Kaspersky Embedded Systems Security

kaspersky

組み込みデバイスのセキュリティ課題

1. **旧式の脆弱なソフトウェア。** ライフサイクルが長いと、サポート終了状態のオペレーティングシステムやアプリケーションが使用され続ける可能性があり、これらは修正されていない脆弱性を抱えたまま、攻撃の標的とされかねません。

2. **不規則なセキュリティ更新。** ソフトウェアがサポートされている場合でも、パッチがすぐに適用されない恐れがあります。地理的に分散した複数のデバイスをアップデートする際の問題として、デバイスをオフラインにする必要があり（そのため一時的なサービスの停止が余儀なくされ）、また適用する前にアップデートをテストする必要があるため、パッチ適用が遅れる原因となります。

3. **プロセスの継続性。** 医療機器などの特定の種類のデバイスであれば、たとえ一時的であってもサービスが停止してしまうことは大きな問題となり、パッチが適用されるまでにさらに時間がかかる可能性があります。

4. **公共の場所。** 多くの組み込みデバイスは開かれた公共の場所で動作するため、改竄のリスクが大幅に高まります。ネットワークレベルの防御では、直接的で物理的な感染からデバイスを保護することはできません。

5. **本質的にリスクの高い環境。** 場合によっては、デバイスは金融業務に直接的に関連しており、機密性の高い個人情報を処理することがあるため、組み込みデバイスはサイバー犯罪者にとって特に魅力的な標的となります。

組み込みシステム（およびその他）向けに設計されたオールインワンセキュリティ

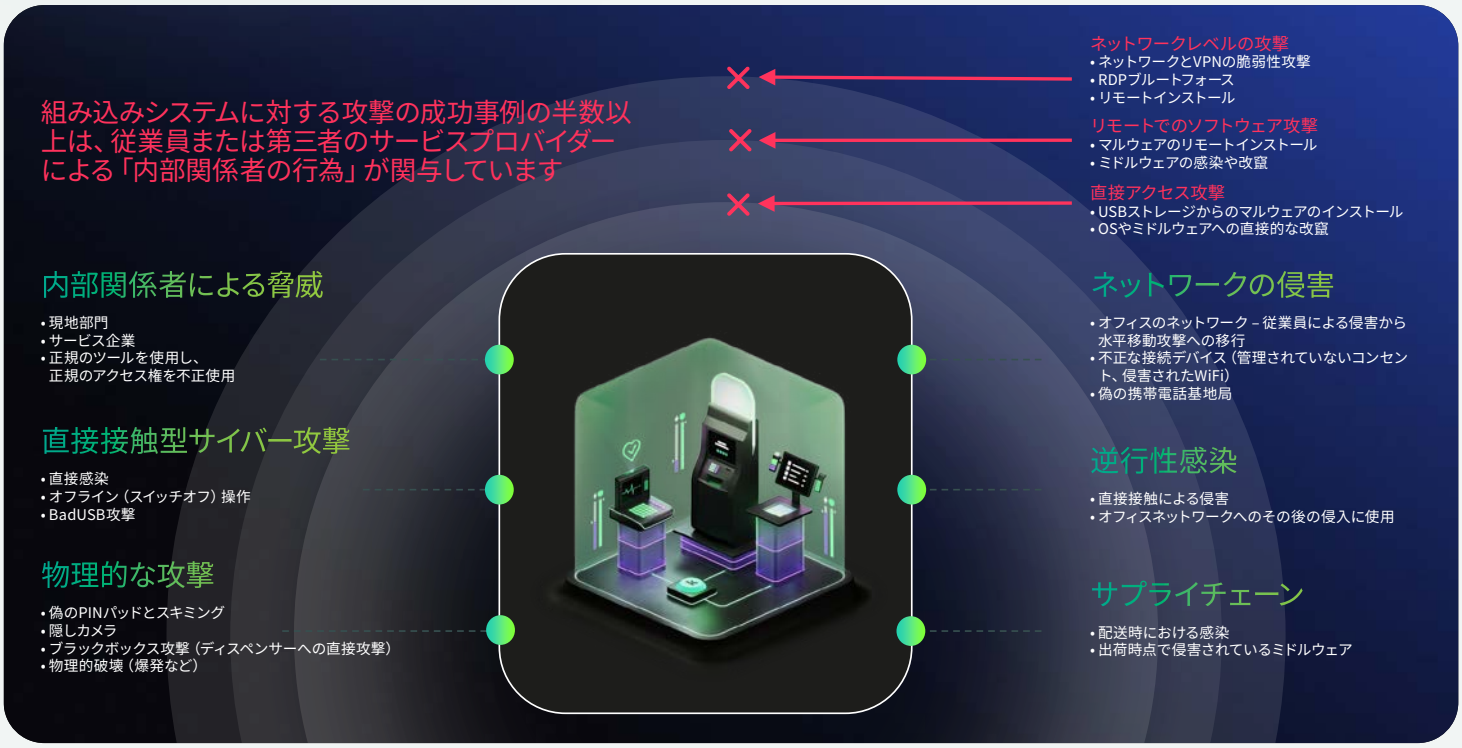
組み込みシステムは至る所にあり、私たちは日々それらのシステムを利用しています。PoSシステムやATMから医療機器やガソリンスタンドまで、あらゆるものが組み込みシステムを使用しています。組み込みシステム市場が拡大するにつれ、サイバー犯罪者もこれに追随し、広く普及しているこれらのシステムの特徴に合わせて、その戦術、テクニック、手順を高度化させています。

