

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】

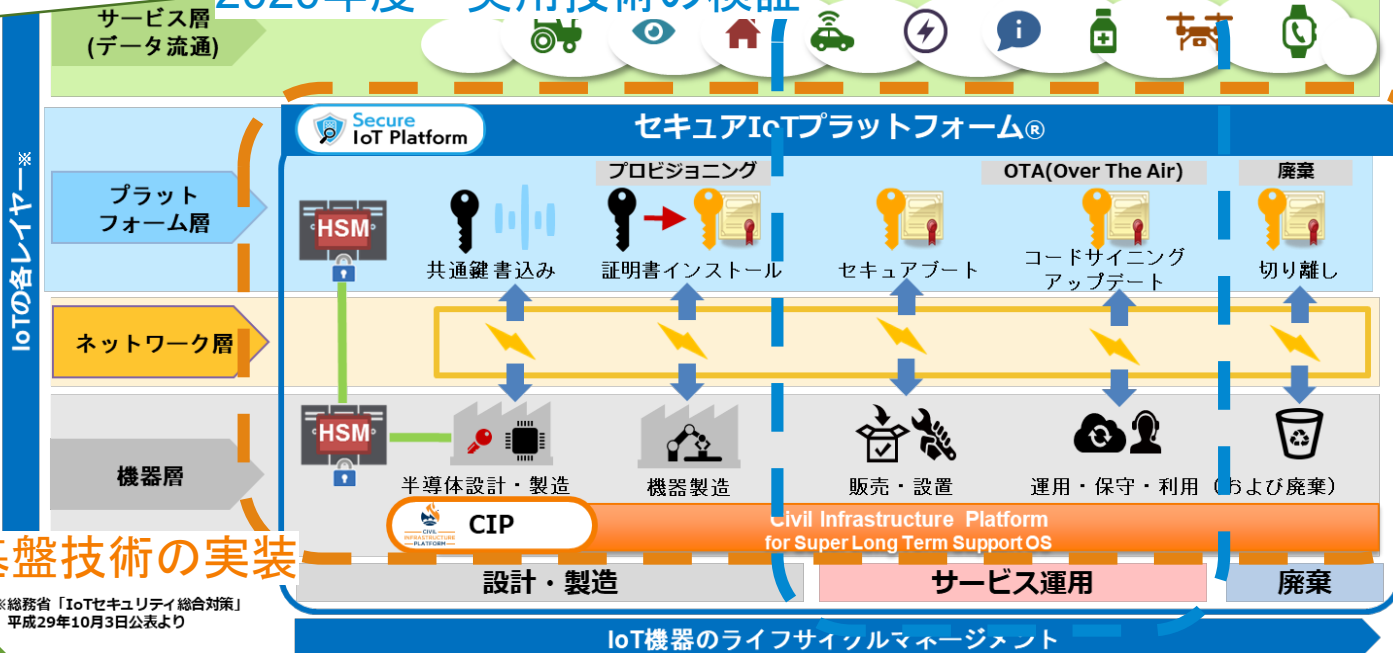
- ・ 介護施設での実証実験に向け、カメラに対する認証の仕組みを実装し、以下のテストを実施
 - ✓機器の改良、撮影映像の品質調査

