組込み機器開発におけるセキュリティの考え方

～セキュリティ設計の2つの視点～

2019年6月14日

安全性向上化委員会/情報セキュリティWG
（日立産業制御ソリューションズ）
牧野 進二
buildlab.koha9ru108@gmail.com
shinji.makino.py@hitachi.com

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

2018年度 活動から

1. STAMP/STPA-SECの実証
    1. IPA様が推進しているSTAMP/STPA-SECの実例を使った検討結果と活用方法のまとめ
2. セキュリティ設計の視点と考え方
    1. システム全体における視点と考え方
    2. 製品ライフサイクルにおける対応の考え方
3. 簡易PKI認証システムの実証実験結果
    1. Block chainを使ったPKI認証の実証実験結果報告

1. STAMP/STPA-SECの実証

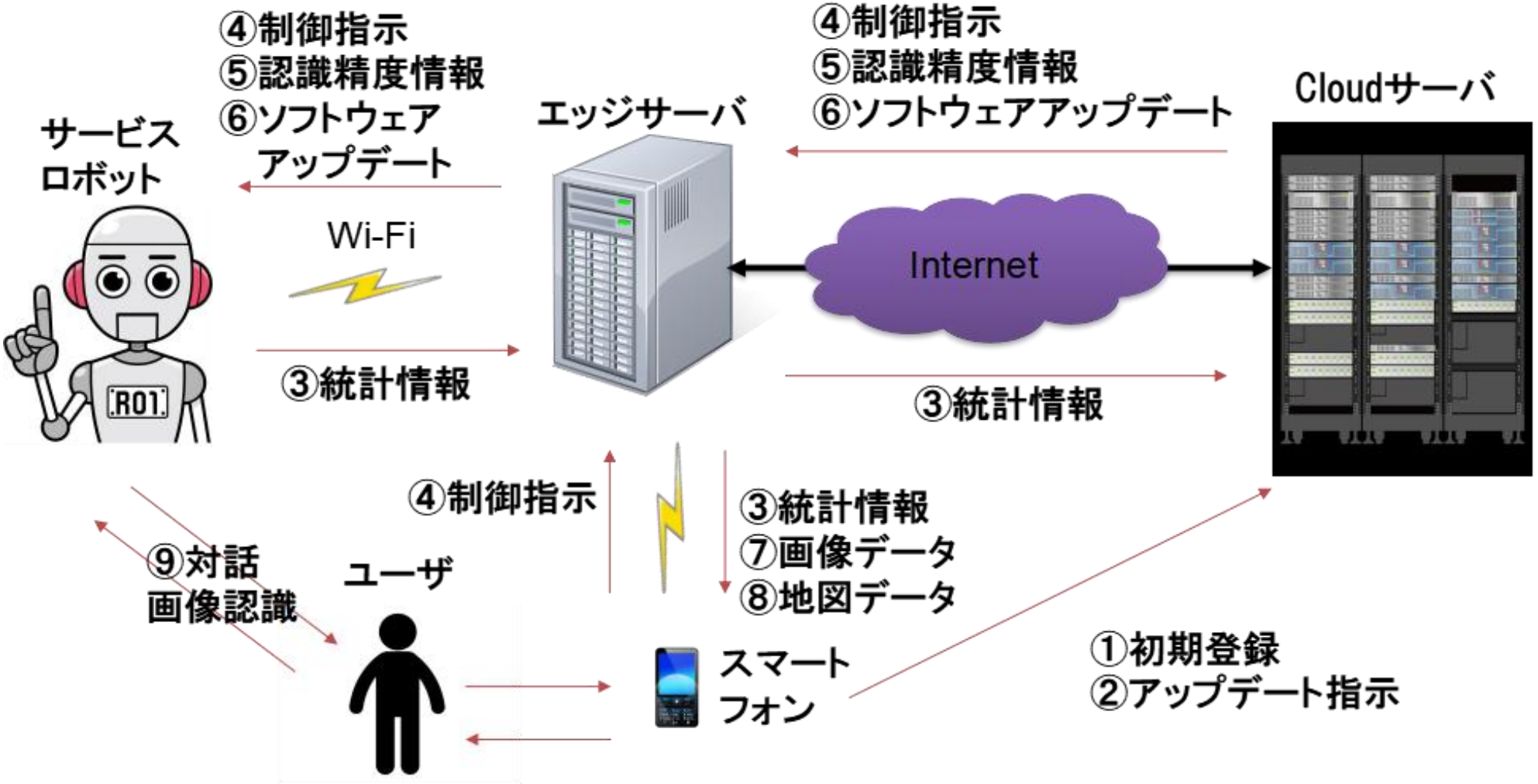
1. STAMP/STPA-SECの実証

■ 17年度に続きSTAMP/STPA-SECに関する検討を実施。

- 実例となるシステム構成を検討し、セキュリティ設計視点で実証を行った。

1. STAMP/STPA-SECの実証

■ システム構成案



1. STAMP/STPA-SECの実証

■ サービス仕様を定義して、STAMP/STPA-SECの検討を実施。

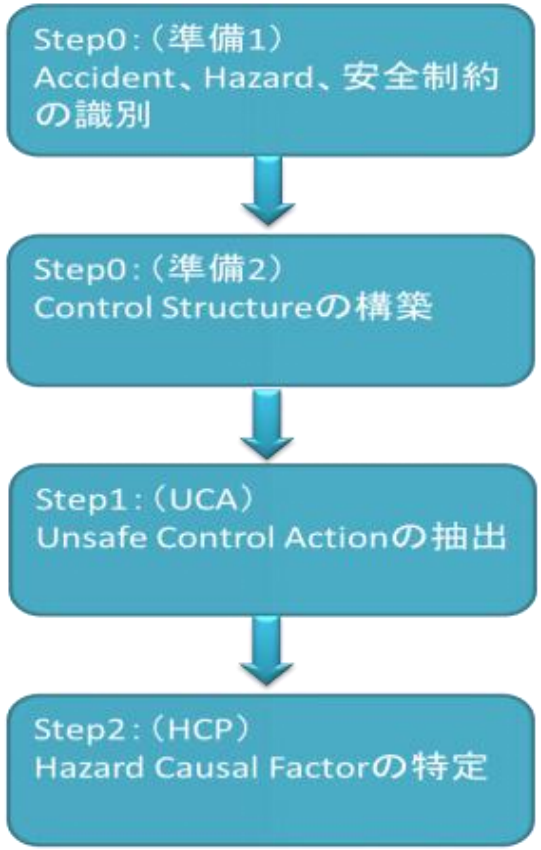
- サービスロボットは、ユーザと会話を行い、ユーザ指示にような行動をする。ユーザからの指示や行動情報の統計を行い、ユーザの特性に合わせた自律行動をする。

機器名	機能
サービスロボット	画像認識、音声認識、各種センサー、GPSを搭載し、センサー情報、位置情報からモータ制御を行う。 ユーザからの指示は、スマートフォン経由、音声認識にて行われる。スマートフォン経由は、遠隔操作もできる。
エッジサーバ	サービスロボットからの統計情報を周期的に収集し、学習を行い認識精度の向上を行う。
Cloudサーバ	エッジサーバに溜まった統計情報を定期収集(1週間単位)に収集し、ユーザの行動認識を行い、ユーザに新たなサービス提供を行う。
スマートフォン	ユーザがサービスロボットに指示するのに利用される。遠隔操作もできる。

1. STAMP/STPA-SECの実証

■　STAMP/STPA-SECの手順通りに検証

■解析手順



■解析内容

対象システムにおいて、分析対象となる①Accident（望ましくない事象）、②Hazard（Accidentが潜在している具体的な状態）を定義し、Hazardを制御するためのシステム上の安全制約を識別する。

システムにおいて、安全制約の実現に関するコンポーネント（サブシステム、機器、組織等）、および、**コンポーネント間の相互作用（コントローラによる指示、フィードバックデータ）**を分析し、Control Structureを構築する。

Control Structure Diagramから安全制約の実行に必要なコントローラによる指示（Control Action）を識別し、**4つのガイドワード**を適用して、ハザードにつながる非安全なControl Action（UCA）を抽出する。

Step1で抽出したUCA毎に、関係するコントローラと制御対象プロセスを識別して、Control Loop Diagramを作成し、**ガイドワード**を適用して、ハザード誘発要因（HCF）を特定する。
特に、ソフトウェアや**ヒューマンに起因**する要因として、コントローラの想定するプロセスモデルが、実際のプロセスの状態と矛盾することで起きる要因を特定する。

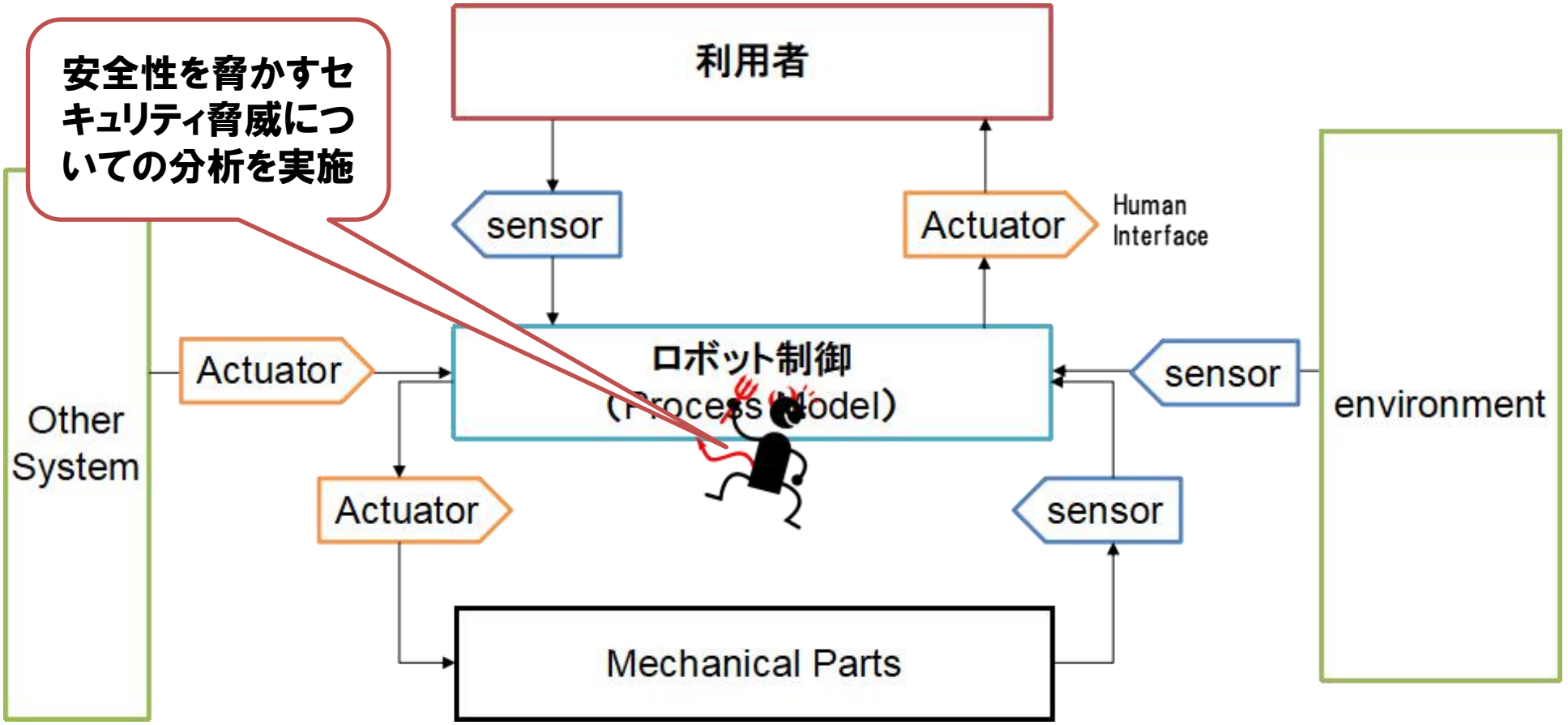
1. STAMP/STPA-SECの実証

■ Step2 Hazard Causal Factorの特定

- この段階でセキュリティ面の「STRIDE」を使ったガイドワードを使って安全性に対する脅威を分析することになる。。
  - Spoofing（なりすまし）
  - Tampering（改ざん）
  - Repudiation（否認）
  - Information Disclosure（情報漏えい）
  - Denial of Service（サービス拒否）
  - Elevation of Privilege（特権の昇格）

