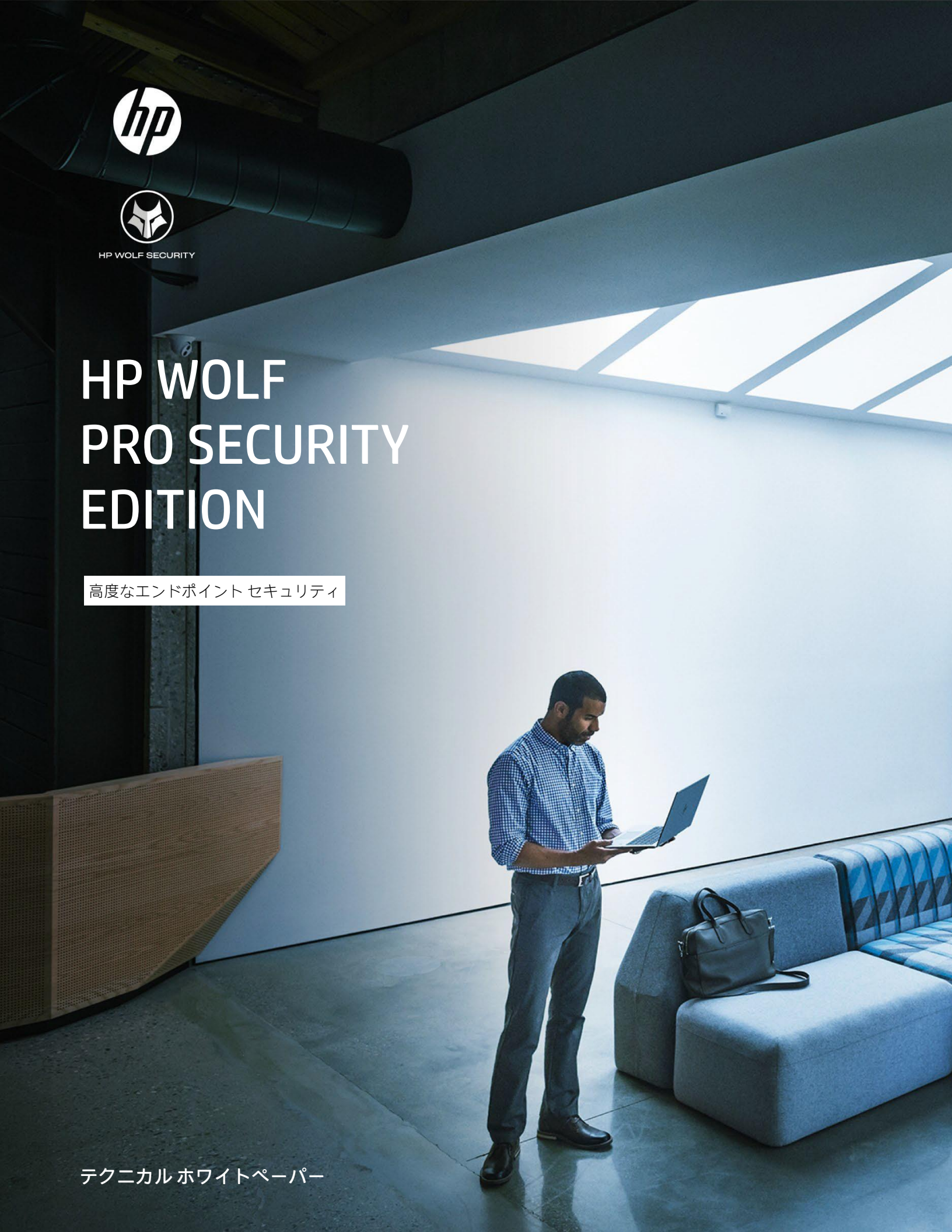


HP WOLF PRO SECURITY EDITION

高度なエンドポイント セキュリティ

テクニカル ホワイトペーパー

HP Wolf Pro Security Editionが提供するエンタープライズレベルのセキュリティ

IT部門の手間をかけずに、シームレスな展開と管理をサポート

目次

はじめに 2

HP Wolf Pro Security Edition - 概要 2

HP Wolf Pro Security Editionの機能 2

HP Wolf Pro Security Editionのアクティブ化 5

HP Wolf Pro Security Editionの更新 6

ダッシュボード 6

ポリシーおよび設定 10

まとめ 11

はじめに

働く場所や働き方の進化とともに、マルウェアやサイバー脅威の数と複雑さはますます増大しています。こうした脅威の状況は高度化し、従来のPCのセキュリティでは簡単にすり抜けられてしまいます。攻撃が一度でも成功すれば、業務停止に追い込まれて経済的な影響が生じ、ビジネスにダメージを受け、破綻する恐れもあります。

中小企業でも今日の脅威の状況に対抗するため、優れたIT部門を擁する大企業と同様の高度なPCセキュリティが必要とされています。

HP Wolf Pro Security Editionは、IT部門の手間をかけずにシームレスな展開と管理をサポートする、エンタープライズ レベルのセキュリティを提供します。1つのコンソールでHP Sure Click ProとHP Sure Sense Proを利用でき、中小企業向けに最適化されています。

HP Wolf Pro Security Edition - 概要

HP Wolf Pro Security Edition[2]は、IT部門によるポリシー管理を必要とせずに、中小企業をマルウェアおよびブラウザーベースの攻撃から保護するために設計された、包括的なセキュリティ ソリューションです。ユーザーの操作なしで、PC上の危害を及ぼすファイルを検出して停止し、隔離します。

HP Wolf Pro Security Editionは、仮想化、フィッシング対策、人工知能、および機械学習を組み合わせた、独自のマルチ テクノロジー アプローチを使用し、グループ セキュリティ ポリシーを介して統合ユーザーコンソールで相互に補完します。ソフトウェア更新と新しいポリシーは、HPクラウドを介して展開され、バックグラウンドで配信され、ユーザーの操作は必要ありません。

