



組み込みシステムと、必要とされるサイバーセキュリティ

組み込みシステム

生活のいたるところで使用されている 組み込みシステム

魅力的な標的

組み込みシステムは、お金や個人情報などの貴重なデータを扱っています。そのため、サイバー犯罪者にとって非常に魅力的な標的となっています。








組み込みシステムは、毎日使用されています。ATM、店舗内POSシステム、自動販売機、自動券売機、医療用CTスキャナ、さらには自動ガソリンスタンドなど、これらはすべて、組み込み型のWindowsまたはLinuxのシステム専用のデバイスで運用されています。

これらのデバイスは、お金や個人情報などの貴重なデータを扱っています。そのため、サイバー犯罪者にとって非常に魅力的な標的となっています。そのため、これらのデバイスを使用する企業にとっては、信頼性の高い保護が不可欠となります。









しかし、企業は組み込みシステムのセキュリティを一般的なオフィスシステムと同等に考えているとは限りません。そのセキュリティは、往々にして後回しにされがちです。しかし、組み込みシステムの保護は非常に重要であり、組み込みシステム独自の仕様を無視することはできません。

組み込みシステム：業界とデバイスの種類

業界

-  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
-  キャッシュレジスター
-  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

組み込みシステムの特徴

組み込みシステムは、従来のワークステーションとほとんど変わらないように見えるかもしれませんが、そうではありません。組み込みシステムには、保護戦略を策定する際に考慮すべき重要な違いがいくつかあります。



利用モデル

典型的な組み込みシステムは、通常のデスクトップコンピューターとは根本的に異なります。デスクトップでは、1人のユーザーが幅広いタスクを使用します。一方、組み込みシステムは通常、ほぼ無制限の数のユーザーが使用し、また実行するタスクの範囲も非常に限定されています。

違いは他にもあります。たとえば、組み込みシステムとの対話は、特定の入力デバイス（テンキーや、高度に専門化されたユーザーインターフェイスを持つタッチスクリーン）を使用して行われることが多く、任意のデータやコマンドを入力することはできません。

外部周辺デバイスを接続できる交換ポートを使用可能なのは、通常は技術者のみです。「外部の世界」とのコミュニケーションは、インターネット経由、ローカルネットワーク経由、または銀行カードのように機能が限定された情報記憶デバイスを使用して行われます。

ATMは、メールを読んだりWebサイトを閲覧したりするのに使用されないことは明白です。したがって、これらのチャンネルを攻撃経路とすることはできません。その一方で、ネットワーク接続の重要性は増すことになります。これは、組み込みシステムへの攻撃に使用される主要なチャンネルの1つです。なぜなら、ほとんどすべての種類の組み込みシステムは、社内のローカルネットワークに接続されているからです。つまり、システムへの侵入後に、攻撃者はネットワーク経由でこれらの専用デバイスを危険にさらすことができるのです。ポートに関しては、悪意のあるアクターは、組み込みシステムの特定の物理的な場所を利用することさえあります。



物理的な場所

組み込みシステムをベースとしたほとんどのコンピューター機器は、利用モデルに従い、公共スペースに設置されています。耐久性のあるスチール製ケースと、デバイスとの対話手段の制限は、システムのハードウェアおよびソフトウェア要素への予期せぬアクセスからの保護を目的としています。しかし、メンテナンスがまったく不要なデバイスは存在しないため、どんなに丈夫なケースでも鍵で開けることができます。つまり、侵入者でも開けることができるのです。コンピューターアプライアンスのハードウェアへのアクセス後、侵入者は標準的なマウスとキーボードを取り付けたり、マルウェアを仕込んだペンドライブを差し込んだりすることができます。または、外部から起動可能なOSを接続して、コンピューターアプライアンスのOSをバイパスして電源をオンにすることも可能です。

場合によっては、シングルボードコンピューターが使用されることもあります。これを使用してシステムをハッキングしたり、またはコマンド（たとえば、ディスプレイが紙幣を出金するコマンド）を解析したりすることも可能です。そこまでたどり着けば後は簡単です。攻撃者が行うべきことは、自分たちが選択したツールをシステムに組み込み、それを使用して組み込みコンピューターを好きなように動かすことだけです。貨幣の払い出し、別名義での取引、ユーザーデータの窃取など、あらゆる悪事が可能になります。組み込みシステムを適切に保護していれば、このような心配をする必要はありません。

セキュリティの課題：

OS、専用ソフトウェア、セキュリティ製品そのものなど、導入済みで稼働中のソフトウェアが直接改竄される高いリスクが存在します。





長期の耐用年数 と制限された システムリソース

特定のタスクを念頭に置いて構築された組み込みシステムは、多くの場合、「必要かつ十分な」レベルのプロセッサ性能しか実装されていません。また、組み込みシステムを使用するコンピューター機器は耐用年数が高い傾向にあります。そのため、性能が低い旧式のハードウェアを実装して運用されているATMを見かけることも珍しくありません。

