

# モノの認証とその応用へ



2019年11月8日  
セキュアIoTプラットフォーム協議会  
仕様検討部会 座長 豊島大朗

- SCOPEへの取り組み
  - ✓ 現状と今後の予定
- セキュアIoTプラットフォーム協議会の取り組み
  - ✓ 現状と今後の予定
- サイバートラストの取り組み
  - ✓ モノの認証とその応用

# SCOPEの取り組み

# SCOPEの取り組み

## ・研究テーマ：

「IoT デバイス認証基盤の構築と新AI 手法による表情認識の医療介護への応用についての研究開発」

## 【2018年度成果】

- ・ IoTデバイスへのPKI電子認証の基本コンセプト発表
  - ✓論文：2018.11 信学技報 (IEICE technical report)
- ・ IoT機器のライフサイクルにおいて想定される脅威、対策、評価方法を整理
  - ✓2018年度:企画・設計フェーズ(完了)



実装イメージ  
を検討中

## ネットワークカメラの対策 (案)

- ・ 802.1x認証によって、カメラ、スイッチのポートに第三者の端末を接続しても、スイッチのポートが有効にならない。
- ・ PoEスイッチの設置場所が第三者に露出しても、ネットワークに接続できない。
- ・ カメラが盗難にあっても、証明書を失効することで、不正接続を防止できる。

## 【2019年度活動内容】

- ・ 介護施設での実証実験に向け、カメラに対する認証の仕組みを実装し、以下のテストを実施
  - ✓証明書ベースでのカメラの個体認証、管理コンソール上からの機器管理、撮影映像への署名およびデータ転送
- ・ 2020年度の事業実証に向けての準備を検討
  - ✓検証項目の洗い出し
  - ✓実証実験協力者の選定



