TTCセミナー
(2022/01/28)

IoT機器から収集するプライバシー情報を含むデータの保護技術の調査

髙山献、伊藤忠彦
（セコム株式会社　ＩＳ研究所）

本日紹介する内容

プライバシー保護の未来像

将来に渡って保護し続けるIoT機器の運用体制

標準化を進めて安全性を確保したい領域

検証　**管理**　**アップデート**

App

プライバシー情報を扱うApp

System

OS/ Firmware

RATS

TEEP

SUIT

Cryptography

署名、暗号化、暗号移行

秘密計算

Hardware

Confidential Computing

一貫したプライバシー保護

普及したTEE技術による切れ目のない情報管理

背景：TEE技術と情報管理

(TEE: Trusted Execution Environment)

- 例）iPhone Touch IDとTEE技術
  - 目的と目標
    - 所有者本人が利用していることを確認する
    - 指紋情報の漏洩や認証の迂回は許されない
    - たとえiOSが乗っ取られても安全な仕組みを作りたい
  - Touch IDの実装にはTEE技術が利用されている
    - 指紋の保管、指紋照合の計算処理は iOSから隔離された計算環境で行われる
    - 耐タンパー性を持ち、登録された指紋情報の漏洩を防ぐ

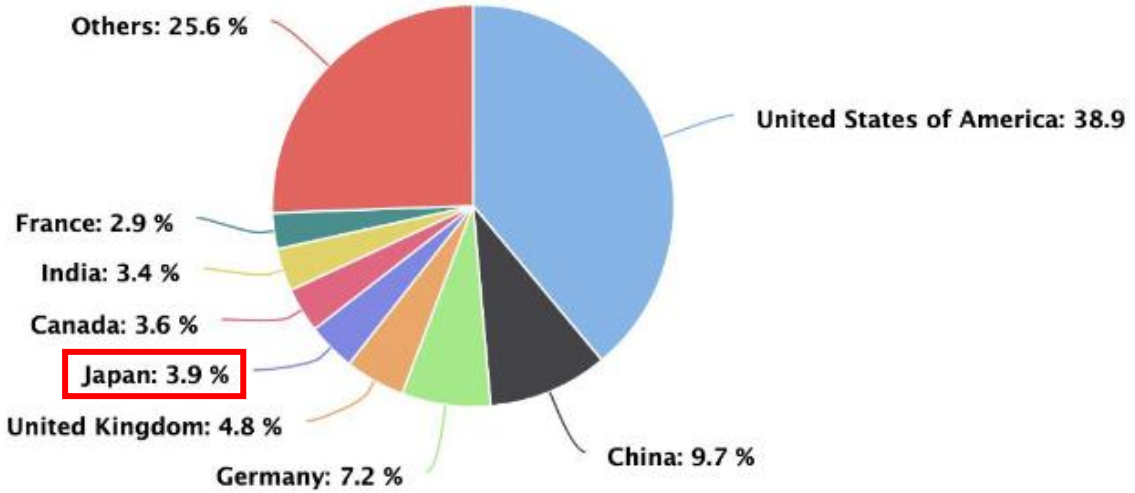
背景：なぜ標準化するのか

- プライバシー保護のためには情報管理が必須
  - 効率的な情報管理のためには暗号技術の利用が有効
- TEE技術を用いることで暗号処理の健全性を担保する
  - TEEによって隔離された実行環境を用意する
  - 鍵の漏洩や改ざん、暗号計算への介入を防ぐ
- 各保護技術は適切に使う必要がある
  - 適切な構成方法、プロトコル、計算方法、運用方法などがある

