Cisco Cyber Vision

目次

Cisco® Cyber Vision は、産業分野の組織および重要なインフラストラクチャ向けに構築されたサイバーセキュリティ ソリューションです。運用テクノロジー（OT）に対するセキュリティ機能を提供し、OT の攻撃対象領域を減らし、脅威の拡大を防止し、リモート アクセス アクティビティを保護し、IT セキュリティを産業向けの設定に拡張して、サイバー攻撃に耐えうる産業用ネットワークの構築に役立ちます。

製品の概要

生産工程のデジタル化を進めて、IT、クラウド、産業用ネットワークを緊密に統合するほど、産業用制御システム（ICS）と OT 設備はサイバー攻撃の脅威にさらされることになります。ここで必要となるのは、生産工程の継続性、復元力、安全性の確保に役立つソリューションです。

Cyber Vision を導入することにより、OT のセキュリティ状況を継続的に可視化できるため、攻撃対象領域を減らすための現状把握ができます。シスコの主要なセキュリティポートフォリオとの緊密な統合により、ネットワークのセグメンテーションによる業務の保護が容易になります。ネットワークのセグメンテーションは、数年ではなく数週間で導入可能です。ゼロトラスト ネットワーク アクセス（ZTNA）機能により、業務チームが OT 設備へのセルフサービス リモート アクセスを実施できるようにする一方で、最小権限のポリシーを適用できます。

Cyber Vision は、OT セキュリティ機能を産業用ネットワークに組み込む独自のエッジ アーキテクチャを使用しています。専用のセキュリティアプライアンスを導入したり、パケット収集用の別面ネットワークを構築したりする必要はありません。設備を接続するネットワークは、接続するすべての設備についてプロファイリングを行い、悪意のあるトラフィックと異常なアクティビティを検出し、IEC 62443 のゾーンとコンジットを適用して、設備にリモートアクセスできるユーザーを制御します。大規模に導入できる OT セキュリティ、それが Cisco Cyber Vision です。

機能と利点

表 1. 機能と利点

機能	利点
OT 設備一覧とセキュリティ態勢に対するリアルタイムの可視性	把握していないものを保護することはできません。生産設備の一覧を使用して、OT セキュリティプラクティスを構築できます。この一覧は自動生成され、常に最新の状態に保たれます。脆弱性、通信パターン、悪意のある通信、異常な動作などに関する包括的な可視性に基づいた対策を促進し、OT のセキュリティ態勢を強化します。
OT ネットワーク セグメンテーション	IEC 62443 のゾーンとコンジットを導入して、生産工程を保護します。Cyber Vision は、制御エンジニアが設備をゾーン（生産セル、建物、変電所など）にグループ化するのに役立ちます。これにより、IT チームは Cisco ISE または Secure Firewall を使用して適切なセグメンテーション ポリシーを適用するためのすべての情報を取得できます。
ゼロトラスト リモート アクセス	Cyber Vision に新たに組み込まれた Cisco Secure Equipment Access により、業務チームは最小権限のポリシーを適用できるセルフサービス リモート アクセスを実施できます。
ネットワーク組み込みセンサー	一部のシスコのネットワーキング機器に組み込まれた Cyber Vision センサーにより、OT セキュリティを大規模に簡単に導入できます。 • 専用アプライアンスを導入する必要はありません。OT の可視化は、スイッチとルータで有効化するソフトウェア機能であり、CAPEX と OPEX の両方を節約できます。 • ネットワークリソースや複雑なネットワークセットアップを追加する必要はありません。Cyber Vision センサーは、軽量のメタデータを Cyber Vision Center に送信します。これは、ネットワーク通信量の 2% ～ 5% の追加にすぎません。 • ネットワークに接続するスイッチで実行されている Cyber Vision センサーのおかげで、最も低い Purdue レベルのものであっても、すべての OT 設備を簡単に識別できます。

