ケーススタディ

Moxa

Moxa V2406Cシリーズ、産業用コンピューターによるサイバーセキュリティ対策、エンドポイント保護の強化

より安全なコンピューティングプラットフォームとインテルのハードウェア対応セキュリティソリューションにより、サイバー脅威から身を守り、機密データを保護します

目次:

はじめに

今日、データは間違いなく現代のビジネスの生命線となっており、重要なプロセスや業務のリアルタイム管理を最適化するための貴重な洞察を与えてくれます。毎日、世界中の遠隔地や過酷な環境で動作するセンサーやIoTデバイスから、大量のデータが日常的にリアルタイムで収集されています。このデータは増え続けており、企業の運営方法やITインフラストラクチャも変化しています。一元化されたデータセンター上に構築されていた従来のコンピューティング環境は、増え続けるペースの速いリアルタイムデータの流れにはもはや適合しません。待ち時間や予測不可能な中断は、業務に支障をきたす可能性があります。企業はこれらのデータ課題への対応としてエッジコンピューティングアーキテクチャを採用しています。エッジコンピューティングは、計算とデータストレージの一部を、IoTデバイスやローカルのエッジサーバーなど、データが生成される場所の近くに移動させる分散コンピューティングの構想です。

エッジコンピューティングを採用することで、AIを活用した機能とユーザーエクスペリエンスを実現しながら、アプリケーションのレイテンシを大幅に短縮できます。しかし、エッジコンピューティングの普及に伴い、より多くのデバイスが分散した場所に配置されるようになり、サイバーセキュリティ対策が新しい環境に合うように調整されなければ、不正アクセスやデバイスの物理的な改ざんによる干渉や損害のリスクが高まります。エンドポイントを悪意のある活動から守ることは、ハッカーがデータを盗んだり、重要な操作を妨害したり、企業のインフラやシステムにアクセスしたりするのを防ぐことができるため、非常に重要です。Operational Technology(OT)のエンドポイントを適切に保護しないと、企業はサイバー攻撃の重大なリスクにさらされ、事業運営全体とITインフラストラクチャに深刻な影響を与える可能性があります。近年、鉄道部門はサイバー脅威による攻撃を受けることが増えています。[1] 専門家は、重要な安全システムにマルウェアが潜んでいて、運行に重大な脅威を与える可能性があるため、サイバー攻撃者が公共鉄道システムを破壊するリスクが高まっていると考えています。[2] 2020年、スイス鉄道車両メーカーのITネットワークがマルウェアに攻撃され、同社が600万ドルの身代金の支払いを拒否すると、サイバー攻撃で盗まれた文書がオンラインで公開されました。[3]

サイバー攻撃が進化するにつれて、これらのセキュリティ上の脅威から保護するにはソフトウェアだけではもはや十分ではありません。ソフトウェアは、ハッカーがビジネスシステムにアクセスすることを可能にする侵害によってなりすまされる可能性があります。Moxaは、インテルと提携して、ソフトウェアとハードウェアベースのセキュリティ機能を組み合わせることで、侵入防止と侵害への対応を両立するように設計されたソリューションを提供しています。これにより、パートナーのサイバーセキュリティフレームワークをサポートし、OT分野のデータセンターのインフラストラクチャを安全に保つのに役立ちます。

Moxaについて*
Moxaは、産業用IoT(IIoT)の接続を可能にするエッジ接続、産業用コンピューティング、ネットワークインフラストラクチャソリューションの大手プロバイダーです。30年以上の業界経験を持つMoxaは、世界中で8200万台以上のデバイスを接続し、80か国以上の顧客にリーチする流通およびサービスネットワークを持っています。Moxaは、信頼できるネットワークと誠実なサービスで業界を強化することで、永続的なビジネス価値をもたらします。

インテルのハードウェア・セキュリティ:次世代のセキュアな産業用コンピューターの基盤

セキュリティはハードウェアに根ざしたシステム特性で、ソフトウェアからシリコンまで、あらゆるコンポーネントがデータの保護とデバイスの完全性の維持に役立ちます。私たちには、脅威検出、データ/コンテンツ保護、メモリ保護などのソリューションを含む、多層防御戦略に基づいて構築して実行するための一連のテクノロジーがあります。

