電力インフラストラクチャ向け サイバーセキュリティ

www.kaspersky.com/ics
#truecybersecurity

目次

はじめに 1

情報セキュリティの脅威に直面したときの発電所PACSの脆弱性 1

サイバーセキュリティの脅威防止、検知、軽減のための技術的ソリューション 4

KICS for Nodes 4

KICS for Networks 5

KICS for NodesとKICS for Networks：最新の変電所における配置の例 6

用語と定義 9

電力インフラストラクチャ向け サイバーセキュリティ

最新の電力システムは複雑な技術的施設であり、その規模と人命にとっての重要性という観点から特異な存在です。電力の物理的特性と、電気関連プロセスが一般的に高速であることを前提とすれば、このような施設の運用制御は、組織および技術の両方の観点で複雑なものになります。だからこそ、電力業界の創設と同時に、電力設備とオートメーションを緊急時に保護するための装置も出現したのです。これらの装置やその設計および機能に対する要件は、消費者および運用面での要求の拡大に対応する形で、保護対象の電力システムとともに進化してきました。

今日の保護/オートメーション/制御システム（PACS）は、発電所業務を全面的にカバーする、相互に関連するいくつもの情報システムから成る複合体です。計算と通信の技術が急速に発展したことで、電力コンポーネントの保護/オートメーションシステムも様変わりしました。さらに、最新の保護/オートメーションシステムに統合された新しい制御機能によって、電力供給ネットワーク施設の構築理念も変化しています。

制御品質の向上が、今後の電力業界の発展やスマートグリッドシステムへの移行における最大の課題の1つです。そのため、制御システムは、発電、電力輸送、電力供給における重要な役割を果たします。

現在、PACSは高度に統合されており、IEC 60870、IEC 61850、IEC 61970などの国際的なオープン標準に基づいたデジタル通信技術を利用しています。別々のサブシステムを統合することで、保護/制御システムの能力が強化され、よりインテリジェントで利用効率の高いものになりました。さらに、共通規格によって統合コストが大幅に下がり、機能の信頼性が向上しました。

発電所の制御と保護のための最新システムには、以下のようなさまざまな情報サブシステムがあります。

- オートメーション化された給電制御のためのハードウェアおよびソフトウェアアプライアンス
- 発電システム運用モードの維持のための自動制御
- 保護システム
- 緊急時自動保護システム
- プロセス制御システム
- オートメーション化された電力計測システム
- 電力品質制御システム

情報セキュリティの脅威に直面したときの発電所PACSの脆弱性

電力システムは高度なオープン性と統合性を備え、さらにIT技術やインターネット技術が日常生活に広く浸透していることから、電力業界に新たな課題が浮上しています。発電所向けのオートメーション化された最新の保護/制御システムは統合された分散型計算システムであり、各システムはオープンなプロトコル経由で互いに通信しています。これらのシステムでは、サイバーセキュリティの優先順位は低くなっています。電力制御システムが分離された環境のソリューションとして構築されているためです。しかし、最新の制御システムの場合は、グローバルに統合され、企業のサービスと接続されているため、サイバーセキュリティのリスクは非常に高くなります。

IEC 62351「Power systems management and associated information exchange – Data and communications security（電力システムの管理と関連する情報交換 - データおよび通信のセキュリティ）」規格では、発電所における情報セキュリティについて、以下の問題とその原因を重視しています。

オープンな通信

保護/制御システムコンポーネント間、および電力インフラストラクチャ施設間における、保護されていないオープンな通信回線について：

- **IDの確認不足**
  相互に通信するエージェントの認証がされていないか、十分ではありません。たとえば、技術的ネットワーク上のあるネットワーク装置が最上位システムに不正な制御コマンドや悪意のある制御コマンドを送信して、その結果、給電担当のオペレータが無効な操作を実行する可能性があります。

- **オープン標準、オープンなデータ転送**
  使用されているデータ転送プロトコルは、一般公開され詳細に文書化されているオープン標準に基づいています。プロトコルの無償の実装とソースコードが、分析およびエミュレーション用のツールとともに、一般に利用できる状態になっています。通常、このようなネットワーク内で転送されるデータについては、捕捉、参照、変更、再現が簡単であり、潜在的な侵入者にとっては、アクセスや脅威の実行が簡素化されます。

