第11回 NPO/GCM交流フォーラム

OTゼロトラスト手法を通じてICS及びOT環境の信頼性と安全を確保するサイバーセキュリティ製品ご紹介

2024年4月27日

株式会社アリス
ARIS Advanced Research & Information Service
上田 裕

Contents

1. OTゼロトラストベースの技術とは

従来のサイバーディフェンスの限界を超え、管理を合理化し、課題を
より迅速に解決する

結論

ネットワークベースとエンドポイントベースの両方のソリューション製品群を
揃えており、ミッションクリティカルなデバイスとOTネットワークの両方に
多層防御のサイバーセキュリティ製品群を提供します

2. Incident Command Systemとは
緊急事態対応の指揮命令の仕組み

1970年代に米国で開発された緊急時総合調整システムで障害・事故の
現場における指揮系統や管理手法を標準化したのがICSです

OTとは
Operational Technologyの略で、システムを最適に稼働させるための
『制御・運用技術の総称』を意味します

特に社会インフラを高度化するためにモノに関わる製造・建設・設備・エンジニアリングの分野、
インターネットを通じて情報活用するICT（Internet・Communication・Technologyの分野、
それらのシステム制御・運用に欠かせないOT（Operation Technology）の分野は個々に
高度化してきました
しかし、IoT（Internet of Things）の推進においては、これらの分野の高度な融合が欠かせません

3. まずは可視化検知、そして同時に防御対策も！

まずは可視化！

工場/制御：OTセキュリティ

OTデバイスを
脅威から防御

可視化・検知

・リスク管理
・アセスメント
・資産の可視化
・通信の可視化/NW把握
・脆弱性管理
・脅威検知
・異常検知
・ネットワーク状態監視
・トラフィック把握

防御（保護）

・制御LAN/産業デバイスを攻撃から保護
⇒エッジ周辺のセキュリティを強化！
・工場内のNW横感染を防御
・産業用IPSでOTに特化した環境も考慮

4. 先ずは導入が容易なUSBによるポータブル検査から

- ソフトウェアのインストールおよびシステム再起動不要
- ITおよびOT環境の可視性の向上
- 管理ツール（ElementOne）による統合管理
- 安全なデータ交換*
- Legacy OS対応（Windows XP ~）

*Portable Inspector Proのみ

txOne networks

5. TXOne Networksについて

txOne networks

トレンドマイクロとMoxaが産業制御システムを保護するサイバーセキュリティ・ソリューションを共同開発することを目的に2019年に設立

世界の4,200社（大手企業350社以上）が導入

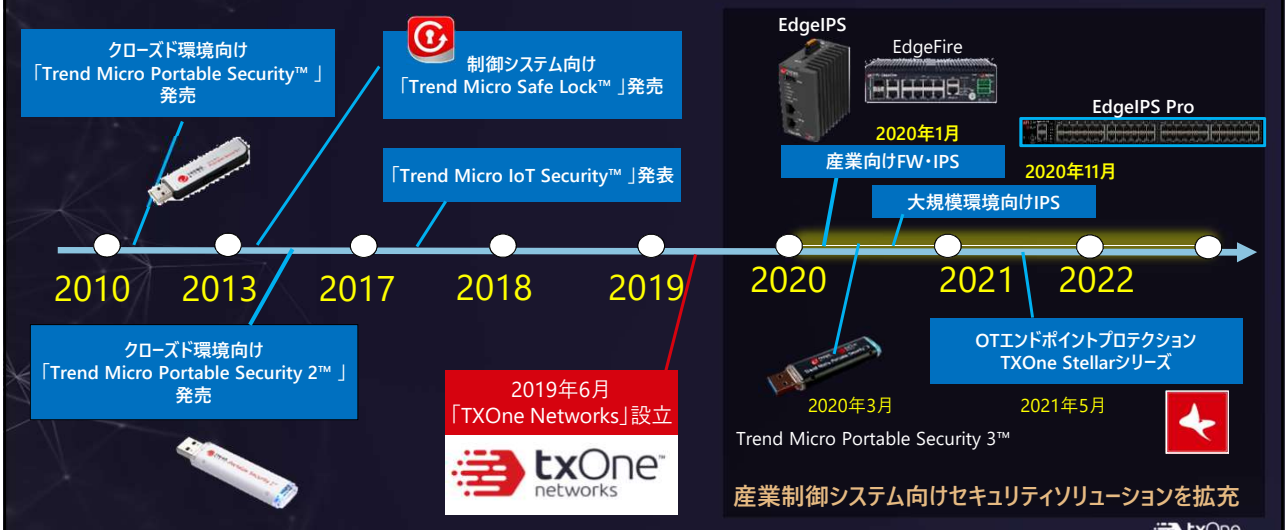
- 半導体製造
  - 半導体製造装置　TOP10の 8社
  - 半導体製造　TOP10の 6社
  - パッケージング　TOP10の 5社
- 医薬品業界　TOP10の 6社
- 自動車業界　TOP10の 5社
- 航空業界　TOP10の 4社

