IoTセキュリティ・デバイス管理における国際動向と標準化技術の方向性

セコム株式会社 IS研究所
暗号・認証基盤グループ
国井 裕樹

IoTの重要な要素：セキュリティとデバイス管理

- セコムは多数のセンサーを運用してサービスを提供
  - 全てのセンサーが正しく運用・管理されることで事業をスケール化
  - 機器のセキュリティの重要性ともに、デバイス管理の重要性を理解
- IoTシステムのサービス運用期間全般において機器をセキュアな状態で正しく管理することは簡単ではない
- 公開されているものとしては、AWSやAzureやArmなどからIoT機器のデバイス管理を目的としたサービスを展開
- セキュリティに関しては各国が法制度化を行ったり、認証スキームが始まったりしている

アジェンダ

- IoTセキュリティにおける各国の状況
  - 法規制
  - 認証制度
- IoTセキュリティ対策のスコープ
  - ハードウェアセキュリティの関連
- デバイス管理におけるIETFでの標準化
  - 既存サービス等と標準化技術との関係

アジェンダ

- IoTセキュリティにおける各国の状況
  - 法規制
  - 認証制度
- IoTセキュリティ対策のスコープ
  - ハードウェアセキュリティの関連
- デバイス管理におけるIETFでの標準化
  - 既存サービス等と標準化技術との関係

各国の状況

IoT 機器のセキュリティ基準に係る技術基準適合認定等（国内）

インターネット網に直接接続されるIoT機器を販売するためには2020年4月以降、以下の機能を実装したうえで技術基準適合認定（技適）を取得する必要がある

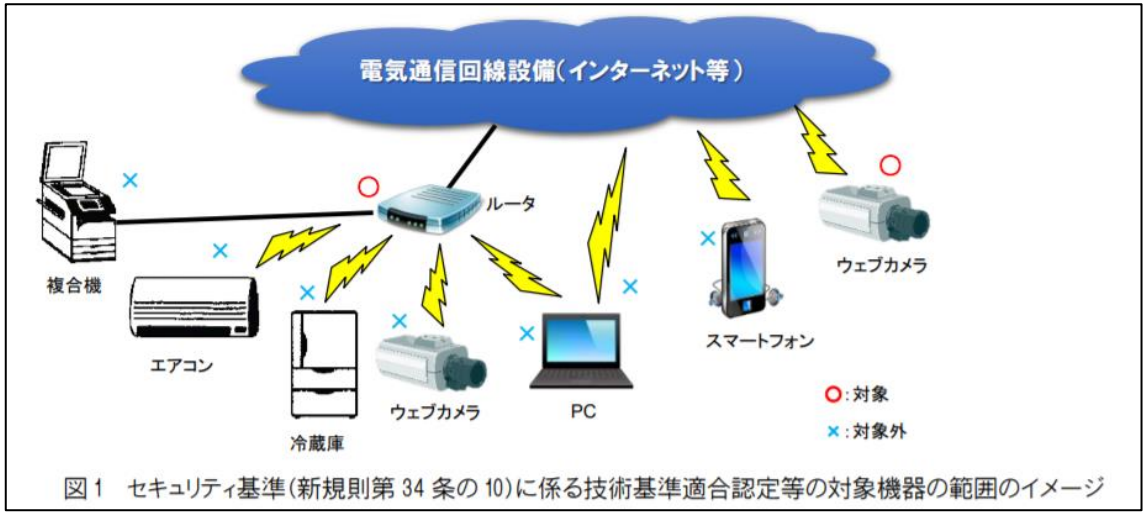


図１　セキュリティ基準（新規則第 34 条の 10）に係る技術基準適合認定等の対象機器の範囲のイメージ

出典： https://www.soumu.go.jp/main_content/000615696.pdf

1. アクセスコントロール機能と変更機能の実装
2. ソフトウェア更新機能の実装
3. 電源復帰後の設定維持機能の実装

各国の状況

カリフォルニア州のIoTセキュリティ法 [1798.91.04 - 1798.91.06](2020年1月施行)

IoT機器製造事業者に対して以下の2項目が義務として定められている

1. あらかじめプログラムされたパスワードは，製造された機器ごとに固有のものであること
2. 当該機器は，初回アクセスが許可される前にユーザーが新しい認証手段を生成しなければならないセキュリティ機能を備えていること

出典：福岡真之介, 北條孝佳, 沼澤周（訳）「米カリフォルニア州の IoT セキュリティ法について（日本語仮訳）」, https://www.jurists.co.jp/sites/default/files/newsletter_pdf/ja/ja_newsletter_1810_2_robotics-artificial-intelligence.pdf

