arm

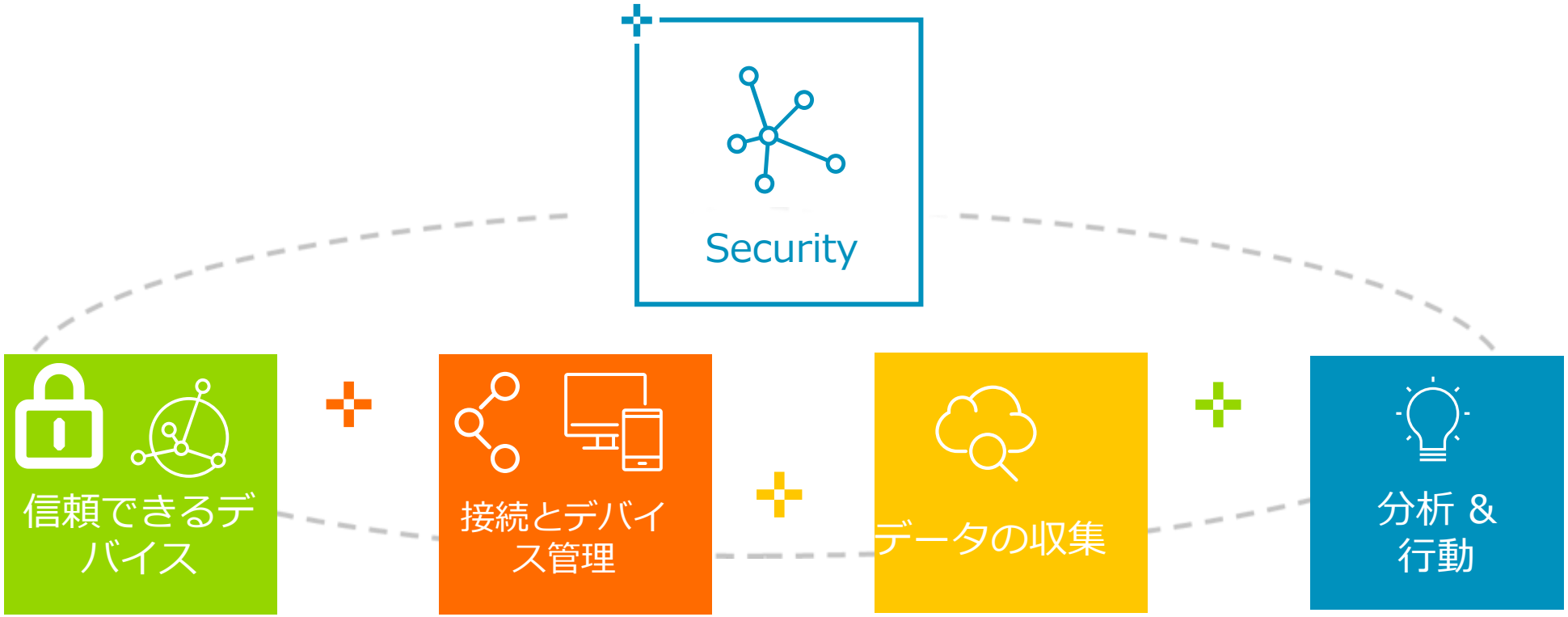
PSAの紹介

2021年12月

セキュリティの動向

arm

信頼がなければDXは成立しない

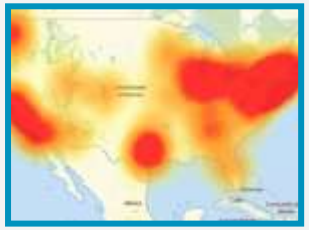


セキュリティはかつてないほど重要に

攻撃のモチベーションが高まっている

- ネットワークに接続する機器の増加やシステムの複雑化に伴い、攻撃対象が急速に拡大
- デバイスより貴重な資産を保有し、機密性の高い活動を制御
- IoTのハッキングはますます巧妙になり、安価に実行可能

ハッカーは脆弱性を容易に利用する



2016: Mirai Botnet[1]

2017: Pacemaker[2]

2017: Casino Fishtank[3]

2018: Bluetooth Lock[4]

2020: Baby Monitor[5]

セキュリティの欠如が大きなリスク

- ハッキングによるブランドの毀損
- 脆弱性により、製品のリコールやデバイスの寿命が短くなる可能性
- 消費者はセキュリティやプライバシーへの懸念からIoT導入に不安を感じている
- サイバー犯罪が国家の安全を脅かすため、主要な地域や業界で規制遵守が求められている

[1]krebsecurity.com/tag/mirai-botnet | [2]www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update | [3]thehackernews.com/2018/04/iot-hacking-thermometer.html | [4]www.bbc.com/news/technology-44457166 | [5]www.pcmag.com/news/exclusive-popular-baby-monitor-wide-open-to-hacking