## 【2020年度活動予定】

- ・ 介護施設での実証実験に向け、カメラに対する認証の仕組みを実装し、以下のテストを実施
  - ✓機器の改良、撮影映像の品質調査

# SCOPEへの取り組み

## 2018年度 認証の基本コンセプト

## 2020年度 実用技術の検証

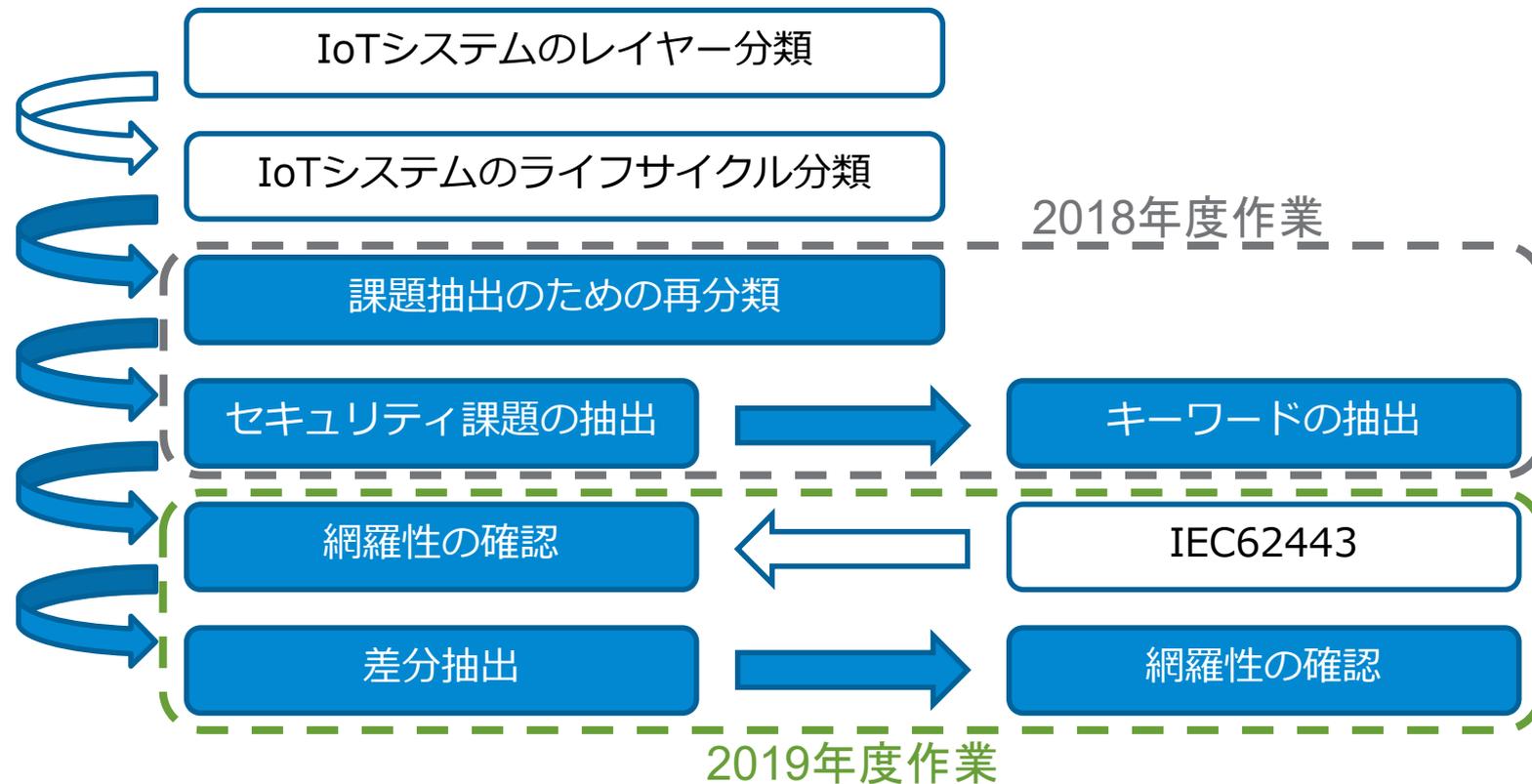
介護現場における  
シニアおよび要介護  
者の体調/ストレス状  
態の把握における、  
カメラのなりすまし、  
個人データ盗聴・改  
ざんの防止



## 2019年度 基盤技術の実装

※総務省「IoTセキュリティ総合対策」  
平成29年10月3日公表より

# セキュアIoTプラットフォーム協議会の取り組み



## 1. 「セキュリティガイドラインの素案」の収集

会員企業の事業領域から、ライフサイクルを「企画・設計／開発／製造／量産／運用／廃棄」の6レイヤに分類し、セキュリティガイドラインの素案を「カテゴリ／基準／対策」の項目で収集

