

IETF102参加報告

セコム株式会社
伊藤 忠彦

今回の活動(の一部)は、一般社団法人情報通信技術委員会(TTC)による以下の助成を受けて行いました。
平成30年度「IoT/BD/AI時代に向けたデジュール及びフォーラム標準に関する標準化動向調査」調査者の募集
<http://www.ttc.or.jp/j/info/topics/20180410/>

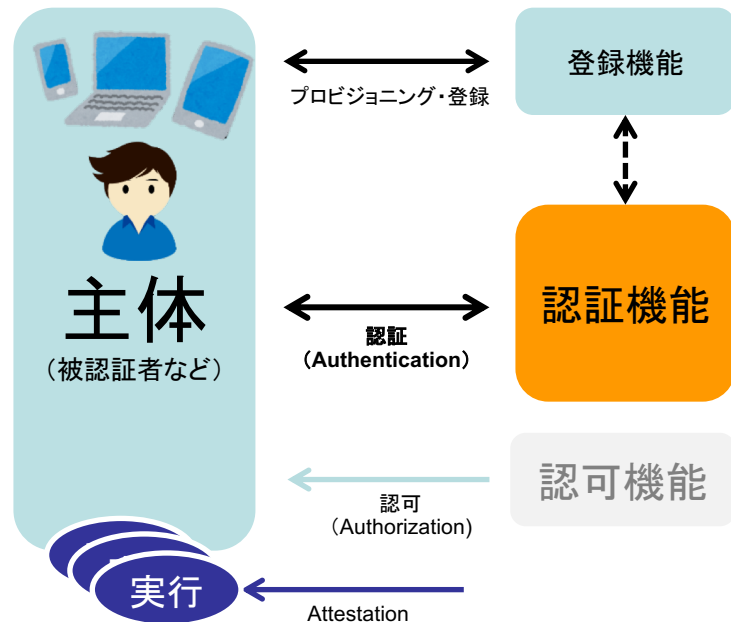
2018/08/31

- RADIUS (RFC2865)
 - EAP (RFC3784)
 - IPsec/IKE (RFC7296)
 - SSH (RFC4253)
 - TLS (RFC 8446)
 - Kerberos/SASL (RFC4422)
- etc...

