



# HP Wolf Pro Security スタートガイド

バージョン1.0



# スタートガイド - HP Wolf Pro Security

## 目次

はじめに.....	4
対象となるお客様.....	4
クイックリンク.....	6
HP Wolf Security Controllerへのアクセス.....	6
システム要件：ハードウェアとソフトウェア.....	6
テクニカルサポートとよくある質問.....	6
サポートへのお問い合わせ.....	6
製品用語.....	7
セルフオンボーディング(初回導入時のみ).....	7
ライセンスアクティベーションのメール.....	7
オンボーディングウィザード.....	8
手順1：HPIDを使用してログインする.....	8
手順2：ライセンスの検証.....	10
手順3：テナント情報.....	11
手順4：ユーザーを追加する.....	13
手順5：登録を完了する.....	15
エージェントをインストールする.....	19
単一のデバイスにインストールする.....	19
複数のデバイスに展開する.....	22
エージェントをアンインストールする.....	22
HP Wolf Security Controllerの概要.....	24
ログイン.....	24
ライセンス.....	25
同じテナントへの新しいライセンスキーの適用.....	25
デバイスセキュリティ.....	26
(すべてのデバイス) グループとポリシー.....	28
Sure Clickポリシーの設定.....	28
ソフトウェア更新チャンネル.....	28
ユーザー資格情報の保護を有効にする.....	30
ユーザーによるWPSエンドポイント機能の制御.....	30
アイコンのオーバーレイの制御.....	31
リンクの保護.....	32



# スタートガイド - HP Wolf Pro Security

[Outlook]の添付ファイル.....	32
USBドライブの制御.....	33
リムーバブルメディアの設定.....	33
ネットワーク（UNC）ドライブの制御.....	34
SureSenseポリシーの設定.....	35
Sure Senseの有効化/無効化.....	35
ローカル除外リストの制御.....	36
ローカル隔離リストの制御.....	36
除外リストの制御.....	37
サブグループポリシーの設定.....	37
リモート コマンド.....	39
マルウェア.....	40
ユーザー資格情報の保護.....	44
イベント.....	44
アカウント.....	45
<b>リモート コマンドの説明.....</b>	<b>46</b>
<b>トラブルシューティングのヒント.....</b>	<b>48</b>
まず問題の原因となっている機能を特定する.....	48
<b>サポートのためのログバンドルを収集する.....</b>	<b>50</b>
<b>パートナー向け：複数のお客様の管理.....</b>	<b>52</b>
<b>連絡とサポートのリクエスト.....</b>	<b>53</b>
連絡.....	53
情報収集/サポート チケットの送信.....	53
一般情報の収集.....	53
その他の詳細の収集.....	54
<b>HPの脅威の封じ込めについて.....</b>	<b>56</b>
HPの脅威の封じ込め機能の解除.....	57
<b>マルウェア防止について.....</b>	<b>59</b>
<b>ユーザー資格情報の保護.....</b>	<b>59</b>
サポートされているブラウザ.....	59
保護の動作.....	59
Credential Protection拡張機能を有効にする方法.....	61
Credential Protection拡張機能を無効にする方法.....	61
HP Credential Protectionブラウザ拡張機能が有効であるかどうかを確認する方法.....	62



# スタートガイド - HP Wolf Pro Security

---

ユーザー定義のログインページの除外を管理する方法.....	62
<b>ローカルでの管理（デスクトップコンソール）.....</b>	<b>64</b>
デスクトップコンソールを起動する.....	64
デスクトップコンソールの詳細.....	66
隔離されたファイルに対する独自のワークフロー.....	Error! Bookmark not defined.
デスクトップコンソールの状態カード.....	74
脅威の封じ込め機能.....	74
マルウェア防止.....	78
認証情報保護.....	79
<b>安全な閲覧.....</b>	<b>81</b>
<b>サポートの利用.....</b>	<b>82</b>
情報の収集.....	82



# スタートガイド - HP Wolf Pro Security

## はじめに

HP Wolf Pro Security (WPS) は、3つの主要な保護機能で構成されています。サポートされるすべてのコンピューターで、3つのテクノロジーすべてを有効にすることができます。

1. 脅威の封じ込め：ハードウェアによるファイルの隔離とフルスタックの仮想マシン(VM)への封じ込め。
2. 次世代アンチウイルス：シグネチャベースおよびふるまい検知ベースの保護。AIとディープラーニングツールを利用した悪意のあるコンテンツの隔離。
3. ユーザー資格情報の保護：既知の不正サイトへの資格情報の入力ブロックされ、不明なサイトではユーザーに警告が表示される

エンドポイントのPCに対する攻撃は、メールの添付ファイル、悪意のあるWebサイト、および感染したリンクからのダウンロードを通じて最も頻繁に発生するため、脅威の封じ込めでは、隔離されたVMで信頼できないコンテンツを開き、ハードウェアで強化された仮想マシン内でマルウェアが実行されるようにします。このアプローチでは、脅威がエンドポイントに感染したり、ネットワーク上で拡散したりすることを防止できます。また、コンテンツによっては不審な動作が行われていないかを監視することもできます。ファイルが隔離されて開かれるため、未知の攻撃（ゼロデイ）の脅威でさえ封じ込められます。次世代アンチウイルスと強力な資格情報の保護機能を追加することにより、Windows PCを最先端の脅威から保護するための完全なスイートを手に入れることができます。

業界最高のセキュリティテクノロジーに加え、管理サーバーとエージェントの自動アップグレード、およびプラットフォームの整合性監視が含まれています。オンボーディングは簡単なプロセスであり、本ガイドを参照いただくことで、確実に実施することができます。

## 対象となるお客様

本ガイドは、トライアルリクエストを送信、もしくはWPS製品を購入されたお客様が対象です。お客様には、WPSの導入手順の指示が記載されたメールが届きます。

**注：正しいメールアドレスの提供が重要です。すべてのメールはそのメールアドレスに送信されます。**

トライアルリクエストを送信後、メールが届かない場合、HPパートナーもしくはHPトライアルサポート窓口 (hp-wps-trial@hp.com)にお問い合わせください。また、WPS製品を購入後、メールが届かない場合、HP販売代理店・HP営業にお問い合わせください。メールの受領後、オンボーディングセクションに進んでください。

このガイドには、最初に直面すると思われるほぼすべての質問に対する回答をご覧ください。問題が発生した場合は、HPパートナーもしくはHPトライアルサポート窓口 (hp-wps-trial@hp.com)にお問い合わせください。

このガイドの前半部分、**IT管理者およびサイバーセキュリティ管理者**を対象としています。ここでは次の内容について説明しています。

- 技術的な観点からの製品の概要
- IT管理者およびサイバーセキュリティ管理者がHP Wolf Security Controllerを操作する方法の概要
- お客様へ実施するサポートからの連絡内容



# スタートガイド - HP Wolf Pro Security

---

- サポート ポータルの概要

このガイドの後半部分では、**エンドユーザー**向けにWPSのエクスペリエンスについて説明します。

- デスクトップUI
- 正常性の状態
- システム ポップアップおよび製品の操作
- 支援のリクエストを送信する方法



# スタートガイド - HP Wolf Pro Security

---

## クイックリンク

### HP Wolf Security Controllerへのアクセス

HPIDを使用して<https://portal.hpwolf.com/>でサインインします

### システム要件：ハードウェアとソフトウェア

WPSを適切に動作させるためには、システム要件を満たしたハードウェアとソフトウェアにインストールする必要があります。詳細については、以下を参照してください。

<https://www.hp.com/jp/wps>

### テクニカルサポートとよくある質問

よくある質問については、以下を参照してください。

<https://www.hp.com/jp/wps>

### サポートへのお問い合わせ

WPS購入後の問い合わせについては、HPパートナーもしくはHPサポート窓口(電話番号：0120-566-589)にお問い合わせください。になります。



## IT管理者およびサイバーセキュリティ 管理者向け

### 製品用語

HP Wolf Pro Securityソリューションは、次の2つの主要なコンポーネントで構成されています。

- HP Wolf Security Controller : HPクラウドでホストされた管理者用の「コントローラー」であり、エンドポイントの「エージェント」を管理します。
- HP Wolf Security : 個々のエンドユーザーのコンピューターにインストールされるいくつかのソフトウェア機能で構成される「エージェント」です。
  - HP Wolf Pro Securityの保護機能
  - HP Wolf Securityの「デスクトップコンソール」: ローカルデバイスでエージェントの状態を確認したり、機能を有効/無効にしたりします。
  - HP Sure Click Pro Secure Browser : 脅威の封じ込め機能を使用してページを隔離して開くブラウザ。追加のブラウザ拡張機能とOutlook用プラグインも自動的にインストールされます

### セルフオンボーディング(初回導入時のみ)

WPSをインストールしてエンドポイントの保護を開始するためには、セルフオンボーディングを行う必要があります。

WPSの購入方法によっては、HPパートナーがこの手順を実行する場合があります。その場合は、HPパートナーに確認してください。

### ライセンスアクティベーションのメール

トライアルリクエストを送信もしくはWPSを購入した場合、お客様（またはHPパートナー）にHPからメールが届きます。このメールには、ライセンスキー、SKU情報、およびアクティベーションリンクが含まれています。



# スタートガイド - HP Wolf Pro Security

Your trial evaluation of HP Wolf Pro Security is ready



Bromium Sales Operations <salesops@bromium.com>

To

Reply Reply All Forward

Fri 4/15/2022 9:22 PM



15/04/2022

**Customer:** [REDACTED]

**Company:** [REDACTED]

**Country:** Japan

Thank you for requesting a trial of HP Wolf Pro Security.

Please click the button below to start your onboarding journey.

License Number:  
[REDACTED]

**Product:** HP Wolf Pro Security Trial      **Quantity:** 50  
**Product SKU:** HP\_WPS\_FT\_60

**Activate**

© Copyright 2021 HP Development Company, L.P.

アクティベーションリンクをクリックすると、オンボーディングが開始されます。

## オンボーディングウィザード

WPSをアクティブにするために実行する必要があるいくつかの簡単な手順があります。

### 手順1：HPIDを使用してログインする

アクティベーションリンクをクリックすると、最初にHPIDを使用してログインすることを求められます。

4. HPIDのアカウントが既にある場合は、資格情報の入力に進んでください。
5. HPIDアカウントがない場合は、以下の操作を行います。
6. ページの下部にある[サインアップ]を選択します。



# スタートガイド - HP Wolf Pro Security



HPアカウントでサインイン

接続先 :

**HP Wolf Security**

以下を使用してサインイン :

ユーザー名または電子メールアドレス

次へ

このアカウントを記憶する

ユーザー名またはパスワードをお忘れですか?

別のアカウントでサインインする :



Facebookで続行する



Googleで続行する



Microsoftで続行する

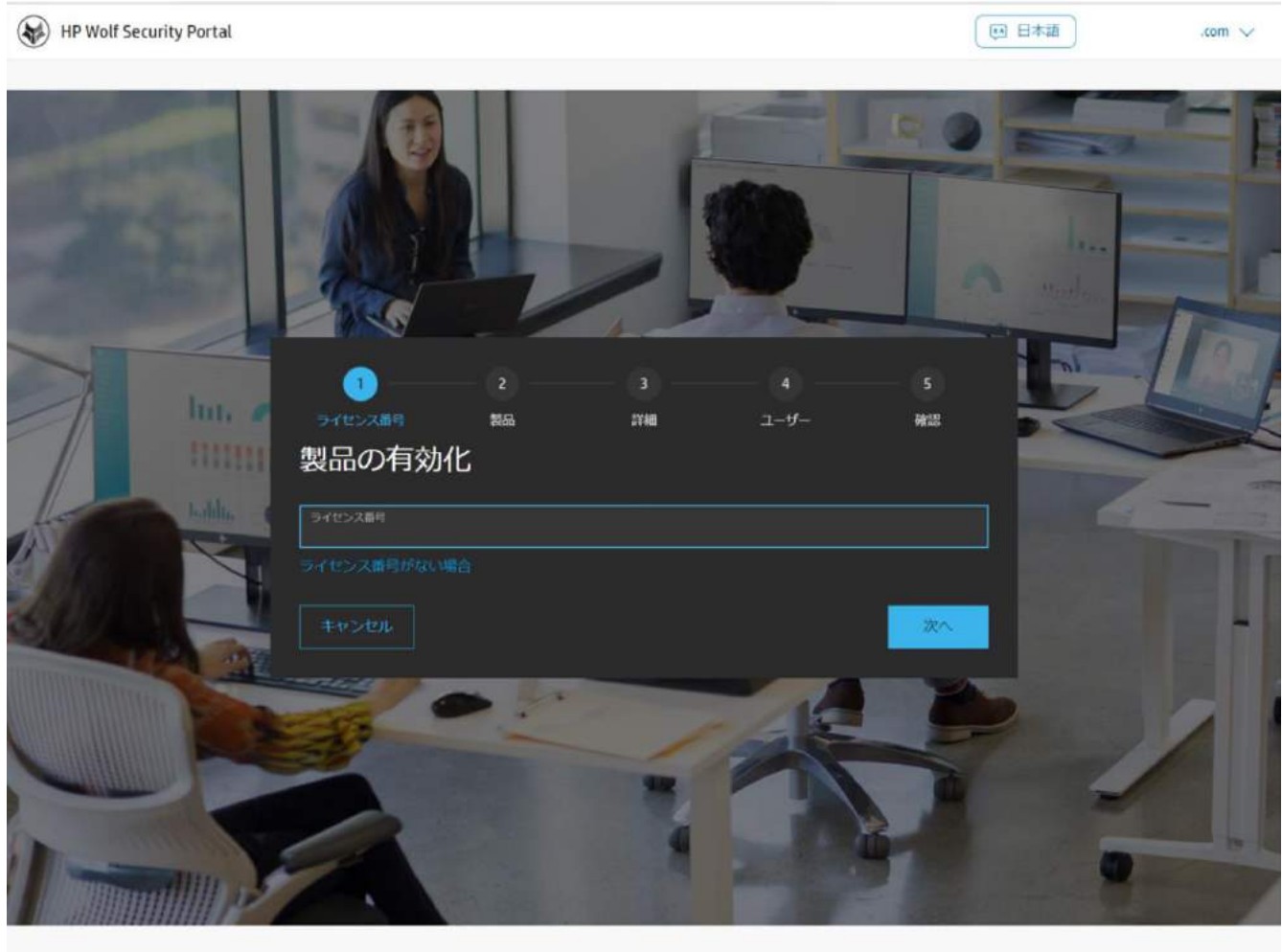
アカウントをお持ちでない場合は[サインアップ](#)

7. アカウント情報を入力して、[アカウントの作成]を選択します。
8. 2要素認証のため、入力したメールアドレスに送信されるコードを入力する必要があります。
9. アカウントが正常に作成されると、コントローラーに自動的にリダイレクトされ、次のように表示されます。



# スタートガイド - HP Wolf Pro Security

## 手順2：ライセンスの検証



© 2022 HP Inc.

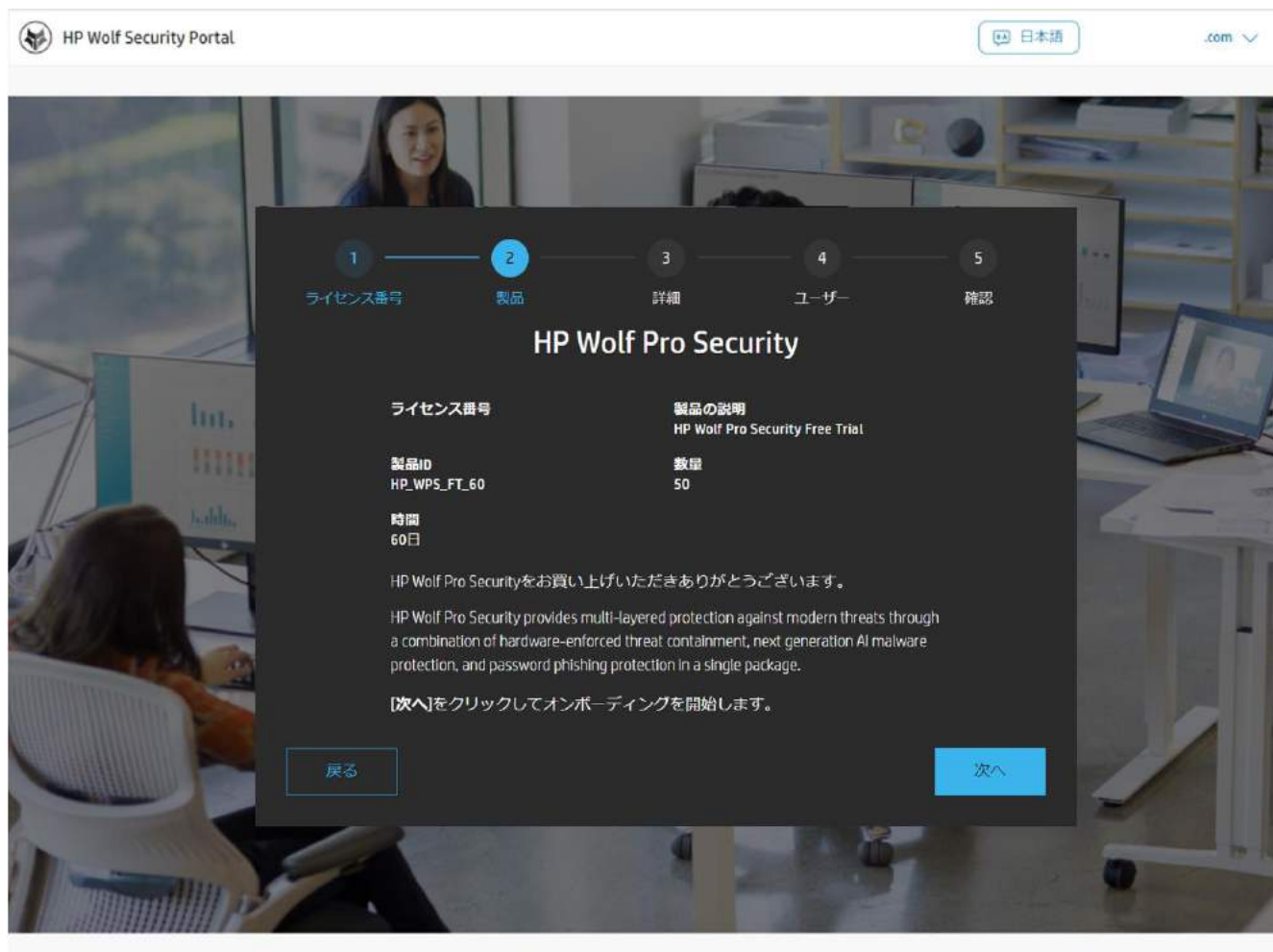
HP Wolf Security

ほとんどの場合、ライセンス番号は自動的に入力されます。入力されない場合は、メールメッセージの一部として送信されたライセンス番号をコピーして貼り付け、[次へ]をクリックしてください。

ライセンスが正常に検証されると、次の画面が表示されます。



# スタートガイド - HP Wolf Pro Security



© 2022 HP Inc.

