HITACHI
Inspire the Next

News Release

2019年6月5日
株式会社日立製作所

日立の工場現場で培ったノウハウを活用し、事業の継続性を重視したリスク分析を実現する「工場向けサイバーBCP リスクアセスメント」を提供開始

幅広い工場向け IoT セキュリティソリューション群によりお客さまの工場の安定稼働を支援

株式会社日立製作所(執行役社長兼 CEO:東原 敏昭/以下、日立)は、日立の工場で実際に適用してきたセキュリティ対策のノウハウを用い、事業の継続性を重視したリスク分析を実現するコンサルティングサービス「工場向けサイバーBCP*1 リスクアセスメント」を、製造業および重要インフラ事業者向けに6月11日より提供開始します。

日立はこれまで、社内外で得られた知見やノウハウをもとに、「現状把握」、「多層防御・検知」、「運用・対処」の3つのステップでお客さまのセキュアな工場を実現する幅広い工場向け IoT セキュリティソリューションを提供してきました。本サービスは、その中で特に、工場の IoT 化に伴うセキュリティ対策において重要な「現状把握」のサービスを強化するものです。

本サービスでは、IEC 62443*2 などの制御システムの国際標準規格に関する高い専門性を有する日立のコンサルタントが、工場現場へのサイバー攻撃による事業停止リスクを分析し、事業継続のために必要なセキュリティ対策を提案します。これにより、制御システム特有のセキュリティリスクを効率的に洗い出すとともに、幅広い工場向け IoT セキュリティソリューション群と組み合わせて提供することで、お客さまの工場の安定稼働を支援します。

*1 BCP(Business Continuity Plan):企業が自然災害や大火災、サイバー攻撃などを受けた場合に、被害を最小限にとどめ、早期復旧を図るために、平常時や緊急時の事業継続するための方法・手段を取り決めておく計画のこと。
*2 IEC 62443:産業制御システムを対象に、マネジメントや制御システム、制御用コンポーネントのセキュリティ要件を規定する規格群。

近年、IoT の進展に伴い、工場内のあらゆる機器を外部ネットワークとつなぎ、データを収集・分析して生産効率を上げる取り組みが増えています。一方、サイバー攻撃により、電力や水などの社会インフラや工場現場の生産ラインが停止するといったインシデントが国内外で多数発生し、深刻な社会課題となっており、外部ネットワークとの接続を想定していなかった工場においては、新たに必要となるセキュリティ対策が分からないといった課題に直面しています。

日立は、IEC 62443 の国際標準化活動や H-ARC*3 コンセプトに基づく国際的な啓発活動、国内のセキュリティガイドライン策定へ参画してきた実績をもち、これらの活動で得られた豊富な知識やノウハウをもとに、自社工場の制御システムにおいてさまざまなセキュリティ対策を実施してきました。

*3 H-ARC:工場や重要制御システムの事業継続を目的に4つの軸(Hardening, Adaptive, Responsive, Cooperative)によるセキュリティ評価を推奨する考え

今回提供開始する「工場向けサイバーBCP リスクアセスメント」は、サイバー攻撃によるお客さまの工場現場の事業停止リスクを分析し、事業継続性を重視した実効性の高い改善計画を提案します。

具体的には、日立独自の診断ツールを用いて、効率的にお客さまの工場のセキュリティレベルを把握し、診断結果をもとにお客さまのセキュリティリスクを見える化することで課題を洗い出します。ひとたび稼働停止するとサプライチェーン全体にまで波及するなど影響が大きく、事業の継続性を重

視した対策が求められる工場システムに対し、社内外の工場で培ったノウハウや実績を生かし、BCP 観点での現場の改善策のみならず、組織体制の確立や運用環境の整備といった実効性の高いセキュリティ対策を提案し、その策定を支援します。

また、現場ごとに異なる環境に応じてカスタマイズした診断ツールにより、定期的な自己診断といったお客さま自身による継続したチェック・改善が可能となり、お客さまの事業継続に寄与するほか、セキュリティスキルの維持・向上に向けた教育カリキュラムの策定支援や教育講座の提供も行います。

