TOSHIBA

W3C Web of Things Japanese Community Group 主催

WoTセキュリティ勉強会

IoTセキュリティ国際標準化動向(IETF)

2024-03-08

株式会社東芝 デジタルイノベーションテクノロジーセンター
戦略室 クラウドCoEオフィス
安次富 大介

目次

- IoT/WoTサービスと標準化
- IETF とは
- IETFにおけるWoT/IoTセキュリティ関連標準化動向
- おわりに

IoT/WoTサービスと標準化

IoT (Internet of Things) サービスと標準化

利用

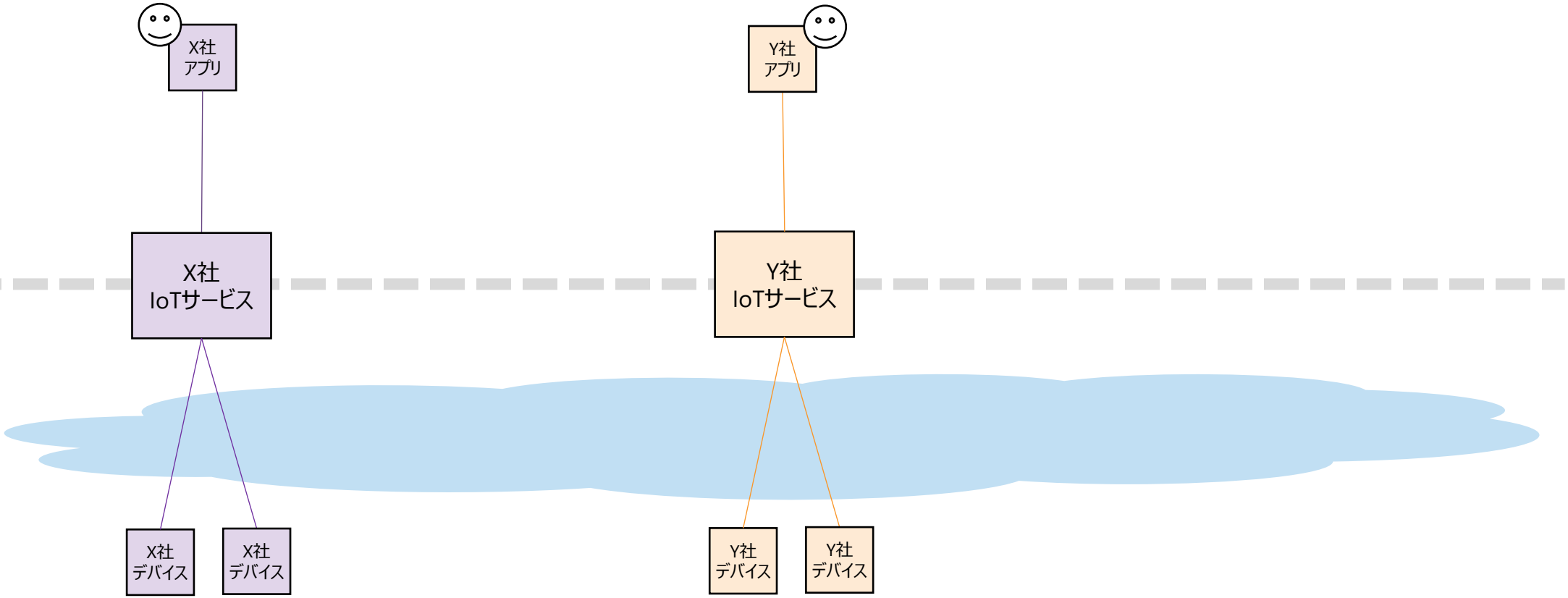
for

App

収容

for

Device



IoT (Internet of Things) サービスと標準化

利用

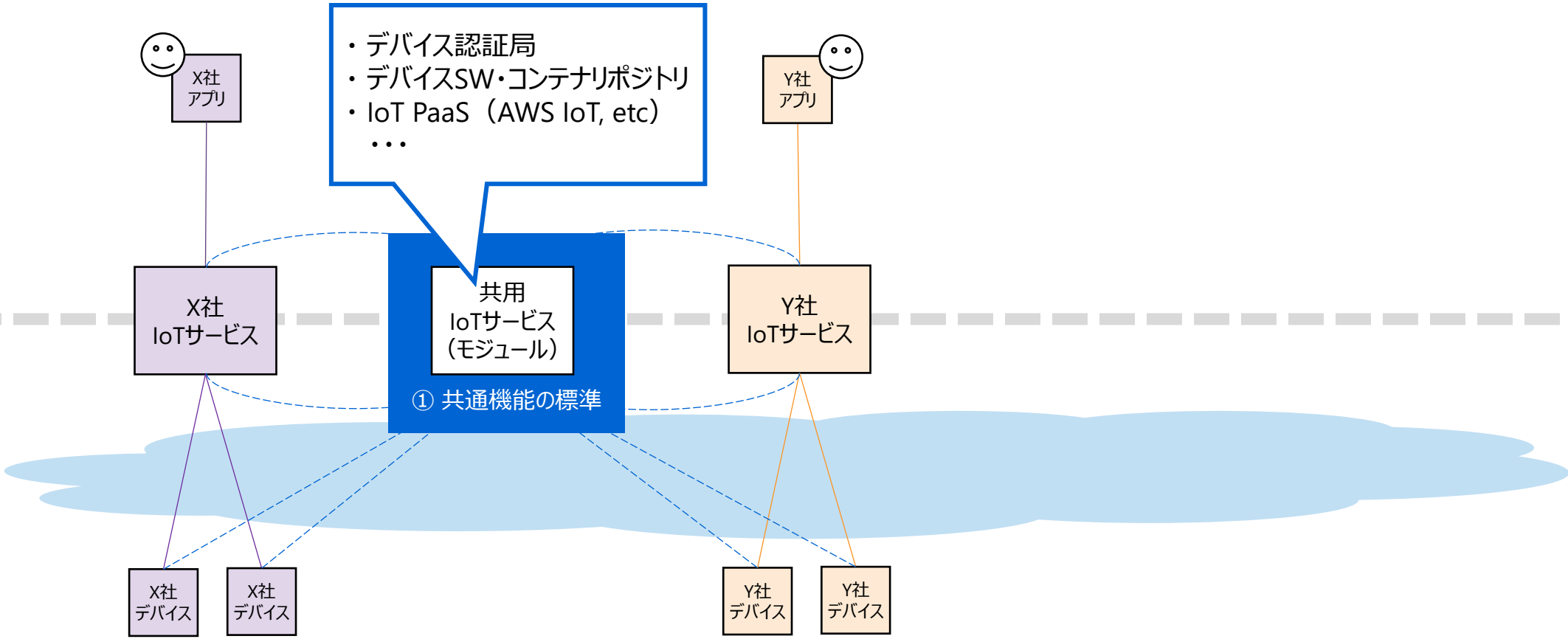
for

App

収容

for

Device



IoT (Internet of Things) サービスと標準化

利用

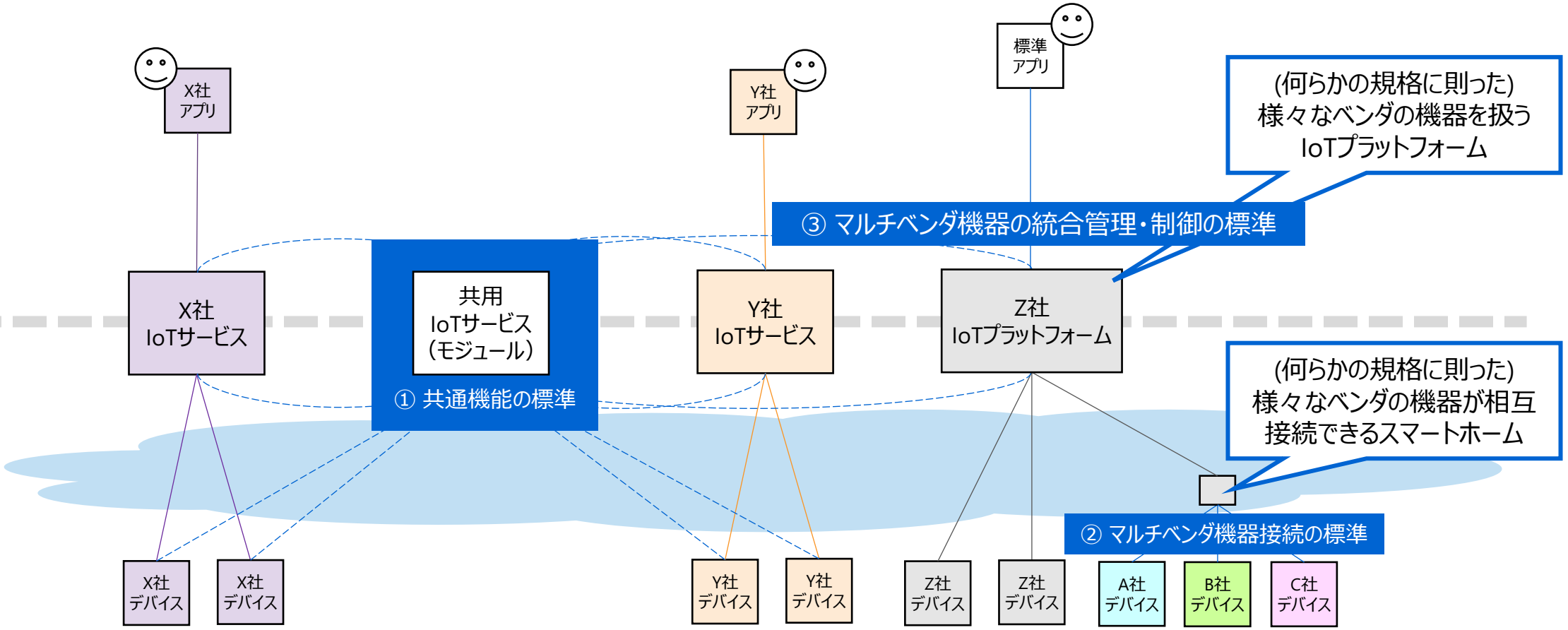
for

App

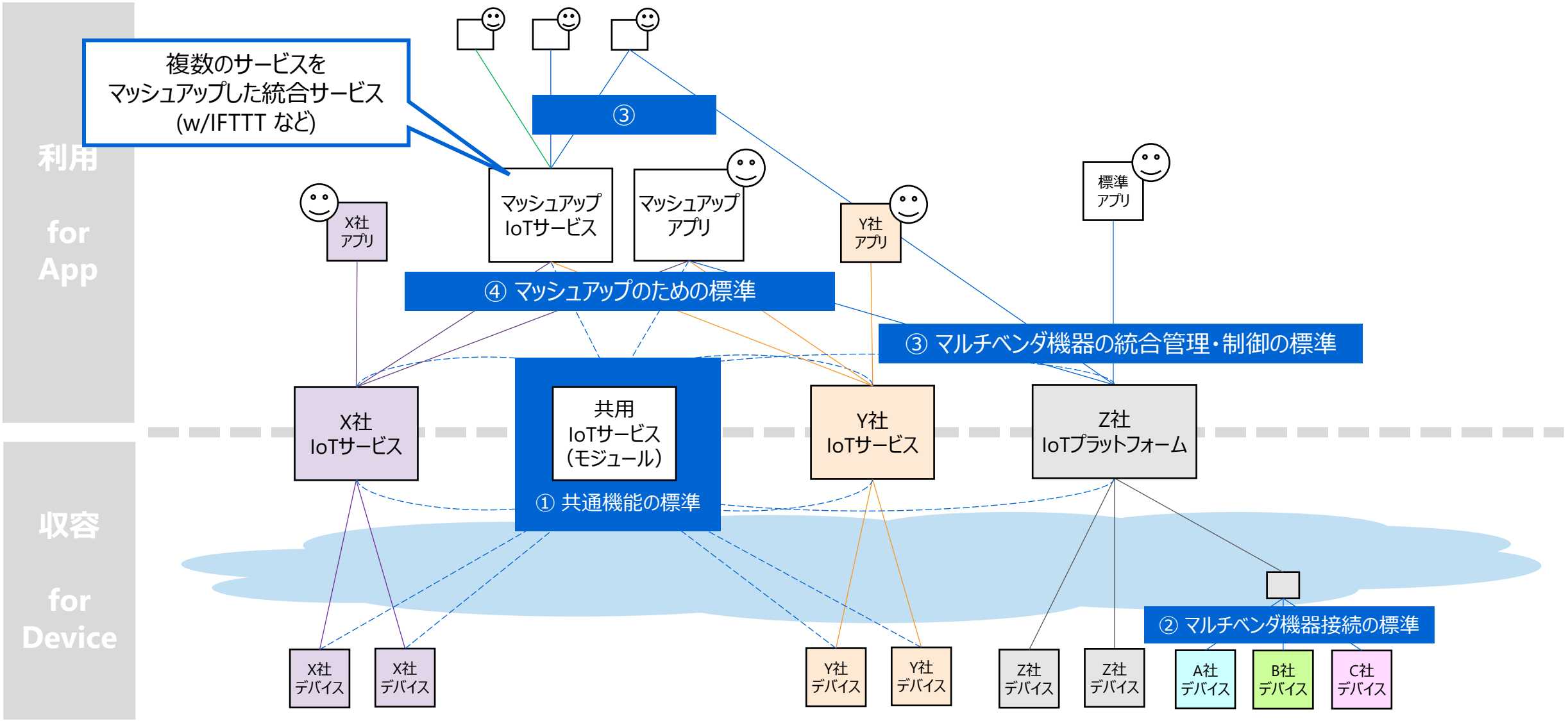
収容

for

Device



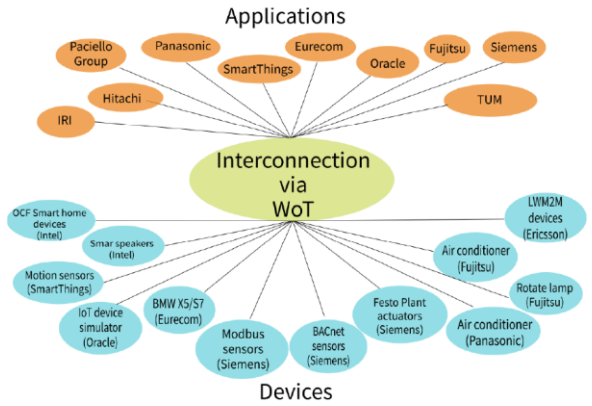
IoT (Internet of Things) サービスと標準化



IoT (Internet of Things) サービスと標準化

Web of Things(WoT)とは

- 異なるIoTプラットフォームを、Web技術を使って、相互接続できるようにすることを目的に、Web技術の国際標準化を行うWorld Wide Web Consortium(W3C)で Web of Things(WoT)の標準化が行われている。
- WoTはプロトコルではなく、様々なプロトコル、プラットフォーム、サービスがWoTに対応することによって、異なるプロトコル、プラットフォーム、サービスを相互接続しやすくするための仕組みである。



利用 for App

収容 for Device

De-Siloを標榜するWoTはこの位置づけ

W3C WoT (Web of Things)

X社 アプリ

マッシュアップ IoTサービス

マッシュアップ アプリ

Y社 アプリ

④ マッシュアップのための標準

ECHONET Lite Web API, etc.

③ マルチベンダ機器の統合管理・制御の標準

X社 IoTサービス

共用 IoTサービス (モジュール)

① 共通機能の標準

Y社 IoTサービス

Z社 IoTプラットフォーム

IETF, etc.

IETFでは主にセキュリティ領域の共通仕様策定が進められている

ECHONET, CSA Matter, etc.

② マルチベンダ機器接続の標準

X社 デバイス

X社 デバイス

Y社 デバイス

Y社 デバイス

Z社 デバイス

Z社 デバイス

A社 デバイス

B社 デバイス

C社 デバイス

IETF とは

IETF とは

- **I**nternet **E**ngineering **T**ask **F**orce
  - https://www.ietf.org/
- インターネット関連技術の標準化作業をおこなうオープンな組織
  - 関心のある企業・団体・**個人**が集まってつくる"フォーラム標準"の１つ
    - <=> 国・公的機関が関与してつくる "デジュール標準"(ISO/IEC など)
