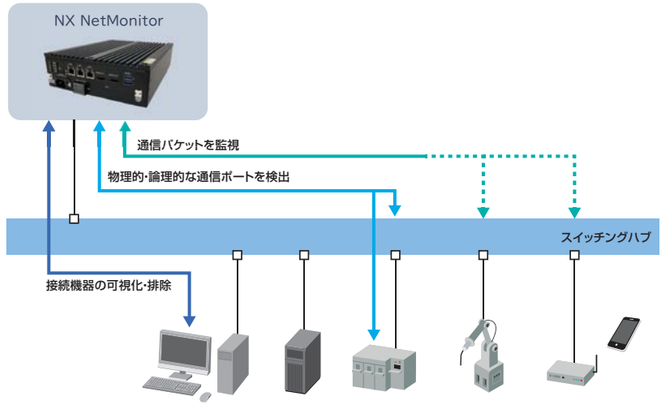
制御システムに適した日立のセキュリティ対策装置

ネットワーク可視化&不正機器排除装置「NX NetMonitor」

ネットワークを可視化し、不正な通信の検知および不正機器接続を防止

ネットワーク内の通信や機器を監視し、稼働状況の可視化や、不正機器をネットワークから排除することでセキュリティを確保します。



機器の検出&不正機器排除

クライアントソフトウェアが不要。他端末に影響を与えずに不正機器をネットワークから排除可能

通信ポートの検出(オプション)

機器の接続・通信ポートを物理的・論理的に記録。既存の通信ポートを登録し、変化を検出することも可能

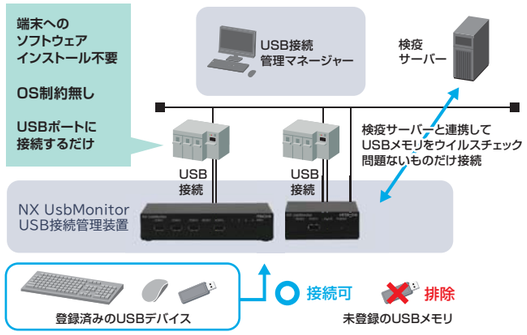
通信パターンの検出(オプション)

通信パケットを監視・記録。異常パターン発見時の通知も可能

USB接続管理装置「NX UsbMonitor」

不正なUSBメモリ利用による ウイルス侵入や情報漏えいを防止

後付けで、未登録のUSBメモリの使用を制限する装置です。装置と端末は取り外し防止機構で物理的に固定し悪用を防止します。USBメモリの使用状況のログは監査に利用できます。検疫サーバーと連携することでより安全にUSBメモリを使用できます。



一方向中継装置「NX Oneway-Bridge」

片方向の通信を物理的に遮断し 外部からの不正アクセスを防止

片方向の通信を物理的に遮断することで、外部からの悪意のあるアクセスを防止。内部のデータは外部に対してより安全に送信できます。ソフトウェアレスで設定項目もなく、パッチ適用漏れや誤った設定による脆弱性は生まれません。

⚠ 安全に関するご注意	正しく安全にお使いいただくため、ご使用の前に必ず「取扱説明書」、「使用上のご注意」などをよくお読みのうえ、おまもりください。

●カタログに記載の仕様は、製品の改良などのため予告なく変更することがあります。 ●製品の色は印刷されたものですので、実際の製品の色調と異なる場合があります。
●本製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。
なお、ご不明な場合は、当社担当営業にお問い合わせください。

製品に関する詳細・お問い合わせは下記へ

■ 製品情報サイト・インターネットでのお問い合わせ
https://www.hitachi.co.jp/security-control/

株式会社 日立製作所　制御プラットフォーム統括本部

SP-012　2022.4

社会インフラ向け 制御システムセキュリティ

HITACHI
Inspire the Next

社会インフラ向け 制御システム セキュリティ

社会インフラの事業継続を支え続けてきた日立の知見を制御システムのセキュリティへ。

制御システムにさまざまなIoT機器やネットワークがつながり、制御システムもセキュリティの脅威にさらされている今、万が一社会インフラが停止すると世の中に多大な影響が及びます。電力・鉄道・ガス・水道など長年にわたり社会インフラの制御システムを構築・運用してきた日立は、セキュリティを検討する国際規格団体や委員会などとの連携を推進。確かな知見に基づき制御システムのセキュリティ確保に加えて、事業継続の視点を兼ね備えたトータルなソリューションを提供します。