事業領域ごとに用語がことなり、意味が不明瞭になる

## 2. 「キーワード集」の作成

素案内の用語から、キーワードを抽出し、これに解説を入れた「キーワード集」を作成。（※2019年公開予定）

セキュリティガイドラインの網羅性検証

## 3. 「IEC62443」勉強会の実施

セキュリティガイドラインの網羅性への対応から、IEC62443をモデルに学習。本年度は収集したセキュリティガイドラインの素案とIEC62443との差異を確認中。

出典	内容の概要	注記 (注脚)
1	商業した機器を読み、ネットワークに再接続し、他の機器を送信する	商業向けクラウドサービスで、認証キーを無効化し、商業向けは、ストレージエリアを整理済。または、物理破壊、結果内業を外務委託する場合は、商業エビデンスを受審する
2	商業した機器の中からプログラムを読み、実行内容を解析する	プログラムの読み取りは許可される。暗号化、暗号化/エンコード/暗号、セキュリティアップデート、ITAC/コト等、プログラムの不正確な読み取りは拒否される
3	商業した機器中のデータを読み	商業向けは、ストレージエリアを整理済。または、物理破壊、外部委託する場合は、商業エビデンスを受審する
4	商業した機器から情報収集を行う	基礎的な機能化の物理保護をする
5	商業した機器の中心認証キー「パスワード」を読み、他の機器に転送し、正当な機器に送り出す	商業向けは、基礎的な物理保護、外部委託する場合は、商業エビデンスを受審する 認証キーは、ストレージエリアに格納する 商業向けは、ストレージエリアを整理済。または、物理破壊/外部委託する場合は、商業エビデンスを受審する
6	商業した機器の中心認証キーが格納されたメモリを読み、他の機器に転送し、正当な機器に送り出す	商業向けクラウドサービスで、認証キーを無効化する メモリは物理的に保護、物理的な保護による認証キーの無効化、外部委託する場合は、商業エビデンスを受審する
7	コンソールで取得情報等、商業の管理が困難	認証キーは、ストレージエリアを整理済。または、物理破壊、外部委託する場合は、商業エビデンスを受審する
8	中古販売等、高利得を目的とした商業	商業向けクラウドサービスで、認証キーを無効化する 商業向けは、ストレージエリアを整理済。または、物理破壊、外部委託する場合は、商業エビデンスを受審する
9	利用者の商業方針の通知	商業方針、利用規約、説明書等による通知

**IEC62443勉強会資料**

ID	タイトル	備考
01	230 ルール	1 セット
02	230 リードタイム	1,41214 セット
03	230 リモートアクセス	2,00207 セット
04	230 リモートアクセス	1,86121 セット
05	230 リモートアクセス	1 セット
06	230 ログ	2 セット
07	230 ログファイル	1,48170 セット
08	230 標準	1,41214 セット
09	230 標準	1,41214 セット
10	230 標準	2,12009 セット
11	230 標準化	1,86121 セット
12	230 標準化	2,30347 セット
13	240 標準化	2,30347 セット
14	241 標準化	6,41302 セット

**IEC62443とは**

- 汎用制御システム向けのセキュリティ標準規格
- 業界ごとの標準規格を統合

制御システム分野での標準化に関する技術動向

米国NISTの調達基準「SP800-53」をほぼ包含

■欧州・米国共通の標準規格→グローバルスタンダードになると予想

IEC62443の対応範囲 ~運用・管理・製造・技術の観点から~

# サイバートラストの取り組み

# 課題と対応策（サイバートラストの対応策）

【課題シナリオ】すべてのIoT機器に認証の仕組みを導入するためには

## ■ 導入の課題

- ✓ 単価（コスト）の上昇
- ✓ サービス提供事業者の事業継続性
- ✓ 大量のIoT機器の管理
  - 電子証明書の発行スピードの課題
  - CRL、OCSPの大量問合わせの課題
  - DBの検索性（スピード、アクセスログetc）