CEO：Dr. Terence Liu
従業員数：400名+（30か国）
総資金調達額: 約1億470万ドル（シリーズB）

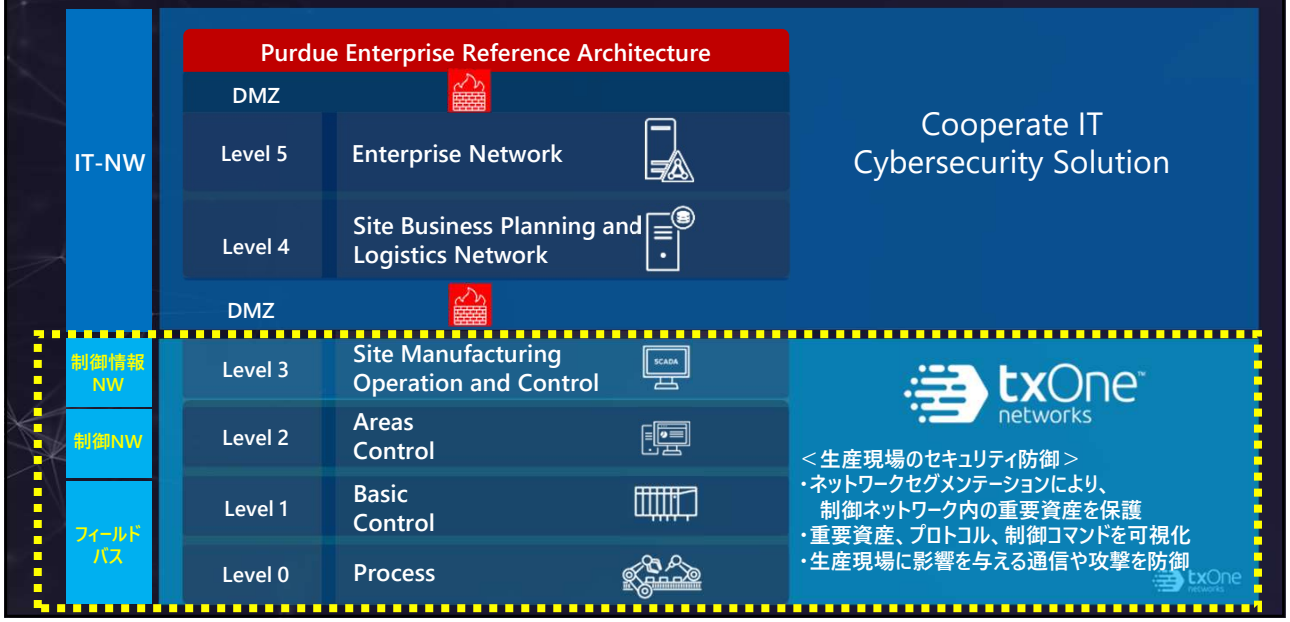
SC awards 2023 WINNER

ICS Cybersecurity関連のAwardで製品戦略、製品の先進性が評価

6. 産業制御システム向けセキュリティ対策の豊富な知見と 実績及びソリューション



7. TXOne Networksの注力領域



8. なぜOT現場は狙われるのか？

工場や重要インフラは生産設備の建設・運用に莫大な費用を投資して生産活動の停止はビジネスに多大な影響を与える

大規模投資を行い、且つ付加価値の高い高額製品を製造する企業ほど、サイバー攻撃をうけた場合のビジネスインパクトが大きい

資産やビジネス損失のみならず、従業員の安全衛生にも影響を与える可能性があります

医療機関も同様

9. OT環境特有の課題

- 環境的要因による潜在的リスクが存在