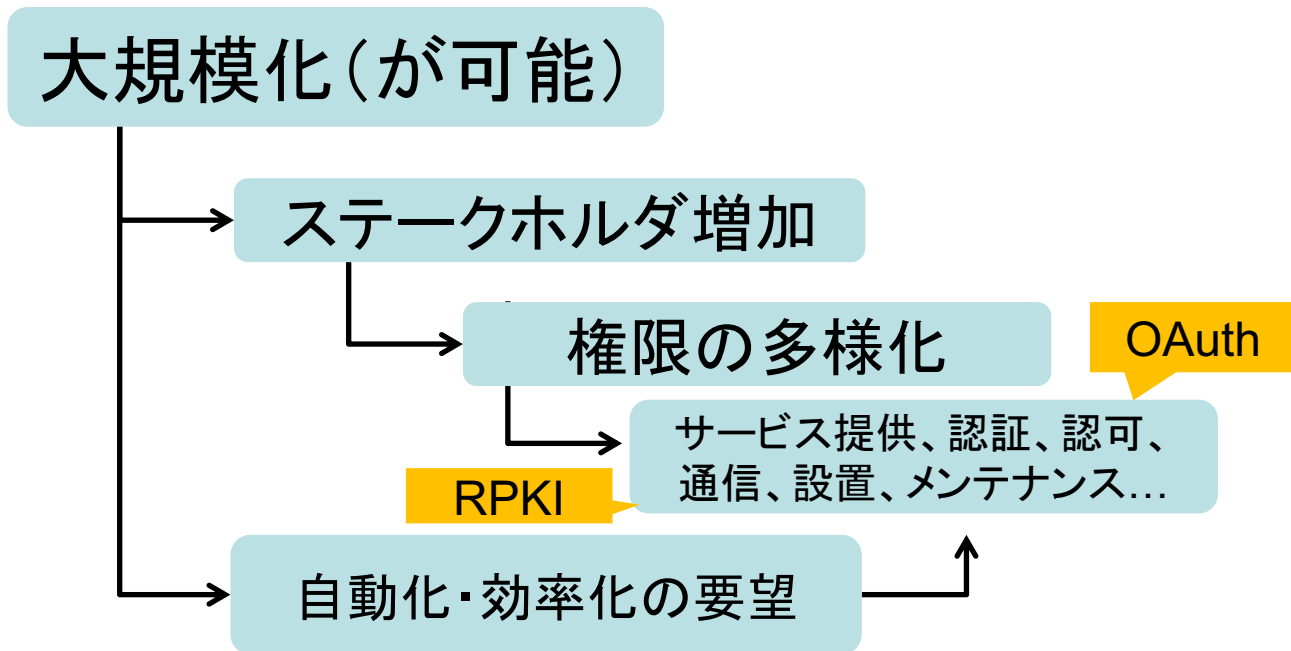
- 認証技術について
 - 認証とは
- 最近のトレンド@IETF

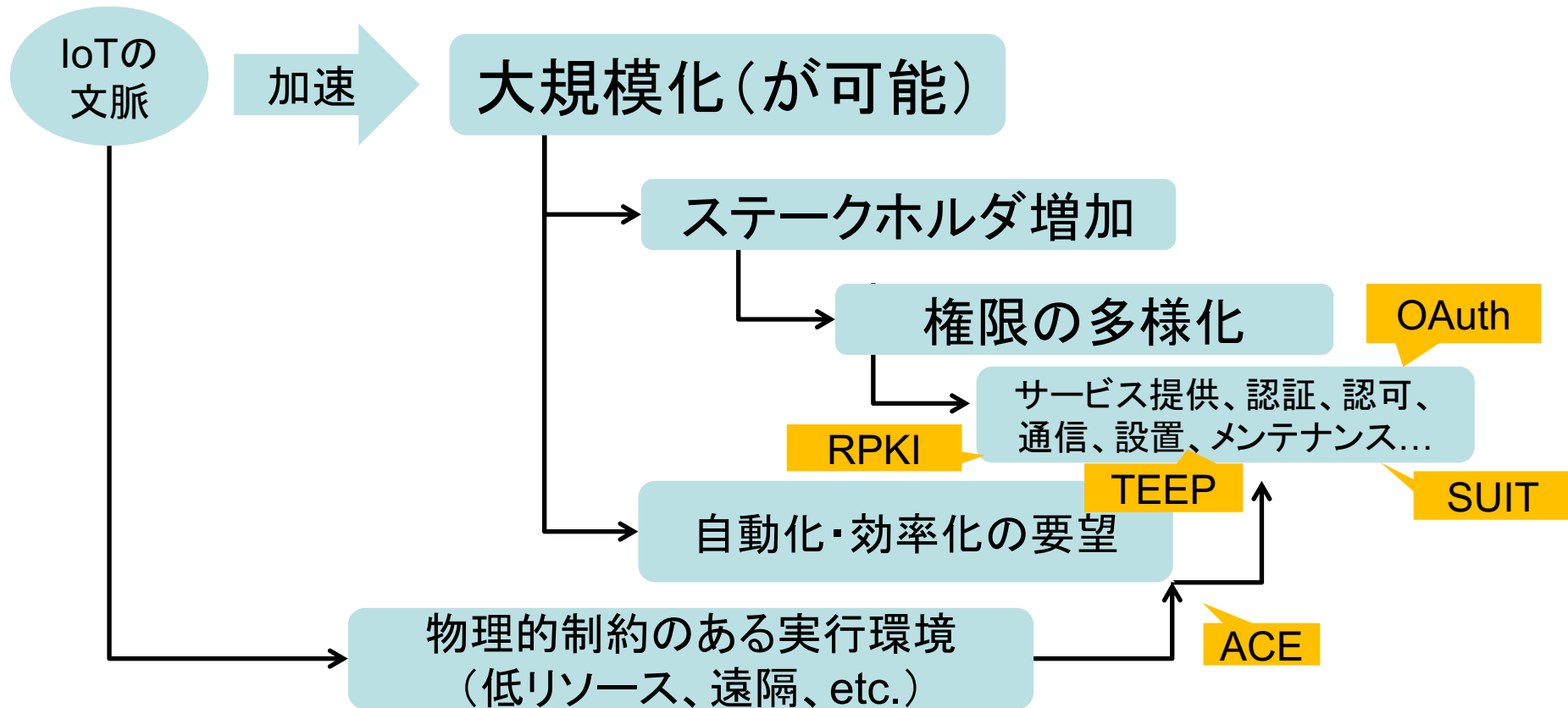
認証(Authentication)とは

- Authentication
 - 【一例】人の認証
 - 相手(被認証者)が本人であるかを確認する行為
 - 認証の目的:
 - 登録された**主体**と、同一の主体である事を**同定**すること。
 - 認証を行う為の前提:
 - プロビジョニングが既に行われている
 - 事前に認証手順について合意している(パスワードの確認、証明書の検証など)
- 認証関連用語（日本語で「認証」と呼ばれがちな用語）
 - Authorization : 認可、OAuth等(前田さんから詳しく説明があります)