IoT:Internet of Things

DX環境の社会インフラを守るのは、制御システムを知る日立のセキュリティ。

制御とITの豊富な知見でDXに伴う新たな脅威に対応

長年にわたる社会インフラ構築で蓄積した制御、IT、コンポーネントベンダーとしての豊富な知見でDXに対応したセキュリティ対策を支援。

当社工場のDX環境下でのセキュリティ運用実績

当社工場のDX環境下にある制御システムにおいてセキュリティ機能実装および事業継続対策を運用。そこで得たノウハウをお客さまに適用。

DXを見据えたOT/IoTセキュリティの標準化を推進

国際規格団体とともに、拡大するDXなど最新の動向を踏まえたOT/IoTセキュリティの普及活動を推進。

OT:Operational Technology

先進のデジタル技術を活用したセキュリティソリューションの開発

当社の研究所において、先進のデジタル技術を活用し、DXに対応した多彩なセキュリティソリューションを開発。

組織・運用・システムで守る日立のアプローチ、H-ARC。IECおよびIICのホワイトペーパーに採択されています。

日立は、お客さまの安全・安心を実現するため、「組織で守る、システムで守る、運用で守る」というセキュリティ提供のアプローチを取ります。セキュリティ対策のためのシステム構築はもちろん、対策の効果を継続的に維持するための組織マネジメントシステムや、異常なふるまいを監視、検知する運用方策をあわせて提供します。

IEC:International Electrotechnical Commission　IIC:Industrial Internet Consortium

H-ARC

Hardening：強靭性（システムの強靭性）
Adaptive：適応性（脅威やシステム変化に対する持続的適応）
Responsive：即応性（攻撃への迅速な対応）
Cooperative：協調性（脅威への連携した対応）

IEC White Paper "Factory of the future"
http://www.iec.ch/whitepaper/futurefactory/

IIC "Industrial Internet of Things Volume G4: Security Framework"
https://www.iiconsortium.org/IISF.htm

サイバー攻撃に対する防御に加え、インシデント発生時の事業継続への対応と事前計画づくりをサポートします。

DX導入時のセキュリティ方針を決めたい。

「DX環境下でどう対策すればいいのかわからない」
「DXを見据えた国際・業界標準に準拠したい」
「効果的な社員教育を実施したい」
「制御システムで実績があるセキュリティを実施したい」

→ セキュリティコンサルティングサービス P3

新しいセキュリティリスクを考慮したセキュリティ対策を導入したい。

「DX環境下で刻々と変わるセキュリティ状況を見える化したい」
「どのような機器が接続されているのか把握したい」
「ネットワークで不正な通信が行われていないだろうか」

→ セキュリティ対策導入支援ソリューション P4

DXに伴う新たなセキュリティ脅威にも迅速に対応したい。

「24時間365日の監視体制の確保が難しい」
「DX環境化でインシデントを高度に監視・分析できる人財に乏しい」
「セキュリティ健全性を定期的にチェックしたい」

→ セキュリティ監視・分析支援サービス P5

DXに伴う新たなサイバー攻撃に備えて組織体制を強化したい。

「サイバー攻撃を受けた時の組織的な対応方法を学びたい」
「故障とサイバー攻撃による異常の違いがわからない」
「DXに伴う新たな脅威に備え実践的な訓練を受けたい」

→ サイバー防衛訓練サービス P6

セキュリティコンサルティングサービス

事業継続を第一に、DXによる将来像まで見据えて幅広い対策をさまざまな段階から支援します。

DXによるシステムの将来像を考慮しながら現状調査と評価を実施。制御システムを維持し、事業を継続するために必要なセキュリティ対策を、システム、人材、組織運用を含む幅広い視点から立案します。

事業レベルとシステムレベルで、調査から対策立案まで。

事業レベルとシステムレベルの２つの側面から、リスク識別を行い、それぞれのリスクを評価。その結果を踏まえ、システム、人材、組織運用を見据えたリスクマネジメントをご提案します。