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

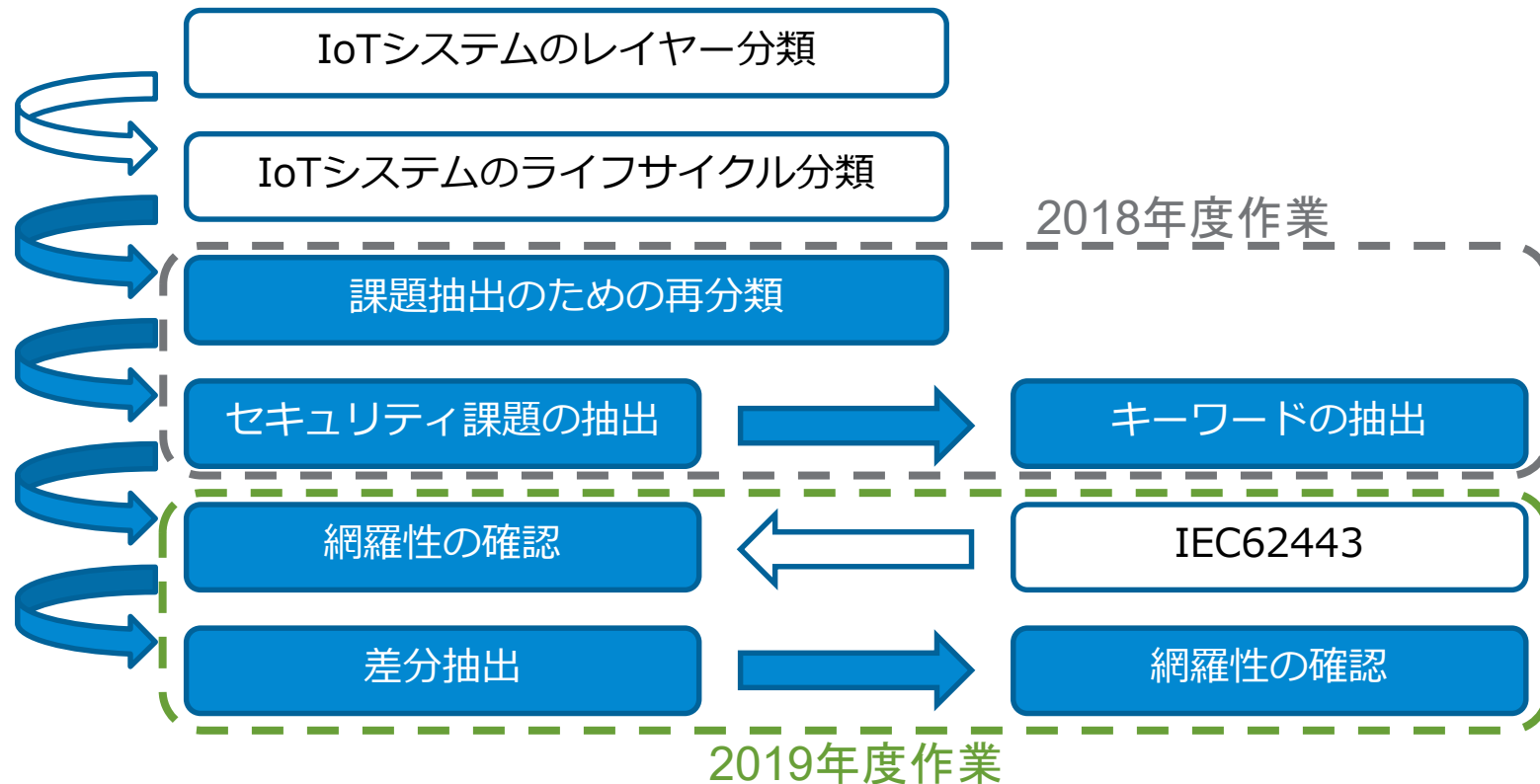
介護現場における
シニアおよび要介護
者の体調/ストレス状
態の把握における、
カメラのなりすまし、
個人データ盗聴・改
ざんの防止



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



活動内容

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）

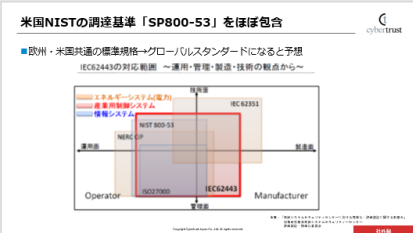
セキュリティガイドラインの網羅性検証

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。

項目	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	商業用ソフトウェア一式が、認証キーを無効化し、商業用は、ストレージエリアを整理済。または、物理破壊、結果内蔵を外付する場合は、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が可能な場合は、暗号化、鍵管理/鍵管理/鍵管理、セキュリティアップデート、IT/CIC/IT等、プログラムの必要数値が読み取れない
3	商業した機器中のデータを読み	商業用は、ストレージエリアを整理済。または、物理破壊、外付する場合は、商業エビデンスを受審する
4	商業した機器から認証情報を盗む	基礎の暗号化の物理保護をする
5	商業した機器の中心認証キー「データ」を読み、他の機器に転送し、正当な機器に渡ります	商業用は、基礎の物理破壊、外付する場合は、商業エビデンスを受審する 認証キーは、暗号化/鍵管理/鍵管理 商業用は、ストレージエリアを整理済。または、物理破壊、外付する場合は、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転送されたメモリを読み、他の機器に移り、正当な機器に渡ります	商業用は、ストレージエリアを整理済。または、物理破壊、外付する場合は、商業エビデンスを受審する
7	コンソールで取得情報、商業の管理が困難	以下の項目を認め、商業時にクラウドサービスで、認証キーを無効化、認証キーは、暗号化/鍵管理/鍵管理、プログラムの暗号化/鍵管理/鍵管理
8	中古販売等、高利得を目的とした商業	商業用は、ストレージエリアを整理済。または、物理破壊、外付する場合は、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

