kaspersky BRING ON THE FUTURE

Kaspersky Embedded Systems Security

組み込みシステム向けに設計された一体型セキュリティ製品

着実に成長している組み込みシステム市場に、サイバー犯罪者も関心を寄せており、2019 年は ATM および POS システムに対する感染の試みが前年比で 28 % 増加しています。

組み込みシステムは身近な存在として、日常生活のあらゆる面に影響を与えています。POS システム、ATM、医療機器、通信機器など、さまざまなものに組み込みシステムが使用されていることから、攻撃経路がかつてないほど増加しています。

Windows 7 のサポート期限が最近終了したことを受けて、企業には、組み込みシステムの OS を速やかに更新すると同時に、必要に応じて追加の保護対策を講じることが求められます。注目すべきことに、Windows XP はサポート終了から何年も経っているにもかかわらず、組み込みシステムでは今もなお一般的なオペレーティングシステムとして広く使用されています。これでは、ハッカーの攻撃を自ら招いているようなものです。

サイバー犯罪者の間では相当な金銭的損害が見込める攻撃対象として、このような組み込みシステムに対する注目が集まってきています。このような状況を踏まえると、企業は自社のシステムとデータを安全に守るために、これまで以上にスマートなセキュリティ対策をとる必要があります。強力な脅威インテリジェンス、リアルタイムのマルウェア検知、アプリケーションおよびデバイスの包括的なコントロールと柔軟な管理を備えた Kaspersky Embedded Systems Security は、組み込みシステム専用に設計された一体型セキュリティです。

特長

効率的な設計によりローエンドのハードウェアにも対応

Kaspersky Embedded Systems Security は、ローエンドのハードウェア（RAM：256 MB、CPU：Pentium III）や古いソフトウェア（Windows XP 用）でも、システムに負荷をかけず、効果的に機能するように特別につくられています。モバイルモデムが唯一の通信オプションで、電波状態が悪く 2G のみで動作するような、十分な通信速度を確保できない通信チャネル（56 kbps と低速）でも問題ありません。

強力なメモリ保護

強力な脆弱性攻撃ブロック技術を駆使した重要プロセスの監視により、アプリケーションやシステムコンポーネントに含まれるパッチ未適用の脆弱性やゼロデイ脆弱性を悪用した攻撃を防止します。これは、広範囲におよぶランサムウェア攻撃（WannaCry や ExPetr など）から保護する上で特に重要です。

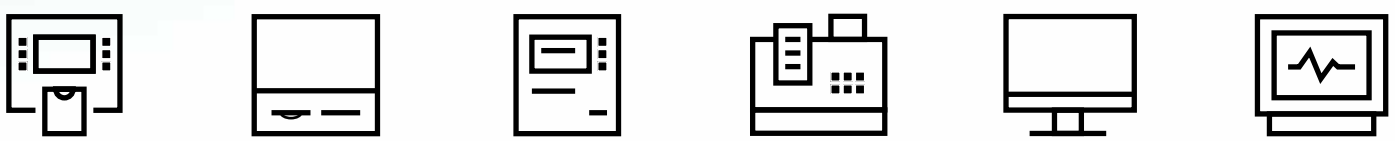
Windows XP 向けに最適化

現在もなお、多くの組み込みシステムは、サポートが終了した Windows® XP OS 上で動作しています。Kaspersky Embedded Systems Security は、Windows 7、Windows 8、Windows 10 と同様に、Windows XP プラットフォームでも動作するように最適化されています。

Kaspersky Embedded Systems Security では、当面の間 Windows XP がサポートされるため、企業は段階的にアップグレードを進める時間を確保できます。

コンプライアンス

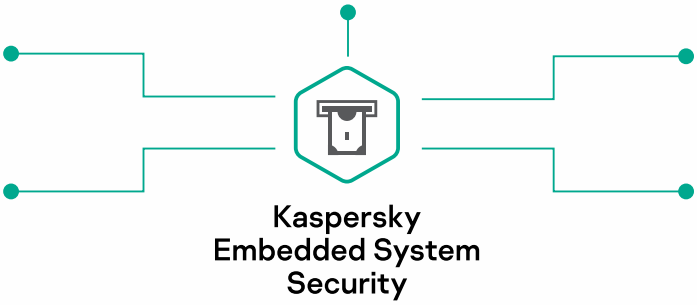
Kaspersky Embedded Systems Security は、アンチマルウェア、アプリケーションおよびデバイスコントロール、ファイアウォール管理、ファイル変更監視、Windowsイベントログ監視という、独自の包括的な保護コンポーネントセットで構成されており、システムに対する悪意のある動作を識別およびブロックし、セキュリティ侵害のさまざまな痕跡を検知します。このため企業は、PCI DSS、SWIFT などの規制で求められるコンプライアンス要件を満たすことができます。