- **RFC**3935: A Mission Statement for the IETF
  - ***"To make the Internet work better."***

IETFとは：RFC（Request For Comments）

- IETFが提案という形で発行・公開する文書シリーズ
  - 例） IP：RFC791、TCP：RFC793 → RFC9293 (40年越しの改訂)
- 現時点(2024-02-16)で、RFC9500番台に突入
- インターネットを支える多くの重要な技術仕様がRFCとして公開されている
  - IP, UDP, TCP, DNS, HTTP, TLS, OAuth, QUIC ・・・

Stream: Internet Engineering Task Force (IETF)
RFC: 9458
Category: Standards Track
Published: January 2024
ISSN: 2070-1721
Authors: M. Thomson, *Mozilla*; C. A. Wood, *Cloudflare*

RFC 9458
Oblivious HTTP

Abstract

This document describes Oblivious HTTP, a protocol for forwarding encrypted HTTP messages. Oblivious HTTP allows a client to make multiple requests to an origin server without that server being able to link those requests to the client or to identify the requests as having come from the same client, while placing only limited trust in the nodes used to forward the messages.

Status of This Memo

This is an Internet Standards Track document.

https://www.rfc-editor.org/rfc/rfc9458.pdf

技術分野 と Working Groups (WGs)

- 現在127の作業グループ。最近のエリア再編により、Webを冠する"WIT" エリアが新設。

技術分野 (Area)	WG数	代表的WG
Applications and Real-Time Area (ART) アプリケーションとリアルタイム通信	24	emailcore, sipcore, mmusic, stir, etc.
General Area (GEN) 一般	1	gendispatch
Internet Area (INT) インターネット	16	6lo, 6man, dnssd, ntp, etc.
Operations and Management Area (OPS) 運用と管理	17	dnsop, netconf, v6ops, etc.
Routing Area (RTG) ルーティング	24	mpls, babel, manet, etc.
Security Area (SEC) セキュリティ	29	acme, oauth, tls, scim, jose, etc.
Transport Area (TSV) トランスポート ※廃止	0	--
Web and Internet Transport (WIT) Webとインターネットトランスポート ※新設	16	httpbis, httpapi, rtcweb, webtrans, etc.

