

HP Wolf Pro Security ポリシー設定ガイド

2022年4月版



はじめに

- この資料はWolf Pro Security のIT管理者様によるポリシーの設定をガイドする目的で作られています。

WPSのポリシーの設定方法

The screenshot shows the HP Wolf Security Controller web interface. The left sidebar contains navigation items: ライセンス, デバイスセキュリティ (highlighted), 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, マルウェア, Credential Protection, イベント, and アカウント. The main content area is titled '(All Devices)' and shows 'グループ情報' (Group Information). A text box contains '(All Devices)' and a note states: 'This built-in group contains all devices known to the controller, whether they are in other group'. Below this, the 'デバイス' (Devices) tab is selected, and the 'グループの構成' (Group Composition) sub-tab is highlighted with a yellow circle. At the bottom, there are filter options for 'デバイスのグループ化', 'リモート管理', and a table header with columns: 'デバイス名', '隔離ステータス', and 'MALWARE PREVENTIONのステータス'.

デバイスセキュリティ→デバイスグループ→（デバイスグループ名）を選択→「グループの構成」から設定できます。

WPSのポリシーの種類

デバイス グループの構成

Sure Click 10
Sure Sense 5

ソフトウェアの更新チャンネル
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）。

Wolf Pro Security GA [Maintained]



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。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



Enable Credential Protection
Credential Protection delivers a browser extension to the endpoints to provide protection against phish

- Sure Clickは仮想による隔離機能を指しています。
- Sure Senseはホスト環境のNGAVを指しています。

ポリシーの説明

Sure Click(脅威の封じ込め)編

Sure Clickのポリシー設定

デバイス グループの構成

Sure Click 10

Sure Sense 5

ソフトウェアの更新チャンネル

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）。

Wolf Pro Security GA [Maintained]

✎

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。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

✎

Enable Credential Protection

Credential Protection delivers a browser extension to the endpoints to provide protection against phish

設定可能なポリシーが10種類あります。

ソフトウェアの更新チャンネル

WPSクライアントの更新頻度の設定項目

ソフトウェアの更新チャンネル

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）。

Wolf Pro Security GA [Maintained]



デフォルト値

「Wolf Pro GA [Maintained]」

GAリリースと共にHPより自動プッシュ
されます。



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



ネイティブブラウザ（ChromeやEdge）を使って開くURLを指定。（仮想ブラウザを利用しない、信頼できるサイト）

イントラネットサイトや社内正規利用のクラウドサービスなどを入れることをお勧めします。

（ブラウザのゼロデイ攻撃を受ける可能性が低いサイト）

例

https://*.google.com

^https://mail.google.com

192.168.1.0/24

Credential Protection(ユーザー資格情報の保護)を有効にする

ネイティブブラウザ（ChromeやEdge）を使っている場合フィッシングサイトなどを検出してユーザーに通知する機能を有効にします。

Credential Protectionを有効にする

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

- オン
- オフ



暗号化されていないHTTPサイトなど警告をしてくれるため有効がお勧めです。

デフォルト値・推奨値
オン

ユーザーがHP Wolf Securityの機能を無効化することを許可する

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

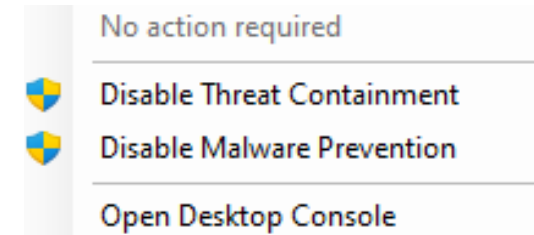


WPSの無効化をユーザーに許可

デフォルト値・推奨値

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

ユーザー表示例：



隔離されたファイルにアイコンのオーバーレイを表示する

[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



隔離対象ファイルに「ウルフ」マークを表示させる。

OneDriveフォルダ配下は「容量節約モード」をOFFにした場合のみ表示されます。

デフォルト値

オン

ユーザー表示例：



WPS_GS_v1.pdf

オーバーレイON



WPS_GS_v1.pdf

OneDrive容量節約
オーバーレイON

リンクに対して保護を有効にする

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



メールやPDFビューアー、Word、Excelなどのアプリケーションに含まれているリンクをクリックした際に仮想環境で実行されるセキュアブラウザを使ってリンクを参照します。

デフォルト値・推奨値
オフ※

※攻撃の99%以上はダウンロードされたファイルからの攻撃であり、リンクを使ったブラウザのゼロデイを狙った攻撃はほぼ発生しないため、推奨値は無効としています。

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



Outlookで受信したすべての添付ファイルを隔離環境で実行します。
(Outlookのみが対象です)

デフォルト値・推奨値
オン

リムーバブルメディアを信頼する権限

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



リムーバブルメディアに保存されているすべてのファイルの保護解除を誰が実行できるか設定します。

デフォルト値
許可済み

推奨値
管理者権限を持つ場合に許可

USBファイル

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



USBドライブに保存されているすべてのファイルを隔離環境で実行するようにします。

コピーされたファイルも同じように隔離されます。

デフォルト値・推奨値
オン

ネットワーク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

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



ネットワークドライブに保存されているすべてのファイルを隔離環境で実行するようにします。

コピーされたファイルも同じように隔離されます。

デフォルト値・推奨値

オフ

ポリシーの説明
Sure Sense(次世代アンチウイルス
NGAV) 編

Sure Senseのポリシー設定

デバイス グループの構成

Sure Click 10

Sure Sense 5

[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

✎

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

✎

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

設定可能なポリシーが5種類あります。

Sure Senseを有効にする

[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



Sure Sense（次世代アンチウイルス-NGAV）を有効化するポリシーです。

デフォルト値・推奨値

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

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

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



Sure Senseがほかのアプリケーションとのバッティングを起こした際にユーザー自身が除外設定を追加を許可する設定。

デフォルト値・推奨値
オン

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

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

Sure Senseが検疫したファイルをユーザー自身が復元することを許可する設定。 ※

※復元されたファイルは自動的に許可リストへ追加されません。

デフォルト値・推奨値
オン



ファイルおよびディレクトリのパス除外

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



Sure Senseが定期スキャンから除外するファイルやディレクトリのパスを指定します。

特にほかのアンチウイルスやEDR、構成管理アプリケーション、DLP製品は除外するようにしてください。（動作が遅くなるなど影響が発生した場合）※

※ Windows Defenderの除外設定は不要です。

プロセス除外リスト

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ビングはサポートされていません

値の追加



Sure Senseがオンアクセススキャンから除外するプロセスパスを指定します。

特にほかのアンチウイルスやEDR、構成管理アプリケーション、DLP製品は除外するようにしてください。（動作が遅くなるなど影響が発生した場合）※

※ Windows Defenderの除外設定は不要です。

ありがとうございました。



keep reinventing