PKI Day 2019
午前の部　IoTのトラスト

IoTにおけるトラスト実現に向けた技術的な仕組み

2019/4/17

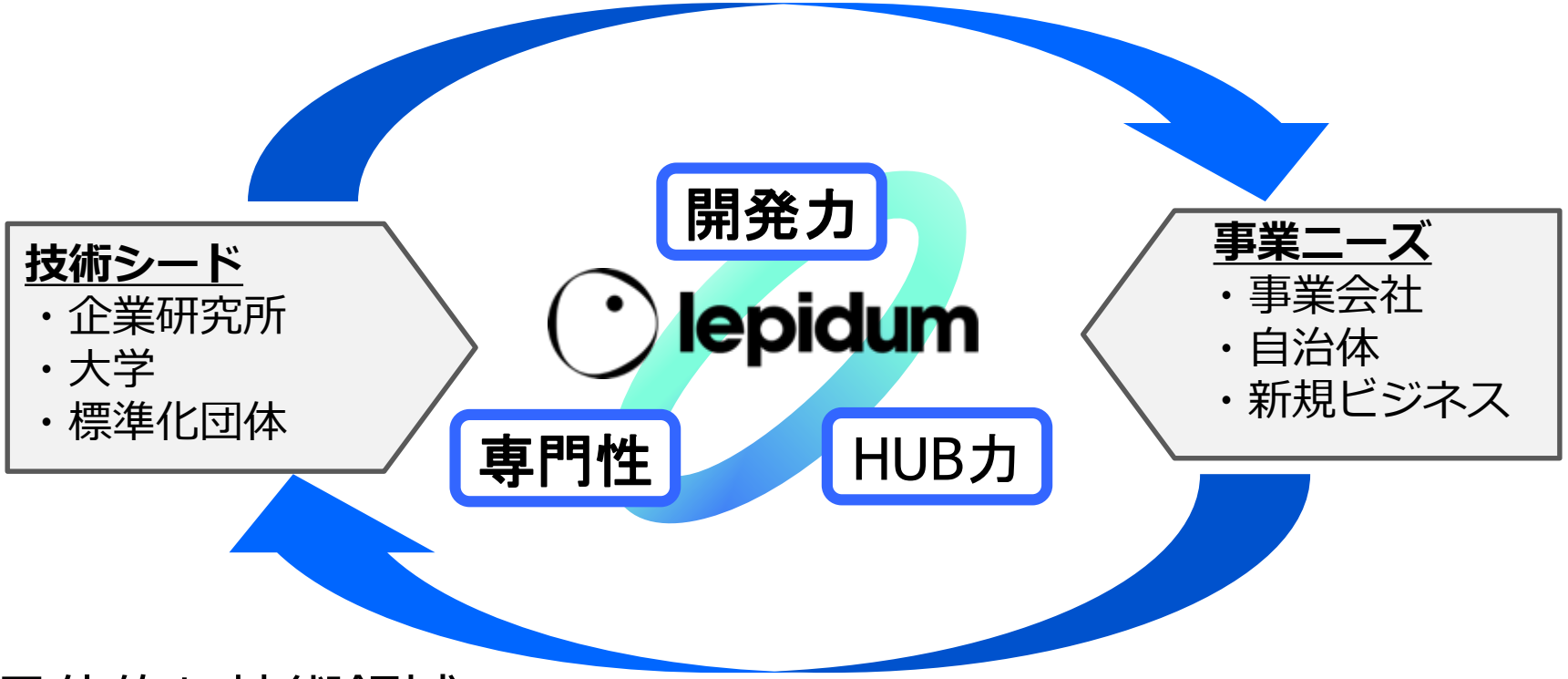
株式会社レピダム
菅野 哲

この人、誰？

- 名前
  - 菅野 哲（かんの さとる）
- 所属
  - 株式会社 レピダム 代表取締役
  - ココン株式会社 技術研究室 室長
  - AI TOKYO LAB株式会社 取締役
- どんなことやっていた／やっているの？
  - 学生時代～
    - 暗号プロトコルの研究、ベンチャーで暗号製品を売り歩く（？）
  - 社会人時代～
    - 暗号ライブラリや情報セキュリティ関連システム開発
    - IETFなどでCamellia関連の標準化活動
  - ここ最近
    - もっぱら会社経営と営業的な活動が色濃い
    - TCG Invited Expertとして活動（2018年10月～）