 - Accountability : action(実行)から主体へ紐付ができる(ISO27002)
 - Attestation : 主体に属する何か(実行とか、インスタンスとか)の確認？
その場での判断に利用する？
※セキュアブートシーケンスの実行、インフラ等でのヘルスチェック等
※明確に定義されないまま使われる傾向アリ
 - Certification : Attestationを行った結果を踏まえ、
主体に所定の基準以上の機能や属性等がある事を示す
(ANSI、Assessment System)
Attestation結果を、後で不特定多数の人が使える？
 - Etc.



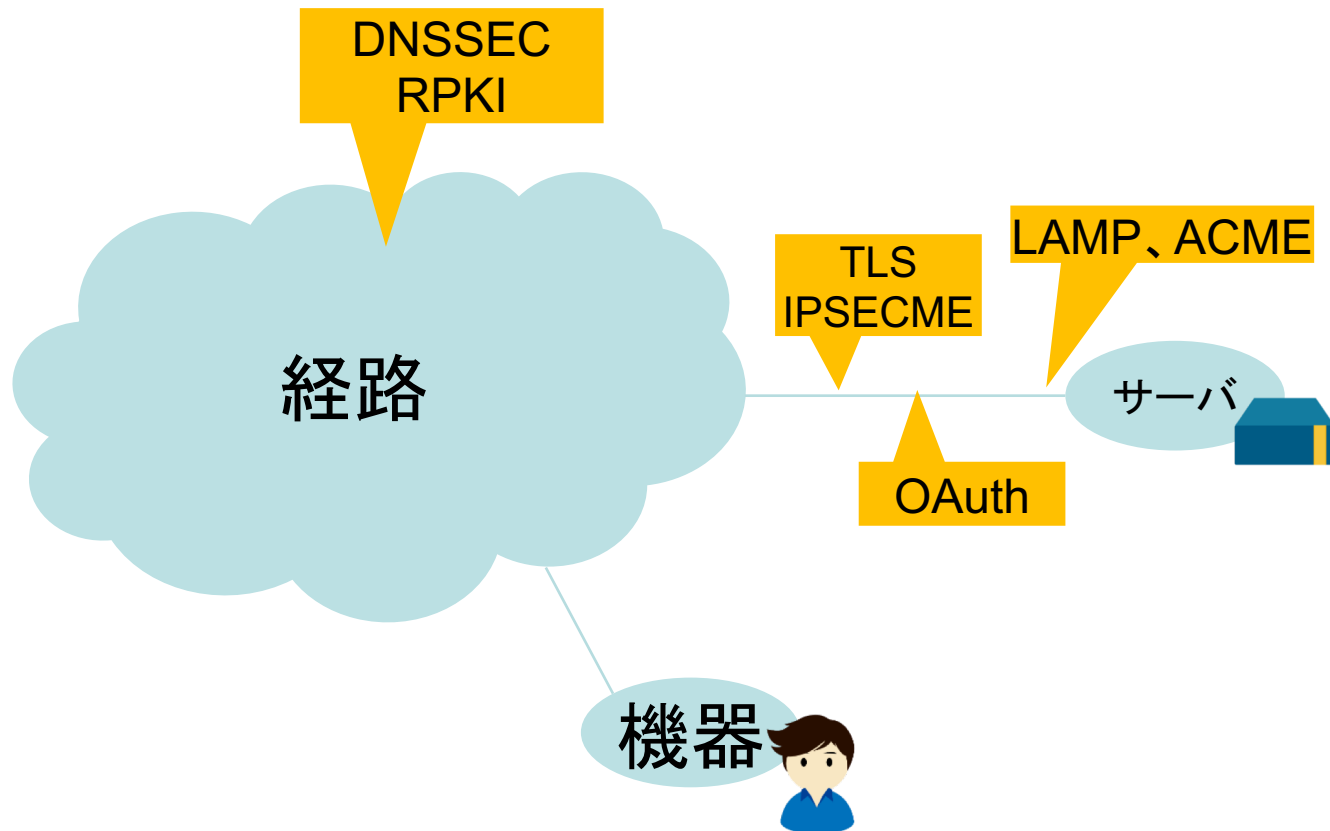
- 人と人
 - 割符とか
- 人と機械
 - パスワードとか
- 機械と機械
 - 様々な要望



