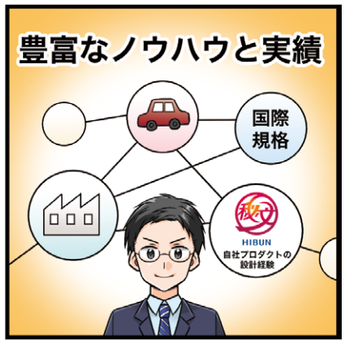
日立グループのものづくり・セキュリティ対策ノウハウを生かしコンサルティング

日立ソリューションズは、日立グループの一員として、製造業や重要インフラで培ったセキュリティ対策のノウハウや、自動車産業におけるセキュリティコンサルティング、IEC 62443などの国際規格を考慮したセキュリティ対策支援などの実績を多数持っています。また、情報漏洩防止ソリューション「秘文」をはじめとする自社プロダクトの設計経験なども豊富です。

IoT分野で培った知識や技術で、限られたリソースでどこまでのセキュリティ対策が必要かといった設計の支援や、既存・開発中のIoT機器・システムで不足している対策についてピンポイントで提案します。また海外のお客様向け製品への対応など、お客様のニーズに合わせた柔軟な対応が可能です。

自社のIoT製品のセキュリティ対策について不安があり専門家に評価してほしい、万が一セキュリティ事故が起きた際に、自社のセキュリティ対策について説明できる自信がない、これから自社機器のIoT化を推進していくなど、セキュリティ対策のノウハウを必要とされるお客様は、日立ソリューションズにご相談ください。



IoT機器のセキュリティ対策でお悩みの方は ぜひ、日立ソリューションズにご相談ください。

製造業や重要インフラで培ったセキュリティ対策の 豊富なノウハウを生かし、IoT機器のセキュリティ設計を支援

IoT機器のセキュリティ対策を、セキュリティ製品開発者の目線で
開発段階から支援。さまざまな課題を洗い出し、
システム全体を考慮した対策をコンサルティングします。

セキュリティ設計支援コンサルティング
www.hitachi-solutions.co.jp/security_consul/sp/iot_consul.html

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/column/shion/vol15/

C21K-01-00 | 2021.05

HITACHI
Inspire the Next

IT探偵しおんが解決! 企業潜入調査物語

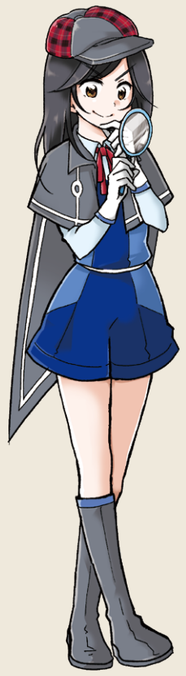
IoT機器のセキュリティ対策、設計から支援します

プロローグ

都内某所に、ITを駆使して企業の悩みを解決するという、特別な探偵事務所がある。
そこで働くエリートIT探偵の「伊野部しおん」は、企業が悩むセキュリティや業務効率化の課題を次々と調査・解決していく。

伊野部（いのべ） しおん

IT探偵事務所に勤めるエリート探偵。3年前までは某企業のスーパーエンジニアだったらしい。
依頼先の関係者に変装をしてITの課題を探し出して解決していく変装調査型の仕事を得意とする。



登場人物

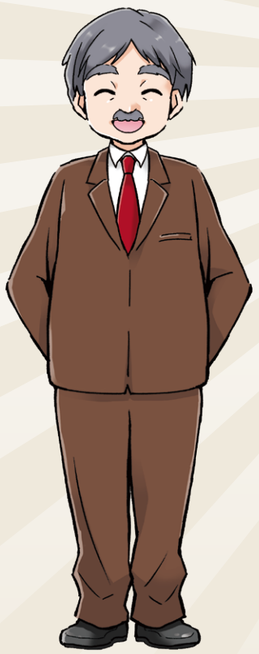
相央（あいおう） 哲夫（てつお）

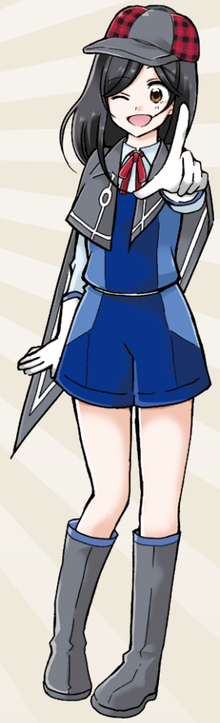
産業機器メーカー開発担当者。開発技術についての知識は豊富だが、セキュリティについての知見はあまりない。IoT化が進むにつれセキュリティの重要性は分かっているつもりだが、どうしていいか分からない。