脅威の状況

Malware-as-a-Service（マルウェア・アズ・ア・サービス）のような新たな犯罪ビジネスモデルが次々と登場し、攻撃を計画する犯罪者にとって必要なスキルのハードルが、ますます低くなっています。旧バージョンのWindowsは既にサポート終了となって久しいものの、現在も稼働を続けています（Windows XPは組み込みデバイスにおいて最も広く使用されているOSです）。何百万もの組み込みデバイスやPCが、何らかの理由でアップグレードされていない古く脆弱なOSを、今もなお使用し続けています。この状況が、ハッカーによる攻撃を誘発しています。

一方で、Linuxベースの組み込みシステムは急速に人気を高めており、サイバー犯罪者の関心を引きつけています。サイバー犯罪は Linuxベースの組み込みシステムに特化したまったく新しい手段を用意し、犯罪技術を適合させています。Linuxが元々備えているセキュリティを過信することは危険です。攻撃者がLinuxベースの組み込みデバイスに関心を持つようになったのは比較的最近のことですが、彼らは遅れを取り戻そうとしています。Linuxベースの組み込みデバイスに対する現行のサイバーセキュリティ機能が、Windowsと比較して限られているということは何の助けにもなりません。

システムとデータを安全に保つために、企業は今まで以上に賢明である必要があります。強力な脅威インテリジェンス、オプトイン方式のマルウェア検知および脆弱性攻撃ブロック、総合的なシステムハードニングコントロール、柔軟な管理機能を搭載したKaspersky Embedded Systems Securityは、組み込みシステム向けに特化して設計されたオールインワンのセキュリティソリューションです。 ほとんどのサイバーセキュリティベンダーによるサポートが終了したレガシーシステムに対して、他社に真似できないレベルの保護を可能にしております。さらに最近では、Linux OSを実行するより近代的なデバイスに対しても、同等の保護レベルを適用できるようにになりました。



組み込みシステム：脅威モデル

組み込みセキュリティの課題

6 **厳格な規制。**金融情報および個人情報を処理する場合があるので、多くの組み込みデバイスは、極めて慎重なセキュリティへの取り組みを義務付ける規制の下で稼働しています。

7 **内部者の脅威。**Kasperskyのデータによると、組み込みシステムに対する攻撃の成功事例の50%以上は従業員または第三者のプロバイダーによる「内部関係者の行為」が関与しています。

8 **Linuxの普及。**組み込みプラットフォームは、優れた柔軟性を備えた上に幅広い構成を使用できることから、急速に普及しています。サイバー犯罪者もこの状況に関心を持っている一方で、専門的なセキュリティソリューションは、Windows向けに提供されているものに比べてかなり限定されています。

