



WindowsのレガシーOSで稼働するシステムに最適なKasperskyのソリューション

更新が困難な
Windowsの旧OSで
稼働するシステムに
特化した保護製品

Kasperskyは、旧バージョンのWindowsをこれからも保護し続けます

Microsoftは数年前に、Windows XPオペレーティングシステムのサポートを終了しました。これに伴い、このOSを現在も使用するユーザーは、メーカーからアップデートやセキュリティパッチの提供を受けられなくなりました。加えて、Windows XPのシステムコード全体が流出しました。その結果、このOSのデバイスは、誰でも新しい方法でハッキングできるようになっています。広く普及しているオペレーティングシステムが非常に脆弱な状態になっているのには、こうした背景があります。この問題はさらに悪化しています。というのも、大部分の大規模企業向けセキュリティソリューションは、もはやWindows XPやWindows 7をサポートしていないためです。

2025年10月14日以降は、MicrosoftによるWindows 10のサポートも終了しています。

Microsoftは2014年4月8日、12年間続けたWindows XPのサポートを終了しました。

Windows 7のサポートは、有料の延長セキュリティアップデートも含めて、2023年1月に終了しました。Windows 10のサポートは、2025年10月に終了しています。これらのレガシーオペレーティングシステムに対するセキュリティ更新プログラムおよびテクニカルサポートは提供されなくなりました。そのため、ユーザーはより新しいバージョンへアップデートする必要があります。

Microsoftが推奨するアップグレード方法は、最新バージョンがインストールされた新しいデバイスを購入することです。

2023年11月現在、世界中で**16億台**以上のWindows OS搭載コンピューターが稼働しています。**StatCounter**のデータによれば、Windowsは世界のデスクトップOS市場の約70%を占めており、Windows XPはそのシェアの約0.38%を占めています。つまり、世界中で約600万台のコンピューターが依然としてWindows XPを稼働させていることになります。

Kaspersky Security for BusinessがWindows XPをサポート対象外とした理由

2020年まで、法人向けの総合的なエンドポイントセキュリティソリューションであるKaspersky Security for Businessは、多くのセキュリティベンダーがサポートを終了した後も、Windows XPオペレーティングシステムをサポートしていました。しかし時間が経つにつれ、サポートの継続は不可能になりました。

現実問題として、旧バージョンのWindowsとは異なり、脅威の状況は進化し続けています。多様化、複雑化する脅威に対して、当社は最先端の保護技術（例：アダプティブアノマリーコントロール）をお客様に提供できるよう不断の努力を続けています。しかしながら、これらの技術がいかに高度で効果的であっても、Windows XP環境では正常に機能させることができません。

代替的なソリューションの限界

サポート対象外のWindowsバージョンが稼働しているシステムの寿命は、もはや長くはありません。こうしたOSを保護対象とする代替的なセキュリティソリューションの品質と機能は、非常に限定されています。そのほとんどは個人向けデバイスを想定したものであり、ベンダーによるサポートが終了したOSに必要なレベルのセキュリティを確保できるものは存在しません。さらに、これらのソリューション自体も、まもなくサポートが終了する可能性があります。レガシーなWindowsオペレーティングシステムをサポートするセキュリティ製品の市場が、急速に縮小しているためです。

オペレーティングシステムの定期的な更新

もうその時が来ています。時代遅れでサポート対象外のシステムを使い続け、増大するリスクや非効率性との悪戦苦闘を続けるのは、得策ではありません。貴社は、最新のハードウェアとソフトウェアに投資するべき時期を迎えています。今こそ、長期的なアップグレードプランを策定しましょう。

旧式のオペレーティングシステムを今後も使用し続ける限り、リスクからは逃れられません。理由は2つあります：1つは、Microsoft社によるサポートやアップデートの提供が終了していること、そしてもう1つは、Kaspersky Security for BusinessやKaspersky Symphonyといった最新のセキュリティ製品を使用することができないということです。

保護を継続する方法

新しいオペレーティングシステムへの移行には、時間がかかります。この移行期間中に無防備な状態になることは、いかなる企業であれ容認しがたい事態です。

幸運なことに、当社はWindowsのレガシーバージョンを現在もサポートしている別のエンドポイントセキュリティソリューションを用意しています。このソリューションのサポートは、今後も継続される予定です。

