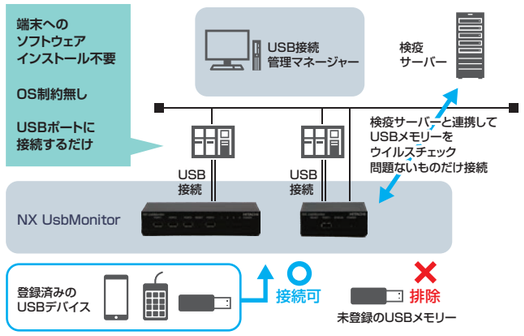
制御システムに適した日立のセキュリティ対策装置

USB接続管理装置「NX UsbMonitor」

不正なUSBメモリー利用による
ウイルス侵入や情報漏えいを防止

後付けで、未登録のUSBメモリー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メモリー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メモリーを使用できます。



一方向中継装置「NX Oneway-Bridge」

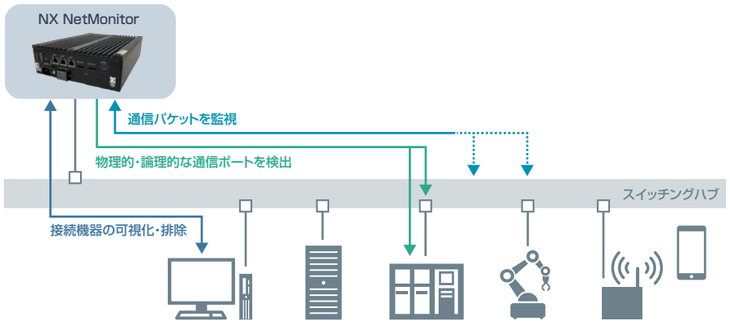
片方向の通信を物理的に遮断し
外部からの不正アクセスを防止

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。

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

⚠ 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

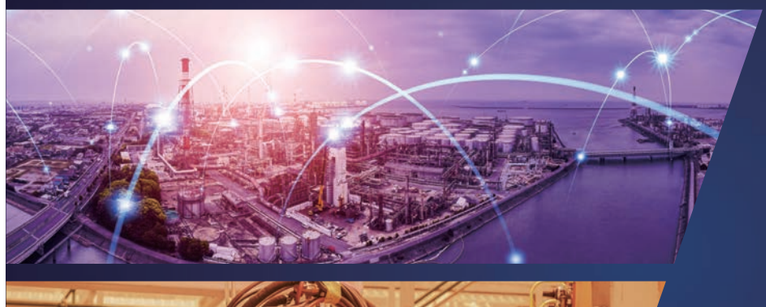
■ 製品情報サイト・インターネットでのお問い合わせ
https://www.hitachi.co.jp/security-control/

株式会社 日立製作所　制御プラットフォーム統括本部

SP-010　2022.1

製造業向け制御システムセキュリティ

HITACHI
Inspire the Next



製造業向け
制御システム
セキュリティ

製造業のさらなる発展に向けて
日立がリードするDX with Cybersecurity

ネクストノーマル時代を迎え、社会インフラや製造現場ではDX推進により大きな変化に直面しています。
日立は長年にわたり、電力・鉄道・ガス・水道など、社会インフラの制御システムを構築・運用してきました。自社工場のDXや、さまざまな社会インフラのセキュリティ対策で培った運用実績・ノウハウを集結し、確かな知見に基づいた制御システムのセキュリティ確保と、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。

DX：Digital Transformation

DXによる製造業の変化と工場のスマート化

急速に広がるオンラインの導入や多様化するセキュリティリスクの増加など、ビジネス環境の変化により製造業にも改革が求められています。次世代の製造業にとって重要となる「制御システムの4つのシフト」を実現するために、DXによる「工場のスマート化」が進んでいます。

