TTC「デジュール及びフォーラム標準に関する
国際標準化活動動向調査」

# IETFにおけるソフトウェアサプライチェーンとIoTデバイス向け構成管理の標準化動向調査

セコム IS研究所
磯部光平
髙山献

# 発表者の紹介

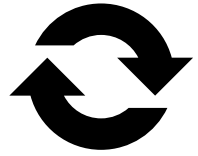
## 磯部 光平(発表者)

- 2016年セコム入社
- 2019年より
  IETFにてTEE付き
  IoTデバイスへのソフト配信仕様
  (TEEP*)の標準化に参画
- 標準仕様案準拠の配信サーバの
  実装**を通じて、仕様策定に貢献

## 髙山 献

- 2019年セコム入社
- 2020年よりIETFで
  IoTデバイス管理に
  関連する標準化に参画
- 標準ドキュメントを執筆しつつ
  OSSでlibcsuitを開発して
  ドキュメントの提案内容を検証

ドキュメント執筆



OSSでの検証

* TEEP Trusted Execution Environment Provisioning
** tamproto https://github.com/ko-isobe/tamproto
*** libcsuit https://github.com/kentakayama/libcsuit

# サプライチェーンセキュリティ

- サプライチェーンを狙った攻撃・問題
  - 多数の主体や要素で構成されるソフトウェア・PF
  - Solarwinds事件
    - 正規のOTA基盤を利用し、バックドアの広域配信・侵入が発生
  - Log4j脆弱性
    - 多数のソフトウェアに含まれるログライブラリの脆弱性
    - 暗黙に含まれるソフトも多く、影響範囲の確認・検出が課題に

- サプライチェーンセキュリティ
  - ソフトウェア構成管理の強化 (SBOM)
  - ソフトウェアコンポーネントの出自管理・流通の透明性確保

# IoTとサプライチェーンセキュリティ

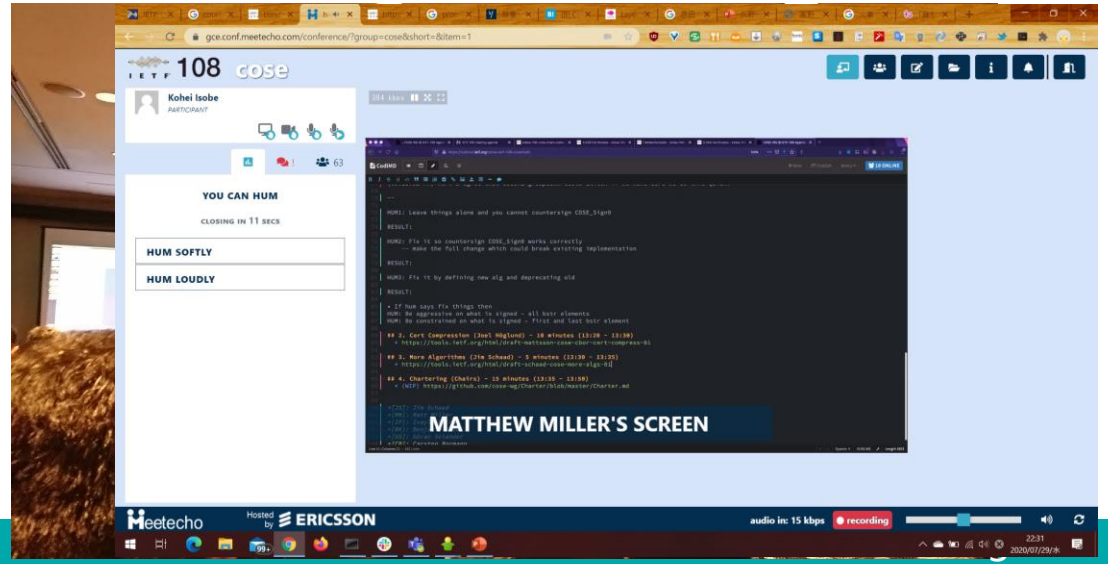
- IoTデバイス
  - 大量、大規模に展開される
    - 人手による管理・維持は困難。攻撃時の損害は甚大
      →リモート・自動化を前提としたIoTデバイスの管理
  - 多数の構成要素
    - HWドライバ、ミドルウェア、ユーザアプリなど多数のソフトウェアで構成
      →効率的・透明性のあるソフトウェア構成管理・維持