主な機能

あらゆる組み込みシステムに対する最適な保護

Kaspersky Embedded Systems Security は複数層の保護を提供し、異なる電力レベルや実装シナリオのデバイスに対しても最適なセキュリティを実現します。これには、WindowsやLinuxなどの各種オペレーティングシステムに基づくプラットフォームのサポートも含まれます。

レガシーシステムも新しいシステムも保護

Kaspersky Embedded Systems Security は、Windows XP、7、8、10、11を搭載したシステムで実行できるように最適化されています。Kaspesrkyは、お客様がシステムをアップグレードできるようになるまでの時間を確保できるよう、Windows XPのサポートを当面は継続する予定です。Kaspersky Embedded Systems Security はまた、Windows または Linux OS を実行している最新のアーキテクチャもサポートします。

低リソース、高レベルの保護

Kaspersky Embedded Systems Security は、ローエンドのハードウェアでも効果的に機能するように設計されています。

Kaspersky Embedded System Securityは統一されたエコシステムの一部であり、ソリューションファミリーの有機的な一部として動作します。他のカスペルスキー製品と同一のコンソールでの管理が可能であるほか、一元的な可視化やワークフローの統一などのメリットを享受できます。

主な特徴

システム強化（セキュリティコントロール）。アプリケーション、デバイス、アップデート管理から構成されるこれらのシステムハードニング技術により、信頼済みのアプリケーション、周辺機器、およびアップデート元のみを使用することが可能となります。これにより、不正なプログラム（マルウェアや悪意のある目的に使用される可能性があるアプリなど）が起動、実行されるのを防止します。

オプトインのマルウェア対策。オプトインセキュリティ層では、ローカルまたはクラウドベースの脅威インテリジェンスと、オンプレミスまたはクラウドで実行されるヒューリスティックや機械学習モデルを使用して、正確な検知ロジックで既知の脅威、未知の脅威、高度な脅威を検知します。専用のアンチクリプター技術により、デバイスをランサムウェアの脅威から保護します。

脆弱性攻撃ブロック。Windowsシステムコンポーネントやサードパーティアプリの実行による脆弱性攻撃を防ぎ、Default Denyモードのアプリケーションコントロールを回避するように設計された攻撃やファイルレス技術を使用する攻撃など、より高度な攻撃に対抗するのに役立ちます。

ネットワーク脅威対策。オペレーティングシステムへのいかなる侵入も防ぎ、ポートスキャンおよびブルートフォース攻撃や、ネットワーク関連の脆弱性を悪用して標的のデバイスを侵害するサイバー攻撃から保護します。これにより、組み込みシステムに対する主要な攻撃ベクトルの1つをブロックします。

整合性監視とコンプライアンスのサポート。ファイルの整合性とレジストリアクセスの監視機能[1]は、指定されたレジストリキー、ファイル、フォルダーに対して実行された動作を追跡し、望ましくない変更をブロックすることができます。マルウェアベースの侵入を検知するだけでなく、重要なリソースへの直接アクセスやオフラインでの変更の検知にも役立ちます。こうした対策は、特にデータ保護規則で推奨されるため、有効にすることでコンプライアンスの維持を促進します。

性能の低いレガシーシステムをサポート。旧式のハードウェアやサポート終了したオペレーティングシステム上で動作する低電力の組み込みシステムでさえも幅広くサポートいたします。Windows XP SP2まで対応しています。アップグレードの準備が整うまで、古いデバイスやレガシーデスクトップを安全に実行し続けることができます。

ログ検査[1]。Windowsイベントログの監視と検査に基づいて、保護違反の可能性を検知します。サイバー攻撃の可能性がある異常な動作を検知すると、管理者に通知します。