HP Wolf Security

利用規約は必ずお読みいただき、同意してください。利用規約には、プライバシーポリシーとデータに関するよくある質問のドキュメントへのリンクも含まれています。

利用規約を受け入れないと、[次へ]ボタンを使用できません。利用規約を読んで同意したら、[次へ]ボタンをクリックしてください。

## 手順3：テナント情報

次のステップは、お客様のエンドユーザー名を入力して、データプライバシーリージョンを選択することです。これにより、HP Wolf Security Controllerにお客様専用のテナントが作成され、お客様のデータが保存される場所が決まります。プライバシーリージョンのオプションは次の2つのみです。

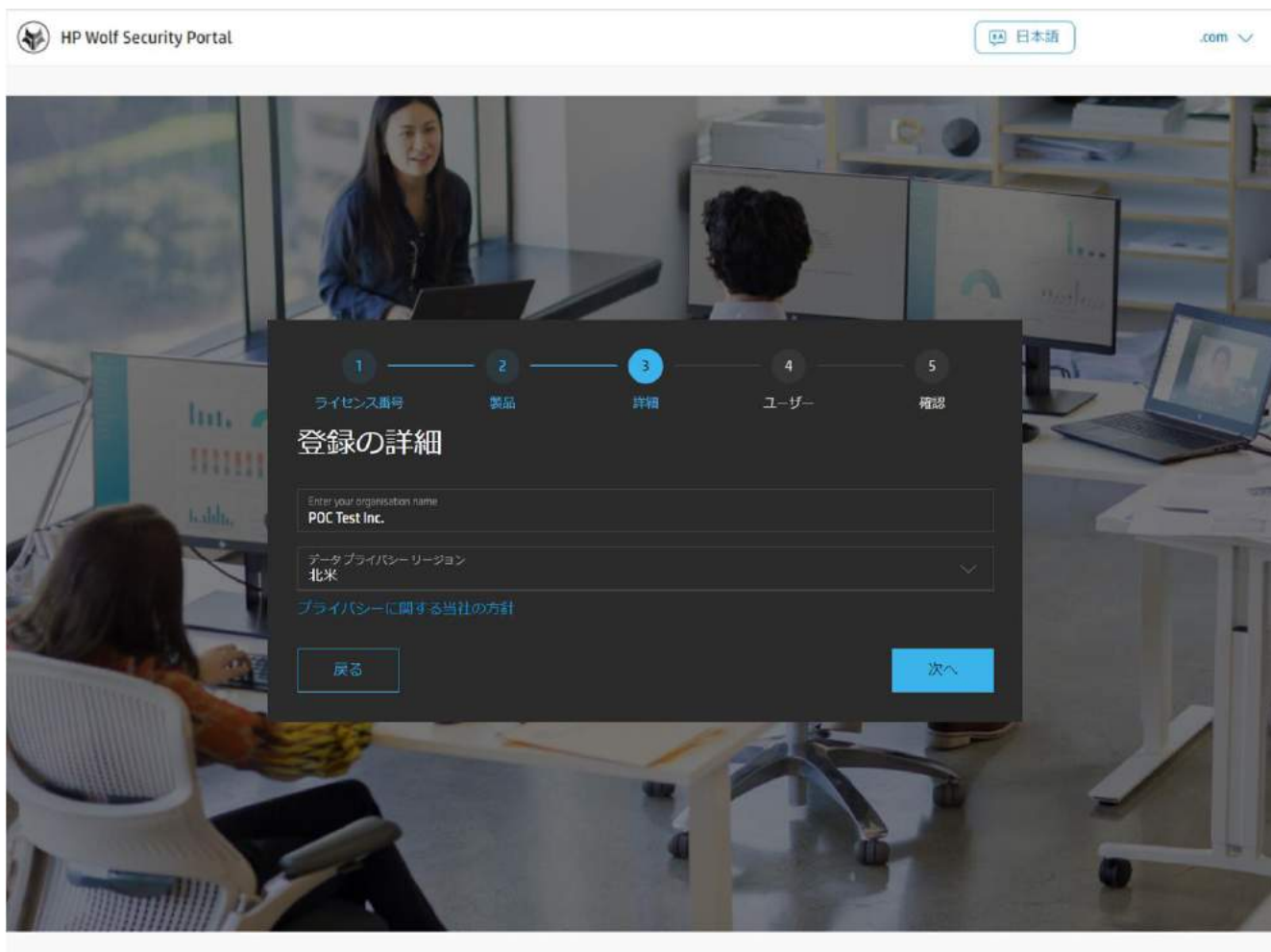
「EU」もしくは「北米」

日本の場合は、E北米を選択してください。地域やその他のプライバシー制限を満たすために、今後「日本」が選択可能になる予定です。





# スタートガイド - HP Wolf Pro Security



© 2022 HP Inc.

HP Wolf Security

## 手順4：ユーザーを追加する

オンボーディングに使用したHPIDには、作成時に初期設定のお客様管理者ロールが付与されています。必要に応じて、テナントへのアクセスを必要とするユーザーをここで追加します。現時点では、オプションは2つのみです。

**Administrator**：管理者はHP Wolf Security Controllerで変更を行うことができます。

**Read Only**：HP Wolf Security Controllerの設定とレポートの表示のみを行うことができます。



# スタートガイド - HP Wolf Pro Security

HP Wolf Security Portal

日本語 .com

1 ライセンス番号 2 製品 3 詳細 4 ユーザー 5 確認

## ユーザー アカウント

ここでは、アカウントにユーザーを追加できます。これらのユーザーは、ライセンスを管理し、デバイスおよび脅威情報の表示を行うことができます。今行わない場合でも、後でユーザーを追加できます。

Administrator .com

電子メール @hp.cc ロール Administrator

保存 キャンセル

戻る 次へ



# スタートガイド - HP Wolf Pro Security

HPパートナーが、お客様をオンボーディングしているか、お客様に代わってWPSをアクティベーションする場合は、お客様のIT管理者または同等の認可ユーザーのメールアドレスをここで入力できます。同様に、お客様がセルフオンボーディングしていて、HPパートナーにアクセス権を与える必要がある場合は、HPパートナーのメールアドレスをここで入力します。

これらの追加は後で行うこともできます。

必要なユーザーを追加したら、次のステップに進みます。

## 手順5：登録を完了する

次に、確認ページが表示されます。すべての詳細が正しいことを確認してください。必要であれば、戻って変更を加えます。それ以外の場合は、「登録の完了」ボタンを押してウィザードを終了してください。

The screenshot shows the HP Wolf Security Portal interface. At the top left is the logo and text 'HP Wolf Security Portal'. At the top right are language options '日本語' and a '.com' dropdown. The main content area features a progress bar with five steps: 1. ライセンス番号, 2. 製品, 3. 詳細, 4. ユーザー, and 5. 確認 (highlighted in blue). Below the progress bar is the title '詳細の確認' and a sub-header 'ライセンスの有効化を完了する前に、下の詳細をチェックして、正しいことを確認してください。'. The form contains the following information:

ライセンス番号	製品の説明 HP Wolf Pro Security Free Trial
数値 50	組織名 POC Test Inc.
ユーザー @hp.com (Administrator)	

変更を行うには「戻る」を押します。表示されている情報が正しい場合には、「登録の完了」をクリックします。

Buttons: [戻る](#) (Return) and [登録の完了](#) (Complete Registration)



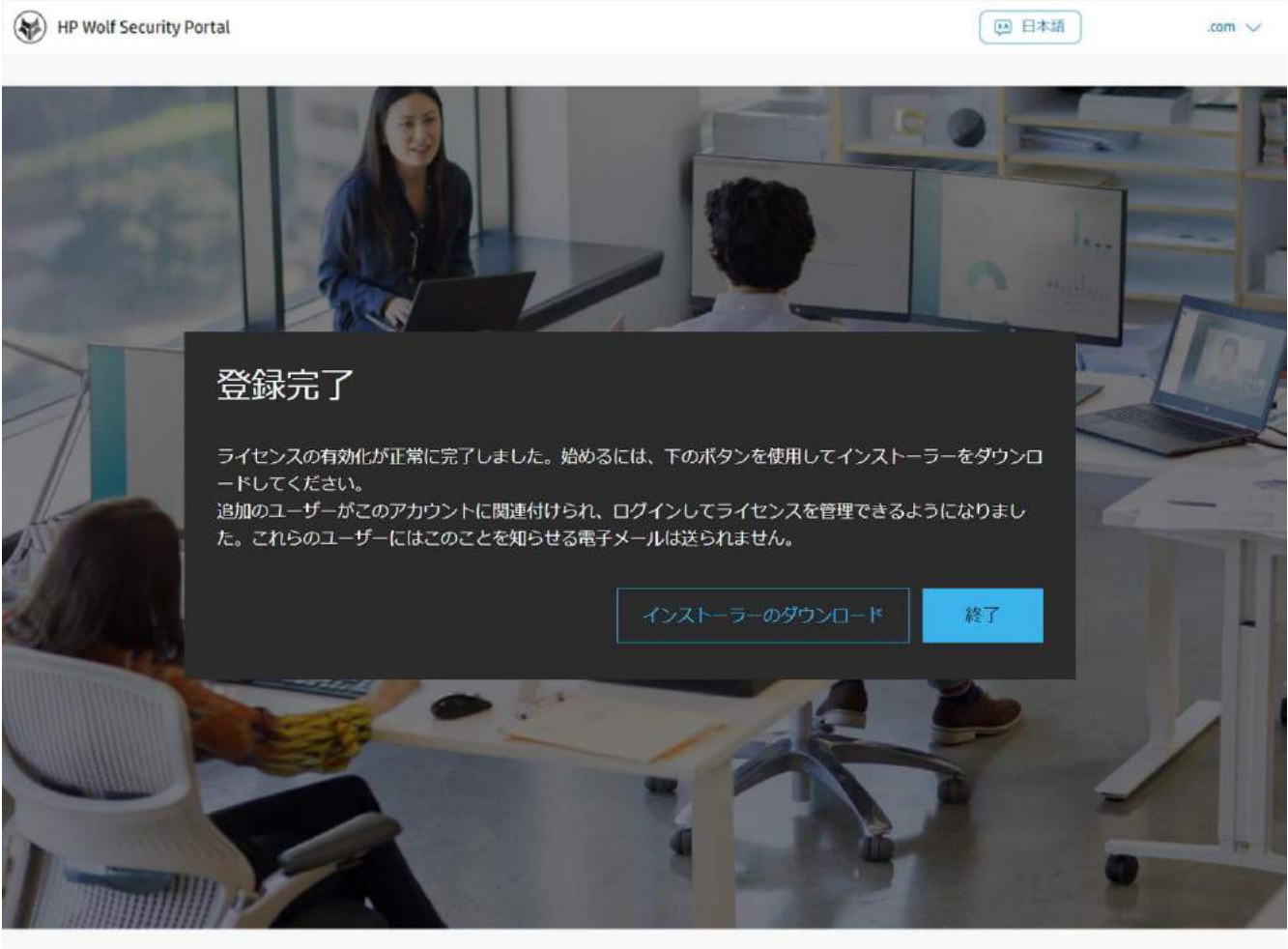
# スタートガイド - HP Wolf Pro Security

登録が完了しました。

問題がなければ「終了ボタン」をクリックしてください。

またWPSのインストーラーがダウンロード可能になります。

※ インストールには次の章で必要事項を確認した後に実施してください。



HP Wolf Security Portal

日本語 .com

## 登録完了

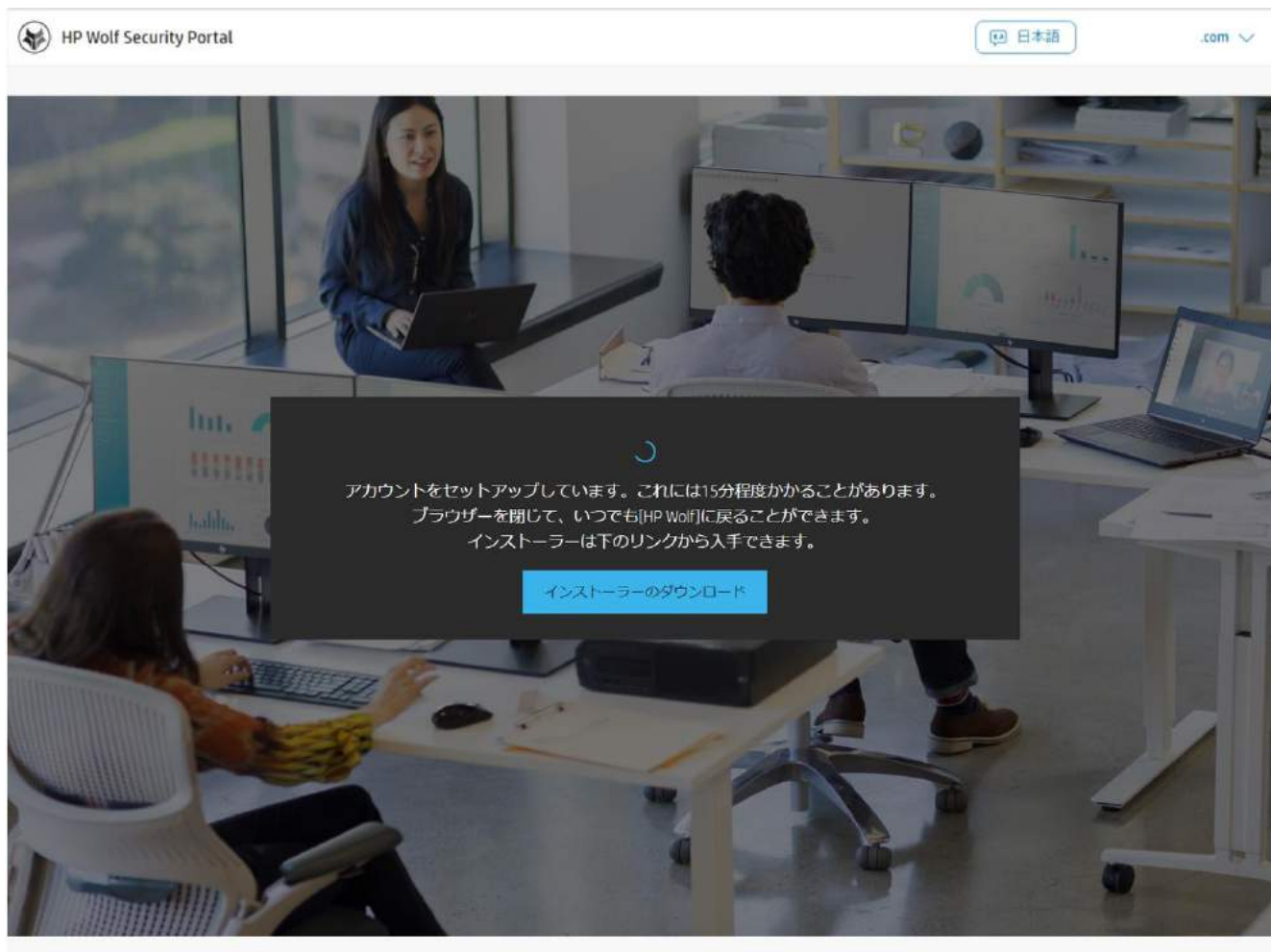
ライセンスの有効化が正常に完了しました。始めるには、下のボタンを使用してインストーラーをダウンロードしてください。

追加のユーザーがこのアカウントに関連付けられ、ログインしてライセンスを管理できるようになりました。これらのユーザーにはこのことを知らせる電子メールは送られません。

[インストーラーのダウンロード](#) [終了](#)

# スタートガイド - HP Wolf Pro Security

HP Wolf Security Controllerに、お客様のアカウント情報を含むテナントの作成が実行されています。



© 2022 HP Inc.

HP Wolf Security

テナントが作成されると、そのテナントに自動的にリダイレクトされ、次のようにコントローラーが表示されます。25シート以上のライセンスを購入した場合、または既存のテナントに対してこのライセンスをアクティベーションして合計25シート以上を割り当てた場合は、テナントの完全な管理機能が自動的にアクティベーションされ、このコントローラー画面が表示されます。



# スタートガイド - HP Wolf Pro Security

The screenshot shows the 'ライセンス ダッシュボード' (License Dashboard) in Japanese. The interface includes a sidebar with navigation options like 'ライセンス', 'デバイスセキュリティ', 'マルウェア', 'Credential Protection', 'イベント', and 'アカウント'. The main content area displays license statistics: 50 purchased, 1 allocated, 49 unused, and 0 about to expire. An activation code is provided, and there is a 'Download personalized installer' button. An 'Allocation Status' donut chart shows 100% of licenses as unused. Below this, a table lists the license details for 'HP Wolf Pro Security Free Trial'.

PRODUCT	LICENSE NUMBER	PURCHASED	USED	TERM	EXPIRY DATE
HP Wolf Pro Security Free Trial	47F62DC155AC45698A08133D38F35423	50	1	60 Days	2022-06-12

購入したライセンスが25シート未満の場合は、前のステップで登録を完了した直後に、この画面が表示されます。

The screenshot shows the 'Licenses' overview in the HP Wolf Security Portal in English. It displays a summary table with 2 purchased licenses, 0 allocated, 2 unused, and 0 about to expire. An activation code is shown, and there is a 'Download personalized installer' button. An 'Allocation' donut chart shows 100% of licenses as unused. Below this, a table lists the license details for 'HP Wolf Pro Security (L: Subscr E-ETU)'.

PRODUCT	LICENSE NUMBER	PURCHASED	USED	TERM	EXPIRY DATE
HP Wolf Pro Security (L: Subscr E-ETU)	195a08ab-d732-4af8-8d55-22fee8e5d420	2	0	365 Days	Sep 30, 2022

このコントローラーを使用すると、ライセンスとユーザー アカウントを表示および管理し、テナントに接続されているデバイスの基本的な詳細を確認できます。完全な管理機能のロックを解除するには、25シート以上をテナントに接続する必要があります。



# スタートガイド - HP Wolf Pro Security

## エージェントをインストールする

テナントの登録が完了すると、コントローラーインスタンスが作成される前に、WPSインストーラーをダウンロードできるようになります。

**WPSインストーラーは、コントローラーが完全に作成されてから実行することをおすすめします。これは、インストーラーでコントローラーから特定の製品情報とパッケージをダウンロードする必要があるためです。**

WPSインストーラーは、コントローラーにログインした際、[ライセンス]ページに表示されます。

前のステップで（コントローラー インスタンスが作成される前に）WPSインストーラーを既にダウンロードした場合は、再度ダウンロードする必要はありません。

HPSecurityUpdateServiceという名前のインストーラー（[ご使用のテナントの名前].msi）は、サイズが約2 MBであり、コンピューターにすぐにインストールされます。

実行後すぐに一連のチェックが行われ、コンピューターへのエージェントのダウンロードとインストールが開始されます。

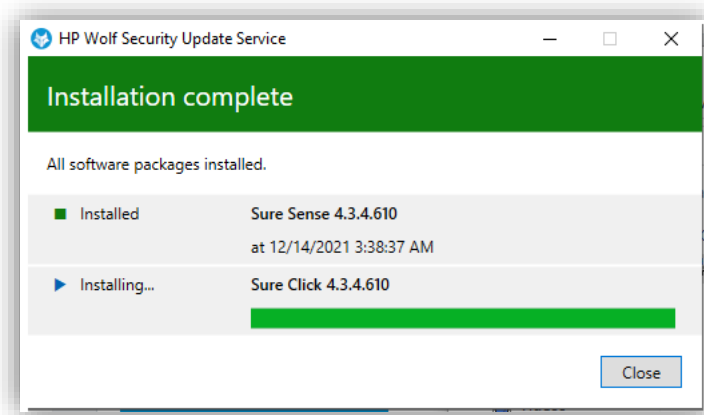
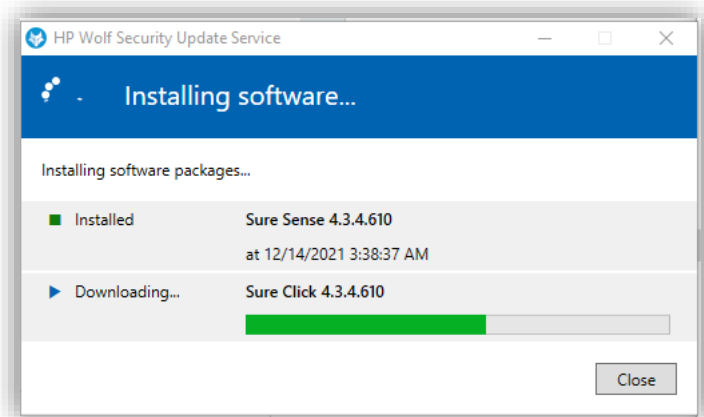
## 単一のデバイスにインストールする

- WPSインストーラーを右クリックして、[インストール]を選択します。
- **注：インストーラーは自動的に適切なクラウドテナントに接続されます。エージェントをサイレントインストールする場合を除いて、特殊なコマンドラインを使用してインストーラーを実行する必要はありません。**



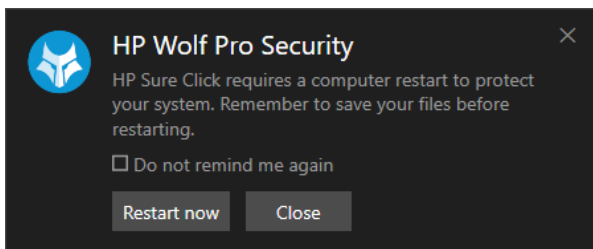
# スタートガイド - HP Wolf Pro Security

- 実行時に一般権限ユーザーである場合は、管理資格情報を入力する必要があります。
- この方法で実行すると、インストーラーは対話型になり、アプリケーションが一度に1つずつダウンロードされ、コンポーネントがインストールされることを確認できます。コンピューターの利用可能なリソースによっては、この処理に最大10分かかる場合があります。




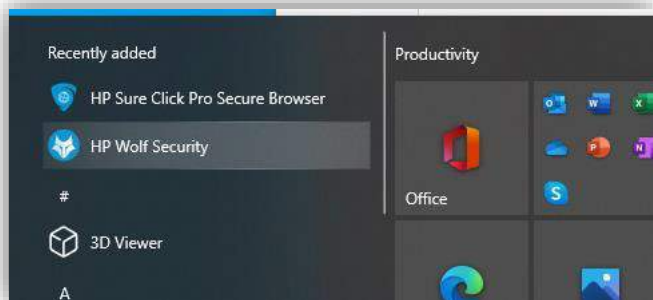
表示の右下にポップアップが表示され、インストールを完了するためにコンピューターを再起動するように求められます。

通知の[今すぐ再起動]ボタンを使用すると再起動できます。後から再起動するには、スタートトレイの隅にあるWindowsアイコンをクリックし、[電源]→[再起動]の順に選択します。([シャットダウン]を選択しないでください)

