思ったより側にあったPKI関連の標準化
（IETF, CA/BForum）

セコム株式会社　IS研究所
伊藤 忠彦

2021/11/25

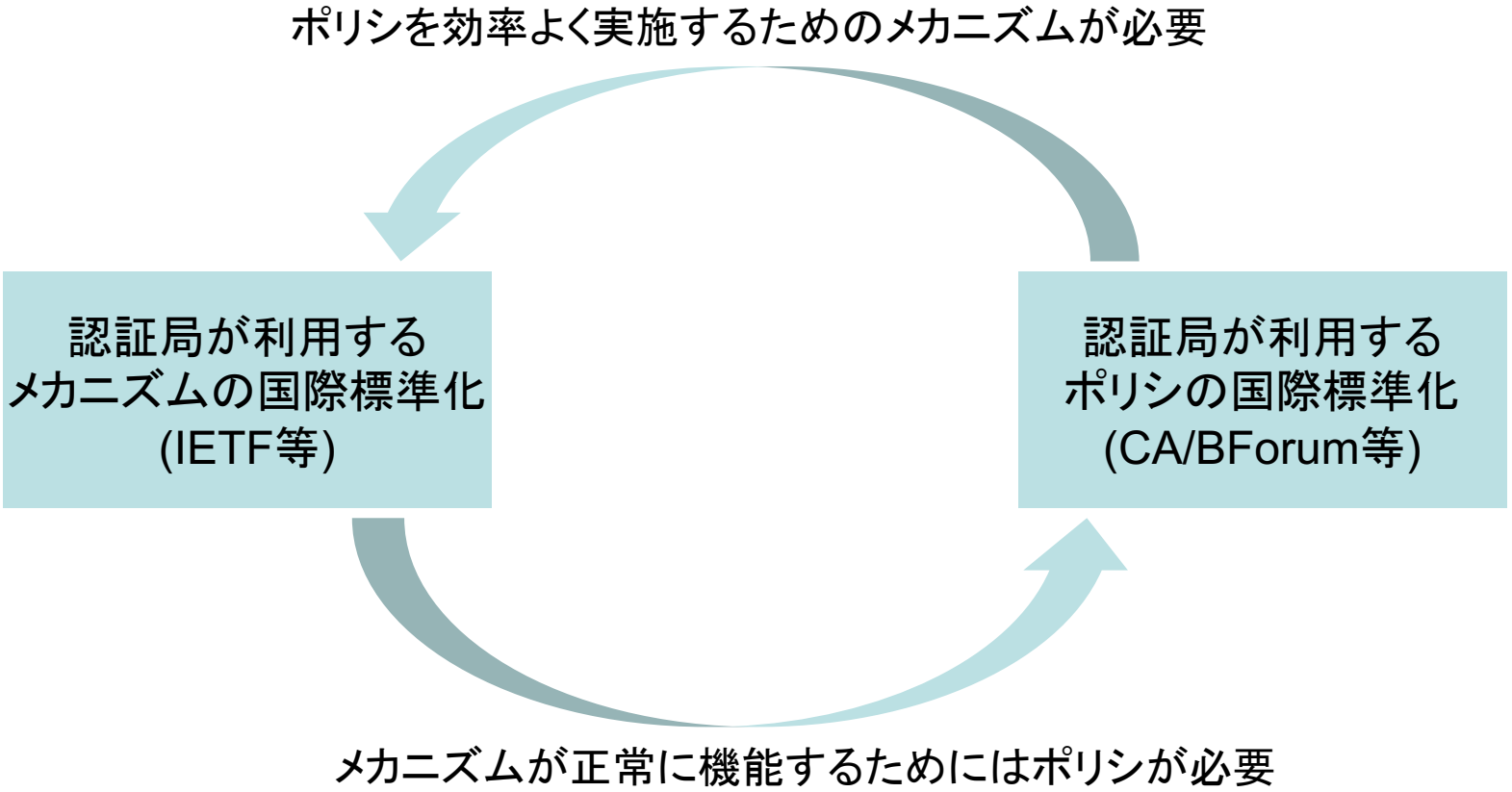
自己紹介

伊藤忠彦（セコム株式会社、IS研究所、暗号認証基盤グループ、主務研究員）

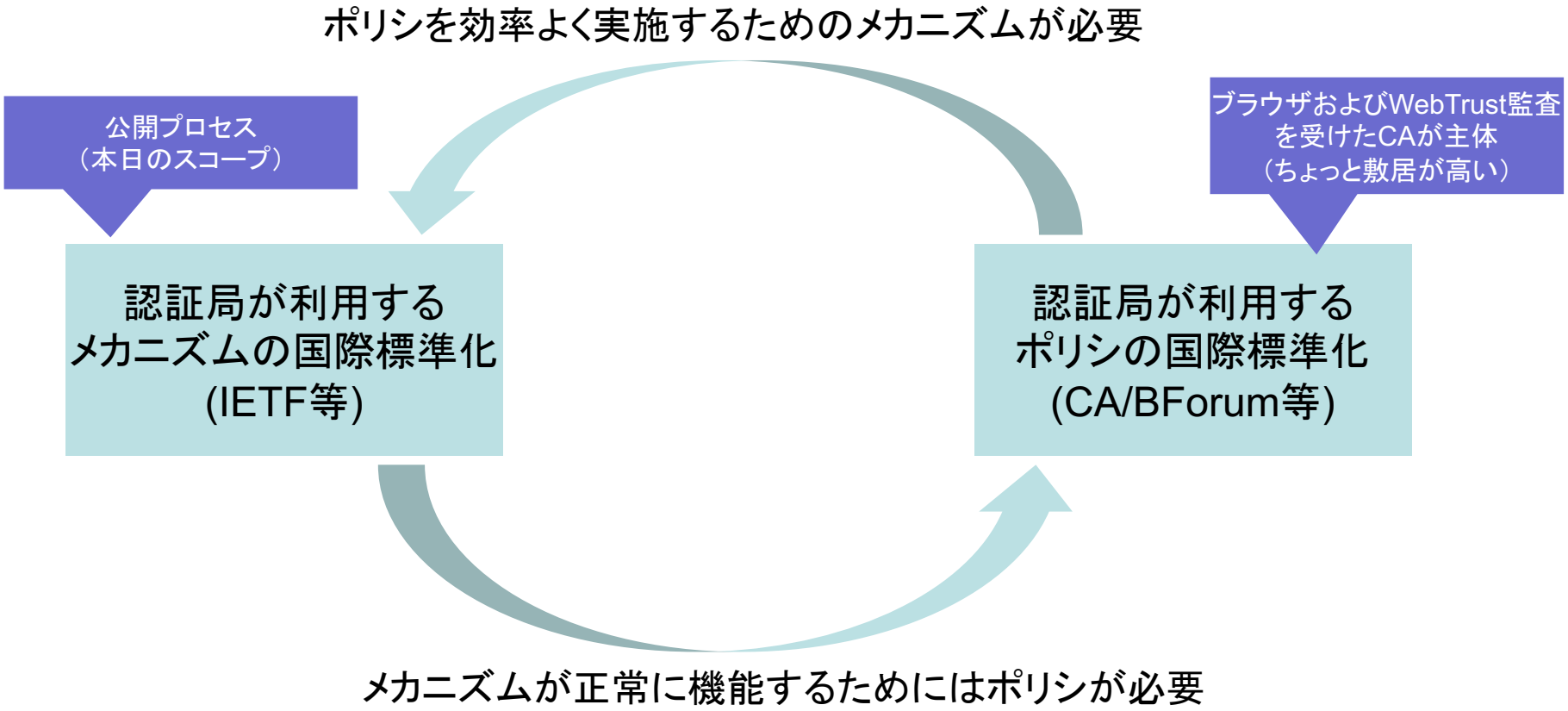
- 暗号プロトコル・暗号鍵管理に関する研究に従事
  - 低リソースデバイス（IoTデバイス等）
  - 長期的な鍵管理に関する検討
    - 量子コンピュータの影響なども
- ルート認証局関連業務（PKI分野）にも従事
  - ルート認証局構築
  - CA/Bforumでの活動
  - IETFでの活動

他にも、暗号鍵管理についての仕組みやルール作りで活動しています

PKI方面の標準化



PKI方面の標準化



IETFとは

- RFCで有名