遠隔からの安全なIoTデバイスの管理
（FW更新やリモート検証）

透明性確保による
より安全なソフトウェア開発・配信

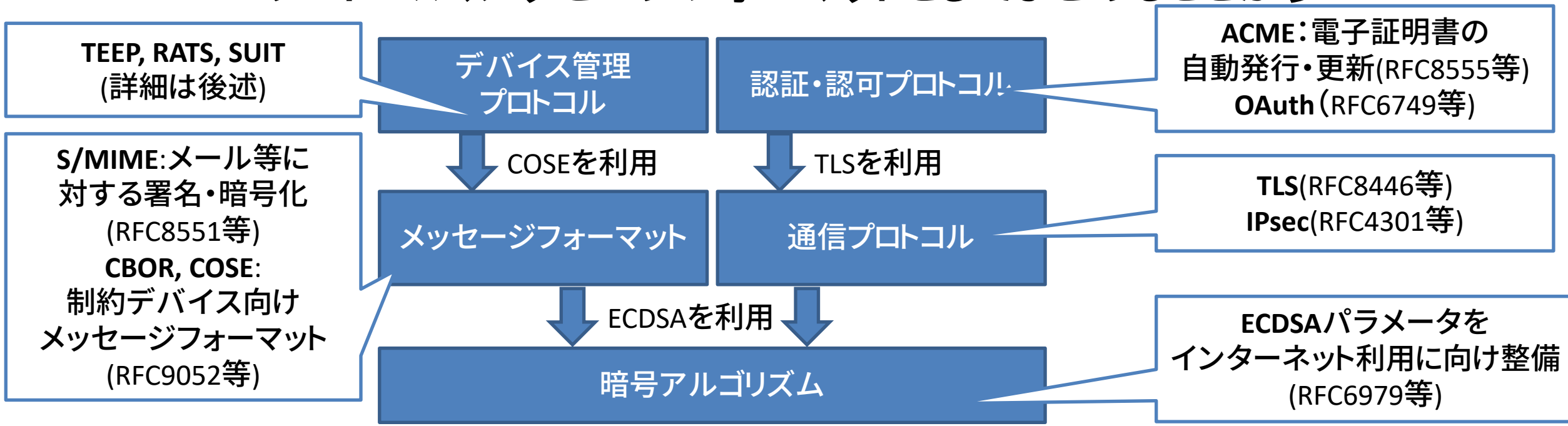
# IETF (Internet Engineering Task Force)

- インターネットをよりよく機能させるため、
  良質な技術文書の作成が使命
- フォーラム標準
  - 標準化文書はRFC(Request for Comments)として発刊
- 標準化プロセス
  - 誰でも参加可能。会員制度はなく
    個人として参加
  - 主にメーリングリストで議論
  - F2F会議を年3回開催。
    IETF117 San Francisco
    IETF118 Prague
    IETF119 Brisbane



# セキュリティに関するIETFの取組

- secエリア
  - IETFの6つの技術領域のうちの一つ
  - セキュリティ関連技術を幅広く取り扱う
    - プロトコル、メッセージフォーマットとしてまとめることが多い



# IETF標準のモットー

- *An unofficial motto of the IETF is, "We believe in rough consensus and running code."*
  - 実運用性を重視する
  - 実装に基づくフィードバックが歓迎される