株式会社レピダムとは

エッジの効いた技術でお客様の事業を加速させる燃料

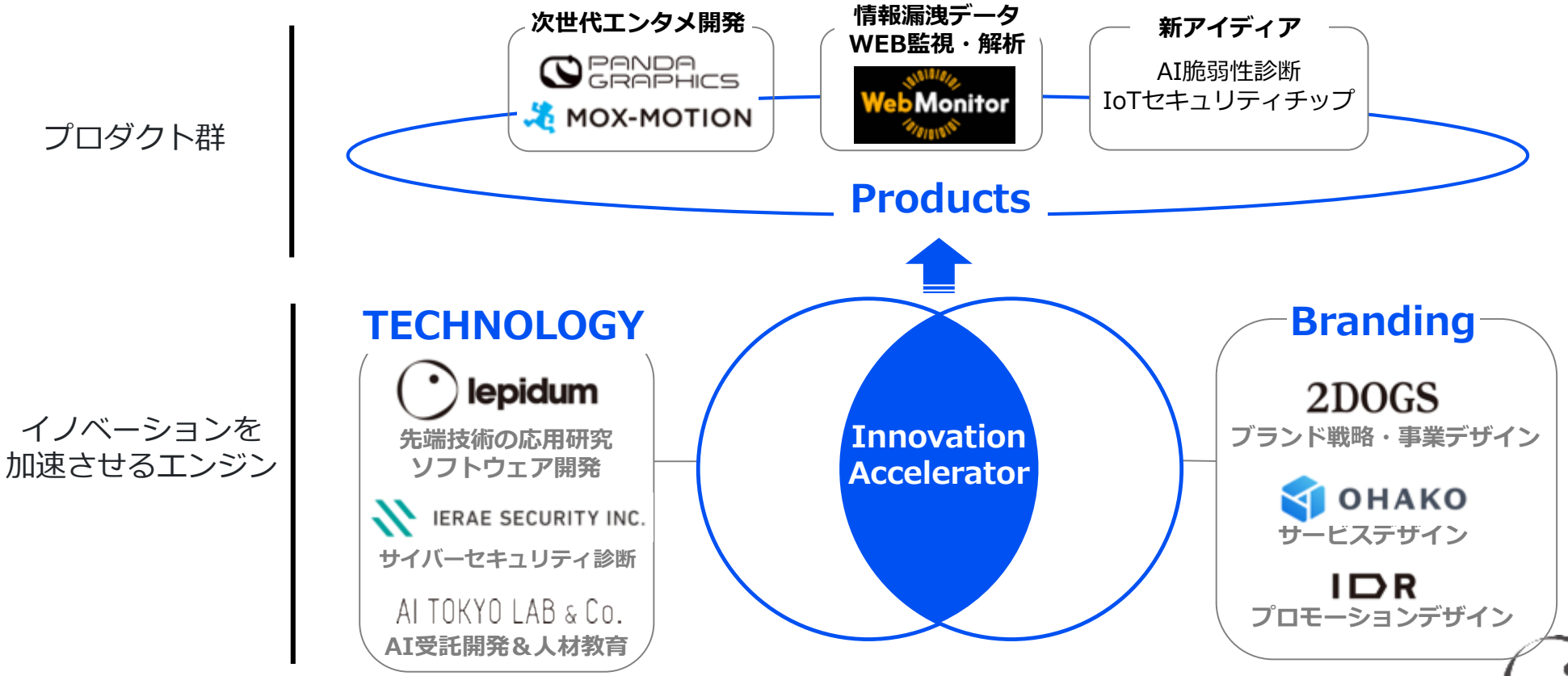


具体的な技術領域：
「標準化支援、アイデンティティ、プライバシ、認証・認可、情報セキュリティ」に関する開発、調査・コンサル

ココングループとは？

- 人々が進むべき時代の先を示す**羅針盤**であり、**古今東西**愛されるサービスによって**22世紀への前進に貢献**する

ココングループの事業領域



本講演でのお題を振り返る

<<午前の部 IoTのトラスト プログラム>> ※タイトルは今後変更する可能性があります。ご了承ください。

【ご挨拶】10：00 - 10：20

「PKI day 2019の午前の部 オーバビュー」　セコム株式会社 IS研究所／PKI相互運用技術WGリーダー　松本　泰 氏

【講演】10：20 - 10：50

「IoTにおけるトラスト実現に向けた技術的な仕組み」　株式会社レピダム　代表取締役　菅野 哲 氏

＜概要＞
Society5.0に代表されるスマート化される社会を実現には、膨大な数のIoTデバイスにより収集されたビックデータに対する利活用が非常に重要になります。 この状況を実現するために必要な要素として、膨大な数のIoTデバイスのセキュアな管理かつ簡便な運用が求められます。 これらの要件を実現するために、様々な仕組みが必要 ではありますが、重要な仕組みとしてトラストがあります。
本講演では、IoTにおけるトラストを検討する上で重要となる、トラストと関係が深いIoTセキュリティに対してガイドライン等で懸念されている現状の課題やIETFをはじめとする標準化団体における技術動向を踏まえて議論するための情報を提供しま す。

概要に小難しいことを書きましたが・・・
「IoTを取り巻く技術」の動向を知ることが目的！
より具体的なIoTに関する後の2つの講演で！

術を展開することを指向したいと思います。活発なご討論をいただき、ご助言をいただければ幸いです。

https://www.jnsa.org/seminar/pki-day/2019/

本日のお題を紐解く・・・

お題である「IoTにおけるトラスト実現に向けた技術的な仕組み」からキーワードを振り返ってみる

- **IoT**
  - 「IoT」という同じ言葉を使って話していても異なる意味合いな時も多々あることってありませんか？
- **トラスト**
  - トラストって何なのかってのも難しいですよね？
  - セキュリティとトラストの関係は？
- **技術的な仕組み**
  - トラストを実現する上で評価可能な技術要素であるセキュリティとの関係性
    - 現実的な話題として、既存ガイドラインでセキュリティ技術をどう利用しているのか？
