Customer Confidential

NTT DATA UnifiedMDR® for OT Securityのご紹介

2025年7月1日
株式会社NTTデータ
セキュリティ＆ネットワーク事業部

NTTデータにおける セキュリティビジネス

世界最大級のセキュリティ企業 NTTデータグループ

人材・施設など多角的な面で強みを持つNTTデータグループは**世界最大級のサイバーセキュリティ企業**です。

サイバーセキュリティ専門家

7,500人 以上

世界中のさまざまな業界やテクノロジーに高度に特化されたセキュリティ専門家をグローバルに多数雇用

サイバーセキュリティデリバリセンター

80 以上

世界中にデリバリセンターを構えており、コストや規制遵守の要件を満たすソリューションを提供可能

データセンタグローバルシェア

3 位

世界中に構えるNTTデータグループのデータセンターを利用したソリューションを提供可能

グローバル脅威インテリジェンス

世界トラフィックの

40% 以上

NTTバックボーンにおける世界のインターネットトラフィックの40%以上を分析して得たグローバル脅威インテリジェンスを活用

マネージドセキュリティサービス市場シェア

MSS市場シェア分析2023

2 位

長年のインシデント対応の経験と世界最大のゼロトラスト環境の実装から得たノウハウを活用したサービスを提供し、世界のMSS市場をリード

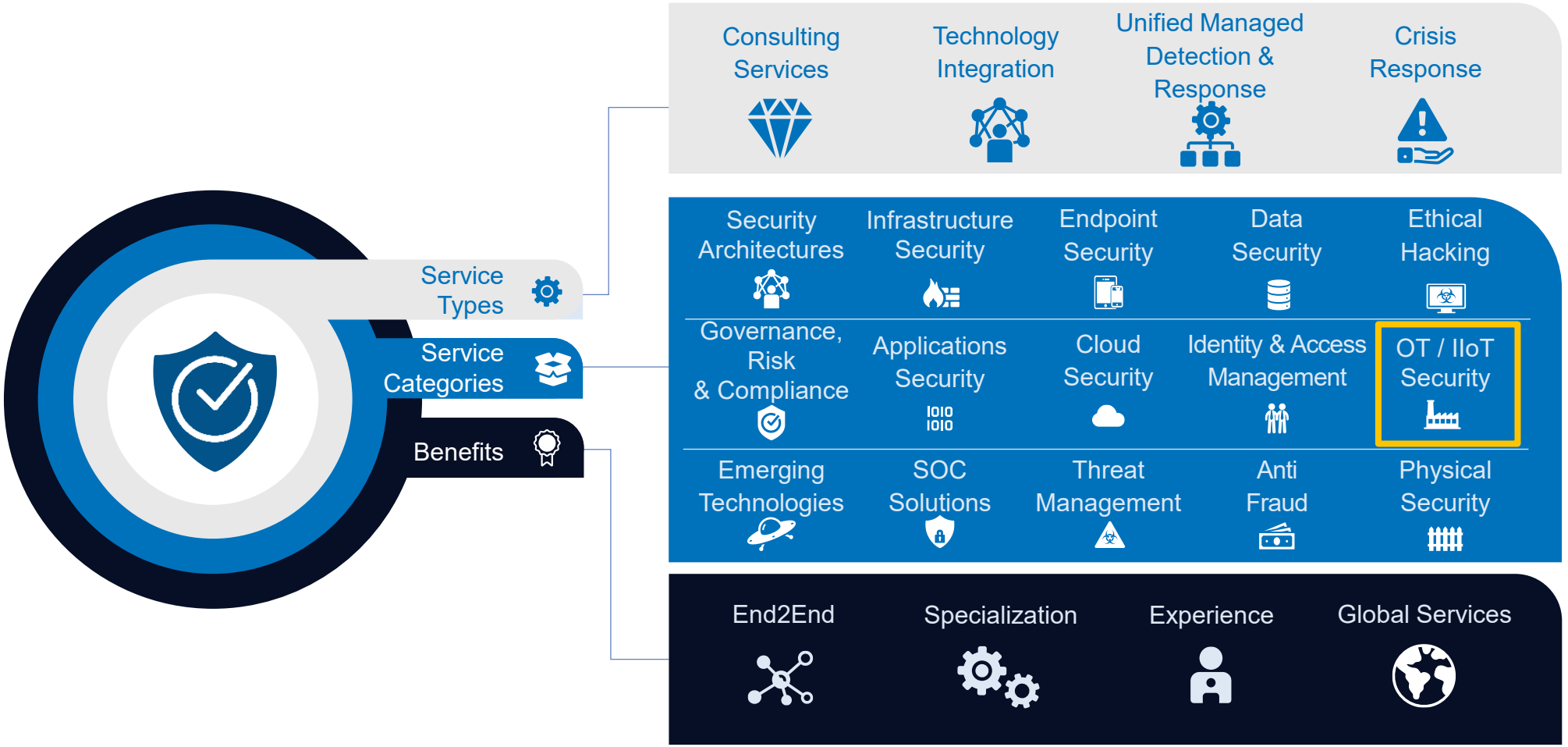
セキュリティサービス経験値

30年 以上

30年以上のサイバーセキュリティサービス経験のノウハウ活用が可能

NTTデータグループのサイバーセキュリティサービス群

当社は、幅広いサイバーセキュリティ領域において、パートナーとのアライアンス整備、サービス開発を行っています。
