産業企業のサステナビリティとデジタルトランスフォーメーションのためのセキュリティプラットフォーム

Kaspersky Industrial CyberSecurity Platform

kaspersky BRING ON THE FUTURE

マルウェアによる攻撃

2022 年の年初以来、マルウェアによる攻撃を受けた ICS 関連のコンピューターは約 30% で、前年よりも約 10% 減少しています。

カスペルスキー ICS-CERT、2022 年 6 月

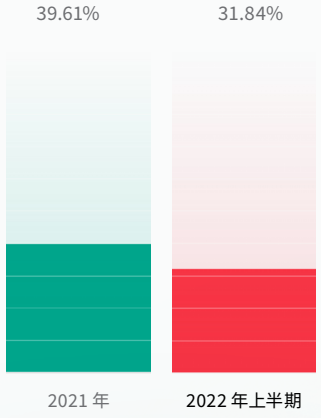
詳しくはこちら

産業企業では、IT と OT（運用技術）インフラストラクチャのサイバーセキュリティに対してさまざまなアプローチをとっています。ほとんどの企業は、既に自社ネットワーク内に成熟した検出および対応の手段を備えていますが、OT に関しては、多くの企業が時代遅れのエアギャップアプローチに依存しています。産業企業はますます「デジタル化」を進めており、スマートテクノロジー、新しい自動化システム、デジタルトランスフォーメーションの採用への投資を増やしています。これにより、IT 環境と OT 環境の間に従来あったギャップ（つまり、サイバー脅威が産業用オートメーションおよび制御システムに到達するのを防ぐために用いられてきたギャップ）が消失しつつあります。

標的にされても、決して被害者にはならない

たとえ標的にされていなくても、偶発的なエアギャップ違反やマルウェア感染の犠牲者になる可能性はあります。たった 1 つのフラッシュドライブ、スマートフォン、フィッシングメール、ランサムウェアが ICS 環境に持ち込まれるだけで、企業のコアビジネスに深刻な影響を与えかねません。同時に、意欲的なハッキンググループが OT ネットワークに侵入して、機器、プロセス、生産、安全性、品質に多大な損害を与えたり、貴重な情報を盗んだりする可能性もあります。

2022 年の年初以来、悪意のあるオブジェクトをブロックしたことがある ICS コンピューターの割合



OT に不可欠なサイバーセキュリティ

エンドポイント保護

（スタンドアロンおよび接続システムを対象とする）テスト済みの安全なソリューションが、セキュリティポリシーの適用、コンプライアンスのサポート、セキュリティ監査の実施、インベントリ管理、パッチ適用タスクの実行、エンドポイントセンサーとしての正確なテレメトリの収集を可能にします。

ネットワーク攻撃からの保護

（通信の可視化、脅威の検出、資産管理を目的とする）ネットワークトラフィック分析と侵入検知システムが、ファイアウォール設定の有効性、ネットワークセグメンテーション、ネットワークの使用に関するコンプライアンスをコントロールし、安全な応答を手動で提供するのに役立ちます。

トレーニングプログラム

従業員の事故を減らし、人的要因（ヒューマンエラー）を最小限に抑えます。

エキスパートサービス

インフラストラクチャの調査、専門的な分析の実施、インシデントの影響軽減に役立ちます。

世界的な認知度

Frost and Sullivan は、全世界での産業用 (OT/ICS) サイバーセキュリティ市場の分析に基づいて、2020 年度の Global Company of the Year Award の受賞者としてカスペルスキーを選びました。

VDC の年次グローバル調査において、カスペルスキーは産業用オートメーションコミュニティの 250 人を超える有資格専門家による総合的な評価に基づいて、産業用サイバーセキュリティ分野のトップベンダーに選ばれました。

カスペルスキーが提供する価値

ネイティブに統合されたテクノロジーである Kaspersky Industrial CyberSecurity (KICS) プラットフォームを、カスペルスキーが提供する専門的なトレーニングとサービスのポートフォリオと組み合わせることで、産業企業および重要インフラストラクチャのオペレーターのあらゆるサイバーセキュリティニーズに対応できます。