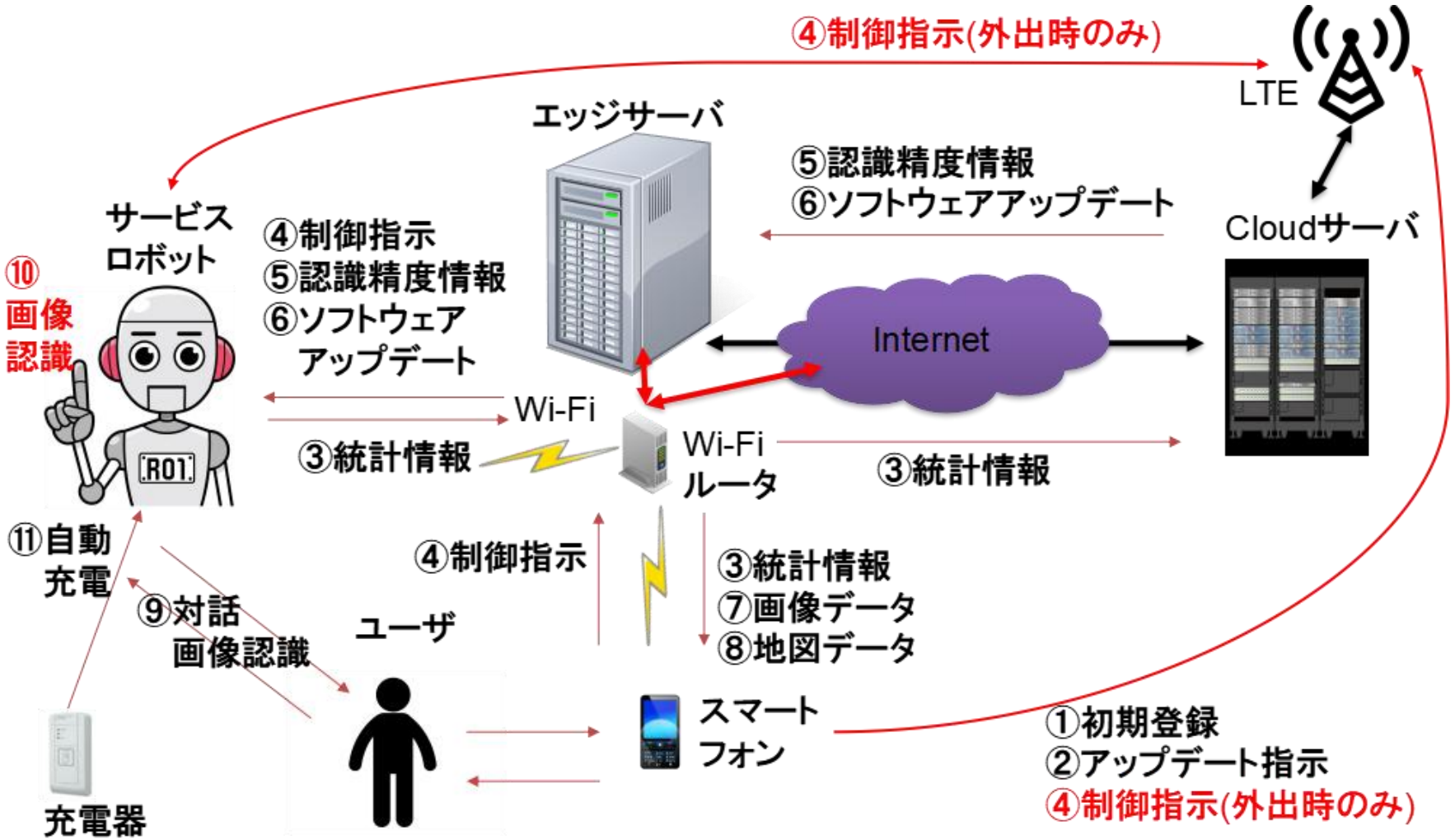
1. STAMP/STPA-SECの実証

■ Control Structureを用いて分析



1. STAMP/STPA-SECの実証

■　システム構成の見直し



1. STAMP/STPA-SECの実証

■ 仕様案の見直し

- 不足部分に対する仕様の見直しを実施。

機器名	機能
サービスロボット	画像認識、音声認識、各種センサー、GPSを搭載し、センサー情報、位置情報からモータ制御をする。 ロボットの用途は、対話と監視をするためのもの。 ユーザからの指示は、スマートフォン経由、音声認識にて行われる。スマートフォン経由は、遠隔操作(LTE経由)もできる。
エッジサーバ	サービスロボットからの統計情報を周期的に収集し、学習を行い認識精度の向上を行う。 ロボットの電池残量監視を行い、電池残量が10%以下になるとロボットに充電指示をする。
Cloudサーバ	エッジサーバに溜まった統計情報を定期収集(1週間単位)に収集し、ユーザの行動認識を行い、ユーザに新たなサービス提供を行う。
スマートフォン	ユーザがサービスロボットに指示するのに利用される。遠隔操作(LTE経由)もできる。 ロボットの状態を画像や位置情報でモニタリングできる。電池残量やロボットに行ってもらいたい事を制御指示として送ることで、ロボットを育てていく。

1. STAMP/STPA-SECの実証

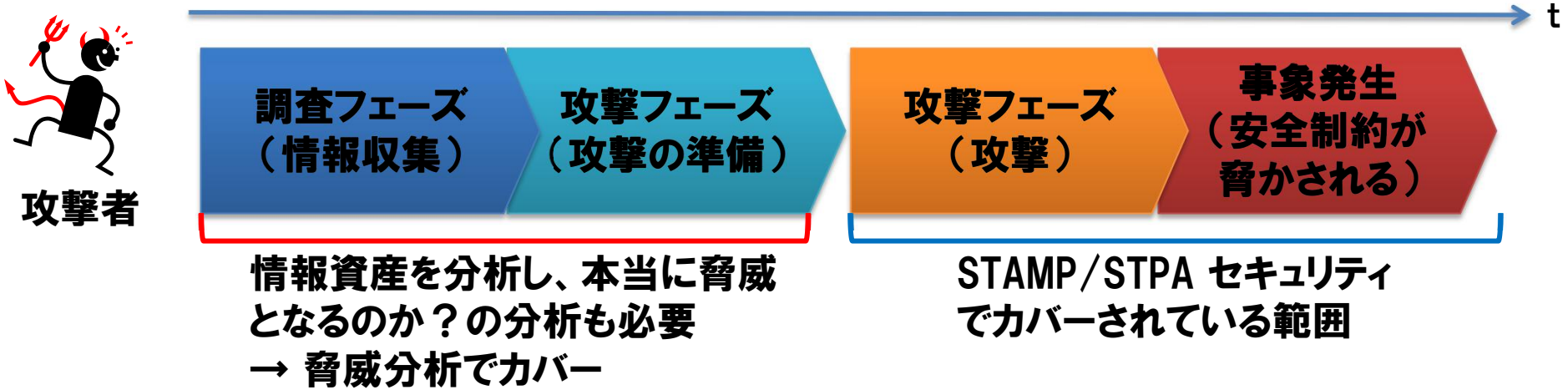
■ ２つの視点（まとめ）

- STAMP/STPA-SECを使うことで、システム全体を見渡した上流設計での安全性を脅かす脅威についての分析が有用であることが分かった。
  - ー システム改善や仕様の変更などに有用に使えることが分かった。
- 上流設計における改善点を下流設計にて証明することが重要であることが分かった。

1. STAMP/STPA-SECの実証

■ 課題となる点

- 攻撃者の行動を想定した場合、攻撃フェーズに移行する前の段階の分析についての分析視点も必要であることが分かった。



2. セキュリティ設計の視点と考え方

2. セキュリティ設計の視点と考え方

■　システム全体における視点と考え方

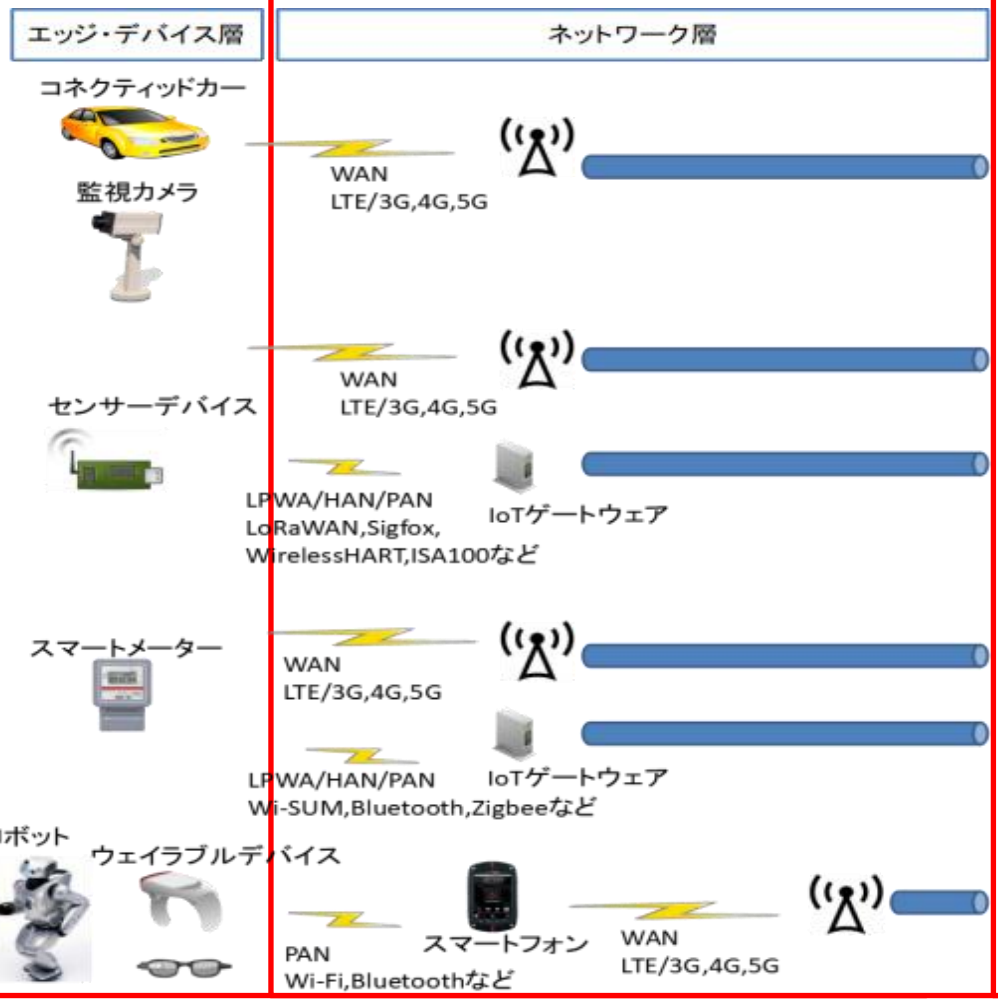
- IoT機器における組込み製品に対する全体的な視点をもって設計を行うことが必要となる。
- 組込み製品がシステム全体に及ぼす影響を踏まえたセキュリティ対策や設計が必要になる。
- スタンドアローンであった組込み製品は、IoTでの活用が必要になったことで、広いスキルが求められる。
  - ー　システム設計のスキル
  - ー　ネットワーク設計のスキル
  - ー　OSS活用などの開発プロセス改善のスキル