イギリスのコンシューマ向けIoTデバイスのセキュリティ法規制（検討中）

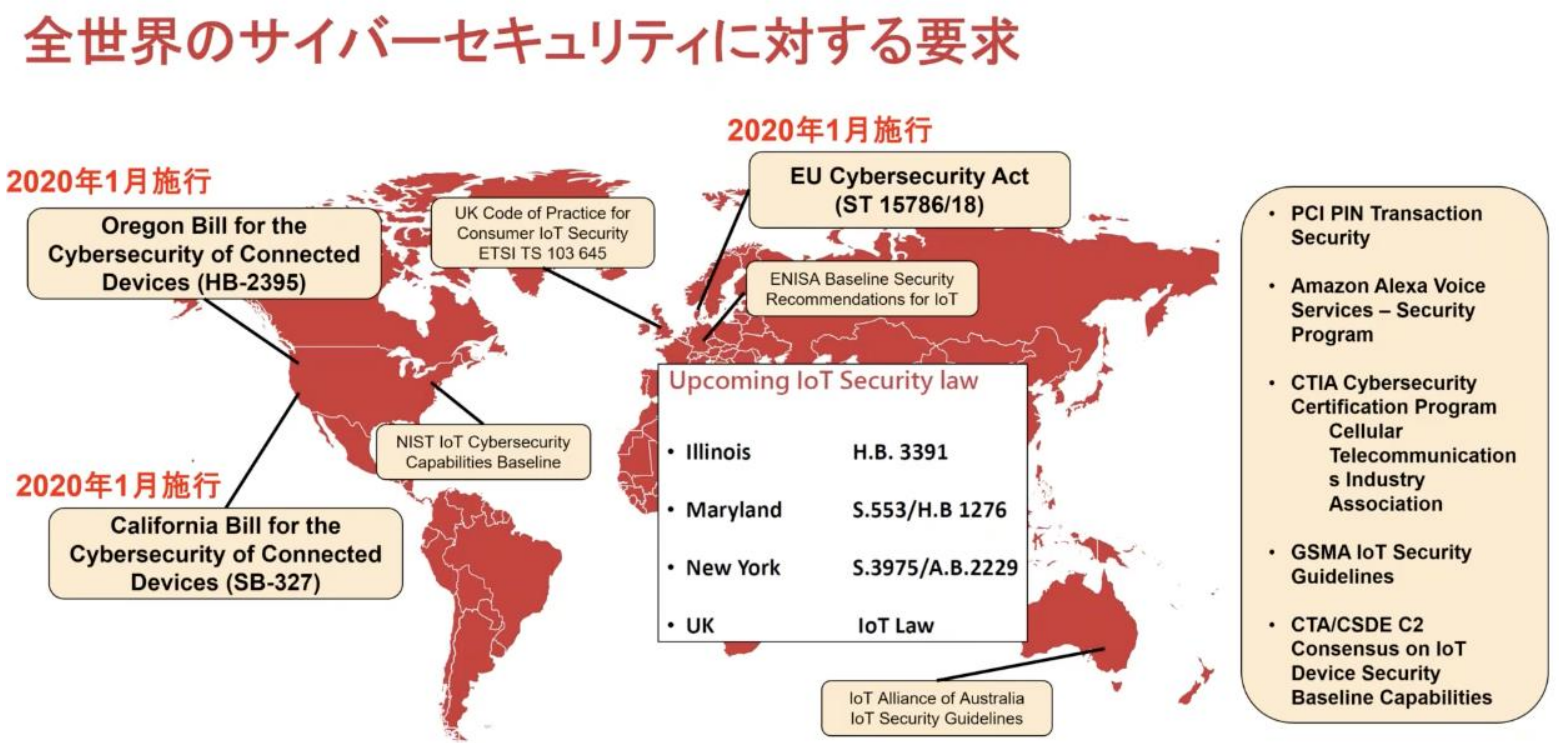
コンシューマIoTのセキュリティにおける指針

特に以下の3項目について強制力を持たせようと検討している

1. デバイス毎にユニークなパスワード設定
2. 脆弱性報告窓口を設置すること
3. セキュリティパッチの更新ポリシを提示すること

出典： https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

各国の状況

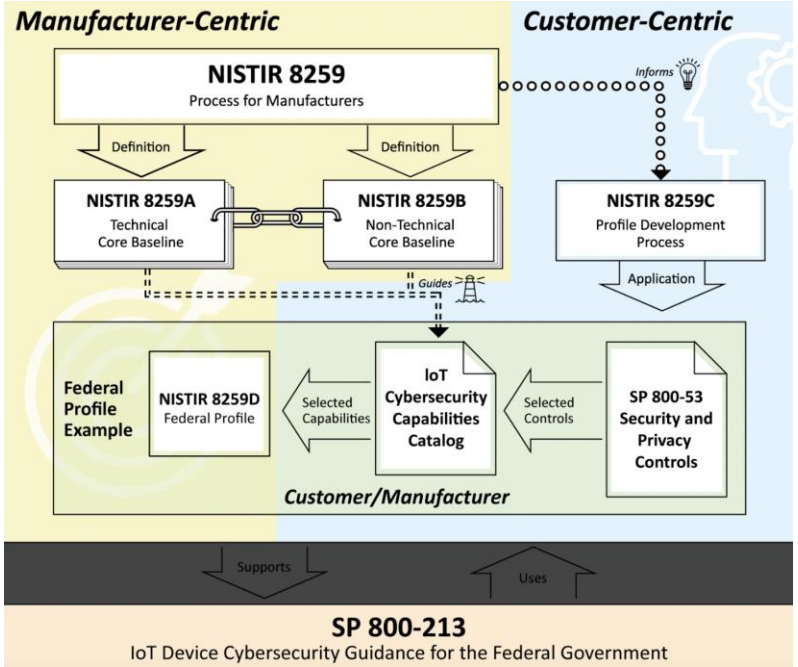


[出典]https://japan.ul.com/resources/iot_security_rating_video/

各国の状況

IoT Cybersecurity Improvement Act.

- 2020年12月に連邦法として制定
- 政府機関情報システムに接続されたIoTデバイスの適切な使用と管理に関する連邦政府の標準とガイドラインを作成するようNISTに指示
- 制定から180日以内に、情報システムに関連するセキュリティの脆弱性の開示プロセスに関連する基準とガイドラインを確立するように要求。
- これ以前にNISTはIoTセキュリティに関してSP800-213とIR 8259を発行済み（パブコメ中）
  - PSA Certified Level1にNIST IR 8259AやETSI TS 303 645をマップしていると主張している



[出典] https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity

各国の状況

IoT機器のセキュリティを認証・評価するようなスキームも確立されてきている

- SESIP(オランダ)：
  TrustCBが開発・運用していたIoT向けセキュリティ認証スキームSESIP（Security Evaluation Standard for IoT Platform）が発行されていたが、それにつながる形でGlobal platformからもSESIPが発行されている。様々なコンシューマIoTデバイス向けに利用されるようにモジュール化され、SESIP1～SESIP5までのレベルが用意されている。
- PSA Certified(イギリス)：
  Armが提唱するIoT機器のセキュリティフレームワーク（Platform Security Architecture）。脅威モデル、ファームウェアのセキュリティアーキテクチャ仕様、APIのテスト仕様などを提供しており、API仕様の準拠、セキュリティ機能の準拠性について認証プログラムを自己宣言のレベル1から第3者認証機関によるテストが必要なレベル2,3まで用意している。
