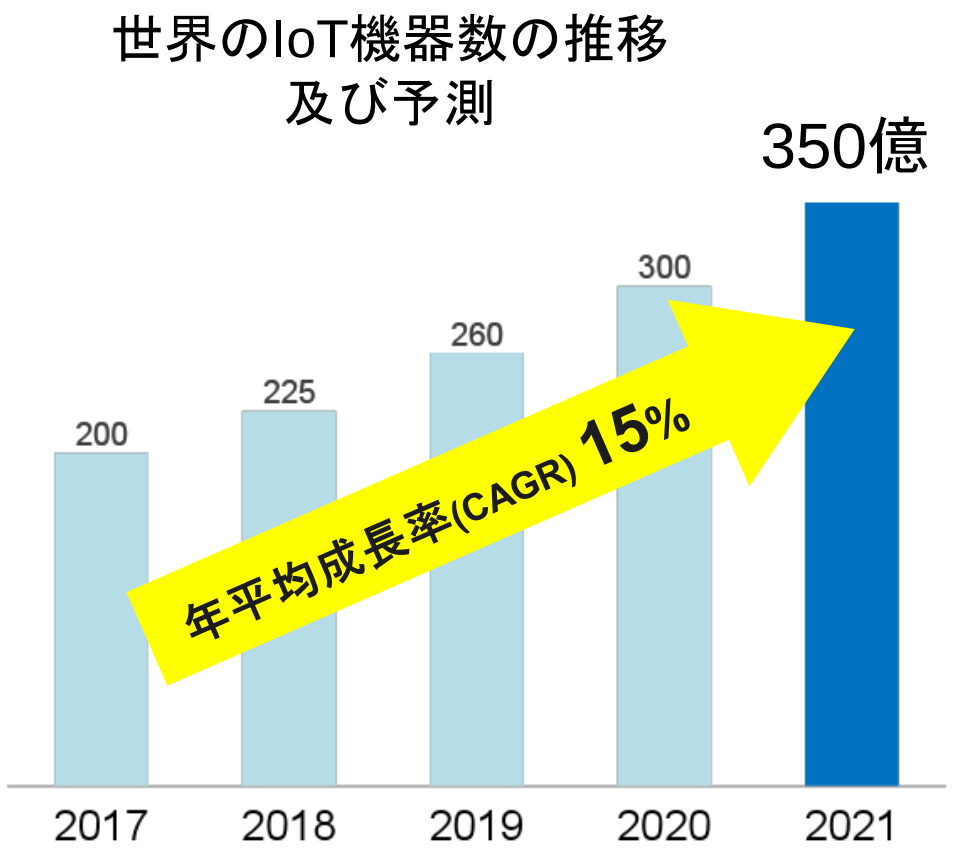
Secure IoT Platform のご紹介

公開

IoTデバイスの増加とリスク

350億台以上がインターネットにつながりセキュリティリスク拡大



（出典）総務省、平成29年版 情報通信白書

公開

IoTデバイスの事件、事故

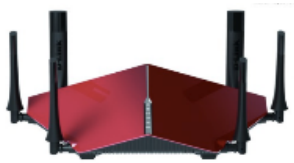
市場に出回る70%のデバイスが脆弱性を抱えている

*source: IoT Research, HP, 2014

セキュアでない

中国の
電子機器メーカー

4万台のカメラがDefault Passwordでボット化でリコール



米公取 が
D-LINKを提訴

セキュリティが十分でない
ルーター、カメラ販売で提訴

信頼できない

サンフランシスコ
市営路線バス

システムがHackerに乗っ取られ、
2日間タダで乗り放題！

米国大手
DNSサービス事業者Dyn

DDOS攻撃でDNSサービス停止
結果1200以上のサイト閉鎖

監視されていない

仏のクラウド
ホスティング会社

15万台のデバイスが感染
1TbpsのDDOS攻撃の犠牲

ダラス
緊急警報システム

156台のトルネードのサイレンが
130万人の住民に警報を繰り返す

IoT機器に関連する政府の動向

cybertrust

【改正民法2020年4月施行】

- IoT機器も5年間はセキュリティパッチ供給が定常化へ

【米議会2017年8月上院提出】

- 国が調達する重要IoT機器はアップデート可能であること

SW Updateが必須機能へ
（OTA：Over-the Air）