機能	利点
ハードウェアおよび Docker センサー	ルータやスイッチでセンサーソフトウェアを実行できない場合に、ブラウンフィールド環境に Cyber Vision センサーを簡単に導入できます。 • 産業用ネットワーク内にサイバービジョンセンサーを導入することで、SPAN 収集ネットワークを構築する必要がなくなります。Cisco IC3000 産業用コンピューティング ゲートウェイまたは Docker を実行しているコンピューティング ハードウェアにセンサーソフトウェアをインストールし、短い 1 ホップ SPAN を使用して既存のスイッチから可視性を取得します。 • 既存の SPAN 収集インフラストラクチャを使用して、既存のスイッチから Cyber Vision Center に通信を送信します。Cyber Vision Centerには、通信をデコードして情報を抽出し、アクティブクエリを設備に送信するセンサーソフトウェアがインストールされています。
OT 可視性センサーと ZTNA ゲートウェイの組み合わせ	シスコの産業用ネットワーク機器を使用して、Cyber Vision センサーと Secure Equipment Access ZTNA ゲートウェイソフトウェアを同時に実行することにより、大規模な導入を簡素化します（一部のモデルのみ）。
ゼロタッチプロビジョニング	Cyber Vision センサーの登録を自動化し、大規模なインフラストラクチャを数分で展開します。手動タスクやサービスの中断を行うことなく、センサーを簡単に最新の状態に保ちます。
パッシブディスカバリとアクティブディスカバリ	Cyber Vision は、産業用制御プロトコルのディープ パケット インスペクション（DPI）を使用してネットワーク通信を受動的にキャプチャおよびデコードすることにより、生産工程を監視します。実行中の特定の ICS プロトコルの意味論において非常に正確で非破壊的な要求を送信するアクティブディスカバリによって、より多くの情報を収集できます。
分散エッジアクティブディスカバリ	Purdue モデルの最下位レベルに展開されているものも含め、すべてのネットワーク接続された設備を包括的かつ詳細に可視化します。センサーは設備が接続されているスイッチで実行されているため、Cyber Vision のアクティブディスカバリ要求はファイアウォールまたはネットワークアドレス変換（NAT）の境界によってブロックされません。
すべての拠点の広域ビュー	すべての産業拠点の詳細なセキュリティ情報でガバナンスと規則遵守を推進します。Cyber Vision Global Center はすべてのローカルセンターからのデータをシームレスに集約するため、CISO とセキュリティチームは、拠点ごとや拠点をまたがって設備とイベントを一元的に可視化できます。
設備一覧レポート	設備の有意義な可視化と内訳を示す正式に作成されたエグゼクティブ サマリー レポートで、設備一覧を常に把握します。必要に応じてレポートをカスタマイズしてホワイトラベルを付け、Word または PDF ドキュメントとして関係者と共有します。
OT タグ	各デバイスの役割と何を実行しているかをすぐに理解します。Cyber Vision はアプリケーションフローを人間が読み取れるタグに変換するため、プロトコルのエキスパートでなくても現在の状況を把握できます。
脆弱性の検出	生産設備を安全に保ちます。Cyber Vision は、パッチを適用する必要があるハードウェアやソフトウェアの脆弱性を警告します。
リスクスコアリング	差し迫った脅威に焦点を当て、アクションに優先順位を付けて、セキュリティ態勢を迅速に改善します。Cyber Vision は、各デバイス、特定の拠点、回線、またはデータセットのリスクを計算します。また、リスクをプロアクティブに削減するために何ができるかについてのガイダンスも提供します。
マップビュー	制御ネットワークのアクティビティを可視化します。Cyber Vision では設備とその通信を表示するための複数のタイプのマップを提供しています。カラーコーディングにより脅威や異常をすばやく特定できます。
プリセットビュー	事前に設定されたビューとカスタムビューを使用してデータセットを簡単に分析し、重要な情報を強調表示することで、検出戦略に集中し、同僚とターゲット情報を共有できます。
運用状況の把握	ダウンタイムを減らし、ネットワーク効率を向上させます。Cyber Vision は、すべての

機能	利点
	OT イベントを監視して、生産が中断される前にデバイスの問題を特定し、保全チームが問題をより迅速にトラブルシューティングできるようにします。問題のあるネットワークパターンを識別して、IT が構成とネットワーク性能を最適化できるようにします。
セキュリティに関する現状把握	現在のセキュリティステータスをすばやく理解し、異常や脆弱性を特定し、脅威に対応します。Cyber Vision はセキュリティの問題を簡単に特定し、すべての関係者と情報を共有できるように、さまざまなダッシュボード、レポート、イベント履歴を提供します。
セキュリティ態勢レポート	OT 環境に展開された不正なリモート アクセス ゲートウェイを検出するリモートアクセスレポートなど、産業の業務または事業の特定の部分のセキュリティ態勢に関する詳細なレポートにより、OT セキュリティ統治をより適切に推進します。
侵入検知（IDS）	IT ネットワークから発生するサイバーセキュリティの脅威を発見します。Cyber Vision は Talos® サブスクリプションルール（共有オブジェクトルールなど）を活用した Snort IDS エンジンを統合し、マルウェアや悪意のある通信などの既知の脅威や新たな脅威を検出します。
逸脱検知	通常のプロセス動作からの逸脱を検知します。複数のベースラインを簡単に作成して、生産工程をプロファイリングしたり、最も重要なもの（特定の設備や、リモートアクセスなどの特定の動作など）に焦点を当てます。逸脱を検知するとすぐにアラートを発報します。
IT/OT セキュリティイベントの関連付け	セキュリティイベント管理の実践を強化します。Cyber Vision は、Splunk や QRadar などの主要な SIEM および SOAR プラットフォームと事前に統合されており、Syslog を使用して OT イベントとアラートを他のツールに転送できます。警報疲れを回避するため、共有するイベントタイプを選択することもできます。
IT/OT コラボレーション	生産設備とプロセスに関する OT の知識を活用します。Cyber Vision は、IT と OT 間のコラボレーション ワークフローの構築を助長し、生産を効率的に保護します。OT は、追加のコンテキストを提供することでセキュリティイベントを報告できます。IT は OT 設備とグループにカスタムプロパティを追加して、特異性、依存関係、および関係者を文書化できます。
IT セキュリティを OT に拡張	統合された OT/IT SOC を構築します。Cyber Vision はシスコの IT セキュリティ プラットフォームと完全に統合されており、OT 設備とイベントに関する詳細な情報を提供します。既存の IT ツールを使用して OT のセキュリティポリシーを作成し、脅威を修復することがはるかに簡単になりました。
IT との豊かな統合	OT コンテキストを IT ツールと簡単に共有できます。Cyber Vision には、サードパーティソリューション（ServiceNow の OT の管理）が事前に統合されており、カスタム統合を構築するための豊富な REST API が備わっています。API Explorer は、使いやすいユーザーインターフェイスを介して API コールを作成およびテストするのに役立ち、ユーザーが作業を開始するためのコードサンプルが付属しています。
オンプレミスまたはクラウド	希望する場所と方法で導入できます。ハードウェアまたは仮想アプライアンスを使用するオンプレミス、またはクラウド内。Cyber Vision は Amazon Web Services または Microsoft Azure にインストールできます。
情報保証と規則遵守	FIPS 140-2 モードの Cyber Vision を使用して、組織のデータを保護し、情報セキュリティ標準規格に準拠します。

