accenture

Dragos

AI脅威インテリジェンス活用型 OTセキュリティソリューション

OTネットワーク全体を一元的に可視化し、稼働するアセットの状態をリアルタイムで把握。
設備を止めることなく攻撃の兆候を早期に捉え、迅速かつ的確な対応を実現します。

製造業・重要インフラが直面する4つの課題

- 工場にどんな機器がつながっているか **把握できていない**
- ITのセキュリティ製品をOT環境に **導入しようとしたが使えなかった**
- 設備を止めずに**セキュリティ対策を強化する手段がわからない**
- 能動的サイバー防御法・NIS2などの **規制への対応方法が不明確**

なぜ今、OTセキュリティが急務なのか

49%
増加

産業組織を狙うランサムウェア攻撃グループの増加率。製造業は国内ランサムウェア被害の約4割を占め、全産業No.1の被害を受けています。

出典：Dragos「2026 OT Cybersecurity Report」

10%未満
監視率

継続的な監視が行われているOTネットワークの割合。設備停止の損失は平均約26万ドル（約3,900万円／1ドル＝150円換算）／時です。投資の約95%はIT向けに集中し、OTは後回しです。

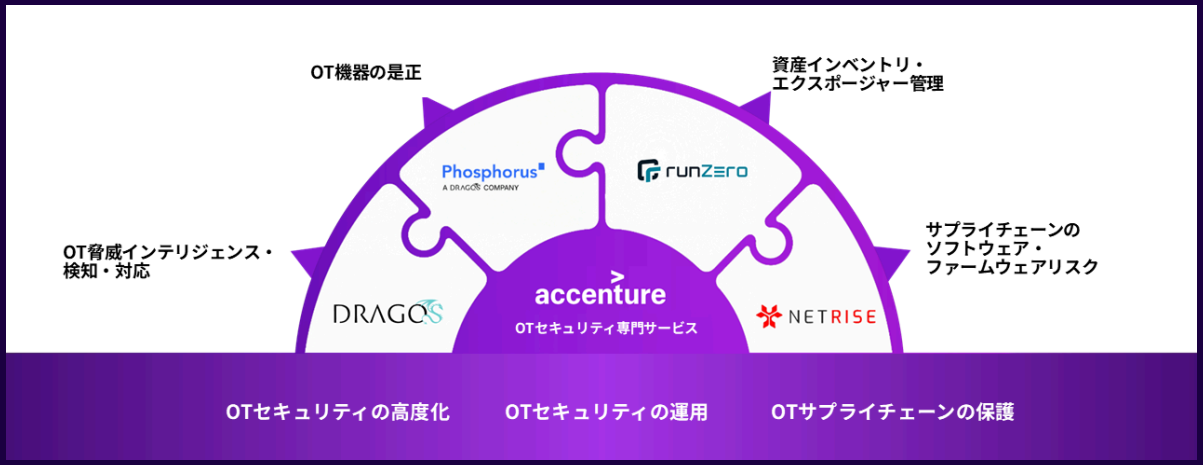
出典：Accenture調査

2026年施行
法規制強化

日本で能動的サイバー防御法が施行。OTを含む包括的なセキュリティ対応と開示・報告義務が法的に求められます。OTが「見えていない」では、報告すらできません。

OT環境を、脅威・資産・機器の中身まで「見える化」する。
止められない現場を、見えないリスクから守るために。

アクセンチュアはDragosの過半数株式を取得し、runZero・NetRise・Phosphorusを含むDragosグループと一体で、戦略立案から導入、24時間体制のマネージド運用までを一気通貫でご支援します。



accenture

アクセンチュア OTセキュリティ専門サービス

OTセキュリティの高度化

- アセスメント
- ポリシー・運用体制の構築
- 資産とネットワークの可視化

OTセキュリティの運用

- OT-SOCの構築
- IT・OT統合SOCの設計・導入
- IDSの導入・運用支援

OTサプライチェーンの保護

- 管理フレームワークの設計
- TPRM管理ツールの導入・運用

3つの「見える化」で、OTの全体像をつかむ

DRAGOS

「誰が狙っているか」を知る

- OT特化の脅威検知・対応
- 設備に触れない受動監視
- 攻撃グループの継続追跡

対象

OT全般

OTネットワーク、制御情報系システム、
OTセキュリティガバナンス、脅威情報など

runZero

「何がつながっているか」を知る

- エージェント不要の資産発見
- IT・OT・IoT・クラウド横断
- 管理外デバイスの特定

対象

IT・OT双方のシステム

社内のあらゆる資産
（IT・OT・IoT・クラウド）

NETRISE

「機器の中身」を知る

- ファームウェア解析とSBOM生成
- 監視では見えない脆弱性の発見
- 調達リスクの可視化

対象

IoT機器・レガシーシステム

IoT・Connected機器、製品、
レガシーシステム
（ソースコードがないものなど）

中核を支える、Dragosの脅威インテリジェンス

OT特化の脅威グループ追跡

ELECTRUM、XENOTIME など26グループを独自に命名・追跡

重大インシデントの解析実績

重要インフラを狙う先進的な攻撃手法を継続的に解析

現場起点の一次情報

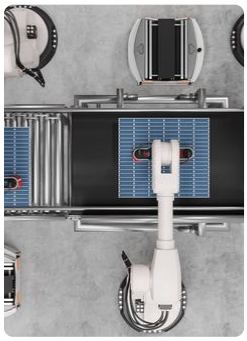
インシデント対応と実環境のOT脅威データから継続収集

検知・対応への直結

知見を検知ロジックとして即座に実装

ご活用いただける業界

製造　エネルギー　電力・ガス・水道　ライフサイエンス　石油化学・素材　ハイテク　通信・メディア　公共インフラ・防衛








※ runZeroはIT資産も対象のため、全業界でご活用いただけます

貴社担当または下記よりお気軽にお問合せください。

お問合せ　https://www.accenture.com/jp-ja/about/company/contact-us