- CCDSサーティフィケーションプログラム(日本)：
  メーカー等から構成される団体CCDSが提供する認証プログラム。IoT機器に対して分野共通のセキュリティ対策が実装されているかの確認であるレベル１から製品分野別の対策であるレベル２～レベル３について、メーカー自身もしくは第三者による検査によって認証される。認証された場合にIoTサイバー保険が自動で付帯することも特徴。

アジェンダ

- IoTセキュリティにおける各国の状況
  - 法規制
  - 認証制度
- IoTセキュリティ対策のスコープ
  - ハードウェアセキュリティの関連
- デバイス管理におけるIETFでの標準化
  - 既存サービス等と標準化技術との関係

IoTセキュリティ対策のスコープ

IoT機器のライフサイクル

一般的なIoTセキュリティのスコープ

サプライチェーンセキュリティ

サービス運用期間全般のセキュリティ

IoT機器の運用前におけるセキュリティ
- 設計開発段階において多くのセキュリティ機能が決定する。
- サプライチェーンでの物理、サイバー両面でのセキュリティが近年注目されはじめている

IoT機器の運用中におけるセキュリティ
- 多数のIoT機器を管理する場合、**自動化**が必須である
- リモート更新だけではなく、設定の自動化や開始時の完全性検証の自動化なども含まれる

IoTセキュリティの基本方策

以下のガイドライン等から基本的セキュリティ要件を抜粋
- IoTセキュリティガイドライン（経産省・総務省）
- 消費者向けIoTデバイスのサイバーセキュリティ基礎要求（ETSI EN 303 645）

ガイドライン	対策
アクセスコントロール・パスワード管理（保守ツールを含む）	デフォルトパスワードの個別化 証明書による認証・認可
リバースエンジニアリング対策	難読化・常時暗号化
FW・データの一貫性確保	セキュアブート・アテステーション
FWの自動更新・リモート更新	OTAアップデート・コードサイン検証
入出力のチェックデバッグ制御	セキュリティ評価・ファジングテスト
物理攻撃対策	耐タンパ性デバイスの採用
セキュリティバイデザイン・セキュリティ認証取得	セキュリティ設計・CC認証取得
暗号や認証の利用・ハードウェアによる暗号鍵管理	通信の暗号化・認証 セキュアチップの利用
初期設定の最適化	セキュリティ設計・ユーザビリティ評価
製品脆弱性報告窓口・レスポンス組織の設置	PSIRTの設置