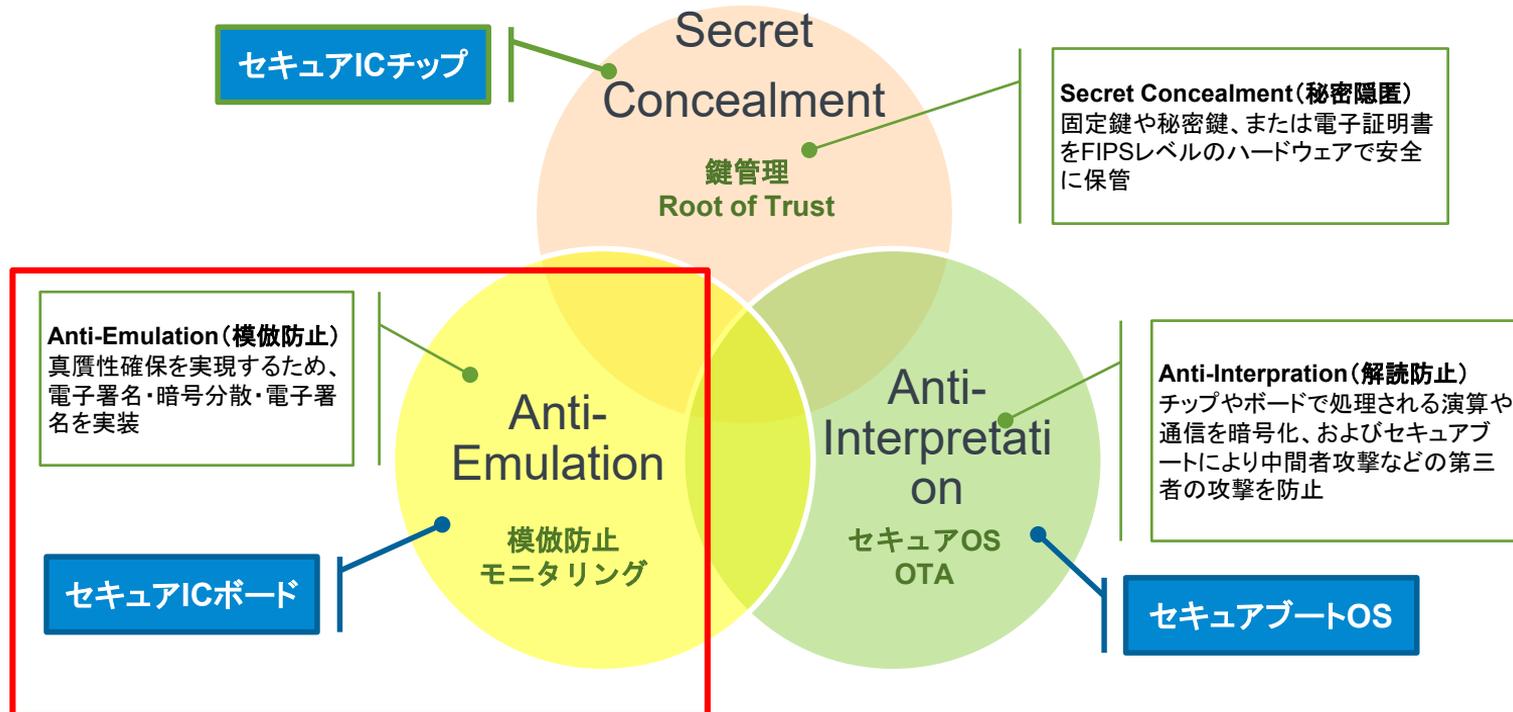
認証局の性能改善

## ■ 普及の課題

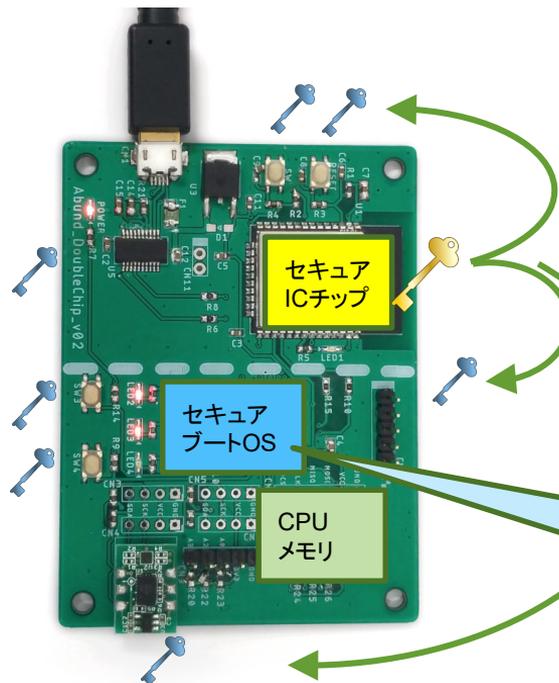
- ✓ 法的根拠
  - 電子署名法における「認定認証業務」相当の認定制度の検討
- ✓ プラットフォーム化／マルチテナント／標準化
  - 誰が作っても同じセキュリティ強度やクオリティが担保できるか
  - 公的資金による普及支援 ・ 国際連携の中で相互接続性が保てるか
- ✓ メーカー側のメリットの整理
  - 費用対効果
  - ユーザー（利用者）からの要求なのか
  - 国際競争力につながるのか