工場のスマート化

：制御システムの4つのシフト

顧客ニーズのダイナミックな変化

ITシステム連携

CAD連携
業務システム連携

働く場所の変化

リモートでの端末利用

外部利用端末
（外部端末での運用・保守）

作業方法の変化

ライン・設備改善

ロボティクス・AI活用
インテリジェント機器導入

サプライチェーンの変化

外部システム連携

外部サービス利用
プロセス分担

**工場のスマート化により制御システムの連携範囲が広がり、
製造現場の環境そのものが拡大**

DXによるセキュリティリスクの変化と新たな制御セキュリティの考え方

システム連携・オープン化が進み、社内・社外間でこれまで以上にさまざまなリソースや情報がやり取りされるようになるため、いままでのような境界に基づくセキュリティ対策だけでは十分対応できなくなっています。制御システムは今後、従来の防御方法に加えて、DXによって生じる新たなセキュリティリスクに対応した、より高度な対策を検討しなければなりません。

オープン機器・ソフトウェア
制御システムで使用する
デバイスの新たなリスク

外部連携
外部との接続リスク

OTとITとの融合
OTとIT間で異なる
インフラ・セキュリティポリシー

OT：Operational Technology

**従来の考え方だけでは通用しないため、
新たな考え方に基づくセキュリティシステムの構築が必要**

DX実現をトータルにサポートする日立のセキュリティソリューション

日立は、一貫したセキュリティ対策ポリシーのもと、現状把握段階から運用段階までお客さまの状況に応じて適切なサポートを行います。実施後は対策や運用の見直しを行い、DXによって変化する現場環境が常に最適な状態になるよう支援します。
お客さまのDX実現のため、組織・運用・システムに沿ったソリューションをトータルに提供します。

DX導入時のセキュリティ方針を決めたい	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	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	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 備えた組織体制を強化したい	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

DX導入時のセキュリティ方針を決めたい

事業継続を第一に、DXによるシステム将来像まで考慮した幅広い対策をさまざまな段階から支援します

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、人財、組織運用を見据えたリスクマネジメントを提案します。

リスク識別

システムレベルリスク分析
- 制御システム調査

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

リスク評価

- システムレベルのリスク評価
- 事業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

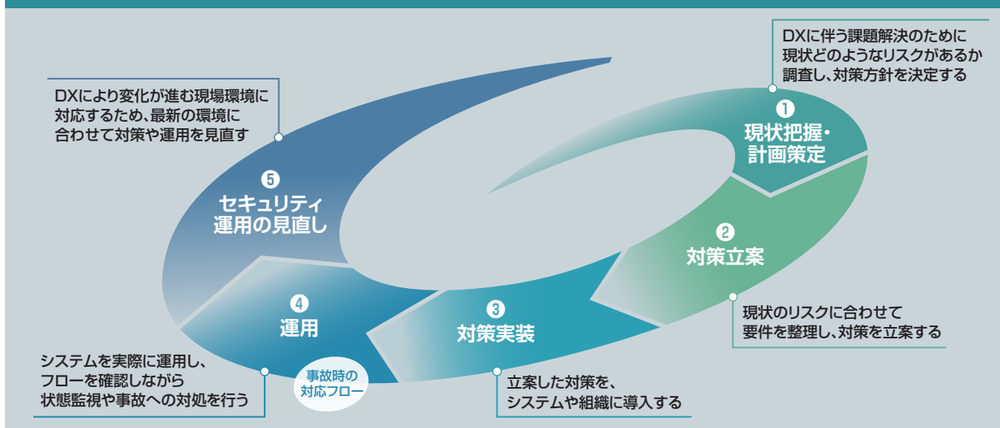
IEC : International Electrotechnical Commission

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、ライフサイクルに沿った制御システムの導入・運用を視野にいれた、安心なセキュリティ対策の立案と実現を、コンサルティングから支援します。

IoT : Internet of Things

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

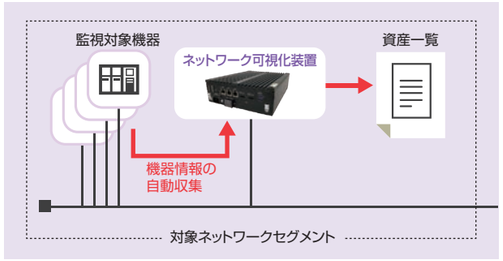
新しいセキュリティリスクを考慮したセキュリティ対策を導入したい

DXにより刻々と変化する制御システムを守るため、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導入を支援します

