JNSA標準化部会セミナー
「IoTセキュリティ標準化の動向を知る」

コンシューマIoTセキュリティ標準化のインパクト

--なぜ「IoTセキュリティ標準化の動向を知る」が重要なのか--

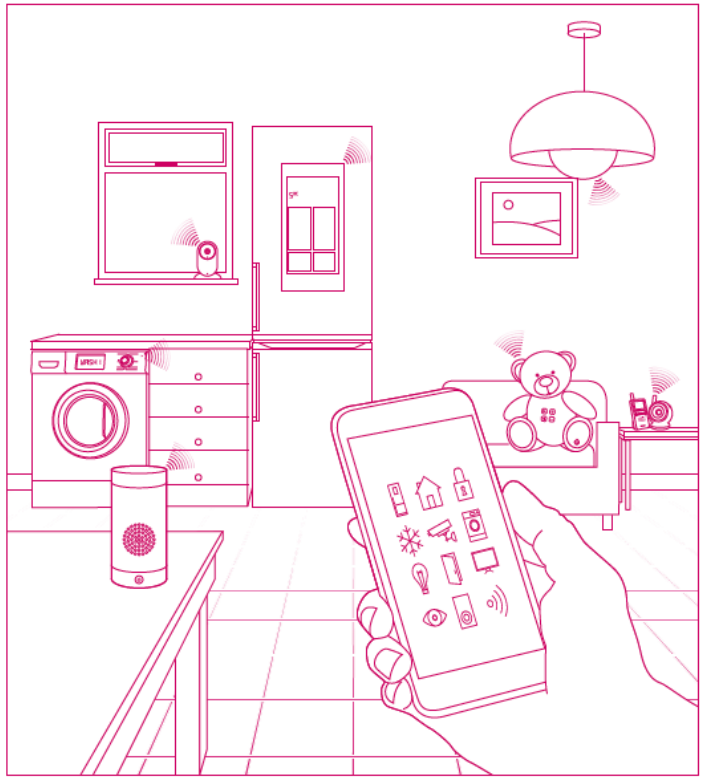
2024年11月15日

NPO JNSA フェロー　松本　泰

英国　2018年

Department for Digital, Culture, Media & Sport

Code of Practice for Consumer IoT Security



October 2018

出典
https://assets.publishing.service.gov.uk/media/60576f54e90e0724c0df4631/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

欧州　2019年

ETSI TS 103 645 V1.1.1 (2019-02)

CYBER;
Cyber Security for Consumer Internet of Things

出典
https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

欧州　2024年

ETSI EN 303 645 V3.1.3 (2024-09)