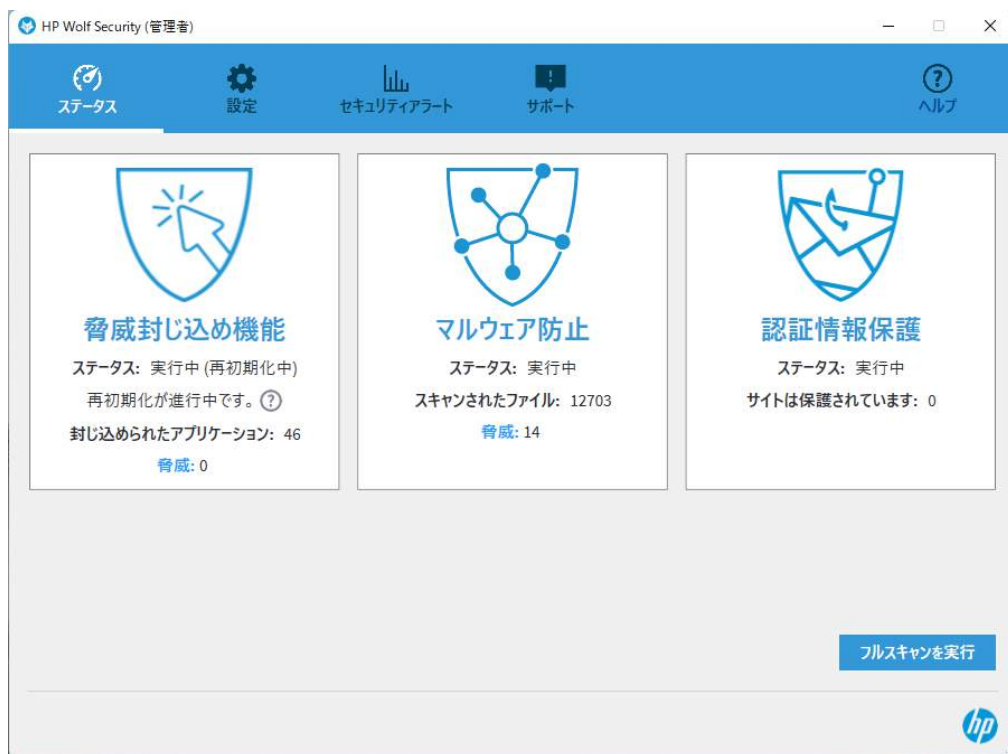


# スタートガイド - HP Wolf Pro Security

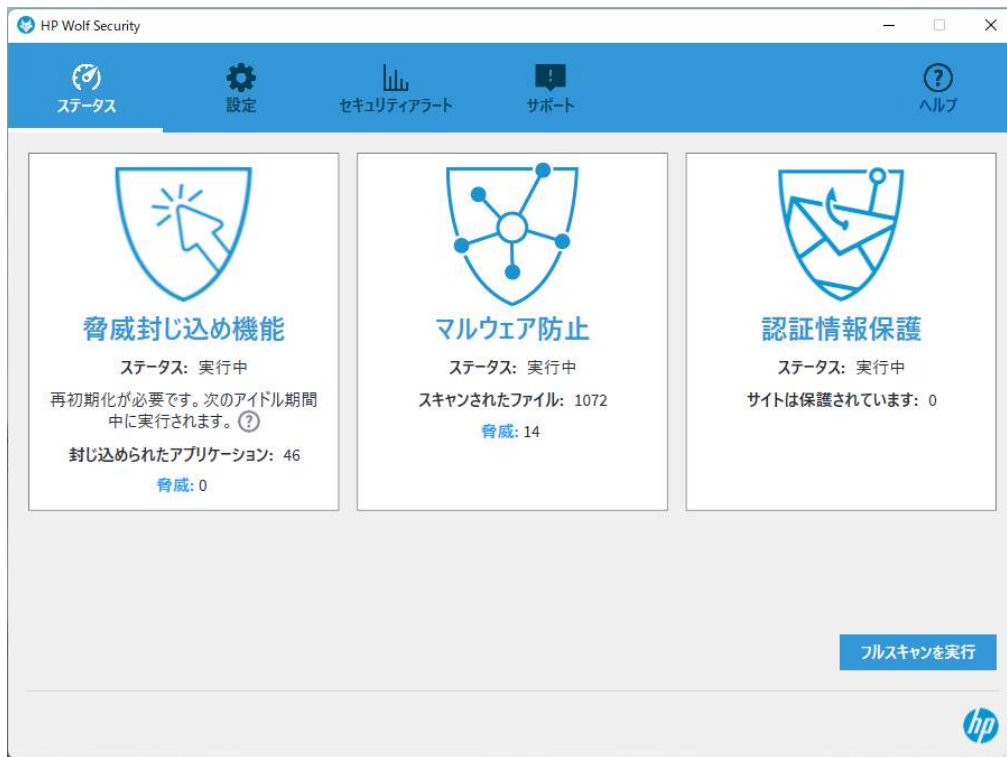
コンピューターが再起動されると、システムトレイに  HP Wolfアイコンが表示され、[スタート]メニューに新しいアプリケーションが表示されます。



エージェントによって、いくつかのハウスキーピング手順が実行されます。これには、初期セットアップ、クラウド テナントとの接続の確立、およびPC上の既存の悪意のあるコンテンツをチェックするフルスキャンの実行が含まれます。このとき、上記の「HP Wolf Security」コンソールを開くと、次のように表示されます。



# スタートガイド - HP Wolf Pro Security



## 複数のデバイスに展開する

WPSインストーラーは、SCCMやSkyseaなどのソフトウェア配布ソリューションから展開できます。GPOとファイル共有を介して簡単に展開することもできます。

WPSインストーラーはmsiパッケージであるため、サイレントインストールやファイルへのログ記録など、Msiexec.exeの標準のすべてのオプションを使用できます。

## エージェントをアンインストールする

アンインストール操作を行うと、PCからHP Wolf Pro Securityが削除されます。

**注：予期しない結果を回避するために、以下に示すすべてのコンポーネントをアンインストールする必要があります。たとえば、HP Security Update Serviceがアンインストールされていない場合、エージェントが再度ダウンロードされ、インストールされることがあります。完全にアンインストールするには、以下のすべてのコンポーネントをアンインストールしてください。**

- Windowsの[設定]で[アプリ]、[アプリと機能]を開きます。
- HP Wolf SecurityとHP Security Update Serviceの両方のアプリケーションをアンインストールします。



# スタートガイド - HP Wolf Pro Security





# スタートガイド - HP Wolf Pro Security

## HP Wolf Security Controllerの概要

**注：HP Wolf Security Controllerは、25シート以上のインストール環境でのみ使用できます。25シート未満のインストール環境の場合は、以下で説明するほとんどの機能を使用できません。**

HP Wolf Security Controllerは、セキュリティサービスを操作するためのゲートウェイです。このコントローラーはお客様専用であり、他のお客様と共有されません。これにより、本当の意味でデータが分離されます。

一部の脅威データは、監視処理およびアラート処理フローの改善のために匿名化されてから集約されますが、このデータはサービス内にとどまり、ベンダーやサードパーティと共有されることはありません。

専任のHP Wolfサポートチームが、サポート目的でお客様のコントローラーにアクセスすることがあります。

HPは、ユーザーおよび管理者のアクセスに関するISOおよびSOCのコンプライアンス標準、またはそれ以上のレベルに準拠しています。

HPのプライバシーポリシーについて詳しくは、[こちら](#)を参照してください。また、[こちら](#)（英語のみ）をクリックして、HP Wolf Pro Securityのデータに関するよくある質問を確認してください。このガイドでは、コントローラーがすでに準備されており、コントローラーにアクセスできることを前提としています。

## ログイン

コントローラーには次の場所からアクセスできます。

<https://portal.hpwolf.com/>

コントローラーに初めてログインすると、次のように表示されます。左側のメニューの一番上のオプションは、[ライセンス]ページです。

RESERVED	ALLOCATED	UNUSED	ABOUT TO EXPIRE
50	1	49	0

Activation Code: da75b681-abd9-4f07-9c32-932367e5939a

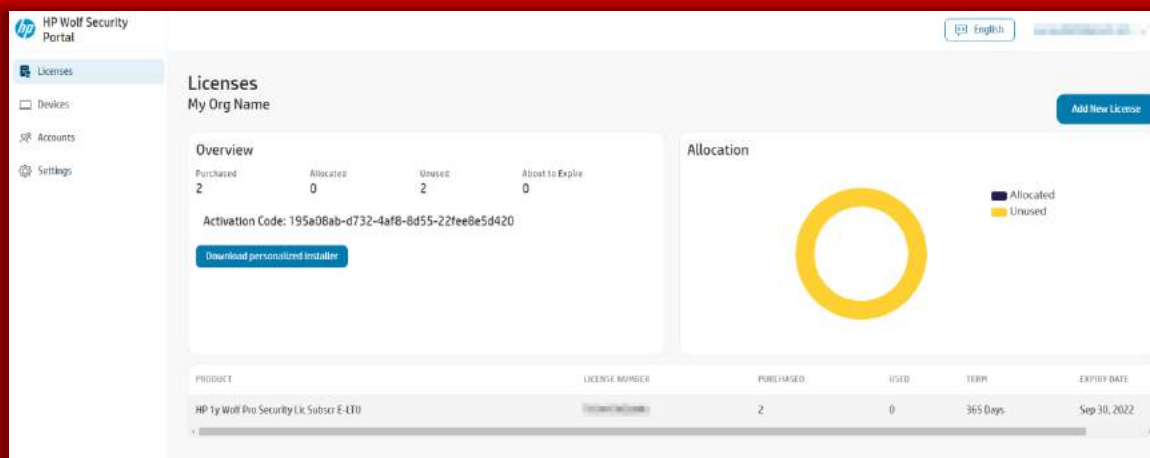
Download personalized installer

PRODUCT	LICENSE NUMBER	ALLOWED	USED	TERM	EXPIRE DATE
HP Wolf Pro Security Free Trial	47F62DC155AC45698A08133D38F35423	50	1	60 Days	2022-06-12



# スタートガイド - HP Wolf Pro Security

注：テナントへの接続が25シート未満の場合、以下の[ライセンス]および[アカウント]セクションのみがテナントに適用されます。追加のライセンス（合計25以上）を購入することで、完全な管理機能セットを有効にできます。



## ライセンス

[ライセンス]ページには、アカウントを確認するために必要なすべての管理データが含まれています。[購入済み]、[割り当て済み]、[未使用]、および[期限切れ間近]のライセンス数が上部に表示されます。

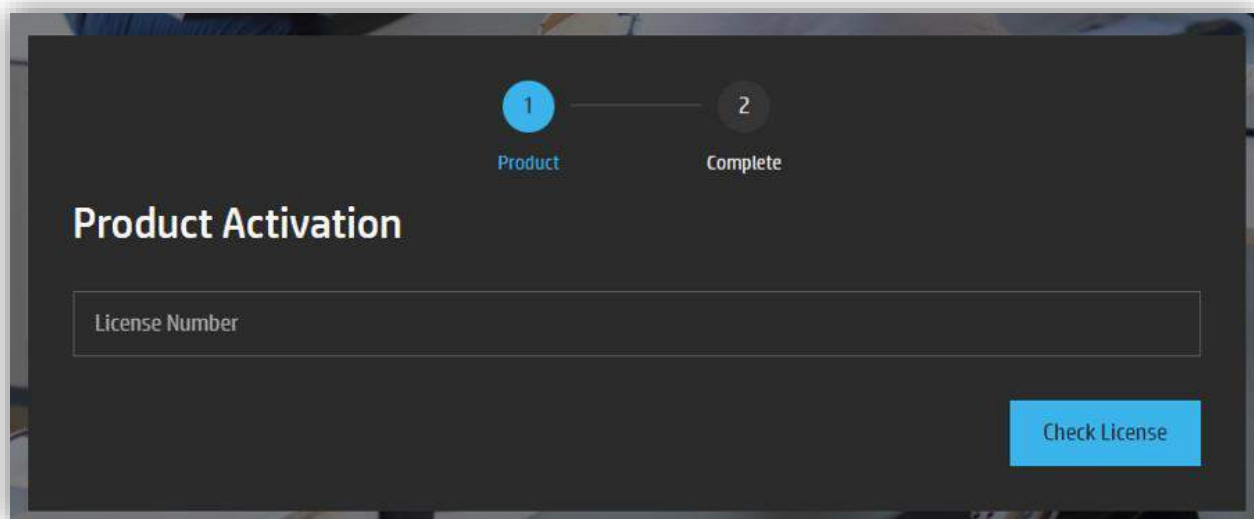
ここでは、ご使用のコントローラー固有で、他の製品やコントローラーの環境では使用できない、HP Wolf Pro Securityインストーラー (.msi) をダウンロードすることができます。インストールについては、「[エージェントにインストールする](#)」セクションをご確認ください。

[ライセンス]ページでは、ライセンス番号、ライセンスされた製品の残りの日数が表示され、新しいライセンスキーも適用することができます。

## 同じテナントへの新しいライセンスキーの適用

ページの右上隅にある[ライセンスの追加]オプションをクリックし、HPから提供されたライセンスキーを入力し、[ライセンスの確認]を選択します。

# スタートガイド - HP Wolf Pro Security



このステップが完了すると、コントローラーの[ライセンス]ページに、新しいライセンスと、追加のシート数および使用可能な期間が自動的に反映されます。

※この操作はトライアルの延長、製品版購入時に実施していただく必要があります。

## デバイスセキュリティ

このセクションは、エージェントの全体数や現在の展開状況に関連するメトリックスの追跡、または一般的な質問（「完全に保護されるデバイスの数はどれくらいですか?」、「どのデバイスを確認する必要がありますか?」など）への回答を担当するデバイス管理者またはセキュリティスペシャリストに役立ちます。

🏠 デバイスセキュリティ >

ダッシュボード

デバイス

デバイスグループ

リモートコマンド

- **ダッシュボード**には、製品を実行しているデバイスの概要が表示されます。ダッシュボードから、主要なデバイスの正常性の統計、全体的な展開の状態、およびリモートコマンドの結果を追跡できます。このダッシュボードはインタラクティブに操作でき、ダッシュボード内の関連するボックスまたは項目をクリックすると、対象の項目の詳細が表示されます。

# スタートガイド - HP Wolf Pro Security

The screenshot shows the 'デバイスのセキュリティ ダッシュボード' (Device Security Dashboard) in the HP Wolf Security Controller. The interface includes a sidebar with navigation options like 'ライセンス', 'デバイスセキュリティ', 'マルウェア', 'Credential Protection', 'イベント', and 'アカウント'. The main area displays four summary cards: '接続済み' (0, 0%), '切断済み' (3, 100%), 'オフライン' (0, 0%), and '未対応' (2, 0%). Below these is a '展開状態' (Deployment Status) chart showing 'Sure Click' at 100% green and 'Sure Sense' at 50% green and 50% red. Two empty panels at the bottom are labeled 'デバイスは注意が必要です' and 'リモートコマンド'.

- [デバイス]には、このテナントに接続されているすべてのデバイスが一覧表示されます。カスタム デバイス ビューを保存できるため、関心のある項目を保存していただければ何度も探す必要がなく、非常に使いやすいページです。このページにアクセスするときに表示する列とフィルターを設定して、[名前を付けて保存]を選択します。保存する各ビューに名前を付け、それらが何を表しているかいつでもわかるようにします。

The screenshot shows the 'デバイス' (Devices) page. It features a search bar with 'フィルターの追加' (Add Filter) and 'デバイスのグループ化' (Group Devices) options. A table header is visible with columns: 'デバイス名', '隔離ステータス', 'MALWARE PREVENTIONのステータス', '管理操作', '最後の接続', and 'グループ'. A dropdown menu is open over the table, showing '保存されたビュー' (Saved Views) with '列' (Columns) selected. Other options include '初期ビュー' (Initial View), '名前を付けて保存...' (Save with Name...), and '保存されたビューの管理' (Manage Saved Views). The table shows 3 results.



# スタートガイド - HP Wolf Pro Security

## デバイスグループ

WPSを使用すると、製品の動作を決定する特定のポリシー値を設定できます。

(すべてのデバイス)グループで**会社全体**のポリシーを作成することを強くおすすめします。このテナントにオンボーディングされる新しいデバイスには、このポリシーが自動的に適用されます。

## ポリシー

ポリシー設定と、それらがエンドポイント製品の動作にどのように影響するかを見てみましょう。

[デバイスグループ]ページの[(すべてのデバイス)]グループをクリックして開始し、[グループの構成]をクリックします。

The screenshot shows the configuration page for the '(All Devices)' group. At the top, the title is '(All Devices)'. Below it is a section titled 'グループ情報' (Group Information). Under this section, there is a '名前' (Name) field containing '(All Devices)'. Below the name field is a descriptive text: 'This built-in group contains all devices known to the controller, whether they are in other...'. At the bottom of the page, there are two tabs: 'デバイス' (Devices) and 'グループの構成' (Group Configuration), with the latter being the active tab.

Sure Clickポリシーの設定

ソフトウェア更新チャンネル

The screenshot shows the configuration page for the software update channel. The title is 'ソフトウェアの更新チャンネル' (Software Update Channel). Below the title is the instruction: 'ソフトウェアの更新のダウンロード元のチャンネルを選択してください (有効な場合) 。' (Select the channel for software updates (if applicable)). There is a dropdown menu with the selected option 'Wolf Pro Security GA [Maintained]'. At the bottom left, there is an edit icon (pencil).

# スタートガイド - HP Wolf Pro Security

エンドポイントのソフトウェアの更新に使用されるソフトウェア更新チャンネルを選択します。ほとんどの場合、これはHPがソフトウェア更新プログラムを管理するための初期設定の選択として残ります。

新しいテストまたはトライアルのビルドが必要になる場合は、最初に新しいデバイスグループを作成して、必要なデバイスをそのグループに追加し、ソフトウェアチャンネルを変更するポリシーをそのグループに割り当てることをおすすめします。詳しくは、次のセクション「カスタム デバイスグループとポリシー」を参照してください

## 信頼できるWebサイト

### 信頼できるWebサイト

このリストは、隔離なしでネイティブに開かれる特定の信頼されるWebサイトを識別します。ドメインアドレスまたはCIDR記法を入力します。ワイルドカードとして\*が使用でき、^でこのリストの例外を指定できます。

https://\*.hp.com ×

https://slack.com ×

https://\*.itmedia.jp ×

Webサイトの追加



HP Sure Click Pro Secure Browserの隔離環境ブラウザで開かないサイトをここに追加します。

内部または既知の信頼できるドメインがある場合に便利です。

ここではURLを具体的に指定してください。設定を間違えるとTLD（トップレベルドメイン）のすべてのサブドメインも保護なしで開くこととなります。

たとえば、

安全：<https://my-company-name.sharepoint.com/> 自社のシェアポイントのみを指定

安全ではない：<https://sharepoint.com/> マイクロソフト社が提供するすべてのシェアポイント



# スタートガイド - HP Wolf Pro Security

## ユーザー資格情報の保護を有効にする

### Credential Protectionを有効にする

Credential Protectionは、エンドポイントへのブラウザーの拡張を提供し、フィッシングリンクから保護します。

- オン
- オフ



これにより、資格情報の保護機能がオンまたはオフになります。これをオフにすると、エンドポイントのユーザーは自身の操作でオンに戻すことができません。

## ユーザーによるWPSエンドポイント機能の制御

### ユーザーが[HP Wolf Security]の機能を無効にすることを許可する

ユーザーが機能を無効にできるかどうかと、理由を入力するかWindowsのUACを使用するかを決定します。

- 管理者アクセス権を持つユーザーが無効にすることを許可
- ユーザーが無効にすることを許可。理由の入力が必要
- ユーザーが無効にすることを許可しない



この設定は、エンドユーザーの動作を強制して保護機能を無効化できないようにする場合、またはローカル管理者であるときにのみ機能が無効にされるようにする場合に使用します。標準のWindowsユーザーに無効化を許可することもできますが、無効化の理由を入力する必要があります。入力された理由については、以下で説明する「イベント」セクションで確認ができます。

# スタートガイド - HP Wolf Pro Security

## アイコンのオーバーレイの制御

### [HP Sure Click]によって隔離されたファイルにファイルアイコンのオーバーレイを表示する

有効にすると、信頼できないと判定されたファイルおよびドライブには、他のファイルとの違いを視覚的に示すため、HPロゴのオーバーレイが表示されます。

- オン
- オフ



WPSによってファイルが信頼できないと見なされた場合、つまり、ファイルがインターネットからダウンロードされたか、外部の送信者からのメールの添付ファイルである場合、またはその他の経路で保存されたファイルの場合、小さいWolfマークがアイコンに表示されます。これは、ファイルがWPSによって保護されており、常に隔離して開かれることをエンドユーザーに示します。



