さらに、トータルで制御システムを守るワンストップソリューションも

もちろん、現状分析だけではなく、対策の実施も必要です。実際に適切なセキュリティ製品の導入やシステム構築を実施し、監視によるシステム異常の早期発見、また状況に応じて新たな脅威にも継続的に対応していく必要があります。

日立ソリューションズでは、制御システムセキュリティのコンサルティングから運用までをワンストップで行う「制御システムセキュリティソリューション」を提供。長年にわたり培ってきた制御システムに対する知見を生かし、「可用性第一」のセキュリティ対策をトータルで提供します。ホワイトリスト方式のマルウェア対策ソリューションや不正侵入検知ソリューションなど、さまざまな製品・ソリューションを用意しています。レガシーOSなど制御システム特有の環境でも、既存システムへの影響を抑えて導入可能なセキュリティ対策を提案可能です。

IoTや汎用OSの利用、ネットワーク連携など、ますます拍車がかかる制御システムのオープン化。それに伴うセキュリティリスクに対抗するために、「セキュリティ現状分析サービス」や「制御システムセキュリティソリューション」の導入を検討してみてはいかがでしょうか。

制御システムのセキュリティについては
お気軽にご相談ください。

制御システムセキュリティソリューション

ネットワークプロトコルなどの標準化や情報ネットワークとの部分的な連携に伴い、
サイバー攻撃などの脅威にさらされている制御システム。
まずは、制御システムセキュリティの国際規格 IEC 62443 に基づいて
セキュリティ要件をチェックする、セキュリティ現状分析サービスが効果的です。
分析後の対策として、セキュリティ製品の導入や、
運用・監視までトータルに支援します。

詳しくは製品情報サイトへ　制御システムセキュリティソリューション　検索
www.hitachi-solutions.co.jp/security/sp/solution/task/seigyo-sec.html

必要なのは、可用性を重視したセキュリティ対策

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/vol6/

C18S-02-01　2018.12

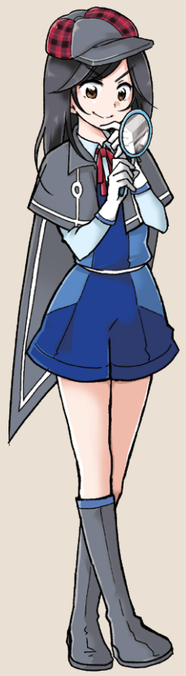
HITACHI
Inspire the Next

IT探偵しおんが解決! 企業潜入調査物語

低コストかつ短期間で!制御システムのセキュリティを専門家が簡単分析!

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。



登場人物

伊野部 しおん（いのべ）

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。

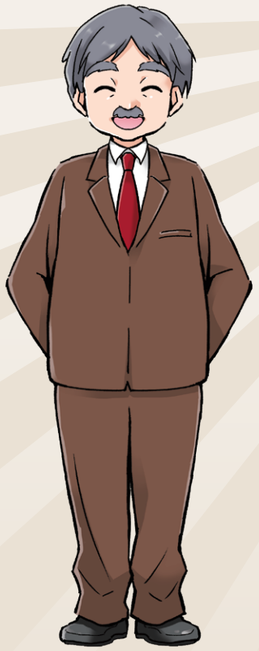
杏丁 健介（あんてい けんすけ）

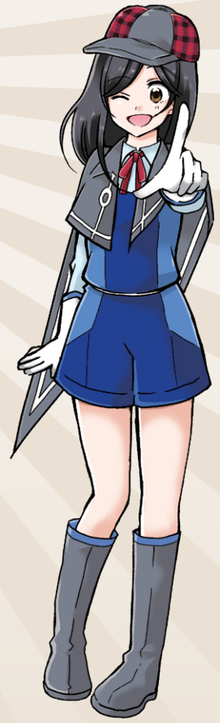
大手企業のIT部門のエースとして活躍し一度は独立したものの父の会社を継ぐために△△製造会社に戻ってきた。趣味は映画鑑賞と散歩で最近はバードウォッチングも始めている。

曾柳 好男（そりゅう 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。

低コストかつ短期間で!
制御システムのセキュリティを専門家が簡単分析!





IT探偵しおんが解決!

