HP Sure Click Enterprise (SCE)

HP Wolf Pro Security (WPS)

詳細比較表

HP SCE vs HP WPS 比較表
（ 全体 ）

販 売	HP WOLF PRO SECURITY	HP SURE CLICK ENTERPRISE
対象製品	マルチベンダー対応	マルチベンダー対応
販売方法	有償 （ 単品ソフトウェア ）	有償 （ 単品ソフトウェア ）

機 能	HP WOLF PRO SECURITY	HP SURE CLICK ENTERPRISE
脅威の封じ込め （ マイクロ仮想マシン ） HP Sure Click	◎	◎
ユーザ資格情報の保護 （ フィッシング防止 ） HP Sure Click	◎	◎
次世代アンチウイルス （ NGAV ） HP Sure Sense	◎	-
統一管理/分析サーバ （ 環境 ） HP Wolf Security Controller	クラウド	クラウド or オンプレミス
統一管理/分析サーバ （ ポリシー設定 ） HP Wolf Security Controller	○	◎
最小ライセンス数（ MOQ ）	25	250

詳細は
次ページ
以降

HP SCE vs HP WPS 比較表
（ HP Sure Click ポリシー設定 ）

※2022/10/13時点の情報です。

HP WPSでは、HP SCEに比べて、HP Sure Click に関して設定可能な項目が限られています。
(HP SCEは、標準項目100程度に加えて、数千以上のパラメータによりカスタマイズが可能です。)

HP WPSで設定可能な、HP Sure Click に関する項目は以下となります。

HP WPSで設定可能な項目	
信頼できるWebサイト	リムーバブル メディアを信頼する権限
信頼できる内部電子メールドメイン	USBメモリファイルに対する保護の有効化
Credential Protection機能の有効化	ネットワーク（ UNC ）ドライブの保護の有効化
ユーザーが機能を無効にすることを許可	ホスト上にナビゲートするブラウザ以外のURL スキーム
隔離されたファイルにブルータグを表示	ロギングの有効化
隔離実行中のアプリケーションに青枠を表示	信頼されていないドキュメント実行時のメッセージ表示
リンクに対する保護の有効化	IMEサポートの拡張設定
Outlook の添付ファイル保護の有効化	

HP WPSで設定できない主な項目は以下です。詳細は次ページ以降を参照ください。

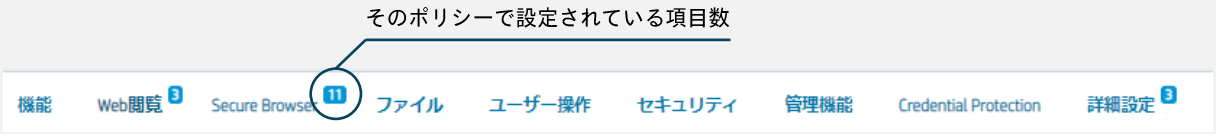
HP WPSで設定できない主な項目（※導入時にHP側で設定が可能な場合があります。詳しくは営業までご相談ください ）	
ドキュメント種別ごとの保護の有効化	セキュアブラウザ拡張機能の制御
ファイルの個別信頼設定	コピー＆ペースト許可の詳細設定
ファイルアップロード/ダウンロード禁止設定	イングレスアプリケーション
個別プロキシ設定	

HP Sure Click Enterprise

ポリシー設定概要および、

WPSポリシーとの比較

HP Sure Click Enterprise ポリシー設定 大項目



HP SCEのポリシー設定は、大きく以下の大項目に分かれます。

大項目	説明
機能	マイクロVM環境で実行するアプリケーション設定
Web閲覧	信頼サイトに関する設定やProxy認証、イントラサイトへのアクセス設定など
Secure Browser	マイクロVMで隔離実行されるChromiumベースのセキュアブラウザに関する設定
ファイル	ダウンロードやメール添付等ファイルの信頼に関する設定 （ユーザーの信頼権限、自動信頼、ファイルハッシュによるアクセスブロック等）
ユーザー操作	ユーザ環境の設定（エンドポイント構成変更時の再初期化、確認・警告ダイアログ表示、信頼できないファイルのアイコン視覚的なタグ付け、トレイアイコン表示等）
セキュリティ	ユーザのファイル操作に関する禁止設定、リアルタイムの脅威データ提供するインテリジェンスクラウドサービスへの接続許可、カット＆ペーストの制限などに関する設定
管理機能	詳細な分離ログファイル、ポリシー更新やリモートコマンド等、管理に関する設定
Credential Protection	アイデンティティ保護に関する設定
詳細設定	既存設定項目にないカスタム設定