このポリシー設定により、このアイコンオーバーレイが表示されなくなります。

**注：この設定は、従業員が作業する前にファイルの保護を解除することが習慣になっている場合に便利で  
ず。WPSでは、隔離されたコンテナでドキュメントを開いているときに、ユーザーがドキュメントを編集  
してローカルに保存できるため、ほぼすべての場合にドキュメントから保護を解除する必要はありません。**



# スタートガイド - HP Wolf Pro Security

## リンクの保護

### リンクに対して保護を有効にする

有効にすると、フィッシングサイトおよびアプリケーションからのリンクは、[Secure Browser]で開かれます。

- オン
- オフ



リンクの保護は、信頼済みサイトのリストと連係して機能します。この設定をオンにすると、ユーザーの既定のブラウザの設定に関係なく、メール、チャット、またはその他のリンクのある場所からクリックされたリンクがSecure Browserで開きます。リンクが信頼済みサイトのリストに含まれている場合は、既定のブラウザで開きます。

**注：この設定は注意して使用してください。近日、マルウェアの進入経路のほとんどは悪意のあるWebサイトからダウンロードされたドキュメントであるため、通常この設定は必要ありません。この設定または信頼済みサイトのリストに関係なく、WPSではダウンロードされたファイルは常に信頼できないものと見なされます。**

## [Outlook]の添付ファイル

### [Outlook]の添付ファイル

[Microsoft Outlook]のローカルクライアントで電子メールの添付ファイルとして到着した添付ファイルの隔離を有効にします。これにより、[Sure Click Outlook]プラグインがインストールされ、有効にされます。

- オン
- オフ



この設定はMicrosoft Outlookに固有のものです。これは、[Outlook]のメールの添付ファイルとして届くファイルの隔離を有効にする場合に使用します。この設定はオンのままにすることをおすすめします。

# スタートガイド - HP Wolf Pro Security

## USBドライブの制御

### USBファイル

USBドライブからのファイルの隔離を有効にします。

- オン
- オフ



この設定では、USBデバイスを信頼するかどうかを決定します。オンのままにした場合、USBドライブから開いたファイル、またはUSBドライブからPCにコピーされたファイルは信頼できないものと見なされ、仮想環境にて隔離して開かれます。

## リムーバブルメディアの設定

### リムーバブルメディアを信頼する権限

この設定は、ユーザーがドライブを信頼できるとマークできるかどうかと、必要な認証を指定します。

- 許可されていません
- 管理者権限を持つ場合に許可
- 許可済み



この設定は、デバイス制御の代わりにはならないことに注意してください。

エンドユーザーがPCに接続されたリムーバブルメディアを信頼できるようにするものです。初期設定では、メディア上のファイルは信頼できないため、仮想環境に隔離されて開きます。より厳格なセキュリティ体制が必要な場合は、これを[許可しない]に設定するか、ローカル管理特権がある場合にのみ許可するように設定します。

# スタートガイド - HP Wolf Pro Security

## ネットワーク（UNC）ドライブの制御

### ネットワーク（UNC）の場所にあるすべてのファイルを信頼できるものとして扱う

ユーザーがネットワーク（UNC）の場所からファイルを開いたときに、初期設定で信頼できるファイルまたは信頼できないファイルとして扱うことができます。

- オン
- オフ



ネットワークフォルダからファイルを開く場合、この設定がオンになっていると、隔離して開くことができます

# スタートガイド - HP Wolf Pro Security

## Sure Senseポリシーの設定

以下のポリシー設定は、WPSの次世代アンチウイルスの部分について構成できます。

## Sure Senseの有効化/無効化

### [HP Sure Sense]を有効にする

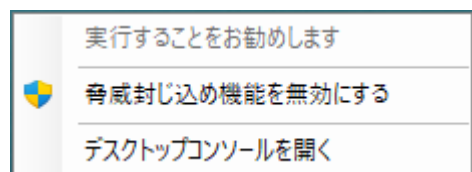
この設定は、[HP Wolf Security]で[HP Sure Sense]を有効にする方法を制御します。有効または無効にするか、ローカル管理者権限を持つユーザーがデスクトップ コンソールを使用して制御できるように設定することができます。初期設定では有効になっています

- 有効にする
- エンドポイントのローカル管理者が有効と無効を切り替えることができるようにする
- 無効にする

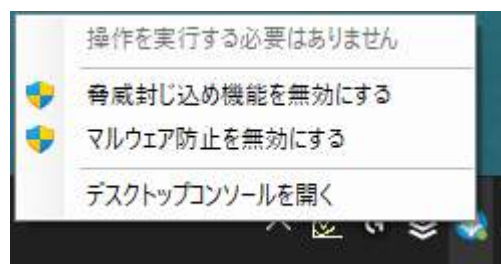


これにより、エンドポイントの次世代アンチウイルスの状態を構成することができます。このポリシーを介して**有効**または**無効**に設定した場合、エンドポイントの次世代アンチウイルス状態をユーザーが変更することはできません。

このポリシーを介して**有効**または**無効**のどちらかに設定すると、エンドポイントでマルウェア防止を有効または無効にするユーザー オプションが自動的に非表示になります。



この設定が[エンドポイントのローカル管理者が有効と無効を切り替えることができるようにする]に設定されている場合、マルウェア防御の最後のエンドポイント設定が維持され、ユーザーはそれを自由に有効または無効にすることができます。



# スタートガイド - HP Wolf Pro Security

## ローカル除外リストの制御

ユーザーがローカルの除外リストを編集することを許可する

- オン
- オフ



この設定は、ユーザーがエンドポイントで次世代アンチウイルス除外リストを編集できるかどうかを制御します。ユーザーが除外リストに含めてはならないプロセスまたはフォルダー（c:\など）を追加する可能性がある場合はオフにします。

これをオフに設定すると、ローカル デスクトップ コンソールの[設定]ページの[除外]タブが非表示になり、ユーザーは除外を設定できなくなります。

## ローカル隔離リストの制御

ユーザーが検疫からファイルを復元することを許可する

ファイルを復元すると、そのファイルがエンドポイントのローカル許可リストにも追加されることに注意してください。

- オン
- オフ



これをオフに設定すると、ユーザーはエンドポイントですでに隔離されているファイルを復元できなくなります。ファイルは隔離リストに表示されます。

# スタートガイド - HP Wolf Pro Security

## 除外リストの制御

### ファイルおよびディレクトリのパス除外リスト

スキャンから除外するファイル/パスのリスト（大文字と小文字が区別されません）。パスの最後の要素は、ファイルまたはディレクトリと完全に一致している必要があります（つまり、「c:\users\dummy」は「c:\users\dummy\_user」を除外しません）。この設定ではワイルドカードまたはグローピングはサポートされていません。

値の追加



### プロセス除外リスト

実行可能ファイルへの完全なパスのリスト（大文字と小文字が区別されません）（例："c:\program files (x86)\google\chrome\application\chrome.exe"）。ワイルドカードおよびグローピングはサポートされていません

値の追加



これにより、IT管理者はポリシーを介してファイル、フォルダー、およびプロセスの除外を追加できるため、これらはこのポリシーが適用されるグループ内のすべてのデバイスに適用されます。ここで指定されたファイル、フォルダー、またはプロセスは、次世代アンチウイルススキャンから除外されます。

## サブグループポリシーの設定

上記のセクションでは、すべてのデバイスのポリシーを構成する方法について説明しました。これは会社全体のポリシーとなります。

ただし、特定のデバイス、または選択したデバイスのグループでは、これらのポリシー設定をそれぞれ異なるものなる場合があります。

[デバイス]セクション/ページは、特定のポリシーを適用できる**デバイスグループ**を作成する場合にも利用できます。[グループの追加]を選択すると開始できます。



# スタートガイド - HP Wolf Pro Security



[グループの追加]ページでは、新しい名前とポリシーでグループを作成できます。



ポリシー値を設定しないでデバイスをグループに追加するだけの場合（たとえば、デバイスのサブセットの正常性を追跡するだけの場合）は、上のページでグループに名前を付け、グループを保存してから、グループへのデバイスの追加を開始します。

新しいグループのポリシーの設定は省略できます。

**ポリシーが設定されていない場合、グループ内のデバイスでは（すべてのデバイス）グループからポリシーが自動的に継承されます。**



# スタートガイド - HP Wolf Pro Security

グループのポリシーを設定する場合は、以下のようにスイッチを切り替えて、(すべてのデバイス)グループからオーバーライドするポリシー設定を指定し、新しい値を設定します。



その他のポリシー設定はすべて、そのままにしておくことができます。コールアウト に、新しいグループで有効にされたポリシーの数が示されます



## リモートコマンド

リモート コマンドは、このコントローラーによって発行された過去のコマンド、および現在キューに入っているコマンドがすべて表示される場所です。

HPでは、監査のために常にこのフィールドにケース番号と日付を入力します。これをビューに追加するには、[列]を選択して[理由]を選択する必要があります。

このビューは保存することもできるため、再度追加する必要はありません。リモート コマンドについて詳しくは、以下の「リモートコマンドの説明」を参照してください。





# スタートガイド - HP Wolf Pro Security

## マルウェア

マルウェア セクションは、社内のセキュリティを担当するセキュリティ アナリストまたはIT管理者に役立ちます。弊社のすべてのテクノロジーで、開いて分析できる脅威ベースのイベントが作成されます。

- **ダッシュボード**には、リスクにさらされている環境とコンピューターで検出された脅威のビューが表示されます。



マルウェア



ダッシュボード

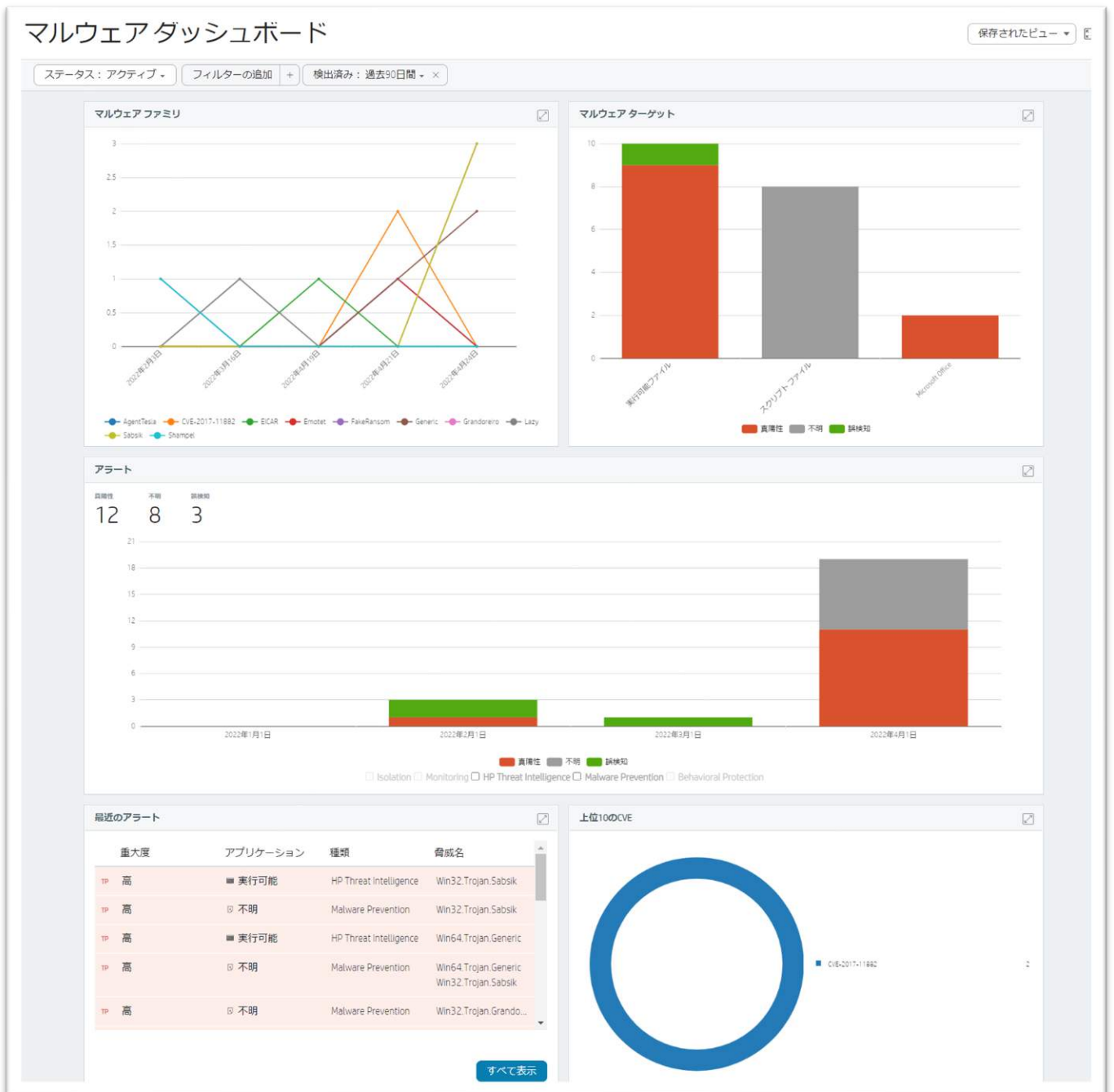
脅威

レポート

ファイルおよびハッシュ



# スタートガイド - HP Wolf Pro Security



- **[脅威]**にはリストビューが表示され、ビューを並べ替えて保存する機能があります。  
ここでは、セキュリティアナリストがイベントを確認するためにそのほとんどの時間を費やします。「調査が必要」などのラベルを作成して脅威に適用し、内部チームが対処した項目を追跡できるようにすることができます。

# スタートガイド - HP Wolf Pro Security

脅威

ハッシュの検索

分類 ラベル オプション

保存されたビュー 列

ステータス: アクティブ フィルターの追加 分類: 不明, 真陽性

78個の結果

100個のエントリの表示 1~78/78

ラベル	受信済み	検出済み	アプリケーション	種類	脅威の応答	リソース	重大度	デバイス名	ユーザー名	デバイスグループ
	2022年4月25...	2022年4月25...	■実行可能	HP Threa...	隔離済み	e73f8310406c...	高	RYZEN9	eduka	(すべてのデバイス)
	2022年4月25...	2022年4月25...	BRHOSTSVR.EXE	Malware ...	検出済み	e73f8310406c...	高	RYZEN9		(すべてのデバイス)
	2022年4月25...	2022年4月25...	■実行可能	HP Threa...	隔離済み	656a047d8aab...	高	RYZEN9	eduka	(すべてのデバイス)
	2022年4月25...	2022年4月25...	BRHOSTSVR.EXE	Malware ...	検出済み	656a047d8aab...	高	RYZEN9		(すべてのデバイス)
	2022年4月25...	2022年4月25...	EXPLORER.EXE	Malware ...	検出済み	\$R10BFHC.msi	高	RYZEN9		(すべてのデバイス)

- [脅威]はクリックして調査することもできます。イベントの発生中にこの情報を使用し、脅威をさらに詳しく調査できます。



# スタートガイド - HP Wolf Pro Security

The screenshot displays the HP Wolf Pro Security interface with the following details:

- HP Japan Demo** (top left)
- Navigation:** 概要 (Overview), グラフ (Graph), ファイル (Files), BEHAVIORAL, ネットワーク (Network)
- Threat Report Header:** THREAT REPORTER: Sure Sense; RESPONSE: Detected; 分類 (Classification): 真陽性 (True Positive); RESOURCE TYPE: .exe
- Device Information:** Device: RYZEN9; User: Unknown user
- Activity Details:** 起動元 (Origin): ユーザーによる操作 (User operation); Application: BRHOSTSVR.EXE; UUID: b9f60dd4-18ee-45d6-bc0a-b78689a3100d; Malware Prevention version: 4.3.7.346; 重大度 (Severity): 高 (High)
- Timeline:** 検出済み (Detected): 2022年4月25日 14:44; 受信済み (Received): 2022年4月25日 14:44; 更新済み (Updated): 2022年4月25日 14:44
- HP Threat Intelligence Indicators of Compromise:** Win32.Virus.Trojan\_GenericKD\_39523954; Win32.Trojan.Sabsik (1)
- Alert Timeline:** Malware Preventionが悪意のある可能性のあるファイルを検出しました (2022/04/25 14:44); Suspicious Trigger: 悪意のあるSure Senseのスキャン結果; Threat Response: Detected (2022/04/25 14:48)
- タイムライン (Timeline):** 合計時間 (Total Time): 00:12:09; 攻撃期間 (Attack Duration): 00:04:02; 実行後 (After Execution): 00:08:07
- 検疫されたリソース (Quarantined Resources):** 1 item. File: e73f8310406ceec868e8e7d3c209cda725438f73bc21bc (6f400e52c26253c825.exe) - Win32.Trojan.Sabsik
- 悪意のあるファイル (Malicious Files):** 1 item. File: e73f8310406ceec868e8e7d3c209cda725438f73bc21bc (6f400e52c26253c825.exe) - Win32.Trojan.Sabsik
- プロセスの操作のグラフ (Process Operation Graph):** (Placeholder for a graph showing process operations)
- [すべてのファイルの表示](#) (Show all files)

- 現在、レポートには環境で検出された脅威に焦点を当てたセキュリティ レポートを作成および表示する機能があります。
- ファイルとハッシュでは、コントローラーに設定されたすべてのホワイトリスト（検出の対象外）のリストが表示されます。監査のためのリストとして利用できます。



# スタートガイド - HP Wolf Pro Security

## ユーザー資格情報の保護

資格情報の保護は、インターネット上でサードパーティと作業することがあり、フィッシングのターゲットとなる可能性のあるすべての人に役立ちます。この機能により、フィッシングの試みに対し、資格情報の保護によって社内を検知されたもの、またはブロックされたものを確認できるようになります。

### Credential Protection

#### アラート

#### ドメインの分類

- **アラート**を使用すると、社内のすべての検出結果またはブロックのリスト ビューを表示できます。確認したい情報に基づいてビューを作成して保存することもできます。
- **ドメイン分類**を使用すると、誤分類されている可能性のあるサイトや、内部ポータルログインなど許可したいサイトをオーバーライドすることができます。ここで分類を変更することができます。

## イベント

このセクションは、登録されているエージェント、展開状況の正常性メトリックス跡、または特定の条件クエリを実行するのに役立ちます。

# スタートガイド - HP Wolf Pro Security

## イベント

デバイス名	重大度	ソース	メッセージ
RYZEN9	警告	Sure Click Threat	Threat recorded for 'Chrome' with resources '...
RYZEN9	警告	Untrusted Files	Malicious file C:\Users\eduka\Downloads\66c...
RYZEN9	警告	Untrusted Files	Untrusted File C:\Users\eduka\Downloads\66...
RYZEN9	情報	Sure Click Threat	The file 'C:\Users\eduka\Downloads\66c8237...
RYZEN9	警告	Sure Click Threat	Threat recorded for 'Executable' with resourc...
RYZEN9	情報	Sure Sense	Sure Sense restored file 'C:\Users\eduka\Dow...
RYZEN9	情報	Sure Click Threat	The file 'C:\Users\eduka\Downloads\66c8237...
RYZEN9	警告	Sure Click Threat	Threat recorded for 'Unknown' with resource...