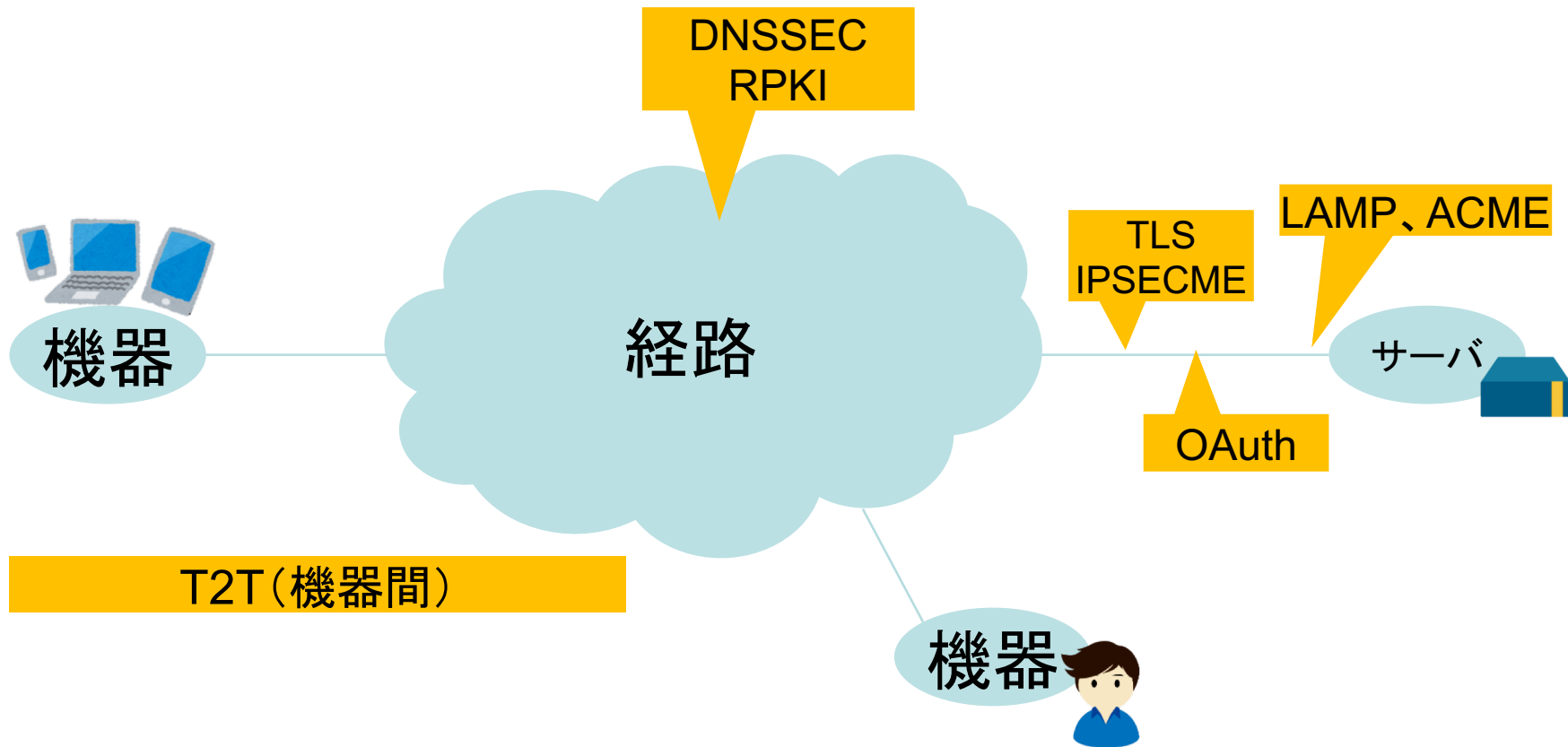


IETFにおける様々な認証関連WG