CYBER;
Cyber Security for Consumer Internet of Things:
Baseline Requirements

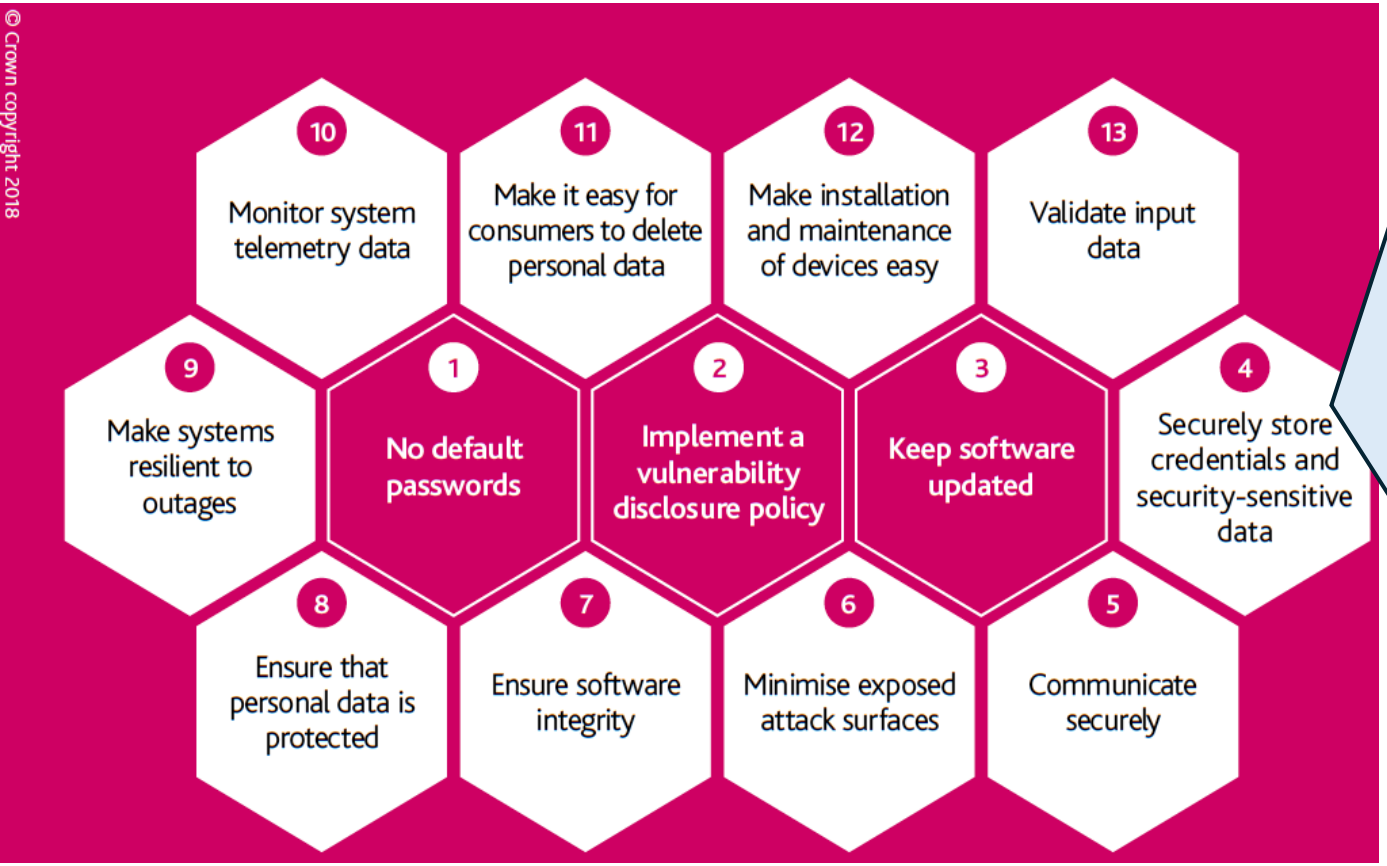
出典
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

History

Document history			
V1.1.1	February 2019	Publication as TS 103 645	
V2.1.1	June 2020	Publication	
V2.1.2	June 2020	Publication as TS 103 645	
V3.1.1	January 2024	Publication as TS 103 645	
V3.1.2	June 2024	EN Approval Procedure	AP 20240909: 2024-06-11 to 2024-09-09
V3.1.3	September 2024	Publication	

- 欧州　2024年10月　EU Cyber Resilience Act
- 英国　2022年 Product Security and Telecommunication Infrastructure Act

英国2018年　Code of Practice for Consumer IoT Security．13項目の要求



「(4) クレデンシャル情報やセキュリティ上重要なデータの安全な保管」の要求は、
・既存のIoTデバイスメーカにとっては、敷居の高い要求
・しかし、入手が容易なコンシューマIoTにとって、リバースエンジニアリングは、現実的な脅威

4) クレデンシャル情報やセキュリティ上重要なデータの安全な保管

デバイスやアプリケーションのリバース・エンジニアリングは、ソフトウェアにハードコードされたユーザー名やパスワードなどのクレデンシャル情報を簡単に発見することができる。このハードコードされた情報を不明瞭にしたり暗号化したりするために使用される単純な難読化手法も、簡単に破られる可能性があります。安全に保存されるべきセキュリティにセンシティブデータには、例えば暗号鍵、デバイス識別子、初期化ベクターなどがある。信頼された実行環境（Trusted Execution Environment ：TEE）および関連する信頼された安全なストレージによって提供されるような、安全で信頼されたストレージ・メカニズムを使用すべきである。

5.4　機密セキュリティパラメータをセキュアに保存する

ETSI EN 303 645の記述

JNSA

規定 5.4-1 永続ストレージにある機密セキュリティパラメータは、機器によってセキュアに保存されなければならない。

機密セキュリティパラメータをセキュアにするために、セキュアなストレージ・メカニズムを使用することができる。適切なメカニズムには、ETSI TR 121 905 [i.29], ETSI TS 102 221 [i.25]による信頼できる実行環境（TEE）、ハードウェアに関連付けられた暗号化されたストレージ、セキュアエレメント (SE) 又は専用のセキュリティ・コンポーネント (DSC)、及び GSMA SGP.22 Technical Specification v2.2.1 [i.26]による UICC で実行されるソフトウェアの処理機能が含まれる。

