デジタル時代におけるサイバーセキュリティの脆弱性

鉄道のデジタル化により、新しく洗練された技術の導入が進んでいます。デジタル化により鉄道産業に大きなメリットがある一方で、ユビキタスネットワークやオープン標準を利用しているため、鉄道ネットワークへのサイバー攻撃のリスクが高まっています。サイバー攻撃のリスクの増加に伴い、従来の鉄道インフラは脆弱なまま危機的な状況にあり、重要なインフラであるがゆえに、既知の問題だけでなく新たな脅威に対しても保護する必要があります。サイバー攻撃は非常に深刻な影響を及ぼし、金銭的な損害や社会的信用の失墜だけでなく、人命の危険にまで及ぶこともあります。

規制要件の順守

サイバーリスクを最小限に抑えるため、規制に関わる機関は、鉄道インフラのサイバーセキュリティ対策を更に強化するように鉄道事業社に促しています。例えば、EUのサイバーセキュリティ法（NIS指令）は、重要なインフラについての保護措置を規定しており、鉄道輸送サービスも含まれます。運行中の車両に対しサイバー攻撃の可能性についてモニタリングし、攻撃を検知した場合には報告する義務があります。怠れば重い罰則が科せられる場合があります。鉄道事業者が鉄道ネットワークを継続的にモニタリングし、安全を確保することは極めて重要です。

鉄道のサイバー攻撃対策

サイバーセキュリティの脅威に対抗し、決められた規則を遵守するには、脅威となる問題を監視する事が基本的な保護対策となります。監視対象となっていないシステムは、セキュリティ対策が施されていることにはなりません。

クノールブレムゼ鉄道システムジャパン株式会社
東京都新宿区西新宿 6-10-1
日土地西新宿ビル 7F
Tel: 03 3346 2620
Fax: 03 3346 2623
kbrsj.restko@knorr-bremse.com
www.knorr-bremse.com

- KNORR-BREMSE
- NEW YORK AIR BRAKE
- IFE
- MERAK
- MICROELETTRICA
- SELECTRON
- KIEPE ELECTRIC
- EVAC
- ZELISKO
- RAILSERVICES

脅威検知ソリューション

鉄道車両用ネットワーク不正侵入検知システム
(INTRUSION DETECTION SYSTEM: IDS)

ネットワークをリアルタイムで監視し、被害が発生する前にサイバー脅威を検知、車両をサイバー攻撃から守ります。
鉄道の稼働率を担保し、セキュリティを確保するよう設計されています。

SELECTRON

ネットワーク侵入検知 ー 仕組み

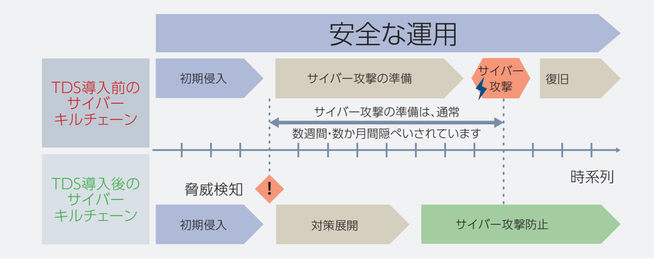
Selectron Thread Detection Solution (TDS) は、鉄道車両用ネットワーク不正侵入検知システム(Intrusion Detection System : IDS)です。鉄道産業特有のサイバーセキュリティ課題に対処します。内側から保護することは、外側への防御につながります。

サイバー攻撃防止にむけて

1. ネットワークシステムのアクティビティを監視。
2. 鉄道ネットワークのトラフィック異常を検知。
3. 行動異常検知機能により疑わしいアクティビティを分析。
4. 調査の初期段階でサイバー脅威を特定。
5. アラートを送信することにより不正侵入の試みを報告。

Selectron TDSによるサイバーリスク対応

- ✓ 新型車両、従来型車両どちらにも対応する認証済みスタンドアロンソリューション。
- ✓ 機械学習ベース。
- ✓ 状況に応じて、柔軟に、最適化し、最新の状態に更新。
- ✓ 行動異常を検知。
- ✓ ゼロデイ脆弱性を狙った攻撃も検知。



詳細はこちら

Selectron TDSは、新型車両だけでなく従来型車両に対するサイバー攻撃も防御します。被害拡散防止対策を駆使した脅威検知機能により、迅速な復旧と安全な運行を確保し、鉄道事業社を支援します。

包括的なサイバーセキュリティ対応アーキテクチャ

Knorr-BremseとSelectronが提供する包括的なサイバーセキュリティアーキテクチャは、安全認証されている車両に対してパワフルなサイバーセキュリティ機能を組みこみ、従来型システム及び新システムどちらにも対応します。