大規模に展開できる OT の可視性

産業用ネットワークに組み込まれたセキュリティ

Cisco Cyber Vision 独自のエッジ コンピューティング アーキテクチャでは、シスコの産業用ネットワーク機器内にセキュリティ監視コンポーネントが組み込まれています。専用のアプライアンスを調達し、それらをどのように取り付けるかを考える必要はありません。また、産業用ネットワークフローを中央のセキュリティ プラットフォームに送信するために別面のネットワークを構築する必要もありません。Cyber Vision は産業用ネットワークが包括的な可視性、分析、脅威の検出を提供するために必要な情報を収集できるようにします。OT セキュリティを大規模に展開する際の Cyber Vision のアーキテクチャの比類のないシンプルさと低コストをネットワークマネージャは実感するはずです。

OT を包括的に可視化できるという点で Cyber Vision が優れている理由の詳細については、ソリューション概要を参照してください。

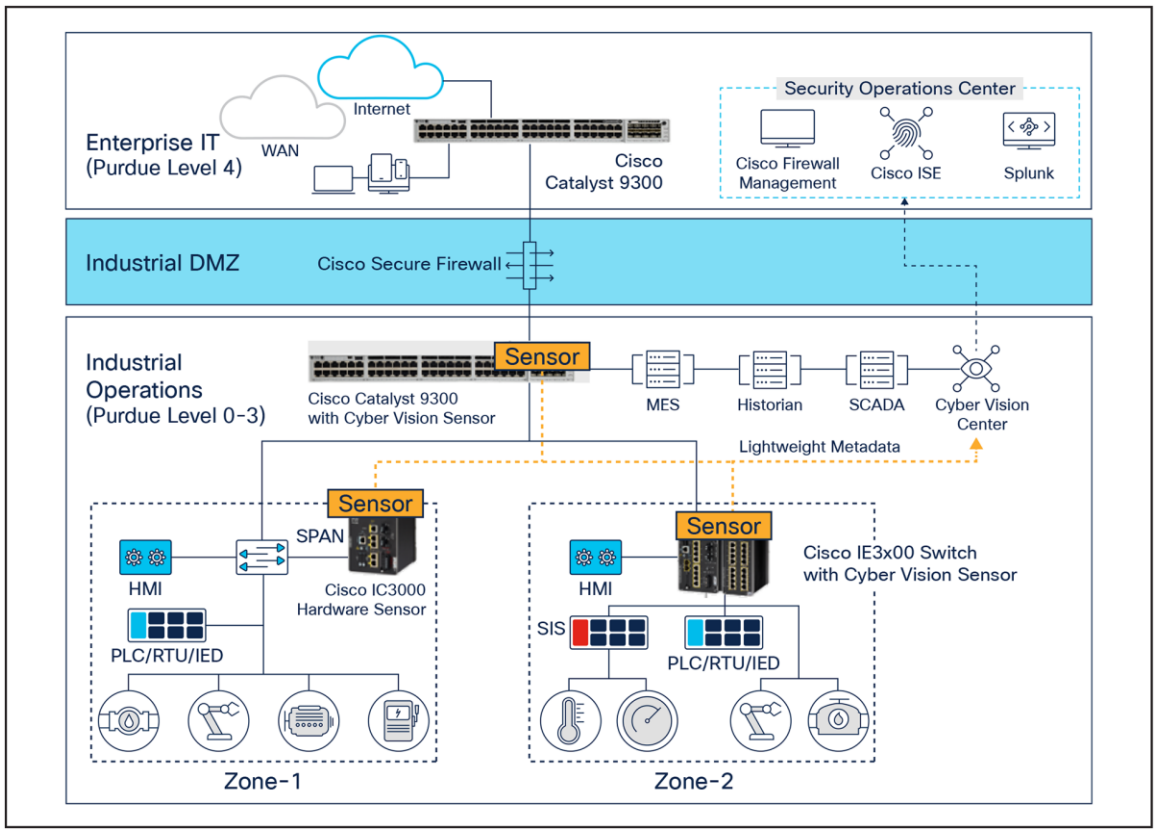

図 1.
Cyber Vision は、ネットワークパフォーマンスに影響を与えることなく大規模に可視性を得るために、非侵入的なエッジアーキテクチャを使用します。

包括的な可視性

Cyber Vision は、パッシブディスカバリとアクティブディスカバリのメカニズムを活用して、すべての設備とその特性および通信を識別します。アクティブ ディスカバリ クエリは極めて正確で非破壊的です。それらは、進行中のプロトコルの意味論を用いて、Windows ベースのシステムを含むすべての生産設備の詳細を収集します。クエリは、産業用ネットワークを形成するシスコネットワーク機器に組み込まれた Cyber Vision センサーから開始されるため、ファイアウォールや NAT 境界によってブロックされることがなく、包括的な可視性が得られます。

設備、通信マップ、運用およびセキュリティイベントに関するこの豊富な情報には、ローカルの OT チームと IT チームのメンバーがアクセスできます。また、Cyber Vision Global Center 内に集約することで、大規模な組織ではすべての拠点にわたる広域的な可視性を得て、統治と規則遵守を推進することもできます。

セキュリティ態勢

Cisco Cyber Vision は、プロトコル分析、侵入検知、脆弱性検知、および動作分析を組み合わせることで、セキュリティ態勢の把握を容易にします。各コンポーネント、デバイス、および生産工程の特定の部分のリスクスコアを自動的に計算して、重要な問題を強調表示するため、修正が必要なものに優先順位を付けることができます。各スコアには、リスクに対処するために能動的に改善プロセスを構築できるように、リスクを軽減する方法に関するガイダンスが付属しています。

Cyber Vision の検出エンジンは、世界有数のサイバーセキュリティ研究チームの 1 つであり、Snort シグネチャファイルの公式開発者である Cisco Talos の脅威インテリジェンスを活用します。Cyber Vision 脅威ナレッジベースは毎週更新され、設備の脆弱性や IDS シグネチャの最新のリストを組み込みます。