【総務省2017年9月実施】

- 脆弱なIoT機器を調査し、メーカーと所有者と情報共有

【総務省2017年10月公開】

- IoTセキュリティ総合対策
  - IoT機器のICチップに電子署名
  - 適合品への認定プログラム案あり

HWでの鍵管理が標準へ
（HW Root of Trust）

ソフトウェア・アップデートとHWでのRoot of Trustがセキュリティ対策の基本

IoTデバイスにおける「Trust Anchor」と「Root of Trust」の定義

cybertrust

「Trust Anchor」の定義

SIOTPにおいては、以下のように定義します。

- **「デバイスの真正性を担保するための情報」**
  →機器ごとに付与された「固有情報」そのもの（秘密鍵 or 共通鍵 or 機器番号）を指す
  - 「PKIにおける信頼基点＝信頼する認証局」を指すことが多い
  - 識別情報がメーカや製品単位で共通であるものは、Trust Anchorとは呼称しない
  - 情報の格納先や保護機構（HW、SW、暗号化有無）に依存しない

「Root of Trust (RoT)」の定義

上記「Trust Anchor」の格納先（入れ物）、保護機構を指す

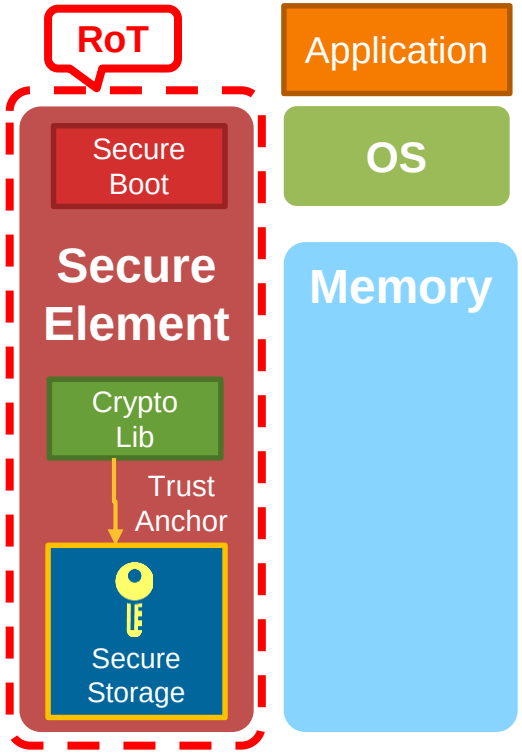
- 当社ではNISTの定義に従い、
  「HWのみで実装、もしくは、HW機構によって保護（暗号化、メモリ保護、セキュアブート機構の一部をHWで実装）しているもの」とする。
  - SWのみで実装されているものは、RoTとは呼称しない→**便宜上「SW Trust Anchor」と呼称する**