このプラットフォームは、産業企業向けの独自のエコシステムを構成する重要な要素であり、次のものが含まれます：

- カスペルスキーの最高クラスの企業向けソリューションは、IT と OT を真の意味で融合し、単一ベンダーアプローチによりさまざまな利点を提供します。
- サイバーフィジカルセキュリティ、産業用 IOT セキュリティ、機械学習、セキュアなリモートワークスペースをはじめ、さまざまな専門ソリューションが、制約のない俊敏なスケーラビリティをもたらします。

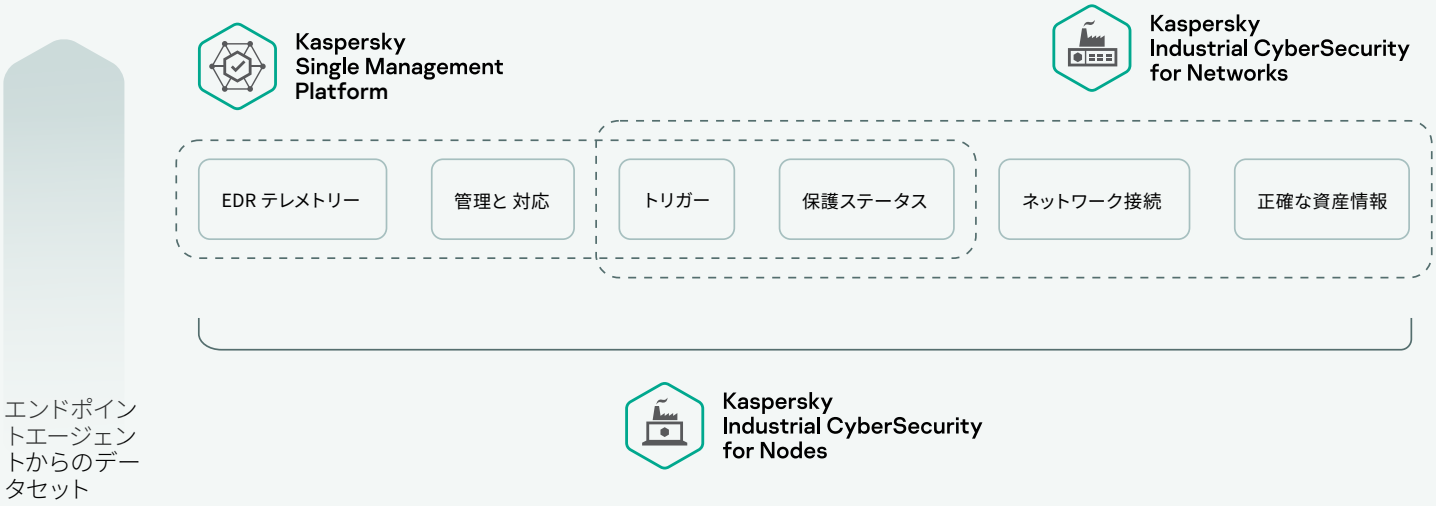
Kaspersky Industrial CyberSecurity Platform は、次の分野のリーダーです：

- OT エンドポイントセキュリティ
- OT ネットワークの監視および可視性
- 異常検出、インシデント対応、および報告
- OT サイバーセキュリティサービス

併用することで、ネットワークやエンドポイントのレベルでの一連のインシデント、正確なアセットパラメーター、トラフィックミラーリングがまだ利用できないセグメントからのネットワーク通信およびトポロジマップなど、全体像とより広いコンテキストを確認できます。

製品

KICS は、産業用オートメーションおよび制御システムのコアコンポーネントをあらゆるレベルで包括的に保護するために設計された OT サイバーセキュリティプラットフォームです。プラットフォームコンポーネント間のシームレスな統合により、地理的に分散した複数の OT ネットワークと自動化システムを完全に可視化して、カスタマーエクスペリエンス、状況認識、展開の柔軟性を向上させます。