HP Sure Click Enterprise ポリシー設定機能 1/1

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
ブラウザー保護		
Internet Explorer	Internet Explorerの保護を有効にします	ON
Chrome(HP Secure Browser)	Chrome(HP Secure Browser)の保護を有効にします	OFF
Firefox	Firefoxの保護を有効にします	OFF
ドキュメントとファイルの保護	ドキュメントとファイルの保護を有効にします	ON
[Outlook] の添付ファイル	Outlook添付ファイルの保護を有効にします	ON
USB ファイル	USBメモリのファイルの保護を有効にします	ON
保護されるファイルの種類		
Word	Wordの保護を有効にします	ON
PowerPoint	PowerPointの保護を有効にします	ON
Excel	Excelの保護を有効にします	ON
PDFドキュメント	PDFの保護を有効にします	ON
イメージ	画像の保護を有効にします	ON
動画	ビデオの保護を有効にします	OFF
アーカイブ	圧縮ファイルの保護を有効にします	ON
実行可能ファイル	実行可能ファイルの保護を有効にします	ON
その他のファイルの種類	その他のファイルタイプの保護を有効にします	OFF

HP Sure Click Enterprise ポリシー設定
Web 閲覧 1/2

青字：WPSで設定変更が可能な項目

ポリシー項目		説明	Default
信頼できるWebサイトのオプション			
	信頼できるWebサイト	隔離せずにネイティブで開く信頼できるWebサイト（ホワイトリスト）を入力します	未設定
	ユーザーが一時的にWebサイトを信頼することを許可する	ユーザーが一時的にWebサイトを信頼できるようにします	User can trust sites but must first enter a reason
	一時的な信頼のワークフローのためにUACが必要	Webサイトを一時的に信頼するときにユーザーは特権の昇格が必要になります	OFF
	脅威アラートがトリガーされている場合に一時的な信頼を許可しない	現在のセッション中に脅威アラートが上がったWebサイトをユーザーが一時的に信頼できないようにします	OFF
IEの広告ブロック		この設定を有効にすると、Internet Explorerサイトに広告が表示されなくなります	ON
[Google Chrome]拡張機能を有効にする		Chrome拡張機能のインストールを許可するには、この設定を有効にします	ON
	許可される[Chrome]拡張機能	許可するChrome拡張機能のリストを入力します	未設定
	ブロックされる[Chrome]拡張機能	禁止するChrome拡張機能のリストを入力します	未設定

HP Sure Click Enterprise ポリシー設定
Web 閲覧2/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
プロキシ認証 (SSO)	企業のプロキシ認証サーバーのアドレスのリストを入力します。	OFF
ネットワークからの分離を有効にする	この設定を有効にすると、マイクロVM内のコンテンツから内部ネットワーク/イントラネットが非表示になります	OFF
イントラネットサイト	企業のイントラネットDNSおよびネットワークゾーンのリストを入力します。	未設定
イントラネットサイトを信頼	この設定を有効にすると、イントラネットサイトリストにリストされているサイトを信頼済みとしてマークし、これらのサイトの隔離を無効にしてネイティブに開きます。	ON
Cloud/SaaS サイト	このリストは、組織にとって価値のあるクラウド/ SaaS Webサイトを識別します。これらのWebサイトはマイクロVMで開きますが、このリストにない他のマイクロVMからは見えないようになります。	OFF
社内ネットワーク上にない場合はイントラネットサイトを隔離する	有効にすると、企業ネットワークに接続されていないデバイスは、イントラネットサイトリストで定義されたサイトも隔離して保護します。	OFF
社内ネットワーク上にない場合は信頼できるサイトを隔離する	有効にすると、企業ネットワークに接続されていないデバイスは、信頼済みサイトリストで定義されたサイトも隔離して保護します。	OFF