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

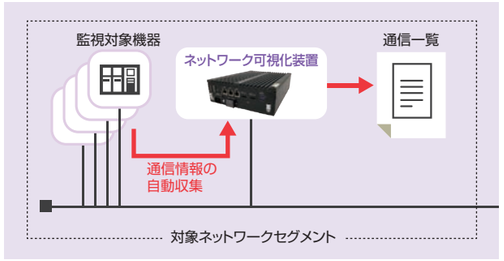
ネットワーク可視化装置の提供機能を利用して、対象ネットワークセグメント内に導入されている資産の洗い出しを実施します。



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

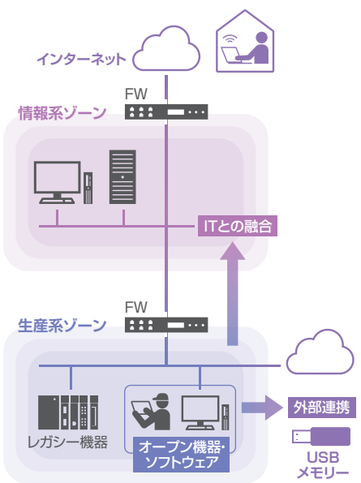
オープン機器の増加でリスクが高まる現場機器の管理を、後付けできる方法で強化したい

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)