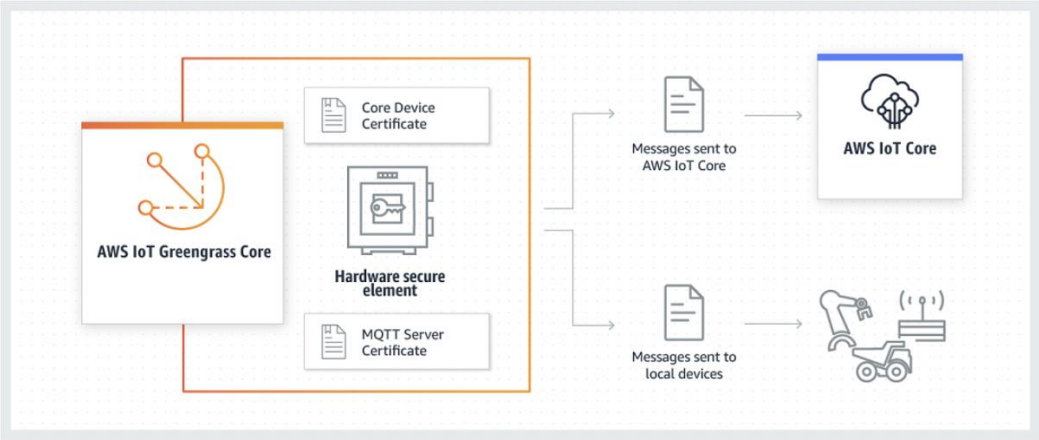
参考:ETSI EN 303 645におけるHWS

- 5.4 Securely store sensitive security parameters
  - Provision 5.4-1 Sensitive security parameters in persistent storage shall be stored securely by the device. Secure storage mechanisms can be used to secure sensitive security parameters. Appropriate mechanisms include those provided by a Trusted Execution Environment (TEE), encrypted storage associated with the hardware, Secure Elements (SE) or Dedicated Security Components (DSC), and processing capabilities of software running on a UICC, according to ETSI TS 121 905 [i.29], ETSI TS 102 221 [i.25]/embedded UICC according to GSMA SGP.22 Technical Specification v.2.2.1 [i.26].
  - Provision 5.4-2 Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.
  - Provision 5.4-3 Hard-coded critical security parameters in device software source code shall not be used.
  - Provision 5.4-4 Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.

ハードウェアセキュリティの実装事例

AWS Greengrass Hardware Security Integration(HSI)

- 2020.02.02時点で19デバイス
- NXPボード、スイッチ、Soracom SIM（接触ICとして利用）、AT ECC、YubiHSM、OptigaTPMが候補
- PKCS＃11インターフェースによってセキュアストレージや鍵の操作が可能
- 鍵はRSA2048以上かP256,P384が利用可能
- 秘密鍵作成、公開鍵取り出し、CSR生成まではベンダーツールを利用する前提



