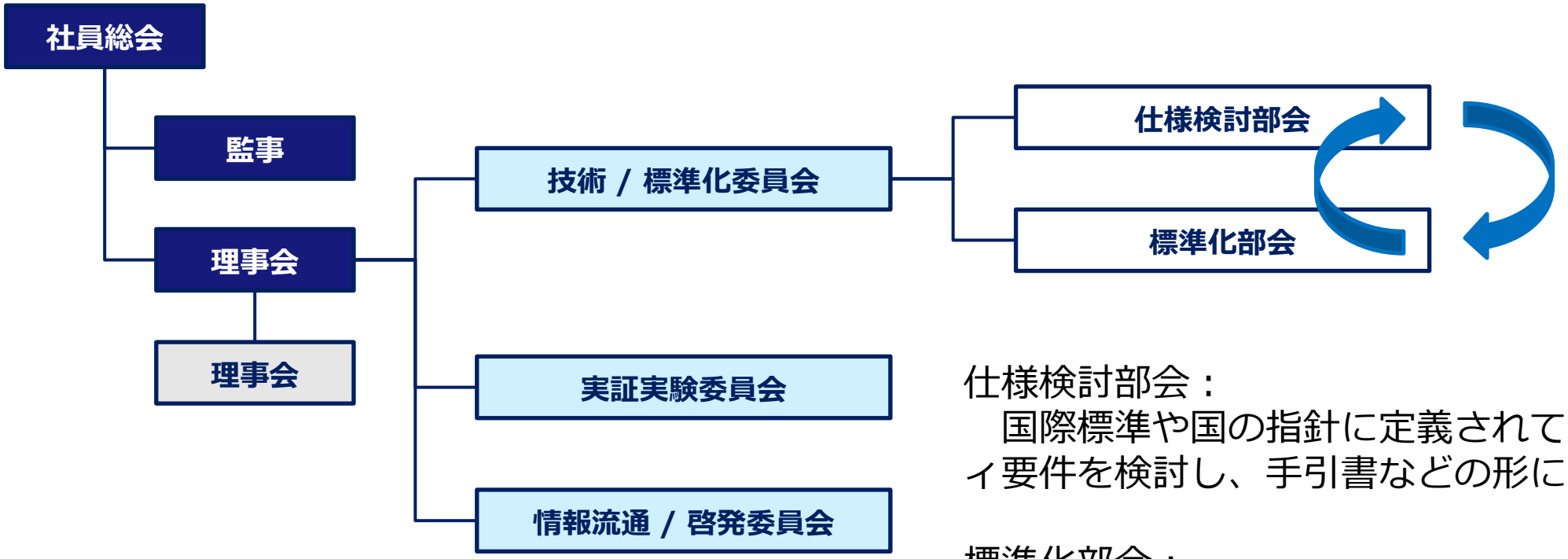
セキュリティフォーラム2021 Online

「IoTセキュリティ手引書」を解説

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

セキュアIoTプラットフォーム協議会の構成

セキュアIoTプラットフォーム協議会　部会構成



仕様検討部会：
　国際標準や国の指針に定義されているセキュリティ要件を検討し、手引書などの形にまとめる。

標準化部会：
　仕様検討部会の成果を実際のシステムに適用し、セキュリティ要件の解釈を深め、仕様検討部会にフィードバックする。

「IoTセキュリティ手引書」のご案内

仕様検討部会　IoTセキュリティ手引書　の目的