➢標準化をする、標準に準拠することで恩恵を受けられる

国際標準化団体IETF

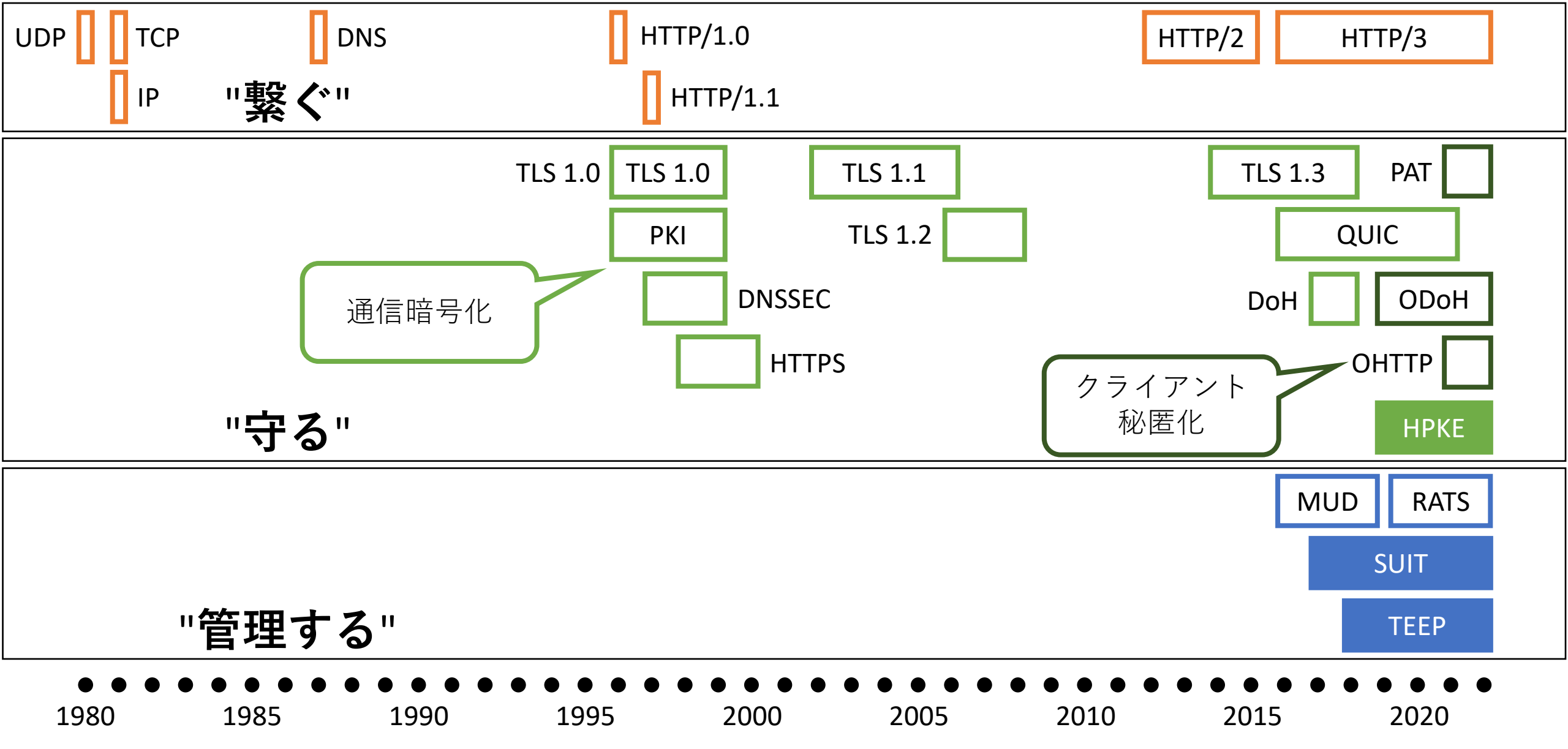
- Internet Engineering Task Force
  - インターネットに関連する技術標準をまとめる団体の一つ
- Internet Draft (I-D)とRequest for Comments (RFC)
  - I-D: 標準を策定している段階からその下書きを公開する
  - RFC: 出版して公開段階にある標準
- IETF Meeting (オンライン開催)
  - 第111回 (2021/07/26-30)、1369人
  - 第112回 (2021/11/08-12)、1037人



IETF112参加者の国の内訳

https://datatracker.ietf.org/meeting/112/materials/slides-112-ietf-sessa-all-slides-ietf-112-plenary-02