柔軟な認証方式の提供

## 3つのセキュリティ要素と構成 (セキュアICチップ+セキュアICボード+セキュアブートOS)



## 秘密分散とモニタリングで不正を防止／検知する



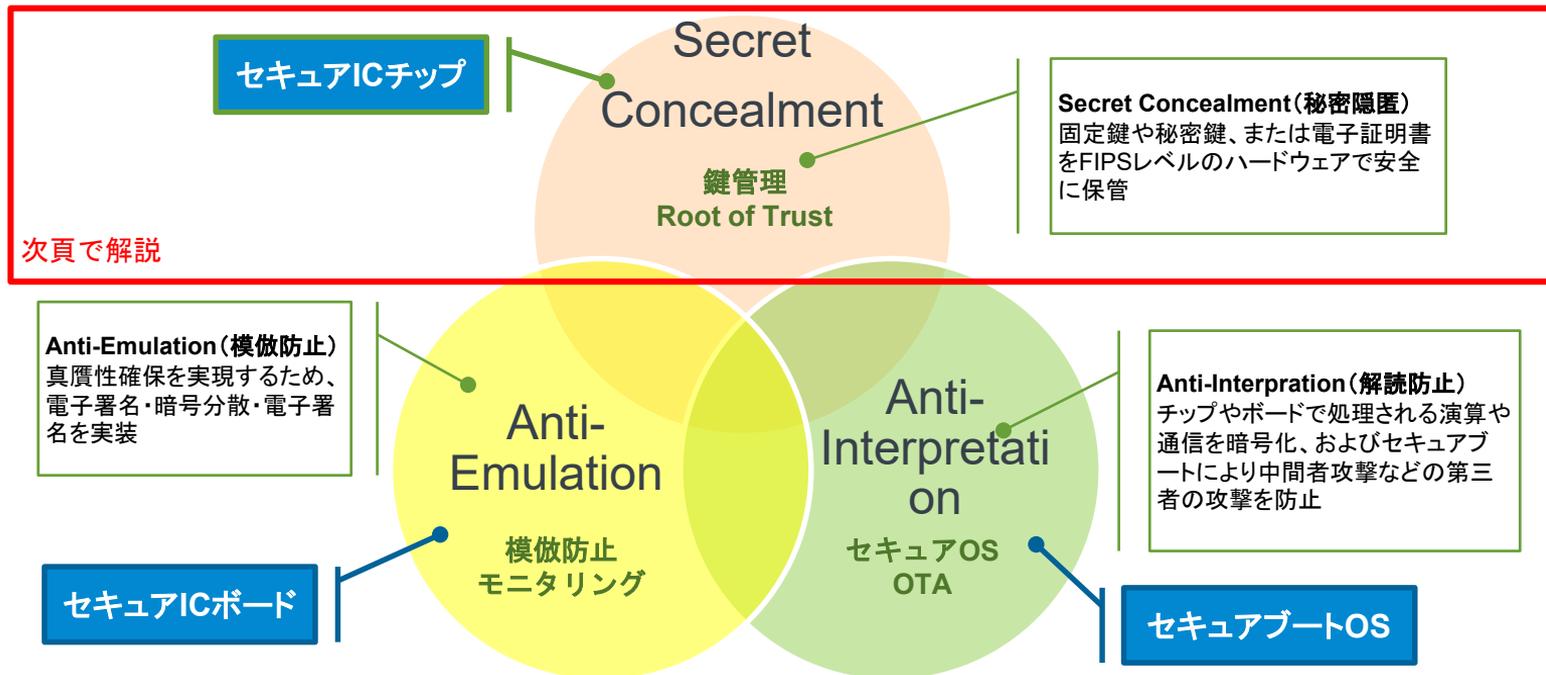
セキュアICボード実装例

1. セキュアICチップ（耐タンパ）に格納されている固定鍵／秘密鍵を分散させ、各パーツに配付。
2. これらの分散処理をブート毎、もしくは定期的にボード上で実行することで、不正パーツを検知もしくは行動不能にすることを實現。
3. 分散鍵が入らない小さなパーツについては、ボード全体のモニタリングを実行することで、異常動作を検知し、ボード全体の真贋性を向上させることができる。

