OTセキュリティ / 技術データシート

zcrOT

OT通信を可視化。
コンテキストに基づいて調査。

zcrOTは、パッシブなネットワーク可視化、Modbus対応の検知、エネルギーテレメトリを統合し、産業・エネルギー分野の運用チームを支援します。

提供形態

- クラウド / SaaS
- 仮想マシン（VM）
- ハードウェア機器

1 **観測** TAP / SPAN・テレメトリ

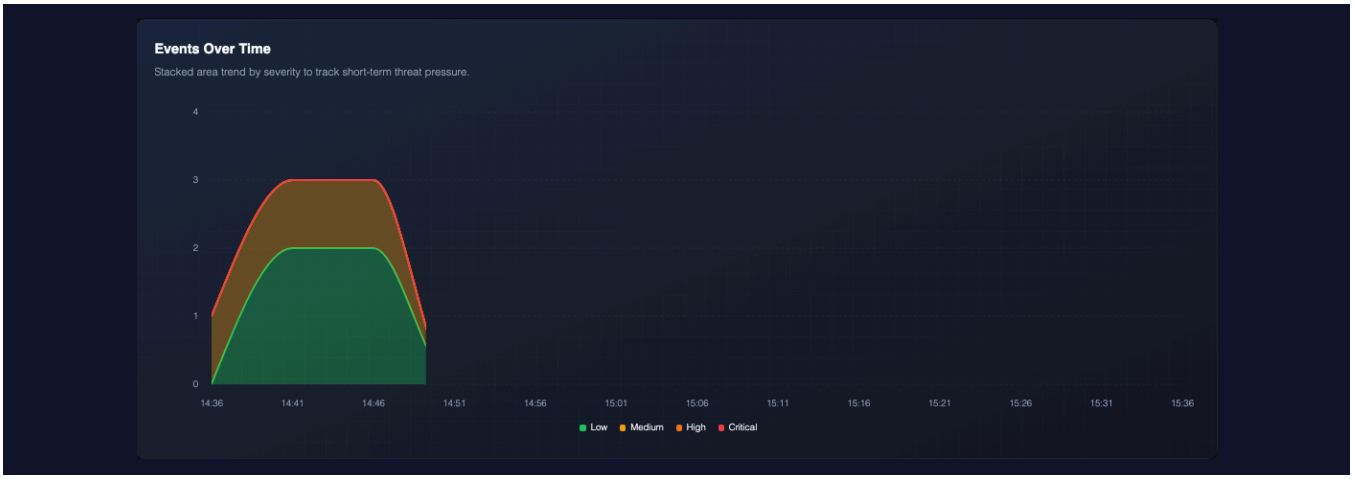
2 **関連付け** 資産・経路・基準値

3 **調査** リスク・イベント分析

4 **報告** 週次・月次のレビュー

概念的な運用フローであり、物理構成図ではありません。制御や通信の遮断を示すものではありません。

イベントの推移を確認



Security Exposure → Events Over Time：選択期間における重大度別のイベント件数の推移です。デモ環境のサンプルデータであり、数値は顧客実績、処理上限、検知精度を示しません。製品画面は英語表示です。 元の画面を拡大表示

本書の構成

2 技術的な機能範囲
3 提供形態と商用条件
4 導入と運用の境界
5 導入前に根拠を確認する
6 資産とプロトコルメタデータ
7 検知と制御の信頼性
8 パケット証拠とエクスポート
9 相関分析・管理・レポート

技術的な範囲

技術的な機能範囲

02

観測した通信、プロトコル、テレメトリの情報から、調査すべき資産やイベントを絞り込みます。

機能	技術的な範囲
パッシブな資産把握	ネットワークTAP、SPAN／ミラーポート、センサーフィードからOT通信とIT/OT境界を観測します。可視化範囲は収集範囲に依存します。
通信マッピング	送信元、宛先、プロトコル、ポート、方向を表示。OTゲートウェイや論理ユニットと観測された通信経路を関連付けます。
Modbus対応検知	read、write、error、malformedコマンドを分類します。必要なプロトコルバージョンと現場固有の通信は評価時に検証してください。
識別とリスク情報	既知・未知デバイスのタグ、識別情報、リスクスコア、攻撃可能性の判定を調査の優先付けに利用します。侵害の確証ではありません。
行動ベースライン	センサー通信をリアルタイムまたは準リアルタイムに分析し、基準となる挙動と比較して変化を調査します。経路全体の遅延保証ではありません。
エネルギーテレメトリ	現在・過去のテレメトリを保存・分析します。入力が得られる範囲で、太陽光発電の出力、電気自動車（EV）充電器の状態、工場電力を扱います。
データ取り込み	送信元ごとの専用syslog取り込みポートとリアルタイムの通信カウンターで、想定した入力の到着を確認します。
調査とレポート	インシデントのトリアージでイベントを確認し、OT可視化・セキュリティの週次／月次レポートを作成します。内部レビュー用であり、認証取得を証明するものではありません。
API連携	システム接続用インターフェース（API）と連携基盤を通じ、セキュリティ運用センター（SOC）、セキュリティ情報・イベント管理（SIEM）、監視・分析の業務に接続します。具体的なインターフェースと項目は要確認です。