KICS for Nodes は、コンプライアンス監査とエンドポイントセンサー機能を備えたエンドポイント保護、検出、応答ソフトウェアです。

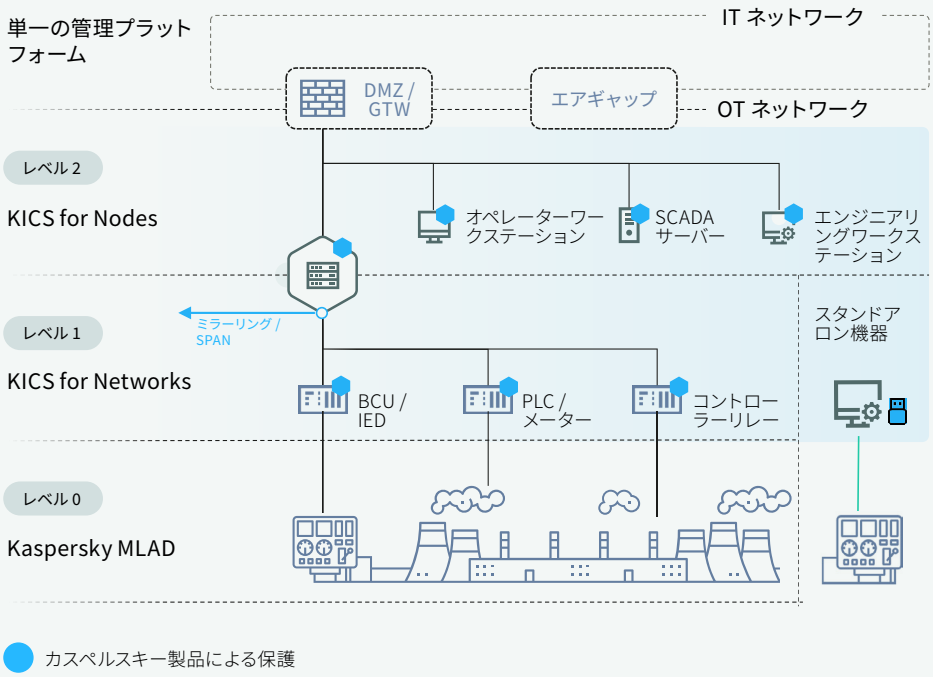
KICS for Networks は、OT ネットワークトラフィックの分析、検出、応答用に設計されています。

単一の管理プラットフォームが、高度な EDR インターフェイスと迅速なスケーラビリティをさまざまな場所に提供します。

追加機能

このソリューションは、その他にも多数の機能を提供します。Network **Active Polling** テクノロジーにより、ネットワークトポロジとアセット設定を迅速かつ正確に収集できます。 **Endpoint Audit** 機能により、現在の設定の安全性を含むセキュリティポリシーのコンプライアンスを確保し、脆弱性を制御できます。KICS for Nodes の **Portable Scanner** 配信方法により、スタンドアロンのエアギャップ機器セキュリティ監査のベストプラクティスを確立できます。**異常検出のための機械学習**は、技術プロセスの奥深くで機能する早期の異常検出システムです。

ソリューションアーキテクチャ



主な機能

資産ディスカバリ
パッシブ OT 資産識別とインベントリ

ディープパケットインスペクション
テクニカルプロセステレメトリをほぼリアルタイムで分析

ネットワークインテグリティの制御
無許可のネットワークホストとフローを検出

侵入検知システム
悪意のあるネットワークアクティビティに関する警告を送信

コマンド制御
産業用プロトコルでコマンドを検出

外部統合
柔軟な API 統合により、検出機能と防止機能を追加

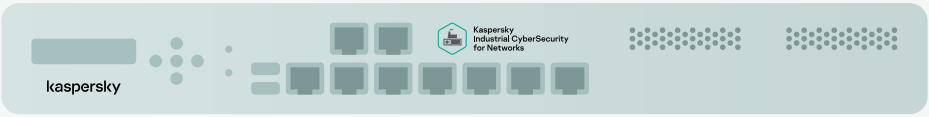
異常検出のための機械学習（MLAD）
リアルタイムのテレメトリと履歴データのマイニング（リカレントニューラルネットワーク）を通じて、サイバーまたは物理的な異常を検出