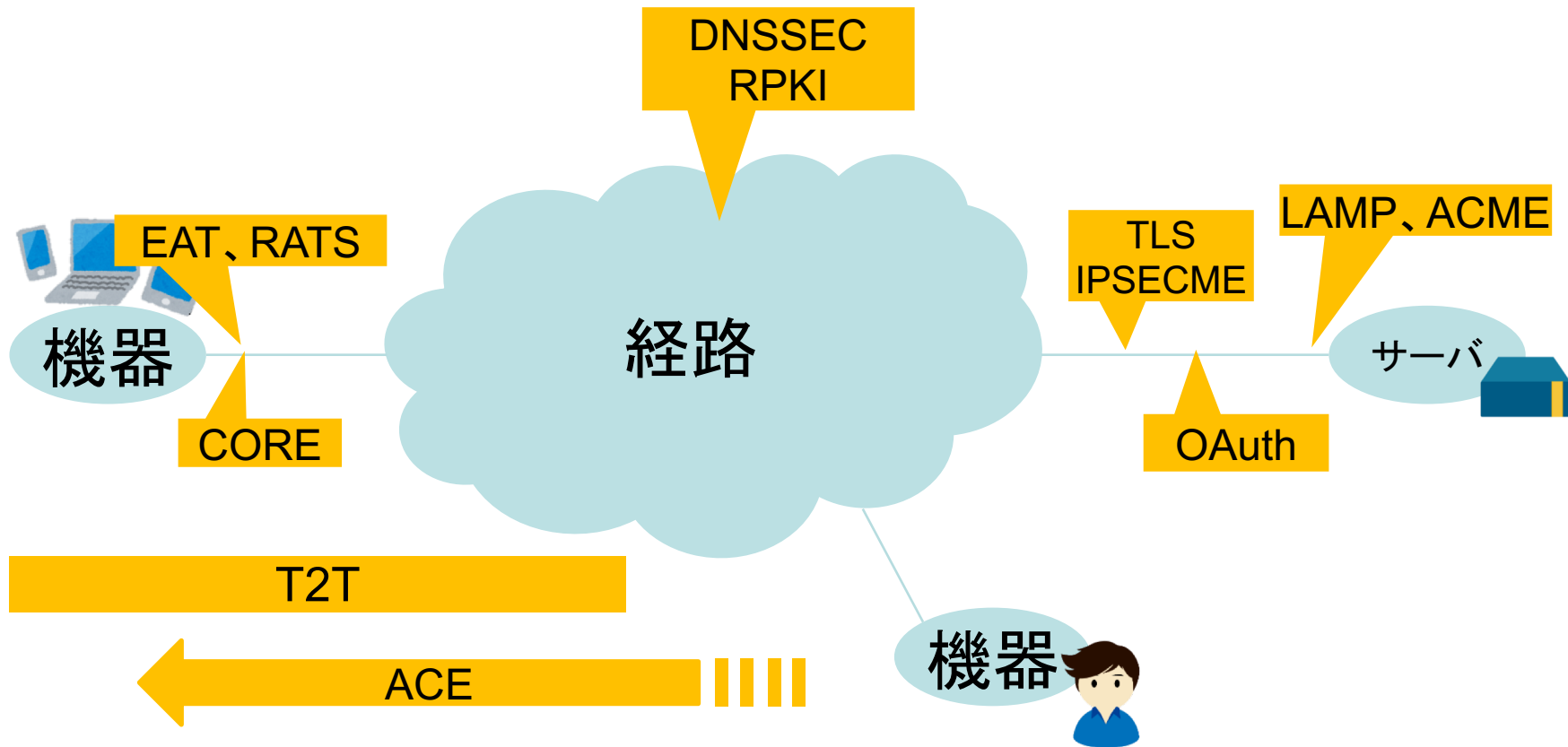
様々な環境での「認証」(一部)