項目	内容	注記
01	230-ルール	1 setkat ✓
02	230-ルール	1.43214 setkat ✓
03	230-ルール	2.00237 setkat ✓
04	230-ルール	1.86121 setkat ✓
05	230-ルール	1 setkat ✓
06	230-ルール	2 setkat ✓
07	230-ルール	1.43214 setkat ✓
08	230-ルール	1.43214 setkat ✓
09	230-ルール	1.43214 setkat ✓
10	230-ルール	1.43214 setkat ✓
11	230-ルール	1.43214 setkat ✓
12	230-ルール	1.43214 setkat ✓
13	230-ルール	1.43214 setkat ✓
14	230-ルール	1.43214 setkat ✓
15	230-ルール	1.43214 setkat ✓
16	230-ルール	1.43214 setkat ✓
17	230-ルール	1.43214 setkat ✓
18	230-ルール	1.43214 setkat ✓
19	230-ルール	1.43214 setkat ✓
20	230-ルール	1.43214 setkat ✓
21	230-ルール	1.43214 setkat ✓
22	230-ルール	1.43214 setkat ✓
23	230-ルール	1.43214 setkat ✓
24	230-ルール	1.43214 setkat ✓
25	230-ルール	1.43214 setkat ✓
26	230-ルール	1.43214 setkat ✓
27	230-ルール	1.43214 setkat ✓
28	230-ルール	1.43214 setkat ✓
29	230-ルール	1.43214 setkat ✓
30	230-ルール	1.43214 setkat ✓
31	230-ルール	1.43214 setkat ✓
32	230-ルール	1.43214 setkat ✓
33	230-ルール	1.43214 setkat ✓
34	230-ルール	1.43214 setkat ✓
35	230-ルール	1.43214 setkat ✓
36	230-ルール	1.43214 setkat ✓
37	230-ルール	1.43214 setkat ✓
38	230-ルール	1.43214 setkat ✓
39	230-ルール	1.43214 setkat ✓
40	230-ルール	1.43214 setkat ✓
41	230-ルール	1.43214 setkat ✓
42	230-ルール	1.43214 setkat ✓
43	230-ルール	1.43214 setkat ✓
44	230-ルール	1.43214 setkat ✓
45	230-ルール	1.43214 setkat ✓
46	230-ルール	1.43214 setkat ✓
47	230-ルール	1.43214 setkat ✓
48	230-ルール	1.43214 setkat ✓
49	230-ルール	1.43214 setkat ✓
50	230-ルール	1.43214 setkat ✓
51	230-ルール	1.43214 setkat ✓
52	230-ルール	1.43214 setkat ✓
53	230-ルール	1.43214 setkat ✓
54	230-ルール	1.43214 setkat ✓
55	230-ルール	1.43214 setkat ✓
56	230-ルール	1.43214 setkat ✓
57	230-ルール	1.43214 setkat ✓
58	230-ルール	1.43214 setkat ✓
59	230-ルール	1.43214 setkat ✓
60	230-ルール	1.43214 setkat ✓
61	230-ルール	1.43214 setkat ✓
62	230-ルール	1.43214 setkat ✓
63	230-ルール	1.43214 setkat ✓
64	230-ルール	1.43214 setkat ✓
65	230-ルール	1.43214 setkat ✓
66	230-ルール	1.43214 setkat ✓
67	230-ルール	1.43214 setkat ✓
68	230-ルール	1.43214 setkat ✓
69	230-ルール	1.43214 setkat ✓
70	230-ルール	1.43214 setkat ✓
71	230-ルール	1.43214 setkat ✓
72	230-ルール	1.43214 setkat ✓
73	230-ルール	1.43214 setkat ✓
74	230-ルール	1.43214 setkat ✓
75	230-ルール	1.43214 setkat ✓
76	230-ルール	1.43214 setkat ✓
77	230-ルール	1.43214 setkat ✓
78	230-ルール	1.43214 setkat ✓
79	230-ルール	1.43214 setkat ✓
80	230-ルール	1.43214 setkat ✓
81	230-ルール	1.43214 setkat ✓
82	230-ルール	1.43214 setkat ✓
83	230-ルール	1.43214 setkat ✓
84	230-ルール	1.43214 setkat ✓
85	230-ルール	1.43214 setkat ✓
86	230-ルール	1.43214 setkat ✓
87	230-ルール	1.43214 setkat ✓
88	230-ルール	1.43214 setkat ✓
89	230-ルール	1.43214 setkat ✓
90	230-ルール	1.43214 setkat ✓
91	230-ルール	1.43214 setkat ✓
92	230-ルール	1.43214 setkat ✓
93	230-ルール	1.43214 setkat ✓
94	230-ルール	1.43214 setkat ✓
95	230-ルール	1.43214 setkat ✓
96	230-ルール	1.43214 setkat ✓
97	230-ルール	1.43214 setkat ✓
98	230-ルール	1.43214 setkat ✓
99	230-ルール	1.43214 setkat ✓
100	230-ルール	1.43214 setkat ✓



