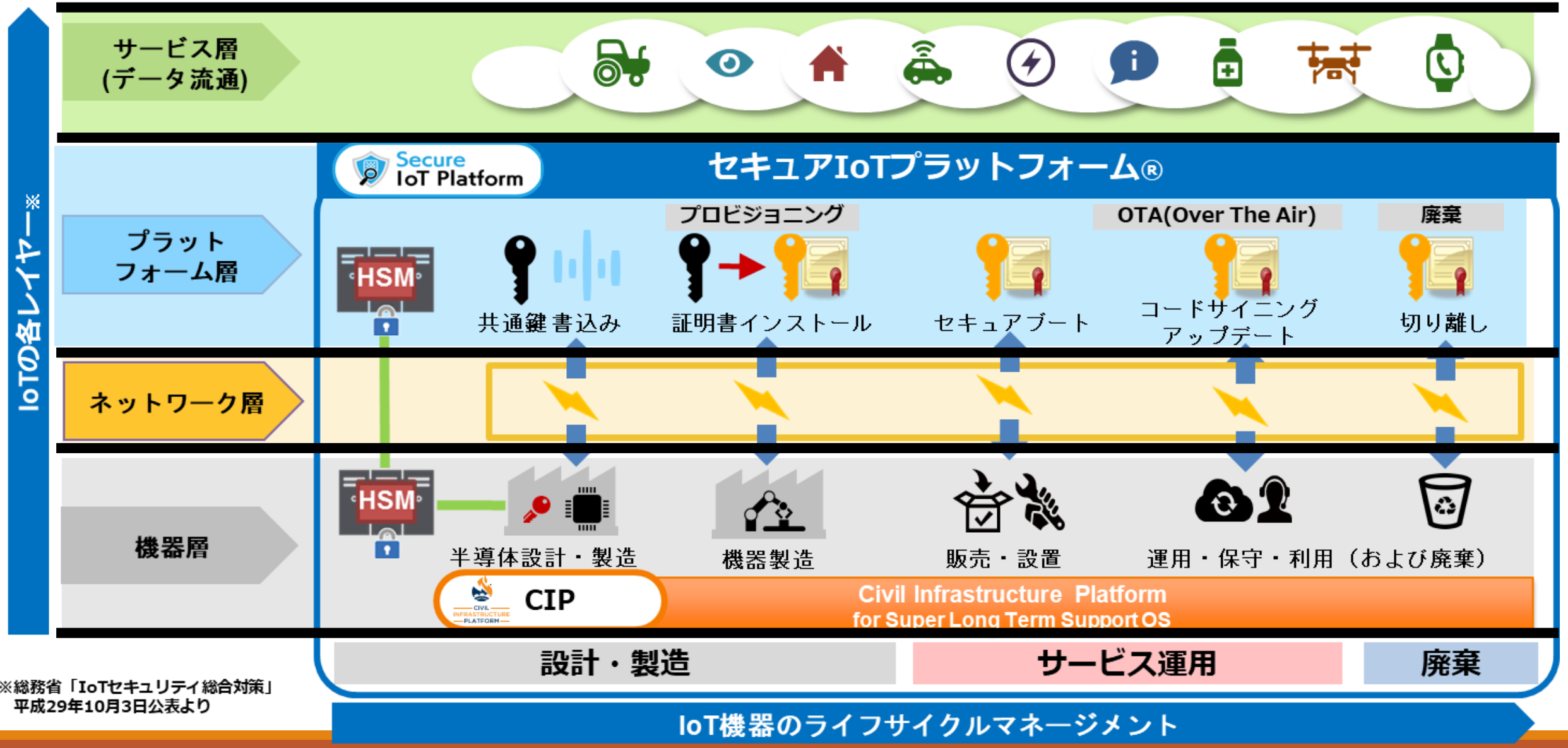
機器開発における現実の役割分担を反映するため、垂直方向の分類となる、製品のライフサイクル（設計・製造／サービス運用／廃棄）を「企画」「設計」「開発」「製造」「量産」「運用」「廃棄」に細分化しました。