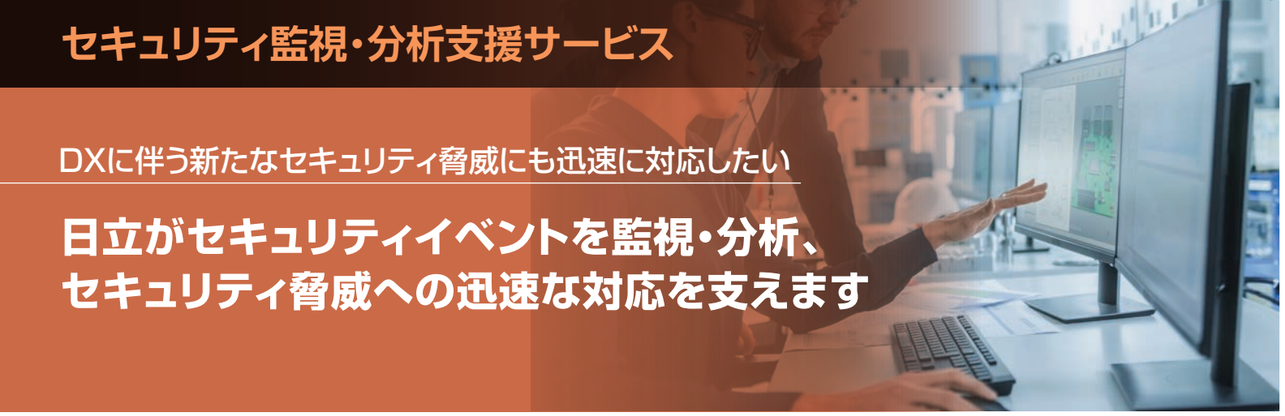
メンテナンスでUSBメモリーを使い続けたい

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



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

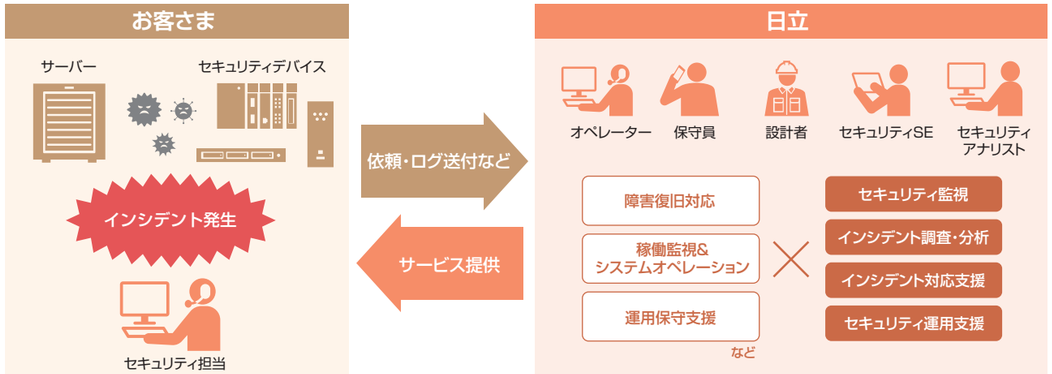
日立がセキュリティイベントを監視・分析、セキュリティ脅威への迅速な対応を支えます

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。

SOC：Security Operation Center



特長01 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。

特長02 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あわせて柔軟にサービスを提供します。

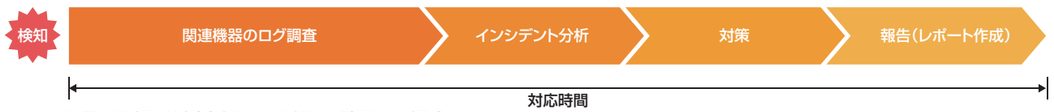
特長03 24時間365日対応

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を迅速化。
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に伴う新たなサイバー攻撃に備えた組織体制を強化したい

実践的な訓練により、DX環境下におけるセキュリティ人財の育成と個人・組織の対応力向上を図ります

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。

特長01 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」

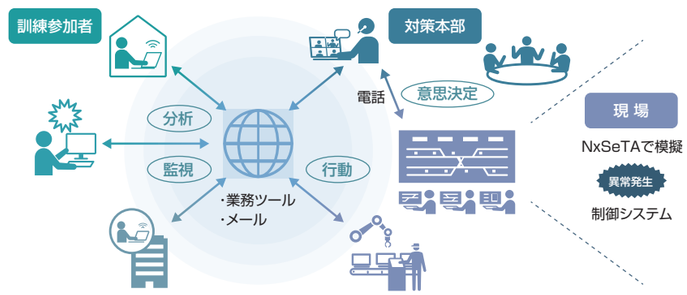
特長02 人と組織の持続的なセキュリティスキル向上の計画策定支援

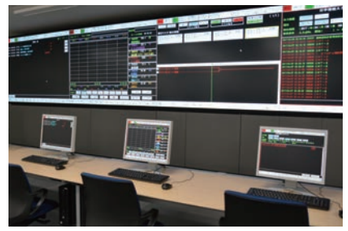
- コミュニケーション力やレジリエンスなどヒューマンスキルを評価
- 個人および組織における継続的な教育・訓練計画を提案
- 経営層から現場層まで中長期的に持続的なスキルアップを支援

特長03 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

リモートでの訓練「オンラインNxSeTA」

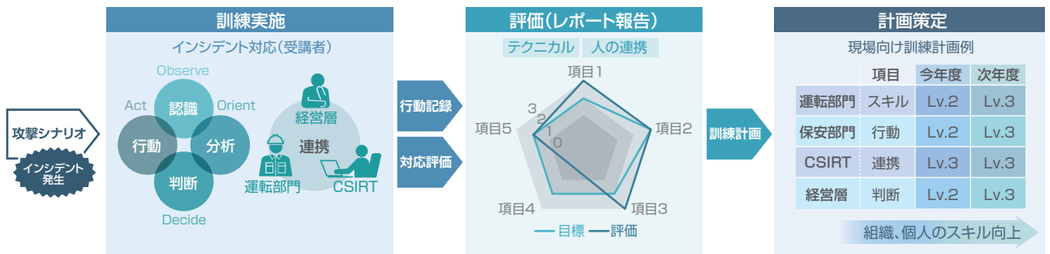




サイバー防衛訓練施設「NxSeTA」

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