KASPERSKY lab

Kaspersky Industrial CyberSecurity：2018年ソリューション概要

www.kaspersky.com/ics
#truecybersecurity

Kaspersky Industrial CyberSecurity：2018年ソリューション概要

増え続ける産業用システムへの攻撃

産業用制御システムへのサイバー攻撃は、単にその数を増やしているばかりか、投機的なものから手堅いものへと変化しています[1]。今後、ICSサイバー攻撃を経験するだろうと考える産業メーカーは、4社のうち3社にのぼります[2]。ビジネスやサプライチェーンの中断は、過去6年間にわたって世界的に懸念されるリスクのトップに位置付けられてきました。2018年には、サイバーインシデントがそれに続いています[3]。産業用または基幹インフラストラクチャシステムを運用している企業にとって、これらのリスクはかつてないほど大きなものとなっています。産業向けセキュリティにより、事業や評判の保護をはるかに上回る範囲の保護を実現することができます。サイバー脅威からの産業用システムの保護においては、この分野特有の環境的、社会的、マクロ経済的な視点で捉えることが重要です。

[1] PwC：「グローバル情報セキュリティ調査2015」

[2] 「The state of industrial cybersecurity 2017」、Kaspersky Lab

[3] 「Allianz Risk Barometer 2018」

運用テクノロジーと情報テクノロジー

オートメーション規格IEC 62443で定義されているように、産業用制御システム（ICS）は、産業（技術）プロセスの安全で信頼性の高い運用に影響を与える可能性のある個人、ハードウェア、ソフトウェアの集合です。

産業用制御システムは、たとえば次の要素で構成されます（がこれに限定されるものではありません）：

- 分散型制御システム（DCS）、プログラマブル論理制御装置（PLC）、遠隔端末装置（RTU）、インテリジェント電子装置（IED）、監視制御およびデータ収集システム（SCADA）、および診断システム。
- 連続、バッチ、離散、およびその他プロセスに制御、安全性、および生産業務機能を提供するために使用される、関連する内部、ヒューマン、ネットワーク、またはマシンインターフェイス。

さらに大局的な見方をすれば、どの産業用システムインフラストラクチャも以下の2つの領域に分けることができます：

- 情報テクノロジー（IT）：事業目標の観点からデータを管理するために必要で、OTと対になるシステム
- 運用テクノロジー（OT）：産業オートメーションの物理的な産業プロセスを管理するために必要なシステム

ITセキュリティ戦略は、データの保護に重点を置き、「C-I-A」モデル（データの機密性、整合性、および可用性）の目標に沿う傾向にあります。一方、多くのOTシステムにとっては、サイバーセキュリティは「データ」だけでなく、産業プロセスの継続性の問題でもあります。そのため、C-I-Aモデルで言うところの「可用性」が、OTに適用されるセキュリティ戦略の中心となります。ここに、産業向けサイバーセキュリティのニーズと他のシステムのニーズの違いがあります。つまり、従来のIT向けサイバーセキュリティソリューションがどんなに効果的でも、OTシステムにはそぐわず、プロセスの可用性を（場合によっては整合性も）危険にさらしかねません。

リスクと脅威

産業用制御システム（ICS）を標的としたサイバー攻撃の広がりが認知されつつあるとは言え、多くのITセキュリティモデルは依然として、（「空間的な隔たり（エアギャップ）」によって）物理的に隔離されたシステムと「分かりにくさによるセキュリティ」で十分だという時代遅れの思想に固執しています。ただし、Industry 4.0の時代にこのアプローチは通用しません。今では、Industry 4.0に適合する産業用制御システムネットワークは、好むと好まざるとにかかわらずインターネットからアクセスできる状態にあります[4]。また、Kaspersky LabのICS CERTがKaspersky Security Networkのデータをもとに実施した大規模な調査から、トロイの木馬、ウイルス、ワームなどのよく知られたウイルスを含む、業務システム（IT）を悩ましているものと同じ一般的なマルウェアの攻撃が、産業用PCを繰り返し襲っていることが判明しています。2017年の後半には、カスペルスキー製品で保護された産業用コンピューターの37.8%にマルウェア攻撃が仕掛けられ、カスペルスキー製品によって阻止されました[5]。

