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

– 本フレームワークは製品メーカ、調達者など製品や機器のセキュティレベルについての指標を作成

– IoTセキュリティガイドラインをベースとして分かりやすく検索しやすいデータベースとして構築
  - セキュリティ脅威を「STRIDE（※4）＋CCDSの独自モデル」で分析
  - クラウドからエッジ端末に必要なセキュリティ要件をレイヤー毎にプロット

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