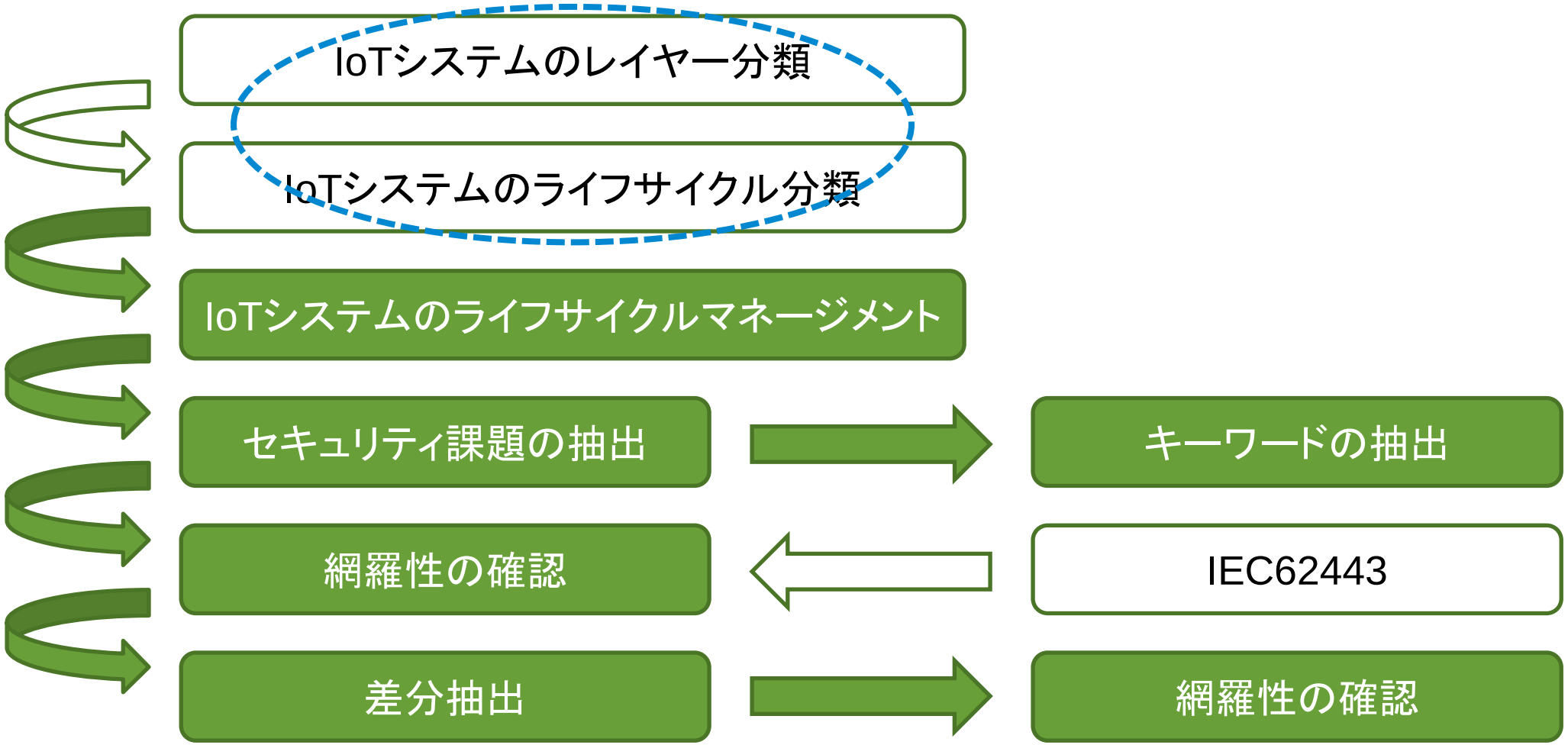
目的

本書では、IoT機器の開発において セキュリティで必要となる項目を国際標準と照らし合わせ差異と解釈を取りまとめるものとします。2020年度は、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 を基準としました。

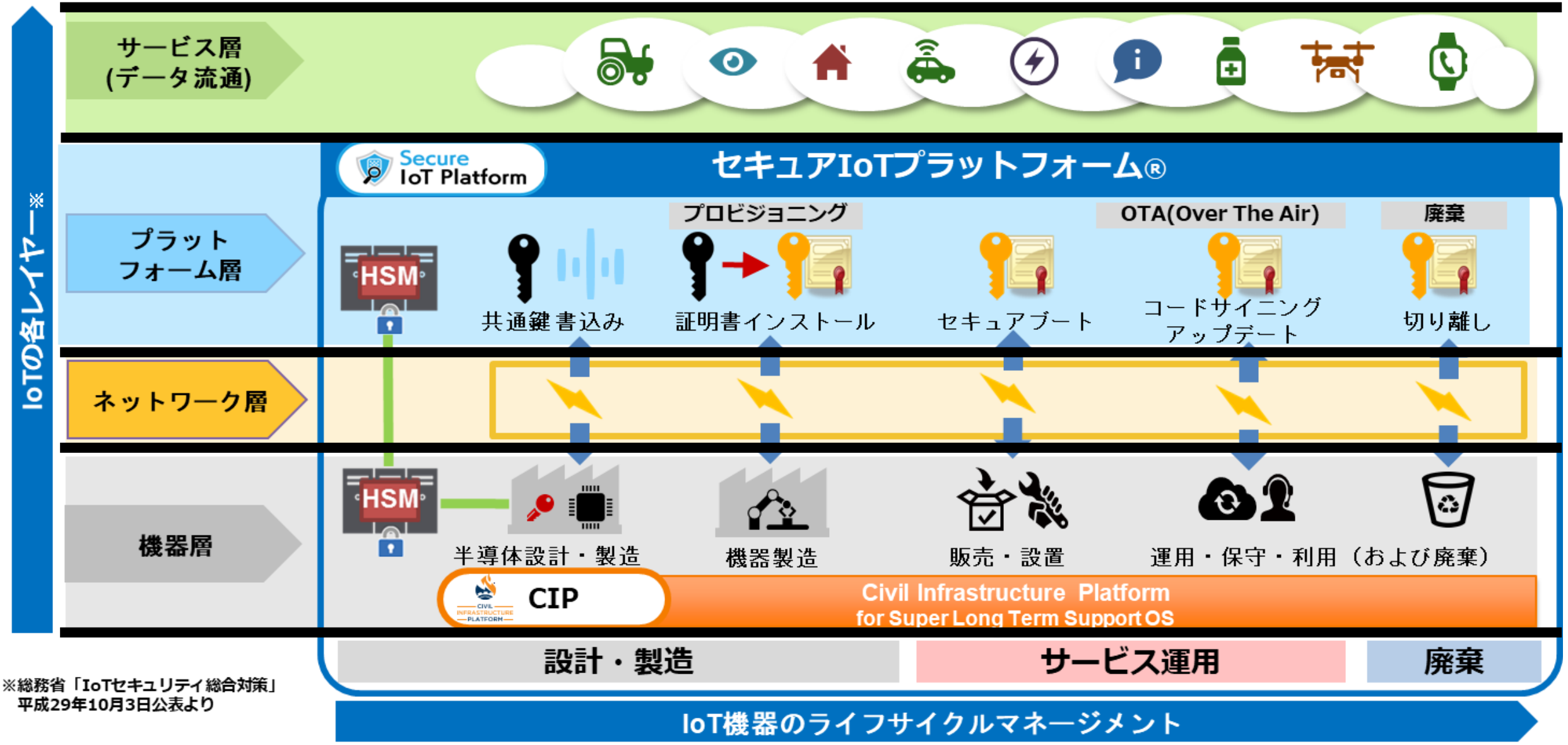
本協議会では様々な分野の会員の方々から、それぞれの分野で必要と考えられる IoT セキュリティの課題と対応策について意見を収集してきました。これらの意見を集約するにあたり、網羅性の観点から IEC62443-4 を基準とし、基準の検証を行いました。