伝統的なトランスポート領域だけでなく、
セキュリティ、そして近年ではIoT領域も活発

https://datatracker.ietf.org/wg/

IETF meeting

- 年に3回、7日間のIETF会合(オンライン参加可能)
  - 土・日：ハッカソン、月～金：Working Group 会合

https://twitter.com/ietf/status/1757536346170675273/photo/2

https://twitter.com/ietf/status/1592079938424778752/photo/2

IETFにおける WoT/IoT セキュリティ関連標準化動向

IoT関連のWG（Working Group）

- ART: アプリケーションとリアルタイム通信
  - ASDF: A Semantic Definition Format for Data and Interactions of Things
- INT: インターネット
  - 6LO: IPv6 over Networks of Resource-constrained Node
- OPS: 運用と管理
  - ANIMA: Autonomic Networking Integrated Model and Approach
  - IOTOPS: IOT Operations
  - OPSAWG: Operations and Management Area Working Group
- RTG: ルーティング
  - ROLL: Routing Over Low power and Lossy networks
  - DETNET: Deterministic Networking

モノの情報モデルの中間表現

低消費電力な無線モジュールのIPv6マルチホップネットワーク「6LoWPAN」など

IoTデバイスの運用問題。特に、デバイス・オンボーディングやライフサイクル管理を扱う

IoT関連で MUD (Manufacturer Usage Description) がある

高信頼かつロス・遅延変動が極めて小さいL2/L3ネットワーク。
産業オートメーションや車両制御など IoT/CPS なユースケースあり

IoT関連のWG（Working Group）

- SEC: セキュリティ
  - ACE: Authentication and Authorization for Constrained Environments
  - LAKE: Lightweight Authenticated Key Exchange
  - SCIM: System for Cross-domain Identity Management
  - COSE: CBOR Object Signing and Encryption
  - RATS: Remote Attestation Procedures
  - SCITT: Supply Chain Integrity, Transparency, and Trust
  - SUIT: Software Updates for Internet of Things
  - TEEP: Trusted Execution Environment Provisioning
  - OAuth: Web Authorization Protocol
  - JOSE: JSON Object Signing and Encryption
- WIT: Webとインターネットトランスポート
  - CORE: Constrained RESTful Environments