ランサムウェアもまた、ICSにとって大きな脅威になりつつあります。ランサムウェアの攻撃範囲と多様性は2015年から2017年の間で飛躍的に増大しました。ランサムウェアの出現は、産業セクターにとってきわめて大きな問題です。その感染が基幹システムに打撃、範囲ともに大きな損害を引き起こすことから、ICSは攻撃者にとって特に魅力のある標的候補となっています。このことは、2017年中にICS/SCADAシステムに向けられたランサムウェア攻撃（特にWannaCryおよびexPetrの感染）のインシデント件数が膨大な数にのぼることからも明らかです。近い将来ICSを攻撃するために、データの暗号化に代わる特定の意図を独自に持つランサムウェアが設計され、運用の中断や重要な資産へのアクセスのブロックに着手する可能性もあります。

産業向けセキュリティでは、一般的な脅威に加えて、ICS特有のマルウェアや標的型攻撃にも対処する必要があります。こういった攻撃にはStuxnet、Havex、BlackEnergy、Industroyerや、安全計装システムを標的としたTritonなど新たなマルウェアがあり、その数は急速に増えつつあります。StuxnetおよびBlackEnergyによる攻撃からわかるように、1つの感染したUSBドライブまたは1通のスピアフィッシングメールさえあれば、用意周到な攻撃者は空間的な隔たり（エアギャップ）を乗り越え、隔離されたネットワークに侵入することができます。

産業界は、マルウェアや標的型攻撃の他にも、人、プロセス、テクノロジーを標的とするその他の脅威とリスクにも直面しており、これらのリスクを過小評価すれば、深刻な結果につながる可能性があります。Kaspersky Labは、お客様がマルウェアや標的型攻撃だけでなく、以下のような多くのサイバーインシデントおよびリスク要因に取り組み、対処するうえで役立つソリューションとサービスを開発しています：

- SCADAシステムのオペレータや請負業者（サービスプロバイダ）のミス
- 不正操作
- サイバー妨害工作
- コンプライアンス問題
- フォレンジック調査の認識およびハードデータの欠如

[4] 「ICS and their online availability 2016」、Kaspersky Lab

[5] 「Threat Landscape for Industrial Automation Systems for H2 2017」、Kaspersky Lab ICS CERT

専用の産業向けサイバーセキュリティの必要性

ITシステムとOTシステムの違いを理解しているサイバーセキュリティベンダーでなければ、産業用の制御システムとインフラストラクチャに特有のセキュリティ要件を満たすソリューションは提供できません。Forrester Researchは産業組織に対し、セキュリティベンダーを選ぶときには「産業に特化した専門知識を探す」ようにアドバイスしており、このセクターのスペシャリストとして本物の専門知識を持つ数少ないベンダーの1社としてKaspersky Labの名前をあげています。

Kaspersky Lab：信頼できる産業向けサイバーセキュリティプロバイダ

産業用インフラストラクチャと基幹インフラストラクチャに対する脅威は、とどまることなく進化しています。サイバーセキュリティおよび産業保護におけるリーダーとして認められている[6]Kaspersky Labは、これらの脅威に対処するため、さらに高度な機能を備えたソリューションの研究と開発に継続的に取り組んでいます。運用の管理からICSレベル、さらにその先まで、Kaspersky Labは、世界中の産業、規制当局、政府機関による脅威の変化の予測と攻撃からの防御の支援において主導的な役割を果たしています。

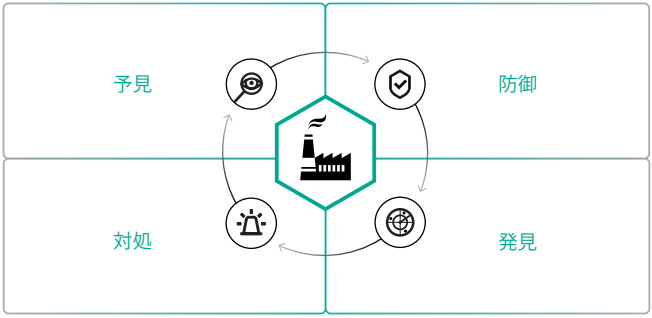
Kaspersky Labは、長年にわたって当社のアンチマルウェアによる保護を利用してきた主要な産業界の信頼されるセキュリティプロバイダでありパートナーであり続けるために、Emerson、SAP、Siemens、Schneider Electric、Industrial Internet Consortiumをはじめとする著名な産業オートメーションベンダーおよび組織との協力体制を築き、既存の脅威だけでなく、高度な標的型攻撃など新たな攻撃からも産業環境を保護する互換性、専用の手順、および連携フレームワークの確立を目指しています。