本書 は 2020 年度の協議会の成果として発表しています。

仕様検討部会　活動紹介　step 1

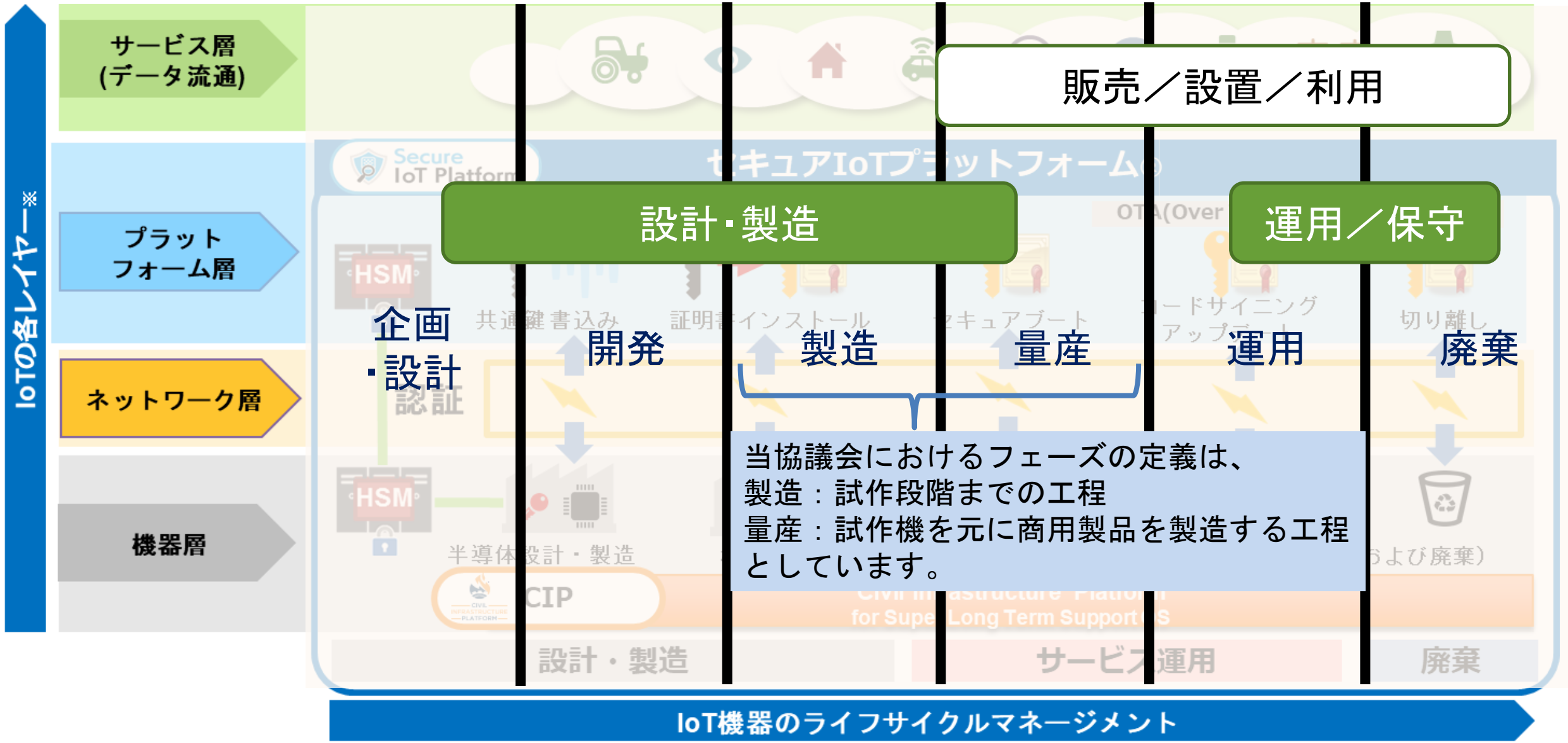


IoTシステムのレイヤー分類



※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



IoTセキュリティ手引書の検討モデル

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

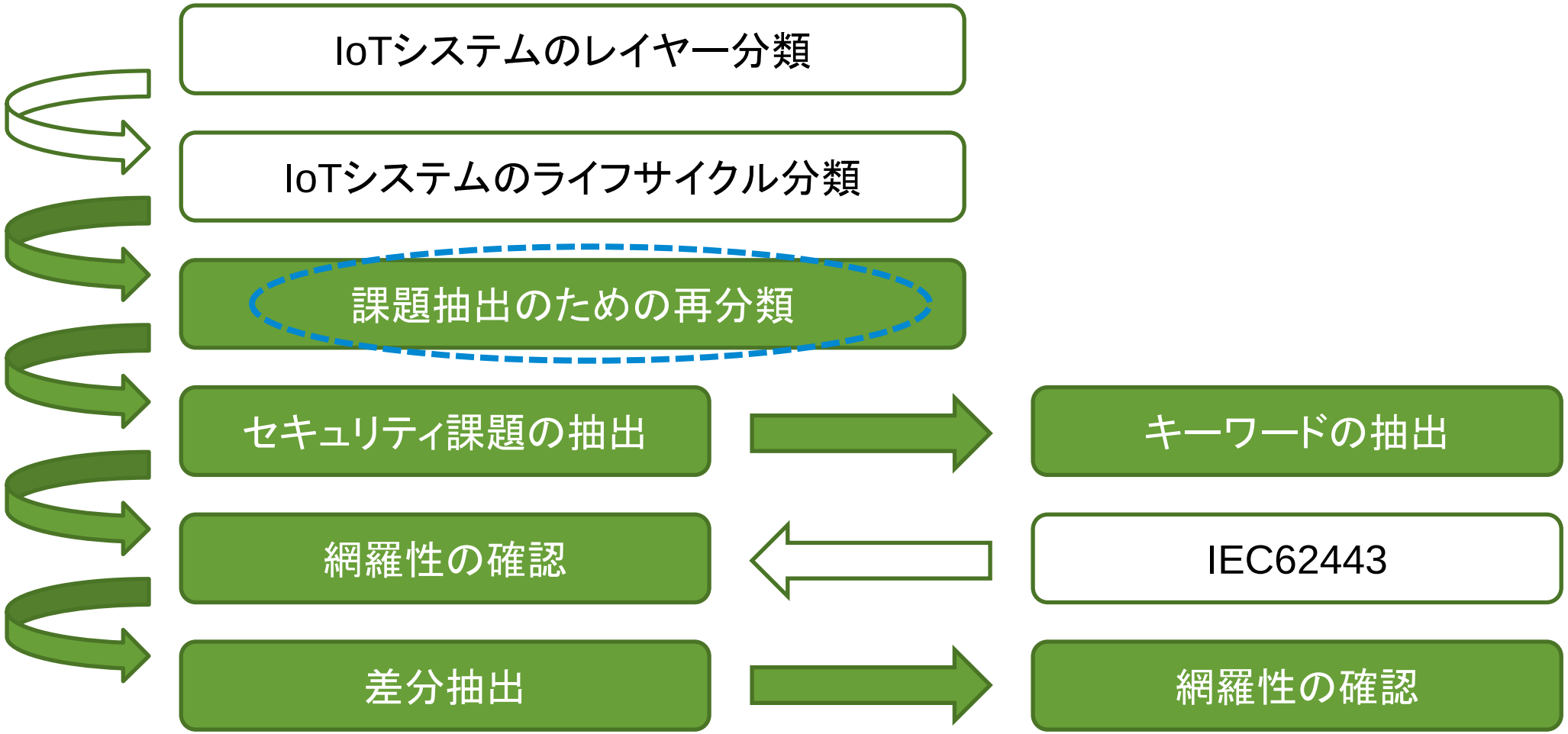
機器開発における現実の役割分担を反映するため、垂直方向の分類となる、製品のライフサイクル（設計・製造／サービス運用／廃棄）を「企画」「設計」「開発」「製造」「量産」「運用」「廃棄」に細分化しました。

IoT 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。

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。

仕様検討部会　活動紹介　step 2



IoTセキュリティ手引書の検討フェーズ詳細

2.2.1.検討フェーズ詳細

収集した情報の整理の過程で、特に「設計」「開発」のフェーズでは「図 2-2　IoT 機器の H/W 製造プロセスと S/W 開発プロセス」に示されるよう、H/W と S/W でセキュリティ対策に差異があることが判明しました。本書では、「設計」を「アーキテクチャ設計」「H/W 設計」「S/W 設計」に分けさらに「開発」を「H/W 開発」「S/W 開発」に分けることでこの差異へ対応しています。