IETFの標準化対象の広がり

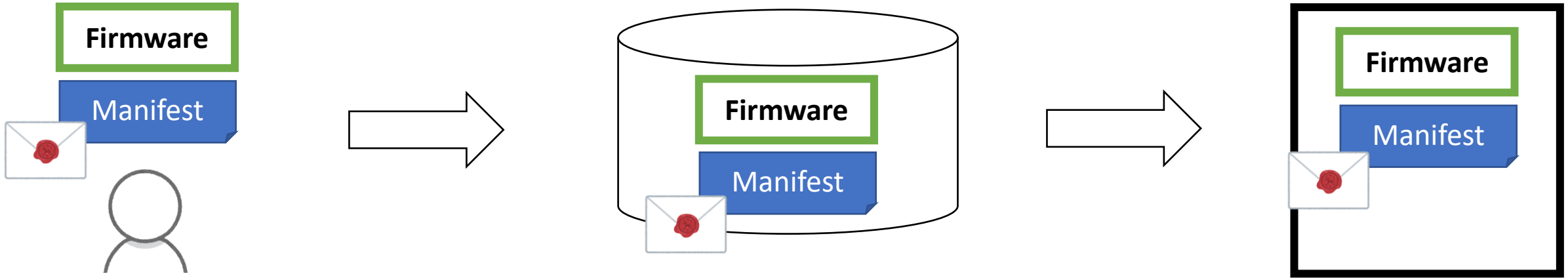


本日紹介する標準

- IoT機器の安全な管理を行うための標準
  - SUIT: IoT機器のFirmwareアップデートに関する標準
  - TEEP: TEE環境の管理に関する標準
- PQCやIoT環境を見据えた移行への議論
  - HPKE: (IoT機器でも利用しやすい) ハイブリッド暗号に関する標準
  - PQC移行、低リソース環境での選択

SUIT: Software Updates for Internet of Things

- IoT機器の安全なFirmware更新の仕組みを検討
  - 制約のある (～10KB RAM等) IoT機器でも利用可能
  - IoT機器はアップデート発行者・データが正当であることを検証可能
  - SUITでは主にデータフォーマット (SUIT Manifest) を決める



Author
ファームウェアの作成
Manifestの作成・署名

Device Operator
デバイスとファームウェアの管理

Network Operator

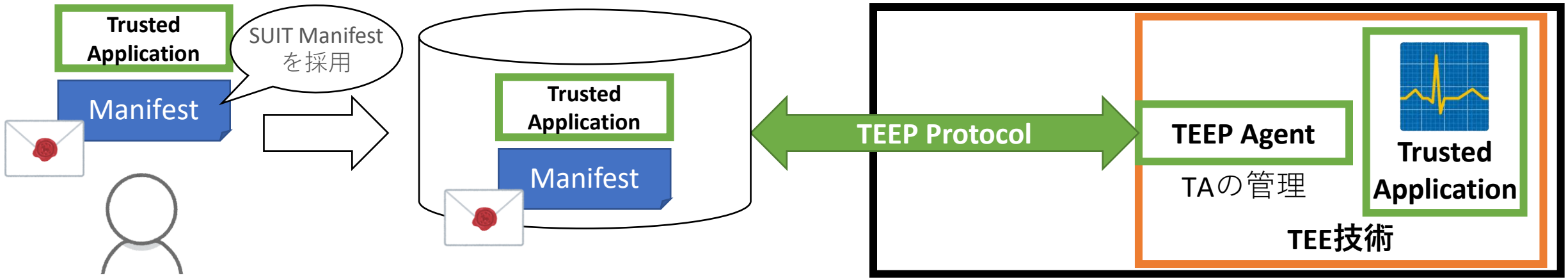
Device
Manifestの署名検証
ファームウェアの更新

SUITに登場する各者の役割

https://www.rfc-editor.org/rfc/rfc9019.html

TEEP: Trusted Execution Environment Provisioning

- TEE外からTEE内のソフトウェア管理を安全に行う仕組みを検討
  - TAMは、IoT機器のTEE内のソフトウェア (TA) を遠隔から管理する
  - 外部から隔離されたTEE内の変更はTEEP Agentが行う
  - TEEPでは主に伝送プロトコル (TEEP Protocol) を決める