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Securityは、レガシーオペレーティングシステムの完全な保護とサポートを提供します。これにより、Kaspersky Security for Businessの最新セキュリティ技術と互換性がある、より新しいWindowsオペレーティングシステムへの移行準備が整うまで、安心して使用を継続できます。

Kaspersky Embedded Systems Securityは、実績のあるマルウェア対策エンジンをベースとした、堅牢で多層的なセキュリティシステムです。また、法人向け製品ではおなじみのKaspersky Security Centerコンソールによる一元的な管理機能のメリットも、同様に享受いただけます。この軽量型ソリューションは、Windows XP SP2以降のWindowsオペレーティングシステム向けに特化して設計されています。

Windowsのレガシーバージョンからの移行に時間が必要な企業や、他のオペレーティングシステムに移行できない企業を対象に、安定感があり操作や管理が容易な保護を提供します。この製品は、ダウンタイムが重視される製造部門、自動化されたシステム、低電力だが重要性が高い機械操作、および信頼性が高く多層的な保護が必要なあらゆる環境に適しており、オペレーティングシステムによる制約を受けることなく使用できます。

機能比較

下のテーブルは、Kaspersky Embedded Systems Security および Kaspersky Endpoint Security for Windows が搭載する機能のリストです。Kaspersky Embedded Systems Securityへのアップグレードがもたらすメリットと変化を把握するために参照ください。Kaspersky Embedded Systems Securityには、Kaspersky Security for Businessで定評のある主要なセキュリティ機能が搭載されており、すべて単一のコンソールで管理できます。

機能	Kaspersky Embedded Systems Security for Windows 4.0	Kaspersky Endpoint Security for Windows 12.x (ワークステーション向け)	メリット
互換性とサポート			
Windows XP以降の旧型オペレーティングシステムのサポート	+	-	アップグレードが困難または不可能な旧式のシステムを搭載したワークステーションを、セキュリティを確立した状態で使用可能。
レガシーハードウェア/低スペックシステムに対するサポート	+	-	低消費電力システムでもセキュリティを確保。
脅威からの保護			
ファイル脅威対策	+	+	マルウェアや、本来の用途とは異なる悪用が可能な正規ツールなど、ファイルベースの脅威からの保護。
メール脅威対策	-	+	メール攻撃からの保護。
ウェブ脅威対策	-	+	Web上の脅威からの保護。
ネットワーク脅威対策	+	+	ネットワーク上の脅威からの保護。
シグネチャベースの手法を使用し、脅威を正確に検知（実行防止）	+	+	マルウェアを誤検知することなく正確に検知（あらゆるエンドポイントセキュリティプラットフォームの基幹機能）
ヒューリスティック分析とクライアント側の機械学習モデル（マルウェアの実行前および実行中）	+	+	間接的な統計指標の包括的な分析による、新種および未知の脅威の検知。
エミュレーションによるローカル環境のサンドボックス	+	+	安全なシミュレーション環境での疑似実行による、高度なステルス/暗号化マルウェアの検知。

