

# CROWDSTRIKE FALCON PREVENT™

## 次世代アンチウイルス

最新の脅威から身を守るために、次世代のアンチウイルス・ソリューションを導入しませんか？



## FALCON PREVENT：業界で認められた アンチウイルスの新しい選択肢

動作が重く、定義ファイルに依存し、最新の攻撃に対応できないレガシーなアンチウイルス製品にエンドポイントの保護を任せていませんか？

Falcon Prevent™ は、業界で最も完全なアンチウイルスの代替ソリューションで、1つの軽量エージェントで優れたプロテクション機能を提供します。定期的にシグネチャーを更新したり、オンプレミスの管理サーバーを用意したり、複雑なインテグレーション作業をする必要はありません。大量のエンドポイントに展開する場合でも Falcon Prevent なら短時間で稼働させることができます。

レガシーなアンチウイルスの代替ソリューションとして認定 — AV-Comparatives や SE Lab といった独立系のテスト機関が、Falcon Prevent のアンチウイルス機能を認定しています。Falcon Prevent は PCI、HIPAA、NIST や FFIEC でも評価され、規制条件を満たしています。

Gartner のエンドポイント・プロテクション・プラットフォーム・マジック・クワドラントが「Visionary」と評価 — 革新的なプロテクション機能とシンプルな導入モデルで、Visionary の評価を受けました。

### 製品の主な機能

従来のアンチウイルス製品では対応できないファイルレス（マルウェアを使わない）攻撃にも対応

- 古いアンチウイルスでは対応できないギャップを埋める — Falcon Prevent は、単に従来のアンチウイルスの代わりとなるだけでなく、新たな

### 主な特長

- » 既知並びに未知のマルウェアやランサムウェアを防ぎます
- » ファイルレス攻撃やインメモリ攻撃を防ぎます
- » マルウェアを使わない各種攻撃を防ぎます
- » シグネチャーを使わないシンプルな SaaS です
- » 古いアンチウイルス製品を迅速に確信を持って置き換えられます

「現代の高度な攻撃を止めるために、これまで以上に多くの組織がもっと効果のあるソリューションを探中、CrowdStrike Falcon はその解決策になると思う」

— スティーブ・フィルポット  
WESTERN DIGITAL CORP. CIO



プロテクション機能をエンドポイントに提供します。標準的なアンチウイルス製品では検知できないファイルレス攻撃やインメモリ攻撃などの巧妙なテクニックをブロックするために、Falcon Preventにはマシンラーニングや振る舞い分析の機能が追加されています。

- **1つのエージェント** — Falconのすべての機能を利用する場合でも、エンドポイントに入れるエージェントは1つだけです。マシンラーニング、エクスプロイトブロッキング、カスタマイズされたホワイトリストやブラックリストの作成、振る舞いIndicator of Attack (IOA)、攻撃元の識別やアドウェアブロックなど、1つのエージェントに最高の次世代技術を集約しています。
- **オンラインでもオフラインでも完全なプロテクションを実現** — Falcon Preventはエンドポイントがネットワークに接続していないときにも、クラウドに接続した際に得た付加機能を活用して保護を行います。

## 導入の早さとエンドポイントの軽さも魅力

- **時間、労力、費用を削減** — Falcon Insightはクラウドから全て提供されるため、オンプレミスのサーバーなどは一切必要ありません。
- **数分で導入完了** — Falconエージェントを各エンドポイントに展開するだけで導入が完了します。例えば7万台のエンドポイントにFalcon Insightを展開されたあるお客様では、1日以内に導入作業を全て完了されました。
- **短時間で稼働開始** — 導入にあたり、エンドポイントの再起動は必要ありません。複雑なチューニングやコンフィギュレーション設定もありませんので、導入初日からその効果を発揮します。

## 存在を忘れるほど負荷のないシステム

- **エンドポイントが重くならない** — Falconの軽量エージェントはわずか20MBのサイズ。エンドポイントやネットワークへの影響はほとんどありません。
- **リポート不要** — インストールやアップデートの際の再起動は不要で、エンドポイントに影響を与えません。
- **頻繁に生じる煩わしいスキャンやアップデートは不要** — Falcon Preventならシグネチャーのアップデートやディスクスキャンなどのパフォーマンスを著しく低下させるタスクをなくすことができます。

## 安心の移行作業

- **簡単な移行** — 移行中もFalcon Preventはアンチウイルスと共にシームレスに稼働します。



## 組織をマルウェアや侵入から守る 最速かつ 最も簡単な手法

現代の攻撃者はその手口をマルウェアやエクスプロイトだけに留めません。そのため、Falcon Preventは新時代の防御機能を提供し、こうした進化するツールや技術に打ち勝っています。



CrowdStrikeは、クラウドベースの次世代エンドポイントプロテクションの業界を牽引しています。CrowdStrikeは、次世代のアンチウイルス、EDR、および24時間体制のマネージド脅威ハンティングサービスを統合し、すべてを1つの軽量エージェントで提供する、業界初、かつ唯一の企業として、革新的なエンドポイントプロテクションを提供しています。

詳細は、[crowdstrike.com](https://crowdstrike.com) をご覧ください。