標準化文書の議論

文書・仕様案

実装を経た知見
フィードバック

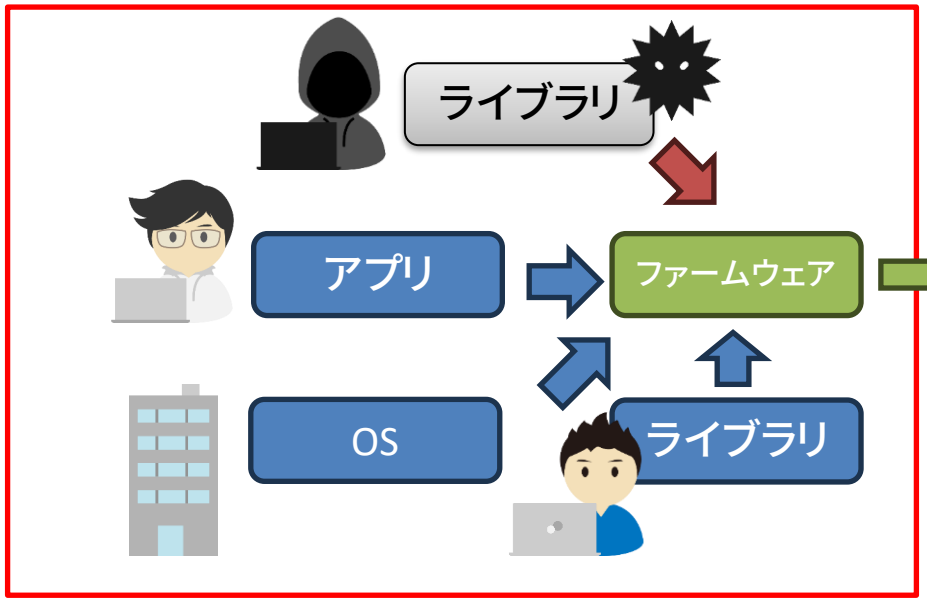
会議直前の土日に開催

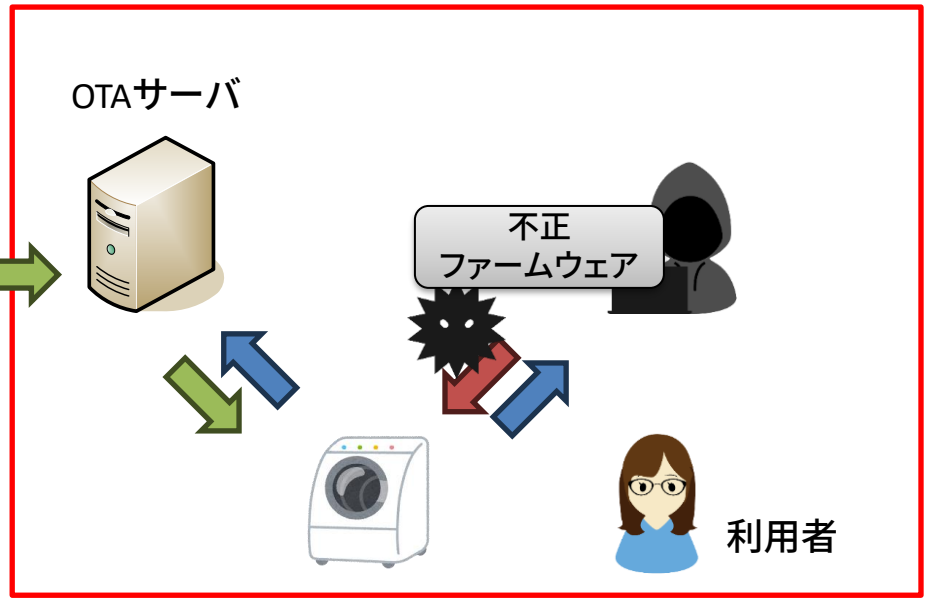
実装A

実装B

実装・ハッカソン

# 調査目標




サプライチェーンセキュリティ
↓
構成要素の信頼性を高める

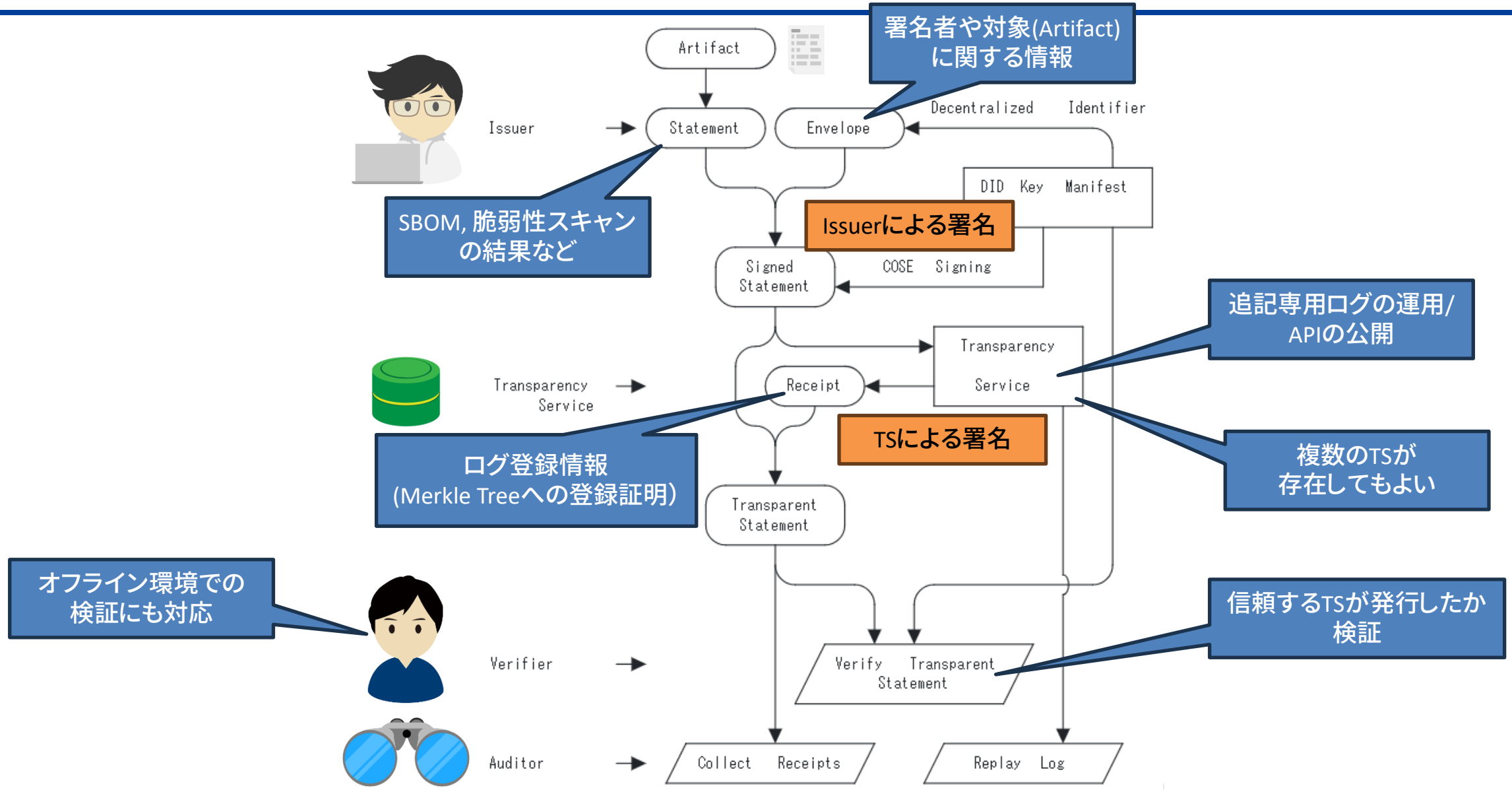
IoTデバイス構成管理
↓
信頼できる構成要素を展開・維持する

（開発中の）IETF標準仕様は、ライフサイクル全体の安全性向上に寄与するか

# サプライチェーンセキュリティ

# SCITT (Supply Chain Integrity, Transparency and Trust)

- 部品の一貫性・追跡可能性を支える標準仕様
  - 部品(ソフトウェアコンポーネント等、Artifact)の情報流通のためのメカニズム
  - 流通させる情報（ペイロード）は任意（SPDX, SLSA, CycloneDXなどを想定）
  - Statementデータの発行・検証が主なメカニズム
- 役割
  - Issuer
    - Artifactに関するStatementを作成し、署名する(Signed Statementを作る）