インテルのハードウェア・セキュリティ・テクノロジーは、3つの主要な優先事項を中心とした特定の課題に対応しています:

- 基礎的なセキュリティー
  プラットフォーム全体で重要な保護基盤を確保し、アイデンティティと完全性に重点を置いています。インテルは、プラットフォームが正しく稼働し、期待どおりに動作することを保証するテクノロジーを提供してきた長い歴史があります。当社のセキュリティエンジンは世界中で10億回以上使用されており、当社のプロセッサーはパフォーマンスを向上させ、グローバルな商取引を保護するために強化された暗号化機能を備えています。

- ワークロードとデータ保護
  すべての正当なワークロードに、使用中のデータをハードウェアで分離して保護するための信頼できる実行環境を提供し、さまざまな規模のワークロードに合わせてスケーリングします。強固な基盤ができれば、セキュリティ技術は仮想マシンやオペレーティングシステムを標的型攻撃から保護するために拡張されます。

- ソフトウェアの信頼性
  インテルは、一般的なソフトウェア攻撃や新たなソフトウェア攻撃から保護するハードウェアプラットフォームを提供しています。これにより、効率が向上し、パフォーマンスが維持されます。私たちはソフトウェアを強化し、一部のセキュリティ機能をハードウェアに移行し、検証の層を増やしています。

Moxa V2406Cシリーズのインテル® プロセッサーに搭載されたインテルのハードウェア対応セキュリティ・テクノロジー:

1. インテル® ブートガード
   インテル® ブートガードは、ハードウェアベースの完全性の重要な要素を提供し、UEFIセキュアブートのMicrosoft Windows要件を満たし、BIOSブートブロックの不正な変更を軽減します。CPUがIBBを実行する前に、このコードの正しさを検証します。Intel Boot Guardを有効にして起動しても、ハードウェアヒューズに固定されているため、起動の完全性は変わりません。Intel Boot Guardはハードウェアのルートオブトラストとなり、UEFIブートプロセスが各ソフトウェアモジュールを実行する前に暗号的に検証および/または測定する信頼連鎖プロセスに堅牢性を追加します。Intel Boot Guardプロセスの結果、マルウェアがプラットフォーム上のハードウェアやソフトウェアコンポーネントを悪用する可能性が低くなります。

2. インテル® トラステッド・エグゼキューション・テクノロジー (インテル® TXT)
   インテル® Trusted Execution Technologyは、インテル® プロセッサーとチップセットにハードウェアを拡張したセットで、測定された起動や保護された実行などのセキュリティ機能でデジタルオフィスプラットフォームを強化します。インテルのTrusted Execution Technologyは、ソフトウェアベースの攻撃から保護し、クライアントPCに保存または作成されたデータの機密性と完全性を保護するハードウェアベースのメカニズムを提供します。(4)

3. インテル® アドバンスト・暗号化規格の新しい指示 (インテル® AES-NI)
   インテル® AES-NIは、高度暗号化標準 (AES) アルゴリズムを改善し、エンドポイントコンピューティングデバイス用の最新のインテルプロセッサーのデータ暗号化を高速化します。Intel AES-NIは、7つの新しい命令で構成され、エンドポイントのコンピューティングデバイスで広範囲にわたる暗号化を実現できるようにします。(5)

産業用OTセキュリティを念頭に置いたMoxa V2406C

1. Moxa V2406Cでセキュア・ブート
   セキュアブートは、コンピューターが常に検証され承認されたブートローダーとオペレーティングシステムから起動するように設計されたセキュリティ保護メカニズムです。これは、マルウェアのような無許可のソフトウェアが起動時にコンピューターを制御するのを防ぐのに役立ちます。Moxa V2406Cは、ハードウェアのルート・オブ・トラスト (RoT) としてTPM 2.0を採用しました。ハードウェアは、インテル® ブートガード付きのセキュア・ブート・チェーンを採用し、プロセッサーからBIOS、Linuxオペレーティングシステムまで、あらゆる重要な起動段階でデジタル署名を行いました。これにより、検証プロセスの根本が常に信頼できるものになります。Moxa V2406Cシリーズは機密情報を保護するために設計されており、IEC 62443-3-3およびIEC-62443-4-2のシステムセキュリティ要件を満たしています。