IoT セキュリティの検討モデル

IoT システムは「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。

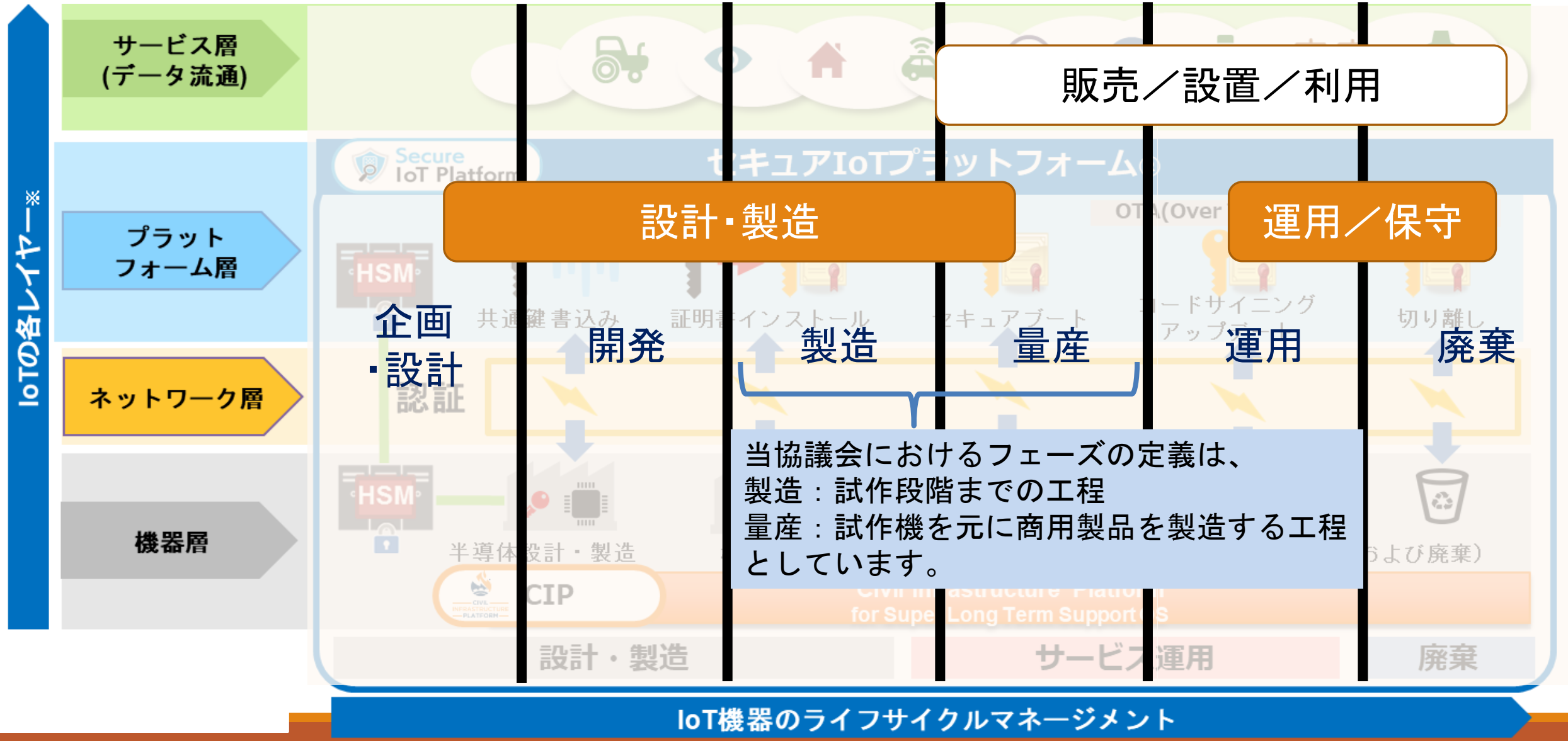
機器開発における現実の役割分担を反映するため、垂直方向の分類となる、製品のライフサイクル（設計・製造／サービス運用／廃棄）を「企画」「設計」「開発」「製造」「量産」「運用」「廃棄」に細分化しました。