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）

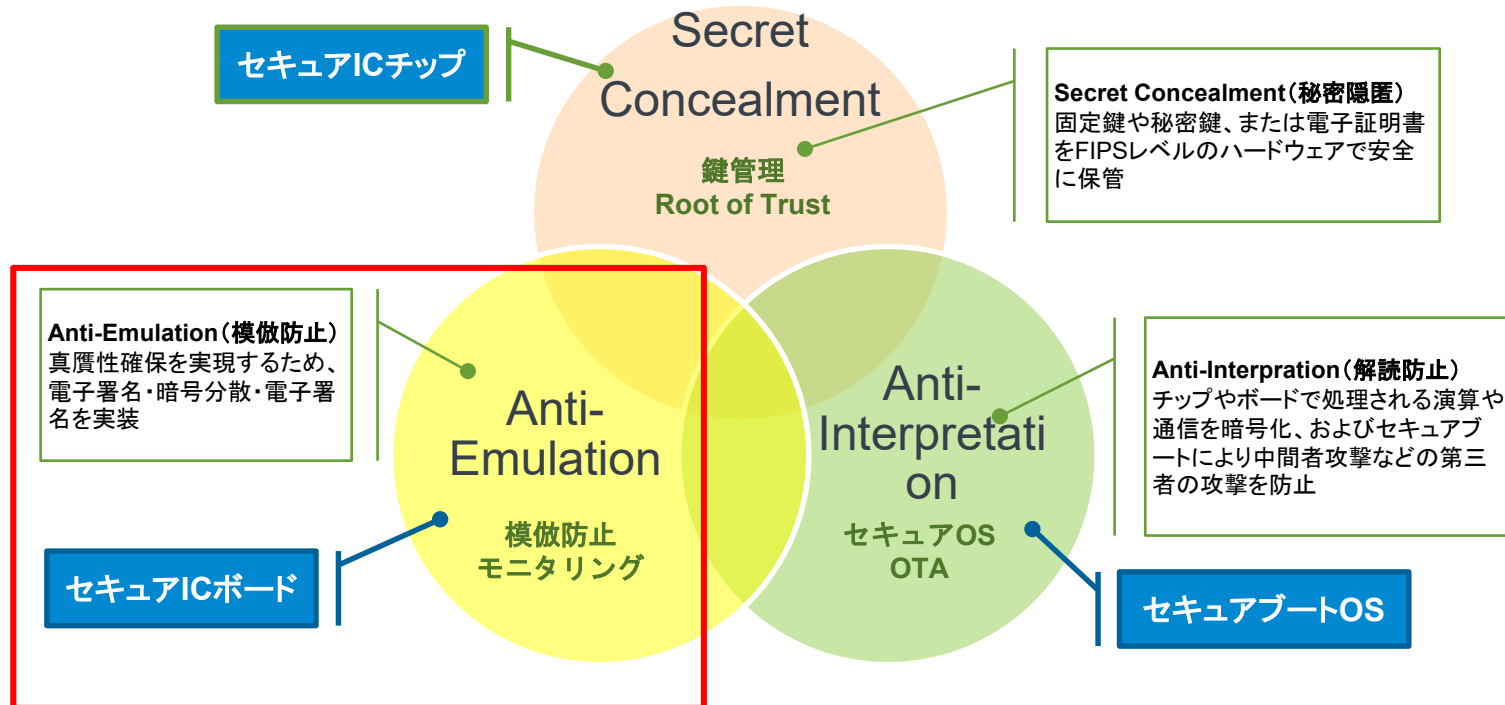
認証局の性能改善

■ 普及の課題

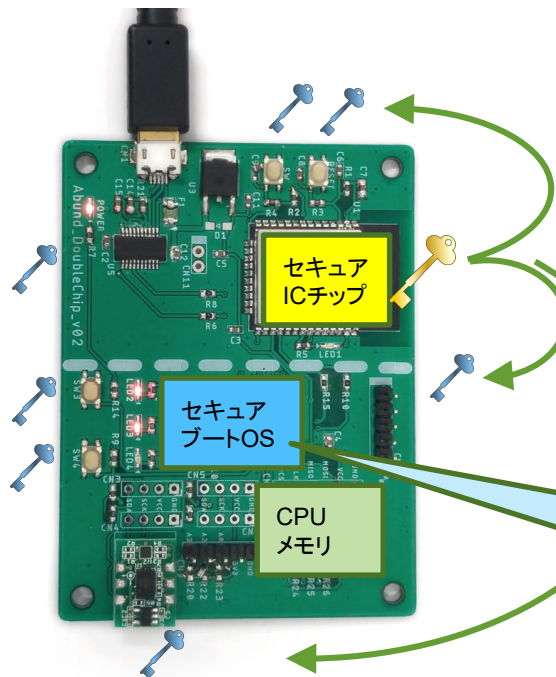
- ✓ 法的根拠
 - 電子署名法における「認定認証業務」相当の認定制度の検討
- ✓ プラットフォーム化／マルチテナント／標準化
 - 誰が作っても同じセキュリティ強度やクオリティが担保できるか
 - 公的資金による普及支援 ・ 国際連携の中で相互接続性が保てるか
- ✓ メーカー側のメリットの整理
 - 費用対効果
 - ユーザー（利用者）からの要求なのか
 - 国際競争力につながるのか