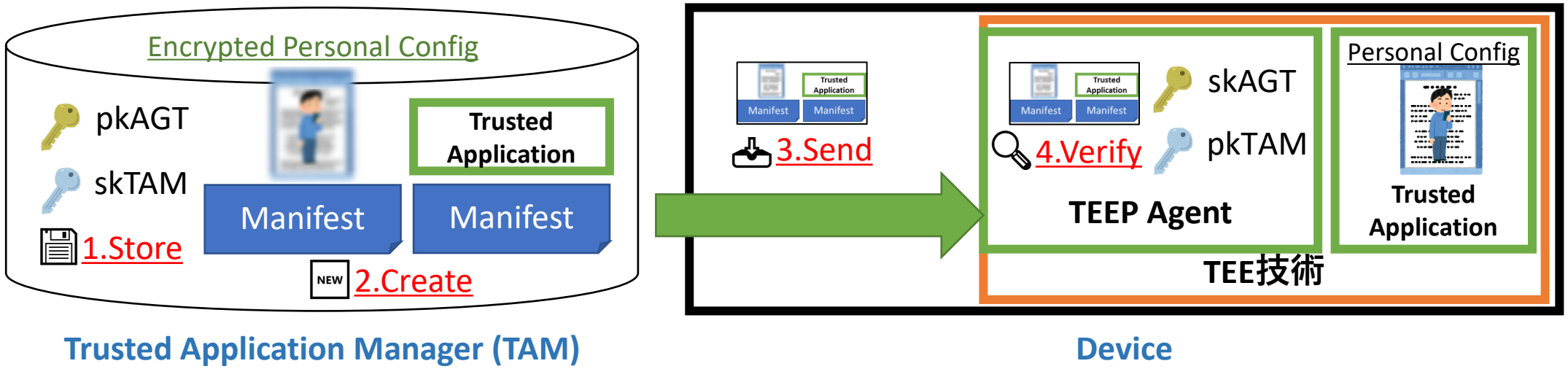
TEEPに登場する各者の役割

https://datatracker.ietf.org/doc/html/draft-ietf-teep-architecture-15

標準の活用例：プライバシー情報を扱うTA

A) IoT機器の安全なプロビジョニング

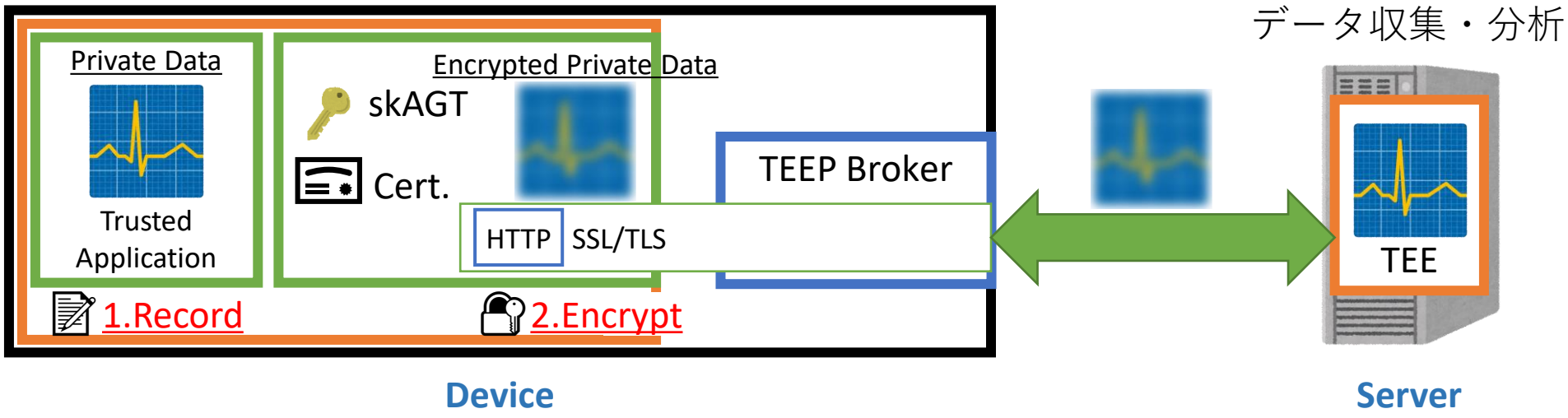
1. TEEP AgentとTAMは互いの公開鍵を安全な場所に所持しておく
2. DeveloperはTrusted Applicationとそのsuit Manifestを作成する
   - プライバシー情報を含む部分はHPKE (後述) を用いて暗号化する
3. TAMはTEEP Agentと通信をしてSUIT Manifestを送信する
4. TEEP AgentはSUIT ManifestとTAの正当性を検証してインストール