HP Wolf Pro Security Editionは、一部のHPノートブックにプリインストールされた状態で購入できます。1年間または3年間のライセンスには、ソフトウェア、HPクラウドで配信される更新、およびHPサポート デスクによるサポートが含まれます[1、2]。

HP Wolf Pro Security Editionの機能

HP Wolf Pro Security Editionでは、次の3種類の保護を提供します。

保護1：脅威の封じ込め

HP Wolf Pro Security Editionには、HP Sure Click Proが付属しています。PCにおいて最も脆弱性の高いタスク（Webの閲覧や電子メール添付ファイルのオープン）の実行中、HP Wolf Pro Security Editionでは、HP Sure Clickのコア機能であるアプリケーション隔離を使用し、セキュリティを強化します。HP Sure Clickは、マルウェアを特定しようとするのではなく、信頼できないWebサイトやファイルをマイクロ仮想マシン（マイクロVM）と呼ばれる隔離された仮想コンテナ内で開きます。悪意のあるコードが存在する場合、これらのマイクロVMはマルウェアをだまして、実際には封じ込められているにもかかわらず、コンピュータ内で実行していると思い込ませます。

ハードウェア強制のマイクロVMの内部では、マルウェアは、ユーザーのPCに悪影響を及ぼすことも、ファイルにアクセスすることも、ブラウザーの他のタブに移動することもできません。ブラウザーのタブやMicrosoft Officeファイルを閉じると、マイクロVM全体が自動的に廃棄され、内部に封じ込められているマルウェアも削除されます。特別なトレーニングや追加の隔離手順は必要ありません。ブラウザーのタブやファイルを閉じるだけで、マルウェアを消去できます。

閲覧の安全性に対する確信

HP Wolf Pro Security Editionに搭載されたHP Sure Click Proの機能として、ChromiumベースのHP Sure Click Pro Secure Browserがあります。この安全なブラウザーでは、Webサイトを常に隔離された独自のマイクロVM内で開くため、新しいブラウザーについて学んだり、制約の多いホワイトリストを扱ったりしなくても、インターネットを安全に閲覧できます。遭遇したマルウェアはすべて、システムの他の部分から隔離され、ブラウザーのタブを閉じると破棄されます。