Kaspersky Labは、産業向けサイバーセキュリティ市場特有のニーズを解決することに特化したソリューションのポートフォリオを開発しました。それが、Kaspersky Industrial CyberSecurity（KICS）です。これらのソリューションは、事業継続性や産業プロセスの一貫性に影響を与えることなく、SCADAサーバー、HMI、エンジニアリング用ワークステーション、PLC、産業用ネットワーク接続を含むあらゆるICS層において、サイバー脅威に対する効果的なセキュリティを提供します。

Kaspersky Industrial CyberSecurityには、Kaspersky Labの総合的な多層型セキュリティ戦略に則って複数の保護手法が組み合わされています。潜在的な攻撃経路の予測から、産業に特化された防止および検知テクノロジー、サイバーインシデントに対する先を見越した対応まで、すべてをカバーする総合的なアプローチを採用した産業向けサイバーセキュリティは、中断のない安全な運用のための究極の後ろ盾となります。

[6] Gartnerの「Market Guide for Operational Technology Security」、2017年

適応型セキュリティアーキテクチャ



Kaspersky Industrial CyberSecurity：サービス

産業向けサイバーセキュリティアセスメントからインシデントへの対応まで、Kaspersky Labの一連のサービスは、KICSポートフォリオの重要な役割を担っています。

知識（教育とインテリジェンス）

- **トレーニング：**Kaspersky Labには、サイバーセキュリティのエキスパート、OT管理者やICSオペレータのために設計されたトレーニングコースが用意されています。たとえば、「Advanced Industrial Cybersecurity in Practice（高度な産業向けサイバーセキュリティの実践）」コースでは、関連するサイバー脅威とその進化の動向、これらの脅威から保護する最も効果的な方法を学びます。また、スキル開発コースでは、セキュリティ担当者がICSペネトレーションテストやデジタルフォレンジックなど特定分野のスキルに磨きをかけることができます。

- **意識向上プログラム：**関連する産業向けサイバーセキュリティ問題への意識を高めるため、またこれらの問題の対処と解決に必要なスキルを育成するために、Kaspersky Labは、セキュリティ管理者およびエンジニアを対象とした「ゲーム形式」のトレーニングを提供しています。このKaspersky Industrial Protection Simulation（KIPS）では、産業オートメーションシステムに対する実世界のサイバー攻撃をシミュレートし、産業向けサイバーセキュリティの備えに関連する主な問題を明らかにしていきます。

- **インテリジェンスレポート：**Kaspersky Labの専任のICSサイバー緊急対応チームにより、お客様の業種に適した最新の脅威インテリジェンスレポートが作成されています。

エキスパートサービス

- **サイバーセキュリティ評価：**ITおよびOTのセキュリティが運用におよぼし得る潜在的影響を懸念する組織のために、Kaspersky Labは、システムへの影響を最小限に抑えた産業向けサイバーセキュリティ評価を実施しています。これは、セキュリティ要件を運用上のニーズと関連させながら確立するうえできわめて重要となる最初のステップです。また、保護テクノロジーをさらに配置しなくても、サイバーセキュリティレベルについて意味のある知見が得られます。

- **ソリューションの統合：**産業用制御システムのアーキテクチャが独自のものであるか、または産業では一般的でないカスタムハードウェアおよびソフトウェアコンポーネントが使用されている場合でも、推奨サイバーセキュリティツールを適応させ、お客様のシステムと連携させることができます。このサービスには、SCADA、PLC、産業用通信プロトコルなど、独自のソフトウェアおよびハードウェアシステムのサポートも含まれています。