脅威検知ソリューションは、当社の包括的サイバーセキュリティアーキテクチャの要となる機能です。TCMS装置を保護し、制御システムの運用上のセキュリティをリアルタイムに監視します。

当社が提供するサイバーセキュリティ対策製品と侵入検知システムを搭載することにより、多層防御を実現します。脅威検知システムはIEC 62443に準拠しており、包括的な対策を保証し、識別管理用の公開鍵暗号基盤(PKI)、セキュアブート、整合性検証等、当社のセキュリティ対応アーキテクチャと統合することができます。

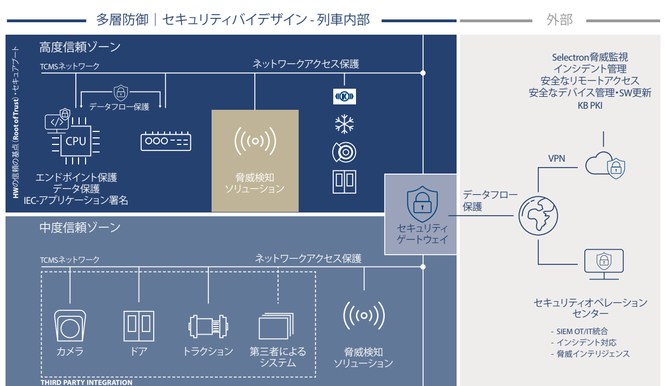
IECアプリケーションとして署名されることになり、アプリケーションの機密性と信頼性が保証されます。ハッキングされ操作されたアプリケーションを不正に使用してしまうという脅威を回避することができ、知的財産は保護されます。

鉄道事業社がサイバー攻撃に迅速に対応し、サイバーセキュリティ規制を遵守するには、異常事態の早期検知および報告が必要不可欠となり、偵察段階の初期に脅威を特定することが極めて重要です。

多層防御アプローチの一環として、TDSはEU NIS、IEC 62443およびTS50701規格、NIST対応のDETECT機能を搭載しています。

TDSは、認証済の車体上で動作し、SelectronおよびKnorr-Bremseが提供する製品(ドア、空調設備、ブレーキ、他)のプロトコル含め、鉄道車両に特有の各種プロトコルに対応します。

モジュール式で機能拡張が可能なため、新型車両だけでなく従来型車両にもコスト効率良く最適な改良をすることができます。



機能

- ハイレベルの経験則を基に、鉄道ネットワーク上のデータ異常を検知・分析し、攻撃が具体化する前にすばやく修復します。
- 新しい脆弱性を発見するごとに、検知ルールを更新します。
- 各種ネットワーク上のTDSセンサーからの情報と共に、クラウド上で一元化され、文書化されたイベント管理。
- セキュリティ侵害を検知すると、収集したイベントログをもとに迅速かつ徹底した科学的分析とリスクアセスメントを実施、早期解決につなげます。
- イベントログは改ざんされないよう保護されているため、法規制が適用される場合もログを使用することができます。
- セキュリティ警告は、バックエンドのコンポーネントから受信することができ、グラフィックダッシュボードで可視化することも可能です。
- クラウド仕様を含むすべてのTDSサービスは、お客様固有の認証情報をベースにアクセスを制御することができます。
- 保存データおよび転送中のデータを常に暗号化します。
- プラグアンドプレイ型のパッシブセンサーや構成設定が最適化されており、取り付けが容易です。
- 新旧双方の鉄道ネットワークを監視します。CAN、MVBに対応、将来的にイーサネットにも対応する予定です。
- パッシブモードで動作するため、列車制御システムに干渉しません。
- 標準インターフェースを使用しているためSIEM/SOCへ情報を送信することが可能。保有する車両へのサイバー攻撃に対する防御力を強化します。
- オプションで、セキュリティ運用と管理のためのRail SOCをマネージドサービスとして提供できます。
- 柔軟なソリューション
  - ローカル:ホワイトリストに基づく自律システム。
  - 高機能:クラウド接続により機械学習機能のあるIDS。

TDSのメリット

- ✓ EU NIS指令といった規制を順守しています。
- ✓ 車両の再認証を受ける必要がなく、新旧車両にシンプルに実装することができます。
- ✓ サイバー脅威に効果的な防御シールドを構築し、鉄道の運行とセキュリティを確保します。
- ✓ Selectronが提供する各種サイバーセキュリティソリューションとの組合せにより多層防御を実現します。
- ✓ 社会的信用や知的財産といった企業にとって極めて重要な資産を保護します。
- ✓ 単独でセキュリティを強化する唯一のソリューションです。EN 50129:2019セキュリティ要件を順守するのにも有効な対策です。