標準の活用例：プライバシー情報を扱うTA

B) Applicationの実行段階

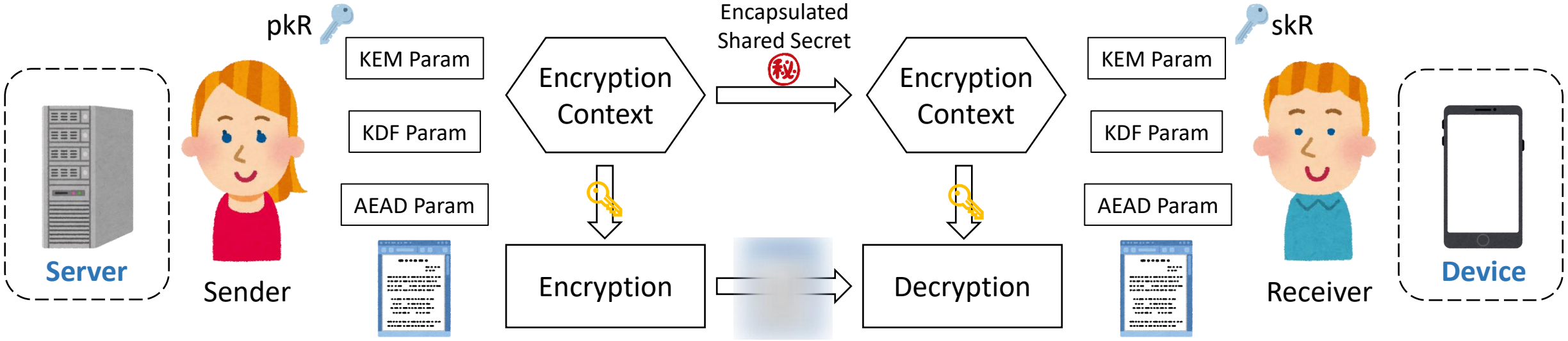
1. プライバシー情報を含むデータはTEE内で格納・計算する
2. TEE外のサーバ等と送受信するときの暗号化と復号はTEE内で行う
   - 標準化中のTEEP over HTTPSも参考にすることができる
   - TLS通信を行う場合は、信頼する証明書データもTAと一緒に用意しておく
3. TAの更新を検知した場合はTEEP Agentに通知する実装も可能



HPKE: Hybrid Public Key Encryption

- ハイブリッド暗号に関する標準化
  - 既存暗号を組み合わせ、より多様な環境で利用できる
    - 例：計算量の限られたIoT機器向けに、ストリーム暗号を利用
  - RFC化間近

IoT機器の
ネットワークに
制約がある場合も
利用しやすい



HPKEでの暗号化手順と復号手順

https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hpke-12

今後の暗号アルゴリズムについての議論も盛り上がっている

- PQC時代でも安全な秘匿目的の通信に向けての方向性
  - 対称鍵暗号部分は、AESの鍵長伸長で対応
  - 既存暗号とPQCの両方が危殆化しない限り安全な方式が採用可能な仕組み整備（RFC8773, HPKE）
  - 収集対象となりうるデータを増やし、攻撃コストを上げる（意図せず？進行中）

- 通信のエンティティ認証を保護するための方向性
  - データの分類、棚卸し[1]
  - Cryptographic Agilityの向上（ファームウェアアップデート、暗号のモジュール化、証明書有効期間短縮等）[2]

[1]NCCoE(NIST), Data Classification Project, https://www.nccoe.nist.gov/data-classification
[2] EKR, ” Securing Cryptographic Protocols Against Quantum Computers”, https://educatedguesswork.org/posts/pq-security/

検討中の問題：低リソースの機器

- 【選択１】従来暗号又はPQCの片方のみを利用する事を想定[3]
  - 利点：ソフトウェアの複雑性低下、ハードウェアのコスト低下
  - 欠点：PQCが従来暗号（例えばeddsa）より早く危殆化する可能性がある
    - Latticeを利用した暗号方式の想定される安全性が再三低下している点は無視できない[4]