- **高水準のネットワーク通信**
  IEC 60807-5-10xおよびIEC 61850 MMSのプロトコル間の高水準通信を利用することは、電力会社の運用としては一般的です。しかし、これらのオープンな通信により、無効なデータパケットの大量送信によって、技術的インフラストラクチャの装置（給電所のプロセス制御システム、保護端末など）に対するサービス妨害（DoS）攻撃が容易になります。

- **パブリックネットワークへの接続**
  最新の産業施設の企業ネットワークおよび技術的ネットワークでは、制御システムのほぼすべての階層で複数の相互接続が発生することがあり、この状態は技術的装置に対する外部からの不正アクセスのリスクを増大させます。

従業員のサイバーセキュリティ意識の欠如

限られた数の技術者が多数の装置を管理し、それらの装置は大抵、永続的に監視されることなく1つの領域や部署で分散されています。以下のように、施設内のスタッフが基本的なサイバーセキュリティの知識を持っていないことも珍しくありません。

- **信頼できないネットワークからのリモートによる特権アクセスの実行**
  保守のしやすさや便利さを優先して、技術スタッフはしばしば、リモート施設の機器に対して完全な特権アクセスを可能にします。このようなアクセスは大抵、非公式に、しかも安全性を無視して構成されます（企業のワークステーションからインターネット経由でアクセスするなど）。

- **パスワードによる保護をしておらず、ユーザー管理ポリシーが存在しない**
  多数の装置を限られた数の担当者のみが保守していれば、パスワードによる保護やユーザー管理ポリシーを含む、装置のアクセスポリシーの構成と維持が難しくなります。これにより、技術的装置がしばしばデフォルトのパスワードのまま運用され、不正なアクセスが助長されています。

- **古いソフトウェアを使用している**
  IEDソフトウェアが技術的施設での稼働期間中にアップデートされることはほぼありません。既知のソフトウェアのバグは、産業プロセスに直接影響しない限り、除去されません。

- **安全でないワークステーションから保守を行う**
  技術的インフラストラクチャの保守中に使用されるポータブルワークステーション（ノートブック）は、通常の企業ワークステーションやソフトウェアテスト用の「試験」装置として、あるいは個人用に使用されることが多くあります。

- **構成やソフトウェアの定期的管理を行わない**
  デバイスの構成とソフトウェアの確認は年に1回も行われず、行われるとしても非定期で手動です。

セキュリティ要件が遵守されない

技術的インフラストラクチャ用の装置やソフトウェアの設計/開発プロセスでは、情報セキュリティ要件がほとんど考慮されません。

- **ハッキングへの抵抗力が弱い**
  開発者は一般的に、技術的インフラストラクチャとその構成要素に対する標的型攻撃や違法操作に対するコードの脆弱性を考慮しません。そのため、装置のハッキングに対する抵抗力は一般的に弱くなっています。

- **ネットワークセキュリティ設定が無効であるか不十分である**
  技術的ネットワーク内でのネットワークのセグメント化やネットワークセグメント間のアクセス制御の設定が無効になっていること、およびPACS実装プロジェクトで具体的なネットワーク設計ソリューションが存在しないことが、典型的な問題になっています。この理由で、ネットワークインフラストラクチャ設定の品質を維持できるかは、通常、設置担当チームのスキルと適格性にかかっています。

- **オープンチャネル経由の転送時にデータを保護しない**
  オープンな通信回線を利用するデータ転送に対して、安全策が取られていません。

- **ロールベースのアクセス制御を行わない**
  ロールベースのアクセス制御を行わないために、装置へのアクセス権が正しく設定されず、ユーザーが職務に見合わないアクセス権を得ることがあります。

- **アプリケーション起動コントロールソリューションが存在しない**
  不正なアプリケーション起動からコンピューターシステムを保護するための互換性のあるソリューションが存在しないために、産業環境のシステムが不正なソフトウェアの起動から保護されていないことも珍しくありません。アプリケーション起動コントロール用の一般的なツールは、産業用システムとの互換性がないか、効力がないことが多々あります（技術的ソフトウェアとの互換性がない、特定の技術的システムのリソースが不十分であるなど）。

- **セキュリティイベント登録ツールが存在しないか不十分である**
  プロセス制御システム内に専用の監視ツールやサイバーセキュリティイベント登録ツールが存在しないか、その機能が状況を十分に正しく解釈できません。