HP Sure Click Enterprise ポリシー設定
Secure Browser 1/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
[Secure Browsing]拡張機能		
[Chrome]で有効にする	ChromeでSecure Browsing eXtension(SBX)機能が有効になります。	ON
[Microsoft Edge Chromium]で有効にする	EdgeでSecure Browsing eXtension(SBX)機能が有効になります。	ON
[Firefox]で有効にする	FirefoxでSecure Browsing eXtension(SBX)機能が有効になります。	ON
[Secure Browsing]拡張機能の設定		
リンクに対して保護を有効にする	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がHP Secure Browserで開きます。	OFF
ファイルURL（file:// ）に対する保護を有効にする	File://を使用する信頼できないファイルリンクURLがHP Secure Browserで開きます。	ON
コンテンツの種類がPDFのリンクに対する保護を有効にする	コンテンツタイプPDFのナビゲーションリンクがHP Secure Browserで開きます。	OFF
信頼できないWebサイト	このリストは、HP Secure Browserで開く特定のWebサイトを識別します。	未設定
[HP Sure Click]で管理される信頼リスト	この設定により、エンドポイントはHP脅威インテリジェンスから信頼済みサイトのリストをダウンロードできます。このリストには、HPが推奨するWebサイト（Web会議サイトなど）が含まれており、一般的にワークフローが中断されないように顧客環境に追加されます。	ON
イントラネット上の信頼リストだけを使用する	企業ネットワークに接続されているときのみ信頼できるサイトのリストを使用します。	OFF

HP Sure Click Enterprise ポリシー設定 Secure Browser 2/2

青字：WPSで設定変更が可能な項目

ポリシー項目		説明	Default
以下のソースからのフィッシング リンクからユーザーを保護する			
	アプリケーション	セキュアブラウジング拡張機能を使用してリンクを開くチャットクライアントなどの特定のアプリケーションを識別します。タスクマネージャーの[詳細]ペインに表示されるプロセス名を入力します。	OFF
	Gmail 【固有】	セキュアブラウジング拡張機能を使用してリンクを.開くGmail URLを識別します。	OFF
	Webメール	セキュアブラウジング拡張機能を使用してリンクを開く特定のウェブメールサイト（Gmailを除く）を識別します。	OFF
	ユーザープロンプトを有効にする	すべてのフィッシングリンクがユーザーにSecure Browserで開くかどうかを尋ねます。無効にすると、ユーザープロンプトは表示されず、すべてのフィッシングリンクがSecure Browserで直接開きます。	OFF
信頼できるサイトのリストを無視する		これを有効にするとSecure Browserを使用するときに、信頼済みサイトリストにリストされているサイトはすべて無視されます。	ON
信頼できるダウンロードサイト		保存されたファイルを信頼済みとしてマークする特定の信頼済みサイトを識別します。	$bromium_trusted_group※
信頼できないブラウザーファイルの種類に対して[Secure Browser]を使用する		.htmlなどの信頼できないブラウザファイルタイプにセキュアブラウザが使用されます。	ON
[Chrome]のリダイレクトを有効にする		ユーザーは常にSecure Browserを使用するようにリダイレクトされます。	OFF
[Google Chrome]の外観		HPセキュアブラウザーがエンドユーザーにどのように表示されるかを制御します。ブラウザは、ネイティブのChromeとして、またはHPアイコンとブラウザ名とともにユーザーに表示できます。	Use HP Secure Browser appearance

※ $bromium_trusted_group = Trusted Websitesで登録されているURLs

HP Sure Click Enterprise ポリシー設定ファイル 1/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
ユーザーがファイルを信頼することを許可する	ユーザーがファイルを信頼済みとしてマークできるかどうかを指定します。	YES
ユーザーは理由を入力する必要がある	ユーザーはファイルを信頼できますが、最初に理由を入力する必要があります。	OFF
複数ファイルの信頼	ユーザーが複数のファイルを信頼すると自動的にチェックを実行し、それらが悪意があると判断された場合、それらのファイルの信頼を許可しません。	OFF Allow user to choose
信頼できるサイトからのファイルダウンロードの初期設定の状態	「信頼済みサイト」、「イントラネット」、および「IE信頼ゾーン」にリストされているサイトからブラウザーで保存されたファイルを、信頼済みまたは非信頼としてマークします。	Use ADS zone identifiers
ネイティブブラウザからのファイルダウンロードの初期の設定	ネイティブブラウザで保存されたすべてのファイルを信頼できないものとしてマークするか、ADSゾーン識別子を持つファイルのみをマークします。	Use ADS zone identifiers
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。	OFF
自動的に信頼するファイルの種類	コンテンツチェックでファイル拡張子との一致が確認された場合に自動的に信頼できるとマークされるファイルタイプを指定します。	Appendix 参照
信頼に権限の昇格が必要なファイルの種類	ユーザーが信頼済みとしてマークするためにWindowsユーザーアカウント制御プロンプトを介して認証する必要があるファイルの種類を指定します。	Appendix 参照
署名によるファイルの種類の信頼	署名またはファイルハッシュによって、自動または手動で信頼するファイルの種類を指定します（特権の昇格が必要）。	OFF