OAuth(認可)のIoTデバイス版

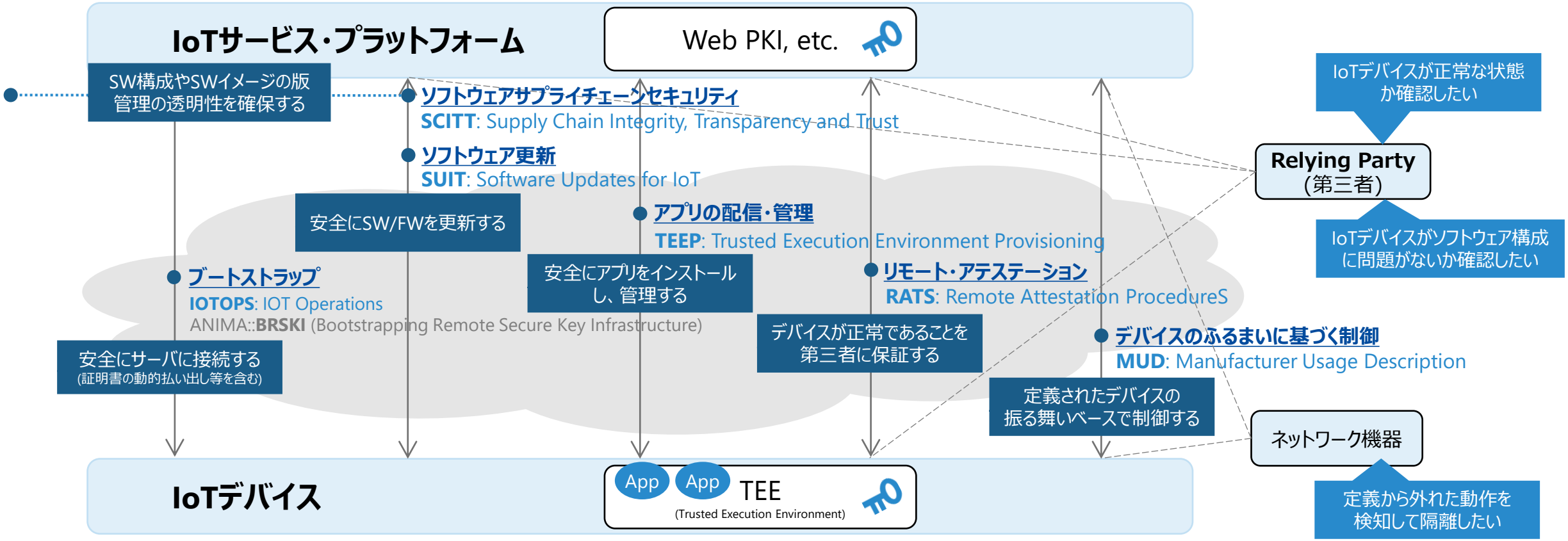
複数のドメインをまたがったID管理

後述

RESTful APIのIoTデバイス版
(HTTPではなくCoAP)

IETFにおけるIoTセキュリティ標準化：概要

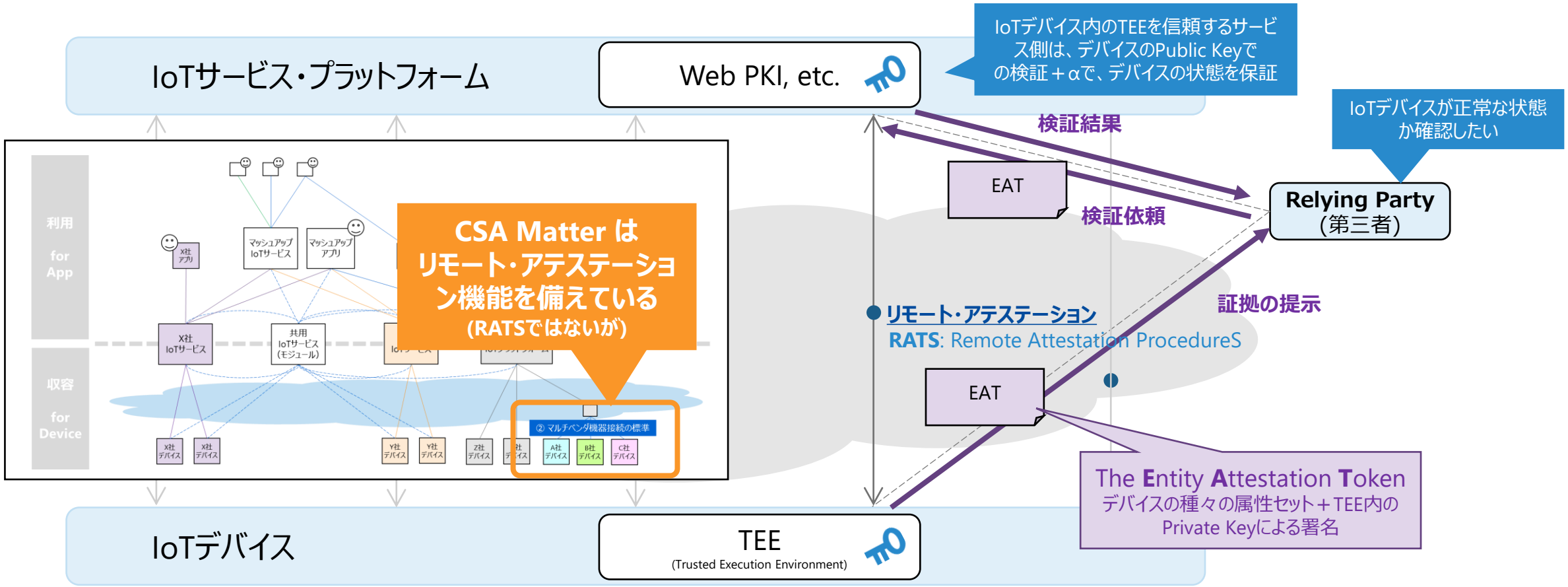
- IETFでは、デバイスのリソース制約があること(Constrained)を前提とした省リソースな通信プロトコル、デバイスが持つセキュア・コンポーネント(TEE)を信頼の起点とした、IoTライフサイクルを通したデバイスとサーバ間の種々のインタラクションを扱う