リスク識別

- 事業レベルリスク分析（事業影響度分析）
  - 事業活動とマネジメントシステム調査
- システムレベルリスク分析
  - 制御システム調査

リスク評価

- 事業レベルのリスク評価
- システムレベルのリスク評価

リスクマネジメント（対策立案）

- システム
  - システム対策支援
- 組織運用
  - ポリシー・基準策定支援（事故対応フロー、サプライチェーン対策）
  - 人財育成施策立案
  - 組織の運用設計支援

国際規格・ガイドラインを考慮したコンサルテーション、または準拠の支援

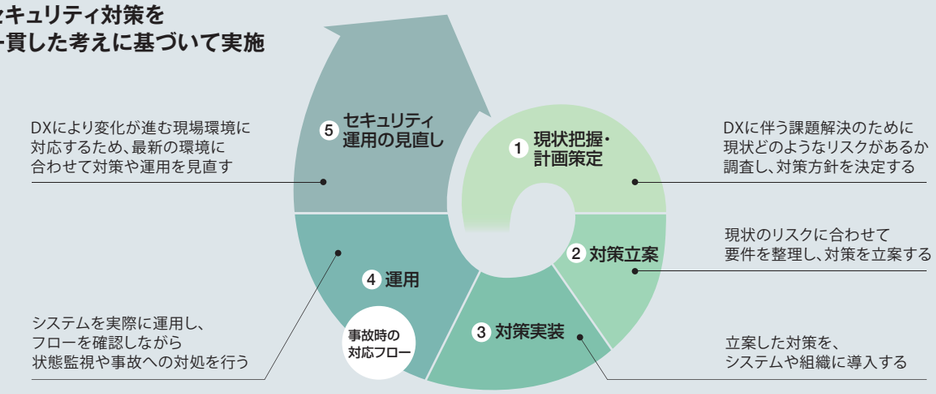
国際標準規格（IEC 62443ほか）、電力制御システムセキュリティガイドラインなど

IEC:International Electrotechnical Commission

制御システムセキュリティへのアプローチ

制御システムにおけるDXの推進、IoT・クラウド活用では、計画の初期からセキュリティを検討し、段階的に実施するのが効率的です。日立は制御システムの導入・運用を視野にいれた、ライフサイクルに沿った堅牢なセキュリティ対策の立案と実現をコンサルティングサービスにより支援します。

セキュリティ対策を一貫した考えに基づいて実施



セキュリティ対策導入支援ソリューション

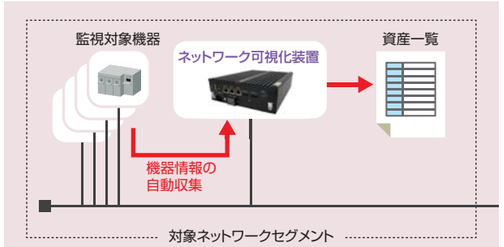
DXにより状況が変化する制御システムを脅威から守り続ける対策の導入を支援します。

制御系ネットワークにどのような機器がつながっているのか、ネットワーク内や外部とどのような通信を行っているのか、などDX環境下で刻々と変化するセキュリティ状況を監視する基盤を実現。制御システム内の機器の外部からの一元監視も支援します。

資産可視化

ネットワークに接続されている機器の洗い出しを実施。

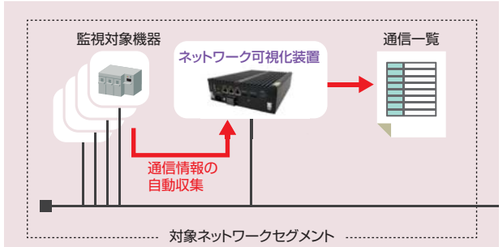
ネットワーク可視化装置の提供機能を利用して、対象ネットワークセグメント内に導入されている資産の洗い出しを実施します。