- 【選択２】従来暗号とPQCの両方を（ハイブリッドモードで）利用する事を想定
    - １枚の証明書には1つの公開鍵と署名を入れる方法と、１枚の証明書に複数の公開鍵と署名を入れる方法がある
    - ソフトウェアスタックのどの部分に組み込むのが適切かの別の議論もある
    - 実装の複雑性や、鍵管理の煩雑性に影響する
  - 利点：従来暗号と既存暗号の両方片方が危殆化してもある程度の安全性を保てる、
  - 欠点：実装の複雑性増加、バグの増加

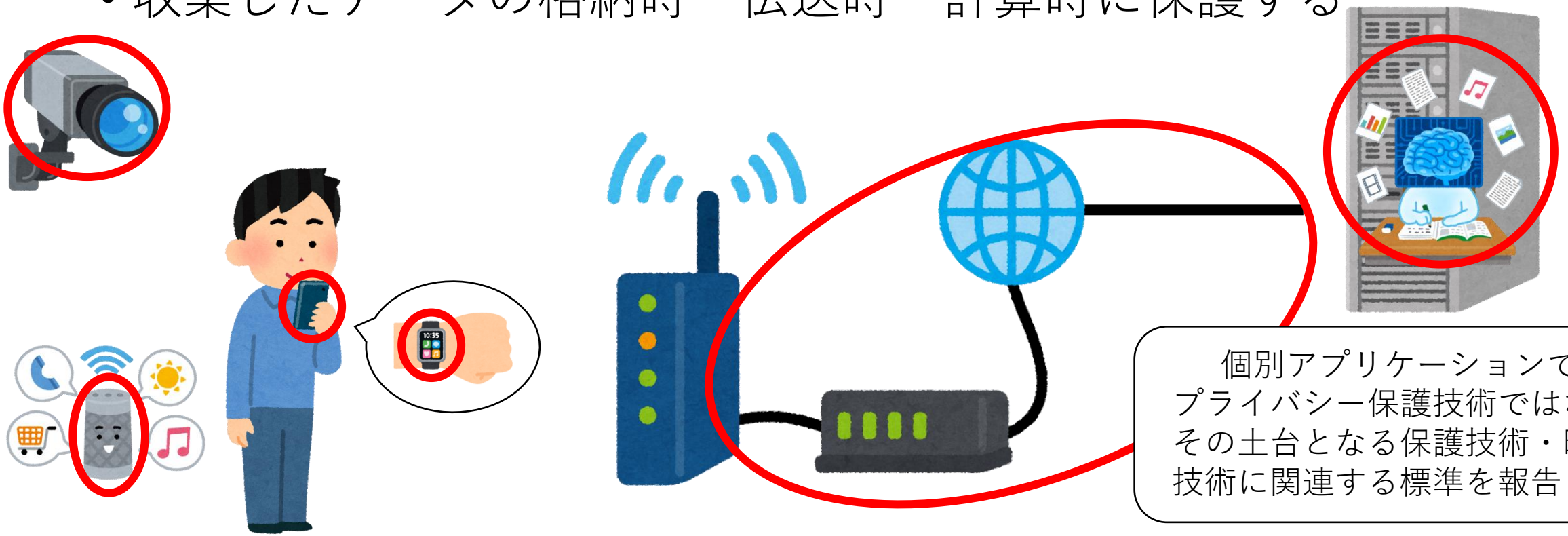
[3] G. Banegas他“Quantum-Resistant Security for Software Updates on Low-power Networked Embedded Devices” https://arxiv.org/abs/2106.05577
[4] https://mailarchive.ietf.org/arch/msg/cfrg/T3XgKeJr4-PvmPrS5TwVNfW9t_w/
[5] NSA, “HYBRID DESIGNS” https://datatracker.ietf.org/meeting/112/materials/slides-112-lamps-hybrid-non-composite-multi-certificate-00

まとめ

- IoT機器関連の標準化動向調査
  - SUIT: 中核部分は固まりRFC化へ、拡張部分はこれから
  - TEEP: 中核部分はADレビュー中、プロトコル策定は継続中
  - 暗号: IoT機器本体やネットワークの制約の中で適するものを選択

想定するIoT機器とその環境

- プライバシー情報を含むデータをやり取りするIoT機器
  - IoT機器にはセンサデバイス、スマートフォンなどを含む
  - 収集したデータの格納時・伝送時・計算時に保護する