セキュリティの課題：

旧式で脆弱なハードウェアは重大な問題であり、最新のセキュリティソリューションの多くに対応するには性能が不十分です。

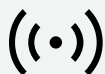


アップデートされておらず 脆弱なソフトウェア

組み込みシステムをベースにした高価なコンピューターアプライアンスの耐用年数が高いことによるもう1つの副作用は、ソフトウェアも陳腐化することです。システム構成が手薄なため、往々にして新しいOSを使用することができません、また、専用に開発されたアプリケーションの新しいバージョンが、旧式のOSでは動作しないことがよくあります（または逆に、ミドルウェアの新しいバージョンが使用できない一方で、旧バージョンが新しいOSで動作しない場合もあります）。その結果、セキュリティ更新プログラムがリリースされなくなったシステムが現役で使用されることになります。つまり、専用の保護対策を講じない限り、あらゆる脆弱性が悪意のある第三者によって悪用される可能性があるということです。

セキュリティの課題：

ソフトウェアの脆弱性による攻撃リスクの増大と、セキュリティソリューションの選択肢が極めて限定的であることが相まって、Windows XPのような旧式のOSと互換性のある最新のセキュリティ製品を見つけることは非常に困難です。大半のメーカーがサポートを終了しています。



脆弱なインターネット接続

ATM、チケット端末、自動給油ステーションなどの一部のデバイスは、有線インターネットがないか、無線インターネットの速度が遅いか信頼性が低い遠隔地に設置されています。本製品は、このようなシナリオを考慮しています。たとえば、「接続の状況が許す場合」に、トランザクションを非同期で処理することができます。一方、最新のセキュリティ製品の多くは、良好なインターネット接続に大きく依存しています。インストール時間を短縮し、インストールするソフトウェアのサイズを縮小するために、開発者はローカルコンポーネントの量を減らし、代わりにクラウドインフラに大きく依存しています。

セキュリティの課題：

安定した信頼性の高い高速インターネット接続がなければ、犯罪者が取引を侵害する機会がさらに増えます。同時に、ベンダーのクラウドインフラとの通信に過度に依存する多くの最新ソリューションの有効性も、著しく低下する可能性があります。



規制要件

ほとんどの組み込みシステムは、貴重な金融データや個人データを扱うため、それらを扱う作業は法律で規制されています。規制当局は、インシデントのリスクを最小限に抑え、インシデントが発生した場合に詳細なデータを確実に調査できるようにするため、信頼性の高い保護を必要としています。システムの整合性監視など、特定の技術が推奨リストに含まれる場合があります。

セキュリティの課題：

データ保護の要件が増えるにつれ、高性能かつ効果が高い対策が要求される一方で、標準的なEPPクラスのソリューションの一部としてはすぐに使用できない（または、サーバー保護に特化したソリューションの一部としてのみ使用可能な）技術も同時に推奨されます。

折衷案の模索

まとめると、マルチユーザー、シングルタスク、低消費電力の組み込みシステムには、特定の攻撃経路（ネットワーク、デバイスへの直接アクセス）があるという結論になります。同時に、これらのシステムは、非常に貴重なデータ（財務データに加えて、たとえば医療機器の場合のように、機密性の高い個人データである可能性もあります）を運用しています。こうしたデータの取り扱いには機密性だけでなく、不変性も重要になります。このようなシステムに汎用的な保護ソリューションを導入すると、多くの問題が発生する可能性があります。一般的なEPPクラスのソリューションは、脆弱なハードウェアでは十分に機能せず、旧式のOSとは互換性がないためです。起動して問題がないように見えても、パフォーマンスや互換性に問題がある可能性があります。

セキュリティソリューションのメーカーの多くは、デバイスの主要なタスクの実行に不要なものを完全に禁止することを選択しています。



Default Denyモードのアプリケーションコントロール技術は、いわゆる「許可リスト」に初期状態でリストアップされていないプログラムを完全にブロックします。



理論上は、これにより脅威検知メカニズムが不要になります。というのも、マルウェアが起動することが単純になくなり、このアプローチはリソースをほとんど必要としなくなるからです。



しかし、この戦略は一部の攻撃に対しては有効でない場合があります。たとえば、メモリ上で既に実行されている正規のプロセスに悪意のあるコードを注入することができる「ファイルレス」「メモリオンリー」タイプのマルウェアなどです（古いソフトウェアの脆弱性により、これらの攻撃が可能となる場合があります）。

一般的に、脆弱なシステムほどサイバー犯罪者が攻撃する機会は少なくなりますが、銀行や小売業など、組み込みシステムを使用する企業では、1世代の技術しか使用しないということはまずないでしょう。

では、そのような機密資産はどのように保護すればよいのでしょうか。

別のソリューションを使用しますか？

脆弱なシステムにはDefault Denyソリューションを使用し、より強力なシステムには、互換性の問題が発生しないことを祈りつつ、通常のEPPアプリを実装するのでしょうか？