- OT環境に新たなセキュリティソフトの導入を検討する場合、様々な課題に直面する

【環境的要因】

内部脅威
従業員による誤用・誤操作

管理外のデバイス
外部から持ち込まれた未知のレガシーデバイス・管理外のデバイス

フラットなネットワーク
ネットワーク分割が無いか不十分

パッチ適用が困難
パッチ適用やアップデートが困難

【導入時の課題】

煩雑な導入作業
導入には設置場所・電源・配線などの大がかりな調整が必要

レガシー資産
保守期限切れの古いOSを搭載した設備が多数存在

部門間の壁
IT/OT/セキュリティ部門でシステムの入替サイクルや優先度の考え方が大きく異なる

可用性が最重要
運用を止めることは許容されない

txOne networks

10. OT環境のセキュリティ対策の難しさ

OT環境では一般的ではない動作（異常）

= OTにおいて予期しない動作は異常とみなす

Windowsの正規プログラム(PowerShell)を悪用するファイルレス・マルウェア攻撃の増加

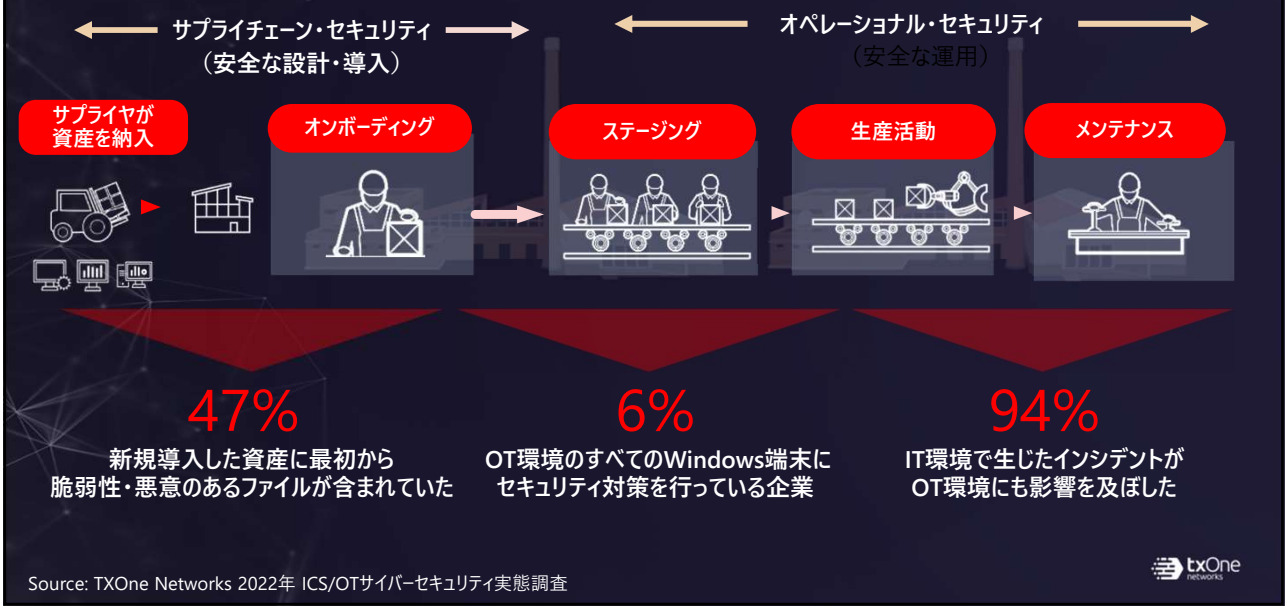
IT環境で日々行われている動作（正常）

= IT EDRでは検知できない可能性

Endpoint Detection and Response

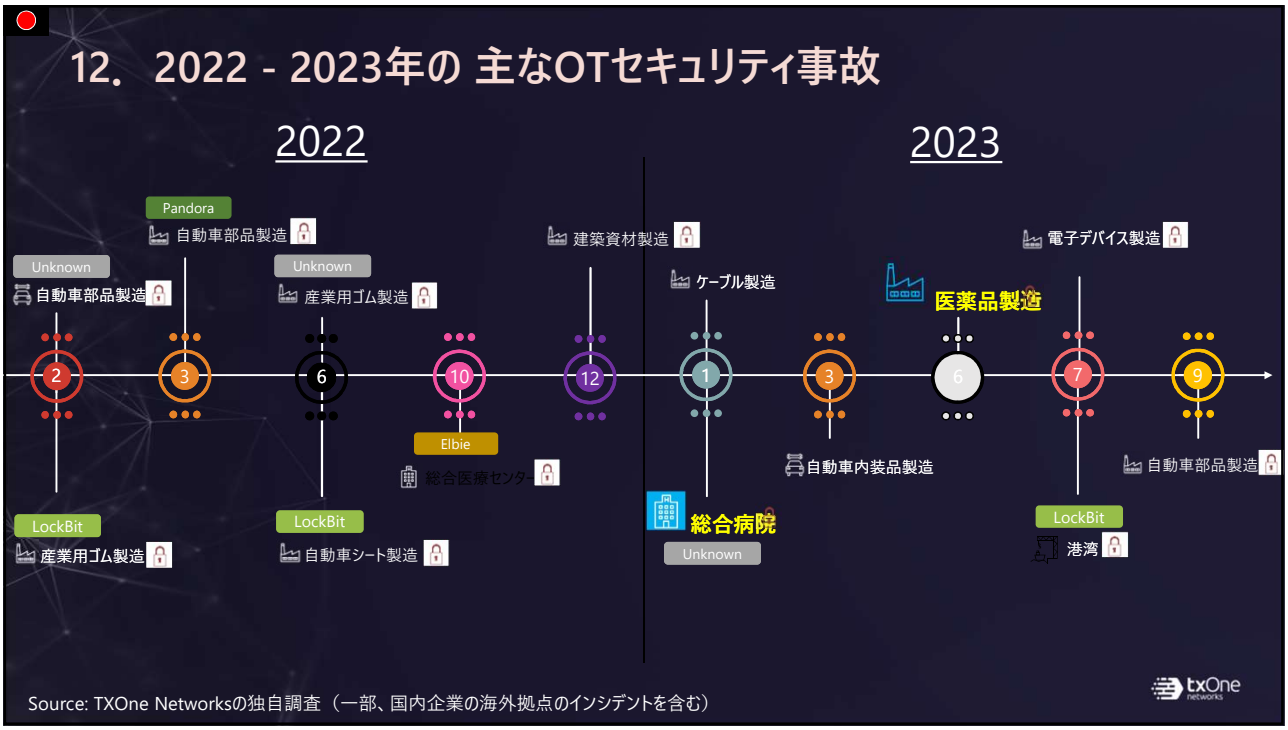
txOne networks

11. OT資産のライフサイクルに関係した感染要因



Source: TXOne Networks 2022年 ICS/OTサイバーセキュリティ実態調査

12. 2022 - 2023年の 主なOTセキュリティ事故

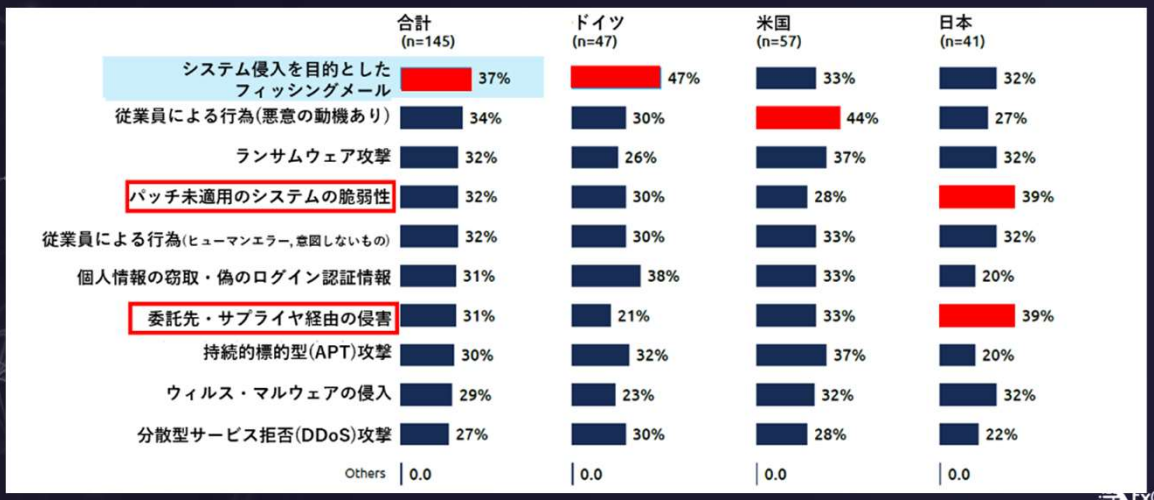


Source: TXOne Networksの独自調査（一部、国内企業の海外拠点のインシデントを含む）

13. OTセキュリティ事故の種類

- IT由来のフィッシングメール、従業員による行為、ランサムウェア攻撃がトップ３
- 国内では、パッチ未適用のシステムの脆弱性、委託先・サプライヤ経由の侵害が多い