  - Transparency Service
    - Signed Statementを自ら持つAppend-Only Logに登録する
    - 登録の証としてReceiptを(Transparency Serviceの署名付きで）発行する
  - Verifier
    - Transparent Statement (Signed Statement + Receipt)を検証する
  - Auditor
    - 発行済みのすべてのTransparent Statementの一貫性・正確性を検証する


署名者や対象(Artifact)
に関する情報
Artifact
Issuer
Statement
Envelope
Decentralized Identifier
DID Key Manifest
SBOM, 脆弱性スキャン
の結果など
Issuerによる署名
Signed
Statement
COSE Signing
追記専用ログの運用/
APIの公開
Transparency
Service
Transparency
Service
Receipt
TSによる署名
ログ登録情報
(Merkle Treeへの登録証明)
複数のTSが
存在してもよい
Transparent
Statement
オフライン環境での
検証にも対応
信頼するTSが発行したか
検証
Verifier
Verify Transparent
Statement
Auditor
Collect Receipts
Replay Log

# WG動向 (1)

- 標準化アイテム
  - Architecture
    - SCITTの各アクターの役割・責務などを規定
    - COSE (簡約バイナリフォーマット)の署名ヘッダへの情報埋め込み・パースがコア仕様
  - Usecase for Software Supply Chain
  - SCRAPI (SCITT Reference API)
    - 相互運用性確保のため、REST API仕様を規定

- 実装
  - ハッカソンでの勢力的な開発が並行して進む

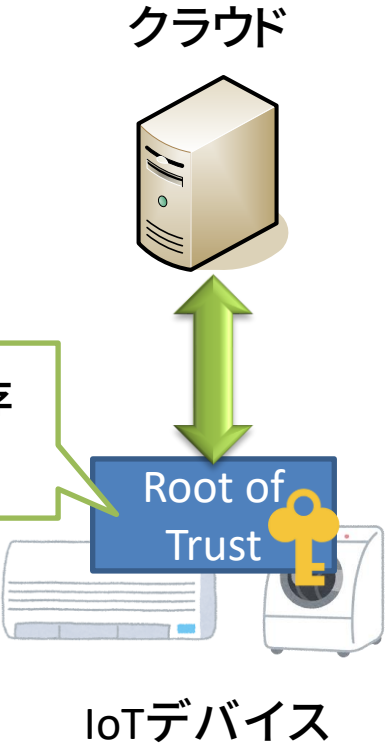
# WG動向 (2)

- 関連標準の整備
  - COSE
    - CWT Claims in COSE Headers
      Statement情報のエンコーディングに利用
    - Merkle Tree Proof
      Append-only Logへの格納証明・検証に利用
  - SPICE
    - Verifiable Credential対応COSE
    - SBOMやSCITTにおいても、セキュリティ上の理由等で
      選択的開示(Selective Disclosure)が必要