繋がるデバイスに対する法制化の動き

国や団体、省庁ごとにそれぞれにガイドラインを発行
多くはガイドラインだが、どこかの時点で法制化

US: NIST

UK: DCMS

California: SB-327

EU: ENISA

ETSI

GSMA

IoTに対する脅威

物理的攻撃

- 侵襲的：装置を物理的に破壊/誤動作させて中の情報を取得
- 非侵襲的：外部に出る変化から情報を取得

ライフサイクル攻撃

- コードのダウングレード：旧いソフトのバグの脆弱性を利用
- 非認可生産：デバイスのなりすまし

デバイス

ネットワーク

クラウド

デバイスが踏み台にされる

デバイスを直接攻撃する

ネットワークを攻撃する

デバイスがなりすまされる

ビジネスとブランドが毀損

- バッファオーバーフロー：外部からのソフトウェア攻撃
- マルウェア：侵入したソフトウェアによる攻撃

ソフトウェア攻撃

- 弱いRNG：通信を傍受して情報を取得
- マンインザミドル：送受信者になりすまして情報操作

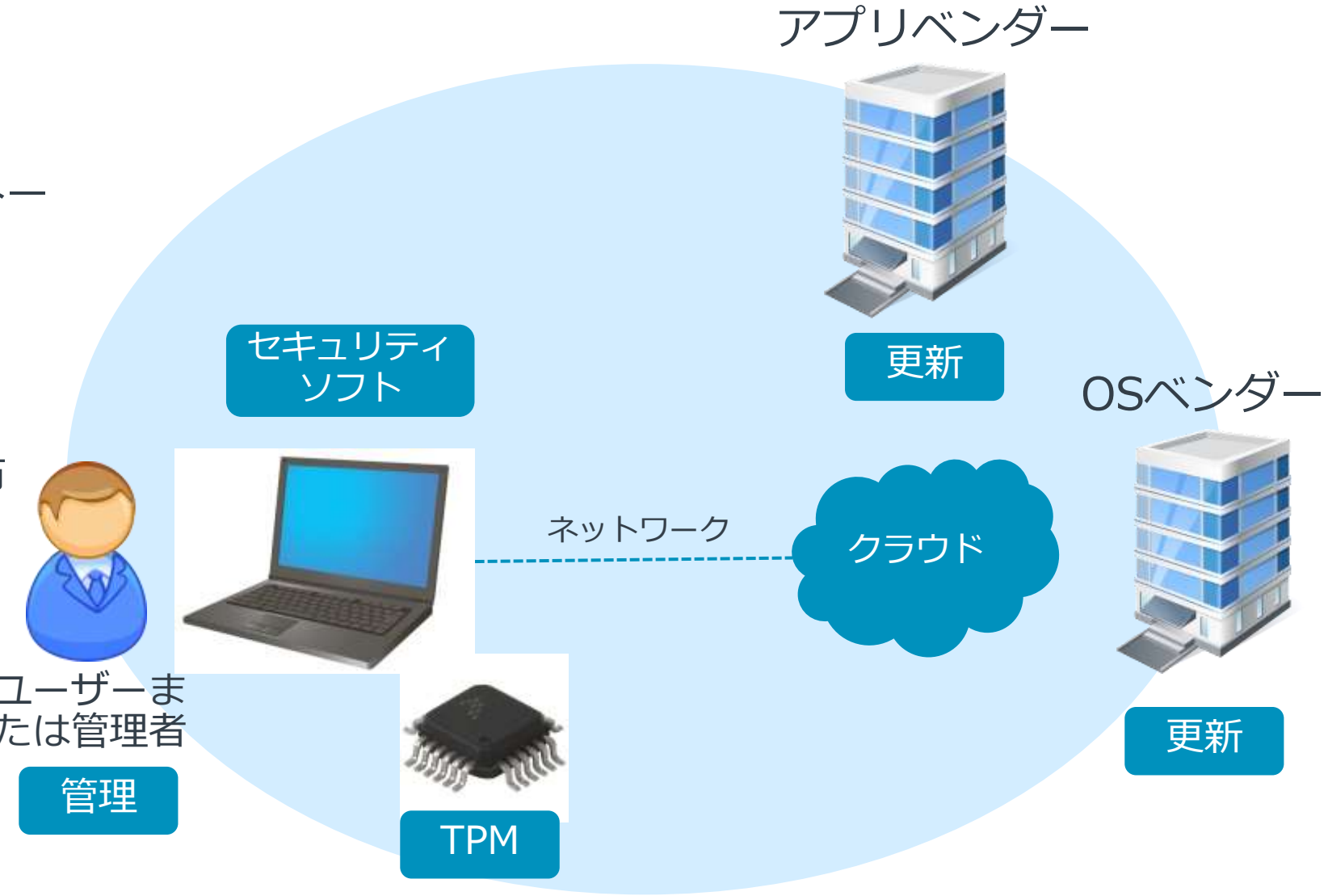
通信攻撃

セキュアなIoT

arm

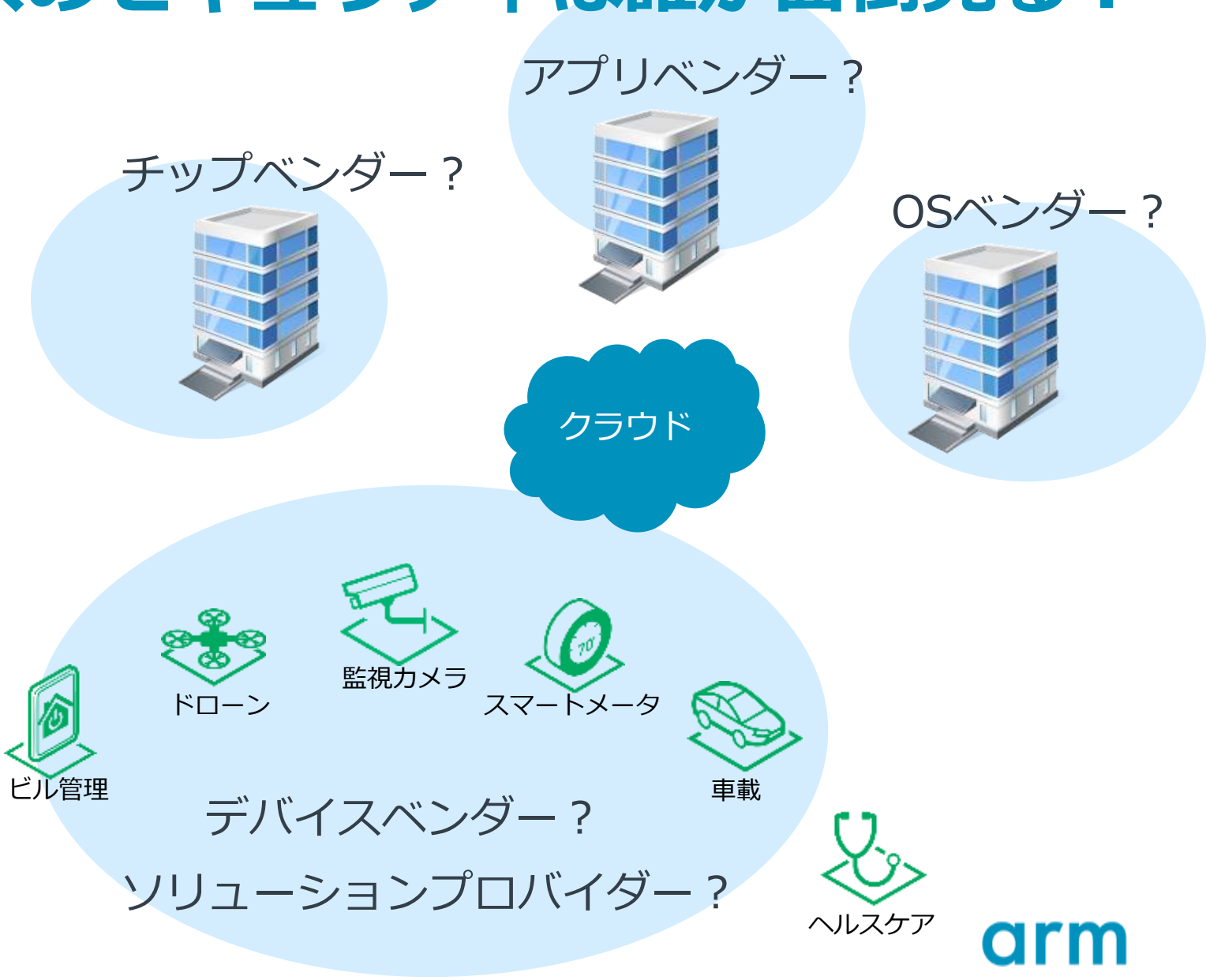
PCの世界では

- ユーザーの自衛手段
  - ソフトウェアの更新処理
  - ウイルスソフトのインストール
- メーカの努力
  - 一社でやっている
  - セキュリティパッチを配布
- 製品の対策
  - 暗号通信
  - TPMを搭載
  - 認証装置

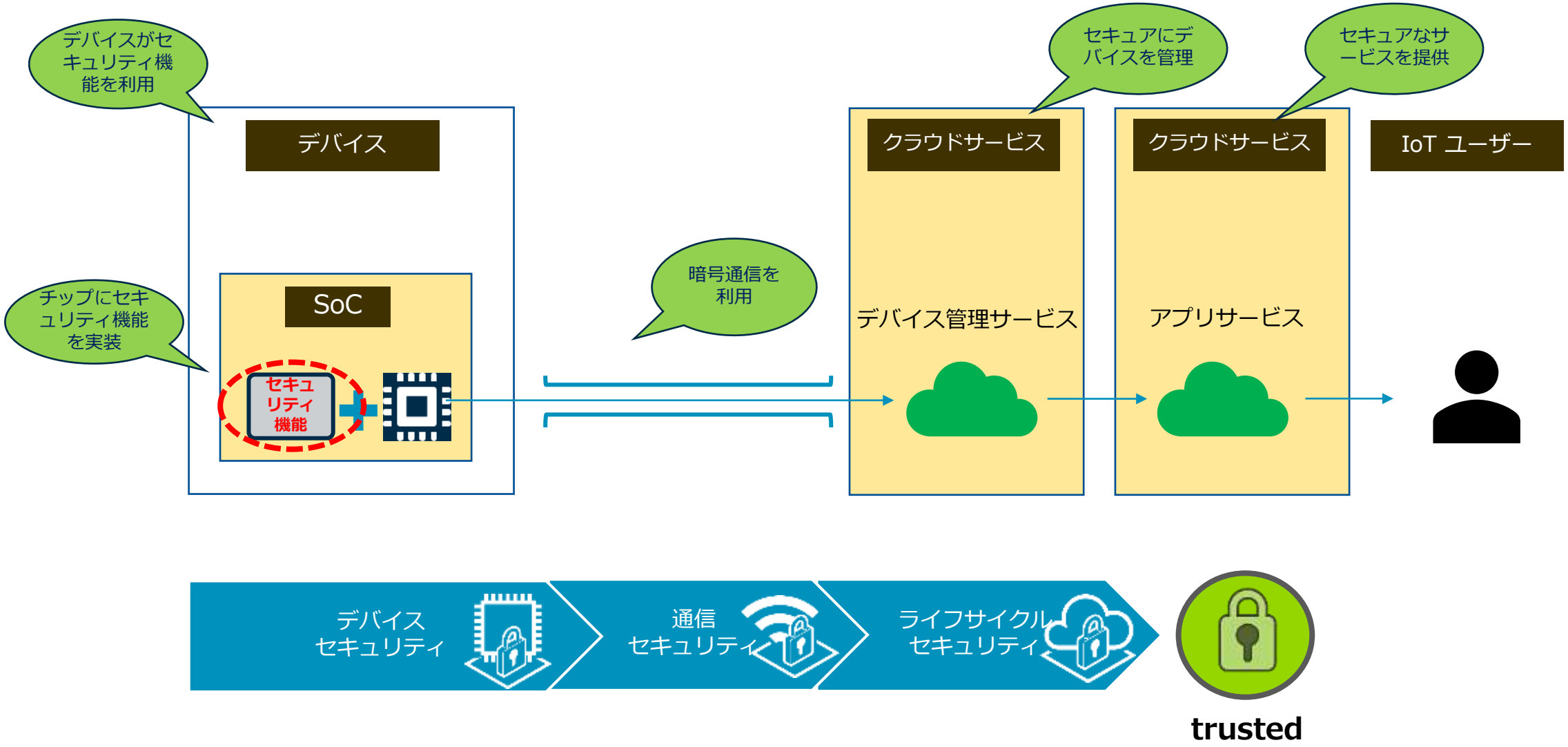


私が作ったIoTデバイスのセキュリティは誰が面倒見る？

- 管理者はそばにいない
  - アップデートは？
- デバイスは自社で開発
  - TPMは？
  - 認証は？
- 世界中に膨大な数を展開
  - メンテに回れるか？
- 社会インフラにも適用
  - ダウンは社会問題
- 膨大なプレーヤー
  - 一社が全部やっていない
  - 責任は分散している
- 様々な製品形態