一般的なファイルに対する保護

マルウェアは、Webからダウンロードした、または電子メールの添付ファイルとして送信された、無害に見えるファイルにも潜んでいる場合があります。そのため、HP Wolf Pro Security Editionではブラウザー以外にも保護の対象を広げ、マイクロVM内でのPDFの閲覧中やMicrosoft Word / Excel /PowerPointドキュメントの編集中も保護されるようにしています。

見慣れないファイルは、疑わしいWebサイトを隔離する場合と同じハードウェア強制の隔離環境内で開くことで保護します。ファイルが感染している場合、マルウェアを封じ込めてPCへの感染を防ぎます。

保護2：マルウェアの防止

HP Wolf Pro Security Editionは、HP Sure Senseのコア機能を利用して、ゼロデイ攻撃（未知のコンピューター セキュリティの脆弱性を悪用する脅威）およびAdvanced Persistent Threat（APT）攻撃をリアルタイムで検出し、防御します。プロアクティブな保護によって検出の精度とリアルタイムの防御を実現し、あらゆる（既知および未知の）脅威に対してPCを保護します。

HP Sure Sense Proは、次の主要なコンポーネントを利用して、セキュリティ ソリューションを実装します。

- エンドポイント レイヤー：ヒューリスティック分析、シグネチャベースの検出、エミュレーション、汎用的な検出、およびシグネチャを利用した機械学習モデルなど、幅広い保護レイヤーをサポートします。
- ファイル レピュテーション クラウド サービス：ファイル レピュテーション サービスは、高速で拡張性の高いインフラストラクチャをクラウド内に提供して、分類のための第2レイヤーを追加します。これらのサービスを使用すると、既知のファイルに関する知的情報のデータベースを利用して検証の第2レイヤーでファイルを再分類し、リアルタイムで判定を正しく更新できます。

保護3：アイデンティティ保護

アイデンティティ保護は、電子メール、チャット クライアント、PDFなどのフィッシング リンクに潜む資格情報の窃取攻撃に対して、ユーザーが資格情報を送信することがないよう保護することを目的としています。

アイデンティティ保護は、HP Wolf Pro Security Editionの脅威封じ込め（隔離）機能とは別のものであり、その機能は、単にWebブラウザーの使用中にユーザーを保護するだけです。現時点で、HP Wolf Pro Security Editionのアイデンティティ保護機能は、次のブラウザーに対応しています。

- Google Chrome
- Edge Chromium
- HP Sure Click Pro Secure Browser

ユーザーを保護する仕組み

電子メール、Webメール、チャット クライアント、PDFなどにあるリンクをユーザーがクリックすると、通常どおりリンク先がブラウザーで開きます。バックグラウンドでは、HPの拡張機能がドキュメント オブジェクト モデル（DOM）、Webページのコンテンツ、およびその構造を調査し、Webページにログイン フォーム/ページ/オプションが含まれているかどうかを確認します。ページの読み込みとの並列処理で、HPクラウド サービスに対して完全なURLの問い合わせが行われ、既知の不正なサイト、既知の安全なサイト、または未知のサイトでないかどうかが確認されます。

- HPクラウドで既知の不正というレピュテーション スコアが検出された場合、ブラウザー拡張機能のステータス アイコンが赤色に変わります。
- HPクラウドで肯定的なレピュテーション スコアが検出された場合、ブラウザー拡張機能のステータス アイコンは緑色に変わります。
- HPクラウドで不明という評価が検出された場合、ブラウザー拡張機能のステータス アイコンは灰色に変わります。