IETFにおけるIoTセキュリティ標準化：リモート・アテステーション

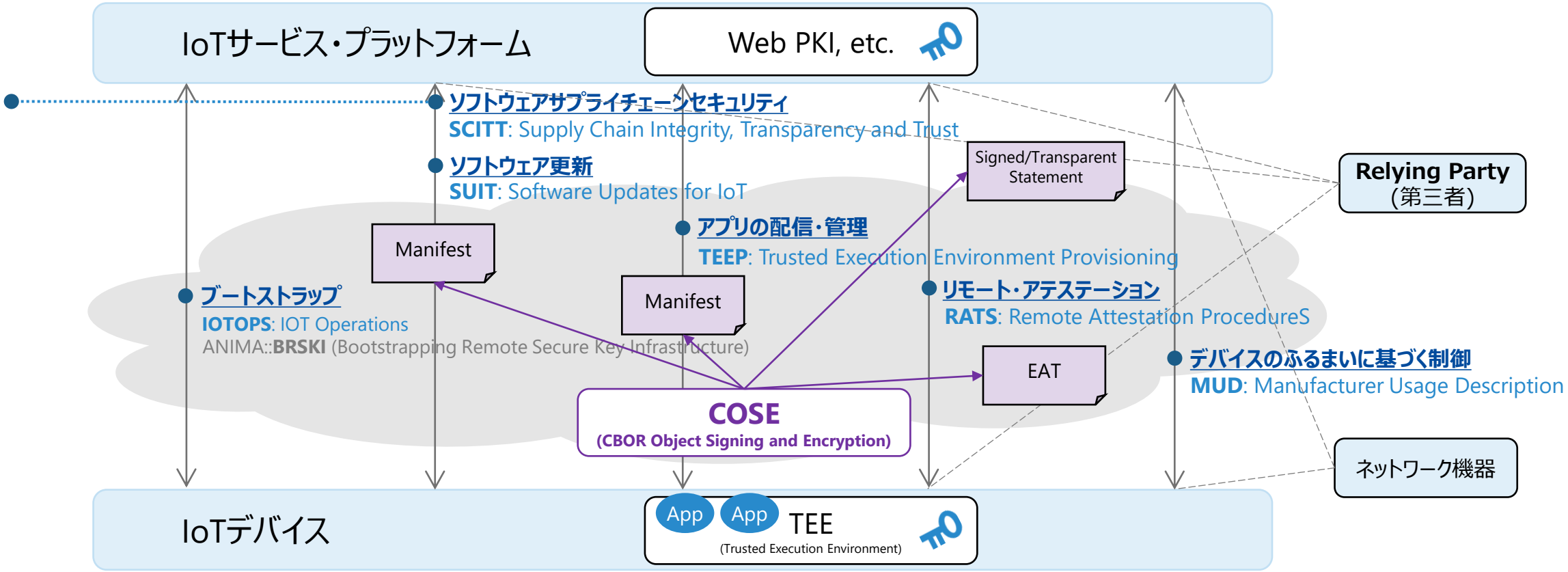
ピックアップ

- RATS： **R**emote **AT**testation Procedure**S**
  - デバイスが正常な状態にあること（危殆化していない等）を第三者に証明するためのアーキテクチャ＆プロトコル
- その信頼の拠り所は、IoTデバイス内のTEE(Trusted Execution Environment)内のPrivate Key



IETFにおけるIoTセキュリティ標準化：検証可能なデータコンテナの利用

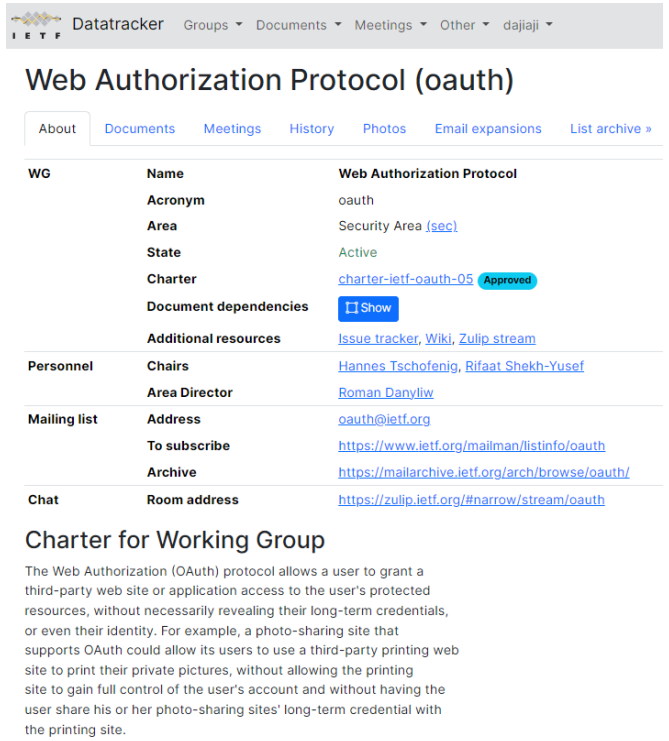
- デバイスとサービス間でやり取りされる検証可能な署名付きデータには、COSE (RFC9052) というセキュリティデータコンテナ仕様が使われている。署名にはデバイス・サービス双方のPrivate Keyが用いられる
- COSE: データ＋署名に、検証や相互接続性のために必要な種々のデータを付加できるデータコンテナ仕様
  - データフォーマットは CBOR（JSONのバイナリ版的なもの）