通信可視化

各機器がどのような通信を行っているのかを明確化。

ネットワーク可視化装置の提供機能を利用して、資産可視化によって洗い出された各機器がどのような通信をしているのかを明らかにします。



セキュリティ対策インテグレーション

DXと制御システムのノウハウを生かしたセキュリティインテグレーションを提供

資産と通信の可視化で得られた情報を活用し、生産系、情報系の各ゾーンを考慮しながら、制御システムの設計から機器選定・導入までの効果的なセキュリティ対策を支援します。

現場の機器を管理したい

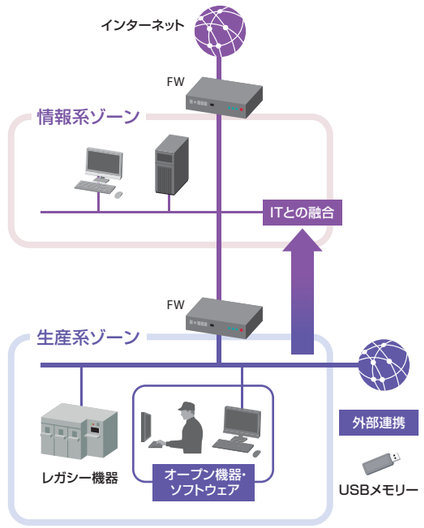
オープン機器の増加でリスクが高まる現場機器の管理を、後付けできる方法で強化したい

機器の接続監視・不正機器排除
（NX NetMonitor）

レガシー機器が現場にあるが更新できない

現場に設置したレガシー機器について、後付けできる方法でセキュリティ対策を強化したい

制御用IDSによる通信監視
（NX NetMonitor　IDSオプション）



現場機器の稼働状況を外部から知りたい

機器の稼働情報を外部に発信したいが、外部からの不要なアクセスは防ぎたい

一方向通信制御
（NX Oneway-Bridge）

メンテナンスでUSBメモリーを使い続けたい

外部から持ち込まれるUSBメモリーまたは管理不十分なUSBメモリーからのウイルス感染を防ぎたい

USBデバイスの接続監視・不正USB排除
（NX UsbMonitor）

FW:Firewall　IDS:Intrusion Detection System

セキュリティ監視・分析支援サービス

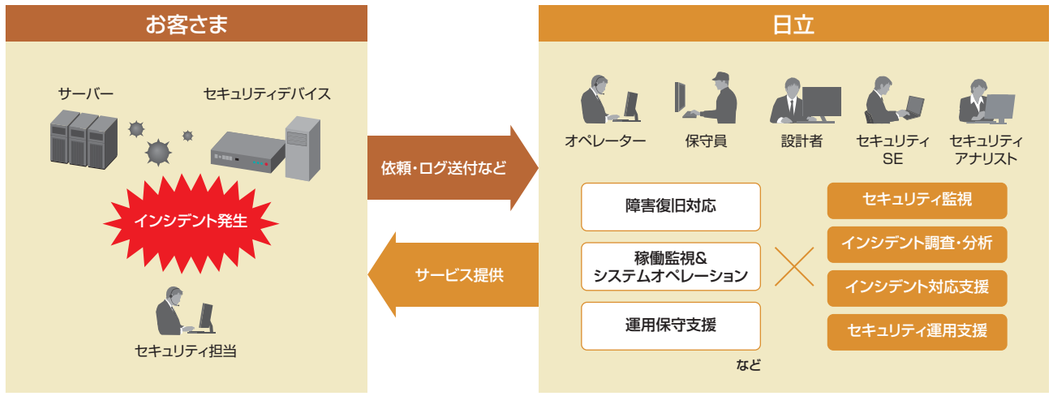
日立がセキュリティイベントを監視・分析。セキュリティ脅威への迅速な対応を支えます。

日立が社会インフラ分野で培った制御システムの運用・保守のナレッジ、そしてIT/OT/IoTを網羅する多彩なセキュリティの知見を結集して、お客さまのSOC運用を支援。DXに伴う新たな脅威にも対応し、制御システムの安定稼働を支えます。

セキュリティ監視・分析

制御・セキュリティの知見を結集し、お客さまのSOC運用をサポート

高度なセキュリティ監視基盤と制御システムセキュリティの専門チームによりお客さまのセキュリティ運用を支援します。監視、分析によるインシデントの予防から、発生したインシデントへの迅速な対応までサポートし、制御システムの安定稼働および万が一の際の被害の最小化に貢献します。



