



# HP WOLF PRO SECURITY

仕様書



HP WOLF SECURITY

## 簡単に使用できる 包括的な エンドポイント セキュリティ



多くのお客様は、セキュリティ知識の不足などの理由のため、フィッシングやランサムウェアなどのサイバー攻撃への対応が難しくなっています。またこのような攻撃は、システムへの侵害、データの盗難、長時間のダウンタイムなどの問題を引き起こします。

HP Wolf Pro Securityは、次世代アンチウイルス機能に加え、マイクロ仮想マシンを使用した脅威の封じ込めおよびフィッシング対策を含む包括的なエンドポイントセキュリティです。HP Wolf Pro Securityは、管理者の負担を増やしたり、従業員の生産性を低下させたりすることなく、巧妙化する脅威に対する多層防御により、お客様のセキュリティ課題を克服することを支援します。

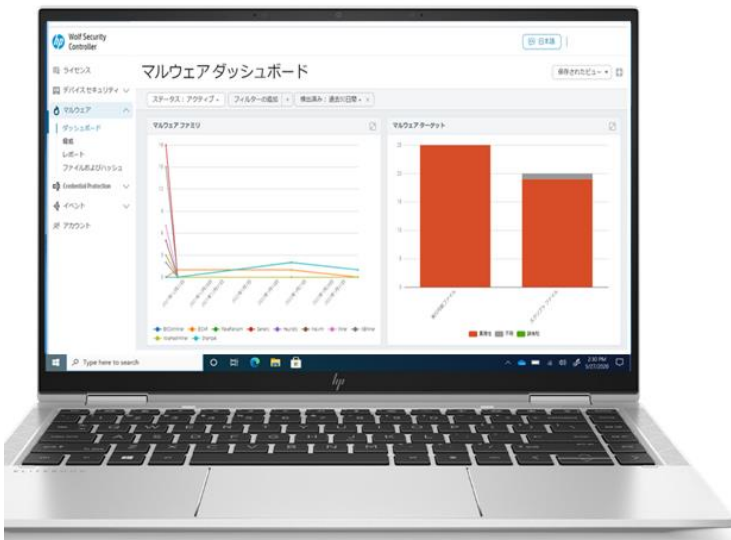
### 簡単に導入および運用できるエンドポイントセキュリティ

HP Wolf Pro Securityは、シンプルさを追求した包括的なエンドポイントセキュリティです。HP Wolf Pro Securityを簡単な3ステップで導入後、事前に構成されたポリシーを使用することで、すぐに使用することが可能です。また、日本語に対応したHP Wolf Security Controller<sup>1</sup>により、簡単な管理を実現します。

クラウドベースのコントローラであるHP Wolf Security Controllerは、お客様の保有PC全体のセキュリティおよび正常性を簡単に管理するための機能を提供します。管理者はいつでもどこからでも脅威に関する洞察を確認することができます。

事前構成された「すぐに使用できる」ポリシーは、迅速かつ簡単な導入を実現します。また、ポリシーは簡単で理解しやすく、ほとんどの環境で継続的な調整は必要ありません。

セキュリティアラートは、管理者がPC上の不審な行動を、必要な分だけ簡単に特定できるようにします。



HP Wolf Security Controller

## 従業員の生産性を低下させることなく保護する

従業員はセキュリティのエキスパートではないため、ソーシャルエンジニアリング攻撃に対して常に「警戒態勢」で攻撃を見つけることを従業員に期待することは現実的ではありません。また、そのような従業員の作業を妨げるセキュリティ対策は、従業員が安全に作業し、かつ生産性の向上を期待しているお客様には十分ではありません。

HP Wolf Pro Securityは、PCユーザーを保護する包括的なエンドポイントセキュリティを提供するとともに、従業員に最適なユーザー体験を提供します。

- 従業員は「セキュリティ センサー」としての役割を負うことなく、添付ファイルおよびリンクを安心して開くことができます。
- PCがインターネットに接続されていないときでも従業員はいつでもどこからでも安全に作業できます。

お客様は、**日常の業務を妨げることなく機能するエンドポイントセキュリティ**であるHP Wolf Pro Securityを使用することで、従業員がデータ、パスワード、およびお客様のシステムを安全に保つように安心して作業をしながら、生産性を向上させることを実現できます。

## 証明済みの信頼できる保護

HP Wolf Pro Securityは、お客様を保護することが既の実証されているセキュリティテクノロジーを使用しています。HP Wolf Securityテクノロジーを搭載したPCは、セキュリティ侵害の報告なく、100億を超える電子メールの添付ファイル、Webページおよびダウンロードにアクセスできています。