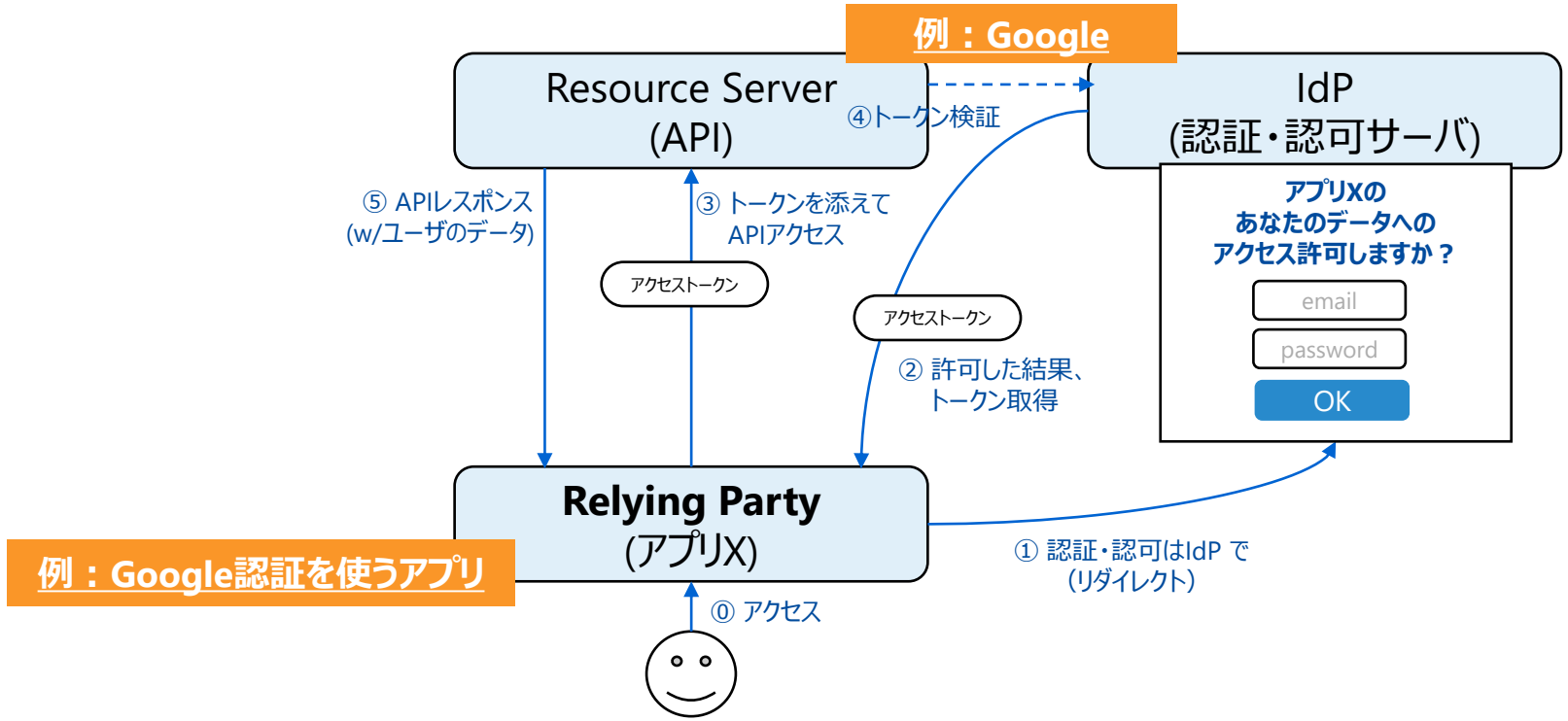


IETFにおけるWeb標準のIoT領域への応用

- リッチなIoT機器は、一般的なWebのプロトコルスタックで Webクライアントとして動作させることが一般的
- セキュリティに関しても OAuth (Web Authorization Protocol) や JWT (JSON Web Token) が利用できる
  - OAuth2.0は、Webの世界で非常に広く普及している認可プロトコル
  - 認証も含めたOpenID Connect（OIDC）が、お馴染みの「Googleでログイン」「Facebookでログイン」

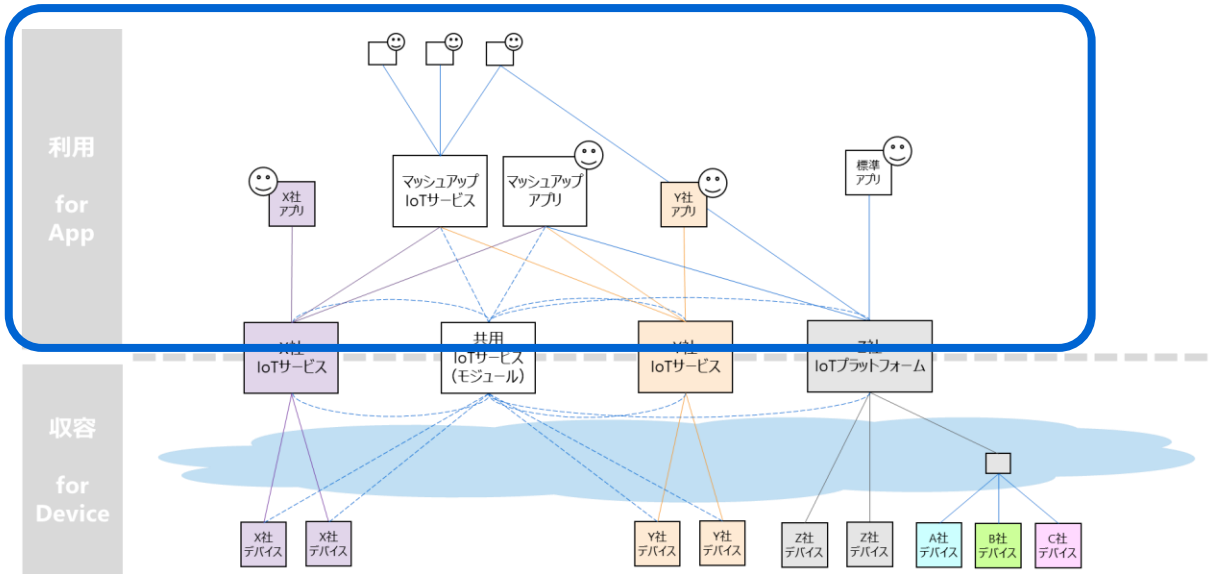
https://datatracker.ietf.org/wg/oauth/about/