システム要件の最適化
- RAM：256 MB 以上
- OS：Windows XP 以降
- ネットワーク帯域幅：56 kbps～

アンチマルウェア保護
- 機能のインストール有無を選択可
- リアルタイム／オンデマンド
- ランサムウェアやその他の脅威に対する脆弱性攻撃ブロック

ネットワーク保護
- ファイアウォール管理
- ネットワーク上の脅威からの保護



システムの変更監視
- ファイル変更監視
- Windowsイベントログ監視

システムの堅牢化
- アプリケーション起動コントロール
- ソフトウェア配信コントロール
- デバイスコントロール

機能

強力なアンチマルウェア

プロアクティブなクラウド支援型の脅威検知と分析が従来型のテクノロジーと連携することで、既知、未知、そして高度な脅威に対する防御を提供します。ローエンドのハードウェアや低速の通信チャネルの場合は、オプションのアンチマルウェアコンポーネントを無効にすることもできます（ただし、有効にすることが強く推奨される）。

Kaspersky Security Network によるリアルタイムのマルウェア検知

Kaspersky Security Network（KSN）は、Kaspersky が運営する、クラウド支援型のグローバルな脅威インテリジェンスネットワークです。世界中に分散配置された数百万のノードにより、現実世界の脅威インテリジェンスが Kaspersky のシステムに常時フィードされるため、新たに出現して進化を続ける最新の脅威（大規模攻撃を含む）に対しても迅速に対応することが可能になります。

マルウェア攻撃の試みや不審なふるまいに関する最新情報が常に集まってくることで、ファイルを即座に判断し、最新の脅威に対するリアルタイム保護を提供することができます。

アプリケーションコントロール

アプリケーション起動コントロールを使用したホワイトリスト方式の採用により、データ侵害に対するシステムの耐性が最適化されます。
指定されたプログラム、サービス、信頼できるシステムコンポーネントを除くすべてのアプリケーションの実行を禁止することで、ほぼすべての形態のマルウェアを完全かつ自動的にブロックできます。
ソフトウェア配信のコントロールには「信頼できるインストーラー」のアプローチをとることで、ソフトウェアのアップデートやインストール時にファイルのホワイトリストを手動で作成したり、変更したりするという、時間のかかる作業の手間を省きます。インストーラーを「信頼できる」と指定し、通常の方法でアップデートを実行するだけで済みます。

デバイスの監視とコントロール

Kaspersky のデバイスコントロールを使用すると、システムのハードウェアに接続されている、または物理的に接続されようとしている USB ストレージデバイスを管理できます。不正なデバイスによるアクセスを防止することで、マルウェア攻撃の最初のステップでサイバー犯罪者によって利用される、一般的な侵入口をブロックできます。

すべての USB デバイスの接続状態が監視およびログ記録されるため、不適切な USB が使用されている場合は、インシデント調査と対応プロセス時に攻撃ソースの可能性があると特定できます。

Windows ファイアウォールの管理

Kaspersky Security Center から Windows ファイアウォールを直接構成できます。単一の統合コンソールでローカルファイアウォールを管理でき、利便性が高いです。これは、組み込みシステムがドメインに属しておらず、Windows ファイアウォールの設定を一元的に構成できない場合に重要です。

ネットワーク上の脅威からの保護

ネットワーク上の脅威からの保護は、ポートスキャン、サービス妨害攻撃、バッファオーバーランなどのネットワーク上の脅威を防止するのに役立ちます。ネットワークでの動作を常時監視し、不審なふるまいが検出された場合には、事前に定義された対応を実行します。

ファイル変更監視*

範囲内の指定されたファイルやフォルダーに対して実行されるアクションを追跡します。監視が中断された期間中の変更を追跡するように構成することもできます。

Windowsイベントログ監視*

Kaspersky Embedded Systems Security は Windows イベントログの調査に基づいて、保護違反の可能性がないかを監視します。サイバー攻撃の試みを示すと思われる異常なふるまいが検出された場合は、アプリケーションによって管理者に通知されます。

SIEM 連携

Kaspersky Embedded Systems Security では、アプリケーションログに含まれるイベントを syslog サーバーでサポートされている形式に変換できるため、これらのイベントを SIEM システムに転送して認識されるようにすることができます。イベントは、Kaspersky Embedded System Security から SIEM に直接エクスポートすることも、Kaspersky Security Center 経由で一元的にエクスポートすることもできます。

柔軟な管理

一元管理を実現する単一コンソールの Kaspersky Security Center から、セキュリティポリシー、シグネチャアップデート、アンチマルウェアのスキャンと結果の収集を容易に管理できます。また、ローカル GUI コンソールやコマンドラインを使用して、ローカルネットワーク内のクライアントを管理できます。これは、組み込みシステムで典型的な、分離つまりセグメント化されたネットワークで作業する場合に特に便利です。

* Kaspersky Embedded Systems Security Compliance Edition ライセンスが必要です。

製品情報：www.kaspersky.co.jp/enterprise-security/embedded-systems
サイバー脅威に関する最新情報：securelist.com
IT セキュリティに関する最新情報：blog.kaspersky.co.jp
ご購入相談窓口：jp-sales@kaspersky.com

www.kaspersky.co.jp

Kaspersky は、実証された独立した企業で、透明性が確保されています。Kaspersky は、テクノロジーによって私たちのより良い生活、より安全な世界の構築に取り組んでいます。そのため Kaspersky は、テクノロジーがもたらす無限の機会をすべての人がすべての場所で享受できるよう、そのテクノロジーを守ります。より安全な未来に向けて、サイバーセキュリティを実現します。

詳しくはこちら：kaspersky.co.jp/transparency

Proven.
Transparent.
Independent.