IoTシステムのレイヤー分類

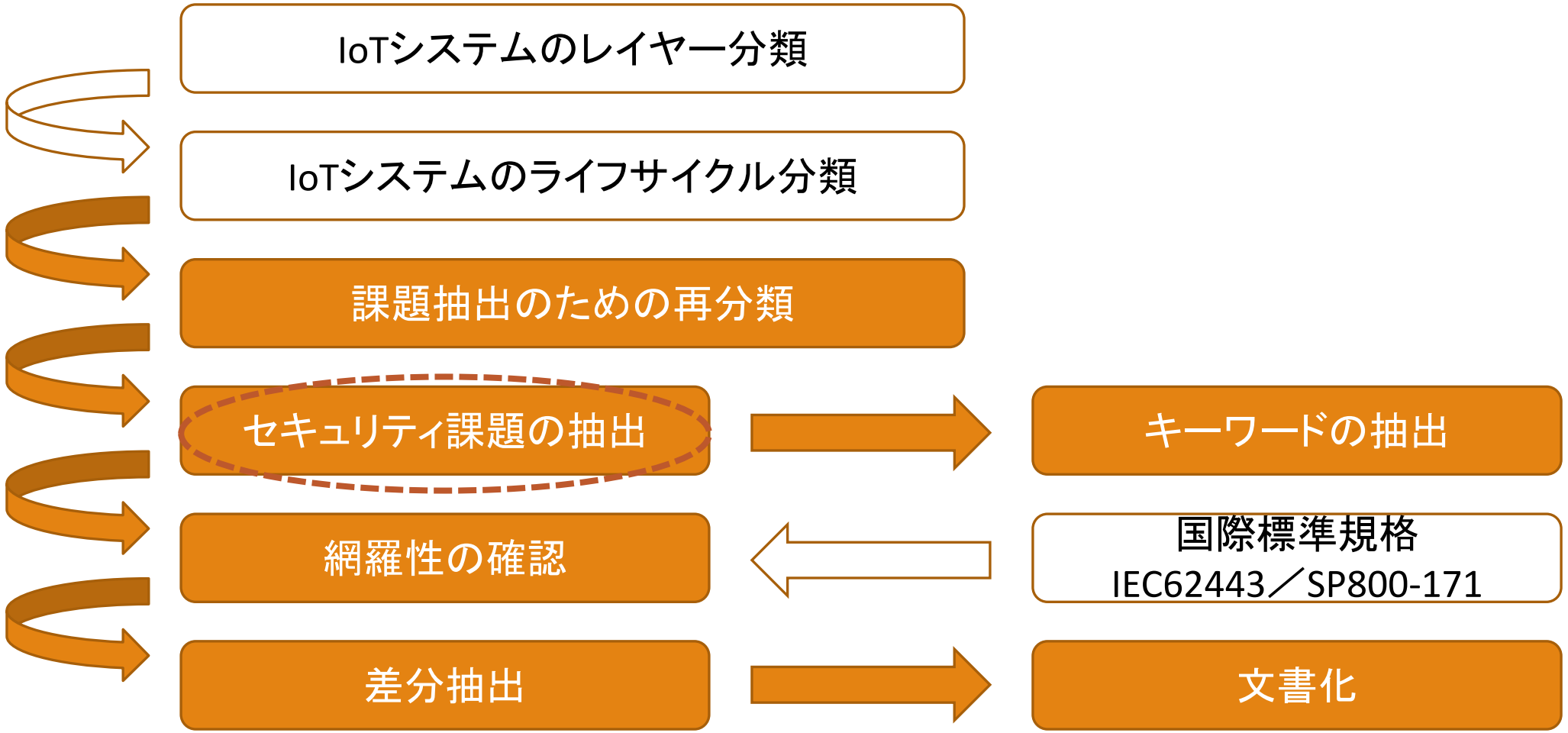


※総務省「IoTセキュリティ総合対策」
平成29年10月3日公表より

IoTシステムのライフサイクル分類



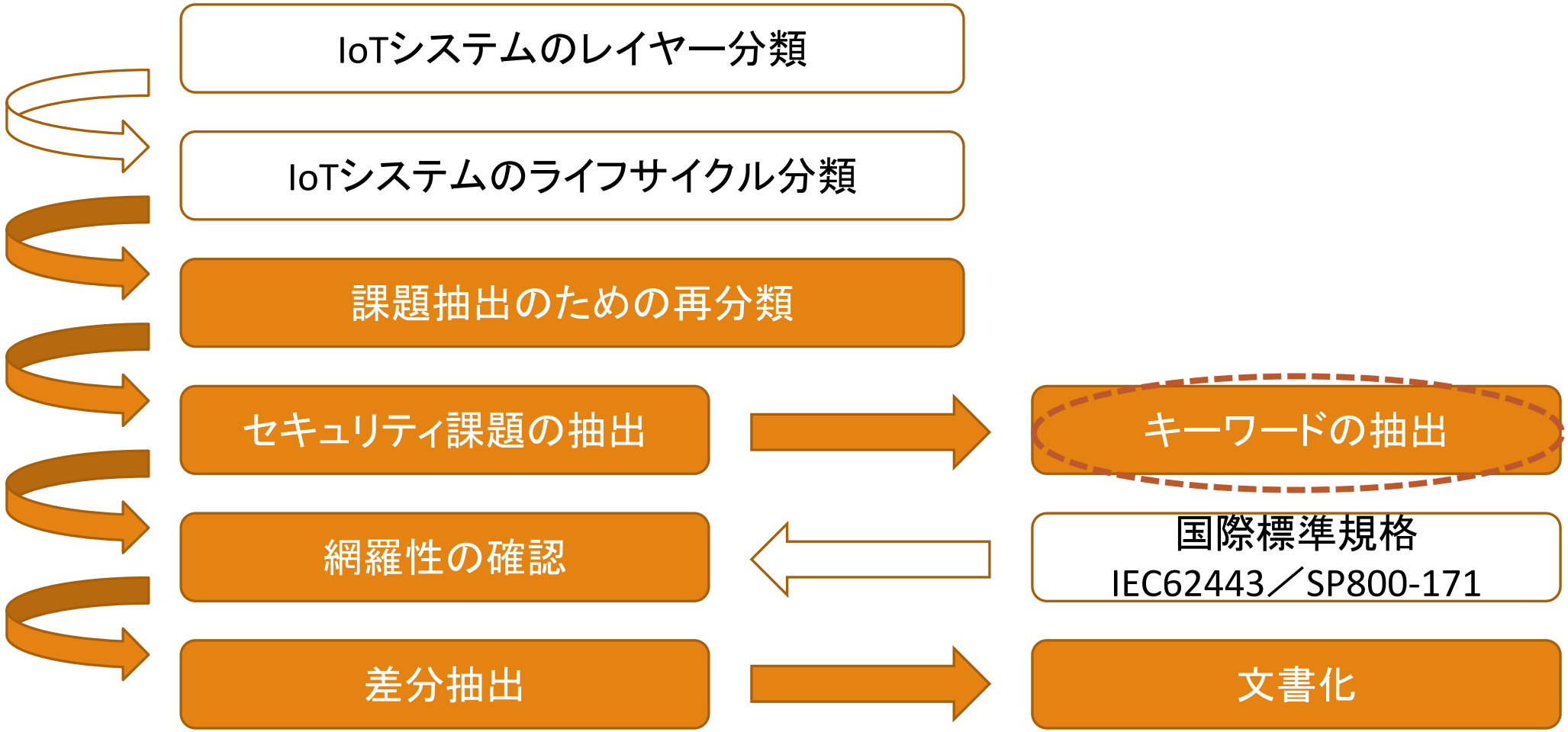
仕様検討部会　活動紹介　step 3



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。
		アクセス制御	認証されたユーザ情報からアクセス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ンツのみを表示すること。
		セッション管理	認証済みのセッションが一定時間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。

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。

国際標準におけるIoTセキュリティ用語

セキュリティ用語例

下表は「SP800-171rev.2」の「付属書 B」と「IEC62443-4-2」の「3章 用語、定義、略語、頭字語、慣用句」で共通となっている用語の一覧です。