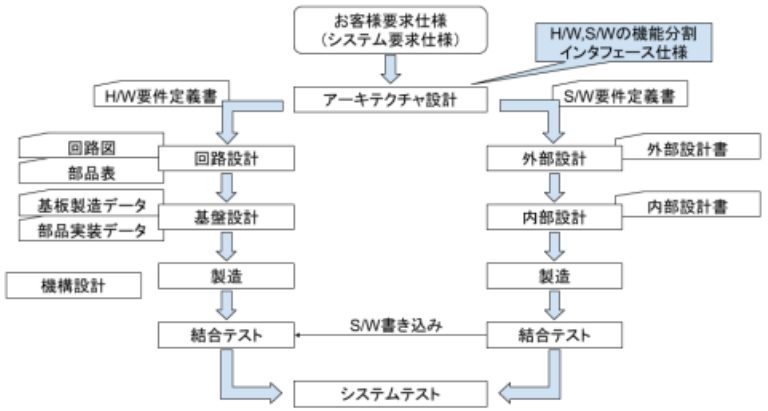


図 2-2　IoT 機器の H/W 製造プロセスと S/W 開発プロセス

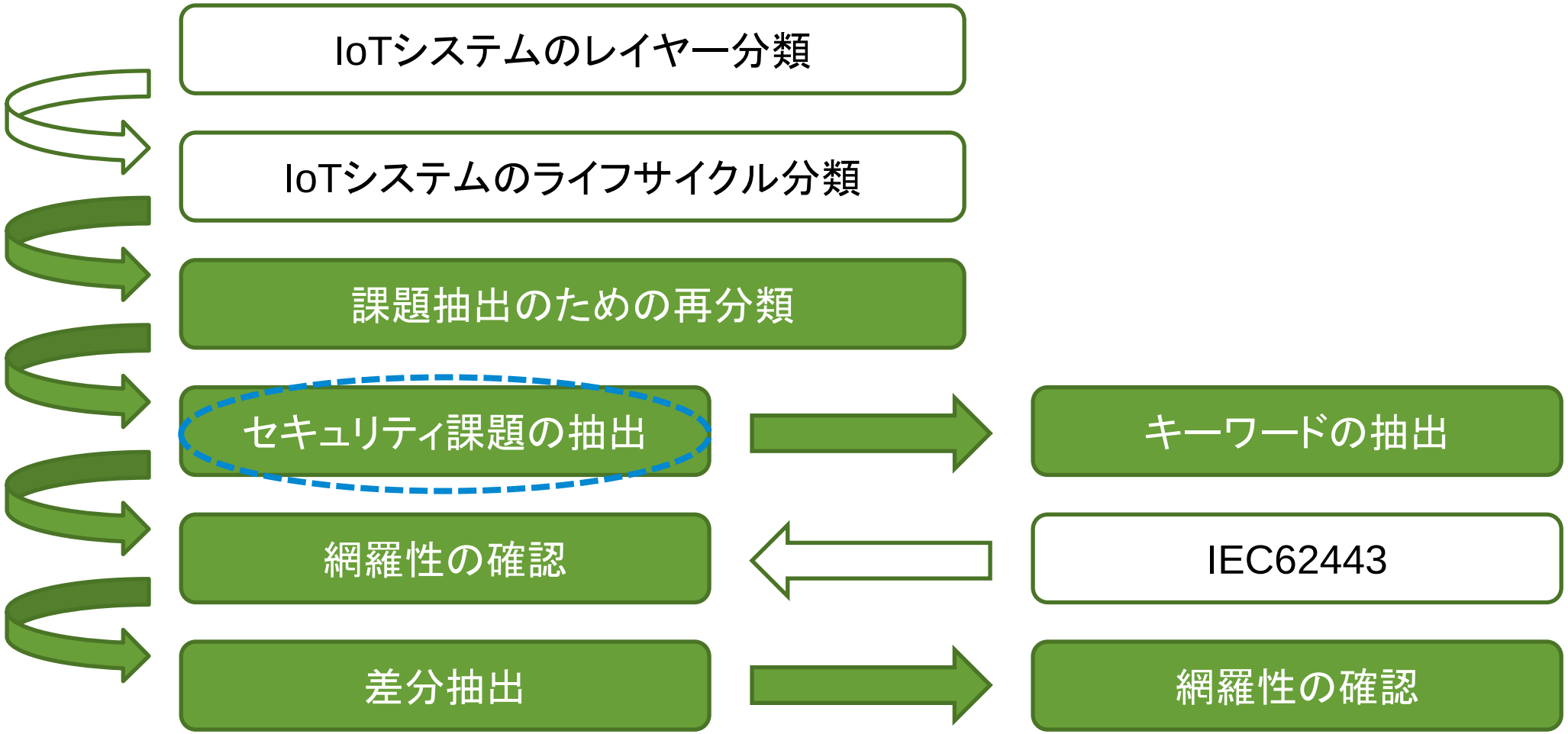
これらフェーズをあらためて整理すると「表 2-1　IoT 機器の製品ライフサイクル」のように整理できます。続く章ではそれぞれのフェーズごとに要件と対策をまとめています。本書を参照される各位が個々に該当する項を中心に参照いただくことにより、本書の適用が高まることを期待しています。

検討フェーズ

収集した情報の整理の過程で、特に「設計」「開発」のフェーズでは「図 2-2 IoT機器の H/W 製造プロセスと S/W 開発プロセス」に示されるよう、H/W と S/W でセキュリティ対策に差異があることが判明しました。

本書では、「設計」を「アーキテクチャ設計」「H/W 設計」「S/W 設計」に分けさらに「開発」を「H/W 開発」「S/W 開発」に分けることでこの差異へ対応しています。