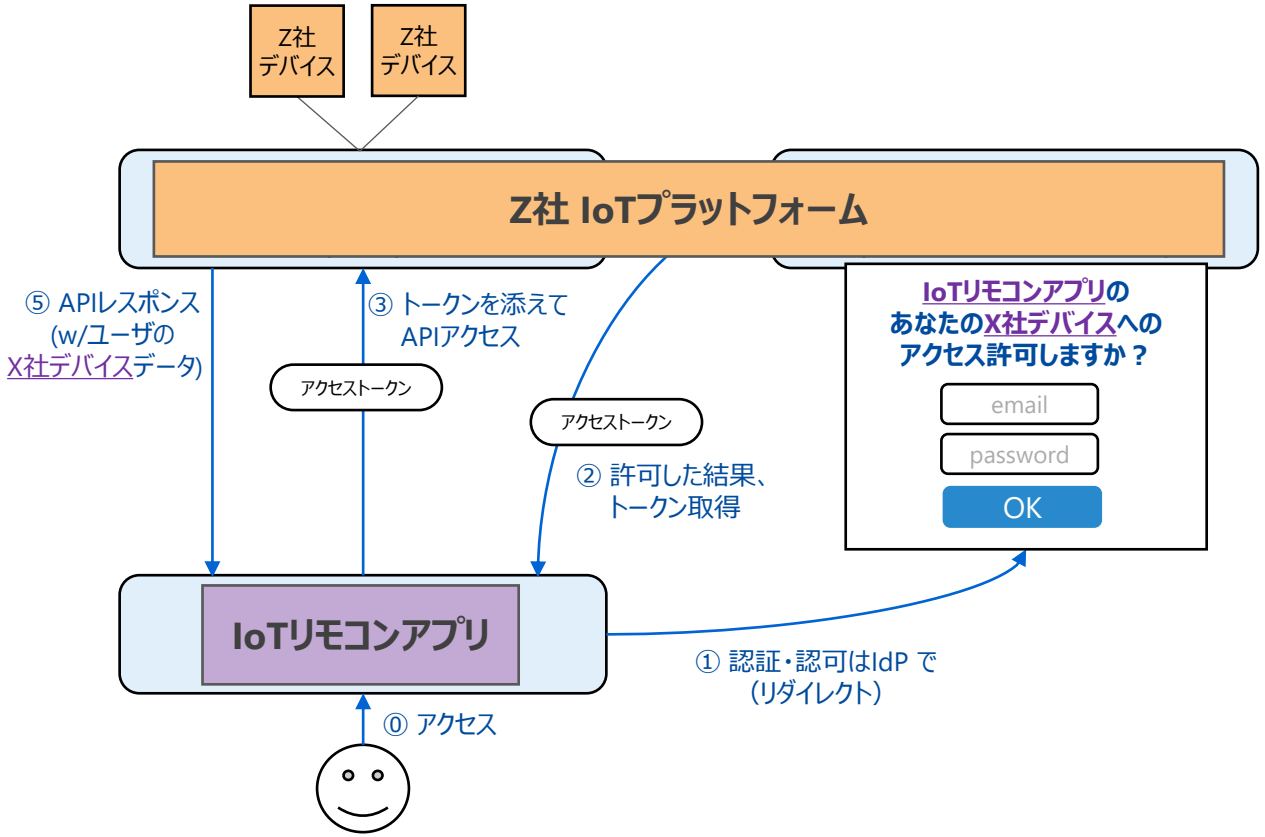




IETFにおけるWeb標準のIoT領域への応用

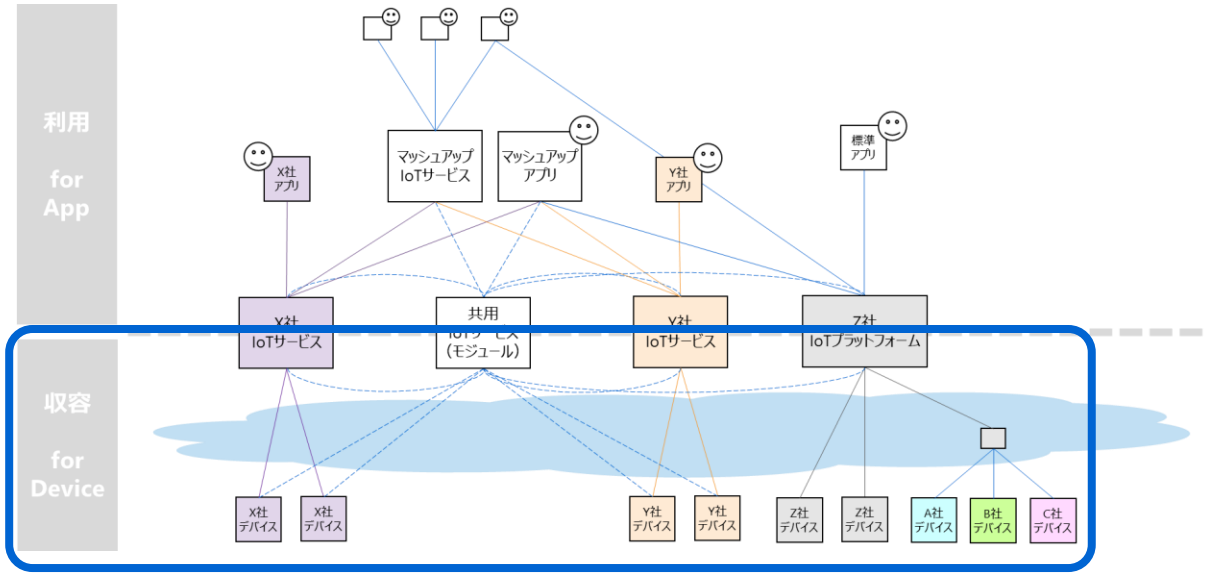
- IoTプラットフォームと、それと連携するアプリの認証・認可・アクセス権限管理にも