    - 将来的な話題として、未来を見据えた標準化団体で起きていることは？

準備：IoTとは？

一般的なIoTとは

- みんな大好きなWikipediaでIoTとIoTデバイスを参照すると・・・

モノのインターネット

出典: フリー百科事典『ウィキペディア（Wikipedia）』

「IoT」は情報通信用語について説明しているこの項目へ転送されています。その他の用法については「IOT」をご覧ください。

モノのインターネット（物のインターネット[1][2]、英語: Internet of Things：**IoT**）とは、様々な「モノ（物）」がインターネットに接続され（単に繋がるだけではなく、モノがインターネットのように繋がる[3]）、情報交換することにより相互に制御する仕組みである[4][5]。それによるデジタル社会（クロステック）の実現を指す[6][7][8]。現在の市場価値は800億ドルと予測されている[9]。経済産業省が推進するコネクテッドインダストリーズやソサエティー5.0との関連でも注目を集めている[10]。近年ではIoTに次ぐ技術として、**ヒトのインターネット**（Internet of Human：**IoH** ＝ ヒトがインターネットと繋がる）[11]、能力のインターネット化であるIoA[12]が言われている。

IoTデバイス [編集]

ここでいう「モノ（物）」をIoTデバイスという[49]。センサやアクチュエータなどが、動的拡張・有機的接続・自律協調・多様性を持つ[50]。業界の方向としてニューラルネットワークのハードウェアアクセラレーションへと進んでいる[51]。

スマートデバイスのようにIPアドレスを持つものや、IPアドレスを持つセンサーから検知可能なRFIDタグを付けた商品（コンピュータを組込まない二次元コードも含まれる）[52]、IPアドレスを持った機器に格納されたコンテンツのことである[53]。マシンツーマシンのスマートメーターは良い例である[54]。

「第1段階：見える化」「第2段階：制御」「第3段階：最適化・効率改善の自動化」となる[55]。複数のフェーズがあり、IoT-Iではモノ・人工物、IoT-IIでは人・生物、IoT-IIIではデータ・プロセス、IoT-IVではあらゆるモノが接続される[56]。

https://ja.wikipedia.org/wiki/モノのインターネット

一般的なIoTとは

- ざっくりとIoTをまとめると「モノがインターネットに接続されて情報交換を行い相互に制御すること」って感じ
- 冷静になるとモヤモヤポイントがある。例えば・・・
  - モノ（=IoTデバイス）ってどんな性能で機能要件を満たしているの？
  - IoTはインターネットプロトコルを話せないとダメなの？
  - 情報交換されて得た情報を暗黙的に信頼するの？