HP Sure Click Enterprise ポリシー設定ファイル 2/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
信頼できる内部電子メール ドメイン	内部メールの添付ファイルを自動信頼できます。信頼する内部電子メールSMTPドメインのリストを入力します。	OFF
信頼できる内部電子メール ドメインからの[Outlook]添付ファイルの信頼	Exchangeサーバーとドメイン間で受け渡すOutlook添付ファイルの信頼情報を許可します。	ON
[Outlook]からの添付ファイルを信頼する	Outlookからの添付ファイルを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かどうかを制御します。 Outlookを使用している場合、HP Sure Click 対応デバイスはメタデータを電子メールに追加して、特定の信頼できる/信頼できない添付ファイルを識別できるようにします。	Treat attachment as trusted based purely on the sender domain being a trusted email domain.
リムーバブル メディアを信頼する権限	ユーザーがドライブを信頼済みとしてマークできるかどうか、および必要な認証を指定します。	管理者権限を持つ場合に許可
リムーバブル ドライブ（USB）の信頼設定を記憶する	この設定を無効にすると、ユーザーが切断またはログオフすると、リムーバブルメディア（USBなど）の信頼設定がリセットされます。	ON
[SharePoint]のWebDAV共有上のファイルを信頼する	SharePoint WebDAV共有上のファイルを信頼できないものとしてマークするかどうかを制御します。	All files are trusted
イングレス アプリケーション	選択したアプリケーションは、ダウンロードしたファイルを信頼できないものとして保存します。	Appendix参照
ブロック リストのサポート	管理者はファイルハッシュを指定してファイルへのユーザーアクセスをブロックできます。検疫するファイルを識別するために、アラートの手動トリアージ（優先順付け）が必要です。エンドポイントの隔離もパフォーマンスに影響する場合があります。	OFF

HP Sure Click Enterprise ポリシー設定
ユーザー操作 1/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
ユーザーが[HP Wolf Security]の機能を無効にすることを許可する	この設定を無効にすると、ユーザーはユーザーインターフェイスを介して隔離をオフにできなくなります。	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
[HP Sure Click]を自動的に有効にする	HP Sure Clickが有効になっていない場合の自動有効化動作を決定します。	Auto-enable after an upgrade
システム アップデート時の初期化動作	バージョンの変更など、特定のデスクトップ構成が変更された場合、再初期化が必要です。再初期化が必要になった場合の再初期化動作を選択できます。	Immediately
印刷の確認を表示する	印刷時にユーザーに確認ダイアログを表示するかどうかを決定します。これにより、悪意のあるコンテンツがユーザーの知らない間にプリンターにアクセスしようとするのを防ぎます。	OFF
PDF署名の確認を表示する	PDFにデジタル署名するときに確認ダイアログをユーザーに表示するかどうかを決定します。これにより、悪意のあるコンテンツがユーザーの知らないうちにホストの証明書ストアにアクセスしようとするのを防ぎます。	OFF

HP Sure Click Enterprise ポリシー設定
ユーザー操作 2/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
ファイルを信頼する際にユーザーに警告する	信頼されていないファイルを信頼する際にユーザーに警告が表示されます。	ON
[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	信頼できないと識別されたファイルとドライブが他のファイルと異なることを視覚的に示すためにHPロゴが表示されます。	ON
Display border on isolated applications	有効にすると、隔離されたマイクロ VM で安全に開かれたドキュメントが青い境界線で表示されます。	ON
ネットワーク隔離の違反を表示する	サイトが構成にリストされている他のWebサイト（SaaSサイトリストなど）からリソースをプルする場合、Webページが期待どおりに表示されない場合があります。構成設定によってコンテンツがブロックされたときに警告が表示されます。	ON
エンド ユーザー メッセージ	エンドユーザーに表示するメッセージがあれば、それを構成します。	Don't display any message popups
[HP Wolf Security]のトレイ アイコンを表示	ユーザーのタスクバー領域にHP Sure Clickトレイアイコンを表示するかどうかを決定します。	ON
Enable product education messages	有効にすると、ユーザーが信頼できないドキュメントを開くときに紹介メッセージが表示されます。	ON
Enable Input Method Editor (IME) Support	複雑な文字セットを持つ言語 (通常は東アジア言語) のサポートを強化できる拡張入力方式エディター (IME) を有効にします。 これは、そのようなサポートを必要とするエンドポイントにのみ使用してください。	OFF