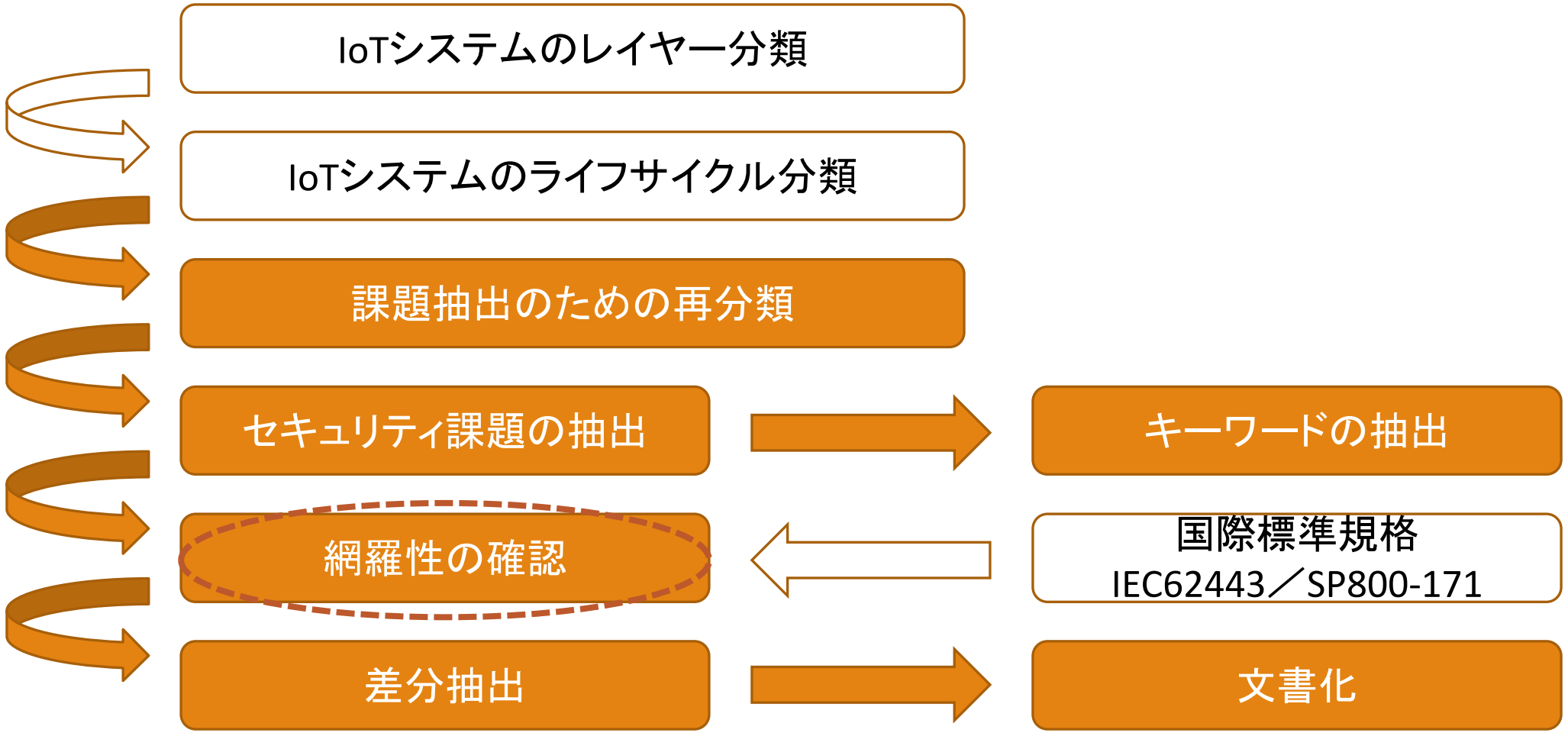
用語	意味
Authentication（認証）	多くの場合、システム内の資源へのアクセスを許可する前提条件として、ユーザー、プロセス、または装置のアイデンティティを照合すること。
Availability（可用性）	情報に対する適時かつ信頼できるアクセス、およびその使用を確実にすること。
Confidentiality（秘匿性）	情報のアクセスおよび開示について、権限を与えられた制限を存続させること。個人のプライバシーおよび所有権の情報を保護する手段を含む。
Identifier（識別子）	個人のアイデンティティおよびそれに伴う属性を表す固有のデータ。名前またはカード番号は、識別子の例。特定のエンティティ、オブジェクト、またはグループを示すためにシステムによって使用される一意のラベル。
integrity（完全性）	不適切な情報変更や破壊の防止であり、情報の否認防止と真正性の保証が含まれる。
least privilege（最小限の特権）	各エンティティがその機能を実行するために必要な最小のシステム資源と権限を付与されるべくセキュリティアーキテクチャーが設計される原理。