日立はこれまで、社内外で得られた知見やノウハウをもとに、「現状把握」、「多層防御・検知」、「運用・対処」の 3 つのステップでお客さまのセキュアな工場を実現する、工場向け IoT セキュリティソリューションを提供してきました。本サービスは、特に、工場の IoT 化に伴うセキュリティ対策において重要な「現状把握」のサービスを強化するもので、制御システム特有のセキュリティリスクを効率的に洗い出すとともに、工場現場の実態を考慮した実効性の高い対策の立案や実行施策の提案をします。また、サイバーセキュリティのみならず、フィジカルセキュリティまで網羅した幅広い工場向け IoT ソリューション群の中から、お客さまのニーズに合った最適な製品・サービスを組み合わせ、ワンストップで提供することで、お客さまの工場の安定稼働を支援します。

日立は、今後もセキュリティに関する最新動向を反映した対策を自社工場に適用していくとともに、その実績・ノウハウをコンサルティングサービスへとフィードバックしていくことで、お客さまの工場のセキュリティ対策強化に貢献していきます。

■工場向け IoT セキュリティソリューションの概要

■「工場向けサイバーBCP リスクアセスメント」の特長

1. 日立のノウハウの活用により、効率的に工場のセキュリティレベルの把握が可能

日立の工場で策定・運用しているセキュリティガイドラインのノウハウを反映した診断ツールを利用することで、効率的にお客さまの工場のセキュリティレベルを診断することが可能です。これにより、お客さまの工場現場のセキュリティリスクを見える化し、対策が必要となる箇所を迅速に洗い出し、対策立案に繋げることができます。

2. お客さまの環境に合わせた実効的な改善計画の策定が可能

本サービスで用いる診断ツールは、IEC 62443 や NIST サイバーセキュリティフレームワーク*4 といった世界中で適用されている規格群に準拠しているほか、それらではカバーしきれない BCP における制御システム特有のセキュリティリスク観点についても、日立独自の視点を取り込んだ網羅的な構成となっています。

工場の現場を熟知し、制御セキュリティに関する豊富な知識を持つコンサルタントが、多種多様な項目の中から、お客さまの現場に必要となる項目を備えた診断ツールを作成・提供します。現場担当者が実行可能な運用環境の整備など改善計画の策定を提案し、現場のセキュリティレベルの向上を図るだけでなく、セキュリティマネジメント体制の確立についても支援します。

*4 NIST サイバーセキュリティフレームワーク：米国 NIST (National Institute of Standards and Technology)が規定するサイバーセキュリティに関する規定集

3. お客さま自身による継続的なチェック・改善とセキュリティスキルの維持・向上に貢献

お客さまごとにカスタマイズされた診断ツールは、システム自体に関する項目のみならず、その運用やマネジメントに関する項目までカバーしており、繰り返し利用することができます。定期的な自己診断に活用し、新たに発見したリスクに対する改善策の立案につなげるなど、お客さま自身による継続的なチェック・改善を実現し、お客さまの事業の継続に寄与します。

また、セキュリティスキルの維持・向上のため、現場担当者からネットワーク管理者、経営幹部まで対象とするセキュリティ教育のカリキュラム策定を支援します。さらに、お客さまの要望に応じてセキュリティ教育講座やセキュリティ演習、訓練施設を使った総合訓練を提供することも可能です。

■「工場向けサイバーBCP リスクアセスメント」の価格および提供開始時期

メニュー	内容	価格	提供開始日
セキュリティ詳細リスク評価	IEC 62443、各種ガイドラインなどに基づく、お客さまのシステムの網羅的なリスク評価	個別見積り	2019 年 6 月 11 日
セキュリティベースライン リスク評価	セキュリティの重要項目を中心としたお客さまのシステムのリスク評価		
セキュリティ自己診断支援	セキュリティ診断ツールの提供		
セキュリティ教育策定支援	対象者の業務内容に応じたセキュリティスキル教育カリキュラム策定支援と教育講座の提供		

■日立の工場向け IoT セキュリティソリューションに関するウェブサイト

http://www.hitachi.co.jp/security-iot/

■「日立セキュリティフォーラム 2019」での紹介について

「工場向けサイバーBCP リスクアセスメント」を含む、工場向け IoT セキュリティソリューションの全体像は、日立が 2019 年 6 月 11 日(火)に、虎ノ門ヒルズフォーラムで開催する「日立セキュリティフォーラム 2019」にて、セミナーおよび展示を行います。

https://www.hitachi.co.jp/sss/

■本件に関するお問い合わせ先

株式会社日立製作所　日立セキュリティ総合窓口

http://www.hitachi.co.jp/security-inq/

以上