それとも、真に普遍的なソリューションを探しますか？



専用デバイス向けの専用の保護

現在市販されている組み込みシステムの保護オプションを見てみると、大部分のベンダーが提示するオプションは次の2つです：

オプション1.「経済的」で資源効率の高いソリューション

旧式のシステムと互換性があり、アプリケーションコントロール技術とDefault Denyモードに基づく、最も単純な単層型のソリューションです。組み込みシステムに典型的な数多くの攻撃に対抗するツールがないことに加え、この種類の専用ソリューションはスタンドアロンであることがほとんどで、ベンダーのエコシステム内の他の製品とは別に管理されます。

オプション2.従来のエンドポイントセキュリティ

組み込みシステムの場合、ほとんどのメーカーは、従来のワークステーションを保護するのと同じソリューションの使用を選択肢として提示しています。このようなソリューションには、間違いなく最新のセキュリティ技術が集積されている上、ベンダーのエコシステムと統合することもできます。しかし、通常、上記のような組み込みシステムの特長性が考慮されていません。さらに、このようなソリューションは、最新の強力なコンピュータアプライアンスでのみ効果的に機能し、まだ機能しているが時代遅れのデバイスは対象外として切り捨てられます。

両方のオプションを同時に使用しても、問題は解決しません。さらに、(特に異なるメーカーが関与する) 混成的な管理アプローチは、ITチームとサイバーセキュリティチームの作業を著しく複雑にする可能性があります。



理想的なセキュリティソリューション

では、幅広い組み込みシステムとシナリオに適した理想的なセキュリティソリューションの要件とは何でしょうか？

可能な限り最高レベルの保護を提供するソリューションであること

現代の状況では、サイバー犯罪者が使用する攻撃経路やテクニックが影響する範囲（つまり、あらゆる種類の組み込みシステムに典型的な攻撃）から、各種の技術を組み合わせ駆使してシステムを保護することを意味します。

あらゆるレベルのシステムに対して、可能な限りの最大限の保護を提供するソリューションであること

旧式の低出力なシステムから、十分な性能とシステムリソースを有する最新のシステムまでをカバーする必要があります。

しかし、技術スタック内で使用可能なすべてのものを脆弱なハードウェアで同時に実行することは事実上不可能であるため、拡張性が不可欠となります。

言い換えれば、このソリューションでは、保護の階層を個別に管理し、特定のハードウェアとシステム使用シナリオに対して最大限の保護を実現する設定をオンまたはオフにできる必要があります。

最もよく使用されているOSをサポートするソリューションであること

組み込みシステムの作成で最もよく使用されるOS。最低でも、WindowsとLinuxです。

レガシーOSのバージョンをサポートしているソリューションであること

組み込みシステムで使用し、現在も運用されているレガシーOSバージョン。

規制要件を満たすソリューションであること

ソリューションは、推奨する技術をそのセキュリティスタックに実装しており、集中型のセキュリティイベント監視システム (SIEM) にイベントの詳細をログとして記録できる必要があります。

徹底的に互換性がテストされたソリューションであること

少なくとも、各種の組み込みシステムの典型的な構成でテストされている必要があります。理想的には、コンピューターアプライアンスの一部として供給され、このコンピューターアプライアンスの製造業者（または組立業者）によってすべてのコンポーネントがテストされ、問題のない動作が保証されている必要があります。

一元管理が可能なソリューションであること

ベンダーのエコシステム内の他の製品と連携し、単一コンソールで企業のITインフラストラクチャの全レベルを監視、保護する一体型セキュリティシステムを構築するのが理想的です。



Kaspersky Embedded System Security

Kaspersky Embedded Systems Security

以前、組み込みシステムを保護するためにKaspersky Security for Business 製品ラインのアプリケーションを使用した経験に基づき、組み込みシステム独自の保護に特化したソリューションが不可欠であることを当社は認識しています。

そこで当社は、WindowsとLinuxをサポートするKaspersky Embedded Systems Securityを開発しました。

ソリューションが実現するもの：



比類ないセキュリティ構成

保護階層を有効にするための最適化方式を特徴とする、各種プラットフォーム向けの多層的な技術スタックの市場において、他に類例を見ないセキュリティ構成を実現します



最小限のシステム要件

システム要件は最小です



旧バージョンのOSをサポート

(Windows XP SP2まで)



多彩な機能を持つ Kasperskyのセキュ リティエコシステム

その一部として機能します



他の製品と同じ管理コ ンソールで管理可能

他のカスペルスキーセキュリティ製品と同じ管理コンソールで管理可能です



組み込みシステムの保護 は、企業全体のセキュ リティ戦略に不可欠な要 素です

また、既存の情報セキュリティプロセスにシームレスに統合することができます。

本製品の主なメリットや機能の詳細は、製品のWebページを参照してください。

技術仕様については、サポートサイトのWindows向け製品のセクションを参照してください。

技術仕様については、サポートサイトのLinux向け製品のセクションを参照してください。

[詳細はこちら](#)

[詳細はこちら](#)

[詳細はこちら](#)



Kaspersky Embedded System Security

[詳細はこちら](#)

www.kaspersky.co.jp

© 2023 AO Kaspersky Lab.登録商標とサービスマークに関する権利は各所有者に帰属します。

#kaspersky
#bringonthefuture