セキュアなIoT

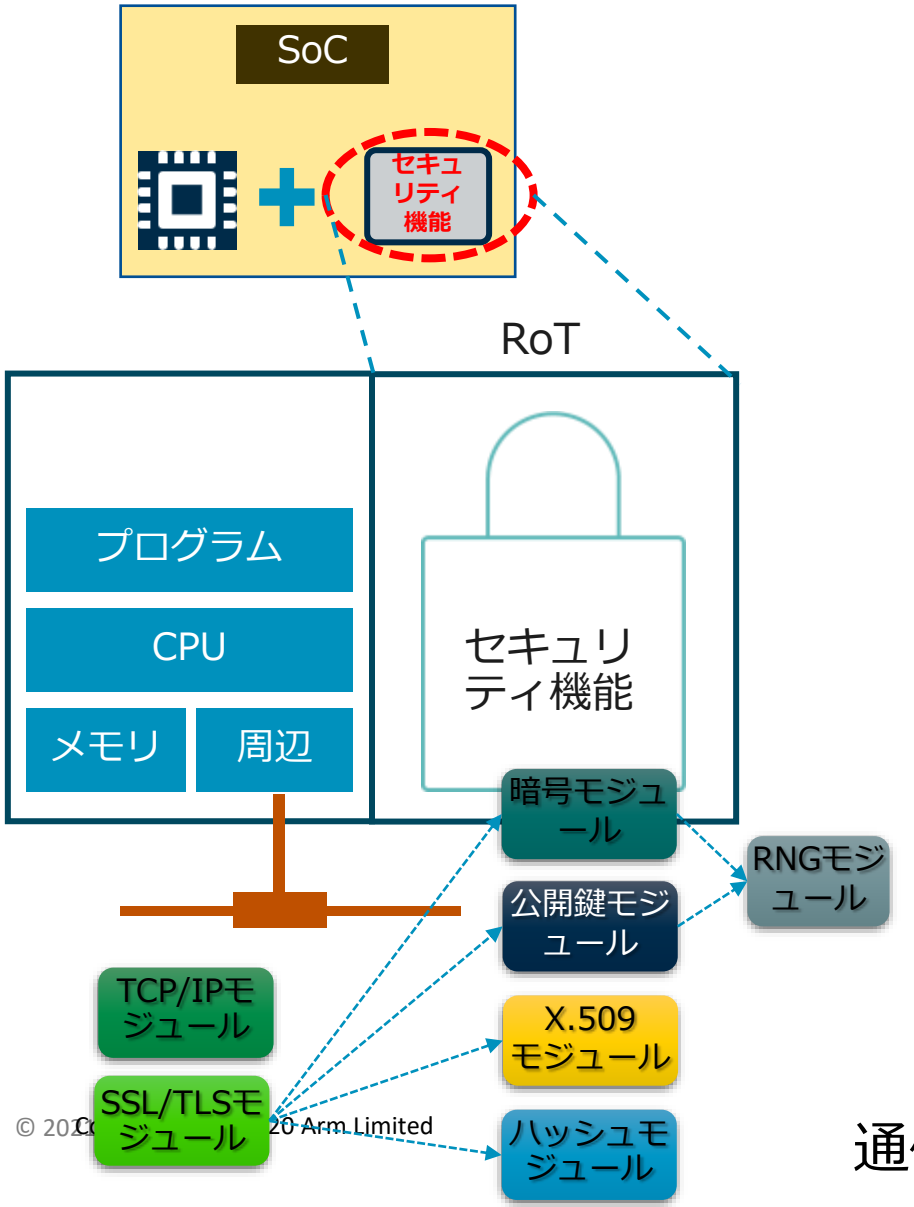


RoT: Root of Trust

What is Root of Trust ?