国際標準におけるIoTセキュリティ用語

用語	意味
mobile code （モバイルコード）	受信者による明示的なインストール行為なしに、遠隔システムから入手され、ネットワークを越えて送信され、そしてローカルシステムで実行されるソフトウェアプログラムまたはプログラムの部分。
mobile device （モバイル装置）	以下のような携帯型コンピューティング装置。すなわち、 (i)小型形状因子であり、その結果、一人で容易に持ち運びできるもの、(ii) 物理的接続なしに(無線送受信情報など)作動することを意図しているもの、(iii) 取外し不能または取外し可能なローカルデータ・記憶を有するもの、そして (iv) 内蔵型電源を包含するもの。モバイル装置には、音声通信能力、当該装置の情報捕捉を可能にする搭載センサー、そしてローカルデータ を遠隔地と同期させる組込型特性も含まれることがある。例として、スマートフォン、タブレット、および電子ブックリーダーがある。
remote access （リモートアクセス）	外部ネットワーク（インターネットなど）を通じて通信するユーザー（またはユーザーの代理として作用するプロセス）による、組織所有のシステムへのアクセス。

※　IPA/ISEC（独立行政法人情報処理推進機構 セキュリティセンター）により公開されている、「セキュリティ関連NIST文書」より引用

仕様検討部会　活動紹介　step 5



標準規格による網羅性の確認

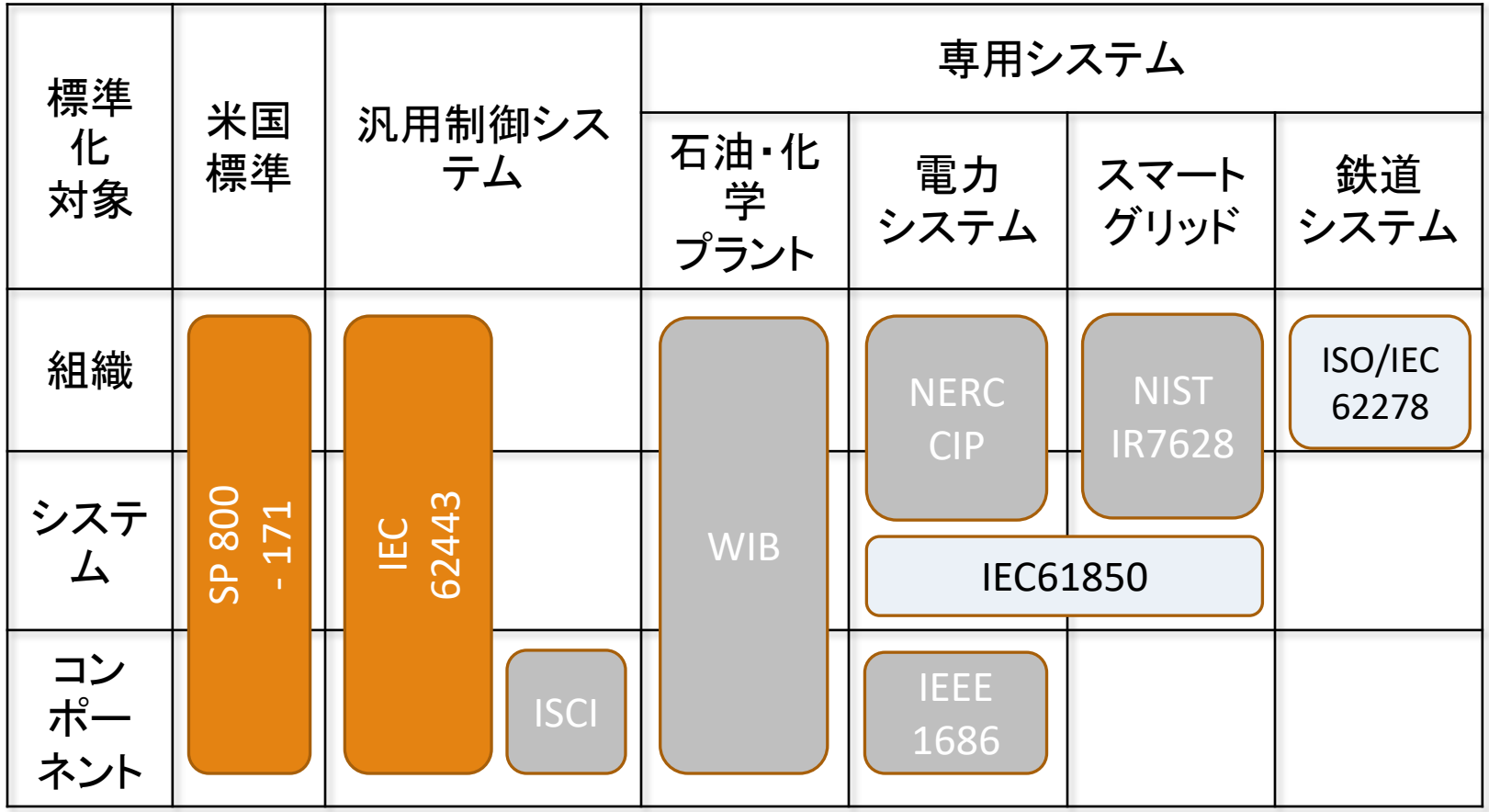
システムセキュリティには
網羅性が重要

＋

世界標準規格

＝

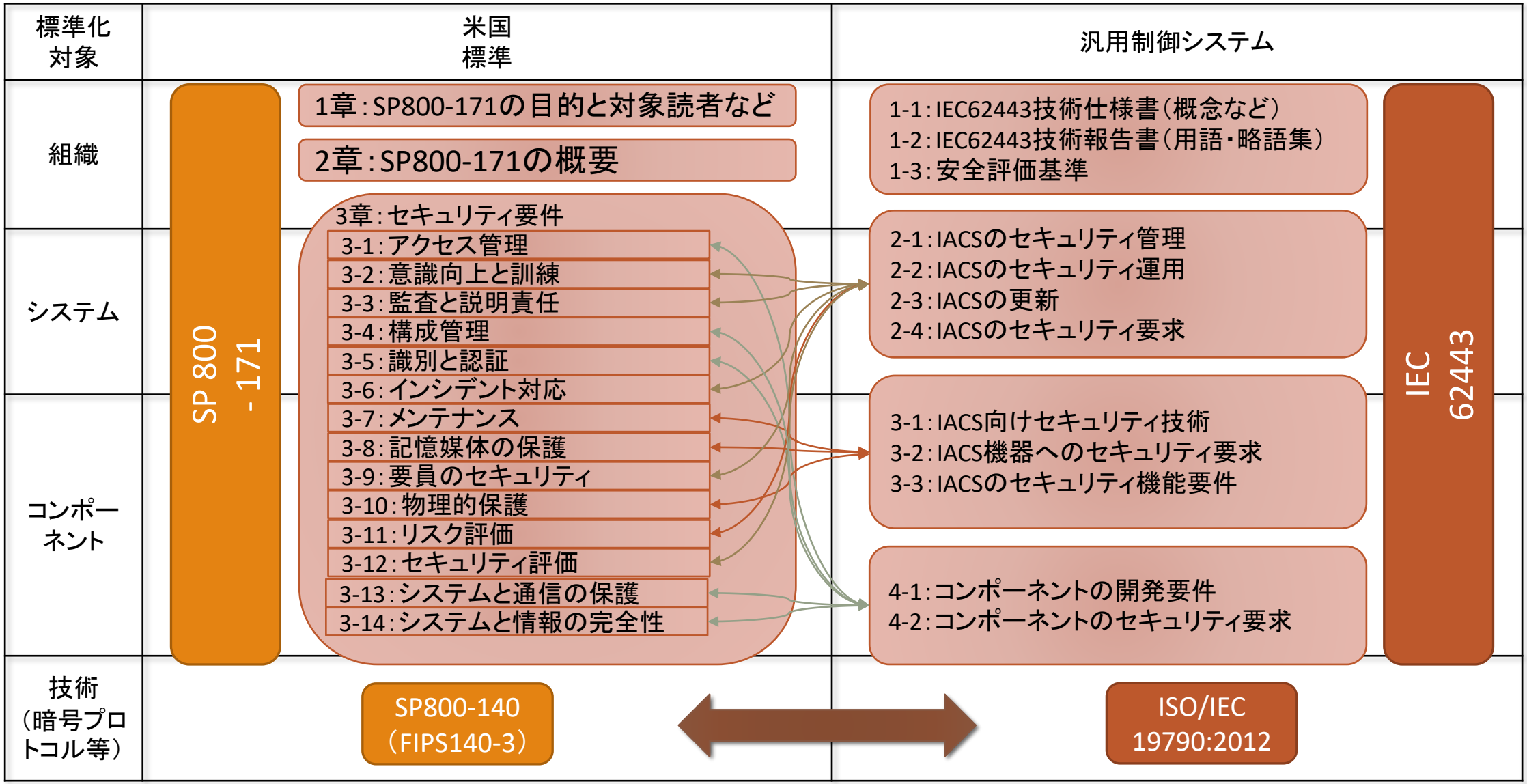
IEC62443／SP800-171
を基準とする



制御システム分野での標準規格マッピング※

※IPA技術解説 「制御システムセキュリティへの対応」より
https://www.ipa.go.jp/files/000066496.pdf

国際標準規格の相関関係



FIPS140-3