  - RFC（Request for Comments）は、インターネットで用いられるさまざまな技術の標準化や運用に関する事項など幅広い情報共有を行うために公開される文書シリーズです。(by JPNIC)
  - 世界で最も普及しているフォーラム標準の1つ
    - tcp, ip, smtp, udp, quic, etc.

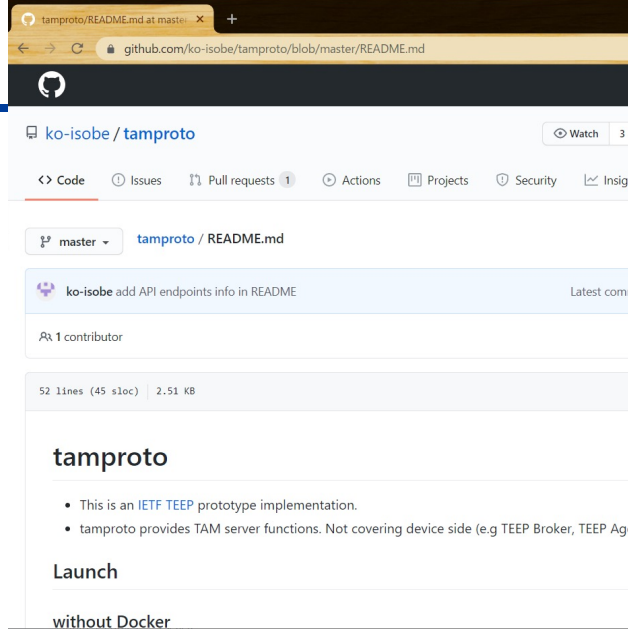
- 主にメカニズムに関する標準化

IETFでの標準化に参加するには？

- 誰でも参加できます

- 実装する人は特に歓迎されます
  - 趣味でも実装したいという人は歓迎されます
  - 色々教えてもらえるので勉強にもなります

- 実際のユースケースを持っている人（困っている人）も特に歓迎されます
  - 機能が多いほど実装の複雑性が上がる
  - ある程度の規模のユースケースがあるものを優先したい
  - 「運用で困っている事」は非常に重要
  - 関連する標準化団体に所属していると、その団体の人が助けてくれることも（反対意見に回ることも当然ありますが、同じ価値観を持つので話が早い）