請負業者のアクセス制御の複雑さ

特定の保守作業を請負業者に任せることは一般的です。そのため、他のシステムコンポーネントに影響しない限られた機器に対する一時的なアクセス権のみを付与することが極めて重要になります。また、作業の完了時にアクセス権を取り消すことが不可欠です。

長寿命の脆弱なコンポーネント

装置や保護/制御システムの寿命は20～30年です。今日設置した安全でないシステムは、約20年後まで取り換えられないのです。安全なソリューション（暗号化を利用するものなど）は、脆弱性のある標準ソリューションと互換していないことも多く、即座の部分的アップグレードは、一般的には極めて困難です。

これらの技術上の問題に加えて、組織上の重大な問題も存在します。まず、オートメーション化されたシステム内で不審なアクティビティが検知されたときに何をすべきかを定義しているガイドがありません。次に、情報技術による制御システムへの悪影響を含む、技術的環境の障害の調査に関するガイドやプラクティスも不足しています。たとえば、技術的障害の調査と分類の方法を示す一部の参照用ガイドは、古いものであるために、サイバーセキュリティのインシデントを誤動作の原因の1つとして挙げることすらしていません。そのようなインシデントが発生した場合、真の原因は解明されません。これにより、適切な対策が取られず、インシデントが再発する可能性があります。

上記より、以下のような複数の構造的問題があることが明白です。

- 保護/発電装置の制御用の最新電力システムが分離されておらず、クローズドシステムになっていない
- 保護/オートメーション/制御システムに搭載されているサイバーセキュリティの機能が十分ではない
- 組織的、技術的な観点から、現在の条件下では悪影響を検知することが極めて難しい
- 攻撃が検知されたときの対応方法を明確に示したガイドラインが存在しない

サイバーセキュリティの脅威防止、検知、軽減のための技術的ソリューション

IEC 62351「Power systems management and associated information exchange - Data and communications security」規格では、発電所における複雑な情報セキュリティ対策のために利用可能なツールを詳細に説明しています。しかし、このソリューション案のほとんどは、フォーマットと通信プロトコルの手順変更が必要になったときに、オートメーション装置を完全に取り換えることでしか実装できないものです。

このような状況下では、IEC 62351の完全な実装は遠い目標のように思えますが、一部の要件を満たして、それらを最新のシステムに適用することができます。

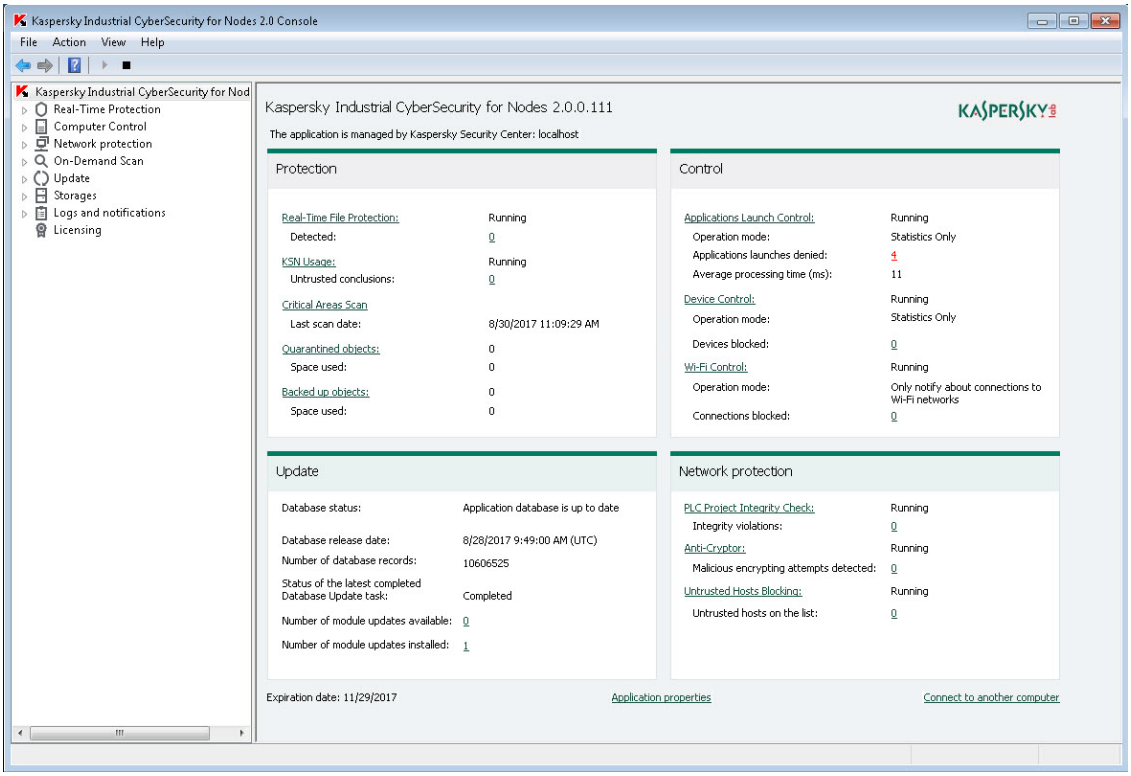
Kaspersky Industrial CyberSecurity（KICS）は、これらの要件を満たした、産業用インフラストラクチャ向けの総合的ソリューションです。