生産性の向上などを目的として、制御システムの世界にもIoTなどによるシステムのオープン化が進みつつあります。
制御システムの各機器をネットワークでつなぐことで、生産機器・設備からのデータ取得によるメリットが多い半面、これまでネットワーク接続を意識していなかったこともあり、セキュリティリスクへの十分な対策が多くの企業で行われていない、という現状もあります。日立ソリューションズの「制御システム向け セキュリティ現状分析サービス」は、このような制御システムにおけるセキュリティの現状把握と分析を簡単かつ低コストで実施し、今後のセキュリティ対策検討に役立つ情報を提供します。

制御システムにもサイバー攻撃リスクが増加

従来、設備や機器を制御するシステムは、基本的にスタンドアロン、もしくは閉鎖ネットワーク（クローズドネットワーク）で利用されており、情報ネットワークとは隔離されていました。さらに、独自のOSやプロトコル、アプリケーションによって環境が構築されていたため、外部からの攻撃は受けにくい状況でした。

しかし、近年のIoTに代表される生産効率向上の動きに伴い、これら制御システムのオープン化が進んでおり、さらにインターネットに接続されるケースもあります。

これまでは、生産ラインにおける生産個数の指定や各処理の指示は、工場の作業員が手動で操作していましたが、生産管理システムとの連携など部分的な情報ネットワークへの接続により、人の手を介さずにすべて自動で制御、生産状況の把握を行うといった変化が見られます。また、Windowsなど汎用OSの利用やプロトコルの標準化などによって、以前に比べ、攻撃者が制御システムに攻撃を仕掛けやすい環境になりつつあり、情報システムと同様に、サイバー攻撃などのセキュリティリスクがあります。

実際、国内外で攻撃を受けた制御システムもあり、その結果、マルウェア感染による生産ラインの停止や生産設備の故障など、実被害を受けている企業も出てきています。また、制御システムは社会インフラを支えるシステムも多く、電力の停止や爆発事故など、攻撃された企業の損害だけでなく、社会的混乱や人命にかかわる事態につながる可能性もあり、セキュリティ対策は重要です。

制御システムのセキュリティ対策、どこから手をつければよいのか

多くの企業で制御システムの保守管理を行っているのは、製造部門です。製造部門は、日頃から運用を行っている制御システムに対する知見は豊富ですが、ネットワークやセキュリティ対策など、これまでの担当範囲外の領域に対する知見は必ずしも十分とは言えません。また、セキュリティは製造部門ではなく情報システム部門の管轄とする企業もあります。情報システム部門も制御システムに対する知見がないなど、セキュリティリスクが高まっていることは理解しつつも、どこから手をつけて、どのように対策すればよいのかわからないという担当者も多いでしょう。また、制御システムにセキュリティ上の問題があっても、担当者が気づいていない場合も多くあります。

では、どのように制御システムのセキュリティ対策を進めていけばよいのでしょうか。その第一歩としてお薦めしたいのが、現状のシステムのセキュリティ状況を把握するということです。さまざまなセキュリティ脅威に対して、自社の制御システムがどのような弱点を持ち、どのような対策を打てばよいのか。まずはこれを把握することが、対策を進めていくうえで重要です。

まずは簡易的なセキュリティ現状分析を

制御システムのセキュリティリスクが高まっていることもあり、近頃ではさまざまなセキュリティの分析サービスが提供されています。これらのサービスは、詳細にセキュリティの調査と分析を行うため、非常に精度が高いのですが、コストや時間が掛かるデメリットもあります。

そこで、日立ソリューションズでは、概略の調査分析を行う「制御システム向け セキュリティ現状分析サービス」を提供しています。この「セキュリティ現状分析サービス」では、制御システムのセキュリティを現地視察やヒアリングベースで診断。その結果を15の対策カテゴリに分類してレーダーチャート化し、セキュリティレベルを100点満点で点数化したものをレポートとして報告します。対策カテゴリには、USBメモリやモバイル機器などの接続に関する「利用制御」や、PC・サーバーへのマルウェア感染防止の対策状況をチェックする「マルウェア対策」などがあります。また、カテゴリごとの評価や、対策案の提示も行っています。

概略調査とは言え、制御システムセキュリティの国際規格であるIEC62443に基づいた診断を行いますので、対策の方針を決める段階では十分なレポートとなっています。