



## サービスのメリット

- 複数階層の保護によって既知と未知のあらゆるサイバー攻撃に対応し、エンドポイントを保護
- 従業員の生産性を阻害することなくサイバー攻撃から保護

## サービスの特徴

- 高度な複数階層のリアルタイム防御によって、エンドポイントセキュリティに対応
- セキュリティの専門家による管理
- タイムリーで実用的な分析と洞察

## サービスの概要

HP Proactive Securityは、中規模企業に最適な規模の複数階層からなるエンドポイントセキュリティ サービスを提供し、組織の安全維持に役立ちます。<sup>1</sup> エンドポイントのセキュリティを管理する保護優先のアプローチによって攻撃のリスクを軽減し、IT部門の負担が増えることもなく、ユーザーはどこからでも安全に作業できるようになります。

HP Proactive Securityには、ディープラーニングと隔離テクノロジーを組み合わせた、複数階層の保護によるマルウェア対策、実用的な洞察、マネージドサービスとして提供されるセキュリティ エキスパートによる管理が統合されています。

## 機能と仕様

### 保護

HP Proactive Securityは、コンピューティング エンドポイントに対して、[HP Sure Sense Advanced] および[HP Sure Click Advanced]を含めた高度な複数階層の保護を提供します。<sup>2</sup>

[HP Sure Sense Advanced]のディープラーニングに基づく保護テクノロジーは、何億ものマルウェアのサンプルに対してトレーニングされ、非常に巧妙に偽装されたマルウェアファイルでも難なく認識し、一意のシグネチャに依存するのではなく、その特性に基づいてファイルレス攻撃の脅威を検出できる性能を誇ります。このソリューションでは、既知のマルウェアを止めるだけでなく、ゼロデイ攻撃を行う未知のマルウェアも検出できます。しかも、クライアントを更新する必要はありません。

[HP Sure Click Advanced]は、他のエンドポイント保護を回避した脅威を封じ込めるための最終防衛ラインとして、隔離テクノロジーを使用します。ユーザーのPCをサイバー攻撃から保護するため、電子メールの添付ファイル、ファイルのダウンロード、さらにはUSBドライブの中身さえ、アプリケーション隔離によって切り離されたマイクロVMの内部で開きます。また、隔離中の脅威のアクティビティも監視します。これにより、攻撃のキルチェーンをより深く調査できます。

HP Proactive Securityは、これら2つの高度な補完的テクノロジーを組み合わせ、デバイスに対して複数階層からなるプロアクティブな保護をリアルタイムで提供します。

## 機能と仕様（続き）

### 洞察

HP Proactive Securityは、AIベースの強力な分析プラットフォームであるHP TechPulseを通して、実用的な洞察をお客様に提供します。<sup>3</sup>ITチームは、デバイスの保護状態の監視、レポートの表示、および保護されていないデバイスやブロックされた脅威のアクティビティに関するアラートの受信が可能です。これらはすべて、統合されたワンストップのダッシュボードから利用できます。

### 管理

純粋なソフトウェアソリューションとは異なり、HP Proactive Securityはマネージドサービスとして提供されます。HPセキュリティエキスパートは、お客様の代わりに脅威の隔離を管理するなど、構成およびセキュリティポリシーの実装と管理を行います。デバイスのオンボーディングが完了すると、HPセキュリティエキスパートはデバイスのセキュリティ保護状態を監視します。そして、これまでに見つかっていないゼロデイ攻撃の脅威に対して、ソースを特定して将来の攻撃からお客様を保護するために、フォレンジック分析およびキルチェーン分析を実施します。

カテゴリ	機能
保護	[HP Sure Sense Advanced] : AIベースの脅威防御。Windows 10、Mac OS、およびAndroidデバイス向け [HP Sure Click Advanced] : Windows 10向けの添付ファイルおよびダウンロード隔離
セキュリティレポート	会社のセキュリティへの準拠レポート 安全性に疑問があるデバイスレポート デバイスのセキュリティへの準拠レポート レポートしないデバイスレポート [HP Sure Click Advanced]のセキュリティレポート [HP Sure Sense Advanced]のセキュリティレポート
セキュリティインシデント	[HP Sure Click]の保護されていないデバイス [HP Sure Click]のTrue Positiveの隔離された脅威 [HP Sure Sense]の保護されていないデバイス [HP Sure Sense]の防止された脅威
管理	ポリシーの調整および設定 脅威の分析および洞察 セキュリティエージェントの状態モニター セキュリティエージェントの更新 詳細な[HP Sure Click Advanced]の脅威レポート <sup>4</sup> 可能性のあるソースおよび推奨される修復手順（該当する場合）を12営業日以内にお客様に提供します。
その他の機能	HP APIによるSIEMの有効化

## サービスの仕様

HPによって管理されるデバイスには、リアルタイム保護を提供し、デバイスの情報を収集するためのソフトウェア エージェントがインストールされています。セキュリティ ポリシーのセットアップまたは更新、およびお客様への洞察の提供には、インターネット接続が必要です。セットアップの完了後は、これらのソフトウェア エージェントの保護の利用時にインターネット接続が必要になることはありません。資格情報、ファイル、コンテンツ、および個人データなどのユーザーの機密データは取り込まれません。収集されたデータは安全なクラウドリポジトリに保管されます。<sup>5</sup>

お客様のためのポータルが提供され、ダッシュボード、レポート、インシデントなど、セキュリティの洞察情報にアクセスできます。

認定されたセキュリティ エキスパートが、お客様のためにエンドポイントセキュリティをプロアクティブに管理します。この管理には、セキュリティ ポリシーの調整および設定、True Positiveの脅威が検出された場合のインシデントの分析、[HP Sure Click Advanced]で新規の脅威またはゼロデイ攻撃の脅威が捕捉された場合の詳細な分析レポートの提供、セキュリティ エージェントの更新の管理、エージェントの状態に関連する問題の調査などが含まれます。