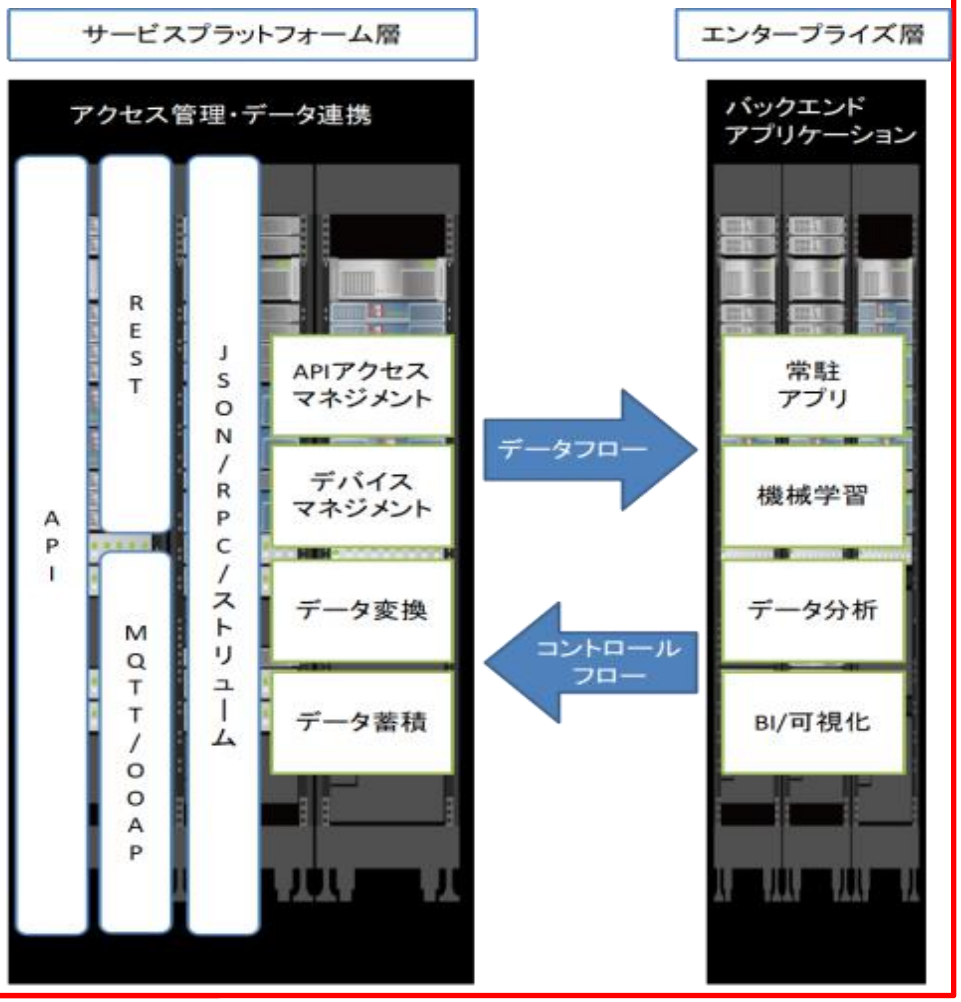
組込み製品開発スキル以外のスキルが求められる。

2. セキュリティ設計の視点と考え方

電気通信事業者の約款や契約内容などを確認する。

Cloud事業者の約款やサービス提供会社の契約内容などを確認する必要がある。





2. セキュリティ設計の視点と考え方

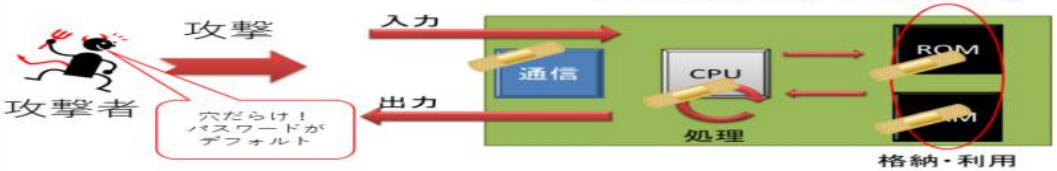
★ 組込み機器開発の範疇

エッジ・デバイス層

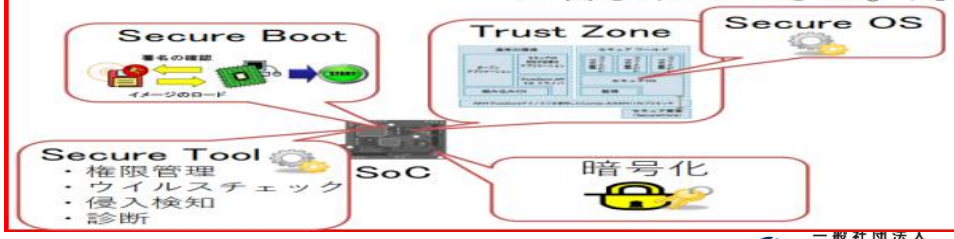
★**ハードウェアのリスク**：分解、基板の解析よってソフトウェアの解析が攻撃の準備に繋がる。

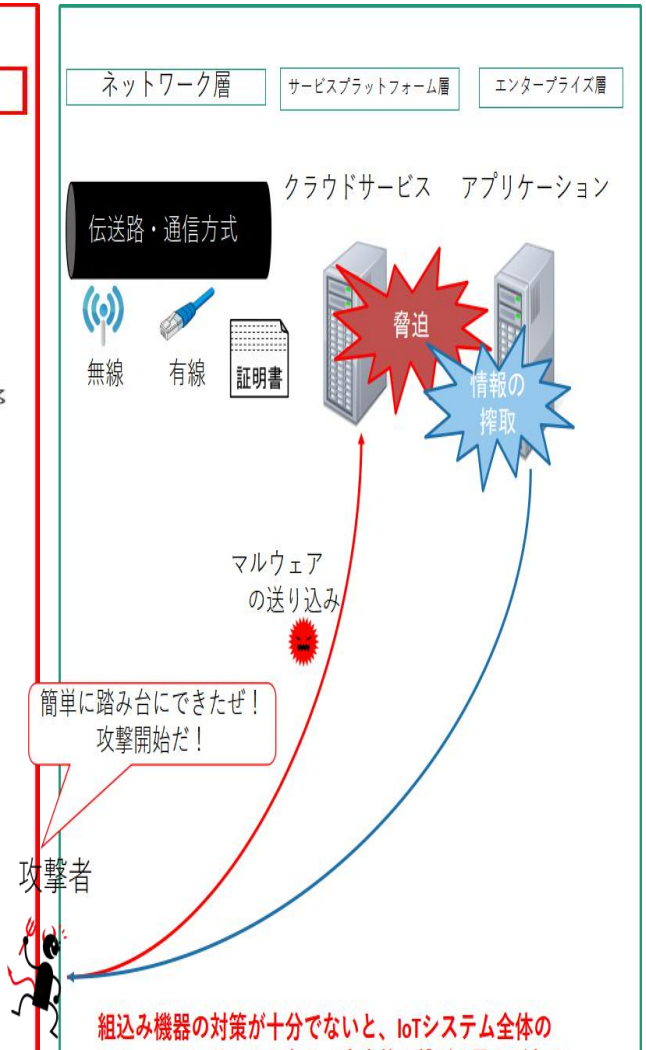
★**ソフトウェアのリスク**：OSSは公開情報なので、攻撃者は内部構造の解析・推測がしやすい。

★**開発スキル不足のリスク**：スキル不足のため「認識不足」「考慮不足」な対策で穴だらけの状態になっている。



★**開発コストのリスク**：セキュリティの対策コストが開発コストに含まれていない。対策できない。





2. セキュリティ設計の視点と考え方

■ IoTシステムにおいては、組込み製品開発での「エッジ・デバイス層」のセキュリティ対策を重視する必要がある。

- 組込み製品の対策が不十分であるとシステム全体の脆弱性につながる恐れがある。
- 組込み機器の視点においては、他の機器との連携した動作の「考慮漏れ」や組込み製品のセキュリティ機能の「誤った使い方」が脆弱性につながる。
  - スマートカードや携帯電話のUSIMなど一部の重要なコンポーネントのみでは不十分で、システム全体から考えた対策を考慮する必要がある。

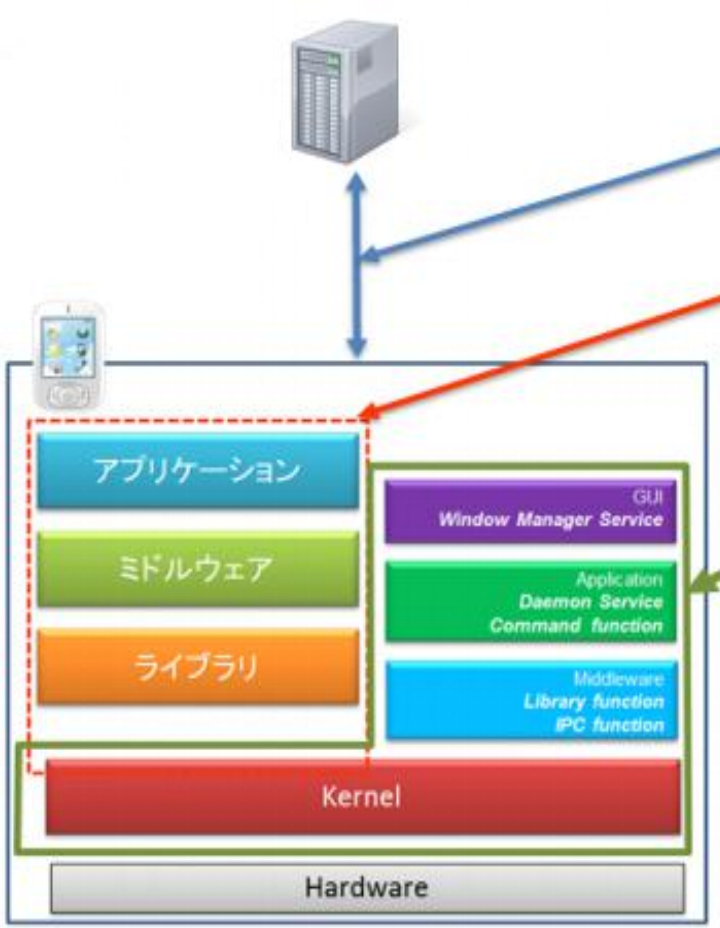
2. セキュリティ設計の視点と考え方

■　エッジ･デバイス層の脆弱性対策（案）

脆弱性の観点	概要
「記憶媒体」の脆弱性	不揮発メモリなどの記憶媒体に「ファームウェア」や「ファイルシステム」、暗号鍵、証明書などの「機徴情報」を平文で保存されているなど → 窃取、改ざんなどされ、攻撃の糸口となる可能性がある。
基板上の通信路における脆弱性	IoT機器が複数の基板からできている場合、基板間のデータの送受が平文になっていることが多い。基板上の信号線からデータをモニタリングすることで、「機徴情報」や「制御パラメータ」などが読み取られ、攻撃の糸口となる可能性がある。
デバッグ端子の脆弱性	プロセッサ/マイコンが備える保護機能を正しく利用していなかったり、デバッグ機能が無効化されていなかったりすることで、ファームウェアやメモリ状態などの読み書き可能となり、「機徴情報の読み取り」や「ファームウェア改ざん」など、攻撃の糸口となる可能性がある。
メンテナンスコンソールの脆弱性	メンテナンスコンソールが有効で出荷されると、シリアル通信端子、JTAG端子などから特権的な操作を行うことができる場合がある。無認証で操作できることも少なくない。認証が設定されていても、他の脆弱性と組み合わせて認証自体が無効化されることもある。
外部インタフェースの脆弱性	SoC持つ汎用インターフェース（USBやBluetooth、Wi-Fiなど）が攻撃を受ける可能性がある。例えば、USBでは、USBメモリ経由でのマルウェアの感染などが考えられる。 Bluetoothは暗号鍵を窃取して機器同士の通信を解析したり、なりすまして不正接続することも考えられる。
ファームウェア解析で判明した脆弱性	デバッグ端子を利用してファームウェアの抽出がされると解析することで、IoT機器の構成や外部からの通信データに脆弱性（サービス拒否や任意コード実行など）を解析され実際の攻撃の糸口となる可能性がある。 アップデートするファームウェアが公開されてDownload可能であれば、Downloadされ解析される恐れがある。

