



ユーザーガイド

HP Sure Sense

© Copyright 2019 HP Development Company,
L.P.

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。

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、その保有、使用、または複製には、HP から使用許諾を得る必要があります。FAR 12.211 および 12.212 に従って、商業用コンピューターソフトウェア、コンピューターソフトウェア資料、および商業用製品の技術データは、ベンダー標準の商業用ライセンスのもとで米国政府に使用許諾が付与されます。

本書の内容は、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。本書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、省略に対して責任を負いかねますのでご了承ください。

初版：2019年6月

製品番号：L63508-291

目次

1 お使いになる前に	1
メインメニュータブ	1
フルスキャン	1
脅威からの強化された保護	1
2 セキュリティプロセス	2
マルウェアからの保護	2
検疫のために隔離されたファイルの復元および削除	2
信頼できるファイルの追加および削除	3
除外	3
付録 A HP Sure Sense のアンインストール	4

1 お使いになる前に

HP Sure Sense は、ディープラーニングモデルを用いて悪意のあるファイルを検出し、マルウェア、ゼロデイ攻撃、ランサムウェア、および APT (Advanced Persistent Threat) 攻撃からお使いのコンピューターを守ります。

HP Sure Sense は、以下のコンポーネントを使用します。

- **予測モデル**: 軽量のディープラーニング予測モデルです。これによって、サイバー脅威が自動的に検出され、ゼロデイ攻撃や APT に対する保護が有効になります。
- **ファイルレピュテーションクラウドサービス**: 既知のファイルに関するクラウドベースの情報データベースであり、2 番目の階層の分類を追加します。このオプションが有効になっている場合、PE (Portable Executable) ファイルのハッシュがクラウドのファイルレピュテーションサービスに送信されます。
- **コンテンツデリバリネットワーク**: HP Sure Sense の最新の予測モデルとソフトウェア更新プログラムを配信するシステムです。

メインメニュータブ

メインメニューには、以下のタブが含まれています。

- **[状態]**: 保護の状態や脅威の概要などの情報が表示されます。
- **[アラートログ]**: セキュリティイベントおよびログを一覧表示するテーブルが表示されます。セキュリティ、更新、および管理についての情報が含まれています。このページでは、セキュリティ警告に関する詳しい情報を表示したり、その他の操作を実行したりできます。
- **[検疫]**: 検疫のために隔離されたすべてのファイルを一覧表示するテーブルを表示します。各エントリは、一意のハッシュ値に基づいています。エントリには、ファイルおよびファイルの元の場所に関する情報が含まれます。**[操作]**列から検疫のために隔離されたファイルを復元できます。
- **[設定]**: 通知を表示するかどうかの設定、コンソール言語の設定、その他の設定の管理を行うことができます。**[詳細設定]**を表示または変更するには、**[編集]**を選択し、管理者の資格情報を入力します。

フルスキャン

フルスキャンでは、コンピューターのローカルドライブ上に存在するすべてのファイルが分析されます。悪意のあるファイルとして識別されると、そのファイルはブロックされ、検疫のために隔離されます。

脅威からの強化された保護


脅威からの強化された保護が有効になっている場合は、実行中のすべてのプロセスの動作を監視してマルウェアを探します。プロセスがランサムウェアとして識別された場合、そのプロセスは終了されます。

2 セキュリティ プロセス

マルウェアからの保護

コンピューターのローカルドライブに追加されたすべてのファイルが自動的にスキャンされ、分析されます。悪意のあるファイルとして識別されると、以下の操作が行われます。

- ファイルがブロックされ、検疫のために隔離されます。検疫プロセスがファイルを検疫フォルダーにコピーし、ファイルを元の場所から削除し、検疫テーブルにファイルを追加します。
- **[アラートログ]**ページにイベントが追加されます。脅威から保護されていることを示す通知が表示されます。通知をクリックすると、関連するエントリが強調表示された状態で**[検疫]**ページが表示されます。