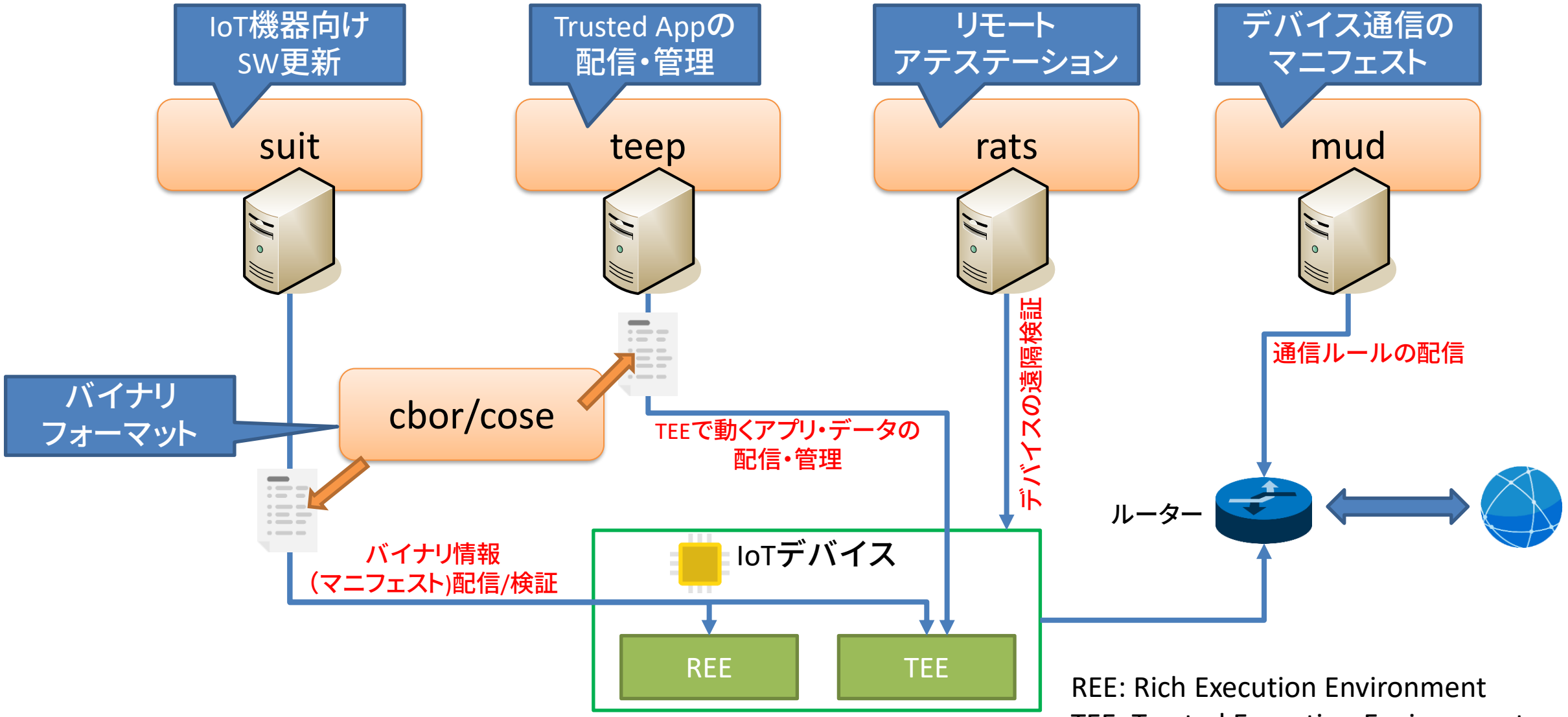
# IOT向けデバイス構成管理

# IoTセキュリティとデバイス管理

- ネットワーク越しに信頼したい
  - クラウド：正規のデバイスか見分けたい・認証したい
  - デバイス：正規のファームウェアだけ適用したい
- Root of Trust
  - 信頼の基点
  - Hardware Root of Trust
    - ハードウェア機構を利用し、攻撃耐性を持ったRoot of Trust
    - TEE(Trusted Execution Environment), セキュアエレメントなど
  - Root of Trustを拠り所にしたデバイス管理
    - デバイス認証、アップデート、アテステーションなど
    - これらの機能に必要なロジックや暗号鍵などをRoot of Trustに実装する