2. セキュリティ設計の視点と考え方

■　組込み機器の対策事例

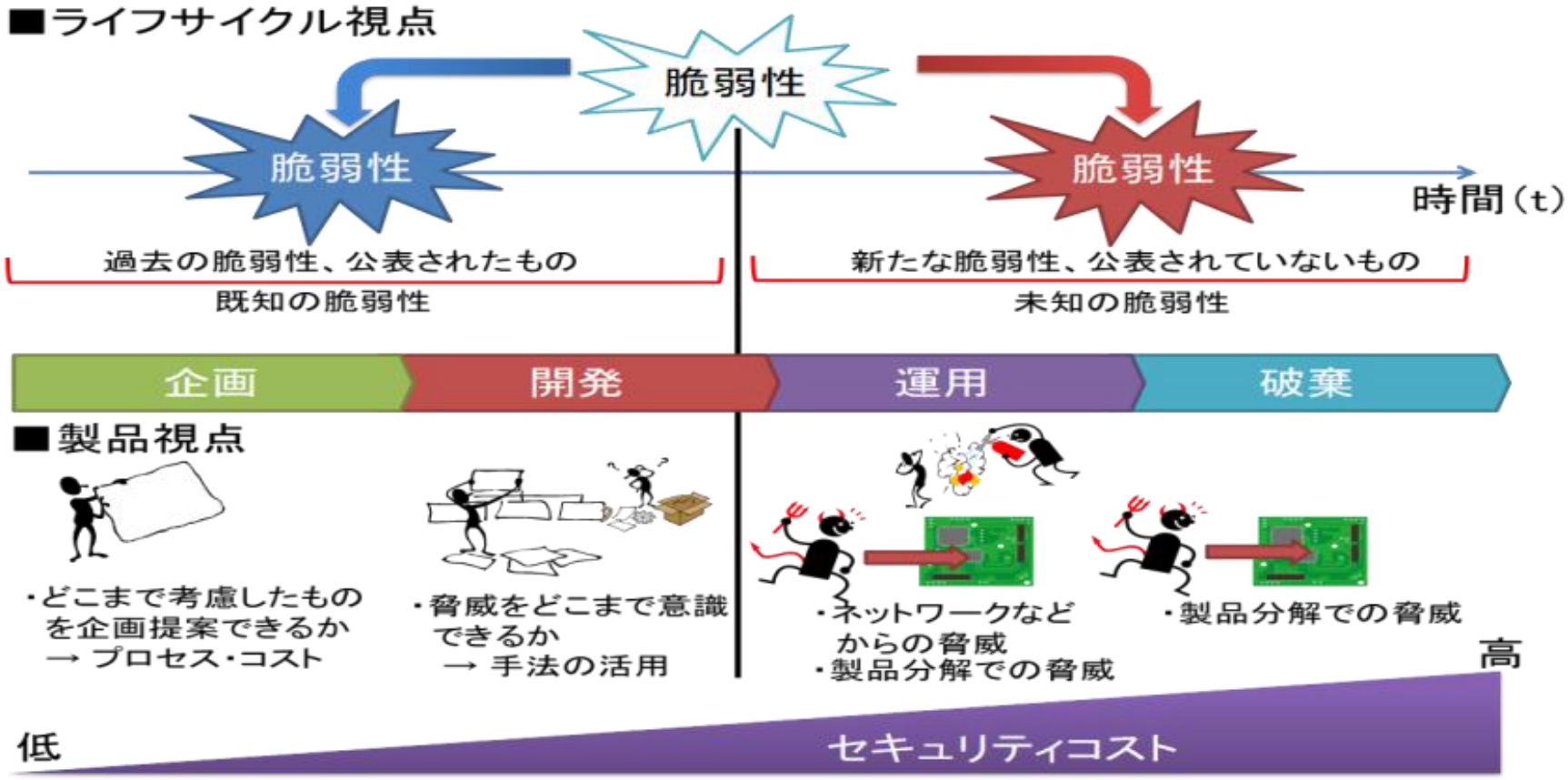


対策	説明	対策者	
		機器側	サーバ側
通信の暗号化	独自暗号でサーバと通信	アプリ	アプリ
デバッガ検知	デバッガを検知すると動作をとめる	ドライバ/アプリ	–
アプリケーション暗号化	インストールした以外の機器で動作していることを検知すると動作を止める	アプリ	–
暗号ロジックと暗号鍵の頻繁な変更	攻撃者に対して解析に十分な時間を与えない	アプリ	アプリ
パッチの迅速な適用	特権に昇格できるような脆弱性を塞ぐ	全般	–
Root化の検知	Root化を検知するとシステムロックをかける	全般	–
JTAGの無効化	秘密鍵を知らないとJTAGを利用できなくする。若しくは、JTAGを物理的に使えなくする	全般(ハード)	–
ストレージの暗号化	別の機器につないでも解析できない	全般	–

2. セキュリティ設計の視点と考え方

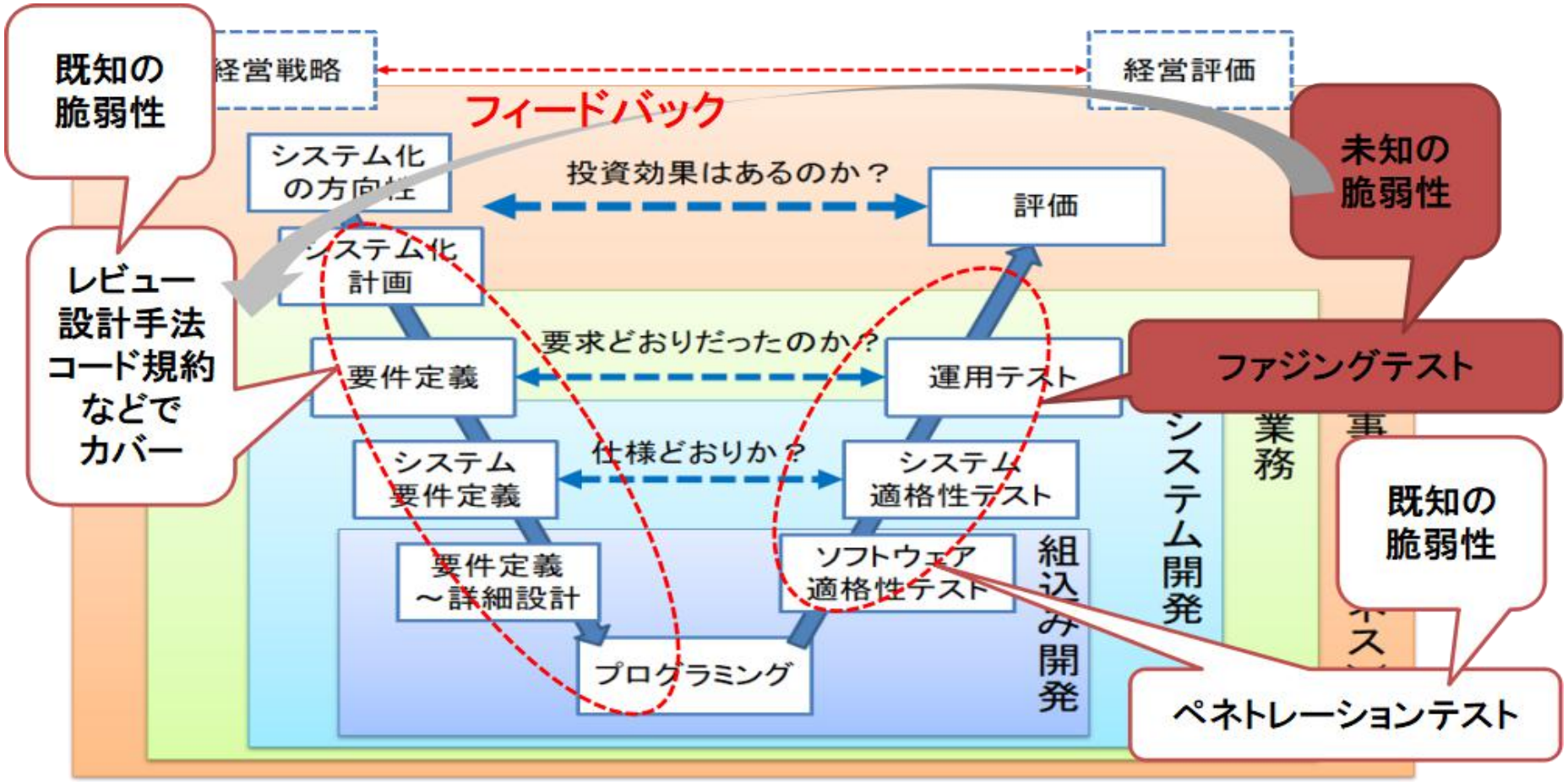
■ 製品ライフサイクルの考慮

- セキュリティ脅威は、時間とともに変化する。セキュリティ対策は、運用面の考慮をした上で、システム設計を実施する。



2. セキュリティ設計の視点と考え方

■ 開発プロセスでは、未知の脅威に対するプロセス改善を定義する必要がある。



2. セキュリティ設計の視点と考え方

■ 未知の脅威に対しては、セキュリティ関連の規定書にセキュリティテストを重視することと定義されていされている。

- テスト結果のフィードバックが上流での設計の対策向上につなげられる。

分野	文書	概要
情報セキュリティ全般	NIST SP800	セキュリティテストの1つとして実施を奨励している。
	重要生活機器連携セキュリティ協議会（CCDS）	未知の脆弱性検査手法として、実施を推奨している。
自動車	NHTSA	セキュリティ評価の手法として実施が奨励されいる。
	J3061	同上

2. セキュリティ設計の視点と考え方

■ 認証プログラムにおいてもテスト実施が定義されている。

分野	認証プログラム	概要
産業機器、医療機器	UL CAP (アメリカ)	ネットワークデバイスのソフトウェアに対するテストとして実施が定義されている
制御機器	EDSA (国際学会)	認証要求項目の堅牢制テストして実施が定義されている。

2. セキュリティ設計の視点と考え方

■ 2つの視点（まとめ）

- IoTシステムは、システム全体の視点が必要である点が分かった。
  - 特にエッジ・デバイスとなる組込み機器の対策に考慮漏れがあるとシステム全体の脆弱性につながるので対策は不可欠となる。
- セキュリティ脅威は、時間とともに進化する。設計段階の未知の脅威に対する設計考慮が必要となる。
  - 上流設計での結果を下流設計で対策漏れがないことを証明し、フィードバックして改善する。
  - 未知の脅威に対しては、ファジングテストが有用である。
    - ✓ OSSを使う場合は、テストと診断をした上で上流設計での考慮をする必要がある。

3. 簡易PKI認証システムの実証実験結果

3. 簡易PKI認証システムの実証実験結果

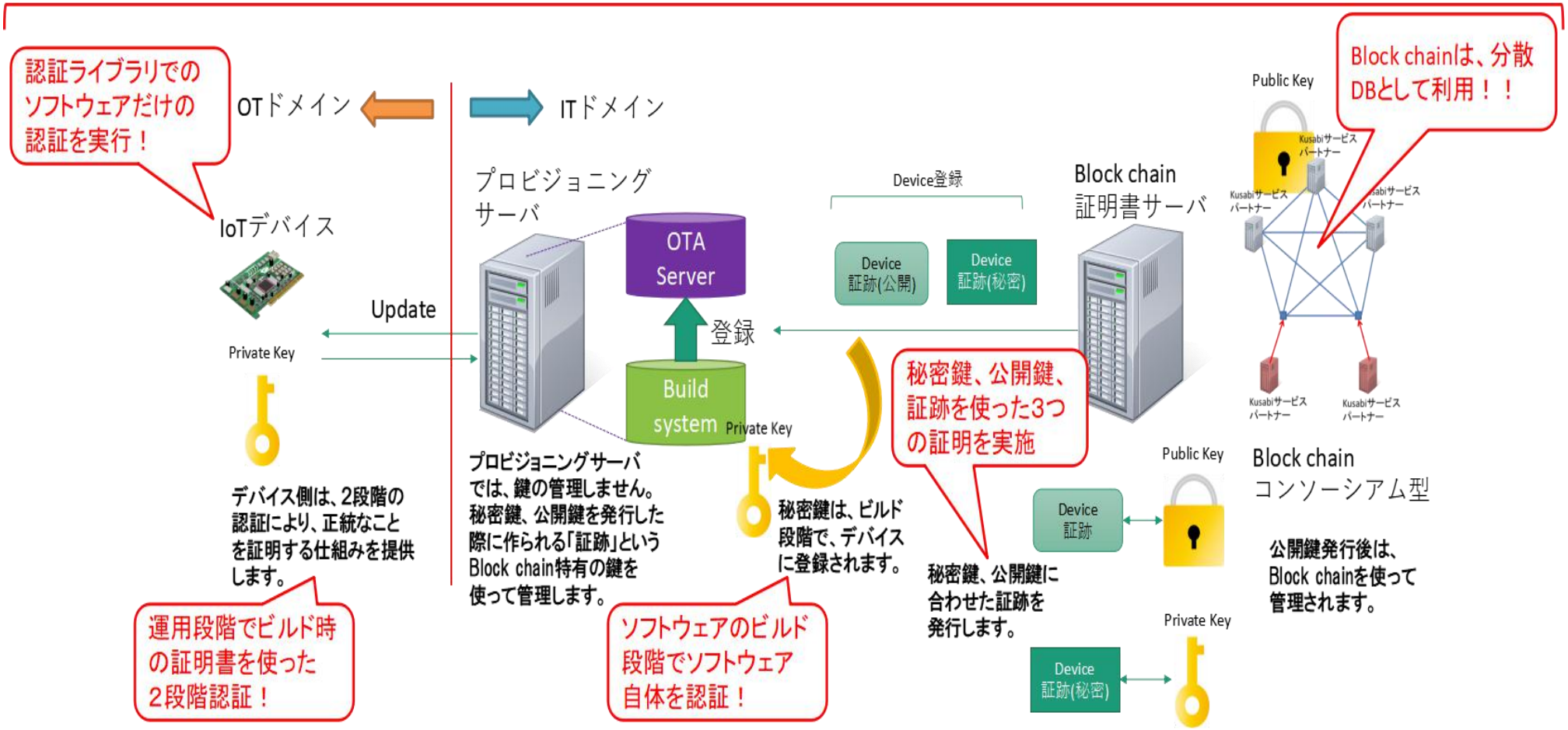
■ 目的としては、安価な組込み製品における運用をする場合に、Trust zone/TPMなどの高価なハードウェアを使わないIoT機器の管理・監視ができるシステムを検討した。