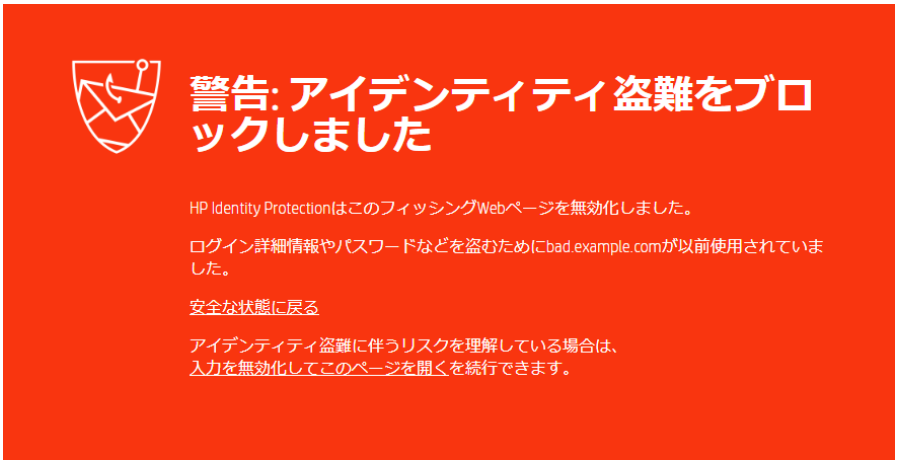
このアイコンは、ブラウザーでステータスを通知するものであり、ユーザーの操作は必要ありません。

Tracking Cookieや広告などのオフサイト資産へのアクセスを含め、Webページの読み込みが完了するには少し時間がかかる場合がありますが、バックグラウンドの並列チェックはページの読み込みを妨げることはなく、読み込みの完了を待機します。

ユーザーがWebページのダイアログ ボックスで資格情報の入力を開始すると、HP Wolf Pro Security Editionは、入力されたパスワードや資格情報データの最初の1文字に応じて動作します。既知の不正なWebサイトでユーザーが資格情報を入力しようとしない限り、ブロッキング テクノロジーは起動しません。

既知の不正なページ

Webページが既知の不正なページである場合、HP Wolf Pro Security Edition（拡張機能）のステータス アイコンは赤色の表示になります。パスワードまたは資格情報データの1文字目を入力すると、Webページの上に、透明の赤色が重ねて表示されます。表示されるメッセージで、既知の不正なWebサイトであること、またHP Wolf Pro Security Editionによりこのサイトへの資格情報の入力がブロックされていることがわかります。ユーザーは、すべての入力がブロックされた状態のままページの閲覧を続けるか、安全のために（タブを閉じて）ページを終了できます。



未知のページ

Webページが未知であるか、悪質なページの可能性がある場合、HP Wolf Pro Security Edition（拡張機能）のステータス アイコンは灰色の表示になります。パスワードまたは資格情報データの1文字目を入力すると、Webページの上に灰色が重ねて表示され、そのサイトがフィッシング サイトである可能性があり、続行する場合は注意が必要であると警告されます。

ユーザーは、入力が無効な状態でWebページの閲覧を続行するか、または資格情報の入力を続行するよう選択できます。入力の続行を選択すると、そのサイトはローカルのホワイトリストに追加され（サイトが「ホワイトリスト化」され）、ユーザーのブラウザーの拡張機能ストアに保存されます。

HP Wolf Pro Security Editionのアクティブ化

HP Wolf Pro Security EditionをHPの工場出荷時のプリインストールされた状態で購入した場合、次のプロセスを使用してソフトウェアをアクティブ化します。

- HP Wolf Pro Security Editionがプリインストールされた新しいHP PCの電源をオンにします。
- 新しいPCで、HPの自動セットアップ（OOBE：アウトオブボックス エクスペリエンス）とソフトウェア ライセンス同意の手順が実行されます。
- OOBEの完了時、OOBE中のユーザーの選択内容に応じて、PCの再起動が必要になる場合があります。
- ユーザーがHPのセキュア ブラウザー、HP Wolf Pro Securityデスクトップ コンソールを開くか、再起動を開始します。
- 1回のみのバナー（例：表示されるテキストはバージョンによって異なります）。[HP Wolf Pro Security Editionをご利用いただきありがとうございます。これでPCは保護されました。]が表示されます。（ユーザーに[OK]をクリックするよう促します）。
- これでアクティブ化が完了します。