制御・運用技術（OT）、産業用制御システム（ICS）、プラント、ネットワーク、セキュリティの担当者、およびマネージドセキュリティサービスを提供するパートナー向けです。

技術的な範囲

提供形態と商用条件

03

SaaS、VM、ハードウェアアプライアンスで提供します。インフラ仕様を決める前に、承認済みパートナーと導入方式・データの境界を確認してください。

導入方式	パッケージと商用条件
zcrOT-Appliance	初年度を含む買い切り価格は฿3,200,000（VAT別）です。セキュリティコレクター1台、zcrLogサーバー1台、zcrOTソフトウェアスタック1式を含みます。2年目からの年間保守（MA）はパッケージ税抜価格の30%、年額฿960,000にVATを加算します。
クラウド / SaaS	年額฿1,500,000（VAT別）です。セキュリティコレクター1台、zcrLog SaaSの1年分、zcrOTソフトウェアスタック1式を含みます。
仮想マシン（VM）	顧客管理のオンプレミスVMも提供しています。構成、インフラ、提供範囲に応じて承認済みパートナーが見積もります。このパッケージ資料にVM単体の定価はありません。

両パッケージに含まれるもの

システム連携・導入試運転、AI検知モデル、脅威インテリジェンスと更新、Cloud APIによる監視、サポート。ハードウェア仕様、導入の検収条件、更新時の範囲、対応時間、SLAは承認済みパートナーと合意してください。

> 2026年10月31日時点。記載価格はすべてVAT別で、機器、SaaS、年間保守の料金にVATを加算します。機器の保守は2年目から、パッケージ税抜価格の30%です。実際の見積もりとその有効期間はパートナーが確認します。

デモの数値ではなく、現場からサイジング

セグメント、コレクター、通信量、テレメトリ入力元、保存期間、報告頻度でサイジングします。同梱の台数・式数は、利用許諾されたセグメント数や処理容量を示しません。CPU、RAM、保存容量、処理性能、センサー上限、追加取得ポイント、VM価格、ハードウェア構成、SLAはパートナーの提案で確定します。既定の処理容量は示していません。

技術的な範囲

導入と運用の境界

04

制御経路から独立したパッシブ可視化

パッシブ監視は制御通信の経路上ではなく、複製された通信を利用します。この監視方式では端末エージェントは不要で、OT機器を直接制御しません。収集設定の変更や作業時間はプラント管理者と合意してください。パッシブ方式でも導入リスクがゼロとは限りません。

分離ネットワークとオフライン環境

アプライアンスによるオフライン監視を計画する場合は、ライセンス、更新、サポート接続、時刻同期、データ出力手順を分離環境で検証してください。すべての連携機能がオフラインで動作するとは限りません。

外部連携の境界を決める

入力元 → 収集機器 → プラットフォーム → 連携先を整理し、syslog/APIの形式、認証、データ方向、担当者を確認します。本書は特定ベンダーのコネクターや自動対応を約束するものではありません。

> 一次サポートはチャネルパートナーが担当し、zcrがパートナーを支援します。対応時間、エスカレーション、SLA、導入範囲、保守責任は提案時に合意します。

OTネットワークで何が起きているか？

観測した資産と通信経路を可視化し、既知・未知のデバイスを識別。プロトコルの背景情報を使って異常な活動を調査します。可視化の範囲は、プラットフォームに提供される通信とテレメトリに依存します。

技術的な範囲

導入前に根拠を確認する

05

評価の成果は画面を表示することだけではありません。可視化の範囲と運用引き継ぎの条件を合意します。

評価項目	確認する内容
収集の範囲	セグメント、取得ポイント、接続口、観測できない通信を明確にします。
プロトコルと機器	代表的なModbus read/write/error、ゲートウェイ、既知・未知デバイスの識別を確認します。
データとイベント	現場で承認されたテストデータを使い、入力カウンター、時刻、電力単位、イベントの背景情報を確認します。
運用条件	保存期間、報告頻度、権限管理、サポート・保守の責任範囲を合意します。

