Trellix

SOLUTION BRIEF 翻訳版

Securing the Oil and Gas Digital Frontier

石油・ガス業界において、サイバー侵害はもはや単なるデータ損失にとどまりません。業務の中断、安全性の脅威、環境リスク、そしてより広範な国家のエネルギー安全保障への懸念を引き起こす可能性があります。

2024年から2025年の間に同セクターを狙ったランサムウェア攻撃が935%増加し、計画外のダウンタイムには1時間あたり平均12万5,000ドルのコストがかかる現状を考慮すると、石油・ガスのリーダーは、エンタープライズITとミッションクリティカルな運用技術(OT)の両方を保護する、回復力のあるサイバーセキュリティ戦略を必要としています。[1,2]

この戦略を実現するため、Trellixは、企業ITからOT隣接環境、そして上流・中流・下流の業務にわたる重要産業環境までを網羅する、統合されたセキュリティアーキテクチャを提供します。脅威インテリジェンス、エンドポイント保護、ネットワーク検知・対応(NDR)、データセキュリティ、セキュリティオペレーション、コンサルティングサービス、および戦略的パートナーシップを組み合わせることで、Trellixは石油・ガス組織がバリューチェーン全体にわたって運用のレジリエンス(回復力)を強化し、産業上の機密データを保護し、資産の可用性を維持できるよう支援します。

Trellixはまた、厳格な規制や標準に基づく要件に対応するため、お客様が可視性と制御性を向上できるよう支援します。これには、対象となるパイプライン事業者が、米国のTSA(運輸保安庁)パイプラインセキュリティ指令(TSA Pipeline Security Directives)のネットワークセグメンテーション(ネットワーク分離)、アクセス制御、継続的モニタリング、およびサイバーセキュリティ実施計画に準拠できるよう支援すること、米SEC(証券取引委員会)のサイバーインシデント開示への備えとして、より迅速な調査と対応をサポートすること、そして、多層防御、ネットワーク分離、資産の可視性、リスクベースのセキュリティ設計を含む、産業サイバーセキュリティのためのISA/IEC 62443の原則にお客様が準拠できるよう支援することが含まれます。

1 Dragos OT Cybersecurity Report: Adversaries Increase Real-World Impact, Map Control Loops Across Industrial Infrastructure, 2026

2 IBM, Cost of a data breach: The industrial sector, 2024

IT/OTのコンバージェンス(融合)に最適化された統合ソリューションの提供

クラウド技術やリモートアクセス、自動化、デジタル運用の導入により、石油・ガスの操業(オペレーション)の相互接続が拡大するにつれ、組織はエンタープライズITと産業用OT環境の両方で増大するサイバーセキュリティリスクに直面しています。これらの主なリスクは以下の通りです。

- 脆弱なIT/OTのセグメンテーション(ネットワーク分離)
- レガシーOTの脆弱性と安全性の低いプロトコル
- 安全でないリモートアクセス
- 限定的な資産の可視性
- ランサムウェアや国家主導の脅威への直面
- 専門的なOTサイバーセキュリティ人材・専門知識の不足

Trellixは、エンドポイント保護、ネットワークの検知と対応(NDR)、データセキュリティ、およびセキュリティオペレーションに重点を置いた、IT/OT 融合型環境向けの統合サイバーセキュリティ機能を提供することで、これらの課題解決を支援します。Trellixのソリューションは、厳格な制限が課された環境やエアギャップ(隔離)環境を含む完全なオンプレミス展開をサポートすると同時に、ハイブリッドやクラウド接続アーキテクチャ全体に保護を拡張することも可能です。

これにより、石油・ガス事業者は、重要な業務に求められる可用性と安定性を損なうことなく、上流、中流、下流のすべての環境において、可視性の向上、保護の強化、脅威の早期検知、そして迅速な対応を実現できます。

多層的な検知・対応アーキテクチャの提供

断片化されたポイントソリューションとは異なり、Trellixは稼働時間、運用制御、およびサイバーレジリエンス(回復力)を維持・サポートするように設計された、OT環境を考慮した統合セキュリティアーキテクチャを提供します。この防御の中核となるのが、エンドポイント保護、ネットワークの可視化、脅威インテリジェンス、そしてセキュリティオペレーションを融合させた多層的な検知・対応フレームワークです。