2. Moxa V2406Cによるフルディスク暗号化
   フルディスク暗号化は、主にハードディスク全体を完全に暗号化することにより、盗まれたハードディスクの機密データが漏洩するのを防ぐために使用されます。Moxa Computerは、TPM 2.0を使用して、各コンピューターの固有のディスク復号化キーを保存および保護しています。TPM 2.0の復号化キーは、セキュアブートプロセスが検証されて初めてアクセス可能になります。そのため、ハードディスク内のデータに特定のMoxaコンピューターからしかアクセスできないようにするために、信頼連鎖検証プロセスを作成しました。Moxa Industrial Linux (MIL) 2.0を搭載したMoxa V2406Cシリーズは、IEC 62443-3-3のシステムセキュリティ要件を満たすため、機密情報を保護するように設計されています。

鉄道網がますます混雑するにつれて、インテルとそのエコシステムが鉄道業界の未来を牽引しています。当社のソリューションは、業界パートナーと協力して、セキュアブート、認証、コンテンツ保護を通じて、鉄道業界が線路脇から管制センターまでの安全とセキュリティを実現できるよう支援しています。

ケーススタディ:信頼性の高い鉄道旅客情報システム (PIS) とゲートウェイネットワークビデオレコーダー (NVR) 用のV2406C産業用PC、セキュリティを念頭に置いて開始