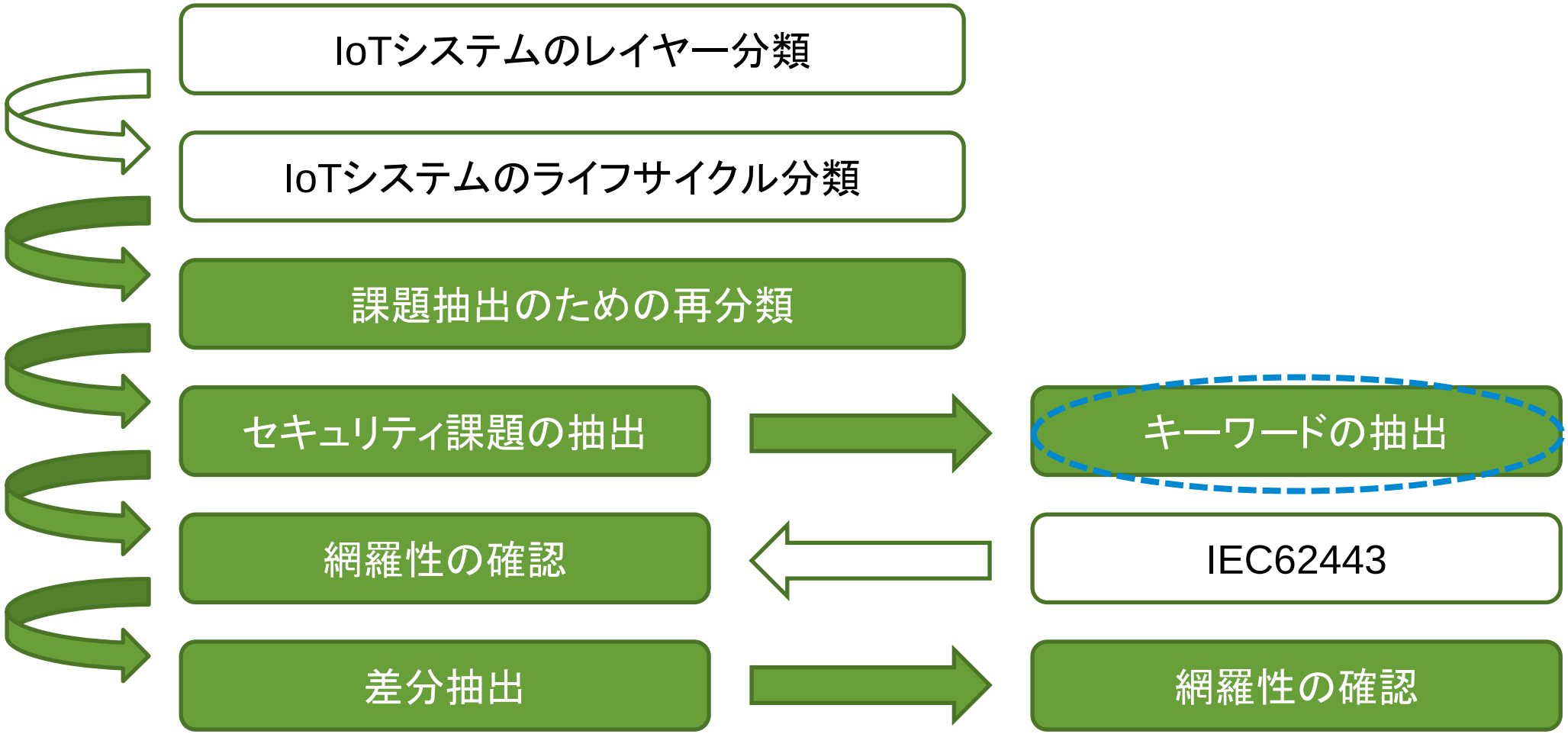
仕様検討部会　活動紹介　step 3



セキュリティ課題の抽出（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

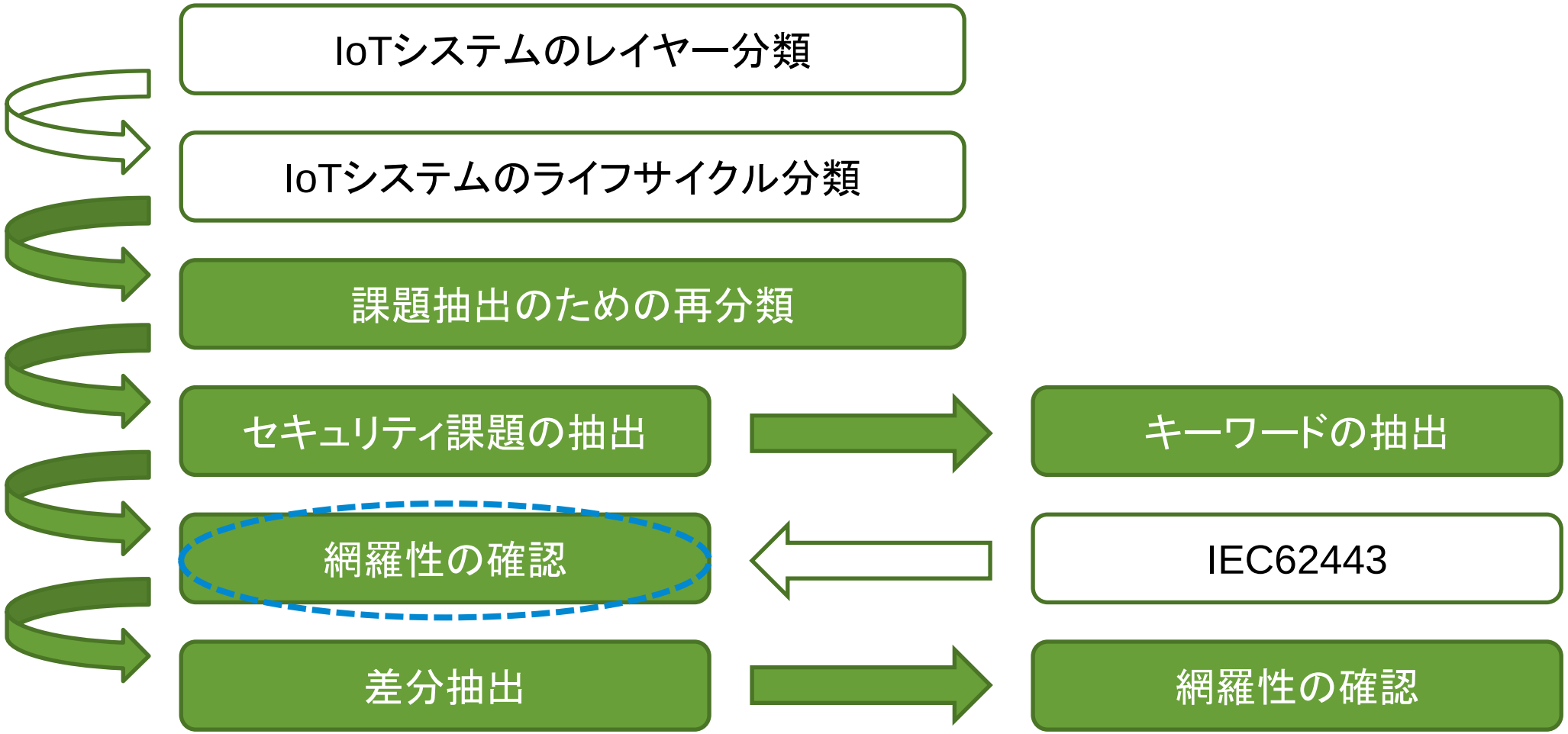
4. 付録 A　IOT セキュリティ用語

- 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、これをそれぞれ得意な分野について解説を入れていただき、これをIoTセキュリティ用語集として加えました。