- **エンドポイントセキュリティ:** Trellix endpoint security ソリューションは、上流、中流、下流のすべての環境において、サーバー、ワークステーション、エンジニアリングシステム、中継ホスト、フィールドデバイス、およびOT隣接エンドポイントの保護を支援します。これらの機能は、防御、検知、調査、封じ込め、および復旧をサポートすると同時に、アプリケーション制御、デバイス制御、許可/拒否リスト、ホストファイアウォールポリシー、フォレンジック主導の対応などの制御を通じて攻撃面の縮小を支援します。またTrellixは、クラウド接続が制限または禁止されている環境向けに、オンプレミスやネットワークから切り離された(隔離された)導入モデルもサポートしています。

- **ネットワークの検知と対応(NDR):** Trellix Network Detection and Response (NDR)、NozomiNetworksなどのパートナーが提供するOTエコシステム機能と連携し、IT、OT、およびSCADAに接続された環境全体における可視性の向上を支援します。ネットワーク通信パターンの監視、不審な挙動の特定、異常検知、および資産の可視化のサポートにより、Trellixはセキュリティチームが産業環境を標的とするラテラルムーブメント(組織内横展開)、不正アクセスの試み、および高度な脅威を特定できるよう支援します。

- **セキュリティ運用:** Trellixは、統合セキュリティプラットフォームを通じて、エンドポイント、ネットワーク、データ、脅威インテリジェンス、およびセキュリティオペレーションのテレメトリ(遠隔測定データ)を相互に接続します。Trellix Wiseをはじめとする AI支援機能により、アナリストは重要アラートの優先順位付け、アラート疲れの軽減、そして調査と対応の迅速化を図ることができます。OT環境においては、セキュリティチームがエンタープライズIT、OT隣接システム、産業ネットワーク、およびSOCワークフローにまたがるアクティビティを相互に関連付けられるようになると同時に、重要な業務の可用性と安定性の維持を支援します。

これらの機能が一体となることで、石油・ガス組織は、単独の検知からバリューチェーン全体にわたる協調的な防御へと移行できるようになります。これにより、可視性が向上し、対応時間が短縮され、ランサムウェア、不正な変更、ラテラルムーブメント(組織内横展開)、および標的型攻撃に対するレジリエンス(回復力)が強化されます。

機密データの保護

石油・ガス企業は、パイプラインのテレメトリ(遠隔測定データ)、地震データ、生産記録、製油所データ、エンジニアリング設計、商業契約、取引情報、顧客記録、規制データなど、大量の機密情報や運用上重要な情報を扱います。

Trellixは、エンドポイント、ネットワーク、クラウドストレージ、およびデータベース全体のデータを保護する、**データ損失防止**(Data Loss Prevention (DLP))および**データベースセキュリティ機能**(Database Security)を通じて、これらの情報の保護を支援します。これらのソリューションは、機密データの移動の監視、不正アクセスの検知、データベースアクティビティの監査、特権ユーザーの監視、そしてデータ漏洩リスクの低減を支援します。

これは、運用データがエンタープライズシステム、クラウドプラットフォーム、ヒストリアン(操業実績)データベース、分析環境、データレイクなどとますます共有されるようになっている、IT/OTのコンバージェンス(融合)領域において特に重要です。Trellixは、保存データ(Data at rest)と移動データ(Data in motion)の両方を保護することにより、石油・ガス事業者が知的財産を守り、コンプライアンスを維持し、運用上または商業上のリスクにさらされる危険性を低減できるよう支援します。

石油・ガスバリューチェーン全体の強化

Trellixのソリューションは、IT、OT隣接環境、および産業用環境における保護、可視性、検知、対応を強化することにより、石油・ガスの上流、中流、下流の各工程における固有のサイバーセキュリティ課題への対処を支援します。