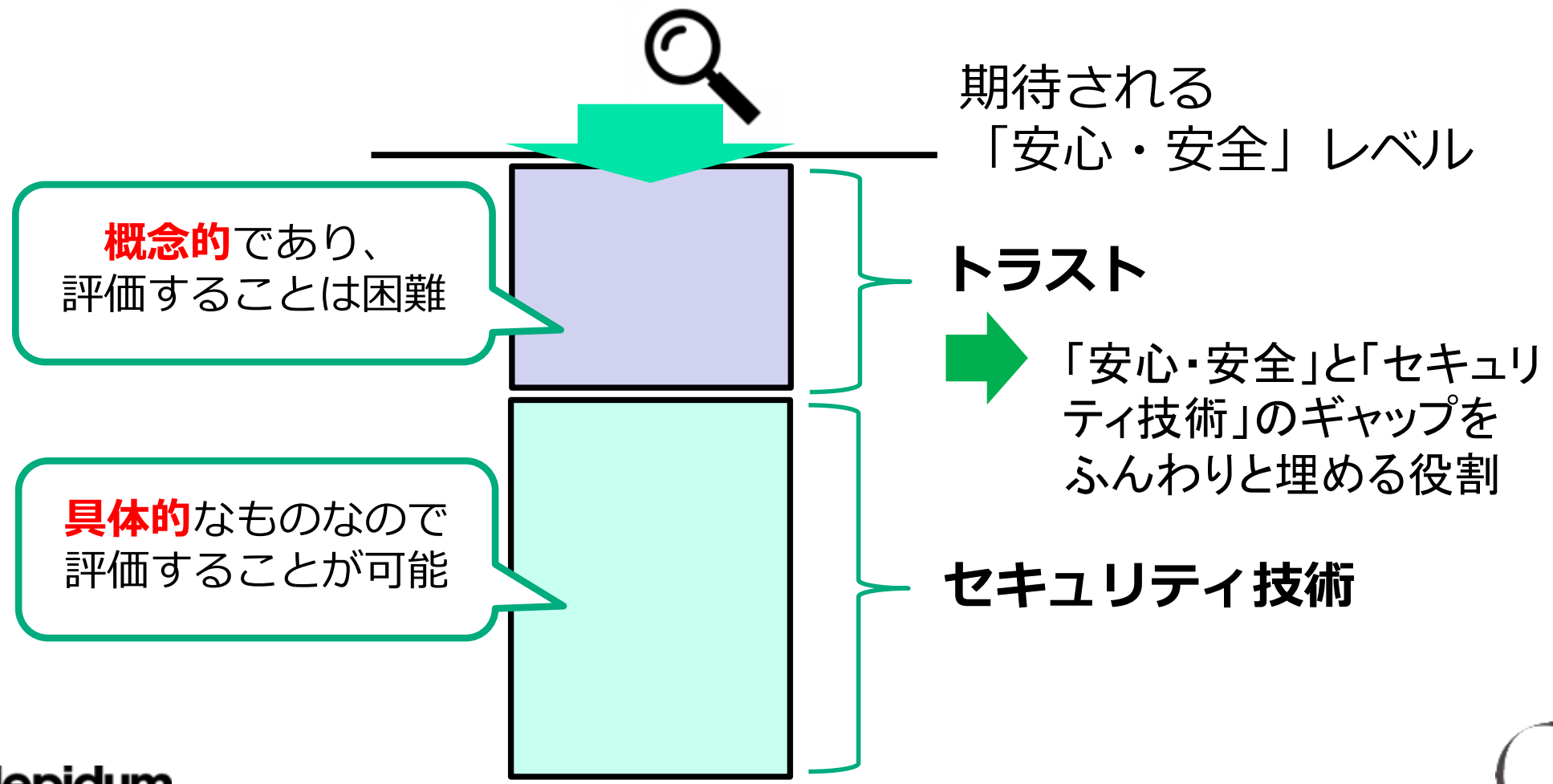
IoTと言っても様々な状態がありそう・・・。
例えば、同じIoTについて議論をしていても噛み合わないことが起きるのではないか？！