OT/IIoTセキュリティについてもグローバルでサービスを推進しています。



なぜNTTデータがOTなのか

01 EUをはじめとするグローバルでのOTセキュリティノウハウをサービス化

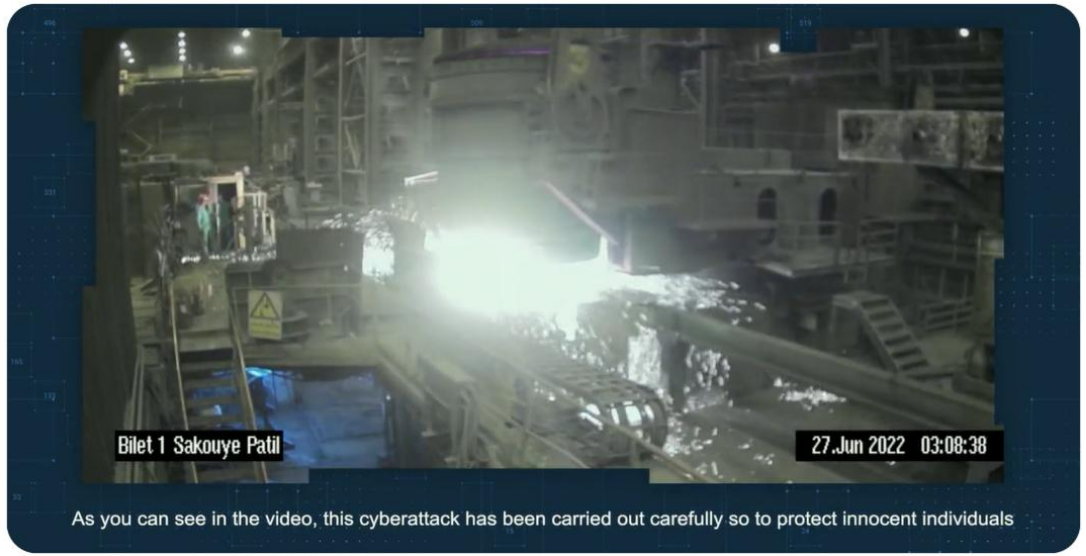
02 世界的にも事例が殆どない時代から、**グローバルOT MSSサービスを提供**し、ノウハウを蓄積

03 分野別の専門知識を持つ約**200**名のグローバルOTセキュリティチーム

04 先端企業とのアライアンスを通じて現場の課題に対する実践的なソリューションを提供

スマートファクトリー化による セキュリティリスクの増加

2022年6月27日 とあるハッカーグループがXにて・・・



本来見ることのできない工場内のカメラに侵入した映像を流した。

制御系システムに侵入した攻撃者は溶鉱炉に攻撃し爆発させた。

人的被害に加え、生産ラインの事業も停止し、約1億ドルの損失が発生

cyberattacks against Iran's steel industry

OTセキュリティは気づいた時点で実施すべき

国内外の工場・プラントにおいてセキュリティインシデントが発生しています。

石油パイプラインにおける被害事例（2021年、アメリカ）

- ✓ 攻撃者は、情報システム部門の把握していなかったVPN装置を経由して侵入した。侵入後、ネットワーク内の端末を探索し、機密情報を外部へ運び出し、配布したランサムウェアによってコンピュータを暗号化した。
- ✓ サイバー攻撃を受けたことが判明した時点で、現場担当者が被害拡大を懸念して制御システムを6日間停止した。これにより**顧客への燃料の供給がストップし、市場に燃料が枯渇**することになった。