注：この規定は永続ストレージに適用されるが、製造業者はメモリ内の機密セキュリティパラメータに同様のアプローチを実装することも可能である。

例 1：認可された無線周波数（例：LTE-m 携帯アクセス）への認可及びアクセスに関連するルートキーは、UICC に保存される。

例 2：信頼できる実行環境（TEE）を使用して機密セキュリティパラメータを保存し、アクセスするリモート制御ドアロック。

例 3：ワイヤレスサーモスタットは、無線ネットワークの認証情報を、外部のフラッシュストレージではなく、改ざん防止されたマイクロコントローラに保存する。

出典
欧州規格 ETSI EN 303 645 V2.1.1 (2020-06)の翻訳
https://www.ipa.go.jp/security/controlsystem/etsien303645.html

- リバースエンジアリングに対しては触れられていない？
- ネットワーク経由の攻撃のみの対応？？

IoT製品に対するセキュリティ適合性評価制度

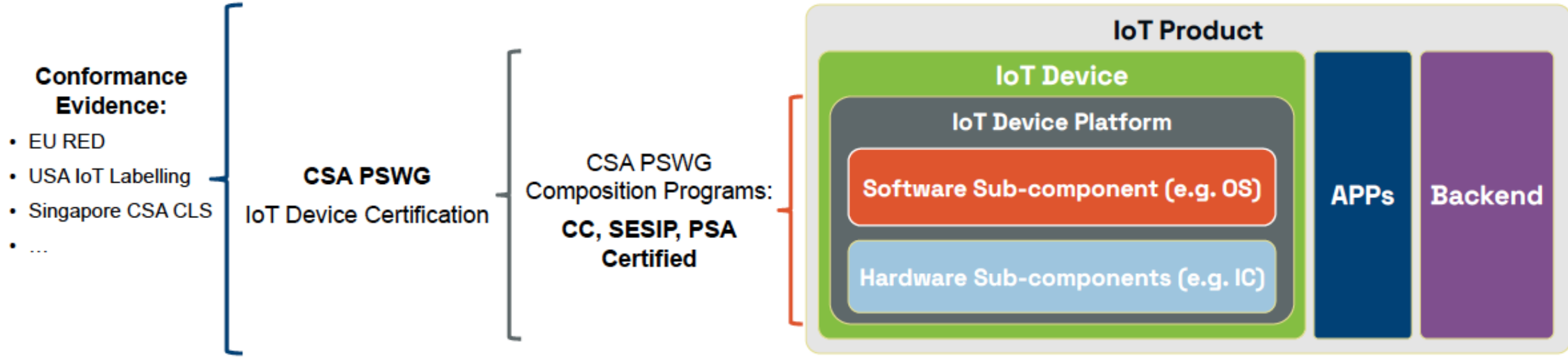
4. 機密セキュリティパラメータをセキュアに保存する	4-1. 製品のストレージにある機密セキュリティパラメータは、製品によってセキュアに保存されなければならない。	✓	11	製品のストレージに保存される守るべき情報資産（SDカード等、ストレージメディアに保存される守るべき情報資産も含む。）が、ネットワーク経由の不正アクセスに対して、セキュアに保存されること。

出典　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_2.pdf

コンシューマIoTセキュリティ標準化 → IoTデバイスのプラットフォーム化

PSWG Certification

2023年10月のETSI security Week でのプレゼン資料
CSA ： Connectivity Standards Alliance → Matter
PWSG ： Product Security Working Group



出典： CSA IoT Certification: Is EN 303 645 your one-stop shop for Global Consumer IoT Regulatory Compliance? October 18, 2023
Presented by: Nataliya Stanetsky, Google
https://docbox.etsi.org/Workshop/2023/10_ETSISECURITYCONFERENCE/D33_IOTandMobileCertification/Google_Stanetsky.pdf