柔軟な管理 – オンプレミスでもクラウドでも。貴社の組み込みシステムのセキュリティは、ビジネスニーズに応じて、オンプレミス管理サーバーまたはKaspersky Security Center SaaS Cloud コンソールのいずれかから、他のカスペルスキー製品とともに管理できます。オンプレミス管理は厳格なプライバシー保護が必要な場合に有益であるのに対し、ベンダーが実行するクラウド SaaS コンソールは、CAPEX と OPEX の両方を節約する上で役立ち、安全な作業プロセスの迅速な開始を可能にし、メンテナンスの手間を軽減します。

[1] Windows OS のみ

ファイアウォール管理。オペレーティングシステムのファイアウォールを Kaspersky Security Centerから直接設定できるため、一元化された単一のコンソールを使用してローカルのファイアウォールを管理することができます。組み込みシステムがドメイン内に存在せず、Windows / Linuxファイアウォール設定を一元的に設定できない場合に不可欠です。WindowsOS向けに、アプリケーションレベルの専用ファイアウォールが使用可能です。これにより、アプリケーションのネットワーク接続のより綿密な管理が可能であり、攻撃対象領域の縮小を促進します。

低品質な接続への耐性。多くの種類の組み込みデバイスは遠隔地に設置されることが多いため、携帯電話の電波状況の不安定さや、近隣の電波源からの干渉などによる接続品質の低下は、決して珍しいことではありません。Kaspersky Embedded System Securityは、かなり低い帯域幅でも安定性を維持し、接続がない状態が長期間にわたって発生しても信頼できる保護を提供し続けます。

Managed Detection & Response integration：このソリューションはKasperskyのセキュリティオペレーションセンターと連動し、24時間365日の監視と迅速なレスポンスを実現します。これにより、組み込みデバイスに対する高度な攻撃を早期に検知して封じ込めることが可能となり、事業における深刻な金銭的損失を防ぐことができます。

Professional Servicesとプレミアムサポート

セキュリティソリューションのライフサイクルの適切な維持には労力を要します。また、組み込みデバイスは通常のエンドポイントとは異なる特性を持つため、そのセキュリティのメンテナンスは特に手間がかかる場合があります。Kaspersky Professional Servicesは、導入やアップデート、設定やパフォーマンス最適化から、新しいハードウェアへの移行に至るまで、ライフサイクルのあらゆる段階においてお客様をサポートします。また、当社のプレミアムサポートは、比類のない専門知識を備えた専任の技術アカウントマネージャーによる、優先的なインシデント解決を保証します。

関連製品とサービス

Kaspersky Threat Intelligence：
組織を標的としたサイバー脅威の総合的な見解を提供する、多角的なサービス群です。インテリジェンス情報源、脅威データフィード、および社内調査を組み合わせ、当社のセキュリティエキスパートが分析を行います。

Payment Systems Security Assessment：ATMおよびPOSデバイスを総合的に分析することで、現在のセキュリティレベルを明確に把握できます。これにより、セキュリティのさらなる強化、設定の最適化、そしてセキュリティ上の欠陥の解消が可能となります。

Kaspersky Next 製品ラインナップ：
卓越したエンドポイント保護と強力なセキュリティ管理機能に加え、EDRの透明性とスピード、XDRの可視性と強力なツールを組み合わせた、柔軟な階層型製品ラインナップです。

業界

- 金融サービス
- 交通と観光（チケット販売）
- 流通・小売
- 接待費
- 医療機関
- 政府、非営利団体
- エンターテインメント

デバイス

- ATM
- 券売機
- 燃料販売機
- チェックアウト
- POS
- 医療機器
- レガシーエンドポイント
- スロットやアーケードマシン

組み込みデバイスを使用している業界

www.kaspersky.co.jp

サイバーセキュリティ業界での25年以上の実績。独立系機関からの数々の受賞歴。グローバルな透明性。当社は技術による生活向上を通じて、より安全な世界の実現に取り組んでいます。こうした世界にはセキュリティが不可欠であるという信念のもとに、また、技術がもたらす恩恵が全世界の誰もに行き渡ることを願いつつ、当社は活動しています。より安全な**未来**に向けて、サイバーセキュリティを強化しましょう。

詳細はこちら：kaspersky.com/about/transparency

Proven.
Transparent.
Independent.