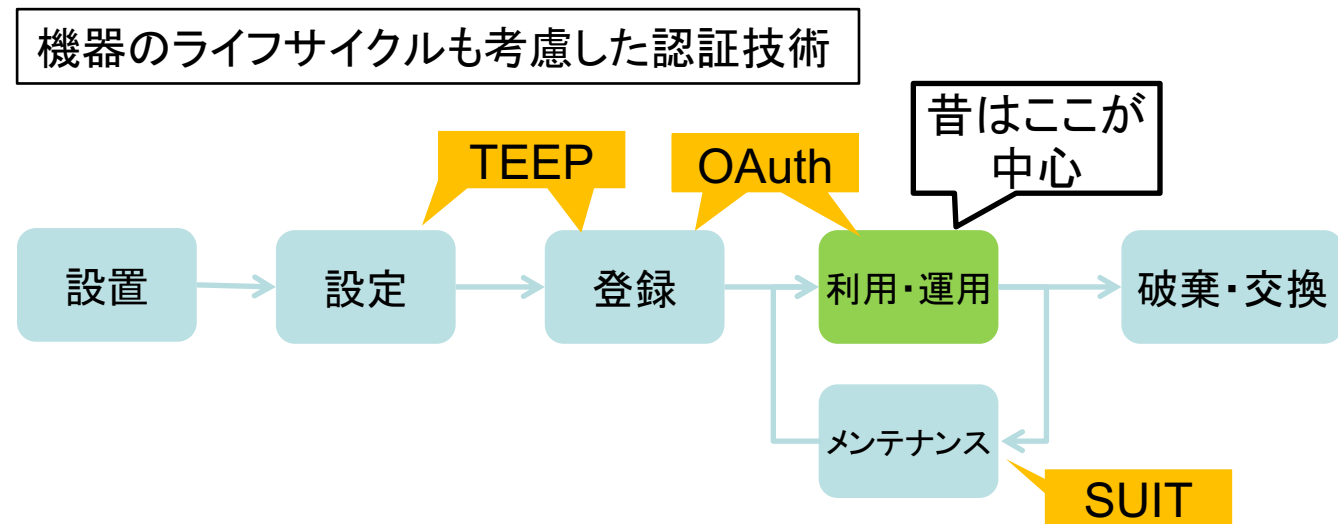
様々な環境での「認証」(一部)



様々な環境での「認証」(一部)



各ライフサイクルのフェーズに応じた認証の効率化



- SUIT WG活動中です
 - M4(メイン)とM0+(無線?)
 - SEとかも搭載
- セコムSUIT部発足