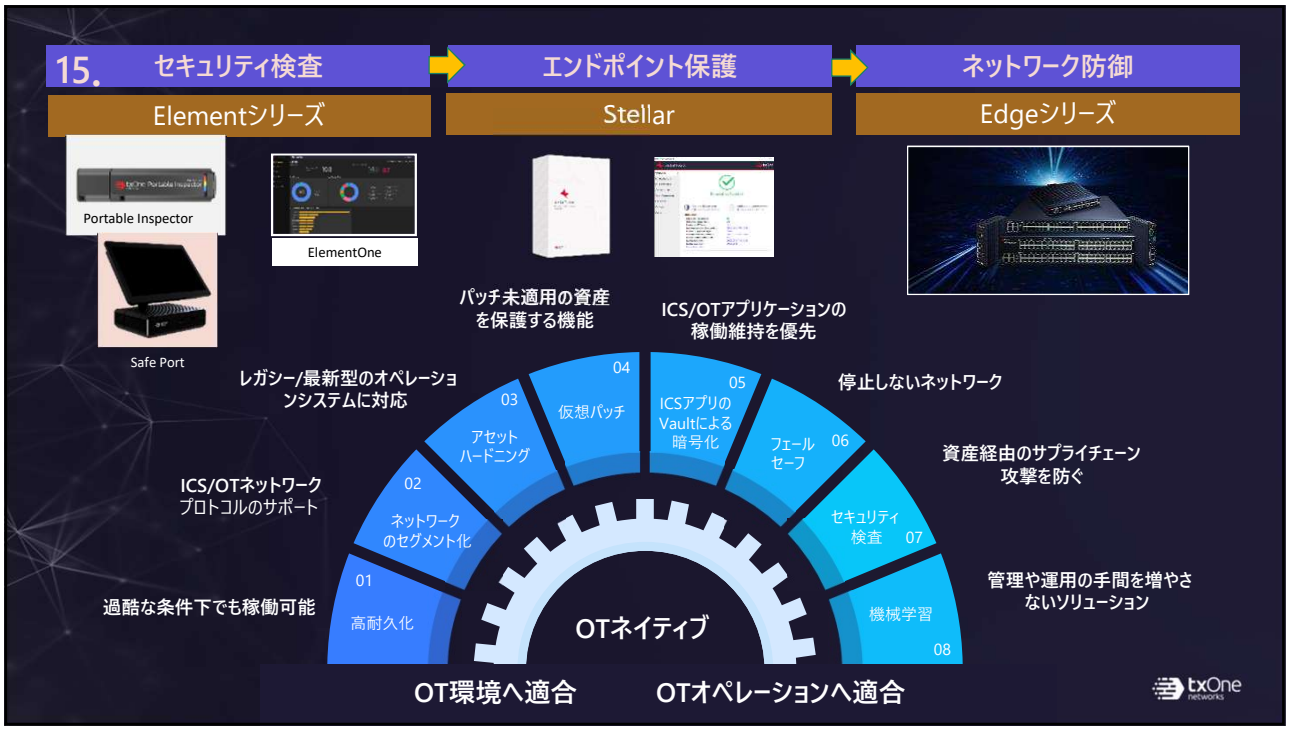
Q - 過去12カ月に経験したOTセキュリティインシデントは次のうちどれですか？