暗号モジュールに関するセキュリティの仕様。FIPSとはFederal Information Processing Standardizationの略称で日本語では「連邦情報処理標準」もしくは「連邦情報処理規格」と訳されています。
1994年1月11日に発行された長い歴史を持つ規格であり、対象はハードウェア、及びソフトウェアコンポーネントの両方に適用され、鍵の生成から利用、廃棄まで、米国連邦政府省庁・行政機関が求める、暗号モジュールのあり方について定められています。

以下のように暗号モジュールを保護するうえで必要となる要素が含まれ、セキュリティレベル（Lv.1-4）により順守すべき水準を定めています。

- 暗号モジュールの仕様
- 暗号モジュールのインタフェース
- 役割、サービス及び認証
- ソフトウェア・ファームウェアセキュリティ
- 動作環境
- 物理セキュリティ
- 物理セキュリティ（非破壊）
- Security Sensitive Parameter 管理
- 自己テスト
- ライフサイクル保証
- その他の攻撃への対処

「セキュアIoTプラットフォーム協議会」のご案内

仕様検討部会　活動紹介　new steps

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中です。

SP800-171 については本文の引用も可能となっているため、より具体的な手引書となることを期待しています。

標準化部会の活動

診断作業

　標準化部会では下記のような、チェックシートを作成し、会員企業のソリューションに対して診断を実施しています。この活動は、まだ試験段階ですので、診断をしながら検査項目の不備や検査基準も並行して検討・設定しています。
　この診断内容を仕様検討部会にフィードバックしIoTセキュリティ手引書を充実させていく方針です。

IEC62443-3-3 check sheet

Target:

classification: ☐H/W ☐S/W ☐cloud system ☐component

Date:

Time:

FR 1 - Identification and authentication control (IAC)