出典：https://www.arm.com/ja/why-arm/architecture/platform-security-architecture

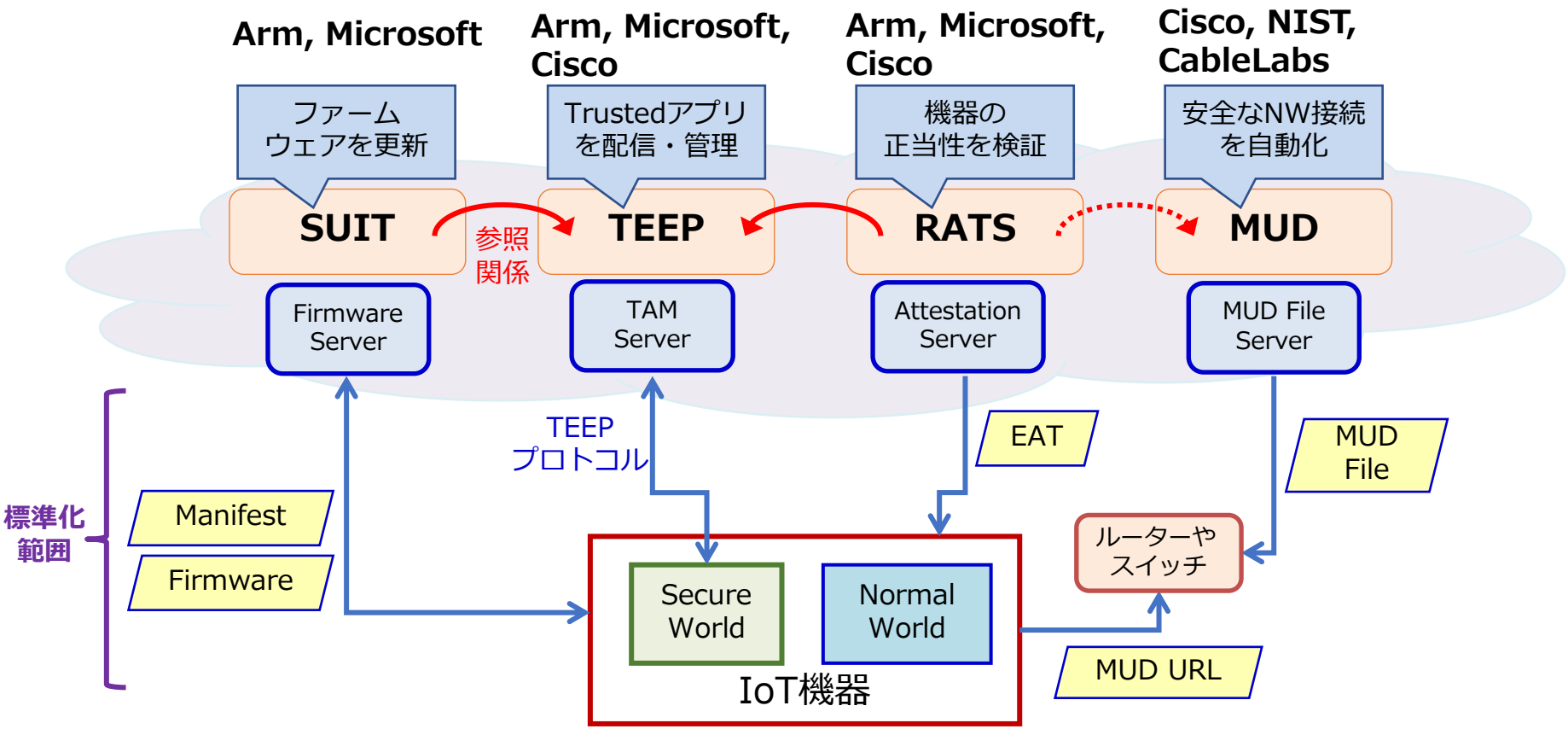
IoT向けハードウェアAPI

- PKCS#11
  - ICカードやPC等で長年広く使われてきてたAPI。鍵管理や暗号処理を中心にハードウェアやアプリケーションによらない抽象的なAPIを定義
  - PC向けの各種OSだけでなく組み込み向けOSやSoftHSMなどでもサポート
- PSA Functional APIs
  - Cryptography API, Secure Storage API, Attestation APIから構成される。PKCS#11に比べて現代的なアプリケーションを意識した具体性が高い構成。
  - mbed TLSなどで利用

アジェンダ

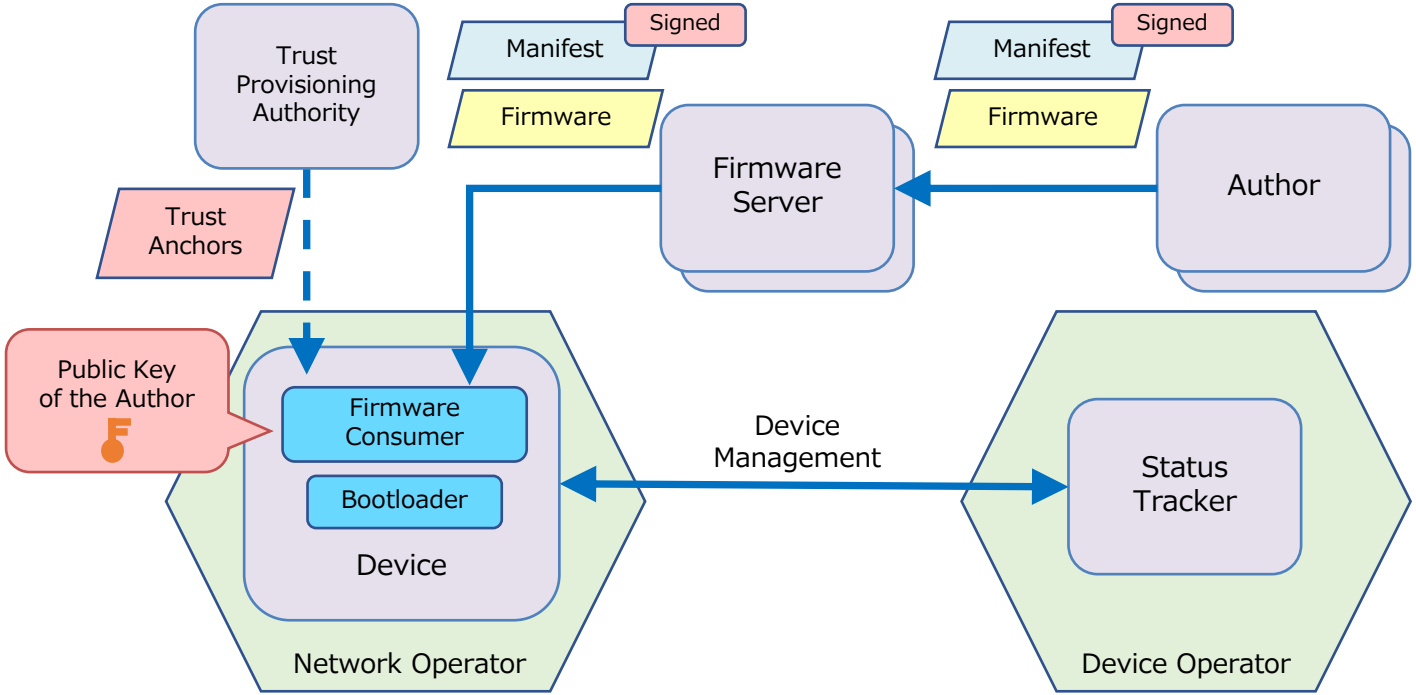
- IoTセキュリティにおける各国の状況
  - 法規制
  - 認証制度
- IoTセキュリティ対策のスコープ
  - ハードウェアセキュリティの関連
- デバイス管理におけるIETFでの標準化
  - 既存サービス等と標準化技術との関係