## アカウント

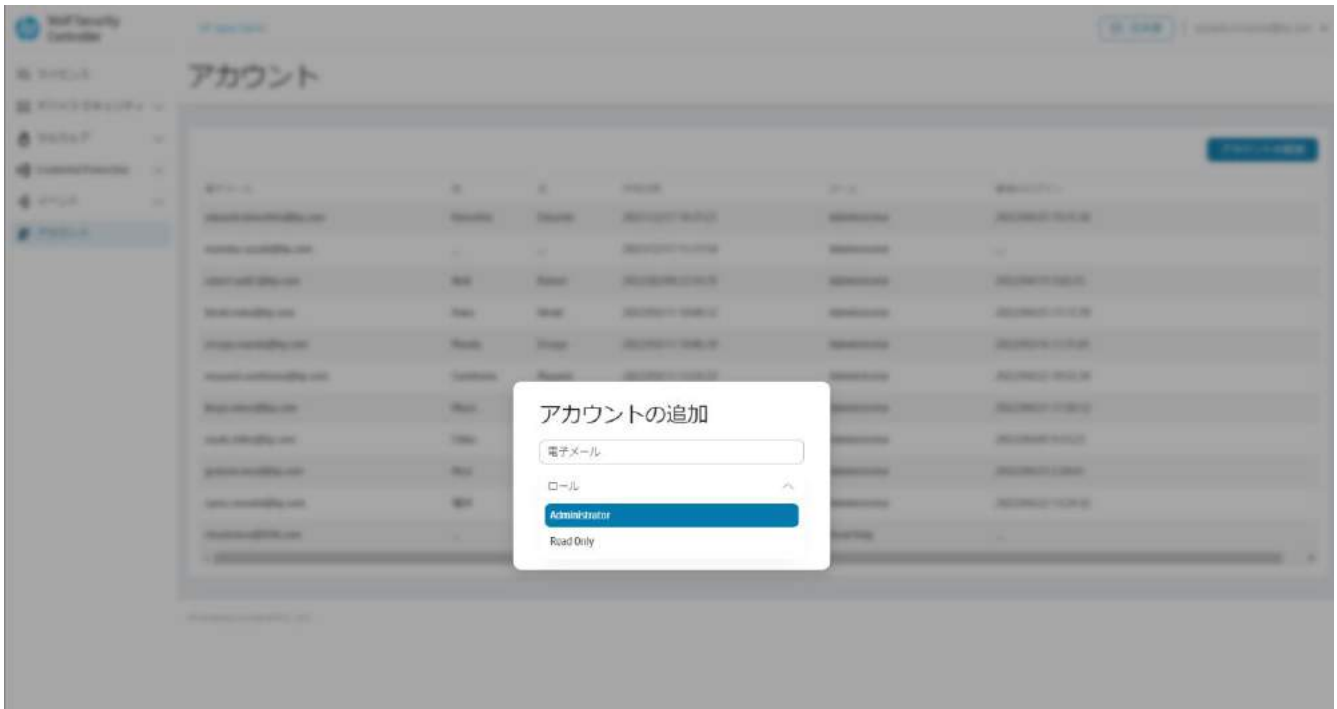
コントローラーを最初にセットアップするとき（HPまたはパートナーがお客様に代わってこれを開始する場合があります）に、ユーザーを追加するオプションが表示されます。「Administrator」のアクセス権がある場合は、いつでもユーザーを追加できます。[アカウント]ページに移動して、[アカウントの追加]を選択するだけです。新しいユーザー登録にメールアドレスを入力し、許可するアクセスのレベルを指定します。

割り当てることができるアクセスのレベルは2つあります。

Administrator : 管理者はControllerで変更を加えることができます。

Read Only : Controllerの設定とレポートの表示のみを行うことができます。

# スタートガイド - HP Wolf Pro Security



## リモート コマンドの説明

リモート コマンドは、展開されたエージェントコンピューターをコントローラーから管理するための1つの方法です。

リモート管理オプションは、ドロップダウンを選択するだけで、コマンドを見つけることができます。

コンピューターの管理に使用するリモート コマンドの概要を次に示します。

# スタートガイド - HP Wolf Pro Security



- **隔離の再開**：「脅威の封じ込め」固有のものであり、このコマンドにより、エージェントコンピューター上のWPSソフトウェアを再起動し不具合を解消できる場合があります。このコマンドを選択することはほとんどありません。
- **隔離の再初期化**：「脅威の封じ込め」固有のもので、これは、問題のあるデバイスで最初のトラブルシューティング手順として実行する必要があります。
- **再起動**：**警告!** このコマンドによって、エンドユーザーのコンピューターは警告なしにWindowsが強制再起動されるため、そのデバイス上で保存されていない作業内容は失われます。ユーザーは再起動を回避または遅延させることはできません。
- **隔離を無効にする**：エージェントコンピューターのデスクトップ コンソールから行う操作と同様にリモートコマンドで実行できます。通常はトラブルシューティングの目的で脅威の封じ込め機能を無効にします。
- **隔離を有効にする**：無効の逆です。エージェントコンピューターのデスクトップ コンソールでも実行できます。
- **隔離ログのクリア**：特定の問題に関するトラブルシューティング セッションを開始する前に実行するようサポートから求められることがあります。
- **デバイスから隔離ログを収集する**：エージェント ログがコントローラーにアップロードされ、後ほどサポートにより分析されます。
- **キューに入れられたコマンドのキャンセル**：大規模なエージェントコンピューターに対してリモートコマンドを発行し、途中で元のコマンドを終了したい場合に役立ちます。



# スタートガイド - HP Wolf Pro Security

## トラブルシューティングのヒント

エンドユーザーによる問題のトラブルシューティングを支援するために、IT管理者として実行できる一連の手順を以下に示します。

### まず問題の原因となっている機能を特定する

製品の問題箇所は、通常、簡単に特定することができます。以下のフローに従って問題を特定し、必要に応じてサポートをリクエストする準備をしてください。

Officeやその他ドキュメントをVMで開くときに問題が発生した場合、ほとんどの場合は「再初期化」することで解決することができます。それでも解決しない場合は、最初の切り分けとしては「脅威の封じ込め」機能を無効化してみてください。

### 脅威の封じ込めのトリアージフロー

脅威の封じ込めを無効にします。

これにより問題が解決しましたか?

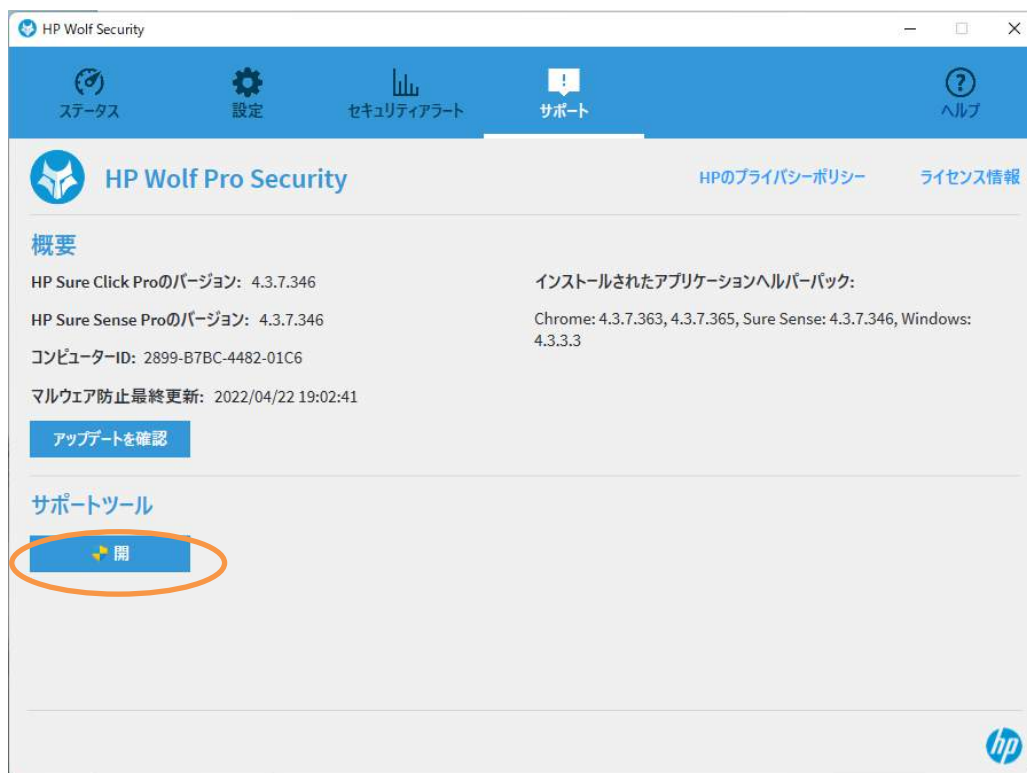
「はい」の場合は、修正できるかどうか確認してみましょう。以下の手順に進みます。

「いいえ」の場合は、マルウェア防御のトリアージフローにスキップします

脅威の封じ込めを有効にします

コンピューターを再起動します

再起動後、Wolfデスクトップコンソールを開き、再初期化します



# スタートガイド - HP Wolf Pro Security



## マルウェア防御のトリアージフロー

「マルウェア防止」機能を無効にします これにより問題が解決しましたか？

「はい」の場合は、修正できるかどうか確認してみましょう。以下の手順に進みます。

「いいえ」の場合は、弊社の製品に問題がないか、問題を解決するためにカスタマー サポート ケースを作成する必要があります。

「マルウェア防止」機能を無効のままにして、サードパーティのアンチウィルス ソリューションなど、競合する製品が除外されるように設定を追加します。必要な除外を適用した後、コンピューターを再起動してください。



# スタートガイド - HP Wolf Pro Security

## サポートのためのログバンドルを収集する

サポートでケースを開始する場合、問題のデバイスからのログの準備をしておくことを推奨します。メールのリクエストに添付する形でも送付することもできます。

- ログを生成するには、コントローラーからリモート コマンドを使用して要求するか、エンド ユーザーの都合のよいときにご自身で操作をして送信してもらいます。

The screenshot shows the HP Wolf Pro Security management console interface. The top navigation bar includes 'ステータス' (Status), '設定' (Settings), 'セキュリティアラート' (Security Alerts), 'サポート' (Support), and 'ヘルプ' (Help). The main content area is titled 'HP Wolf Pro Security' and includes sections for '概要' (Overview) and 'サポートツール' (Support Tools). The 'サポート' tab is active, showing a 'レポートを送信...' (Send Report...) button circled in orange. A dialog box titled 'レポートを送信' (Send Report) is open, containing a consent message and a text input field for additional information. The 'レポートを送信' (Send Report) button in the dialog is also circled in orange.

- アップロードされたログは、コントローラーの[デバイス情報]ページで表示できます。

# スタートガイド - HP Wolf Pro Security

ライセンス RYZEN9 (All Devices)

シリアル番号: 732c78c9y 6LJK HPユーザーID: 228-873E-492-0163 HP管理コード: 84M8M5

Device Groups リモート管理

### License Information

ステータス	Learned	License Number	E1AF29EFA35447A548596600D1595714
Expiry Date	2022年5月9日	製品	HP Wolf Pro Security, Free Trial

Block device

### デバイスのセキュリティのステータス

Windows 10/11 x64 (HP Pro Securityサービス) のSure Click 4.3.7.346 (アクティブ)	強弱	無効済み
Windows 10/11 x64のSure Click support for Chrome 4.3.7.365	最後の接続	2022年4月25日 20:43
Windows 10/11 x64のSure Click support for Windows (upcoming) 4.3.3.3	最後の取得	2022年4月25日 0:27 (最新)
Windows 10/11 x64のSure Sense 4.3.7.346	IP	192.168.1.31.2
Windows 10/11 x64 (アクティブ) のSecurity Update Service 4.3.7.346	IP	192.168.1.31.2

### 管理操作

このデバイスの管理操作が存在していません。

検索 検索 Credential Protectionのアラート イベント ユーザー リモートコマンド **アップロードされたファイル** プロバティ 送信されたファイル

1 件の結果

ファイルの種類	ステータス	実行状況	開始時刻	メッセージ
ユーザーがアップロードした診断	● アップロード済み	アップロードが完了しました	ファイル	2022年4月25日 22:00 助けてー

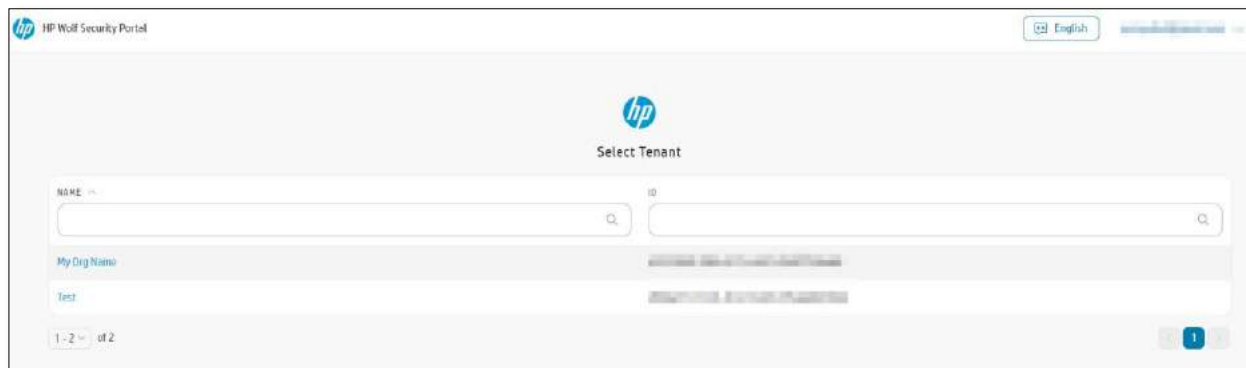


## HPパートナー向け：複数のお客様の管理

HPパートナーは、基本のパートナー コンソールを使用して複数のお客様を管理することができます。このパートナー ビューを有効にするには、パートナー担当者のメール アドレス（またはお客様支援の担当となったユーザーのメール アドレス）が複数のお客様のテナントに管理者ユーザーとして追加されている必要があります。

お客様A	お客様B
<div><h3>アカウントの追加</h3><p>電子メール support@partne.com</p><p>ロール Administrator</p><p>保存    キャンセル</p></div>	<div><h3>アカウントの追加</h3><p>電子メール support@partne.com</p><p>ロール Administrator</p><p>保存    キャンセル</p></div>

同じHPIDアカウントに2つの別々のテナントへのアクセスが許可されている場合は、そのHPIDでログインすると次のように表示されます。



これにより、HPパートナーはこのページを使用してお客様コントローラーにシングル サインオンすることができます。パートナー様が多数のお客様を管理している場合は、名前やIDによる検索などの基本機能を使用できます。

# スタートガイド - HP Wolf Pro Security

## サポートと連絡

### サポート

- サービス展開のトライアルフェーズの場合は、HPパートナーもしくはHPトライアルサポート窓口 (hp\_wps\_trial@hp.com)にお問い合わせください。
- サービスのトライアルフェーズが終了しWPSを購入いただいたお客様の場合は、HPパートナーもしくはHPサポート窓口(電話番号：0120-566-589)にお問い合わせください。

### 連絡

HPでは以下のような場合にお客様に連絡します。

- WPSのアップグレードがスケジュールされたときに送信する通知。

### 情報収集

HPパートナーもしくはHPサポート窓口のサポートにお問い合わせをする際、以下の情報を提供してください。

### お客様情報の収集

利用者個人および組織に関する情報を収集していただけますようお願いいたします。

以下の情報を必ず提供してください。

- お客様のお名前
- お客様のメールアドレス
- お客様の連絡先電話番号
- お客様の所在地とタイムゾーン
- お客様のHP担当者またはパートナー担当者情報

### 一般情報の収集

報告されている問題や実行可能な解決策を説明するために、いくつかの情報が必要になります。

以下の情報を必ず提供してください。

- デバイス名
- 問題の概要
- 推奨される解決策の概要、必要とする支援内容
- 影響を受けるユーザー数
- 問題は一貫して再現可能か



# スタートガイド - HP Wolf Pro Security

## その他の詳細の収集

可能であれば以下の質問をご確認ください。(省略可能ですが有益な情報です)。

- ファイルは隔離されましたか?
  - このサイトは自動的に信頼できますか？理由は何ですか？
  - 問題の解決に役立つエラー メッセージはありますか？
  - HP Wolf Pro Security デスクトップ コンソールのスクリーンショット
    - [ステータス] ページ
    - [サポート] ページ
- パフォーマンスが低下しましたか?
  - 問題が発生しているときのデスクトップのスクリーンショット
  - タスク マネージャーの[プロセス] タブのスクリーンショット
  - HP Wolf Pro Security デスクトップ コンソールのスクリーンショット
    - [ステータス] ページ
    - [サポート] ページ
- 想定される解決策を提案できますか？
- どのような支援が必要ですか？
  - ファイルのブロックを解除する必要がありますか？
  - サイトを信頼されたサイトにする必要がありますか？
  - パフォーマンスの問題をトラブルシューティングするためにエージェントを無効にする必要がありますか？
- デバイスのシリアル番号を教えてください？
- ログオンしたユーザー名を教えてください？
- お客様はこれまでにどのようなテスト/トラブルシューティングを実行しましたか？
- この問題の優先度はクリティカル、高、中、低のどれでしょうか？  
**注：**これは、問題解決のためのサービス レベル目標 (SLO) を示すものではなく、どのようにチケットに回答すべきかを判断するための簡単な指標になります。

# スタートガイド - HP Wolf Pro Security

---

HP Wolf Pro Securityでは、年に最低2回のエージェントアップグレードがあります。

- エージェントアップグレード：毎年最低2回のエージェントアップグレードがあります。通常Microsoft社のOSリリースカレンダーと前後する時期にあたります。これらのアップグレードはコントローラーからリモートで実行されるため、利用者は何も行う必要はありません。弊社からQAおよび本番リリースのスケジュールをお知らせします。問題がある場合は、詳細を記載したメールを送信してください。また、弊社で問題を確認した場合、チケットを新規に作成し、お客様に連絡することがあります。これは、問題の解決を支援し、確認している問題についてフィードバックを提供していただくためです。問題が発生した場合は、アップグレードが遅れることがあります。





## ユーザー向け

このセクションは、HP Wolf Pro Securityのエンドユーザーを対象としています。ただし、問題のトリアージとエンドユーザーの懸念事項への対処を向上させるために、IT管理者にもこのセクションをご覧くださいことをおすすめします。

## HPの脅威の封じ込めについて

HPの「脅威の封じ込め」では、組織外の信頼できないソースからダウンロードされたファイル内にある潜在的に悪意のあるコンテンツを隔離することにより、ユーザーを保護します。

IT部門は、ファイルをダウンロードして良いサイトを**信頼できる**サイトとして定義しています。通常、組織内のファイル共有サイトや会社のWebアプリは、信頼できるダウンロードソースとして設定します。これらの信頼できるサイトからダウンロードされたファイルはこれまでと同じように開くことができます。

内部サイト、Webアプリ、およびメール アドレスを信頼できるものとして確認するプロセスは、ホワイトリストの作成と呼ばれます。

IT部門は、添付ファイルの信頼できるソースとして内部メール アドレスも定義しています。内部で作成されたファイル、信頼できるサイトからダウンロードされたファイルは組織内の同僚へメールに添付して送付できます。これらの信頼されたファイルは通常通りに開きます。

他の場所からダウンロードされたファイルやメールの添付ファイルは信頼できません。メールで受信した、信頼できないMicrosoft Word、Excel、PowerPoint、Adobe Acrobat Readerファイルでも、安全に開いて表示、編集、印刷、保存を行うことができます。HPの「脅威の封じ込め」機能では、信頼できないファイルからの悪意のある挙動を自動的に隔離します。

そのため、HPの「脅威の封じ込め」機能では、悪意がある可能性のあるファイルからコンピューターを保護します。

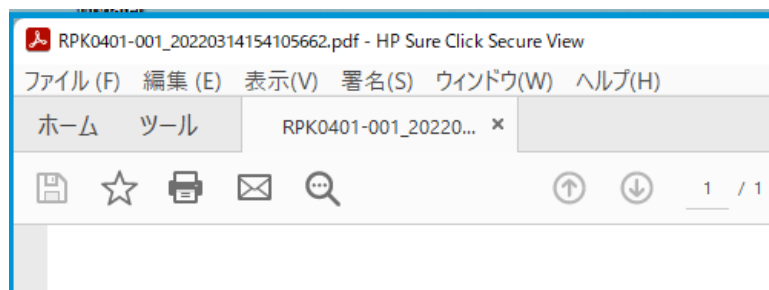
- インターネットからダウンロードされた、またはメールから保存されたファイルは、信頼できないファイルとしてマークされます。
- 信頼できないファイルは隔離され、「脅威の封じ込め」機能の中で開かれます。
- 隔離されたファイルであっても完全に表示、保存、コピー、編集、共有することができます。

信頼できないファイルを保存すると、そのファイルは信頼できないとマークされます。Wolf Pro Securityを使用している組織内のユーザーにこのファイルを送信すると、信頼できないマーク維持されたまま共有されます。

開くファイルがHPの「脅威の封じ込め」機能によって保護されているかどうかを確認するには、アプリケーション ウィンドウの上部にあるタイトル バーで[HP Sure Click Secure View]という単語が表示されていることを確認してください。この状態であれば、最も安全な方法でファイルを操作していることを示しています。



# スタートガイド - HP Wolf Pro Security



信頼されないと判断されたWebサイトまたはメール アドレスが信頼できると思われる場合は、IT部門に該当するサイトまたはメール アドレスの信頼性確認を依頼してください。IT部門はビジネスの要求を承認すると、該当サイトまたはメールを信頼される設定に追加します。

## HPの脅威の封じ込め機能の解除

インターネットから悪意のあるファイルがダウンロードされると、ほとんどの場合、デバイスが侵害されます。HPの「脅威の封じ込め」機能では、信頼できないサイトやファイルを仮想環境内で開くことにより、デバイスが侵害されないようにします。

信頼できるサイトをホワイトリストに登録理由を以下に示します。

- ユーザーのワークフローを簡素化する
- Webベースアプリケーション認証のサポート
- 安全なサイトが繰り返し仮想環境に隔離されることを回避する

また、ファイルがHPの「脅威の封じ込め」機能によって保護されている場合、MS OfficeまたはAdobe Acrobat Readerの一部の機能が利用できません。たとえば、ExcelのアドインやPowerPointの発表者ツールが無効になります。業務上の正当な理由があり、ファイルが悪意のないものである場合は、「脅威の封じ込め」機能の保護をファイルから解除できます。