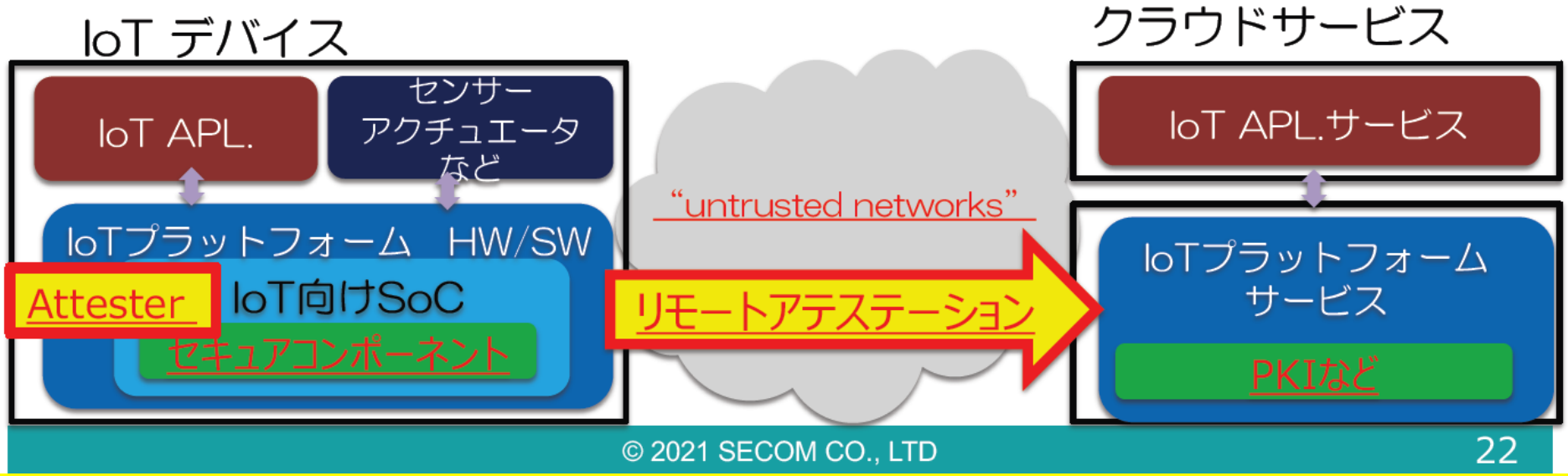
既存のIoTデバイスベンダーにとって敷居の高い要求は、
IoTデバイス・プラットフォームが提供というビジネスモデルの変化

認証（Certification）＆ラベリングの次に来る（かも）
認証されたIoTデバイスが、意図通りの状態なのか？ソフトウェアが最新なのか？
→　リモートから検証（リモートアテステーション）

リモートアテステーション

IETF Remote ATtestation ProcedureS (rats)WG
https://datatracker.ietf.org/wg/rats/about/

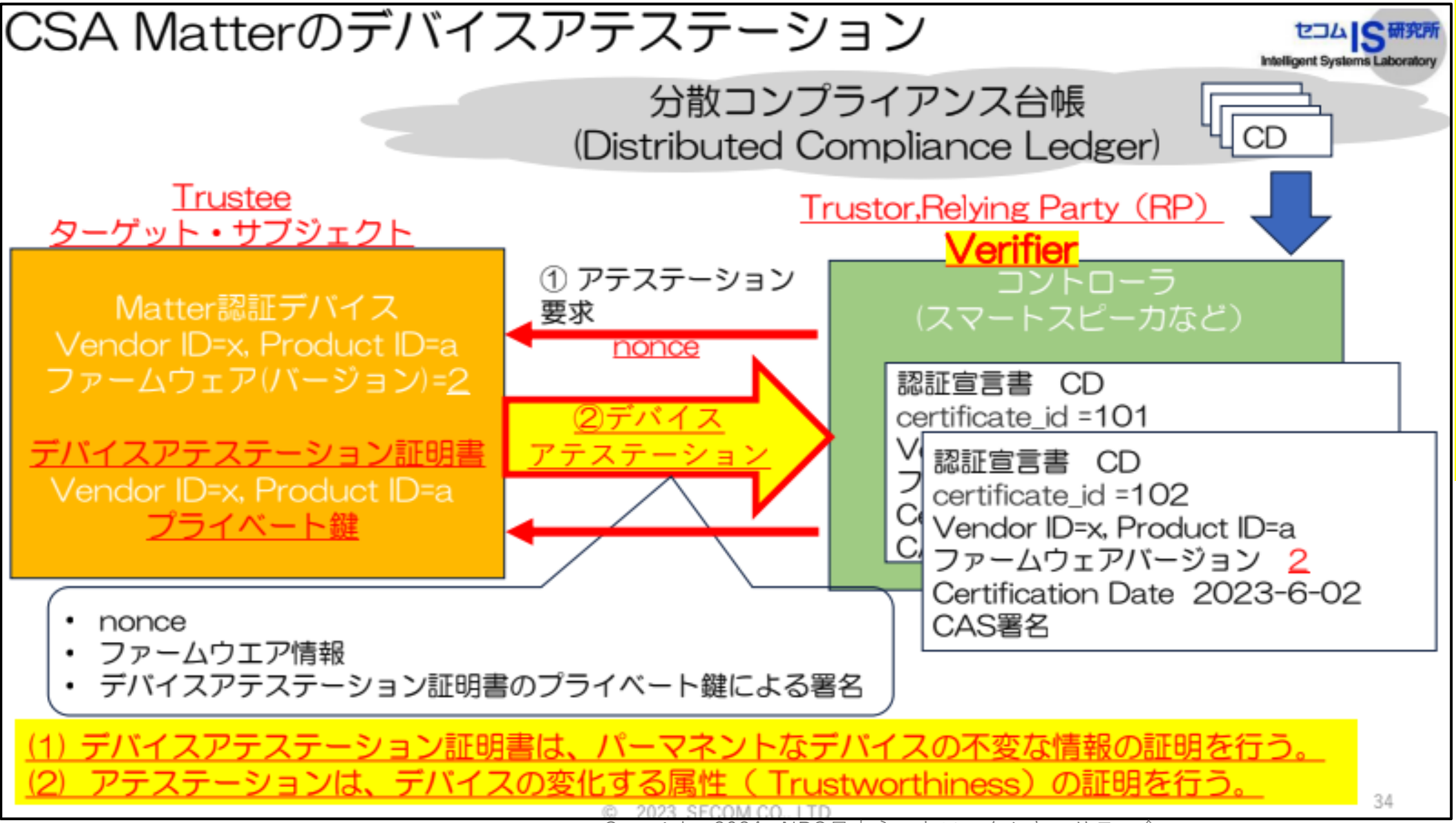
高信頼実行環境TEE(Trusted Execution Environment）など、現在IoTデバイス・環境への搭載　→　ここが、本講演の主旨するところ
・従来からの「デバイスの識別・認証」
・IoTデバイスにおける利用時の様々な信頼性（trustworthiness）の証明