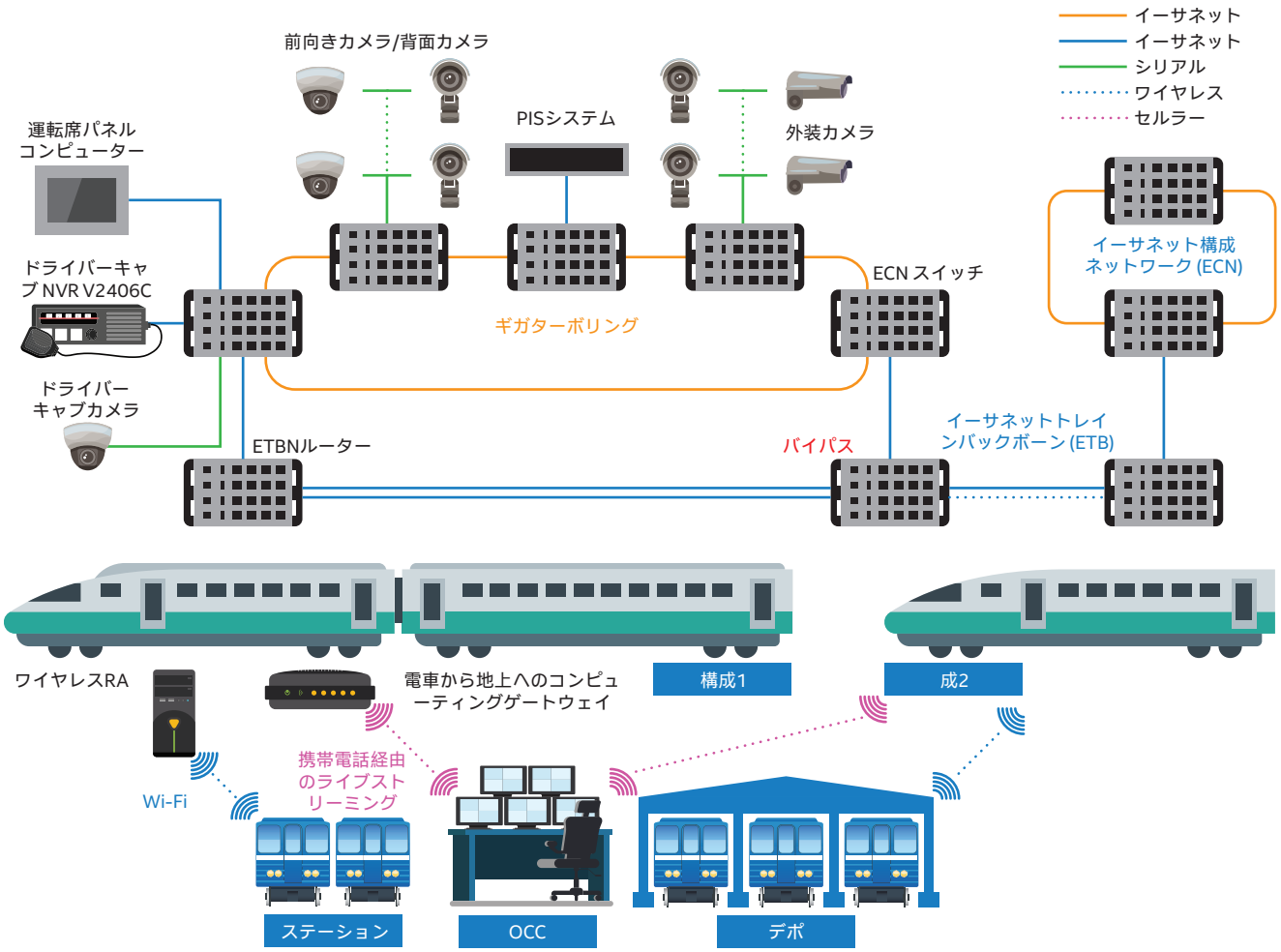

図1。NVRの鉄道車両

Moxa V2406C産業用パソコンの紹介

Moxaの産業用PC（IPC）V2406Cシリーズは、厳しい環境向けに設計された頑丈な人工知能（AIoT）エッジコンピューターです。IEC-62443-4-2、セキュリティレベル2に準拠して設計された、高性能で堅牢で安全なV2406Cシリーズレールコンピューターは、インテル® Core™ i7/i5/i3またはCeleron® ハイパフォーマンスプロセッサーを中心に構築されており、十分なメモリストレージ拡張とワイヤレス接続サポートをすべてコンパクトなケースに入れています。車載列車システムは、過酷な環境で長期間動作するため、高湿度、変動する温度、持続的な振動に耐えられる十分な頑丈さと耐性を備えている必要があります。また、配線規制のある制限された場所にも適合する必要があります。厳しいテストに合格し、業界標準に厳密に準拠しているV2406Cシリーズは、過酷な環境や高速で移動する列車でも長持ちし、確実に動作するため、鉄道業界のAIやエッジコンピューティングアプリケーションに最適です。2つのギガビットイーサネットポート、4つのRS-232/422/485シリアルポート、6つのDI、2つのDoS、4つのUSB 3.0ポート、2つのMPCIeワイヤレス拡張スロット、4つのSIMカードスロットを含む豊富なインターフェースを備えたV2406Cシリーズは、鉄道の車内や沿線での使用に適しています。これらのインターフェースは、冗長なLTE/Wi-Fi接続を確立するのに役立ち、動きの速い電車と沿線のアプリケーション間の確実な双方向通信を保証します。

課題:レガシー車両は手動のメンテナンスが必要です

V2406Cシリーズは、監視目的で新旧両方の車両にネットワークビデオレコーダー（NVR）コンピューターとして導入されています。ただし、従来の車両では、監視映像をオペレーションコントロールセンター（OCC）にリアルタイムで同期させるために、信頼できるインターネット接続がない場合があります。そのため、監視映像を含むV2406Cシリーズのホットスワップ可能な2つのHDD/SSDは、メンテナンススタッフによる手動メンテナンスを通じて、定期的にOCCのサーバーに転送されます。また、USB経由でのBIOSやOSのアップグレードなど、その他のメンテナンス作業もメンテナンススタッフによって行われます。V2406Cシリーズで撮影された監視映像は、一般データ保護規則（GDPR）によって規制されています。そのため、データの盗難や不正公開の脅威は、資産所有者にとって最大の懸念事項となっています。V2406シリーズは安全なキャビネットに設置されていますが、特定のシナリオによる脅威を軽減するには多層防御戦略が必要です。たとえば、メンテナンス期間中や電車からOCCへの移動の合間に、HDDの盗難や紛失により、不正なデータ漏洩が発生する可能性があります。それ以外にも、廃止措置の段階でも不正なデータ漏洩が発生する可能性があります。最後に、メンテナンススタッフが悪意のあるBIOSやOSを意図的または意図せずにインストールしているときに、不正なデータ漏洩が発生する可能性があります。