- **インシデントへの対応：**サイバーセキュリティインシデントの発生時には、Kaspersky Labのエキスパートがデータを収集して分析し、インシデントタイムラインを再現します。また、考えられる原因と動機を突き止め、修復計画を立てます。この他、マルウェア分析サービスも提供しています。このサービスでは、お客様から提供されたマルウェアサンプルをKaspersky Labのエキスパートが分類してその機能とふるまいを分析し、システムから取り除くため、また悪意のある操作をロールバックするための推奨事項と計画を作成します。

Kaspersky Industrial CyberSecurity：セキュリティの一元管理

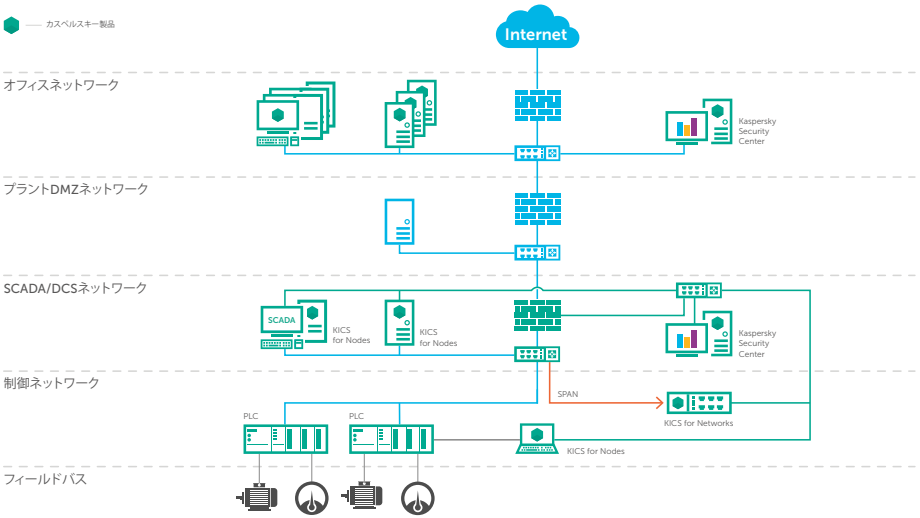
Kaspersky Security Center

あらゆる攻撃経路で最高レベルの保護を実現するためには、生産現場のセキュリティをノードレベルとネットワークレベルの両方で機能させる必要があります。Kaspersky Labのその他すべての保護テクノロジーと同様に、1つの管理コンソール、すなわちKaspersky Security CenterからKICSを管理することで、最適な制御、管理しやすさ、そして可視性を確保できます。具体的には、以下の利点が得られます：

- セキュリティポリシーの一元管理 - ノードごと、グループごとに異なる保護設定を設定可能。
- ネットワークへの展開前のアップデートのテストが容易になり、プロセスの完全な整合性を確保。
- セキュリティポリシーに則したロールベースのアクセスおよび緊急時のアクション。

Kaspersky Security Centerを使用すれば、下図に示すように、生産に直接かかわる複数拠点の層だけでなく、それを取り巻くオフィスの管理も容易になり、可視性が得られます。

Kaspersky Industrial CyberSecurityの展開例



Kaspersky Security Gateway

KICSでは、イベントに関連するデータをSIEM、MES、ビジネスインテリジェンスソリューションなど、他のシステムに送信することもできます。検知されたすべてのイベントと異常は、CEF 2.0、LEEF、およびSyslogプロトコルによってSIEM、メール、syslogサーバー、ネットワーク管理システムなどのサードパーティシステムにレポートされます。また、サイバー攻撃の検知、対処、調査に役立つだけでなく、予測的メンテナンスを支援する詳細な産業向けネットワークの監視も利用できます。

ヒューマンマシンインターフェイス（HMI）との統合

このソリューションでは、セキュリティ通知をHMIに直接送信できます。これにより、生産現場の作業員は、サイバーインシデントに対する即時対応およびそのエスカレーションに関する具体的な情報を受け取ることができます。

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodesは、ICS環境のオペレータレベルで脅威に対処するために特に設計されました。人的要因、一般的なマルウェア、標的型攻撃、または妨害行為に起因する様々なタイプのサイバー脅威からICS/SCADAサーバー、HMI、エンジニアリング用ワークステーションを守ります。KICS for Nodesは、SCADA、PLC、DCSなどの産業オートメーションシステムのソフトウェアおよびハードウェアコンポーネントと互換性があります。

