戦略的イノベーション創造プログラム（SIP）

【パナソニック】

2－3 「防御」、「検知」、「対策」でエンドポイントを守る トータルサイバーセキュリティ

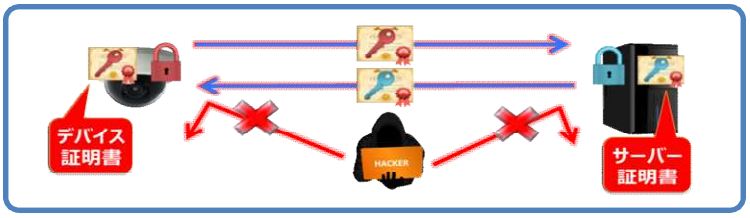
IoT向け対策技術

IoT機器内で生成した推測リスクの少ないシードから 暗号・認証鍵を生成することで、安全な暗号・認証機能を実現

①「防御」技術：暗号・認証

セキュリティが脆弱な IoT機器は攻撃対象

- 中間者攻撃
- 総当り攻撃



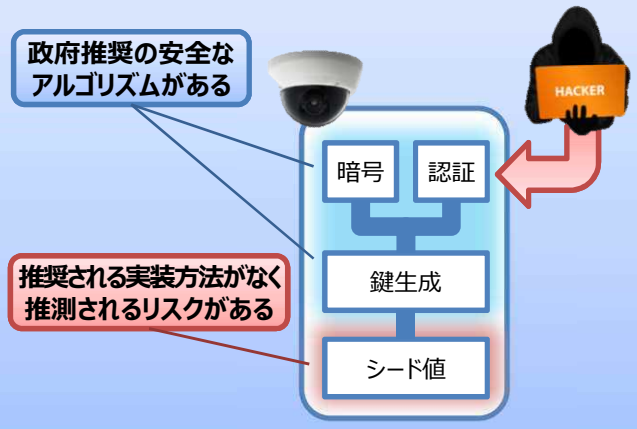
エンドポイント間での PKI認証が必須

② シード生成 ： 推測リスクの少ないシードから安全な鍵を生成

従来の課題　Before	導入による効果　After
ゆらぎの少ないシードや設計者秘密は、鍵を推測されるリスクがある	IoT機器が持っている機能で推測困難なシードを生成
機器の外部で生成した鍵は、漏えい時に漏えい元の特定が困難	機器の内部でシード、鍵を生成し、漏えいリスクを低減

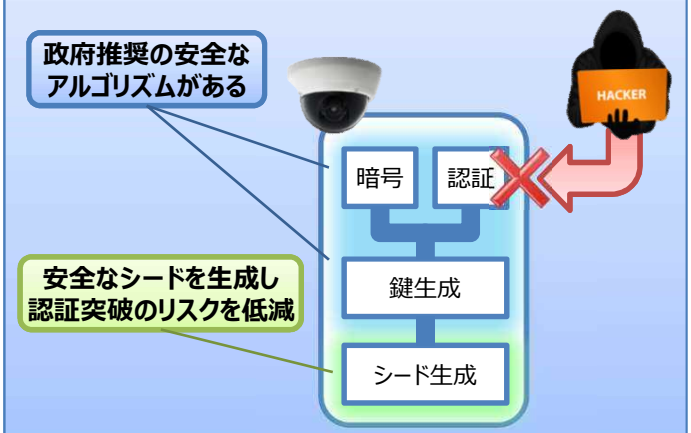
Before

シード値から暗号・認証鍵を推測され 暗号・認証を突破されるリスクがある



After

IoT機器内で生成した推測困難なシードから 鍵を生成し、安全な暗号・認証機能を実現



	ノイズ源 方式	ノイズ源 概要	メリット	デメリット
従来の手法	機器固有ID等	MACアドレス等を利用	・生成速度が速い ・コストアップがない	・設計者秘密から推測されるリスクあり
	/dev/random	割り込みを利用 (ブロッキング型)	・推測が難しい ・コストアップがない	・割込みが少なく生成速度が遅い
	/dev/urandom	割り込みを利用 (ノンブロッキング型)	・生成速度が速い ・コストアップがない	・推測されるリスクあり
	物理乱数生成器	専用ハードウェアを利用	・生成速度が速い ・推測が難しい	・専用ハードウェアのコストアップが発生
研究成果手法	HW/SWのゆらぎ	オシレータ、実行パイプライン、分岐予測ユニット、スケジューラ、キャッシュ等のゆらぎ利用	・生成速度が速い ・推測が難しい ・コストアップがない	・安全性の評価が必要

