CCDS
セキュリティ技術ワーキンググループ

IoTシステム調達のための
セキュリティ要件フレームワーク

はじめに

- 安心安全な社会に向けた指標に向けて
  - Society5.0やコネクティッドインダストリーズなど生活の利便性を向上させる為のサービスがリリース
  - サービスを行う為の様々なIoT機器が出荷
    IoT機器を踏み台にしたサイバー攻撃も増加傾向
  - IoTセキュリティにChain of Trust, Root of Trustなど信頼性を高める取組は行われている
  - ただし、機器やサービスが安全であるか見極めは非常に難しい

「製造者や調達者など、分かりやすい指標が必要」

セキュリティ技術WG 活動の背景と目的

- **背景　～IoTセキュリティ対策って わかりにくい～**
  - **ユーザー企業の声**
    - どのガイドラインを見たらいいか わからない…
    - どの製品を買ったらよいか 評価方法が わからない…
  - **ベンダー企業の声**
    - 価格競争の中で 高セキュアな製品を売る方法がわからない…
    - セキュリティ要件が広範にわたり 何を訴求すべきか わからない…

- **WGの目標 ～具体的な対策が簡単にわかるフレームワークを考案～**
  - IoTシステム調達時のセキュリティ**評価**ポイントがわかるリスト
  - IoTシステム提案時のセキュリティ**訴求**ポイントがわかるリスト

- **本フレームワークの対象と特長**
  - IoTデバイスから クラウドまで システム全体を対象
  - 「IoTセキュリティガイドライン」の各要点ごとに要件を整理
  - 他の標準(NIST SP800等)の管理レベル評価基準も盛り込める

本フレームワークにおける分類と要件

- IoTシステムをコンポーネント単位（クラウド～エッジ端末）に分けて、各コンポーネント毎に、リスクとそれに対応するセキュリティ要件を下記分類に毎にカテゴライズ

  ① **IoTセキュリティガイドライン（要点13～21への対応）**
  - ユーザからベンダーまで包括的な視点でセキュリティ対策検討が可能

  ② **リスクカテゴリ**
  - セキュリティリスク、セーフティリスク、信頼性リスク、品質リスク、性能リスク

  ③ **脅威分類：STRIDE＋CCDS（脆弱性評価検証ガイドライン）**

  STRIDE：なりすまし・データ改竄・否認・情報漏洩・サービス不能・権限の昇格

  CCDS：不正アクセス・マルウェア感染・踏み台・不正改造・未知の脆弱性

- セキュリティ要件
  - 製造から運用のプロセスにおいてのリスクを見える化したうえで、そのリスクに対するセキュリティ要件を対策レベル毎に数値化
    - NIST SP800-53における3段階評価
    - 数値の合計値を用いることで対策達成度の指針として利用可能に

IoTセキュリティリスク対策評価シートの構成と見方

IoTセキュリティリスク対策評価シートは、調達者がセキュリティについて検討する際の視点とそれに対して実施されている対策・評価で構成されています。
調達者は以下の３つの視点から必要とする要件を選らぶことができます。

①コンポーネント：IoTシステムを構成するサービスや機器を基準に検討する場合、この中から必要とするものを選ぶことで、それに関連する要点・リスク・脅威・対策が表示されます。

②要点：IoTセキュリティガイドラインから調達者が検討する要点13～21を参考としており、必要な要点を選ぶことで、それに関連するコンポーネント・リスク・脅威・対策が表示されます。