➡ IoTを定義する参照ドキュメントが必須

準備：トラストとは？

トラスト

- 安心・安全を実現するためのトラストは、評価可能な「セキュリティ技術」によって実現される



トラストってモヤっとするけど・・・

- トラストを実現するセキュリティ技術の側面から構成技術を考えるとトラストが見えてくる？
  - 暗号技術
    - 暗号アルゴリズム
    - 鍵長 など
  - ハードウェアセキュリティ
    - 耐タンパ性 など
  - 安心・安全を維持するための仕組み
    - 鍵管理
    - アテステーション
    - セキュアファームアップデート など
- 大事な視点：誰にとってのトラストなのか？
  - 「○○におけるトラスト」と言った場合は**誰視点**なのか？
    - 製造者？　利用者？　サービス提供者？
    - それぞれの役割で求められる/期待されるトラストは異なるのではないか？

では、IoTにフォーカスして考える

- IoTにおいてトラストを実現するセキュリティ技術である**「Root of Trust（RoT）」**があるかどうかで実現できる世界に違いがある
  - 最近では、IETFのようなインターネットプロトコルを議論する団体でもIoTは重要課題！

IETF 103 RATS BoFより

Root of Trust (RoT)

- NIST SP 800-164
  - "Security **primitives** composed of hardware, firmware and/or software that provide a set of trusted, security-critical functions. They must always **behave in an expected manner** because their **misbehavior cannot be detected**. As such, RoTs need to be secured by their design"
- "Trusting" a Root of Trust is a **decision** made by the relying party.

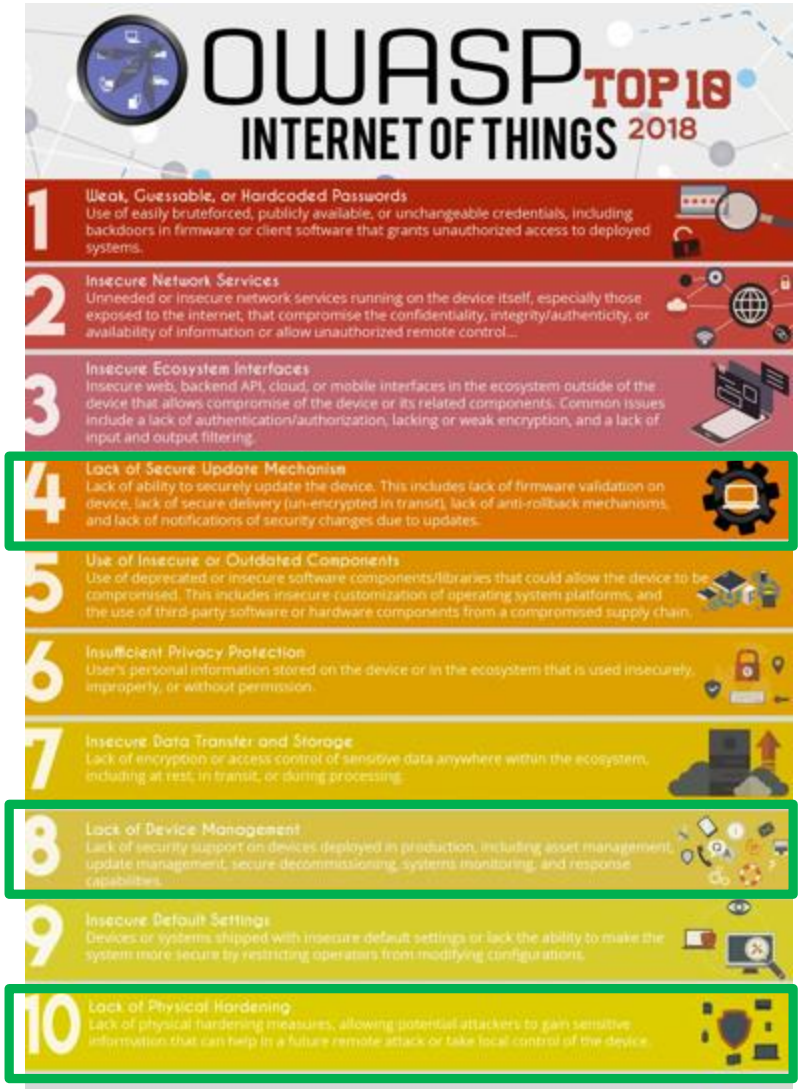
https://datatracker.ietf.org/meeting/103/materials/slides-103-rats-rats-problem-statement-02