港内コンテナターミナルシステムにおける被害事例（2023年、日本）

- ✓ 港内に5つあるコンテナターミナルを一元的に管理するターミナルシステム（NUTS）においてサイバー攻撃による障害が発生。**約3日間にわたりコンテナの搬出入作業の停止**を余儀なくされた。
- ✓ 船舶37隻の荷役スケジュールに最大24時間程度の遅延が発生。最終的に**約2万本のコンテナ搬出入に影響**があったとされる。
- ✓ 重要なシステムにもかかわらず、セキュリティー専任者が不在だったこともわかった。

水道システムにおける被害事例（2021年、アメリカ）

- ✓ 攻撃者は、インターネット上から遠隔操作ソフトウェアによって事務用PCにログインし、さらにネットワークを探索し、制御系の操作が可能な操作端末に不正侵入した。
- ✓ 攻撃者は、**水処理システムにおける水酸化ナトリウム投入量の設定値を、通常の濃度から100倍以上の値に不正に変更**した。

光学メーカーにおける被害事例（2024年、日本）

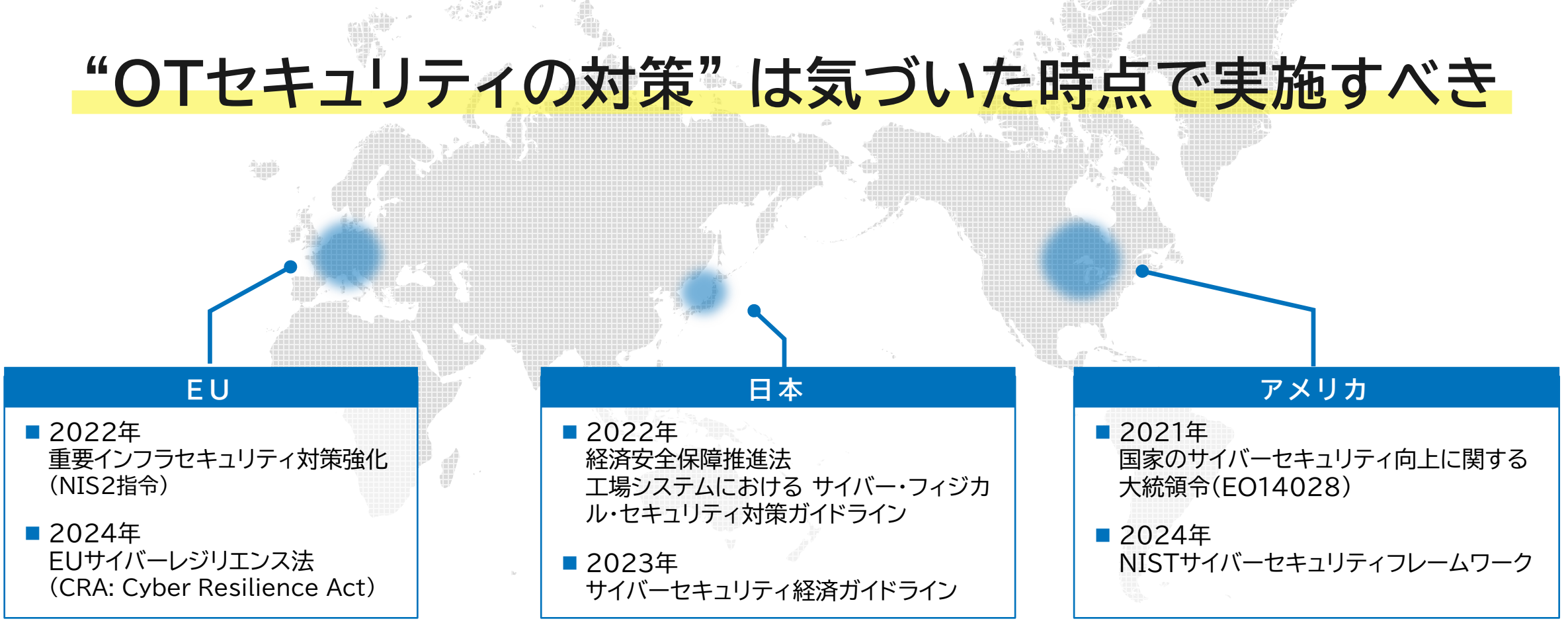
- ✓ 眼鏡用レンズの国内市場でトップシェアを誇る大手光学メーカー本社と複数の事業所でサイバー攻撃によるシステム障害が発生。海外の事業所で社内ネットワークに異常が起き、サイバー攻撃が発覚。
- ✓ 眼鏡用レンズの**受注や出荷が滞り**、一部の製品の生産や供給に影響。
- ✓ 販売店では、一部**商品の販売を停止**した。