このソリューションは、以下の2つのコンポーネントで構成されています。

- KICS for Nodes – 産業用ネットワークのエンドポイント（エンジニアリング用ステーション、オペレータ用ステーション、SCADAサーバーなど）を保護するためのコンポーネント
- KICS for Networks – 産業用ネットワークを監視するためのコンポーネントであり、ネットワークの整合性チェックとアプリケーションプロトコルの詳細インスペクション機能を搭載（電力インフラストラクチャ向けのIEC 60870-5-104、IEC 61850などに対応）

KICS for Nodes

KICS for Nodesは、産業用システム専用の製品です。コンピューター用のソフトウェアアプリケーションとして、Windows OSが稼働する技術的サーバー、エンジニアリング用ワークステーション、オペレータ用ワークステーション、HMIを保護するように設計されています。



画像1：KICS for Nodesローカルインターフェイス

このソリューションの主な機能は以下のとおりです。

- アプリケーションのホワイトリスト機能（アプリケーション起動コントロール） – 明示的に許可されたものを除くすべてのアプリケーションの起動をブロックします。この保護コンポーネントでは、開発段階で容易なセットアップとデバッグを行うためのテストモードを利用できます。
- デバイスコントロール – 保護された産業用ホストに接続可能な装置を、管理者が定義して指定することができます。この技術によって、産業用システムを不正な装置の接続から保護できます。マスクがサポートされているため、管理がしやすく、装置の一括操作も可能です。
- Wi-Fiネットワークコントロール – 不正なWi-Fiネットワークへの接続の試みを監視することができます。
- 悪意のあるソフトウェアの検知（ランサムウェアを含む） – 保護手段としてシグネチャとヒューリスティックを組み合わせて、既知または未知の高度な脅威からWindowsワークステーションを保護します。特殊なアンチクリプター技術によってランサムウェア攻撃を防ぐことができます。
- ホストベースのファイアウォール – 産業用ホストへのネットワーク接続を制限することができます。
- PLC整合性チェック – プロジェクト内に変更箇所がないかを定期的にチェックすることで、制御装置の構成に対する追加の管理が可能になります。

KICS for Nodesでは、Kaspersky Security Centerをベースとするセキュリティインフラストラクチャ制御システムへの統合後、一元管理によって以下の機能を実行できます。

- 一元管理とセキュリティポリシー管理 – 個々の装置用とグループ用に、セキュリティ設定を構成することができます。
- 保護されたネットワークノード上のアンチウイルスデータベースの一元的なアップデート（技術的ネットワークがインターネットに接続されていない場合でも可能） – 技術的ネットワーク内の単一の管理サーバーからセキュリティエージェントをアップデートすることで、高いセキュリティレベルを確保できます。アップデートファイルは、再送用ノード（ITネットワーク上またはDMZ内に設置するもの）からインターネット経由で直接管理サーバーにダウンロードすることも、管理者がUSBデバイスを使用して管理サーバーに移すこともできます。
- 配信前の新しいアップデートのテスト – アップデートを産業用ホストに配信する前に、産業用ソフトウェアとの互換性をチェックすることができます。
- ロールベースモデルによる個別のポリシー管理とセキュリティエージェントによる操作 – 管理サーバー上でセキュリティポリシーが不正に変更される可能性を排除し、さらに保護の無効化やエンドポイントソリューション設定の変更を防ぎます。
- エンドポイントのセキュリティイベントデータ収集の一元化 - 登録済みイベントに基づいた包括的な情報セキュリティデータ分析と、インシデントの正確な原因の特定、および軽減策の容易な作成を可能にします。