脅威とリスクの要因	Kaspersky Labのテクノロジー
不正なソフトウェアの実行	ホワイトリスト、ブロックモードまたは検知のみ（ブロックせずに登録）モード
マルウェア	高度なアンチマルウェアのシグネチャベース検知エンジン、Kaspersky Labのパブリッククラウド（KSN）またはプライベートクラウド（KPSN）を使用したクラウドベースの検知エンジン
ランサムウェアを含むクリプター	アンチクリプター
ネットワーク攻撃	ホストベースのファイアウォール
不正なデバイスへの接続	デバイスコントロール
不正な無線接続	Wi-Fiネットワークコントロール
PLCプログラムのスプーフィング	PLC整合性チェック
ICS特有の要因 — 空間的な隔たり、ICSソフトウェア/プロセスの誤検知など	主要産業オートメーションベンダーのソフトウェアを使用してテストされた信頼性の高いアップデート、主要産業オートメーションベンダーによる製品の認定

アプリケーションホワイトリスト

ICSのエンドポイント構成は比較的静的です。つまり、動的な企業ネットワークよりも、整合性管理措置が格段に効果的に働きます。KICS for Nodesには、以下のような整合性管理テクノロジーが搭載されています：

- ホワイトリスト（産業用制御ネットワークのベストプラクティス）またはブラックリストポリシーに基づくアプリケーションのインストールと起動の管理。
- ファイル、フォルダー、システムレジストリなどのオペレーティングシステムのリソースに対するアプリケーションアクセスの管理。
- .exe、.dll、および.ocxファイルや、ドライバー、ActiveX、スクリプト、コマンドラインインタプリタ、カーネルモードドライバーなど、Windows環境で実行されるあらゆる種類の実行可能ファイルの管理。

- アプリケーションのレピュテーションデータの更新。
- 事前定義およびユーザー定義のアプリケーションカテゴリによる管理対象アプリケーションリストの管理。
- 様々なユーザーによるアプリケーションコントロールの微調整。
- ブロックモードまたは検知のみモードでホワイトリストにないアプリケーションをすべてブロックするか、「監視」モードでホワイトリストにないアプリケーションの実行を許可して、アクセス可能な場合はKaspersky Security Centerにこのアクティビティを登録。

デバイスコントロール

デバイスのカテゴリ、ファミリー、および特定のデバイスIDに基づいてリムーバブルデバイス、周辺機器、およびシステムバスへのアクセスを管理します。

- ホワイトリストおよびブラックリストの両アプローチをサポート。
- 個々のユーザーやコンピューターまたはユーザーやコンピューターのグループへのコンピューターごと、ユーザーごとのきめ細かいポリシー割り当て。
- ブロックモードと検知のみモード。

ホストベースのファイアウォール

ネットワークアクセスポリシーを設定し、サーバー、HMI、ワークステーションなどの保護対象ノードに適用します。主な機能は以下のとおりです：

- 制限されたポートおよびネットワークによりアクセスを管理。
- 産業用ネットワークへの侵入直後にホストのスキャンと感染を図るマルウェアを送り込む可能性のある、請負業者のラップトップなど内部から仕掛けられたネットワーク攻撃を検知してブロック。

Wi-Fiネットワークコントロール

不正なWi-Fiネットワークに接続しようとする試みを監視できます。Wi-Fiコントロールタスクは、タスク設定で「許可されていない」あらゆるWi-Fiネットワークへの接続を自動的にブロックする「デフォルト拒否」テクノロジーに基づきます。

PLC完全性チェック

カスペルスキー製品で保護された特定サーバーの定期的なチェックにより、PLCの構成をさらに確実に管理できます。結果的なチェックサムは保存されている「標準」値と比較され、同じでない場合はレポートされます。

ファイル完全性モニター

この機能は、タスク設定で指定された監視範囲にある指定のファイルおよびフォルダー内で実行されたアクションを追跡するように設計されています。SCADAサーバーに保存されたSCADAプロジェクトの変更など、保護対象サーバー上でセキュリティ侵害になる可能性のあるファイル変更を検知するために使用できます。