「Trust Anchor」と「Root of Trust」イメージ

cybertrust

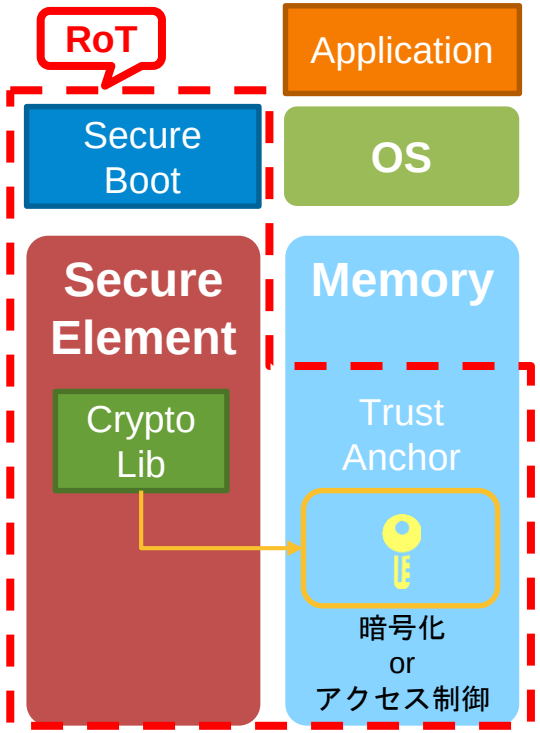
高 — セキュリティ強度 — 低

Trust Anchor Secured by HW RoT



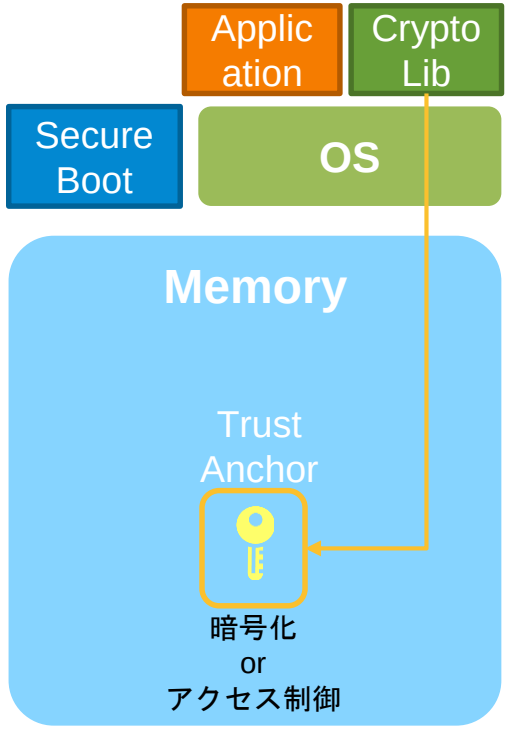
ex.
- CM Core
- TI CC3220
- Microchip
- SIM

Trust Anchor Secured by SW RoT



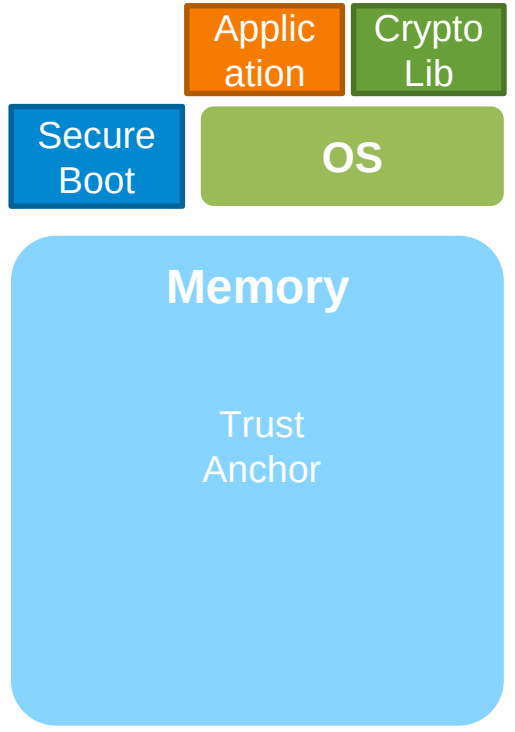
ex.
- NXP i.MX7
- arm TrustZone
- Renesas TSIP