# デバイス管理に関連するプロトコル




REE: Rich Execution Environment
TEE: Trusted Execution Environment

# IoTデバイス管理関連

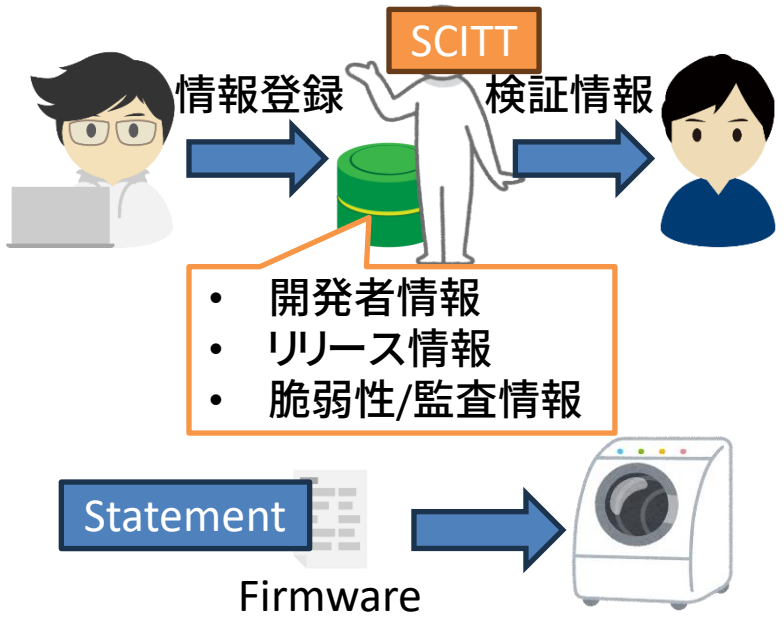
- SUIT (Software Updates for IoT, ファームウェア更新)
  - WGLC済み。AD Review対応が中心。
- TEEP (Trusted Execution Environment Provisioning)
  - TEE(隔離実行領域)へのソフトウェア配信
  - 標準仕様案の開発が完了。RFC出版待ち
  - 形式検証(Formal Verification)に関連する報告
    from NTT社会情報研究所 奥田さん
    - UFMRGにもTEEPを題材とした形式検証例I-Dが投稿

- RATS (Remote ATtestation procedureS, 遠隔検証)
  - Endorsement (製造者による証明情報)のI-DがWGアイテム化

多数の仕様の標準化(RFC化)が完了の見通し

# IoTデバイスマネジメントとの関連

- Usecase (SCITT)
  - IoTデバイスへのファーム配信
    - ファームウェアバージョンの真正性の検証
    - 適切な主体・鍵によるファームウェア署名の有無
    - 適用ファームウェアのレピュテーションの収集




- Append-Only Log
  - 信頼性確保にTEEの利用やアテステーション対応に言及
  - 上記信頼性確保状況のログへの記録も言及
- デバイス管理仕様との関連
  - 現時点ではSUIT等の仕様の参照や拡張などの動きは見られない

# まとめ

- IETFにおけるサプライチェーンセキュリティに向けた標準
  - SCITT
  - SBOMや脆弱性スキャンログなどの情報を流通させるメカニズム
    - 署名ヘッダへの拡張（追記専用ログへの記録＋記録証跡の追記・検証）
  - 仕様案と実装、関連仕様が並行して精力的に開発が進む
    - Merkle Tree Proof, Selective Disclosure
- IoTデバイスマネジメントとの関連
  - IoTデバイス管理関連仕様(SUIT, TEEP, RATS)
    - 標準化仕様案はほぼ完成し、RFC化待ちのものが多い
  - SCITTとの関連
    - ユースケースとしてファームウェアや配信の透明性検証が列挙
    - SCITTのデプロイにはよりセキュアな環境や運用が求められている
    - 明確な協業や仕様参照は現時点では存在しない