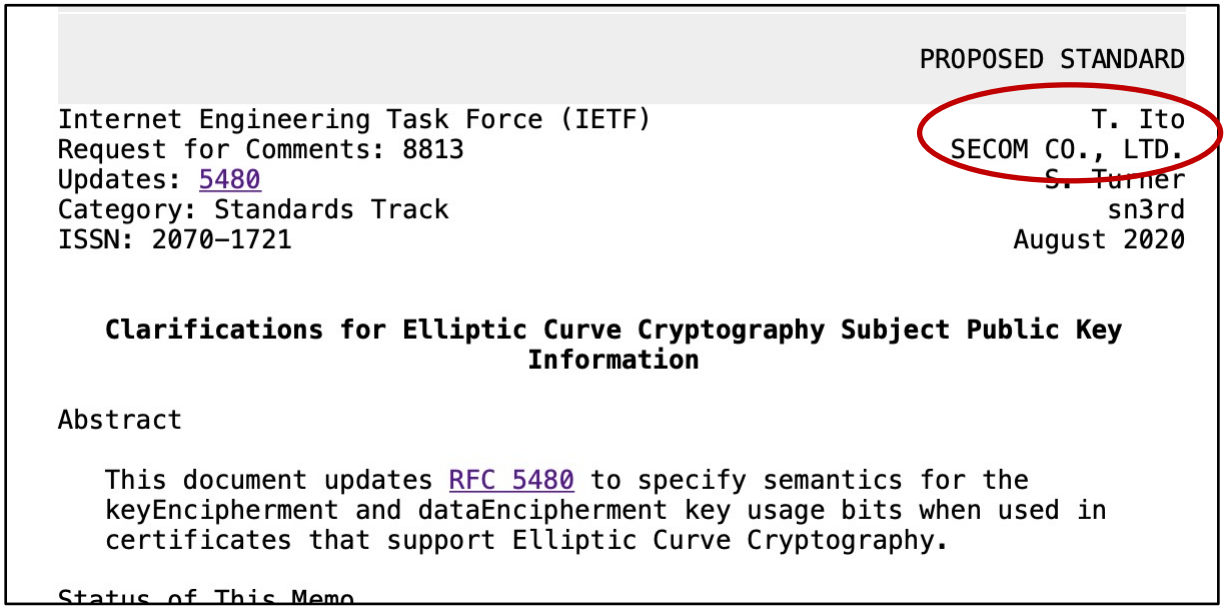
実装が歓迎される例

例：磯部光平・高山献・瀧田悠一（セコム株式会社）のケース

- Trusted Excution Enviroment Provisioning(teep) WG
  - 標準化と並行して議論している仕様を実装し、標準化にフィードバック
    - Trusted Execution Environment(TEE)を持つ
      デバイスに対するアプリケーション配信/管理プロトコル
    - 実装をOSSとして公開し、標準化プロセスにcontribute

ユースケースが歓迎されるケース（RFC8813）

- 英語圏の人があまり気にしなかった表現について、詳しい人に聞いてみた
  - 運用する上で、文章の解釈に迷った
  - 詳しい人に相談したところ、表現自体に問題があった
  - 非常に親身に相談に乗ってもらううちに、RFC化してた



PROPOSED STANDARD

Internet Engineering Task Force (IETF)
Request for Comments: 8813
Updates: 5480
Category: Standards Track
ISSN: 2070-1721

T. Ito
SECOM CO., LTD.
S. Turner
sn3rd
August 2020

Clarifications for Elliptic Curve Cryptography Subject Public Key Information

Abstract

This document updates RFC 5480 to specify semantics for the keyEncipherment and dataEncipherment key usage bits when used in certificates that support Elliptic Curve Cryptography.

Status of This Memo

活動する上での注意点

- 知財周り
  - 提案するのであれば、検討が必要になる
- Anti-Trust周り
  - 反するような提案はしない
- 相手の立場を難しいものにしない気遣い
  - 相手のモチベーションや価値観等をある程度想定しておいた方がいい

標準化に関わってよかったこと

- 周辺知識を凄い勢いで蓄積できる
  - 多様な視点からレビューもしてもらえる
- 仲間が増えた
  - 有名な技術者も相談に乗ってくれる
- 昔話が面白い