- ガイドラインや標準化団体における「RoTに基づく技術動向」の現状が気になるところ

技術的な仕組み：ガイドライン

※ Attack Surface： ざっくり説明すると「攻撃可能な箇所」という感じです。

OWASP Internet of Things TOP10



https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

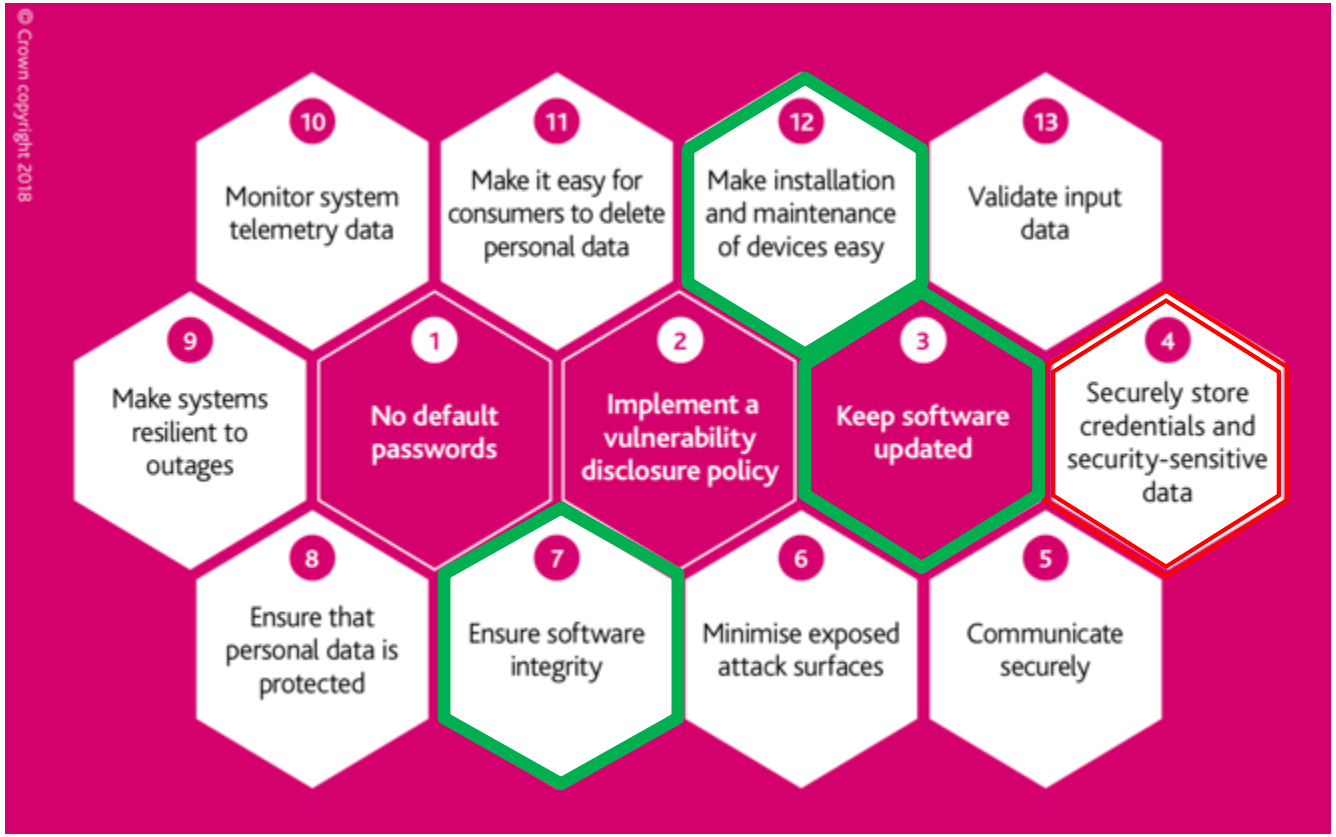
IoTデバイスで留意すべき10の脆弱性が共有。例えば・・・

- 安全な更新メカニズムの欠如
- デバイス管理の欠如
- 物理的な堅牢化の欠如

「トラスト」を実現に向けた本質的な課題が多い・・・。
決定打となるセキュリティ技術は存在している？！

Code of Practice for Consumer IoT Security

英国デジタル・文化・メディア・スポーツ省によるデバイスメーカー、IoTサービス提供事業者、モバイルアプリ開発事業者、小売業者に対するIoTセキュリティに関するドキュメント



・重要なデータを安全な保存

・ソフトウェアの完全性確保

・容易なデバイスの設置＆メンテナンス

運用的な観点での考慮すべき事項も

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

ガイドラインからわかること

- IoTデバイス脆弱性Top10の変化からIoTへの理解度を考える
  - 例示：OWASP IoT Top10を2014年版と2018年版で比較

Internet of Things (IoT) Top 10 2014

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

Internet of Things (IoT) Top 10 2018

The OWASP IoT Top 10 - 2018 is now available.