HP Wolf Pro Securityには3つの機能があり、これらはすべてWolf Security Controllerを使用して管理することができます。

**ハードウェアベースの脅威封じ込め<sup>2</sup>**は、ソーシャルエンジニアリングまたはその他の方法を介したマルウェア攻撃をマイクロ仮想マシンに隔離して封じ込めることで、PCやネットワーク上の他のデバイスに感染するのを防ぎます。

**フィッシング対策のユーザー資格情報の保護**は、ユーザーをだまして偽のWebサイトにパスワードを入力させようとするフィッシング攻撃をブロックすることで、ユーザー資格情報の盗難を防ぎます。

**次世代アンチウィルス**は、既知のマルウェアを阻止するだけでなく、ディープラーニングAIを使用して新しい脅威を検出します。



## シンプルで包括的なエンドポイントセキュリティのメリット

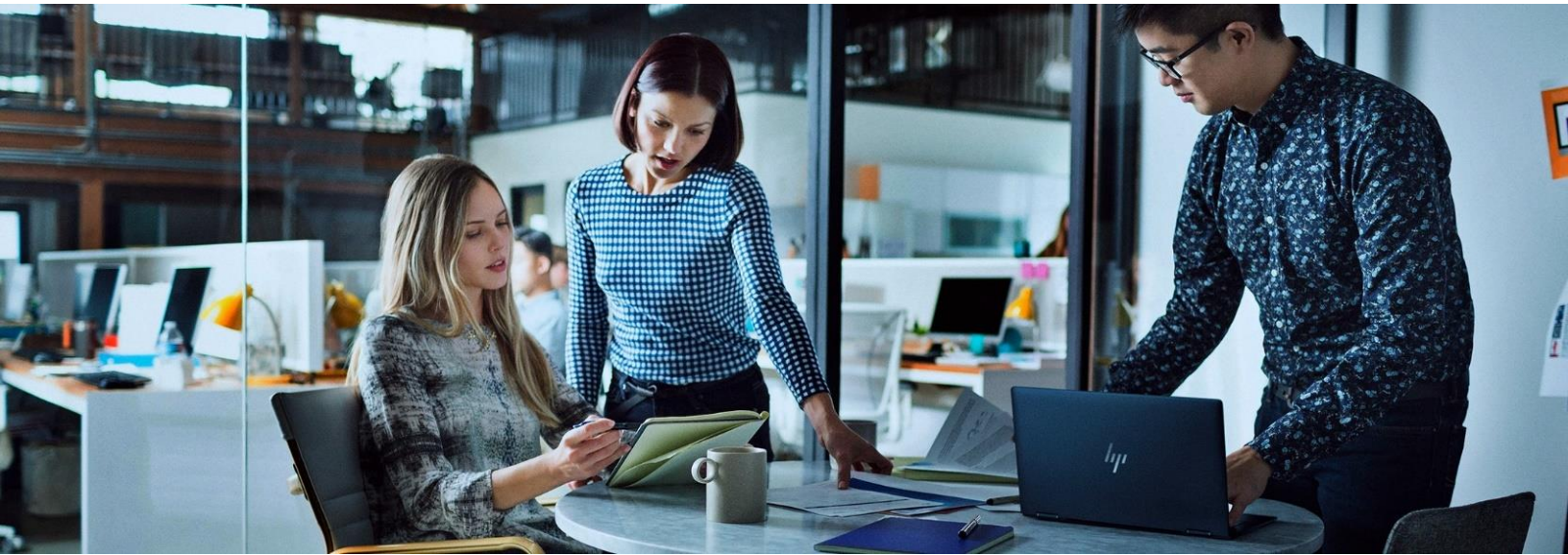
HP Wolf Pro Securityは、セキュリティ対策への投資を抑えながら、エンドポイントセキュリティを強化しようとしているお客様に最適です。従来のウィルス対策をHP Wolf Pro Securityに置き換えることで、セキュリティ対策が強化され、またユーザー体験および生産性を最大化できるようになります。

- リアルタイムのAIによる保護、ゼロトラストのハードウェアベースの隔離など、予防を最優先したエンドポイントセキュリティによる**リスクの低減**
- クラウドベースのWolf Security Controllerを含むHP Wolf Pro Security導入の簡素化
- Wolf Security Controllerを使用した継続的な管理の簡素化

## HP WOLF PRO SECURITYの要件およびコンポーネント

Wolf Security Controller	25台以上のPCを持つすべてのお客様で利用できます。
セキュリティソフトウェア要素	Windows用のHP Wolf Pro SecurityクライアントおよびWolf Security Controller(クラウド)
サポートされているオペレーティングシステム	Windows 11 64ビット、Windows 10 Pro 64ビット、Windows 10 Enterprise、Windows 10 Enterprise LTSC (64ビットのみ)
必要なメモリ/ディスク領域	8 GB以上のシステムメモリ/10~20 GBの空きディスク領域
言語サポート (エンドポイント)	英語、オランダ語、フランス語、ドイツ語、イタリア語、日本語、ポルトガル語 (ブラジル)、スペイン語、スウェーデン語
言語サポート (コントローラ)	英語、日本語
ネットワーク要件	脅威の分析には、管理対象デバイスとクラウド管理サービス間の通信のためのインターネット接続が必要です。ただし、保護はオフラインの状態でも正常に機能し、ネットワーク接続は必要ありません。
導入要件	本製品を使用するには、購入後にHPからの電子メールの指示に従って、アクティブにする必要があります。アクティブにする際、ユーザーアカウントおよびセキュリティポリシーのセットアップに必要な情報を提供する必要があります。
サービス利用規約	サービス利用規約については、 <a href="#">こちら</a> を参照してください。
アクティベーション	ライセンスアクティベーションメールは、HPからパートナー様もしくはエンドユーザー様が受領後、90日以内にアクティベーションを完了してください。

[HP Wolf Pro Security](#)にて詳細をご覧ください。



### 免責事項

<sup>1</sup> HP Wolf Pro Security Controllerには最低25台のデバイスが必要です。

<sup>2</sup> 脅威の封じ込めのためにサポートされているブラウザには、Microsoft Windows用の次のブラウザが含まれます。Microsoft Edge、Google Chrome、Mozilla Firefox、またはChromium。Microsoft OfficeまたはAdobe Acrobatがインストールされている場合、サポートされる添付ファイルには、Microsoft Office (Word、Excel、PowerPoint) のファイルおよびPDFファイルが含まれます。

© Copyright 2022 HP Development Company, L.P.ここに記載されている情報は、将来予告なしに変更されることがあります。HP製品およびサービスに対する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。ここに記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対してHPは責任を負いかねますのでご了承ください。

MicrosoftおよびWindowsは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。IntelおよびCoreは、米国およびその他の国/地域におけるIntel Corporationおよびその子会社の商標です。

4AA8-0275JPN 2022年4月