③リスク分類～脅威分析：コンポーネントと要点から洗い出されたリスク・脅威が表示されます。

検討する際の視点

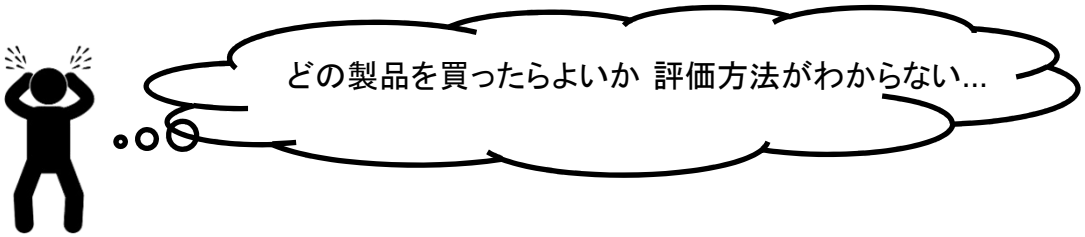
実施されている対策とその評価

コンポーネント (1)	主体者	リスク分類 (3)	リスク (3)	リスク詳細 (3)	脅威分析 (3)	要点 (2)	調達時の対策	製造時の対策	流通・販売時の対策	運用開始～終了時の対策	廃棄・回収時の対策
クラウド	クラウド事業者監視範囲	セキュリティ	不正利用される	IDパスワードが破られる	情報の暴露(漏洩)	13					
		信頼性	監視ログの消失	ログ記録装置の故障	・・・・	14					
		性能	・・・・	・・・・	・・・・	15					
ネットワーク	サービス提供者の監視範囲	セーフティ	・・・・・	・・・・・	・・・・	16					
専用ターミナル	・	・・・	・・・	・・・・・・	・・・・	17					
スマートロック	・	・・・	・・・・・	・・	・・・・	18					
開錠デバイス	・	・・・	・・・・・	・・・・・	・・・・	19					

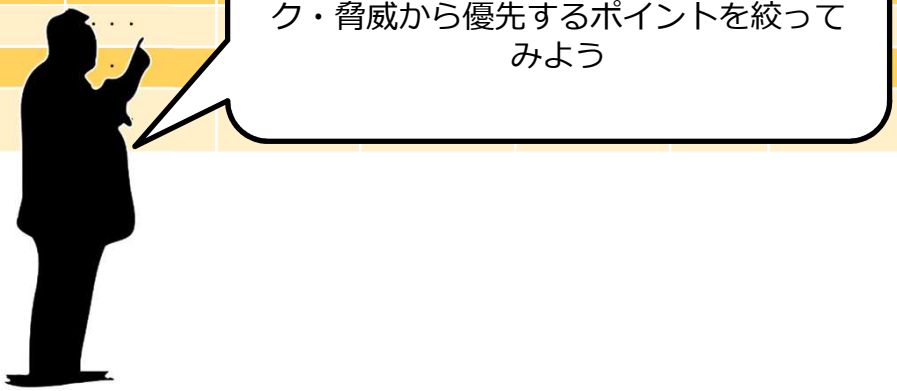
調達者が利用（購入）するときに検討すべき観点として、IoTセキュリティガイドラインから要点13～21を参考としています

要点13. 機器等がどのような状態かを把握し、記録する機能を設ける
要点14. 機能及び用途に応じて適切にネットワーク接続する
要点15. 初期設定に留意する
要点16. 認証機能を導入する
要点17. 出荷・リリース後も安全安心な状態を維持する
要点18. 出荷・リリース後もIoT リスクを把握し、関係者に守ってもらいたいことを伝える
要点19. つながることによるリスクを一般利用者に知ってもらう
要点20. IoT システム・サービスにおける関係者の役割を認識する
要点21. 脆弱な機器を把握し、適切に注意喚起を行う

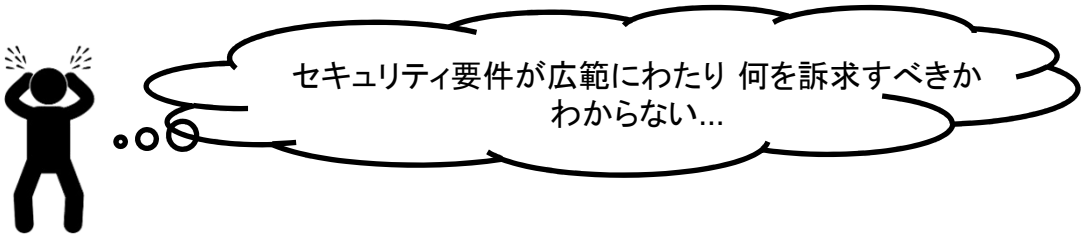
評価シートの活用例(ユーザー/調達目線)



コンポーネント	主体者	リスク分類	リスク	リスク詳細	脅威分析	要点	調達時の対策	・・・	廃棄・回収時の対策	実現製品
クラウド	クラウド事業者監視範囲	セキュリティ	不正利用される	IDパスワードが破られる	情報の暴露(漏洩)	13	対策A	・・・・	・・・・	A社 X製品
		信頼性	監視ログの消失	ログ記録装置の故障	・・・・	14	対策B	・・・・	・・・・	B社 Y製品
		性能						・・・		
ネットワーク	サービス提供者の監視範囲	セーフティ						・・・		
専用ターミナル	・	・・・						・・・		
スマートロック	・	・						・・・		
開錠デバイス	・							・・・・	・・・	・・・・