- 既存の認証局（中央管理）コストダウンとなる構成を検討
  - 分散管理した認証基盤を検討（Block chainの活用）
- パスワードなしでの機器管理が可能な構成を検討
- 専用ハードウェアデバイスを使わないで、ソフトウェアだけの認証方法を検討。
- 脅威に脅かされたときに検知し、自動的に正常な状態に戻すことを検討。
- 開発段階での認証を行える構成を検討。

3. 簡易PKI認証システムの実証実験結果

■ Block chainを活用したシステムの検討し、IoTデバイスの管理・監視ができるシステムを構築・実験を実施。

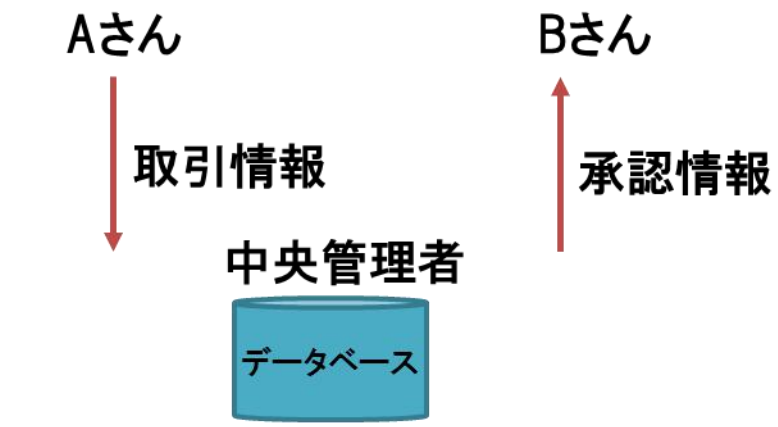
ハードウェアデバイスを使わず、ソフトウェアのシーケンスに工夫をした認証システムを実現



3. 簡易PKI認証システムの実証実験結果

■ Block chain利用メリット1

- 中央管理型のシステムでは管理者の一任となるが、Block chainを使うことで、分散データベース運用と参加者の合意形成ができ、真正性が向上できる点。



管理者が保有するデータベース上で情報を管理する。

図 中央管理型

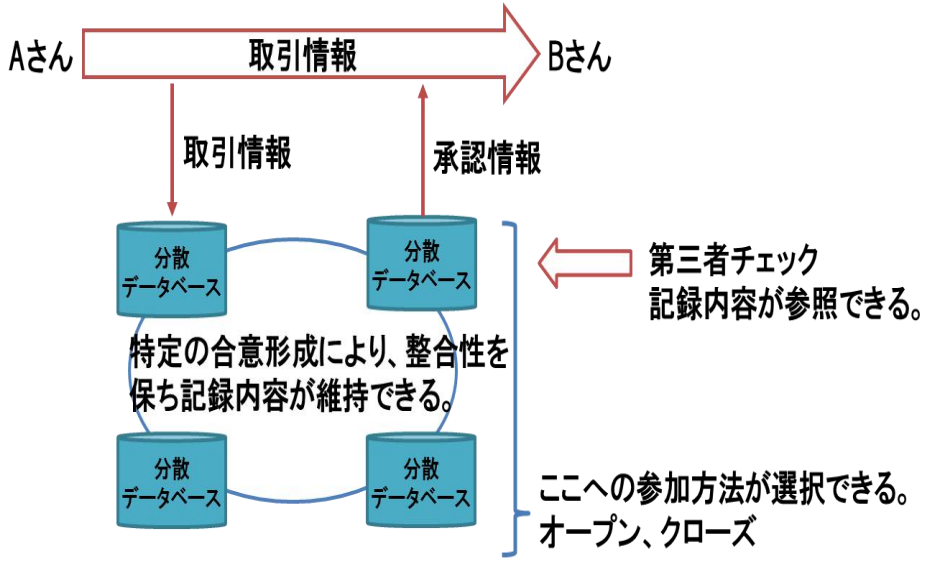
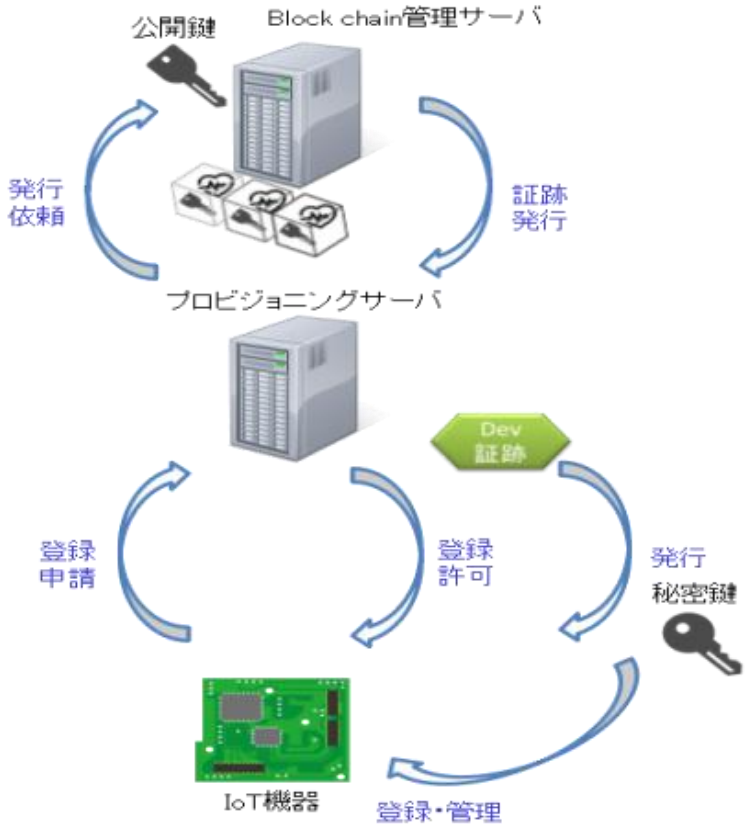


図 分散管理型

3. 簡易PKI認証システムの実証実験結果

■ Block chain利用メリット2

- 既存の認証局では人手を介した認証となるが、Block chainを使うことで自動的な認証が行え、有効期限を管理できる。



Block chain方式では、機器を管理するプロビジョニングサーバの管理で機器を管理することで、人手を介さないで、証明書の発行ができるようになる。
→ 青字の部分が自動化

IoT機器が運用される運用段階で証明書の発行ができるようになる。

Block chain特性を使うことで、追跡性の恩恵を受けられ、機器の状態管理、異常検知が行える。

証明書自体に有効期限がなく、機器が運用されている間は、自動化、分散管理ができるようになる。

従来の証明書管理では、サーバ証明のみとなるが、今回のシステムでは、サーバクライアント両方の認証が自動的に行える。

証明書管理後、通信は何でも使える。
→ データの取引情報をBlock chainにて管理できるので、改ざん検知、不正アクセス等が取引情報から確認できる。

パブリック型ではなく、プライベート型/コンソーシアム型を選択することで、管理主体者の制限、ネットワークの安定性が望める。

3. 簡易PKI認証システムの実証実験結果

■ 市販の安価なIoTデバイス（Raspberry PiやUpボードなど）を使って、「認証、監視、OTA（On The Air）」の検証を実施。

- 既存の認証局（中央管理）システムと同様の認証ができること、パスワードなしでの機器のID管理ができることが証明できた。
- 専用ハードウェアを使わずにソフトウェアのみで認証、管理できることを証明できた。
  - 開発段階から認証でき、運用フェーズで認証された状態で管理・監視できることが証明できた。
- 総務省「IoTの普及に対応した電気通信設備の技術基準等に関する制度整備」など省庁のガイドラインに合わせた運用ができていることも証明できた。

3. 簡易PKI認証システムの実証実験結果

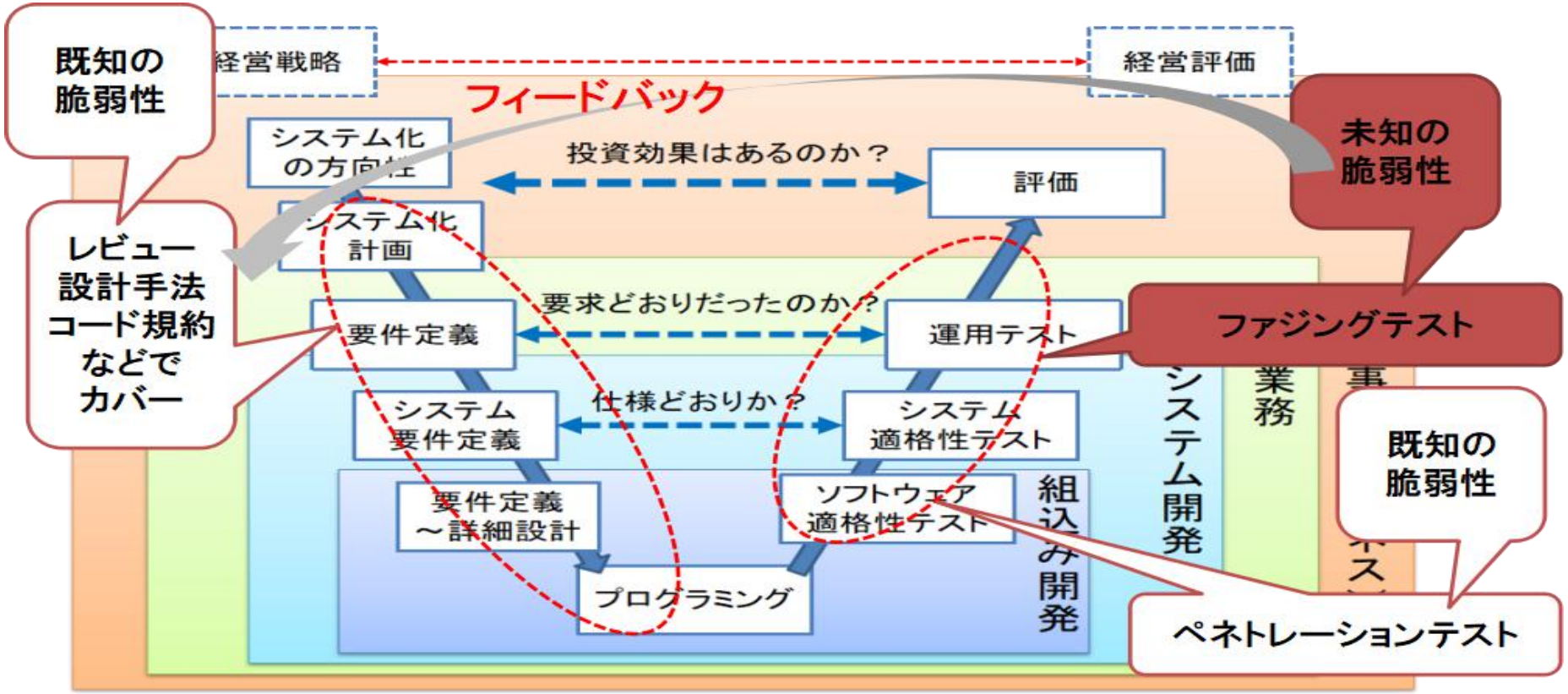
■ ２つの視点（まとめ）

- 認証・監視を安価にシステム実現することで、IoT機器の運用を低コストにできることが分かった。
  - ー パスワード認証を省くことで運用管理が簡易化できる。
- セキュリティ・バイ・デザインに代表されるように製品自体の設計は大事であるが、運用面を考えた全体システムを導入することで、脆弱性対策になることが分かった。