デモの数値ではなく、現場からサイジング

セグメント、コレクター、通信量、テレメトリ入力元、保存期間、報告頻度でサイジングします。同梱の台数・式数は、利用許諾されたセグメント数や処理容量を示しません。CPU、RAM、保存容量、処理性能、センサー上限、追加取得ポイント、VM価格、ハードウェア構成、SLAはパートナーの提案で確定します。既定の処理容量は示していません。

承認済みパートナーと評価を計画する

ネットワーク構成図、セグメント・センサーの概数、入力元、導入上の制約をご用意ください。商用提案、契約、顧客への提供は承認済みのディストリビューター、販売代理店／SI、MSP／MSSPを通じて行います。zcr.aiはパートナーへの橋渡しを支援します。

パートナーの紹介・範囲の相談 ↗　zcrOTの詳細 ↗　公開デモを試す ↗

zcr.ai/ja/contact/ · zcr.ai/ja/product/zcrot/ · demo.ot.zcr.ai

技術範囲・合意した導入構成

資産とプロトコルメタデータ

06

現場の代表的な通信で、項目、プロトコル対応範囲、フィルターを検証します。

技術範囲・合意した導入構成

以下の機能は、合意した導入構成で提供できます。承認済みパートナーと、入力元、プロトコルのバージョン、インターフェース、権限、保存期間、運用条件の検収基準を定めてください。必要な相互運用性と分離環境の運用手順は導入前に検証します。本書は容量、性能、認証、SLAの数値や保証を規定しません。

機能	技術的な範囲
資産情報	IP・MACアドレス、プロトコル、ポート、機器種別、論理ユニット、通信方向、マッピング状態。名称、説明、グループにより既知・未知の機器、エンジニアリング端末、ネットワーク基盤、産業用ゲートウェイ、その他のOT資産を区別します。
経路とフィルター	内部・外部・主要な通信経路と、初めて観測した通信経路、および通信量。時間、機器、プロトコル、リスク、方向で絞り込みます。ベースラインと比較し、未知の機器、外部宛先、経路変更、横展開や指令通信の可能性を調べます。
ゲートウェイの背景情報	Ethernet/IPで直接観測した資産と、ゲートウェイのテレメトリで識別する論理OTユニットを区別します。IPアドレスだけでは各ユニットを識別できない場合があります。
メタデータ項目	時刻、送信元IP/MAC、宛先IP/MAC、プロトコル、ポート、方向、セッション情報、分類、関連する異常状態。毎回生パケットを開かずに検索・関連付けを行います。
プロトコル一覧	HTTP、DNS、SMB、HTTPS、TLS、TCP、UDP、ICMP、SNMP、Modbus TCP、EtherNet/IP。パーサーのバージョンと項目の対応範囲を検証します。この一覧は相互運用性の認証ではありません。
アプリケーション項目	HTTP：メソッド、ホスト、URI、ステータスコード、ユーザーエージェント、方向。DNS：クエリ、応答、レコード種別、解決先IP、異常挙動。SMB：セッション、ユーザー、共有、ファイル操作、横展開に関連する活動。

技術範囲・合意した導入構成

検知と制御の信頼性

07

ルールと運用指標を検証します。防御や検知精度の保証とは解釈しません。

技術範囲・合意した導入構成

以下の機能は、合意した導入構成で提供できます。承認済みパートナーと、入力元、プロトコルのバージョン、インターフェース、権限、保存期間、運用条件の検収基準を定めてください。必要な相互運用性と分離環境の運用手順は導入前に検証します。本書は容量、性能、認証、SLAの数値や保証を規定しません。

機能	技術的な範囲
Modbusの信頼性	ユニット・操作ごとのリクエスト量、エラー数、応答時間、Slow Poll、成功率、論理ユニット状態。履歴比較で運用性能の低下や生産への影響の可能性を調べます。処理量や遅延の数値は規定していません。
運用上の異常	異常なリクエスト、これまで観測されていなかったModbusファンクション、不許可ユニットへの接続、エラー増加、異常な応答時間、稼働時間外の活動。
ルールの入力	通信、プロトコルメタデータ、資産情報、運用テレメトリを使う標準・カスタムルール。条件は送信元、宛先、プロトコル、ポート、方向、資産、時間枠、ベースライン、重大度、イベント分類です。
検知例	未知のクライアント、新規経路、外部通信、営業時間外の活動、不許可プロトコル、不審なポート、Modbusの中断、異常なリクエスト量、反復エラー、Slow Poll、ベースラインからの逸脱。
優先順位と調整	重大度、リスクスコア、判定、分類。承認済み活動の許可リストとルール調整。誤検知への効果は検証し、削減を保証するものとは扱いません。
状況とライフサイクル	セキュリティイベント、高・緊急イベント、未知のクライアント、攻撃可能性の判定、推移、判定分布、主要リスク元と、詳細・証拠への掘り下げ。関連インシデントは資産、アラート、プロトコル、送信元・宛先、重大度、時系列、証拠を検知から終結まで扱います。