https://www.ipa.go.jp/security/controlsystem/incident.html

新たな法規制への適応

各国にてOT環境(工場システム)を含むサイバーセキュリティガイドラインの整備が進められています。
日本でも経済産業省から工場システムにおけるサイバー・フィジカル・セキュリティ対策 ガイドラインが発出されております。
セキュリティガイドラインは強制力を持たせていく傾向にあり、OTセキュリティ対策も急務となっております。

“OTセキュリティの対策”は気づいた時点で実施すべき



EU

- 2022年
  重要インフラセキュリティ対策強化
  (NIS2指令)
- 2024年
  EUサイバーレジリエンス法
  (CRA: Cyber Resilience Act)

日本

- 2022年
  経済安全保障推進法
  工場システムにおける サイバー・フィジカル・セキュリティ対策ガイドライン
- 2023年
  サイバーセキュリティ経済ガイドライン

アメリカ

- 2021年
  国家のサイバーセキュリティ向上に関する大統領令(EO14028)
- 2024年
  NISTサイバーセキュリティフレームワーク

OTセキュリティ対策の必要性

DX化が進むにつれ、気づかぬうちにOTネットワークがセキュリティリスクに晒されているケースが増えています。
独自プロトコルが多い、**可用性が重要**等、**OTセキュリティに特化したセキュリティ対策**が求められています。
OTをターゲットにしたサイバー攻撃は**業務の停止に留まらず、人命を脅かすなど被害が甚大**になるおそれもあり、
OTセキュリティリスクの把握や、**OT資産の可視化・脅威検知対応**を行う対策が必要です。

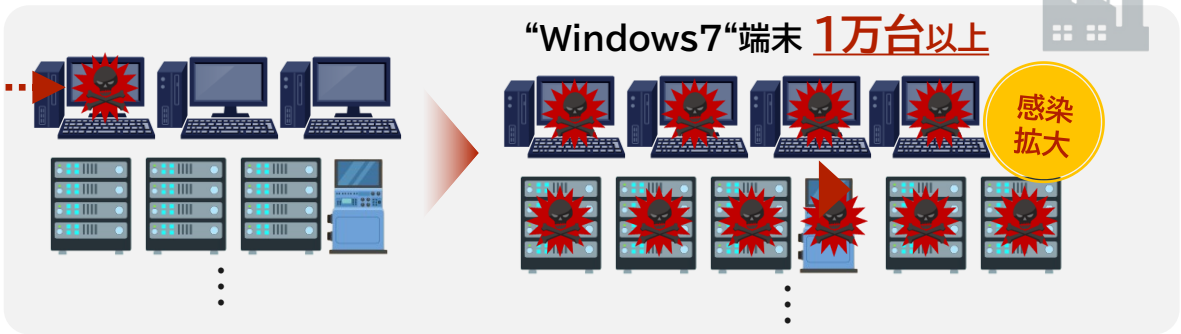
サイバー攻撃事例　● 半導体工場のマルウェア感染（2017年、台湾）

1 ランサムウェア感染

2 ウイルススキャンをせずに工場側NWに接続（作業ミス）

保守業者のメンテナンス端末

3 工場内のWindows端末にランサムウェア感染・拡大



対策

- セキュリティアセスメント
- 資産可視化
- 脅威検知対応

被害内容

- 3拠点の生産施設に影響
- 3日間の生産停止
- 被害額は最大190億

OTセキュリティ対策の必要性

DX化が進むにつれ、気づかぬうちにOTネットワークがセキュリティリスクに晒されているケースが増えています。
独自プロトコルが多い、**可用性が重要**等、**OTセキュリティに特化したセキュリティ対策**が求められています。
OTをターゲットにしたサイバー攻撃は**業務の停止に留まらず、人命を脅かすなど被害が甚大**になるおそれもあり、
OTセキュリティリスクの把握や、**OT資産の可視化・脅威検知対応**を行う対策が必要です。