高度なアンチマルウェアによる保護

Kaspersky Labが提供するクラス最高のプロアクティブなマルウェア検知およびブロックテクノロジーは、大量のリソース消費要件とシステム可用性要件を満たすことができるように再設計されました。当社の高度なアンチマルウェアによる保護は、静的な環境やほとんど更新されることのない環境でも十分な効果を発揮します。Kaspersky Labのアンチマルウェアは、以下のようなあらゆるテクノロジーをカバーしています：

- マルウェアのシグネチャベース検知。
- オンアクセスおよびオンデマンドでの検知。
- インメモリ（常駐）検知。
- 特殊なアンチクリプターテクノロジーによるランサムウェアの検知。
- 究極のマルウェア検知サービスを実現するKaspersky Security Network（KSN）とKaspersky Private Security Network（KPSN）。

信頼できるアップデート

Kaspersky Labのセキュリティアップデートは、保護対象システムの可用性に影響しないことを確認するために、データベースやコンポーネントのリリースおよびプロセス制御システムのソフトウェアや構成のアップデートに先立って互換性チェックが実行されます。潜在するリソース消費問題は、様々なシナリオを通して解決することができます：

- Kaspersky Labが自社のテストベッドで産業オートメーションベンダーのソフトウェアを使用して定義データベースのアップデートの互換性テストを実施。
- IAVが互換性チェックを実施。
- Kaspersky Labがお客様に代わってセキュリティ定義データベースのアップデートをチェック：SCADAサーバー、ワークステーション、およびHMIのイメージをKaspersky Labのテストベッドに統合。
- Kaspersky Labのセキュリティアップデートをお客様のサイトでテストし、Kaspersky Security Centerから自動化。

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Labが提供するネットワークレベルのセキュリティソリューションは、産業用通信プロトコル（Modbus、IECスタック、ISOなど）層で動作します。高度なDPI（ディープパケットインスペクション）テクノロジーを利用して産業にかかわるトラフィックに異常がないか分析します。ネットワークの完全性管理機能とIDS機能も提供されます。

脅威とリスクの要因	Kaspersky Labのテクノロジー
産業用ネットワークへの不正なネットワークデバイスの出現	ネットワーク完全性管理による新規/不明なデバイスの検知
産業用ネットワークでの不正な通信の発生	ネットワーク完全性管理による既知/不明なデバイス間の通信の監視
以下のものによる悪意のあるPLCコマンド： • **オペレータまたはサードパーティ（請負業者など）による誤り** • **内部関係者（不正行為）** • **攻撃者/マルウェア**	DPIテクノロジーにより、PLCとの間の通信を分析し、技術プロセスのコマンドおよびパラメータ値を管理
ネットワーク攻撃	高度な不正侵入検知システムにより、産業用ソフトウェアおよびハードウェアの脆弱性の悪用など、既知のあらゆるネットワーク攻撃パターンを特定
調査およびフォレンジック用のデータの欠如	フォレンジック用ツール：疑わしい産業用ネットワークイベントや検知された攻撃を監視して安全に記録

非侵入型の産業用ネットワークトラフィックの調査

KICS for Networksは、潜在的な攻撃者に気付かれないように異常とネットワークセキュリティを受動的に監視するネットワークモニターを備えています。この機能は、ポートミラーリングを有効にして構成するだけでインストールできます。また、既存のスイッチまたはTAPデバイスのSPANポートを使用して、ソフトウェアや仮想またはハードウェアアプライアンスを既存の産業用ネットワーク装置に簡単に統合できます。KICS for Networksはモジュール型アーキテクチャのため、センサーを中央制御装置から個別に導入できます。

産業向けDPIによる異常の検知

KICS for Networksでは、産業ユーザーにプロセス制御コマンドの流れとテレメトリデータを監視する信頼性の高いプラットフォームが提供されます。これにより、特に以下のことが可能になります：

- PLCの構成を変更したりPLCの状態を変える可能性のあるコマンドをすべて検知。
- 技術プロセスにおける制御パラメータの変更。
- システムに直接アクセスできるエンジニア、SCADAオペレータなどの社内スタッフによる内部からの「高度な」妨害のリスクを緩和しながら、外部からの脅威に対する保護を提供。