KICS for Nodesの運用が、既定では産業用プロセスに影響を及ぼさないアプローチに基づいていることも注目すべき点です。

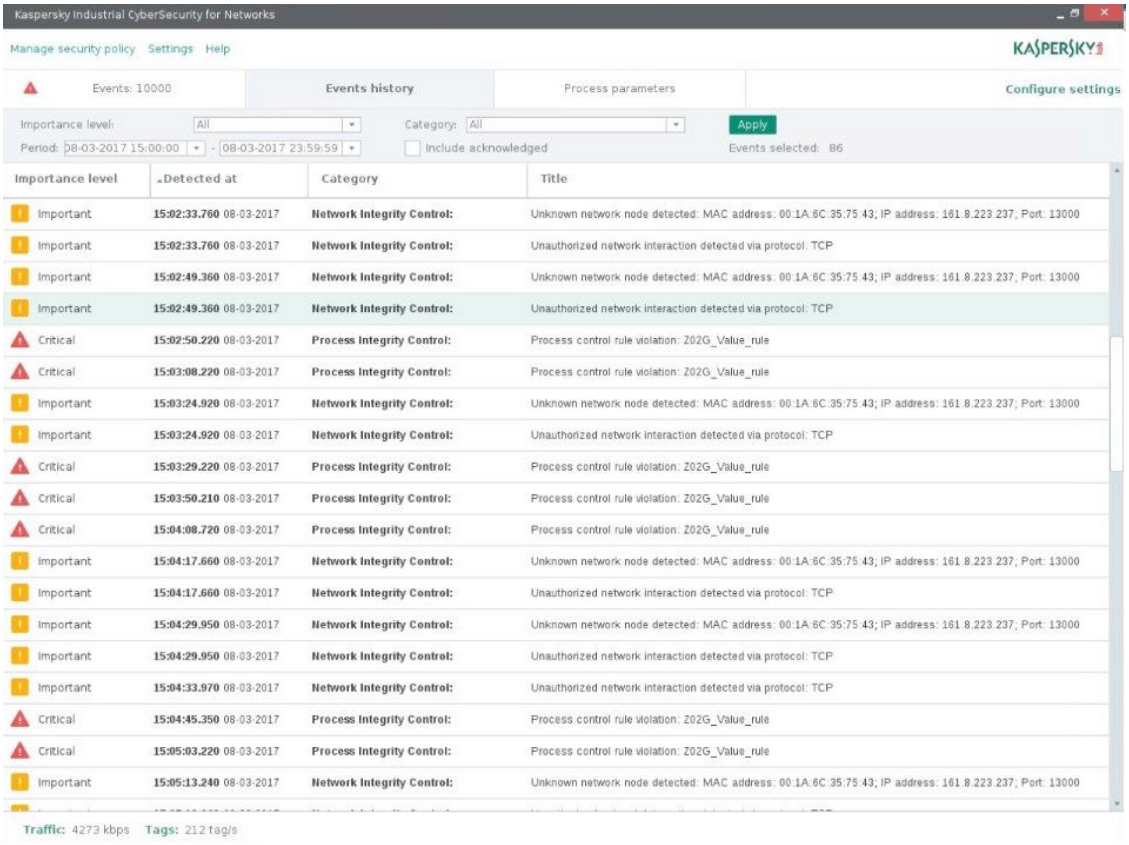
KICS for Networks

KICS for Networksは、産業用ネットワークの監視のための専用ソフトウェアソリューションです。このソリューションは、産業用プロセスを妨害せずに、異常を特定して、産業用ネットワークトラフィックから取得した重要な情報イベントを登録することができます。

このソリューションの主な機能は以下のとおりです。

1. ネットワーク整合性の監視：

- 利用可能なすべてのLANノードとそれらノード間の通信を検知し登録できるセルフトレーニングモード – このデータは後で参照ポイントとして、および変更の追跡の目的で使用できます。
- IPアドレスとMACアドレスに基づいて、技術的ネットワークの管理対象セグメントに接続された新しいネットワーク装置を検知し、登録します。
- 送信者ノードのアドレス、受信者ノードのアドレス、ネットワークプロトコル、ポート、許可された接続数などの属性に基づいて、ノード間の新しいネットワーク通信を検知し、登録します。