ほとんどの場合、IT部門に連絡して、Webサイトとメール アドレスをホワイトリストに登録することにより、保護を対象から外す必要があります。ただし、必要に応じて「脅威の封じ込め」機能を個々のファイルから手動で解除して、ファイルを信頼済みにすることができます。

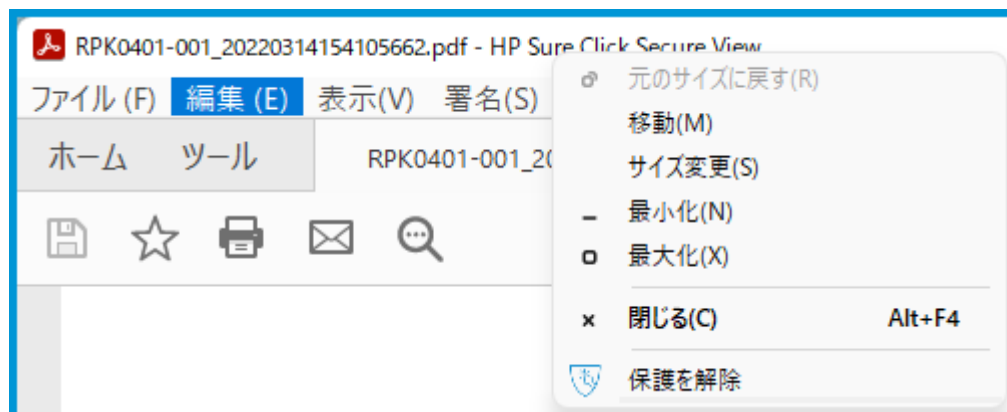
**注：ファイルから封じ込め保護を解除すると、コントローラーに通知が送信されます**

保護を解除するには、次の2つの方法があります。

- 「脅威の封じ込め」機能内でファイルが開いている場合は、アプリケーションの上部にあるHP Sure Click Pro Secure Viewを右クリックします。次に、**[保護の解除]**をクリックします。



# スタートガイド - HP Wolf Pro Security



- エクスプローラーでファイルを右クリックし、[保護の解除]を選択します。



「保護の解除」が実行される前に、ファイルがHPの「脅威の封じ込め」機能によってファイル自体が分析されます悪意があるファイルか確認します。安全が確認され、保護が解除されたファイルは、その時点からMS OfficeまたはAdobe Acrobat Readerで保護なしで開かれます。一度信頼されたファイルを保存して再度開いても、ファイルは信頼されたままです。

ファイルが組織外の信頼できない相手からメールで送られてきた場合、そのファイルは自動的に信頼できない状態にリセットされます。

HPの「脅威の封じ込め」機能によってMS Office、Adobe Acrobat Reader、または実行可能な.EXEファイルで疑わしいコンテンツが検出された場合、そのファイルは信頼されず、安全に閉じることができます。

追加の支援が必要な場合は、IT部門に連絡して指示を受けてください。

# スタートガイド - HP Wolf Pro Security

## マルウェア防止について

HP Wolf Pro Securityソフトウェアのマルウェア防御機能は、これまで使用してきた従来のアンチウイルスソフトウェアのようなものです。これは常に稼働しており、何かを検出すると、それを隔離してブロックします。会社のポリシーによっては、追加のサポートの支援を受けなくても隔離から項目を解放できる場合があります。

隔離されている項目を表示するには、システムトレイからデスクトップコンソールを開いて、[セキュリティアラート]ページを表示します。

ポリシーで許可されており、トラブルシューティングに必要な場合は、マルウェア防止を無効にすることもできます。これは、再び有効にするまで無効のままになります。

## ユーザー資格情報の保護

ユーザー資格情報の保護は、以下では認証情報保護とも呼ばれ、ユーザーが既知の不正なWebサイトにパスワードを入力するのを防ぎ、フィッシングサイトをユーザーに警告するために役立ちます。

## サポートされているブラウザ

Credential Protection拡張機能は、現在、Google Chrome、Mozilla Firefox、およびMicrosoft Edge（Chromiumベース）の各Webブラウザの最新リリースでサポートされています。HP Sure Click Pro Secure Browserにも対応していません。

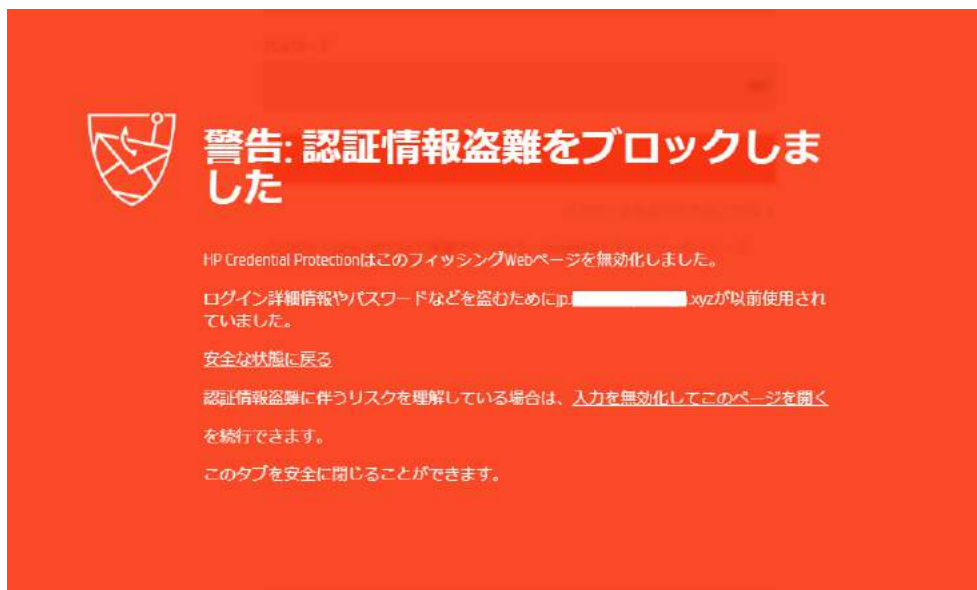
## 保護の動作

この機能が有効になっているデバイスで、ユーザーが保護されたブラウザから疑わしいWebサイトまたは既知の悪意のあるWebサイトにパスワードを入力しようとする、ページに警告メッセージが表示されます。

Webサイトのリスクが高いと評価された場合は、次のような赤い警告画面がユーザーに表示されます。ユーザーは警告されますが、その警告は回避できません。そのサイトへのアクセスが制限され、ログインフォームのログインコントロールが無効になります。



# スタートガイド - HP Wolf Pro Security



サイトが中程度のリスク（疑わしい）と評価された場合は、次のような黒色の警告画面がユーザーに表示されます。



これらのサイトでは悪意のある意図は確認されていないため、ユーザーは引き続き、資格情報の入力またはWebサイトへのアクセスが可能です。ユーザーが誤ってパスワードを入力しないように、サイトのログインフィールドが無効になります。また、ユーザーがそのWebページへの資格情報入力を続行することを選択すると、そのサイトはエンドユーザーの信頼できるログインサイトのリストに追加され、そのページに対する追加の警告は表示されなくなります。

# スタートガイド - HP Wolf Pro Security

## HP Wolf Security拡張機能を有効にする方法

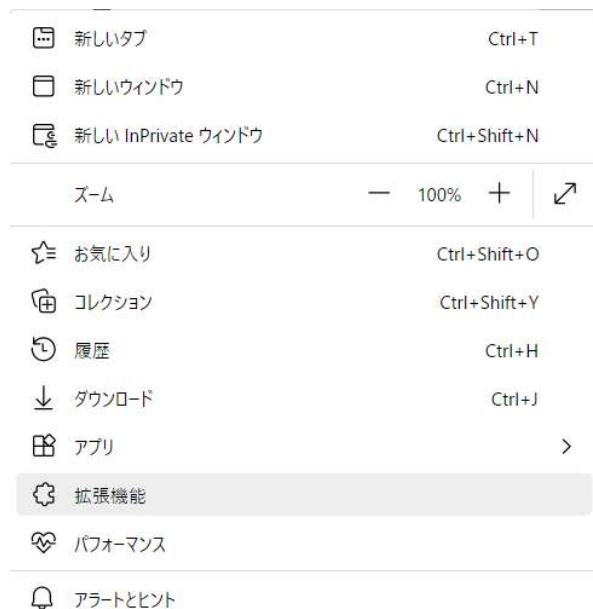
HP Wolf Security拡張機能が有効であるかどうかを確認するには、Webブラウザの拡張機能ツールバー アイコンから、HP Wolf Security拡張機能アイコンをクリックします。ユーザーのブラウザ プロファイルでこの拡張機能が有効になっていない場合は、次のポップアップが表示されます。



この拡張機能を有効にするには、Webブラウザのメニューから[その他のツール] → [拡張機能]を選択します。

## HP Wolf Security拡張機能を無効にする方法

HP Wolf Security拡張機能を無効にするには、お使いのブラウザの[拡張機能]メニュー項目に移動し、拡張機能を[オフ]に切り替えて機能を無効にします。Google ChromeおよびMicrosoft Edge (Chromium) ブラウザーでは、これはブラウザ メニューの[詳細設定] → [拡張機能]の下にあります。



# スタートガイド - HP Wolf Pro Security

拡張機能の一覧が読み込まれたら、HP Wolf Security拡張機能のタイルを見つけて、機能をオフに切り替えます。



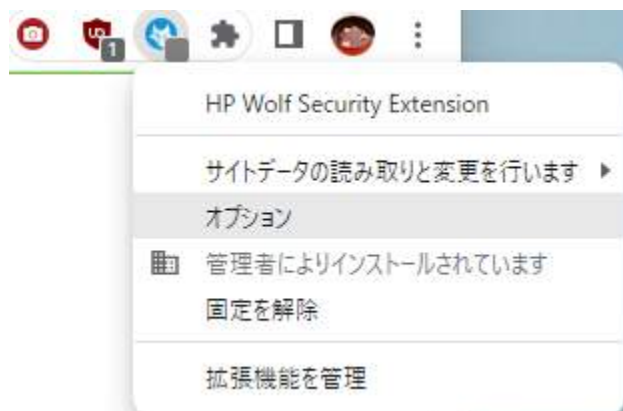
## HP Wolf Security拡張機能が有効であるかどうかを確認する方法

有効にした後、ブラウザのメニューバーのHP Credential Protection拡張機能アイコンをクリックすると、拡張機能がアクティブであることを確認できます。



## ユーザー定義のログインページの除外を管理する方法

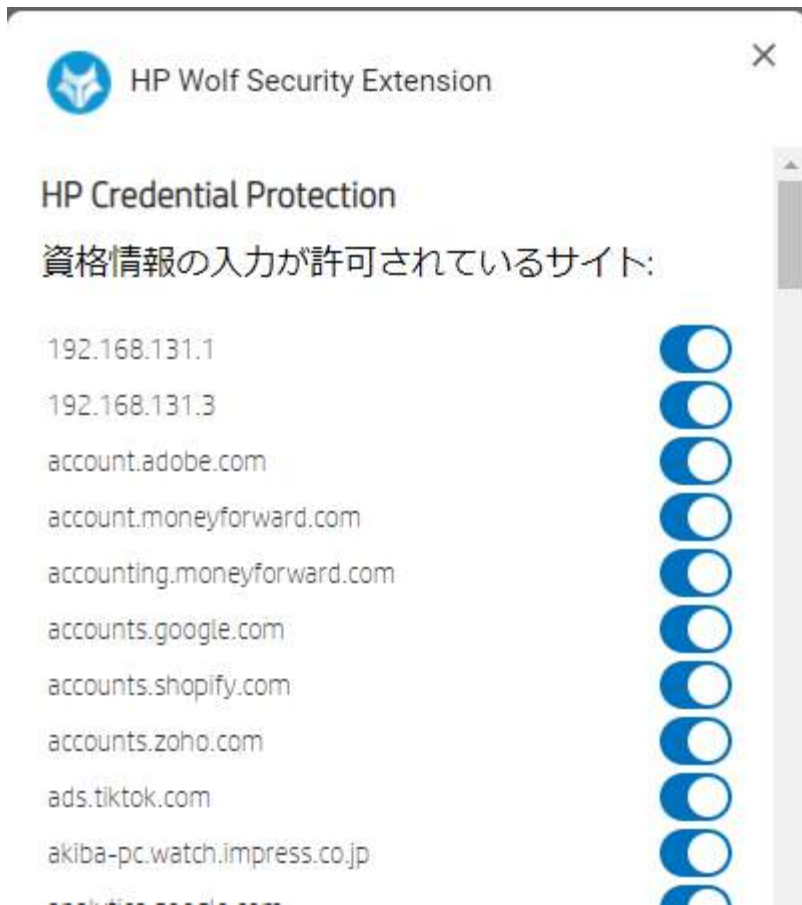
許可またはブロックされたログインページのリストを管理するには、ブラウザのメニューバーのHP Credential Protectionブラウザ拡張機能アイコンを右クリックし、[オプション]を選択します。





# スタートガイド - HP Wolf Pro Security

ユーザーはこのメニューから、許可されたWebサイトの信頼設定を変更するかどうかを選択できます。これは組織によって変更が制限されている場合があることに注意してください。





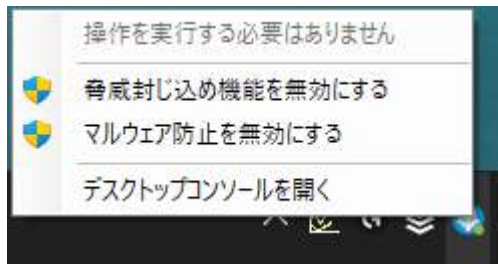
# スタートガイド - HP Wolf Pro Security

## ローカルでの管理（デスクトップコンソール）

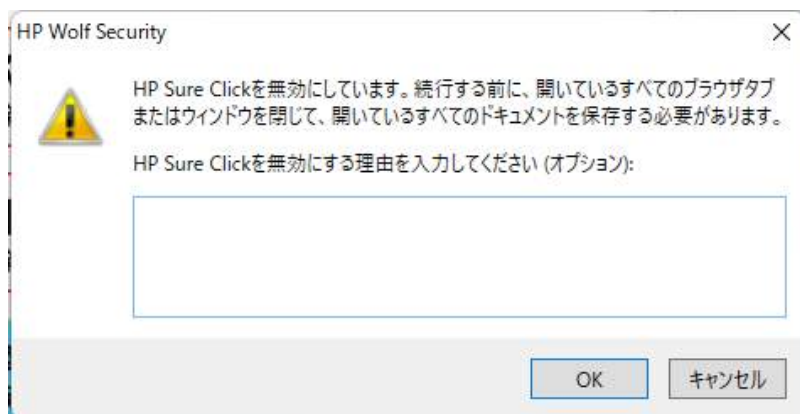
このセクションでは、エンドユーザーがHP Wolf Pro Securityエージェントおよびサービスを操作する方法について説明します。

### デスクトップコンソールを起動する

タスクバーの時計の横にあるHP Wolf Pro Securityアイコンをクリックすると（次の図を参照してください）、デスクトップコンソール（ユーザーインターフェイス）が表示されます。



- [ステータス]では、アクションが必要かどうかわかります。
- [脅威封じ込め機能を無効にする]または[脅威封じ込め機能を有効にする]を実行するには、そのオプションをクリックします。これにより、脅威の封じ込めテクノロジーが無効・有効になります。
  - 機能を無効にするときは、理由を入力する必要があります。これによって問題の切り分けをスピードアップできます。

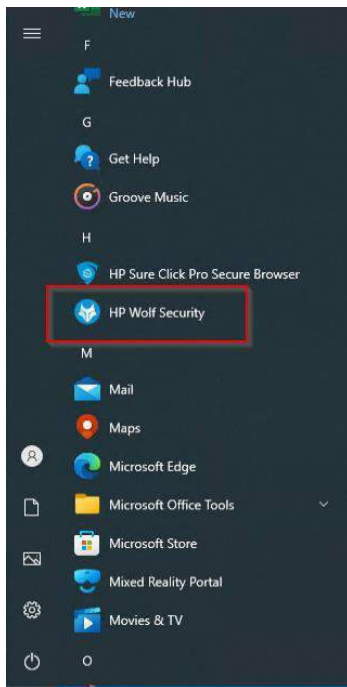


- [マルウェア防止を無効にする]または[マルウェア防止を有効にする]を実行するには、そのオプションをクリックします。これにより、SureSenseテクノロジーが無効・有効になります。
- デスクトップコンソールを開くと、ユーザーインターフェイスが表示されます。

デスクトップコンソールは、スタートメニューをクリックし、HP Wolf Securityを選択して開くこともできます。

# スタートガイド - HP Wolf Pro Security

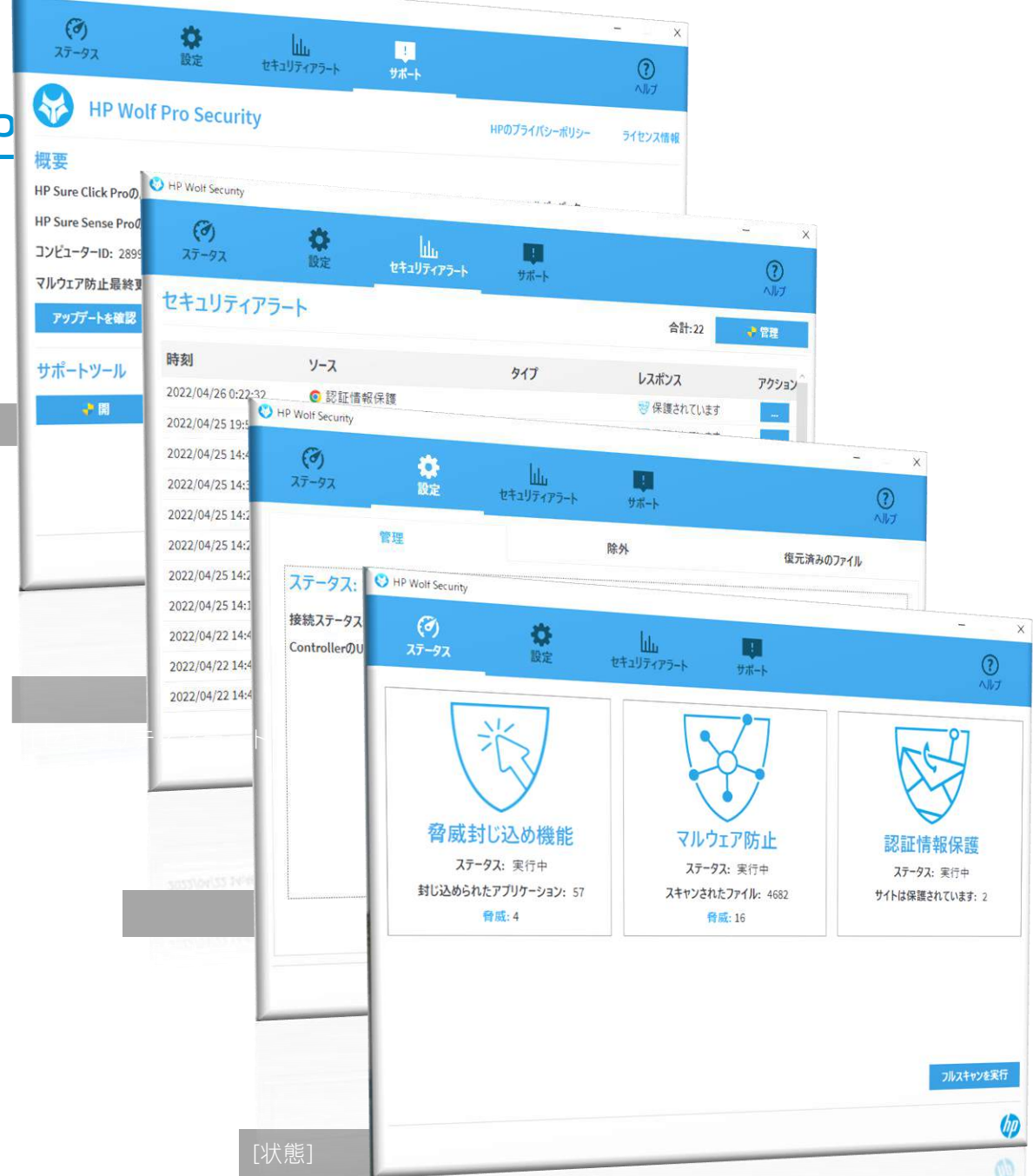
---



# スタートガイド - HP

## デスクトップコンソールの詳細

- [ステータス]
  - アクティブな正常性状態、エラーメッセージ、検出および軽減された脅威の数、スキャンされたファイル数。
- [設定]
  - 状態：コントローラーへのエンドポイントの接続
  - ローカルのファイルとフォルダーの除外を設定したり、隔離から復元されたファイルに対してアクションを実行したりします
- セキュリティアラート
  - 検出された悪意のあるファイル、Webサイト、および検出された資格情報フィッシング攻撃のイベントリスト
  - 隔離テクノロジーを使用して隔離されたファイルを安全に開き、そのファイルを修正および操作します
- [サポート]
  - バージョン情報：バージョン番号、PC番号
  - 高度なツール
  - ログ、VMの再初期化、ライブビュー



# スタートガイド - HP Wolf Pro Security

WindowsのスタートメニューからHP Pro Securityダッシュボードを起動すると、ダッシュボードが開いて[ステータス]ページが表示されます。HP Pro Securityに含まれる3つの保護メカニズムのそれぞれについて、以下で説明します。上部のアイコン（[ステータス]、[設定]、[セキュリティアラート]、[サポート]）をクリックすると、ソフトウェアの各属性の設定と情報が表示され

**[ステータス]**：保護がアクティブであることを示し、悪意のあるWebサイトや疑わしいメールの添付ファイルからユーザーを保護します。アイコンが黄色または赤色で表示されている場合は、

**[封じ込められたアプリケーション]**：Secure Viewで開かれたドキュメント/Webサイトを。

**[脅威]**：ブロックおよび隔離されたファイル/Webサイト（脅威の名前と種類の詳細については、[セキュリティアラート]ページを参照してください）。

**[マルウェア防止]**：ディープラーニングAI：マルウェア対策保護。

**[ステータス]**：AI保護エージェントがアクティブであり、PCに到達した悪意のあるファイルからPCを保護および隔離していることを示します。

**[スキャンされたファイル]**：エージェントによってスキャンされたドキュメント/Webサイト。注：エージェントがアクティブな場合、PCに到達したすべてのファイルの種類がスキャンされます。

**[脅威]**：ブロックされたファイル/項目（脅威の名前と種類の詳細については、[セキュリティアラート]ページを参照してください）。

**[認証情報保護]**：ユーザーが疑わしいWebサイトにパスワードを入力することを警告または阻止する機能を備えたフィッシング対策エンジン

**[ステータス]**：HPのフィッシング対策保護がアクティブか非アクティブかを示します。

**[サイトは保護されています]**：資格情報（ユーザーログイン、パスワード）を盗もうとしたWebサイトの数を示します

The screenshot shows the HP Pro Security (Administrator) dashboard. At the top, there are navigation icons for 'ステータス' (Status), '設定' (Settings), 'セキュリティアラート' (Security Alerts), 'サポート' (Support), and 'ヘルプ' (Help). The main content area features three large cards representing different security features:

- 脅威封じ込め機能 (Threat Blocking)**: Status: 実行中 (Running). 封じ込められたアプリケーション: 57 (Quarantined Applications: 57). 脅威: 4 (Threats: 4).
- マルウェア防止 (Malware Prevention)**: Status: 実行中 (Running). スキャンされたファイル: 4682 (Scanned Files: 4682). 脅威: 16 (Threats: 16).
- 認証情報保護 (Credential Protection)**: Status: 実行中 (Running). サイトは保護されています: 2 (Sites Protected: 2).

