Kaspersky Embedded Systems セキュリティ

kaspersky

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から医療機器や自動給油所まで、あらゆるものが依存しています。組み込みシステム市場の成長に伴い、サイバー犯罪者は広く普及しているこのようなシステムの特性に適したテクニックや手順に従ってその戦術に磨きをかけています。

組み込みデバイスのセキュリティ課題

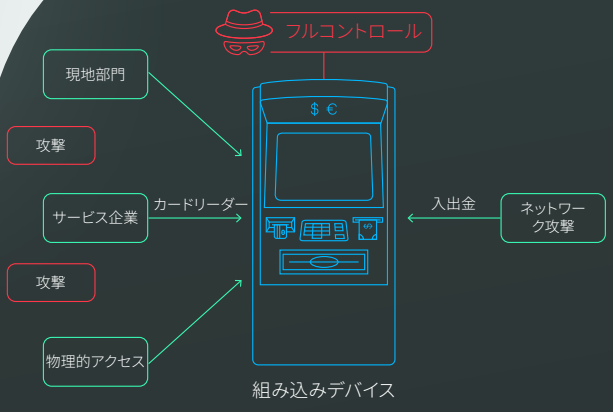
1. **旧式の脆弱なソフトウェア。**ライフサイクルが長いと、サポート対象外のオペレーティングシステムやアプリが実行され、その結果パッチが適用されず悪用される恐れのある脆弱性が含まれる可能性があります。
2. **不規則なセキュリティ更新。**ソフトウェアがサポートされている場合でも、パッチがすぐに適用されない恐れがあります。地理的に分散した複数のデバイスをアップデートする際の問題として、デバイスをオフラインにする必要があり（そのため一時的なサービスの停止が余儀なくされ）、また適用する前にアップデートをテストする必要があるため、パッチ適用が遅れる原因となります。
3. **プロセスの継続性。**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、改ざん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。

脅威の状況

Malware-as-a-Service のような新しい犯罪ビジネスモデルが現れることで、攻撃志望者に求められるスキルレベルが低下します。旧バージョンの Windows はサポートが終了して長いこと経ちますが、引き続きサービスを提供しています（Windows XP は組み込みデバイスで最も多く使用されている OS です）。数百万もの組み込みデバイスや PC は、古くて脆弱性のある OS を実行しており、その理由が何であれアップグレードされないままです。これではハッカーに、攻撃してくださいと言っているようなものです。

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全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。攻撃者は比較的最近 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にもかかわらず、その技術に追いついてきています。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、オプトインのマルウェア検出およびぜい弱性攻撃からの保護機能、包括的なシステムの強化コントロールおよび柔軟な管理を特徴として、Kaspersky Embedded Systems Security は組み込みシステムに特化して設計されたオールインワンのセキュリティです。大部分のサイバーセキュリティベンダーによってサポート対象外となっているレガシーシステムに対しても、他にはないレベルでの保護を提供するだけでなく、Linux OS を実行するより現代的なデバイスに対しても同等の保護を提供するようになりました。



組み込みシステムに対して成功したすべての攻撃の 50% 以上が、従業員またはサードパーティのサービスプロバイダーの「内部者による行為」が関係しています

物理レベルの攻撃

- ブラックボックス攻撃
- PIN パッドの改ざん／クレジットカードデータ読み取り装置
- 隠しカメラ
- 爆発

ソフトウェアレベルの攻撃

- マルウェアのリモート／ローカルインストール
- メモリースニファ／OS 攻撃
- ミドルウェア感染／改ざん

ネットワークレベルの攻撃

- VPN 脆弱性
- RDP のブルートフォース攻撃
- RCE 脆弱性を悪用したネットワーク攻撃
- リモートインストール

組み込みシステム：典型的な攻撃ベクトル

組み込みデバイスのセキュリティ課題

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動作します。

7 **内部者の脅威。**カスペルスキーのデータによると、組み込みシステムに対して成功したすべての攻撃の 50% 以上が、従業員またはサードパーティサービスプロバイダーの「内部者による行為」が関係しています。

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。サイバー犯罪者の関心を引いているものの、Windows プラットフォームと比べて最新鋭の専門的なセキュリティソリューションが非常に限られている状態です。