運用状況の把握

Cisco Cyber Vision は、ベンダーの詳細、ファームウェアとハードウェアのバージョン、シリアル番号、ラックスロットの設定など、実稼働インフラストラクチャの些細な詳細を自動的に発見し、設備の関係性、通信パターンなどを特定します。情報は、さまざまなタイプのマップ、テーブル、およびレポートに表示されます。

Cisco Cyber Vision は予期しない変数の変更やコントローラの変更などの生産プロセスの実際のステータスに関するリアルタイムの状況を OT エンジニアが把握できるようにします。そのため、製造における問題を迅速にトラブルシュートし、稼働時間を維持することができます。サイバーエキスパートは、容易にこれらすべてのデータを調べて、セキュリティイベントを調査できます。インシデント報告書を作成し、規則遵守を推進するために必要なすべての情報が最高情報セキュリティ責任者に提供されます。

製品はタグを使用して設備の役割と通信コンテキストを強調表示するため、OT や IT のチームメンバーは設備のブランドや参照情報に関係なく、産業インフラストラクチャと運用イベントを容易に理解できます。IT チームは OT スタッフと連携して、脆弱な設備へのパッチ適用、デフォルトパスワードの使用状況の追跡、ネットワーク セグメンテーションの改善などのベストプラクティスを推進できます。

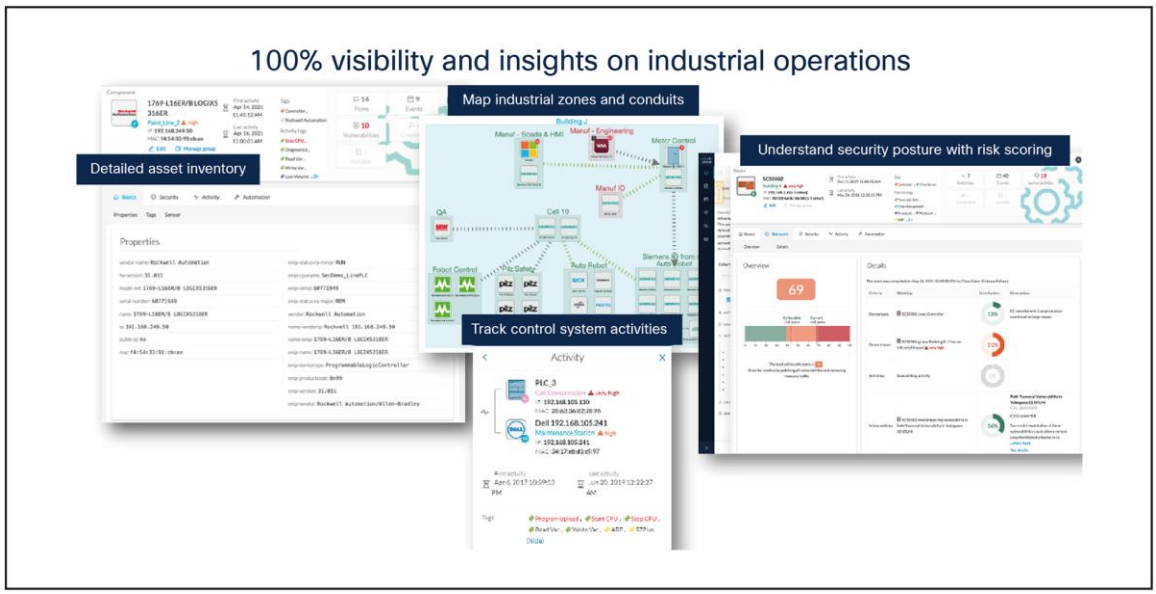

図 2.
設備、生産プロセス、通信フロー、セキュリティ態勢に関する運用状況を把握

適応型ネットワーク セグメンテーションによる業務の保護

ネットワーク セグメンテーションは、産業用ネットワークを保護するための重要な柱です。Cyber Vision はワークフローを合理化するため、セグメンテーションは数年ではなく数週間で実装できます。生産プロセスにおける機能に応じた OT 設備のグループ化、論理ゾーンとコンジットの作成、産業用ネットワークのセグメント化方法の文書化といった、制御エンジニアが行う一連の作業に役立ちます。IT/NetSec チームは、生産を中断しないアクセス制御ポリシーを作成するために必要な情報が得られるようになりました。

Cisco Secure Firewall

制御エンジニアが作成した Cyber Vision 設備グループは Firewall Management Center（FMC）と共有されるため、IT チームは、産業用ネットワーク内の通信を制限するファイアウォールルールを作成できます。OT 設備グループは動的オブジェクトとして Cisco Secure Dynamic Attribute Connector（CSDAC）を介して共有されるため、Cyber Vision で行われた変更は FMC に自動的に反映され、面倒な手動更新やポリシー展開を行うことなくルールを最新の状態に保ちます。

Cyber Vision と Cisco Secure Firewall の連携の詳細については、ソリューションの概要をご覧ください。

Cisco ISE（Identity Services Engine）

アイデンティティベースのマイクロセグメンテーションポリシーを産業用制御ネットワークに適用することにより、ラテラルムーブメントを防止します。Cisco ISE はデフォルトですべての通信を拒否し、Cyber Vision 設備グループを使用して、明示的な許可ポリシーが関連付けられている設備間のアクティビティのみを許可します。設備プロファイルが pxGrid を介して Cisco ISE と共有されるため、Cyber Vision 設備に対する変更は即座に ISE にプッシュされてポリシーが更新され、産業用ネットワークで適応型のマイクロセグメンテーションが有効になります。設備を Cyber Vision の別のグループに移動するだけで、この設備に対応するセキュリティポリシーが ISE に自動的に適用されます。