Trust Anchor Secured by SW（RoT無し）



ex.
- arm Mbed + CM Infra

Trust Anchor無し（後から書込み）



ex.
- arm Mbed + CA

Secure IoT Platform 概要

Secure IoT Platform - IoTセキュリティの対策

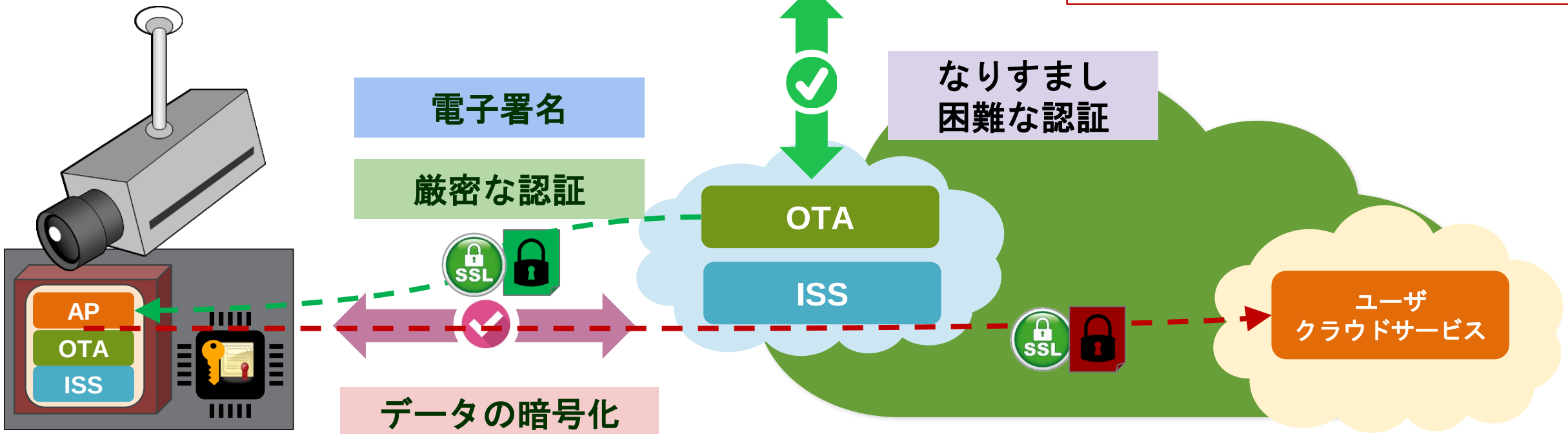