主な強化ポイント

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、異なるパワー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 といった、異なるオペレーティングシステムに基づくプラットフォームへ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、および 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。カスペルスキーでは、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、しばらくの間は Windows XP へのサポートを継続する予定です。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作られています。

ATM & PoS 攻撃の増加
カスペルスキーの調査データによると、ATM および PoS システムへの攻撃数は 2022 年に大幅に増加しており、2020 年と比べて 19% 増、2021 年と比べて 4% 増となっています。

主な特徴

システム強化（セキュリティコントロール）。こうしたシステム強化テクノロジーは、アプリケーションコントロール、デバイスコントロール、更新コントロールで構成されており、信頼するアプリケーション、周辺機器、更新ソースのみを使用できます。これにより、悪質な目的で使用される可能性のあるマルウェアやアプリなど、不正なプログラムが起動して実行されるのを防ぐことができます。

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。

脆弱性攻撃からの保護[1]。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、デフォルト拒否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。

ネットワーク脅威からの保護。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。そうすることにより、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アクションを追跡し、不要な変更をブロックできます。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／オフラインでの変更も検知するのに役立ちます。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。Windows XP SP2 に至る、旧型のハードウェアやサポートされていないオペレーティングシステムで実行されている低性能の組み込みシステムもサポートします。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クラウド SaaS Kaspersky Security Center 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は Kaspersky Security Center から直接構成できるため、単一の統合コンソールを使用してローカルファイアウォール管理を行うことができます。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構成できない場合に不可欠です。

低接続性への耐性。多くの種類の組み込みデバイスはリモートで設置され、接続が弱いことがよくあります。モバイルデータ通信ネットワークが弱いことで、近くの電波からの干渉を受けることがよくあります。しかし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。

プロフェッショナルなサービス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を適切に保守するには努力を要します。また通常のエンドポイントとは異なる組み込みデバイスの特性により、組み込みシステムのセキュリティを維持することは特に労力を要します。Kaspersky Professional Services は、展開およびアップデート、構成やパフォーマンスの最適化から、新しいハードウェアへの移行まで、ライフスタイルの各ステージにおいてサポートを提供します。また、カスペルスキーのプレミアムサポートでは、比類のない専門知識を備えた専任のテクニカルアカウントマネージャーが割り当てられ、専門家が優先的にインシデントを解決することを保証します。

関連製品とサービス

Kaspersky Threat Intelligence：脅威データフィードや、カスペルスキーによる調査、カスペルスキーのセキュリティ専門家による分析情報を含め、お客様の組織を標的としたサイバー脅威の包括的な情報をお届けするサービスです。

Payment Systems Security Assessment：ATM や POS デバイスに関する包括的な分析データを基に、現在のセキュリティレベルについて明確に把握し、セキュリティの強化、構成の最適化、そして隙のないセキュリティ防御を可能にします。

Kaspersky Endpoint Security for Business：エンドポイント、サーバー、ワークステーション、およびモバイルデバイスを最も多くテストされ多くの受賞歴を誇るセキュリティで保護する、世界的に高い評価を得ているエンドポイント保護プラットフォームです。すべてを 1 つのコンソールで管理できます。

産業

- 金融サービス
- 運送および旅行（チケット発行）
- 流通・小売
- レストランおよびサービス業
- 医療機関
- 政府および非営利
- エンターテイメント

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

サイバー脅威ニュース：securelist.com
Kaspersky のテクノロジー：kaspersky.com/technowiki
IT セキュリティニュース：blog.kaspersky.co.jp/category/business/
中小企業向けの IT セキュリティ：kaspersky.com/business
大規模企業向けの IT セキュリティ：kaspersky.com/enterprise

www.kaspersky.com

実証済みの品質、独立性、透明性をお約束します。カスペルスキーは、安全な世界を作り上げ、テクノロジーを活かして人々の暮らしを良くすることを目指しています。そのために、世界中の誰もがテクノロジーの無限の恩恵を受けることができるよう、セキュリティサービスを提供しています。より安全な**未来**のために、サイバーセキュリティをお届けいたします。

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

Proven. Transparent. Independent.