解決策:セキュリティを強化するための対策を事前に構成します。
V2406Cシリーズは、機密データの保存を保護するために設計されたフルディスク暗号化機能を備えており、許可されたデバイスまたは担当者のみがデータを読み取れるようにしています。V2406Cシリーズは、インテル® ブートガードをハードウェアのルートオブトラストとして使用し、ブート時に一連のトラスト検証シーケンスを開始することで、データアクセス用にストレージを復号化する前に、起動時にBIOSとOSの完全性と信頼性を確保するのに役立ちます。インテル® ブートガードを活用して、Moxaの公開鍵はワンタイムプログラマブル(OTP) CPUヒューズに保存され、検証プロセスのルートが常に信頼できるものであることを保証します。

さらに、製造段階では、各Moxa V2406Cシリーズの独自のソフトウェアとハードウェアのフットプリントは、Trusted Platform Module (TPM) 2.0の安全なストレージアクセスによって制限されます。これにより、暗号化されたストレージは、この非常に特殊なMoxaデバイスでのみ復号化できます。TPM 2.0の復号化キーは、セキュアブートプロセスが検証されて初めてアクセスできます。そのため、ハードディスク内のデータに特定のMoxaデバイスからのみアクセスできるようにする信頼連鎖検証プロセスを作成することで、盗まれたハードディスクから機密データが意図せず公開されるのを防ぐことができます。(図2を参照してください)

図2: 起動中のMoxaチェーン・オブ・トラスト・バリデーション

結論

OTセキュリティは、ハードウェアとソフトウェアのスタックを通じてセキュリティ対策を行います。これらは、企業内の物理システムの監視、検出、制御に欠かせません。鉄道網が混雑し、悪意のある攻撃が増え続ける中、実行時にITシステムの完全性を保証するために、機密データやその他の機密資産を保護することがますます重要になっています。

IntelとMoxaは、企業が交通網やシステムを悪意のある攻撃から保護できるようにするスマートなソリューションで、鉄道業界の未来を牽引しています。インテルのTrusted Execution Technologyを使用して、ソフトウェアベースの攻撃から保護し、Moxa V2406Cシリーズの産業用コンピューターに保存または作成されたデータの機密性と完全性を保護するのに役立つハードウェアベースのメカニズムを提供しています。これらの機能は、アプリケーションの実行環境を信頼するために必要な、ハードウェアに根ざした保護メカニズムを提供します。また、これらのメカニズムは、プラットフォーム上で実行される悪意のあるソフトウェアによって重要なデータやプロセスが危険にさらされるのを防ぐのに役立ちます。IEC 62443のような業界のセキュリティ基準を満たす最終ソリューションを提供したいビジネスパートナー向けに、Moxa V2406Cは、ホストコンポーネントの要件であるIEC 62443-4-2に沿ったセキュリティ目標を達成するように設計されています。
詳細については、インテルの営業担当者にお問い合わせください。

もっと詳しく知る
- Moxa産業用パソコンについてもっと知るには https://www.moxa.com/jp/products/industrial-computing/x86-computers/v2406c-series
- インテルの担当者に相談して、組織が必要とするリソースを見つけてください。

参考資料とリソース:

1. 鉄道におけるサイバーセキュリティは、今まで以上に重要になっていますか? https://www.railway-technology.com/analysis/is-cybersecurity-rail-important-now-ever/
2. 専門家によると、鉄道輸送はサイバー攻撃に対して脆弱である https://www.cybersecuritydive.com/news/rail-transit-cyberattacks/619123/
3. 鉄道におけるサイバーセキュリティ:IRSのウェビナーから学んだ3つの教訓 https://www.railway-technology.com/analysis/cybersecurity-rail-three-lesson s-irs-webinar/
4. インテル® トラステッド・エグゼキューション・テクノロジー(インテル® TXT)の概要 https://www.intel.com/content/www/us/en/support/articles/000025873/tech nologies.html
5. インテルのバーチャライゼーション・テクノロジーを使用して、ユーザーエクスペリエンスに影響を与えずにエンドポイントのアプリケーションとデータを保護するホワイトペーパー https://www.intel.com/content/www/us/en/architecture-and-technology/cybersec urity-virtualization-technologies-paper.html
6. Moxa インダストリアルリナックス(MIL) https://www.moxa.com/jp/products/industrial-computing/system-software/moxa-industrial-linux

0622/KSW/ln2/PDF