IoT機器の遠隔管理に関する標準化技術



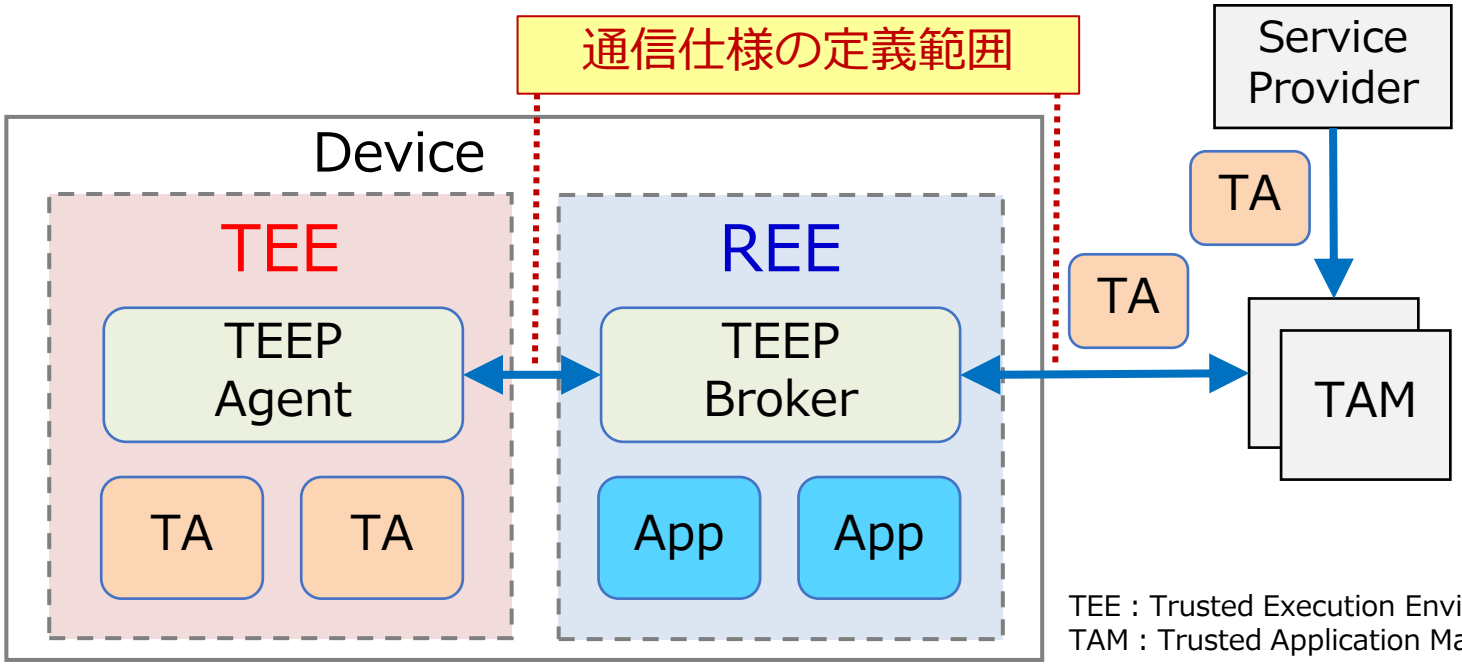
SUIT (Software Updates for Internet of Things)とは