19年度 活動計画

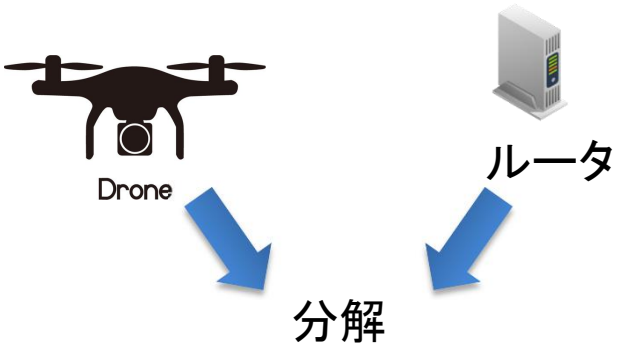
5. 19年度活動計画

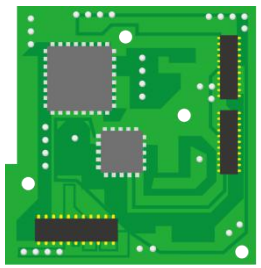
■ 実際のデバイスを使ったセキュリティに対する分析・検討を行い、セキュリティ設計のプロセス定義を実施する。



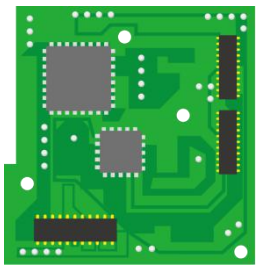
5. 19年度活動計画

■　イメージ

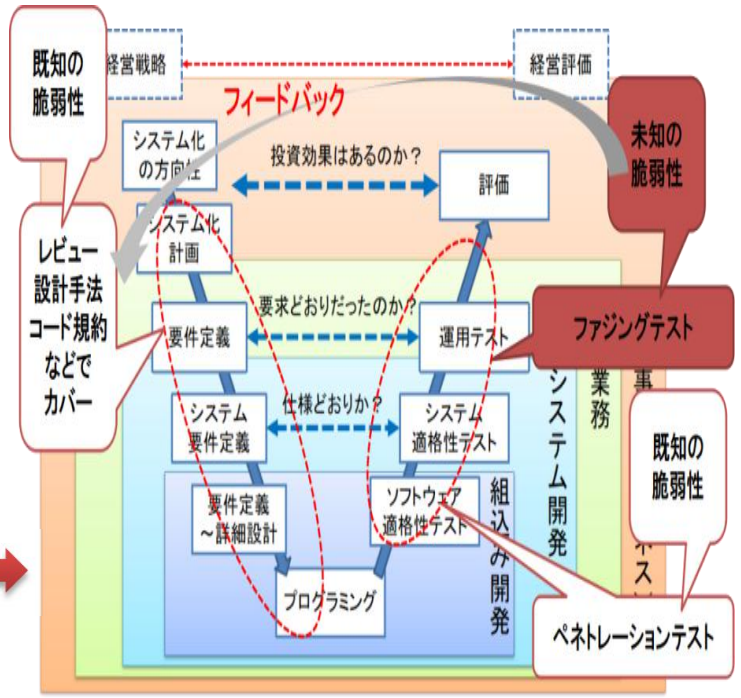




ハードウェアの
フィジカルな面
での分析検討
（基板回路も
分析対象）



ソフトウェアを
脆弱性診断して
分析検討
ファジング、脆弱性
診断ツールを選定適用

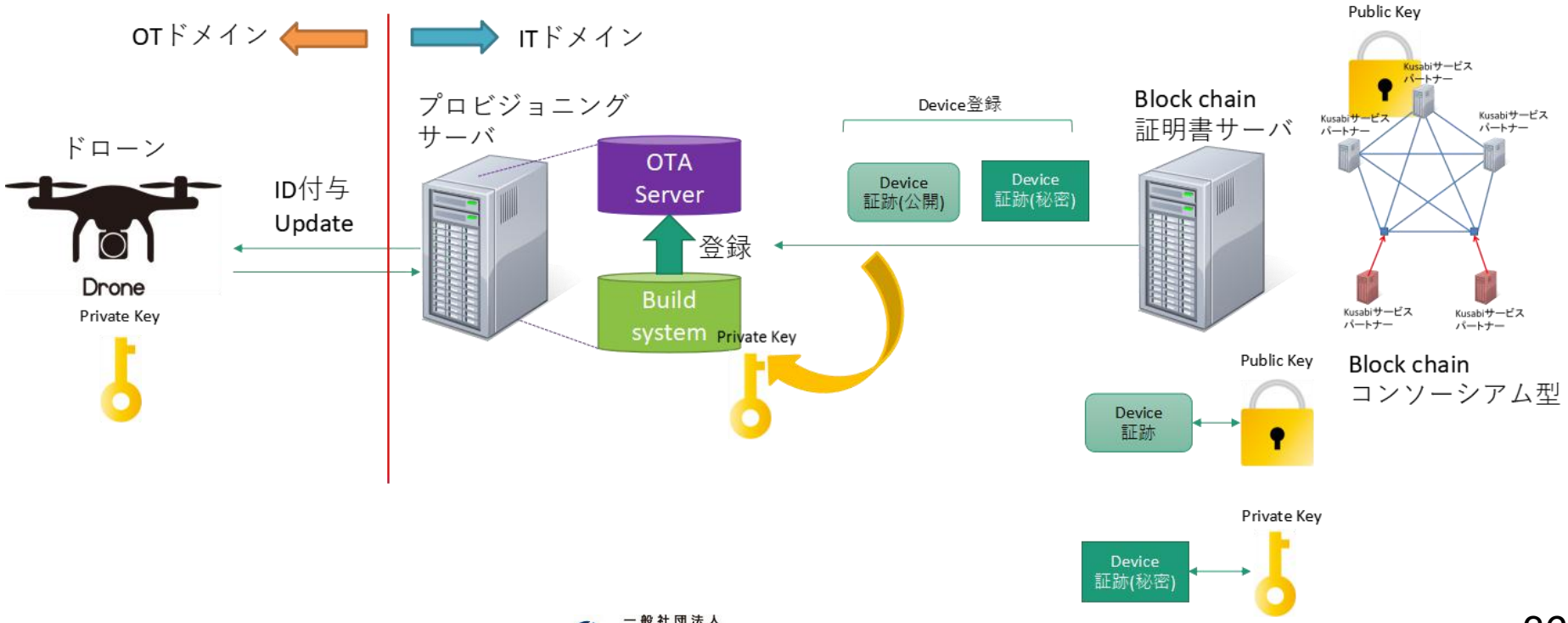


開発プロセスにフィードバックして
セキュリティ設計の定義を行う。

5. 19年度活動計画

■ 簡易PKIシステムの応用事例として。。。

- ドローンWGとの連携を図り、ドローンの認証・監視に応用することができること実証実験を行う。
  - ー システムの自動番号付与できる機能を使って、ナンバープレートとして利用できるか？の実証実験を実施予定。

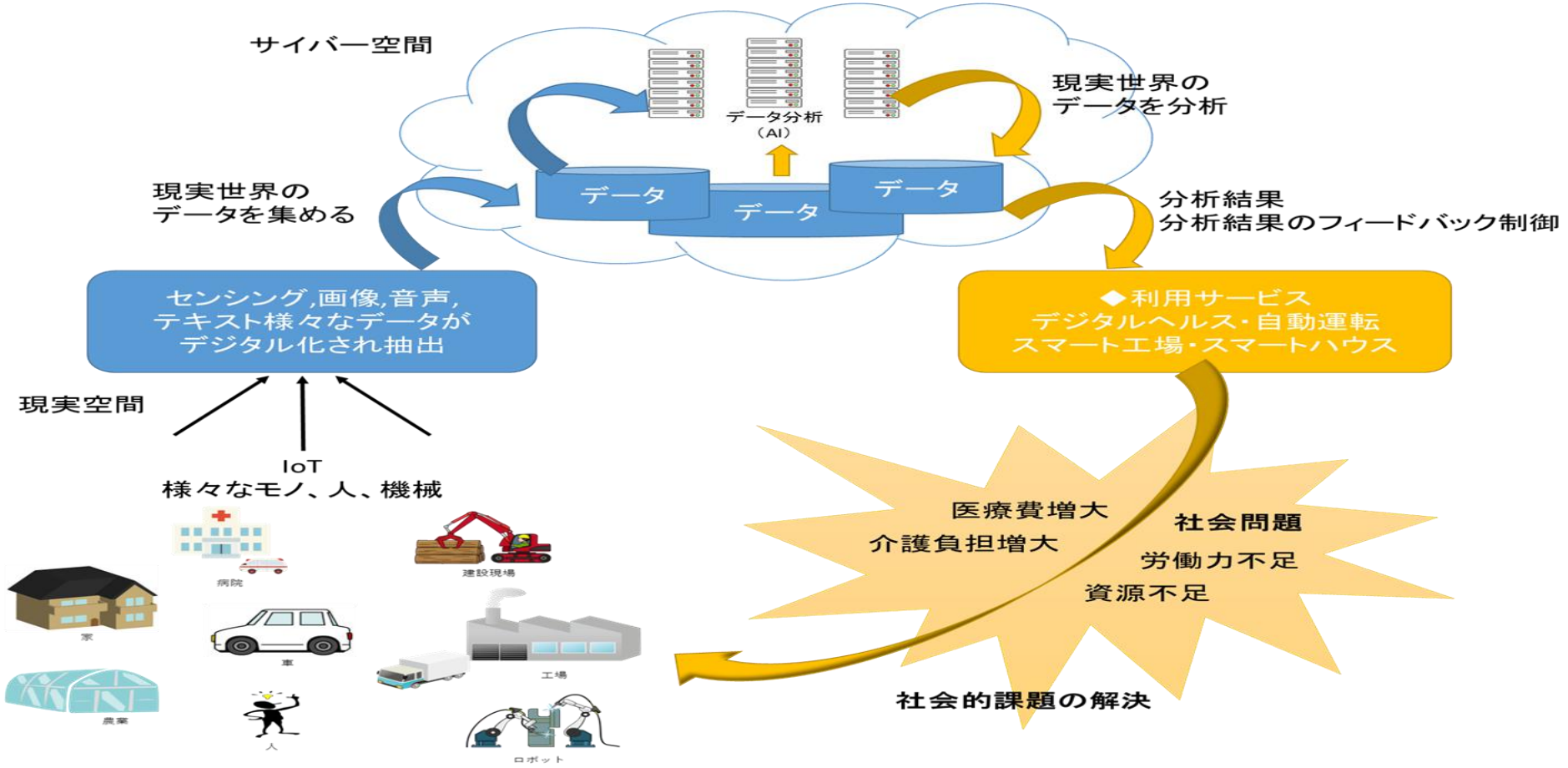


経営戦略としてのセキュリティ対策

1. 各省庁の動き

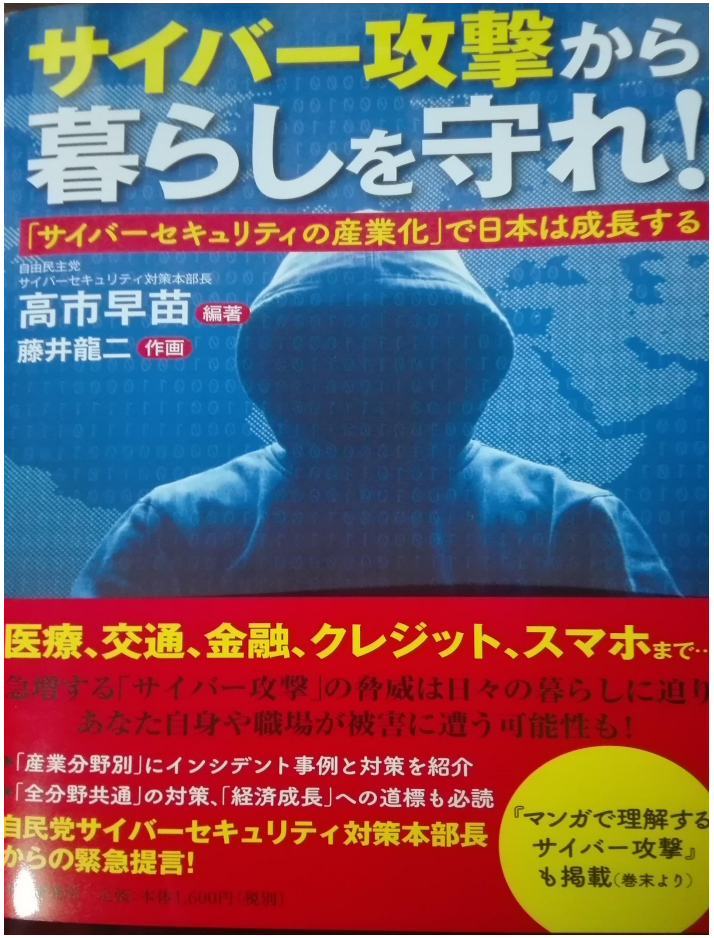
■ 内閣府

- Society（ソサエティ）5.0、Connected Industriesの社会



1. 各省庁の動き

■　自民党 サイバーセキュリティ本部



分野ごとのセキュリティ対策に関するセキュリティ対策をまとめたものです。

- 情報通信分野
- 航空・鉄道・物流分野
- 自動車・自動運転分野
- 医療分野
- 電力・ガス・水道分野
- 石油・化学分野
- クレジット分野
- 政府・行政サービス分野
- 安全保障分野