PKIベースのRoot of Trust でIoTサービスをシンプルに守る

：基板
：セキュアメモリ(ICチップ)
：ファームウェア
：認証局発行の証明書付き鍵

国際監査基準

OTA ：FW, SWアップデート
ISS ：個体認証, 個体管理, HW監視
AP ：ユーザ・アプリケーション
：OS

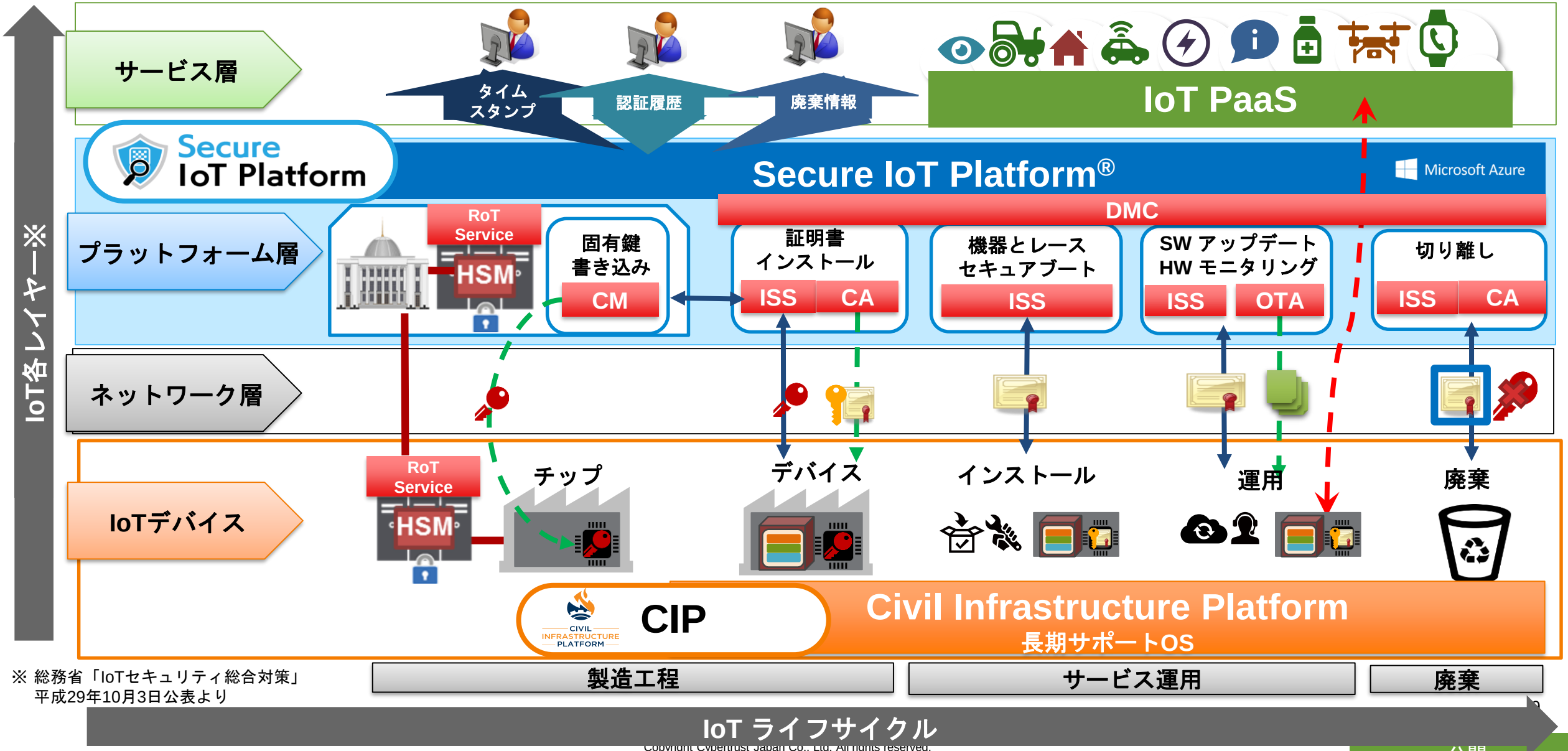
※OTA：Over The Air
※ISS：IoT Secure Service