arm

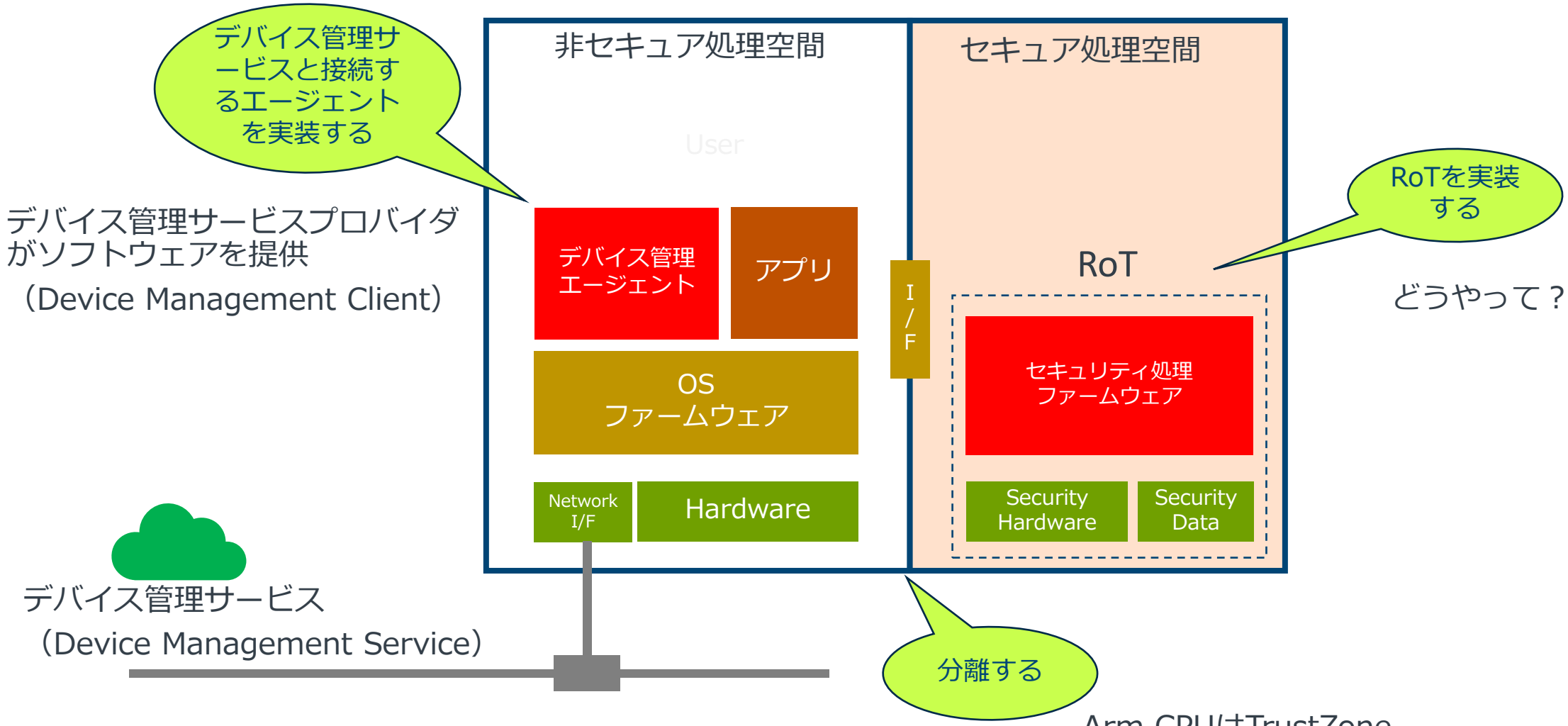
RoT：Root of Trust – セキュリティの基点



- デバイスのセキュリティには
  - RoT（デバイスのセキュリティの基点）が必要
  - 攻撃に対する対策（暗号化処理、証明書）を実現する、おおもと
- RoTはセキュリティ機能を提供するコンピュート実体
- RoTで実現するセキュリティ機能例
  - セキュリティ実行空間分離
  - 通信暗号化
  - セキュアブート、更新
  - セキュアストレージ

通信攻撃に対抗する暗号通信の実現例

セキュアなIoTデバイスのアーキテクチャ



Arm CPUはTrustZoneで分離を実現

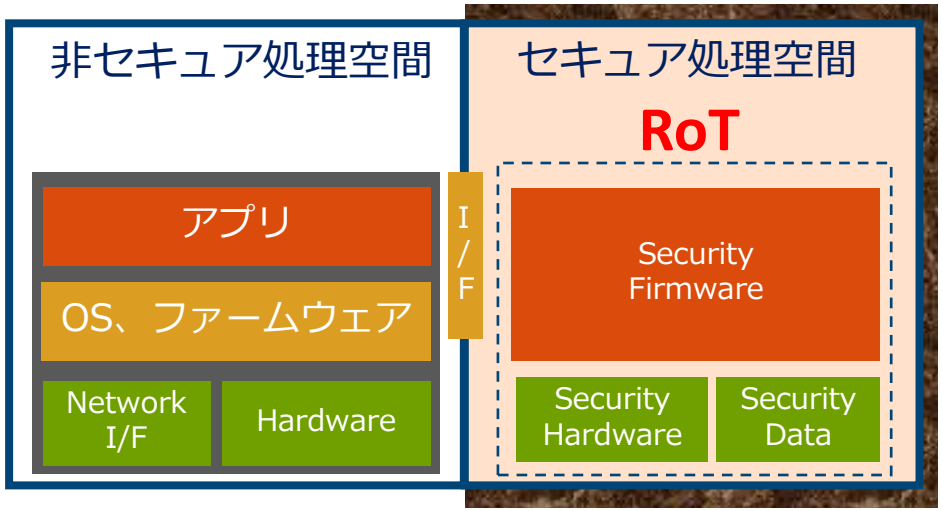
セキュアなIoTデバイスの設計ガイドライン

Platform Security Architecture：

arm

IoTにおけるセキュアなデバイスはどうなっていればいいのか？

- セキュアなIoTデバイスを実現したい
- しかし、多様なIoTデバイスにセキュリティのアーキテクチャ標準はない
- セキュリティアーキテクチャガイドラインを作ろう
  - セキュアな要件を定義
  - RoT設計指針を定義



arm

PSAはArmの提唱するデバイスのセキュリティガイドライン

プラットフォームセキュリティアーキテクチャ（PSA）

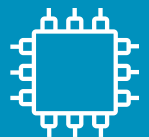
セキュリティモデル
10のゴール

複数のユースケールにまたがる
共通の指針（達成する目標）

実現する機能

分析
脅威モデル &
セキュリティ分析

設計
ハードウエア & ファーム
ウェアアーキテクチャ仕様



実装
ファームウェアソースコード

認証
第三者機関による認証

手順

開発する手順

SM: Security Model
PSR: Platform Security Requirements
TMSA: Threat Models and security analyses
TBSA: Trusted Base System Architecture
FF: Firmware Framework
BOOT-PSG: Trusted Boot and Firmware
ADAC: Authenticated Debug Access Control