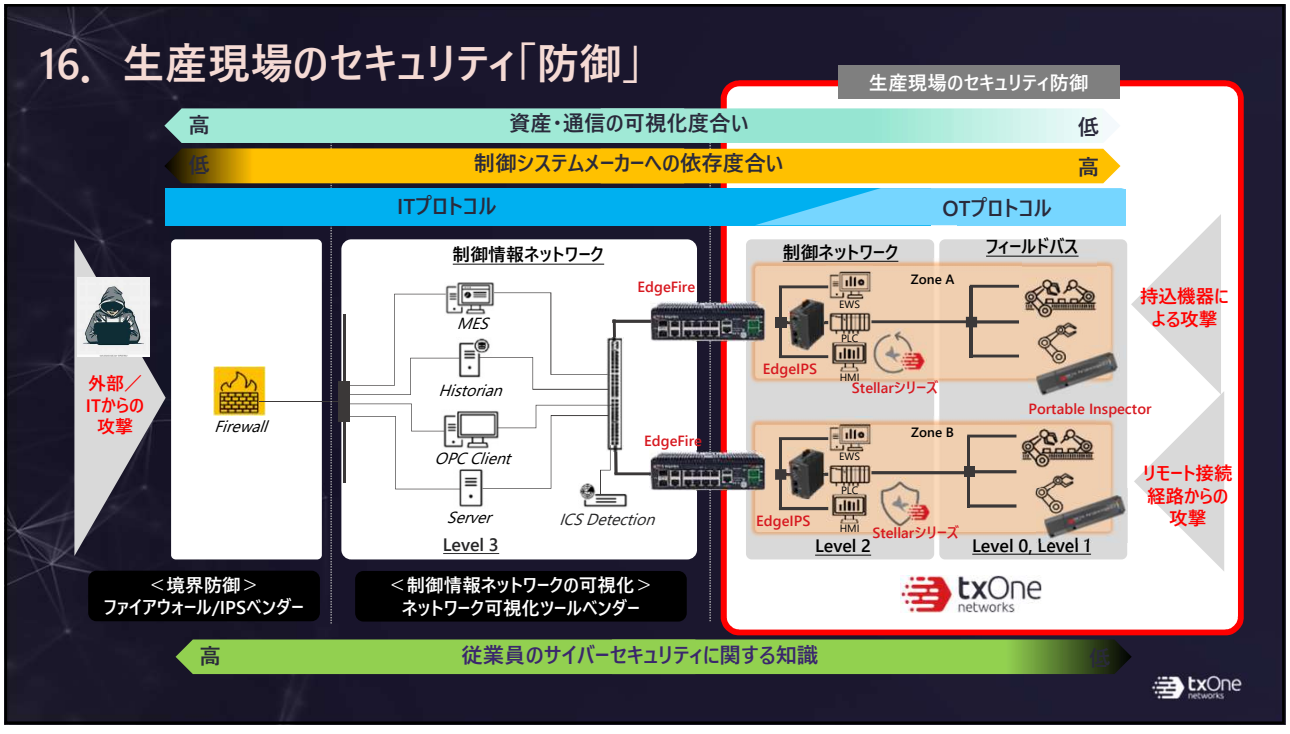


Source: TXOne Networks OT サイバーセキュリティレポート 2022

14. OTゼロトラストアプローチ - OT資産のライフサイクルを保護する

すべてのステージでOT資産に対し「常に疑い、常に検証」を実行する


15. セキュリティ検査
エンドポイント保護
ネットワーク防御
Elementシリーズ
Stellar
Edgeシリーズ
Portable Inspector
ElementOne
Safe Port
パッチ未適用の資産を保護する機能
ICS/OTアプリケーションの稼働維持を優先
レガシー/最新型のオペレーションシステムに対応
停止しないネットワーク
ICS/OTネットワークプロトコルのサポート
資産経由のサプライチェーン攻撃を防ぐ
過酷な条件下でも稼働可能
管理や運用の手間を増やさないソリューション
01 高耐久化
02 ネットワークのセグメント化
03 アセットハードニング
04 仮想パッチ
05 ICSアプリのVaultによる暗号化
06 フェールセーフ
07 セキュリティ検査
08 機械学習
OTネイティブ
OT環境へ適合
OTオペレーションへ適合
txOne networks


16. 生産現場のセキュリティ「防御」
生産現場のセキュリティ防御
高 資産・通信の可視化度合い 低
低 制御システムメーカーへの依存度合い 高
ITプロトコル
OTプロトコル
外部／ITからの攻撃
Firewall
制御情報ネットワーク
MES
Historian
OPC Client
Server
Level 3
EdgeFire
EdgeFire
制御ネットワーク
フィールドバス
Zone A
Zone B
EWS
PLC
HMI
EdgeIPS
EdgeIPS
Stellarシリーズ
Stellarシリーズ
Portable Inspector
Level 2
Level 0, Level 1
持込機器による攻撃
リモート接続経路からの攻撃
＜境界防御＞
ファイアウォール/IPSベンダー
＜制御情報ネットワークの可視化＞
ネットワーク可視化ツールベンダー
高 従業員のサイバーセキュリティに関する知識
txOne networks

ご清聴ありがとうございました！

本製品およびサイバーセキュリティに関する ご相談、ご質問・お問合せは

株式会社アリス CS事業部　東京都新宿区西新宿1-26-2
新宿野村ビル10階　TEL：03-3340-1053
URL:https://www.aris-kk.co.jp

窓口 os-sales@aris-kk.co.jp
E-mailの件名に【TXOne】問合せ・・・と表記して下さい