HP Wolf Pro Security Editionの更新

HP Wolf Pro Security Editionは、一部のHPコンピューター（ノートブック、デスクトップ、ワークステーション）にプリインストールされたソフトウェア アプリケーションとして提供されます[2]。クラウドベースのセキュリティ ソリューションとして、更新はHPのクラウドによって配信されます。これらの更新には、新しいセキュリティ ポリシー、更新された脅威プロファイル、およびHPが適用を選択した拡張機能が含まれます。新しいコードをアクティブ化するための再起動以外に、更新の受信に必要なユーザー アクションはありません。

ダッシュボード

統合されたセキュリティ コンソール

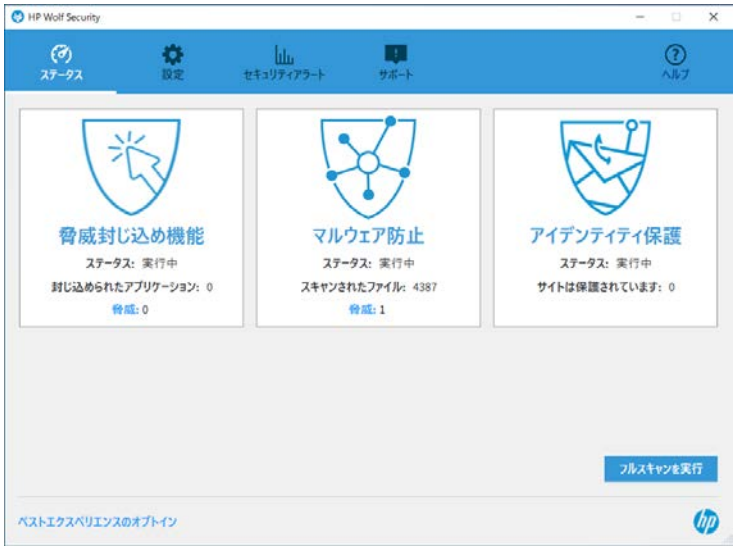
HP Wolf Pro Security Editionにはシンプルなダッシュボードが用意されており、ユーザーはそこから、[ステータス]、[設定]、[セキュリティアラート]、および[サポート]にアクセスできます。ダッシュボードでは、すべてのセキュリティ保護が、使いやすい4つの選択可能なページにまとめられています。

技術系以外のユーザー向けのメモ：ユーザーがHP Wolf Pro Security Editionダッシュボードを一度も開いていないか、アクセスしていない場合でも、保護と設定はHPの工場で製造プロセス中にインストールされ、構成されているため、ダッシュボードにアクセスしたかどうかにかかわらず、ユーザーは保護されます。このため、中小企業のユーザーなど、セキュリティやソフトウェアに関する知識がない場合でも、確実に保護されます。

ステータス

HP Wolf Pro Security Editionダッシュボードには、Windowsの[スタート]メニュー（アイコン）からアクセスできます。初期設定では、ユーザーが選択できる4つのアイコン カテゴリを含むステータス ページが表示されます。さらに、3つの保護メカニズムを示す大きいアイコンが表示されます。[脅威封じ込め機能]、[マルウェア防止]、および[アイデンティティ保護]のアイコンです。また、[フルスキャンを実行]アイコンでは、PC全体の再スキャンを実行できます。
（**注記：**HP Wolf Pro Security Editionには、既存のファイルや新規ファイルを常時スキャンして監視する「エージェント」が含まれています。PCの全ファイルを再スキャンしたい場合、ユーザーは、リセットして新規スキャンを開始できます。）

[脅威封じ込め機能]のアイコンは、ソフトウェアに新しいセキュリティ ポリシーや更新が追加された場合は色が変わってこれを示します。ほとんどの場合、HP Wolf Pro Security Editionのすべての更新はHPクラウドから自動的に展開され、必要に応じて再起動を行う以外にユーザーの操作は必要ありません。



機能またはポリシーが更新されていることを示す黄色いアイコンは、ユーザーがPCを再起動する必要があることを表しています。

[設定]

[設定]アイコンを選択すると、HP Wolf Pro Security Editionには、各種機能を含む3つのタブ ページが表示されます。

[設定]