Cyber Vision と ISE の連携の詳細については、ソリューションの概要をご覧ください。

OT 設備へのセキュアなリモートアクセス

リモートアクセスは、事業部門、保守請負業者、および機械メーカーが、時間とコストのかかる現場への訪問を行わずに OT 設備を管理およびトラブルシューティングするための鍵です。Cyber Vision は、OT ワークフロー専用に設計された包括的なゼロトラスト ネットワーク アクセス（ZTNA）機能を備えています。Cisco Secure Equipment Accessを搭載した Cyber Vision の OT リモートアクセス機能により、MFA または SSO を介した堅牢な認証、タイムスケジュール、使用されているリモートアクセスプロトコル、リモート ユーザー ポスチャ チェックなどのアイデンティティやコンテキストに基づいて、最小権限リモートアクセスポリシーを容易に適用できます。リモートユーザーは IP ネットワーク全体にアクセスすることはできず、アクセス権限が付与されている設備にのみアクセスできます。

OT コンテキストで IT セキュリティツールを強化する

Cyber Vision の詳細な設備一覧と OT イベントの可視性は、業務チームと IT セキュリティチームの両方に価値をもたらします。シスコのセキュリティポートフォリオや広範なサードパーティ ソリューションとの統合がすぐに使用できるため、Cyber Vision が把握した現状がセキュリティ オペレーション センター（SOC）に拡張され、IT および OT ドメインを通過する脅威の検出や、生産工程と IT を保護するための IT セキュリティツールの使用に役立ちます。

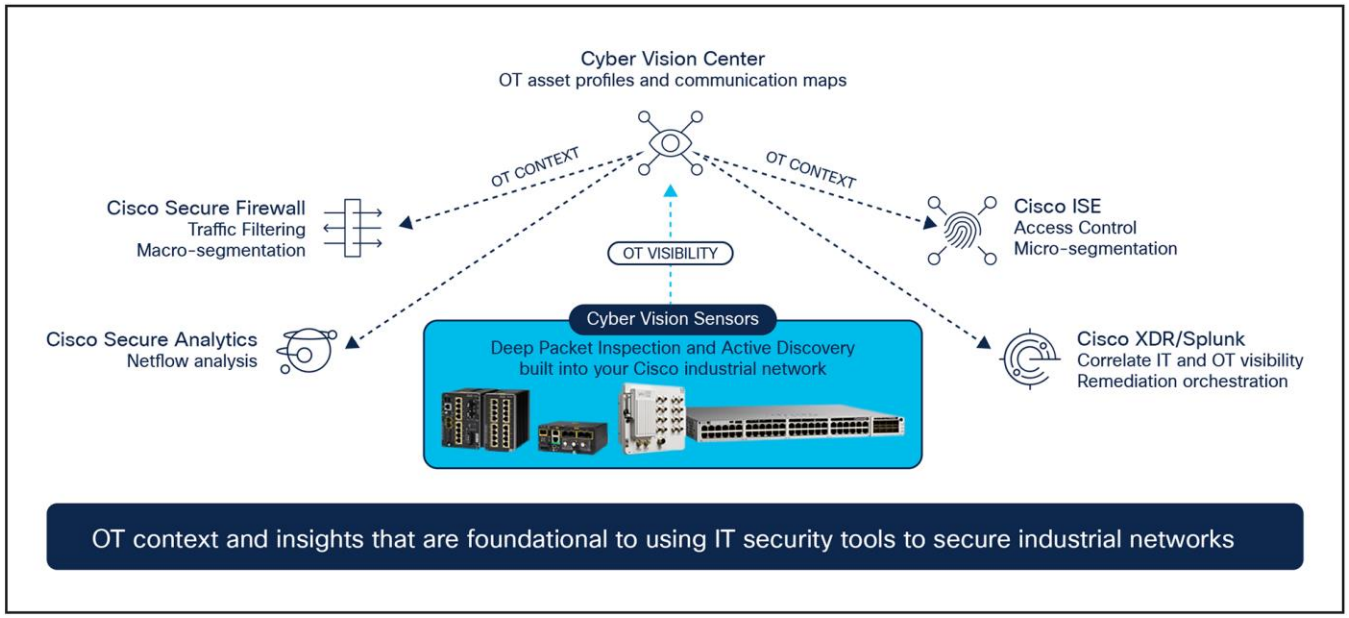

図 3.
Cyber Vision は、既存のツールに生産設備とイベントのコンテキストを提供することで、IT セキュリティ運用を OT に拡張します。

Cisco XDR

Cisco Cyber Vision に異常な振る舞いが見られますか。[Report to XDR] ボタンをクリックするだけで Cisco XDR にケースが作成され、アナリストが特定のプレイブックやカスタムワークフローを使用して調査し、修復を開始できます。Cyber Vision のユーザーインターフェイスで常に使用可能な XDR リボンにより、修復ワークフローをこれまで以上に簡単に開始し、脅威を迅速に封じ込めます。リボンでは、Cyber Vision が検出したすべての観測可能データ（IP/MAC アドレス、ユーザー名、ホスト名、URL など）が強調表示されるため、OT コンテキストを使用して XDR に簡単に視点を移し、詳細な調査を開始できます。Cisco XDR は、Cisco Secure Endpoint、Cisco Secure Network Analytics、Cisco Secure Firewall、Umbrella、Talos インテリジェンスフィード、およびその他の接続テクノロジー（シスコおよびサードパーティ製）のインテリジェンスを活用して、IT および OT ネットワーク全体の脅威とアクティビティを完全に把握します。