- I1 Weak Guessable, or Hardcoded Passwords
- I2 Insecure Network Services
- I3 Insecure Ecosystem Interfaces
- I4 Lack of Secure Update Mechanism
- I5 Use of Insecure or Outdated Components
- I6 Insufficient Privacy Protection
- I7 Insecure Data Transfer and Storage
- I8 Lack of Device Management
- I9 Insecure Default Settings
- I10 Lack of Physical Hardening

脆弱性に関する項目が**具体的＆本質的**に！
明確な事象になったことにより明確な対策へ

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

技術的な仕組み：標準化編

標準種別標準化団体

- デジュール標準

- フォーラム標準

- デファクト

IETFにおけるIoTでのトラスト

- IETFはインターネットプロトコルに関する標準化団体のため、IoTに関する技術的仕組みや仕様を検討している。

- INT Area
  - lwig (Light-Weight Implementation Guidance) WG

制約のある機器（例：IoT）に関する利用を主眼に検討

- SEC Area
  - SUIT (Software Updates for Internet of Things) WG
  - TEEP (Trusted Execution Environment Provisioning) WG
  - RATS (Remote ATtestation ProcedureS) WG

IoTでのトラストを実現するための仕組みを検討

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

lwig WG

- 制約のあるデバイスで実際に利用され他のデバイスとの相互運用性に影響を及ぼさない技術を題材にしています。検討範囲としてメモリ使用量、電力使用量の削減などです。

- 代表的なドキュメント
  - RFC7228 Terminology for Constrained-Node Networks
    - みんなの心の中にある**「IoTデバイスに関する要件」**を規定
    - CPU、メモリ、電力使用量など制約された機器に対して、処理能力毎にクラスが定義
    - 具体例：
      - Class 0 Device :
        - ROM « 100KiB / RAM « 10KiB とサイズ 小
        - デバイス単体では**インターネット接続不可**
        - SSL/TLSなどのセキュア通信は困難
      - Class 1 Device :
        - ROM ~100KiB / RAM ~ 10KiB とサイズ 小
        - インターネットに直接接続可能でSSL/TLSなどの通信はギリギリ可能
      - Class 2 Device :
        - ROM ~ 250KiB / RAM ~ 50KiB とサイズ 小
        - PCで利用可能なプロトコルスタックが全て利用可能