機能	Kaspersky Embedded Systems Security for Windows 4.0	Kaspersky Endpoint Security for Windows 12.x (ワークステーション向け)	メリット
ふるまい分析	+	+	ふるまい分析による未知の高度な脅威の検知。
脆弱性攻撃ブロック	+	+	重要アプリケーションの脆弱性攻撃を防止。
ファイアウォール	+	+	不要かつ検証されていない危険な接続を、システムと外部ノードとの間で制限。
Advanced Detection and Responseソリューション (Kaspersky EDR、Kaspersky MDR) との連携	MDR	EDR、MDR	複雑な脅威の検知を目的として追加された機能と、広範かつ自動化されたインフラにおけるレスポンス機能。
KSN/KPSNとの連携	+	+	Kasperskyのクラウドインフラから直接アップデートされる脅威データ。
ファームウェアスキャナー	+	+	特定のマルウェアの検知を目的として対象を絞り込んだファームウェアスキャン (例: UEFIフラッシュドライブ上に潜伏するマルウェアなど)。
ネットワークフォルダーを暗号化から保護	+	+	ランサムウェアからの保護。
システムの強化 (攻撃対象領域の縮小)			
「Default Deny」に基づく、省力化されたセキュリティ設定	+	-	効率的でシステム負荷が低い設定: 既定で「拒否」するポリシーが基本として使用され、リソース消費量が多い保護レベルは無効化されています。
セルフディフェンス	+	+	ソリューションの構成要素に中断が発生した場合に生じるセキュリティレベルの低下からの保護。
不正な設定変更からの保護	+	+	ソリューション設定への不正な変更によるセキュリティ低下からの保護。
プログラムコントロール	+	+	信頼できない外部デバイスの使用を防止し、感染リスクやデータ漏洩のリスクを低減。
デバイスコントロール	+	+	個々のWebリソースとそのカテゴリを制御する機能により、感染の可能性やフィッシング攻撃の被害を低減し、情報および認証情報の損失を防止。
ウェブコントロール	-	+	プログラムの使用シナリオの分析と不審な活動の検知により、高度な脅威を検知。
アダプティブアノマリーコントロール	-	+	プログラムの実行を制御し、ファイルベースのマルウェアなどの不正な起動をブロック。
侵入防止システム	-	+	信頼性が低いアプリケーションに対して許可される一定数の動作に基づく攻撃からの保護。
脆弱性対策とパッチ管理	+(Compliance Edition)	+(Kaspersky Next EDR Optimumより提供開始)	ワークステーションにインストールされたシステムに存在する脆弱性の監視と、タイムリーな自動アップデートによる修正。

機能	Kaspersky Embedded Systems Security for Windows 4.0	Kaspersky Endpoint Security for Windows 12.x (ワークステーション向け)	メリット
システム整合性監視			
ファイル変更監視	+ (Compliance Edition)	+ (Kaspersky Hybrid Cloud Security Enterprise Server/CPUのみ)	不正なシステム変更の検知（電源オフ時に行われた変更など、あらゆる干渉的な動作を検知）。
ログ分析	+ (Compliance Edition)	+ (Kaspersky Hybrid Cloud Security Enterprise Server/CPUのみ)	システムログの変更を監視し、システム内における禁止された活動を検知。
レジストリアクセス監視	+ (Compliance Edition)	+ (Kaspersky Hybrid Cloud Security Enterprise Server/CPUのみ)	システムレジストリへの不正な変更の試行の監視とブロック。
監視と管理			
Kaspersky Security Centerによる、一元的なローカル管理	+	+	カスペルスキー製品の一元的な管理を可能にする、統一されたセキュリティ環境。
アプリケーション設定をデバイス上のローカルコンソールを使用して管理	+	+	制御サーバーとの通信が確立されていない状態でも、ソリューションの設定が可能。
Kaspersky Security Center Cloud コンソール	+	+	容易な導入とリソースの節約：管理サーバーを別途インストール、保守する必要がありません。
コマンドラインコントロール	+	+	グラフィカルインターフェースを必要としない、管理が容易でシンプルなワークフロー。
SIEMシステムとの連携	+	+	このソリューションは、ワークステーションレベルのイベントデータにより、セキュリティの全体像を補完します。

産業環境での使用

産業用制御システムまたはSCADAシステムがWindows XP上で動作している場合、ICS保護専用設計されたソリューションである **Kaspersky Industrial CyberSecurity for Nodes** を推奨します。長期間にわたりレガシーオペレーティングシステムへの継続的なサポートを提供し、産業用システムとの互換性を維持します。

今すぐ対策を始めましょう

使用中のオペレーティングシステムを、可能な限りすみやかにアップグレードしてください。ITの観点から効率的かつセキュリティを担保した業務運営を継続するためには、移行計画を今すぐ開始する必要があります。意思決定と導入を進めている間は、Kaspersky Embedded Systems Securityが既存のワークステーションを保護します。

既存のインフラで稼働しているWindowsのレガシーオペレーティングシステムをKaspersky Embedded Systems Securityで保護する方法は、[このリンク](#)を参照してください。