サイバー攻撃事例　● 半導体工場のマルウェア感染（2017年、台湾）

1 ランサムウェア感染

2 ウイルススキャンをせずに工場側NWに接続（作業ミス）

保守業者のメンテナンス端末

3 工場内のWindows端末にランサムウェア感染・拡大

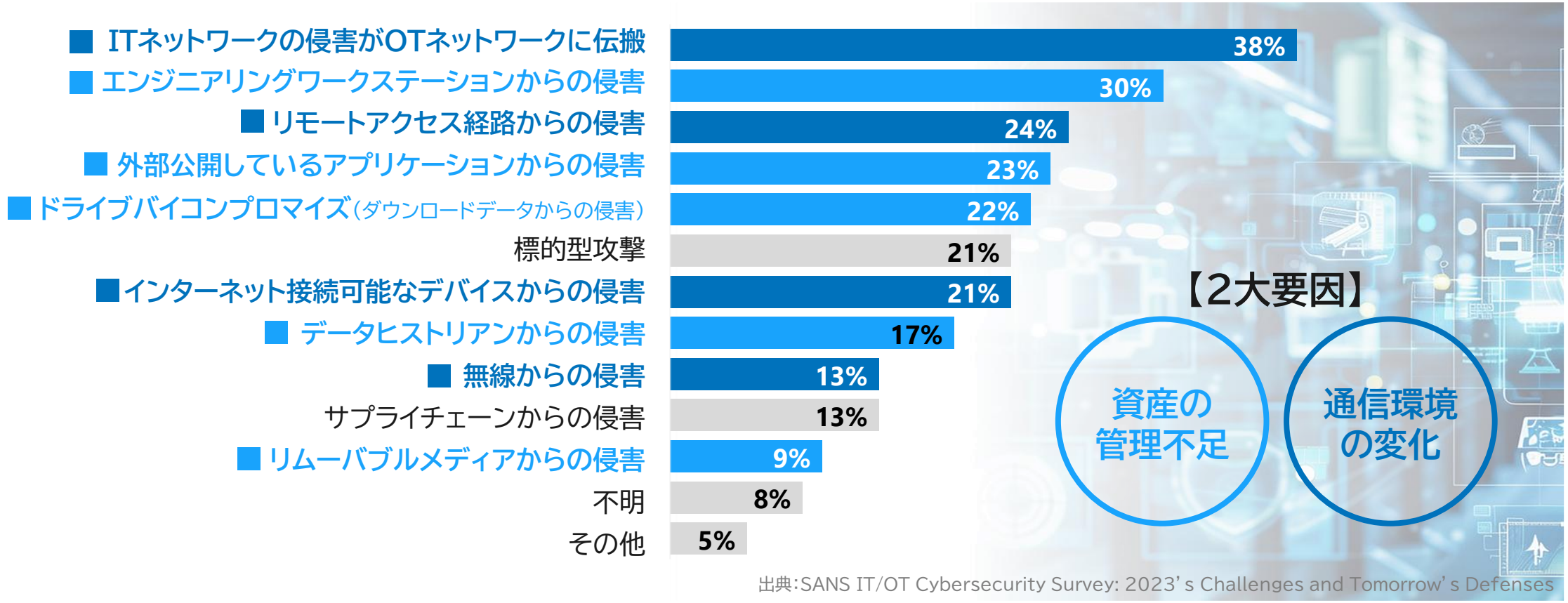
被害内容
- 3拠点の生産施設に影響
- 3日間の生産停止
- 被害額は最大190億

対策

- ●セキュリティアセスメント
- ●資産可視化
- ●脅威検知対応

OTセキュリティ対策の2大ポイント

Q OTネットワークで発生したセキュリティ事故を引き起こした要因はなんですか？（複数回答可）



出典：SANS IT/OT Cybersecurity Survey: 2023’s Challenges and Tomorrow’s Defenses

守るべきOT資産の管理・可視化 と **通信のモニタリング・脅威検知** がポイント

NTTデータが提供する OTセキュリティ対策

当社の考えるOTセキュリティの全体像

弊社はOTセキュリティの全体(セキュリティポリシー策定、運用体制整理、現状把握／リスク管理、対策の実行、実行後の運用等)を把握しており、お客様のOT環境に必要なセキュリティ対策を漏れなく実施し、**セキュアなOT環境運用**を実現します。