画像2：KICS for Networksローカルインターフェイス

2. パケットの詳細インスペクション：

- 構成に従って、技術的プロトコルの重要なメッセージの確認、分析、登録を以下のように行います。
  - 産業用ネットワークプロトコル（IEC 61850、IEC 60870-5-104）による装置管理コマンドの検知（スイッチングのオン/オフなど）
  - 産業用ネットワークプロトコル（IEC 61850、IEC 60870-5-104）による保護/制御システム運用パラメータを変更するコマンドの検知（グループスイッチのポイント設定など）
  - 管理対象のネットワークセグメント経由での、サービスソフトウェアによるIED制御/パラメータ設定の試みの検知
- 一般的な遠隔測定メッセージの監視

3.イベントの保存：

- KICS for Networksシステムは、検知されたイベントを安全な内部データベースに保存します。
- この情報は、保存期間とアーカイブサイズの上限に基づいて制限されます。画像3に、KICS for NetworksとKICS for Nodesの配置シナリオの例を示しています。

KICS for NodesとKICS for Networks：最新の変電所における配置の例

リング型トポロジによる2つのLANセグメントで構成される、安全な保護/制御システムの例をご紹介します。この変電所の1つ目のセグメントは「ステーションバス」（IEC 61850の「Station Bus」のこと）であり、これはIED間の通信を実現するものです。また、より上位にある給電制御装置との情報交換用に、変電所バス、変電所制御装置、遠隔測定ゲートウェイが使用されています。このLANセグメントでは、エンジニアリング用ソフトウェアを利用して、保護/制御システム機器へのアクセスを実現します。サービス用のアクセスは、ローカル、リモートの両面で実現可能です。ローカルサービス用のアクセスでは、ノートブックをIEDまたはステーションバスLANに直接接続します。サービス用のアクセスは、リモートのワークステーションからも実行できます。安定した運用の間は、IEC 61850 MMSプロトコルに従ってネットワークノード間の高速通信が実行されます。保護/制御システム装置のパラメータ設定に関するサービス用通信は、装置製造元の独自のアプリケーションプロトコルに従って実行されます。

このバスの物理的なLANセグメントは、接続された2つのスイッチによって形成されるリング型ネットワークです。すべての装置がこれらのスイッチに、二重接続型ノード（DAN）として接続されています。そのため、このセグメントに単一障害点はなく、比較的高度なネットワーク信頼性が確立されています。IEDはスイッチが内蔵されており、IED同士はチェーン方式でつながれています。このチェーンの終端が、このリング型ネットワークのスイッチに接続されています。そのため、あるチェーンの装置間のトラフィックが、リング型ネットワークスイッチ経由で転送されることはありません。リング型トポロジのネットワーク制御は、RSTPを使用して実行されます。リモートサービスがVPN経由で産業用ネットワークにアクセスできるように、このネットワークスイッチが設置されています。

2つ目のセグメントはオペレータ用のネットワークセグメントであり、このセグメントも同じようにリング型ネットワークトポロジで表現されています。このセグメントは、オペレータ用ワークステーションおよびプロセス制御システムのサーバー通信のためのものです。

ネットワーク制御センターおよびシステムオペレータとの通信は、オートメーションシステムに接続された変電所の制御装置経由で直接行われます（画像3を参照）。データ交換は、IEC 60870-5-104プロトコル経由で実行されます。