評価シートの活用例(SIer/メーカー目線)



コンポーネント	主体者	リスク分類	リスク	リスク詳細	脅威分析	要点	調達時の対策	・・・	廃棄・回収時の対策	実現製品
クラウド	クラウド事業者監視範囲	セキュリティ	不正利用される	IDパスワードが破られる	情報の暴露(漏洩)	13	対策A	・・・・	対策C	**A社 X製品**
		信頼性	監視ログの消失	ログ記録装置の故障	・・・・	14	対策B	・・・・	対策D	B社 Y製品
		性能	・・・・	・・・・	・・・・	15	・・・・	・・	・・・・	・・・・
ネットワーク	サービス提供者の監視範囲	セーフティ					・・	・・	・・・・	・・・・
専用ターミナル	・	・・・					・	・・	・・・・	・・・・
スマートロック	・	・・・					・	・・	・・・・	・・・・
開錠デバイス	・	・・					・	・・	・・・・	・・・・

調達者からのリクエストから開発要件が整理できた！

要件化

開発要件

今後の取り組み、課題

- **想定されるリスクと対策案は、WGメンバーが保有する製品・サービスを基に記載しています。**
  ☞より多くのケースに対応する為、CCDS会員からのインプットをお待ちしています。
  調達者視点及び提供者視点のコメントもお願いします。

- **市場に出ているセキュリティ製品を網羅するようなデータベースを構築・維持していく為には、相応の資金が必要となります。**
  ☞国から支援を頂く為の活動を進めます。

- **初版の公開範囲は、次の通りとします。**
  概要（パワーポイント）　→　一般公開
  フレームワーク（エクセル）→　CCDS会員限定

「より多くの参加者と予算で分かりやすい指標を」

協力企業名

主　　査：　Planetway Japan株式会社
副　　査：　大日本印刷株式会社
　メンバー：
　　NTTコミュニケーションズ
　　独立行政法人　製品評価技術基盤機構
　　株式会社ソリトンシステムズ
　　日本ダイレックス株式会社
　　トレンドマイクロ株式会社
　　日本プロセス株式会社
　　パナソニック アドバンストテクノロジー株式会社
　　株式会社マストトップ
　　株式会社メタテクノ
　　株式会社ラック
　　その他2社

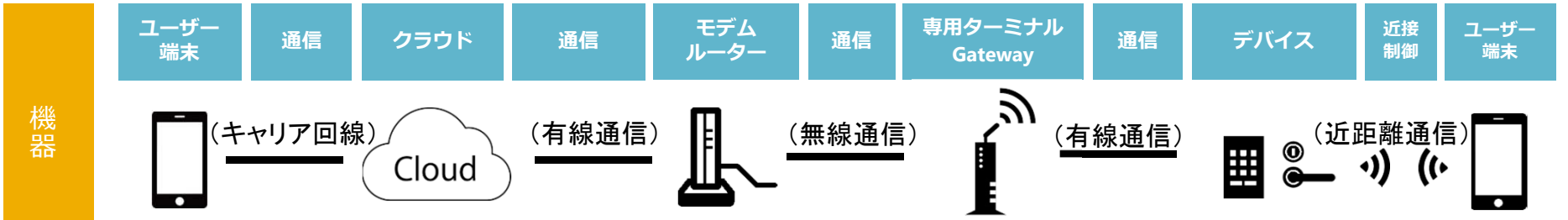
オブザーバー：　横浜市

Appendix

- 今回の検証対象
- 開発段階からのセキュリティプロセス
- 製造時のセキュリティ対策基準
- 想定される脅威の抽出（STRIDE+CCDS）

（Appendix）今回の検証対象

- アクチュエータ（スマートロック）を対象に検証
  - 誰がどのようなセキュリティを提供するのか？
  - 機器もサービスも複数社により提供され対策は非常に難しい