At the bottom right, there is a button labeled 'フルスキャンを実行' (Run Full Scan) and the HP logo.

# スタートガイド - HP Wolf Pro Security

Windowsのスタートメニューから**HP Pro Security**ダッシュボードを起動すると、ダッシュボードが開きます。

**[設定]**アイコンを選択すると、ソフトウェアで制御可能な機能の3つのタブを持つページ（**[設定]**、**[除外]**、および**[復元されたファイル]**）が表示されます。

**[管理]**：この（**[設定]**）ページの3つのタブのうちの1番目のタブ

**[管理]**：**[接続ステータス]**：コントローラーへのエンドポイントの接続の状態が表示されます。

The screenshot shows the HP Wolf Security dashboard interface. At the top, there is a navigation bar with icons for '設定' (Settings), 'セキュリティアラート' (Security Alerts), and 'サポート' (Support). Below this, there are three tabs: '管理' (Management), '除外' (Exclusions), and '復元済みのファイル' (Recovered Files). The '管理' tab is active and displays the following information:

- ステータス: 接続済み
- 接続ステータス: 接続済み
- ControllerのURL: i772c0be5.api.control.hpwolf.com

The HP logo is visible in the bottom right corner of the dashboard.

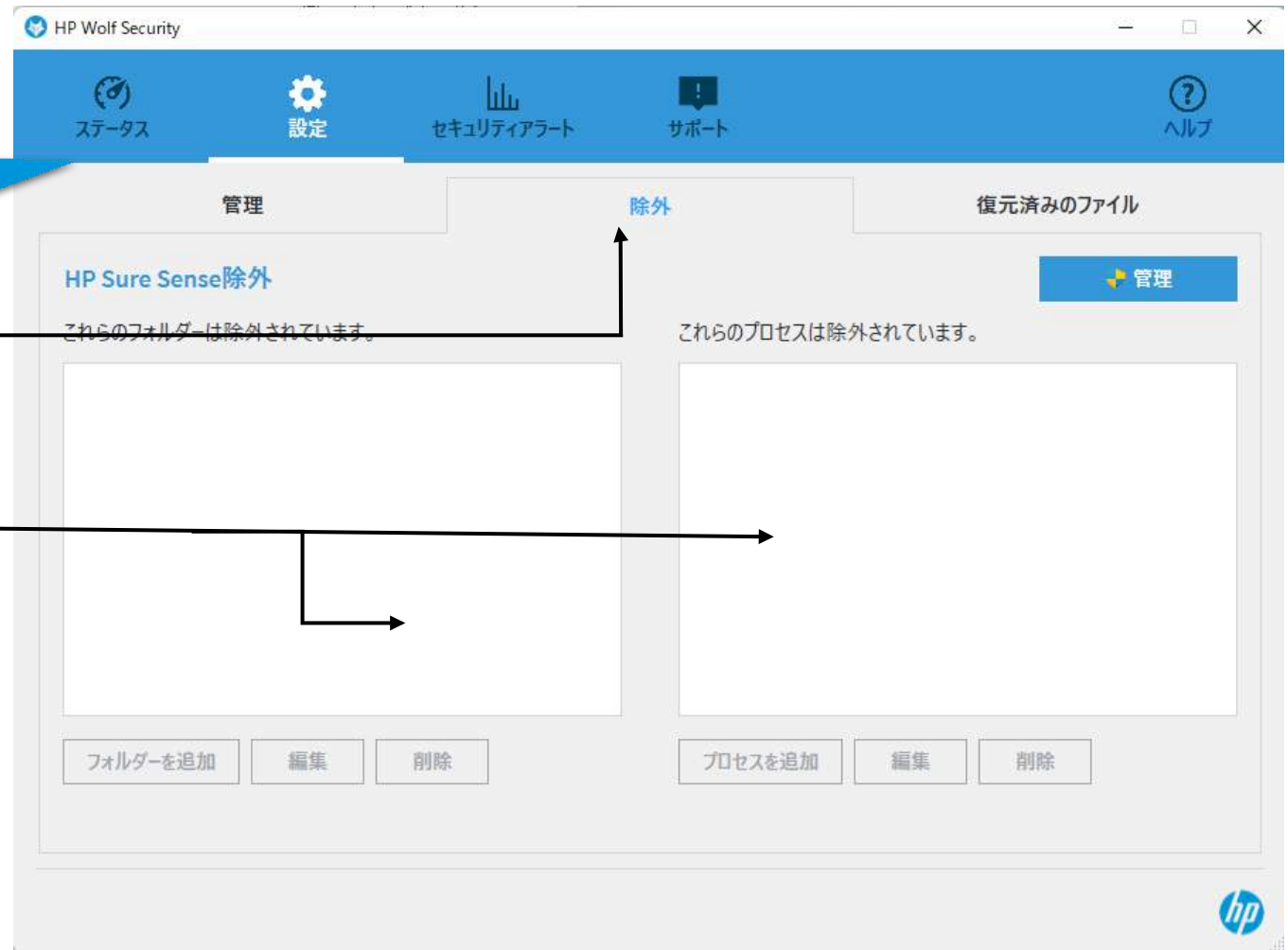
# スタートガイド - HP Wolf Pro Security

Windowsのスタートメニューから**HP Pro Security**ダッシュボードを起動すると、ダッシュボードが開きます。  
[設定]アイコンを選択すると、ソフトウェアで制御できる機能の3つのタブを持つページ（[管理]、[除外]、[復元済みのファイル]）が表示されます。

[除外]：この（[設定]）ページの3つのタブのうちの2番目のタブ

[除外]：安全であることがわかっているフォルダー、ファイル、またはプロセスのフォルダーやプロセスのリスト。HP Pro Securityで**セキュリティスキャン**が実行されているときに、このページのどちらかのリストに（ファイルが含まれている）フォルダーまたはプロセス名を追加しようとしても無視されます（「安全」と見なされます）。

このカスタム アプリケーションを除外リストに追加すると、今後のマルウェア スキャンからそのファイルが除外されます。



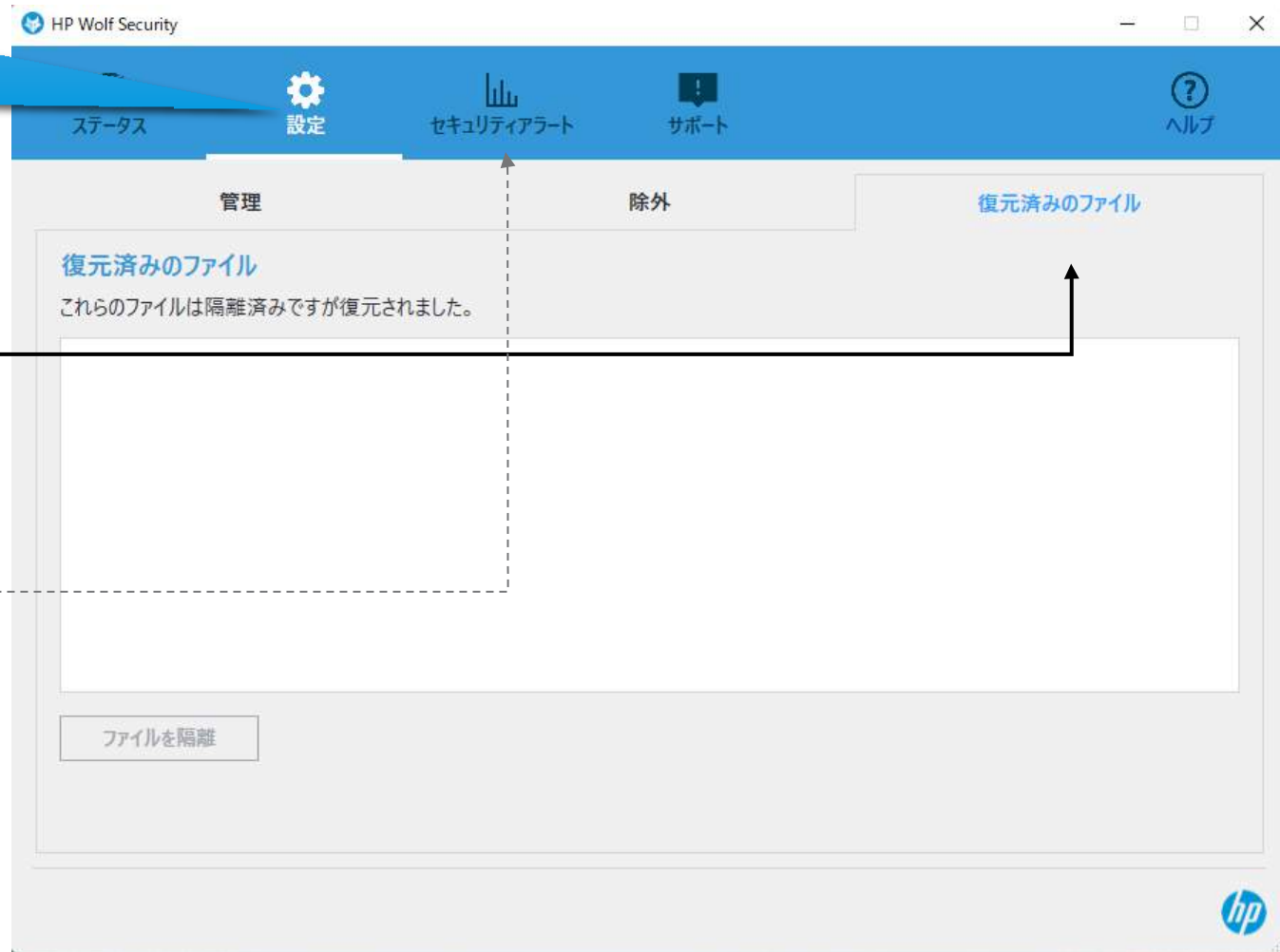
# スタートガイド - HP Wolf Pro Security

Windowsのスタートメニューから**HP Pro Security**ダッシュボードを起動すると、ダッシュボードが開きます。**[設定]**アイコンを選択すると、ソフトウェアで制御可能な機能の3つのタブを持つページ（**[管理]**、**[除外]**、**[復元済みのファイル]**）が表示されます。

**[復元済みのファイル]**：この（**[設定]**）ページの3つのタブのうちの3番目のタブ

**[復元済みのファイル]**：このページには、HP Wolf Pro Securityで当初は悪質としてフラグ付けされたが、ユーザーが安全としてマークすると選択したファイルのアクティブなリストが保持されます。通常、安全なファイルは信頼できるソースから取得されたものであるため、ユーザーが安全としてマークするアクションを実行します。

注：安全でないとしてフラグが立てら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





# スタートガイド - HP Wolf Pro Security

WindowsのスタートメニューからHP Pro Securityダッシュボードを起動すると、ダッシュボードが開きます。[セキュリティアラート]アイコンを選択すると、隔離されたか、悪意のあるものとしてフラグが立てられたファイル名やWebサイトのリストが表示されます。

攻撃データには、[時刻]、[ソース]、[攻撃の]タイプ、[レスポンス]、および[アクション]が含まれます。

**[時刻]**：脅威が検出された月、日、年、および時刻。

**[ソース]**：潜在的に悪意のあるファイルとして分類および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]**：一部のマルウェアの種類は分類でき（ランサムウェアなど）、可能であれば、HP Pro Securityによってこの列に情報が表示されます。

**[レスポンス]**：悪意のあるファイルまたはWebサイトが検出されたときにHP Pro Securityで実行されたアクション。

**[アクション]**：アクション（[...]）ボタンには、複数のユーザーオプションがあります。

1. 隔離されたファイルの場合、ユーザーに4つのオプションが表示されます

- i. ファイルの詳細：場所、時刻、およびハッシュ値。
- ii. 安全に表示する：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、隔離されたままにするべきかを判断します。
- iii. PCからファイルを削除する
- iv. 復元：ファイルを「信頼された」状態に変更します。

2. 保護されたファイルの場合、ユーザーはフィッシングが行われた場所として識別されたWebサイトの詳細を表示できます。

- i. ファイルの詳細を表示する：URLの場所、時刻、およびハッシュ値。

時刻	ソース	タイプ	レスポンス	アクション
2022/04/26 0:22:32	認証情報保護		保護されています	...
2022/04/25 19:56:09	認証情報保護		保護されています	...
2022/04/25 14:45:28	e73f8310406ceec868e8e7d3c209cda	Win32.Trojan.Sabsik	分離済み	...
2022/04/25 14:33:19	656a047d8aab12690dc09d214aff92e	Win64.Trojan.Generic	分離済み	...
2022/04/25 14:27:56	b75775a0ca6997e799bb42e9ac8bba	Win32.Trojan.Sabsik	隔離済み	...
2022/04/25 14:20:43	\$R10BFHC.msi	Win32.Trojan.Grandoreiro	隔離済み	...
2022/04/25 14:20:06	76d2a46d1ef0c77e7e6dcc56a1e8ccb	Win32.Trojan.Grandoreiro	分離済み	Details View Securely Delete File Restore File
2022/04/25 14:18:05	76d2a46d1ef0c77e7e6dcc56a1e8ccb	Win32.Trojan.Grandoreiro	分離済み	...
2022/04/22 14:48:47	6ae54004e33156bd1637210c05261a	Win32.Trojan.Emotet	隔離済み	...
2022/04/22 14:48:28	1878d067011a763e3fdf15143b9c407	Document-Office.Exploit.C	隔離済み	...
2022/04/22 14:46:35	solo_mine_example.cmd		隔離済み	...

これは業界でも独自の隔離ワークフローであり、以下で詳しく説明します。



# スタートガイド - HP Wolf Pro Security

HP Sure Click ProとHP Sure Sense Proによって、WPSの一部である機能が提供されます。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プログラムを受信します。**バージョン番号**は同じではありません。

**[コンピューターID]**は、このエンドポイントに割り当てられた一意のIDです。これは、コントローラーでこのエンドポイントを識別するためのものであり、サポートにも役立ちます。

**[ログ記録を有効にする]**にチェックを入れると、サポートに情報を提供する目的のために、ユーザーが定義したPCのディレクトリ（[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、さらにトリガーするためにログファイルがコントローラーに送信されます

**[再初期化]**は、脅威の封じ込めで予期しないエラーが発生した場合の特定の状況で役立ちます。このボタンを押すと、悪意のあるコンテンツを隔離するための仮想マシン テンプレートが再作成されます。

**[ライブビューを開く]**は、サポートに役立つ高度な機能です。**[ライブビューを開く]**ボタンを押すと、ダイアログウィンドウが（右端などに）作成され、PC上で現在実行されている仮想マシンが表示されます。

この更新の確認を選択すると、更新が利用可能な場合、次世代アンチウイルスの最新の既知のシグネチャの更新がダウンロードされます

# スタートガイド - HP Wolf Pro Security

## 隔離されたファイルに対する独自のワークフロー

ハードウェアによる隔離と次世代アンチウイルスとの組み合わせにより、WPSでは業界でも独自の隔離ワークフローを実現します。

次世代アンチウイルスのほとんどの場合では、潜在的に悪意のあるファイルに対する標準的な対応は、ファイルを削除するか、検出が誤検知であるとエンドユーザーが確信している以外の場合は、解析のためにファイルを安全に隔離してアップロードします。このため、誤検知が発生した場合はユーザーにファイルの表示さえ許可されずにワークフローが中断されます。

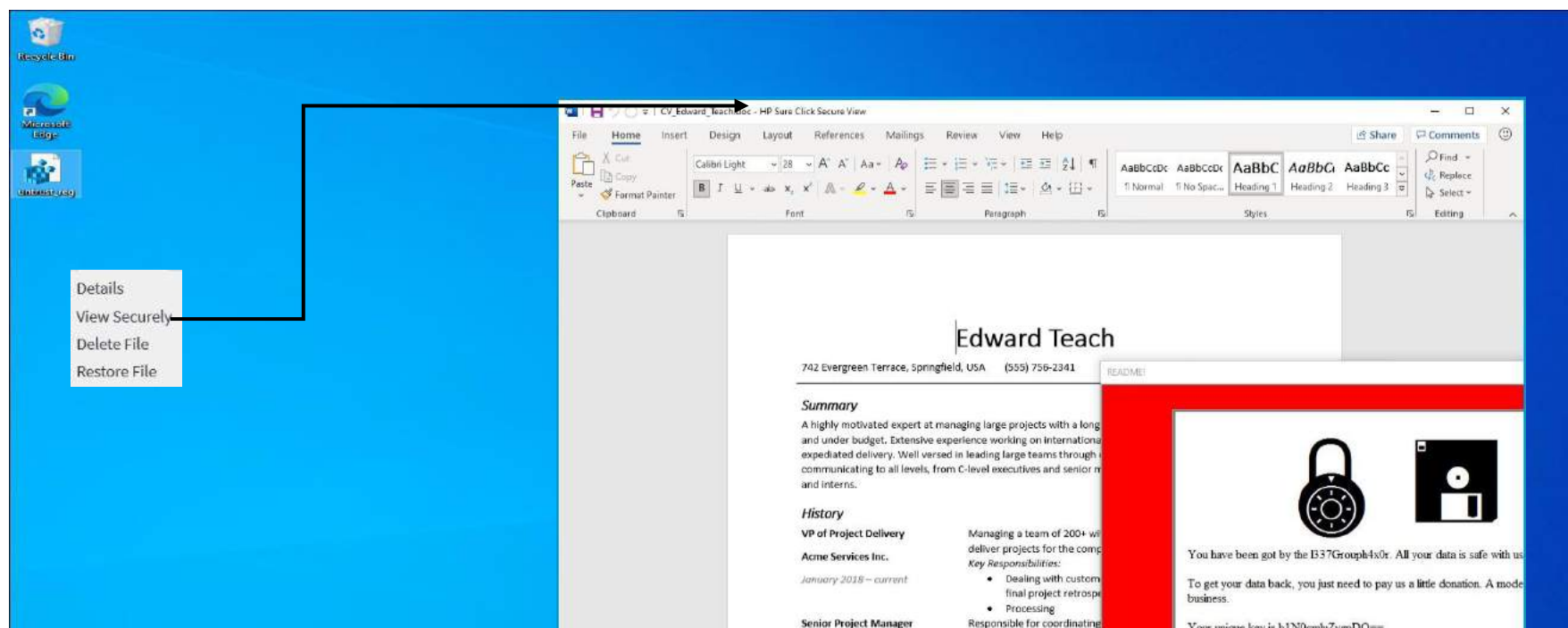
つまり、隔離によってユーザーがアクセスできなくなったファイルは、ユーザーに不快な状態を引き起こす可能性があります。