曾柳（そりゅう） 好男（よしお）

IT探偵事務所所長兼取締役を務める社長。さまざまな企業に監査などの内部調査を依頼され、しおんを送り込んでは企業課題を解決させている。

IoT機器のセキュリティ対策、
設計から支援します





1T探偵しおんが解決！

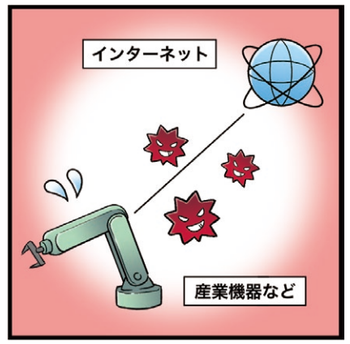
コネクテッドカー、IoT対応の産業用機器・医療用機器――これまでスタンドアロンやクローズドなネットワーク環境でしか使われてこなかった組み込み機器が、オープンなインターネットに接続される、いわゆるIoT化が急激に進みつつあります。
IoTは機器の利便性や保守性、可用性を高める一方で、インターネットに接続されるがゆえにサイバー攻撃の矢面に立つことになります。実際にIoT機器に対するサイバー攻撃は始まっており、産業用ロボット・工作機械・医療機器などが狙われ、大規模な被害が発生しています。
このような状況の中、欧米では導入・調達される機器に、セキュリティ設計フレームワークへの準拠やIEC 62443のような産業セキュリティ認証を求める流れになりつつあります。しかしながら、これまで産業用機器・医療用機器の中には、インターネットに接続することが想定されていなかったため、開発段階でサイバー攻撃に対するセキュリティが重視されていなかったものも多く、十分な対策が取れているか不安だという技術者の方も多いでしょう。
日立ソリューションズは、セキュリティ設計でお困りの設計者の方々を対象に、日立グループのセキュリティノウハウをもとにした、「セキュリティ設計支援コンサルティング」を提供しています。

狙われるIoT機器の脆弱性に、欧米では規制を強化

組み込み機器のIoT化は、クラウドを使った統合管理や、遠隔管理・操作などにより、機器の利便性や、新たな活用方法、そしてリモート監視・保守、予防保守による可用性の向上など、さまざまなメリットがあります。

その一方で、組み込み機器がインターネットに接続されたことにより、サイバー攻撃の標的となる可能性が高まっています。実際、2010年ごろからIoT機器を狙ったプラントやシステムなどへのサイバー攻撃は増加傾向にあり、大きな被害が出ている事例もあります。また大規模なものとしては2016年にWebカメラなどを狙ったマルウェア「Mirai」による攻撃があります。

このような状況を受けて、欧米では組み込み機器のセキュリティ対策を強化する動きを見せています。米国ではNIST（米国国立標準技術研究所）を中心にIoT機器に関する設計フレームワークを次々と策定。また欧州でもENISA（欧州ネットワーク情報セキュリティ庁）が中心となって、欧州サイバーセキュリティ認証フレームワークの創設に向けて活発な動きを見せています。これらの動きを背景に、欧米では採用・調達にあたって、セキュリティフレームワークへの準拠や、制御システムのセキュリティ標準であるIEC 62443に対応していることを条件にする企業などが増えてきています。

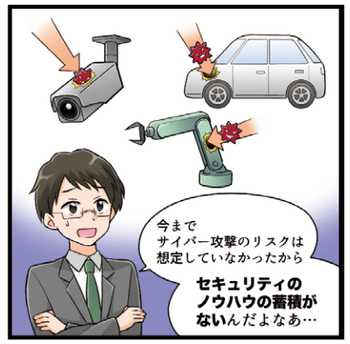


NIST:National Institute of Standards and Technology
ENISA:European Network and Information Security Agency

難しいIoT機器のセキュリティ対策

このように、これまで以上のセキュリティ対策を求められているIoT機器開発ですが、ハードルの1つが、設計部門の開発ノウハウです。これまでのスタンドアロン環境、クローズドネットワーク環境では、サイバー攻撃を受けることが想定されていなかったため、セキュリティ設計のノウハウが蓄積されていないケースもあります。このため、脆弱性に対する対策が十分ではない可能性が高くなっています。

また、IoT対応のためのハードウェアやソフトウェアを外部のベンダーから購入して、自社の機器に組み込んでいる場合、サプライチェーンのセキュリティ脅威と向き合うことになります。これは、購入したコンポーネントが持つ脆弱性によって、サイバー攻撃の被害に遭うリスクがあるということです。2020年にはイスラエルのサイバーセキュリティ企業が「Ripple20」と呼ばれるIoT機器の脆弱性を発見しました。これは米国のベンダーが1990年代後半にリリースしたソフトウェアに起因するもので、このソフトウェアを使ったIoT機器は数百万台とも数億台とも言われています。外部ベンダーのコンポーネントはブラックボックス状態であることが一般的ですから、サプライチェーンのセキュリティ脅威への対応は容易ではないことがご理解いただけるでしょう。



日立ソリューションズのコンサルタントが、IoT機器のセキュリティ対策を支援

このように、IoT機器のセキュリティ対策には多面的なアプローチが必要ですが、ノウハウ・経験が少ないメーカーにとっては難しい課題です。さらに、セキュリティを考慮した設計を行うとしても、製品のリソースやコストに制約があるIoT機器のハードウェア・ソフトウェアに対して、どこまでセキュリティ対策をすればよいのか、どのようなセキュリティ対策をしておけば客観的に説明ができるのか悩まれている企業も少なくないでしょう。

これらの課題を解決するため、日立ソリューションズでは「セキュリティ設計支援コンサルティング」を実施しています。日立ソリューションズのコンサルタントが、製品開発者の目線でシステム全体のセキュリティを考えて、開発段階からIoT機器、IoTシステムのセキュリティ対策を支援します。セキュリティの課題を洗い出し、対策をコンサルティング可能です。また、ステークホルダーに対して客観的に対策を講じていることを説明できるように支援します。