1番目のタブは[設定]タブで、HP Wolf Pro Security EditionがユーザーのPCだけでなく、他のユーザーの保護に役立つようにします。HPでは、ユーザーがこのチェックボックスをオンにして、この機能を有効にすることを推奨しています。HP Wolf Pro Security Editionユーザーが悪質なイベントに遭遇すると、そのデータがHPクラウドに共有されます。このような脅威データを共有することで、HPはデータを記録して、他のユーザーが同じ攻撃を受けないようにすることができます。

注記：この機能を有効にしても、個人データやユーザー データはHPクラウドに送信されません。攻撃から取得したデータのみが記録されます。

[除外]

2番目のタブは、[除外]タブです。ユーザーはこのタブで、安全性が確認されているフォルダーとプロセスを選択できます。このページでどちらかのリストに、(1つまたは複数のファイルを含む）フォルダー名またはプロセス名を追加すると、HP Wolf Pro Security Editionによるセキュリティ スキャンの実行時に、(「安全」であるとみなされ）バイパスされます。

たとえば、作業環境で一連のカスタム アプリケーションを作成した場合、HP Wolf Pro Security Editionでは、その固有ファイルを脅威として捉える場合があります。このカスタム アプリケーション（または関連ファイル）を除外リストに追加すると、そのファイルは、その後のマルウェア スキャンから除外されます。

[復元済みのファイル]

3番目のタブは、[復元済みのファイル]タブです。HP Wolf Pro Security Editionにより当初悪質としてフラグ付けされたファイルのアクティブなリストが保持されますが、ユーザーはこのファイルを安全としてマークすることができます。通常、安全なファイルは信頼できるソースから取得したもの、ユーザーがそのファイルを安全としてマークしたもの、またはその両方です。

注記：安全でないとフラグ付けされたファイルはキャプチャされ、[セキュリティアラート]ページに記録されています（[セキュリティアラート]ページについては次に説明します）。

[セキュリティアラート]

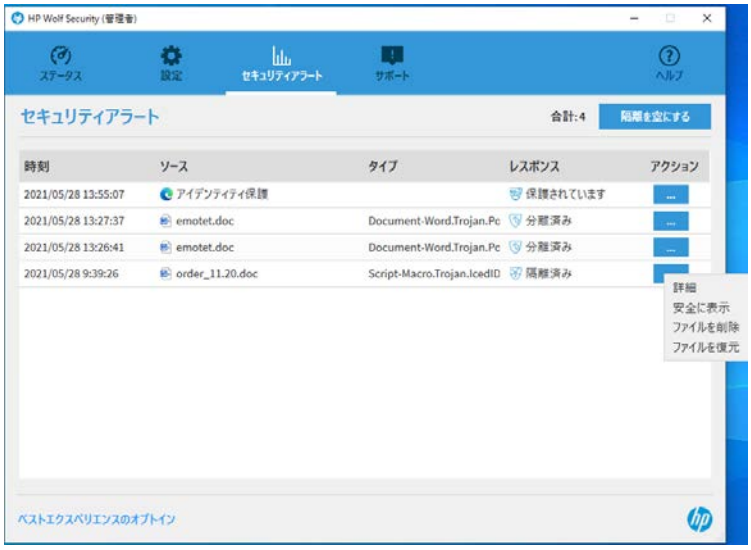
[セキュリティアラート]アイコンを選択すると、隔離され、悪質とフラグ付けされたファイル名やWebサイトのリストが表示されます。

HP Wolf Pro Security Editionで保護対策が取られたファイルに関する情報は、次の列見出しの下に表示されます。

- [時刻]：脅威が検出された年、月、日、および時間。
- [ソース]：[ソース]列にはアイコンとファイル名が表示され、悪質な可能性のあるファイルとして分類され、隔離されたファイルの種類を示します。通常、アイコンは、疑わしいファイルがドキュメント（Word、Excelなど）であるか、またはWebブラウザー経由で遭遇したものであるかを示しており、資格情報を盗もうとしているWebサイトにフラグを付けます。
- [タイプ]：マルウェアの一部のタイプ（ランサムウェアなど）を分類でき、可能であれば、HP Pro Securityによりこの列に情報が表示されます。
- [レスポンス]：悪質なファイルやWebサイトに遭遇したときに、HP Wolf Pro