- IoT機器の安全なファームウェア更新の仕組み
- Constrained Devices(～10KiB RAM, ～100KiB ROM)での動作を目標



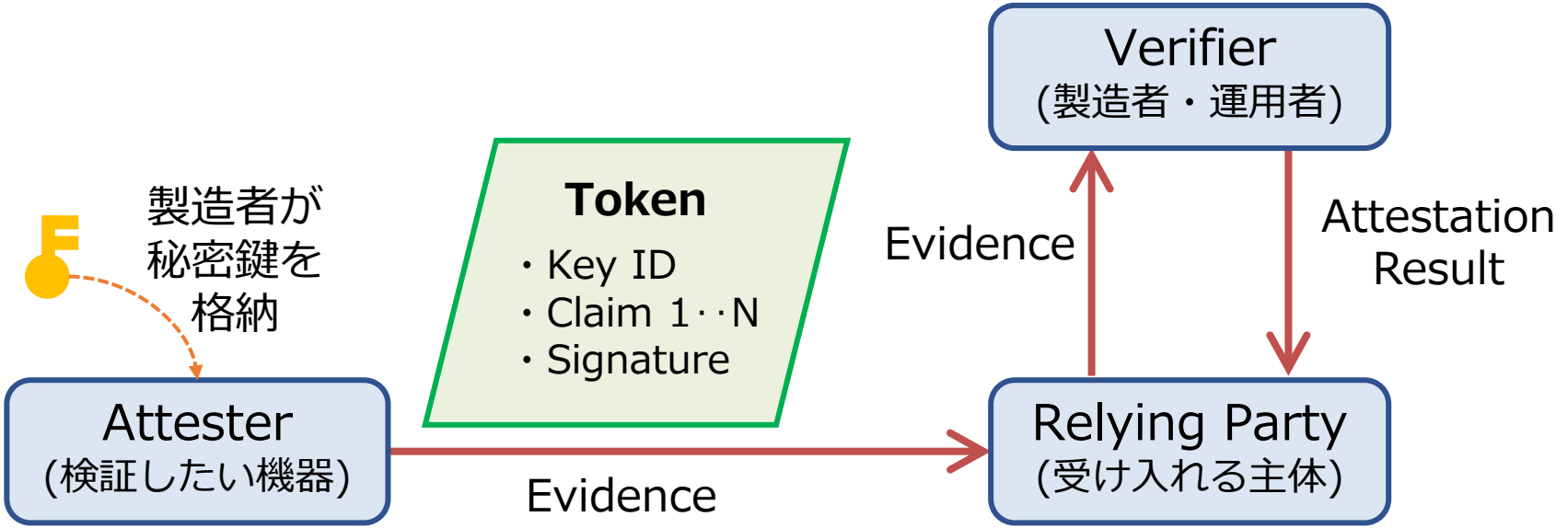
TEEP (Trusted Execution Environment Provisioning)とは

- 信頼できる実行環境（TEE）で動作するアプリ（TA：Trusted Application）を安全にインストール、実行、削除する仕組み



RATS (Remote ATtestation ProcedureS)とは

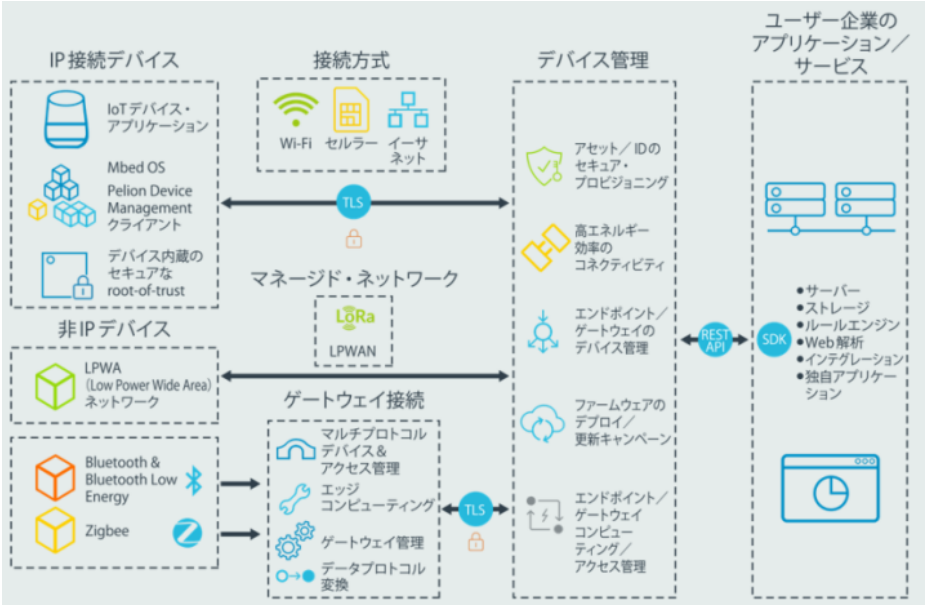
- Attestation：製品のセキュリティが保たれているか証明する仕組み
  - 製造元の正当性、HW/SWの完全性などを遠隔から検証



標準規格と既存サービス等の比較

Pelion™ Device Management

- Arm傘下のPelionが提供するクラウド型IoTデバイス管理サービス
- コネクション管理やエッジコンピューティングなどの機能もある
- OTA更新機能に用いられるマニュフェストとSUITを比較する



出典：https://www.arm.com/ja/products/iot/pelion-iot-platform/device-management

出典：https://www.arm.com/ja/why-arm/architecture/platform-security-architecture

Pelion Device ManagementとSUITの比較

ファーム更新のためのメタデータとしてManifestファイルがSUITで定義されているが、Pelionでのファーム更新でもManifestを作成する仕様となっている。両者を比較するとエンコード等の細かな違いもあるが項目に関しては類似点が多く、SUITのほうが標準規格である分、広範囲にカバーしている