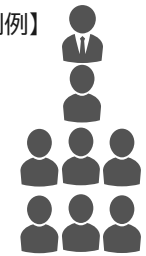
OTセキュリティポリシー

✓ IEC62443等の標準規格を参考に組織としての**OTセキュリティポリシーが定義**されている。

OTセキュリティ推進・維持体制

✓ OTセキュリティを推進・維持する**責任者・担当者が定義**されている。

【体制例】



経営層,CISO

OTセキュリティ管理責任者

部門セキュリティ管理者

拠点担当者

現状把握とリスク管理

✓ 守るべき業務を把握・管理できている。
✓ 業務を実現しているOT資産、通信を把握・管理できている。

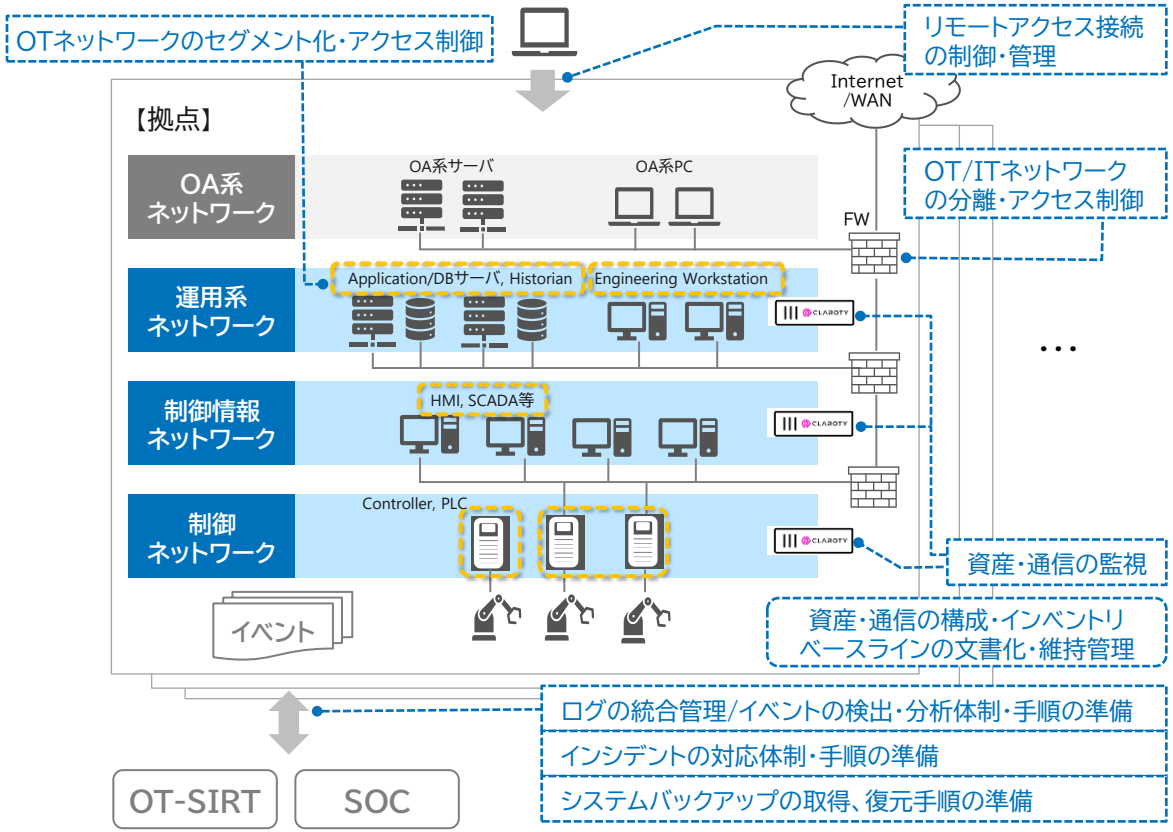
【OT資産・通信・業務の現状把握】

✓ 現状把握から導かれるリスクとその対応優先度を管理できている。
✓ リスクとその対応優先度に応じて対応策を検討している。

【リスク管理と対応策の検討】

対応策の実行・維持運用

✓ 検討した**対応策を実行・維持運用**できている。



NTTデータの考えるOTセキュリティ推進ロードマップ案

セキュリティアセスメントも必要ですが、管理できている資産に対してアセスメントを行っても多大な稼働がかかり、意味のある結果がでるかは疑問が残ります。NTTデータは、工場の運用に一切影響を与えない方法でソリューションを導入し、工場の資産を可視化することを推奨します。その後、顕在化した問題に対する対策の検討、対策の実施を行い、DX時代のセキュアな工場運用を支援します。