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

＝

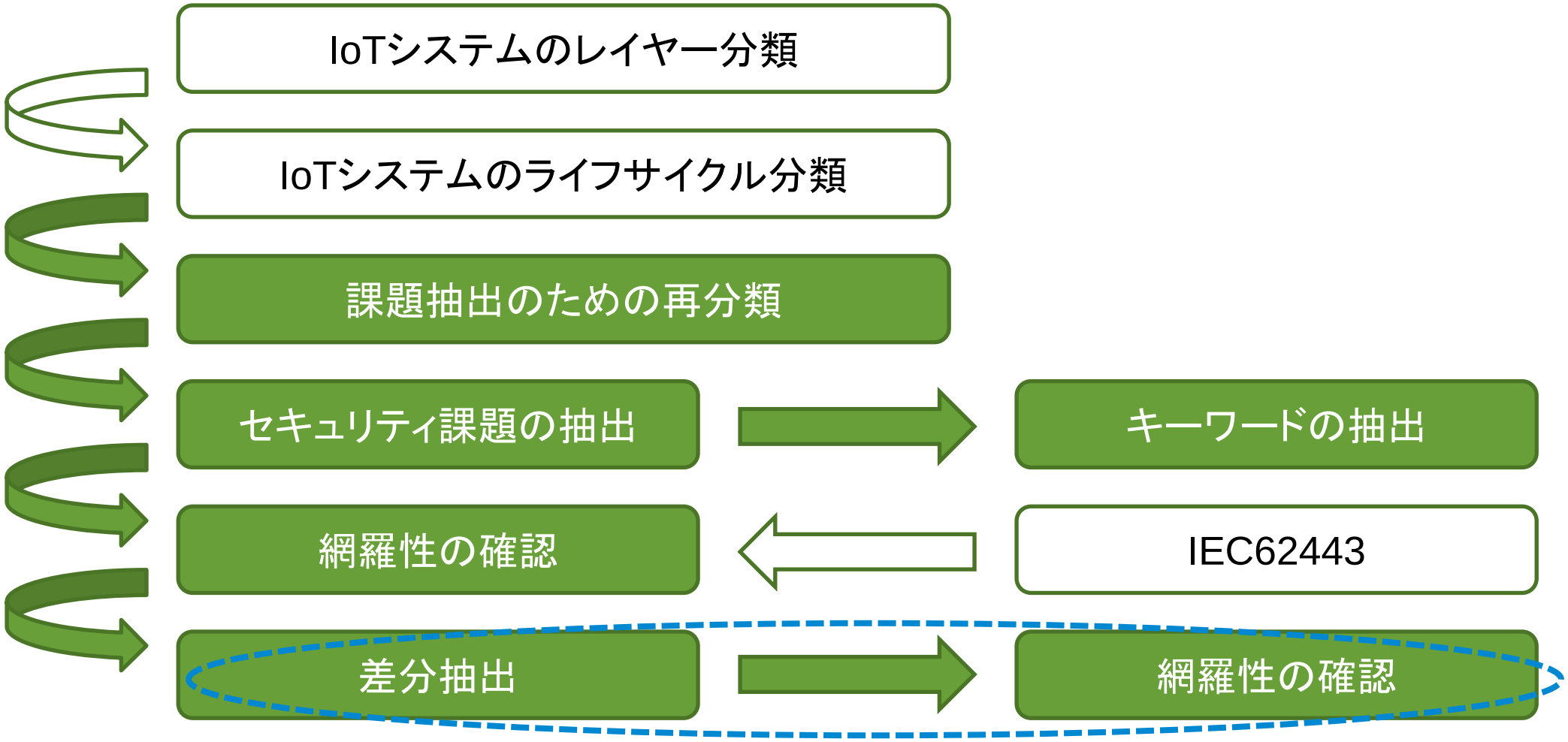
IEC62443
を基準とする

標準化対象	汎用制御システム		専用システム			
			石油・化学プラント	電力システム	スマートグリッド	鉄道システム
組織	IEC 62443		WIB	NERC CIP	NIST IR7628	ISO/IEC 62278
システム				IEC61850		
コンポーネント		ISCI		IEEE 1686		