Manifestの項目	SUIT	Pelion™
Vendor ID	✓	✓
Class ID	✓	✓
Image Digest	✓	✓
Use Before	✓	
Component Offset	✓	
Strict Order	✓	
Soft Failure	✓	
Image Size	✓	✓
Encryption Inof	✓	✓

Manifestの項目	SUIT	Pelion™
Compression Info	✓	
Unpack Info	✓	
URI	✓	✓
Source Component	✓	
Run Arguments	✓	
Device ID	✓	✓
Minimum Battery	✓	
Priority	✓	✓
Payload type		✓
Storage Identifier		✓

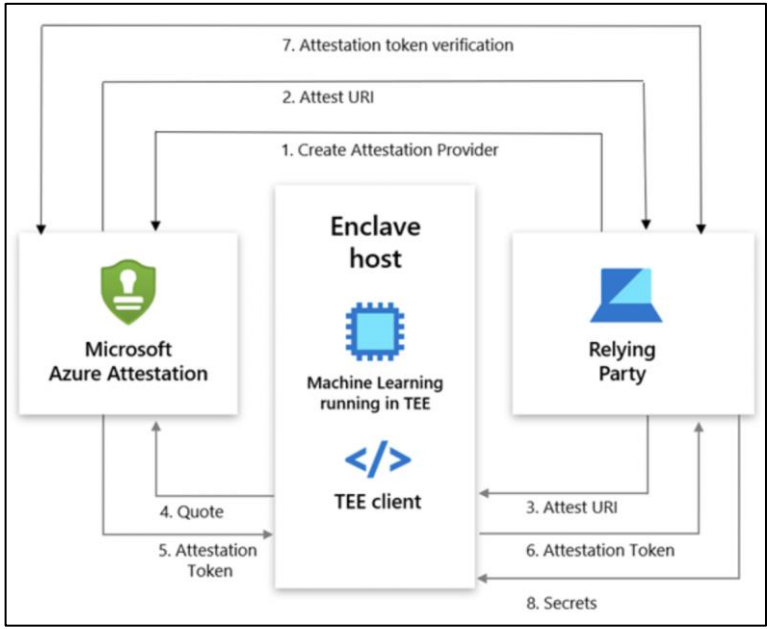
Platform Security ArchitectureでのAttestation

- RATSのEntity Attestation Token(EAT)の標準化と深い関係
- EATはIoT機器が自身のセキュリティ状態をクラウドサービス側に伝達するTokenのデータ仕様
- PSAでもRemote Attestationが必要とされており、Tokenの互換性が一定程度ある
  - 具体的にはTokenの内容であるClaimにはPSA独自のものも含まれるが、フォーマットはEATと同一のCWT(CBOR web Token)となっている
- 詳細は左のホワイトペーパーに書かれている

出典：https://www.psacertified.org/app/uploads/2020/02/PSA_Certified_Entity_Attestation_Overview_Whitepaper.pdf

Microsoft Azure Attestation

- Intel SGXやOpen EnclaveといったTEEや、従前からあるTPMでのAttestationを実現するサービス
- ユーザーはAttestationポリシを作成してサービスをデプロイするとポリシに従ってAttestationを行ったデバイスにオンボーディングなどの認可を行うことが可能
- ポリシのカスタマイズは容易でカスタムクレームをセットできる
- SGX用の固有クレームも準備されている



Azure Attestationの概要

出典：https://techcommunity.microsoft.com/t5/microsoft-security-and/microsoft-azure-attestation-is-now-generally-available/ba-p/2156693

PSA・AzureとRATS(EAT)の比較

Claimの項目	EAT	PSA	Azure
Token ID	✓		✓
Timestamp	✓		✓
Nonce	✓	✓	✓
UEID	✓	✓	
Origination	✓		
OEM ID	✓		
Hardware Version	✓		
Software Description and Version	✓	✓	
Security Level	✓		
Secure boot	✓	✓	
Debug Status	✓		
Including Keys	✓		
Location	✓		
Uptime	✓	✓	
Intended Use	✓		
Profile	✓	✓	

Attestationで利用されるTokenのデータモデルを比較した。
RATSで定義されているEAT（Entity Attestation Token）はSUIT同様、標準として利用されそうな項目を広く定義しているのに対して、PSAとAzureで共通している項目はNonceの1項目のみと少ない。

PSA、Azureともにここには表記していない項目が多数あり、各ベンダごとに必要な項目が異なっている事がわかる

まとめ

- IoTセキュリティに関する制度化・認証・標準化が進んでいる
- IoTセキュリティに関する実装も増加
  - デファクトが存在する
  - 標準を意識した実装も見受けられる
  - ハードウェアセキュリティに関連するエリアもある
- 今後の流れを引き続き注視していくことが重要