	SRs and REs SL 1			SL1	SL2	SL3	SL4
SR 1.7	Strength of password-based authentication	パスワードベースの認証の強さ	5.9	✓	✓	✓	✓
SR 1.7 RE 1	Password generation and lifetime restrictions for human use	ユーザーのためのパスワード生成とライフタイム	5.9.3.1			✓	✓

	要件		和訳	✓	選択した理由	エビデンス
SR1.7		**Strength of password-based authentication** For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.	**パスワードベースの認証の強度** パスワードベースの認証を利用する制御システムの場合、制御システムは 最小の長さと種類に基づいて構成可能なパスワード 強度を適用する機能 のタイ			
	RE 1	**Password generation and lifetime restrictions for human users** The control system shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform with commonly accepted security industry practices.	**ユーザーのためのパスワード生成とライフタイム制限** 制御システムは、特定の人間のユーザーアカウントが構成可能な世代数のパスワードを再利用するのを防ぐ機能を提供するものとします。さらに、制御システム人間のユーザーにパスワードの最小および最大有効期間制限を強制する機能を提供するものとします。これらの機能は、一般に受け入れられているセキュリティ業界に準拠する必要があります実践。			

セキュアIoTプラットフォーム協議会 問合せ先

- 協議会ホームページ
  https://www.secureiotplatform.org/

- メールアドレス
  info@secure-iot.org

以上