

ライフサイクルを通じたIoTデバイスの真正性確保

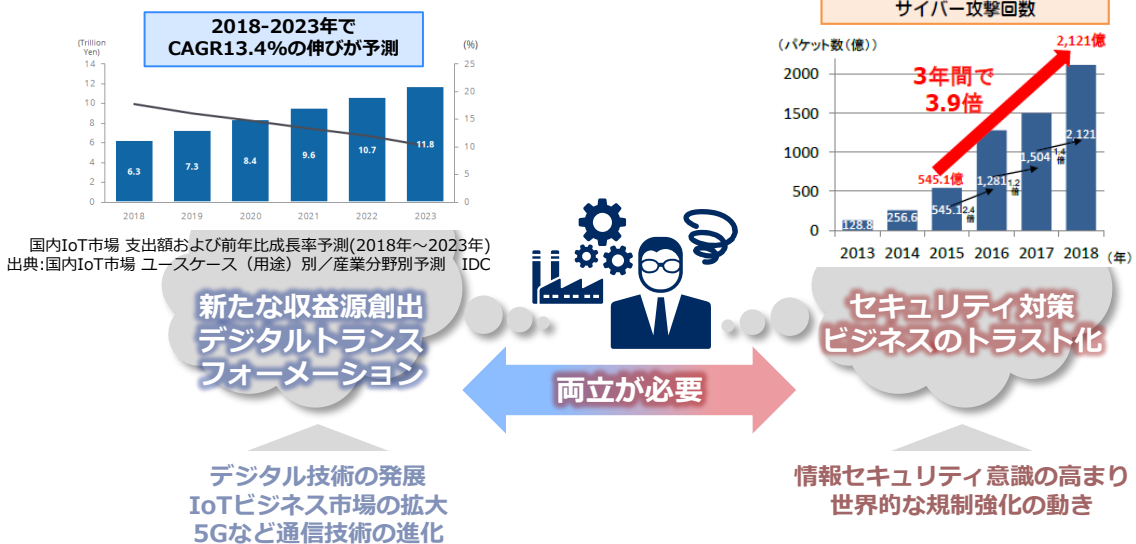
NEC IoT System Security Lifecycle Services

お客様のデジタルトランスフォーメーションを実現するセキュアなシステム構築に向けて、IoTデバイスの真正性を確保するセキュリティサービス、及びサービスを適用したエッジデバイスを提供します。

デジタルトランスフォーメーション実現に必要なセキュリティ対策とは

■セキュリティ対策と新たな顧客価値創出の両立の必要性

IoTが注目を浴び、さまざまなモノがネットワークへとつながり始め、デジタルトランスフォーメーションを通じた新しい顧客価値が様々な業界で創出されています。その中で利用されるデバイスはセキュリティ攻撃の標的とされるリスクも高まっており、製造段階からの網羅的かつ継続的な対策が必要な時代が到来しています。



対策のポイント

■デバイスの真正性を確保することが対策のカギ

現在、サイバー空間における脅威が深刻化しており、業界ごとにセキュリティに関わる標準規格やガイドライン(NIST SP 800シリーズ、IEC62443、CPSFなど(注))が示されています。これらの標準規格やガイドラインに沿ったデバイスのライフサイクルを通じたセキュリティ対策が重要となっています。その中で、IoTデバイスやデータが正しいものであるかの確認や、サイバー攻撃の発生とその原因を特定するための証拠を管理することも重視されています。



デバイスのライフサイクル

(注) NIST SP 800 シリーズ:

米国立標準技術研究所(NIST)が定めているセキュリティ対策基準

IEC62443:

制御システムの製造やオペレーションを行う企業がセキュリティに関して取り組むべき産業用オートメーション及び制御機器及び開発プロセスを対象とした国際標準

CPSF:

経済産業省がサイバー・フィジカル・システム(サイバー空間とフィジカル空間(現実世界)の双方に影響を与えるシステム)のセキュリティ対策に必要な概念、ポリシー、具体的なメソッドを体系的にまとめたフレームワーク

本サービスの概要

IoTセキュリティ

エッジデバイス管理

IoTセキュリティとエッジデバイス管理サービス、真正性が確保されたエッジデバイスを用いて、サイバー攻撃などの異常の早期検知とアラート表示を行い、ライフサイクル全体で高い信頼性を保持したセキュアなシステム運用を実現します。



1. IoTセキュリティ

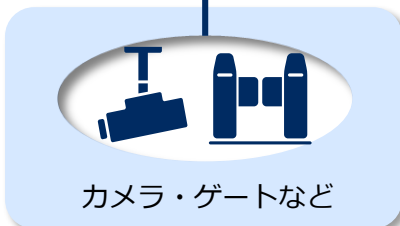
エッジデバイスに対する不正アクセス・データ改ざんなどの検知

2. エッジデバイス管理

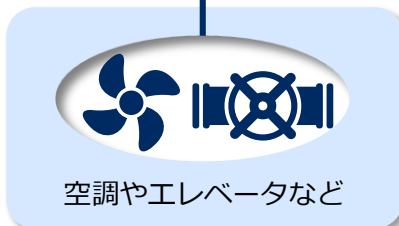
デバイス製造時に搭載済みの証明書認証機能を利用したなりすまし防止や異常なデバイスに対しての証明書無効化

3. ダッシュボード

証明書の期限切れや不正アクセスなどの異常をアラート表示



カメラ・ゲートなど



空調やエレベータなど



工作機械・制御装置など



活用例①顔認証入退



活用例②ビル設備管理



活用例③工場制御システム

対応エッジデバイス

NEC AI Accelerator

エッジ領域で省電力・高速処理を行い通信量・クラウド負荷を削減できます。また、セキュリティチップ上に証明書を書き込むことによって、信頼性の高いデバイス認証を行えます。



※その他、機能や価格、動作環境など詳細については、下記までお問合せください。

NEC デジタルプラットフォーム事業部

〒211-8666 神奈川県川崎市中原区下沼部1753

E-mail: til-pr@dpf.jp.nec.com

- 本紙に記載された社名、商品名は、各社の商標または登録商標です。
- 本製品の輸出(非居住者への役務提供等を含む)に際しては、外国為替及び外国貿易法等、関連する輸出管理法令等をご確認の上、必要な手続きをお取りください。ご不明な場合、または輸出許可等申請手続きにあたり資料等が必要な場合には、お買い上げの販売店またはお近くの弊社営業拠点にご相談ください。
- 本紙に掲載された製品は、改良のため予告なく仕様を変更することがあります。
- 本紙の一部、または全部を複写、転載、複製、引用することは禁じられています。