戦略的イノベーション創造プログラム（SIP）

【パナソニック】

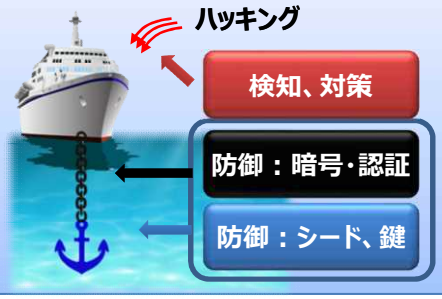
2－3 「防御」、「検知」、「対策」でエンドポイントを守るトータルサイバーセキュリティ

IoT向け対策技術

ネットワーク通信に加え、IoT機器のログを監視することで サイバー攻撃を早期に発見し、被害拡大を低減

① 求められるセキュリティ

ライフサイクルが長く、人が介在しないIoTでは、「防御」に加え、「検知」と「対策」も重要

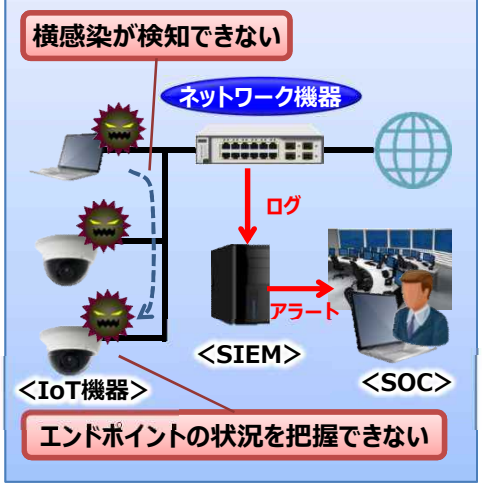


	ITセキュリティ	IoTセキュリティ
対　策	Windows Update ウィルスの隔離 等	サイバー攻撃対策
検　知	アンチウィルスソフト 等	
防　御	標準暗号通信 PKI認証	標準暗号通信 PKI認証

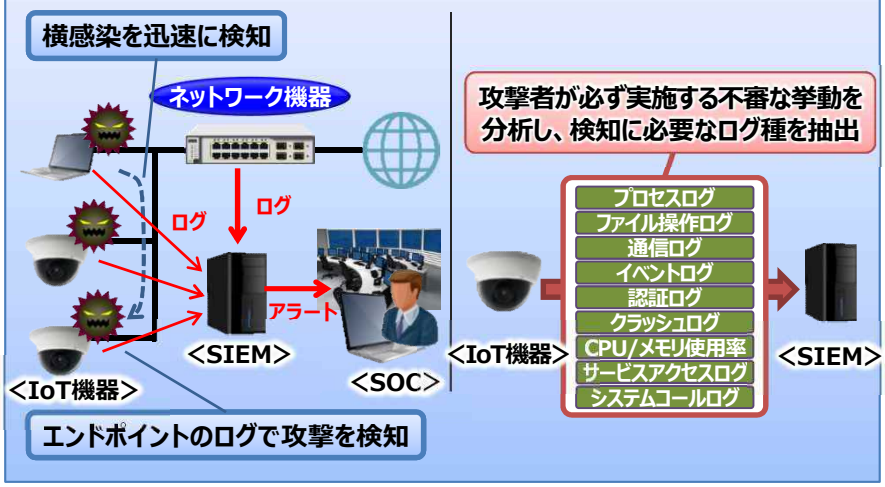
② サイバー攻撃対策：IoT機器のログを使って迅速に検知、対策

従来の課題　Before	導入による効果　After
ネットワーク内部の横感染が検知できない	IoT機器のログで、横感染を迅速に検知
IoT機器のログがなく、分析に時間がかかる	IoT機器のログを利用してインシデント対応工数を効率化
IoT機器からログ出力しても形式が多様で活用が難しい	ITと同じ形式でログ出力し、既存のSOCを活用

Before：ネットワーク機器のログを利用



After：IoT機器のログも利用



IoT機器から収集したログを利用することでインシデント時のSOC対応工数を削減