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



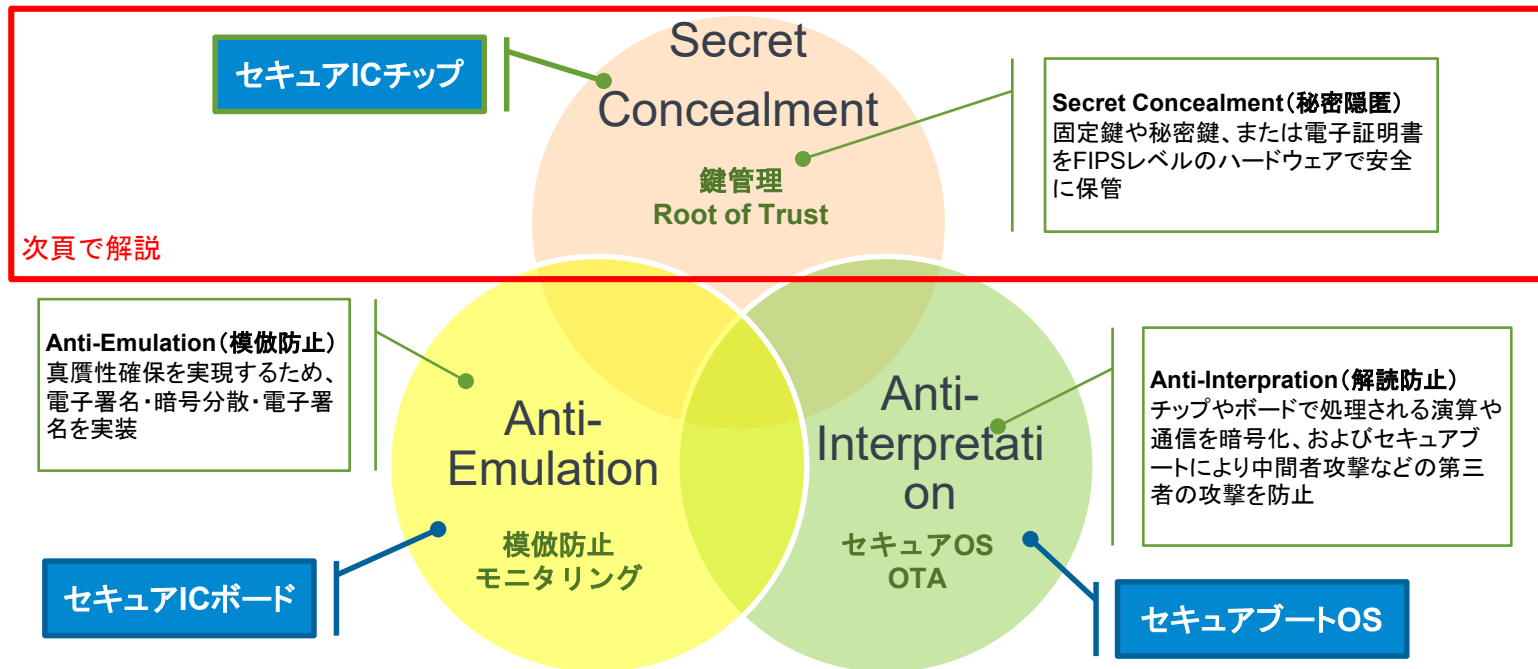
セキュアICボード実装例