HPサービス エキスパートは第1レベルのカスタマー サポートを提供し、お客様が報告した問題を解決するためにセキュリティ エキスパートを含めたHP社内のチームと連携します。HPサービス エキスパートのサポート体制は以下のとおりです。

- **日本：**  
窓口受付時間：月曜日～日曜日 9:00～21:00  
サポート方法：メール  
メールアドレス：hpdaas\_japan@hp.com

### お客様の責任

- HPがアカウントをセットアップできるように必要な情報を提供する
- お客様の管理対象デバイスにHP Proactive Securityエージェントを展開する
- 管理対象ユーザーおよびデバイスの追加または削除を要求する
- ホワइटリストに登録されたWebサイト、ダウンロードサイト、および電子メールアドレス（添付ファイルの隔離用）の追加または削除を要求する
- 隔離の対象にしない会社のIPアドレス範囲の追加または削除を要求する
- 隔離されたファイルのリリースまたはブロックされたファイルの除外を要求または承認する
- HP TechPulseコンソールにログオンしてダッシュボード、レポート、インシデントを確認する
- セキュリティ レポートを確認し、必要に応じて対処する



## システム要件

プラットフォーム	OSの要件	ハードウェアの要件
Windows	一般的に利用できる最新のWindows 10 OSリリース、または2つ前までのメジャーリリース	<b>HP Sure Click Advanced<sup>2, 6</sup></b> <ul style="list-style-type: none"><li>• BIOS/UEFIで仮想化テクノロジーを有効にしたIntel Core i3、i5、i7（または、最新のAMD CPU）</li><li>• 8GB以上のRAM</li><li>• 6 GB以上のディスク空き容量</li></ul> <b>HP Sure Sense Advanced</b> <ul style="list-style-type: none"><li>• 8 GB以上のRAM</li></ul>

### サードパーティ ソフトウェアの要件

Adobe Acrobat Reader DCをPDFファイルの初期設定アプリケーションにする必要があります。

### ネットワーク要件

管理対象デバイスとクラウド管理サービスとの通信にはインターネットへの接続が必要です。

### 前提条件

- 本サービスを提供するハードウェア製品の合計台数は50台以上である必要があります。
- サービスを使用するには、購入後にHPの指示に従って登録する必要があります。オンボーディングプロセスでは、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。
- 途中解約によるお支払い済のサービス料金※は返金はできかねますので、予めご了承ください。サービス料金はHPの[Webサイト](#)を参照ください。

## 制限事項

HP Proactive Securityは、不審なコンテンツまたは悪意のあるコンテンツを自動的にブロックまたは隔離して、デバイスを確実に保護します。HP Proactive Securityには、セキュリティ侵害の場合の修復サービスなどは含まれません。

## 使用条件

このサービスをHP Care Packとして購入した場合、[HP Care Packの取引条件](#)が適用されることがあります。

[HP TechPulseの使用条件](#)、[HP Personal Data Rights Notice](#)<sup>7</sup>（個人データの権利に関する通知）、および[HPのプライバシーに関する声明](#)は、すべてこのサービスに適用されます。

## 詳細情報

詳しくは、お近くのHPパートナーまたはHP営業担当者にお問い合わせになるか、HPのWebサイト、<http://www.hp.com/jp/proactive/>を参照してください。

1. HPのサービスは、ご購入時にお客様に提供または提示される、適用可能なHPサービス使用条件に準拠します。お客様によっては該地域の法令に従ってその他の法的権利を有することもあり、当該権利はHPサービスお取引条件書またはお使いのHP製品に付属のHP限定保証による影響を一切受けません。完全なシステム要件については、<https://www.hpdaas.com/requirements/ja/>を参照してください。
2. [HP Sure Click Advanced]のテクノロジーはHP Proactive Securityに含まれ、Windows 10およびMicrosoft Internet Explorer、Google Chrome、またはChromiumを必要とします。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。
3. HPは、ユーザーがアクセスしたURLを特定する詳細情報を追跡または監視しません。HP TechPulseのレポートは、脅威およびそのソースの特定に焦点を合わせています。HP TechPulseはGDPRおよびISO 27001に準拠しています。
4. HPサービス エキスパートによる脅威の分析は、[HP Sure Click Advanced]ソフトウェア クライアントによってマルウェア イベントがブロックまたは隔離された後にトリガーされるフォレンジック プロセスです。24時間365日の「リアルタイム」監視サービスではありません。[HP Sure Click Advanced]クライアント エージェントは、不審なコンテンツまたは悪意のあるコンテンツを自動的に隔離して、分析の前に確実に保護します。また、セキュリティ侵害の場合には、どちらのプランにも修復サービスなどは含まれません。
5. クライアント デバイスからWebサーバーへのデータ転送中のデータはSSLを使用して保護されます。データはHP DaaS Webサーバー経由でのみアクセスできます。
6. サポートされるWindows 10のバージョンの完全なリストについては、BromiumのWindowsサポート ポリシー（英語サイト）を参照してください。HP Proactive Securityでは、Windows 7および8.1はサポートされていません。
7. HP Personal Data Rights Noticeは、日本国内のみでの利用の場合、適用されません。

© Copyright 2020 HP Development Company, L.P. 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。AdobeおよびAcrobatは、Adobe Systems Incorporatedの商標です。AppleおよびmacOSは、米国およびその他の国で登録されたApple Inc.の商標です。Android、Google、Chrome、およびChromiumは、Google Inc.の商標です。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。