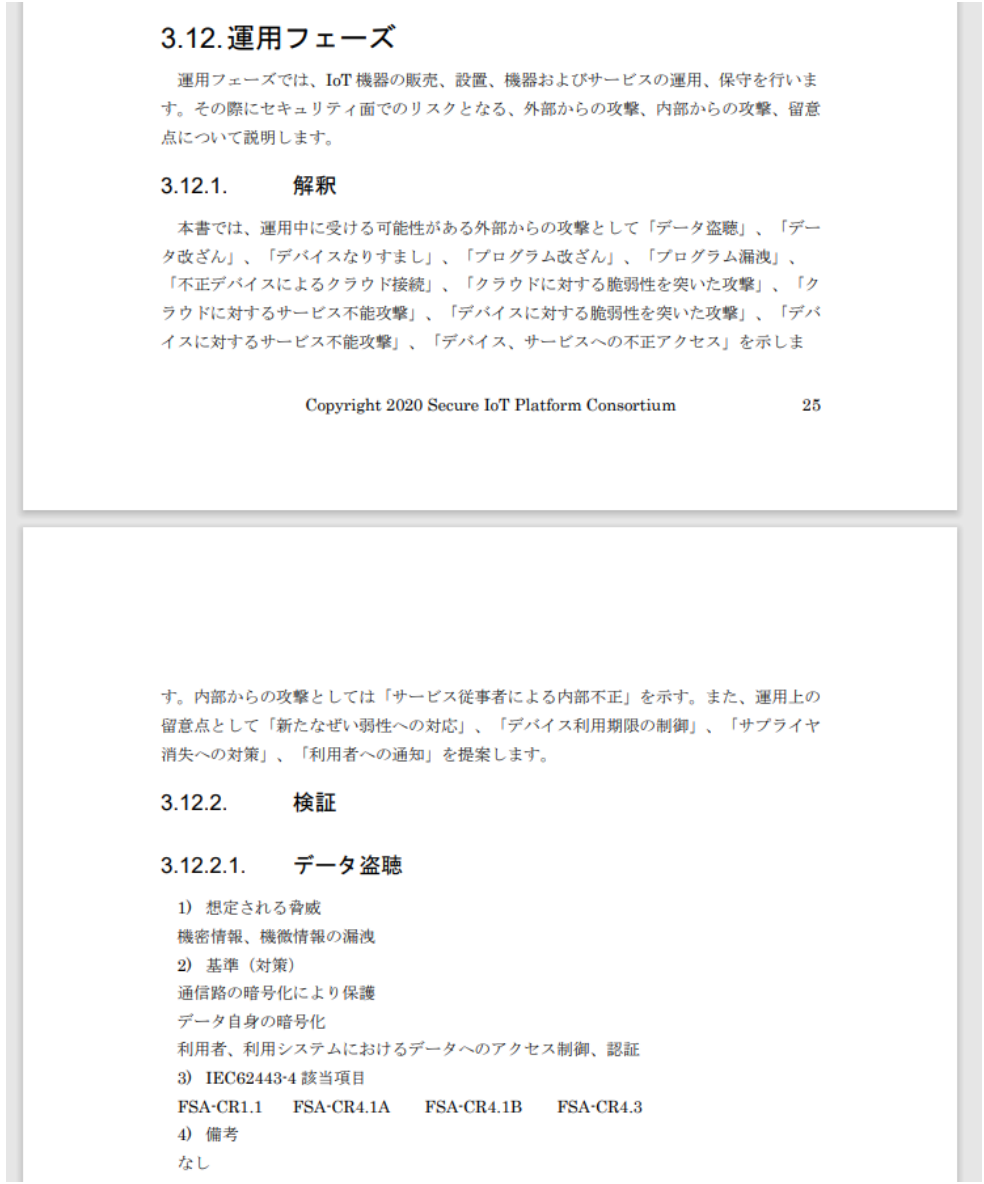
制御システム分野での標準規格マッピング※

※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

仕様検討部会　活動紹介　step 6



IoTセキュリティ手引書　本文



3.12. 運用フェーズ

運用フェーズでは、IoT 機器の販売、設置、機器およびサービスの運用、保守を行います。その際にセキュリティ面でのリスクとなる、外部からの攻撃、内部からの攻撃、留意点について説明します。

3.12.1.　解釈

本書では、運用中に受ける可能性がある外部からの攻撃として「データ盗聴」、「データ改ざん」、「デバイスなりすまし」、「プログラム改ざん」、「プログラム漏洩」、「不正デバイスによるクラウド接続」、「クラウドに対する脆弱性を突いた攻撃」、「クラウドに対するサービス不能攻撃」、「デバイスに対する脆弱性を突いた攻撃」、「デバイスに対するサービス不能攻撃」、「デバイス、サービスへの不正アクセス」を示しま

す。内部からの攻撃としては「サービス従事者による内部不正」を示す。また、運用上の留意点として「新たなぜい弱性への対応」、「デバイス利用期限の制御」、「サプライヤ消失への対策」、「利用者への通知」を提案します。

3.12.2.　検証

3.12.2.1.　データ盗聴

1) 想定される脅威
機密情報、機微情報の漏洩
2) 基準（対策）
通信路の暗号化により保護
データ自身の暗号化
利用者、利用システムにおけるデータへのアクセス制御、認証
3) IEC62443-4 該当項目
FSA-CR1.1　FSA-CR4.1A　FSA-CR4.1B　FSA-CR4.3
4) 備考
なし

本文

本文では、各フェーズに対して以下のようにまとめています。

解釈
各フェーズで想定される攻撃のパターンについて記載しています。また可能な場合、攻撃パターンに対する対策も記載しています。

検証
解釈で想定された攻撃パターンを基準にIEC62443のどの項目に相当するかを検証しています。
※検証については、協議会でさらに追記していく予定です。

仕様検討部会　本年度の活動

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

セキュリティ仕様検討部会

2020 年 9 月 30 日　版

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る。

本活動はは 2021年度の協議会の成果として発表する予定です。

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かけさせていただいています。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:

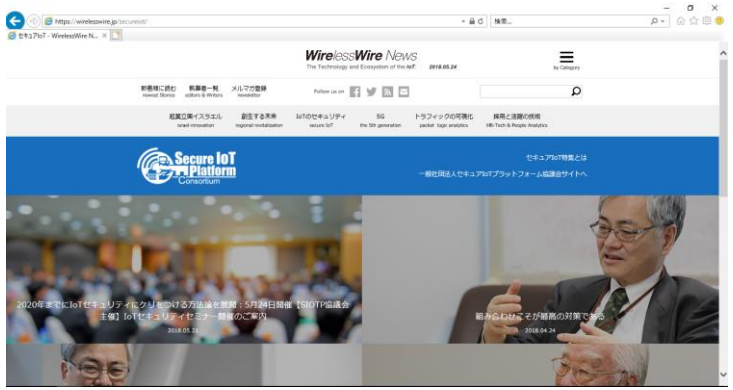
Time:

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の強度を適用する機能 文字タイプの。			
	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。			

情報提供/お問合せ先



【ホームページ】　https://www.secureiotplatform.org/
【情報発信サイト】　https://wirelesswire.jp/secureiot/
【Facebook】　https://www.facebook.com/SIOTP.JP/
【E-mail】　info@secure-iot.org

ご質問は、上記【E-mail】宛に、お送りください。

ご視聴ありがとうございました。

JAPAN
Security Summit