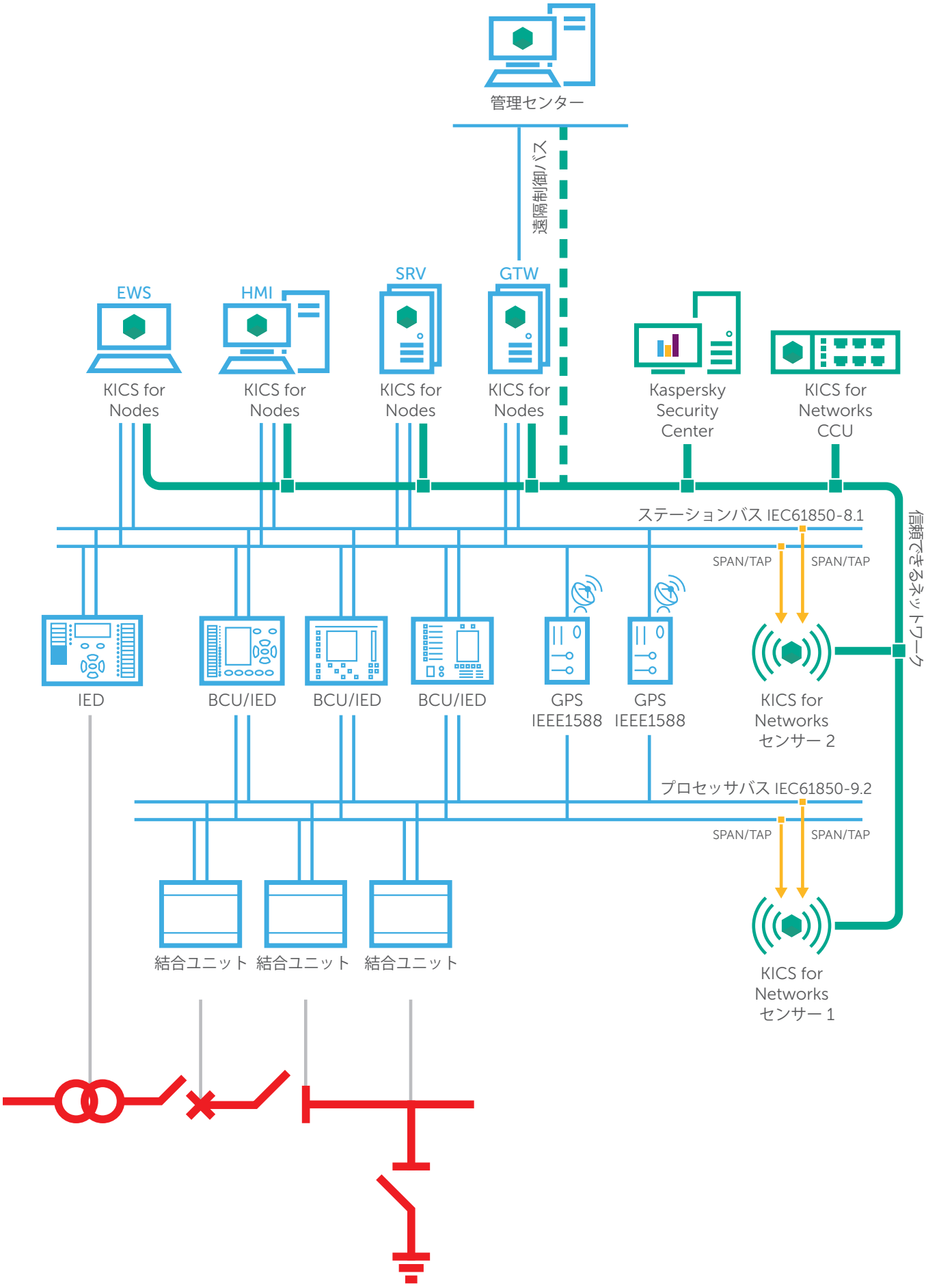
KICS for Networksは、技術的ネットワークインフラストラクチャを完全に監視する目的で、選択した各ネットワークセグメントにインストールする必要があります。そのため、この図では、ステーションバスセグメント用、オペレータネットワークセグメント用、そしてより上位にある制御装置との通信回線用に、3台のKICS for Networksサーバーを設置する必要があります。これらのKICS for Networksサーバーをインフラストラクチャに接続するためには、スイッチング機器を再構成して、各ネットワークセグメントのすべてのSPANトラフィックを該当するサーバーに転送することが必要になります。

KICS for Networksサーバーは、ネットワークスイッチのSPANポートに接続されます。このように構成することで、産業プロセスに影響を及ぼすことなく、産業用トラフィックのみを受信できるようになります。KICS for Networksは産業用トラフィックを処理し、不審なイベントを検知します。登録済みのイベントに関連するデータは暗号化された上で安全に保存されます。さらに、イベントは暗号化されたチャネル経由でKaspersky Security Centerに転送され、セキュリティ専門家向けに、検知済みイベントの確定版リストが作成されます。