技術範囲・合意した導入構成

パケット証拠とエクスポート

08

証拠として利用する前に、取得、保存期間、アクセス権、出力動作を検証します。

技術範囲・合意した導入構成

以下の機能は、合意した導入構成で提供できます。承認済みパートナーと、入力元、プロトコルのバージョン、インターフェース、権限、保存期間、運用条件の検収基準を定めてください。必要な相互運用性と分離環境の運用手順は導入前に検証します。本書は容量、性能、認証、SLAの数値や保証を規定しません。

機能	技術的な範囲
取得形式	現場のネットワークセンサーでフルパケットを取得し、ネットワーク・OT調査用にPCAPまたはPCAPNGを保存します。実際の取得口、容量、保存領域、保存期間を確認します。本書は数値を規定しません。
取得ポリシー	センサー、セグメント、プロトコル、資産、時間枠、検知ルール、重大度で取得範囲と量を制御し、重要システム・資産の通信を優先します。
条件付き証拠取得	IDSシグネチャー致時に、検知前・検知中・検知後の関連PCAPを自動記録し、アラートやインシデントへ関連付けます。提案構成でバッファー、発火時刻、動作を検証します。
インシデント参照	調査画面のセンサー、取得時刻、送信元IP、宛先IP、プロトコル、ファイルサイズ、ハッシュ、インシデント参照。ハッシュの表示だけでは証拠保全の連続性を認証しません。
権限に基づく出力	権限を持つ利用者が関連PCAPを安全な経路でコピー、ダウンロード、出力し、Wiresharkや外部のネットワークフォレンジックツールで分析します。
証拠の継続性	時刻、取得メタデータ、インシデント参照、監査に必要な参照情報を保持し、SOC、インシデント対応、デジタルフォレンジック担当が外部で分析できるか確認します。権限、転送方式、保持項目も検証します。

技術範囲・合意した導入構成

相関分析・管理・レポート

09

提案するエディションで、システム間の関連付け、管理、レポートを検証します。

技術範囲・合意した導入構成

以下の機能は、合意した導入構成で提供できます。承認済みパートナーと、入力元、プロトコルのバージョン、インターフェース、権限、保存期間、運用条件の検収基準を定めてください。必要な相互運用性と分離環境の運用手順は導入前に検証します。本書は容量、性能、認証、SLAの数値や保証を規定しません。

機能	技術的な範囲
システム間の相関	ネットワーク、端末、ID・利用者、クラウド、その他のセキュリティ制御のイベントを同一ケースへ自動分類。照合ロジック、入力元、エディションを確認します。自動対応を意味しません。
関係と根本原因	アラート、エンティティ、ホスト、利用者、IP、資産、プロセス、ファイル、セッションの関係と時系列・キルチェーン表示。ネットワーク・端末・ID・クラウド・制御のイベント、メタデータ、検知、PCAPから初動、横展開、指令通信、データアクセス、影響を追います。
EDRと外部入力	API、Webhook、Syslog、連携基盤。端末アラート、プロセス、コマンドライン、ファイル、ハッシュ、利用者、接続、緩和措置の情報。EDR、SIEM、ID、クラウド、ファイアウォール、IDS/IPS、チケット、監視との接続を検証します。特定コネクターや緩和措置の実行は未確認です。
管理	資産、経路、露出、インシデント、電力、ポート、利用権限、入力状態の集中表示。IP、MAC、Modbus Unit IDから名称・種別・詳細を設定。専用syslogポート、センサー入力、テレメトリ元の最終活動、カウンター、追加・無効化・編集を確認します。
レポート	Executive SummaryとOT Visibility & Security Report：観測資産、既知・未知機器、経路、イベント、高・緊急イベント、インシデント、主要リスク元、制御信頼性、全体リスク。期間、推移、主要イベントの要約、経営・OT・セキュリティ・内部レビュー用出力を検証します。
分離環境	オンプレミスVM・機器では、合意したオフライン・分離環境を計画します。データ所在地、ライセンス、更新、時刻同期、支援、出力を確認します。すべての連携がオフラインで動くとは限りません。