 **注記**：外部ストレージデバイスの悪意のあるファイルはブロックされて実行できなくなりますが、検疫のための隔離は行われません。

検疫のために隔離されたファイルの復元および削除

検疫フォルダーに移動したファイルは、必要に応じて復元または削除できます。復元されたファイルは元の場所に移動し、実行できるようになります。検疫のために隔離されたファイルを削除すると、検疫テーブルからそのエントリが削除され、検疫フォルダーからファイルが削除されます。ファイルの分類は変更されず、ファイルの新しいインスタンスはすべてブロックされ、検疫のために隔離されます。

検疫のために隔離されたファイルを削除または復元するには、以下の操作を行います。

1. **[検疫]**ページを開きます。
2. 削除するファイルを選択します。**[操作]**アイコンを選択します。
3. オプションから**[ファイルの復元]**または**[ファイルの削除]**を選ぶか、**[ファイルの詳細]**を表示します。

 **重要**：検疫のために隔離されたファイルを復元する場合は、ファイルがマルウェアではないことを確認してから復元してください。

すべてのファイルを一度に削除するには、以下の操作を行います。

- ▲ **[検疫]**ページで、検索ボックスの右側にあるごみ箱アイコンを選択します。


信頼できるファイルの追加および削除

信頼できるファイルとは、ブロックされた後、ユーザーによって復元され、実行を許可されたファイルです。信頼できるファイルは、**[検疫]**ページまたは**[アラートログ]**ページから、信頼できるファイルの一覧に追加します。プロセスは、**[アラートログ]**ページからのみ、信頼できるファイルの一覧に追加できます。

信頼できるファイルの一覧に追加されたファイルは、元のフォルダーに復元され、検疫フォルダーから削除されます。信頼できるファイルの一覧に追加されたプロセスは、実行を許可され、ランサムウェアの動作監視の対象外になります。信頼できるファイルの一覧に追加されたファイルおよびプロセスは、スキャンされません。

信頼できるファイルまたはプロセスを追加するには、以下の操作を行います。

1. **[アラートログ]**ページを開きます。
2. 追加するファイルまたはプロセスのエントリで、**[操作]**アイコンを選択します。
3. ファイルを追加するには、**[ファイルの復元]**を選択します。
プロセスを追加するには、**[[信頼できるファイル]に追加]**を選択します。

 **重要**：信頼できるファイルの一覧にファイルまたはプロセスを追加する場合は、マルウェアではないことを確認してから追加してください。

信頼できるファイルの一覧からファイルまたはプロセスを削除するには、以下の操作を行います。

1. **[設定]**ページで、**[信頼できるファイルの編集]**を選択します。
2. 削除するファイルまたはプロセスを選択し、**[操作]**アイコンを選択します。
3. ファイルを削除するには、**[検疫ファイル]**を選択します。
プロセスを削除するには、**[一覧から削除]**を選択します。

除外

フォルダーおよびプロセスは、**[除外]**オプションを使用してスキャンされないようにすることもできます。

 **重要**：フォルダーを除外リストに追加する前に、以下の対策を行うことをおすすめします。

- 読み取り専用フォルダーのみを追加すると、信頼できるフォルダーが攻撃者によって悪用される可能性を最小限に抑えることができます。
- 一時フォルダーを追加しないでください。マルウェアは、モジュールを一時フォルダーに書き込む傾向があります。この推奨事項は、Windows®または system32 などのシステムフォルダーにも該当します。
- 特定のソリューションに対して誤検知が繰り返される場合は、ソリューションのベンダーに推奨事項を問い合わせてください。

除外リストにアクセスするには、以下の操作を行います。

1. **[設定]**ページを開き、**[詳細設定]**まで下にスクロールします。
2. **[[除外]の編集]**を選択します。

A HP Sure Sense のアンインストール

HP Sure Sense が現在インストールされていて、新しくインストールする必要がある場合は、まず現在のバージョンを削除する必要があります。アンインストールの方法は、HP Sure Sense をどのようにインストールしたかによって異なります。

インストールウィザードを使用して手動で HP Sure Sense をインストールした場合は、以下の操作を行います。

▲ インストーラーを実行し、**[アンインストール]**を選択します。

お使いのデバイスに HP Sure Sense がプリインストールされていた場合は、以下の操作を行います。

1. **[Windows の設定]**の**[アプリと機能]**に移動します。
2. **[HP Sure Sense Installer]**をアンインストールします。