Security Editionで行われたアクションが表示されます。

- [アクション]：アクションの[…]ボタンには、複数のユーザー オプションがあります。
  - [隔離済み]の対応には、次の4つのオプションが表示されます。
    - ファイルの[詳細]：時刻、ファイルの場所、タイプ、およびハッシュ値。
    - [安全に表示]保護された仮想マシンでファイルを開いて表示し、ファイルが安全であるか、または隔離したままにするかを判断できます。
    - PCから[ファイルを削除]します。
    - [ファイルを復元]ファイルの状態を[信頼済み]に変更します。
  - [保護されています]の対応には、[アイデンティティ保護]（HP Wolf Pro Security Editionのフィッシング対策保護）で、安全でないとフラグ付けされたWebサイトについて、次の詳細を確認できます。
    - ファイルの[詳細]：時刻、URLの場所。



[サポート]

HP Wolf Pro Security Editionダッシュボードの[サポート]タブには、次のような複数の情報ポイントがあります。

[概要]

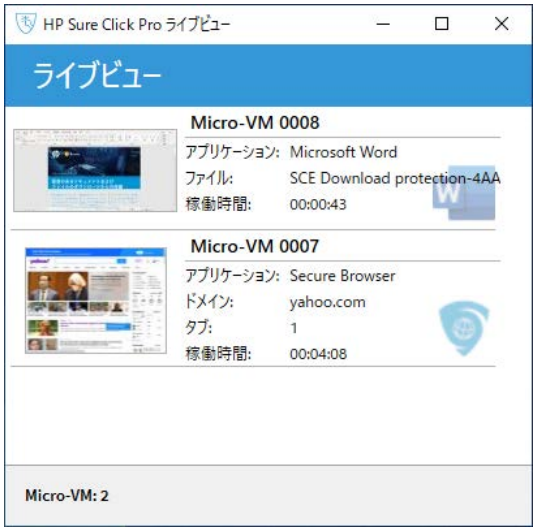
HP Sure Click ProとHP Sure Sense Proは、相互に補完するよう組み合わせて統合され、この統合コンソールに表示される固有のアプリケーションです。それぞれのアプリケーションは、HPクラウドから個別に更新を受信できます。各セキュリティ要素が固有の更新を受信できるため、そのバージョン番号は同期されず、必ずしも同じになりません。

[サポート]ページに表示される[コンピュータID]はPCごとに一意であり、そのPCにライセンス版のHP Wolf Pro Security Editionがインストールされていることを示します。

[サポートツール]

ログ記録を有効にすると、HP 3LSサポートへの情報提供を目的として、ユーザーが定義したPCのディレクトリの場所（デスクトップなど）に、.zipログ ファイルが作成されます。[レポートを送信]ボタンを押すと、ログ ファイルがHPサポート エージェントに電子メールで送信されます。

[ライブビューを開く]は、HP Sure Click Pro Secure Browserなどを使用する場合の高度な機能です。[ライブビューを開く]ボタンを押すと、次に示すダイアログ ウィンドウが作成され、HP Sure Click Pro Secure Browserなどの仮想環境で実行されているアプリケーションが表示されます。ライブビューに表示されるアプリケーションは、PCのメモリおよびハード ドライブから隔離されています。



HPのプライバシー ポリシーとライセンス情報も、[サポート]ページから確認できます。

ポリシーおよび設定

HP Wolf Pro Security Editionは、工場出荷時にクラウドベースのセキュリティ ポリシーが事前構成されています。つまり、IT管理やバックエンドのコンソール制御を必要としない「ヘッドレス」アプリケーションです。有効なインターネット接続があれば、ソフトウェアは自動更新されます。中小企業環境向けに最適化する場合も、ユーザー定義のポリシーを作成したり、構成したりする必要はありません。