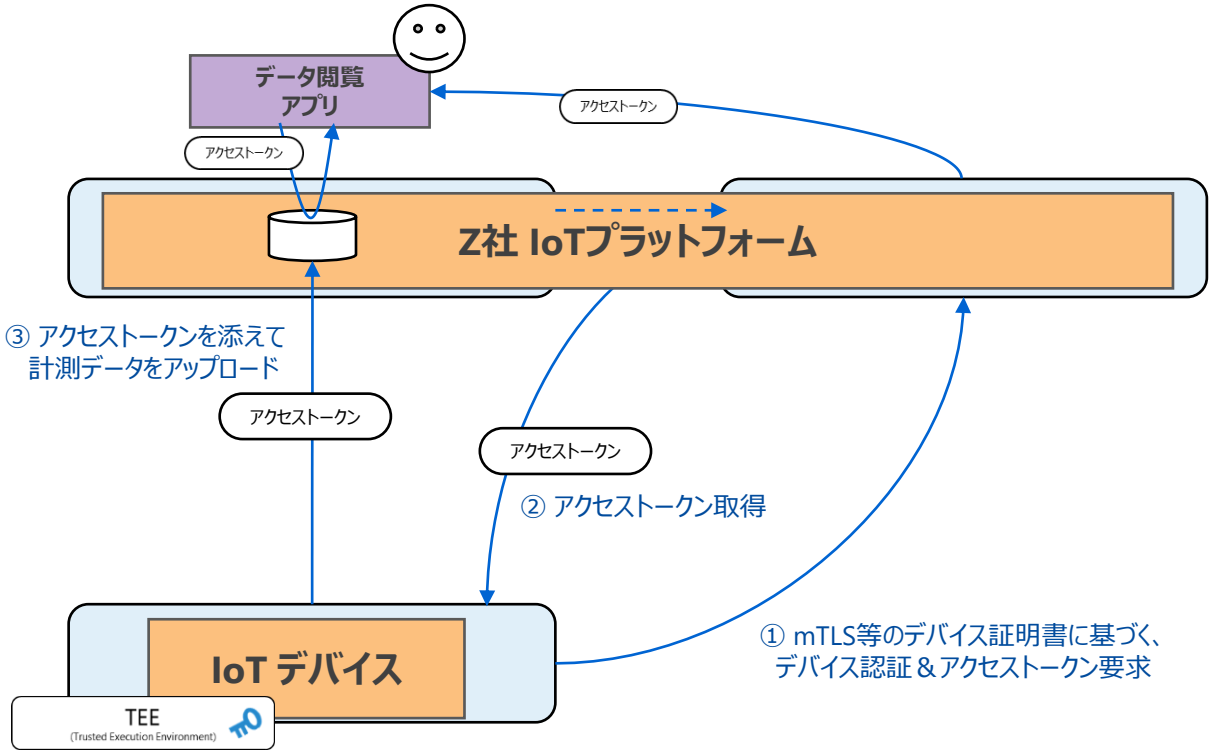




IETFにおけるWeb標準のIoT領域への応用

- IoTプラットフォームと、つながるデバイスの認証・認可・アクセス権限管理にも

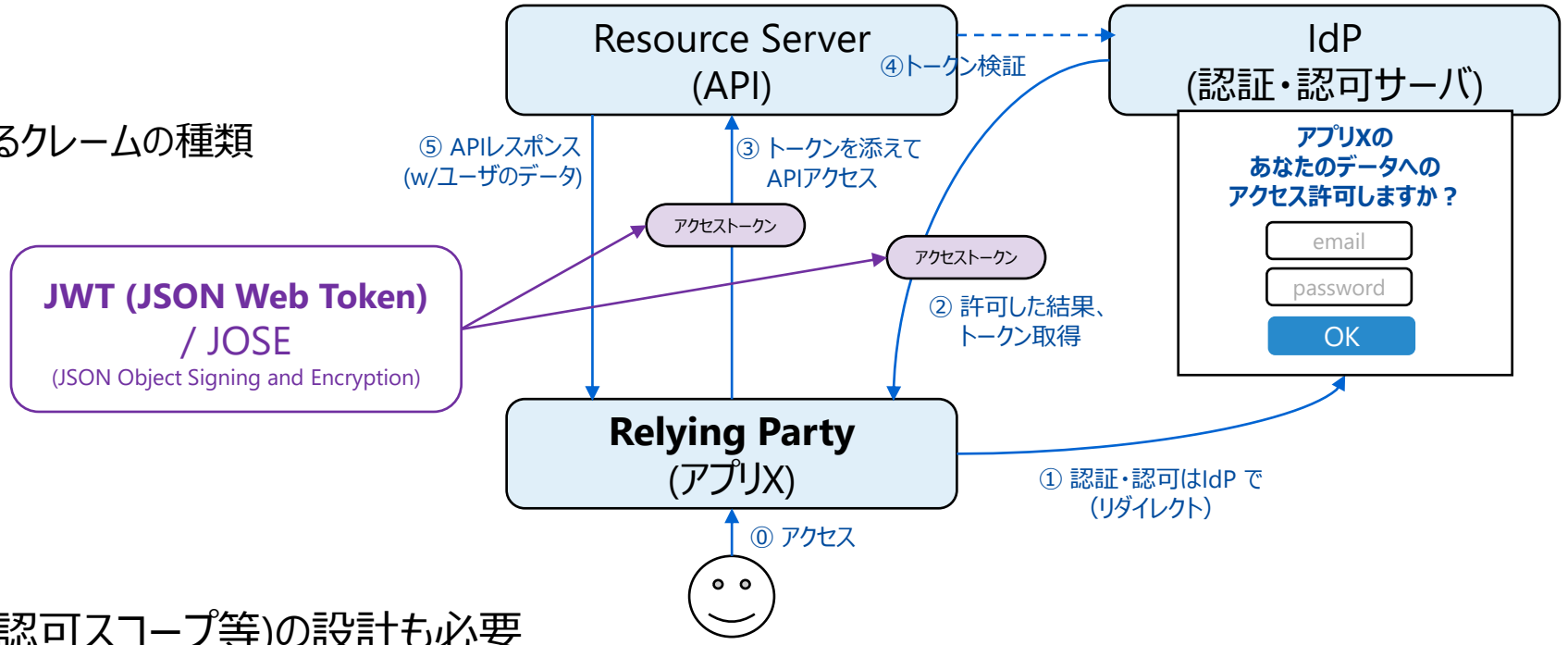




IETFにおけるWeb標準のIoT領域への応用：課題

単に「OAuth」を使います、では済まない世界

- アクセストークン形式としては、ランダム文字列に加えて、JWT（JSON Web Token）が普及している
- JWTは、前掲のCOSEのJSON版「JOSE」のペイロードに属性データ(クレーム群)を定義したもの
- ・・・アクセストークンの種類だけでなく、OIDC/OAuth2.0を利用する場合、多様な選択肢からの「選択」を迫られる
  - アクセストークンの種類
  - アクセストークンの取得方法
  - アクセストークン(JWT)に含めるクレームの種類
  - 認可フロー
  - クライアント認証方法
  - (JWTを選択する場合・・・)
  - 鍵タイプ・曲線
  - 署名アルゴリズム
  - 含めるヘッダ
  - ・・・
- その他、自由度の高いパラメータ(認可スコープ等)の設計も必要



セキュリティ重視の潮流を見据えた W3C WoT の方向性とは？

利用

for

App

収容

for

Device

WoTの立ち位置は、異なるIoTプラットフォームをつなげられる「Relying Party」の標準か

De-Siloを標榜するWoTはこの位置づけ

W3C WoT (Web of Things)

X社 アプリ

マッシュアップ IoTサービス

マッシュアップ アプリ

Y社 アプリ

④ マッシュアップのための標準

X社 IoTサービス

共用 IoTサービス (モジュール)

① 共通機能の標準

Y社 IoTサービス

IETF, etc.

IETFでは主にセキュリティ領域の共通仕様策定が進められている

X社 デバイス

X社 デバイス

Y社 デバイス

Y社 デバイス

Z社 デバイス

Z社 デバイス

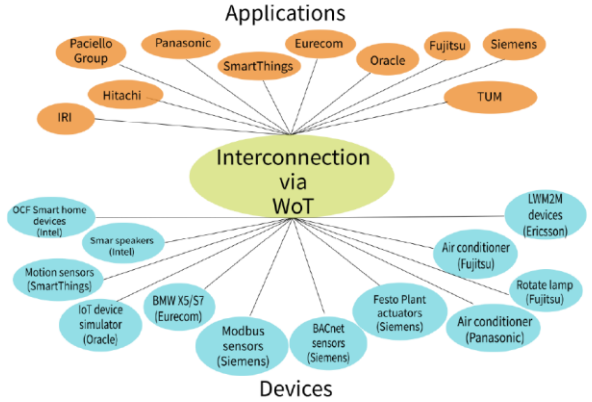
A社 デバイス

B社 デバイス

C社 デバイス

Web of Things(WoT)とは

- 異なるIoTプラットフォームを、Web技術を使って、相互接続できるようにすることを目的に、Web技術の国際標準化を行うWorld Wide Web Consortium(W3C)で Web of Things(WoT)の標準化が行われている。
- WoTはプロトコルではなく、様々なプロトコル、プラットフォーム、サービスがWoTに対応することによって、異なるプロトコル、プラットフォーム、サービスを相互接続しやすくするための仕組みである。



おわりに

まとめ

- 2つのフォーラム標準化団体（W3C と IETF）のIoT領域における守備範囲を、実世界のIoTサービス・プラットフォームの中に位置づけ、俯瞰した
- IETF と、IETFで議論されているIoT・セキュリティ関連の標準化動向を概観した
- IETFでは、IoTデバイス(クライアント側)の中のセキュア・コンポーネント(TEE)に信頼の起点をおき、これを前提としてデバイスを安全に扱うための様々な通信プロトコル（<-->IoTプラットフォーム等）が開発されている
- OAuthやJOSEといったWeb向けに開発された仕様も、昨今のリッチなIoTデバイスには有用であり、IoT領域にも応用されている

TOSHIBA