マシンラーニング（機械学習）

Kaspersky Labの産業向けDPIは、標準的なルールベースのアプローチでの構成はもちろん、強力なLSTMベースの予測モデルを使用して産業プロセス内部の異常を検知することもできます。マシンラーニング機能により、産業設備における異常検知がかつてないレベルへと進化し、きわめて複雑で、頻繁に構成変更が行われる産業用ネットワークでのインシデントの発見が可能になります。

セキュリティおよび資産インベントリのネットワーク完全性管理

KICS for Networksでは、SCADAサーバー、HMI、エンジニアリング用ワークステーション、PLC、IED、RTUなど、Ethernetで接続されたネットワーク資産をすべて識別できます。新しいデバイスや不明なデバイスとそのデバイスによる通信は自動的に検知されます。この機能により、セキュリティチームは信頼性の高いセキュアなネットワーク資産インベントリを独自に開発できるようになります。潜在的に脆弱で、攻撃者の格好の標的となるOT/IT資産管理ツールに頼る必要はもうありません。

フォレンジック用ツール

Kaspersky Labのソリューションには、産業ユーザー向けに、データ分析およびデジタルフォレンジック用のツールを備えた安全な記録システムが用意されています。また、このシステムにより、ICSログのあらゆる改変が阻止されます。

Kaspersky Industrial CyberSecurityのその他のサービス

Kaspersky Security Network

Kaspersky Security Network（KSN）は、世界中の数百万ものノードからセキュリティ上の脅威に関するインテリジェンスを収集して分析する、クラウドベースの複合分散型専用アーキテクチャです。KSNは、最新の脅威やゼロデイ攻撃を検知してブロックするだけにとどまらず、オンライン攻撃の攻撃元を突き止めてブラックリストに登録し、Webサイトやアプリケーションのレピュテーションデータを提供するうえでも役立ちます。

Kaspersky Labのすべての企業向けソリューションは、産業向けソリューションも含め、必要に応じてKSNに接続できます。主な利点は以下のとおりです：

- 卓越した検知率。
- 対応時間を短縮 – シグネチャベースの従来の対応時間は数時間：KSNは約40秒で対応。
- 誤検知率を低減。
- オンプレミスのセキュリティソリューションのリソース消費量を削減。

Kaspersky Private Security Network（KPSN）

データプライバシーに関して非常に特殊な懸念を抱いている組織のために、Kaspersky LabはKaspersky Private Security Networkオプションを開発しました。KSNのほぼすべての利点が提供される一方、いかなる情報もネットワーク外に送信されることはありません。

KPSNは、どんな組織の自社データセンターにも導入でき、社内のITスペシャリストがすべて管理することができます。KPSNをローカルにインストールすることで、国ごとのコンプライアンス要件や業界固有のその他の法規を遵守するために役立てることができます。

KPSNの主な機能：

- ファイルおよびURLのレピュテーションサービス：ファイルのMD5ハッシュ、URLの正規表現、およびマルウェアのふるまいパターンを中央に保存して分類し、クライアントに迅速に導入します。
- レコード管理システム（RMS）：セキュリティソフトウェアがファイルやURLを信頼するものとして、または信頼しないものとして間違って分類することもあります。RMSは「誤検知」の抑制手段として機能し、誤りの修正と継続的な分析によって品質を高めます。
- クラウドベースのインテリジェンスと情報。

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurityは、運用技術層および組織の構成要素（SCADAサーバー、HMI、エンジニアリング用ワークステーション、PLC、ネットワーク接続、エンジニアも含めて）を保護するよう設計された技術とサービスのポートフォリオであり、事業継続性や産業プロセスの一貫性に影響を及ぼさないよう設計されています。

詳細情報はこちら：
www.kaspersky.co.jp/enterprise-security/industrial

ICSサイバーセキュリティについて:
https://ics-cert.kaspersky.com
サイバー脅威に関する最新情報:www.securelist.com

#truecybersecurity

www.kaspersky.co.jp

© 2018 AO Kaspersky Lab.All rights reserved.登録商標および
サービスマークは、それぞれの所有者に属しています。

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* 第3回世界インターネット大会「World Leading Internet Scientific and Technological Achievement Award」

** 2016年China International Industry Fair(CIIF)特別賞