Cyber Vision と Cisco XDR の連携の詳細については、ソリューションの概要をご覧ください。

Splunk

多くの OT セキュリティインシデントは IT ドメインから発生しています。産業用ネットワークで発生したインシデントは、企業のネットワークにも伝播する可能性があります。セキュリティアナリストが脅威をより迅速に検出してグローバル企業を保護するためには、IT と OT 全体を一元化して可視化する必要があります。Cyber Vision は OT セキュリティイベントを Splunk に送信し、セキュリティアナリストは IT イベントと OT イベントを関連付けて、脅威をより効果的に検出し、セキュリティスタック全体を使用してセキュリティイベントを修復できます。Cyber Vision は、OT の設備プロファイルを Splunk Asset Risks Intelligence（ARI）と共有し、接続されているすべてのツールからの設備一覧を集約して、グローバルインフラストラクチャに接続されているすべての設備と関連するリスクに関する包括的なビューをセキュリティアナリストに提供します。

Cisco Secure Network Analytics

ネットワーク インフラストラクチャからテレメトリを調べることで、振る舞い分析を拡張します。Cisco Secure Network Analytics は Cyber Vision が把握した現状を利用して監視対象のネットワークフローにコンテキストを追加し、アラームでの ICS 設備を特定することでインシデント対応とフォレンジックを高速化します。

REST API

Cyber Vision は、REST API を介して機能とデータアクセスを公開します。これにより、規則遵守およびリスクレポートの作成、システムおよびイベントの監視とダッシュボードなどのために、サードパーティ製アプリケーションと自社製アプリケーションのカスタム統合が可能になります。API Explorer が組み込まれており、使いやすい Swagger ユーザーインターフェイスで独自の API コールの作成とテスト、およびコード生成を簡単に行うことができます。ServiceNow OT 管理など、すぐに使用できる統合を利用できます。

Common Event Format（CEF）

Cyber Vision の検出およびイベントデータは、SIEM ソリューション、セキュリティ オーケストレーション、自動化、および対応（SOAR）のプラットフォームなどの任意の数のサードパーティ製アプリケーションで使用するために、Common Event Format（CEF）syslog で出力できます。Splunk および QRadar と簡単に統合できる無料のアドオンを利用できます。

プラットフォームのサポート

Cisco Cyber Vision は、独自のエッジアーキテクチャ上に構築されています。このアーキテクチャは、産業用ネットワーク内のディープ パケット インスペクション、プロトコル分析、設備に対する安全なアクティブクエリ、および侵入検知を実行する複数のセンサーデバイスで構成されます。Cyber Vision Center はセンサーからのデータを保存し、ユーザーインターフェイス、分析、振る舞い分析、レポート作成、アラート、API などを提供する集約プラットフォームです。Cyber Vision Center は、ハードウェアアプライアンス上で実行することも、オンプレミスまたはプライベートクラウド、パブリッククラウドで仮想マシンとして実行することもできます。Cyber Vision センサーは次の表に示すプラットフォームでサポートされています。

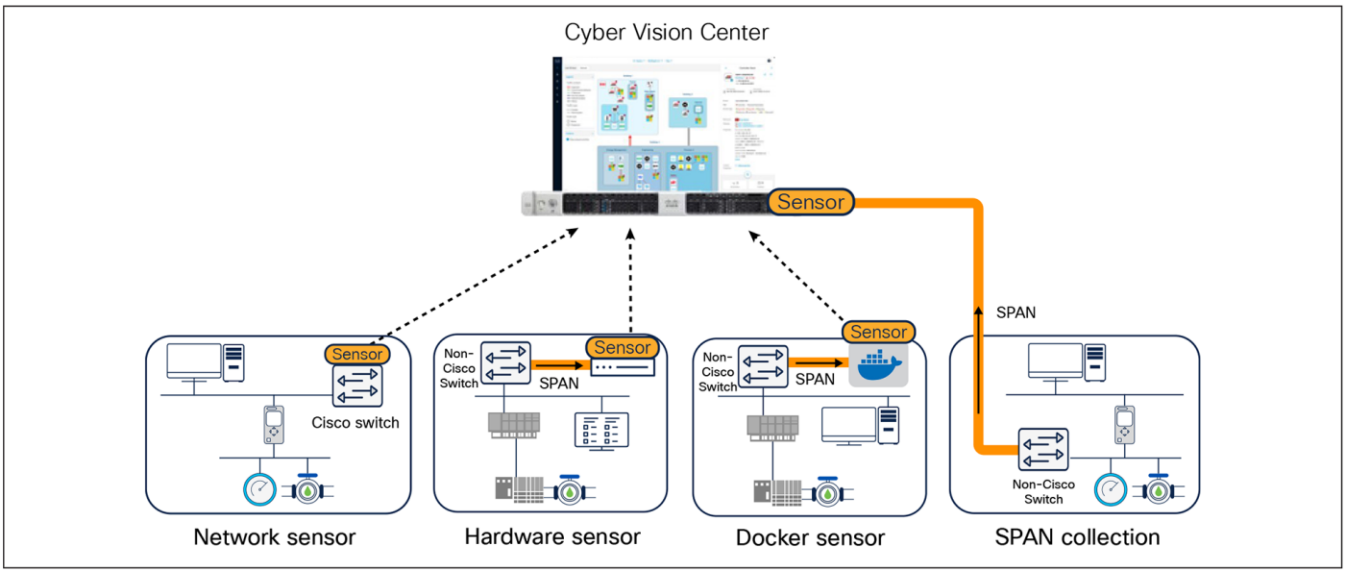

図 4.
Cyber Vision は、シスコのネットワーク機器を使用しない場合を含めて、どのような環境にも簡単に導入できます。

一部のプラットフォームでは、Cyber Vision センサーは ZTNA ゲートウェイエージェントを同時に実行でき、Cyber Vision Advantage ライセンスに含まれる Cisco Secure Equipment Access を使用したゼロ トラスト リモート アクセスを有効にします。リモートアクセスの機能とパフォーマンスの詳細については Cisco Secure Equipment Access データシート を参照してください。