公開

Secure IoT Platform

- 認証事業とLinux事業で培った長期サポート対応した事業構造を踏襲



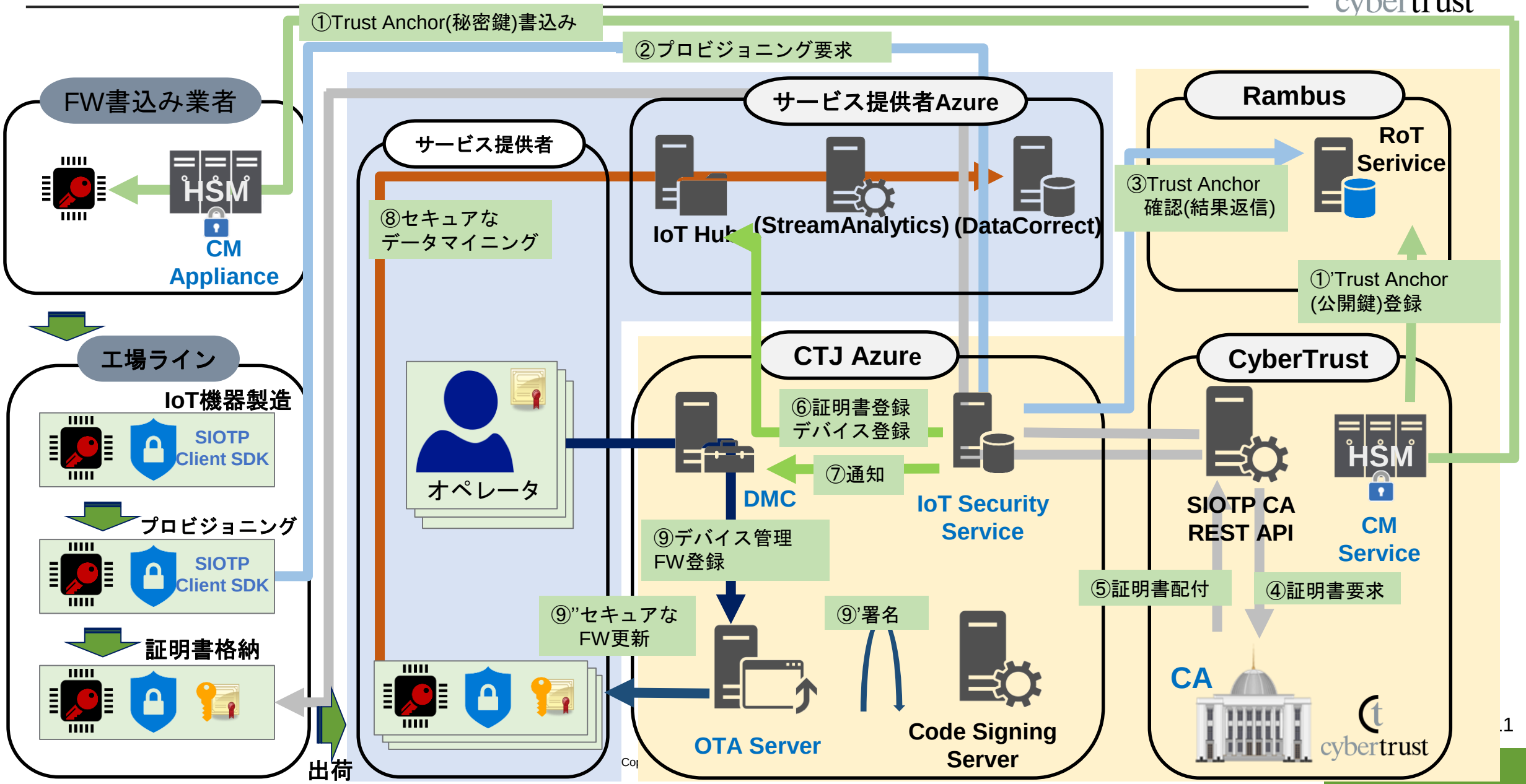
※ 総務省「IoTセキュリティ総合対策」
平成29年10月3日公表より

公開

Secure IoT Platform 要素サービス・コンポーネント

製品	内容
SIOTP Crypto Manager (CM)	半導体に Trust Anchor(個体識別番号と固有鍵)を安全に書込む。半導体内にRambus社のセキュアエレメント(CM Core)を搭載したチップではより安全にTrust Anchorが保護される。
SIOTP IoT Security Service (ISS)	IoTデバイス(チップ)に格納された Trust Anchor を RoTサービスで確認し、IoT PaaSへの デバイス情報の登録とSIOTP認証局に証明書発行要求を行う プロビジョニング機能 を提供する。
SIOTP 認証局 (CA)	ISSからの要求に基づき、デバイス認証用の証明書を発行する。
SIOTP Secure OTA (OTA)	SIOTP認証局より発行された証明書によりデバイス認証を行い、ファームウェア、OS、Security ソフトのパラメータファイルなどのアップデート機能を提供する。 ファームウェア等の改ざん検知のため、コード署名及び署名検証機能を提供する。
SIOTP Device Management Console (DMC)	IOTデバイスをクラウド上で一元管理する機能を提供する。