HP Sure Click Enterprise ポリシー設定
セキュリティ1/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
悪意のあるドキュメントの信頼をブロックする	ユーザーがドキュメントを信頼しようとしたときに、自動的に隔離された脅威チェックを実行し、悪意があると判断された場合に信頼を許可しません。	ON
悪意のある実行可能ファイルの信頼をブロックする	ユーザーが実行可能ファイルを信頼しようとしたときに、自動的に隔離された脅威チェックを実行し、悪意があると判断された場合、信頼されません。	ON
悪意のあるスクリプトの信頼をブロックする	ユーザーがスクリプトを信頼しようとしたときに、隔離された脅威チェックを自動的に実行し、悪意があると判断された場合、信頼されません。	ON
隔離によって保護されたアクセスを提供できない場合、保護されないアクセスを許可する	この設定をオフにすると、保護されたアクセスが提供できない場合に、ユーザーがイントラネットまたは信頼済みサイトとしてマークされたWebサイト以外のWebサイトにアクセスしたり、信頼できないドキュメントを開くことができなくなります。これは通常、最初の初期化プロセスの間に起こります。 これをチェックすると、いつでもインターネットの閲覧と信頼できないドキュメントのオープンが許可されますが、システムはこの最初の初期化中やテンプレートが利用できないときは保護されません。	ON
サポートされないバージョンのPDFおよびOfficeドキュメントを自動的に信頼しますか？	サポートされていないバージョンのMS OfficeまたはAcrobatがデスクトップにインストールされている場合、OfficeおよびPDFファイルは自動的に信頼されます。	ON
[HP Threat Intelligence]を有効にする	リアルタイムの脅威データを提供するHP Threat Intelligence Serviceへのデバイスの接続を許可します。このデータは、実行可能ファイルのマルウェア分析の実行に使用されます。	ON
ファイルに対して[HP Threat Intelligence]を有効にする	HP Threat Intelligence Serviceデータを使用した、ファイルのマルウェア分析を有効にします。	ON

HP Sure Click Enterprise ポリシー設定
セキュリティ2/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
脅威イベントの際にユーザーにアラートを表示する	Webブラウジングまたはドキュメントを開いている間に隔離環境が悪意のあるアクティビティを検出した場合に、ユーザーにアラートを表示するかどうかを制御します。感染したドキュメントまたはWebページは、実行の継続または停止を許可できます。	何も表示せずに操作を続行
クリップボードのアクセスポリシー	隔離されたドキュメントまたはWebページへの、および、そこからのカットアンドペーストアクセスを制限します。	隔離されたWebサイトおよび信頼できないドキュメントからのクリップボードへのユーザー アクセスと自動アクセスの両方を許可
クリップボードのデータの保護	この設定は、クリップボードを介して信頼できないWebページおよびドキュメントから他の信頼できないWebページ、ドキュメント、およびユーザーのデスクトップにコピーできるオブジェクトのタイプを制御します。	ノーマル（ほとんどのユーザーに推奨）
プロアクティブな[Outlook]添付ファイルのチェック		
完全なマイクロVM動作チェック	Outlook電子メールに添付ファイルが含まれている場合、添付ファイルは到着時にマイクロVMで分離され、完全な動作分析のために悪意があるかどうかを判断します。この機能は、完全なOutlookクライアントアプリケーションでのみサポートされています。	ON
[HP Threat Intelligence]によるチェックのみ	Outlook電子メールに添付ファイルが含まれている場合、到着時に添付ファイルのハッシュがHP Threat Intelligence Serviceに対してチェックされ、悪意があるかどうかが判断されます。この機能を使用するには、HP Threat Intelligence Serviceを有効にする必要があり、完全なOutlookクライアントアプリケーションでのみサポートされています。	ON
List of non-browser URL schemes to navigate on host	ホスト上へナビゲートする、ブラウザ以外の URLスキームのリストを定義します。	Appendix参照

HP Sure Click Enterprise ポリシー設定管理機能 1/1

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
ロギングを有効にする	詳細な分離ログファイルを許可するには、この設定を有効にします。	ON
隔離のアップデート間隔	この設定は、隔離ポリシーの更新とリモートコマンドのチェックインの頻度を制御します（秒単位）。	900
無効なサーバー証明書を無視する	この設定を有効にすると、無効または信頼されていないHTTPS証明書がサーバーにインストールされている場合でも、ポリシーの更新のダウンロードとステータス情報のアップロードが可能になります。このオプションは安全ではないため、テスト目的でのみ使用してください。	OFF
製品ライセンス キー	製品のライセンスキーのリスト。通常の展開では、単一のライセンスキーのみが使用されますが、複数のキーが提供される場合があります。	[License keys]