Cyber Vision センサープラットフォーム

表 2. Cyber Vision センサーのプラットフォーム

プラットフォーム	可視性センサーと ZTNA ゲートウェイの組み合わせ	可視性センサーのみ	ZTNA ゲートウェイのみ
産業用イーサネットスイッチ			
Cisco IE3500 高耐久性シリーズ スイッチ	•		
Cisco IE3500 Heavy Duty シリーズ スイッチ	•		
Cisco Catalyst IE3400 高耐久性シリーズ スイッチ	•		
Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチ	•		

プラットフォーム	可視性センサーと ZTNA ゲートウェイの組み合わせ	可視性センサーのみ	ZTNA ゲートウェイのみ
Cisco Catalyst® IE3300 高耐久性シリーズ スイッチ（4 GB RAM 搭載モデルのみ）	•		
Cisco Catalyst IE3100 高耐久性シリーズ スイッチ			•
Cisco Catalyst IE3100H Heavy Duty シリーズ スイッチ			•
Cisco Catalyst IE9300 高耐久性シリーズ スイッチ	•		
Rockwell Stratix 5800 スイッチ		•	
エンタープライズ スイッチ			
Cisco Catalyst 9300 シリーズ スイッチ	•		
Cisco Catalyst 9300X シリーズ スイッチ		•	
Cisco Catalyst 9400 シリーズ スイッチ		•	
産業用ルータ			
Cisco Catalyst IR1100 高耐久性シリーズ ルータ		•	•
Cisco Catalyst IR1800 高耐久シリーズ ルータ		•	•
Cisco Catalyst IR8300 高耐久性シリーズ ルータ		•	
産業用コンピューティング			
Cisco IC3000 産業用コンピューティング ゲートウェイ**[英語]（IC3000-2C2F-K9）**		•	
2 GB 以上の専用 RAM（IDS エンジンを使用している場合は 4 GB）を搭載した、Docker 仮想化エンジン（バージョン 27.0 以上）をサポートする x86 または arm64 コンピューティング ハードウェア。		•	

Cyber Vision Center プラットフォーム

表 3. Cyber Vision Center のプラットフォーム

センタータイプ	サポートされているプラットフォーム
センターのハードウェアアプライアンス	Cisco UCS C225 M6N ラックサーバー [英語]（CV-CNTR-M6N 構成）
センターの仮想アプライアンス	VMware ESXi ソフトウェアアプライアンス Microsoft Hyper-V ソフトウェアアプライアンス Nutanix AHV ソフトウェアアプライアンス
センターのクラウドアプライアンス	Amazon AWS ソフトウェア アプライアンス Microsoft Azure ソフトウェア アプライアンス

表 4. Cyber Vision Center ハードウェアアプライアンスの仕様

項目	CV-CNTR-M6N
フォーム ファクタ	1RU Cisco UCS C225 M6N ラックサーバー
プロセッサ	AMD 2.85 GHz 7443P（24 コア）
メモリ	16GB RDIMM SRx4 3200MHz X 8
RAID	ソフトウェア対応 RAID は、ドライブの数に応じて RAID 1 または RAID 10 を提供します。
内蔵ストレージ	1.6 TB NVMe Extreme Perf. X 2 または X 4 高耐久性ドライブ
組み込みネットワーク インターフェイス カード（NIC）	デュアル 10GBASE-T Intel x710 イーサネットポート
電源装置	ホットプラグ可能、ラックサーバー用 Cisco UCS 1050W AC 冗長電源
管理	Cisco Intersight™ Cisco Integrated Management Controller (IMC) Cisco UCS Manager
ラック オプション	Cisco ボール ベアリング レール キットまたはフリクション レール キット（オプションのリバーシブル ケーブル管理アーム）

その他のハードウェア仕様については、Cisco UCS C225 M6N ラックサーバー のデータシートを参照してください。

Cyber Vision Center ハードウェアアプライアンスの性能

表 5. Cisco Cyber Vision Center （スタンドアロン/ローカル）ハードウェアアプライアンスのスケール

項目	CV-CNTR-M6N
コンポーネントの最大数	50,000
センサーの最大数	300
保存されるフローの最大数	1600 万

表 6. Cisco Cyber Vision Global Center のスケール

項目	CV-CNTR-M6N
同期可能なコンポーネントの最大数	150,000
登録可能なセンターの最大数	20

Cyber Vision Center 仮想アプライアンスの仕様

表 7. Cyber Vision Center 仮想アプライアンスの最小仕様*

特性	プライベートクラウド	パブリッククラウド
CPU	最小 10 コアの x86 サーバー CPU	最小 10 コアの x86 サーバー CPU
メモリ	最小 32 GB	最小 32 GB
ストレージ	最小 1 TB SSD	最小 1 TB SSD
仮想ソフトウェア	• VMware ESXi 6.x 以降 • Windows Server 2016 以降の Microsoft Hyper-V • Nutanix AHV ソフトウェアアプライアンス	• Amazon Web Services • Microsoft Azure

*これらの VM 要件は、最大 10000 の端末の監視をサポートします。

Cisco Cyber Vision Center 仮想アプライアンスは、software.cisco.com から直接ダウンロードできます。

ライセンス

Cisco Cyber Vision は、監視対象の端末の数に基づいた定期的なサブスクリプションモデルを使用してライセンスが供与され、1 年、3 年、5 年、および 7 年の期間で利用できます。ライセンスは、特定の要件を満たすためのさまざまなレベルの機能を提供する 2 つの階層（Essentials と Advantage）で使用できます。製品は、エアギャップネットワーク用の特定のライセンス予約（SLR）ライセンスのオプションとともに Cisco Smart Licensing を使用します。現在のサブスクリプション ライセンスには、Cyber Vision Center とセンサーソフトウェアへのアクセスが含まれます。これらのソフトウェアは、software.cisco.com から直接ダウンロードできます。