出典：
セキュアコンポーネントとPKIが作るデジタルトラストの世界
IETFのIoT標準化動向などから見えてくるIoTのプラットフォーム化
2021年9月27日
https://www.ieice.org/~dpf/wp-content/uploads/2021/08/松本DPF研究会.pdf

リモートアテステーションは、「クレデンシャル情報（署名鍵）の安全な保管」が大前提

認証されたIoTデバイス同士が繋がる仕組みを提供　CSA Matter
認証宣誓書（CD: Certification Declaration)は、ファームウェアバージョン毎に作成
→　IoTデバイス出荷後のファームウェア更新に対応



認証されたIoTデバイスであっても

脆弱性が発見されたファームウェアは、更新される必要がある。

そうでなければ、信頼できるIoTデバイスではないはず。

出典：
Socity5.0実現にとっての(ゼロ)トラスト
2023年12月14日
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

コンシューマIoTセキュリティ標準化のインパクト
--なぜ「IoTセキュリティ標準化の動向を知る」が重要なのか--

- ETSI EN 303 645などのコンシューマIoTデバイスセキュリティ標準と、適合性評価制度などの制度は
  - コンシューマIoTデバイスを中心としたビジネス構造を、大きく変える可能性がある。
  - → 標準化がIoTデバイスのプラットフォーム化を可能にし、制度がこうした動きを加速している。
- 適合性評価＆ラベリングの次に来るのは、IETFなどで標準化が進展しているリモートアテステーションでは？
  - IoTデバイスセキュリティなどを高めるための認証(Certificate)は、ともて重要だが、それだけでは、なかなか、 継続的にセキュリティなどを高めるインセンティブが、ベンダーに働かない。
  - リモートアテステーションでは、リライングパーティからの自動的な検証と接続ができることとなり、これは、IoTデバイスの継続的なセキュリティを高めるインセンティブが強力に働く。
  - 結果として、 IoTデバイス自体のセキュリティなどを高めることにつながると考えられる。
- リモートアテステーションを部分的に実現しているCSA matter
  - 「モノ」の認証(Certificate)は、さまざまな分野で存在している（自動車、医療機器などの型式認証、etc.）
  - しかし「モノ」の認証(Certificate)が、リモートから動的に検証できる手段は、提供されていなかった
  - また、出荷後の個別の「モノ」のセキュリティなどの変化（ソフトウェア更新など）に対応する仕組みも無かったと考えられる。 → 出荷後は、更新、未更新のデバイスが混在する。
  - CSA matterは、こうした課題の対応に対応したフレームワークを提供しつつある。
- 「IoTセキュリティ標準化の動向を知る」は、とっても重要
  - これは、Society 5.0 「サイバー空間とフィジカル空間を高度に融合させたシステム」の技術標準の動向
  - こうした動向を的確に捉え、社会に情報を提供していくのがJNSA 標準化部会の果たすべき役割のひとつ