HP Sure Click Enterprise ポリシー設定
Credential Protection 1/1

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	Default
Credential Protectionを有効にする	クレデンシャル保護を有効にします。ブラウザ拡張機能をエンドポイントに提供して、フィッシングリンクに対する保護を提供します。	ON
操作モード	アラートがコントローラーに送信されるタイミング、および警告オーバーレイがユーザーに表示されるタイミングを制御します。	(Blocklist Only Mode) Only prevent access to blocked sites. Send user and controller alerts when a blocked site is visited. No controller or user alerts on unknown sites.
不明なサイトでのユーザー入力を許可する	不明なサイトのフィッシング警告を確認した後、ユーザーが資格情報を入力できるようにします。チェックを外すと、不明なサイトはブロックされたサイトのように扱われ、ユーザーは資格情報を入力できなくなります。	OFF
パスワードが自動的に入力されるページを自動的に許可する	ブラウザまたはパスワードマネージャがユーザーの既知のサイトのパスワードを自動的に入力する場合は、それを信頼できるものとして扱い、ユーザーに警告しません。	ON
HTTPログインページをブロック済みとして扱う	HTTP (クリアテキスト) ログインサイトをブロックされたものとして扱い、すべての入力を防ぎ、ユーザーに通知します。	OFF
Webサイトのスクリーンショットを許可する	未知のWebサイトのスクリーンショットを含めて、潜在的なフィッシングサイトのより正確なトリアージを可能にします。	ON

HP Sure Click Enterprise ポリシー設定
詳細設定 1/2

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	設定例
Advanced.Browser.SBX.PrioritiseTrustedSites	有効になっている場合、信頼できるサイトのリストはSBXの信頼できないサイトのリストよりも優先されます。	1
Browser.Chrome	Google ChromeがNetive環境にインストールされていなくても、HP Secure Browserがインストール、実行可能とします。	1
MimeHandler.Other.LavaCheckOnIngress	HP Secure Browserによるファイルダウンロード時に、自動でマルウェアチェックを行い、問題なければファイルが保存されます。	1

HP Sure Click Enterprise ポリシー設定 詳細設定 2/2

※ 以下は環境確認後、必要に応じて設定を追加します。

青字：WPSで設定変更が可能な項目

ポリシー項目	説明	設定例
BMS.PrefferdProxies	SCE エージェントからの通信のプロキシ設定	例) 12.34.56.78:8080
XVM.CustomProxyConfig	MicroVM上のアプリからの通信のプロキシ設定	例) 12.34.56.78:8080
Browser.BlockAllDownloads	HPセキュアブラウザ経由でのファイルダウンロードを許可、あるいは、禁止します。	1(禁止)
IEDownloadDirectory	HPセキュアブラウザでファイルをダウンロードする際の保存フォルダを指定のフォルダに限定します。ユーザはダウンロード時に保存先を選択できなくなります。	例)C:\Users\%username%\Input
Browser.PermitUploads	HPセキュアブラウザ経由でのファイルアップロードを許可、あるいは、禁止します。	0(禁止)
Browser.UploadAllowedSites	HPセキュアブラウザ経由でファイルをアップロードできるサイトを指定します。	例)gigafile.nu,*.datadeliver.net
XVM.EnableAudioCapture	HPセキュアブラウザで、マイクを利用可能とします。	1(ON)

Appendix

・自動的に信頼するファイルの種類

.bmp
.jpg
.png

・信頼に権限の昇格が必要なファイルの種類

.bat
.chm
.cmd
.com
.cpl
.dll
.exe
.hta
.js
.jse
.lnk
.mht
.msi
.msp
.ps1
.py
.reg
.scr
.vbe
.vbs
.wsf
.SettingContent-ms

・Ingressアプリケーション

Google Chrome	ON
Lotus Notes	OFF
Microsoft Edge	ON
Microsoft Internet Explorer	ON
Microsoft Office Lync	ON
Microsoft Office Outlook	ON
Microsoft Teams	OFF
Mozilla Firefox	ON
Skype)	ON
Skype App	ON
Skype for Business	ON
Slack	ON
Webex	ON
Windows Mail App	ON
Zoom	ON

・ホスト上へナビゲートする、ブラウザ以外の URL スキーマ

mailto
odopen
onenote
ms-word
ms-excel
ms-powerpoint
zoommtg
msteams