KICS for Nodesソフトウェアは、Windows OSが稼働するコンピューターインフラストラクチャを保護するために、各産業用ホストにインストールする必要があります。KICS for Nodesも、検知されたイベントをKaspersky Security Centerサーバーに送信します。これらの産業用ホストには、制御ネットワークセグメントに接続するための追加のネットワークインターフェイスが必要になります。

すべての制御ネットワークの通信が暗号化されます。制御ネットワークの障害発生時、KICS for NetworksコンポーネントとKICS for Nodesコンポーネントは、スタンドアロンモードで運用を継続します。収集されたデータは、ネットワークセグメントの運用が復旧したときにKaspersky Security Centerに転送されます。

KICSは、SIEMシステムとの統合をサポートしています。Kaspersky Security Centerは、SIEMシステムとの暗号化されたチャネルを構成して、設定済みイベントをSIEM（HP ArcSight、IBM QRadar、syslog形式によるその他のプラットフォーム）に送信します。メールやSMSを使用して通知を送信することもできます。



画像3：Kaspersky Industrial CyberSecurityコンポーネントの配置図

用語と定義

CD - 計算装置（Computing Device）。事前に定義されたプログラムロジックに従ってデータ処理を実行できる技術的設備。

CSPS – サイバーセキュリティ保護システム（CyberSecurity Protection System）。保護対象の施設にサイバーセキュリティをもたらすように設計された、オートメーション化されたシステム。

IED – インテリジェント電子装置（Intelligent Electronic Device）。広範なデジタル通信機能を備える、特殊なマイクロプロセッサベースの多目的計算設備。

Industrial Cybersecurity – 産業向けサイバーセキュリティ。IT/OTレベルで産業プロセスの可用性、完全性、機密性を実現できる保護の状態。

LAN – ローカルエリアネットワーク（Local Area Network）。一定のネットワーク装置を対象としたコンピューターネットワークであり、これらの装置はローカルで管理される媒体経由で接続され、制限領域における位置情報原則に従ってグループ化される。

PACS –保護/オートメーション/制御システム（Protection, Automation & Control System）。施設に設置される、目的の異なるオートメーション化された自動制御システムの集合体の総称。

PCS – プロセス制御システム（Process Control System。産業用オートメーション/通信施設に設置される、人と機械によるシステムであり、管理下の施設で、オンサイトの包括的でオートメーション化された自動プロセス制御を行い、リモート給電所からのリモート制御実行を可能にするシステム。

Protection System – 保護システム。管理下の電力システムの中で故障した箇所を迅速に検知して分離し、安定したシステムパフォーマンスを保証するように設計されたIEDの集合体。

SCL – 変電所構成言語（Substation Configuration Language）。IEC 61850-6に定められている、変電所装置の構成を行うための言語および表現フォーマット。SCLには、装置の情報モデル、データセット、通信サービスを表現するためのリソースが含まれている。XML言語ベース。

Smart Grid – スマートグリッド。すべてのリソース（天然資源、社会資源、生産資源、さらには人的資源も）を効果的に利用することを目的として、運用および開発の構成と管理をマルチエージェントで行うことを原則とした、新世代の電力システム。このシステムでは、最新技術と統一的な階層型インテリジェント制御システムに基づいて、あらゆる主体（あらゆる種類の発電所、電力ネットワーク、および消費者）が柔軟に相互作用することで、消費者に対して安全、定性的、効率的な電力供給を行う。

SPAN – スイッチドポートアナライザ（Switched Port Analyzer）またはポートミラーリング。分析目的で、管理下のスイッチの選択したポートからネットワークトラフィックをミラーリングして収集するために使用するネットワークスイッチポート。

Station Bus – ステーションバス。プロセス機能（セルレベル）が実装されたインテリジェント装置によるデータ転送を行う、高速かつ信頼性に優れたコンピューターネットワーク。一般的な変電所の機能（変電所レベル）が実装された装置、ハードウェア、ソフトウェアの複合体（SCADA、遠隔操作ゲートウェイなど）によるデータ転送もその対象となる。ステーションバスで、セルレベルの装置間での水平通信が可能な場合もある。通信への電磁干渉を避けるために、ステーションバスではデータ転送媒体として光ファイバーが使用されることが多い。

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

* 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