脆弱性管理
Kaspersky ICS CERT を利用した、産業機器の脆弱性に関する更新可能なデータベース

Kaspersky Industrial CyberSecurity for Networks

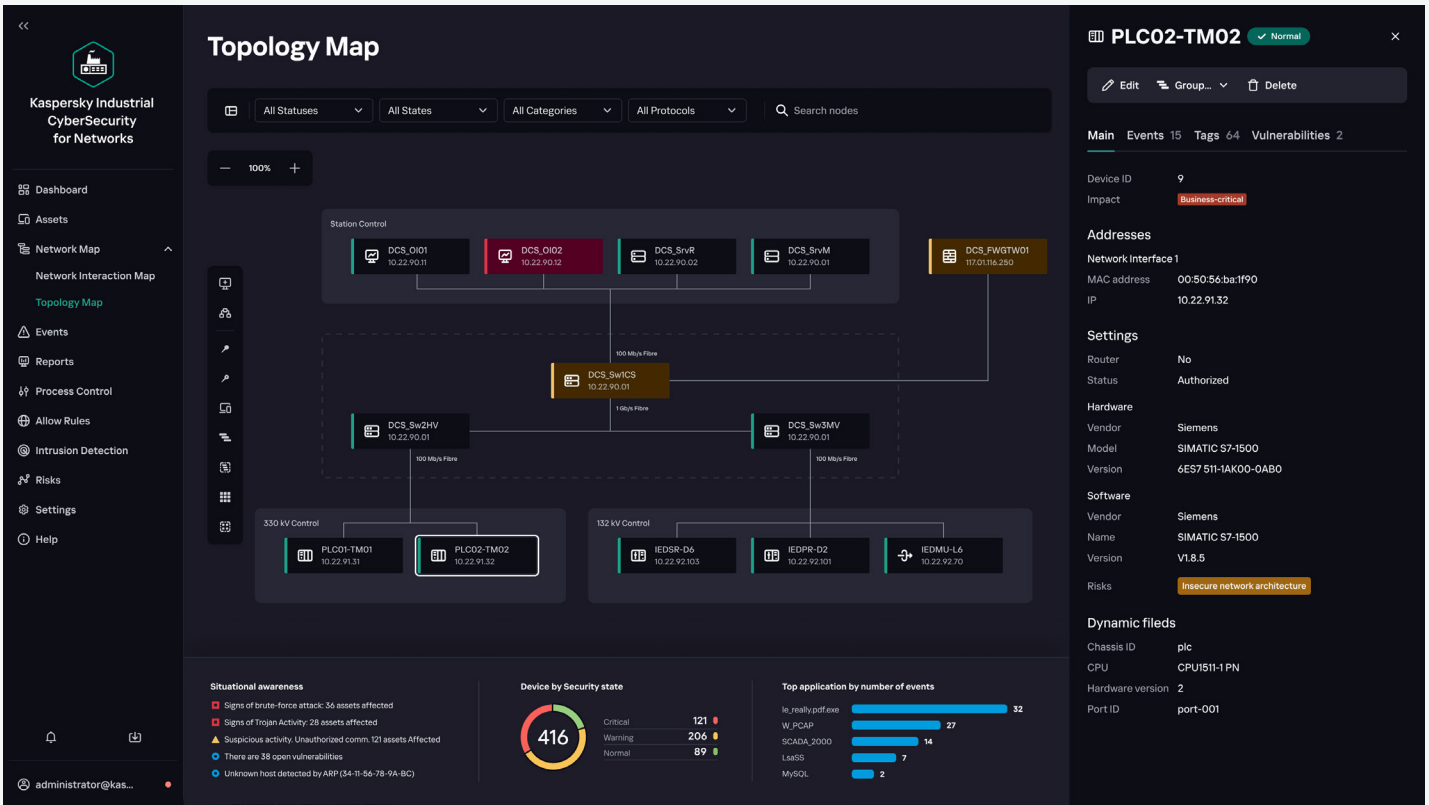
OT ネットワークトラフィックの分析、検出、対応。パッシブトラフィックモニタリング、アクティブポーリング、およびエンドポイントセンサーにより、リスクを明確に可視化します。

ICS ネットワーク内の異常や侵入を初期段階で検出し、産業プロセスへの悪影響を防ぐために必要な措置を確実に講じます。



お客様の確立された調達、統合、保証慣行に迅速かつ最適に統合できる、アプライアンスに依存しないソリューション。

インターフェイス



KICS for Nodes は分散型自動化システムの厳しい要件に適合するよう特別に設計されています。混在環境や複雑な環境、運用時間の延長、スタンドアロンのユースケースおよび接続されたユースケース、有人およびメンテナンスフリーのインスタンス、そして制御可用性の優先順位にすべて対応します。