ワンストップサービス

制御システムセキュリティに関する高度な知識と技術を持つ専門チームが、セキュリティの監視・分析からインシデントへの対応まで適切な対策をワンストップでサポートします。

柔軟なサービス提供

オンラインでの常時監視だけでなく、オフラインでの定期診断やインシデント抽出、調査・分析、対応支援など、お客さまの環境に合わせて柔軟にサービスを提供します。

24時間365日対応

止まってはならない制御システムに対して十分な監視体制の構築が困難なお客さまへ、日立が24時間365日体制のサービスを提供します。

サービス効果

高度な監視基盤によりインシデント検知後の初動対応は迅速。
対応時間を短縮し、対策の早期着手を実現することでセキュリティ被害を最小化。経営へのダメージを抑えます。

監視対応なし（お客さま運用）の場合

セキュリティ監視・分析支援サービスを利用した場合

*グラフはイメージです。セキュリティインシデントにより短縮できる時間は変わります。

サイバー防衛訓練サービス

DX環境を見据えたセキュリティ人財の育成と個人・組織の対応力向上のための訓練を行います。

制御システムのセキュリティ対策においては、DXに伴う新たな攻撃に備え情報・制御システムを維持するための運用の強化が不可欠です。そこで社会インフラ事業向けに人や組織の強化に着目した実践的な訓練が行えるサービスを提供します。

NxSeTA（Nx Security Training Arena）

サイバー攻撃への組織としての対応力・判断力を訓練。

大みか事業所内に、サイバー攻撃を想定した防衛訓練施設「NxSeTA」を設置。社会インフラ事業や製造業向けにリモート環境での実践的なインシデント対応訓練を提供しています。DXを推進する組織のレジリエンス強化と安心・安全な社会の実現のため、お客さまの人財育成に貢献します。


サイバー防衛訓練施設「NxSeTA」

特長.1

DX人財育成ソリューション「NxSeTA」

- 組織的なインシデント対応能力とDX対応人財育成の強化に貢献
- リモートから訓練参加を可能とする「オンラインNxSeTA」
- お客さまの拠点・事業所で訓練を実現する「ポータブルNxSeTA」

特長.2

人と組織の持続的なセキュリティスキル向上の計画策定支援

- コミュニケーション力やレジリエンスなどヒューマンスキルを評価
- 個人および組織における継続的な教育・訓練計画を提案
- 経営層から現場層まで中長期的に持続的なスキルアップを支援

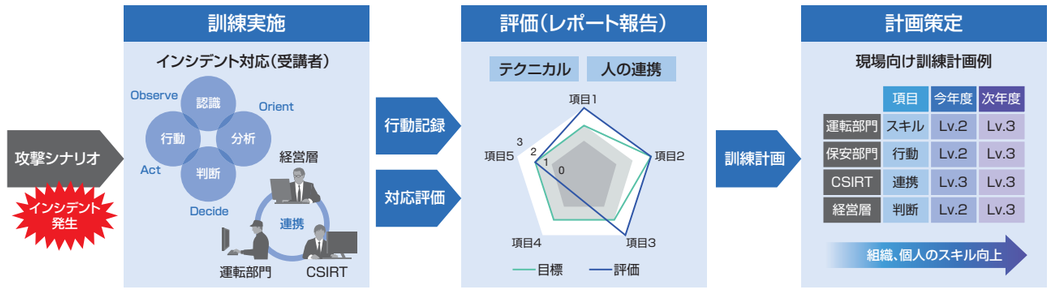
特長.3

現場力・レジリエンス強化のためのトータルサポート

- 重大事故を引き起こさないよう、実践訓練を通じたスキル強化を支援
- 日立セキュリティコンサルタントによるインシデント対応アセスメント実施
- 人財・運用・システム視点で現場力、レジリエンス強化をトータルサポート

目的・レベルに応じた評価と訓練計画をサポート

お客さまの目的・レベルに応じてスキルを定量評価し、継続的な訓練計画を提案してスキルアップを支援します。



CSIRT:Computer Security Incident Response Team