Cyber Vision Advantage ライセンスには、エンドポイントと同数の Cisco Secure Equipment Access Advantage ライセンスが含まれています。

Cisco IE3500 および Catalyst IE9300 高耐久性シリーズ Network Advantage ライセンスベーススイッチ SKU（例：IE-3500-8T3S-A、IE-9310-26S2C-A）には、Cyber Vision および Secure Equipment Access の Advantage ライセンスが 3 年間の期間限定で 24 エンドポイント分、追加コストなしで付属しています。追加のエンドポイントのライセンスは別途ご購入いただけます。

表 8. ライセンス階層

ライセンスレベル	
Essentials	**Advantage**
設備一覧 • デバイス一覧 • 通信パターンの特定 • 設備一覧レポートの生成 **脆弱性** • デバイスの脆弱性の特定 • 脆弱性データのエクスポート	Essential 機能の他以下を搭載 **セキュリティ態勢** • デバイスリスクの評価 • セキュリティ態勢レポート • リモートアクセスレポート **侵入検知（IDS）** • サポートされているセンサーの Snort IDS • Talos コミュニティの署名（新しいルールはリリースから 30 日後に追加される可能性

ライセンスレベル	
Essentials	**Advantage**
アクティビティ • 制御システムのイベントの追跡 **RESTful API** • REST API プログラミング インターフェイス	があります） **ふるまい監視** • 設備のふるまいに対するユーザー作成ベースライン • 逸脱に関するアラート **セキュアなリモートアクセス** • Cisco Secure Equipment Access を搭載した、OT ワークフロー専用のゼロトラスト ネットワーク アクセス（ZTNA）。 **高度な統合** • Cisco XDR リボン • Cisco ISE との pxGrid の統合 • SIEM 統合：Splunk、QRadar • ServiceNow OT 管理の統合
	Cyber Vision IDS の Talos サブスクライバ ルール オプション （Cyber Vision Advantage が必要です。IDS センサーごとにライセンスが必要です） • Talos サブスクリプション シグニチャ（特に産業用ネットワーク向けに管理されているもの） • すぐに利用できるルールの可用性 • コミュニティ署名と比較して 15 倍のルール

エンドポイント ライセンス パックは、必要な任意の数のエンドポイントで使用できます。IDS は、Cyber Vision Center、Cisco IC3000 ハードウェアセンサー、Docker センサー、Catalyst IR8300 Rugged ルーター、および Catalyst 9300、9300X または 9400 スイッチで利用できます。

発注情報

Cisco Cyber Vision は現在注文可能です。詳細については、シスコの購入案内のページを参照してください。

表 9. Cyber Vision の製品 ID

製品 ID	製品の説明
CV-LICENSE	Cyber Vision サブスクリプション ライセンス*
CV-CNTR-M6N	Cyber Vision Center ハードウェアアプライアンス（Cisco UCS C225 M6N ラックサーバー）
IC3000-2C2F-K9	Cyber Vision Sensor ハードウェアアプライアンス（Cisco IC3000 産業用コンピューティング ゲートウェイ）
CV-IDS-CNTR	Cyber Vision Center または Docker センサー上で実行される IDS（ハードウェアおよび仮想アプライアンス）の Talos サブスクライバ ルール ライセンス
CV-IDS-IC3000	IC3000-2C2F-K9 センサー上の Cyber Vision IDS 用 Talos サブスクライバ ルール ライセンス
CV-IDS-IR8300	Catalyst IR8300 センサー上の Cyber Vision IDS 用 Talos サブスクライバ ルール ライセンス
CV-IDS-C9000	Catalyst 9300/9300X/9400 センサー上の Cyber Vision IDS 用 Talos サブスクライバ ルール ラ

製品 ID	製品の説明
	イセンス

* Cyber Vision Advantage ライセンスには、エンドポイントと同数の Cisco Secure Equipment Access Advantage ライセンスが含まれます。

保証情報

保証情報については、IC3000 産業用コンピューティング ゲートウェイと Cisco UCS C225 M6N ラックサーバーのそれぞれのデータシートを参照してください。

シスコの環境保全への取り組み

持続可能性に関する情報については、IC3000 産業用コンピューティング ゲートウェイと Cisco UCS C225 M6N ラックサーバーのそれぞれのデータシートを参照してください。

シスコおよびパートナーの提供サービス

計画、展開、およびサポートのためのサービス

シスコとシスコの認定パートナーが提供するサービスは、お客様の Cisco Cyber Vision プロジェクトの評価、設計、展開、運用の各フェーズでご利用いただけます。必要とされているのがエキスパートのアドバイスでもプロジェクト全体のサポートでもその間の何らかのサポートでも、シスコはパートナーとともにお客様の成功を支援するエキスパートと専門知識を提供できます。詳細については、https://www.cisco.com/go/services [英語] を参照してください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital® により、目標を達成するための適切な技術を簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、および他社製製品を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明箇所	日付
Catalyst IE9300 高耐久性スイッチ、**FIPS** 準拠に対するサポートを追加	バージョン 4.1.4	2023 年 1 月
可視性機能とその他の可用性に関する詳細を追加	バージョン 4.2	2023 年 4 月
UCS M6、**Catalyst 9300X** スイッチ、および新機能のサポートを追加	バージョン 4.3	2023 年 11 月
UCS M5 を削除。**Cisco XDR** および **FMC CSDAC** のサポートを追加	バージョン 4.4	2024 年 4 月
Catalyst IR1800 高耐久性ルータおよび **ZTP** のサポートを追加	バージョン 5.0	2024 年 7 月
Docker センサーと新機能を追加	バージョン 5.1	2024 年 12 月
ZTNAリモートアクセス機能、**Nutanix** のサポート、ライセンス関連の更新、および新機能に関する情報の追加	バージョン 5.3	2025 年 8 月

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-743222-09 08/25