- **上流工程 - インテリジェントエッジの保護:** Trellixは、オフショア・リグ(海洋掘削リグ)、掘削作業、フィールドエンドポイント、エンジニアリングワークステーション、請負業者のアクセスなど、リモートでの探査および生産環境の保護を支援します。これには、ウェルヘッド(坑口)センサー、フィールドシステム、エッジ環境からエンタープライズやクラウドプラットフォームへのデータフローの安全確保を支援すると同時に、地震データ、坑井データ、生産データ、エンジニアリング設計などの高価値な知的財産の保護も含まれます。

- **中流工程 - パイプラインの完全性維持:**高度に分散したインフラの保護を支援するため、Trellixはパイプラインの運用、ターミナル、ポンプステーション、圧縮ステーション、およびSCADAに接続された環境全体の可視性を向上させます。ネットワークの検知と対応(NDR)、エンドポイント保護、および脅威インテリジェンスは、輸送・貯蔵インフラを標的とする不審なアクティビティ、不正アクセスの試み、ラテラルムーブメント(組織内横展開)、および潜在的な脅威の特定を支援します。

- **下流工程 - 安全第一の製油所保護の推進：** 稼働時間、安全性、およびプロセスの継続性が最優先される製油所や石油化学プラントにおいて、TrellixはOT隣接システム、エンジニアリングワークステーション、プラントエンドポイント、データリポジトリ、およびネットワーク通信の保護を支援します。エンドポイント、ネットワーク、データ、およびセキュリティオペレーションのテレメトリを相互に関連付けることで、Trellixは重要な産業業務を中断することなく、異常の検知、重要アラートの優先順位付け、そして調査と対応の迅速化を支援します。

Trellixのコンサルティングとパートナーシップによるセキュリティの強化

テクノロジー単体では、極めて複雑でミッションクリティカルな石油・ガス環境を完全に保護することはできません。多くの組織が、専門的なOTサイバーセキュリティの専門知識、アーキテクチャ設計、導入準備、運用ガバナンス、およびインシデント対応計画におけるギャップに直面しています。これらの課題は、生産活動、安全システム、またはプラントの可用性を阻害することなくセキュリティ統制を導入しなければならない場合に、さらに極めて重大なものとなります。

Trellixは、経験豊富なプロフェッショナルサービス、アドバイザリーサポート、およびテクノロジーと業界における広範なパートナーエコシステムを通じて、このギャップを埋める支援をします。Trellixのプロフェッショナルサービスは、お客様が現在のIT/OTセキュリティ状況を評価し、実用的な導入アーキテクチャを設計し、セグメンテーション（ネットワーク分離）と可視性の要件を検証し、実装をサポートし、検知機能をチューニングし、そしてセキュリティオペレーションをビジネスおよび運用上のリスクと整合させることを支援します。

コンサルティング主導の取り組みとパートナーとの協調を通じて、Trellixは石油・ガス組織が単なる製品の導入にとどまらず、可視性の向上、重要な資産に対する制御の強化、脅威検知の迅速化、運用リスクの低減、そしてよりレジリエンス（回復力）の高い上流、中流、下流の運用を含む、測定可能なセキュリティ成果を達成できるよう支援します。

Trellix プロフェッショナルサービス

Trellixプロフェッショナルサービスは、複雑なIT/OT環境向けに設計されたカスタムの作業範囲（SOW）、導入に関する専門知識、および特化した手法を通じて、石油・ガス組織がTrellixへの投資価値を最大限に高められるよう支援します。これらのサービスは、稼働時間、安全性、または生産の継続性を損なうことなく、お客様がリスクを評価し、レジリエンス（回復力）の高いアーキテクチャを設計し、統制を実装し、そしてセキュリティを運用化できるよう支援します。主なサービスは以下の通りです。