ドキュメント

各機能の設計仕様

PSAは公開されたガイドライン（文書と手順）
ライセンスするソリューションではない

セキュリティモデル：セキュアなデバイスが満たすべき共通要件

セキュリティモデル
10のゴール

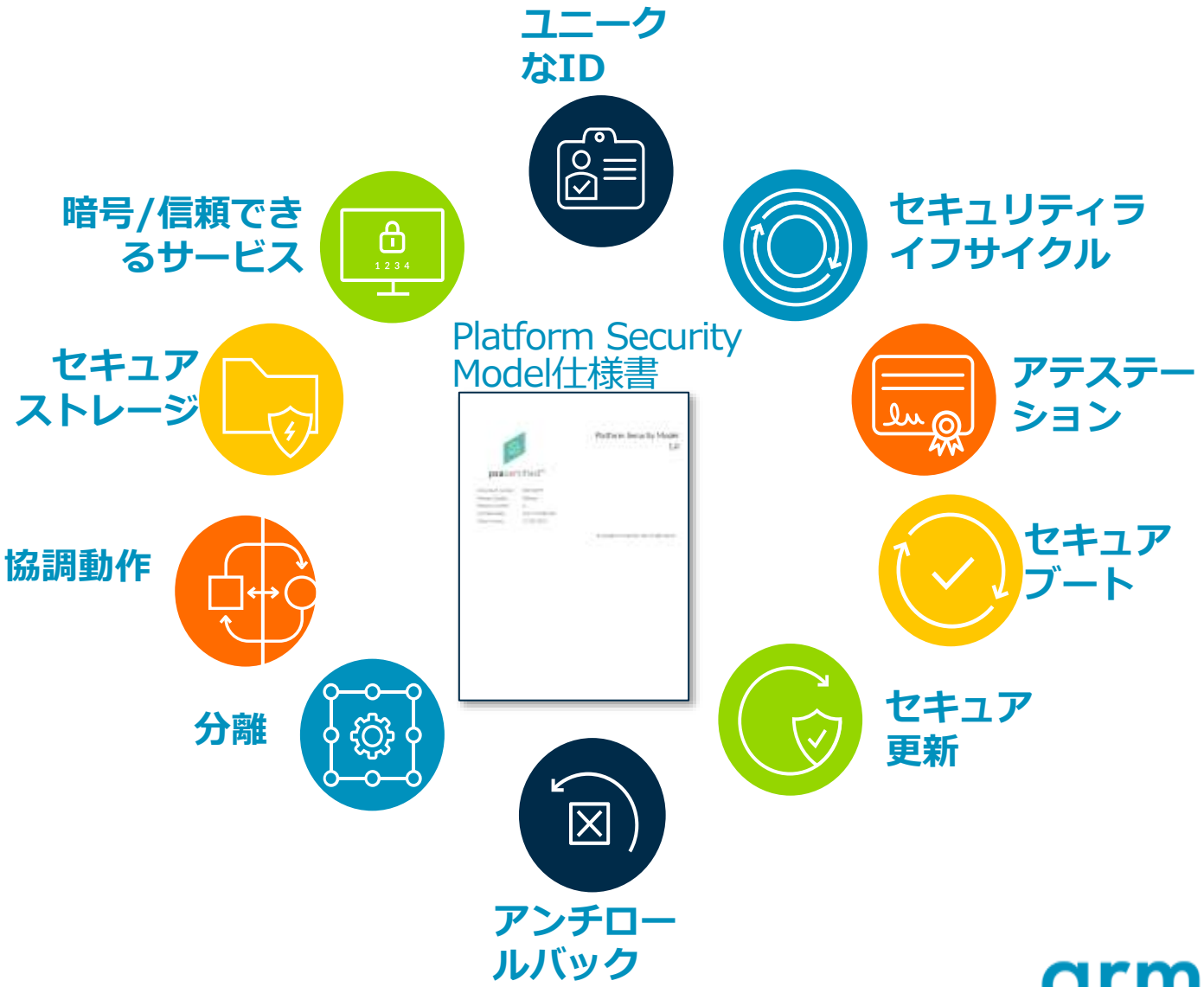
複数のユースケールにまたがる
共通の指針（達成する目標）

分析
脅威モデル &
セキュリティ分析

設計
HW & FW
アーキテクチャ仕様

実装
FWソースコード

認定
第三者機関による認定



ネットにつながるデバイスは共通してこの要件を満たすべき

PSA: 分析（セキュリティに関する）

Threat Model Security Analysis文書例

セキュリティモデル
10のゴール

複数のユースケールにまたがる
共通の指針

分析
脅威モデル &
セキュリティ分析

設計
HW & FW
アーキテクチャ仕様

実装
FWソースコード

認定
psacertified™
第三者機関による認定

システムの記述

↓

アセットの特定

↓

脅威の評価

↓

セキュリティの
目標設定

↓

セキュリティの
要件決定

- 自分のデバイスはどんな脅威にさらされるか？
- 自分のデバイスにはどんなセキュリティ機能が必要か？
- Armは代表的なIoTデバイスの脅威モデルとセキュリティ分析を発行

セキュリティに関する分析を、自分の製品に関して行う

PSA: 設計

複数のユースケールにまたがる
共通の指針

- デバイスのセキュリティハードウェア仕様は要件を満たすか？
- ソフトウェアは改竄されず、更新できるか？
- デバッグはハッキングの入り口にされないか？
- ファームウェアの構造