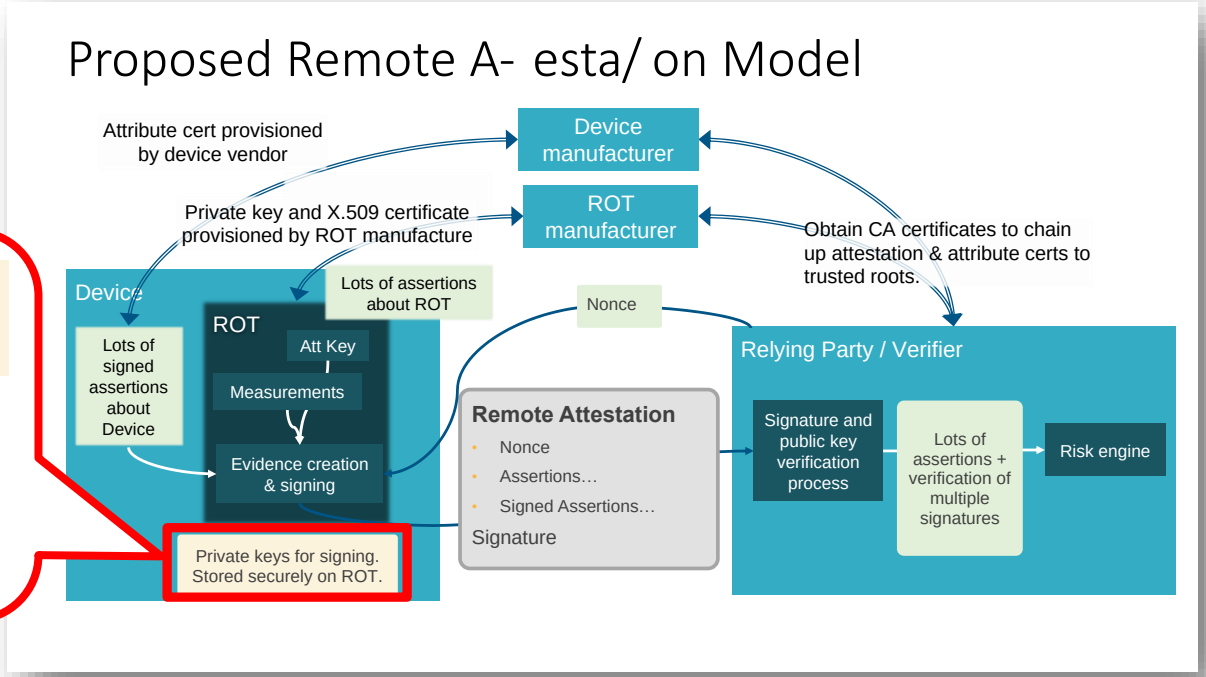
SUIT WG & TEEP WG

- ほぼ同時期に設置され、ターゲット的に似てるけど異なる「安全なアップデート」を行うための仕組み

- SUIT WG
  - IoT機器の安全な**ファームウェア更新**の仕組みを検討
  - 取り扱うデバイス性能
    - Class1 (~10KiB RAM、~100KiB ROM) が対象
    - ファームウェア以外(例:PCのソフトウェア)の更新は対象外
- TEEP WG
  - TEE(Trusted Execution Environment)上で動く信頼できる**アプリケーション**(TA: Trusted App)**のライフサイクル管理**(インストール、アップデートなど)プロトコルを検討

RATS WG

- IETF 104（2019年3月）からWG化
- IoTデバイス等が自身の正当性(システムとして認定されたものであること)を証明する仕組みを検討
- 例：Remote Attestation
  - ベンダーを信頼する第三者が、あるデバイスをベンダーによって製造されたものであることの検証する仕組み



Private keys for signing.
Stored securely on ROT.

RoTに秘密鍵が格納される前提

https://datatracker.ietf.org/meeting/103/materials/slides-103-rats-rats-problem-statement-02

IETFで注目を集めているAttestation！

- ここ最近のIETFにおいてAttestationに関する議論が多く取り扱われている。IETF以外での団体においても多くの技術が存在

IETF 102 secdispatch「Entity Attestation Token (EAT)」資料より

Technology	Use Case
FIDO Attestation	Attestation of FIDO Authenticator implementations
Android Key Store	Attestation key pairs in the key store
NEA	Collect and send endpoint security posture (e.g. anti-virus SW state and config) to enterprise collection / monitoring point
RATS / NSF	Attestation / Measurement of SW on Network Security Functions (e.g., firewalls)
TPM	Attestation / Measurement of SW running on a device
BRSKI / Zero Touch	Authenticates IoT devices for enrollment in IoT management system

https://datatracker.ietf.org/meeting/102/materials/slides-102-secdispatch-entity-attestation-token-draft-mandyam-eat-00-00

まとめにかえて

- 本講演において、「IoT」と「トラスト」ってどう言う状況なのかを振り返り、ガイドラインや標準化におけるトラストの実現に向けたセキュリティ技術について紹介

IoT時代の「トラスト」を実現するための準備として、ガイドラインや標準化される技術は整いつつあります。その一方で・・・

- 標準化によりトラストを実現する仕組みが提供されると安全に？！
  - トラストを実現する技術が標準化されることでのリスク顕在化
    - 攻撃対象が絞られる？！
- トラストを実現する仕組みが正しく機能しても、悪意あるデバイスだった場合は…
  - 製造メーカー自体のトラスト → なし崩し的にトラストしてしまっている？
- 機能制約があるIoT自体を頼るには、限界があることを意識しておく必要があるのでは？
  - デバイス数が増加した時に点での管理が困難に？！

何か気になることなどあれば・・・

- E-mail
  - kanno@lepidum.co.jp
- SNS
  - Twitter(satorukanno)
  - Facebook(satoru.kanno)

お気軽にご連絡ください！