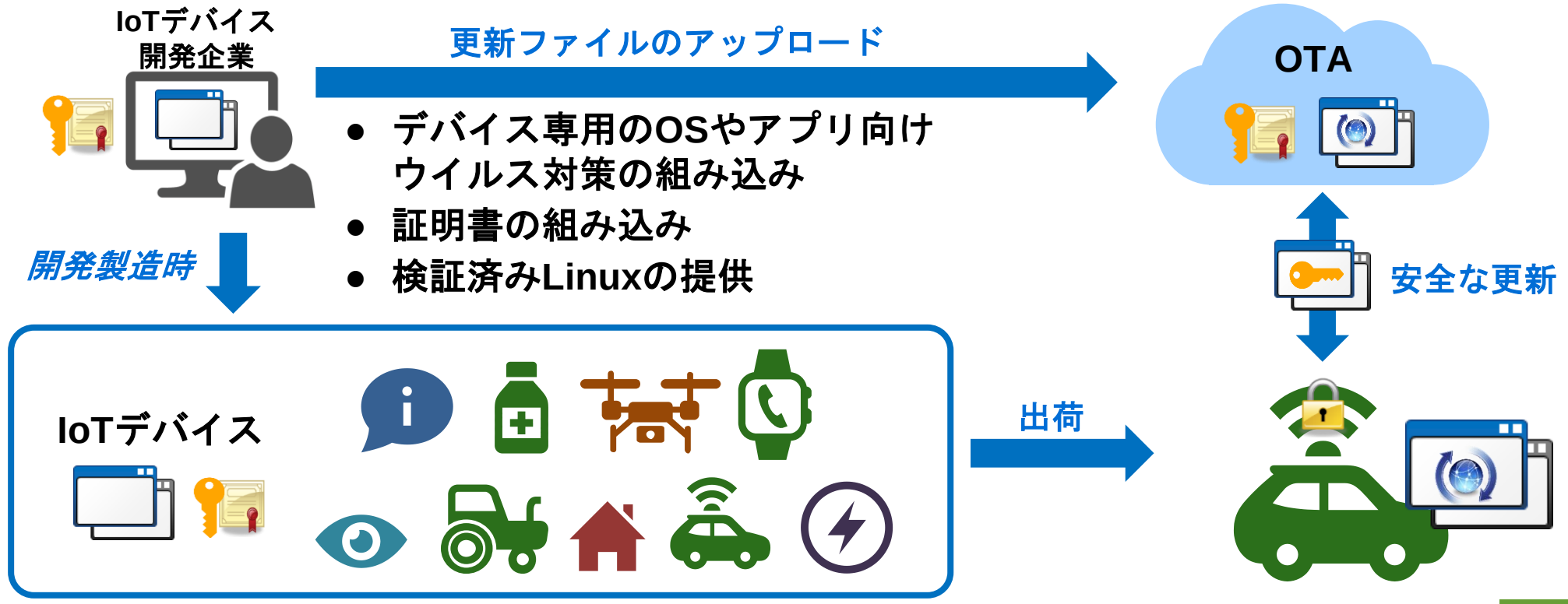
Secure IoT Platform 論理アーキテクチャ



＜SIOTP機能紹介＞ - OTA

IoTデバイス製造時から出荷後まで
安全にソフトウェア更新を行う仕組みを提供

電子認証 ＋ **電子署名**



公開

Secure IoT Platform - 付加価値まとめ

cybertrust

製造工程からのトレーサビリティ

半導体～機器製造時に専用チップに安全に鍵を書き込みその鍵の真正性を確認後、認証局から電子証明書を発行し、**デバイスのトレーサビリティを供給**

IoT機器の長期瑕疵担保

証明書の更新機能とIoT機器に対する長期サポート供給により、製品出荷後の
IoT機器の安全なメンテナンスを提供

機器のIoT化を支援

エコパートナーと連携し、Secure IoT Platform環境をクラウドサービスとして提供することで
IoT基盤の構築コスト削減に寄与

お問い合わせはこちら

サイバートラスト株式会社
IoT 総合お問い合わせ窓口

iot-contact@cybertrust.co.jp

cybertrust

信頼とともに

ソフトバンク・テクノロジー グループ

ソフトバンク・テクノロジー

エムソリューションズ

フォントワークス

環

サイバートラスト

アソラテック

リデン

モードツー

公開