Phase 1 工場の可視化

工場にどのような資産があり、どのようなNW構成になっているかを把握します。まずは一つの工場でPoCという位置づけで実施を推奨します。

- ソリューション導入
- 可視化
- 現状の把握

Phase 2 顕在化した問題に対する対応

どの装置にどのような脆弱性があるのか、意図しない通信に対する対策の検討をします。

- 資産、通信の洗い出し
- リスクの洗い出し
- リスクの特定、分析、評価
- リスク対策の検討

Phase 3 リスクに対する対策実施

リスクに対する対策を実施します。

- 機器に対して最新のセキュリティパッチ適用もしくは代替策の実行
- 工場⇔インターネット間の通信見直し
- 不必要な通信の見直し
- 機器のリプレイス　etc…
- 本フェーズでは緊急度の高いもののみを実施することを推奨します。

Phase 4 全工場への展開及び監視

パイロット拠点での効果を確認していただいた後、可視化ソリューションを全拠点に導入します。
また、セキュリティ製品は導入して終わりではなく、いかにして運用するかが重要です。**OTセキュリティ監視については弊社のManaPlusで実施します。**

Phase 5 Phase 3の残対応実施

弊社は、可視化以外にもNWセグメンテーションソリューション、SIEM等多岐にわたるOTセキュリティソリューションノウハウを有しています。工場にとって最適なセキュリティ製品導入を実施し、DX時代のセキュアな工場運用を支援します。

サービス概要

「**OT資産の管理・可視化**」と「**通信のモニタリング・脅威検知**」を実現するOT-IDSの導入・運用サービスを提供します。

フェーズ	計 画	設計・構築	運 用
提供サービス	**① コンサルティング** ● セキュリティグランドデザイン ● セキュリティポリシー策定 ● セキュリティアセスメント ● 脆弱性診断/TLPT ● XSIRT/SOC構築支援/教育	**② テクニカルソリューション** ● ネットワークセキュリティ ● アプリケーションセキュリティ ● エンドポイントセキュリティ	**③ マネジメントサービス** ● SOC ● 脅威インテリアジェンス ● MDR
特徴	• 現状整理、戦略の立案 • 法規制を考慮したルール策定 • ネクストアクションの提示	• お客さま要件への柔軟な対応 • 多様なOTプロトコルへの対応 • 業務影響のないソリューション導入	• 脅威の常時監視・継続的な改善 • 専門家チームによる検知・対応 • 世界各国を統合的に監視・運用

事例紹介

事例１：国外

世界各国に生産拠点を持つ製造業C社のOTネットワークの可視化と脅威の検知

顧客概要

ドイツに本社を置く大手化学・製薬企業。
製薬およびクロップサイエンス分野で世界各地に**約60の生産拠点**を有し、**99,000人以上**の従業員を抱える。

提供サービス

- **全生産拠点**のOT資産可視化・脅威検知ソリューションの**グローバル展開**
- **25カ国以上**でのローカルサポート
- 生産拠点の資産発見、リスク評価、脆弱性評価
- トラフィックフローの分析
- **OT-SOC構築/運用**と**お客様SOCとの接続**

事例２：国内

日系製造業D社のOT-SOCサービス提供（PoC）

顧客概要

日本を代表する大手製造企業。
次期中計にてサイバーセキュリティリスクの軽減を掲げるべく、
OTセキュリティ領域の対策を強化

提供サービス

- **ICS製品ベンダ**と協業し**OT-SOC構築**（定常監視/レポーティング）
- **AIと機械学習**を使用した脅威情報の可視化・リスクの先読み

お客様の声

- **IT/OT境界**を意識し、**既存環境への影響を少なく**サービスの導入ができている点が好印象
- 改善提案や課題提起などOT領域の豊富なノウハウ提供がgood


NTT DATA