個別アプリケーションでの
プライバシー保護技術ではなく、
その土台となる保護技術・暗号化
技術に関連する標準を報告します

IoT機器への技術標準の導入

- IoT機器同士の相互接続性が高まる
  - 同じプロトコルを用いて通信すれば他社製品との連携が可能になる
  - プラットフォームの利用・切り替えコストが低下する
- 公開してもなお安全な仕様を利用できる
  - Security by Obscurityとは別のアプローチを取れる
  - 標準化プロセスの中でSecurity Considerationsは議論されている

現在のiPhoneはApple社が
独自仕様のTEEを占有している

他社AppもTEEを利用できれば
安全性の高いAppを実現可能

参考：IETFの主要な標準化プロセス

1. Individual Internet Draftの提出、Working Groupを指定可能
2. Working GroupへのAdopt→WG Internet Draft
3. Working Group Last Call (WG内で異存がないことを確認)
4. Area Director Review (by WGが所属するAreaの専門家など)
5. IETF Last Call (IETF内で異存がないことを確認)
6. RFC Editor Review (出版前の校正)
7. RFC

参考：https://datatracker.ietf.org/help/state/draft/ietf
https://datatracker.ietf.org/help/state/draft/irtf

IETF SUIT

※I-D=Internet Draft（下書き段階）
RFC=Request for Comments（標準）

- 各標準の進捗状況
  - ドキュメントの基礎部分はRFC化
  - Manifestは3分割して、中核になる部分を優先して標準化中
  - Firmware EncryptionはCOSE、HPKEなど他の標準とも関連

Document	Status (次ページ)	Content
SUIT Architecture	RFC9019 (7/7)	SUITの目的の設定、用語の定義
SUIT Information Model	RFC9124 (7/7)	Manifest内の要素の定義、セキュリティ要件
SUIT Manifest	WG I-D (2/7)	Manifestの具体的なフォーマット定義
SUIT Multiple Trust Domains	Individual I-D (1/7)	複数者が絡む場合などのManifestの拡張
SUIT Update Management	Individual I-D (1/7)	詳細な条件分岐を行うためのManifestの拡張
Firmware Encryption	WG I-D (2/7)	暗号化したFirmwareをDeviceが復号するための拡張
SUIT Report	WG I-D (2/7)	Manifestの実行結果のログフォーマット

SUIT WGに関連付けられた各ドキュメントの進捗（参考：https://datatracker.ietf.org/wg/suit/documents/）

IETF TEEP

- 各標準の進捗状況
  - ドキュメントの基礎部分はArea Directorの査読中
  - 主にTEEP Protocolを整備中
    - SUIT ManifestやRATS Claimのサンプルを整備して検証中
    - 現時点で電子署名による改ざん対策のみ、暗号化対応について協議中
      - 暗号化は他のメッセージレイヤでの提供も可能な構成（HTTPSなど）

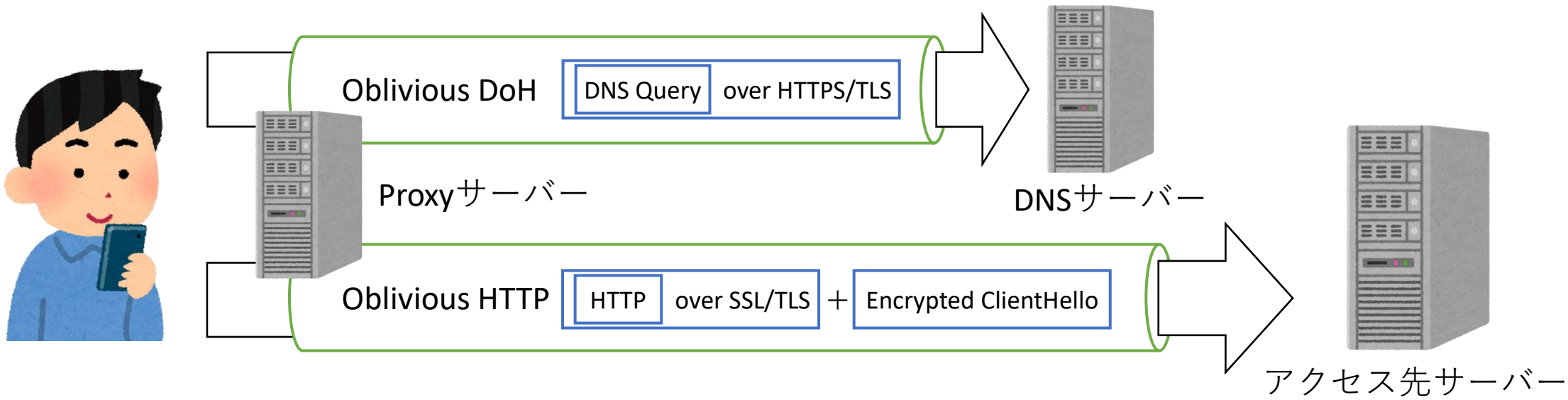
Document	Status	Content
TEEP Architecture	AD Review (4/7)	TEEPの目的の設定、用語の定義
TEEP Protocol	WG I-D (2/7)	遠隔からのTEE管理のための通信プロトコルの定義
TEEP over HTTP	AD Review (4/7)	TEEP Protocolの下でHTTP(S)を使う場合の手引