Kaspersky Industrial CyberSecurity for Nodes

産業グレードの、テスト済みで認定を受けたエンドポイント保護、検出、対応。Linux、Windows、スタンドアロンシステム向けの、低インパクトで互換性があり安定したソリューションです。

産業エンドポイントの保護、検知、対応

最新のデジタル管理および分散型自動化システムのあらゆるエンドポイントを保護します。それにより、根本原因分析プロセスにおいてインシデントを新たなレベルで可視化します。エージェントがエンドポイントテレメトリを収集し、ワークステーション、サーバー、ゲートウェイ、その他のエンドポイントでのインシデントの進行状況を明確かつ詳細に視覚表現するため、自動化システムの管理者はインシデントが完全に処理され、二度と発生しないことを確信できます。

メリット

低インパクト
保護対象デバイスへの影響を抑え、最高のシステムパフォーマンスを実現

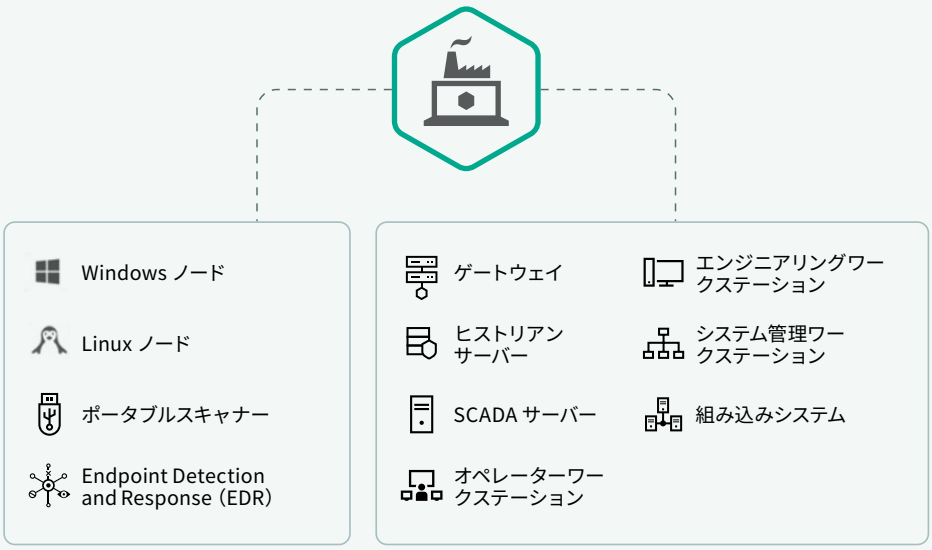
互換性
旧世代の低パフォーマンスコンピューター、Windows XP SP2 および Windows Server 2003 SP1 以降のシステムなどとの互換性

延長ライフサイクル
最長 5 年間のライセンスと延長サポート

機能をフル装備
あらゆる MS デスクトップ、サーバー、組み込み Windows OS に対応

モジュール型の展開
柔軟なオプションと安全な非侵入型の設定

混合インフラストラクチャをカバー
Windows、Linux、およびポータブル



KICS for Nodes ポータブルスキャナー
セキュリティソフトウェアをインストールできないスタンドアロンの機械、自動化システム、または機器にサイバーセキュリティポリシーを適用します。スタンドアロンインフラストラクチャからでも、究極の状況認識と OT 可視性が実現します。

インストール不要のソリューション
KICS for Nodes は、多数のポータブルスキャナーフラッシュドライブで追加で有効化できます。これにより、メンテナンス期間中に複数のマシンで同時にオンデマンドスキャンを実行し、エンドポイントデータを収集して、便利な概要レポートにまとめることができます。

規制および社内ポリシーの遵守
KICS for Nodes ポータブルスキャナーは、OT サイトにアクセスする機器（サードパーティの請負業者のコンピューターを含む）のアンチマルウェアコンプライアンスチェックを実行します。運用フットプリントが非常に小さいため、既存のセキュリティソリューションに干渉しません。