このホワイトペーパーに記載しているように、ユーザーが定義できるフォルダーとファイルの除外設定があり、ここではHP Wolf Pro Security Editionでマルウェアとして分類されないように、ファイルとプロセスを安全であると指定することができます。

まとめ

HPが10年以上にわたって培ってきたセキュリティのリーダーシップに基づき、HP Wolf Pro Security Editionには、複雑な攻撃に対抗する備えがあります。サイバー脅威は、会社の規模を選びません。大企業だけがサイバー攻撃の標的になっていたのは過去のことです。あらゆる種類の企業が攻撃にさらされており、中小企業（SMB）を狙う攻撃はますます増えています。

HPの調査では、中小企業のほとんどが常に攻撃にさらされながら、会社のPCを効果的に保護するためのリソースやツールを確保していない可能性があることが報告されています[3]。

HPは長年にわたってPCセキュリティ製品のリーダーシップを発揮し、デバイス、データ、およびIDを保護するセキュリティ ソリューションを提供してきました。HPが10年以上にわたって培ってきたセキュリティのリーダーシップに基づき、HP Wolf Pro Security Editionには、ますます増加する複雑なサイバー攻撃に対抗する備えがあります。

HP Wolf Pro Security Editionは、中小企業が直面すると考えられる、IT担当者の不足、セキュリティに投資できる予算の制約、サイバー攻撃への適切な対抗策を把握するリソースの不足といった課題に対応しています。

HP Wolf Pro Security Editionは、強固なITインフラストラクチャを確保する予算のない環境を標的にしたサイバー脅威に対して、高度な保護を提供します。

詳細情報：hp.com/go/computersecurity

技術情報へのリンク：support.hp.com/us-en/topic/goIT

1. HP PCのシステム要件
   a. Window 11 Pro 64、 Window 10 Pro 64、 Windows 10 EnterpriseまたはWindows 10 Enterprise LTSC（64ビットのみ）
   b. 第11世代以降のIntel® Core™ i7プロセッサ、第11世代以降のIntel® Core™ i5プロセッサ、第11世代以降のIntel® Core™ i3プロセッサ、またはAMD Ryzen以降のプロセッサ
   c. 最小8 GBのメモリ

2. 一部のSKUにはHP Wolf Pro Security Edition（HP Sure Click ProおよびHP Sure Sense Proを含む）がプリインストールされており、購入されるHP製品によっては、1年間または3年間の支払い済みライセンスが付属します。HP Wolf Pro Security Editionソフトウェアは、「HP Wolfセキュリティソフトウェア – ソフトウェア使用許諾契約書（EULA）」のライセンス条件に従って使用許諾されます。この使用許諾契約は、次の場所でご確認いただけます。https://hp-wolfsecurity.bromium-online.com/EULA/2021/eula.html?locale=ja-JP#locale=ja-JP。このEULAは、次の条項によって変更が加えられます。「7.期間このEULAに定められた条件に従って早期に終了される場合を除き、HP Wolf Pro Security Edition（HP Sure Sense ProおよびHP Sure Click Pro）のライセンスは、アクティブ化によって有効となり、12か月または36か月のライセンス期間（「最初の期間」）継続するものとします。最初の期間の終了時、（a）HP Wolf Pro Security Editionの更新ライセンスをHP.com、HP営業担当者、またはHPチャネルパートナーから購入するか、または（b）追加費用なしで、それ以降ソフトウェア更新もHPサポートも利用しないでHP Sure ClickおよびHP Sure Senseのスタンダード版の使用を続けることができます」

   HP Wolf Pro Security Editionは、 HP Manageability Integration Kitで使用可能な一部のツールセットをサポートしています。このキットは、http://www.hp.com/go/clientmanagementからダウンロードできます。

3. 出典：『2019 Verizon Data Breach Investigations Report』（2019年Verizonデータ侵害調査レポート）、『2018 State of Cybersecurity in Small & Medium Businesses』（中小企業のサイバーセキュリティに関する2018年の状況）

サインインして最新情報（英語）をご覧ください：http://hp.com/go/getupdated/

HP WOLF SECURITY

4AA7-7373JPN、2021年5月