WPSでは、ファイルの種類が隔離機能でサポートされていれば、隔離されたファイルをその状態で安全に開くことができるようにし、上記の問題を完全に回避します。ユーザーは、ファイルが悪意のあるものであるかどうかを気にすることなく、安全に表示することができます。

ファイルに悪意があるものの場合、マルウェアは隔離された環境で実行され、また隔離されたファイルを閉じるとすぐに破棄され、エンドユーザーのデバイスはまったく影響を受けません。

以下は、ランサムウェアを含み、悪意のある履歴書がすでに隔離されている例ですが、エンドユーザーはそれが本当に悪意があるかどうかはわかりません。それでもユーザーはこれを安全に表示でき、完全に隔離されたVMで開きます。

以下に示すように、本当に悪意のあることが判明した場合でも、マルウェアはVM内に完全に封じ込められており、Wordファイルを閉じると破棄されます。



# スタートガイド - HP Wolf Pro Security

## デスクトップコンソールの状態カード

### 脅威の封じ込め機能

隔離と監視には、次の3つの状態があります。

- **実行中**：すべてが正常に動作しています。
- **アクションを推奨**：アプリケーションが正常ではないため、調査する必要があります。
- **無効**：これはエージェントが無効にされていて、コンピューターが保護されていないことを意味します。
- 封じ込められたアプリケーションの数を確認できます
- 防御された脅威の件数を確認できます



このタイルには、次の状態メッセージが表示されることがあります。

[状態]	説明
HP Sure Clickを待機しています	HP Sure Clickがこの状態のままの場合は、コンピューターを再起動してみてください。
HP Sure Clickが実行されています	HP Sure Clickによって、マルウェアを含むWebサイトやドキュメントからユーザーが保護されています。
HP Sure Clickを有効にしてシステムを保護してください	HP Sure Clickが無効になっています。システム トレイのアイコンメニューから[脅威の封じ込め機能]を選択して、有効にします。
HP Sure Clickが実行されていません	HP Sure Clickが実行されていません。コンピューターを再起動してみてください。
HP Sure Clickを初期化する必要があります	HP Sure Clickが初期化されていません。初期化するには、[サポート]ページの[再初期化]ボタンを押します。
HP Sure Clickの要件を確認しています...	このメッセージは、HP Sure Clickの起動時に短時間表示される場合があります。
HP Sure Clickの状態を確認しています...	このメッセージは、HP Sure Clickの起動時に短時間表示される場合があります。
HP Sure Clickの更新を確認しています...	HP Sure Clickでは、実行前に更新をダウンロードする必要がある場合があります。この処理が完了するまでお待ちください。

# スタートガイド - HP Wolf Pro Security

構成の受信を待機しています	HP Sure Clickでは、実行前にControllerから構成をダウンロードする必要があります。この処理が完了するまでお待ちください。
構成のフェッチに失敗しました。ネットワーク接続を確認してください。	HP Sure Clickでは、実行前にControllerから構成をダウンロードする必要があります。コンピューターがインターネットに接続されていることを確認してください。
コンピューターがインターネットに接続されていることを確認してください	コンピューターがインターネットに接続されていることを確認してください
HP Sure Clickの準備があと数分で完了します	HP Sure Clickを使用するための準備を整えています。この処理が完了するまでお待ちください。
初期化プロセスを実行しています	HP Sure Clickで、コンピューターの現在のシステム状態をキャプチャしています。この処理が完了するまでお待ちください。
初期化が必要です/初期化プロセスが一時停止しています	HP Sure Clickでは、コンピューターの現在のシステム状態をキャプチャする必要があります。これは、システムがアイドル状態になったときに発生します。または、[サポート]ページの[初期化]ボタンを押して、この処理を開始することもできます。
再初期化プロセスを実行しています	HP Sure Clickで、コンピューターの現在のシステム状態をキャプチャしています。HP Sure Clickは引き続き実行されているため、この処理の間も保護されます。
再初期化が必要です/再初期化プロセスが一時停止しています	HP Sure Clickでは、コンピューターの現在のシステム状態をキャプチャする必要があります。これは、システムがアイドル状態になったときに発生します。または、[サポート]ページの[再初期化]ボタンを押して、この処理を開始することもできます。HP Sure Clickは引き続き実行されているため、この処理の間も保護されます。
HP Sure Clickのアップグレードを有効にするためにコンピューターを再起動する必要があります	HP Sure Clickの更新がインストールされています。コンピューターを再起動して、更新後のバージョンに切り替えます。

このタイルには、次のエラーメッセージが表示されることがあります

エラーメッセージ	説明
このCPUはHP Sure Clickでサポートされません	このCPUはHP Sure Clickでサポートされないため、実行できません。
HP Sure Clickには、VT-x対応システムが必要です	このCPUではVT-x仮想化拡張機能（または同等のもの）がサポートされていないため、HP Sure Clickを実行できません。
HP Sure Clickでは、VT-xを有効にする必要があります	VT-x仮想化拡張機能（または同等のもの）が、システムBIOSで無効にされています。 <a href="#">HP Sure Clickを実行</a> できるようにするには、システムBIOSでVT-xを有効にする必要があります。 <a href="#">「BIOSでバーチャライゼーションテクノロジーを有効にする方法」</a> を参照してください。
HP Sure Clickでは、EPT（Extended Page Table）を有効にする必要があります	Extended Page Table仮想化拡張機能がシステムBIOSで無効にされています。HP Sure Clickを実行できるようにするには、システムBIOSでEPTを有効にする必要があります。
サポートされていないAMD CPUファミリー	HP Sure ClickでサポートされないAMDプロセッサがコンピューターに搭載されています。



# スタートガイド - HP Wolf Pro Security

HP Sure Clickのメモリ要件が満たされていません	HP Sure Clickでメモリ不足が検出されました。メモリ容量を増やすために、プログラムをいくつか終了してください。
十分な空きメモリがありません。プログラムを終了してメモリ容量を増やしてください	HP Sure Clickでメモリ不足が検出されました。メモリ容量を増やすために、プログラムをいくつか終了してください。
空きディスク領域を増やしてからコンピューターを再起動してください	HP Sure Clickの初期化では、システムディスクに少なくとも1.5 GBの空き容量が必要となります。1.5 GBのディスク領域が空いていることを確認してから、コンピューターを再起動してください。
HP Sure Clickは、Gladinetを使用するシステムと互換性がありません	HP Sure Clickは、Gladinetソフトウェアと互換性がありません。
HP Sure Clickが別のユーザーセッションでアクティブになっています	HP Sure Clickは、同じコンピューターに同時にログインしている複数のユーザーをサポートするように構成されていません。
HP Sure Clickでシステムを保護するにはコンピューターを再起動する必要があります	HP Sure Clickを実行する前に、コンピューターを再起動する必要があります。
インストールされているWindowsのバージョンをサポートするにはHP Sure Clickを更新する必要があります。コンピューターを再起動して、これらの更新プログラムがインストールされるようにしてください。	HP Sure Clickでは、このバージョンのWindowsをサポートするには追加のコンポーネントが必要です。このコンポーネントがインストールされるようにするには、システムを再起動する必要があります。
インストールされているWindowsのバージョンのサポートに必要な更新プログラムをHP Sure Clickでダウンロードできません。インターネット接続を確認してください。	このバージョンのWindowsをサポートするには、HP Sure Clickに追加コンポーネントが必要です。システムで必要なコンポーネントをダウンロードできませんでした。システムがインターネットに接続されていることを確認して、ダウンロードが完了するまでお待ちください。
インストールされているWindowsのバージョンをサポートするにはHP Sure Clickを更新する必要があります。更新プログラムがインストールされるまでお待ちください。	このバージョンのWindowsをサポートするには、HP Sure Clickに追加コンポーネントが必要です。システムでこのコンポーネントのインストールが完了するまでお待ちください。
インストールされているWindowsのバージョンをサポートするにはHP Sure Clickを更新する必要があります	このバージョンのWindowsをサポートするには、HP Sure Clickに追加コンポーネントが必要です。
サポートされているWindows言語パックがインストールされていません	HP Sure Clickを使用するには、Windows言語パックをインストールする必要があります。
ユーザーのWindows表示言語はサポートされていません	ユーザーのWindows表示言語はサポートされていません
コンピューターを再起動して、保留中のWindowsの更新プログラムをインストールしてください	コンピューターを再起動してWindowsの更新プログラムを適用するため、HP Sure Clickを初期化できません。コンピューターを再起動して、更新プログラムが適用されるのを待ってから、[初期化]ボタンを押して初期化プロセスを開始してください
Windows Updateが実行されています	Windows Updateが実行されているため、HP Sure Clickを初期化できません。完了するまで待つか、コンピューターを再起動してください。その後、[初期化]ボタンを押して初期化プロセスを開始します。
HP Sure Clickでは、Microsoft OfficeにVBAコンポーネントがインストールされている必要があります	HP Sure Clickでは、Microsoft OfficeにVisual Basic for Applicationsがインストールされている必要があります。VBAコンポーネントをインストールし、[初期化]ボタンを押して初期化プロセスを開始してください。
Officeがアクティブ化されていません	HP Sure Clickを使用するには、Microsoft Officeがアクティブ化されている必要があります。Microsoft Officeをアクティブ化し、[初期化]ボタンを押して初期化プロセスを開始してください。





# スタートガイド - HP Wolf Pro Security

サポートされているOffice UI言語パックがインストールされていません	HP Sure Clickでは、次のMicrosoft Office UI言語パックのどれかがインストールされている必要があります
このコンピューターではHP Sure ClickでHyper-Vがサポートされません	HP Sure Clickを実行できるようにするには、Hyper-Vを無効にするか、Windowsハイパーバイザー プラットフォームを有効にします（「 <a href="#">Windows Hyper-Vサポート</a> 」を参照してください）。
HP Sure Clickでは、Hyper-VをサポートするためにUEFIブートが必要です	UEFIブートが検出されませんでした。HP Sure Clickを実行できるようにするには、Hyper-Vを無効にするか、Windowsハイパーバイザー プラットフォームを有効にします（「 <a href="#">Windows Hyper-Vサポート</a> 」を参照してください）。
HP Sure Clickでは、Hyper-VをサポートするためにWindows10以降が必要です	サポートされていないオペレーティング システム バージョンが検出されました。HP Sure Clickを実行できるようにするには、Hyper-Vを無効にします。
Hyper-Vが有効にされている場合、HPSureClickでこのCPUはサポートされません	サポートされていないCPUが検出されました。HP Sure Clickを実行できるようにするには、Hyper-Vを無効にするか、Windowsハイパーバイザー プラットフォームを有効にします（「 <a href="#">Windows Hyper-Vサポート</a> 」を参照してください）。
Hyper-Vをサポートするには、HP Sure Clickでセキュア ブートのサードパーティ キーが必要です	システムBIOSで、[安全なブート構成]メニューを開きます。HP Sure Clickを実行できるようにするには、[MS UEFI CAキーを有効にする]を選択します。
Hyper-Vをサポートするには、HP Sure ClickでVMCSシャドウイング対応のCPUが必要です	このCPUではVNCシャドウイングがサポートされていません。HP Sure Clickを実行できるようにするには、Hyper-Vを無効にするか、Windowsハイパーバイザー プラットフォームを有効にします（「 <a href="#">Windows Hyper-Vサポート</a> 」を参照してください）。
HP Sure ClickでHyper-Vのサポートを有効にできませんでした	この問題を修正するには、HPサポートにお問い合わせください。
Hyper-Vのサポートを有効にしているときに、マイクロ仮想化がブロックされました	この問題を修正するには、HPサポートにお問い合わせください。
コンピューターをシャットダウン/再起動する前に、BitLockerを一時停止する必要があります	コンピューターを再起動する前に、BitLockerを一時停止する必要があります。 Windowsのコントロール パネルから、[BitLockerドライブの暗号化]を選択し、[保護の一時停止]を選択します
Hyper-Vのサポートを有効にするときに、HP Sure ClickでUEFIブートの順序を構成できません	この問題を修正するには、HPサポートにお問い合わせください。
Hyper-Vのサポートを有効にするときに、HP Sure Clickで起動デバイスを特定できません	この問題を修正するには、HPサポートにお問い合わせください。
最後の初期化がキャンセルされました	HP Sure Clickの初期化プロセスがキャンセルされたため、完了しませんでした。
最後の初期化がブロックされました	HP Sure Clickで初期化プロセスを完了できませんでした。[サポート]ページの[初期化]ボタンを押し、初期化プロセスを再度開始してみてください。それが失敗した場合は、HPサポートにお問い合わせください。
最後の初期化の試行が失敗しました	HP Sure Clickで初期化プロセスを完了できません。[サポート]ページで[初期化]ボタンを押して、初期化プロセスを再度開始してみてください。それが失敗した場合は、HPサポートにお問い合わせください。
最後の初期化の試行が正常に終了しませんでした	HP Sure Clickで初期化プロセスを完了できませんでした。HP Sure Clickは以前に初期化されているため、引き続きコンピューターを保護できます。[サポート]ページの[再初期化]ボタンを押して、初期化プロセスを再度開始してみてください。
サポートされていない構成。サポートにお問い合わせください。	この問題を修正するには、HPサポートにお問い合わせください。



# スタートガイド - HP Wolf Pro Security

内部エラー。コンピューターを再起動してください	この問題を解決するには、コンピューターを再起動します。それでも解決しない場合は、HPサポートにお問い合わせください。
Micro-VMをロードできませんでした。コンピューターを再起動し、問題が解決しない場合はサポートにお問い合わせください。	HP Sure ClickでMicro-VMを正しくロードできなくなる問題が発生しました。コンピューターを再起動し、それでも問題が再発する場合はHPサポートにお問い合わせください。
HP Sure Clickのインストールが破損しているため、修復する必要があります	HP Sure Clickのインストールに一部のファイルが含まれていません。これは、Windowsシステムの復元を実行した結果である可能性があります。製品の最新バージョンをダウンロードしてインストールし、破損を修正します。「 <a href="#">最新バージョンのダウンロード</a> 」を参照してください。

## マルウェア防止

この機能には3つの状態があります。

- **実行中**：すべてが正常に動作しています。
- **アクションを推奨**：アプリケーションが正常ではないため、調査する必要があります。
- **無効**：これはエージェントが無効にされていて、コンピューターが保護されていないことを意味します。
- スキャンされたファイルの件数を確認できます
- 防御された脅威の件数を確認できます



このタイルには、次の**状態メッセージ**が表示されることがあります。

状態メッセージ	説明
HP Sure Senseが実行されています	HP Sure Senseによって、悪意のあるファイルからユーザーが保護されています。
HP Sure Senseを有効にしてシステムを保護します	HP Sure Senseが無効にされています。システムトレイのアイコンメニューから[マルウェア防止を有効にする]を選択して有効にします。
HP Sure Senseの準備がまもなく完了します	HP Sure Senseを使用するための準備を整えています。この処理が完了するまでお待ちください。
HP Sure Senseのアップグレードを有効にするにはコンピューターを再起動する必要があります	HP Sure Senseの更新がインストールされています。コンピューターを再起動して、更新後のバージョンに切り替えます。



# スタートガイド - HP Wolf Pro Security

HP Sure Senseにアクセスできません	HP Sure Senseはインストールされているようですが、HP Wolf Pro Securityからそれにアクセスできません。コンピューターを再起動してみてください。
更新プログラムのダウンロードに失敗しました	HP Sure Senseでは、実行前に更新をダウンロードする必要があります。コンピューターがインターネットに接続されていることを確認してください。
互換性のない製品が存在するため、動作保護が無効になっています	動作保護を有効にするには、互換性がないことがわかっている製品をすべて削除してください。
構成の受信を待機しています	HP Sure Senseでは、実行前にControllerから構成をダウンロードする必要があります。このプロセスが完了するまでお待ちください。
構成のフェッチに失敗しました。ネットワーク接続を確認してください。	HP Sure Senseでは、実行前にControllerから構成をダウンロードする必要があります。コンピューターがインターネットに接続されていることを確認してください。
不明なエラー	この問題を修正するには、HPサポートにお問い合わせください。

## 認証情報保護

認証情報保護には次の3つの状態があります。

- **アクションの必要なし**：すべてが正常に動作しています。
- **アクションを推奨**：アプリケーションが正常ではないため、調査する必要があります。
- **無効**：これは、ブラウザーでこのアドインが無効になっているか、保護全体が無効になっていることを示します。
- 保護されたサイトの数を確認できます



このタイルには、次の状態メッセージが表示されることがあります。

[状態]	説明
Credential Protectionが実行されています	HP Credential Protectionによって、なりすまし攻撃からユーザーが保護されています。



# スタートガイド - HP Wolf Pro Security

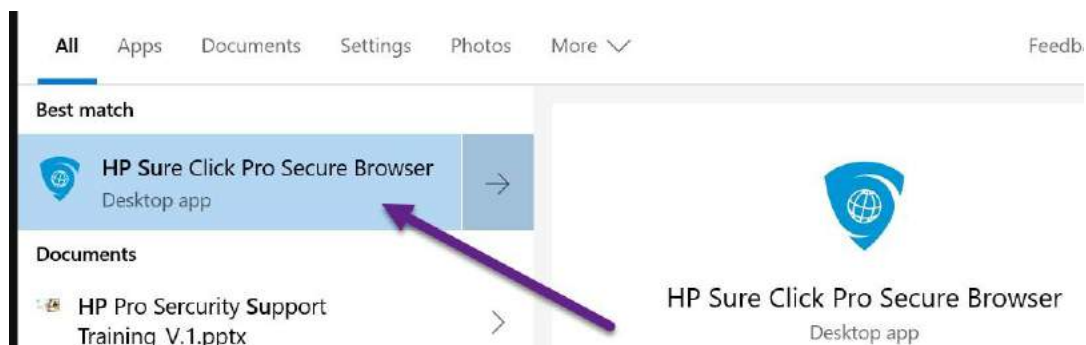
初期設定のブラウザでHP Sure Click Secure Browsing拡張機能が無効になっているようです。有効にしてください。	初期設定のブラウザを開いたときに、HP Sure Click Secure Browsing拡張機能を有効にするように求められることがあります。初期設定のブラウザで、[拡張機能]メニュー項目を選択して[拡張機能]ページを開くこともできます。HP Sure Click Secure Browsing拡張機能を捜して有効にします。
脅威の封じ込めが実行されていません。有効にするか、起動されるまでお待ちください。	HP Sure Click Secure Browsing拡張機能では、HP Sure Click Proが実行されている必要があります。無効になっている場合は、有効にしてください。使用のために準備中の場合は、完了するまでお待ちください。
HP Sure Click Secure Browsing拡張機能が初期設定のブラウザでサポートされていません	HP Sure Click Secure Browsing拡張機能は、HP Sure Click Secure Browser、Google Chrome、Mozilla Firefox、および新しいMicrosoft Edgeで利用できます。Windowsのスタートメニューで「既定のWebブラウザ」を検索して、初期設定のブラウザをこのどれかに変更することができます。
Credential Protectionを実行できません	HP Credential Protectionを実行できません。コンピューターを再起動してみてください。



# スタートガイド - HP Wolf Pro Security

## 安全な閲覧

リスクの高いサイトを閲覧することがわかっている場合は、HP Secure Browserを直接開くことができます。開始するには、以下の操作を行います。



Secure Browserが開きます。他のブラウザの場合と同じように、Webの閲覧を開始します。このブラウザはChromiumベースであり、開いたすべてのタブが隔離されたコンテナで開きます。疑わしいWebサイトがワークフローで必要とされている場合は、このブラウザを使用して直接閲覧します。ポリシーによってリンク保護が有効になっている場合、WPSではこのブラウザで信頼できないリンクを自動的に開きます。

## サポートの利用

### 情報の収集

報告されている問題や実行可能な解決策について説明するために、いくつかの情報が必要になります。問題を迅速に解決するために、以下の情報をIT管理者またはセキュリティ チームに転送して、リクエストの送信を代行してもらいます。

次の**必須**情報を必ず送信してください。

- デバイス名
- 問題の概要
- 解決策の提案の概要：どのような支援が必要であるかわかりますか?
- 一貫して再現可能ですか?
- 解決を早めるために役立つポップアップまたはエラーのスクリーンショットを含めることができますか?

このガイドからの抜粋は、サードパーティの許可を得て提供されており、必要に応じてHPソフトウェアソリューションで再配布されます。

# スタートガイド - HP Wolf Pro Security

---

© 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。