メリット

状況認識

システム / ポリシー管理

キルチェーンと応答

レポートと通知

SIEM との連携

HMI / MES 統合

Kaspersky
Single Management
Platform

単一管理プラットフォームが、OT インフラストラクチャ全体のセキュリティオーケストレーションのための集中セキュリティ管理ソリューションとなります。イベントやインシデント分析などによって強化された、地理的に分散するすべての資産のマップを備えています。OT と IT が混在するセキュリティチームの効率を高めます。すべてのセキュリティ制御が調和して機能することで、迅速かつ正確な対応を可能にします。

エキスパートサービス

カスペルスキーのサービス群は、KICS ポートフォリオの重要な一部となります。カスペルスキーは、産業用サイバーセキュリティ評価からインシデント対応まで、セキュリティサービスの全サイクルを提供しています。

“ ICS サイバーセキュリティ分野におけるカスペルスキーの経験、専門性、およびソリューションの複雑さは、他のサプライヤーと比較して、当社に大きな価値をもたらし、当社のセキュリティ戦略の明るい未来を保証してくれました。

Plzeňský Prazdroj、
C&A マネージャー、
Ondřej Sýkora 氏

産業用サイバーセキュリティ評価

産業用サイバーセキュリティ評価：カスペルスキーは外部および内部の侵入テスト、OT セキュリティ評価、自動化ソリューションのセキュリティ評価など、侵襲性を最小限に抑えた産業用サイバーセキュリティ評価を提供します。カスペルスキーの専門家が、企業のインフラストラクチャに関する重要な洞察と、ICS のサイバーセキュリティ体制を強化する方法に関する推奨事項を提供します。

“ 演習を行い、カスペルスキーチームの知識から学ぶことで、サイバーセキュリティの脅威に対して保護を強化することができました。

PacificLight、
最高経営責任者（CEO）、
Yu Tat Ming 氏

脅威インテリジェンス

カスペルスキーの専門家が収集した最新の分析が、標的型産業サイバー攻撃からお客様を保護します。これらのインテリジェンスは、TI フィードまたはカスタマイズされたレポートとして配信され、地域や業界、および ICS ソフトウェアのパラメータに従って、個別の顧客ニーズを満たします。

インシデント対応

インシデントが発生した場合、カスペルスキーの専門家がデータとマルウェアを収集して分析し、インシデントのタイムラインを再構築し、考えられる原因と動機を特定して、詳細な修復計画を策定します。この計画には、顧客のシステムからマルウェアを削除し、悪意のあるアクションをロールバックするための推奨事項が含まれます。

トレーニングと意識向上

> 当社の ICS グループに専門的な産業用サイバーセキュリティスキルトレーニングを提供する企業として、カスペルスキーは最適でした。
>
> 最高技術責任者、
> Søren Egede Knudsen 氏

産業用サイバーセキュリティ意識向上トレーニング

コンピューター化された産業用システムを使用する従業員とその管理者を対象とする、オンサイトおよびオンラインでのインタラクティブなトレーニングとサイバーセーフティゲーム。参加者は、現在の脅威の状況と、特に産業環境を標的とする攻撃のベクトルについて新たな洞察を得て、実際のシナリオを探り、サイバーセーフスキルを習得します。

エキスパートトレーニングプログラム

ICS Penetration Testing および ICS Digital Forensics トレーニングコースは、サイバーセキュリティの専門家を対象としています。参加者は、産業環境で包括的な侵入テストやデジタルフォレンジックを実施するために必要となる高度なスキルをすべて習得できます。

特化したソリューションエコシステム

Kaspersky IoT Infrastructure Security

カスペルスキーのサイバーイミュニティアプローチに基づいて、IoT をゲートウェイレベルで保護

詳しくはこちら

Kaspersky Antidrone

あらゆる規模の施設でドローンから空域を保護

詳しくはこちら

Kaspersky Secure Remote Workspace

サイバーイミュニティを備えた機能的なシンクライアントインフラストラクチャ

詳しくはこちら

Kaspersky Security CAD

設計および運用段階の情報セキュリティシステムのデジタルモデリング

詳しくはこちら

Kaspersky Machine Learning for Anomaly Detection

産業技術プロセスにおける早期異常検知システム

詳しくはこちら

Kaspersky Industrial CyberSecurity

詳しくはこちら

www.kaspersky.co.jp