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。

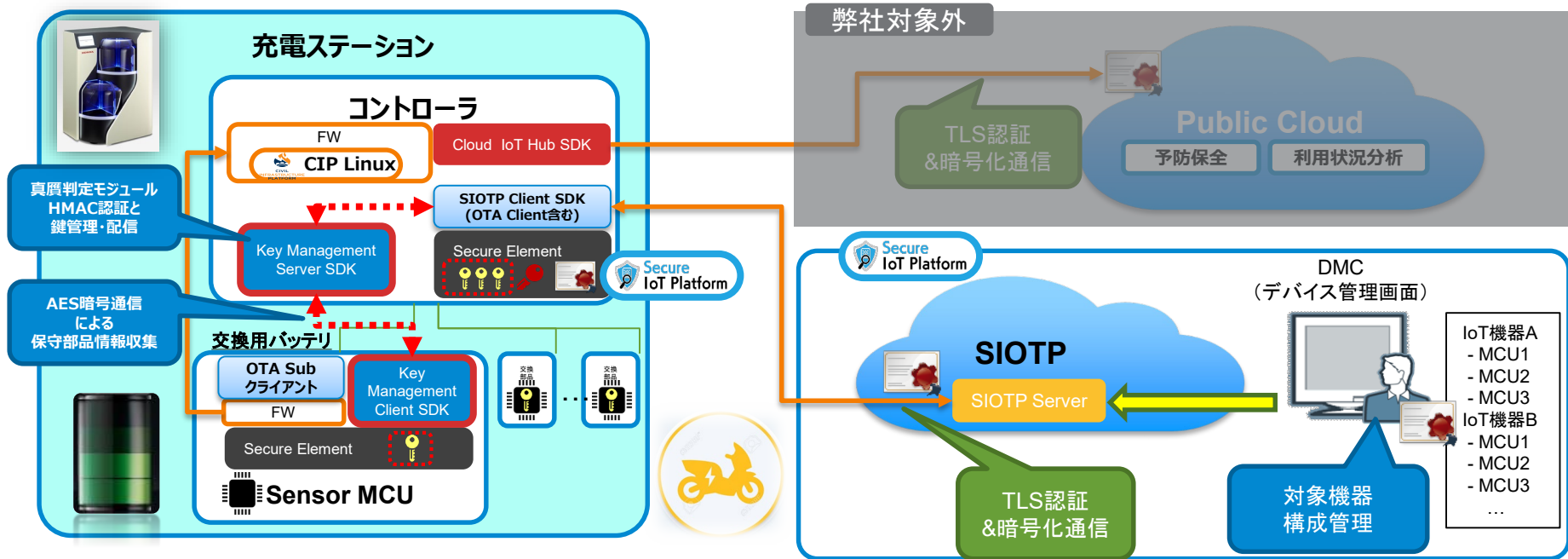
【モニタリング】

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