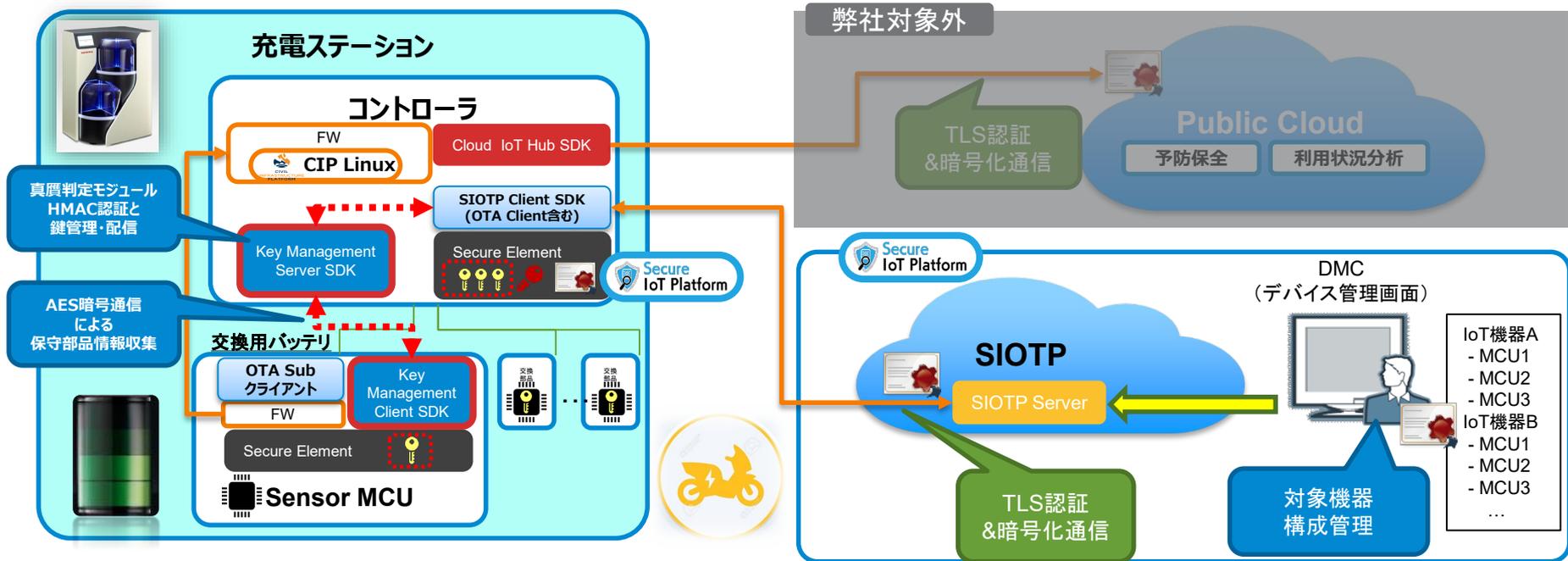
### 【モニタリング】

セキュアブート実行時や、通常稼働時にモニタリングを実行することで、不正パーツの混入とバグ動作などを検知することができる。  
(電圧、送信パケット、振る舞い、CPU稼働率などを検出)

## 3つのセキュリティ要素と構成 (セキュアICチップ+セキュアICボード+セキュアブートOS)



# 真贋判定ソリューション (ソリューション概要)



真贋判定モジュール(上記Key Management Server/Client)にて認定バッテリーと模造品をローカルで判別  
・東芝D&S社半導体に打ち込まれた固有情報とCTJ側SIOTPサーバに登録された固有情報を比較  
・バッテリーの利用状況についてはCloud IoT Hub SDKを通じて指定のPublic Cloudへ直接送信(証明書認証アクセス)

ご清聴ありがとうございました