TEEP WGに関連付けられた各ドキュメントの進捗（参考：https://datatracker.ietf.org/wg/teep/documents/）

Webアクセス時のプライバシー

- Webアクセスをトラッキング・広域監視から保護
  - PCやスマートフォンは多岐にわたるWebアクセスを行う
  - アクセス履歴はユーザーにとってプライバシー情報
  - アクセストラッキングに用いられる情報を保護したい
    - MACアドレス、クライアントIPアドレス、サーバードメイン名、サーバーIPアドレス、 Cookie、 …

本報告の対象範囲



プライバシー関連の動向

- プライバシーに配慮するプロトコルは近年のトレンド
  - 多機能なIoT機器を介してプライバシー情報が収集されることを防ぐ
  - 単体で保護する範囲は狭いので組み合わせが大事

Document	WG	Status	Start	End	保護対象	誰から
HTTP Proxy (HTTP/1.1)	HTTP	RFC2068	1995	1997	クライアントIPアドレス	アクセス先サーバー
HTTPS	TLS	RFC2818	1998	2000	HTTP通信本体	中間者
DNS over HTTPS (DoH)	DOH	RFC8484	2017	2018	サーバードメイン名・IP	中間者
Encrypted ClientHello	TLS	I-D	2018	-	サーバードメイン名・IP	中間者
Oblivious DoH	-	I-D	2019	-	クライアントIPアドレス サーバードメイン名・IP	DNSサーバー、中間者 Proxyサーバー、中間者
Oblivious HTTP	HTTP	I-D	2021	-	クライアントIPアドレス HTTP通信本体	アクセス先サーバー、中間者 Proxyサーバー、中間者
Private Access Tokens	-	I-D	2021	-	ユーザーアカウント クライアントIPアドレス アクセストークン	アクセス先サーバー、中間者 アクセストークン発行サーバー、中間者 Proxyサーバー、アクセストークン発行サーバー

セコムによる標準化への貢献 (2021年度)

- I-D提出2件、I-D修正の提案4件

Document	WG	区分	URL
draft-ito-documentsigning-eku	LAMPS	新規I-D	https://datatracker.ietf.org/doc/draft-ito-documentsigning-eku/
draft-mtis-lamps-8410-ku-clarifications	LAMPS	新規I-D	https://datatracker.ietf.org/doc/draft-mtis-lamps-8410-ku-clarifications/
TEEP Protocol	TEEP	I-D修正	https://github.com/ietf-teep/teep-protocol/pull/172
TEEP Protocol	TEEP	I-D修正(Review中)	https://github.com/ietf-teep/teep-protocol/pull/169
TEEP Protocol	TEEP	I-D修正(Review中)	https://github.com/ietf-teep/teep-protocol/pull/177
SUIT Manifest	SUIT	I-D修正(Review中)	https://github.com/suit-wg/manifest-spec/pull/41

- IETFハッカソンで策定中の標準を検証→I-Dに反映
  - TEEP Protocolの通信プログラムの実装をしたlibteep開発
  - SUIT Manifestのエンコーダ・パーサを実装したlibcsuit開発