- **OT環境の評価およびインベントリ（資産棚卸）：** Trellixのコンサルタントは、OTセキュリティ評価、資産の可視性レビュー、ネットワークおよびエンドポイントの振る舞いに関するベースライン分析、そしてIT/OTのセグメンテーション（ネットワーク分離）レビューをサポートします。これらの取り組みにより、エンタープライズ側の侵害が生産環境へ拡散するリスクを低減し、重要なOTの依存関係に対するお客様の理解を向上させます。
- **インシデント対応の備え：**Trellixの専門家は、産業固有の運用要件、安全上の配慮、および適用される規制上の義務に沿った、OTを考慮したインシデント対応プレイブック、エスカレーションモデル、および対応テンプレートの開発を支援します。これにより、セキュリティチームと運用チームが、重要なシステムへの影響を最小限に抑えながら、より迅速に対応できるよう支援します。
- **データセキュリティの展開:** Trellixプロフェッショナルサービスは、地震データ、坑井データ、生産データ、エンジニアリング文書、商用契約、および運用記録を含む、機密性の高い石油・ガスデータに対するデータ分類（クラシフィケーション）の取り組み、データベースのリスク評価、およびDLP（データ損失防止）ポリシーの設計をサポートします。これらのサービスにより、知的財産の漏洩や不正なデータ移動のリスクを低減します。

- **継続的モニタリングの導入（デプロイメント）：**Trellixのコンサルタントは、上流、中流、下流の各環境におけるエンドポイント、EDR、NDR、およびセキュリティオペレーション機能の導入と設定を支援します。サービスには、センサー配置に関するガイダンス、検知機能のチューニング、SOC（セキュリティオペレーションセンター）ワークフローとの統合、脅威ハンティングの有効化、ならびに継続的な監視を行う社内SOCチームやマネージドサービスパートナーへの運用引き継ぎなどが含まれます。

戦略的OEMおよびインテグレーターとのパートナーシップ

Trellixは、テクノロジーパートナー、OEM、システムインテグレーター、およびマネージドサービスパートナーと連携し、石油・ガス組織が複雑な産業環境全体にセキュリティを拡張できるよう支援します。これらのパートナーシップは、安全性、稼働時間、システムの完全性、およびベンダーによるサポート可能性を維持するために、サイバーセキュリティ統制を慎重に導入しなければならないOT環境において特に重要となります。

- **OEMおよびテクノロジーパートナー：**Trellixは、テクノロジーおよびインフラストラクチャのパートナーと連携し、産業用アーキテクチャや運用要件に沿ったセキュリティ統制の調整を支援します。お客様のアーキテクチャやベンダーのエコシステムでサポートされている場合、Trellixの機能は、OT隣接システム、エンジニアリングワークステーション、サーバー、および重要な運用インフラストラクチャ全体におけるエンドポイント保護、アクセス制御、データ保護、暗号化通信、およびモニタリングの強化に貢献します。これにより、運用の整合性とコンプライアンス要件を維持しながら、レジリエンス（回復力）を高めることができます。
- **システムインテグレーター：** Trellixは、石油・ガス事業、OTネットワーク、SCADA環境、および産業特有の導入制約を熟知しているシステムインテグレーターと提携しています。パートナーの能力向上、アーキテクチャ面での協調、および導入サポートを通じて、Trellixはシステムインテグレーターが、OTセキュリティ評価、資産の可視性、エンドポイント保護、ネットワークモニタリング、セグメンテーション（ネットワーク分離）レビュー、SOC統合、そして運用引き継ぎなどの領域にわたり、より安全な導入を計画・実行できるよう支援します。

これらのパートナーシップが一体となることで、お客様は個別に孤立したテクノロジーの導入から、上流、中流、下流の各運用全体にわたって調整・統合されたセキュリティモデルへと移行できるようになります。

結論

統合されたセキュリティアーキテクチャ、深いコンサルティングの専門知識、そして強力なパートナーエコシステムを組み合わせることで、Trellixは石油・ガスのリーダーが自社の運用、人材、データ、および評判を保護できるよう支援します。隔離された環境（エアーギャップ環境）、遠隔地の上流拠点、高度に分散されたパイプラインネットワーク、またはIT/OTが融合した環境のいずれにおいても、Trellixは運用のレジリエンス（回復力）を強化するために必要な可視性、保護、脅威検知、および対応機能を提供します。Trellixにより、石油・ガス組織はバリューチェーン全体にわたるサイバーリスクを低減し、セキュリティ運用を改善し、産業上の機密データを保護するとともに、より安全でレジリエンス（回復力）の高い上流、中流、下流の運用を支援することができます。

詳細については、お問い合わせいただくか、弊社ウェブサイトをご覧ください。trellix.com