TBSA-M仕様書

セキュアなハードウェアの要件チェックリスト

Firmware Framework仕様書

RoTのファームウェアの構造を記述

BOOT-PSG仕様書

セキュアにブートする手順と要件、ファームウェアをセキュアに更新する手順と要件を記述

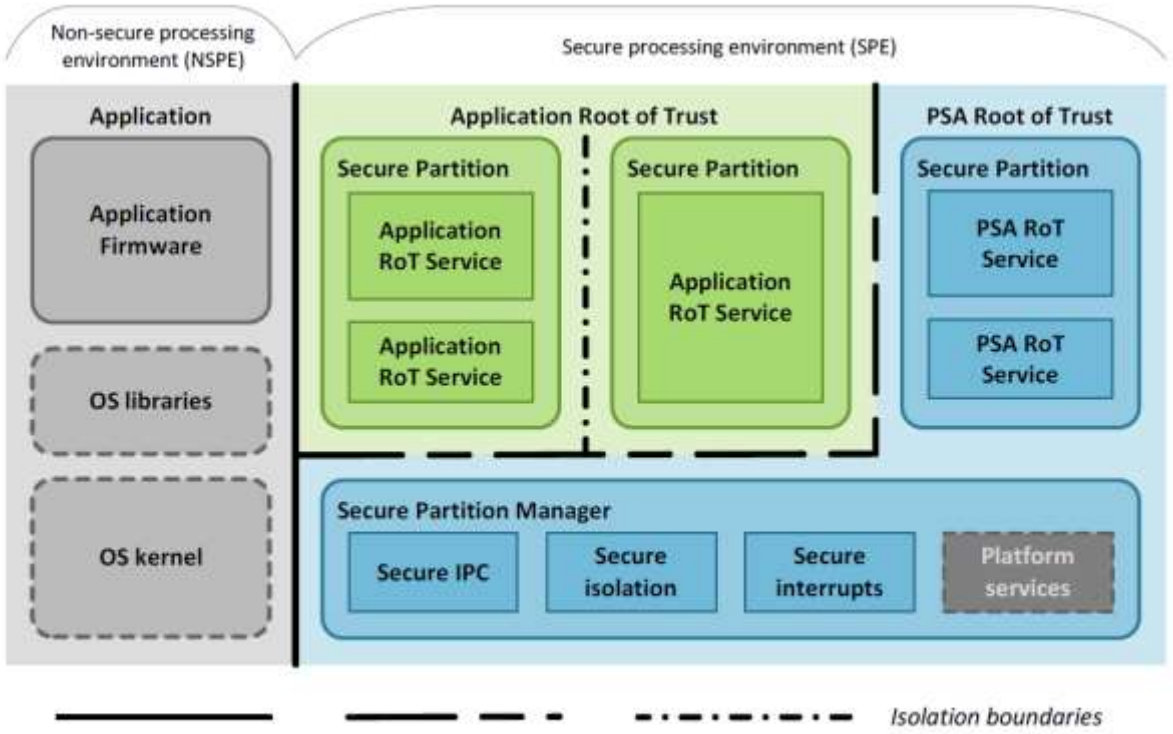
ADAC仕様書

セキュア認証デバッグに関する手順と要件

PSA Firmware Framework (PSA-FF)

信頼できる実行環境でセキュリティサービスを実装するためのプログラミングモデルとソフトウェアインターフェースを定義するソフトウェアアーキテクチャ

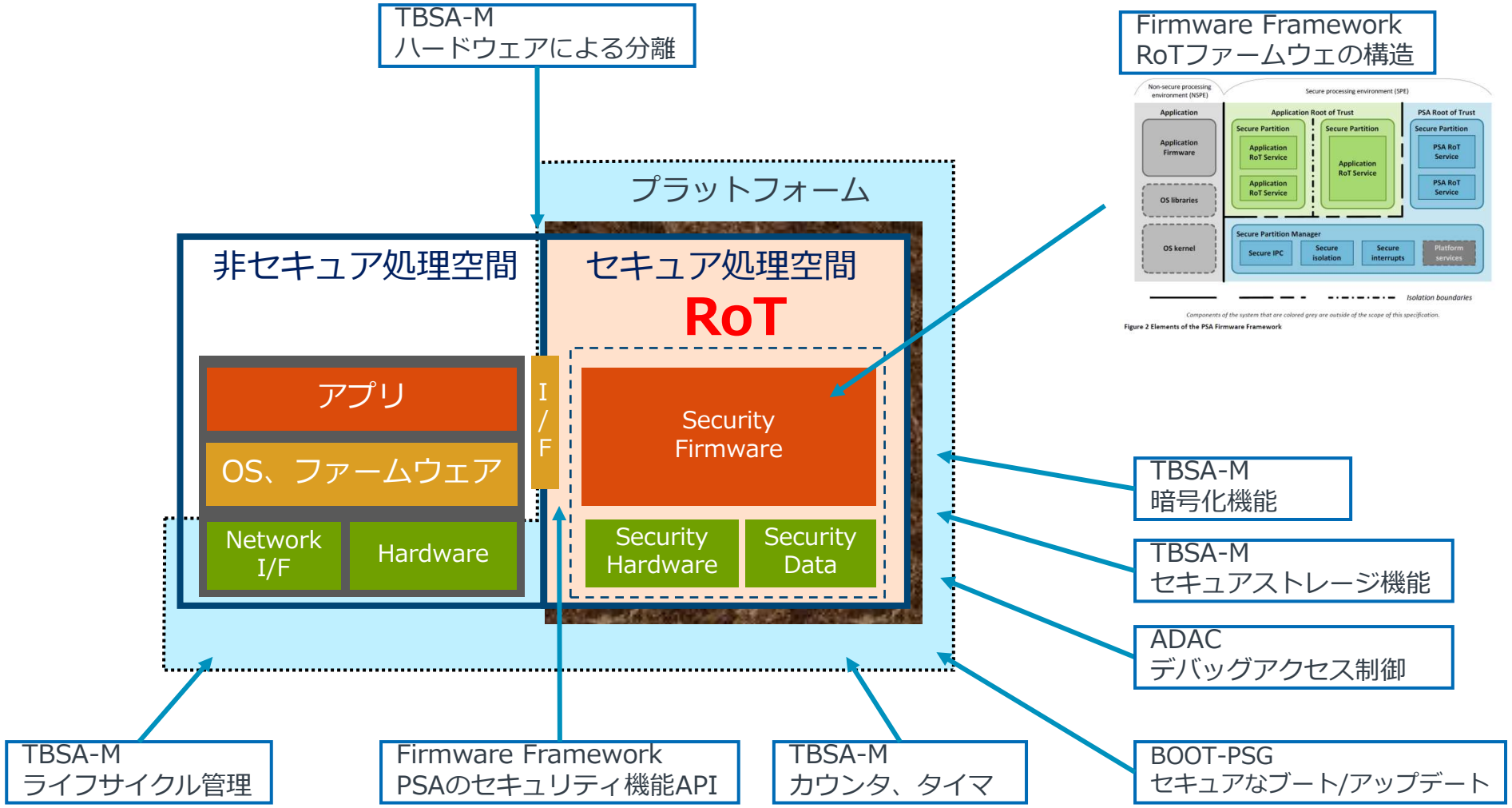
- 1 紹介
  - 1.1 範囲
  - 1.2 設計ゴール
- 2 ソフトウェアアーキテクチャ
  - 2.1 セキュアパーティション
  - 2.2セキュアパーティションマネージャ
  - 2.3 分離
  - 2.4 RoTサービス
  - 2.5 セキュアIPC
  - 2.6 スタートアップ
- 3 セキュア処理環境プログラミングモデル
  - 3.1 分離アーキテクチャ
  - 3.2 セキュアパーティション
  - 3.3 RoTサービス
  - 3.4 セキュア周辺ドライバ
  - 3.5 エラー処理
- 4 プログラミングAPI
  - 4.1 マニフェスト定義
  - 4.2セキュアパーティションCランタイム
  - 4.3 ステータスコード
  - 4.4 クライアントAPI
  - 4.5 セキュアパーティションAPI
- 5 PSA RoTサービス
  - 5.1 PSA 暗号API
  - 5.2 PSA 初期アテステーションAPI
  - 5.3 PSA 内部トラステッドストレージAPI
  - 5.4 PSA RoT ライフサイクルAPI