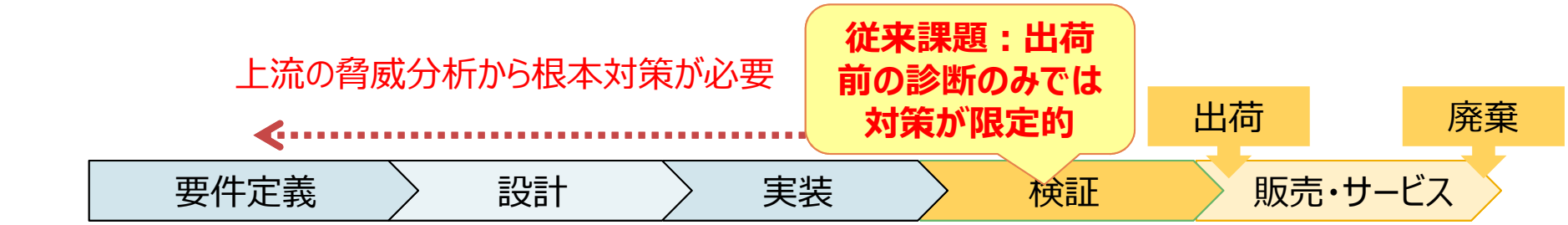
サービス						
携帯キャリア	クラウド事業者	固定通信事業者	Gatewayメーカ	スマートロックメーカ	携帯キャリア	
携帯アプリ会社	クラウドサービス会社	モデムメーカ	顧客			
			施工業者			

技術対策			
PLANET GUARDIANS ホワイトハッカー育成	PLANET ECO 安全なデータトランザクション	Wi-Fiセキュリティ対策ソリューション「AIRTMS」 日本ダイレックス(株) https://www.direx.com/assets/airtms_catalog.pdf	大日本印刷（DNP） スマートフォンで鍵を開閉できるデジタルキーのプラットフォームを開発 https://www.dnp.co.jp/news/detail/1187775_1587.html

＊対応技術は例として記載

セキュリティ開発プロセスと活動イメージ

Security by Designに基づき、要件定義～保守までセキュリティ品質を確保
→ 製品ライフサイクル全般で脆弱性排除、セキュリティ対策にかかるコストを削減



方針	混入防止（脆弱性を作りこまない）			検出除去（脆弱性を検知し除去）	保守・改修（出荷後の対応）
対応	**脅威分析、** 脅威分析ツール	**脆弱性分析、** セキュリティアーキ設計・機能開発	**セキュアコーディング対応、ハードウェア攻撃対策、** 組込み対応セキュリティ機能群	**脆弱性評価、** 脆弱性診断	インシデント対応 SIRTコンサル

太字は製造時のセキュリティ対策基準の対応項目

（Appendix）セキュリティ要件ガイドサンプル

- 製造時のセキュリティ対策基準

開発フェーズ	セキュリティ対策	対応レベル	点数
要件定義	脅威分析	システムに関連する脅威を網羅的に抽出し、リスク評価を行い、高リスクの脅威に対してセキュリティ要件を定め、設計以降で正しく対策を行っている	10
		システムに関連する一部の脅威を抽出し、リスク評価を行い、高リスクの脅威に対してセキュリティ要件を定め、設計以降で正しく対策を行っている	5
		脅威分析を行っていない	0
設計	脆弱性分析	・・・・・・・・・・・・・・・	
実装（ソフトウェア）	セキュアコーディング	・・・・・・・・・・	
実装（ハードウェア）	ハードウェア攻撃対策	・・・・・・・・・・・・・・・・・	
検証	脆弱性評価	・・・・・・・・・	

（Appendix）想定される脅威の抽出

- STRIDEにCCDSで脅威を追加したモデル

脅威名称	英語表記	説明
なりすまし（偽装）	Spoofing	コンピューターに対し、他のユーザーや機器を装うこと
データの改ざん	Tampering with Data	権限なしでデータを改ざんし、データの完全性を失わせること
否認	Repudiation	ユーザーがあるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
情報の暴露(漏洩)	Informal Disclosure	アクセス権限を持たない個人に情報が公開されること
サービス不能(DoS)	Denial of Service	正規のユーザがサーバやサービスにアクセスできないこと ※(D)DoS攻撃やジャミングによるサービス妨害など
権限の昇格	Elevation of Privilege	権限のないユーザーがアクセス権限を得ること
不正アクセス	Unauthorized access	アクセス権限を持たない者にアクセスされること
マルウェア感染	Malware infection	他の機器への汚染源になる。ランサムウェアなどにより業務妨害を受けること
踏み台	Stepping stone attack	他の機器へ不正アクセス等を行う際の中継地点として使用されること
不正改造(HW/SW)	Tampering with device	不正（違法）なハード、ソフトウェアの改造により、内部データを抜き取ったり、脆弱性の要因を組み込まれること
未知の脆弱性	Unknown Vulnerabilities	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性のこと