1. 各省庁の動き

■ 総務省

- 電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第1版）
  - ー 2019/4/22に公表されています。

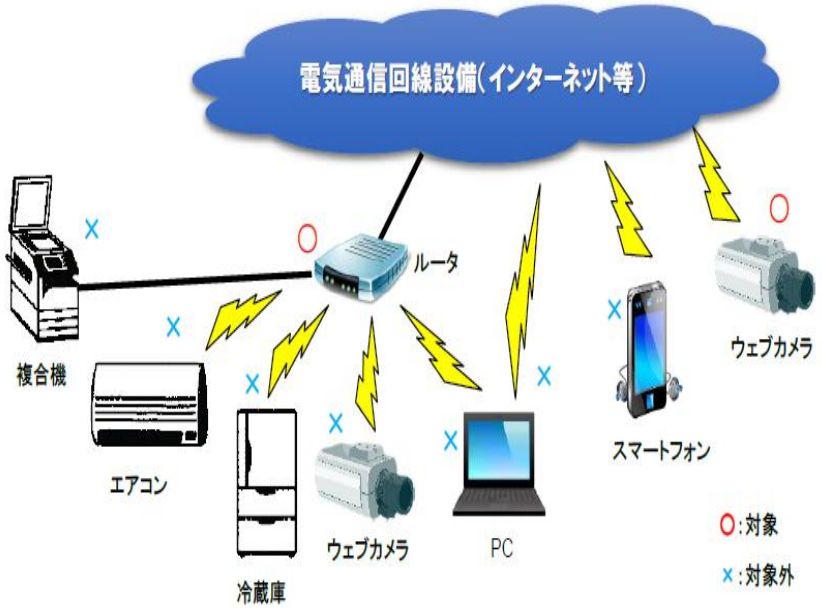


図1　セキュリティ基準（新規則第34条の10）に係る技術基準適合認定等の対象機器の範囲のイメージ

■省令改正の概要

①不特定多数からのアクセスを遮断できる機能
②IDやパスワードを初期値から変更を促す機能
③ソフトウェアを常に更新できる機能

これらの機能を持っていることを証明しなければ2020年4月以降には製品を出荷できない。

参考URL：http://www.soumu.go.jp/menu_news/s-news/01kiban05_02000179.html

1. 各省庁の動き

■ 厚生労働省

- 医療情報システムの安全管理に関するガイドライン 第5版

No	改定テーマ	主な改定内容
1	電子カルテの代行入力を時間経過で自動確定することへの言及	・診療録等の代行入力を行う際、時間経過で自動的に記録確定する運用がみとめられないこと明確化 ・記録の作成にかかわる当事者の役割を明確化
2	「製造業者による情報セキュリティ開示書」ガイドVer2.0への言及	・保健医療福祉情報システム工業会(JAHIS)標準及び日本画像医療システム工業会(JIRA)規格となっている「製造業者による医療情報セキュリティ開示書」ガイド(MDS)に言及
3	モバイルデバイスへの対応	・機器管理の運用管理規定の設定、データ暗号化、業務に不要なアプリのインストールはしない、公衆無線LAN利用時の基準設定BYODは原則禁止、覗き見防止策など
4	標的型攻撃への対応	・サイバー攻撃の具体例、連絡先、対処項目を追加 ・数世代分のデータのバックアップを推奨など
5	TLS1.2によるオープンネットワーク接続への言及	・インターネット等のオープンネットワークに接続する際は、TLS1.2に限定し、「SSL/TLS暗号設定ガイドライン」における「高セキュリティ型」の要求設定に則るべき旨を追記
6	小規模医療機関が順守すべき項目の明確化	・ガイドラインの本文の変更に伴い、医療機関の規模別運用管理の実施項目の見直し
7	医療情報システムの対象範囲の検討	・電子的な医療情報を取り扱う介護事業者及び医療情報連携ネットワーク運営事業者をガイドラインの対象として追加
8	IoTセキュリティへの対応	・総務省、経済産業省、IoT推進コンソーシアムが策定した「IoTセキュリティガイドライン」等、各種ガイドライン及び医療現場の状況を鑑み、修正
9	2要素認証の採用	・医療情報システムの2要素認証について、医療現場への影響を考慮し、猶予期間を設けて段階的に移行を進めること等を記載 ※猶予期間は、第5版公開から10年後を目処。
10	電子署名の採用	・平成28年度の診療報酬改定において、電子的診療情報提供書の算定要件に保健医療福祉分野の公開鍵(HPKI)による電子署名の採用が盛り込まれたことに合わせて修正

1. 各省庁の動き

■ 経済産業省

- サイバー・フィジカル・セキュリティ対策フレームワークの策定

階層	特性	機能・役割	分析対象	分析対象の具体的イメージ
第1層	各組織の適切なガバナンス・マネジメント	・各組織のセキュリティマネジメント [信頼性の基点]組織・マネジメント	・組織で管理されるモノ、システム等 ・組織内で流通するデータ等	・社員、従業員 ・企業のIT資産 等
第2層	フィジカル空間とサイバー空間の繋がり拡大	・フィジカル空間とサイバー空間との間のデータのやりとり [信頼性の基点]ルールに沿って正しくフィジカル空間とサイバー空間とを転写する機能	・データを転写するモノ・システム ・転写されるデータ等	・センサ ・アクチュエータ ・3Dプリンタ ・監視カメラ 等
第3層	サイバー空間で組織を超えた多様・大量のデータの流通・処理	・データの送受信、加工、分析、保管 [信頼性の基点]データ	・データを送受信/加工・分析/保管するモノ・システム等 ・組織を超えて流通するデータ等	・サーバ ・ルータ ・スマートメータ ・オープンデータ 等

参考URL：https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_1/pdf/001_06_00.pdf

1. 各省庁の動き

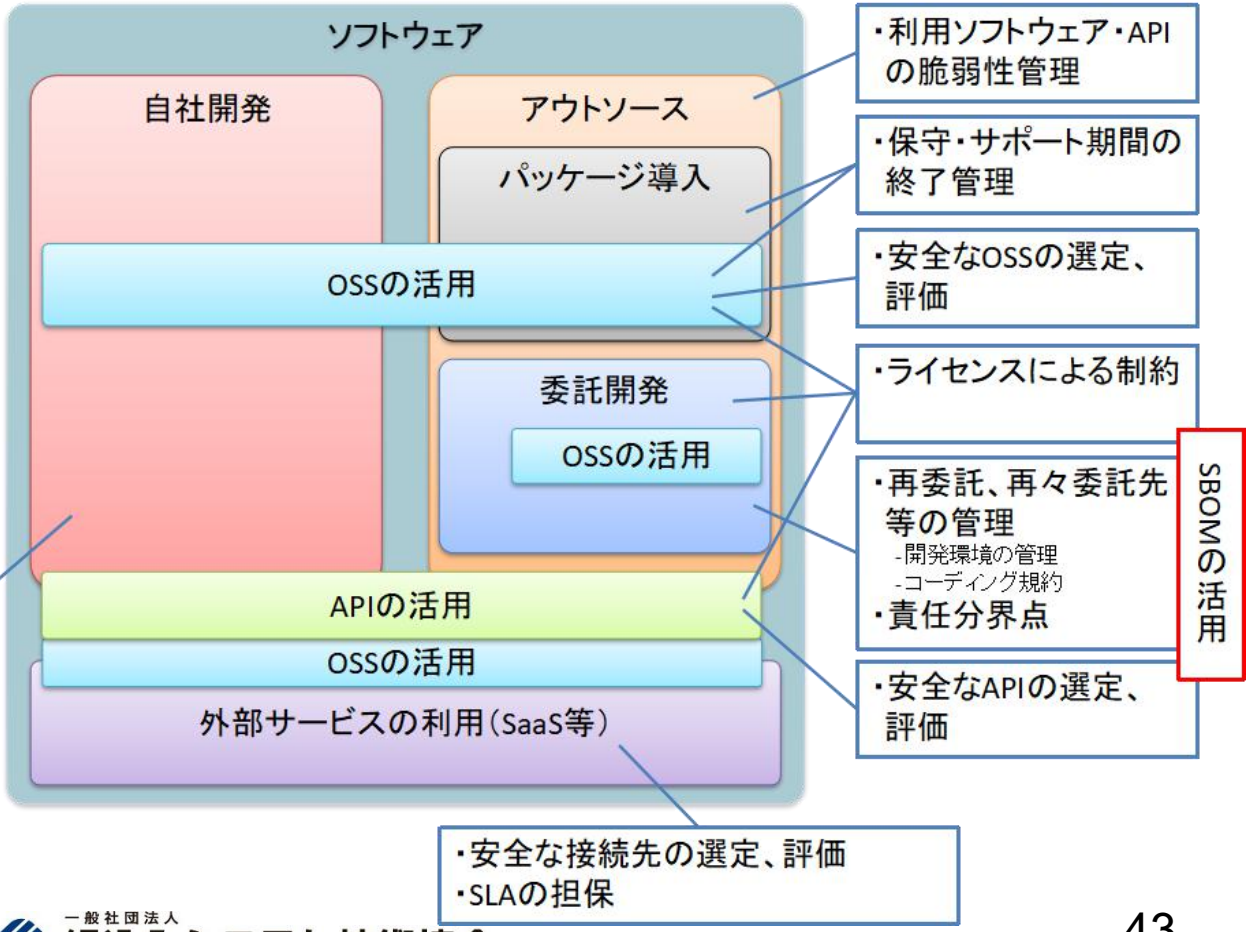
■ 経済産業省

- サイバー・フィジカル・セキュリティ対策フレームワークの策定
  - ー 安全なOSSの選定及び活用のための枠組みの検討例

検討されている内容

- OSSの安全性を評価するために必要な要件・体制
- OSSのライセンス評価
- OSS活用を前提とした契約のあり方
- OSS活用のベストプラクティス
- OSSコミュニティへの発信力向上

SBOMは、米国商務省電気通信情報局(National Telecommunications and Information Administration)で検討されている調達、サプライチェーンの要件



2. 各国の動き

■ アメリカ合衆国

- サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）の設置（2018年11月に設置）
  - ー 重要インフラ、医療機器などにも波及している。
- 2017年 サイバーセキュリティフレームワーク（NIST策定のガイドライン）にサイバーセキュリティマネジメント明記
- 2017年末 防衛調達に参加する全ての企業に対してセキュリティ対策（NIST SP800-171の厳守）を義務化
  - ー 実際は、NIST SP800-53で監査されるらしい。

参考URL：https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_1/pdf/001_05_00.pdf

2. 各国の動き

■ 欧州（EU）

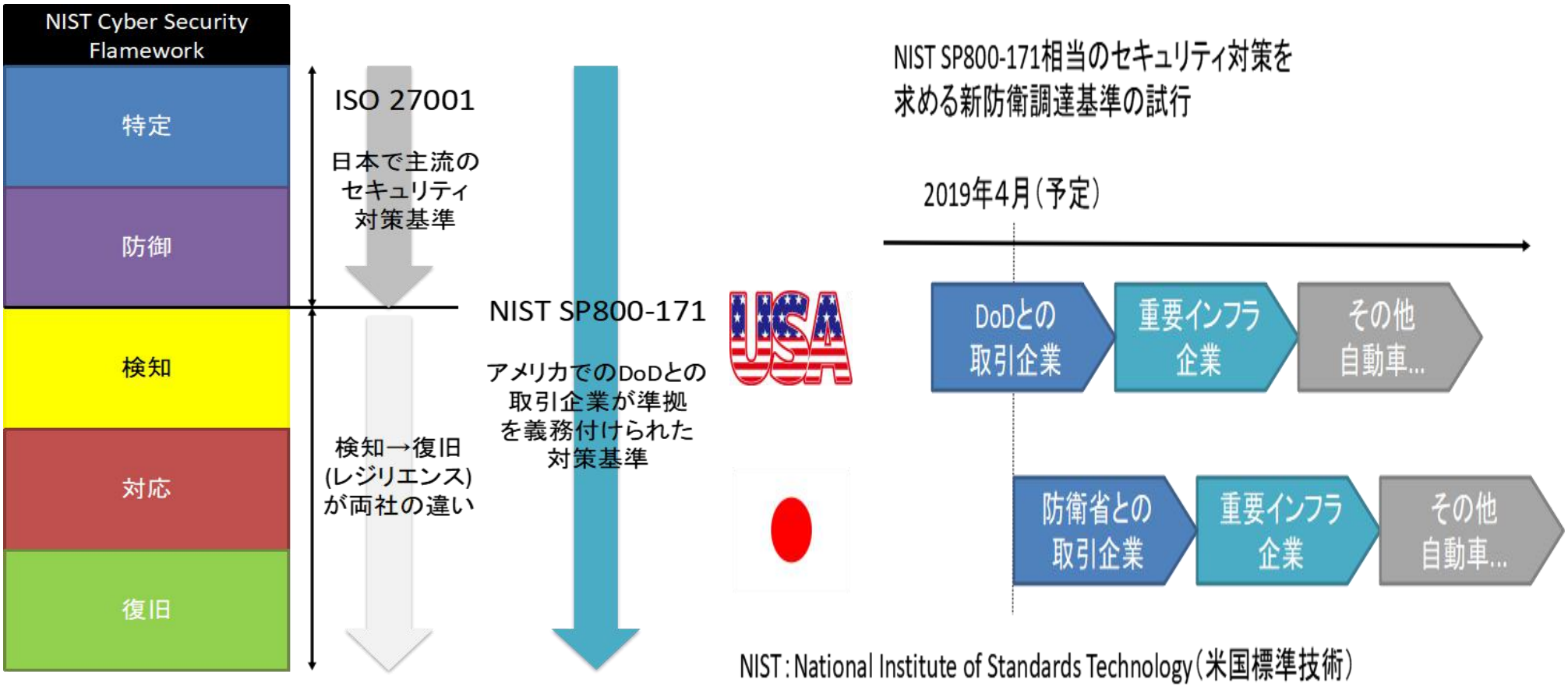
- 単一サイバーセキュリティ市場を目指し、ネットワークに繋がる機器の認証フレームの導入を検討。
  - ー 規制ではなく、自主的な仕組み 国際標準に基づく自己適合宣言
- 2016年、EU各国の重要インフラ事業者(エネルギー、交通、銀行、金融等)に対して、セキュリティ対策を義務化。
  - ー セキュリティ関連国際標準を考慮することを指示（NIS指令）
- 2018年から、EU顧客データを扱う企業い対して、データ処理制限、流出などの際の通知義務などをEU域外においても義務化
  - ー EU一般データ保護規則（GDPR）

参考URL：https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_1/pdf/001_05_00.pdf

2. 各国の動き

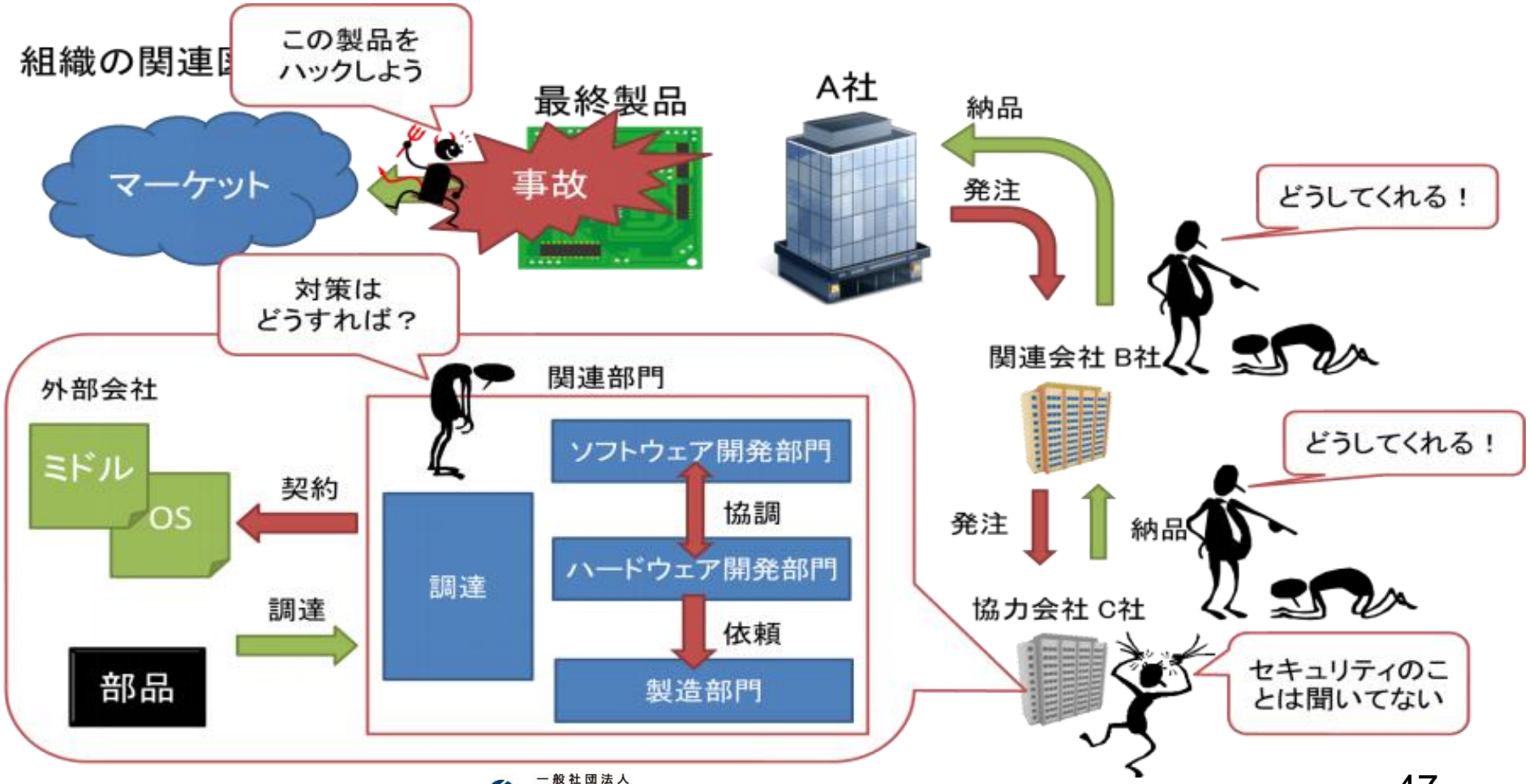
■ アメリカ合衆国

- 侵入前提のNISTセキュリティ対策が義務化の流れになる。



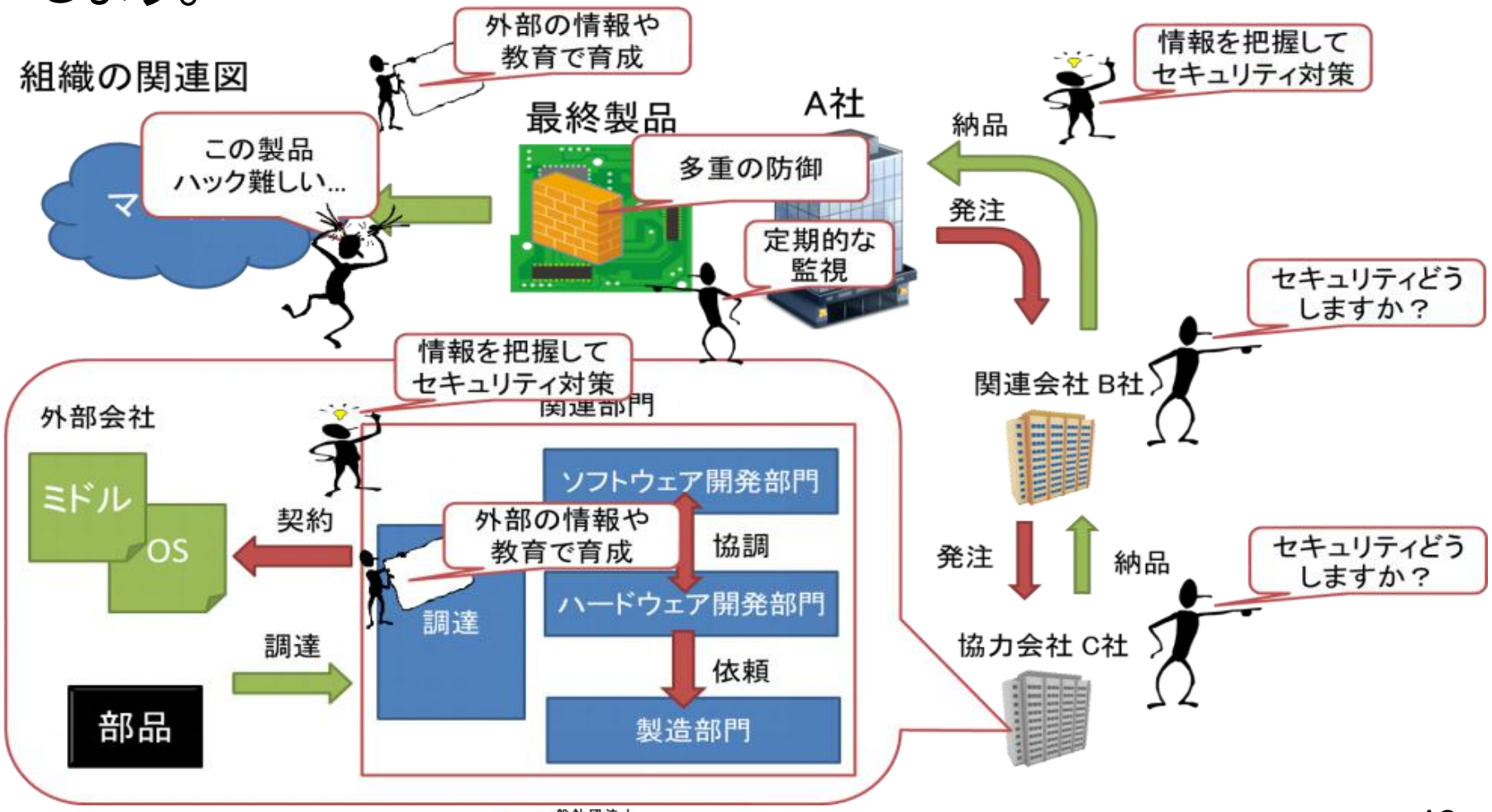
3. 世の中の動向から

■ セキュリティ対策が「コスト」→「経営戦略」となってきている。



3. 世の中の動向から

■ 「経営戦略」としてセキュリティ意識を向上していきましょう。



【講演タイトル】組込み機器開発におけるセキュリティの考え方

2019/5/20 発行

発行者　一般社団法人 組込みシステム技術協会
東京都中央区日本橋大伝馬町6-7
TEL: 03(5643)0211 FAX: 03(5643)0212
URL: http://www.jasa.or.jp/