Components of the system that are colored grey are outside of the scope of this specification.

Figure 2 Elements of the PSA Firmware Framework

PSA：プラットフォームに求められるセキュリティ機能をガイドラインで提示



参照実装: Trusted Firmware for Cortex-M（TF-M）

PSAにおけるRoTファームウェアの参照実装

- TF-M
  - Firmware Frameworkに基づいたArm Cortex-Mデバイス用セキュリティファームウェアのオープンソース参照実装

- TrustedFirmware
  - Linaroが主催するオープンガバナンスプロジェクト
  - Armアーキテクチャ用のセキュアワールドソフトウェアのリファレンス実装を提供
  - ここからTF-Mのソースコードをダウンロード可能
  - TF-Mの進捗や紹介情報などを入手可能

https://www.trustedfirmware.org

PSA認証

独立したテストで信頼を構築

セキュリティモデル
10のゴール

複数のユースケースにまたがる
共通の指針

分析
脅威モデル &
セキュリティ分析

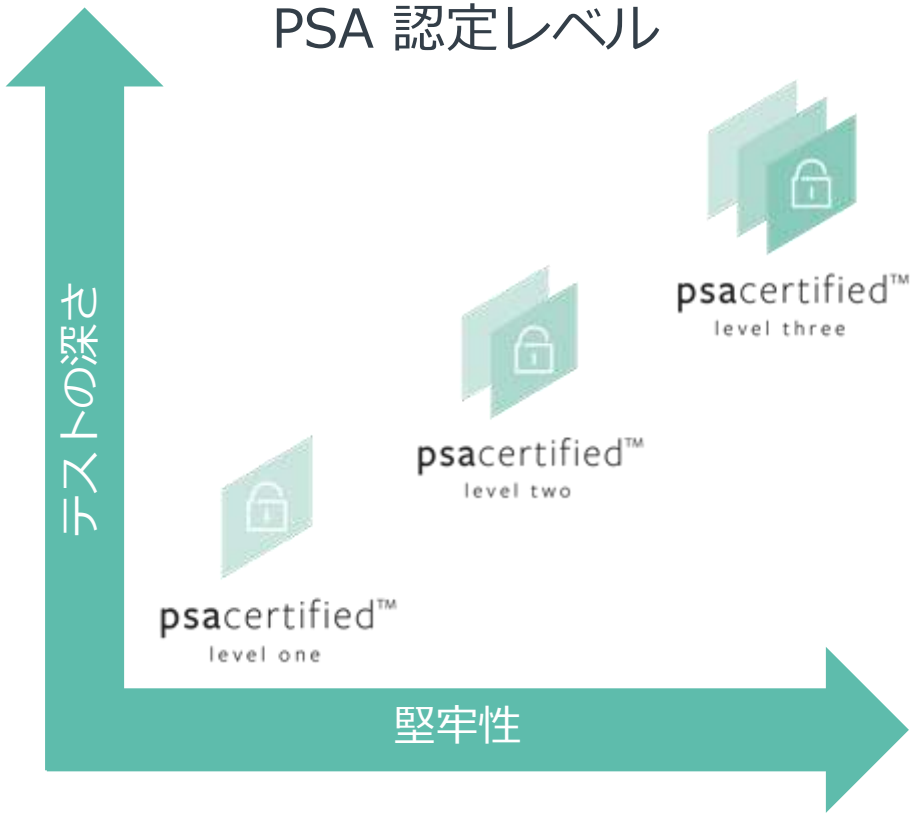
設計
HW & FW
アーキテクチャ仕様

実装
FWソースコード

認定
第三者機関による認定

- IoT脅威モデル、政府の事例、PSAセキュリティモデル、PSA-RoT Protection Profileの上に構築

簡潔な3つの認証レベル



Thank You
Danke
Gracias
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה