

エンドポイントプロテクション管理者ガイド



Copyright 2019 Webroot.All rights reserved.

ウェブルートエンドポイントプロテクション管理者ガイド

この文書に記載されている情報は予告なく変更されることがあります。この文書で説明されているソフトウェアは、使用許諾契約または秘密保持契約に基づいて提供されています。このソフトウェアの使用または複製は、これらの契約の条件に従って行うものとします。複写や記録を含む、電子的または機械的ないかなる形態や手段によっても、書面による許可なく、購買者の個人的な使用以外の目的で、本書のいかなる部分についても複製、検索システムへの保存、または転送を行うことはできません。

目次

第1章: WSA Business エンドポイントプロテクション管理者ガイド	1
WSA Business - エンドポイントプロテクション管理者ガイドの概要	2
第2章:エンドポイントプロテクションの基本情報	
システム要件	4
セットアップの準備	
設定手順	
ファイアウォールを介した通信	
プロキシバイパスの入力	
インストーラー内でのプロキシ情報の入力	
配備後の各エンドポイントでのプロキシ情報の入力	9
アカウントの作成	11
2 要素認証 (2FA) の有効化	16
ログインとセット アップウィザードの使用	
設定中のデフォルトのポリシーの選択	
配備方法の選択とテストインストールの実行	
管理コンソールの使用	
エンドポイントプロテクションの主要なタブ	
エンドポイントプロテクションのメニューを開く	
パネルの展開と折りたたみ	
スプレッドシートへのデータのエクスポート	41
ビデオチュートリアルを開く	
ヘルプファイルを開く	
製品情報へのアクセス	
表とレポートのデータの並べ替え	45
管理コンソールへのアクセス	
第3章:ユーザーアカウントの管理	
自分のアカウント設定の編集	
ポータルユーザーの管理	
新規ポータルユーザーの作成	68
ユーザー情報の編集	
コンソールユーザーの権限設定	
アカウントへのキーコードの追加	
アカウントへのコンソールの追加	84
コンソールの追加	
コンソールの名前の変更	

コンソールの切り替え	
アカウントの更新またはアップグレード	
サイト管理者の追加	
サイト管理者設定の編集	
サイト管理者の削除	
第4章:エンドポイントの管理	
エンドポイントへの SecureAnywhere の配備	
SecureAnywhere インストーラーの使用	
MSI 配備オプションの使用	
GPO 配備オプションの使用	
インストーラーのオプション	
ターミナル (RDS) サーバーおよび Citrix XenApp へのインストール	
複製イメージまたは VM へのインストール	
エンドポイントキーコードの変更	
エンドポイントの名前の変更	
エンドポイントの検索	
エンドポイントへのコマンドの発行	
エンドポイントのアップデートとその他の変更の管理	
新しい OS への 移行	
エンドポイントのハードウェアの変更	
新しいサブネット へのエンドポイントの移動	
ファイアウォールを介した通信	
エンドポイントでの SecureAnywhere の使用	
Windows コンピュータで SecureAnywhere を開く	
Mac コンピュータで SecureAnywhere を開く	
Mac の[Webroot SecureAnywhere] メニュー	
Mac の[システムツール] ドロップダウンメニュー	
スキャンの結果確認と脅威の管理	
スキャン履歴の表示	
ファイルの隔離からの復元	
ファイルのオーバーライドの設定	
アップデートのダウンロードと強制実行	
即時のアップデートの強制実行	
Web 脅威シールド Chrome ブラウザエクステンションのインストール	
Active Directory グループポリシーの使用	
Google スイートを利用した単一カスタムアプリの強制インストール	
レジストリの使用	
エンドポイントでのコマンドの実行	

エンドポイントの非アクティブ化	
エンドポイントの非アクティブ化	
エンドポイントでの SecureAnywhere の再アクティブ化	
SecureAnywhere のアンインストール	
第5章:状態の確認	
エンドポイントの状態の表示	
脅威の最新状況の表示	
エージェントのバージョンの概要表示	
滞留時間について	
エンドポイントプロテクションからの CSV ファイルのエクスポート	
第6章:ポリシーの管理	
ポリシーの導入	222
新しいデフォルトのポリシーの選択	
ポリシーの作成	
ポリシーの作成	
ポリシーのコピー	
ポリシーの名前の変更	
ポリシー設定の変更	
基本設定	
スキャンのスケジュール	
スキャン設定	
自己保護の設定	
ヒューリスティック	
リアルタイムシールドの設定	
動作シールドの設定	
コアシステムシールド	
Web 脅威シールド	
ID シールド	
ファイアウォール	
ユーザーインターフェイス	
システム最適化ツール	
ホリシーに割り当てられたエンドボイントの表示	
ホリシー間でのエントホイントの移動	
ホリシーの削除	
第7章:グループの管理	
新規グループの追加	
グループの名前の変更	

エンドポイントのグループへのポリシーの適用	324
エンドポイントのグループへのポリシーの適用	
単一のエンドポイントへのポリシーの適用	325
グループ間でのエンドポイントの移動	328
エンドポイントをグループに整理	330
ビュー内の「アクティブディレクトリ」 タブの使用	332
ビュー内の[IP 範囲] タブの使用	
ビュー内の「ワークグループ」タブの使用	336
グループの削除	
第8章:レポートの操作	339
エンドポイントプロテクションのレポートの生成	340
「確認されたすべての脅威」 レポートの生成	342
[確認されたすべての未判定のソフトウェア] レポートの生成	
[ブロックされたすべての URL] レポートの生成	356
「最新のスキャンで脅威が存在したエンドポイント」レポートの生成	
[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートの生成	
[脅威の履歴 (日単位)]レポートの生成	369
[脅威の履歴 (内訳)]レポートの生成	377
- [ブロックされた URL の履歴 (日単位)] レポートの生成	
[インストールされたエージェント] レポートの生成	
レポートのスプレッドシートのダウンロード	402
第9章:警告の管理	404
警告の導入	405
配信先リストの作成	
カスタムの警告の作成	
定義済みの警告メッセージの表示	420
警告の一時停止または削除	
第 10 章: オーバーライドの使用	423
オーバーライドの導入	424
ブラックリストのオーバーライドの作成	426
ホワイトリストのオーバーライドの作成	432
[オーバーライド] タブからのオーバーライドの適用	439
グループからのファイルへのオーバーライドの適用	
レポートからのファイルへのオーバーライドの適用	
滞留時間のポップアップからのオーバーライドの適用	
オーバーライドの表示	466

スプレッドシート へのオーバーライド のエクスポート	
オーバーライドの削除	
第 11 章: ウェブのオーバーライドの使用	
ウェブのオーバーライドの作成	
[グループの管理] でのウェブのオーバライドの作成	
[レポート] でのウェブのオーバライドの作成	
ウェブのオーバーライドの編集	
ウェブのオーバーライドの削除	
第 12 章:設定の管理	
データフィルタの設定	
第 13 章: ログの表示	
変更ログの表示	
コマンドログの表示	
データフィルタログの表示	
第 14 章: 使用状況データへのアクセス	
使用状況データへのアクセスについて	
第 15 章: WSA Business エンドポイントプロテクションのサポート	
テクニカル サポートを受けるには	
索引	i

第1章:WSA Business エンドポイントプロテク ション管理者ガイド

エンドポイントプロテクションの基本情報については、以下のトピックを参照してください。

WSA Business - エンドポイントプロテクション管理者ガイドの概要 2

WSA Business - エンドポイントプロテクション管理者ガイドの 概要

Webroot SecureAnywhere[™] Endpoint Protection は、ウェブルートによる動作の認識技術とクラウドコンピュー ティングを組み合わせて、マルウェアなどの脅威から企業を守ります。エンドポイントプロテクションには、エンド ポイントの表示と管理に使用する一元的な Web サイトである管理ポータル (管理コンソールとも呼ばれます) があります。

PC、ノートパソコン、サーバー、仮想サーバーなど、Windows のあらゆる企業向けワークステーションをエンドポイントとして使用できます。これらのエンドポイントへの Secure Anywhere ソフトウェアの配備はわずか数秒で完了でき、ユーザーの保護を即座に開始できます。Secure Anywhere はエンドポイントのスキャンを実行し、管理ポータルにエンドポイントの状態を報告します。



このオンラインヘルプでは、管理者による SecureAnywhere の配備方法と、管理ポータルを使用した脅威に 対する警告やデータのグラフ、エンドポイントのアクティビティに関するその他の情報の表示方法を説明しま す。実行できるタスクは、与えられているアクセス権限と、エンドポイントの設定時に選択した管理モードに よって異なります。このガイドは、完全なアクセス権限を与えられた状態でエンドポイントプロテクションを使用 する管理者を対象としています。

第2章:エンドポイントプロテクションの基本情報

エンドポイントプロテクションの基本情報については、以下のトピックを参照してください。

システム要件	4
セットアップの準備	5
設定手順	5
ファイアウォールを介した通信	6
プロキシバイパスの入力	8
インストーラー内でのプロキシ情報の入力	8
配備後の各エンドポイントでのプロキシ情報の入力	
アカウントの作成	11
2 要素認証 (2FA) の有効化	16
ログインとセットアップウィザードの使用	24
設 定 中 のデフォルト のポリシーの選 択	
配備方法の選択とテストインストールの実行	
管理コンソールの使用	
エンドポイントプロテクションの主要なタブ	
エンドポイントプロテクションのメニューを開く	38
パネルの展開と折りたたみ	40
スプレッドシートへのデータのエクスポート	
ビデオチュートリアルを開く	
ヘルプファイルを開く	
製品情報へのアクセス	
表とレポートのデータの並べ替え	45
管理コンソールへのアクセス	

システム要件

システム要件については、Business エンドポイントプロテクション Web ページのシステム要件のセクションを参照してください。

セットアップの準備

このセクションの設定手順を読み、環境がシステム要件を満たしていることを事前に確認してください。

注意:以下の設定手順は、完全なアクセス権限を与えられたエンドポイントプロテクション管理者を 対象としています。

設定手順

1. キーコードを使用してアカウントを作成します。

キーコードは事前にウェブルートから電子メールで送信されています。詳細については、「<u>アカウントの作</u> 成ページ11」を参照してください。

2. 管理ポータルにログインし、セットアップウィザードを開きます。

ウィザードでは、エンドポイントへの Secure Anywhere のインストールにデフォルトのポリシーを選択する必要があります。

- ポリシーは、プログラムが脅威をスキャンする方法や検出されたアイテムを管理する方法など、 Secure Anywhereの設定を定義するものです。
- PC、ノートパソコン、サーバー、仮想サーバーなど、Windows のあらゆる企業向けワークステーション をエンドポイントとして使用できます。

ポリシーを選択すると[ようこそ] ウィンドウが表示され、SecureAnywhere のエンドポイントへの配備方法 に関する情報が提示されます。詳細については、「<u>ログインとセットアップウィザードの使用ページ24</u>」を 参照してください。

3. 連絡先の電話番号や所在地のタイムゾーンなど、管理ポータルのアカウント設定を編集します。詳細 については、「自分のアカウント設定の編集ページ55」を参照してください。

また、他の管理者が管理ポータルにアクセスできるよう、ログインを作成することもできます。詳細については、「ポータルユーザーの管理ページ68」を参照してください。

注意:この手順は任意です。

- 4. Secure Anywhere ソフトウェアをエンドポイントに配備します。詳細については、「エンドポイントへの Secure Anywhere の配備 ページ112」を参照してください。
- 5. デフォルトのポリシーがビジネス要件を満たしているかを判断します。ウェブルートのデフォルトのポリシー は変更できません。

必要に応じて、設定の異なる新しいポリシーを追加してください。詳細については、「<u>ポリシーの導入</u> ページ222」を参照してください。また、正当なアプリケーションと思われるファイルに対して、オーバーライ ドを作成する必要がある場合があります。詳細については、「<u>「オーバーライド</u>] タブからのオーバーライド の適用 ページ439」を参照してください。

6. 管理目的に応じて、複数のエンドポイントのグループを作成する必要があるかを判断します。

SecureAnywhere をエンドポイントに配備する際、エンドポイントプロテクションはすべてを1つのデフォル トグループに配備します。必要に応じて、新しいグループを作成し、それらを新しいポリシーに割り当て ることができます。詳細については、「エンドポイントをグループに整理ページ330」を参照してください。

 エンドポイントが感染を報告した際、または新しいエンドポイントに SecureAnywhere がインストールされた際に、レポート配信先リストに送信される警告メッセージをカスタマイズします。詳細については、「<u>警</u> *告の導入 ページ405」を参照してください。*

注意:この手順は任意です。

ファイアウォールを介した通信

ファイアウォールがある場合、以下の表に記載されたウェブルートのパスマスクを許可してください。

パス	ポート	詳細
		エージェントの通信とアップデート。
.webrootcloudav.com	ポート 443 (https)	注意:一部のファイアウォール では、単一のワイルドカードマ スクを使用したダブルドットを含 むサブドメイン名(例: 「g1.p4.webrootcloudav.com」を 「.webrootcloudav.com」で表 示)をサポートしていません。こ のため、一部の環境では 「*.p4.webrootcloudav.com」ま たは「*.*.webrootcloudav.com」 のいずれかにしなければならな いことがあります。
*.webroot.com	ポート 443 (https)	エージェントのメッセージ送受信。
https://wrskynet.s3.amazonaws.com/*	ポート 443 (https)	エージェントのファイルのダウンロードと アップロード。
https://wrskynet-eu.s3-eu-west- 1.amazonaws.com/*	ポート 443 (https)	エージェントのファイルのダウンロードと アップロード。
https://wrskynet-oregon.s3-us-west- 2.amazonaws.com/*	ポート 443 (https)	エージェントのファイルのダウンロードと アップロード。

パス	ポート	詳細
WSAWebFilteringPortal.elasticbeanstalk.com	ポート 80 (http) & 443 (https)	エージェントの Web フィルタリングに必 要。elasticbeanstalk は Amazon の AWS ドメイン。
*.webrootanywhere.com	ポート 80 (http) & 443 (https)	管理ポータルとサポートチケット ログの アップロード。

Webroot SecureAnywhere Business - Endpoint Protection でプロキシ設定を使用する際は、ご使用の製品が ウェブルートのクラウドサーバーと通信できるようにする方法が他にもあります。詳細については、以下を参照 してください。

プロキシバイパスの入力

注意:ウェブルート推奨の方法です。

プロキシバイパスを入力するには

1. g*.p4.webrootcloudav.com のプロキシバイパスを入力します。

注意: このオプションを選択する場合、ワイルドカードマスク(*)がサポートされていることを確認 してください。サポートされていない場合、g1、g2、g3、...g99、g100のように 100 個の URL を個別に追加しなければなりません。

インストーラー内でのプロキシ情報の入力

これはウェブルートが推奨する別の方法です。

インストーラー内でプロキシ情報を入力するには

1. SecureAnywhere MSI インストーラーをネットワーク共有にダウンロードします。

http://anywhere.webrootcloudav.com/zerol/wsasme.msi

- 2. msi エディタを使用します。
- 3. プロパティの表で、以下のコマンドを使用して GUILIC プロパティに定期購入契約のキーコードを、 CMDLINE プロパティにプロキシの資格情報をそれぞれ入力します。

-proxyhost=X -proxyport=X -proxyuser=X -proxypass=X -proxyauth=#

4. すべてのパラメータを使用し、不要なパラメータについては値を入力せずに二重引用符のみを入力してください。以下のように入力します。

proxypass=""

proxyauth # being: 0 = Any authentication 1 = Basic 2 = Digest 3 = Negotiate 4 = NTLM

5. これらの引数は実行可能なインストールで適用することも可能です。以下のように入力します。

C:\wsasme.exe /key=xxxx-xxxx-xxxx-xxxx /silent -proxyhost=nn.nn.nn -proxyauth=n proxyuser="proxyuser" -proxypass="password" -proxyport=port_number

配備後の各エンドポイントでのプロキシ情報の入力

この方法は、プロキシバイパスを入力できない場合や、インストーラー内でプロキシ情報を入力できない場合 にのみお勧めします。

- 1. SecureAnywhere エンドポイントプロテクションの [グループの管理] タブを開き、グループを開いて、エンドポイントを選択します。
- 2. 選択したエンドポイントの[ポリシー] カラムでポリシー名をダブルクリックし、使用可能なポリシーの一覧 を表示します。
- 3. 非管理ポリシーを選択して適用します。新しいポリシー名に赤いフラグが付き、変更されたことを示しま す。
- 4. [変更を保存]をクリックします。
- 5. ポリシーが適用されたら、各エンドポイントのワークステーションで以下の手順に従います。
- 6. システムトレイアイコンから SecureAnywhere エンドポイントプロテクションを開きます。
- 7. [設定]をクリックします。
- 8. [設定] ウィンドウで [プロキシ] タブをクリックします。

- 9. プロキシ情報を入力します。
- 10. [すべて保存]をクリックして変更を保存します。
- 11. プロキシ情報を入力した後、マシンを元のポリシーに戻すことができます。

注意: プロキシ設定の最適なテスト方法は、デフォルトのゲートウェイ経由でのインターネットア クセスが存在しないことを確認することです。デフォルトのゲートウェイや DNS サーバーを追加し なくても、エンドポイントのネットワークカードの IP アドレスおよびサブネット マスクをハードコード 化 することができます。プロキシサーバーが同じサブネット上にある限り、プロキシサーバー経由以外 のインターネットアクセスが存在しないことを確信できます。.

アカウントの作成

エンドポイントプロテクションにログインする前に、ライセンスキーコードを使用してアカウントを作成する必要があります。キーコードは、アクティブ化と設定の手順に関する電子メールに記載されています。

アカウントを作成するには

- 1. 管理コンソールに移動し、[アカウントの作成]ボタンをクリックします。
- ^{2.} 製品キーコードと管理者の電子メールアドレスを入力します。また、パスワードと個人用セキュリティコードを作成します。詳細については、以下の表の情報を参照してください。

フィールド	説明
ウェブルート製品のキー コード	エンドポイントプロテクションの購入時に受け取ったライセンスキーコー ドを入力します。
電子メールアドレス	エンドポイントプロテクションを管理する管理者の電子メールアドレスを 入力します。 アカウントをアクティブ化するための確認のメッセージがこの電子メール アドレスに送信されます。このメールアドレスは、管理ポータルにログイ ンする際のユーザー名にもなります。
パスワード	9文字以上を入力してください。パスワードは、少なくともアルファベット6文字と数字3文字を含む必要があります。パスワードは最小文字数の9文字を超えても問題ありません。山括弧(<>)以外の特殊文字は使用可能です。パスワードの大文字と小文字は区別されます。 入力を始めると、強度メーターがパスワードの安全性を示します。最適なセキュリティを確保するために、パスワードはできるだけ強力なものにすることをお勧めします。

フィールド	説明
個人用セキュリティコード	文字または数字を入力してください。ログインする際に、パスワードを 入力した後の追加のセキュリティ対策として使用されます。6文字以 上で、覚えやすいコードを使用してください。 管理ポータルへのログイン時には毎回、このコードからランダムな2文 字を入力するように求められます。たとえば、コードが123456で、4番 目と6番目の文字を入力するよう求められた場合、「4」と「6」を入力 します。この個人用セキュリティコードでは大文字と小文字が区別さ れます。
セキュリティの質問	ドロップダウンリストから質問を選択します。 ログインの詳細情報を忘れた場合に、この質問に答えることで情報を 取得できます。
セキュリティの回答	セキュリティの質問に対する回答を入力します。セキュリティの回答で は大文字と小文字が区別されます。

3. アカウントの詳細を入力したら、[今すぐ登録] ボタンをクリックします。

Secu	i re Any	where.	
Log in		Create Account	
Create Account			
Webroot Product Keycode			
Email Address			
Repeat Email Address			
Password			
Strength:			
Repeat Password			
Your Personal Security Code			
Security Question			
			Ŧ
Security Answer			
	Register Now		

SecureAnywhere により確認メッセージが表示され、指定した管理者の電子メールアドレスに確認のメールが送信されます。これには数分かかることがあります。

4. 電子メールのアプリケーションを開き、確認の電子メールメッセージに記載されたリンクをクリックします。

SecureAnywhere の登録確認ページが開いたら、アカウント作成の際に指定したセキュリティコードから ランダムに選択された2文字を入力します。

5. [今すぐ登録確認する]をクリックします。

セキュリティコードを入力すると、2要素認証 (2FA)の設定に関するオプションが表示されます。このト ピックの詳細については、「2要素認証 (2FA)の有効化ページ16」を参照してください。

2 要素認証 (2FA) の有効化

Webroot SecureAnywhere では、2要素認証 (2FA)を有効化することで、承認されていないユーザーによるアカウントへの無許可のアクセスを防止できます。

2FA を有効にするには

- 1. まず、ウェブルートの管理コンソールに移動し、ビジネス管理者アカウントの資格情報を使用してログインします。
- 2FA の設定画面が表示されます。管理コンソールへのログインが初めての場合は、[2FA を設定する] をクリックしてプロセスを開始することも、[今はスキップする]をクリックしてコンソールを開くこともできます。

Two-Factor Authentication (2FA)	FAQs
Simple Setup Choose two additional security questi Download an Authenticator app. Use the Authenticator app to scan a p Enter the verification code. Setup 2FA If you would rather 'Skip for Now' and se options in the Admin section of the Busi Account Settings section of the Consume I don't want to be asked again Skip for now	ons. provided QR (Quick Response) Code. et it up later, you can find the 2FA ness Management Console or the er Web Console.	 What is 2FA? Two-factor authentication improves your digital security by protecting your account with an additional login step. Why should I use it? Two-factor authentication makes it harder for unauthorized users to gain access to an account without permission. Are there any other benefits? This will replace the need to enter your security code when logging in to your console.
Consumer Release Notes	Business Release Notes	Webroot Community

以前に管理コンソールにログインし、2FA を設定するプロセスのスキップを選択している場合は、こちらをクリックして最初に 2FA の設定をスキップした後に 2FA を有効化する手順を確認してください。

2FA の設定プロセスは、エンドポイントコンソールの右上隅にある [アカウント設定] から開始することもできます。ユーザーの詳細情報が表示される [アカウント設定] ページで [有効化] をクリックします。

Account Settings	=
Edit Details	
User Details	
Name	
Display Name	
Email	
Office Phone	
Mobile Phone	
Time Zone	United States, Colorado, Colorado Springs, Denver
2FA	Enable
Password	Change
Security Code	Change
Security Question	Change
Access & Permissions	
SecureAnywhere Console	Admin
Endpoint Protection Console	Admin

3. 次に表示される [2FA を設定する] 画面で、セキュリティの質問を2つ選択して回答を入力するよう求められます。設定が完了したら、[続行] をクリックします。

Setup 2FA		
Step 1		
2FA requires you to choose two addition and click 'Continue'.	al security questions. Please choose two o	questions below, type your answers
It is important that you type the answers	correctly because you will be asked agair	n if your device gets lost or stolen.
Security Question		
Choose a question from the list	~	
Security Answer		
Security Question		
Choose a question from the list	~	
Security Answer		
Cancel		Continue
Consumer Release Notes	Business Release Notes	Webroot Community

4. スマートフォンまたはカメラ付きタブレットに、Google Play ストアまたは Apple App Store から認証用アプリをダウンロードしてインストールする必要があります。

etup 2FA			
tep 2		Step 3	Step 4
ownload an Auth your Smart phor as a camera. Web commends using ollowing free apps	ne or tablet that root one of the one of the , from either the	Open your app and scan the QR code below.	Enter the verification code from your Authenticator app in the field below:
oogle Play Store o tore:	or the Apple App		
Google	Microsoft	EXAMPLE	Verify Code
Authenticator	Authenticator	Sec. 2010	
e	0	⊡¢832A	
LastPass Authenticator	Authy 2-Factor Authenitication	Can't scan the QR code?	
	8		
Cancel			Complete Setup
	N		
Consumer Rel	ease Notes	business kelease Notes	webroot Community

モバイル認証用アプリの例は以下のとおりです。

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy の2要素認証
 - 認証用アプリをダウンロードしたら、アプリを開き、画面の指示に従ってアプリがスマートフォンのカメラに アクセスできるようにします。これにより、管理コンソールに表示されるQRコードをスキャンできるように なります。QRコードをスキャンできない場合は、ディスプレイの明るさを調整するか、[QRコードをスキャ ンできない場合]をクリックして、表示されたコードをデバイスの認証アプリに入力します。コードの大文 字と小文字は区別されます。

Step 2		Step 3	Step 4
Download an Au to your Smart pho has a camera. We recommends usin following free app Google Play Store Store:	thenticator App one or tablet that broot og one of the os, from either the or the Apple App	Open your app and scan the QR code below.	Enter the verification code from your Authenticator app in the field below:
Google Authenticator	Microsoft Authenticator		Verify Code
LastPass Authenticator	Authy 2-Factor Authenitication	Can't scan the QR code? If you can't scan the QR code please enter the below secret manually into your authenticator application on your device. You must set your new secret to be 'time-based' and six characters long. VZYEU HXNL MYYD2X	
Cancel			Complete Setup

6. 認証アプリから取得した認証コードを [ステップ 4] のボックスに入力し、[認証コードを確認する] をクリックします。

Setup 2FA			
Step 2		Step 3	Step 4
Download an Authe to your Smart phone has a camera. Webro recommends using o	enticator App or tablet that oot ne of the	Open your app and scan the QR code below.	Enter the verification code from your Authenticator app in the field below:
following free apps, f Google Play Store or Store:	rom either the the Apple App	<u>回蹤回</u>	
Google Authenticator	Microsoft Authenticator	EXAMPLE	Verify Code
	Û		
Authenticator	Authy 2-Factor Authenitication	Can't scan the QR code?	
Cancel			Complete Setup

7. コードの確認が行われ、"認証が成功しました というメッセージが画面に表示されます。[設定を完了 する]をクリックして 2FA の設定を完了します。



注意: コードは 30 秒で有効期限が切れるため、コードの入力時に "認証に失敗しました" というメッセージが表示された場合は、認証アプリから新しいコードを取得して入力し、[認証コードを確認する] をクリックする必要があります。

8. 2FA が有効になり、"おめでとうございます!" という画面が表示されます。[コンソールに進む] をクリック し、2FA を使用してエンドポイントプロテクションのコンソールにログインします。

ログイン時に入力する認証用コードは認証用アプリから提供されます。このコードがセキュリティコードの

代わりになります。

Congratulations, you have now	completed Webroot 2FA setup.	
Please have your smart phone or tablet Authenticator app each time. If you pre	with you the next time you log into your co viously used the Security code to log in, 2FA	onsole. You will need to use your A will now replace that step.
Thank you for choosing Webroot.		Go to Console
hank you for choosing Webroot.	Business Release Notes	Go to Console

注意: セキュリティコードはアカウントに保存され、2FA が無効になった場合に使用されます。

9. アカウントで 2FA が有効になったことを知らせる電子メールが <u>no-reply@webrootanywhere.com</u> から 届きます。

N To	Tue 11/5/2019 10:45 AM no-reply@webrootanywhere.com IMPORTANT- Account Information
Hello,	
The account	t associated with this email address has had 2 Factor Authentication enabled.
If this was n	ot you please check your settings or if you need additional assistance please contact a support representative.
Thank you,	
The Webroo	ot Team

これでエンドポイントプロテクションのコンソールにログインして、設定を開始できます。詳細については、「<u>ログイ</u> <u>ンとセットアップウィザードの使用ページ24</u>」を参照してください。

ログインとセットアップウィザードの使用

アカウントを作成すると、管理ポータルにログインできるようになります。初回のログイン時にセットアップウィザードが開き、設定を開始することができます。

このトピックでは、次の手順について説明します。

- <u>ログイン</u>
- 設定中のデフォルトのポリシーの選択
- 配備方法の選択とテストインストールの実行

詳細については、「アカウントの作成ページ11」を参照してください。

初回のログイン

- 1. <u>SecureAnywhere Web サイト</u>に移動します。
- 2. 英語以外の言語で表示するには、ページ下部のドロップダウン矢印をクリックし、目的の言語を選択します。



注意: ダブルバイト文字セットを使用する言語を有効にするには、適切な言語パックがコン ピュータにインストールされている必要があります。computer. 3. [ログイン] 画面で、アカウント作成時に指定した電子メールアドレスとパスワードを入力します。

注意:光通信のユーザーは、[電話番号]タブをクリックすると、電話番号とパスワードを使って ログインできます。[電話番号]タブはすべてのユーザーに表示されますが、光通信ユーザー以外 は電子メールアドレスとパスワードでログインしてください。

4. [**ログイン**] ボタンをクリックします。

Log in		Create Account
mail / Phone		
Password		Forgotten Passwor
	Log In	
Looki	ng to renew your license? Get	Started
Consumer Release Notes	Business Release Notes	Webroot Community
Website Terms Of Service	Privacy Statement	License Agreement
	© 2019 Webroot Inc.	

</bpt>1ログインに3回失敗すると、パスワードまたはセキュリティコードをリセットするリンクを記載した電子メールが送信されます。

Iさらに、次のメッセージが表示されます。

"残念ながら、このコンソールへのアクセス試行の最大限度回数を超えました。15分後にコンソールへのアクセスを試みることができます。アカウント情報を忘れた場合は、<u>https://my.webrootanywhere.com</u>にアクセスし [パスワードをお忘れですか。] リンクをクリックしてください。"

パスワードまたはセキュリティコード忘れた場合は、[パスワードをお忘れですか。] リンクをクリックして、 [パスワードを忘れました] または [セキュリティコードをお忘れの場合] をクリックします。

システムから電子メールアドレスを入力するよう求められ、パスワードまたはセキュリティコードをリセットするリンクを記載した電子メールが送信されます。

5. 2FA を有効にしている場合は、モバイル認証用アプリに表示されたコードを [ログオン確認] ウィンドウ に入力し、[確認] ボタンをクリックします。

WEBROOT	
Authentication Code	
Please enter your authentication code.	
Authentication Code	Lost or Stolen Device?
Confirm	

2FA を有効にしていない場合は、[ログオン確認] ウィンドウでウェブルートアカウントの登録時に作成し たセキュリティコードを入力します。エンドポイントプロテクションは、ログイン時に毎回この追加のセキュリ ティ手順を要求します。このコードからランダムな2文字を入力するよう求められます。たとえば、コード が123456で、4番目と6番目の文字を入力するよう求められた場合は、「4」と「6」を入力します。.

Secure Anywhere.
Home
Confirm Logon:
Please enter the FIFTH and SIXTH characters of your Security Code (case sensitive)
Login Forgotten Security Code?
6. SecureAnywhere Web サイトにアクセスできたら、[エンドポイントプロテクションに進む] ボタンをクリックします。



注意: モバイルプロテクションも購入した場合は、モバイルプロテクションのポータルにもアクセス できます。購入していない場合は [モバイルプロテクション] パネルは表示されません。詳細につ いては、WSA Business - モバイルプロテクション管理者ガイドを参照してください。

初めてログインするときに、セットアップウィザードが表示されます。「<u>設定中のデフォルトのポリシーの選</u>」 択」に進んでください。

設定中のデフォルトのポリシーの選択

セットアップウィザードで、Windows エンドポイントでの新規の Secure Anywhere のインストールに適用するデフォルトのポリシーを選択するよう求められます。ポリシーは、プログラムが脅威をスキャンする方法や検出されたアイテムを管理する方法など、Secure Anywhere の設定を定義するものです。

Home Endpoint Protection Mobile	Protection
Setup Wizard	
Select the default policy to apply to all These policies are provided with Webroot Se create new policies and apply them to your of Select your default settings *	Il endpoints during installation. ecureAnywhere Endpoint Protection so that you can get started quickly. You can nanaged endpoints after installation. Recommended Defaults Submit
Note: You can change your default policy after in	stallation.

セットアップウィザードは次のようなデフォルトのポリシーを提供します。

- 推奨デフォルト設定 脅威に対する自動削除と隔離機能を備えた推奨セキュリティ設定です。
- 推奨サーバーデフォルト設定 脅威に対する自動削除と隔離機能を備えたサーバー向けの推奨セキュリティ設定です。サーバーが最適なパフォーマンスで実行されるようにします。
- サイレント監査 ユーザーの操作なしで脅威をスキャンします。検出されたアイテムのブロックまたは隔離は行いません。このポリシーでは、SecureAnywhere が検出した脅威をユーザーが最初に確認できるため、ユーザーは検出されたアイテムを確認し、すべての正当なアプリケーションファイルにオーバーライドを追加することができます。このポリシーは、誤検出に対する懸念がある場合や、SecureAnywhereを重要なサーバーに適用する際に使用します。検出されたアイテムを自動修正する厳格なポリシーを適用する前に、オーバーライドをあらかじめ設定する際に便利です。オーバーライドの詳細については、「「オーバーライド」 タブからのオーバーライドの適用ページ439」を参照してください。
- 管理対象外 推奨されるセキュリティを設定します。ユーザーは Secure Anywhere 設定をエンドポイントで 変更できます。管理対象外のエンドポイントは引き続き管理ポータルへの報告を行い、スキャン結果が表 示されます。管理者はコマンドを送信できますが、ポリシーの設定を変更することはできません。

注意: どのポリシーを選択すべきかわからない場合は、エンドポイントの保護をただちに開始する[推 奨デフォルト設定] ポリシーを選択することをお勧めします。「<u>新しいデフォルトのポリシーの選択 ページ</u> <u>227</u>」で説明するように、デフォルトのポリシーは後で簡単に変更できます。「<u>ポリシーの作成 ページ233</u>」 で説明するように、独自のポリシーを作成してエンドポイントのグループに割り当てることもできます。

デフォルトのポリシーを選択するには

1. [デフォルトの設定を選択してください]ドロップダウンメニューで、適用するポリシーを選択します。

Select your default settings *	Recommended Defaults	×
	Recommended Defaults Recommended Server Defaults Silent Audit Unmanaged	6

2. [送信] ボタンをクリックします。

エンドポイントプロテクションの[状態]ページが開き、[ようこそ]パネルが上に、配備オプションが下に、サポートリソースが右側に、それぞれ表示されます。次のセクションに進み、配備方法を選択します。

配備方法の選択とテストインストールの実行

[ようこそ] パネルで、SecureAnywhere プログラムをエンドポイントに配備する方法を確認できます。

注意: これらの配備方法は、Windows コンピュータのみを対象としています。Mac コンピュータにインストールする必要がある場合は、「エンドポイントへのSecureAnywhere の配備ページ112」の説明に従って SecureAnywhere Mac インストーラーを使用してください。

- エンドポイントの数が100 未満の小規模ネットワークでは、[使用を開始するには] パネルで説明されている 簡単な方法を使用することをお勧めします。表示される手順に従ってください。
- 大規模なネットワークで Active Directory を使用している場合は、下部にある [Webroot Secure Anywhere の配備]をクリックし、高度な配備オプションの詳細を確認することをお勧めします。詳細については、「エン

<u>ドポイントへのSecureAnywhereの配備ページ112</u>」を参照してください。

come		(a) Webroot Threat Blog
No endpoints have reported in y How to get started The quickest and essiest way to get endpoints.	et	New IRCHTTP based DDo5 bot wipes out competing malware By Dancho Danchev Everyday, new verdors: offering malicious software enter the underground marketplace. And athrough mark will fail to differentiate their underground market proposition in market promoted with association, burder through
reporting into the console is by downloading a copy of the Webroot SecureAnywhere software which has one of your keycodes automatically applied. The user then simply needs to run the file, and their endpoint will automatically report into the console. Your available keycodes / downloads: SAEA-TEST- TEST-TEST-TEST-	Secure AnyWhere Secure AnyWhere Secure Any	verified sellers, others will quickly build their rapudation on the basis of their "innovalive" work, potentially stealing some market share and becoming rich by offening the [] A peek inside a CVE-2013-0422 explorting DYT maticious Java applet generating tool By Dancho Danchev On a regular basis we profile various DYT (do it yourself) releases offered for sale on the underground marketplace with the idea to highlight the re-emergence of this concept which allows withually anyone obtaining the leaked tools, or suchasing them. I succh tarseted Witted and Support
Advanced Deployment Options: For advanced deployment options, such as using MSI, Co Deploying Webroot SecureAnywhere	mmand Line, GPO, etc, click the link below:	Administrator Guide Webroot Education Videos Support * News and Updates News from Webroot

注意: [ようこそ] パネルを閉じた場合は、[リソース] タブをクリックすると、キーコードおよび配備に関する 情報を確認できます。

最初は、管理ポータルで状態を確認できるよう、少なくとも1つのテストエンドポイントに Secure Anywhere を配備することをお勧めします。

テストエンドポイントに SecureAnywhere を配備するには

1. [使用を開始するには] パネルでキーコードを探します。このキーコードは、エンドポイントプロテクションの ライセンスを識別するものです。 2. [ダウンロード] リンクをクリックして SecureAnywhere インストーラーファイルをダウンロードします。



- 3. エンドポイントからインストーラーファイルを実行します。
- 4. 次のような [インストール] パネルが表示されたら、エンドポイントプロテクションのキーコードを入力して [同意してインストール] ボタンをクリックします。

Secure/	Anywhere.			
Installation				
	Installation will only take a few seconds and will not require a Please enter your keycode: Agree and Install By clicking Agree and Install Agree and Install Help me find my keycode	you accept the tr	erms and preement	
	Ser Installation options			

または、SecureAnywhere をインストールするエンドユーザーにテスト電子メールを送信する方法もあります。この場合は、[ようこそ] パネルまたは [リソース] タブで [**電子メールテンプレート**] リンクをクリックし、テキストをカット & ペーストして電子メールメッセージに入力します。正しいキーコード がリンクにより自動的に追加されます。次に、ユーザーがリンクをクリックしてインストールを開始します。プログラムは、入力

済みの正しいキーコードを使用してバックグラウンドでインストールを実行します (サイレントモード)。終 了すると、ウェブルートのアイコンがエンドポイントのシステムトレイに表示されます。

5. Secure Anywhere が最初のスキャンを完了するまで待ちます。スキャンは数分で済みます。

スキャンが完了すると、SecureAnywhere は管理ポータルへの報告を行います。

エンドポイントのスキャンが完了したら、SecureAnywhere Web サイトに再度ログインし、その状態を確認します。[エンドポイントプロテクションに進む]をクリックすると、管理ポータルが開きます。セットアップウィザードは再表示されません。

Endpoint Protection		
	1 Endpoint Protected 0 Endpoints Currently Infected 0 Endpoints Infected (last 24 hours)	
	Go to Endpoint Protection	

詳細については、「管理コンソールの使用ページ33」を参照してください。

管理コンソールの使用

管理コンソールは、管理者がネットワークの状態を一元的に表示、管理できる Web サイトです。管理者はまずウェブルートアカウントを作成します。このアカウントを使用して、ポータルのすべての機能にアクセスできます。詳細については、「*アカウントの作成ページ11*」を参照してください。

必要に応じて、管理者は完全なアクセス権または制限されたアクセス権をもつ追加のユーザーを作成できま す。詳細については、「ポータルユーザーの管理ページ68」を参照してください。

このトピックでは、次の手順と情報を紹介します。

- 管理コンソールの使用
- エンドポイントプロテクションの主要なタブ
- エンドポイントプロテクションのメインメニューを開く
- パネルの展開と折りたたみ
- スプレッドシートへのデータのエクスポート
- ビデオチュートリアルを開く
- ヘルプファイルを開く

管理コンソールを使用するには

- 1. <u>SecureAnywhere 管理コンソールにログインします。</u>
- 2. [ログイン] パネルで、アカウント作成時に指定した電子メールアドレスとパスワードを入力し、[ログイン] ボタンをクリックします。

Secure Anywhere.	
Log in	Create Account
Log in	
Email or Phone	0
example@gmail.com	
Password	Forgotten Password?
Log in	

注意: 光通信のユーザーは、[電話番号] タブをクリックすると、電話番号とパスワードを使って ログインできます。[電話番号] タブはすべてのユーザーに表示されますが、光通信ユーザー以外 は電子メールアドレスとパスワードでログインしてください。

3. [認証コード] ページ (2FA の場合) または [ログオン確認] ページで、要求されたセキュリティコードの文 字またはモバイル認証用アプリのコードを入力し、[**ログイン**] をクリックします。

Secure Anywhere.
Confirm Logon:
Please enter the SECOND and THIRD characters of your Security Code (case sensitive)
••
Log in Forgotten Security Code?

注意:個人用セキュリティコードは、ウェブルートアカウントの作成時に定義したものです。エンドポイントプロテクションは、ログイン時に毎回この追加のセキュリティ手順を要求し、セキュリティコードのランダムな2文字またはモバイル認証用アプリのコードの入力を促します。たとえば、コードが123456で、4番目と6番目の文字を入力するよう求められた場合は、「4」と「6」を入力します。

SecureAnywhere Web サイトが開き、ネットワーク内で保護されているエンドポイントの総数、脅威のあるエンドポイント、過去 24 時間以内に脅威が検出されたエンドポイントが表示されます。

エンドポイントプロテクション]パネルで、[エンドポイントプロテクションに進む]ボタンをクリックして管理ポータルを開くか、感染したエンドポイントがある場合は感染したエンドポイントのリンクをクリックして管理ポータルを開き、脅威に関する情報のパネルに直接進みます。

Secure Anywhere.		
Home Endpoint Protection		
Endpoint Protection	Community	
12 Endpoints Protected 1 Endpoint Needs Attention 1 Endpoint Encountered a Threat (last 24 hours)	Interact with other Webroot users on our Community forum. Discuss security news, suggest features, and access our knowledge base.	
Go to Endpoint Protection	Go to the Webroot Community	

管理ポータルが表示されます。[状態] パネルには、脅威に関する警告、エンドポイントのアクティビ ティ、データのグラフがあります。



5. 上部に表示されるタブをクリックし、設定やその他の操作を行うことができます。

エンドポイントプロテクションの主要なタブ

このセクションでは、タブ、メニュー、パネル、表、検索機能、エクスポート機能など、管理ポータルの各エリアについて説明します。

次の表で、エンドポイントプロテクションのタブについて説明します。

タブ	説明
サイト に戻る	管理コンソールに戻ります。詳細については、「 <u>管理コンソールへのアクセスページ52</u> 」を参照し てください。
ホ ーム	メインのコンソールに戻ります。コンソールでは、セキュリティ意識向上のためのトレーニング、カス タマーサポート、ウェブルートコミュニティなどのその他の機能を選択できます。
状態	次の情報が表示されるダッシュボードです。 ・エンドポイントで注意が必要な場合に警告を通知するパネル。脅威にさらされたエンドポイン トの一覧を確認するには、通知をクリックします。 ・過去7日以内に脅威にさらされたエンドポイントの数を示す棒グラフ。 ・エンドポイントにインストールされているSecureAnywhereのバージョンを示す円グラフ。 ・遅択した期間に基づき、管理ポータルに報告しているエンドポイントの数を示す、エンドポイ ントアクティビティパネル。最近状態を報告していないエンドポイントがある場合は、[未確認] の横にある[表示]リンクをクリックして、どのエンドポイントが状態を報告していないかを確認 できます。 ・最新の脅威が存在するエンドポイントを示すパネル。行をクリックすると詳細情報が表示され、必要に応じてオーバーライドを追加できます。 ・ウェブルートの脅威ブログ、ガイド、ビデオ、リリースノート、その他ニュースへのリンクをまとめた パネル。前述の例には示されていません。詳細については、「 <u>製品情報へのアクセスページ</u> 43」を参照してください。
ポリ シー	ポリシーはエンドポイントにおける SecureAnywhere の動作を定義します。たとえば、スキャンを 実行するタイミングや、潜在的脅威のブロック方法などです。

ウェブルートエンドポイントプロテクション管理者ガイド

タブ	説明
グル― プの管 理	グループを使用すると、エンドポイントを整理して管理を簡略化できます。 グループやグループ内 の各エンドポイントを表示できます。 また、個々のエンドポイントを選択して、スキャン履歴を表 示することもできます。
レポー ト	レポートには、エンドポイントに存在する脅威と未判定のソフトウェアと、実行中の SecureAnywhereのバージョンが表示されます。
警告	管理者の配信先リストに送信する、警告や状態に関するメッセージをカスタマイズできます。
オー バーラ イド	環境内で実行中のファイルを管理できます。ファイルをオーバーライドして、ファイルをブロックしな いか、常に隔離するかを設定できます。
ログ	変更とコマンドの使用履歴を確認できます。
リソース	DWP クライアントのダウンロード、テンプレートとして使用する構成ファイル、オンラインヘルプなどの文書へのリンクを利用できます。

エンドポイントプロテクションのメニューを開く

ログイン ID の横にある下向き矢印をクリックすると、エンドポイントプロテクションのメニューが表示されます。メニューに表示されるオプションは、アクセス権限によって異なります。



次の表で、エンドポイントプロテクションのメニューのオプションについて説明します。

オプション	説明
アカウント設定	パスワードなどの情報を含む、アカウント設定を編集できます。 詳細については、「 <u>自分のアカウント設定の編集ページ55</u> 」を参照してください。
ユーザーの管理	他のユーザーに管理ポータルへのアクセス権を付与できます。 詳細については、「 <u>ポータルユーザーの管理ページ68</u> 」を参照してください。
キーコードの管理	現在のエンドポイントプロテクションのライセンスキーコードを表示し、追加のキー コードを購入した場合はポータルに追加することができます。 詳細については、「 <u>アカウントへのキーコードの追加 ページ81</u> 」を参照してください。

オプション	説明
ダウンロード	SecureAnywhere のインストーラーファイルをダウンロードし、配備オプションに関する詳細を確認できます。
ヘルプ	オンラインの WSA Business エンドポイントプロテクションユーザーガイドを開きます。
Ⴘポート	対話型のナレッジベースが開き、製品情報を検索できます。
ログアウト	管理ポータルを終了します。

パネルの展開と折りたたみ

データのグラフを大きく表示する場合は、一番左と一番右の折りたたむボタンをクリックします。

中央のパネルにある棒グラフは固定です。折りたたんだり、表示するグラフのタイプを変更したりできません。

Status Policies Group Management Reports Alerts Overrides Logs Resources				
📮 Status 🥢	Endpoints encountering threats (last 7	Agent Version Spread	Webroot Threat Blog	
Alert	2		Managed 'Russian ransomware' as a service spotted in the wild	
16 Endpoints need attention We recommend you check		11.69% 8.0.2.128 8.0.2.127 8.49% 24.6 8.0.2.126	By Dancho Danchev In 2013, you no longer need to posses sophisicated programming skills to manage a ransomware bofnet, potentially tricking	

パネルを再び開くには、もう一度折りたたむボタンをクリックします。



スプレッドシートへのデータのエクスポート

スプレッドシートのアイコンが表示されている場合は、このアイコンをクリックすると表示されているデータをスプレッドシートにエクスポートできます。

Ove	Overrides Logs Resources					
2						287
Dno 🛓	lo Changes 🌄 M	love endpoints to a	nother group 🕴 💽	Apply policy to end	points	»
	Policy	Status	Last Seen	Last Infected	Agent Version	
D	Recommended	📀 Not Seen R	May 7th 2013,		8.0.2.127	

ビデオチュートリアルを開く

テレビのアイコンが表示されている場合は、このアイコンをクリックするとパネルに関連する手順を説明するビデオを見ることができます。

Alerts Overrides Logs Resources			
Export to CSV 🛛 💭 Set as Default		Show Deleted Policies	
'n	Date Created	Draft Changes	
	May 24th 2013, 15:15	No	

ヘルプファイルを開く

疑問符のアイコンが表示されている場合は、このアイコンをクリックすると現在のパネルに関するヘルプが開きます。

ウェブルートエンドポイントプロテクション管理者ガイド

Ove	Overrides Logs Resources					
Dnd 🧕	Undo Changes 🌄 Move endpoints to another group 🔜 Apply policy to endpoints 🔅 🚿					
	Policy	Status	Last Seen	Last Infected	Agent Version	
D	Recommended	🔶 Not Seen R	May 7th 2013,		8.0.2.127	

製品情報へのアクセス

ウェブルートの脅威ブログ、ガイド、ビデオ、リリースノート、その他ニュースは、右側のパネルから確認できます。

リソースにアクセスするには、[ヘルプとサポート] または [ニュースおよびアップデート] にあるリンクをクリックしてください。

Webroot Threat Blog	>>
Managed 'Russian ransomware' as a service spotted in the wild	Î
By Dancho Danchev In 2013, you no longer need to posses sophisticated programming skills to manage a ransomware botnet, potentially tricking tens of thousands of gullible users, per day, into initiating a micro-payment to pay the ransom for having their PC locked down. You've got managed ransomware services doing it for you. In this post I'll profile a recently [] many legitimate Web sites as nossible tarnet server farms and the	
C Help and Support	
Administrator Guide	
Webroot Education Videos	
Support	
News and Updates	
News from Webroot	
Webroot Threat Blog	
Release Notes	
5	

このパネルが開かない場合は、右端にある折りたたむボタンをクリックしてください。

ウェブルートエンドポイントプロテクション管理者ガイド



表とレポートのデータの並べ替え

表やレポートでのデータの並べ替え、非表示、表示の操作方法は以下のとおりです。

- カラムを使用した並べ替え カラムの見出しをクリックすると、そのカラムを基準として簡単に並べ替えることができます。たとえば、ポリシー名でデータを並べ替えるには、「ポリシー」の見出しをクリックします。
- 昇順または降順の変更 カラム見出しの右端にあるドロップダウン矢印をクリックすると、ドロップダウンメ ニューが表示されます。[昇順に並べ替え] または [降順に並べ替え] を選択すると、カラム内でデータポイ ントの順番が変更されます。
- カラムの表示または非表示 カラム見出しの右端をクリックするとドロップダウン矢印が表示され、この矢印をクリックするとメニューが表示されます。チェックボックスを選択するとカラムが表示されます。チェックボックスの選択を解除するとカラムが非表示になります。



次の表で、エンドポイントプロテクションの表やレポートに表示されるデータ項目について説明します。表示 されるデータは、表示されている表やレポートのタイプによって異なります。

オプション	説明
エージェントの言語	SecureAnywhere をインストールした際に選択した言語。 en - 英語 ja - 日本語 es - スペイン語 fr - フランス語 de - ドイツ語 it - イタリア語 nl - オランダ語 ko - 韓国語 zh-cn - 簡体字中国語 pt — ポルトガル語 (ブラジル) ru - ロシア語 tr - トルコ語 zh-tw — - 繁体字中国語
エージェントのバージョン	エンドポイントにインストールされている SecureAnywhere ソフトウェア のバージョン。
すべてのエンドポイント	ファイルが検出されブロックされたエンドポイントに関する詳細情報。

オプション	説明
すべてのバージョン	ファイルが検出されブロックされた SecureAnywhere のバージョンに関 する詳細情報。
概算のスキャン時間	スキャン時間 (分 / 秒単位)。
エリア	エンドポイントが所在する国のフラグ。
クラウド判定	ウェブルートによるファイルの分類。[正当]、[不正]、[未判定] のい ずれか。 分類にカーソルを合わせると、この分類に決定された経緯に関する 情報が表示されます。
感染日数	エンドポイントが感染状態にあった日数。
デバイス MID	エンドポイントのハードウェアを識別するマシン ID の値。ウェブルート はアルゴリズムを使用してこの値を決定します。
滞留時間	脅威がデバイス内に存在していた時間。ファイルが最初にアクティブ になった時から、ファイルが最後に確認されるまでの期間で計算され ます。 詳細については、「 <u>滞留時間についてページ214</u> 」を参照してください。

オプション	説明
影響を受けたエンドポイント	検出されたファイルが存在するエンドポイントの数。
ファイルサイズ	ファイルのサイズ (バイト単位)。
ファイル名	検出された脅威のファイル名。
最初の脅威	脅威が検出された日時。
初回確認日時	このエンドポイントが初めて管理ポータルにチェックインした日時。
グループ	エンドポイントに割り当てられたグループ。
ホスト名	エンドポイントのマシン名。
インスタンス MID	Windows OS の SID (セキュリティ識別子)を識別する値。ウェブルートはアルゴリズムを使用してこの値を決定します。
IP アドレス	エンドポイントの IP アドレス。
+-⊐-ド	エンドポイントで SecureAnywhere のインストールに使用されたライセンス。

オプション	説明
最近の感染	エンドポイントで感染が報告された日時。
最新のス キャ ン時間	このエンドポイントでの最新のスキャンの時刻。
最終確認日時	前回このエンドポイントが管理ポータルにチェックインした日時。
マルウェアグループ	マルウェアの分類。トロイの木馬やシステム監視など。
MD5	ファイルを固有に識別するための指紋のような働きをする、メッセー ジダイジェストアルゴリズム 5 の値。
OS	エンドポイントのOS。
パス名	ファイルが検出されたディレクトリまたはフォルダ。
ポリシー	エンドポイントに割り当てられたポリシー。
製品	ファイルに関連する製品の名前。SecureAnywhere が情報を特定で きる場合のみ。

オプション	説明
	スキャンの種類:
スキャンの種類	 ディープスキャン クリーンアップ後のスキャン カスタム / 右 クリックスキャン
	エンドポイントの現在の状態:
	• 保護 - 感染なし。
状態	• 感染 - マルウェアを検出。
	• 最近確認されていません - ポータルへの報告なし。portal.
	•期限切れ - SecureAnywhere ライセンスが期限切れ。
	• 感染および期限切れ
システムパック	OS のサービスパックの番号。
システムの種類	32 ビットまたは 64 ビット。
ベンダー	ファイルに関連するベンダーの名前。SecureAnywhere が情報を特定できる場合のみ。

オプション	説明
バージョン	ファイルに関連する製品のバージョン。SecureAnywhere が情報を特定できる場合のみ。
VM	エンドポイントが仮想マシンにインストールされている場合に[はい]。
Windows フル OS	Windows OS の名前。

管理コンソールへのアクセス

エンドポイントプロテクションで管理コンソールの[サイト]タブに戻るには、次の手順に従ってください。

管理コンソールにアクセスするには

- 1. エンドポイントコンソールで、以下のいずれかを実行します。
 - [サイトに戻る] ボタンをクリックします。

Secure Anywhere. Managed by 2019 Webroot Sales Demo Console		
Back To Sites Home Endpoint Protect	ction Admins Downloads	
Status Policies Group Management R	teports Overrides Alerts Settings Logs Resources	
🔤 Status 🔍	Endpoints encountering threats (last 7 days)	
Protected 0 Endpoints need attention		

• コンソール名のドロップダウンメニューで [サイトに戻る]を選択します。

Prestige Direct Sales Solution	Sites
Search	h for hostname Q Advanced Search
	🐵 Webroot Threat Blog 🛛 🚿
	Antivirus vs. VPN: Do You Need Both?

2. [サイト] タブがアクティブになった状態で管理コンソールに戻ります。

Secure Any	where	0												Con	sole v 🏠 v	⊘ ∨ JaneDoe	@gmail.com ~
Dashboard Sites	Admins	Groups	Policies	Overrides	Alerts	Reports	Settings	Security Awareness Traini	ng								
Sites 4 Results 11 Sites Acces	sible 11 T	īotal											Q Search			+ 🕁	⊒0 ¢
Status 🔶	Site	¢									Devices \Leftrightarrow	Site Seats 👳	DNS Protection 👄		Security Awaren	ess Training 🔶	
Protected	Cafe	Disco							Manage	©7	11	11	Active	\$	Active		\$ Z
Protected	Down! The Pet Emporium			Manage	©7	0 🛈	4	Active	鐐	Active		\$ Z					
Protected	Haymont Tires				Manage	07	3 🕕	9	Active	\$	S Active		\$ Z				
Protected	Prest	tige Direct Sa	les Solutions						Manage	©7	9 🛈	25	Active	\$	S Active		\$ Z
											23 Active Devices 0 Trial Active Device	49 Site Seats 0 Trial Site Seats					

第3章:ユーザーアカウントの管理

アカウントの管理方法については、以下のトピックを参照してください。

ポータルユーザーの作成 68 新規ポータルユーザーの作成 68 ユーザー情報の編集 72 コンソールユーザーの権限設定 75 アカウントへのキーコードの追加 81 アカウントへのコンソールの追加 84 コンソールの追加 84 コンソールの追加 90 コンソールの名前の変更 90 コンソールの切り替え 90 オンソールの切り替え 90 コンソールの切り替え 90 コンソールの短航 91 サイト管理者の追加 93 サイト管理者設定の編集 98	自分のアカウント設定の編集	
新規ポータルユーザーの作成 68 ユーザー情報の編集 72 コンソールユーザーの権限設定 75 アカウントへのキーコードの追加 81 アカウントへのコンソールの追加 84 コンソールの追加 84 コンソールの追加 90 コンソールの切り替え 90 アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98	ポータルユーザーの管理	68
ユーザー情報の編集 72 コンソールユーザーの権限設定 75 アカウントへのキーコードの追加 81 アカウントへのコンソールの追加 84 コンソールの追加 84 コンソールの追加 90 コンソールの引り替え 90 アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98	新規ポータルユーザーの作成	
コンソールユーザーの権限設定 75 アカウントへのキーコードの追加 81 アカウントへのコンソールの追加 84 コンソールの追加 84 コンソールの追加 90 コンソールの名前の変更 90 コンソールの切り替え 90 アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98	ユーザー情報の編集	72
アカウントへのキーコードの追加 81 アカウントへのコンソールの追加 84 コンソールの追加 84 コンソールの名前の変更 90 コンソールの切り替え 90 アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98	コンソールユーザーの権限設定	
アカウントへのコンソールの追加 84 コンソールの追加 84 コンソールの名前の変更 90 コンソールの切り替え 90 アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98	アカウントへのキーコードの追加	
コンソールの追加 84 コンソールの名前の変更 90 コンソールの切り替え 90 アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98 サイト管理者の追加 98	アカウントへのコンソールの追加	
コンソールの名前の変更 90 コンソールの切り替え 90 アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98 リイト管理者の追加 93	コンソールの追加	84
コンソールの切り替え 90 アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98 サイト管理者設定の編集 98	コンソールの名前の変更	
アカウントの更新またはアップグレード 91 サイト管理者の追加 93 サイト管理者設定の編集 98 サイト管理者: 91	コンソールの切り替え	
サイト管理者の追加 93 サイト管理者設定の編集 98 リイト管理者の追加 93	アカウントの更新またはアップグレード	
サイト管理者設定の編集	サイト管理者の追加	
	サイト管理者設定の編集	
サイト官理者の削除	サイト管理者の削除	

自分のアカウント設定の編集

アカウントでは、ログイン名やパスワードなどユーザーの詳細のほか、アクセス権限を定義します。自分のアカウントについては、ログイン名に指定した電子メールアドレス以外の設定を変更することができます。

注意:他のポータルユーザーの設定を編集する場合は、「<u>ポータルユーザーの管理ページ68」を参照</u> してください。

自分のアカウント設定の編集の詳細については、以下の手順を参照してください。

- 管理者の詳細 / 権限の編集 ページ55
- <u>2 要素認証の無効化ページ59</u>
- パスワードの変更ページ61
- セキュリティコードの変更ページ63
- セキュリティの質問の変更ページ65

管理者の詳細 / 権限の編集

1. ログイン ID の横にある下向き 矢印をクリックし、[アカウント設定]をクリックします。

Secure Anywhere.		User	rs @ webroot.com
Home Endedint Protection	C.e.	0	Account Settings
Lingdon Protection		2	Manage Users
Status Policies Group Management Reports Alerts Overrides Log	s Resources	P	Manage Keycodes
Endpoints encountering threats (last 7 days)	Agent Version Spread	٢	Downloads
1	2.67%	0	Help
	20.00%	c,	Support
		20	Logout
No endpoints have encountered	1.33%		8.0.2.127
threats in the tast 7 days			8.0.2.126
	12.00%		8.0.2.118
	1.33%		8.0.2.109 Others

2. [アカウント設定] ページで [詳細を編集] をクリックすると、[管理者の詳細] タブが表示されます。 このタ ブで情報を編集できます。

🖞 Edit Details 📋 Edit Per	missions	
User Details		
Name	6	
Display Name		
Email		
Office Phone		
Mobile Phone		
Time Zone		United States, Colorado, Colorado S
2FA		Enable
Password		Change
Security Code		Change
Security Question		Change
Access & Permissions		
SecureAnywhere Console		Admin
Endpoint Protection Console		Admin

3. [管理者の詳細]パネルで名前、電話番号、タイムゾーンを変更し、[情報を保存]をクリックして [アカウント設定]ページに戻ります。

注意: [表示名] は、管理コンソールに表示される名前です。

Seci	ureAnywhe	ere.		
Home	Endpoint Protection	Admins	Downloads	
Accou	nt Settings			
Admin Deta	ils Access & Permission	ns		
First Nam	ie			
Last Nam	e			
Display N	ame			
Office Ph	one			
Mobile Pl	2006			
Mobile II				
Time Zon	e			
(UTC/G	MT)			
Save D	etails			

4. 次に、アクセス権限を確認するために、[アクセスおよび権限]タブをクリックします。

Account Settings
Admin Details Access & Permissions
SecureAnywhere Console
Admin
Endpoint Protection Console
Admin
Groups
- Create & Edit
Seactivate/Reactivate Endpoints
Sasign Endpoints
Policies
🧭 Create & Edit
Assign Policies to Endpoints
Overrides
File and Web Overrides
File Determination Capabilities Good & Bad 🔻
Commands
O None
Simple
Advanced
• Expert
Alerts
🧭 Create & Edit
Save Access & Permissions
@ 2019 Webroot Inc. Privacy Stat

注意: メインのエンドポイントプロテクション管理者の場合は、デフォルトの設定のままにしておく ことをお勧めします。

設定の詳細については、「コンソールユーザーの権限設定ページ75」を参照してください。

5. 終了したら、[アクセスおよび権限を保存]ボタンをクリックして [アカウント設定] ページに戻ります。

2要素認証の無効化

- 1. <u>エンドポイントコンソール</u>にログインし、画面の右上隅にあるドロップダウンメニューで [**アカウント設定**]タ ブをクリックしてアカウント設定を表示します。
- 2. [2FA] の横にある [無効化] をクリックして [2FA を無効にする] ワークフローを開きます。

ccount Settings	
了 Edit Details 首 Edit Permissions	
Jser Details	
Name	
Display Name	
Email	
Office Phone	
Mobile Phone	
lime Zone	United States, Colorado, Colorado Springs, Denver
2FA	Disable (To Disable 2FA you will need to reauthenticate your console session)
Password	Change
Security Code	Change
Security Question	Change
Access & Permissions	
SecureAnywhere Console	Admin
Endpoint Protection Consolo	Admin

3. アカウントに関連付けられた電子メールアドレスまたは電話番号とパスワードを入力し、[続行]をクリックします。

Disable 2FA	
Step 1	
In order to disable two-factor authenticatio	n, you will first need to reauthenticate.
Email / Phone	
Password	
•••••	

4. モバイル認証用アプリを開き、そこに表示されているコードを[認証コード] ボックスに入力して [確認] をクリックします。

WEBRO	OT
Authentication Code	
at a	
Please enter your authentication code.	
Authentication Code	Lost or Stolen Device?
123456	
Confirm	

5. [2FA を無効にする]をクリックします。

WEBROO	T C
Disable 2FA	
By disabling 2FA, the next time that you log in, you be will a instead. You can re-enable 2FA at any time in the Admin sec Console or the Account Settings section of the Consumer W	sked to enter your Security Code tion of the Business Management eb Console.
Cancel	Disable 2FA

注意: 2FA を無効にする場合、アカウントの登録時に作成したセキュリティコードを入力する必要があります。2FA は、コンソールの[管理者] タブでいつでも再び有効にできます。詳細については、「2 要素認証 (2FA) の有効化 ページ16」を参照してください。

6. 2FA が無効になりました。アカウントで 2FA が無効になったことを通知する確認の電子メールが送信されます。

Reply Q	Reply All GForward GtilM Mon 11/18/2019 1:19 PM no-reply@webrootanywhere.com IMPORTANT- Account Information			
Hello,				
The account associated with this email address has had 2 Factor Authentication Disabled.				
If this was not you please check your settings or if you need additional assistance please contact a support representative.				
Thank you,				
The Webroo	The Webroot Team			

パスワードの変更

1. [アカウント設定] ページで [パスワード] の横にある [変更] をクリックすると、[パスワードの変更] ページ が開きます。

Secure Any where.	
account Settings	
🖞 Edit Details 📋 Edit Permissions	
User Details	
Name	
Display Name	
Email	
Office Phone	
Mobile Phone	
Time Zone	United States, Colorado, Colorado Springs, Denver
2FA	Disable (To Disable 2FA you will need to reauthenticate your console session)
Password	Change
Security Code	Change
Security Question	Change
Access & Permissions	
SecureAnywhere Console	Admin
Endpoint Protection Console	Admin
2. 現在のパスワードと新しいパスワードを入力したら、[パスワードの変更]をクリックします。

Change D	acurard				
Change F	ISSWOID				
Current Pa	ssword				
New Pass	word				
	•••				
Strength:		Very Strong			
Retype	our password	to avoid mista	kes		
			•		

セキュリティコードの変更

1. [アカウント設定] ページで [セキュリティコード] の横にある [変更] をクリックすると、[セキュリティコードの 変更] ページが開きます。

ccount Settings	
중 Edit Details 집 Edit Permissions	
Name	
Display Name	
Email	
Office Phone	
Mobile Phone	
Time Zone	United States, Colorado, Colorado Springs, Denver
2FA	Disable (To Disable 2FA you will need to reauthenticate your console session)
Password	Change
Security Code	Change
Security Question	Change
Access & Permissions	
SecureAnywhere Console	Admin

2. 新しい個人用セキュリティコードをボックスに入力し、パスワードを入力したら、[セキュリティコードの変 更]をクリックします。

Secure Anywhere	2
Change Security Code	
Change Security Code	
New Personal Security Code	ſm
Enter Password	
Change Security Code	

セキュリティの質問の変更

1. [アカウント設定] ページで [セキュリティの質問] の横にある [変更] をクリックすると、[セキュリティの質問の変更] ページが開きます。

Secure Anywhere.	
Account Settings	
Edit Details	
User Details	
Name	
Display Name	
Email	
Office Phone	
Mobile Phone	
Time Zone	United States, Colorado, Colorado Springs, Denver
2FA	Disable (To Disable 2FA you will need to reauthenticate your console session)
Password	Change
Security Code	Change
Security Question	Change
Access & Permissions	
SecureAnywhere Console	Admin
Endpoint Protection Console	Admin

2. セキュリティの質問を選択するには、それぞれのドロップダウンの矢印をクリックしてリストから質問を選択します。また、該当するボックスにその回答も入力します。最後に [セキュリティの質問の変更] をクリック

すると、アカウントのセキュリティの質問が更新されます。

Secure Anywhere	
Change Security Questions	
Change Security Questions	
Question 1	
Who was your best childhood friend?	\odot
Provide the answer to your security question (excluding characters < >).	
Question 2	
What was the make and model of your first car?	\odot
Answer 2	
Question 3	
What was your favourite childhood food?	\bigcirc
Answer 3	
Confirm Password	
Change Security Questions	

ポータルユーザーの管理

エンドポイントプロテクションの管理者権限を持っている場合、管理ポータルの新規ユーザーを作成し、そのア クセス権限を設定したり情報を編集したりできます。新規ユーザーを作成すると、エンドポイントプロテクション から、パスワードの作成とログインに関する詳細情報が記載された電子メールが新規ユーザーに送信されま す。

詳細については、「コンソールユーザーの権限設定ページ75」を参照してください。

このトピックでは、次の手順について説明します。

- 新規ポータルユーザーの作成
- ユーザー情報の編集

新規ポータルユーザーの作成

他の管理者を追加して、その管理者がエンドポイントプロテクションのレポートにアクセスできるようにした方が よい場合もあります。また、データの表示のみが可能で変更はできないように、追加したユーザーの権限を制 限することもできます。

新規ポータルユーザーを作成するには

1. ログイン ID の横にある下向き矢印をクリックし、[ユーザーの管理]を選択します。



2. [ユーザーの管理]パネルで [新規ユーザーの作成] ボタンをクリックします。



3. [新規ユーザーの作成] パネルで、ユーザーの電子メールアドレスを入力します。これは、ユーザーが確認メッセージを受信するアドレスで、ユーザーのログイン名としても使用されます。

間違った電子メールアドレスを入力したためにメッセージを受信できない場合は、後から電子メールア ドレスを変更してメッセージを再送信することができます。詳細については、「<u>ユーザー情報の編集</u>」を 参照してください。

4. [タイムゾーン] フィールドの右側の鉛筆アイコンをクリックして、国、地域、または主要都市を入力する と、タイムゾーンのドロップダウンメニューが開き、ユーザーの所在地を選択できます。

Create New User		
Please complete the details below to o	create a new user	
Email Address Time Zone Do you wish to give this user Console access?	Gallagher@webroot.com United States, Colorado, Denver, Colorado Springs (MDT)	Ø

5. [はい] チェックボックスを選択します。

ペインの下部にさらに2つのフィールドが表示されます。

Please complete the details be	elow to create a new user	
mail Address	Gallagher@webroot.com	
ime Zone	United States, Colorado, Denver, Colorado Springs (MDT)	
nine source		
Do you wish to give this user Console	access? Ves	
Do you wish to give this user Console SecureAnywhere	access? Ves Basic	
Do you wish to give this user Console a SecureAnywhere Endpoint Protection	Basic No Access	

 SecureAnywhere - <u>my.webrootanywhere.com</u>のホームページです。ユーザーはこのページから、モバ イルプロテクションポータル(モバイルプロテクションを購入した場合)など、ウェブルートの他のポータル にアクセスできます。詳細については、WSA Business - モバイルプロテクション管理者ガイドを参照し てください。

Nobile Protection
2 Devices Protected 0 Infected 0 Need Attention

エンドポイントプロテクション - エンドポイントプロテクションの管理ポータルまたは管理者コンソールです。ユーザーがこのポータルにアクセスできる場合、[エンドポイントプロテクションに進む] ボタンをクリックして管理ポータルにアクセスすることができます。Portal.

Secure Anywhere.	
Home Endpoint Protection Mobile Protection	
Endpoint Protection	Mobile Protection
7 Endpoints Protected 0 Endpoints Currently Infected 0 Endpoints Infected (last 24 hours) Go to Endpoint Protection	2 Devices Protected 0 Infected 0 Need Attention Go to Mobile Protection

- 6. Secure Anywhere のドロップダウンの矢印で、次のいずれかを選択します。
 - 基本 コンソールとアカウント設定への制限付きアクセス権を付与します。
 - 管理者 ウェブルートポータルのすべてのキーコード、ユーザー、アカウント設定への完全なアクセス 権を付与します。
- 7. エンドポイントプロテクションのドロップダウンメニューで、次のいずれかを選択します。
 - ・アクセス不可
 - 基本 エンドポイントスキャンへの読み取り専用アクセス権
 - 管理者 すべての設定への完全なアクセス権

このユーザー権限を後から変更する方法の詳細については、「<u>コンソールユーザーの権限設定ページ</u> <u>75</u>」を参照してください。

8. 完了したら、[ユーザーを作成] ボタンをクリックします。

新しいユーザーに確認の電子メールが送信されます。この電子メールメッセージには、初回にログインするための仮のパスワードが記載されています。ユーザーが電子メールに記載された確認のリンクをクリックすると、[登録確認] パネルが開き、ログイン情報を入力できます。

A temporary password had b	een emailed to you.	
Temporary Password *		
Create New Password *		
	Strength: Internet in the	
Repeat New Password *		
Your Personal Security Code *		
Security Question *		~
Securty Answer*		
	Confirm	

ユーザー情報の編集

ユーザーが登録を確認すると、[ユーザーの管理] パネルに戻り、そのユーザーの情報を編集することができます。他のユーザーのパスワード、セキュリティコード、セキュリティの質問を表示または編集することはできません。これらの情報にアクセスできるのはそのユーザーのみです。

ユーザーが登録を確認していない場合、ユーザーの状態は [確認待ち] と表示されます。ユーザーが電子メールを受信して登録を確認すると、状態が [アクティブ] に変わります。必要に応じて、 [確認待ち] 状態の横にある封筒のアイコンをクリックすると、確認の電子メールを再送信できます。

Manage L	lsers
Create New	User
Name	Email
	bj@webroot.com (Activated)
	jan@webroot.com (Awaiting Confirmation)
	giri@webroot.com (Activated)

ポータルユーザーを編集するには

1. 編集する必要のあるユーザーの行を探し、右端にあるそのユーザーの編集アイコンをクリックします。

Manag	je Users			
Create	New User			
Name	Email	Permissions		
		Secure Anywhere	Endpoint Protection	~
	ph4@webroot.com (Activated)	Admin	Basic	(&)
	ph5@.webroot.com (Activated)	Admin	Admin	×

注意: アカウントに複数のコンソールがある場合、現在アクティブなコンソールのキーコードに関連付けられたユーザーのみが表示されます。コンソールの詳細については、「アカウントへのコンソールの追加ページ84」を参照してください。

2. [ユーザーの詳細]パネルでは、必要に応じて名前や電話番号を変更できます。

ユーザーの状態が[確認待ち]の場合、このウィンドウの上部に電子メールフィールドが表示されます。 ユーザーの電子メールアドレスを間違って入力したために登録を再送信する必要がある場合は、電子 メールアドレスを変更してください。

Account Settings		
User Details Acces	s & Permissions	
Email Address	SME_2013@ webroot.com	
First Name	I	
Last Name		
Display Name		
Office Phone		
Mobile Phone		
Time Zone	(UTC/GMT)	1
	Save Details	

注意:[アクセスおよび権限]の設定を変更する方法の詳細については、「<u>コンソールユーザーの</u> <u>権限設定ページ75</u>」を参照してください。

3. 完了したら、[情報を保存]ボタンをクリックします。

コンソールユーザーの権限設定

エンドポイントプロテクションの管理者権限を持っている場合、他の管理ポータルのユーザーについて、次のような権限を編集することができます。

- サイトへのアクセス Secure Anywhere Web サイト、my.secureanywhere.com のホームパネル、エンドポイント プロテクションの管理ポータルのアクセスレベルを基本レベルと管理者レベルの間で切り替えます。
- グループ ユーザーがエンドポイントのグループの作成および修正、エンドポイントの非アクティブ化または再 アクティブ化、グループへのエンドポイントの割り当てを実行できるかどうかを指定します。
- ポリシー ユーザーがポリシーの作成および修正、またはエンドポイントへのポリシーの割り当てを実行できる かどうかを指定します。
- オーバーライド ユーザーがファイルを [正当] または [不当] としてオーバーライドできるかどうかを指定します。
- コマンド ユーザーがエンドポイントに対して発行できるコマンドの種類を指定します。
- 警告 ユーザーが警告メッセージを作成および編集できるようにします。

ポータルユーザーの権限を設定するには

1. ログイン ID の横にある下向き矢印をクリックし、[ユーザーの管理]を選択します。



2. 編集する必要のあるユーザーの行を探し、そのユーザーの編集アイコンをクリックします。
 編集アイコンは右端に表示されています。

ウェブルートエンドポイントプロテクション管理者ガイド

Manag	e Users			
Create	New User			
Name	Email	Permissions		
		Secure Anywhere	Endpoint Protection	-
	ph4@webroot.com (Activated)	Admin	Basic	
	ph5@.webroot.com (Activated)	Admin	Admin	¥

[ユーザーの詳細] パネルが表示されます。

3. [**アクセスおよび権限**] タブをクリックして、エンドポイントプロテクションの各種機能とそれらに関連するアクセス権限の一覧を表示します。

User Details Access & Permissions	
Do you wish to give this user Console access?	Ves Yes
SecureAnywhere Console	Admin
Endpoint Protection Console	Admin
Groups	
Create & Edit	V
Deactivate/Reactivate Endpoints	V
Assign Endpoints to Groups	V
Policies	
Create & Edit	V
Assign Policies to Endpoints	V
Overrides	
MD5	¥.
Determination Capability	Good & Bad
Commands	
None	0
Simple	0
Advanced	0
Expert	0
Alerts	
Create & Edit	V
	Save Access & Permissions

^{4.} このユーザーにアクセス権限を割り当てます。次の表で各権限について説明します。

オプション	説明
グループ	 作成・編集 - エンドポイントのグループを定義および修正します。 エンドポイントの非アクティブ化 / 再アクティブ化 - 管理ポータルからエンドポイントを非アクティブ化および再アクティブ化します。詳細については、「エンドポイントの非アクティブ化 ページ199」を参照してください。 グループへのエンドポイントの割り当て - ポータルユーザーが、あるグループの1つ以上のエンドポイントを別のグループに移動できるようにします。 詳細については、「エンドポイントをグループに整理ページ330」を参照してください。
ポリシー	 作成・編集 — ポリシーの定義、削除、名前変更、コピー、エクスポートを行います。 エンドポイントへのポリシーの割り当て - ポリシーをエンドポイントまたはエンドポイントのグループに関連付けます。 詳細については、「ポリシーの導入ページ222」を参照してください。

オプション	説明
オーバーライド	 MD5 - ファイルの MD5 値を入力して、ファイル検出方法をオーバーライドします。 MD5 (メッセージダイジェストアルゴリズム 5) とは、指紋のように動作してファイルを一意に識別する暗号学的ハッシュ関数です。 判定の範囲 - 次のような設定に基づいてオーバーライドを指定します。 正当 - 指定した MD5 値を含むファイルを許可します。 不正 - 指定した MD5 値を含むファイルをブロックします。スキャン中に該当するファイルが検出された場合、フラグが付けられ、SecureAnywhereユーザーによる対応が求められます。 正当 & 不正 - [正当] または [不正] のいずれかを許可します。 詳細については、「オーバーライドの導入 ページ424」を参照してください。
コマンド	 なし - このユーザーがエンドポイントにコマンドを送信することを許可しません。 シンプル - エージェントコマンドとデータ消去コマンドにアクセスし、選択したエンドポイントのコマンドを表示できます。 高度 - エージェント、データ消去、キーコード、電源 & ユーザーアクセス、マルウェア対策ツール、ファイル & プロセスの各コマンドにアクセスし、選択したエンドポイントのコマンドを表示できます。 エキスパート - エキスパート上級オプションを含むすべてのコマンドへのアクセスが可能です。 詳細については、「エンドポイントへのコマンドの発行ページ144」を参照してください。

オプション	説明
警告	作成・編集 - エンドポイントのアクティビティに対する警告の即時発行やスケ ジュールを設定できます。
	詳細については、「 <u>警告の導入ページ405</u> 」を参照してください。

5. 完了したら、[アクセスおよび権限を保存]ボタンをクリックします。

アカウントへのキーコードの追加

ウェブルートアカウントには1つまたは複数のキーコードを指定できます。キーコードは、SecureAnywhereをエンドポイントにインストールする際に使用される20文字から成るライセンスで、インストールで利用可能なシートの数を識別します。キーコードを追加購入する場合は、このセクションの説明に従って手動で追加する必要があります。

注意:既存のキーコードを参照して新しいコードを追加するには、エンドポイントプロテクションの管理 者権限を持っている必要があります。詳細については、「<u>コンソールユーザーの権限設定 ページ75</u>」を 参照してください。

アカウントにキーコードを追加するには

1. ログイン ID の横にある下向き矢印をクリックし、[キーコードの管理]を選択します。



[キーコードの管理]パネルが表示されます。

- それぞれのエンドポイントプロテクションのライセンスに関する属性がキーコードの一覧に表示されます。
- アカウントに複数のコンソールがある場合、現在アクティブなコンソールに関連付けられたキーコードのみが表示されます。

ウェブルートエンドポイントプロテクション管理者ガイド

Manage Keycodes					
Add Product Keycode Buy a Keycode no	w				
Keycode	Edition	Devices	Days Remaining	Renew	Upgrade
	Endpoint Protection	25	318 (Feb 23 2014)	Renew	Upgrade
	Endpoint Protection	100	296 (Jan 31 2014)	Renew	Upgrade

それぞれのエンドポイントプロテクションのライセンスに関する属性がキーコードの一覧に表示されます。

属性	説明
<i>+</i> ⊐ド	エンドポイントプロテクション購入時に受け取った20文字のライセンス。
エディション	購入したエンドポイントプロテクションまたは他のウェブルート製品。
デバイス	このキーコードを使用できるエンドポイントの数。
有効期限までの日数	このキーコードの使用期限が切れるまでの日数と有効期限の期日。
更新	定期購入契約を更新するためのリンク。 詳細については、「 <u>アカウントの更新またはアップグレード ページ91</u> .
アップグレード	このライセンスに対してエンドポイントのシートを追加購入するためのリン ク。 詳細については、「 <u>アカウントの更新またはアップグレード ページ91</u> 」を参 照してください。

^{2.} キーコードを追加購入するには、[キーコードを今すぐ購入]ボタンをクリックします。

ウェブルートビジネスのWebサイトが開きます。ここで別のキーコードを購入できます。

3. キーコードの購入後、[製品キーコードを追加]ボタンをクリックしてエンドポイントプロテクションにその キーコードを追加します。

Manage Keycodes					
Add Product Keycode Buy a Keycode now					
Keycode	Edition	Devices	Days Remaining	Renew	Upgrade
	Endpoint Protection	25	318 (Feb 23 2014)	Renew	Upgrade
	Endpoint Protection	100	296 (Jan 31 2014)	Renew	Upgrade

4. [キーコードを追加する] ダイアログで購入したキーコードを入力し、[追加]をクリックします。

新しいキーコードが[キーコードの管理]パネルと[リソース]タブに表示されます。

アカウントへのコンソールの追加

初めてアカウントを作成するときに、管理中のデバイスはエンドポイントプロテクションによって1つのコンソール にまとめられます。コンソールは、SecureAnywhere または他のウェブルート製品を実行している1つまたは複数のエンドポイントをひとまとめにした単位です。数百のエンドポイントを含む大規模なネットワークでは、複数のコンソールを作成してデバイスのグループの簡略化されたビューを使用した方がよい場合もあります。たとえば、リモートオフィスのエンドポイントや別々の部門のエンドポイントに対してそれぞれ別のコンソールを作成できます。

注意: コンソールを追加するには、ウェブルートから新しいキーコードを取得する必要があります。エンドポイントプロテクションの請求システムは、キーコードの数ではなくシートの数に基づいていることに注意してください。エンドポイントのシート数が上限に達していなければ、新たにキーコードを購入する必要はありません。詳細については、ウェブルートの販売部門までご連絡ください。

このトピックでは、次の手順について説明します。

- コンソールの追加
- コンソールの名前の変更
- コンソールの切り替え

コンソールの追加

コンソールを作成する前に、まず新しいキーコードを取得し、そのキーコードを使用して SecureAnywhere をエンドポイントに配備する必要があります。コンソールを作成すると、新しいキーコードを使用するエンドポイントが自動的に検出されます。既存のエンドポイントを別のコンソールへ移行する必要がある場合は、ウェブルートを法人向けサポートまでご連絡ください。

アカウントにコンソールを追加するには

- 1. SecureAnywhere の管理コンソールに移動します: <u>https://my.webrootanywhere.com.</u>
- 2. アカウントにはログインせずに [アカウントの作成] ボタンをクリックします。

Secu	reAny	where.	
Log in	\sim	Create Account	\supset
Log in			
Email or Phone			0
Password		Forgotten Passv	word?
Log in			
Renewing your license?			
Get started			

ウェブルートエンドポイントプロテクション管理者ガイド

3. [ウェブルート製品のキーコード]フィールドに新しいキーコードを入力します。

Secu	reAnywhere.
Log in	Create Account
Create Account	
Webroot Product Keycode	
Email Address	
Repeat Email Address	
Password	
Strength:	
Repeat Password	
Your Personal Security Code	
Security Question	-
Security Answer	
	Register Now

^{4.} その他のフィールドについては、電子メールアドレス、パスワード、セキュリティコード、セキュリティの質問と回答に関して既存のアカウント情報を指定します。

フィールド	説明
電子メールアドレス	エンドポイントプロテクションを管理する管理者の電子メールアドレスを 入力します。 アカウントをアクティブ化するための確認のメッセージがこの電子メール アドレスに送信されます。このメールアドレスは、管理コンソールにログ インする際のユーザー名にもなります。
パスワード	9文字以上を入力してください。パスワードは、少なくともアルファベット6文字と数字3文字を含む必要があります。パスワードは最小文字数の9文字を超えても問題ありません。山括弧(<>)以外の特殊文字は使用可能です。パスワードの大文字と小文字は区別されます。 入力を始めると、強度メーターがパスワードの安全性を示します。最適なセキュリティを確保するために、パスワードはできるだけ強力なものにすることをお勧めします。
個人用セキュリティコード	文字または数字を入力してください。ログインする際に、パスワードを 入力した後の追加のセキュリティ対策として使用されます。6文字以 上で、覚えやすいコードを使用してください。 管理ポータルへのログイン時には毎回、このコードからランダムな2文 字を入力するように求められます。たとえば、コードが123456で、4番 目と6番目の文字を入力するよう求められた場合、「4」と「6」を入力 します。この個人用セキュリティコードでは大文字と小文字が区別さ れます。

フィールド	説明
セキュリティの質問	ドロップダウンリストから質問を選択します。 ログインの詳細情報を忘れた場合に、この質問に答えることで情報を 取得できます。
セキュリティの回答	セキュリティの質問に対する回答を入力します。セキュリティの回答で は大文字と小文字が区別されます。

^{5.} [今すぐ登録] ボタンをクリックします。

ウェブルートでユーザーのアカウント情報が認識されます。ここで、キーコードに対して新しいコンソールを 作成するか、既存のコンソールにキーコードを追加します。

nywhere console already owned by you.
de to an existing console
xisting account
Key Codes*
Product Key Code" button
code into the box and press "Add"
has now been successfully added to your el

6. 左側のパネルの[選択]ボタンをクリックして、新しいコンソールを追加します。

コンソールが作成され、ログインを促すプロンプトが表示されます。

7. アカウント情報を使ってログインした後、新しく作成された [名前のないコンソール]を選択します。名前の変更については、「コンソールの名前の変更」セクションで説明します。

新しいコンソールに、入力したキーコードを使用するすべてのエンドポイントの一覧が表示されます。

ウェブルートエンドポイントプロテクション管理者ガイド

Console name	Date created	Keycodes	Devices allowed	Expired keycodes
Unnamed Console	Feb 8 2012 20:41	1	50	0
SME	Jan 12 2012 17:04	1	10	0

コンソールの名前の変更

コンソールの名前を変更するには

1. 右上のログイン名の下にある[名前変更]ボタンをクリックします。

(Gallaghe	er@webroot.com	Ŧ
SME Re	name	E Change Cons	sole

2. 新しい名前を入力し、[保存]ボタンをクリックします。名前には数字とスペースを使用できますが、特殊文字は使用できません。

コンソールの切り替え

コンソールを切り替えるには

1. 右上のログイン名の下にある[コンソールを変更する]ボタンをクリックします。



2. 表示された表でコンソールの名前を選択します。

アカウントの更新またはアップグレード

管理ポータルから、エンドポイントプロテクションのライセンスの更新またはライセンスへのシートの追加を簡単に 行うことができます。ライセンスの有効期限がもうすぐ切れる場合、またはすでに切れている場合、[状態] パネルに警告メッセージが表示されます。

🕎 Status	*
Protected 0 Endpoints need attention	
All Keycodes Expired	
To continue using Webroot SecureAnywhere Endpoint Protection you must upgrade or renew a keycode.	
Upgrade / Renew	J

このメッセージに表示されている [アップグレード/更新] をクリックするか、以下の手順に従って [キーコードの管理] パネルに進みます。

アカウントを更新またはアップグレードするには

1. ログイン ID の横にある下向き矢印をクリックし、[キーコードの管理]を選択します。

Secure Anywhere.	(Jsen	s @ webroot.cor
Hama Endepint Destaction		٥	Account Settings
Home Endpoint Protection	Searc	퇸	Manage Users
Status Policies Group Management Reports Alerts Overrides Logs	Resources	"Q	Manage Keycodes
39 Kendpoints encountering threats (last 7 days)	Agent Version Spread	٢	Downloads
1	2.67%	0	Help
	20.00%	0	Support
	22	0	Logout
No endpoints have encountered	1.33%		8.0.2.127
uncere in unc last 7 days			8.0.2.119
	12.00%		8.0.2.118
	1.33%		8.0.2.109 Others

- 2. [キーコードの管理]ペインで、次のいずれかをクリックします。
 - 更新 ライセンスを更新する場合。
 - アップグレード ライセンスにシートを追加する場合。

Manage Keycodes					
Add Product Keycode Buy a Keycode no	w				
Keycode	Edition	Devices	Days Remaining	Renew	Upgrade
	Endpoint Protection	25	318 (Feb 23 2014)	Renew	Upgrade
	Endpoint Protection	100	296 (Jan 31 2014)	Renew	Upgrade

注意: ライセンスはキーコードに関連付けられているため、更新またはアップグレードするキー コードに該当する行を選択してください。

ウェブルートのWebサイトが開き、詳細な手順が表示されます。

サイト管理者の追加

エンドポイントプロテクションの管理者は、追加の管理者を作成できます。追加された管理者は、エンドポイントプロテクションのレポートやデータを閲覧することができます。

新規ユーザーを作成すると、エンドポイントプロテクションから、パスワードの作成とログインに関する詳細情報が記載された電子メールが新規ユーザーに送信されます。

サイト管理者を追加するには

- 1. ja-my.webrootanywhere.com にログインします。
- 2. [**エンドポイントプロテクション**] タブをクリックします。

エンドポイントプロテクションのコンソールが表示されます。

3. ログイン ID の横にあるドロップダウンメニューで [管理者の管理]を選択します。



4. [新規管理者の作成] ボタンをクリックします。



[新規管理者の作成]パネルが表示されます。

Secure Anywhere.		
Home Endpoint Protection Mobile	Protection	
Create New Admin		
Please complete the details below to c	reate a new admin	
Email Address	[
Time Zone	(UTC/GMT)	
Do you wish to give this admin console access?	Yes Yes	

5. [電子メールアドレス] フィールドにユーザーの電子メールアドレスを入力します。

Secu	ire Anywhere	e,		
Home	Endpoint Protection	Mobile Protection		
Create N Please c	New Admin	low to create a new	admin	
Email Addr Time Zone	ess	UTC/GMT)		2
Do you wis	h to give this admin console	access? 🔲 Yes		

ユーザーが確認メッセージを受信するアドレスを入力します。この電子メールアドレスは、ユーザーのログ イン名としても使用されます。間違った電子メールアドレスを入力したためにメッセージを受信できない 場合は、電子メールアドレスを変更してメッセージを再送信することができます。詳細については、「<u>サ</u> <u>イト管理者設定の編集 ページ98</u>」を参照してください。

- 6. タイムゾーンのフィールドで右側の鉛筆のアイコンをクリックし、国、地域、または主要都市を入力すると、ドロップダウンメニューに選択肢が表示されます。ドロップダウンメニューで、新しい管理者のタイム ゾーンを選択します。
- 7. [このユーザーにコンソールへのアクセス権を付与しますか?] チェックボックスを選択します。checkbox.

次のフィールドが表示されます。

- SecureAnywhere
- エンドポイントプロテクション
- モバイルプロテクション

Secure Anywhere.	
Home Endpoint Protection Mob	pile Protection
Create New Admin	
Please complete the details below to	o create a new admin
Email Address	
Time Zone	(UTC/GMT)
Do you wish to give this admin console access	? Ves
SecureAnywhere	Basic
Endpoint Protection	No Access
Mobile Protection	No Access
	Create Admin

- 8. SecureAnywhere のドロップダウンメニューで、次のいずれかを選択します。
 - 基本 コンソールとアカウント設定への制限付きアクセス権を付与します。
 - 管理者 ウェブルートポータルのすべてのキーコード、ユーザー、およびアカウント設定への完全なアクセス権を付与します。
- 9. エンドポイントプロテクションのドロップダウンメニューで、次のいずれかを選択します。
 - ・アクセス不可
 - 基本 エンドポイントスキャンへの読み取り専用アクセス権を付与します。
 - 管理者 すべての設定への完全なアクセス権を付与します。
- 10. モバイルプロテクションのドロップダウンメニューで、次のいずれかを選択します。

・アクセス

- ・アクセス不可
- 11. 設定が完了したら、[管理者を作成]ボタンをクリックします。管理者となる新規ユーザーに確認の電子メールが送信されます。

Secure Anywhere.	w
Home Endpoint Protection	Mobile Protection
Create New Admin	
Please complete the details below	w to create a new admin
Email Address	
Time Zone	(UTC/GMT)
Do you wish to give this admin console ac	cess? 🔽 Yes
SecureAnywhere	Basic
Endpoint Protection	No Access
Mobile Protection	No Access
	Create Admin

この電子メールメッセージには、初回にログインするための仮のパスワードが記載されています。

電子メールに記載された確認のリンクをクリックすると、管理者がログイン情報を入力するための[登録 確認]パネルが表示されます。 ウェブルートエンドポイントプロテクション管理者ガイド

サイト管理者設定の編集

管理者が登録を確認したら、[管理者の管理]パネルに戻り、そのユーザーの情報を編集することができます。

ユーザーが電子メールを受信して登録を確認すると、状態が [アクティブ] に変わります。

ユーザーが登録を確認していない場合、ユーザーの状態は[確認待ち]と表示されます。必要に応じて、[確認待ち]状態の横にある封筒のアイコンをクリックすると、確認の電子メールを再送信できます。

サイト管理者設定を編集するには

- 1. ja-my.webrootanywhere.com にログインします。
- 2. [**エンドポイントプロテクション**] タブをクリックします。

エンドポイントプロテクションのコンソールが表示されます。

3. メインメニューの[管理者]タブをクリックします。

Sec	ureAnywhe	ere.		
Home	Endpoint Protection	Admins	Downloads	

管理者のリストが表示されます。
SecureAnywhere.					
Home	Endpoint Protection Admins Downloads				
Manage	e Admins				
(+) Create	Admin				
Name	Email	Permissions			
		Secure Anywhere	Endpoint Protection		
		Admin	Admin	Edit	
		Admin	Admin	Edit	
	and the second sec	Admin	Admin	Edit	
	a supervise preserve a basis, but any feature of the	Admin	Admin	🗹 Edit	
1 2	> >				

4. 編集する必要のあるユーザーの行を探し、そのユーザーの[編集]ボタンをクリックします。

Seci	SecureAnywhere.					
Home	Endpoint Protection Admins Downloads					
Manag	ge Admins					
(+) Create	e Admin					
Name	Email	Permissions				
Name	Liioi	Secure Anywhere	Endpoint Protection			
		Admin	Admin	Edit		
	in product of the second	Admin	Admin	🗹 Edit		
	angewant of strength	Admin	Admin	Edit		
		Admin	Admin	Edit		
1	2 > >					

[アカウント設定] ウィンドウが、[管理者の詳細] タブがアクティブになった状態で表示されます。

Seci	ureAnywhe	ere.			
Home	Endpoint Protection	Admins	Downloads		
ACCOU Admin Deta	nt Settings ils Access & Permission	ns			
First Nam	ie				
Last Nam	Last Name				
Display N	Display Name				
Office Pho	one				
Mobile Pr	ione				
Time Zon	e MT)				
Save De	etails				

- 5. 完了したら、[情報を保存]ボタンをクリックします。
- 6. アクセスおよび権限]タブをクリックします。

Account Settings
Admin Details Access & Permissions
SecureAnywhere Console
Admin
Endpoint Protection Console
Admin
Groups
Create & Edit
Deactivate/Reactivate Endpoints
Assign Endpoints
Policies
Create & Edit
Assign Policies to Endpoints
Overrides
File and Web Overrides
File Determination Capabilities Good & Bad 👻
Commands
O None
Simple
Advanced
• Expert
Alerts
Create & Edit
Save Access & Permissions
© 2019 Webrott Inc. Privacy Stat

7. 必要に応じて、次の表の情報に従って設定を変更します。

設定	説明
SecureAnywhere ⊐ ンソール	次の権限レベルのいずれかを選択します。 • アクセス不可 • 基本 • 管理者
エンドポイント プロテ クションのコンソール	次の権限レベルのいずれかを選択します。 アクセス不可 基本 管理者
グループ	
作成·編集	このチェックボックスを選択すると、管理者がエンドポイントのグループを定義 したり修正したりできるようになります。
エンドポイントの非ア クティブ化 / 再アク ティブ化	このチェックボックスを選択すると、管理者が管理ポータルからエンドポイント を非アクティブ化したり再アクティブ化したりできるようになります。 詳細については、「エンドポイントの非アクティブ化ページ199」を参照してく ださい。

設定	説明
グループへのエンドポ イントの割り当て	このチェックボックスを選択すると、管理者があるグループの1つ以上のエン ドポイントを別のグループに移動できるようになります。 詳細については、「 <u>エンドポイントをグループに整理ページ330</u> 」を参照してく ださい。
ポリシー	
作成·編集	このチェックボックスを選択すると、管理者がポリシーの定義、削除、名前変 更、コピー、エクスポートを実行できるようになります。
エンドポイントへのポ リシーの割り当て	このチェックボックスを選択すると、管理者がポリシーをエンドポイントまたはエ ンドポイントのグループに関連付けられるようになります。 詳細については、「 <u>ポリシーの導入ページ222</u> 」を参照してください。
オーバーライド	
MD5	このチェックボックスを選択すると、管理者がファイルの MD5 値を入力して、 ファイル検出方法をオーバーライドできるようになります。 MD5 (メッセージダイジェストアルゴリズム 5) とは、指紋のように動作してファ イルを一意に識別する暗号学的ハッシュ関数です。

設定	説明
	ドロップダウンメニューから次のいずれかを選択してオーバーライドを決定します。
判定の範囲	 正当 - 指定した MD5 値を含むファイルを許可します。 不正 - 指定した MD5 値を含むファイルをブロックします。スキャン中に該当するファイルが検出された場合、フラグが付けられ、SecureAnywhereユーザーによる対応が求められます。
	• 正当 & 不正 - [正当] または [不正] のいずれかを許可します。 詳細については、「 <u>オーバーライドの導入 ページ424</u> 」を参照してください。
コマンド	
なし	管理者がエンドポイントにコマンドを送信できないようにするには、このラジ オボタンを選択します。
シンプル	管理者がエージェントコマンドとデータ消去コマンドにアクセスし、選択したエ ンドポイントのコマンドを表示できるようにするには、このラジオボタンを選択 します。
詳細	管理者がエージェント、データ消去、キーコード、電源 & ユーザーアクセス、 マルウェア対策ツール、ファイル & プロセスの各コマンドにアクセスし、選択し たエンドポイントのコマンドを表示できるようにするには、このラジオボタンを 選択します。
エキスパート	管理者がエキスパート上級オプションを含むすべてのコマンドにアクセスでき るようにするには、このラジオボタンを選択します。

設定	説明
警告	
作成·編集	管理者がエンドポイントのアクティビティに対する警告の即時発行やスケジュールを設定できるようにするには、このチェックボックスを選択します。 詳細については、「 <u>警告の導入ページ405</u> 」を参照してください。

8. 完了したら、[アクセスおよび権限を保存]ボタンをクリックします。

サイト管理者の削除

サイト管理者を削除するには

- 1. ja-my.webrootanywhere.com にログインします。
- 2. [**エンドポイントプロテクション**] タブをクリックします。

エンドポイントプロテクションのコンソールが表示されます。

3. ログイン ID の横にあるドロップダウンメニューで [管理者の管理]を選択します。



管理者のリストが表示されます。.

Secure Anywhere.							
Home Endpoint Protection Mobile Protection				201	4 Sales Demonstration	n Cons	sole
Manage Admins							
Create New Admins							
Name	Email		Permissions				
			Secure Anywhere	Endpoint Protection	Mobile Protectio		
John Doe	jdoe@gmail.com	(Activated)	Admin	Admin	Access	&	×
Mary Doe	mdoe@gmail.com	(Activated)	Admin	Admin	Access	&	×
John Smith	jsmith@gmail.com	n (Activated)	Admin	Admin	Access	&	×
Mary Smith	msmith@gmail.co	om (Activated)	Admin	Admin	Access	&	×

4. 編集する必要のあるユーザーの行を探し、そのユーザーの[削除] アイコンをクリックします。

secureAnywhere.							
Home Endpoint Protection	Iobile Protection		2014 Sales Demonstration Cons			ole	
Manage Admins							
Create New Admins							
Name	Email		Permissions				
			Secure Anywhere	Endpoint Protection	Mobile Protectio		
John Doe	jdoe@gmail.com	(Activated)	Admin	Admin	Access	&	×
Mary Doe	mdoe@gmail.com	(Activated)	Admin	Admin	Access	&	×
John Smith	jsmith@gmail.con	n (Activated)	Admin	Admin	Access	&	B
Mary Smith	msmith@gmail.co	om (Activated)	Admin	Admin	Access	&	×

警告メッセージが表示されます。



- 5. [はい] ボタンをクリックして削除を承認します。
- 6. ブラウザを更新し、サイト管理者がシステムから削除されたことを確認します。

第4章:エンドポイントの管理

エンドポイントの管理方法については、以下のトピックを参照してください。

エンドポイントへの SecureAnywhere の配備	112
SecureAnywhere インストーラーの使用	116
MSI 配備オプションの使用	
GPO 配備オプションの使用	
インストーラーのオプション	132
ターミナル (RDS) サーバーおよび Citrix XenApp へのインストール	
複 製 イメージまたは VM へのインストール	
エンドポイントキーコードの変更	
エンドポイントの名前の変更	
エンドポイントの検索	
エンドポイントへのコマンドの発行	144
エンドポイントのアップデートとその他の変更の管理	
新しい OS への移行	
エンドポイントのハードウェアの変更	
新しいサブネット へのエンド ポイントの移動	
ファイアウォールを介した通信	
エンドポイントでの SecureAnywhere の使用	165
Windows コンピュータで SecureAnywhere を開く	
Mac コンピュータで SecureAnywhere を開く	
Mac の[Webroot SecureAnywhere] メニュー	
Mac の[システムツール]ドロップダウンメニュー	
スキャンの結果確認と脅威の管理	171
スキャン履 歴 の表 示	
ファイルの隔離からの復元	
ファイルのオーバーライドの設定	
アップデートのダウンロードと強制実行	
即時のアップデートの強制実行	
Web 脅威シールド Chrome ブラウザエクステンションのインストール	
Active Directory グループポリシーの使用	
Google スイートを利 用した単 ー カスタムアプリの強 制 インストール	
レジストリの使用	
エンドポイントでのコマンドの実行	
エンドポイントの非アクティブ化	
エンドポイントの非アクティブ化	
エンドポイントでの SecureAnywhere の再 アクティブ化	

第4章:エンドポイントの管理

cureAnywhere のアンインストール

エンドポイントへの SecureAnywhere の配備

ビジネス要件やネットワークの規模に応じて、さまざまな方法で SecureAnywhere をエンドポイントに配備する ことができます。Windows の PC、ノートパソコン、サーバー、またはネットワークにインストールされている仮想 サーバーをエンドポイントとして使用できます。エンドポイントのシステム要件については、「<u>セットアップの準備</u> <u>ページ5」</u>を参照してください。

注意:新しいエンドポイントがインストールされると管理者に通知が送信されるよう、警告を設定することができます。詳細については、「<u>警告の導入ページ405</u>」を参照してください。

エンドポイントに SecureAnywhere を配備するには

1. キーコードを確認します。キーコードが不明な場合は、管理ポータルの[**リソース**] タブをクリックしてください。

Status	Policies	Group Managemen	t Reports	Alerts Overrides	Logs Resources
👆 Reso	+ Resources				
Simp	ple Deployr	nent Options			
The	quickest ar	nd easiest way to ge	t endpoints repo	rting into the console	e is by downloading a copy o
The	user then s	simply needs to run t	the file, and their	endpoint will autom	atically report into the conso
Y	our availab	le keycodes / dowr	loads:		
S	SA23-TEST-TEST-TEST + Download Email template]
S	AA2-TEST-	TEST-TEST-TEST	🕹 Download	🖂 Email template]
Adva	Advanced Deployment Options:				
Rur	Run the installer in the background from a command line				
1. 2.	On the end Run the in:	dpoint, download the staller from a comma	Webroot Secur and line, using th	eAnywhere installer. ne commands listed i	Click here to download. in the deployment help. Click

注意: 管理ポータルへの報告を行うには、デバイスでエンドポイントプロテクションのキーコードを 使用している必要があります。SecureAnywhere がすでに異なる種類のキーコードを利用してイ ンストールされている場合は、「<u>エンドポイントキーコードの変更ページ135</u>」を参照してください。

2. 環境に最も適した配備の方法を選択します。

次の表では、さまざまな配備の方法について説明しています。

オプション	説明
SecureAnywhere 実行可 能ファイルの配備	次のいずれかの方法で Secure Anywhere のインストーラーファイルを配備します。
	 インストーラーでコマンドラインオプションを使用。プロキシサーバーの背後にあるエンドポイントへの配備が可能です。
MSI 配備オプションの使 用	Microsoft インストーラー (MSI) を使用して SecureAnywhere インストーラーファイルを配備。
Windows グループポリシー オブジェクト (GPO) の使用	グループポリシーオブジェクト (GPO) を使用して SecureAnywhere イン ストーラーファイルを配備。 Microsoft の Active Directory および GPO エディタに関する知識が必要です。

注意: Iエンドポイントの数が100未満の小規模ネットワークでは、[リソース] タブで説明するシ ンプルな配備オプションを使用することをお勧めします。大規模なネットワークで Active Directory を使用している場合は、高度な配備オプションを使用してください。大規模なネット ワークでは、エンドポイントを別々のコンソールに整理して、小さいグループごとの簡略化された ビューを使用することもできます。詳細については、「<u>アカウントへのコンソールの追加ページ84</u>」 を参照してください。

- 3. 以下のいずれかのセクションの説明に従って、SecureAnywhereをエンドポイントに配備します。
 - SecureAnywhere インストーラーの使用
 - <u>MSI 配備オプションの使用</u>。
 - GPO 配備オプションの使用

注意:管理ポータルで、エンドポイントの状態が報告されていることを確認します。詳細については、「エンドポイントの状態の表示ページ204」を参照してください。

- 4. 以下のいずれかの操作を行います。
 - エンドポイントがデフォルトのポリシーおよびグループに割り当てられるようにします。すべてのエンドポイントはまず、デフォルトのポリシーおよびグループに割り当てられます。割り当ては、必要に応じて後で変更することができます。詳細については、「<u>ポリシーの導入ページ222</u>」および「<u>エンドポイントのグ</u>ループへのポリシーの適用ページ324」を参照してください。
 - エンドポイントを特定のグループに割り当てるには、エンドポイントを追加するグループを選択し、[アクション]ドロップダウンメニューで[このグループにエンドポイントを配備]を選択します。

Status Policies Group Management F	Reports Alerts
Groups Views Search < 🕏	💻 Endpoints
Create Actions -	Save Chang
Group Name 🏝 Edit Group	Host
All Endpoints 😑 Delete Group	1 📄 WRI
Deactivated I 📑 Deploy Endpoints to this Group	2 📃 WRI
Default Group 4	
Bracknell 1	
Broomfield 2	
Dublin 1	

コマンドリンクからソフトウェアをインストールするために必要な情報が表示され、選択したグループにエンドポイントが追加されます。

Deploy Endpoints to this Group	×
Please find below instructions on how to deploy endpoints directly into a specified group:	
1. On the endpoint, download the Webroot SecureAnywhere installer file: http://anywhere.webrootcloudav.com/zerol/wsasme.exe	
2. Run the installer from a command line, using these commands:	
wsasme.exe /key=xxxx-xxxx-xxxx-xxxx /group=-135260017840748808 /silent	
For further deployment guidance, please reference the Deployment section of the help guide.	
Ok	

5. 設定が完了したら、[OK] ボタンをクリックします。

SecureAnywhere インストーラーの使用

次のいずれかの方法で SecureAnywhere のインストーラーファイルを配備します。

• 各エンドポイントに Secure Anywhere をインストール。Mac にインストールする場合はこのオプションを使用してください。

- エンドユーザーに電子メールを送信。エンドユーザーは、電子メールテンプレートに記載されたリンクをクリックしてソフトウェアをインストールできます。
- キーコードを使用して実行可能ファイル名を変更。この方法は、独自の配備ツールを使用することを計画している場合や、MSIコマンドを使用せずにバックグラウンドでインストールを実行することが望ましい場合に適しています。
- 追加コマンドを使用して実行可能ファイルをバックグラウンドで配備。
- インストーラーでコマンドラインオプションを使用。プロキシサーバーの背後にあるエンドポイントへの配備が可能です。

Windows 版の SecureAnywhere インストーラーを使用するには

1. エンドポイントで、SecureAnywhereのインストーラーファイルをダウンロードします。

インストーラーファイルは [リソース] タブにあります。または、次のリンクをクリックしてください。

http://anywhere.webrootcloudav.com/zerol/wsasme.exe

2. インストールパネルでキーコードを入力します。

キーコードが[リソース]タブに表示されます。

Se	CUre/	Anywhere.				
Insta	lation					
		Installation will only take Please enter your key Agree and Ins Agree and Ins Help me find my keycoo Installation options	e a few second ycode: stall de	s and will not require a reboot. By clicking Agree and Install, you accept the conditions of the Webroot software license	terms and	

- 3. 必要に応じて、インストールパネル下部にある [インストールオプション] ボタンをクリックし、次のオプション を設定できます。
 - SecureAnywhere へのショートカットをデスクトップに作成する このオプションを選択すると、 Windows のデスクトップに SecureAnywhere のショートカットアイコンが作成されます。
 - 感染を回避するために、インストールファイルの名前をランダムに変更する このオプションを選択す ると、ウェブルートのインストールファイルの名前がランダムに変更されます (「QrXC251G.exe」など)。 これにより、マルウェアによるウェブルートのインストールファイルの検出とブロックを回避できます。
 - SecureAnywhere のファイル、プロセス、メモリを改ざんから保護する このオプションを選択すると、 自己保護とCAPTCHAのプロンプトが有効になります。CAPTCHAを使用する場合、重要なアクションを実行する前に、ユーザーが画面上の歪んだ文字を読みとり、文字をフィールドに入力する必要があります。
 - 言語を変更する SecureAnywhere で表示される言語を変更する場合は、[言語を変更する] ボ タンをクリックして、サポートされている言語を選択してください。表示言語はインストールの際にのみ 変更できます。インストール後は変更できません。
- 4. [同意してインストール] ボタンをクリックします。

インストール中に Secure Anywhere によるクイックスキャンがエンドポイントで実行されます。

Mac版のSecureAnywhere インストーラーを使用するには

1. エンドポイントで、SecureAnywhere のインストーラーファイルをダウンロードします。

インストーラーファイルは [リソース] タブにあります。または、次のリンクをクリックしてください。

http://anywhere.webrootcloudav.com/zerol/wsamac.dmg

- 2. SecureAnywhere インストーラーを Mac にダウンロードします。
- 3. wsamac.dmgをダブルクリックしてインストーラーを開きます。
- 4. [**アプリケーション**] フォルダをダブルクリックして開きます。
- 5. [アプリケーション] フォルダの Webroot SecureAnywhere のアイコンをダブルクリックし、アクティブ化を開始します。
- 6. 初期アクティブ化ウィンドウの言語選択ドロップダウンメニューで言語を選択し、[次へ] ボタンをクリックします。

注意:必ず適切な言語を選択してください。SecureAnywhere のインストール後に言語を変更 することはできません。

🤫 Window
SecureAnywhere.
MAC
Secule VII) VIII EI E
Language Selection Please select a language that will be used for Webroot SecureAnywhere. To change the language you must uninstall and reinstall the application.
Next Cancel

7. 次のパネルでキーコードを入力し、[アクティブ化]ボタンをクリックします。

🛞 Webroot SecureAnywhere
SecureAnywhere.
MAE
Enter your keycode to activate your software
Help me find my keycode
By clicking Activate, you accept the terms of the Webroot software license agreement.
View the Webroot software license agreement
Activate

8. その他の画面のプロンプトに従ってインストールを最後まで進めます。

エンドユーザーが自分で SecureAnywhere をインストールできるよう電子メールを送信するには

- 1. [リソース] タブをクリックします。
- 2. [**電子メールテンプレート**] リンクをクリックします。

電子メールテンプレートが[使用を開始するには]ウィンドウに表示されます。



3. 電子メールメッセージにテキストをカット & ペーストします。正しいキーコードがリンクにより自動的に追加されます。ユーザーに電子メールを送信します。

ユーザーがインストールを開始するリンクをクリックします。プログラムは、入力済みの正しいキーコードを 使用してバックグラウンドでインストールを実行します。プロセスが完了すると、エンドポイントのシステム トレイにウェブルートのアイコンが表示されます。

実行可能ファイルの名前を変更してバックグラウンドでインストールを実行するには

キーコードを含む実行可能ファイルの名前を変更して SecureAnywhere を配備することができます。この方法 は、独自の配備ツールを使用することを計画している場合や、MSI コマンドを使用せずにバックグラウンドでイ ンストールを実行することが望ましい場合に適しています。前述の電子メールテンプレートを使用することもで きます。その場合、名前を変更したインストーラーをキーコードに含めるようあらかじめ設定されています。

注意: UAC (ユーザーアカウント制御) 環境では、インストーラーの実行に使用するアカウントにローカ ルの管理者権限が必要です。エンドユーザーに対して UAC プロンプトが表示されないようにするに は、UAC 環境で上級権限を持つプロセスからインストーラーを実行する必要があります。 1. エンドポイントで、以下の Secure Anywhere のインストーラーファイルをダウンロードします。

http://anywhere.webrootcloudav.com/zerol/wsasme.exe

2. インストーラーファイル名の wsasme の部分をキーコードに置き換えます。

ファイル名は XXXX-XXXX-XXXX-XXXX-XXXX.exe という形式になります。

3. 独自の配備ツールを使用して Secure Anywhere ソフトウェアをエンドポイントにインストールします。

コマンドラインからバックグラウンドでインストールを実行するには

1. エンドポイントで、以下の Secure Anywhere のインストーラーファイルをダウンロードします。

http://anywhere.webrootcloudav.com/zerol/wsasme.exe

以下の表に記載されているコマンドオプションを使用して、コマンドラインからインストーラーを実行します。他にも利用できるオプションがあります。詳細については、ウェブルート法人向けサポートまでお問い合わせください。

Windows のコマンドラインオプション

コマンドライン	説明	
/key=keycode	指定されたキーコードを使用してインストールします。ハイフンは 入力しなくても構いません。 例: wsasme.exe /key=xxxx-xxxx-xxxx-xxxx	
/silent	バックグラウンドでインストールします。	
/nostart	SecureAnywhere を起動せずにインストールします。	

コマンドライン	説明
	指定したパスワードを使用して SecureAnywhere を自動アンイ ンストールできます。このオプションは、SecureAnywhere をバック グラウンドでアンインストールする必要が生じた場合に適してい ます。
/lockautouninstall=password	アンインストールを実行するには、/autouninstall コマンドを使用 します。
	/lockautouninstall を使用する場合、コントロールパネルの [プログ ラムの追加と削除] に SecureAnywhere は表示されません。 SecureAnywhere を [プログラムの追加と削除] に含めるには、 /exeshowaddremove を使用します。
	/lockautouninstall に対応するコマンドです。例: wsasme.exe/autouninstall=password
/autouninstall=password	デフォルトでは、非管理モードでユーザーがソフトウェアを削除で きないようにするため、コントロールパネルの[プログラムの追加と 削除]には SecureAnywhere は表示されません。

コマンドライン	説明		
-clone	クローン化したマシン / VM に対して使用します。ポータルで表 示するマシン ID および PC のホスト名を変更するための、永続 的な一意の値をエージェントが PC 上で作成できるようにしま す。 製品ログでは、管理者が対象の PC を認識できるよう、このフラ グが示されます。たとえば、"適用された一意のマシン ID: C8137921" の場合、C8137921 はホスト名 (例: PCHOSTNAME-C8137921) に一致し、InstanceMID と DeviceMID の最初の 8 バイトに対応します。これにより、それぞ れが元の ID とは異なる、特定可能な値となります。 この値は、エージェントがアンインストール/再インストールされた 場合に、既存のエージェントが他の ID に移動することがないよ う保持されます。OS が再インストールされると、ID は変更されま す。 例: wsasme.exe /key=xxx-xxxx-xxxx-xxxx /silent -clone 注意: InstanceMID が一致することによりコンソールまた はエンドポイントで重複が発生する場合に使用し、各 ポーリング間隔でエンドポイントを置き換えます。		

コマンドライン	説明	
/exeshowaddremove	SecureAnywhere をコントロールパネルの [プログラムの追加と削除] に表示します。 例: wsasme.exe /key=xxxx-xxxx-xxxx /lockautouninstall=password/exeshowaddremove	
	注意: SecureAnywhere を [プログラムの追加と削除] に 表示すると、非管理モードでエンドポイントユーザーがソフ トウェアを削除できるようになります。	

グループに直接配備するコマンドラインスイッチです。 例: wsasme.exe /key=xxxxxxxx /group=-135260017840748808 /silent エンドボイントを特定のグループに割り当てるには、エンドボイントを追加するグループを選択し、[アクション]ドロップダウンメニューで[このグループにエンドボイントを配備]を選択します。 GROUPCODEをメモしておきます。 その他の要件: ・ グループがコンソールに既に存在している必要があります。 アンソールで確認されたことのないシステムでの新規インストールはこついてのみ使用できます。 コマンドラインの例: msiexec /i "C:\wsasme.msi" GUILIC="XXXX-XXXX-XXXX" WMSI のインストールの場合は、コマンドラインとMSI エディタを使用できます。 MSI エディタの場合の CMDLINE フィールドの例: Group=-135260017840748808	コマンドライン	説明
	/group=groupcode	 グループに直接配備するコマンドラインスイッチです。 例: wsasme.exe /key=xxxxxxxx /group=-135260017840748808 /silent エンドポイントを特定のグループに割り当てるには、エンドポイン トを追加するグループを選択し、[アクション]ドロップダウンメ ニューで[このグループにコンドポイントを配備]を選択します。 GROUPCODEをメモしておきます。 その他の要件: グループがコンソールに既に存在している必要があります。 コンソールで確認されたことのないシステムでの新規インストー ルについてのみ使用できます。 コマンドラインの例: msiexec /i "C:\wsasme.msi" GUILIC="XXXX-XXXX-XXXX" CMDLINE="SME, quiet, Group=-135260017840748808" /qn /1*v %windir%\wsa_install_log.txt MSI のインストールの場合は、コマンドラインとMSI エディタを使用できます。 MSI エディタの場合の CMDLINE フィールドの例: Group=- 135260017840748808

コマンドライン	説明
-proxyhost=X -proxyport=X - proxyuser=X -proxypass=X - proxyauth=#	プロキシ設定を指定します。
	注意:エンドポイントがプロキシサーバーを使用して接続する場合、SecureAnywhere は自動的にプロキシ設定を検出します。SecureAnywhere は、エンドポイントの再起動時および15分おきにプロキシ設定に対する変更を チェックします。プロキシ設定については自動検出を使用 することをお勧めしますが、コマンドラインオプションを使用 することも可能です。
	プロキシのサポートを有効にするには、以下のコマンドラインオプ ションを使用します。wsasme.exe -proxyhost=nn.nn.nn - proxyauth=n (where n can be 0=Any, 1=Basic, 2=Digest, 3=Negotiate, 4=NTLM) -proxyuser=proxyuser - proxypass=password -proxyport=port_number
	-proxyauth には、0 (Any) ではなく別の数値を使用することをお 勧めします。 Any オプションでは、エンドポイントがすべての認証 タイプを検索する必要があります。 このため、プロキシサーバー上 で不要なエラーや通信の遅延が発生することがあります。
	このコマンドラインオプションを使用する場合は、すべてのパラ メータを使用し、不要なパラメータについては値を入力せずに二 重引用符のみを入力してください(例:proxypass=""

コマンドライン	説明
Image: Angle of the second	<pre>デフォルト言語の検出を許可する代わりに、製品に対して使用 する言語を指定します。コードは以下のとおりです。</pre> en - 英語 ja - 日本語 es - スペイン語 fr - フランス語 de - ドイツ語 it - イタリア語 nl - オランダ語 ko - 韓国語 zh-cn - 簡体字中国語 pt - ポルトガル語 (ブラジル) ru - ロシア語 tr - トルコ語 zh-tw - 繁体字中国語 例: wasme.exe /key=xxxxxxxx /silent /lang=ru

Mac のコマンドライン

コマンドライン	説明
-silent	サイレントモードでインストールされます。 sudo "/Applications/Webroot SecureAnywhere.app/Contents/MacOS/Webroot SecureAnywhere" install -keycode= <keycode> -silent</keycode>
	認証方式、ホスト、ポート、ユーザー、パスワードを含むプロキ シのインストール引数を指定します。
-proxy_auth= -proxy_host= -proxy_port= -proxy_user= -proxy_pass=	<pre>auth_any_0 auth_basic_1 auth_digest_2 auth_negociate_3 auth_ntlm_4 open "/Applications/Webroot SecureAnywhere.app"args install -keycode=<keycode> -proxy_auth=auth_any_0 - proxy_host=<host> -proxy_port=<port> -proxy_user=<user> -proxy_pass=<password></password></user></port></host></keycode></pre>
-keycode=	インストールでキーコードが要求されません。 open "/Applications/Webroot SecureAnywhere.app"args install -keycode= <keycode></keycode>

コマンドライン	説明
-language=	指定された言語でインストールします。 open "/Applications/Webroot SecureAnywhere.app"args install -language=en 注意:言語の一覧は今後追加予定です。
文字列全体	<pre>sudo "/Applications/Webroot SecureAnywhere.app/Contents/MacOS/Webroot SecureAnywhere" install -keycode=XXXX-XXXX-XXXX-XXXX- XXXX -language=en -silent -proxy_auth=auth_basic_1 - proxy_host=proxy.proxy.com -proxy_port=8080 -proxy_ user=proxyuser.com -proxy_pass=proxypass</pre>

ウェブルートエンドポイントプロテクション管理者ガイド

MSI 配備オプションの使用

Microsoft インストーラー (MSI) を使用したインストールでは、エンドポイントプロテクションのインストールモード をアクティブにするキーコードおよびオプションを適用するために、インストール中にコマンドが必要となります。 MSI インストーラーはデフォルトでは対話型であり、バックグラウンドで自動インストールを実行するには、 msiexec.exe のオプション "/qn" を必要とします。

MSI コマンドの例:

msiexec /i wsasme.msi GUILIC=licensekey CMDLINE=SME,quiet /qn /l*v install.log

注意: UAC (ユーザーアカウント制御) 環境では、インストーラーの実行に使用するアカウントにローカルの管理者権限が必要です。エンドポイントのユーザーに対して UAC プロンプトが表示されないようにするには、UAC 環境で上級権限を持つプロセスからインストーラーを実行する必要があります。

後で SecureAnywhere を削除するには

Secure Anywhere ソフトウェアを後でエンドポイントから削除する必要がある場合は、次の標準の MSI コマンドを使用します。

msiexec /x wsasme.msi /qn /L*v uninstall.log

MSI エディタを使用するには

自分で Secure Anywhere ソフトウェアをエンドポイントに配備する場合は、以下の表のコマンドをインストール中に msiexec.exe に渡すことができます。

コマンド	説明
CMDLINE	SME,quiet
GUILIC	ライセンスキー。 ハイフンの入力は必須ではありません。 注意:キーコードを入力しなくてもインストールは続行されますが、エ ンドポイントにキーコードが関連付けられないためエンドポイントは保 護されません。キーコードなしでインストールする場合、ソフトウェアをア ンインストールしてから再インストールしてキーコードを追加する必要が あります。
ARPNOREMOVE	エンドユーザーがアンインストールできないようにします。

ORCA などの MSI エディタを使用して、これらのコマンドを直接変更することもできます。

- [プロパティ] テーブルで CMDLINE のプロパティを適切な値に設定します。
- [プロパティ] テーブルで GUILIC のプロパティを使用するキーコードに設定します。
- [プロパティ] テーブルで ARPNOREMOVE のプロパティを適切な値に設定します。

GPO 配備オプションの使用

GPO を使用して Secure Anywhere をインストールするには、Microsoft の Active Directory および GPO エディタに関する知識が必要です。

また、GPO の使用方法に関するビデオ「<u>How to Deploy Using Group Policy - SecureAnywhere Business</u>」(英語版) も参照してください。

GPO を使用して SecureAnywhere をインストールするには

1. 以下の場所から、SecureAnywhere MSI インストーラーをネットワーク共有にダウンロードします。

http://anywhere.webrootcloudav.com/zerol/wsasme.msi

ファイルをダウンロードし、SecureAnywhere を配備するすべてのエンドポイントからアクセスできるようにします。

- 2. 配備グループのドメインコントローラーとなるサーバーに移動します。
- 3. ドメインコントローラー上の GPO エディタを開いて、 配備 グループのポリシーを作成します。
- 4. グループポリシーを作成する組織単位に属するすべてのエンドポイントに Secure Anywhere を割り当てます。

グループ内のエンドポイントを再起動すると、SecureAnywhere がインストールされます。

インストーラーのオプション

WSA エージェントには、EXE と MSI の 2 つの形 式 のインストーラーが用 意 されており、 どちらも WSA コンソー ルの [リソース] タブにあります。

- EXE EXE ファイル形式は、汎用 EXE ファイル wsasme.exe を使用するか、WSA キーコードを使用して 名前が変更された EXE ファイルである Windows ダウンロードリンクを実行してダウンロード、インストールす ることができます。後者は実行するとインストールプロセスにキーコードを埋め込み、操作のいらないサイレン トインストールとして実行されます。
- MSI MSI 形式は、「MSI を使用してインストール」セクションにある <u>wsasme.msi</u> リンクを利用してダウン ロードすることができます。 MSI は、GUILIC プロパティのキーコード や CMDLINE プロパティのコマンドライン オプションを含むインストールをカスタマイズするために編集することができ、GPO を使用して配備できます。

ターミナル (RDS) サーバーおよび Citrix XenApp へのインストール

ターミナルサーバー (RDS サーバー) あるいはデスクトップ / セッションブローカーまたはホスト 共有 デスクトップ用 Citrix XenApp にインストールすると、WSA エージェントが、セッション間でカーネルモジュールを共有 することに より環境を保護し、それぞれにユーザープロセスを提供します。ウェブルート 管理コンソールが、ホストサーバー と各 セッションを組み合わせ、レポートおよび管理用に単一のエントリまたはデバイスとして表示します。WSA エージェントは、アプリケーションの仮想化を経由したストリーミングに対応していません。

複製 イメージまたは VM へのインストール

Webroot SecureAnywhere Business Endpoint Protection がインストールされると、ホスト名、SID、MAC アドレスなど、さまざまなハードウェアおよびソフトウェアのデータポイントから "マシン ID" が生成されます。エンドポイ

ントイメージが "Sysprep (システム準備)" されることなく再利用される、または VM がマスターイメージからコ ピーまたはプロビジョニングされ、配備やプロビジョニングの一環として Sysprep されない仮想環境にある場合、 エンドポイントは同じ "マシン ID" を使用してコンソールに報告し、同じポジションを奪い合うことになるか、ウェ ブルート管理コンソール内に複製が生成される可能性があります。

ウェブルート管理コンソールでこの事態が発生した場合、影響を受けたエンドポイントから Webroot SecureAnywhere Business Endpoint Protection をアンインストールしてください。構成ファイルが残らないように %PROGRAMDATA% にある"WRDATA" フォルダを削除するか名前を変更して、コマンドラインオプション "uniquedevice" で再インストールします。

例:

実行可能ファイルを使用した方法

"wsasme.exe /key=xxxx-xxxx-xxxx-xxxx /silent -uniquedevice"

MSI を使用した方法

CMDLINE -uniquedevice

これにより、SecureAnywhere がホスト名のチェックサムを取得して "マシン ID" を変更し、システムに対して一 意の ID を作成します。これは、マシンの OS やハードウェアがクローンされ、ホスト名が常に異なる場合に便 利です。この場合、一意のホスト名により、ウェブルート管理コンソールへの報告用に、デバイスの一意のイン スタンスを存在させることが可能になります。ホスト名はそのまま残るため、OS 内で存在するとおりにコンソー ルに報告されます。

この理由から、まず最初に Sysprep されることなくコピーされるイメージ、またはプロビジョニングに使用されるイ メージへの Webroot SecureAnywhere Business Endpoint Protection のインストールは推奨されません。非永続 VM 環境を含むほとんどの仮想環境では、グループポリシーやログオンスクリプトなどを使用して VM を配備し てから、Webroot SecureAnywhere Business Endpoint Protection をインストールする必要があります。

配備内でホスト名が一意ではない場合、"clone" インストールスイッチを使用してください。例:

実行可能ファイルを使用した方法

"wsasme.exe /key=xxxx-xxxx-xxxx-xxxx /silent -clone"

MSI を使用した方法

これによりレジストリキーが作成され、HKLM\System\CurrentControlSet\Control\CloneTimeStampFlags

これを使用して、ポータルで表示するマシン ID および PC のホスト名を変更するための、永続的な一意の値 をエージェントが PC 上で作成できるようにします。

スキャンログでは、管理者が対象のPCを認識できるよう、次のようなフラグが示されます。

"適用された一意のマシン ID: C8137921"

C8137921 はウェブルート管理コンソールに報告されたホスト名に一致します (例: PCHOSTNAME-C8137921 など)。この値は、エージェントがアンインストール / 再インストールされた場合に、既存のエージェントが他の ID に移動することがないよう保持されます。 OS が再インストールされると、 ID は変更されます。

Citrix 環境内での配備方法に関する詳細については、次のドキュメントを参照してください。

http://download.webroot.com/Citrix/Citrix.pdf
エンドポイントキーコードの変更

管理ポータルへの報告を行うには、エンドポイントでエンドポイントプロテクションのキーコードを使用している必要があります。ネットワーク内のエンドポイントに、SecureAnywhereの消費者向けバージョンなど、異なる種類のキーコードを利用して SecureAnywhere がすでにインストールされている場合は、新しいキーコードをエンドポイントから直接アクティブ化してキーコードを変更します。詳細については、以下の手順を参照してください。

キーコードを変更するコマンドの発行方法の詳細については、「<u>エンドポイントへのコマンドの発行ページ144</u>」 を参照してください。

エンドポイントのキーコードを変更するには

- 1. エンドポイントから、システムトレイのウェブルートのアイコンをダブルクリックして SecureAnywhere を開きます。
- 2. マイアカウントの歯車のアイコンをクリックします。
- 3. [新しいキーコードのアクティブ化] フィールドでキーコードを入力します。
- 4. [**アクティブ化**] ボタンをクリックします。

Secure	Anywhere.	? Ø: Advanced Settings
4 Keycode	About SecureAnywhere	My Account
My Subscription		Activate a new keycode
Keycode	SAES-****.****.****	Enter a new keycode into the field below and click "Activate"
Product	Endpoint Protection	
Status		
Subscription		
Copy keycod	e to dipboard	

新しいキーコードを入力すると、SecureAnywhere がスキャンを開始します。システムで自動的にスキャンが開始されない場合は、[PC セキュリティ] タブの [**コンピュータをスキャン**] をクリックします。スキャンが完了すると、SecureAnywhere は管理ポータルへの報告を行います。

Mac のエンドポイントキーコードを変更するには

- 1. エンドポイントから、メニューバーのウェブルートのアイコンをクリックし、続けてドロップダウンメニューで [Webroot SecureAnywhere を開く]を選択します。
- 2. メインウィンドウで [マイアカウント] を選択します。



3. [マイアカウント] ウィンド ウで [新しいキーコードのアクティブ化] ボタンをクリックします。

0	阙 Webroot SecureAnywhere
Home	My Account
My Account	
Status	Active 365 days remaining in your subscription Upgrade or renew Check for updates
Keycode	Activate a New Keycode

4. ダイアログでエンドポイントプロテクションのキーコードを入力し、[アクティブ化]ボタンをクリックします。

新しいキーコードがアクティブ化されたら管理ポータルに戻り、デフォルトのグループで新しいエンドポイントを探します。

必要に応じて、別のグループにエンドポイントを再割り当てします。詳細については、「<u>グループ間での</u> エンドポイントの移動ページ328」を参照してください。

Groups Views	«	¢		💂 Endpoints in Default Group							
😌 Create 😑 Delete 📺	Rename			Save (Changes 拘 Und	o Ch	ange 🔰 🜄 I	Move end	lpoints to and	other group	Apply policy to endpoints
Group Name	No.	1			Hostname		Policy	Status	First Seen	Last S	Last Infected
All Endpoints	16	Г			W7VM_SE_KH1		Unmana	②	Mar 9th	Aug 15	Aug 15th 2013, 19:38
Deactivated Endpoints	19		1		WEBROOT-0K	E	Unmana	۰۰۰ 🚯	Aug 5th	Aug 14	
Default Group	8	2	1		WEBROOT-0		Unmana	🚯	Jul 24th	Jul 24t	

エンドポイントの名前の変更

エンドポイントを追加する際、SecureAnywhere は、管理ポータルでそのエンドポイントを識別するためにマシンの名前を使用します。このため、"*Winchester-Laptop*"や "*LabTest-1*" など、分かりやすい名前に変更することをお勧めします。

注意: 仮想マシンでは、エンドポイントの名前を変更しないでください。名前を変更すると、管理ポータ ルに新しいエンドポイントとして表示され、不要なライセンスのシートが使用されます。

エンドポイントの名前を変更するには

- 1. [**グループの管理**] タブをクリックします。
- 2. 左側の[グループ]パネルで、名前を変更するエンドポイントを含むグループを選択します。
- 3. 右側の[エンドポイント]パネルで、エンドポイントの名前をダブルクリックします。



4. 新しい名前を入力して Enter キーを押します。

フィールドの左上に赤いフラグが付き、変更がまだ保存されていないことを示します。

5. コマンドバーの [変更を保存] ボタンをクリックします。

[ホスト名] カラムに新しい名前が表示されます。

6. 元の名前に戻す場合は、行の右端にある[戻す]ボタンをクリックします。

	V	Hostname	Policy	Group	
1		Webroot23	Recommended Defaults	Test2	
					Revert to original hostname

エンドポイントの検索

ダイナミックでフレキシブルな検索機能を使用して、単一または複数のエンドポイントを検索することができます。また、高度な検索オプションも利用できます。

各フィールドまたはドロップダウンメニューでは、あらゆる条件を組み合わせて対象を絞り込むことができます。 たとえば、状態のタイプとポリシーのタイプを検索する場合は、これら2つのフィールドのみを使用します。さらに フィルタリング機能を使用するには、追加情報を入力します。

エンドポイントを検索するには

- 1. [エンドポイントプロテクション] パネルで [グループの管理] タブをクリックします。
- 2. [検索]タブをクリックします。

[検索]パネルが表示されます。

Status Policies	Group Management	Repor	ts /	Alerts	Overrides	Logs	Resources	1	
Groups Views	Search < 🕫		Search	n Resul	ts				
Hostname:		 s	ave Cl	nanges	🛛 🖢 Undo Ch	anges ,	Move endpo	pints to ano	ther gro
nostiunic.				Host	name		Agent Ve	Workg	Keyco
Status:	All	1		СВА	SH-1234V-BRI	M EN	8.0.4.70	BOUL	SAFD-
Group:	All 🖍	2		DAC	-WIN7	EN	8.0.3.3	BOUL	SAFD-
Policy:	All 👻	3		NMIL	L-V-BRM	EN	8.0.4.68	BOUL	SAFD-
Active Directory:		4		PRA	VI-3255V-BRM	EN	8.0.4.70	BOUL	SAFD-
Keycode:	×	5		RDA	UB-1944V2	EN	8.0.4.63	BOUL	SAFD-
Distance		6		RDA	UB-1944V-BRI	M EN	8.0.4.63	BOUL	SAFD-
Platform:	All	7		RDA	UB-3560V-BRI	M EN	8.0.4.68	BOUL	SAFD-
Windows OS:	All 🖍	8		SWL	-1344V-SMT	EN	8.0.4.46	BOUL	SAFD-
Include Deactivated:		9		SWL	-1463V-SMT	EN	8.0.4.70	BOUL	SAFD-
Advanced		10		WIN	732RDAUB	EN	8.0.4.42	BOUL	SAFD-
- Advanced									
Agent Version:	e.g. 8.0.4.70								
Agent Language:	All								
Virtual Machine:	Yes 💌								
Device MID:									
Instance MID:									
Current User:	e.g. JSmith								
Public IP:	e.g. 66.35.53.194								
Internal IP Address:									
Workgroup:	¥								
MAC Address:	e.g. 00:26:B9:EF:22:02								
Reset	Submit								

3. [ホスト名] フィールドにホスト名を入力します。

このフィールドには自由形式でテキストを入力でき、大文字と小文字は区別されません。

- 4. [状態]ドロップダウンメニューで以下のいずれかを選択します。
 - 保護

- 感染あり
- 期限切れ
- 感染および期限切れ
- 最近確認されていません
- 5. [グループ]ドロップダウンメニューで、検索するグループを選択します。
- 6. [ポリシー]ドロップダウンメニューで、検索するポリシーを選択します。
- 7. [アクティブディレクトリ] フィールドで、以下のいずれかの操作を行います。
 - Active Directory 名を入力する。
 - Active Directory の場所を参照する。
- 8. [キーコード]ドロップダウンメニューで、検索するキーコードを選択します。
- 9. [プラットフォーム]ドロップダウンメニューで、検索するプラットフォームを選択します。
- 10. [Windows OS] ドロップダウンメニューで、以下のいずれかの OS を選択します。
 - Windows XP
 - Windows Vista
 - Windows 7
 - Windows 8
 - Windows Server
 - MacOS
 - ・その他
- 11. 以下のいずれかの操作を行います。
 - 非アクティブ化されたエンドポイントを含める場合は、[非アクティブ化されたエンドポイントを含む]
 チェックボックスを選択する。
 - 非アクティブ化されたエンドポイントを含めない場合は、[非アクティブ化されたエンドポイントを含む]
 チェックボックスの選択を解除する。
- 12. 設定が完了したら、[送信]ボタンをクリックして結果を絞り込みます。

管理ポータルの右のパネルに、検索条件に一致するすべてのエンドポイントが表示されます。

高度な検索を実行するには

[エンドポイントプロテクション]パネルで、パネル右上にある[高度な検索]ボタンをクリックします。
 [高度な検索]パネルが表示されます。

dvanced Search			
All freeform (e.g. Searchir	a fields are case insensitive, and a	will match any part o	f the interrogated data.
(o.g. oodronn		onanco and inton y	
Hostname:			
Status:	*	Keycode:	~
Group:	*	Platform:	~
Policy:	*	Windows OS:	~
Active Directory:		Include Deactivated:	
Advanced			
Agent Version:	e.g. 8.0.4.70	Current User:	e.g. JSmith
Agent Language:	¥	Public IP:	e.g. 66.35.53.194
Virtual Machine:	Yes 💌	Internal IP Address:	
Device MID:		Workgroup:	~
Instance MID:		MAC Address:	e.g. 00:26:B9:EF:22:02
	Search	Cancel	

2. [エージェントのバージョン] フィールド にエージェントの番号を入力します。

これは自由形式のフィールドです。

3. [エージェントの言語]ドロップダウンメニューで、あらかじめ設定されたサポートされている言語のリストから選択します。

- 4. [VM] ドロップダウンメニューで、以下のいずれかを選択します。
 - はい デフォルトです。
 - ・いいえ
- 5. [デバイス MID] フィールドに、デバイスのウェブルートベースの一意の識別子を入力します。 これは自由形式のフィールドです。
- [インスタンス MID] フィールドに、インスタンスのウェブルートベースの識別子を入力します。
 これは自由形式のフィールドです。
- 7. [現在のユーザー] フィールドに現在のユーザー名を入力します。
 これは自由形式のフィールドです。
- [パブリック IP アドレス] フィールドにパブリック IP アドレスを入力します。
 これは自由形式のフィールドです。
- 9. [ローカル IP アドレス] フィールド にローカル IP アドレスを入力します。 これは自由形式のフィールドです。
- 10. [ワークグループ] ドロップダウンメニューで、あらかじめ設定された利用可能なワークグループのリストから 選択します。
- 11. [MAC アドレス] フィールドに MAC アドレスを入力します。 これは自由形式のフィールドです。
- 12. 設定が完了したら、[送信]ボタンをクリックして結果を絞り込みます。

管理ポータルの右のパネルに、検索条件に一致するすべてのエンドポイントが表示されます。

ウェブルートエンドポイントプロテクション管理者ガイド

エンドポイントへのコマンドの発行

管理ポータルでは、個々のエンドポイントまたはエンドポイントのグループに対してコマンドを発行することが可能です。たとえば、遠隔地のエンドポイントをスキャンすることができます。ここで紹介するコマンドを使用すると、エンドポイントのSecureAnywhere ソフトウェア上で利用できるものと同じコマンドを簡単に実行することができます。

ただし、エンドポイントは次回のポーリング間隔までコマンドを受信できないことに注意してください。必要に応じて、関連するポリシーでポーリング間隔を変更するか、即時のポーリングを強制することができます。詳細については、「<u>ポリシー設定の変更ページ247」</u>または「<u>即時のアップデートの強制実行ページ180</u>」を参照してください。

注意: コマンドに対するアクセス権限 (シンプル、アドバンスト、またはエキスパート)によっては、このセクションで紹介するコマンドの一部が表示されない場合があります。管理者は、アクセス権限を変更することができます。詳細については、「コンソールユーザーの権限設定ページ75」を参照してください。

エンドポイントにコマンドを発行するには

Secure Anywhere		
Home Endpoint Protection	Support	
Status Policies Group Managemen	t Reports Overrides Alerts Settings Logs Resources	Sear
🔤 Status	🥢 具 Endpoints encountering threats (last 7 days) 🗌 Agent Version Spread	
Protected 0 Endpoints need attention	Endpoint	1 Endpoint 9.0.10.19 9.0.4.12 8.0.2.127
	1E	ndpoint
	So most recent endpoints encountering threats (last 7 days)	*
	Hostname Policy Group Status Last Thr	Blocked Progr
	No endpoints have encountered	

1. エンドポイントのコンソールで [グループの管理] タブをクリックします。

[グループの管理] タブが表示されます。

Home Endpoint Protection Support									
Status Pointies Group Management	Reports 0	vernues Aleris Settings Lu	ligs inesources						
Groups Views Search « @	📕 All End	points							
🕒 Create 🗃 Actions 🗸	Save Ch	anges 🖕 Undo Changes 🌄 Mo	ve endpoints to another group 📃 Ap	oply policy to endpoints 🛒 Agent Co	ommands 🗸 📋 😑 Deactivate				
Group Name No.		Hostname	Policy	Group	Status				
All Endpoints 3	1	Endpoint A	test	Default Group	Protected				
Deactivated Endpoints 2	2	Endpoint B	Unmanaged	Default Group	Protected				
Default Group 3	3 🔳 🎽	Endpoint C	Unmanaged	Default Group	Protected				
new group 0									

2. [グループ] カラムで、コマンドを発行するエンドポイントが含まれるグループを選択します。

Home Endpoint F	Home Endpoint Protection Support									
Status Policies Gr	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources									
Groups Views Sea	Groups Views Search < 🛊 💻 All Endpoints									
🔂 Create 🛐 Actions 🗸		E s	ave Ch	anges 🔄 Undo Changes 🌄 Mov	e endpoints to another group 🔜 Ap	ply policy to endpoints 🛒 Agent Co	ommands 🗸 📔 🖨 Deactivate			
Group Name	No.			Hostname	Policy	Group	Status			
All Endpoints	3	1		Endpoint A	test	Default Group	Protected			
Deactivated Endpoints	2	2		Endpoint B	Unmanaged	Default Group	Protected			
Default Group	3	3	- 4	Endpoint C	Unmanaged	Default Group	Protected			
new group	•									

- 3. [エンドポイント]パネルで次のいずれかを実行して、エンドポイントの情報を表示します。
 - 1つのエンドポイントの横にあるチェックボックスを選択します。
 - チェックボックスのカラムの一番上にあるチェックボックスを選択します。

Home Endpoint Protection	Support								
Status Policies Group Manag	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources								
Groups Views Search	< 🔹 📃 AI	II Endpoints							
😌 Create 📔 Actions 🗸	🖬 Sa	ave Changes 🔄 Undo Changes 🌄 I	Move endpoints to another group 🛄 Ap	ply policy to endpoints 🛒 Agent Co	ommands 🗸 📔 😑 Deactivate				
Group Name No.		Hostname	Policy	Group	Status				
All Endpoints 3	1 [Endpoint A	test	Default Group	Protected				
Deactivated Endpoints 2	2 [Endpoint B	Unmanaged	Default Group	Protected				
Default Group 3	3	Endpoint C	Unmanaged	Default Group	Protected				
new group 0									

1 つまたは複数のチェックボックスを選択すると、コマンドバーの追加コマンドがアクティブになり、使用できる状態になります。

Home Endpoint Protection Support									
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources									
Groups Views Sear	Groups Views Search < 🖗 🗐 All Endpoints								
🛨 Create 🛐 Actions 🗸		n s	ave Ch	nanges 🔄 Undo Changes 🌄 Mov	ve endpoints to another group	📕 Apply policy to endpoints 📢 Age	nt Commands 🕶 🖨 Deactivate 🔵		
Group Name	No.		V	Hostname	Policy	Group	Status		
All Endpoints	3	1	V	Endpoint A	test	Default Group	Protected		
Deactivated Endpoints	2	2	V	Endpoint B	Unmanaged	Default Group	Protected		
Default Group	3	3	V 🗳	Endpoint C	Unmanaged	Default Group	Protected		
new group	0								

4. コマンドバーで、[エージェントコマンド]の下向きの矢印をクリックします。

Home Endpoint Protection Support										
Status Policies Grou	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources									
Groups Views Searc	Groups Views Search < 🛊 📮 All Endpoints									
🕒 Create 🛛 🛐 Actions 🗸		n s	ave Ch	nanges 눌 Undo Changes 🌄 Move	e endpoints to another group [Ap	ply policy to endpoints 🛒 Agent C	ommands - Deactivate			
Group Name	No.		V	Hostname	Policy	Group	Status			
All Endpoints	3	1	V	Endpoint A	test	Default Group	Protected			
Deactivated Endpoints	2	2	V	Endpoint B	Unmanaged	Default Group	Protected			
Default Group	3	3	V 🗳	Endpoint C	Unmanaged	Default Group	Protected			
new group	0									

選択した項目に応じた [エージェントコマンド] メニューが表示されます。

• PC エンドポイント、または PC と Mac エンドポイントの組み合わせを選択した場合、表示される [エージェントコマンド] メニューは次のとおりです。

I All Endpoints								
Save Ch	🔚 Save Changes 🔄 Undo Changes 🌄 Move endpoints to another group 属 Apply policy to endpoin			Agent Commands - Contractivate				
	Hostname	Policy	Group			Agent		🔍 Scan
1 🔽 🗧	Endpoint A	test	Default Group		\$	Clear Data	• (Change scan time
2 🔽	Endpoint B	Unmanaged	Default Group		***	Keycode		🔂 Scan a folder
3 🔽 🅰	Endpoint C	Unmanaged	Default Group		ø	Power & User Access		💞 Clean up
					ŵ	Antimalware Tools		system Optimizer
					01 10	Files & Processes		- Universal
						Identity Shield	Þ	Deset
				l	•	Advanced	▶ Ľ	Reset
						View commonds for colocted and contra	Ľ	Remove password protection
				l	8	view commands for selected endpoints		
			l		•	How to Use Agent Commands		
			```	1	_		_	

• Mac エンドポイントのみを選択した場合、次のような [エージェントコマンド] メニューが表示されます。ID シールドコマンドやパスワード保護を削除するためのオプションは含まれません。

📕 All	All Endpoints						
Sav	ve Changes   🔄 Undo Changes   🌄 Mov	e endpoints to another group   📃 Ap	oply policy to endpoints	(جا)	Agent Commands 🗸 😑 Deactivate		
E	Hostname	Policy	Group		Agent	0	Scan
1	Endpoint A	test	Default Group	\$	Clear Data		Change scan time
2	Endpoint B	Unmanaged	Default Group		Keycode		Scan a folder
3 👿	🗹 🎼 Endpoint C	Unmanaged	Default Group	ø	Power & User Access		Clean up
				Ê	Antimalware Tools		System Optimizer
				0	Advanced		Uninstall
					View commands for selected endpoints		Reset
				8	How to Use Agent Commands		

5. エージェントコマンドのカテゴリーを選択し、展開されるメニューから実行するコマンドを選択します。

各コマンドの説明については、以下の表を参照してください。

コマンド	説明	
エージェントコマンド		
スキャン	エンドポイントがコマンドを受信した後、ただちにバックグラウンド でディープスキャンを実行します。 スキャンが完了すると[スキャン履歴] パネルが開き、ディープス キャンの結果が表示されます。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。	
	<b>注意:</b> 検出された脅威は自動的に隔離されません。 ポータルで、クリーンアップの実行またはオーバーライドの 作成のいずれかの操作を実行する必要があります。	

コマンド	説明
<i>スキャ</i> ン時間を変更	エンドポイントをスキャンする新しい時間を選択します。 デフォルトでは、SecureAnywhere はインストールされた時刻と ほぼ同じ時刻に毎日スキャンを実行します。たとえば、 SecureAnywhere をエンドポイントに正午にインストールしたとす ると、スキャンは常に正午 12 時頃に始まります。このコマンドを 使用すると、この時刻を別の時刻に変更できます。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。
フォルダをスキャン	指定のフォルダ内の全ファイルに対してフルスキャンを実行しま す。フォルダの完全なパス名を入力してください。 Windows システムでは次のように入力します。 C:\Documents and Settings\Administrator\My Documents Mac システムでは次のように入力します。 /Applications このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。

コマンド	説明		
クリーンアップ	スキャンを開始して、悪意のあるファイルを自動的に隔離しま す。 スキャンが完了すると[スキャン履歴] パネルが開き、[クリーン アップ後のスキャン] の結果が表示されます。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。		
システム最適化ツール	システム最適化ツールをエンドポイントで実行します。このツー ルは、ウェブ閲覧履歴、ユーザーアクティビティを記録するファイ ル、ごみ箱内のファイルや Windows の一時ファイルなど貴重な ディスク容量を消費するファイルの痕跡をすべて削除します。 システム最適化ツールのオプションは、ポリシー設定で変更する ことができます。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。		

コマンド	説明			
アンインストール	SecureAnywhere をエンドポイントからアンインストールします。 このコマンドを使用しても、エンドポイントは管理ポータルに表示されたままとなります。 SecureAnywhere をアンインストールしてライセンスのシートを解放するには、エンドポイントを非アクティブ化します。詳細については、「エンドポイントの非アクティブ化ページ199」を参照してください。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。			
リセット	エンドポイントでの SecureAnywhere の設定をデフォルト値に戻 します。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。			
パスワード保護を削除	エンドポイントのユーザーによる制御でパスワードの保護を無効 にします。これにより、管理者はロックアウトされてもエンドポイン トにアクセスすることができます。 このコマンドは PC エンドポイントでのみ実行できます。			
Showgui	ポリシーで許可されている場合にUIを表示します。 例: "c:\program files\webroot\wrsa.exe" -showgui This command runs only on PC endpoints.			

コマンド	説明	
	サイレントモードでスキャンを開始します。 スキャン用 UI はユー ザーには表示されませんが、トレイアイコンにカーソルを合わせ ると表示されます。	
	コマンドの例:	
	WRSA.exe -silentscan="c:\foldername"	
	フォルダをスキャンする実行コマンドの例:	
Silentscan	"C:\Program Files\Webroot\WRSA.exe" - silentscan="c:\Documents and Settings\Administrator\Desktop"	
	ファイルをスキャンする実行コマンドの例:	
	"C:\Program Files\Webroot\WRSA.exe" - silentscan="c:\Documents and Settings\Administrator\Desktop\eicar.com"	
	このコマンドは PC エンドポイントでのみ実行できます。	
データ消去コマンド	1	
	現在のログファイルを消去して、エンドポイントの領域を解放し ます。	
ファイルを消去   	このコマンドは PC および Mac 両方のエンドポイントで実行できます。	

コマンド	説明	
プロキシ設定を無効化	エンドポイントのユーザーがエンドポイント上で設定したプロキシ 設定を無効にします。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。	
キーコードコマンド		
+—⊐—ドを変更	別のキーコードを入力します。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。 注意:ドロップダウンリストには、このコンソールに割り当 てられているキーコードのみが表示されます。	

コマンド	説明		
キ—⊐—ドを一時的に変更	このエンドポイントで使用するキーコードを一時的に切り替えま す。これは、テストなどの場合に必要になることがあります。 ダイアログボックスでドロップダウンリストからキーコードを選択し、 Secure Anywhere で使用する日付を指定します。指定した変 更日が終了すると、キーコードは元のキーコードに戻ります。 このコマンドは PC エンドポイントでのみ実行できます。		
電源およびユーザーアクセスコマンド			
エンドポイントをロック	ログイン画面を起動して、このエンドポイントをロックします。 再 びログインする際は、 ユーザー名とパスワードを入力する必要が あります。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。		
ログオフ	アカウントからユーザーをログオフします。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。		
再起動	報告時にこのエンドポイントを再起動します。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。		

コマンド	説明			
[セーフモードとネットワーク] で再 起動する	[セーフモードとネットワーク] でこのエンドポイントを再起動しま す。 このコマンドは PC エンドポイントでのみ実行できます。			
シャットダウン	報告時にこのエンドポイントをシャットダウンします。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。			
マルウェア対策ツールコマンド				
デスクトップの壁紙をリセット	デスクトップの壁紙をデフォルト設定にリセットします。これは、エ ンドポイントが最近マルウェアに感染して、壁紙が変更された 場合に必要となることがあります。 このコマンドを送信した後、PC エンドポイントを再起動する必 要があります。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。			
スクリーンセーバーをリセット	スクリーンセーバーをデフォルト設定にリセットします。これは、エ ンドポイントが最近マルウェアに感染して、スクリーンセーバーが 変更された場合に必要となることがあります。 このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。			

コマンド	説明	
システムポリシーをリセット	Windows システムポリシーをデフォルト設定にリセットします。こ れは、エンドポイントが最近マルウェアに感染し、タスクマネー ジャー設定などのポリシーが変更された場合に必要となること があります。 このコマンドは PC エンドポイントでのみ実行できます。 注意: このコマンドは、エンドポイントプロテクションのポ リシーではなく、Windows のポリシーをリセットします。	
ファイルを復元	MD5 値を使用して、隔離されたファイルを元の場所に復元します。 ファイルの MD5 値を確認する方法の詳細については、「 <u>オー バーライド] タブからのオーバーライドの適用 ページ439</u> 」を参照 してください。 このコマンドは PC エンドポイントでのみ実行できます。	
ファイルおよびプロセスコマンド		
すべてのファイルとプロセスを再検 証する	次回のスキャン時に、このファイルの分類を再検証します。 このコマンドは、設定したオーバーライドをエンドポイントで有効 にする必要がある場合に便利です。 このコマンドは PC エンドポイントでのみ実行できます。	

コマンド	説明	
すべてのアイテムを正当と評価	このエンドポイントで検出されたすべてのファイルを安全に実行 可能とみなします。 このコマンドは、エンドポイントで数多くの誤検出が確認され、 それらに素早く"正当" とタグ付けする必要がある場合に便利 です。 このコマンドは PC エンドポイントでのみ実行できます。	
ファイアウォールによりブロックされ たプロセスを許可	ファイアウォールの設定によりブロックされたすべてのプロセスにつ いて通信を許可します。 このコマンドは PC エンドポイントでのみ実行できます。	
信頼できないプロセスの強制終 了	信頼できないプロセスを停止します。これは、マルウェアプログラ ムの痕跡を通常のスキャンで完全に削除できなかった場合に 必要となることがあります。 プロセスはただちに停止されますが、再実行を防止することは できません。 このコマンドは PC エンドポイントでのみ実行できます。	
ID シールドコマンド		

コマンド	説明
アプリケーションを許可	エンドポイントでのアプリケーションの実行を許可します。
	<ul> <li>アプリケーションを特定するには、その MD5 値を入力する必要があります。</li> </ul>
	• MD5 値を確認するには、「 <u>/オーバーライド] タブからのオー</u> バーライドの適用 ページ439」を参照してください。
	このコマンドは PC エンドポイントでのみ実行できます。
アプリケーションを拒否	エンドポイントでのアプリケーションの実行をブロックします。
	<ul> <li>アプリケーションを特定するには、その MD5 値を入力する必要があります。</li> </ul>
	• MD5 値を確認するには、「 <u>/オーバーライド] タブからのオー</u> バーライドの適用 ページ439」を参照してください。
	このコマンドは PC エンドポイントでのみ実行できます。
拒否されているすべてのアプリ ケーションを許可	ブロックされたすべてのアプリケーションをリセットして、エンドポイントで実行できるようにします。
	このコマンドは PC エンドポイントでのみ実行できます。 

コマンド	説明
	エンドポイントで実行されているアプリケーションにセキュリティを 追加します。
アプリケーションを保護	<ul> <li>アプリケーションを特定するには、その MD5 値を入力する必要があります。</li> </ul>
	<ul> <li>MD5 値を確認するには、「<u>/オーバーライド] タブからのオー</u></li> <li>バーライドの適用ページ439」を参照してください。</li> </ul>
	このコマンドは PC エンドポイントでのみ実行できます。
	以前に [アプリケーションを保護] コマンドを使用してセキュリティ を追加した場合に、アプリケーションを標準の保護にリセットしま す。
アプリケーションの保護を解除	<ul> <li>アプリケーションを特定するには、その MD5 値を入力する必要があります。</li> </ul>
	<ul> <li>MD5 値を確認するには、「<u>/オーバーライド] タブからのオー</u></li> <li>バーライドの適用ページ439」を参照してください。</li> </ul>
	このコマンドは PC エンドポイントでのみ実行できます。
高度なコマンド	

コマンド	説明
カスタマー <del>リポー</del> トスクリプトを実 行	実行可能ファイルをエージェントにダウンロードする際の URL を 指定して、リモートで実行します。 このコマンドは PC エンドポイントでのみ実行できます。
カスタマーサポートの診断	<ul> <li>WSABLogs ユーティリティを実行して、感染したエンドポイント に関する情報を収集します。</li> <li>[カスタマーサポートの診断] ダイアログには、ユーティリティの実 行可能ファイルの場所と、エンドポイントアカウントに関連付け られている電子メールアドレスが表示されます。</li> <li>[送信] をクリックするとユーティリティが実行され、結果がウェブ ルート法人向けサポートに送信されます。</li> <li>また、オプションの詳細設定を指定すると、追加のファイルを送 信したり、ログを送信する代わりにローカルに保存したり、メモリ ダンプを収集したりできます。</li> <li>このコマンドは PC および Mac 両方のエンドポイントで実行でき ます。</li> <li>注意:オプションの設定は Mac には適用されないた め、Mac には必要ありません。</li> </ul>

- ^{6.} 必要に応じて、以下のいずれかを実行します。
  - 送信したコマンドの状態を表示するには、[エージェントコマンド]メニューで[**選択したエンドポイント** のコマンドを表示]を選択します。



コマンドログを確認するには、メインのエンドポイントプロテクションのコンソールで [ログ] タブをクリックします。詳細については、「<u>コマンドログの表示ページ520</u>」を参照してください。

Home Endpoint Protection Su	pport	
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources		
🕎 Status	Endpoints encountering threats (last 7 days)	
Protected 0 Endpoints need attention		

次回のポーリング間隔で、エンドポイントプロテクションが Windows コンピュータに対してコマンドを発行 します。必要に応じて、グループのポリシーの[基本設定] でポーリング間隔を変更したり、「<u>即時のアッ</u> <u>プデートの強制実行 ページ180</u>」の説明に従って即時の変更を強制したりできます。

Policy1			ă ? 🗆
Section	Setting	Live	Draft
Basic Configuration	Show a Webroot shortcut on the desktop	Off	
Scan Schedule	Show a system tray icon	On	
Scan Settings	Show a splash screen on bootup	On	
Self Protection	Show Webroot in the Start Menu	On	
Heuristics	Show Webroot in Add/Remove Programs	On	
Realtime Shield	Show Webroot in the Windows Security/Action Center	On	
Behavior Shield	Hide the Webroot keycode on-screen	On	
Core System Shield	Automatically download and apply updates	On	Daily
Web Threat Shield	Operate background functions using fewer CPU resources	Off	12 Hours
Identity Shield	Favor low disk usage over verbose logging (fewer details stored in logs)	Off	6 Hours
Firewall	Lower resource usage when intensive applications or games are detec.	On	4 Hours
User Interface	Allow Webroot to be shut down manually	Off	2 Hours
	Force non-critical notifications into the background	On	1 Hours
	Fade out warning messages automatically	On	30 Mins
	Store Execution History details	On	15 Mins
	Poll interval	15 Mins	15 Mins 🗸
			2
Promote Draft Changes to	Live Save (	Changes Reset	Changes Cancel

# エンドポイントのアップデートとその他の変更の管理

このセクションでは、エンドポイントのハードウェアや OS を変更する際に発生する可能性のある、いくつかの特殊な状況について説明しています。

- 新しい OS への移行
- エンドポイントのハードウェアの変更
- 新しいサブネットへのエンドポイントの移動
- <u>ファイアウォールを介した通信</u>

### 新しい **OS** への移行

エンドポイントに新しい OS をインストールすると、その変更によって管理ポータル内にエンドポイントのエントリの複製が作成されます。新しい OS をインストールする前に、エンドポイントを非アクティブ化してください。詳細については、「エンドポイントの非アクティブ化ページ199」を参照してください。

OS をインストール済みの場合は、管理ポータルで最も古いエントリを非アクティブ化してください。余分なライ センスは削除され、エンドポイントの複製は[非アクティブ化されたエンドポイント]のグループに追加されます。

**注意:** ほとんどの場合、OS をアップグレードするだけではエントリの複製が作成されることはありません。

### エンドポイントのハードウェアの変更

エンドポイントに新しいハードドライブを取り付け、SecureAnywhereを再インストールすると、管理ポータルで は新しいエントリとして表示されます。ハードドライブを交換する前に、余分なライセンスの使用を避けるた め、まず管理ポータルでエンドポイントを非アクティブ化してください。詳細については、「<u>エンドポイントの非アク</u> ティブ化 ページ199」を参照してください。

その他のタイプのハードウェアをエンドポイントで変更する場合 (新しいマザーボードやプロセッサ、ネットワーク アダプタを取り付ける場合など)、アップグレードされたコンピュータが管理ポータルで新しいエントリとして表示されることはありません。その場合は最初にエンドポイントを非アクティブ化にする必要はありません。

### 新しいサブネットへのエンドポイントの移動

エンドポイントを新しいサブネットへ移動する際は、それまでのサブネットと同じ通信回線を使用できるようにします。以下のドメインをファイアウォールで許可する必要があります。

*.webrootcloudav.com

*.webroot.com

*.s3.amazonaws.com

WSAWebFilteringPortal.elasticbean stalk.com

*.webrootanywhere.com

## ファイアウォールを介した通信

ファイアウォールがある場合、以下の表に記載されたウェブルートのパスマスクを許可してください。

ファイアウォールの詳細については、「<u>セットアップの準備ページ5</u>」を参照してください。

パス	詳細
*.webrootcloudav.com	エージェントの通信とアップデート。 注意:一部のファイアウォールでは、単一のワ イルドカードマスクを使用したダブルドットを含 むサブドメイン名 (例: 「g1.p4.webrootcloudav.com」を 「*.webrootcloudav.com」で表示)をサポート していません。このため、一部の環境では 「*.p4.webrootcloudav.com」または 「*.p4.webrootcloudav.com」のいずれかにしな ければならないことがあります。
*.webroot.com	エージェントのメッセージ送受信。
*.s3.amazonaws.com	エージェントのファイルのダウンロードとアップロード。

パス	詳細
WSAWebFilteringPortal.elasticbeanstalk.com	エージェントの Web フィルタリングに必要。 elasticbeanstalk は Amazon の AWS ドメイン。
*.webrootanywhere.com	管理ポータルとサポートチケットログのアップロード。

# エンドポイントでの SecureAnywhere の使用

状況により、設定変更のためSecureAnywhere インターフェイスからエンドポイントにアクセスする必要が生じる場合があります。これは、エンドポイントを非管理ポリシーに割り当てている場合など、管理ポータルからは制御できない場合に必要となることがあります。

このトピックでは、次の手順と情報を紹介します。

- <u>Windows コンピュータで SecureAnywhere を開く</u>
- Mac コンピュータで SecureAnywhere を開く
- <u>Mac の [Webroot SecureAnywhere] メニュー</u>
- <u>Mac の [システムツール] ドロップダウンメニュー</u>

**注意:** エンドポイントで Secure Anywhere インターフェイスを使用する手順の詳細については、<u>Webroot</u> Secure Anywhere の PC ユーザーガイドを参照してください。Mac コンピュータをお使いの場合は、 Secure Anywhere の Mac ユーザーガイドを参照してください。

## Windows コンピュータで SecureAnywhere を開く

Windows コンピュータで SecureAnywhere のメインインターフェイスを開くには

- 1. エンドポイントで次のいずれかの操作を行います。
  - デスクトップにあるウェブルートのショートカットアイコンをダブルクリックする。
  - システムトレイメニューのウェブルートアイコンを右クリックし、[開く]を選択する。



**注意:**システムトレイのアイコンが見つからない場合は、Windowsの[スタート]メニューを開き、[**すべてのプログラム**] > [Webroot SecureAnywhere] > [Webroot SecureAnywhere]の順に選択します。

[概要] ウィンドウが表示されます。



パネルの右側には、ナビゲーションタブを含むメインインターフェイスが表示されています。

歯車のアイコン	説明
PC セキュリティ	カスタムスキャン、シールド設定の変更、隔離の管理を実行で きます。
ID とプライバシー	オンライントランザクション中に脅威にさらされる可能性のある重 要なデータを保護します。
ユーティリティ	ツールを使用して、プロセスとファイルの管理、レポートの表示、 ウェブルートサポートへのファイルの提供を実行できます。また、シ ステム最適化ツールを使用して、インターネットブラウザのアクティ ビティやー 時ファイルを削除できます。
マイアカウント	SecureAnywhere のアカウント情報を表示したり、アップデートを チェックしたりできます。
サポート / コミュニティ	カスタマーサポートおよびウェブルートコミュニティにアクセスできま す。

## Mac コンピュータで SecureAnywhere を開く

### Mac コンピュータで SecureAnywhere のメインインターフェイスを開くには

- 1. エンドポイントで次のいずれかの操作を行います。
  - メインウィンドウを表示するには、メニューバーにある **ウェブルート**のアイコンをクリックします。
  - ドロップダウンメニューで [Webroot SecureAnywhere を開く] を選択します。



システムが安全な場合、次のようなメインウィンドウが表示されます。



ウェブルートのインターフェイスでは、コンピュータの保護の状態を反映して、次のように表示の色を使い分けます。

- 緑 Mac は安全です。
- 黄 1 つあるいは複数の潜在的なリスクへの対応が必要です。
- 赤 1 つまたは複数の重要なアイテムについてユーザーが対応する必要があります。

## Mac の [Webroot SecureAnywhere] メニュー

Secure Anywhere のインターフェイスがアクティブな場合、メニューバーには Secure Anywhere に関するオプションが表示されます。

Ś	Webroot SecureAnywhere	System Too	ols Window	v Help
	About SecureAnywhere			
	Preferences	ж,		
	My SecureAnywhere Accou Check for Updates	nt		
	Hide Webroot SecureAnywh	nere ೫H		

Mac の Webroot Secure Anywhere ドロップダウンメニュー項目の詳細については、以下の表を参照して ください。

オプション	説明
SecureAnywhere について	SecureAnywhere のバージョン番号を表示します。
設定	システム設定、スキャンのスケジュール、その他の設定を変更す ることができます。
My SecureAnywhere アカウント	キーコードおよびその他のアカウント詳細を表示します。
アップデート情報を確認する	最新のプログラムアップデートをダウンロードおよび適用します。
Webroot SecureAnywhere を 非表示にする	メインウィンドウが表示されなくなりますが、SecureAnywhereの保 護はシャットダウンされません。保護をシャットダウンする場合は、 メニューバーにあるウェブルートのアイコンをクリックし、 [SecureAnywhere をシャットダウン]を選択してください。

## Mac の [システムツール] ドロップダウンメニュー

Macの[システムツール]ドロップダウンメニュー項目の詳細については、以下の表を参照してください。

項目	説明
システム制御	Mac で実行中のすべてのプログラムとプロセスに対する脅威検出の設 定を調整できます。
レポート	スキャンログを保存できます。スキャンログは、問題の原因特定のため にウェブルートサポートに問い合わせをする際に役立つ場合がありま す。
ファイルの提供	ファイルを分析のためにウェブルートに送信できます。ファイルが問題を 起こしていると考えられる場合や、ファイルが安全と分かっていてそれを 再分類する必要がある場合に、ファイルを送信できます。
システムアナライザ	脅威、セキュリティ上の脆弱性、その他のコンピュータの問題を検出す るシンプルなユーティリティです。 完了後のレポートでは、システムパ フォーマンス、プライバシー、保護を強化するための推奨事項が提案 されます。
### スキャンの結果確認と脅威の管理

[グループの管理] で、エンドポイントのスキャン履歴を表示し、検出された脅威を管理できます。ファイルが正当なものだとわかっている場合は、隔離されたファイルを復元できます。詳細については、「ファイルの隔離からの復元」を参照してください。

また、ファイルを [正当] (実行を許可)、または [不正] (自動隔離) に再分類することもできます。詳細については、「ファイルのオーバーライドの設定」を参照してください。

### スキャン履歴の表示

[グループの管理] パネルでエンドポイントのスキャン履歴を表示することができます。これは、脅威が見つかった場所を確認する際に役立ちます。

#### スキャン履歴を表示するには

- 1. [**グループの管理**] タブをクリックします。
- 2. 左側の[グループ]パネルで、必要なエンドポイントを含むグループを選択します。

Home Endpoint P	rotection	Mobile	Protecti	on						
Status Policies Group Management Reports Alerts Overrides Logs Resources										
Groups Views		**	📑 All E	ndpoints						
🔂 Create   🖨 Delete   🖞	Rename		Save	Changes   5	<b>b</b> Un	ido Changes	🌄 Move	endpoints to another	group   📃 Apply policy	to endpoints   🛒 Age
Group Name	No.			Hostname		Policy	Group	Status	First Seen	Last Seen
All Endpoints	16		1	DAL-TS		Recomm	Remot	📀 Not Seen Re	Aug 19th 2011, 13:24	Jun 27th 2013, 00
Deactivated Endpoints	19		2	FHAL-3		No Rem	Broom	Infected	Jul 12th 2013, 19:41	Aug 23rd 2013, 14
Default Group	8		3	VMXP3		Unmana	Remot	🐠 Not Seen Re	Apr 11th 2013, 18:54	Jun 20th 2013, 17
			4	] W7VM		Unmana	Defaul	Protected	Mar 9th 2012, 17:50	Aug 15th 2013, 2
			5	WEBRO		Unmana	Defaul	📀 Not Seen Re	Aug 5th 2013, 16:13	Aug 14th 2013, 10

3. 右側の[エンドポイント]パネルで、いずれかのエンドポイントを選択します。

<b>N</b>	II Er	ndpoints								
<b>S</b>	ave	Changes   🖕 U	ndo Ch	anges	Nove endpo	pints to another group	属 Apply	y policy to endpoints 🛛 👫	Agent Cor	mmands •
		Hostname	P	Gro	Status	Last Seen		Last Infected	Agen	Keycode
37		G-ALERTN	G	G	Infected	Apr 8th 2013	11:41	Apr 7th 2013, 18:16	8.0.2	SA23-TE
38		G-RR-VOLGA	G	G	Infected	Feb 1st 2013	, 14:33	Jan 31st 2013, 16:55	8.0.2	SAA2-TE
39		GHULL-1365	R	G	Protected	Apr 16th 201	3, 20:25	Oct 2nd 2012, 14:06	8.0.2	SA23-TE
40		GHULL-1366	R	G	Protected	Apr 22nd 201	3, 10:01	Apr 5th 2013, 14:11	8.0.2	SAA2-TE
	⊲ ican	Page 1 of 2 history for GHUI	2   ▶ LL-136 this er	PI i 6D-SMT adpoint	2					
	Sc	an Start	Stat	us		Scan Type		Windows Full OS		
18	Ap	r 6th 2013, 14:19	0	lean		Deep Scan		Windows 7 Service Pack	1 (Build 76	501) 64bit
19	Ар	r 5th 2013, 14:13	0	lean		Post Cleanup Scan		Windows 7 Service Pack	1 (Build 76	601) 64bit
20	Ар	r 5th 2013, 14:10	01	'hreats d	etected - View	Deep Scan	)	Windows 7 Service Pack	1 (Build 76	601) 64bit
21	1.10	68.2010.10.21	-0-			Custom / Right Olick	Scan	Windows 7 Service Pack	1 (Build 76	601) 64bit

[スキャン履歴] パネルが表示され、エンドポイントにおけるスキャンアクティビティと検出された脅威が提示されます。

**注意:** 脅威が検出された場所のパス名にドライブを示す文字が含まれている場合、この文字は "?" マークに置換されます。たとえば、?:\users\user1\desktop のようなパス名が表示される場合があります。

<b>N</b>	ll Er	ndpoints									
n s	ave (	Changes 🛛 🚖 Ur	ndo Ch	anges	Move endpo	ints to ar	other group	📕 Apply	policy to endpoints   🛒	Agent Con	nmands •
		Hostname	P	Gro	Status		Last Seen		Last Infected	Agen	Keycode
37		G-ALERTN	G	G	Infected		Apr 8th 2013, 1	11:41	Apr 7th 2013, 18:16	8.0.2	SA23-TE.
38		G-RR-VOLGA	G	G	Infected		Feb 1st 2013,	14:33	Jan 31st 2013, 16:55	8.0.2	SAA2-TE
39		GHULL-1365	R	G	Protected		Apr 16th 2013,	20:25	Oct 2nd 2012, 14:06	8.0.2	SA23-TE.
40	☑	GHULL-1366	R	G	Protected		Apr 22nd 2013	, 10:01	Apr 5th 2013, 14:11	8.0.2	SAA2-TE
	Image     1 of 2     Image     Image       Image     Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image     Image       Image										
	Sc	an Start	State	us		Scan T	уре		Windows Full OS		
18	Ap	r 6th 2013, 14:19	0	lean		Deep S	can		Windows 7 Service Pack	1 (Build 76	01) 64bit
19	Ар	r 5th 2013, 14:13	Ø 0	lean		Post CI	eanup Scan		Windows 7 Service Pack	1 (Build 76	01) 64bit
20	Ар	r 5th 2013, 14:10	<b>0</b> T	'hreats d	letected - View	Deep S	can		Windows 7 Service Pack	1 (Build 76	01) 64bit
		68. 2010 10.21	-0-	-		0	I Diale Diale St	can	Windows 7 Service Pack	1 (Build 76	01) 64bit

必要に応じて、エンドポイントとスキャン履歴に関する追加データを表示または非表示にできます。カラム見出しをクリックしてドロップダウンメニューを開き、追加または削除するカラムのチェックボックスを選択します。カラム内のデータの詳細については、「<u>表とレポートのデータの並べ替えページ45</u>」を参照してください。

#### ファイルの隔離からの復元

[スキャン履歴] パネルで、ファイルを隔離から復元できます。ファイルはエンドポイントの元の場所に自動的に 戻ります。

また、[確認されたすべての脅威] レポートからファイルを復元することもできます。詳細については、「<u>(確認されたすべての脅威) レポートの生成 ページ342</u>」を参照してください。

#### ファイルを復元するには

- 1. このセクションの前述の説明に従って、特定のエンドポイントのスキャン履歴を表示します。
- 2. [スキャン履歴] パネルで、次のいずれかを実行して該当するファイルを探します。
  - [状態] カラムで [表示]をクリックして、脅威が検出された日付を確認する
  - [このエンドポイントで確認されたすべての脅威を表示] ボタンをクリックする

ウェブルートエンドポイントプロテクション管理者ガイド

	Scan history for G-RR-VOLGA									
		Scan Start	Status	Scan Type 👻	Windows Full OS					
	1	Jan 31st 2013, 16:	. 🕕 Threats detected - View	Full Scan	Windows XP Professional					
	2	Jan 31st 2013, 16:	. 🥝 Clean	Full Scan	Windows XP Professional					
1	3	Jan 31st 2013, 16:	. 🕖 Threats detected View	Deep Scan	Windows XP Professional					
	4	Jan 31st 2013, 16:	. 🕕 Threats detected - View	Deep Scan	Windows XP Professional					
			•							

- 3. 表示されるダイアログで、チェックボックスを選択してファイルを選択します。
- 4. [隔離先から復元する] ボタンをクリックします。



ファイルがエンドポイントの元の場所に戻されます。

### ファイルのオーバーライドの設定

[スキャン履歴] パネルで、ファイルのオーバーライドを設定できます。また、[オーバーライド] タブでオーバーライ ドを設定することもできます。詳細については、「<u>/オーバーライド] タブからのオーバーライドの適用 ページ439</u>」 を参照してください。

#### ファイルのオーバーライドを設定するには

- 1. このセクションの前述の説明に従って、特定のエンドポイントのスキャン履歴を表示します。
- 2. [スキャン履歴] パネルで、次のいずれかを実行して該当するファイルを探します。
  - [状態] カラムで [表示]をクリックして、脅威が検出された日付を確認する
  - [このエンドポイントで確認されたすべての脅威を表示] ボタンをクリックする

0	Scan history for G-RR-VOLGA									
		Scan Start	Status	Scan Type 👻	Windows Full OS					
	1	Jan 31st 2013, 16:	Threats detected - View	Full Scan	Windows XP Professional					
	2	Jan 31st 2013, 16:	🥝 Clean	Full Scan	Windows XP Professional					
1	3	Jan 31st 2013, 16:	Threats detected View	Deep Scan	Windows XP Professional					
	4	Jan 31st 2013, 16:	Threats detected - View	Deep Scan	Windows XP Professional					

- 3. 表示されるダイアログで、リストからファイルを選択します。
- 4. [**オーバーライドの作成**] ボタンをクリックします。

-	All thre	eats ever seen on this endpoint			
C	Create	override	ntine		
		Filename	Pathname	Malware Group	Last Seen
		NDNUNINSTALL6_38.EXE	%windir%\	Pua.Gen	Jan 31st 2013, 16:55
	2	LINKPAL[1].EXE	?:\documents and settings\owe	W32.Trojan.Downloader-LowZ	Jan 31st 2013, 16:55
	3 📄	MNMYBOH.EXE	?:\documents and settings\owe	Adware.W-find.com.Hijacker	Jan 31st 2013, 16:55
	4 📃	45765FBEB88468B9A7AD0E0	?:\documents and settings\owe	W32.Trojan.Trojan-iejore	Jan 31st 2013, 16:55

[オーバーライドの作成] ウィンドウが表示されます。

Determination.			~
Apply this overrid	e globally?:		

- 5. [判定]ドロップダウンメニューで、次のいずれかを選択します。
  - 正当 ファイルの実行を常に許可します。
  - 不正 常にファイルを隔離します。
- 6. 次の手順に従って、このオーバーライドをポリシー全体または個々のポリシーに適用できます。
  - すべてのポリシーにオーバーライドを適用するには、[オーバーライドをグローバルに適用] チェックボック スを選択します。

• オーバーライドの対象となるポリシーを個別に選択するには、[オーバーライドをグローバルに適用] チェックボックスの選択を解除します。[ポリシー] フィールドが表示されたら、ドロップダウンメニューでポ リシーを選択します。

# アップデートのダウンロードと強制実行

ウェブルートソフトウェアの過去のバージョンとは異なり、Webroot SecureAnywhere はデフォルトですべてのアッ プデートを自動的にダウンロードおよびインストールします。バージョンのアップデートは、リリース時に全世界の ユーザーベース全体で負荷が分散されるため、すべてのエンドポイントに適用されるまで最大 72 時間かかる 場合があります。

スキャンを実行するたびにお使いのウェブルートソフトウェアがクラウドと通信し、新しい判定やアップデートがあれば、それをダウンロードしてマシンに適用します。SecureAnywhere はアップデートがリリースされるとすぐに対応するため、コンピュータがインターネットに接続されている限り、常に最新の保護状態が維持されます。

**注意:**詳細については、「<u>エンドポイントへのコマンドの発行 ページ144</u>」の「高度なコマンド」の表を参照してください。

#### アップデートをダウンロードして強制適用するには

1. <u>エンドポイントプロテクション</u>にログインします。



2. [**グループの管理**] タブをクリックします。

Seci	ure Anywhere	0		1
Home	Endpoint Protection	Support		
Status	Policies Group Managem	ent	ts Overrides Alerts Settings Logs Resources	
🛄 Status		« 县	Endpoints encountering threats (last 7 days)	

3. 左側の[グループ] パネルで[**すべてのエンドポイント**]を選択し、右側のペインで1つ以上のエンドポイントを選択します。

Secure Any	where								
Home Endpoint Pro	tection Supp	ort							
Status Policies Group	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources								
Groups Views Search	1 🔍 Ø	📕 All E	Endpoints						
😌 Create   🛐 Actions 🝷		Save	e Changes 🛛 뉠 Undo Changes 🗍	Move endpoints to another gr	oup Apply policy to endpoints	🛒 Agent Commands 🔻			
Group Name	No.		Hostname	Policy	Group	Status			
All Endpoints	12	1 🔽	AB-WIN10-DEMO	Unmanaged	Default Group	Protected			
Deactivated Endpoints	10	2	BCOFF3571LBRM		Mac OS X Systems				
Default Group	7	3 📃	🛛 🙀 Webroot Sydney Mac		Mac OS X Systems				

メニューバーに [エージェント コマンド] ボタンが表示されます。

Secure Any	where.							
Home Endpoint Pro	otection Supp	ort						
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources								
Groups Views Searc	h < 🕫	📕 All Endp	oints		_			
🔂 Create 🕴 🛐 Actions 🝷		Rave Cha	anges 🛛 🔄 Undo Changes	Bove endpoints to another group	Apply policy to endpoints	Agent Commands		
Group Name	No.		Hostname	Policy	Group	Status		
All Endpoints	12	1 🔽 📕	AB-WIN10-DEMO	Unmanaged	Default Group	Protected		
Deactivated Endpoints	10	2 📃 🌿	BCOFF3571LBRM		Mac OS X Systems			
Default Group	7	3 🔳 🌿	Webroot Sydney Mac		Mac OS X Systems			

 [エージェントコマンド]ドロップダウンメニューで、[詳細] >3 [カスタマーサポートスクリプトを実行] を選択 します。

<b>F</b> A	gent Commands 🗸 📄 😑 Deactivate		
	Agent	₽	
2	Clear Data	₽	Seen Recently
-	Keycode	₽	ds Attention
-	Power & User Access	₽	Seen Recently
	Antimalware Tools	₽	
01	Files & Processes	₽	
	Identity Shield	₽	
0	Advanced	Þ	💱 Run Customer Support script
	View commands for selected endpoints		Customer Support Diagnostics

5. [URL] フィールド に次の URL を入力します。:

http://anywhere.webrootcloudav.com/zerol/wsasme.exe

Run Customer Support script	×
Specify a URL to download an executable file to the agent and run it remotely	
URL:	
Command Line Options (optional):	
Download and Execute Cancel	

**注意:** この URL を使用して、インストーラーをエンドポイントにローカルでダウンロードし、手動で実行することも可能です。

6. ダウンロードのウィザードに従って最新のアップデートをインストールします。

### 即時のアップデートの強制実行

ポーリング間隔によって、エンドポイントがその状態を送信しコマンドを受信する頻度 (15 分毎、1 時間毎な ど)が決まります。必要に応じて、グループのポリシーの [基本設定] でポーリング間隔を変更したり、以下の 手順に従って即時のアップデートを強制実行したりできます。

詳細については、「ポリシー設定の変更ページ247」を参照してください。

#### アップデートを強制するには

- 1. エンドポイントで、システムトレイにあるウェブルートのアイコンを右クリックします。
- 2. 表示されるドロップダウンメニューで [設定のリフレッシュ]を選択します。

	Scan Now
	Open
	About
4	Refresh configuration
	Save a Scan Log
W)TX	🛛 🛪 🚺 🥯 👘 🗱 🖂 💌

システムがアップデートされます。

# Web 脅威シールド Chrome ブラウザエクステンションのインストール

ウェブルートではブラウザエクステンションの配備に関して、Google と Chromium プロジェクトのベストプラクティス を採用しています。そのため、ウェブルートがエンドユーザーに通知することなくブラウザエクステンションを配備 することはできません。管理された環境での Chrome ブラウザエクステンションのサイレントモードのインストール を希望する場合は、以下の手順に従って強制インストールを実行できます。

管理された環境での Webroot SecureAnywhere の強化 Web 脅威シールド (EWTS) 向け Chrome ブラウザエ クステンションの強制インストールは簡単です。 強制インストールではユーザーにエクステンションのアクティブ化 や承諾を促さず、 ユーザーによる無効化も回避されます。

非強制の環境では、Chromeのエクステンションを有効化するように促す、次の図のようなプロンプトが表示されます。



非強制のエクステンションは、chrome://extensions/を介してユーザーが有効化、無効化、削除を実行できるようになっています。次の図を参照してください。

	Webroot Filtering Extension 1.2.0.64	1	Enabled	Î
V	Keeps you safe when browsing the web by identifying and blocking dangerous websites.			
	Details			
	Allow in incognito Allow access to file URLs			

管理された環境でサイレントモードにより配備した Chrome エクステンションは、次の図のように表示されます。 この場合、ユーザー側で無効化や削除を行うことはできず、管理者が行います。ユーザーに対してエクステン ションの有効化を促すプロンプトは表示されません。

W	Webroot Filtering Extension 1.2.0.64 Keeps you safe when browsing the web by identifying and blocking dangerous we Details	Enabled Enables.	
	Allow in incognito Allow access to file URLs		

### Active Directory グループポリシーの使用

Google は Windows Server 2003 (ADM テンプレート) と Windows Server 2008+ (ADMX テンプレート) の管理 用テンプレートを提供しており、これをインポートすることでグループポリシー向けの Chrome 固有のポリシーを 使用できるようになります。

次の Google のリンクから該当する管理用テンプレートをダウンロードしてください。

Google Chrome テンプレート / ドキュメントの Zip ファイル

Active Directory グループポリシーを介して Chrome ブラウザエクステンションの強制 インストールを行うには

1. [グループポリシー管理] コンソールを開きます。ドメインを右クリックし、[**このドメインに GPO を作成し、** ここでリンクする] を選択します。



2. 新しい GPO に名前を付けます。ここでは仮に "Chrome Enforced Policy" とします。

- Linked Group Policy Objects Group Policy Inheritance Delegation Status Link Order GPO Enforced Link En 숲 S Default Domain Policy No 1 Yes Chrome Enformed P Vas Edit Enforced  $\nabla$ Link Enabled √ ¥ Save Report... Delete Rename Refresh
- 3. 新しい GPO を右クリックし、[編集] を選択します。以下のようなウィンドウが開きます。

- 4. [コンピュータの設定]を展開します。
- 5. [管理用テンプレート]を右クリックします。

6. [テンプレートの追加 / 削除]をクリックします。

- 7. [追加]をクリックします。
- 8. Google Chrome テンプレートアーカイブにあるダウンロード済みの ADM ファイルまたは ADMX ファイルを 指定します。

J		Group Policy Management Editor			Ŀ	-   -	x
File Action View Help							
🗢 🔿 🙍 🖬 🗟 🖬 👌	7						
Chrome Enforced Policy [LINZ1 Computer Configuration Policies Software Settings	Administrative Temp Select an item to view its descrip	lates: Policy definitions (ADMX files) ret tion. Setting Control Panel	rieved from the loo	cal computer. State	Comn	nent	
Windows Settings	<u></u>	Policy	Templates				x
⊿ Administrative Temp		BC - Developedo - político terrolateo - político	laura di adres di ara U	с	C		
Network	😌 😌 🕈 T 🌆 🖡 The	PC Downloads policy_templates wind	lows ▶ adm ▶ en-U	s v 0	Search en-US		p
Printers	Organize 🔻 New folder						- 🔲 🔞
Server	🕹 Enumitar	Name	Date modified	Туре	Size		
b System		D abromo adm	11/20/2016 4-24 DM	ADM Eile	50.4 KP		
Windows Compc	Downloads		11/30/2010 4:24 PIVI	ADM FILE	J04 KD		
Real All Settings	Recent places						
Preferences	100 C						
Solution     Solution	🛤 This PC						
Preferences	Pesktop						
	Documents						
	Downloads						
	🚺 Music						
	📔 Pictures						
	📔 Videos						
	🊢 Local Disk (C:)						
	🖆 DVD Drive (D:) IRM_!						
	👊 Network						
	File par	ne: chrome adm			Policy Temp	atec	
	File har	enome.aum			- Foncy remp		
					Open		Cancel

9. [開く]をクリックしてから [閉じる] をクリックします。

管理用テンプレートの中にGoogleのフォルダが追加されていることを確認します。

10. 管理用テンプレート内の Google Chrome Extensions を展開します。



- 11. [強制インストールエクステンションのリスト設定]をクリックします。
- 12. [有効化]をクリックします。
- 13. [表示]をクリックします。
- 14. インストールがサイレントモードで行われるようにするため、[エクステンション / アプリ ID] のリストに下のテキストを入力して URL をアップデートします。

kjeghcllfecehndceplomkocgfbklffd;https://clients2.google.com/service/ update2/crx



15. すべてのダイアログ / ボタンを確認します。

これで、ウェブルートの Chrome EWTS エクステンションが、このポリシーが適用されるすべてのドメインコンピュータにインストールされます。

### Google スイートを利用した単一カスタムアプリの強制インストール

Google スイートで管理された環境であれば、EWTS 向け Chrome エクステンションの強制インストールを実行 できます。エクステンションとアプリケーションの一般的なインストール手順については、Google ヘルプを参照し てください。

EWTS 向け Chrome エクステンションをインストールするには、以下の手順に従ってカスタムアプリを追加する必要があります。.

#### Chrome エクステンションをインストールするには

- 1. Google管理コンソールにサインインします。
- 2. 管理コンソールのダッシュボードにある[デバイス管理]をクリックします。
- 3. 左側の[Chrome 管理] をクリックします。
- 4. [**アプリ管理**]をクリックします。
- 5. 右側にある3つの点をクリックしてオーバーフローメニューを開きます。

<del>.</del> ? :
Setup
Add custom app
Remove app(s)
Manage Apps in User Settings

6. [カスタムアプリの追加]を選択します。

#### 7. カスタムアプリのダイアログで次の ID を入力します。

kjeghcllfecehndceplomkocgfbklffd

#### 8. 以下を入力します。

URL:https://clients2.google.com/service/update2/crx

これは、ウェブルートの Filtering Extension 用です。

9. [追加]をクリックします。



10. アプリ管理の画面で、新しく追加されたエクステンションの ID を選択します。

$\equiv$ Device management > Chrom	ne > App Management
Filters	Apps
Type My Configured Chrome Apps	kjeghcllfecehndceplomkocgfbklffd
Find or Update Apps	

11. アプリのオプションで [ユーザー設定]を選択します。

	kjeghcllfecehndceplo https://clients2.google.com/service/update2/crx
User settings Configure this app f	or users that log in with an account in your domain.
Public session se Configure this app f	ettings or users that log in to a public session on your devices.
Kiosk settings Deploy this app as a	a Kiosk App

12. EWTS 向け Chrome エクステンションをインストールする Org を選択し、[インストール許可] と[強制イン ストール] をオンにします。

∧ User sett	ings		
	Orgs	Settings for	j.com
		Allow installation	Force installation
		Setting inherited Override	
		Pin to taskbar	Configure
		$\bigcirc$	UPLOAD CONFIGURATION FILE
		SAVE	CANCEL

13. [保存]をクリックします。

ここで選択した Org の認証情報を使用して Chrome にログインしているユーザーは、使用している Chrome ブラウザでウェブルートフィルタリングエクステンションが適用されます。 Org の構成 やアプリケー ション管理の詳細オプションについては、 Google の G Suite ドキュメントを参照してください。

**注意:** ウェブルートは現在、Chromebooks での Webroot SecureAnywhere の使用をサポートしていません。これらのデバイスを使用する場合は、トラブルを回避するために G Suite のポリシー制御を使用してください。詳細については、G Suite ヘルプドキュメントを参照してください。

### レジストリの使用

WTS 向け Chrome エクステンションのサイレントモードでのインストールに Active Directory や Google Suite を 使用することが適切でない場合は、Windows レジストリで代用できることもあります。ただし、コンピュータが Microsoft Windows ドメインの一部であることが条件となります。

**注意:** この方法は、Active Directory グループポリシーや G Suite で管理された環境に対応していない 場合があります。

Chrome に使用できるポリシー設定の詳細については、以下のリンクを参照してください。

http://dev.chromium.org/administrators/policy-list-3#ExtensionInstallForcelist

#### Windows レジストリエディター (regedit.exe)の使用

1. 以下のレジストリキーが存在するかどうかを確認します。

```
[HKEY_LOCAL_
MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist]
```

このキーが存在する場合、他の管理アプリケーション(特に強制インストールしたエクステンション)が Chrome ポリシーを強制適用している可能性があります。この場合、以下の手順に進むと競合が発生 することがあります。

2. 次のレジストリ値を追加します。

Windows レジストリエディター バージョン 5.00

```
[HKEY_LOCAL_
MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist]"1"
="kjeghcllfecehndceplomkocgfbklffd;https://clients2.google.com/servic
e/update2/crx"
```

エクステンションを追加登録する場合は、番号が連続するようにしてください。

# エンドポイントでのコマンドの実行

Windows の PC、ノートパソコン、サーバー、またはネットワークにインストールされている仮想サーバーをエンドポイントとして使用できます。コマンドをエンドポイントでローカル実行するには、次の手順に従ってください。

#### エンドポイントでコマンドを実行するには

1. [スタート] メニューをクリックします。

Å	Adobe Acrobat X Pro	•
Ŷ	Oracle VM VirtualBox	
8	Calculator	
P	PowerPoint 2013	•
	Microsoft Mouse and Keyboard Center	
Ζz	7-Zip File Manager	
<b>0</b> ⊻	Outlook 2013	•
•	All Programs	
Sea	arch programs and files	ρ

2. [プログラムとファイルを検索]欄に「CMD」と入力します。

[コマンド] ウィンド ウが表示されます。

C4.	Command Prompt	-	
Microsoft Windows (c) 2012 Microsoft	[Version 6.2.9200] t Corporation. All rights reserved.		^
C:\Users\Christina	a>		
			~

3. コマンドラインに次のコマンドのいずれかを入力します。



コマンド	説明	
-poll	コマンドラインオプションでポーリングを行います。 例: "c:\program files\webroot\wrsa.exe" -poll これによりポーリングを必要に応じて実行でき、SME のお客様は、現在使用してい るソフトウェア実行手段 (例: psexec) でポーリングを強制的に実行できるようになり ます。ソフトウェアのアップデート、設定のアップデート、エージェントコマンドのアップ デート、ライセンスの確認を同時に行うことができます。	
-showgui	ポリシーで許可されていれば、UI が起動し表示されます。 例: "c:\program files\webroot\wrsa.exe" -showgui	
-silentscan	サイレントモードでスキャンを開始します。スキャン用 UI はユーザーには表示されま せんが、トレイアイコンにカーソルを合わせると表示されます。コマンドの例: WRSA.exe -silentscan="c:\foldername" フォルダをスキャンする実行コマンドの例: "C:\Program Files\Webroot\WRSA.exe" -silentscan="c:\Documents and Settings\Administrator\Desktop" ファイルをスキャンする実行コマンドの例: "C:\Program Files\Webroot\WRSA.exe" -silentscan="c:\Documents and Settings\Administrator\Desktop\eicar.com" 注意:コマンドは 8.0.1.196 以降のビルドでのみ利用可能です。	

コマンド	説明
-scan	特定のロケーションのスキャンを開始し、開始後にスキャン進捗状況のUIをユー ザーに表示します。 形式:WRSA.exe -scan="c:\foldername" フォルダをスキャンする実行コマンドの例: "C:\Program Files\Webroot\WRSA.exe" -scan="c:\Documents and Settings\Administrator\Desktop" ファイルをスキャンする実行コマンドの例: "C:\Program Files\Webroot\WRSA.exe" -scan="c:\Documents and Settings\Administrator\Desktop\eicar.com" 注意:コマンドは 8.0.1.196 以降のビルドでのみ利用可能です。
-uninstall	製品がインストールされている場合、アンインストールします。WRSA.exe でも実行 できます。 アンインストールはサイレントモードでは実行されません。エンドポイントが非管理の 場合のみ有効です。エンドポイントが管理されている場合、コマンドは Windows の [セーフモードとネットワーク] でのみ動作します。実際にネットワークに接続されてい る必要はありません。 例: wsasme.exe -uninstall "c:\program files\webroot\wrsa.exe" -uninstall

4. 終了したら、[コマンド] ウィンドウ右上の赤い X マークをクリックしてウィンドウを閉じます。

# エンドポイントの非アクティブ化

エンドポイントを非アクティブ化して、エンドポイントプロテクションに報告を行わないようにすることができます。 必要に応じて、後からエンドポイントを再アクティブ化することができます。エンドポイントを非アクティブ化することにより、ライセンスシートを解放して別のエンドポイントをインストールすることができます。

**注意:**管理ポータルでエンドポイントを非アクティブ化せずに、エンドポイントにアンインストールコマンド を送信することもできます。この場合、管理ポータルにエンドポイントのエントリが維持されます。ただ し、7日が経過すると[未確認]と表示されます。詳細については、「<u>エンドポイントへのコマンドの発行</u> ページ144」を参照してください。

このトピックでは、次の手順について説明します。

- <u>エンドポイントの非アクティブ化</u>
- エンドポイントでの Secure Anywhere の再アクティブ化

### エンドポイントの非アクティブ化

非アクティブ化するとエンドポイントにアンインストールコマンドが送信され、管理ポータルからエンドポイントのエントリが削除されます。

#### エンドポイントを非アクティブ化するには

- 1. [グループの管理] タブをクリックします。
- 2. 左側の[グループ]パネルで、必要なエンドポイントを含むグループを選択します。

Home Endpoint F	Protection	Mobile	Prote	ctio	1						
Status Policies Gr	oup Manage	ment	Reports	3	Alerts (	Overri	ides Logs	Resou	rces		
Groups Views		* \$	P A	ll En	dpoints						
🔂 Create   🤤 Delete   📺 Rename 🔚 Save Changes   🔄 Undo Changes   🌄 Move endpoints to another group   🔜 Apply policy to endpoints   📢 Age											
Group Name	No.				Hostname		Policy	Group	Status	First Seen	Last Seen
All Endpoints	16		1		DAL-TS		Recomm	Remot	🐠 Not Seen Re	Aug 19th 2011, 13:24	Jun 27th 2013, 00
Deactivated Endpoints	19		2		FHAL-3		No Rem	Broom	🕕 Infected	Jul 12th 2013, 19:41	Aug 23rd 2013, 14
Default Group	8		3		VMXP3		Unmana	Remot	🐠 Not Seen Re	Apr 11th 2013, 18:54	Jun 20th 2013, 17
	_		4		W7VM		Unmana	Defaul	Protected	Mar 9th 2012, 17:50	Aug 15th 2013, 21
			5		WEBRO		Unmana	Defaul	Not Seen Re	Aug 5th 2013, 16:13	Aug 14th 2013, 16

3. コマンドバーで1つまたは複数のエンドポイントを選択して、「非アクティブ化」ボタンをクリックします。

Reports Alerts Overrides Logs Resources								
📑 End	🗐 Endpoints in Default Group							
🔚 Save Changes   🔄 Undo Changes   易 Move endpoints to another group   🖺 Apply policy to endpoints   📢 Agent Commands 🔹 🤤 Deactivate)								
	Hostname	Policy	Status	Last Seen	Last Infected	Agen	Keycode	VM 🔺
35 🕅	SME-M-NE	Recommend	\pm Not Seen Rece	Jan 31st 2013, 14:18		8.0.2	SAA2-TEST-E	Yes
38 🔽	SME-M-SA	Recommend	🚯 Not Seen Rece	Feb 4th 2013, 16:02	Feb 1st 2013, 15:23	8.0.2	SAA2-TEST-E	Yes

非アクティブ化したエンドポイントはエンドポイントプロテクション対して報告を行えなくなることを示す警告メッセージが表示されます。

4. [**はい**] をクリックするとエンドポイントにアンインストールコマンドが送信され、SecureAnywhere が削除されます。

SecureAnywhere が削除されると、エンドポイントは [非アクティブ化されたエンドポイント] グループに表示されます。7日間が経過すると、状態が [最近確認されていません] に変わります。

**注意:** [非アクティブ化されたエンドポイント] グループから自分でエンドポイントを完全に削除することはできません。このリストをクリーンアップして古いアイテムを削除する場合は、ウェブルートテクニカルサポートまでご連絡ください。

### エンドポイントでの SecureAnywhere の再アクティブ化

[グループの管理] タブでエンドポイントを非アクティブ化する場合は、必要に応じて後から再アクティブ化することができます。

#### エンドポイントを再アクティブ化するには

- 1. エンドポイントに Secure Anywhere を再インストールします。
- 2. 管理ポータルを開き、[グループの管理]タブをクリックします。
- 3. [非アクティブ化されたエンドポイント] グループで目的のエンドポイントを選択します。

4. コマンドバーの[**再アクティブ化**] ボタンをクリックします。

Status Policies Group	Management	Reports Alerts Overrides	Logs Resou				
Groups Views 🔍 🥏 Endpoints in Deactivated Endpoints							
🕀 Create   😑 Delete   🏥 R	lename	🔂 Reactivate					
Group Name	No.	Hostname	Status Firs				
All Endpoints	16	1 32WIN7EP-0970E	💾 🐠 N 🛛 Jun				
Deactivated Endpoints	19	2 🔲 ANGELAWIN7VM	📒 한 N Mar				
Default Group	8	3 🔲 BROW-2308-WIN8	<table-cell-rows> 한 N Oct</table-cell-rows>				

エンドポイントが以前のグループに戻されます。

# SecureAnywhere のアンインストール

以下のいずれかの方法で、エンドポイントから SecureAnywhere プログラムを削除することができます。

 エンドポイントを非アクティブ化し、エンドポイントプロテクションに報告しないようにします。必要に応じて、 後からエンドポイントを再アクティブ化することができます。

エンドポイントを非アクティブ化することにより、ライセンスシートを解放して別のエンドポイントをインストール することができます。詳細については、「エンドポイントの非アクティブ化ページ199」を参照してください。

管理ポータルからアンインストールコマンドをエンドポイントに送信します。この方法では、エンドポイントは管理ポータルに表示されたままになります。

SecureAnywhere をアンインストールしてライセンスのシートを解放するには、エンドポイントを非アクティブ化します。詳細については、「エンドポイントへのコマンドの発行ページ144」を参照してください。

# 第5章:状態の確認

状態を確認する方法については、以下のトピックを参照してください。

エンドポイントの状態の表示	
脅威の最新状況の表示	
エージェントのバージョンの概要表示	
滞留時間について	
エンドポイントプロテクションからの CSV ファイルのエクスポート	

ウェブルートエンドポイントプロテクション管理者ガイド

## エンドポイントの状態の表示

管理ポータルですべてのエンドポイントの状態を確認できます。SecureAnywhere によるスキャン時、または ポーリング間隔の終了時に、エンドポイントから状態が報告されます。

**注意:** エンドポイントのスキャン履歴の詳細については、「<u>スキャンの結果確認と脅威の管理ページ</u> <u>171</u>」を参照してください。

#### エンドポイントの状態を表示するには

- 1. <u>SecureAnywhere の Web サイト</u>にログインします。
- 2. [エンドポイントプロテクションに進む] ボタンをクリックします。

Secure Anywhere.						
Home	Endpoint Protection	Mobile Protection				
Endpo	bint Protection 13 Endpoints 1 Endpoint II Go to End	s Protected Currently Infected Infected (last 24 hours)				

3. 感染しているエンドポイントがある場合、そのエンドポイントへのリンクをクリックして詳細パネルに直接進むことができます。

Secure Anywhere.						
Home	Endpoint Protection Mobile Protection					
Endpo	Dint Protection 13 Endpoints 1 Endpoint C 1 Endpoint In Go to End	s Protected Currently Infected Infected (last 24 hours)				

4. 管理ポータルが表示されたら、左側の[状態]パネルと[エンドポイントのアクティビティ]パネルでエンドポ イントの状態を確認します。

Secure Anywhere.		
Home Endpoint Protection Mobile	e Protection	
Status Policies Group Management R	eports Alerts Overrides	Logs Resources
🛄 Status 🔍	Endpoints encountering three	ats (last 7 days)
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.		1 Hori H
	16 ¹⁰ 1 ¹⁰	28°. 28°.
	So most recent endpoints en	Countering threats
	1 WRDemoEP05	No Remedia
Endpoint activity Last 24 Hours Seen 9 Not Seen 4 View Total 13 / 100		
- 5. 2 つのパネルでは、以下のいずれかの操作で、さらに詳細を確認できます。
  - [状態] パネルに警告メッセージが表示された場合は、リンクをクリックしてエンドポイントに関する詳細情報を表示できます。
  - どのエンドポイントからもポータルに報告がない場合は、[エンドポイントのアクティビティ]パネルの[未確認]行にある[表示]リンクをクリックします。
- 6. エンドポイントは [状態] タブと[グループの管理] タブで確認できます。[グループ管理] タブの詳細については、「エンドポイントをグループに整理ページ330」を参照してください。

# 脅威の最新状況の表示

[状態] タブで、過去1週間に脅威を報告したエンドポイントを素早く表示できます。

#### 脅威の最新状況を表示するには

1. [状態] タブをクリックします。

上部にある棒グラフは、エンドポイントで検出された脅威を示した日別概要です。パネル下部にある表には、それらのエンドポイントに関する詳細な情報が表示されます。



2. 脅威の詳細を確認するには、その脅威の行の [ブロックされたプログラム] カラムで [**表示**] リンクをクリックします。

ブロックされたプログラムが表示されます。

All threats ever seen on this endpoint								
🎓 Create override 🖳 Show all PCS which have encountered this file 📑 Restore from Quarantine								
Filename Pathname Malware Group Last Seen O Dwell Time								
1		SURIV.EXE	%temp%\501.tmp\	Uncategorized file	Sep 4th 2014, 07:08	260 days, 22 hr, 0 min, 45 sec		
2	2 🔄 SURIV.DLL %windir%lsystem32\ Uncategorized file Sep 4th 2014, 07:08 260 days, 22 hr, 0 min, 39 sec							
3		MOCKVIRUS.EXE	%temp%\temp1_mockvirus.zip\	Uncategorized file	Aug 25th 2014, 07:09	Whitelisted		

注意:滞留時間の詳細については、「滞留時間について」を参照してください。

- 3. 最近感染したエンドポイントについての追加データを下部のパネルに表示したり、非表示にしたりでき ます。カラム見出しをクリックしてドロップダウンメニューを開き、カラムを追加する場合はチェックボックス を選択し、カラムを削除する場合はチェックボックスの選択を解除します。
- 4. カラム内のデータの詳細については、「表とレポートのデータの並べ替えページ45」を参照してください。
- 5. 脅威や未判定のファイルタイプによるリスクについての追加情報を表示するには、ファイル名をクリックします。

DLM.EXE **?** X Propagation Timeline File Information Determination: Bad Malware Group: Pua.Opencandy Global Popularity: 36,523 Console Popularity: 2 Determined: May 12 2014, 16:28 Filename: DLM.EXE 12014 ep 22 2014 May 21 201 101222 MD5: 1CB3A1365543E07611A90EF9F1C9A3F3 Endpoints encountering this file FS First Seen LS Last Seen DD Date Determined 0TA0I-1772L-8PM May 21 2014, 19:44 Owell Time Perspective First Seen Last Seen W00076-4144L-DUB Jun 5 2014, 9:20 Jan 23 2014, 23:37 Globally May 21 2014, 19:44 Console Jun 5 2014, 9:20 May 21 2014, 19:44 May 21 2014, 19:44 0s 🕑 📒 Endpoint POWERED BY WEBROOT Endpoint*Forensics* 

ファイルインテリジェンスのビューが表示されます。

このビューの各フィールドの詳細については、以下の表を参照してください。

フィールド	説明
判定	判定にマウスカーソルを合わせると、エージェント、ルール、ク ラウドに関する情報が表示されます。
グローバル頻度	WIN が初めて (FS) ファイルを確認した際の情報と、そのグ ローバル頻度 (他のユーザーにより確認された頻度) が表示 されます。
Google 製品 / ベンダーリンク	リンクをクリックすると、ファイルの追加情報にアクセスできます。これは、分類が不明な場合に便利です。
オーバーライドの作成	このボタンをクリックすると、ファイルをオーバーライドして、ホワ イトリストまたはブラックリストを作成できます。
コンソール頻度	コンソール内でファイルが確認された回数と時刻を表示します。
コンソール滞留時間	コンソール内でファイルが確認された回数と時間の長さを表示します。.
エンドポイント滞留時間	問題のデバイスでファイルが確認された時間の長さを表示します。

^{6.} 脅威および追加オプションの詳細については、[最新のスキャンで脅威が存在したエンドポイント] レポートを作成して確認してください。このレポートから、エンドポイントのポリシーの変更、スキャンの実行、ファイルのオーバーライドの作成、隔離されたファイルの復元を実行できます。

詳細については、「<u>/最新のスキャンで脅威が存在したエンドポイント] レポートの生成 ページ361</u>」を参照してください。

# エージェントのバージョンの概要表示

[状態] タブにあるエージェントのバージョンの円 グラフは、エンドポイントにインストールされた Secure Anywhere バージョンの概要を示しています。エージェントとは、エンドポイントで実行されている Secure Anywhere ソフト ウェアです。

## エージェントのバージョンの円グラフを表示するには

1. [状態] タブをクリックします。

[状態] パネルが表示され、その右側にエージェントのバージョンの円グラフがあります。





2. 詳細を確認するには、カーソルを円グラフの各セクションに合わせます。

3. 詳細については、「<u>「エージェントのバージョンの使用状況」レポートの生成ページ390</u>」を参照してください。

## 滞留時間について

ウェブルートは、複数の保護メカニズムを備えた、市場最軽量のエージェントを提供しています。エージェントは、最新の脅威に対して優れた保護機能を発揮します。

ウェブルートインテリジェンスネットワークでは1日に何百万ものイベントを処理し、ソリューションの検出能力を 向上させています。デバイス上のすべてのマルウェアを初見で把握することは業界のどの企業にとっても困難 です。ウェブルートでは別な方法で高い保護機能を実現しています。

2014 年、ウェブルートは、ガートナー社のマジッククアドラントで "滞留時間を確認する能力を持つ唯一のベンダー" と評価されました。

ウェブルートは、ユーザーが悪意のあるイベントに関してできる限り多くの状況を把握できるように、フォレンジック機能の導入を続けています。他のイベントベースのソリューションでレポートされるようなノイズは排除されます。

## アプリケーションが未分類の場合

エージェントは未分類のアプリケーションに対して、ディスクで行われた変更を記録します。その際、永続的な変更は行われません。アプリケーションが不正として分類された場合、そのアプリケーションによって行われた記録変更をロールバックし、PCを修復します。この手法は、ウェブルートで分類が済んでいないマルウェアに対して、セーフティネットとして機能します。IDシールドなどのコンポーネントも併せて使われます。

#### 滞留時間とは

- 滞留時間とは、脅威がデバイス上に存在していた時間です。ファイルが最初にアクティブになった時から、 ファイルが最後に確認されるまでの期間で計算されます。
- ゼロ (0) 秒の滞留時間は、そのファイルが初見でブロックされたことを意味します。

滞留時間がゼロ(0)秒より長いということは、ウェブルートが削除する前に、そのファイルがシステムに一定時間存在していたことを意味します。

滞留時間がゼロ(0)秒を超える理由としては、ユーザーがクリーンアップ手順を完了していなかった、削除されたファイルが再びシステムに作成された、ファイルが最初は悪意のある振舞いをしていなかったためすぐに悪意があると分類されなかった、などが挙げられます。

Webroot SecureAnywhere は常にシステムを監視し、悪意がある可能性のあるファイルによって行われる変更を記録します。その後、変更をロールバックします。また、滞留時間の長さにかかわらずシステムを確実に悪意のある攻撃から保護するため、他の保護メカニズムも採用しています。

## ウェブルートが最初にすべての分類を行わない理由

初見で各ファイルをブラックリスト化するモデルは実現不可能です。脅威と戦う唯一の方法は、デバイスで行われるすべての変更を監視して、その変更をロールバックできるようにすることです。これが競合他社に対する ウェブルートの差別化要因になっています。

## 滞留時間が表示される場所

導入の最初の段階では、滞留時間はすべてのレポートと、コンソールの感染を確認できるエリアに表示されます。以降の段階では、電子メールアラートや、特定の滞留時間レポート、概要などで確認できます。

# エンドポイントプロテクションからの CSV ファイルのエクスポート

このセクションの手順に従うと、対応が必要なエンドポイントの情報が含まれる CSV ファイルをエクスポートできます。 CSV ファイルを保存しておくと、必要に応じて後から参照したり共有したりできます。

CSV へのエクスポート用のアイコンが表示されていれば、この機能を使用できます。

エンドポイントプロテクションで CSV ファイルをエクスポートするには

- 1. エンドポイントプロテクションで [状態] タブをクリックします。
- 2. [状態] エリアで [エンドポイントに対応が必要です] というリンクをクリックします。

Secure Anywhere.	MANAGED BY 2015 SALES GSM DEMC
Home Endpoint Protection Supp	ort
Status Policies Group Management	Reports Alerts Overrides Logs Resou
E Status	Redpoints encountering threats (last 7 day
Alert <u>Indpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	2 1 1 1
	0 28 ^{m Mal} 28 ^{m Mal} 29 ^{m Mal} 30 ^{m Mal}

対応が必要なエンドポイントのウィンドウが表示されます。

Endp	pints needing atte	ntion						
1	😵 Endpoints with threats							
	Hostname	Policy	Group	First Seen	Last Seen	Last Threat		
1	WRDemoEP05	No Remediation View	Default Group	Dec 17th 2013, 0	Jun 4th 2015, 09:57	Jun 4th 2015, 05:09	1	
<b>-</b>	Threats seen on this endpoint							
-								
	Filename	Patnname	Malware Gr	oup Last Se	en	Dwell Time		
		Selec	t an endpoint to pop	ulate this window				

- 3. 以下のいずれかの操作を行います。
  - [脅威が存在したエンドポイント]の情報をエクスポートするには、右上のCSV へのエクスポート用の アイコンをクリックします。

Endp	Indpoints needing attention								
۷	😵 Endpoints with threats								
	Hostname	Policy	Group	First Seen	Last Seen	Last Threat	-		
1	WRDemoEP05	No Remediation View	Default Group	Dec 17th 2013, 0	Jun 4th 2015, 09:57	Jun 4th 2015, 05:09	1		
2	<ul> <li>Threats seen on this endpoint</li> <li>Create override Show all endpoints encountering this file Restore from Quarantine</li> </ul>								
	Filename	Pathname	Malware Gro	oup Last Se	en (	Owell Time			
	Filename     Pathname     Malware Group     Last Seen     Dwell Time								

• [このエンドポイントで確認された脅威]の情報をエクスポートするには、エンドポイントを選択して[このエンドポイントで確認された脅威]内に情報を表示してから必要な項目を選択し、CSV へのエク

スポート用のアイコンをクリックします。

Endpoints with threats											
	Ho	stname	Policy		Grou	р	First Seen		Last Seen	Last Threat	
1	WF	RDemoEP05	No Reme	diation View	Defa	ult Group	Dec 17th 20	13, 0	Jun 4th 2015, 09:57	Jun 4th 2015, 05:09	1
<ul> <li>Threats seen on this endpoint</li> <li>Create override Show all endpoints encountering this file <a>Restore from Quarantine</a></li> </ul>											
C	reate	e override 🛛 💂 Sl	now all endp	oints encountering t	this file	Restore from	Quarantine				
C	reate	e override 🛛 🖳 Si Filename	how all endp	oints encountering t Pathname	this file	Restore from	Quarantine p	Last Se	en	2 Dwell Time	
1	reate	e override 🖳 SI Filename WEBROOTTES	how all endp	oints encountering t Pathname %cache%\	this file	Restore from Malware Grou W32.Webroott	Quarantine p estfile	Last Se Jun 4th	en 2015, 05:09	2 Dwell Time 104 day 18 hr 2 min 20	se
1		Filename WEBROOTTES	how all endp TFILE.E XE	oints encountering t Pathname %cache%\ %temp%\temp1_m	this file	Restore from Malware Group W32.Webroott W32.Bot.Gen	Quarantine p testfile	Last Se Jun 4th Jun 3rd	en 2015, 05:09 2015, 05:09	<ul> <li>Dwell Time</li> <li>104 day 18 hr 2 min 20</li> <li>532 day 20 hr 1 min 50</li> </ul>	se
1 2 3		e override SI Filename WEBROOTTES MOCKVIRUS.E SURIV.DLL	how all endp TFILE.E XE	oints encountering t Pathname %cache%\ %temp%\temp1_n %windir%\system?	this file [ mockvir	Restore from Malware Group W32.Webroott W32.Bot.Gen W32.Suriv.Tes	Quarantine p estfile	Last Se Jun 4th Jun 3rd Jun 3rd	en 2015, 05:09 2015, 05:09 2015, 05:09	Dwell Time 104 day 18 hr 2 min 20 532 day 20 hr 1 min 50 532 day 20 hr 1 min 37	se se

CSV ファイルがリクエストされたことを示すメッセージが表示されます。

CSV File	Requested	0				
(i)	Your CSV file has been successfully requested, and will be emailed to your account email address.					
	This should be received within the next 5 minutes. If not received within this time period, please check your email junk folder.					
	οκ					

4. [OK] ボタンをクリックしてウィンドウを閉じます。



ログインに使用した電子メールアドレス宛てにリンクが送信されます。s



5. CSV ファイルを表示するには、電子メールで届いたリンクをクリックします。その後、このファイルをコン ピュータに保存できます。

# 第6章:ポリシーの管理

ポリシーの管理方法については、以下のトピックを参照してください。

ポリシーの導入	
新しいデフォルトのポリシーの選択	
ポリシーの作成	
ポリシーの作成	
ポリシーのコピー	
ポリシーの名前の変更	
ポリシー設定の変更	
基本設定	
スキャンのスケジュール	
スキャン設定	
自己保護の設定	
ヒューリスティック	
リアルタイムシールドの設定	
動作シールドの設定	
コアシステムシールド	
Web 脅威シールド	
ID シールド	
ファイアウォール	287
ユーザーインターフェイス	
システム最適化ツール	290
ポリシーに割り当てられたエンドポイントの表示	
ポリシー間 でのエンドポイントの移動	
ポリシーの削除	

# ポリシーの導入

エンドポイントプロテクションの初期設定では、デフォルトのポリシーが選択されています。ポリシーは、スキャンのスケジュールやシールドの動作など、エンドポイントにおける Secure Anywhere の設定を定義します。

選択したデフォルトのポリシーの使用を続けるか、その他のポリシーを定義してエンドポイントに割り当てること ができます。たとえば、システム管理者に対してその他の社員よりも多くの権限を与える必要がある場合があ ります。そのような場合は、管理者用に新しいポリシーを作成し、その他の社員に対してはデフォルトのポリ シーを継続して適用することができます。

注意:ポリシーを完全に導入するには、[ポリシー]の[作成・編集]および[ポリシー]の[エンドポイント へのポリシーの割り当て]へのアクセス権限が必要です。アクセス権限の変更に関しては、「<u>コンソール</u> <u>ユーザーの権限設定ページ75</u>」を参照してください。

#### ポリシーを導入するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.								
Home Endpoint Protection Suppor	t							
Status Policies Group Management Re	ports Overrides Alerts Settings Logs Resources							
🕎 Status 🔍	🔜 Endpoints encountering threats (last 7 days)							
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.								

^{2.} [ポリシー] タブをクリックします。

Secure Anywhere.	
Home Endpoint Protection Suppo	ort
Status Policies Group Management F	Reports Overrides Alerts Settings Logs Resources
🕎 Status 🔍	Endpoints encountering threats (last 7 days)
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	

## [ポリシー] タブが表示されます。

Secure Anywhere.						
Home Endpoint Protection Support						
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
Policies						
😳 Create   😑 Delete   📁 Rename   🛅 Copy   🗅 Set as Default   🛃 Import	Export					
Policy Name 🔺	Policy Description					
Add Policy Copy with Draft	Add Policy Copy with Draft 1					
Add Policy Rename	Add Policy Description Renamed					
ALEndpointPolicy	For Ali & Leo tests.					
Copied from non dns policy June	Copied from non dns policy June					
e Hotfix policy	Policy test for Hot fix					
Import Live New Policy	Import Live New Policy					

3. デフォルトのポリシーの使用を継続するかどうかを決定します。

デフォルトのポリシーはペインの左側にあり、白い水平の矢印で示されています。

Secure Anywhere.							
Home Endpoint Protection Support							
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources							
Policies							
🕒 Create   😑 Delete   📺 Rename   🛅 Copy   🗁 Set as Default   🖓 Import	Export						
Policy Name	Policy Description						
AdminPolicy	AdminPolicy						
All shields off	To disable shield for troubleshooting						
default but gui on	default but gui on						
Hide Gui	Only setting change from default is H						
Mac	Mac						
RestU	Rec+UI						
C Recommended Defaults	Recommended setup with protection						
Recommended Server Defaults	Recommended setup for servers, pro						
Silent Audit	Non-remediating Security Audit with						

TEST			ð?D:
Section	Setting	Live	Draft
Basic Configuration	Show a SecureAnywhere shortcut on the desktop	On	
Scan Schedule	Show a system tray icon	Off	
Scan Settings	Show a splash screen on bootup	On	
Self Protection	Show SecureAnywhere in the Start Menu	Off	
Heuristics	Show SecureAnywhere in Add/Remove Programs	On	
Realtime Shield	Show SecureAnywhere in the Windows Action Center	On	
Behavior Shield	Hide the SecureAnywhere keycode and subscription i	Off	
Core System Shield	Automatically download and apply updates Off		
Web Threat Shield	Operate background functions using fewer CPU resou     Off		
Identity Shield	Favor low disk usage over verbose logging (fewer det	Off	
Firewall	Lower resource usage when intensive applications or	On	
User Interface	Allow SecureAnywhere to be shut down manually	Off	
System Optimizer	em Optimizer Force non-critical notifications into the background		
	Fade out warning messages automatically		
	Store Execution History details	On	
	Poll interval	Daily	
Promote Draft Changes t	D Live Save (	Changes Reset Ch	anges Cancel

4. デフォルトのポリシー名をダブルクリックして設定を表示します。

• Windows PC のみに適用される設定には、Windows のアイコンが表示されます。



• Windows PC と Mac に適用される設定には、Windows アイコンと Mac アイコンの両方が表示されます。



**注意:** 非管理ポリシーの設定は、管理者ではなく、エンドポイントユーザーが権限を持つよう指定されているため、表示されません。

ポリシーの設定を確認して、デフォルトのポリシーがビジネス要件を満たしているかどうかを判断します。
 満たしていない場合、ウェブルートのデフォルトは修正できないため、新しいポリシーを作成する必要があります。

詳細については、「ポリシーの作成ページ233」を参照してください。

6. 新しいポリシーを作成したら、[グループ管理] タブのエンドポイントに割り当てることができます。

詳細については、「エンドポイントのグループへのポリシーの適用ページ324」を参照してください。

# 新しいデフォルトのポリシーの選択

Secure Anywhere が新しいエンドポイントにインストールされる場合は必ず、エンドポイントプロテクションによっ てデフォルトのポリシーに割り当てられます。必要に応じて、将来インストールするエンドポイントに対しては異 なるデフォルトのポリシーを設定することができます。

### 新しいデフォルトのポリシーを選択するには

1. <u>エンドポイントプロテクションのコンソール</u>にログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.				
Home Endpoint Protection Supp	ort			
Status Policies Group Management	Reports Overrides Alerts Settings Logs Resources			
E Status	🖳 Endpoints encountering threats (last 7 days)			
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.				

2. [ポリシー] タブをクリックします。

Secure Anywhere.				
Home Endpoint Protection Supp	ort			
Status Policies Group Management	Reports Overrides Alerts Settings Logs Resources			
🔄 Status 🔍	🖳 Endpoints encountering threats (last 7 days)			
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.				

## [ポリシー] タブが表示されます。

Secure Anywhere.				
Home Endpoint Protection Support				
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources				
Policies				
😌 Create   😑 Delete   📺 Rename   🛅 Copy   🗅 Set as Default   🛃 Import   📑 Export				
Policy Name 🔺 Policy Description				
Add Policy Copy with Draft	Add Policy Copy with Draft 1			
Add Policy Rename	Add Policy Description Renamed			
ALEndpointPolicy	For Ali & Leo tests.			
Copied from non dns policy June	Copied from non dns policy June			
e Hotfix policy	Policy test for Hot fix			
Import Live New Policy	Import Live New Policy			

デフォルトのポリシーはペインの左側にあり、白い水平の矢印で示されています。

Secure Anywhere.				
Home Endpoint Protection Support				
Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources			
Policies				
😳 Create   😑 Delete   📺 Rename   🛅 Copy   🗔 Set as Default   🛃 Import	Export			
Policy Name	Policy Description			
AdminPolicy	AdminPolicy			
All shields off	To disable shield for troubleshooting			
default but gui on	default but gui on			
Hide Gui	Only setting change from default is H			
Mac	Mac			
RestUl	Rec+UI			
Recommended Defaults	Recommended setup with protection			
Recommended Server Defaults	Recommended setup for servers, pro			
Silent Audit	Non-remediating Security Audit with I			

3. [ポリシー名] カラムで、新しいデフォルトとして使用するポリシーをクリックします。

Secure Anywhere.					
Home Endpoint Protection Support					
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources					
Policies	Policies				
🔁 Create   😑 Delete   🎘 Rename   🛅 Copy   🕞 Set as Default   🛃 Imp	ort   📑 Export				
Policy Name	Policy Description				
AdminPolicy	AdminPolicy				
All shields off	To disable shield for troubleshooting				
default but gui on	default but gui on				
Hide Gui	Only setting change from default is Hide GUI				
Mac	Mac				
Rec+UI	Rec+UI				
Recommended Defaults	Recommended setup with protection and remediation				
Recommended Server Defaults Recommended setup for servers, protection enabled					
Silent Audit	Non-remediating Security Audit with limited protection enabled				

[デフォルトに設定] アイコンがアクティブになります。

4. [デフォルトに設定] アイコンをクリックします。

Secure Anywhere.				
Home Endpoint Protection Support				
Status         Policies         Group Management         Reports         Overrides         Alerts         Settings         Logs         Resources				
Policies				
😳 Create   😑 Delete   📺 Rename   🛅 Copy 🕞 Set as Default 💽 Import   🕃 Export				
Policy Name	Policy Description			
AdminPolicy	AdminPolicy			
All shields off	To disable shield for troubleshooting			
default but gui on	default but gui on			
Hide Gui	Only setting change from default is Hide GUI			
Mac	Mac			
Rec+UI	Rec+UI			
Recommended Defaults	Recommended setup with protection and remediation			
Recommended Server Defaults	Recommended setup for servers, protection enabled			
Silent Audit	Non-remediating Security Audit with limited protection enabled			

[デフォルトのポリシーを設定] ウィンドウが表示されます。

Set Defa	ult Policy	×
?	Set "Recommended Server Defaults" as the default policy / settings for all endpoints to pick up during install?	
	Yes No	

## 5. [はい] ボタンをクリックします。



白い矢印が新しいデフォルトのポリシーに移動し、このポリシーが Secure Anywhere の新しいインストールすべてに適用されるようになります。

Secure Anywhere.				
Home Endpoint Protection Support				
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources				
Policies				
🔁 Create   😑 Delete   🏝 Rename   🛅 Copy   🕞 Set as Default   🚭 Import	Export			
Policy Name Policy Description				
AdminPolicy AdminPolicy				
All shields off	To disable shield for troubleshooting			
default but gui on	default but gui on			
Hide Gui	Only setting change from default is Hide GUI			
Mac	Mac			
Rec+UI	Rec+UI			
Recommended Defaults	Recommended setup with protection and remediation			
Recommended Server Defaults     Recommended setup for servers, protection enabled				
Silent Audit Non-remediating Security Audit with limited protection enable				

## ポリシーの作成

ポリシーを追加するには、新しいポリシーを作成するか、既存のポリシーをコピーして使用します。以下は、それぞれの手順についての説明です。ポリシー名を定義して説明を入力すると、ポリシー設定を指定できるようになります。詳細については、「ポリシー設定の変更ページ247」を参照してください。

このトピックでは、次の手順について説明します。

- 新しいポリシーの作成
- <u>ポリシーのコピー</u>

注意:ポリシー名は一意のものである必要があるため、後で競合することがないよう、事前にポリシー 名について考えておいてください。一度ポリシー名をつけると、そのポリシーを削除した後でも同じ名前 を再利用することはできません。

## ポリシーの作成

名前と説明を指定し、新規ポリシーを作成します。新規ポリシーでは推奨されているデフォルト設定が最初に選択されますが、設定は後で変更できます。

#### 新しいポリシーを作成するには

1. <u>エンドポイントプロテクションのコンソールにログインします</u>。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.				
Home Endpoint Prot	tion Support			
Status Policies Group	anagement Reports Overrides Alerts Settings Logs Resources	3		
🖳 Status	< 🖳 Endpoints encountering threats (last 7 days)			
We recommend you check we endpoint has automatic reme on the assigned policy.	attention ther this tion enabled			

2. [ポリシー] タブをクリックします。

Secure Anywhere.							
Home	Endpoint Protection	Support					
Status	Policies Group Managen	nent Repor	ts Overrides	Alerts	Settings	Logs	Resources
🛄 Status		۲	Endpoints enco	untering t	threats (last	7 days)	
We recon endpoint l on the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this has automatic remediation end signed policy.	on s abled					

[ポリシー] タブが表示されます。

Secure Anywhere.				
Home Endpoint Protection Support				
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources				
Policies				
🕒 Create   😑 Delete   📺 Rename   🛅 Copy   🗅 Set as Default   🛃 Import   📑 Export				
Policy Name 🔺	Policy Description			
Ndd Policy Copy with Draft	Add Policy Copy with Draft 1			
Add Policy Rename	Add Policy Description Renamed			
ALEndpointPolicy For Ali & Leo tests.				
Copied from non dns policy June Copied from non dns policy June				
Hotfix policy	Policy test for Hot fix			
Import Live New Policy	Import Live New Policy			

3. コマンドバーの[作成]ボタンをクリックします。

Secure Anywhere.			
Home Endpoint Protection Support			
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources			
Policies			
🕒 Create ) 😑 Delete   🃺 Rename   🛅 Copy   🖂 Set as Default   🖑 Import   📑 Export			
Policy Name	Policy Description		
AdminPolicy	AdminPolicy		

[ポリシーを作成] ウィンドウが表示されます。

ウェブルートエンドポイントプロテクション管理者ガイド

Create Policy		X
Policy Name: Policy Description:		
(	Create Policy Cancel	

4. [ポリシー名] フィールド にポリシーの名前を入力します。

Create Policy	×
Policy Name:	
Policy Description:	
	Create Policy Cancel

5. [新しいポリシーの説明] フィールドに、最大 50 文字 (英数字)で説明を入力します。

Create Policy	[	×
Policy Name:		
Policy Description:		
	Create Policy Cancel	

6. [ポリシーを作成] ボタンをクリックします。

Create Policy	3	×
Policy Name: Policy Description:		
0	Create Policy Cancel	

7. [ポリシー名] カラムで、新しいポリシーを見つけます。

以下のいずれかの操作を行います。

- ポリシーをダブルクリックして設定を変更します。詳細については、「ポリシー設定の変更ページ247」
   を参照してください。
- ポリシーを、個々のエンドポイントまたはエンドポイントのグループに対して適用します。詳細については、「エンドポイントのグループへのポリシーの適用ページ324」を参照してください。

## ポリシーのコピー

類似したポリシーをすでに定義している場合は、それをコピーして名前を変更することができます。新しいポリ シーはコピーしたポリシーの設定を使用しますが、後でその設定を変更することができます。

#### ポリシーをコピーするには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secu	ireAnywher	0.					
Home	Endpoint Protection	Support					
Status	Policies Group Managen	nent Reports	Overrides	Alerts	Settings	Logs	Resources
🖳 Status			ndpoints enco	untering t	threats (last	7 days)	
We recommendpoint has on the assisted	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation ena- gned policy.	n s bled					

2. [ポリシー] タブをクリックします。

Sec	ureAnywher	e.					
Home	Endpoint Protection	Support					
Status	Policies Group Manager	nent Repor	rts Overrides	Alerts	Settings	Logs	Resources
🕎 Status		«	Endpoints enco	untering t	hreats (last 7	days)	
We reco endpoint on the as	Alert <u>1 Endpoint needs attention</u> mmend you check whether thi has automatic remediation end asigned policy.	on s abled					

[ポリシー] タブが表示されます。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts S	Settings Logs Resources
Policies	
🔂 Create   😄 Delete   🚛 Rename   🛅 Copy   🗅 Set as Default   🛃 Import	Export
Policy Name 🔺	Policy Description
Add Policy Copy with Draft	Add Policy Copy with Draft 1
Add Policy Rename	Add Policy Description Renamed
ALEndpointPolicy	For Ali & Leo tests.
Copied from non dns policy June	Copied from non dns policy June
e Hotfix policy	Policy test for Hot fix
Import Live New Policy	Import Live New Policy

3. [ポリシー名] カラムで、元になるポリシーを選択し、[コピー] アイコンをクリックします。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources
Policies	
🔂 Create   😑 Delete   📺 Rename 🕕 Copy 🕞 Set as Default   🖑 Import	Export
Policy Name	Policy Description
AdminPolicy	AdminPolicy
All shields off	To disable shield for troubleshooting
Rec+UI	Rec+UI
Recommended Defaults	Recommended setup with protection and remediation
Recommended Server Defaults	Recommended setup for servers, protection enabled
Silent Audit	Non-remediating Security Audit with limited protection enabled
test	test
test1	test
test2	test2

[ポリシーのコピー] ウィンドウが表示されます。選択したポリシーが [コピーするポリシー] フィールドに表示 されています。

Copy Policy		
Policy to Copy:	TEST 💌	
Policy Name:		
Policy Description:		
	Create Policy Cancel	

4. 必要に応じて、[コピーするポリシー]ドロップダウンメニューからコピー対象の別のポリシーを選択します。

Copy Policy		×
Policy to Copy:	TEST	
Policy Name:	AdminPolicy	
Policy Description:	All shields off	
Policy Description.	default but gui on	
	– Hide Gui –	
	Mac	
	Rec+UI	_
	Recommended Defaults	
	Recommended Server Defaults	
	Silent Audit	
	TEST	
	test1	
	test2	

5. [ポリシー名] フィールドに一意の名前を入力します。

Copy Policy		×
Policy to Copy:	TEST	~
Policy Name:		
Policy Description:		
	Create Policy Cancel	

6. [新しいポリシーの説明] フィールドに、最大 50 文字 (英数字) で説明を入力します。

Policy to Copy:	TEST	×
Policy Name:		
Policy Description:		

7. [ポリシー名] カラムで、新しいポリシーを見つけます。

以下のいずれかの操作を行います。

- ポリシーをダブルクリックして設定を変更します。詳細については、「ポリシー設定の変更ページ247」
   を参照してください。
- ポリシーを、個々のエンドポイントまたはエンドポイントのグループに対して適用します。詳細については、「エンドポイントのグループへのポリシーの適用ページ324」を参照してください。

## ポリシーの名前の変更

[ポリシー] タブでポリシーの名前を変更できます。ポリシー名は一意である必要があります。

## ポリシーの名前を変更するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.									
Home	Endpoint Protection	Support							
Status	Status         Policies         Group Management         Reports         Overrides         Alerts         Settings         Logs         Resources								
🛄 Status		«	Endpoints enco	untering	threats (last	7 days)			
We recom endpoint h on the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation ena- igned policy.	n s ibled							
2. [ポリシー] タブをクリックします。

Seci	ireAnywhere.
Home	Endpoint Protection Support
Status	Policies Group Management Reports Overrides Alerts Settings Logs Resources
🖳 Status	< 🖳 Endpoints encountering threats (last 7 days)
We recomendpoint hon the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation enabled igned policy.

#### [ポリシー] タブが表示されます。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts S	ettings Logs Resources
Policies	
🔁 Create   😑 Delete   🃺 Rename   🛅 Copy   🖂 Set as Default   🛃 Import	Export
Policy Name 🔺	Policy Description
e Add Policy Copy with Draft	Add Policy Copy with Draft 1
Add Policy Rename	Add Policy Description Renamed
ALEndpointPolicy	For Ali & Leo tests.
Copied from non dns policy June	Copied from non dns policy June
e Hotfix policy	Policy test for Hot fix
Import Live New Policy	Import Live New Policy

3. [ポリシー名] カラムで、名前を変更するポリシーを選択します。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources
Policies	
😌 Create   😑 Delete   📺 Rename   🛅 Copy   🗅 Set as Default   🔄 Imp	ort   📑 Export
Policy Name	Policy Description
AdminPolicy	AdminPolicy
All shields off	To disable shield for troubleshooting
Rec+UI	Rec+UI
Recommended Defaults	Recommended setup with protection and remediation
Recommended Server Defaults	Recommended setup for servers, protection enabled
Silent Audit	Non-remediating Security Audit with limited protection enabled
test	test
test1	test
test2	test2

[名前変更] アイコンがアクティブになります。

4. [名前変更] アイコンをクリックします。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources
Policies	
🔂 Create   😑 Delete   📺 Rename   🛅 Copy   🖂 Set as Default   🖑 Import	Export
Policy Name	Policy Description
AdminPolicy	AdminPolicy
All shields off	To disable shield for troubleshooting
Rec+UI	Rec+UI
Recommended Defaults	Recommended setup with protection and remediation
Recommended Server Defaults	Recommended setup for servers, protection enabled
Silent Audit	Non-remediating Security Audit with limited protection enabled
test	test
test1	test
test2	test2

[ポリシーの名前を変更] ウィンドウが表示されます。

Policy Name:	test	
Policy Description:	test	
	L	

5. [ポリシー名] フィールドに、ポリシーの新しい名前と説明を入力します。

Rename Policy		×
Policy Name:	test	
Policy Description:	test	
	Rename Policy Cancel	

6. [ポリシーの説明] フィールドで、必要に応じてポリシーの説明をアップデートします。

Rename Policy		×
Policy Name:	test	
Policy Description:	test	
	Rename Policy Cancel	

7. 設定が完了したら、[ポリシーの名前を変更]ボタンをクリックします。

Rename Policy	ĺ	×
Policy Name:	test	
Policy Description:	test	
(	Rename Policy Cancel	

[ポリシー名] カラムに新しいポリシー名 が表示されます。

# ポリシー設定の変更

ポリシーを作成したら、ビジネスの目的に合わせてポリシー設定を変更することができます。必要に応じて、一時的に変更 (下書きを作成)し、後で反映 (ライブに昇格) することもできます。詳細については、「<u>ポリシーの</u> 作成 ページ233」を参照してください。

注意:ウェブルートのデフォルトのポリシー設定は変更できません。

管理されているエンドポイントについて、次のような SecureAnywhere の設定をポリシーで制御することができます。

セクション	説明
基本設定	ー 般 設 定 では、エンド ポイント のシステムトレイにプログラムのアイコン を表 示 するかどうか、ユーザーがプログラムをシャット ダウンできるかどう かなど、SecureAnywhere プログラムの動 作を変 更します。
<u>スキャンのスケジュール</u>	スキャンを別の時刻に実行したり、スキャン中の動作を変更したり、 自動スキャンを解除したりすることができます。スキャンのスケジュール を変更しない場合、SecureAnywhere は、ソフトウェアがインストール された時刻と同じ頃に毎日自動的にスキャンを実行します。
<u>スキャン設定</u>	詳細なスキャンの実行など、スキャンを細かく管理できます。
<u>自己保護</u>	保護を追加して、悪意のあるソフトウェアがエンドポイントで SecureAnywhere プログラムの設定やプロセスを変更できないようにし ます。別の製品が SecureAnywhere の機能に干渉しようとしているこ とが検出された場合、保護のためのスキャンを開始して脅威を特定 します。

セクション	説明
<u>ヒューリスティック</u>	エンドポイントのスキャン中に SecureAnywhere が実行する脅威分析 を設定できます。 ヒューリスティックは、 ローカルドライブ、 USB ドライ ブ、 インターネット、 ネット ワーク、 CD / DVD、 オフライン時の動作な ど、 エンドポイントのさまざまなエリアに対して調整できます。
リアルタイムシールド	ウェブルートによる脅威の定義およびコミュニティのデータベースにリス トされている既知の脅威をブロックします。
動作シールド	エンドポイントで実行中のアプリケーションとプロセスを分析します。
コアシステムシールド	コンピュータのシステムの構造を監視し、マルウェアによって改ざんされ ていないか確認します。
<u>Web 脅威シールド</u>	ユーザーがインターネットを閲覧したり、検索結果をクリックしたりする際に、エンドポイントを保護します。
<u>ID シールド</u>	個人情報の盗難や金銭的な損失からユーザーを守ります。キーロ ガーやスクリーングラバー、その他の情報盗用技術からユーザーを守 りながら、重要なデータが確実に保護されるようにします。
<u>ファイアウォール</u>	コンピュータのポートから出力されるデータトラフィックを監視します。インターネットに接続して個人情報を盗もうとする、信頼できないプロセスを探します。一方で、Windows ファイアウォールは、コンピュータに入ってくるデータトラフィックを監視します。

セクション	説明
ユーザーインターフェイス	エンドポイントでの SecureAnywhere プログラムへのユーザー アクセス を設定します。
<u>システム最適化ツール</u>	自動クリーンアップのスケジュール、エンドポイントから削除するファイル や痕跡の種類など、システム最適化ツールの動作を制御します。

#### ポリシーの設定を変更するには

1. <u>エンドポイントプロテクションのコンソール</u>にログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.		
Home Endpoint Protection Sup	pport	
Status Policies Group Management	Reports Overrides Alerts Settings Logs Resource	s
🔤 Status 🔍	Endpoints encountering threats (last 7 days)	
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.		

2. [ポリシー] タブをクリックします。

Secure Anywhere.					
Home Endpoint Protection	Support				
Status Policies Group Manage	ement Reports	Overrides Ale	erts Settings Logs	Resources	
E Status	< 🖳 En	idpoints encounte	ring threats (last 7 days)		
We recommend you check whether the endpoint has automatic remediation error on the assigned policy.	tion nis nabled				

#### [ポリシー] タブが表示されます。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts S	Settings Logs Resources
Policies	
🔁 Create   😑 Delete   📁 Rename   🖺 Copy   🗅 Set as Default   🛃 Import	Export
Policy Name 🔺	Policy Description
Add Policy Copy with Draft	Add Policy Copy with Draft 1
Add Policy Rename	Add Policy Description Renamed
ALEndpointPolicy	For Ali & Leo tests.
Copied from non dns policy June	Copied from non dns policy June
e Hotfix policy	Policy test for Hot fix
Import Live New Policy	Import Live New Policy

3. [ポリシー名] カラムで変更するポリシーを探して、そのポリシーをダブルクリックします。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources
Policies	
😌 Create   😑 Delete   📺 Rename   🛅 Copy   🗅 Set as Default   🚭 Import	Export
Policy Name	Policy Description
AdminPolicy	AdminPolicy
All shields off	To disable shield for troubleshooting
Rec+UI	Rec+UI
Recommended Defaults	Recommended setup with protection and remediation
Recommended Server Defaults	Recommended setup for servers, protection enabled
Silent Audit	Non-remediating Security Audit with limited protection enabled
C test	test
test1	test
test2	test2

[セクション] コラムの基本設定が選択された状態で、ポリシーの設定ウィンドウが表示されます。

TEST ă?D				ĕ?¤×
Section		Setting	Live	Draft
Basic Configuration		Show a SecureAnywhere shortcut on the desktop	On	
Scan Schedule		Show a system tray icon	Off	
Scan Settings		Show a splash screen on bootup	On	
Self Protection		Show SecureAnywhere in the Start Menu	Off	
Heuristics		Show SecureAnywhere in Add/Remove Programs	On	
Realtime Shield		Show SecureAnywhere in the Windows Action Center	On	
Behavior Shield	Ľú	Hide the SecureAnywhere keycode and subscription i	Off	
Core System Shield	Ľú	Automatically download and apply updates	Off	
Web Threat Shield		Operate background functions using fewer CPU resou.	. Off	
Identity Shield		Favor low disk usage over verbose logging (fewer det	Off	
Firewall	<b>.</b>	Lower resource usage when intensive applications or	On	
User Interface	Ľú	Allow SecureAnywhere to be shut down manually	Off	
System Optimizer		Force non-critical notifications into the background	On	
	É	Fade out warning messages automatically	On	
		Store Execution History details	On	
		Poll interval	Daily	
Promote Draft Changes to Liv	ve	Save	Changes Reset Ch	anges Cancel

[設定] カラムにはポリシーの名前が表示されています。アイコンの意味は以下のとおりです。

- Setting Show a SecureAn Show a system tra Show a splash scr Show SecureAnyv Show SecureAnyv Show SecureAnyv Hide the SecureAr Automatically dow Operate backgrou
- Windows PC のみに適用される設定には、Windows のアイコンが表示されます。

• Windows PC と Mac に適用される設定には、Windows アイコンと Mac アイコンの両方が表示されます。



[ライブ] カラムには、設定が現在エンドポイントでどのような状態にあるかが表示されます。

TEST					ă	? 🗆 🗙
Section		Setting	1	Live	Draft	
Basic Configuration		Show a SecureAnywhere shortcut on the desktop	Г	On		
Scan Schedule		Show a system tray icon	L	Off		
Scan Settings		Show a splash screen on bootup	L	On		
Self Protection		Show SecureAnywhere in the Start Menu	L	Off		
Heuristics		Show SecureAnywhere in Add/Remove Programs	L	On		
Realtime Shield		Show SecureAnywhere in the Windows Action Cent	er	On		
Behavior Shield	Ľú	Hide the SecureAnywhere keycode and subscription	i	Off		
Core System Shield	<b>.</b>	Automatically download and apply updates	L	Off		
Web Threat Shield		Operate background functions using fewer CPU res	ou	Off		
Identity Shield		Favor low disk usage over verbose logging (fewer d	et	Off		
Firewall	Ľú	Lower resource usage when intensive applications of	r	On		
User Interface	<b>.</b>	Allow SecureAnywhere to be shut down manually	L	Off		
System Optimizer		Force non-critical notifications into the background	L	On		
	<b>.</b>	Fade out warning messages automatically	L	On		
		Store Execution History details	L	On		
		Poll interval	L	Daily		
Promote Draft Changes to Li	ive	s	ave (	Changes Reset Chan	ges Ca	ancel

[下書き] カラムで値を変更します。

TEST		ă? 🗆 🗙
Section	Setting L	Live Draft
Basic Configuration	Show a SecureAnywhere shortcut on the desktop	Dn
Scan Schedule	Show a system tray icon	Off
Scan Settings	Show a splash screen on bootup	Dn
Self Protection	Show SecureAnywhere in the Start Menu	Off
Heuristics	Show SecureAnywhere in Add/Remove Programs	Dn
Realtime Shield	Show SecureAnywhere in the Windows Action Center	Dn
Behavior Shield	Hide the SecureAnywhere keycode and subscription i	Off
Core System Shield	Automatically download and apply updates	Off
Web Threat Shield	Operate background functions using fewer CPU resou	Off
Identity Shield	Favor low disk usage over verbose logging (fewer det	Off
Firewall	Lower resource usage when intensive applications or C	Dn
User Interface	Allow SecureAnywhere to be shut down manually	Off
System Optimizer	Force non-critical notifications into the background	Dn
	Fade out warning messages automatically	Dn
	Store Execution History details	Dn
	Poll interval	Daily
Promote Draft Changes to	Live Save Cha	anges Reset Changes Cancel

4. [セクション] カラムで編集 するカテゴリを選択します。

TEST			ă?ox
Section	Setting	Live	Draft
Basic Configuration	Enable Scheduled Scans	On	
Scan Schedule	Scan Frequency	Daily	
Scan Settings	Time	Scan at 10:00 a	
Self Protection	Scan on bootup if the computer is off at the schedu	uled On	
Heuristics	Hide the scan progress window during scheduled s	scans On	
Realtime Shield	Only notify me if an infection is found during a sche	edul On	
Behavior Shield	Conot perform scheduled scans when on battery r	power On	
Core System Shield	Construction of the second sec	n ap On	
Web Threat Shield	Randomize the time of scheduled scans up to one	hou On	
Identity Shield	Perform a scheduled Quick Scan instead of a Dee	p Sc Off	
Firewall			
User Interface			
System Optimizer			
Promote Draft Changes to Li	/8	Save Changes Reset Ch	anges Cancel

5. 各設定の[下書き] カラムでセルをダブルクリックしてオプションを表示し、ドロップダウンメニューから適切 な設定を選択します。

TEST			Ľ	i? 🗆 🗙
Section	Setting	Live	Draft	
Basic Configuration	Enable Scheduled Scans	On	On	~
Scan Schedule	Scan Frequency	Daily	Off	
Scan Settings	Time	Scan at 10:00 a.	On	
Self Protection	Scan on bootup if the computer is off at the scheduled	On	-	
Heuristics	Hide the scan progress window during scheduled scans	On		
Realtime Shield	Only notify me if an infection is found during a schedul	On		
Behavior Shield	Do not perform scheduled scans when on battery power	On		
Core System Shield	Do not perform scheduled scans when a full screen ap	On		
Web Threat Shield	Randomize the time of scheduled scans up to one hou	On		
Identity Shield	Perform a scheduled Quick Scan instead of a Deep Sc	Off		
Firewall				
User Interface				
System Optimizer				
Promote Draft Changes to Li	ve Save C	hanges Reset Ch	anges C	ancel

#### それぞれの設定の詳細な説明については、この手順の下にある表を参照してください。

<u>基本設定</u>	リアルタイムシールド	<u>ファイア</u> ウォール
<u>スキャンのスケジュール</u>	<u>動作シールド</u>	ユ <del>ーザー</del> インター フェイス
<u>スキャン設定</u>	<u>コアシステムシールド</u>	<u>システム</u> <u>最適化</u> <u>ツール</u>
<u>自己保護</u>	<u>Web 脅威シールド</u>	
ヒューリスティック	ID シールド	

TEST			ă?ox
Section	Setting	Live	Draft
Basic Configuration	Enable Scheduled Scans	On	Off
Scan Schedule	Scan Frequency	Daily	
Scan Settings	Time	Scan at 10:00	) a
Self Protection	Scan on bootup if the computer is of	f at the scheduled On	
Heuristics	Hide the scan progress window duri	ng scheduled scans On	Off
Realtime Shield	Only notify me if an infection is found	d during a schedul On	
Behavior Shield	Do not perform scheduled scans wh	en on battery power On	Off
Core System Shield	Do not perform scheduled scans wh	en a full screen ap On	Off
Web Threat Shield	Randomize the time of scheduled so	ans up to one hou On	
Identity Shield	Perform a scheduled Quick Scan ins	stead of a Deep Sc Off	On
Firewall			
User Interface			
System Optimizer			
Promote Draft Changes to Live Cancel			

6. 選択内容の変更を完了したら、[変更を保存]ボタンをクリックします。

7. ポリシーの各セクションの変更を続けます。他のセクションへ移動する前に必ず [変更を保存] をクリック してください。

変更が保存されていないポリシーは、[下書きの変更]カラムに表示されます。

TEST		ă)	?0;
Section	Setting	Live Draft	
Basic Configuration	Enable Scheduled Scans	On Off	
Scan Schedule	Scan Frequency	Daily	
Scan Settings	Time	Scan at 10:00 a	
Self Protection	Scan on bootup if the computer is off at the s	scheduled On	
Heuristics	Hide the scan progress window during schee	duled scans On Off	
Realtime Shield	Only notify me if an infection is found during	a schedul On	
Behavior Shield	Conot perform scheduled scans when on ba	attery power On Off	
Core System Shield	Conot perform scheduled scans when a full	screen ap On Off	
Web Threat Shield	Randomize the time of scheduled scans up t	to one hou On	
Identity Shield	Perform a scheduled Quick Scan instead of	a Deep Sc Off On	
Firewall			
User Interface			
System Optimizer			
Describe Desch Obresset			
Promote Draft Changes t	lo Live	Save Changes Reset Changes Ca	ncei

**注意:**緑は設定がオンであることを示し、オレンジは設定がオフであることを示します。この色分けにより、リストを簡単に確認できます。

- 8. 以下のいずれかの操作を行います。
  - この段階ではまだ変更を反映しない場合は、[変更を保存]ボタンをクリックして[ポリシー]タブに戻ります。

iest 🎽 🕄				
Section	Setting	Live	Draft	
Basic Configuration	Enable Scheduled Scans	On	Off	
Scan Schedule	Scan Frequency	Daily		
Scan Settings	Time	Scan at 10:00 a		
Self Protection	Scan on bootup if the computer is off at the scheduled	i On		
Heuristics	Hide the scan progress window during scheduled sca	ns On	Off	
Realtime Shield	Only notify me if an infection is found during a schedu	I On		
Behavior Shield	Do not perform scheduled scans when on battery pow	ver On	Off	
Core System Shield	Do not perform scheduled scans when a full screen a	p On	Off	
Web Threat Shield	Randomize the time of scheduled scans up to one ho	u On		
Identity Shield	Perform a scheduled Quick Scan instead of a Deep S	ic Off	On	
Firewall				
User Interface				
System Optimizer				
Promote Draft Changes to Live Cancel				

• 変更を反映する場合は、[変更を保存]ボタンをクリックしてから[下書きの変更をライブに昇格]ボタンをクリックします。

TEST				ă?¤×
Section	Setting		Live	Draft
Basic Configuration	Enable Scheduled Sca	ns	On	Off
Scan Schedule	Scan Frequency		Daily	
Scan Settings	Time		Scan at 10:00 a	
Self Protection	Scan on bootup if the c	omputer is off at the scheduled	On	
Heuristics	Hide the scan progress	window during scheduled scans	On	Off
Realtime Shield	Only notify me if an infe	ction is found during a schedul	On	
Behavior Shield	E Do not perform schedu	ed scans when on battery power	On	Off
Core System Shield	E Do not perform schedu	ed scans when a full screen ap	On	Off
Web Threat Shield	Randomize the time of	scheduled scans up to one hou	On	
Identity Shield	Perform a scheduled Q	uick Scan instead of a Deep Sc	Off	On
Firewall				
User Interface				
System Optimizer				
Promote Draft Changes to	Live	Save C	hanges Reset Cha	anges Cancel

注意: 昇格するまで変更は有効になりません。

# 基本設定

基本設定は、管理されたエンドポイント上でのSecureAnywhere ソフトウェアの動作を制御します。

設定	説明
SecureAnywhere へのショートカッ トをデスクトップ上に表示する	エンドポイントのデスクトップにショートカット アイコンを配置し、メイン インターフェイスにすばやくアクセスできるようにします。 この設定は PC エンドポイントにのみ適用されます。
システムトレイ アイコンを表示する	エンドポイントのシステムトレイにウェブルートのアイコンを配置し、 SecureAnywhere の各機能にすばやくアクセスできるようにします。 この設定は PC エンドポイントにのみ適用されます。
起動時にスプラッシュ画面を表示 する	エンドポイントの起動時にウェブルートのスプラッシュ画面が表示され ます。 この設定は PC エンドポイントにのみ適用されます。
SecureAnywhere をスタート メ ニューに表示する	Windows のスタート メニューに Secure Anywhere が表示されます。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
[プログラムの追加と削除] パネル に SecureAnywhere を表示する	Windows の [プログラムの追加と削除] パネルに Secure Anywhere が 表示されます。 この設定は PC エンドポイントにのみ適用されます。
Windows アクション センターに SecureAnywhere を表示する	Windows セキュリティ / アクション センターの [ウイルス対策] に SecureAnywhere が一覧表示されるようになります。 この設定は PC エンドポイントにのみ適用されます。
SecureAnywhere のキーコードお よび定期購入契約情報を画面 上に表示しない	エンドポイントの [マイアカウント] パネルで、キーコードを非表示にします。キーコードの最初の4桁以外はアスタリスクで表示します。 この設定は PC および Mac エンドポイントの両方に適用されます。
アップデートを自動的にダウンロー ドして適用する	エンドポイント ユーザーへの警告なしに製品のアップデートを自動的 にダウンロードします。 この設定は PC および Mac エンドポイントの両方に適用されます。
使用する CPU リソースを減らして バックグラウンド機能を作動させる	スキャンに関連しない機能をバックグラウンドで実行することで、CPU リソースを節約します。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
詳細なロギングよりも低ディスク使	保存する最新のログアイテムを4つに制限することで、ディスク容量
用量を優先する(ログ情報量は	を節約します。
少なくなります)	この設定はPC エンドポイントにのみ適用されます。
フル画面アプリケーションまたは	ゲーム、ビデオ、または大量のリソースを使用するその他のアプリケー
ゲームの検出時にリソース使用量	ションを実行中に、SecureAnywhereの機能を抑制します。
を低減する	この設定は PC および Mac エンドポイントの両方に適用されます。
SecureAnywhere の手動シャット ダウンを許可する	エンドポイントのシステムトレイメニューに終了コマンドを表示します。 このオプションの選択を解除すると、終了コマンドがメニューから削除 されます。 この設定は PC および Mac エンドポイントの両方に適用されます。
重要でない通知をバックグランドに	情報の提供のみを目的とするメッセージがシステムトレイに表示されないようにします。
表示する	この設定は PC エンドポイントにのみ適用されます。
警告メッセージを自動的にフェード アウトする	システムトレイの警告ダイアログを数秒で閉じます。このオプションを 無効にした場合、ユーザーがメッセージをクリックするまで警告が表 示されたままになります。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
実行履歴の詳細を保存する	[レポート] の実行履歴ログにデータを保存します。 この設定は PC エンドポイントにのみ適用されます。
ポーリング間隔	エンドポイントがアップデートを確認する頻度を指定します。例: 15 分、30 分、1 時間、2 時間。 この設定は PC および Mac エンドポイントの両方に適用されます。

# スキャンのスケジュール

Secure Anywhere は、インストールされた時刻とほぼ同じ時刻に毎日、自動的にスキャンを実行します。スキャンのスケジュールの設定を使用すると、スケジュールを変更して別の時間にスキャンを実行することができます。

設定	説明
スケジュール スキャンを有 効にする	エンドポイントでのスケジュールスキャンの実行を許可します。 この設定は PC および Mac エンドポイントの両方に適用されます。
スキャン頻度	スキャンを実行する頻度を指定します。曜日を設定するか、起動時のスキャンを選択することができます。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
時間	<ul> <li>スキャンを実行する時間を指定します。</li> <li>コンピュータの待機中のスキャン時間には、午前8:00前、正午前、午後5:00前、深夜0:00前のいずれかを指定できます。</li> <li>リソースが使用可能な場合のスキャン時間には、深夜0:00から午後11:00までの間の時刻を1時間単位で指定できます。to11:00 p.m.</li> <li>この設定はPCおよびMac エンドポイントの両方に適用されます。</li> </ul>
スケジュールされた時刻 にコンピュータの電源が 入っていない場合、起動 時にスキャンする	スケジュールした時刻にスキャンが実行されなかった場合は、ユーザーがコン ピュータの電源をオンにしてから1時間以内にスケジュールされたスキャンを実 行します。このオプションが無効になっていると、SecureAnywhere は実行され なかったスキャンを無視します。 この設定は PC および Mac エンドポイントの両方に適用されます。
スケジュール スキャン中 にスキャンの進行状況 ウィンドウを表示しない	スキャンをバックグラウンドで実行します。このオプションを無効にすると、ウィン ドウが開いてスキャンの進捗状況が表示されます。 この設定は PC エンドポイントにのみ適用されます。
スケジュール スキャン中 に感染が検出された場 合にのみ通知する	脅威が発見された場合にのみ警告を発します。このオプションを無効にする と、脅威が発見されたかどうかにかかわらず、スキャンの完了時に小さなス テータス ウィンド ウが開きます。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
バッテリ電源の場合はス ケジュール ス <del>キャ</del> ンを実 行しない	バッテリの電力を節約します。エンドポイントがバッテリを電源としている場合 に、スケジュールされたスキャンを実行するには、このオプションの選択を解除 します。 この設定は PC および Mac エンドポイントの両方に適用されます。
アプリケーションまたは ゲームをフル スクリーンで 実行中はスケジュールス キャンを実行しない	映画やゲームなど、全画面表示のアプリケーションをユーザーが利用している ときは、スケジュールされたスキャンを無視します。このような場合もスケジュー ルどおりにスキャンを実行するには、このオプションの選択を解除してください。 この設定は PC および Mac エンドポイントの両方に適用されます。
スケジュール スキャン時 間を最大 1 時間ランダム 化してスキャンを分散す る	使用可能なシステム リソースに応じてスキャンを実行するのに最適なタイミン グを判断し、予定時刻の1時間以内にスキャンを実行します。スケジュール した時刻にスキャンを強制的に実行する場合は、このオプションの選択を解 除してください。 この設定は PC エンドポイントにのみ適用されます。
ディープ スキャンではなく スケジュール クイック ス キャンを実行する	メモリのクイックスキャンを実行します。 すべての場所にあるあらゆるタイプのマ ルウェアに対して詳細なスキャンが実行されるように、 このオプションの選択は 解除したままにしておくことをお勧めします。 この設定は PC エンドポイントにのみ適用されます。

# スキャン設定

スキャン設定では、スキャンのパフォーマンスをより詳細に制御できます。

設定	説明
リアルタイムマスターブートレコード (MBR) ス <del>キャ</del> ンを有効にする	エンドポイントのマスターブートレコード (MBR) への感染を防ぎま す。 MBR が感染することによって、システムのコア領域に変更が加えら れ、それが OS の前に読み込まれてコンピュータを感染させる場合 があります。このオプションは選択したままにしておくことをお勧めしま す。この機能を選択していることによるスキャン時間の増加はわず かです。 この設定は PC エンドポイントにのみ適用されます。
拡張ル─トキット検出を有効化す る	ディスクや保護されたエリアに隠されたルートキットや他の悪意のあ るソフトウェアがないかチェックします。 スパイウェアの開発者は、検出や削除を避けるためにルートキット を使用する場合がよくあります。このオプションは選択したままにし ておくことをお勧めします。この機能を選択していることによるスキャ ン時間の増加はわずかです。 この設定は PC エンドポイントにのみ適用されます。
Windows エクスプロ <del>ーラー</del> での "右 クリック" スキャンを有効にする	Windows エクスプローラーでファイルやフォルダを右 クリックすると表示されるメニューから個 々 にスキャンを実行 するオプションを有効に します。 このオプションは、ユーザーがダウンロード 済みファイルをすばやくス キャンする場合に役立ちます。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
スキャンした個 々 のファイル名をス キャン時に表示する	各ファイルがスキャンされる度に表示されるファイル一覧がアップデートされます。 スキャンのパフォーマンスを少しでも向上させるには、このオプションの選択を解除すると、パネル上で1秒に1回のみファイル名がアッ プデートされるようになります。このオプションの選択を解除しても Secure Anywhere はすべてのファイルをスキャンしますが、各ファイル を画面に表示するための時間をかけずに済みます。 この設定は PC エンドポイントにのみ適用されます。
高速ス <del>キャ</del> ンよりも低メモリ使用量 を優先する	スキャン中に使用するメモリを減らすことにより、バックグラウンドでの RAMの使用量を削減します。ただし、スキャンの速度も若干遅く なります。 このオプションの選択を解除すると、スキャンの速度が上がり、より 多くのメモリが使用されます。 この設定は PC エンドポイントにのみ適用されます。
高速スキャンよりも低 CPU 使用量 を優先する	スキャン中の CPU 使用量を抑えます。ただし、スキャンの実行速度も若干遅くなります。 このオプションの選択を解除すると、スキャンの速度が上がります。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
非実行可能ファイルの詳細をスキャ ンログに保存する	スキャン ログにすべてのファイル データを保存します。結果としてロ グ ファイルのサイズが大幅に増加します。 実行可能ファイルの詳細のみをログに保存するには、このオプション の選択を解除したままにしてください。 この設定は PC エンドポイントにのみ適用されます。
新しいファイルを実行時にスキャン するときに [ファイルの認証中] ポップ アップを表示する	ユーザーがプログラムを初めて実行するときに、小さなダイアログを 表示します。ユーザーがこのダイアログを確認する必要がない場合 は、このオプションの選択を解除したままにしてください。 この設定は PC エンドポイントにのみ適用されます。
アーカイブ ファイルをスキャンする	zip、rar、cab、7-zip のアーカイブ中にある圧縮されたファイルをス キャンします。 この設定は PC および Mac エンドポイントの両方に適用されます。
クリーンアップ中にプロンプトで通知 することなく自動的に再起動する	マルウェアファイルの痕跡を完全に削除するためのクリーンアップを 実行した後に、コンピュータを再起動します。 この設定は PC エンドポイントにのみ適用されます。
マルウェアのクリーンアップ中に再起 動しない	マルウェア ファイルの痕跡を完全に削除するためのクリーンアップを 実行中に、エンドポイントが再起動しないようにします。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
<i>バックグラウンドのスキャ</i> ン中に検出 された脅威を自動的に削除する	エンドポイントのバックグラウンドで実行されているスキャン中に脅威 を削除して、隔離先に移動します。 この設定は PC エンドポイントにのみ適用されます。
学習スキャンで検出された脅威を 自動的に削除する	エンドポイントで実行されている最初のスキャン中に脅威を削除し て、隔離先に移動します。 この設定は PC エンドポイントにのみ適用されます。
高度な <del>サポー</del> トを有効にする	ウェブルート カスタマー サポート へのログの送信を許可します。 この設定は PC エンドポイントにのみ適用されます。
感染しているスキャン結果を表示 する	スキャン結果を表示します。有効でない場合、マルウェアが検出さ れてもエンドポイントにスキャン結果が表示されません。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
好ましくない動作をする可能性の あるアプリケーション (PUA) を悪意 のあるものとして検知する	<ul> <li>PUA を検出し、そのインストールをブロックします。</li> <li>望ましくない可能性のあるアプリケーション (PUA) とは、必ずしも悪意があるわけではないものの、アドウェアやツールバー、その他の望ましくないツールなどをシステムに追加するプログラムを指します。</li> <li>一般的に PUA は悪意があるものではありませんが、ビジネス環境での使用には不適切な場合があり、セキュリティ上の問題を引き起こす可能性があります。</li> <li>システム上に PUA がすでにインストールされている場合、Webroot Secure Anywhere はそのメインプログラムを検出しますが、すべてを完全に削除できない可能性があります。</li> <li>この設定は PC エンドポイントにのみ適用されます。</li> </ul>
ファイルを脅威リサーチに送信する ことを許可する	ウェブルートのシステムがまだ分類していない、悪意のある可能性 があるファイルを自動的にウェブルートにアップロードすることを許可 します。 この設定は PC エンドポイントにのみ適用されます。

# 自己保護の設定

自己保護は、悪意のあるソフトウェアがSecureAnywhere プログラムの設定やプロセスを変更できないようにします。別の製品がSecureAnywhereの機能に干渉しようとしていることが検出された場合、保護のためのスキャンを開始して脅威を探します。また、他のソフトウェアとの競合を避けるために、内部の自己保護の状態をアップデートします。

注意: SecureAnywhere に加えて別のセキュリティソフトウェアを使用する場合を除いて、自己保護の設定は[最大]にしておくことをお勧めします。他のセキュリティソフトウェアを併用する場合は、自己保

#### 護の設定を[中] または[最小]に調整してください。[最大]の設定では、他のセキュリティソフトウェア に干渉する場合があります。

設定	説明
自己保護応答のク ローキングを有効に する	自己保護をオンおよびオフにします。 この設定はPC エンドポイントにのみ適用されます。
自己保護のレベル	<ul> <li>以下の検出レベルに設定することができます。</li> <li>最小 - Secure Anywhere の設定とデータベースの整合性を保護します。エンドポイントが他のセキュリティ製品を複数インストールしている場合にお勧めします。</li> <li>中 - 他のプログラムが保護を無効にできないようにします。他のセキュリティソフトウェアとの互換性を可能な限り最大にします。</li> <li>最大 - Secure Anywhere のプロセスに対する保護を最高レベルにします。この設定を使用することをお勧めします。</li> <li>この設定は PC エンドポイントにのみ適用されます。</li> </ul>

### ヒューリスティック

ヒューリスティック設定では、管理されているエンドポイントのスキャン時に SecureAnywhere が実行する脅威 分析のレベルを調整できます。SecureAnywhere には、高度なヒューリスティック、経時ヒューリスティック、頻度 ヒューリスティックの3種類があります。

これらのヒューリスティックは、次のようなさまざまなエリアに対して設定できます。

- ローカルヒューリスティック ローカルドライブ
- USB ヒューリスティック USB ドライブ
- インターネットヒューリスティック インターネット

- **ネット ワークヒューリスティック** ネット ワーク
- CD/DVD ヒューリスティック- CD/DVD
- オフラインヒューリスティック オフライン時

各エリアに対して、以下のオプション設定が可能です。

- ヒューリスティックを無効化-ローカルドライブ、USBドライブ、インターネット、ネットワーク、CD/DVD、あるい はオフライン時の動作に対するヒューリスティック分析をオフにします。推奨しません。
- ・継時/頻度ヒューリスティックの前に高度なヒューリスティックを適用する ローカルドライブ、USBドライブ、インターネット、ネットワーク、CD/DVD、あるいはオフライン時に疑わしい動作がみられる場合に、新しいプログラムと古いプログラムに関して警告を発します。
- 継時/頻度ヒューリスティックの後に高度なヒューリスティックを適用する ローカルドライブ、USBドライブ、インターネット、ネットワーク、CD/DVD、あるいはオフライン時の動作に対する経時/頻度ヒューリスティックの 結果に基づいて、疑わしいプログラムに対して高度なヒューリスティックを適用します。
- ・正当と見なされていない新規プログラムを実行する場合に警告する ローカルドライブ、USBドライブ、インターネット、ネットワーク、CD/DVD、あるいはオフライン時に悪意のあるまたは不審なプログラム、あるいは 未知のプログラムの実行が試みられると警告を発します。この設定では、誤検出が発生する場合がありますので注意してください。

設定	説明
高度なヒューリス ティック	<ul> <li>新しいプログラムに関して、マルウェアによく見られる疑わしい動作がないか分析します。</li> <li>無効 - 高度なヒューリスティックがオフになり、新しい脅威に対して脆弱な状態となります。ただし、既知の脅威に対しては保護されます。</li> <li>低 - 非常に悪意のあるアクティビティを伴うプログラムを検出します。この設定は一部の疑わしい動作を無視し、ほとんどのプログラムの実行を許可します。</li> <li>中 - 情報を集約したコミュニティデータベースを元に微調整されたヒューリスティックを使用して、検出と誤検知のバランスをとります。</li> <li>高 - さまざまなレベルの新しい脅威から保護します。システムが感染している可能性や、非常に高いリスクにさらされているおそれがある場合は、この設定を使用してください。この設定では、誤検出が発生する場合があります。</li> <li>最大 - 新しい脅威に対して最高レベルの保護を行います。システムが感染している可能性や、非常に高いリスクにさらされているおそれがある場合は、この設定を使用してください。この設定では、誤検出が発生する場合があります。</li> </ul>

設定	説明
経時ヒューリスティッ ク	<ul> <li>コミュニティ内で使用された時間の長さに基づいて、新しいプログラムを分析します。正当なプログラムは、通常長期にわたってコミュニティで使用されますが、マルウェアの存在期間は短期である場合が一般的です。</li> <li>無効 - 経時ヒューリスティックがオフになり、新しい脅威に対して脆弱な状態となります。ただし、既知の脅威に対しては保護されます。</li> <li>低 - ごく最近に作成または変更されたプログラムを検出します。</li> <li>中 - 比較的新しい信頼されていないプログラムを検出し、ゼロデイ攻撃やゼロアワー攻撃を防止します。管理されているエンドポイントに一般的でないプログラムをインストールすることを許可せず、変異する脅威を防ぐために追加のセキュリティを必要とする場合に、この設定を使用することをお勧めします。</li> <li>高 - 比較的短期間のうちに作成または変更された、信頼されていないプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムに対して、誤検検出が多くなることがあります。</li> <li>最大 - ここ最近作成または変更された、信頼できないすべてのプログラムを検出します。この設定は、管理されているエンドポイントがリスクの高い状況にあるか、現在感染していると考えられる場合にのみ使用してください。</li> <li>この設定は PC エンドポイントにのみ適用されます。</li> </ul>

設定	説明
頻度ヒューリスティック	<ul> <li>コミュニティでの使用頻度や変更の頻度の統計に基づいて、新しいプログラムを分析します。正当なプログラムはすぐに変わることはありませんが、マルウェアは通常早いペースで変異します。マルウェアはそれぞれのコンピュータに固有のコピーとしてインストールされ、統計上は「非一般的」となることがあります。</li> <li>低 - 初めて確認されたプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムを検出し、ゼロデイ攻撃やゼロアワーウェア開発者である場合にお勧めします。</li> <li>中 - 変異している一般的でないプログラムを検出し、ゼロデイ攻撃やゼロアワー攻撃を防止します。この設定は、管理されているエンドポイントに新しいプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムを検出します。この設定は、管理されている上ディシーに新しいプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムを検出します。この設定は、管理されているエンドポイントが非常に高いリスクにあると考えられ、厳格なヒューリスティック規則のために誤検出を受信する可能性があることを受け入れる場合にお勧めします。</li> <li>この設定は PC エンドポイントにのみ適用されます。</li> </ul>

# リアルタイムシールドの設定

リアルタイムシールドは、ウェブルートの脅威の定義とコミュニティのデータベースにある既知の脅威をブロックします。シールドが疑わしいファイルを検出した場合、警告を発して、そのアイテムをブロックまたは許可するよう プロンプトを表示します。既知の脅威が検出された場合、エンドポイントに被害が及んだり情報が盗まれたり する前に、そのアイテムをただちにブロックして隔離します。

設定	説明
リアルタイム シールド 有	リアルタイムシールドをオンまたはオフにします。
効	この設定は PC および Mac エンドポイントの両方に適用されます。
SecureAnywhere の中	管理されているエンドポイントに小規模な脅威定義ファイルをダウンロードし、
央データベースに基づく	エンドポイントがオフラインのときにも保護します。
オフライン保護を有効に	この設定はオンのままにしておくことをお勧めします。
する	この設定は PC エンドポイントにのみ適用されます。
ブロックされたファイルに	ユーザーが警告に対してどのように対応したか (ファイルを許可したかブロックしたか)を記憶し、次回からは同じファイルを発見した場合にプロンプトを表示しません。
対するアクションを記憶	この設定の選択が解除されると、それ以降は、同じファイルが発見されるたびに警告が表示されます。
する	この設定は PC エンドポイントにのみ適用されます。
以前にブロックされたファ イルを自動的に隔離す る	脅威が発見された場合に警告を開き、ブロックし隔離先に移動するかの選択をユーザーに求めます。 この設定がオフの場合、ユーザーは手動でスキャンを実行して脅威を削除す る必要があります。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
実行時に検出された場 合ファイルを自動的にブ ロックする	脅威をブロックして、隔離先に移動します。 この設定がオフの場合、ユーザーは検出された脅威に関する警告に対応する 必要があります。 この設定は PC および Mac エンドポイントの両方に適用されます。
書き込みまたは変更時 にファイルをスキャンする	ディスクに保存された新しいファイルまたは変更されたファイルをすべてスキャン します。 この設定がオフの場合、新しいファイルのインストールは無視されます。ただ し、脅威が実行されようとしている場合はユーザーに警告が発せられます。 この設定は PC および Mac エンドポイントの両方に適用されます。
ログインしているユーザー がいない場合に自動的 に脅威をブロックする	管理されているエンドポイントがログオフしているときでも、脅威が実行されないようにします。脅威は通知なしに隔離先に移動させられます。 この設定は PC および Mac エンドポイントの両方に適用されます。
リアルタイム イベントの警 告を表示する	疑わしい動作があった場合に警告を発します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
リアルタイム ブロックの警 告を表示する	ヒューリスティックがマルウェアを検出したときに警告を表示し、アクションを許可 またはブロックするようユーザーに指示を求めます。 ヒューリスティックが [正当と見なされていない新規プログラムを実行する場合 に警告する] に設定されている場合は、この設定を [オン] にする必要がありま す。この設定を行わないと、ユーザーは警告を見ることができません。 この設定は PC エンドポイントにのみ適用されます。
リアルタイム ブロックのお 知らせを表示する	リアルタイムシールドがマルウェアを検出した場合、トレイに通知を表示しま す。この設定がオフの場合、トレイに通知は表示されませんが、マルウェアはブ ロックされ、脅威が検出されたことがホーム ページに示されます。 この設定は PC エンドポイントにのみ適用されます。

### 動作シールドの設定

動作シールドは、管理されているエンドポイント上で実行されるアプリケーションとプロセスを分析します。シー ルドが疑わしいファイルを検出した場合、警告を発して、そのアイテムをブロックまたは許可するようプロンプト を表示します。既知の脅威が検出された場合、管理対象のエンドポイントに被害が及んだり情報が盗まれ たりする前に、そのアイテムをただちにブロックして隔離します。

設定	説明
動作シールド有効	動作シールドをオンまたはオフにします。 この設定は PC エンドポイントにのみ適用されます。
新しいプログラムの実行を 許可する前に意図を評価 する	プログラムの実行を許可する前に、そのアクティビティを観察します。問題が ないようであれば、SecureAnywhere は実行を許可し、動作を監視し続け ます。 この設定は PC エンドポイントにのみ適用されます。
複合的な脅威を特定する ための高度な動作解釈を 有効にする	プログラムを分析し、その目的を調べます。 マルウェア プログラムの疑わしい アクティビティの例として、 レジストリエントリを変更して電子メールを送信す るなどの動作があります。 この設定は PC エンドポイントにのみ適用されます。
高度な脅威の削除を行う ため、信頼できないプログラ ムの動作を追跡する	正 当なソフト ウェアまたはマルウェアどちらにも分類されていないプログラムの 動作を監視します。 この設定は PC エンドポイントにのみ適用されます。
設定	説明
--------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------
警告メッセージを表示する のではなく推奨アクションを 自動的に実行	潜在的な脅威の許可またはブロックの選択について尋ねるプロンプトを ユーザーに表示しません。SecureAnywhere が、アイテムの管理方法を決 定します。 この設定は PC エンドポイントにのみ適用されます。
オフライン時、信頼できな いプログラムが低レベルのシ ステム変更を試行した場 合に警告する	管理対象のエンドポイントがオフラインの場合に、未分類のプログラムが変 更を加えようとすると、警告が表示されます。エンドポイントがインターネット に接続していないと、SecureAnywhere はオンラインの脅威データベースを チェックできません。 この設定は PC エンドポイントにのみ適用されます。

## コアシステムシールド

コアシステムシールドは、管理対象のエンドポイントのシステム構成を監視し、マルウェアによって改ざんされて いないか確認します。シールドが変更を試みようとする疑わしいファイルを検出した場合、警告を発してそのア イテムをブロックまたは許可するようプロンプトを表示します。既知の脅威が検出された場合、被害が及んだり 情報が盗まれたりする前に、そのアイテムをただちにブロックして隔離します。

設定	説明
コア システム シールド 有効	コアシステムシールドをオンまたはオフにします。 この設定は PC エンドポイントにのみ適用されます。
システム変更を実行する前 にシステム変更を評価する	新しいサービスのインストールなど、管理対象のエンドポイントに対してシス テムの変更を試みる、あらゆるアクティビティを阻止します。 この設定は PC エンドポイントにのみ適用されます。
破損したシステムコンポーネ ントを検出して修復する	壊れたレイヤードサービスプロバイダー (LSP) のチェーンやウイルスに感染し たファイルなど、破損したコンポーネントを検出し、コンポーネントやファイル を元の状態に復元します。 この設定は PC エンドポイントにのみ適用されます。
信頼できないプログラムが カーネルメモリを変更できな いようにする	未分類のプログラムがカーネルのメモリを変更しないように阻止します。 この設定はPC エンドポイントにのみ適用されます。
信頼できないプログラムがシ ステム プロセスを変更でき ないようにする	未分類のプログラムがシステムのプロセスを変更しないように阻止します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
LSP チェーンと他のシステム 構造の整合性を検証する	レイヤード サービス プロバイダー (LSP) のチェーンおよび他のシステム構造 がマルウェアの被害を受けないよう監視します。 この設定は PC エンドポイントにのみ適用されます。
どのプログラムも HOSTS ファイルを変更できないよう にする	HOSTS ファイルの Web サイトの IP アドレスを追加または変更しようとする スパイウェアを阻止し、変更をブロックまたは許可するようユーザーに警告を 表示します。 この設定は PC および Mac エンドポイントの両方に適用されます。

# Web 脅威シールド

Web 脅威シールドは、ユーザーがインターネットを閲覧中にエンドポイントを保護します。脅威となりうる Web サイトが検出された場合、警告が開き、そのサイトをブロックするか、あるいは警告を無視して続行する かをユーザーが決定できます。ユーザーが検索エンジンを利用するときに、検索結果ページのすべてのリンクを 分析し、信頼できるサイトであれば緑のチェックマークを、リスクとなり得るサイトであれば赤い X のマークをそれ ぞれのリンクの横に表示します。

設定	説明
Web シールドを有効化	Web 脅威シールドをオンまたはオフにします。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。
ブラウザのエクステンションをアク ティブ化	ブラウザエクステンションを使って、悪意のある Web サイトに対するブ ロック保護、リアルタイムのフィッシング対策保護、検索エンジンを使 用する際の安全評価を行います。各機能に対し、この表で説明す る個別のコントロールを使用することにより、各機能を別々に有効化 または無効化することができます。 エクステンションを完全に無効化し、サポートされる各ブラウザから削 除するには、この設定をオフに変更してください。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC エンドポイントにのみ適用されます。
悪意のある Web サイトをブロック	ブラウザに入力したすべての URL および IP はチェックされ、既知の 悪意があるサイトについてはブロック ページが表示されます。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
リアルタイム アンチフィッシングを有 効にする	ゼロデイフィッシングサイトから保護します。 ゼロデイ フィッシング サイト とは、これまで検出されたことがなく、関連のウイルスに定義 がまだな いサイトです。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。
検索エンジンを使用する際に安 全評価を表示する	検索結果にはアイコンとツールヒントの注釈が付き、悪意のあるサイトである確率が示されます。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。
Web フィルタリングドライバを有 効化	悪意のある接続に対してさらなる保護を提供し、場合によってはブ ラウザのエクステンションを無効化します。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
ブロックされた Web サイトをユー ザーが回避する機能を無効化	悪意のある Web サイトが検出された場合に表示されるブロックペー ジを、ユーザーが回避できないようにします。この設定はデフォルトで 選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。
ユーザーが Web サイトの評価をリ クエストする機能を無効化	悪意のある Web サイトが検出された場合に、ブロックページからユー ザーが Web サイトの評価を送信できないようにします。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。

### ID シールド

ID シールドは、オンライントランザクションを実行中に脅威にさらされる可能性のある重要なデータを保護します。ID シールドの動作を変更したり、ブロックする対象を制御したりできます。

設定	説明
ID シールド有効	ID シールドをオンまたはオフにします。 この設定は PC および Mac エンドポイントの両方に適用されます。 <b>注意:</b> Mac では、セキュアキーボード入力モードの設定を制御 します。
オンライン上の個人情報に対す る脅威を探す	ユーザーがインターネットを閲覧したり、リンクを開いたりする際に、 Web サイトを分析します。シールドが悪意のあるコンテンツを検出した 場合、そのサイトはブロックされ、警告が発せられます。 この設定は PC エンドポイントにのみ適用されます。
アクセス時に Web サイトを検証 して正当性を判別する	それぞれの Web サイトの IP アドレスを分析して、リダイレクトされた か、ブラックリストに記載されているかを判断します。 シールドが違法な Web サイトを検出した場合、サイトをブロックして警告を発します。 この設定は PC エンドポイントにのみ適用されます。
Web サイトの DNS/IP 解決を検 証して中間者攻撃を検出する	ユーザーを悪意のある Web サイトにリダイレクト (中間者攻撃など) す る可能性のあるサーバーを検索します。 シールドが中間者攻撃を検 出した場合、脅威をブロックして警告を発します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
Web サイトが危険度の高い追 跡情報を作成しないようブロック する	サードパーティの Cookie が悪意のある追跡型 Web サイトからのもの である場合、それらが管理対象のエンドポイントにインストールされる のをブロックします。 この設定は PC エンドポイントにのみ適用されます。
保護された認証情報にプログラ ムがアクセスできないようにする	プログラムがユーザーのログイン資格情報にアクセスしないようブロック します。たとえば、ユーザーが名前やパスワードを入力したり、Webサ イトでそのような情報を記憶するよう指定したりする際にブロックしま す。 この設定は PC エンドポイントにのみ適用されます。
信頼できないプログラムが保護さ れたデータにアクセスするのをブ ロックする前に警告する	マルウェアがデータにアクセスしようとしたときに、既知のマルウェアを自動的にブロックすることはせず、必ず警告を発します。 この設定は PC エンドポイントにのみ適用されます。
信頼された画面キャプチャ プロ グラムが保護された画面の内容 にアクセスすることを許可	画面に表示されているコンテンツに関係なく、正当なスクリーン キャプ チャ プログラムを使用できるようにします。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
ID シールド対応モードを有効に する	通常処理で ID シールド がブロックする可能性のある特定のアプリケー ションの実行を許可します。このオプションは、Secure Anywhere がエン ドポイントにインストールされた後でアプリケーションの機能に問題があ る場合に有効化することができます。この対応モードが有効化されて いても、エンドポイントは ID シールドのコア機能により保護されていま す。 この設定は PC エンドポイントにのみ適用されます。
非 <del>ラテ</del> ン語のシステム上でキーロ <i>ギ</i> ング保護機能を有効にする	日本語や中国語など非ラテン語のシステムを使用するエンドポイント を、キーロガーから保護します。 この設定は PC エンドポイントにのみ適用されます。

# ファイアウォール

ウェブルートのファイアウォールは、エンドポイントのポートから出ていくデータトラフィックを監視します。インター ネットに接続して個人情報を盗もうとする、信頼できないプロセスを探します。一方で、Windows ファイア ウォールは、管理対象のエンドポイントに入力されるデータトラフィックを監視します。ウェブルートとWindows のファイアウォールをどちらも有効にしておけば、ネットワークデータの出入口を完全に保護することができます。

ウェブルートのファイアウォールは、管理対象のエンドポイント上のトラフィックをフィルタリングするよう設定されて います。通常のアクティビティを中断することなく、バックグラウンドで動作します。ファイアウォールが判別できな いトラフィックを検出した場合には、警告を発します。その際には、そのトラフィックをブロックするか許可するか を決定します。 ウェブルートエンドポイントプロテクション管理者ガイド

設定	説明
有効	ファイアウォールのオン / オフを切り替えます。 この設定は PC エンドポイントにのみ適用されます。
ファイアウォール のレベル	<ul> <li>デフォルトで許可 - 明示的にブロックされている場合を除き、すべてのプロセスにインターネットへの接続を許可します。</li> <li>不明および感染している場合に警告 - 新しい信頼できないプロセスがインターネットに接続する場合やエンドポイントが感染している場合に警告します。</li> <li>不明の場合に警告 - 新しい信頼できないプロセスがインターネットに接続する場合に警告します。</li> <li>デフォルトでブロック - 明示的にブロックされている場合を除き、すべてのプロセスがインターネットに接続する際に警告します。</li> <li>この設定は PC エンドポイントにのみ適用されます。</li> </ul>

設定	説明
ファイアウォール 管理の警告を 表示する	Windows ファイアウォールがオフになっている場合に Secure Anywhere により表示される 警告を制御します。 ・ オン - Secure Anywhere によって Windows ファイアウォールがオフであることが検出さ れると警告が表示されます。 ・ オフ - Windows ファイアウォールがオフになっていても警告は表示されません。 この設定は PC エンドポイントにのみ適用されます。
ファイアウォール プロセスの警告 を表示する	ファイアウォールの警告を制御します。この設定がオフの場合、ファイアウォールの警告 は表示されません。このオプションはファイアウォールのレベルの設定と連携して機能し ます。 例: • [ファイアウォール プロセスの警告を表示する] と[デフォルトでブロック] のオプションが 両方ともオンに設定されている場合、新しいプロセスが接続を試みると、エンドポイ ントのユーザーに警告が表示されます。 • [ファイアウォールプロセスの警告を表示する] がオフに設定されている場合は、エンド ポイントのユーザーに警告は表示されず、プロセスは許可されます。 この設定は PC エンドポイントにのみ適用されます。

## ユーザーインターフェイス

このポリシーを使用するエンドポイント上で、SecureAnywhereのインターフェイスを管理制御できます。

設定	説明
GUI	エンドポイントのユーザーによる Secure Anywhere メインインターフェイスへのアクセスを ブロックまたは許可します。 このオプションが [非表示] に設定されている場合にユーザーが Secure Anywhere を 開こうとすると、インターフェイスにアクセスするには管理者に問い合わせるよう案内 するメッセージが表示されます。 この設定は PC および Mac エンドポイントの両方に適用されます。 注意: このオプションでも PC のシステムトレイのウェブルートのアイコンは非表 示になりません。ただし、Mac ではこのアイコンが非表示になります。

# システム最適化ツール

システム最適化ツールは、エンドユーザーのウェブの閲覧履歴、コンピュータ使用状況についてのファイル、貴重なディスク容量を消費する不要なファイル(ごみ箱内のファイルや Windows の一時ファイルなど)を削除します。システム最適化ツールは自動的には実行されません。最適化をスケジュールし、削除するアイテムを選択する必要があります。

**注意:** 最適化によって削除されるのは不要なファイルと痕跡です。マルウェアの脅威は除去されません。マルウェアはスキャン中に削除されます。システム最適化ツールはコンピュータの掃除係、スキャンは警備係であると考えることができます。

設定	説明
システム最適化ツールを 集中管理	管理者はシステム最適化ツールの設定を以下のように変更することができま す。 ・ オン - システム最適化ツールの設定はパネルに表示され、設定の変更が 可能です。 ・ オフ - このパネルに設定は表示されません。 この設定は PC エンドポイントにのみ適用されます。
スケジュール	
曜日での設定	システム最適化ツールを自動的に実行する曜日を1から7までで設定します。 す。 この設定はPCエンドポイントにのみ適用されます。
指定時間での実行 - 時	エンドポイントでシステム最適化ツールを実行する時刻を設定します。 この設定は PC エンドポイントにのみ適用されます。
指定時間での実行 - 分	エンドポイントでシステム最適化ツールを実行する時刻を15分単位で設定します。 この設定はPC エンドポイントにのみ適用されます。

設定	説明						
スケジュールされた時刻に コンピュータの電源がオフ の場合は、起動時にス キャンする	エンドポイントを起動した際に、スケジュールどおりに実行されなかったクリー ンアップを実行します。これは、クリーンアップをスケジュールした時刻にエンド ポイントがオフであった場合にのみ実行されます。これを設定しない場合、 実行されなかったクリーンアップはスキップされます。 この設定は PC エンドポイントにのみ適用されます。						
Windows エクスプロ <del>ーラー</del> の右クリックで安全なファイ ル消去を有効にする	エンドポイントで、ファイルまたはフォルダを完全に削除するオプションを Windows エクスプローラーに追加します。ファイルまたはフォルダを右クリック ると、次のメニューアイテムが表示されます。						
Windows デスクトップ							
ごみ箱	Windows エクスプローラーのごみ箱からすべてのファイルを削除します。 この設定は PC エンドポイントにのみ適用されます。						

設定	説明
最近使 <i>った</i> ドキュメント履 歴	Windows の [スタート] メニューからアクセス可能な、最近開いたファイルの履 歴をクリアします。 クリーンアップでは実際のファイルは削除されません。 この設定は PC エンドポイントにのみ適用されます。
スタート メニューのクリック 履歴	エンドユーザーが[スタート] メニューを使用して最近開いたプログラムのショー トカットの履歴をクリアします。 この設定は PC エンドポイントにのみ適用されます。
実行履歴	[スタート] メニューからアクセス可能な [ファイル名を指定して実行] ダイアロ グに最近入力したコマンドの履歴をクリアします。 [ファイル名を指定して実行] ダイアログからアイテムを完全に削除するには、 クリーンアップ後にコンピュータを再起動しなければならない場合があります。 この設定は PC エンドポイントにのみ適用されます。
検索履歴	エンドユーザーがコンピュータで検索したファイルやその他の情報の履歴をクリ アします。 検索履歴が保存されていると、エンドユーザーが新しい検索の入力を開始 した際に、同じ文字で始まる最近の検索が表示されます。クリーンアップで は実際のファイルは削除されません。 この設定は PC エンドポイントにのみ適用されます。

設定	説明					
スタート メニューの並べ替 え履歴	[スタート] メニューのプログラムとドキュメントのリストを、デフォルトの設定でるアルファベット順に戻します。 クリーンアップの実行後、システムを再起動すると、一覧がアルファベット順戻ります。 この設定は PC エンドポイントにのみ適用されます。					
Windows システム						
クリップボードの内容	Windows のすべてのプログラムでは、コピーまたは切り取りの機能を使用す るとデータがクリップボードに保管されます。このクリップボードの内容をクリアし ます。 この設定は PC エンドポイントにのみ適用されます。					
Windows 一時フォルダ	Windows 一時フォルダにあるすべてのファイルとフォルダを削除します (現在 開いているプログラムで使用中のファイルは削除されません)。 通常このフォルダは C:\Windows\Temp です。 この設定は PC エンドポイントにのみ適用されます。					

設定	説明
システムー 時 フォルダ	システムー時フォルダにあるすべてのファイルとフォルダを削除します(現在開 いているプログラムで使用中のファイルは削除されません)。 通常このフォルダは C:\Documents and Settings\[username]\Local Settings\Temp にあります。 この設定は PC エンドポイントにのみ適用されます。
Windows Update 一時 フォルダ	このフォルダにあるすべてのファイルとフォルダを削除します (現在開いている プログラムで使用中のファイルは削除されません)。 これらのファイルは、Windows Update の実行時に Windows によって使用さ れます。これらのファイルは通常 C:\Windows\Software\Distribution\Download にあります。 この設定は PC エンドポイントにのみ適用されます。
Windows レジストリスト リーム	Windows レジストリに対して最近行った変更の履歴をクリアします。 このオプションは、レジストリへの変更そのものを削除するものではありません。 この設定は PC エンドポイントにのみ適用されます。

設定	説明						
デフォルト ログオン ユー ザー履歴	コンピュータへの前回のログオンで使用された名前を保存する Windows レジ ストリエントリを削除します。 このレジストリエントリを削除すると、コンピュータの電源を入れたとき、または コンピュータを再起動したときに、毎回ユーザー名を入力する必要がありま す。このクリーンアップオプションは、デフォルトの "ようこそ" 画面を使用するコ ンピュータには影響しません。 この設定は PC エンドポイントにのみ適用されます。						
メモリ ダンプ ファイル	特定のWindows エラーが発生した際に作成されるメモリダンプファイル (memory.dmp)を削除します。このファイルには、エラーの発生時に起きた事 柄に関する情報が保存されています。 この設定は PC エンドポイントにのみ適用されます。						
CD 書き込みストレージ フォルダ	Windows に内蔵の機能を使用して CD にファイルをコピーした際に作成される Windows プロジェクトファイルを削除します。通常、これらのプロジェクトファイルは次のいずれかのディレクトリに保存されています。 C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\CDBurning または C:\Users\[username]\AppData\Local\Microsoft\Windows\Burn\Burn この設定は PC エンドポイントにのみ適用されます。						

設定	説明					
Flash cookie	Adobe Flash によって作成されたデータを削除します。これらのデータはコ ザー設定などを追跡しているため、プライバシーの問題につながる可能作 あります。 Flash Cookie は実際には Cookie ではなく、ブラウザの Cookie のプライバ 制御では制御されません。 この設定は PC エンドポイントにのみ適用されます。					
Internet Explorer						
アドレスバー履歴	Internet Explorer のオートコンプリート機能の一部として保管される、最近表示した Web サイトのリストを削除します。 このリストは、Internet Explorer ブラウザの上部にあるアドレスバーの右側の 矢印をクリックすると、ドロップダウンリストとして表示されます。 この設定は PC エンドポイントにのみ適用されます。					
Cookie	エンドポイントからすべての Cookie を削除します。 すべての Cookie ファイルを 削除した場合、エンドユーザーは Cookie に保存されているパスワードや ショッピングカートの内容などを再入力しなければならない点に注意してくだ さい。 この設定は PC エンドポイントにのみ適用されます。					

設定	説明						
ー時インターネット ファイ ル	エンド ユーザーが最近閲覧した Web ページのキャッシュされたコピーを削除 します。 Web ページをキャッシュするとページを素早く表示できるためパフォーマンスが 向上しますが、ハードドライブで大量の領域が消費されることもあります。 この設定は PC エンドポイントにのみ適用されます。						
URL 履歴	Internet Explorer のツールバーで表示される最近訪問した Web サイトの履歴のリストを削除します。 この設定は PC エンドポイントにのみ適用されます。						
ログの設定	Internet Explorer のアップデート中に作成されたログファイルを削除します。 この設定は PC エンドポイントにのみ適用されます。						
Microsoft ダウンロード フォルダ	Internet Explorer を使用して前回のダウンロード済みファイルを保存している フォルダのコンテンツを削除します。 この設定は PC エンドポイントにのみ適用されます。						
MediaPlayer バー履歴	Internet Explorer でメディアプレーヤーを使用して最近開いたオーディオファイ ルとビデオファイルの一覧を削除します。 クリーンアップでは、 ファイルのそのも のは削除されません。 この設定は PC エンドポイントにのみ適用されます。						

設定	説明
オートコンプリート フォーム 情報	エンド ユーザーが Web サイトのフィールドに情報を入力した際に Internet Explorer によって保存されたデータを削除します。 これは Internet Explorer のオートコンプリート機能の一部です。 この設定は PC エンドポイントにのみ適用されます。
Index.dat の消去 (再起 動時に消去)	index.dat ファイル内のファイルを削除対象としてマークし、システムの再起動 後にこれらのファイルをクリアします。 index.dat ファイルは、Web アドレス、検索クエリ、および最近開いたファイルを 記録する Windows リポジトリで、随時情報が追加されていきます。このオプ ションは、Cookie、一時インターネットファイル、URL 履歴のうち 1 つ以上を 選択している場合に機能します。Index.dat はアクティブなデータベースのよう に機能します。このファイルがクリーンアップされるのは Windows を再起動し た後のみです。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
安全なファイル削除	
ファイルの削除時に適用 するセキュリティのレベルを 制御する	ファイルをランダムな文字で上書きする "ワイププロセス" を使用して、ファイル を完全に削除します。このワイプ プロセスを利用すれば、誰かが復元ツール を使用してエンドポイントのファイルの内容を見るおそれもありません。 デフォルトでは、ファイル削除は [標準] に設定されており、アイテムはごみ箱 には入らず永久に削除されます。ただし、この [標準] 設定で削除されたファ イルは、データ復元ユーティリティにより復元できる場合があります。 ファイルを確実に復元できないようにするには、[最大] を選択します。[中] ではファイルが3回上書きされ、[最大] では7回上書きされて、ファイルの 周辺の領域がクリーンアップされます。なお、[中] または [最大] を選択する と、クリーンアップにかかる時間が長くなることに注意してください。 この設定は PC エンドポイントにのみ適用されます。

# ポリシーに割り当てられたエンドポイントの表示

[ポリシー] タブで、ポリシーに割り当てられたエンドポイントを簡単に確認できます。

#### ポリシーに割り当てられたエンドポイントを表示するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.						
Home Endpoint Protection	Support					
Status Policies Group Managem	ent Reports	Overrides	Alerts	Settings	Logs	Resources
🛄 Status	🔍 🔜 E	Endpoints enco	untering t	threats (last	7 days)	
We recommend you check whether this endpoint has automatic remediation enal on the assigned policy.	n bled					

2. [ポリシー] タブをクリックします。

Secure Anywhere.						
Home Endpoint Protection	Support					
Status Policies Group Manage	ement Reports	Overrides Ale	erts Settings Logs	Resources		
E Status	< 🖳 En	idpoints encounte	ring threats (last 7 days)			
We recommend you check whether the endpoint has automatic remediation error on the assigned policy.	tion nis nabled					

### [ポリシー] タブが表示されます。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts S	Settings Logs Resources
Policies	
😳 Create   😑 Delete   📺 Rename   🛅 Copy   🖂 Set as Default   🛃 Import	Export
Policy Name 🔺	Policy Description
e Add Policy Copy with Draft	Add Policy Copy with Draft 1
e Add Policy Rename	Add Policy Description Renamed
ALEndpointPolicy	For Ali & Leo tests.
Copied from non dns policy June	Copied from non dns policy June
e Hotfix policy	Policy test for Hot fix
Import Live New Policy	Import Live New Policy

3. [ポリシー名] カラムで、エンドポイントの情報を表示するポリシーを選択します。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources
Policies	
😳 Create   😑 Delete   📺 Rename   🛅 Copy   🖂 Set as Default   🛃 Import	Export
Policy Name	Policy Description
AdminPolicy	AdminPolicy
All shields off	To disable shield for troubleshooting
default but gui on	default but gui on
Hide Gui	Only setting change from default is H
Mac	Mac
ReartUl	Rec+UI
C Recommended Defaults	Recommended setup with protection
Recommended Server Deraults	Recommended setup for servers, pro
Silent Audit	Non-remediating Security Audit with

グループとエンドポイントのエリアに、選択したポリシーを使用するグループが表示されます。

-		
Home Endpoint Protection Support		
Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources	
Policies		
🕽 Create   🤤 Delete   🃺 Rename   🛅 Copy   🕞 Set as Default   🛃 Impo	rt   📑 Export	
Policy Name	Policy Description	
AdminPolicy	AdminPolicy	
Recommended Defaults	Recommended setup with protection and remediation	
Recommended Server Defaults	Recommended setup for servers, protection enabled	
Silent Audit	Non-remediating Security Audit with limited protection en	abled
Groups and endpoints using Recommended Defaults		
🖥 Save Changes   늘 Undo Changes   🌄 Move all endpoints on this policy to a	nother policy   📕 View all endpoints using this policy	
Group Name	Number of endpoints	Description
	2 \6ee	Default Oroug

- 4. エンドポイントに関する情報を表示するには、次のいずれかの操作を行います。
  - コマンドバーの [ このポリシーを使用するすべてのエンドポイントを表示]をクリックします。

Groups and endpoints using Recommended Defaults		
🔚 Save Changes   🖕 Undo Changes   🌄 Move all endpoints on this policy to another policy 🖳 View	all endpoints using this policy	
Group Name	Number of endpoints	Description
Default Group	3 View	Default Group

・グループの行で [表示] リンクを選択します。

1 Groups and endpoints using Recommended Defaults			
🔚 Save Changes   늘 Undo Changes   🌄 Move all endpoints on this policy to another policy   🖳 View all endpoints using this policy			
Group Name	Number of endpoints	Description	
Default Group	3 View	Default Group	

[推奨デフォルト設定を使用するすべてのエンドポイント] ウィンドウが表示されます。

	I endpoints using Recommend	ed Defaults			
	Hostname	Group	Status	Last Seen	
1	QADENWSAQA455-DAD90	Default Group	🔶 Not Seen Recently	Jul 20th 2016, 15:48	
2	QADENWSAQA607	Default Group	🔶 Not Seen Recently	Feb 13th 2017, 17:23	
3	QADENWSAQA623	Default Group	📀 Not Seen Recently	Feb 14th 2017, 18:40	

- 5. 必要に応じて、任意のカラム見出しをクリックし、次のいずれか、または両方の操作を行います。
  - 次のいずれかを選択し、カラムを並べ替えます。
    - ・昇順に並べ替え
    - 降順に並べ替え

- 🔜 A	Recommended Defaults					
	Hostname 🔺	•	Group	Status	Last Seen	
1	QADENWSAQA455-DAD90F47	A J	Sort Ascending	🚯 Not Seen Recently	Jul 20th 2016, 15:48	
2	QADENWSAQA607	z	Sort Descending	🔶 Not Seen Recently	Feb 13th 2017, 17:23	
3	QADENWSAQA623	A	, con contraining	📀 Not Seen Recently	Feb 14th 2017, 18:40	
			Columns 🕨			

- [カラム]を選択し、次のいずれかの操作を行います。
  - 表示するカラムのチェックボックスを選択する。

IA 🧔	All endpoints using Recommended Defaults				
	Hostname 🔺	Group		Status	
1	QADENWSAQA455-DAD90F47	A/Z↓ Sort Ascending		Not Seen Recently	
2	QADENWSAQA607	Z Sort Descending		🔶 Not Seen Recently	
3	QADENWSAQA623			Not Seen Recently	
		Columns	Group		
			Status		
			First Seen		
			✓ Last Seen		
			Last Threat		
			Agent Version		
			Keycode		
			Operating Syste	em	
			Device MID		
			Instance MID		
			VM		
			Agent Languag	e	
			IP Address		
	iew all endpoints using this policy		Internal IP Addr	ress	
·	iew all enupoints using this policy		MAC Address		
	Number of endpoints		Active Directory	Domain	
	5 VIEW		Active Directory	OU	
			Workgroup		
			Current User		

• 非表示にするカラムのチェックボックスの選択を解除する。

カラム内のデータの詳細については、「<u>表とレポートのデータの並べ替えページ45」を参照してください。</u>

# ポリシー間でのエンドポイントの移動

[ポリシー] タブで、1 つのポリシーに割り当てられたエンドポイントをすべて別のポリシーに移動することができます。

**注意:** 個 々 のエンドポイントをポリシーに移動する手順については、「エンドポイントのグループへのポリ シーの適用 ページ324」を参照してください。

#### エンドポイントをポリシー間で移動するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.			
Home Endpoint Protection Suppo	vrt		
Status Policies Group Management R	eports Overrides Alerts Settings Logs Resources		
E Status	Redpoints encountering threats (last 7 days)		
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.			

2. [ポリシー] タブをクリックします。

Secure Anywhere.	
Home Endpoint Protection Supp	ort
Status Policies Group Management	Reports Overrides Alerts Settings Logs Resources
🔄 Status 🔍	🖳 Endpoints encountering threats (last 7 days)
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	

### [ポリシー] タブが表示されます。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports Overrides Alerts S	Settings Logs Resources
Policies	
😳 Create   😑 Delete   📺 Rename   🛅 Copy   🗅 Set as Default   🛃 Import	Export
Policy Name 🔺	Policy Description
Add Policy Copy with Draft	Add Policy Copy with Draft 1
e Add Policy Rename	Add Policy Description Renamed
ALEndpointPolicy	For Ali & Leo tests.
Copied from non dns policy June	Copied from non dns policy June
e Hotfix policy	Policy test for Hot fix
Import Live New Policy	Import Live New Policy

3. [ポリシー名] カラムから移動するポリシーを選択します。

Secure Anywhere.				
Home Endpoint Protection Support				
Status Policies Group Management Reports Overrides Alerts S	Settings Logs Resources			
Policies				
😲 Create   😑 Delete   🏣 Rename   🛅 Copy   🖂 Set as Default   🛃 Import	Export			
Policy Name	Policy Description			
AdminPolicy	AdminPolicy			
All shields off	To disable shield for troubleshooting			
default but gui on	default but gui on			
Hide Gui	Only setting change from default is Hide GUI			
Mac	Mac			
new policy	This is a test			
Rec+UI	Rec+UI			
Recommended Defaults	Recommended setup with protection and remediation			
Recommended Server Defaults	Recommended setup for servers, protection enabled			

#### 下のパネルに、このポリシーを使用するグループが一覧表示されます。

St	atus	Policies	Group Management	Reports	Overrides	Alerts	Settings	Logs	Resources		
	Policies										
G	Create	🛛 😑 Delet	e   📺 Rename   🛅 C	opy   🗅 Se	t as Default	E Import	📑 Ехро	Export			
	Policy	Name					Policy De	scription		Date Created	
AdminPolicy							AdminPo	licy		Jul 6th 2017, 21:32	
All shields off					To disable shield for troubleshooting		ing Feb 27th 2012, 22:0	9			
	default but gui on					default but gui on		Aug 9th 2012, 22:57	Aug 9th 2012, 22:57		
	Hide Gui					Only setti	Only setting change from default is Hide GUI		is Hide GUI May 18th 2012, 18:4	5	
Mac					Mac		Jan 12th 2017, 19:0	Jan 12th 2017, 19:08			
Rec+UI					Rec+UI		Apr 14th 2015, 18:23	8			
Recommended Defaults							Recomm	Recommended setup with protection and remediation			
	Recommended Server Defaults						Recommended setup for servers, protection enabled				
	Silent Audit					Non-reme	Non-remediating Security Audit with limited protection enabled				
	test					test May 18th 2012, 22:25		25			
6	Groups and endpoints using test										
	🖕 🔚 Save Changes   🍃 Undo Changes   🌄 Move all endpoints on this policy to another policy   🚽 View all endpoints using this policy										
Gro	Group Name						Number	of endpoints	Description		
Det	Default Group						1 View		Default Group		

4. [このポリシーのすべてのエンドポイントを別のポリシーに移動]ボタンをクリックします。

Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources					
Policies						
🚱 Create   😑 Delete   🏝 Rename   🛅 Copy   🖂 Set as Default   🖓 Import	Export					
Policy Name	Policy Description	Date Created				
AdminPolicy	AdminPolicy	Jul 6th 2017, 21:32				
All shields off	To disable shield for troubleshooting	Feb 27th 2012, 22:09				
default but gui on	default but gui on	Aug 9th 2012, 22:57				
Hide Gui	Only setting change from default is Hide GUI	May 18th 2012, 18:45				
Mac	Mac	Jan 12th 2017, 19:08				
Rec+UI	Rec+UI	Apr 14th 2015, 18:28				
Recommended Defaults	Recommended setup with protection and remediation					
Recommended Server Defaults	Recommended setup for servers, protection enabled					
Silent Audit	Non-remediating Security Audit with limited protection enabled					
test	test	May 18th 2012, 22:25				
1 Groups and endpoints using test						
🔚 Save Changes   🔄 Undo Changes 🎑 Move all endpoints on this policy to anot	her policy 📕 View all endpoints using this policy					
Group Name	Number of endpoints	Description				
Default Group	1 View	Default Group				

[すべてのエンドポイントを別のポリシーに移動] ウィンドウが表示されます。

Move all endpo	ints to another policy	
Policy:		~
	Canal Canal	
	Save Cancel	

5. [ポリシー]ドロップダウンメニューのポリシーの一覧から、エンドポイントの移動先ポリシーを選択します。

Move all end	dpoints to another policy
Policy:	~
	AdminPolicy
	All shields off
	default but gui on
	Hide Gui
	Mac
	Rec+UI
	Recommended Defaults
	Recommended Server Defaults
	Silent Audit

[ポリシー名] フィールドに、選択したポリシーの名前が反映されます。

Policy:	test2		~

6. 保存] ボタンをクリックします。

Move all er	ndpoints to another policy	
Policy:	test2	~
	Save Cancel	

^{7.}ポリシーのリストで、新しいエンドポイントが変更した割り当てに表示されていることを確認します。

詳細については、「ポリシーに割り当てられたエンドポイントの表示ページ301」を参照してください。

# ポリシーの削除

デフォルトのポリシーを除くすべてのポリシーを削除することができます。ポリシーを削除するとアクティブなポリ シーのリストから削除され、削除したポリシーのリストに移されます。削除したポリシーはレポートログで確認で きます。

**注意**:ポリシーを削除した場合、同じポリシー名を再び使用することはできません。また、削除したポリシーを復元することはできません。ただし、コピーして名前を変更することは可能です。

#### ポリシーを削除するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.					
Home Endpoint Protection Suppo	prt				
Status Policies Group Management F	Reports Overrides Alerts Settings Logs Resources				
🔤 Status 🔍	Redpoints encountering threats (last 7 days)				
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.					

2. [**ポリシー**]タブをクリックします。.

Seci	Secure Anywhere.					
Home	Endpoint Protection Support					
Status	Policies Group Management Reports Overrides Alerts Settings Logs Resources					
🖳 Status	< 🖳 Endpoints encountering threats (last 7 days)					
We recomendpoint he on the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation enabled igned policy.					

### [ポリシー] タブが表示されます。

Secure Anywhere.						
Home Endpoint Protection Support						
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
Policies						
😳 Create   😑 Delete   📺 Rename   🛅 Copy   🖂 Set as Default   🛃 Import	Export					
Policy Name 🔺	Policy Description					
e Add Policy Copy with Draft	Add Policy Copy with Draft 1					
e Add Policy Rename	Add Policy Description Renamed					
ALEndpointPolicy	For Ali & Leo tests.					
Copied from non dns policy June	Copied from non dns policy June					
e Hotfix policy	Policy test for Hot fix					
Import Live New Policy	Import Live New Policy					

3. [ポリシー名] カラムから削除するポリシーを選択します。

Secure Anywhere.					
Home Endpoint Protection Support					
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources					
Policies					
🔂 Create   😑 Delete   🚛 Rename   🛅 Copy   🕞 Set as Default   🖓 Import   📑 Export					
Policy Name	Policy Description				
AdminPolicy	AdminPolicy				
All shields off	To disable shield for troubleshooting				
default but gui on	default but gui on				
Hide Gui	Only setting change from default is Hide GUI				
Mac	Mac				
new policy	This is a test				
Rec+UI	Rec+UI				
Recommended Defaults	Recommended setup with protection and remediation				
Recommended Server Defaults	Recommended setup for servers, protection enabled				

[削除] ボタンがアクティブになります。
4. [削除] ボタンをクリックします。

Secure Anywhere.							
Home Endpoint Protection Support							
Status Policies Group Management Reports Overrides Alerts	Settings Logs Resources						
Policies							
😌 Create 📔 🖨 Delete 📔 🗁 Rename   🛅 Copy   🖂 Set as Default   😓 Import	Export						
Policy Name	Policy Description						
AdminPolicy	AdminPolicy						
All shields off	To disable shield for troubleshooting						
default but gui on	default but gui on						
Hide Gui	Only setting change from default is Hide GUI						
Mac	Mac						
new policy	This is a test						
Rec+UI	Rec+UI						
Recommended Defaults	Recommended setup with protection and remediation						
Recommended Server Defaults	Recommended setup for servers, protection enabled						

#### [ポリシーを削除] ウィンドウが表示されます。

Delete P	olicy	×
?	Are you sure you wish to delete "new policy"?	
	Yes No	

5. [はい] ボタンをクリックします。



[代替ポリシー] ウィンドウが表示されます。

this policy is elect a new p	currently used by any groups or endpoints, pleas plicy to replace this:	e
olicy:		*

6. [ポリシー] ドロップダウンメニューから、前のポリシーが関連付けられていたグループまたはエンドポイントと 関連付ける新しいポリシーを選択します。

Replacement P	olicy	
If this policy i select a new	s currently used by any groups or endpoints, plea policy to replace this:	ase
Policy:		~
	AdminPolicy	<b>A</b>
	All shields off	
	default but gui on	
anageu	Hide Gui	
	Rec+UI	
	Recommended Defaults	
	Recommended Server Defaults	

7. [保存] ボタンをクリックします。

Replacement Po	licy							
If this policy is currently used by any groups or endpoints, please select a new policy to replace this:								
Policy:	Policy: v							
Save Cancel								

削除したポリシーは、削除したポリシーのリストに移動されます。

Replacemen	t Policy	
If this pol ⁱ select a r	Connecting	
Policy:	Retrieving Data	
l		

8. 削除されたポリシーを表示するには、[ポリシー] タブの右上隅にある [削除したポリシーを表示] チェック ボックスを選択します。

	ă E ?
(	Show Deleted Policies
Draft Changes	

削除したポリシーはグレー表示されます。

	ă 8 ?
Show	v Deleted Policies
	Deleted
	Deleted
	Deleted

# 第7章:グループの管理

グループの管理方法については、以下のトピックを参照してください。

新規グループの追加	
グループの名前の変更	
エンドポイントのグループへのポリシーの適用	
エンドポイントのグループへのポリシーの適用	
単一のエンドポイントへのポリシーの適用	
グループ間 でのエンドポイントの移動	
エンドポイントをグループに整理	
ビュー内の [アクティブディレクトリ] タブの使用	
ビュー内の [IP 範囲] タブの使用	
ビュー内の [ワークグループ] タブの使用	
グループの削除	

### 新規グループの追加

初めてエンドポイントに Secure Anywhere を配備する際は、エンドポイントプロテクションによってすべてデフォルトのグループに割り当てられます。必要な場合は、異なる管理目的ごとにグループを追加し、この新しく追加されたグループにエンドポイントを再割り当てすることもできます。

#### グループを作成するには

- 1. [**グループの管理**] タブをクリックします。
- 2. コマンドバーの[作成]アイコンをクリックします。

Home Endpoint Pr	otection	Mobile	Prote	ctio	n			20	013
Status Policies Gro	up Managei	ment D	Report	s	Alerts Over	rides	Logs	Resource	s
Groups Views		<b>«</b>	📙 E	ndp	oints in Default	Grou	р		
🔂 Create ) 🖨 Delete   📋	Rename		<b>S</b>	ave (	Changes   🖕 U	ndo Ch	anges   🌄	Move en	dpo
Group Name	No.				Hostname		Policy	Status	Fi
All Endpoints	16		1		W7VM_SE_KH1		Unmana	<b>@</b>	М
Deactivated Endpoints	19		2		WEBROOT-0K.		Unmana	•	A
Default Group	8		з		WEBROOT-0		Unmana	🔶	Ju

3. 表示される [グループを作成] ダイアログで、グループ名と説明を入力し、[グループを作成] ボタンをクリックします。

Create Group		
Group Name: Description:		
Policy:	No Group Policy	~
	Save Cancel	

左側の[グループ]パネルに新しいグループが表示されます。

- 4. この新しいグループにエンドポイントを移動するには、エンドポイントが現在割り当てられているグループ をクリックします。
- 5. 右側の[エンドポイント]パネルで1つ以上のエンドポイントを選択します。

**注意:** リストの一番上にある [**ホスト名**] チェックボックスをクリックすると、指定したグループ内の すべてのエンドポイントを選択することができます。

6. コマンドバーの[エンドポイントを別のグループに移動]ボタンをクリックします。

Groups Views	*	🖳 Endpoints in Default Group							
😌 Create   😑 Delete   🏥 Rename		🔚 Sav	ve Changes   늘 Uno	do Ch	ange 🗌 🌄 I	Move end	dpoints to and	other group	Apply policy to endpoints
Group Name No.			Hostname		Policy	Status	First Seen	Last S	Last Infected
All Endpoints 16			W7VM_SE_KH1		Unmana	📎	Mar 9th	Aug 15	Aug 15th 2013, 19:38
Deactivated Endpoints 19		:	✓ WEBROOT-0K		Unmana	٠٠. 🚯	Aug 5th	Aug 14	
Default Group 8			VEBROOT-0		Unmana	٠ 🚯	Jul 24th	Jul 24t	

[エンドポイントをどのグループに移動しますか?]ウィンドウが表示されます。

Nove endpoints	to which group?	
Group:		*
	Save Cancel	

7. [グループ] ドロップダウンメニューで新しいグループを選択し、[保存] ボタンをクリックします。

Move endpo	pints to which group?	
Group:		¥
	Save Cancel	

これで、ポリシーをグループ全体または個々のエンドポイントに適用できるようになりました。詳細については、「エンドポイントのグループへのポリシーの適用ページ324エンドポイントのグループへのポリシーの適用」を参照してください。

### グループの名前の変更

[グループの管理] タブでは、リストにあるグループの名前を簡単に変更できます。名前を変更したグループのエンドポイントはそのままグループ内に残ります。エンドポイントを移動する必要はありません。

#### グループの名前を変更するには

- 1. エンドポイントのコンソールで [グループの管理] タブをクリックします。
- 2. 左のパネルで、名前を変更するグループを選択します。



3. [アクション] ドロップダウンメニューの [グループの編集] を選択します。

Secure Anywhere.									
Home	Endpoint Protection	Mobile	e Protectio						
Status	Policies Group Manager	nent F	leports						
Groups	Views Search	≪ ⊅	📕 Endpo						
🔂 Create	Actions -		Save C						
Group Nam	Edit Group								
All Endpoint	s 🤤 Delete Group		1						
Deactivated	Deploy Endpoints to t	his Group	2						
Default Grou	up 4								
Bracknell	1								
Broomfield	2								
Dublin	1								

#### [グループの編集] ウィンドウが表示されます。

roup Name:	Broomfield						
escription:	Laptops in Broomfield						
olicy:	No Group Policy	¥					

- 4. [グループ名] フィールドに新しいグループ名を入力します。
- 5. 設定が完了したら[保存]ボタンをクリックします。

Group Name:	Broomfield								
Description:	Laptops in Broomfield								
Policy:	No Group Policy	*							

### エンドポイントのグループへのポリシーの適用

すべてのエンドポイントはまず、デフォルトのポリシーに割り当てられます。ポリシーの割り当てを変更するには、 新しいポリシーを定義してから、以下の手順に従ってそのポリシーをグループに適用する必要があります。詳 細については、「ポリシーの導入ページ222」を参照してください。

このトピックでは、次の手順について説明します。

- エンドポイントのグループへのポリシーの適用
- 単一のエンドポイントへのポリシーの適用

#### エンドポイントのグループへのポリシーの適用

[グループの管理] タブで、複数のエンドポイントにポリシーを適用することができます。

#### エンドポイントのグループにポリシーを適用するには

- 1. [グループの管理] タブをクリックします。
- 2. 左側の[グループ]パネルで、必要なエンドポイントを含むグループを選択します。

Home Endpoint P	rotection	Mobile	Protecti	ion						
Status Policies Gro	oup Manag	ement	Reports	Alerts	Overri	ides Logs	Resou	rces		
Groups Views		**		Endpoints						
🔂 Create   🖨 Delete   🖞	Rename		Save	e Changes   💡	🖢 Un	ido Changes	🌄 Move	endpoints to another	group   📙 Apply policy	to endpoints   📢 Age
Group Name	No.			Hostname		Policy	Group	Status	First Seen	Last Seen
All Endpoints	16		1	DAL-TS		Recomm	Remot	🐠 Not Seen Re	Aug 19th 2011, 13:24	Jun 27th 2013, 00
Deactivated Endpoints	19		2	FHAL-3		No Rem	Broom	Infected	Jul 12th 2013, 19:41	Aug 23rd 2013, 14
Default Group	8		3	VMXP3		Unmana	Remot	🐠 Not Seen Re	Apr 11th 2013, 18:54	Jun 20th 2013, 17
			4	] W7VM		Unmana	Defaul	Protected	Mar 9th 2012, 17:50	Aug 15th 2013, 21
			5	WEBRO		Unmana	Defaul	Not Seen Re	Aug 5th 2013, 16:13	Aug 14th 2013, 16

3. 右側の[エンドポイント]パネルで1つ以上のエンドポイントを選択します。

**注意:** リストの一番上にある [ホスト名] チェックボックスをクリックすると、指定したグループ内の すべてのエンドポイントを選択することができます。 4. コマンドバーの [ポリシーをエンドポイントに適用] ボタンをクリックします。

**注意**: グループのエンドポイントが1ページ以上ある場合は、ポリシーの適用対象が現在のページのエンドポイントか、全ページのエンドポイントかを、ダイアログで尋ねられます。

Status Policies Group	p Management	Report	s	Alerts Overrides	Logs F	lesource	s		
Groups Views	*		ndpo	oints in Default Gro	up				
🔂 Create   😑 Delete   🚛 Rename			ave (	Changes   뉠 Undo (	Changes   🌄	Move end	lpoints to and	other group	Apply policy to endpoints
Group Name	No.		V	Hostname	Policy	Status	First Seen	Last S	Last Infected
All Endpoints	16	1		W7VM_SE_KH1	Unmana	<b>@</b>	Mar 9th	Aug 15	Aug 15th 2013, 19:38
Deactivated Endpoints	19	2		WEBROOT-0K	Unmana	٠٠. 🕁	Aug 5th	Aug 14	
Default Group	8	3	☑	WEBROOT-0	Unmana	•	Jul 24th	Jul 24t	

[ポリシーを適用] ウィンドウが表示されます。

oly Policy		
Policy:		~
	Apply Cancel	

5. [ポリシー]ドロップダウンメニューでグループの新しいポリシーを選択し、[適用 button.

Apply Policy		
Policy:		*
	Apply Cancel	

^{6.} [ポリシー] カラムで、新しいポリシーが選択したエンドポイントに適用されていることを確認します。

単一のエンドポイントへのポリシーの適用

1 つのエンドポイントだけにポリシーを適用するには、[ポリシー] カラムをダブルクリックして変更を加える 方法が最も簡単です。

個々のエンドポイントにポリシーを適用するには

- 1. [**グループの管理**] タブをクリックします。
- 2. 左側の[グループ]パネルで、該当するエンドポイントを含むグループを選択します。
- 3. 右側の[エンドポイント]パネルでエンドポイントを選択します。

Home Endpoint P	Protection	Mobile	Protectio	on						
Status Policies Gr	oup Managem	ent	Reports	Alerts 0	verrides	Logs	Resources			
Groups Views		≪ ¢	📕 Endp	oints in Def	ault Group					
🔂 Create   🖨 Delete   🖞	Rename		🔚 Save Changes   🔄 Undo Changes   🌄 Move endpoints to another group   📴 Apply policy to endpoints							
Group Name	No.			Hostname	Policy	,	Status	First Seen	Last Seen	Last Infec
All Endpoints	16			W7VM_S	Unma	naged	📀 Protec	Mar 9th 012, 17:50	Aug 15th 2013,	Aug 15th
Deactivated Endpoints	19		2 🗖	WEBROO	Unma	naged	Double-Click	to Edit th 2013, 16	Aug 14th 2013,	
Default Group	8		3	WEDDOO	- Home	anged 1	Viet C	1012 Jul 2013, 20:55	Jul 24th 2013, 2	
			4	WEBROO	Unma	naged	Protec	Aug 5th 2013 14	Aug 22nd 2013	

4. 選択されたエンドポイントの[ポリシー] カラムでポリシー名をダブルクリックすると、使用可能なポリ シーのドロップダウンが表示されます。

Home Endpoint Prot	ection Mobile	Protec	ctio	n						
Status Policies Group	Management	Reports		Alerts Over	rride	es Logs	Resources			
Groups Views 🔍 🛊 Endpoints in Default Group										
😌 Create   🤤 Delete   📺 R	lename	🔚 Sa	ve (	Changes   술 U	Indo	o Changes   💂	Move endpo	ints to another group	Apply policy to	endpoints
Group Name	No.			Hostname	ſ	Policy	itatus	First Seen	Last Seen	Last Infec
All Endpoints	16	1	<b>V</b>	W7VM_S		Unmanag 🗸 🤇	Protec	Mar 9th 2012, 17:50	Aug 15th 2013,	Aug 15th
Deactivated Endpoints	19	2		WEBROO		Unmanaged 🤞	Not S	Aug 5th 2013, 16	Aug 14th 2013,	
Default Group	8	3		WEBROO	L	Unmanaged 🤞	Not S	Jul 24th 2013, 20:55	Jul 24th 2013, 2	

5. ポリシーを選択して Enter キーを押します。

</br>

</br>

</br>

</br>

</td

6. 変更を適用するには、[変更を保存]ボタンをクリックします。

Save	ndpoints Changes 🔄 Undo (	Changes   🌄 Move e	ndpoints to
	Hostname	Policy	Group
19 🔽	BILLXP01	Policy1	Default
20 📃	BILLXP_WSA	Recommended	Default

行の赤いフラグが消えます。

### グループ間でのエンドポイントの移動

このセクションの説明に従うと、エンドポイントを別のグループに移動することができます。個々のエンドポイント またはエンドポイントのグループ全体の移動が可能です。

グループ間でエンドポイントを移動するには

- 1. [**グループの管理**] タブをクリックします。
- 2. 左側の[グループ]パネルで、移動するエンドポイントを含むグループを選択します。

**注意:** この手順では、[すべてのエンドポイント] ではなく特定のグループを選択する必要があります。

3. 右側の[エンドポイント]パネルで1つ以上のエンドポイントを選択します。

**注意:** リストの一番上にある [ホスト名] チェックボックスを選択すると、指定したグループ内のすべてのエンドポイントを選択することができます。

4. コマンドバーの [エンドポイントを別のグループに移動] アイコンをクリックします。

**注意**: グループのエンドポイントが1ページ以上ある場合は、ポリシーの適用対象が現在のページのエンドポイントか、全ページのエンドポイントかを、ダイアログで尋ねられます。

Groups Views	< #		📑 Endpoints in Default Group							
🕒 Create   😑 Delete   🏥 Ren	ame	<b>_</b> S	ave (	Changes   🚖 Und	lo Ch	ange 🔰 🜄 I	Move end	dpoints to and	other group	Apply policy to endpoints
Group Name N	0.			Hostname		Policy	Status	First Seen	Last S	Last Infected
All Endpoints 1	6			W7VM_SE_KH1		Unmana	🥥	Mar 9th	Aug 15	Aug 15th 2013, 19:38
Deactivated Endpoints 1	9	1		WEBROOT-0K		Unmana	٠٠. 🚯	Aug 5th	Aug 14	
Default Group 8		4		WEBROOT-0		Unmana	۰۰. 🔶	Jul 24th	Jul 24t	

[エンドポイントをどのグループに移動しますか?]ウィンドウが表示されます。

love endpo	bints to which group?	
Group:		¥
	Save Cancel	

5. [グループ]ドロップダウン矢印でグループを選択し、[保存]ボタンをクリックします。

Move endpo	ints to which group?		
Group:			*
	Save	Cancel	

6. 左側のパネルで選択したグループをクリックします。エンドポイントがすべて、右側の[エンドポイント]パ ネルに表示されることを確認してください。 ウェブルートエンドポイントプロテクション管理者ガイド

### エンドポイントをグループに整理

エンドポイントに SecureAnywhere をインストールする際、対象のエンドポイントは自動的にデフォルトのポリ シーとグループに割り当てられます。グループはエンドポイントをひとまとめにした単位であり、デバイスを整理し やすくして管理を助けるものです。

エンドポイントが最初のスキャンの実行後に管理ポータルへの報告を行ったら、それらのエンドポイントを別のグ ループに移動することができます。たとえば、スキャン時間のスケジュールを統一して指定できるよう、タイム ゾーン別にエンドポイントを整理することも可能です。

**注意:** グループを完全に管理するには、[グループ]の[作成・編集]、[グループ]の[エンドポイントの 非アクティブ化 / 再アクティブ化]、[グループ]の[グループへのエンドポイントの割り当て] へのアクセス権 限が必要です。詳細については、「<u>コンソールユーザーの権限設定 ページ75</u>」を参照してください。

#### エンドポイントをグループに整理するには

- 1. [グループの管理] タブですべてのグループを表示できます。
- 2. 左側の [グループ] パネルでグループを選択すると、関連するエンドポイントとポリシーが右側に表示されます。

エンドポイントは上に、ポリシーは下に表示されます。

Status	Policies	Group Management	Reports	Alerts	Override	s Logs	Resources	s				
Groups	Views	« \$	📑 Endpoints in Default Group									
😌 Create	😳 Create   😄 Delete   📺 Rename 🔚 Save Changes   🔄 Undo Changes   🌄 Move endpoints to another group   📃 Apply policy to endpoints   🛒 Agent Commands-								gent Commands -			
Group Nar	ne	No.		Hostnan	ne	Policy	Status	First Seen	Last S	Last Infected		Agent Version
All Endpoi	nts	16	1	W7VM_	SE_KH1	Unmana	. 🥝	Mar 9th	Aug 15	Aug 15th 2013, 1	19:38	8.0.2.167
Deactivate	ed Endpoints	s 19	2	WEBRO	от-ок	Unmana	. 🐠	Aug 5th	Aug 14			8.0.2.167
Default Gr	oup	8	3 📃	WEBRO	от-о	Unmana	. 🐠	Jul 24th	Jul 24t			8.0.2.155
			4	WEBRO	OT-34	Unmana	. 🥝	Aug 5th	Aug 22			8.0.2.167
			5	WEBRO	от-7	Unmana	. 🔶	Jul 24th	Jul 24t			8.0.2.155
			R T	WEBRO	от-ул	Unmana	4	lul 30th	lul 30t			8 0 2 155
			E Polic	ies used	l in Default	Group						
	🔚 Save Changes   🖕 Undo Changes											
			Policy Na	ime			Endpo	ints using this	s policy		Policy Description	
			Unmanag	jed			7				This policy is for all f	PCs that are user mai
			US_Rem	ote_Policy			1				Demonstration Policy	r

**注意:** サイレントインストール中にコマンドラインで /groupname スイッチを使用していない限り、エンドポ イントはすべてデフォルトのグループに割り当てられます。詳細については、「エンドポイントへの SecureAnywhere の配備ページ112」を参照してください。

#### グループの追加作成とエンドポイントの移動の手順

- 1.1つ以上の新規グループの追加 「新規グループの追加ページ319」を参照してください。
- 2. 新しく作成した別のグループへのエンドポイントの移動 「<u>グループ間でのエンドポイントの移動 ページ</u> <u>328</u>」を参照してください。
- 3. 新しいエンドポイントのグループへのポリシーの割り当て 「エンドポイントのグループへのポリシーの適用 ページ324」を参照してください。

## ビュー内の [アクティブディレクトリ] タブの使用

Secure Anywhere をエンドポイントにインストールする際、エージェントは初回のスキャンを実行してエンドポイントの状態の報告と情報の収集を行い、管理ポータルで識別できるようにします。エンドポイントから管理コンソールに報告が返されると、エージェントによって収集されたデータが[グループの管理]の[ビュー] タブに表示されるようになります。

詳細については、「<u>ビュー内の[IP 範囲] タブの使用 ページ334</u>」および「<u>ビュー内の[ワークグループ] タブの使</u> <u>用 ページ336</u>」を参照してください。

管理ポータルで Active Directory のリストを表示するには

- 1. [**グループの管理**] タブをクリックします。
- 2. 左側のパネルで [ビュー] タブをクリックし、[アクティブディレクトリ] タブをクリックします。

Status Policies Group Management	Report	s	Alerts Overrides Logs	Resources			
Groups Views K	Endpoints under Computers						
Active Directory IP Workgroup	S S	ave	Changes   🖕 Undo Changes	Apply policy to endpoints			
Endpoints with no AD information (426)			Hostname	Policy			
<ul> <li>boulder.webroot.com (458)</li> <li>ABC (15)</li> <li>DEF (216)</li> </ul>			TEST-MACHINE-1	Webroot Default Policy with De			
			TEST-MACHINE-2	Webroot Default Policy with De			
			TEST-MACHINE-3	Webroot Default Policy with De			
Computers (216)	4		TEST-MACHINE-4	Webroot Default Policy with D			
Computers Default (15)	-			reprotection and the start of t			
🖽 🧰 GHI (1)	5		TEST-MACHINE-5	Webroot Default Policy with De			
🙂 🧰 JKL (1)	6		TEST-MACHINE-6	Webroot Default Policy with D			
🕀 🦳 MNO(53)	7		TEST-MACHINE-7	Webroot Default Policy with D			

3. このタブで、Active Directory 別にエンドポイントを確認できます。カラム内のデータの詳細については、 「<u>表とレポートのデータの並べ替えページ45</u>」を参照してください。

**注意:** このリストに含まれているエンドポイントは、エージェントが最新のスキャンで収集したデー タをもとに整理されているため、移動できません。以後のスキャンで異なるデータが検出される と、この情報は変わります。

4. また、一覧のエンドポイントに対してコマンドを送信してポリシーを変更することも可能です。これらの変 更は、個々のエンドポイントまたはページにのみ送ることができ、ビュー全体に適用することはできませ  $\mathcal{h}_{\circ}$ 

**注意:** リストの一番上にある [ホスト名] チェックボックスを選択すると、指定したビュー内のページ上にあるすべてのエンドポイントを選択することができます。

[ビュー] タブでは、グループに対してコマンドを送信して割り当てられたポリシーを変更することはできません。この場合は、[グループ] タブを使用します。詳細については、「エンドポイントへのコマンドの発行ページ144」および「エンドポイントのグループへのポリシーの適用 ページ324」を参照してください。

## ビュー内の [IP 範囲] タブの使用

SecureAnywhere をエンドポイントにインストールする際、エージェントは初回のスキャンを実行してエンドポイントの状態の報告と情報の収集を行い、管理ポータルで識別できるようにします。エンドポイントから管理コンソールに報告が返されると、エージェントによって収集されたデータが[グループの管理]の[ビュー] タブに表示 されるようになります。

詳細については、「<u>ビュー内の[アクティブディレクトリ] タブの使用 ページ332</u>」および「ビュー内の[ワークグルー プ] タブの使用 ページ336」を参照してください。

#### 管理ポータルで IP 範囲リストを表示するには

- 1. [グループの管理] タブをクリックします。
- 2. 左側のパネルで [ビュー] タブをクリックし、[IP 範囲] タブをクリックします。



3. このタブで、IP 範囲別にエンドポイントを確認できます。カラム内のデータの詳細については、「<u>表とレ</u> <u>ポートのデータの並べ替えページ45</u>」を参照してください。

**注意:** このリストに含まれているエンドポイントは、エージェントが最新のスキャンで収集したデー タをもとに整理されているため、移動できません。以後のスキャンで異なるデータが検出される と、この情報は変わります。

また、一覧のエンドポイントに対してコマンドを送信してポリシーを変更することも可能です。これらの変更は、個々のエンドポイントまたはページにのみ送ることができ、ビュー全体に適用することはできません。

**注意:** リストの一番上にある [**ホスト名**] チェックボックスを選択すると、指定したビュー内のページ上にあるすべてのエンドポイントを選択することができます。

[ビュー] タブでは、グループに対してコマンドを送信して割り当てられたポリシーを変更することはできま せん。この場合は、[グループ] タブを使用します。詳細については、「エンドポイントへのコマンドの発行 ページ144」および「エンドポイントのグループへのポリシーの適用 ページ324」を参照してください。

## ビュー内の [ワークグループ] タブの使用

Secure Anywhere をエンドポイントにインストールする際、エージェントは初回のスキャンを実行してエンドポイントの状態の報告と情報の収集を行い、管理ポータルで識別できるようにします。エンドポイントから管理コンソールに報告が返されると、エージェントによって収集されたデータが[グループの管理]の[ビュー] タブに表示されるようになります。

詳細については、「ビュー内の[IP 範囲] タブの使用 ページ334」および「ビュー内の[ワークグループ] タブの使 用」を参照してください。

管理ポータルでワークグループのリストを表示するには

- 1. [**グループの管理**] タブをクリックします。
- 2. 左側のパネルで [ビュー] タブをクリックし、[ワークグループ] タブをクリックします。

Status Policies Group Management	Reports Aler	ts Overrides Logs	Resources
Groups Views «	Endpoints	under WORKGROUP	
Active Directory IP Workgroup	🔚 Save Chan	ges   🔄 Undo Changes	Apply policy to endpoints
Endpoints with no Workgroup information (	E Hos	tname	Policy
BOULDER (506)	1 🔲 TES	T-MACHINE-1	Webroot Default Policy with D
	2 📃 TES	T-MACHINE-2	Webroot Default Policy with D
	3 🗐 TES	T-MACHINE-3	Webroot Default Policy with D
	4 🕅 TES	T-MACHINE-4	Webroot Default Policy with D
Deactivated (149)	5 🕅 TES	T-MACHINE-5	Webroot Default Policy with D
*	6 🔲 TES	T-MACHINE-6	Webroot Default Policy with D
	7 🔲 TES	T-MACHINE-7	Webroot Default Policy with D

3. このタブで、ワークグループ別にエンドポイントを確認できます。カラム内のデータの詳細については、「<u>表</u> <u>とレポートのデータの並べ替えページ45</u>」を参照してください。

**注意:** このリストに含まれているエンドポイントは、エージェントが最新のスキャンで収集したデータをもとに整理されているため、移動できません。以後のスキャンで異なるデータが検出されると、この情報は変わります。

4. また、一覧のエンドポイントに対してコマンドを送信してポリシーを変更することも可能です。これらの変 更は、個々のエンドポイントまたはページにのみ送ることができ、ビュー全体に適用することはできませ  $\mathcal{h}_{\circ}$ 

**注意:** リストの一番上にある [ホスト名] チェックボックスを選択すると、指定したビュー内のページ上にあるすべてのエンドポイントを選択することができます。

[ビュー] タブでは、グループに対してコマンドを送信して割り当てられたポリシーを変更することはできません。この場合は、[グループ] タブを使用します。詳細については、「エンドポイントへのコマンドの発行ページ144」および「エンドポイントのグループへのポリシーの適用ページ324」を参照してください。

### グループの削除

[グループの管理] タブでは、リストにあるグループを簡単に削除したり、エンドポイントを別のグループに移動したりできます。

削除したグループを復元することはできません。ただし、削除されたグループの名前を再利用することは可能 です。

グループを削除するには

- 1. [グループの管理] タブをクリックします。
- 2. [グループ名] カラムで、削除するグループを選択します。
- 3. コマンドバーの [削除 icon.



4. プロンプトが表示されたら[はい]ボタンをクリックします。

エンドポイントがこのグループに割り当てられている場合は、別のウィンドウが表示され、エンドポイントの移動先のグループを選択するよう求められます。

5. 移動先のグループを選択し、[保存]ボタンをクリックします。

# 第8章:レポートの操作

レポートの操作方法については、以下のトピックを参照してください。

エンドポイントプロテクションのレポートの生成	
[確認されたすべての脅威] レポートの生成	
確認されたすべての未判定のソフトウェア  レポートの生成	
[ブロックされたすべての URL] レポートの生成	
[最新のスキャンで脅威が存在したエンドポイント] レポートの生成	
[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートの生成	
[脅威の履歴 (日単位)] レポートの生成	
[脅威の履歴 (内訳)] レポートの生成	
[ブロックされた URL の履歴 (日単位)] レポートの生成	
[エージェントのバージョンの使用状況] レポートの生成	
[インストールされたエージェント] レポートの生成	
レポートのスプレッドシートのダウンロード	

## エンドポイントプロテクションのレポートの生成

エンドポイントプロテクションでは、SecureAnywhereのバージョンとエンドポイントにおける脅威のアクティビティに 関する詳細なレポートを表示できます。次の表に、ビジネス上のニーズ別に生成が推奨されるレポートの種類を示します。

目的	使用するレポート
異なる SecureAnywhere のバージョン がインストールされているエンドポイント を特定する	<i>[エージェントのバージョンの使用状況] レポートの生成 ページ</i> <u>390</u>
SecureAnywhere ソフトウェアが新しく インストールされたエンドポイントを特 定する	<i>[インストールされたエージェント] レポートの生成 ページ395</i>
検出された脅威を特定して管理する	<u>[確認されたすべての脅威] レポートの生成 ページ342</u> または <u>[最新のスキャンで脅威が存在したエンドポイント] レポートの生</u> <u>成 ページ361</u>
未判定と分類されたファイルを特定す る	[確認されたすべての未判定のソフトウェア]レポートの生成ペー ジ349 または [最新のスキャンで未判定のソフトウェアが検出されたエンドポイ ント] レポートの生成ページ365

目的	使用するレポート
検出された脅威の概要を表示する	[脅威の履歴 (内訳)] レポートの生成 ページ377
検出された脅威の概要を日単位で 表示する	[脅威の履歴 (日単位)] レポートの生成 ページ369

## [確認されたすべての脅威] レポートの生成

検出された脅威を特定して管理するには、[確認されたすべての脅威] レポートを生成します。このレポートに は脅威がファイル名で一覧表示され、SecureAnywhere がその脅威を検出した時刻と場所が表示されます。 脅威が繰り返し検出された場合、または複数の場所で検出された場合は、エントリが重複して表示されるこ とがあります。このレポートから、ファイルのオーバーライドの作成や、隔離されたファイルの復元を実行できま す。レポートのデータは次の手順で変更できます。

- 選択したポリシーまたはグループ内で検出された脅威をすべて表示する。特定のエンドポイントのセットに 検索結果を絞り込む場合に便利です。
- ドリルダウンして日付範囲内で検出された脅威を確認する。特定の期間に検索結果を絞り込む場合に 便利です。

[確認されたすべての脅威] レポートを生成するには

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで [確認されたすべての脅威]を選択します。

Secure Anywhere.						
Home Endpoint Protection						
Status Policies Group Management Reports						
Select your report						
Report Type:						
All Threats Seen						
Policy:						
All						
Group:						
All						
Select time period						
Include deactivated and hidden						
Submit						

3. 必要に応じて、特定のポリシーとグループを選択します。この選択を行わない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。

Secure Anywhere.
Home Endpoint Protection
Status Policies Group Management Reports
Select your report
Report Type:
All Threats Seen
Policy:
All
Group:
All
Select time period
Include deactivated and hidden
Submit

4. データの期間を入力するには、[期間を選択] チェックボックスを選択します。この手順はオプションです。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management	Reports
Select your report	
Report Type:	
All Threats Seen 👻	
Policy:	
All	
Group:	
All	
Select time period	
Include deactivated and hidden	
Submit	

5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[非アク ティブ化および非表示を含む] チェックボックスを選択します。この手順はオプションです。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management	Reports
Select your report	
Report Type:	
Policy:	
All	
Group:	
All	
Select time period	
Include deactivated and hidden	
Submit	

6. [送信] ボタンをクリックします。

Secure Anywhere.
Home Endpoint Protection
Status Policies Group Management Reports
Select your report
Report Type:
All Threats Seen
Policy:
All
Group:
All
Select time period
Include deactivated and hidden
Submit

右側のパネルにレポートが開きます。各脅威がファイル名で一覧表示され、SecureAnywhere がその脅威を検出し削除した場所と時刻が表示されます。

R	lepo	orts	Alerts Overrides Logs Reso	purces	
	All	Thre	ats Seen (Apr 23 15:33)		
Ę	3 4	II TR	nreats Seen		
1	¢c	reate	e override 🔄 Restore from Quarantine		
			Filename	Pathname	File Size
	1		SYSTAM.EXE	%desktop%\trojans\trojan-backdoor-p	15,360
	2		SVHOST32.EXE	%desktop%\trojans\trojan-sohanad\	182,672
	3		6TO4SVCN.EXE	%desktop%\trojans\trojan-buzus\	46,080
	4		CALC32.EXE	%desktop%\trojans\trojan-downloader	42,242
	5		CSRS154.EXE	%desktop%\trojans\trojan-phisher-net	789,936

- 7. このパネルで、必要に応じて次のいずれかの操作を行います。
  - オーバーライドの作成 エンドポイントプロテクションを回避してファイルを [正当] (ファイルの実行を許可) または [不正] (ファイルを検出して隔離) に指定するには、コマンドバーの [オーバーライドの作成] アイコンをクリックします。詳細については、「レポートからのファイルへのオーバーライドの適用」を参照してください。
  - 隔離先から復元する ファイルが安全で、エンドポイントの元の場所に復元する場合は、コマンド バーの[隔離先から復元する]をクリックします。
- レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。詳細については、「表とレポートのデータの並べ替えページ45」を参照してください。
- 9. レポートのスプレッドシートをダウンロードするには、「 <u>レポートのスプレッドシートのダウンロード ページ</u> <u>402</u>」を参照してください。

## [確認されたすべての未判定のソフトウェア] レポートの生成

SecureAnywhere は、正当なファイルのように見えても動作が疑わしいファイルを検出することがあります。この場合、そのファイルは [未判定] に分類されます。

SecureAnywhere が [未判定] と分類したファイルを特定するには、[確認されたすべての未判定のソフトウェ ア] レポートを生成します。[確認されたすべての未判定のソフトウェア] レポートには、SecureAnywhere が安 全であるかマルウェアであるかを判定できないすべての未判定のソフトウェア (一般的に実行可能ファイル) が 表示されます。

このレポートにはアイテムがファイル名で一覧表示され、SecureAnywhere がその脅威を検出した時刻と場所 が表示されます。未判定のソフトウェアが繰り返し検出された場合、または複数の場所で検出された場合 は、レポートにエントリが重複して表示されることがあります。また、このレポートを使用してオーバーライドを作 成し、ファイルに[正当]または[不正]のタグを付け、SecureAnywhere に今後の分類方法を指定することが できます。

**注意:**未判定のソフトウェアが最後に検出されたエンドポイントを表示する方法の詳細については、 「*[最新のスキャンで脅威が存在したエンドポイント] レポートの生成ページ361」を参照してください。* 

このレポートでは、レポートデータを次のように変更できます。

- 選択したポリシーやグループ内のすべての未判定のソフトウェアを表示する。特定のエンドポイントのセット に検索結果を絞り込む場合に便利です。
- ドリルダウンして特定の期間内に検出されたファイルを確認する。特定の期間に検索結果を絞り込む場合に便利です。

[確認されたすべての未判定のソフトウェア] レポートを生成するには

ウェブルートエンドポイントプロテクション管理者ガイド

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで[確認されたすべての未判定のソフトウェア]を選択します。

Secure Anywhere.					
Home Endpoint Protection					
Status Policies Group Management Reports					
Select your report					
Report Type:					
All Undetermined Software Seen					
Policy:					
All 🗸					
Group:					
All					
Select time period					
Include deactivated and hidden					
Submit					

3. 必要に応じて、特定のポリシーとグループを選択します。この選択を行わない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。
| Secure Anywhere.                               |         |
|------------------------------------------------|---------|
| Home Endpoint Protection                       |         |
| Status Policies Group Management               | Reports |
| Select your report                             |         |
| Report Type:<br>All Undetermined Software Seen |         |
| Policy:                                        |         |
| All                                            |         |
| Group:                                         |         |
| All                                            |         |
| Select time period                             |         |
| Include deactivated and hidden                 |         |
| Submit                                         |         |

4. データの期間を入力するには、[期間を選択] チェックボックスを選択します。この手順はオプションです。

Secure Anywhere.				
Home Endpoint Protection				
Status Policies Group Management	Reports			
Select your report				
Report Type:				
All Undetermined Software Seen 👻				
Policy:				
All 🗸				
Group:				
All				
Select time period				
Include deactivated and hidden				
Submit				

5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アク ティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management	Reports
Select your report	
Report Type:	
All Undetermined Software Seen 👻	
Policy:	
All	
Group:	
All	
Select time period	
Include deactivated and hidden	
Submit	

6. [送信] ボタンをクリックします。

Seci	<b>ire</b> Anywhere.	
Home	Endpoint Protection	
Status	Policies Group Management	Reports
Select y	our report	
Report Type	ð:	
All Undete	ermined Software Seen 💌	
Policy:		
All	*	
Group:		
All	×	
Select t	ime period	
Include	deactivated and hidden	
(	Submit	

右側のペインにレポートが表示されます。

All	All Undetermined Software Seen (Nov 12 09:56) 🛞						
<u>,</u> A	All Undetermined software						
10							
		Filename	Pathname	File Size	Last Seen	Ø Dwell Time	Hostname
1		NMSERVICE.EXE	?:\kaseya\knm\	16.4 MB	Nov 11th 2015, 10:19	378 day 1 hr 29 min 37 sec	WRDemoSVR01
2		OPERA_33.0.1990.58_AUTOUPDATE.EXE	%temp%\opera autoupdate\cprogram file	3.0 MB	Nov 9th 2015, 10:05	0 sec	WRDemoEP01
3		OPERA_33.0.1990.58_AUTOUPDATE.EXE	%temp%\opera autoupdate\cprogram file	3.0 MB	Nov 8th 2015, 10:05	0 sec	WRDemoEP01
4		OPERA_33.0.1990.58_AUTOUPDATE.EXE	%temp%\opera autoupdate\cprogram file	1.8 MB	Nov 7th 2015, 10:05	0 sec	WRDemoEP01
5		LAUNCHER.EXE	%temp%\opera autoupdate\cprogram file	512.0 KB	Nov 5th 2015, 10:30	0 sec	WRDemoEP04

7. ファイルを選択して [オーバーライドの作成] ボタンをクリックすると、次のようにファイルを再分類することができます。

- ・ 正当 エンドポイントでのファイルの実行を常に許可します。スキャン中にこのファイルを検出せず、
   隔離も行いません。[正当]を選択した後、ファイルは[オーバーライド]タブ内に[手動判定にて正当]と表示されますが、クラウド判定は未判定のままになります。
- 不正 スキャン中に検出された場合、常にファイルを隔離します。[不正]を選択した後、ファイルは [オーバーライド] タブ内に [手動判定にて不正] と表示されますが、クラウド判定は未判定のままに なります。

また、このオーバーライドをすべてのポリシーに適用するか、選択したポリシーのみに適用するかを選ぶことができ、他のエンドポイントのためにオーバーライドを何度も作成する必要がありません。

- 8. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメ ニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除 します。詳細については、「*表とレポートのデータの並べ替えページ45」を参照してください。*
- 9. レポートのスプレッドシートをダウンロードするには、「 <u>レポートのスプレッドシートのダウンロード ページ</u> 402」を参照してください。

## [ブロックされたすべての URL] レポートの生成

Webroot の SecureAnywhere の Web 脅威シールドによってブロックされたすべての URL を表示 するには、[ブ ロックされたすべての URL] レポートを生成します。また、このレポートを生成すると、不正な URL として分類 されブロックされたサイトにアクセスしたエンドポイントを確認することもできます。

レポートのデータは次の手順で変更できます。

- 選択したグループ内のブロックされたすべての URL を表示する。特定のエンドポイントのセットに検索結果 を絞り込む場合に便利です。
- 選択したポリシー内のブロックされたすべての URL を表示する。これにより、修正が必要なポリシー設定を 確認できます。

### [ブロックされたすべての URL] レポートを生成するには

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで [**ブロックされたすべての** URL] を選択します。

Secu	ireAnywhere	Manageo
Home	Endpoint Protection	Support
Status F	Policies Group Manageme	ent Reports
Select ye	our report	?
Report Type All URLs E	: Blocked ~	$\mathbf{D}$
All	~	1
Group:		_
All	~	1
Select tir	ne period	
Include d	leactivated and hidden	
	Submit	

3. 特定の期間を含める場合、または非アクティブ化されたエンドポイントおよび非表示のエンドポイントを レポートに含める場合は、[期間を選択]および[非アクティブ化および非表示を含む]チェックボックスを 選択します。

Secure Anywhere.	Managed
Home Endpoint Protection St	upport
Status Policies Group Management	Reports
Select your report	
Report Type:	
All URLs Blocked	
Policy:	
All	
Group:	
All 👻	
Select time period	
Summer	
3	
And:	
3	
Include deactivated and hidden	
Submit	

4. 期間を選択した場合は、レポートの対象期間を特定の日付で指定します。この手順はオプションです。

Secu	ireAnywhere	e. Managed
Home	Endpoint Protection	Support
Status	Policies Group Managem	ent Reports
Select y	our report	?
Report Type	E	
All URLs E	Blocked	~
Policy:		~
Group:		-
All		~
Select tin Between:	me period	
And:		
Include of	deactivated and hidden	

注意:レポートの対象期間を最長 90 日間まで指定できるようになりました。

5. 設定が完了したら、[送信]ボタンをクリックしてレポートを生成します。

Secure Anywhere.	Managed
Home Endpoint Protection St	ipport
Status Policies Group Management	Reports
Select your report	
Report Type:	
All URLs Blocked	
Policy:	
All Y	
Group:	
All	
Select time period	
Between:	
2	
And:	
Include describuled and bidden	

次の情報を含むレポートの結果が右側に表示されます。

- ブロックされた URL
- ブロックのカテゴリー
- •評価
- ホスト名
- ユーザーアクション
- ブロックの日時

### ウェブルートエンドポイントプロテクション管理者ガイド

Select our record (a) 7	All URLs Blocked must man 8					
and particular and a second	All URLs Birched					
eport rype						
a UHLA BOOMED	7 Create override					
ίψ.	UPL	Calagory	Reputation	Hostrame	User Adian	Dete
1	1 replate/wapter.courter.nd	Malware Sites	🔝 High Rak	ADMASTERS	Buck	Oie 22Hz 2017, 12161
	2 http://dltefvelig8ei.cloudfort.net	Malware Sites	🛄 High Rak	ADMHS/TER3	Back	Oat 20vd 2017, 12:50 /
	3 http://dite/wilipdei.cloudhort.net	Malware Sites	🛄 High Rak	ADMHS/TERS	Back	Oct 22nd 2017, 12:52:5
	4 http://dite/wildet.couthert.nd	Matwore Sites	🛄 High Rak	ADMASTER3	Back	Oel 20x4 2017, 12:52:5
latact time pariod	8 replate/water-countering	Malware Sites	💟 High Rak	ADMASTER3	Buck	Oie 20xe 20x7, 12 49
	8 http://dite/wild/ini.couthort.net	Matwore Sites	High Rak	ADMASTER3	Back	Oid 22Hd 2017, 12 47
include deactivated and hidden	7 replate/velptriceurterine	Malware Sites	🖸 High Rak	ADMKSTER3	Buck	Oie 20x4 20x7, 12 47
. A	E http://diter/wilipdei.courtort.nd	Malware Sites	High Rak	ADMHS/TER3	Buck	Oct 20vd 2017, 12-44
Print	8 Hep/ol/ter/miliples/courters.net	Valvare Sites	High Rak	ADMASTERS	Back	Ore 22Hd 2017, 12-40
	10 http://distant-miliplesi.cloudhort.net	Malware Sites	High Rak	ADMASTERS	Pest.	Oct 22Hd 2017, 12:58
	11 http://diterverilation.countert.net	Valware Sites	High Rak	ADMASTERS	Buck	Ore 22Hz 2017, 12:31
	to installation and plant and plant and	Malware Sites	Han Rak	ADMASTERS	Peek.	Oel 20vel 2017, 12:22
	12 reprintmentation countert ret	Malware Sites	C Hat Rak	ADMASTERS	Back	Oie 20vd 2017, 12:21
	14 http://ditert-milipbei.clouthort.net	Valware Sites	C Hat Rak	ADMASTERS	Back	Out 22nd 2017, 12:20
	15 reprintmentation contraction	Malware Sites	C Hat Rak	ADMASTERS	Back	Oer 20vel 2017, 12 18
	10 http://ditert-milipilmi.clouthort.net	Valware Sites	C Hat Rak	ADMAGTERS	Back	Oct 22vd 2017, 12:17
	17 March 10 March 10 American International Television	Malware Sites	C Hat Rat	ADMASTERS	Perk.	Oct 22nd 2017, 12 18
	10 March and advected and and and	Malware Sites	C Hat Rat	ACMASTERS	Red.	Oie 20ve 2017, 12 15
	12 statisticture administration		C Hat Ray	MARMA NO ORY	Park .	Out 20th 2017, 12:59
	20 Mar had been added and been real	Http://dl/infuniliptini.coudhort.nethospiten/2.js	C Hat Rat	MARMA NEORY	Red.	Out 18th 2017, 1021
	21 http://distant-millediesi.clausteest.com	Malagea Silan	C an Re	Martine Net Oliv	Red.	Out 18th 2017 10-21

## [最新のスキャンで脅威が存在したエンドポイント]レポートの生成

最新のスキャンで検出された脅威を特定し管理するには、[最新のスキャンで脅威が存在したエンドポイント] レポートを生成します。このレポートは、脅威をエンドポイントのロケーション別に表示します。このレポートから、エンドポイントのポリシーの変更、スキャンの実行、ファイルのオーバーライドの作成、隔離されたファイルの 復元を実行できます。

レポートのデータは次の手順で変更できます。

- 選択したポリシーまたはグループ内で検出された脅威をすべて表示する。特定のエンドポイントのセットに 検索結果を絞り込む場合に便利です。
- ドリルダウンして日付範囲内で検出された脅威を確認する。特定の期間に検索結果を絞り込む場合に 便利です。

[最新のスキャンで脅威が存在したエンドポイント] レポートを生成するには

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで [ 最新のスキャンで脅威が存在したエンドポイント]を選択します。

Secure Anywhere.					
Home	Endpoint Protection				
Status	Policies Group Management	Reports			
Select	your report	«?			
Report Ty Endpoin	Report Type: Endpoints with threats on last scan				
Include deactivated and hidden					
Submit					

3. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アク** ティブ化および非表示を含む] チェックボックスを選択します。この手順はオプションです。

Secure Anywhere.				
Home Endpoint Protection				
Status Policies Group Management	Reports			
Select your report	«?			
Report Type:				
Endpoints with threats on last scan				
Include deactivated and hidden				
Submit				

4. [送信] ボタンをクリックします。

Sec	Secure Anywhere.				
Home	Endpo	int Protection			
Status	Policies	Group Management	Reports		
Select	your repo	rt	«?		
Report Typ	be:				
Endpoint	Endpoints with threats on last scan				
Include	Include deactivated and hidden				
	Submit				

レポートと次のオプションが右側のパネルに表示されます。

- ポリシーの表示と変更 エンドポイントのポリシー設定を開き、設定を変更するには、[表示] リンクを クリックします。非管理ポリシーに割り当てられたエンドポイントに関しては、エンドポイントレベルで制 御されているため [表示] リンクがありません。
- スキャンを実行 右端にあるほうきのアイコンをクリックすると、スキャンを開始し、脅威の自働隔離を 行うことができます。

End	Endpoints with threats on last scan (Nov 12 10:27) 🛞							
😵 Endpoints with threats						8?		
	Hostname	Policy	$\frown$	Group	First Seen	Last Seen	Last Threat	0
1	WRDemoEP05	No Remediation	View	Default Group	Dec 17th 2013, 07:52	Nov 12th 2015, 10:19	Nov 12th 2015, 04:09	(🦪 )
			$\sim$					$\smile$

5. エンドポイントで検出された脅威の詳細を確認するには、[ホスト名] カラムのアイテムをクリックします。 詳細が下のパネルに表示されます。

	Endpoints with threats on last scan (Nov 12 10:27) 🛞				
1	Endpoints with threats				
	Hostname	Policy	-	Group	
1	WRDemoEP05	No Remediation View		Default Group	
	Threats seen on this endpoint				
ا 🌉	hreats seen on this endpoint				
및 1 🤊 o	Threats seen on this endpoint	encountering this file 📑 Restore from Quarantine			
=∎ 1 ≁ 0	Threats seen on this endpoint irreate override 🖳 Show all endpoints e	encountering this file Restore from Quarantine			Malware Group
ן 📑 ו	Threats seen on this endpoint reate override 🖳 Show all endpoints e Filename WEBROOTTESTFILE EXE	encountering this file Restore from Quarantine Pathname %cache%\			Malware Group W32.Webroottestfile
-∎ 1 ∳C 1 2	Threats seen on this endpoint         irreate override       Show all endpoints e         Filename       WEBROOTTESTFILE EXE         SURIV.DLL	encountering this file Restore from Quarantine Pathname %cache%\ %windir%\system32\			Malware Group W32.Webroottestfile W32.Suriv.Test
1 <b>€</b> <b>1</b> 2 3	Threats seen on this endpoint         irreate override       Show all endpoints e         Filename       WEBROOTTESTFILE.EXE         SURIV.DLL       MOCKVIRUS.EXE	encountering this file Restore from Quarantine Pathname %cache%\ %windir%\system32\ %temp%\temp1_mockvirus.zip\			Malware Group W32.Webroottestfile W32.Suriv.Test Uncategorized file

- 6. 下のパネルから、選択した脅威に対して次のいずれかの操作を行うことができます。
  - オーバーライドの作成 エンドポイントプロテクションを回避してファイルを [正当] (ファイルの実行を許可) または [不正] (ファイルを検出して隔離) に指定するには、コマンドバーの [オーバーライドの作成] アイコンをクリックします。.詳細については、「レポートからのファイルへのオーバーライドの適用 ページ454」を参照してください。
  - 隔離先から復元する ファイルが安全である場合、エンドポイントの元の場所に復元するには、コマンドバーの[隔離先から復元する]アイコンをクリックします。
- レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。カラムの詳細については、「表とレポートのデータの並べ替えページ45」を参照してください。

レポートのスプレッドシートをダウンロードする場合の詳細については、「<u>レポートのスプレッドシートのダウ</u> <u>ンロードページ402</u>」を参照してください。

# [最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートの生成

SecureAnywhere は、正当なファイルのように見えても動作が疑わしいファイルを検出することがあります。この場合、そのファイルは[未判定]に分類されます。

SecureAnywhere が最新のスキャンで [未判定] と分類したファイルを特定するには、 [最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートを生成します。 エンドポイントを選択してドリルダウンすると、ファイルの詳細を確認できます。

#### [最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートを生成するには

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで [最新のスキャンで未判定のソフトウェアが検出されたエンドポイント]を選択します。

Seci	Secure Anywhere.				
Home	Endpoint Protection				
Status	Policies Group Management Reports Ove				
Select y	rour report 🤍 ?				
Report Typ	e:				
Endpoints	Endpoints with undetermined software on last scan				
Include	Include deactivated and hidden				
	Submit				

3. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[非アク

ティブ化および非表示を含む] チェックボックスを選択します。この手順はオプションです。

Seci	<b>ire</b> Anywhere.
Home	Endpoint Protection
Status	Policies Group Management Reports Ove
Select y	vour report 🔍 ?
Report Typ	e:
Endpoints	with undetermined software on last scan 💌
Include	deactivated and hidden
	Submit

4. [送信] ボタンをクリックします。

Seci	<b>ire</b> Anywhere.
Home	Endpoint Protection
Status	Policies Group Management Reports Ove
Select y	our report
Report Typ	e:
Endpoints	with undetermined software on last scan
🔲 Include	Submit

右側のパネルでレポートが開き、すべてのエンドポイントが表示されます。

End	Endpoints with undetermined software on last scan (Nov 12 11:05) 🛞						
🔥 E	😧 Endpoints with Undetermined Software						
	Hostname	Policy	Group	Status	Last Seen	Last Threat	
1	ACER-PC	Unmanaged	Default Group	📀 Not Seen Recently	Apr 10th 2014, 21:04	Mar 30th 2014, 20:13	
2	BROW-1128-XP	Unmanaged	Default Group	📀 Not Seen Recently	Jun 21st 2013, 11:49	Jun 21st 2013, 07:55	
3	BROW-2308-WIN8	Unmanaged	Default Group	📀 Not Seen Recently	Dec 4th 2012, 08:40	Oct 30th 2012, 12:10	
4	DAL-TST-SRV	Unmanaged	Default Group	📀 Not Seen Recently	Jun 26th 2013, 17:51	Nov 16th 2011, 06:29	
5	FHAL-3377-W7	Unmanaged	Default Group	Needs Attention	Feb 3rd 2014, 09:13	Jan 8th 2014, 06:26	

5. 検出された未判定のソフトウェアの詳細を確認する場合は、エンドポイントの行をクリックすると、下に 詳細が表示されます。

End	Endpoints with undetermined software on last scan (Nov 12 11:05) 🛞						
۰	Endpoints with Undetermined Software						
	Hostname	Policy	Group	Status	Last Seen	Last Threat	
1	ACER-PC	Unmanaged	Default Group	🔶 Not Seen Recently	Apr 10th 2014, 21:04	Mar 30th 2014, 20:13	
2	BROW-1128-XP	Unmanaged	Default Group	🚸 Not Seen Recently	Jun 21st 2013, 11:49	Jun 21st 2013, 07:55	
3	BROW-2308-WIN8	Unmanaged	Default Group	🔶 Not Seen Recently	Dec 4th 2012, 08:40	Oct 30th 2012, 12:10	
4	DAL-TST-SRV	Unmanaged	Default Group	Default Group 🚯 Not Seen Recently		Nov 16th 2011, 06:29	
-	All undetermined software seen o	on this endpoint					
10							
	Filename	Pathname		File Size	Last Seen	Owell Time	
1	MSRATING.DLL	%windir%\\$ntservi	cepackuninstall\$\	129.0 KB	Apr 3rd 2013, 14:02	0 sec	

- 6. このパネルでファイルを選択して [オーバーライドの作成] をクリックすると、次のようにファイルを再分類することができます。
  - 正当 エンドポイントでのファイルの実行を常に許可します。スキャン中にこのファイルを検出せず、 隔離も行いません。[正当]を選択した後、ファイルは[オーバーライド]タブ内に[手動判定にて正 当]と表示されますが、クラウド判定は未判定のままになります。
  - 不正 スキャン中に検出された場合、常にファイルを隔離します。[不正]を選択した後、ファイルは [オーバーライド] タブ内に [手動判定にて不正] と表示されますが、クラウド判定は未判定のままに なります。

また、このオーバーライドをすべてのポリシーに適用するか、選択したポリシーのみに適用するかを選ぶことができ、他のエンドポイントのためにオーバーライドを何度も作成する必要がありません。

7. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメ ニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除 します。カラムの詳細については、「<u>表とレポートのデータの並べ替えページ45」を参照してください。</u>

レポートのスプレッドシートをダウンロードする方法の詳細については、「レポートのスプレッドシートのダ ウンロードページ402」を参照してください。

### [脅威の履歴 (日単位)] レポートの生成

検出された脅威の概要を日単位で表示するには、[脅威の履歴 (日単位)] レポートを生成します。このレポートには、SecureAnywhere によってエンドポイントで脅威が検出された場所が日単位で表示されます。レポートのデータは次の手順で変更できます。

- 選択したポリシーまたはグループ内の脅威を日単位で表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして日付範囲内で検出された脅威を確認する。特定の期間に検索結果を絞り込む場合に 便利です。

[脅威の履歴 (日単位)] レポートを生成するには

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで [脅威の履歴 (日単位)]を選択します。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management	Reports
Select your report	«?
Report Type:	
Threat History (Daily)	~
Policy:	
All	~
Group:	
All	~
Between:	
And:	
Include deactivated and hidden	
Submit	

3. 必要に応じて、特定のポリシーやグループを選択します。ポリシーやグループを選択しない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management	Reports
Select your report	«?
Report Type:	
Threat History (Daily)	~
Policy:	
All	~
Group:	
All	~
Between:	
And:	
	· •
Include deactivated and hidden	
Submit	

4. [開始日]と[終了日]のフィールドに、レポートデータの期間の開始日と終了日を入力します。

Seci	Secure Anywhere.			
Home	Endpoint Protection			
Status	Policies Group Management	Reports		
Select y	our report	«?		
Report Typ Threat Hi	e: story (Daily)	v		
Policy:				
All		*		
Group:				
All		~		
Between:		•		
And:				
Include	deactivated and hidden			
	Submit			

5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アク ティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。

SecureAnyw	here.
Home Endpoint Protect	tion
Status Policies Group Ma	anagement Reports
Select your report	« ?
Report Type:	
Threat History (Daily)	~
Policy:	
All	*
Group:	
All	¥
Between:	
	- 9
And:	
	L.2
Include deactivated and hidd	len
Submit	

6. [送信] ボタンをクリックします。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management	Reports
Select your report	«?
Report Type: Threat History (Daily)	v
Policy:	
All	~
Group:	
All	*
Between:	
	<u> </u>
And:	
	<u> </u>
Include deactivated and hidden	

右側のペインにレポートが表示されます。



7. 脅威の詳細を表示するには、棒グラフをクリックします。その日付の詳細が表示されます。
 脅威が検出されたエンドポイントの詳細が下のパネルに表示されます。



- 8. ブロックされたプログラムの詳細を表示するには、[ブロックされたプログラム] カラムの [**表示**] リンクをクリックします。
- ワポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。カラム内のデータの詳細については、「<u>表とレポートのデータの並べ替えページ45</u>」を参照してください。

### [脅威の履歴 (内訳)] レポートの生成

検出された脅威の概要を表示するには、[脅威の履歴 (内訳)] レポートを生成します。このレポートには、脅威が検出されたエンドポイントとプログラムがブロックされたエンドポイントの棒グラフが表示されます。このレポートから、ブロックされたプログラムのオーバーライドを作成したり、隔離されたファイルを復元したりできます。

**注意:** 脅威の概要を表示するには、「<u>育威の履歴(日単位)] レポートの生成ページ369</u>」を参照してください。[脅威の履歴(日単位)] レポートは概要を確認するためのものであり、このレポートから脅威を管理することはできません。

レポートのデータは次の手順で変更できます。

- 選択したポリシーまたはグループ内の脅威をすべて表示する。特定のエンドポイントのセットに検索結果を 絞り込む場合に便利です。
- ドリルダウンして日付範囲内で検出された脅威を確認する。特定の期間に検索結果を絞り込む場合に 便利です。

|脅威の履歴(内訳)|レポートを生成するには

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで [脅威の履歴 (内訳)]を選択します。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management Rep	orts
Select your report	«?
Report Type:	
Threat History (Collated)	Y
Policy:	
All	~
Group:	
All	*
Between:	
	•
And:	
	•
Include deactivated and hidden	
Submit	

3. 必要に応じて、特定のポリシーやグループを選択します。この選択を行わない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。

Secl	<b>ire</b> Anywhere.	
Home	Endpoint Protection	
Status	Policies Group Management	Reports
Select y	our report	«?
Report Type Threat His	e: story (Collated)	¥
Policy:		
All		~
Group:		
All		~
Between:		
And:		
		•
Include	deactivated and hidden	

4. [開始日]と[終了日]のフィールドに、レポートデータの期間の開始日と終了日を入力します。

Secu	reAnywhere.	
Home	Endpoint Protection	
Status P	Policies Group Management	Reports
Select yo	our report	«?
Report Type Threat His	tory (Collated)	×
Policy:		
All		*
Group: All		¥
Between:		
And:		
Include of	deactivated and hidden	
	Submit	

5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アク** ティブ化および非表示を含む] チェックボックスを選択します。この手順はオプションです。

Home	ndpoint Protection	
Status Polic	ies Group Manage	ment Report
Select your	report	<b>«</b>
Report Type:		
Threat History	(Collated)	~
Policy:		
All		~
Group:		
All		~
Between:		
And:		
		3
Include des	nabbid bre betevits	

6. [送信] ボタンをクリックします。

Home	Endpo	oint Protection		
Status F	Policies	Group Manage	ment	Repor
Select ye	our repo	rt		<
Report Type	:			
Threat His	tory (Co	llated)		
Policy:				
All				1
Group:				
All				1
Between:				
				E
And:				
				E

右側のペインにレポートが表示されます。



7. このパネルでいずれかの棒グラフをクリックすると、[脅威が存在したエンドポイント] または [ブロックされた プログラム] の詳細を確認できます。

[ブロックされたプログラム]の棒グラフをクリックすると、プログラムの詳細が下のパネルに表示されます。



8. 下のパネルで [すべてのエンドポイント] および [すべてのバージョン] カラムの [表示] リンクをクリックする と、それぞれの詳細が表示されます。

[すべてのエンドポイント]の[表示]リンクをクリックすると、このパネルが表示されます。

Endpoints which have seen this Program			
	Hostname	First Infected	Days Infected
1	G_FEB15_WIN8	Apr 6th 2013, 14:24	1
2	G-0306-SUMATRA	Mar 26th 2013, 06:59	13
з	G-0408-SUMATRA	Apr 8th 2013, 15:03	1

[すべてのバージョン]の[表示]リンクをクリックすると、このパネルが表示されます。

	versions encountered of	this program			BOX
	Filename	Pathname	Last Seen	Hostname	Cloud Determination
1	ALL.EXE	%desktop%\trojan h	Apr 8th 2013, 17:26	G-0409-SUMATRA	Bad
2	ALL.EXE	%desktop%\trojan h	Apr 8th 2013, 15:04	G-0408-SUMATRA	Bad
3	ALL.EXE	?:\trojan horses\troja	Apr 7th 2013, 18:16	G-ALERTN-VOLGA	Bad

9. ファイルに対するオーバーライドを設定する、またはファイルを隔離先から復元するには、[脅威が存在 したエンドポイント]の棒グラフを選択すると、詳細が下のパネルに表示されます。



10. ブロックされたプログラムが確認されたエンドポイントの行を探し、[ブロックされたプログラム] カラムの [**表** 示] リンクを選択します。

次のウィンドウが表示されます。

1 Programs blocked on this endpoint				
0	reate	override 📑 Restore from Quarantine		
		Filename		
1		9876.ZIP/9876.EXE		
2		SECURESERVICEPACK.CAB/UPGRADE.EXE		
3		BAZOOKABAR ZIP/BAZOOKABAR EXE		

- 11. このウィンドウで、次のいずれかの操作を行います。
  - オーバーライドの作成 エンドポイントプロテクションを回避してファイルを [正当] (ファイルの実行を許可) または [不正] (ファイルを検出して隔離) に指定するには、コマンドバーの [オーバーライドの作成] をクリックします。詳細については、「レポートからのファイルへのオーバーライドの適用ページ454」を参照してください。
  - 隔離先から復元する ファイルが安全である場合、エンドポイントの元の場所に復元するには、コマンドバーの[隔離先から復元する]をクリックします。

また、このオーバーライドをすべてのポリシーに適用するか、選択したポリシーのみに適用するかを選ぶことができ、他のエンドポイントのためにオーバーライドを何度も作成する必要がありません。

12. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメ ニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除 します。カラム内のデータの詳細については、「<u>表とレポートのデータの並べ替えページ45</u>」を参照してく ださい。

## [ブロックされた URL の履歴 (日単位)] レポートの生成

Webroot の Secure Anywhere の Web 脅威シールドによってブロックされた URL の履歴を表示するには、[ブロックされた URL の履歴 (日単位)] レポートを生成します。

[ブロックされた URL の履歴 (日単位))] レポートを生成するには

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで [ブロックされた URL の履歴 (日単位)]を選択します。

Secure Anywhe	Pre. Managed
Home Endpoint Protection	Support
Status Policies Group Manag	ement Reports
F Select your report	« ?
Report Type: Blocked URL History (Daily) Policy.	
All	~
Group:	
Include deactivated and hidden           Submit	

- 3. 以下のいずれかの操作を行います。
  - すべてのポリシーとグループの結果を表示するように選択する。
  - ブロックされた URL の表示元となるポリシーまたはグループを選択する。
| Secure Anywhere.                            | Managed |
|---------------------------------------------|---------|
| Home Endpoint Protection Su                 | pport   |
| Status Policies Group Management            | Reports |
| Select your report                          |         |
| Report Type:<br>Blocked URL History (Daily) |         |
| Policy:                                     |         |
| All V                                       |         |
| All 👻                                       |         |
| Include deactivated and hidden              |         |
| Submit                                      |         |
|                                             |         |

4. ブロック済みの非アクティブ化された URL および非表示の URL を表示するには、[**非アクティブ化およ び非表示を含む**] チェックボックスを選択します。この手順はオプションです。

Home Endpoi	int Protection	Support
Status Policies	Group Manageme	ent Reports
Select your report	t (6)	7
Report Type:		
Blocked URL Histor	y (Daily) 🍟	1
Policy:		
All	~	1
Group:		
All	~	1
Include deactivated	d and hidden	
Include deactivated  Sub	d and hidden	

5. 設定が完了したら、[送信]をクリックしてレポートを生成します。



次の情報を含むレポートの結果が右側に表示されます。

- ブロックされた URL
- ブロックのカテゴリー
- •評価
- ホスト名
- ユーザーアクション
- ブロックの日時



### [エージェントのバージョンの使用状況] レポートの生成

異なる SecureAnywhere のバージョンがインストールされているエンドポイントを特定するには、[エージェントの バージョンの使用状況] レポートを生成します。エージェントとは、エンドポイントで実行されている SecureAnywhere ソフトウェアです。

このレポートを使用して、アップグレードが必要なエンドポイントを特定できます。このレポートには、ネットワーク 内で使用されているバージョン番号と、各バージョンを使用しているエンドポイントを示す棒グラフが表示され ます。

レポートのデータは次の手順で変更できます。

- 選択したグループ内のすべてのバージョンを表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして特定のバージョンを使用しているエンドポイントを確認する。アップグレードの必要なエンドポイントを判定する場合に便利です。

**注意:** [状態] パネルで、エージェントのバージョンの使用状況を示す円グラフを簡単に確認できます。 ただし、この円グラフでは [エージェントのバージョンの使用状況] レポートほど詳細な情報は提供され ません。詳細については、「<u>エージェントのバージョンの概要表示 ページ212</u>」を参照してください。

[エージェントのバージョンの使用状況] レポートを生成するには

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで [エージェントのバージョンの使用状況]を選択します。

Secure Anywhere. MANAG										
Home Endpoint Protection										
Status Policies Group Management	Reports									
Select your report										
Report Type:										
Agent Version Spread										
Include deactivated and hidden										
Submit										

3. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アク ティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。

Secure Anywhere. Manag									
Home	ndpoint Protection								
Status Polic	ies Group Management	Reports							
Select your	report «?								
Report Type:									
Agent Version	n Spread 🗸 🗸								
Include dea	ctivated and hidden								
	Submit								

4. [送信] ボタンをクリックします。





[エージェントのバージョンの使用状況]レポートと、グループのリストが表示されます。

- 5. 次のいずれか、または両方の操作を行います。
  - 特定のグループのデータを表示するには、左側でグループ名をクリックします。棒グラフに選択したグループのみのデータが表示されます。
  - 特定のバージョンを使用しているエンドポイントを確認するには、棒グラフの棒をクリックして詳細を表示します。下のパネルに各エンドポイントに関するデータが表示されます。



レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。

カラム内のデータの詳細については、「表とレポートのデータの並べ替えページ45」を参照してください。

## [インストールされたエージェント] レポートの生成

インストールされている SecureAnywhere のグラフを表示するには、[インストールされたエージェント] レポートを 作成します。エージェントとは、エンドポイントで実行されている SecureAnywhere ソフトウェアです。このレポー トには、SecureAnywhere がエンドポイントにインストールされた日付と、インストールが行われたエンドポイント の数を示す棒グラフが表示されます。レポートのデータは次の手順で変更できます。

- 選択したポリシーやグループ内のすべての Secure Anywhere のインストールを表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして同じ日に Secure Anywhere がインストールされたエンドポイントを確認する。特定の期間に 検索結果を絞り込む場合や、特定の日にインストールされたエンドポイントのセットにポリシーを割り当てな ければならない場合に便利です。

[インストールされたエージェント] レポートを生成するには

ウェブルートエンドポイントプロテクション管理者ガイド

- 1. エンドポイントプロテクションのコンソールで [レポート] タブをクリックします。
- 2. [レポートの種類]ドロップダウンメニューで[インストールされたエージェント]を選択します。

Secure Anywhere.								
Home Endpoint Protection								
Status Policies Group Management Reports								
Select your report								
Report Type:								
Agents Installed								
Policy:								
All								
Group:								
All 👻								
Between:								
3								
And:								
Include deactivated and hidden								
Submit								

3. 必要に応じて、特定のポリシーやグループを選択します。

ポリシーやグループを選択しない場合、レポートにはすべてのポリシーとグループが表示され、使用する 環境によっては生成に時間がかかることがあります。

Secure Anywhere.									
Home Endpoint Protection									
Status Policies Group Management R	eports								
Select your report									
Report Type:									
Agents Installed									
Policy:									
All									
Group:									
All									
Between:									
And:									
Include deactivated and hidden									
Submit									

4. [開始日]と[終了日]のフィールドに、レポートデータの期間の開始日と終了日を入力します。

Secu	reAny	where.	
Home	Endpoint Pr	rotection	
Status P	olicies Gro	up Management	Reports
Select yo	ur report	«?	
Report Type:			
Agents Inst	alled	~	
Policy:			
All		¥	
Group:			
All		*	
Between:			
		•	
And:			
		•	
Include d	eactivated and	hidden	
	Submit	]	

5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アク ティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。

Secure Anywhere.								
Home Endpoint Protection								
Status Policies Group Management	Reports							
Select your report								
Report Type:								
Agents Installed								
Policy:								
All								
Group:								
All								
Between:								
And:								
<u> </u>								
Include deactivated and hidden								
Submit								

6. [送信] ボタンをクリックします。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management	Reports
Select your report	
Report Type:	
Agents Installed	
Policy:	
All	
Group:	
All 👻	
Between:	
8	
And:	
8	
Include deactivated and hidden	
Submit	

右側のペインにレポートが表示されます。



7. 特定の日付に Secure Anywhere がインストールされたエンドポイントを確認するには、棒グラフの棒をクリックして詳細を表示します。

下のパネルに各エンドポイントに関するデータが表示されます。



8. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメ ニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除 します。詳細については、「<u>表とレポートのデータの並べ替えページ45</u>」を参照してください。

### レポートのスプレッドシートのダウンロード

レポートの実行後、電子メールで送信したり保存したりするために、レポートのスプレッドシート (CSV ファイル) が必要になることがあります。必要に応じてレポートのスプレッドシートをダウンロードするには、次の手順に 従ってください。

以下のレポートのスプレッドシートをダウンロードできます。

- 確認されたすべての脅威
- ・ 確認されたすべての未判定のソフトウェア
- 最新のスキャンで脅威が存在したエンドポイント
- ・ 未判定のソフトウェアが検出されたエンドポイント

#### レポートのスプレッドシートをダウンロードするには

1. レポートの実行後、レポートの右上隅にある CSV のアイコンをクリックします。.

II Time	Hostname	
s 20 hours 2 secs	WRDemoEP05	
s 20 hours 23 mins 43 s	WRDemoEP05	
s 20 hours 7 secs	WRDemoEP05	

2. メッセージがウィンドウの下部に表示されたら、[開く]ボタンをクリックします。

o you want to open or save Most Recent Threats Seen.csv (2.09 KB) from mypcsecurity.webrootanywhere.c	Open	Save	•	Cancel	×
					)

レポートの設定に基づいてデータが入力された状態でスプレッドシートが表示されます。

X	185	· @ · ;	;								Most	Recent_Thr	eats_Seen.cs	v - Excel	
F	FILE HO	OME IN	SERT P.	AGE LAYOUT	FORM	IULAS D	ATA RI	EVIEW \	/IEW						
ľ	Cut		Calibri	- 1	1 · A	≡ ≡	= %	岸 Wra	ap Text	Gene	ral	-			Normal
Pa	-⊡ ≞⊟ Cop iste - ✓ Forr	y ▼ mat Painter	BI	<u>u</u> - 🔛 -	🕭 - 🗛	• = =	≡	🖻 🗮 Me	rge & Cente	r • \$ •	% , *	.0 .00 Co	nditional Fo	ormat as	Good
	Clipboar	d rs		Font		r _a	AI	ignment		r <u>s</u>	Number	E I I	matung ·		Styles
A	1	• : )	X 🗸	<i>f</i> _{<i>x</i>} Mo	st Recent	Threats Se	en								
	Α	В	С	D	E	F	G	Н	I	J	к	L	м	N	0
1	Most Rece	nt Threats	Seen												
2															
з	First Seen	Last Seen	Pathname	Filename	File Size	Cloud Det	MD5	Vendor	Product	Version	Malware (	Hostname	First Seen	Last Seer	VM
4	Dec 17 201	Jan 15 201	%windir%	SURIV.DLL	27,136	Bad	0AA9E950	35007D63D	663D31564	418E2E	W32.Suriv	WRDemo	Dec 17 20	Feb 3 201	5Yes
5	Dec 17 201	Sep 24 20	1%temp%\	SURIV.EXE	215,040	Bad	97690871F	Webroot I	Demonstr	Demonstr	W32.Suriv	WRDemo	Dec 17 20	Feb 3 201	5Yes
6	Dec 17 201	Feb 3 201	%temp%\	MOCKVIR	276,992	Bad	F7CA0D22	Webroot I	Demonstr	Demonstr	W32.Bot.0	WRDemo	Dec 17 20	Feb 3 201	5 Yes
7															

3. 必要に応じてスプレッドシートのソートやフォーマット設定を行ってから、コンピュータに保存します。

# 第9章:警告の管理

警告の管理方法については、以下のトピックを参照してください。

警告の導入	
配信先リストの作成	
カスタムの警告の作成	
定義済みの警告メッセージの表示	
警告の一時停止または削除	

### 警告の導入

警告メッセージをカスタマイズして、次のイベントが発生した際に、配信先リストに送信することができます。

- エンドポイントによる感染の報告
- エンドポイントでの新しい Secure Anywhere のインストール

どちらの場合も、イベントが発生したらすぐに、またはスケジュール(毎日、毎週、毎月)に沿って、管理者に メッセージを送信するように警告の方法をカスタマイズできます。[警告] タブのセットアップウィザードを使用する と、メッセージの件名と本文をカスタマイズすることができます。また、変数を使用して、警告を動作させるエン ドポイント、影響を受けたグループ、イベントに関するその他の詳細について情報を追加することも可能です。

**注意:**警告をカスタマイズするには、[警告]の[作成・編集]へのアクセス権限が必要です。アクセス 権限の変更に関する詳細と手順については、「<u>コンソールユーザーの権限設定ページ75</u>」を参照して ください。

#### 警告を導入するには

- 1. 電子メールアドレスに基づいて配信先リストを作成します。管理ポータルの [ユーザーの管理] パネルで リストのメンバーを定義する必要はありません。詳細については、「 <u>配信先リストの作成 ページ406</u>」を 参照してください。
- エンドポイントが感染を報告した場合やエンドポイントに Secure Anywhere がインストールされた場合に 配信先リストに送信される警告メッセージを作成します。詳細については、「<u>カスタムの警告の作成</u> ページ408」を参照してください。

すべてのカスタムの警告が[警告]タブに表示されます。

Status Policies Gro	oup Management Reports	Alerts Overrides Logs	Resources			
Alerts				\$	Distribution Lists	
🕒 Create 🛛 😑 Delete	Suspend				🔂 Create 🕴 🖨 Dele	le
Alert Name	Alert Type	Date Created A	Status		List Name	Email A
Infection Alert 1	Infection detected	Apr 26th 2013, 09:20	Active	*	US	000wrs
Infection Summary	Infection Summary	Apr 26th 2013, 09:22	Active		Max	MaxNa
Resumen de instalación	Install Summary	Apr 26th 2013, 10:49	Suspended		JA	a@b.ci
Infection Summary 2	Infection Summary	Apr 26th 2013, 11:49	Active			
Installation Alert	Endpoint installed	May 4th 2013, 10:23	Active			

### 配信先リストの作成

[警告] タブでは、警告メッセージを送信するユーザーの配信先リストを簡単に作成することができます。たとえば、脅威が検出された際にリモートオフィスで対応する必要がある管理者の一覧などを作成できます。

**注意:** [警告の作成] ウィザードでも配信先リストを作成できます。詳細については、「<u>カスタムの警告</u> の作成ページ408」を参照してください。

#### 配信先リストを作成するには

- 1. [警告] タブをクリックします。
- 2. [配信先リスト] カラムで、コマンドバーの [作成] をクリックします。

Status Policies Group	Management Reports	Alerts Overrides Logs	Resources			
Alerts				ø	Distribution Lists	
🔮 Create 🛛 🖨 Delete 🛛 🔤	Suspend				Create Octete	
Alert Name	Alert Type	Date Created +	Status		List Name	Email A
Infection Alert 1	Infection detected	Apr 26th 2013, 09:20	Active	*	US	000wrs
Infection Summary	Infection Summary	Apr 26th 2013, 09:22	Active		Max	MaxNa
Resumen de instalación	Install Summary	Apr 26th 2013, 10:49	Suspended		JA	a@b.ci
Infection Summary 2	Infection Summary	Apr 26th 2013, 11:49	Active			
Installation Alert	Endpoint installed	May 4th 2013, 10:23	Active			

#### T[配信先リストの作成] ウィンドウが表示されます。

Create Distribution List	
List Name:	
Distribution List	
Email Addresses (comma separated, maximum of 10):	
user@company.com	*
	*
Save Cancel	

- 3. [リストの名前] フィールドにリストの名前を入力します。
- 4. [電子メールアドレス] フィールドに受信者の電子メールアドレスを入力します。各アドレスはコンマで区切ります。

5. 設定が完了したら[保存]ボタンをクリックします。

[配信先リスト] パネルに新しいリストが追加されます。

後でリストを削除するには、リストの名前を選択してコマンドバーの[削除]アイコンをクリックします。

### カスタムの警告の作成

次のイベントについて、配信先リストに送信される警告メッセージをカスタマイズできます。

- 感染が検出されました エンドポイントが感染を報告するとただちに送信されるメッセージ。
- エンドポイントがインストールされました Secure Anywhere がエンドポイントにインストールされ、管理ポータ ルに報告するとただちに送信されるメッセージ。
- 感染の概要 エンドポイントで検出された脅威の概要を示すメッセージ。概要の配信頻度は、毎日、毎週、毎月のいずれかを設定できます。
- インストールの概要 Secure Anywhere のインストールの概要を示す概要メッセージ。概要の配信頻度は、 毎日、毎週、毎月のいずれかを設定できます。

このトピックで説明するように、[警告の作成] ウィザードを使用してメッセージと配信先リストを定義することができます。また、配信先リストは個別に定義することもできます。詳細については、「<u>配信先リストの作成ペー</u> ジ406」を参照してください。

#### カスタムの警告を作成するには

1. メインコンソールで [警告] タブをクリックします。

Secure Anywhere.	
Home Endpoint Protection Supp	ort
Status Policies Group Management	Reports Alerts Overrides Logs Resources
E Status	Endpoints encountering threats (last 7 days)
Alert <u>1 Endpoint needs attention</u>	2
We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	

[警告] パネルが表示されます。

Secure Anywh	ere		
Home Endpoint Protection	n Support		
Status Policies Group Mana	gement Reports Alerts	Overrides Logs Resource	ces
Malerts			
😌 Create 🛛 🤤 Delete 🛛 🖂 Susp	end / Resume		
Alert Name	Alert Type	Distribution List	Date Created

2. コマンドバーの[作成]アイコンをクリックします。

Secure Anywh	ere		
Home Endpoint Protection	n Support		
Status Policies Group Mana	gement Reports Alerts	Overrides Logs Resource	es
Create Delete Susp	end / Resume		
Alert Name	Alert Type	Distribution List	Date Created

[警告の作成] ウィンドウが表示されます。

Create Alert		
• Step 1: Give this	s alert a name, and select the alert type	
Alert Type:		~
Alert Name:		
💥 Cancel	Previous	Next 🔶

3. [警告のタイプ]ドロップダウンメニューで警告のタイプを選択します。

Give th	is alert a name, and select the alert type	
Josep 1. Olive u	is diert a name, and select the diert type	
Alert Type:		
	Threat Detected	
Alert Name:	Endpoint Installed	Jm
	Threat Summary	<u> </u>

4. [警告の名前] フィールドに、この警告の名前を入力します。

Create Alert		
Step 1: Give the step 1: Give 1: Give 1: Give the step 1: Give the step 1: Give the step	nis alert a name, and select the alert type	
Alert Type:	Threat Detected	¥
Alert Name:	Threat Alert 3	
🗙 Cancel	E Previous	Next =

- 5. 警告のタイプとして [脅威の概要] または [インストールの概要] を選択した場合は、[頻度] フィールド が表示されます。希望する警告の送信頻度を選択します。
  - 毎日
  - ・毎週
  - ・毎月

6. [**次へ**] ボタンをクリックします。

Create Alert			
• Step 1: Give th	his alert a name, and select the alert type		
Alert Type:	Threat Detected		*
Alert Name:	Threat Alert 3		
¥ Cancel		👍 Previous	Next 🛁
X Cancel		Previous	Next

[ステップ 2] ウィンドウが表示されます。

Jup 2. Select un ex	isting distribution list, or create		
Alert recipients:	Ose existing list	Create new list	
Select a Distribution List:	Infection List		¥

- 7. 次のいずれかのラジオボタンを選択し、警告の受信者の一覧を決定します。
  - 配信先リストがすでに作成されている場合は、[既存のリストを使用] ラジオボタンを選択します。

6 Step 2: Select an exi	sting distribution list, or create a new	v list of emails to send this alert to	
Alert recipients:	Use existing list Infection List	Create new list	¥
Cancel		Previous	Next =

• 配信先リストをまだ作成していない場合は、[新規リストの作成] ラジオボタンをクリックしてリストの名前を入力し、電子メールアドレスを入力します。

Alert recipients:	Use existing list	Create new list
Email Addresses (comma	Idoe@webroot.com	
separated, maximum of 10):		

8. 終わったら[次へ]ボタンをクリックします。

[ステップ 3] ウィンドウが表示されます。

Email title:	Threat Alert	Data Inputs
Email message body:	An endpoint has recently encountered a threat: Hostname: [hostname] Group Name: [groupname] Policy Name: [policyname] Keycode: [keycode] Threat List: [infectionlist.filename,malwaregroup,pathname,md5,dwelltim e]	Data Inputs

9. [電子メールの件名] フィールドにメッセージの件名を入力します。

Email title:	Threat Alert Data Input	s •
Email message body:	An endpoint has recently encountered a threat: Hostname: [hostname] Group Name: [groupname] Policy Name: [policyname] Keycode: [keycode] Threat List: [infectionlist.filename,malwaregroup,pathname,md5,dwelltim e] Reset	S •

10. [電子メールメッセージの本文] フィールドにメッセージのテキストを入力します。

Email title:	Threat Alert Data Inputs
Email message body:	An endpoint has recently encountered a threat: Hostname: [hostname] Group Name: [groupname] Policy Name: [policyname] Keycode: [keycode] Threat List: [infectionlist.filename,malwaregroup,pathname,md5,dwelltim e] Reset

11. ウィザードでは、テキスト内へのデータ入力項目も表示されます。これは、エンドポイントのホスト名などの情報を自動的に挿入するための変数です。一部のデータ入力は、サンプルのテキストにすでに表示されています。データ入力は角括弧 ([])で囲まれて表示されます。

データ入力を追加するには、テキスト内で変数を表示する部分をクリックし、[データ入力] ボタンのドロップダウン矢印をクリックします。このボタンは、電子メールの件名と本文のそれぞれに1つずつあります。

Email title:	Threat Alert	Data Inputs 🗸
Email message body:	An endpoint has recently encountered a threat: Hostname: [hostname] Group Name: [groupname] Policy Name: [policyname] Keycode: [keycode] Threat List: [infectionlist.filename,malwaregroup,pathname,md5,dwelltim e]	Hostname Group Name Group Description Policy Name Keycode Current User Console Name

Email title:	Threat Alert		Data Inputs 🔹
Email message body:	An endpoint has recently encountered a threat:	1	Data Inputs 👻
	Hostname: [hostname]		Hostname
	Group Name: [groupname] Policy Name: [policyname]	Ш	Group Name
	Keycode: [keycode]	Ш	Group Description
	Threat List:	Ш	Policy Name
	e]		First Seen
		t	Last Seen
		t	Last Threat
Cancel	4 Previous	T	Operating System
Guildor		•	Agent Version
		Т	IP Address
		L	MAC Address
		L	Country Code
			Keycode
			Current User
			Workgroup
			Active Directory
			Console Name

12. データ入力項目を選択します。それぞれの項目について以下の表で説明します。

**注意**: 定義する警告メッセージのタイプに応じて、該当するデータ入力項目のみがドロップダウンメニューに表示されます。

データ入力	説明	
ホスト名	警告を発信するエンドポイントの名前。	
グループ名	警告を発信するエンドポイントに割り当てられたグループ。	
グループの説明	警告を発信するエンドポイントに割り当てられたグループの説明。	
ポリシー名	警告を発信するエンドポイントに割り当てられたポリシー。	
אב-+	警告を発信するエンドポイントで使用するキーコード。	
現在のユーザー	警告を発信するエンドポイントのユーザー。	
コンソール名	エンドポイントが含まれるコンソールの名前。	
初回確認日時	このイベントが最初に検出された日時。	
最終確認日時	このイベントが最後に検出された日時。	
最近の感染	警告を発信するエンドポイントが最後に感染した日時。	

データ入力	説明	
OS	警告を発信するエンドポイントのOS のバージョン。	
エージェントのバージョン	警告を発信するエンドポイントにインストールされている SecureAnywhere ソフトウェアのバージョン番号。	
MAC アドレス	警告を発信するエンドポイントがインストールされているネットワークの Media Access Control (MAC) アドレス。	
ワークグループ	エンドポイントがあるネットワークのワークグループ(該当する場合)。	
Active Directory	Active Directory の名前。	
感染リスト	感染の一覧。	
感染の概要	感染の概要。	
インストールの概要	SecureAnywhere のインストールの概要。	

**注意:** ワークグループと Active Directory のデータポイントは共に、Mac エージェントでサポートされていません。

- 13. 電子メールメッセージを表示するには、[プレビュー]をクリックします。
- 14. メッセージの作成が完了したら、[終了]をクリックします。

### 定義済みの警告メッセージの表示

すべてのカスタムの警告は、[警告] タブに [アクティブ] の状態で表示されます。このタブで警告の行をダブルク リックすることで、その警告を編集することができます。

パネルの右側には、定義した配信先リストが表示されます。

Status Policies Group	Management Reports A	lerts Overrides Logs	Resources			
Alerts	☑ Alerts					
🔂 Create 🛛 🖨 Delete 🛛 🖓 Suspend			🕒 Create   🖨 Delete			
Alert Name	Alert Type	Date Created A	Status		List Name	Email A
Infection Alert 1	Infection detected	Apr 26th 2013, 09:20	Active	*	US	000wrs
Infection Summary	Infection Summary	Apr 26th 2013, 09:22	Active		Max	MaxNa
Resumen de instalación	Install Summary	Apr 26th 2013, 10:49	Suspended		JA	a@b.ci
Infection Summary 2	Infection Summary	Apr 26th 2013, 11:49	Active			
Installation Alert	Endpoint installed	May 4th 2013, 10:23	Active			

必要に応じて、警告メッセージに関する追加データの表示と非表示を切り替えることができます。

#### 定義済みの警告メッセージを表示するには

- 1. カラム見出しをクリックしてドロップダウンメニューを開き、次のいずれかの操作を行います。
  - チェックボックスを選択してカラムを追加する。
  - チェックボックスの選択を解除してカラムを削除する。



カラム内の情報について、次の表で説明します。

#### 第9章: 警告の管理

カラム	説明		
警告の名前	[警告の作成] ウィザードで定義された名前。これは静的なデータ で、非表示にはできません。		
	次のいずれかの警告タイプを表示します。		
警告のタイプ	<ul> <li>・感染が検出されました</li> <li>・エンドポイントがインストールされました</li> <li>・感染の概要</li> <li>・インストールの概要</li> </ul>		
配信先リストt	この警告の電子メールの受信者。		
作成日	警告メッセージが定義された日付。		
作成者	警告メッセージを作成した管理者。		
編集日	警告メッセージが変更された日付 (該当する場合)。		
編集者	警告メッセージを変更した管理者 (該当する場合)。		
状態	警告の状態 ([アクティブ] または [一時停止])。		

### 警告の一時停止または削除

配信先リストの警告メッセージをカスタマイズした後に、警告が必要なくなることがあります。このような場合、 警告を完全に削除することができます。将来的に再使用する可能性がある場合は、一時的に停止すること も可能です。

警告を一時停止または削除するには

- 1. [警告] タブをクリックします。
- 2. [警告の名前] フィールドで警告を選択します。
- 3. コマンドメニューバーの[削除] または [一時停止] アイコンをクリックします。

Status Policies Group Managem	ent Reports Alerts Overrides
Alerts	
Create	)
Alert Name	Alert Type
Infection Alert 13	Infection detected
Infection Alert 14	Infection detected
Infection Alert 15	Infection detected
Installation Alert 26	Endpoint installed
Installation Alert 27	Endpoint installed

- [一時停止]を選択すると、カラムの警告がグレー表示され、[状態] カラムに [一時停止] と表示されます。後で再使用する場合、警告を再度選択し、[**再開**] をクリックします。
- [削除]を選択した場合は、確認のメッセージが表示されたら [ はい] をクリックします。 警告はエンド ポイントプロテクションから完全に削除されます。
# 第10章:オーバーライドの使用

オーバーライドの使用方法については、以下のトピックを参照してください。

オーバーライドの導入	
ブラックリストのオーバーライドの作成	
ホワイトリストのオーバーライドの作成	
オーバーライド  タブからのオーバーライドの適用	
グループからのファイルへのオーバーライドの適用	
レポートからのファイルへのオーバーライドの適用	
滞留時間のポップアップからのオーバーライドの適用	
オーバーライドの表示	
スプレッドシートへのオーバーライドのエクスポート	
オーバーライドの削除	

### オーバーライドの導入

オーバーライドにより、環境内のファイルとアプリケーションを管理し、ファイルが正当(常に実行)または不正(常に隔離)かを指定できます。例:

- 特定のビジネスの目的で使用する正当なファイルを隔離するよう設定することができます。たとえば、ユーザーに対し営業時間中のSkype 通話を許可しない場合、スキャン中に検出されたSkypeの実行可能ファイルを必ず隔離するようオーバーライドを設定することができます。
- 反対に、許可するファイルがエンドポイントプロテクションにより隔離されている場合は、スキャン中にそのファ イルを無視するようオーバーライドを設定することが可能です。
- 1 つのオーバーライドにグローバルレベルとポリシーレベルで異なる設定を指定することができます。ポリシーの設定はグループの設定よりも優先されることに注意してください。

**注意:** オーバーライドを完全に管理するには、[オーバーライド]の[MD5]と[オーバーライド]の [判定の範囲]のアクセス権限が必要です。権限の変更については、「<u>コンソールユーザーの権限設</u> 定ページ75」を参照してください。

ファイルの検出と管理の方法を変更するには、次のいずれかのオーバーライドを適用します。

- 正当 エンドポイントでのファイルの実行を常に許可します。スキャン中にこのファイルを検出せず、隔離も行いません。
- 不正 スキャン中に検出された場合、常にファイルを隔離します。

以下の複数の場所から、オーバーライドを追加できます。

[オーバーライド] タブ - 任意の種類のファイルに対して [正当] または [不正] のオーバーライドを作成できます。このためには、まずエンドポイントをスキャンしてスキャンログを保存し、ファイルの MD5 値を特定する必要があります。MD5 (メッセージダイジェストアルゴリズム 5) とは、128 ビット値を生成し、指紋のように動作してファイルを一意に識別する暗号学的ハッシュ関数です。

詳細については、「 /オーバーライド / タブからのオーバーライドの適用 ページ439」を参照してください。

• [グループの管理] タブ - 脅威が検出されたエンドポイントを検索し、オーバーライドをすばやく適用することができます。 ファイルの MD5 値はすでに特定されています。

詳細については、「<u>グループからのファイルへのオーバーライドの適用ページ446</u>」を参照してください。

• [レポート] タブ - 特定のレポートで脅威が検出されたエンドポイントを検索し、オーバーライドをすばやく適用することができます。ファイルの MD5 値はすでに特定されています。

詳細については、「レポートからのファイルへのオーバーライドの適用ページ454」を参照してください。

• 滞留時間のポップアップ - このポップアップ内で MD5 のオーバーライドを作成することができます。

詳細については、「滞留時間のポップアップからのオーバーライドの適用ページ459」を参照してください。

# ブラックリストのオーバーライドの作成

エンドポイントプロテクションのコンソールの [オーバーライド] パネルで、ブラックリストのオーバーライドを作成することができます。

#### ブラックリストのオーバーライドを作成するには

1. <u>エンドポイントプロテクションのコンソール</u>にログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Seci	<b>ire</b> Anywher	e.				
Home	Endpoint Protection	Support				
Status	Policies Group Managen	nent Report	s Overrides	Alerts	Settings Logs	Resources
🖳 Status		«	Endpoints enco	ountering t	threats (last 7 days)	)
We recommendpoint has no the assisted	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation ena- igned policy.	on s bbled				

2. [**オーバーライド**] タブをクリックします。

Seci	ireAnywhere.
Home	Endpoint Protection Support
Status	Policies Group Management Report Overrides Alerts Settings Logs Resources
🛄 Status	Endpoints encountering threats (last 7 days)
We recomendpoint hon the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation enabled gned policy.

[ホワイトリスト] タブがアクティブになった状態で [オーバーライド] パネルが表示されます。

Se	BR	<b>ure</b> Anywhere.				
Н	ome	Endpoint Protection S	upport			
Stat	us	Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	S	
File	& F	older Overrides Web Overrides				
Wh	telis	Blacklist				
Whit	elist					
G c	reat	e   😑 Delete   🔄 Import				
		Override Name	MD5	Path Mask	File Mask	
1	1 🗖 Test 4					
2		Test 3				
3		Test 2				
4		Test 1				

[ホワイトリスト] タブがアクティブになった状態で [オーバーライド] パネルが表示されます。

S	Secure Anywhere.							
Н	Home Endpoint Protection Support							
Sta	tus	Policies Group Management	Reports Over	rides Alerts	Settings	Logs	Resources	
File	e & F	older Overrides Web Overrides						
W	itelis	Blacklist						
Whi	telist							
0	🔂 Create   😑 Delete   🖑 Import							
		Override Name	MD5		Path Mask			File Mask
1		Test 4				,		
2	2 🔽 Test 3							
3		Test 2						
4		Test 1					· · · ,	

3. [**ブラックリスト**] タブをクリックします。

Se	Secure Anywhere.						
Hom	Home Endpoint Protection Support						
Status	Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	S			
File & White	File & Folder Overrides     Web Overrides       Whitelist     Blacklist						
🔂 Cre	ate   😑 Delete   ቭ Import						
	Override Name	MD5	Path Mask	File Mask			
1	1 Test 4 c:\windows\system32\drivers\ cmgfve.sy						
2	Test 3		c:\program files\dell\dell data pro	cmgsystray.exe			
3	Test 2		C:\Windows\System32\	EmsServiceHelper.exe			
4	Test 1		c:\program files\dell\dell data pro	cmgshellext.dll			

[ブラックリスト] タブが表示されます。

Secure Anywhere.						
Home Endpoint Protection Support						
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
File & Folder Overrides Web Overrides	File & Folder Overrides Web Overrides					
Whitelist Blacklist						
Blacklist						
🔁 Create   😑 Delete   🔄 Import						
Override Name MD5 Common Filename						
1 🔲 📑 Blacklisted						

4. [作成] ボタンをクリックします。

Secure Anywhere.						
Home Endpoint Protection	Support					
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
File & Folder Overrides Web Override	File & Folder Overrides Web Overrides					
Whitelist Blacklist						
Blacklist						
🔁 Create ) 🖨 Delete   🖧 Import						
Override Name MD5 Common Filename						
1 🔲 📄 Blacklisted						

[オーバーライドの作成] ウィンドウが表示されます。

ウェブルートエンドポイントプロテクション管理者ガイド

Create override		×
Override Name:		
Override Type	Apply to a policy	
MD5:	Apply to a policy:  No Ves	
	Save Cancel	

5. [オーバーライド名] フィールドにオーバーライドの名前を入力します。

Create override		X
Override Name:		
Override Type	Apply to a policy Apply to a policy:   No Yes	
	Save Cancel	

6. [MD5] フィールドに、32 文字の英数字から成るファイルの一意の識別子を入力します。

Create override			×
Override Name:			
Override Type	Apply to a policy		]
MD5:	Apply to a policy:	No	O Yes
	Save Cancel		

7. [いいえ] または [はい] の [1 つのポリシーに適用] ラジオボタンを選択します。

Create override		×
Override Name:		
Override Type	Apply to a policy	
MD5:	Apply to a policy:  No Yes	
	Save Cancel	

8. 設定が完了したら[保存]ボタンをクリックします。

Create override		×
Override Name:		
Override Type	Apply to Policy	
MD5:	Apply to Policy:  No  Yes	
	Save Cancel	

ウェブルートエンドポイントプロテクション管理者ガイド

# ホワイトリストのオーバーライドの作成

グローバル規模のホワイトリストのオーバーライドを、これまでのエンドポイントプロテクションの MD5 (メッセージ ダイジェストアルゴリズム 5) レベルだけでなく、ファイルやフォルダのレベルでも設定できるようになりました。この アップグレードによって、より柔軟にオーバーライドを配備できるようになりました。たとえば、複数の関連する MD5オーバーライドを個別にホワイトリスト化せずに、関連ディレクトリ全体を一括でホワイトリスト化すること ができます。

注意:除外やオーバーライドを設定する前にファイルを検出または削除した場合は、アンインストール してから再インストールするか、検出したファイルを隔離から復元しておく必要があります。ファイルが ローカルで隔離されたままの状態、または[ブロック/許可]タブ内にある状態では除外は適用されま せん。

#### ホワイトリストのオーバーライドを作成するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.	
Home Endpoint Protection Supp	ort
Status Policies Group Management	Reports Overrides Alerts Settings Logs Resources
🔤 Status	Endpoints encountering threats (last 7 days)
Alert <u>Indpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	

2. [**オーバーライド**] タブをクリックします。

Secure Anywhere	2
Home Endpoint Protection	Support
Status Policies Group Manageme	ent Report Overrides Alerts Settings Logs Resources
🔤 Status	K Endpoints encountering threats (last 7 days)
We recommend you check whether this endpoint has automatic remediation enable on the assigned policy.	led

3. [ホワイトリスト] タブがアクティブになった状態で [オーバーライド] パネルが表示されます。

Se	Secure Anywhere.							
H	ome	Endpoint Protection S	upport					
Stat	us	Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	s			
File	& F	older Overrides Web Overrides						
Wh	telis	Blacklist						
Whit	elist							
😲 C	reate	e   😑 Delete   🔁 Import						
		Override Name	MD5	Path Mask	File Mask			
1		Test 4						
2		Test 3		1, 2, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,				
3		Test 2						
4		Test 1						

4. [作成] ボタンをクリックします。

Secure Anywhere.							
Home Endpoint Protection S	upport						
Status Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	S				
File & Folder Overrides Web Overrides	1						
Whitelist Blacklist							
Whitelist							
🕒 Create 🖨 Delete   🛃 Import							
Override Name	MD5	Path Mask	File Mask				
1 🔲 Test 4		c:\windows\system32\drivers\	cmgfve.sy				
2 🔲 Test 3		c:\program files\dell\dell data pro	cmgsystray.exe				
3 Test 2		C:\Windows\System32\	EmsServiceHelper.exe				
4 🔲 Test 1		c:\program files\dell\dell data pro	cmgshellext.dll				

### [オーバーライドの作成] ウィンドウが表示されます。

Create override						×
Override Name: Override Type Override Type:	MD5	O Path/File	Apply to a policy Apply to a policy:	No	Ves	
MD5:		Save	Cancel			

5. [オーバーライド名] フィールドにオーバーライドの名前を入力します。

Create override Override Name:						×
Override Type Override Type: MD5:	€ MD5	O Path/File	Apply to a policy — Apply to a policy:	No	) Yes	
		Save	Cancel			

- 6. 以下のいずれかの操作を行います。
  - 設定が完了したら[保存]ボタンをクリックします。
  - フォルダ / ファイルのオーバーライドを作成するには、この手順を続行します。

注意: ファイル / フォルダのオーバーライドを使用するには、エンドポイントが Webroot SecureAnywhere Endpoint Protection のバージョン 9.0.1 以降を使用していることを確認してくだ さい。それより前のバージョンでは MD5 のオーバーライドにしか対応していません。

7. [新規ホワイトリストエントリ] ウィンドウで、[パス/ファイル] ラジオボタンを選択します。

Create override						×
Override Name:			- Apply to Policy			
Override Type: MD5:	MD5	Path/File	Apply to Policy:	No	Yes	
		Save	Cancel			

[オーバーライドの作成] ウィンドウに、関連するフィールドが表示されます。

Create override						٥
Override Name:						
Override Type				Apply to Policy		
File / Folder or running version	verric on 9.0	les will only be : 1.1 and higher.	supported by endpoints	Apply to Policy:	No	Yes
Override Type:		MD5	Path/File			
File Mask:	0	e.g. notepad.e	xe			
Path Mask:	0	Type % for su	pported system variable 💙			
Include Sub-folders:						
Detect if Malicious:	0	Yes	No			
			Save	Cancel		

8. 次の表を参照して各フィールドに情報を入力します。

フィールド	説明
オーバーライド名	オーバーライドの名前を入力します。
オーバーライドの種類	[パス/ファイル] ラジオボタンをすでに選択しています。
ファイルマスク	オプションのワイルドカードでファイルマスクを指定し、ファイルやファイ ルのグループを絞り込みます (例:選択したフォルダ内のすべての実 行可能ファイルを対象とする場合は *.exe)。指定がない場合はデ フォルトとして、選択したフォルダ / パス内のすべてのファイルが対象 になります。

フィールド	説明
	オーバーライドの対象となるフォルダです。次のような絶対パスを指定することができます。
	x:\myfolder\ または、次のようにシステム変数と任意のパスを指定できます。
パス / フォルダマスク	%SystemDrive%\myfolder.
	デフォルト でサポートされている環境変数は "%" (パーセント記号) を入力すると表示されます。対象のコンピュータ上で設定済みの変 数もすべて使用できます。ただし、サポートされていないユーザー変 数を除きます。たとえば、"%temp%" は特定のユーザーー 時ディレク トリ('username/temp/') であるため使用できません。 ワイルドカードは サポートされていません。
サブフォルダを含める	対象フォルダ内のすべてのサブフォルダにオーバーライドを適用する 場合に、このチェックボックスを選択します。
悪意のある場合は検出	この設定が有効になっている場合、ウェブルートは引き続き、指定 のファイル/フォルダのホワイトリストのオーバーライドにより発生する 脅威からユーザーを保護しますが、監視およびジャーナルは無効に なります。この機能は主に、大量の未判定のファイルに監視とジャー ナルを適用する際、パフォーマンスを向上するために使用します。こ の設定を無効にすると完全なホワイトリスト作成が可能になり、ウェ ブルートの保護なしでファイルを実行することができます。

フィールド	説明
グローバル (GSM) オーバー ライド	 これを選択すると、現在のGSM コンソールにあるすべてのサイトに ついてオーバーライドがグローバルに設定されます。
ポリシーに適用	以下のいずれかの操作を行います。 • グローバルポリシーを含む特定のポリシーにオーバーライドを適用 する場合は [はい] を選択します。 • 選択したサイトにすべてのポリシーに適用する場合は [いいえ] を 選択します。

9. 設定が完了したら[保存]ボタンをクリックします。

Create override						×
Override Name:						
Override Type			Apply to Policy			
File / Folder or running versio	verrides will only b n 9.0.1 and higher	e supported by endpoints	Apply to Policy:	No	Yes	
Override Type:	MD5	Path/File				
File Mask:	@ e.g. notepad	i.exe				
Path Mask:	Type % for s	supported system variable 💙				
Include Sub-folders:						
Detect if Malicious:	🕜 💿 Yes	No				
		Save	Cancel			

# [オーバーライド] タブからのオーバーライドの適用

[オーバーライド] タブからオーバーライドを適用する際は、まずエンドポイントでスキャンを実行し、ファイルの MD5 値を特定する必要があります。SecureAnywhere がデバイスをスキャンすると、実行可能ファイルやプロセ スを実行する他のタイプのファイルのパス名、ファイル名、MD5 値を保存したスキャンログが作成されます。 オーバーライドを作成するには、その MD5 値が必要になります。

[不正] と指定されたファイルをオーバーライドする場合は、[グループ] タブまたは [レポート] タブを使用します。 これらのタブには検出された脅威と関連する MD5 値が表示されるため、[不正] オーバーライドの作成の手 間が省けます。

この手順には2つの段階があります。

- <u>MD5</u> 値の特定と保存
- MD5 値の追加

注意: この手順は Windows コンピュータでしか実行できません。

#### MD5 値を特定して保存するには

1. エンドポイントでスキャンを実行して MD5 値を取得します。

[スキャン] コマンドを実行する場合は、エンドポイントそのものから実行するか、[グループ] タブの [スキャン] コマンドを使用します。詳細については、「エンドポイントへのコマンドの発行ページ144」を参照してください。

- 2. PC やその他のデバイスなどのエンドポイントで Secure Anywhere を開きます。
- 3. [システムツール] タブをクリックします。
- 4. 左側のペインで [レポート]を選択します。
- 5. 開かれたページの[スキャンログ] セクションで、[名前を付けて保存]ボタンをクリックし、ログのファイル名 と場所を指定します。

Overview     PC Security     Identity & Privacy     System Tools     My Account       System Cleaner     System Control     Scan Log       System Control     You may save a scan log, which Technical Support uses for diagnostics.       Reports     Save as       Submit a File     Protection Statistics       SecureAnywhere constantly monitors your computer for threats. Click the button below to see detailed information on what is taking place in your computer in the background	Secure Any	where.
System Cleaner       Scan Log         System Control       You may save a scan log, which Technical Support uses for diagnostics.         Reports       Save as         Submit a File       Protection Statistics         SecureAnywhere constantly monitors your computer for threats. Click the button below to see detailed information on what is taking place in your computer in the background	Overview	PC Security Identity & Privacy System Tools My Account
Reports     Save as     Clear Log       Submit a File     Protection Statistics       SecureAnywhere constantly monitors your computer for threats. Click the button below to see detailed information on what is taking place in your computer in the background.	System Cleaner System Control	Scan Log You may save a scan log, which Technical Support uses for diagnostics.
Submit a File Protection Statistics SecureAnywhere constantly monitors your computer for threats. Click the button below to see detailed information on what is taking place in your computer in the background	Reports	Save as Clear Log
	Submit a File	Protection Statistics SecureAnywhere constantly monitors your computer for threats. Click the button below to see detailed information on what is taking place in your computer in the background.

6. スキャンログを開くと、ファイル名の右側に MD5 値が記載されています。

以下に、"csrss.exe"という名前のファイルの MD5 値の例を示します。



7. 値をコピーして管理ポータルに貼り付けます。

[オーバーライド] タブから MD5 オーバーライドを追加するには

1. <u>エンドポイントプロテクションのコンソールにロ</u>グインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Seci	<b>ire</b> Anywher	e.				
Home	Endpoint Protection	Support				
Status	Policies Group Manager	nent Report	overrides	Alerts	Settings Logs	Resources
🛄 Status		<ul> <li></li> </ul>	Endpoints enco	untering t	threats (last 7 days)	)
We recom endpoint h on the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether thi as automatic remediation end igned policy.	on s abled				

2. [**オーバーライド**] タブをクリックします。

Seci	ure Anywher	e.				
Home	Endpoint Protection	Support				
Status	Policies Group Managen	nent Report	Overrides	Alerts	Settings Logs	Resources
E Status		<u>«</u>	Endpoints enco	untering t	hreats (last 7 days)	;)
We recommendpoint hon the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this has automatic remediation enabling signed policy.	n ibled				

[ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。

S	Secure Anywhere.								
H	Home Endpoint Protection Support								
Sta	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources							1	
File	File & Folder Overrides Web Overrides								
Wh	Whitelist Blacklist								
Whit	elist								
00	reate	e   😑 Delete   🔄 Import							
		Override Name MD5			Path Mask			File Mask	
1	Test 4								
2	Test 3			· · · · · · · · · · · · · · · · · · ·					
3		Test 2							
4		Test 1				· · · · · · · · · · · · · · ·			

3. [作成] アイコンをクリックします。

Secure Anywhere.								
Home Endpoint Protection St	Home Endpoint Protection Support							
Status Policies Group Management	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources							
File & Folder Overrides Web Overrides	File & Folder Overrides Web Overrides							
Whitelist Blacklist								
Whitelist								
🔁 Create 😂 Delete   🐑 Import								
Override Name	MD5	Path Mask	File Mask					
1 🔲 Test 4								
2 🔲 Test 3		· · · · · · · · · · · · · · · · · · ·						
3 🔲 Test 2								
4 🔲 Test 1								

[オーバーライドの作成] ウィンドウが表示されます。

Create override						×
Override Name:						
Override Type			Apply to a policy			_
Override Type:	MD5	Path/File	Apply to a policy:	No	O Yes	
MD5:			]			
		Save	Cancel			

4. [オーバーライド名] フィールドにオーバーライドの名前を入力します。

Create override						×
Override Name:						
Override Type			Apply to a policy			
Override Type:	MD5	Path/File	Apply to a policy:	No	O Yes	
MD5:			]			
		Save	Cancel			

5. [オーバーライドの種類]のエリアで、[MD5] ラジオボタンを選択します。

Create override		×
Override Name:		
Override Type	Apply to a policy	
Override Type:	MD5 Path/File Apply to a policy:      No Yes	
MD5:		
	Save Cancel	

6. [MD5] フィールドで、コピーした MD5 値を貼り付けます。

Create override						
Override Name:						
Override Type			Apply to a policy			_
Override Type:	MD5	O Path/File	Apply to a policy:	No	O Yes	
MD5:						
		Save	Cancel			

- 7. [1 つのポリシーに適用] エリアで、次のいずれかの操作を行います。
  - ポリシーを適用しない場合は、[いいえ] ラジオボタンを選択します。

Create override			(i
Override Name:			Apply to a policy
MD5:	• MD5	Path/File	Apply to a policy: No Yes

• 1 つのポリシーにオーバーライドを適用する場合は、[はい] ラジオボタンを選択します。続いて、ポリ シー選択用のドロップダウンメニューで、オーバーライドを適用するポリシーを選択します。

Create override			X
Override Name:			
Override Type Override Type: MD5:	MD5	O Path/File	Apply to a policy Apply to a policy: No Yes Select a policy to populate
		Save	Cancel

**注意:** グローバルにオーバーライドを適用することも、単一のポリシーに適用することもできます。ただし、両方を行うことはできません。

8. 設定が完了したら[保存]ボタンをクリックします。

Create override						×
Override Name:						
Override Type			Apply to a policy			
Override Type:	MD5	Path/File	Apply to a policy:	O No	Yes	
MD5:			Select a policy to populate this window:			~
		Save	Cancel			

 SecureAnywhere がファイルを検出する方法をテストするには、[すべてのファイルとプロセスを再検証する] コマンドをそのエンドポイントに送信します。詳細については、「エンドポイントへのコマンドの発行 ページ144」を参照してください。

### グループからのファイルへのオーバーライドの適用

グループのレベルから、脅威として指定されたファイルにオーバーライドを適用することができます。これにより、 今後そのファイルが再び検出および隔離されることはなくなります。

#### グループからオーバーライドを適用するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.							
Home	Endpoint Protection	Support					
Status	Policies Group Manager	nent Repor	overrides	Alerts	Settings	Logs	Resources
🛄 Status		«	Endpoints enco	untering	threats (last )	7 days)	
We recommendpoint has no the assisted	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation end igned policy.	on s bled					

2. [**グループの管理**] タブをクリックします。

Secure Anywhere.					
Home Endpoint Protection Supp	ort				
Status Policies Group Management F	Reports Overrides Alerts Settings Logs Resources				
🔄 Status 🔍	🖳 Endpoints encountering threats (last 7 days)				
We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.					

[グループ] タブがアクティブになった状態で [グループの管理] タブが表示されます。

Secure Anywhere.				
Home Endpoint Pro	tection Supp	oort		
Status Policies Group	Management	Reports Overrides Alerts Settings Logs	Resources	
Groups Views Search	n < Ø	Endpoints		
🕒 Create   F Actions -		Hostname	Policy	
Group Name	No.			
All Endpoints	14			
Deactivated Endpoints	78			
Default Group	9			
Bracknell	0			
Broomfield	0			
Dublin	0			
Mac OS X Systems	0			
RemoteUS	0			
Server	0			
Servers	0			
Sydney	3			
Tokyo	0			
Tradeshow	2			
Workstations	0			

3. 左側のペインで、ファイルが検出されたエンドポイントのグループを選択します。

Secure Anywhere.					
Home Endpoint Prot	ection Supp	ort			
Status Policies Group	Management	Reports Overrides Alerts Settings Logs	Resources		
Groups Views Search	* *	Endpoints			
🔂 Create   🛐 Actions 🗸		Hostname	Policy		
Group Name	No.				
All Endpoints	14				
Deactivated Endpoints	78				
Default Group	9				
Bracknell	0				
Broomfield	0				
Dublin	0				
Mac OS X Systems	0				
RemoteUS	0				
Server	0				
Servers	0				
Sydney	3				
Tokyo	0				
Tradeshow	2				
Workstations	0				

エンドポイントのリストが表示されます。

Secure Anywhere.							
Home Endpoint P	Home Endpoint Protection Support						
Status Policies Gro	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
Groups Views Sea	irch < 🕫	Endpoints in Default Group					
😌 Create   🛐 Actions 🗸 🔚 Save Changes   🔄 Undo Changes   🌄 Move endpoints to another group   📃 Apply policy to endpoints   📢 Agent Co				/ to endpoints   📢 Agent Comma			
Group Name	No.	Hostname	Policy	Status			
All Endpoints	14	1 AB-WIN10-DEMO	Unmanaged	Protected			
Deactivated Endpoints	78	2 WRDemoEP01	Demo Policy (Do Not Edit)	🔶 Not Seen Recently			
Default Group	9	3 WRDEMOEP05	No Remediation	🐠 Not Seen Recently			
Bracknell	0	4 WRDemoEP05	No Remediation	Needs Attention			
Broomfield	0	5 WRDemoEP06	Standard Workstation Policy	🔶 Not Seen Recently			
Dublin	0	6 🔲 📕 WRDEMOEP11-W8-L	Standard Workstation Policy	🔶 Not Seen Recently			
Mac OS X Systems	0	7 🔲 📑 WRDEMOEP14	No Remediation	🔶 Not Seen Recently			
RemoteUS	0	8 🔲 📕 WRDEMOEP15	Standard Workstation Policy	🔶 Not Seen Recently			
Server	0	9 🔲 📑 WRDemoSVR01	Recommended Server Defaults	Protected			

4. 右側のペインで、ファイルが検出されたエンドポイントを選択します。

Secure Anywhere.							
Home Endpoint	Home Endpoint Protection Support						
Status Policies C	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
Groups Views S	Search < 🕫	🖳 Endpoints in Default Group					
🕒 Create   F Actions	•	🔚 Save Changes   늘 Undo Changes   🌄 Move et	ndpoints to another group   🖪 Apply policy to	o endpoints   🛒 Agent Commar			
Group Name	No.	Hostname	Policy	Status			
All Endpoints	14	1 AB-WIN10-DEMO	Unmanaged	Protected			
Deactivated Endpoints	78	2 WRDemoEP01	Demo Policy (Do Not Edit)	🔶 Not Seen Recently			
Default Group	9	3 WRDEMOEP05	No Remediation	🔶 Not Seen Recently			
Bracknell	0	4 WRDemoEP05	No Remediation	Needs Attention			
Broomfield	0	5 WRDemoEP06	Standard Workstation Policy	Not Seen Recently			
Dublin	0	6 WRDEMOEP11-W8-L	Standard Workstation Policy	🔶 Not Seen Recently			
Mac OS X Systems	0	7 WRDEMOEP14	No Remediation	🔶 Not Seen Recently			
RemoteUS	0	8 WRDEMOEP15	Standard Workstation Policy	🔶 Not Seen Recently			
Server	0	9 🔲 📲 WRDemoSVR01	Recommended Server Defaults	Protected			
Sanuara	0						

- 5. 下部の[スキャン履歴] リストで、次のいずれかの操作を行います。
  - [このエンドポイントで確認されたすべての脅威を表示]をクリックする
  - [状態] カラムで [表示] をクリックして、脅威が検出された日付を確認する

Sca Sca	Scan History Blocked URLs						
	Scan Start	Status	Scan Type				
1	Jul 28th 2016, 22:06	Threats detected - View	Deep Scan				
2	Jul 28th 2016, 22:01	Threats detected - View	Deep Scan				
3	Jul 28th 2016, 21:55	🥑 Clean	Deep Scan				
4	Jul 28th 2016, 11:07	O Threats detected - View	Deep Scan				

6. このダイアログで、オーバーライドを作成するファイル名のチェックボックスを選択し、[オーバーライドの作成] アイコンをクリックします。

-	All threats ever seen on this endpoint						
Q	Create override						
	1	Filename	Pathname	Malware Group	Last Seen		
		NDNUNINSTALL6_38.EXE	%windir%\	Pua.Gen	Jan 31st 2013, 16:55		
	2	LINKPAL[1].EXE	?:\documents and settings\owe	W32.Trojan.Downloader-LowZ	Jan 31st 2013, 16:55		
	3	MNMYBOH.EXE	?:\documents and settings\owe	Adware.W-find.com.Hijacker	Jan 31st 2013, 16:55		
	4	45765FBEB88468B9A7AD0E0	?:\documents and settings\owe	W32.Trojan.Trojan-iejore	Jan 31st 2013, 16:55		

#### [オーバーライドの作成] ウィンドウが表示されます。

Create override	
Determination:	¥
Description:	
Assign to a policy?:	
Overrides will not be ap	plied to Mac files
Sav	Cancel

- 7. [判定]ドロップダウンメニューで、次のいずれかを選択します。
  - 正当 ファイルの実行を常に許可します。

• 不正 - 常にファイルを隔離します。

Create override					
Determination:	v				
Description:					
Assign to a policy?:					
0 Overrides will not be appli	ied to Mac files				
Save	Cancel				

8. [説明] フィールドにオーバーライドについての説明を入力します。

Create override		
Determination:		×
Description:		
Assign to a policy?:		
Overrides will i	not be applied to Mac files	
	Save Cancel	

- 9. オーバーライドを適用するには、次のいずれかの操作を行います。
  - すべてのポリシーにオーバーライドを適用するには、[ポリシーに割り当てますか?] チェックボックスを 選択しません。
  - 個別のポリシーにオーバーライドを適用するには、[ポリシーに割り当てますか?] チェックボックスを選択しません。[ポリシー] フィールドが表示されたら、ドロップダウンメニューでポリシーを選択します。

Create override		
Determination:	Good	~
Description:		
Assign to a policy?: Policy:		~
0 Overrides will not b	be applied to Mac files	
	Save Cancel	

10. 設定が完了したら[保存]ボタンをクリックします。

Create override		
Determination:	Good	~
Description:		
Assign to a policy?: Policy:		~
Overrides will not be	applied to Mac files	
	Save Cancel	

11. ファイルの検出をテストするには、[すべてのファイルとプロセスを再検証する] コマンドをそのエンドポイントに送信します。詳細については、「エンドポイントへのコマンドの発行ページ144」を参照してください。

### レポートからのファイルへのオーバーライドの適用

[レポート] タブから、脅威として指定されたファイルにオーバーライドを適用することができます。これにより、今後そのファイルが再び検出および隔離されることはなくなります。以下のレポートから、オーバーライドを追加できます。

- [確認されたすべての脅威] レポートの生成 ページ342
- *[確認されたすべての未判定のソフトウェア] レポートの生成 ページ349*
- [最新のスキャンで脅威が存在したエンドポイント] レポートの生成ページ361 [このエンドポイントで確認された脅威] パネル内、個々のエンドポイントのみ。
- [最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートの生成ページ365 [このエンドポイントで確認されたすべての未判定のソフトウェア] パネル内、個々のエンドポイントのみ。

#### レポートからオーバーライドを適用するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.	
Home Endpoint Protection Suppo	ort
Status Policies Group Management R	Reports Overrides Alerts Settings Logs Resources
🛄 Status 🔍	Redpoints encountering threats (last 7 days)
Alert <u>Indpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	

2. [レポート] タブをクリックします。

Secure Anywhere.	
Home Endpoint Protection Supp	ort
Status Policies Group Managemen F	Reports Verrides Alerts Settings Logs Resources
🕎 Status 🔍	Endpoints encountering threats (last 7 days)
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	

[レポート] タブが表示されます。

Secure Anywhere.	
Home Endpoint Protection Support	
Status Policies Group Management Reports	Overrides Alerts Settings Logs Resources
Select your report	All URLs Blocked (Jun 27 10:28) 🛞
Report Type:	💱 All URLs Blocked
All URLs Blocked 🗸	URL Categor
Policy:	
All 👻	
Group:	
All 👻	
Select time period	
Include deactivated and hidden	
Submit	

- 3. [**レポートの種類**]ドロップダウンメニューで前述したレポートのいずれかを選択し、[**送信**] ボタンをクリック してレポートを生成します。
- 4. [確認されたすべての脅威] エリアでファイル名を選択し、コマンドバーの [オーバーライドの作成] アイコンをクリックします。



[オーバーライドの作成] ウィンドウが表示されます。

Create override		
Determination:		*
Description:		
Assign to a policy?:		
Overrides will not t	be applied to Mac files	
	Save Cancel	

- 5. [判定]ドロップダウンメニューで、次のいずれかを選択します。
  - 正当 ファイルの実行を常に許可します。
  - 不正 常にファイルを隔離します。

Create override	
Determination:	~
Description:	
Assign to a policy?:	
0verrides will not be appli	ied to Mac files
Save	Cancel

- 6. オーバーライドを適用するには、次のいずれかの操作を行います。
  - すべてのポリシーにオーバーライドを適用するには、[ポリシーに割り当てますか?] チェックボックスを 選択しません。

• オーバーライド対象のポリシーを個別に選択するには、[ポリシーに割り当てますか?] チェックボックス を選択しません。[ポリシー] フィールドが表示されたら、[ポリシー] ドロップダウンメニューでポリシーを 選択します。

Create override		
Determination:	Good	~
Description:		
Assign to a policy?		
Policy:	*	~
Overrides will not be a	pplied to Mac files	
S	Cancel	

7. 設定が完了したら[保存]ボタンをクリックします。

Create override		
Determination:	Good	¥
Description:		
Assign to a policy?:	<ul> <li>Image: A start of the start of</li></ul>	
Policy:		*
0 Overrides will not b	e applied to Mac files	
	Save Cancel	

8. ファイルの検出をテストするには、[**すべてのファイルとプロセスを再検証する**] コマンドをそのエンドポイントに送信します。詳細については、「エンドポイントへのコマンドの発行ページ144」を参照してください。
# 滞留時間のポップアップからのオーバーライドの適用

滞留時間のポップアップから、脅威として指定されたファイルにオーバーライドを適用することができます。これにより、今後そのファイルが再び検出および隔離されることはなくなります。

### 滞留時間のポップアップからオーバーライドを適用するには

1. <u>エンドポイントプロテクションのコンソール</u>にログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere	2
Home Endpoint Protection	Support
Status Policies Group Manageme	ent Reports Overrides Alerts Settings Logs Resources
🕎 Status	< li>Endpoints encountering threats (last 7 days)
We recommend you check whether this endpoint has automatic remediation enable on the assigned policy.	1 Died

2. [脅威が存在した最近の50個のエンドポイント] エリアで、オーバーライドを作成するアイテムの[表示] リンクをクリックします。



[このエンドポイントでこれまでに確認されたすべての脅威] ウィンドウが表示されます。

<b>-</b>	All threats ever seen on this endpoint							
1	🎓 Create override 🛛 🚽 Show all PCS which have encountered this file 🛛 🕃 Restore from Quarantine							
		Filename	Pathname	Malware Group	Last Seen	Owell Time		
		SURIV.DLL	%windir%\system32\	W32.Suriv.Test	Jun 3rd 2015, 05:09	532 day 20 hr 1 min 37 sec		
-		MOCKVIRUS.EXE	%temp%\temp1_mockvirus	W32.Bot.Gen	Jun 3rd 2015, 05:09	532 day 20 hr 1 min 50 sec		
1		WEBROOTTESTFILE.EXE	%cache%\	W32.Webroottestfile	Jun 3rd 2015, 05:09	103 day 18 hr 1 min 52 sec		
4		SURIV.EXE	%temp%\501.tmp\	W32.Suriv.Test	Apr 22nd 2015, 14:08	491 day 5 hr 38 sec		

3. [ファイル名] カラムで、オーバーライドを作成するアイテムのリンクを選択します。

All threats ever seen on this endpoint						
🎓 Create override 🛛 💂 Show all PCS which have encountered this file 📑 Restore from Quarantine						
Filename	Pathname	Malware Group	Last Seen	Dwell Time		
1 SURIV.DLL	%windir%\system32\	W32.Suriv.Test	Jun 3rd 2015, 05:09	532 day 20 hr 1 min 37 sec		
2 MOCKVIRUS.EXE	%temp%\temp1_mockvirus	W32.Bot.Gen	Jun 3rd 2015, 05:09	532 day 20 hr 1 min 50 sec		
3 🔲 WEBROOTTESTFILE.EXE	%cache%\	W32.Webroottestfile	Jun 3rd 2015, 05:09	103 day 18 hr 1 min 52 sec		
4 SURIV.EXE	%temp%\501.tmp\	W32.Suriv.Test	Apr 22nd 2015, 14:08	491 day 5 hr 38 sec		

滞留時間のポップアップウィンドウが表示されます。

pagation Time	eline			File Information		📌 Create ove	rride
		Jan 31 2012		Determination:	Bad		
		Jul 1 2012		Malware Group:	W32.Suriv.Test		
		F	3	Global Popularity:	155		
		Nov 30 2012	LS	Console Popularity:			
	FS	May 2 2012		Determined:	Oct 9 2014, 8:45		
6		May 2 2013	•	Filename:	SURIV.DLL		
		Oct 1 2013		MD5:	0AA9E95035007D6	3D663D3156A418E2E	
	FS First Seen	S Last Seen DD D	ate Determined	Endpoints encou	ntering this file		
				CAGPSTEST1-139	14862 Aug 12	2013, 17:35	
erspective	First Seen	Last Seen	Owell Time	FHAL-3377-W7	Jan 8 2	2014, 7:26	
Globally	Aug 31 2011, 14:05	-	-	WRDemoEP05	Jun 3 2	2015, 5:09	
Console	Oct 29 2012, 9:49	Jan 15 2015, 5:07	-				
Endpoint	Dec 17 2013, 9:07	Jun 3 2015, 5:09	532 days 20 hours 1 min 37 sec	\$			

4. [オーバーライドの作成] ボタンをクリックします。

	meline			File Information		🖉 📌 Create o
1		Jan 31 2012	<b></b>	Determination:	Bad	
		Jul 1 2012		Malware Group:	W32.Suriv.Test	
		(	3	Global Popularity:	155	
		Nov 30 2012	LS	Console Popularity:		
	FS	May 2 2012		Determined:	Oct 9 2014, 8:45	
(5)		MBy 2 2013		Filename:	SURIV.DLL	
		Oct 1 2013		MD5:	0AA9E95035007	D63D663D3156A418E2
	FS First Seen	LS Last Seen DD D	ate Determined	Endpoints encoun	tering this file	
				CAGPSTEST1-1391	4862 Aug	12 2013, 17:35
erspective	First Seen	Last Seen	Ø Dwell Time	FHAL-3377-W7	Jan	8 2014, 7:26
	Aug 31 2011, 14:05	-	-	WRDemoEP05	Jun	3 2015, 5:09
Globally		Jan 15 2015, 5:07	-			
Globally	Oct 29 2012, 9:49					

## [オーバーライドの作成] ウィンドウが表示されます。

Create override		
Determination:		~
Description:		*
Assign to a policy?:		v
	Save Cancel	

- 5. [判定]ドロップダウンメニューで、次のいずれかを選択します。
  - 正当 ファイルの実行を常に許可します。
  - 不正 常にファイルを隔離します。

Create override		
Determination:		v
Description:		*
Assign to a policy?:		
(	Save Cancel	

6. [説明] フィールドにオーバーライドの情報を入力します。

Create override		
Determination:		~
Description:		Â,
Assign to a policy?:		
	Save Cancel	

- 7. オーバーライドを適用するには、次のいずれかの操作を行います。
  - 特定のポリシーにオーバーライドを適用しない場合は、[ポリシーに割り当てますか?] チェックボックス を選択しません。
  - 特定のポリシーにオーバーライドを適用する場合は、[ポリシーに割り当てますか?] チェックボックスを 選択します。

Create override	
Determination:	*
Description:	*
Assign to a policy?:	
Save Cancel	

チェックボックスを選択した場合、[ポリシー]ドロップダウンメニューが表示されます。

Determination:	Good	~
Description:	Executable file for opening documents.	* *
Assign to a policy?:		
Policy:		~

8. オーバーライドを適用するポリシーを選択します。

Create override		
Determination:	Good	*
Description:	Executable file for opening documents.	*
Assign to a policy?:		
Policy:	Broomfield_Policy	)
	Save Cancel	

**注意:** グローバルにオーバーライドを適用することも、単一のポリシーに適用することもできます。ただし、両方を行うことはできません。

9. 設定が完了したら[保存]ボタンをクリックします。

Create override							
Determination:	Good	*					
Description:	Executable file for opening documents.	*					
Assign to a policy?:	$\checkmark$						
Policy:	Broomfield_Policy	~					
	Save Cancel						

10. SecureAnywhere がファイルを検出する方法をテストするには、「すべてのファイルとプロセスを再検証する] コマンドをそのエンドポイントに送信します。詳細については、「エンドポイントへのコマンドの発行 ページ144」を参照してください。

# オーバーライドの表示

エンドポイントプロテクションに追加したオーバーライドは、[オーバーライド] タブ内に表示されます。

## オーバーライドを表示するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.							
Home	Endpoint Protection	Support					
Status	Policies Group Managen	nent Repor	ts Overrides	Alerts	Settings	Logs	Resources
🛄 Status		<ul> <li></li> </ul>	Endpoints enco	untering	threats (last	7 days)	
We recom endpoint h on the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation ena- igned policy.	on s abled					

2. [**オーバーライド**] タブをクリックします。

Secure Anywhere.							
Home Endpoint Protection S	upport						
Status Policies Group Management	Report Overrides Alerts Settings Logs Resources						
🔤 Status	K Endpoints encountering threats (last 7 days)						
We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.							

## [ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。

Secure Anywhere.							
Home Endpoint Protection Support							
Status Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	S				
File & Folder Overrides Web Override	\$						
Whitelist Blacklist							
Whitelist							
😌 Create   😑 Delete   🔄 Import							
Override Name	MD5	Path Mask	File Mask				
1 🔲 Test 4							
2 🔲 Test 3							
3 🔲 Test 2							
4 🔲 Test 1			2				

3. 左側のパネルでポリシーを選択すると、絞り込まれた結果が右側に表示されます。

選択したオーバーライドは[手動判定]カラムに表示されます。

Status Policies Group Management	Reports	Alerts Overrides	Logs Resources				
Filter Overrides by Policy	📌 Overr	ides					
Policy	Create	Create Create Export to CSV					
All Active Overrides		MD5	Common Filename	Common Pathname	Manual Determination		
All Deleted Overrides	1	986D785023059B1FEF	MEL-69047DAA0D94F	?:\documents and settin	Bad		
Policy1	2	D0361FC39D3D417C8	IMMONITOR FACEBO	%desktop%\badd_fil	Good		
Policy2	3 🕅	A9FD9F97DA98AD7D			Bad		
	4 🕅	EDE344535435FDFD5			Bad		
	5 🕅	65DFEA4535FE453FE			Good		
	6 📄	6876FDFDADFADA564			Bad		
	7 🕅	DA78DA6876A678E68			Good		
	8	A876DA87DA876D8A7			Bad		
=	9	1034ADEE5FB547997	CLICK.CAB/AXFREEA	%desktop%\spyware\n	Bad		
	10 📃	242897AAC49A46D4E	MNMYBOH.EXE	?:\hijackers\w-find.com	Bad		
	11 📃	77C92713297C1C8B4	NDNUNINSTALL6_38	%windir%\	Good		
-	14 4 1	Page 1 of 3 🕨 🕅	2				

4. オーバーライドに関する追加のデータを表示または非表示にするには、まずカラム見出しをクリックして ドロップダウンメニューを表示します。カラムを追加する場合はチェックボックスを選択し、カラムを削除す る場合はチェックボックスの選択を解除します。

▼ Date Created ★	
2↓ Sort Ascending	
Z ↓ Sort Descending	
E Columns ↔ >	MD5
	Common Pathname
	File Size
	Vendor
	Product
	Version
	Manual Determination
	Cloud Determination
	Date Created
	V Policy

カラムには次の情報が含まれています。

データ	説明
MD5	ファイルを固有に識別するための指紋のような働きをする、メッセージダイジェストア ルゴリズム 5 の値。
コマンドファイ ル名	ファイルフォルダに表示される Windows ファイルの名前。これは静的なデータで、非表示にはできません。
共通のパス 名	Windows フォルダ構造の名前。
ファイルサイ ズ	バイト単位でのファイルサイズ。
ベンダー	ファイルに関連するベンダーの名前。SecureAnywhere が情報を特定できる場合のみ。
製品	ファイルに関連する製品の名前。SecureAnywhere が情報を特定できる場合のみ。
バージョン	ファイルに関連する製品のバージョン。SecureAnywhere が情報を特定できる場合のみ。
手動判定	ユーザーによるファイルの [正当] または [不正] の指定。
クラウド判定	ウェブルートのファイル分類。[正当]、[不正]、[未判定]のいずれか。

データ	説明
作成された データ	このオーバーライドが定義された日付と時刻。
ポリシー	このオーバーライドが適用されたポリシー。

# スプレッドシートへのオーバーライドのエクスポート

すべてのオーバーライド情報をスプレッドシートにエクスポートできます。他の管理者と共に設定の確認をする場合などに便利です。

### オーバーライドの設定をエクスポートするには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.							
Home Endpoint Protection Supp	oort						
Status Policies Group Management	Reports Overrides Alerts Settings Logs Resources						
🔄 Status	Superior States (last 7 days)						
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.							

- 2. サイトコンソールで [オーバーライド] タブをクリックします。
- 3. 右側のパネルで結果を絞り込むには、左側で目的のポリシーを選択します。
- 4. コマンドメニューバーの [CSV にエクスポート] アイコンをクリックします。

Status Policies Group Management	Reports Alerts Overrides	Logs Resources
Filter Overrides by Policy	Toverrides	
Policy	😳 Create   😄 Delete 📵 Exp	ort to CSV
All Active Overrides	MD5 Cor	mmon Filena Common Pathn
All Deleted Overrides	1 📃 3ECA9C966A0 CO	MPUSPY - C ?:\
Policy1	2 D0361FC39D3 IMM	MONITOR F %desktop%_b

5. 表示されるプロンプトで、オーバーライドをCSV ファイルに保存します。

エンドポイントプロテクションが "Overrides.csv" という名前のファイルにオーバーライドを保存します。さら にファイルを保存すると、「verrides (2).csv」のように、最初の名前に数字が追加されます。

# オーバーライドの削除

この手順に従うと、ホワイトリストまたはブラックリストのオーバーライドを削除できます。

## オーバーライドを削除するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.							
Home	Endpoint Protection	Support					
Status	Policies Group Managen	nent Repor	ts Overrides	Alerts	Settings	Logs Resources	
🛄 Status		«	Endpoints enco	untering tl	hreats (last 7 d	days)	
We recom endpoint h on the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation ena- igned policy.	on 3 abled					

2. サイトコンソールで [**オーバーライド**] タブをクリックします。



[ホワイトリスト] タブがアクティブになった状態で [オーバーライド] パネルが表示されます。

Se	Secure Anywhere.							
H	Home Endpoint Protection							
Stat	us	P	olicies Group Management F	Reports Alerts Overrides	Logs Resources			
Whi	itelis	st	Blacklist					
Whit	elist							
🔁 c	reat	e	😑 Delete   🛃 Import					
			Override Name	MD5	Pathmask	Filemask		
1		9	Custom Software Absolute Pat		C:\CustomSoftware\Directory	*.*		
2	2 🔲 🌍 Custom Software System Varia %ProgramFiles%\CustomSoft *.*							
3	3 🔲 🔵 Custom Software Executable 73CEC52097EA17156C7A9B							
4	4 🔲 🚔 Media Center CABC32A5147A70B8BD7BDD							
5		9	DWPUI.EXE	09E03535460D4209C58AB59				
6			Good file	796C01FC2954524582BE28F				

3. [ホワイトリスト] または [ブラックリスト] タブで、削除するオーバーライドを選択します。

Secure Anywhere.							
Home Endpoint Protection							
Status Policies Group Management	Reports Alerts Overrides	Logs Resources					
Whitelist Blacklist							
Whitelist							
🔂 Create 🕴 🖨 Delete 🕴 🔁 Import							
Override Name	MD5	Pathmask	Filemask				
1 🔲 🌍 Custom Software Absolute Pat		C:\CustomSoftware\Directory	*.*				
2 🔲 🌍 Custom Software System Varia.		%ProgramFiles%\CustomSoft	*.*				
3 🔲 😑 Custom Software Executable	73CEC52007EA17156C7A0B						
4 🔽 📋 Media Center	CABC32A5147A70B8BD7BDD						
	09E03535460D4209058AD53						
6 🔲 🚔 Good file	796C01FC2954524582BE28F						
7 🔲 🛔 E9E0448D44E3F6836A68E61							
8 🔲 🏢	686E2BAB2D0EF0AFCEC98B						
9	C0496DD1B9ECA905BBC0E8						
10	010E6326D75CE7A7E377E8D						

[削除] ボタンが表示されます。

See	Secure Anywhere.						
Hom	Home Endpoint Protection						
Status	Status Policies Group Management Reports Alerts Overrides Logs Resources						
Whitel	ist	Blacklist					
Whitelis	st						
🔂 Crea	ate	🖨 Delete 📄 Import					
		Override Name	MD5	Pathmask	Filemask		
1	] 🔵	Custom Software Absolute Pat		C:\CustomSoftware\Directory	**		
2	] 🔵	Custom Software System Varia		%ProgramFiles%\CustomSoft	**		
3	] 🔵	Custom Software Executable	73CEC52097EA17156C7A9B				
4 🔽	1	Media Center	CABC32A5147A70B8BD7BDD				
5	]	DWPUI.EXE	09E03535460D4209C58AB59				
6		Good file	796C01FC2954524582BE28F				
7			E9E0448D44E3F6836A68E61				
8			686E2BAB2D0EF0AFCEC98B				
9	1		C0496DD1B9ECA905BBC0E8				
10			010E6326D75CE7A7E377E8D				

4. [**削除**] ボタンをクリックします。

Se	Secure Anywhere.						
Ho	Home Endpoint Protection						
Stat	Status Policies Group Management Reports Alerts Overrides Logs Resources						
Whi	telis	t	Blacklist				
White	elist	-	_				
Go	reat	1	🖨 Delete 📄 Import				
			Override Name	MD5	Pathmask	Filemask	
1		•	Custom Software Absolute Pat		C:\CustomSoftware\Directory	*.*	
2		9	Custom Software System Varia		%ProgramFiles%\CustomSoft	*.*	
3		•	Custom Software Executable	73CEC52097EA17156C7A9B			
4	☑		Media Center	CABC32A5147A70B8BD7BDD			
5		9	DWPUI.EXE	09E03535460D4209C58AB59			
6			Good file	796C01FC2954524582BE28F			
7				E9E0448D44E3F6836A68E61			
8				686E2BAB2D0EF0AFCEC98B			
9				C0496DD1B9ECA905BBC0E8			
10				010E6326D75CE7A7E377E8D			

ホワイトリスト / ブラックリストのエントリの削除を確認するウィンドウが表示されます。

Confirm	Confirm Delete							
?	Are you sure you wish to delete the selected overrides?							
	Yes No							

5. [はい] ボタンをクリックします。



オーバーライドが削除されます。

# 第11章: ウェブのオーバーライドの使用

ウェブのオーバーライドの使用方法については、以下のトピックを参照してください。

ウェブのオーバーライドの作成	480
グループの管理  でのウェブのオーバライドの作成	485
	494
ウェブのオーバーライドの編集	502
ウェブのオーバーライドの削除	506

# ウェブのオーバーライドの作成

[ウェブのオーバーライド] タブでウェブのオーバーライドを作成するには、次の手順に従ってください。

### ウェブのオーバーライドを作成するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.							
Home	Endpoint Protection	Support					
Status	Policies Group Managen	nent Report	s Overrides	Alerts	Settings	Logs	Resources
🖳 Status		«	Endpoints enco	untering t	threats (last	7 days)	
We recom endpoint h on the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation end signed policy.	on s sbled					

2. [**オーバーライド**] タブをクリックします。

Secure Anywhere.						
Home Endpoint Protection	Support					
Status Policies Group Manageme	ent Report Overrides Alerts Settings Logs Resources					
🕎 Status	Kernel Karley Endpoints encountering threats (last 7 days)					
We recommend you check whether this endpoint has automatic remediation enable on the assigned policy.	led					

## [ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。

S	BR	<b>cure</b> Anywhere.						
Н	Home Endpoint Protection Support							
Stat	us	Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	S			
File	& F	older Overrides Web Overrides	ł					
Wh	itelis	Blacklist						
Whit	elist							
🔁 C	reate	e   😑 Delete   🔄 Import						
		Override Name	MD5	Path Mask	File Mask			
1		Test 4			2			
2		Test 3		· · · · · · · · · · · · · · · · · · ·				
3		Test 2						
4		Test 1			· · · · · ·			

3. [ウェブのオーバーライド] タブをクリックします。

Secure Anywhere.							
Home Endpoint Protection Support							
Status Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	s				
File & Folder Overrides Whitelist Blacklist	File & Folder Overrides     Web Overrides       Whitelist     Blacklist						
Create   😑 Delete   🖓 Import							
Override Name	Override Name MD5 Path Mask File Mask						
1 🔲 Test 4							
2 🔲 Test 3			and a second				
3 🔲 Test 2							
4 🔲 Test 1			· · · · ·				

## [ウェブのオーバーライド] タブが表示されます。

Secure Anywhere.								
Н	Home Endpoint Protection Support							
Stat	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources							
File	& Fo	Ider Overrides Web Overrides						
Allov	v Lis	t						
🔁 C	reat	e 😑 Delete						
		URL	Date Last Modified 👻					
1	1 📑 test3.com Jun 29th 2017, 15:52							
2	2 🗍 test2.com Jun 29th 2017, 15:52							
3		test1.com	Jun 29th 2017, 15:52					

4. [作成] ボタンをクリックします。

Seci	Secure Anywhere.					
Home	Endpoint Protection	Support				
Status	Policies Group Managen	ent Reports Overrides Alerts Settings Logs Resources				
File & Fold	File & Folder Overrides Web Overrides					
Allow List						
URL						

[ウェブのオーバーライド] ウィンドウが表示されます。

Web Override		×
URL:	test.com	
	Save Cancel	

5. [URL] フィールドに、オーバーライドを作成する Web サイトの URL を入力します。

Web Override		X
URL:	test.com	
	Save Cancel	

6. 設定が完了したら[保存]ボタンをクリックします。.

Web Override		×
URL:	test.com	
	Save Cancel	

ウェブのオーバーライドが作成されます。

Secure Anywhere.						
Home Endpoint Protection Support						
Status         Policies         Group Management         Reports         Overrides         Alerts         Settings         Logs         Resources						
File & Folder Overrides Web Overrides						
Allow List						
Create 😑 Delete						
URL	Date Last Modified 👻					
1 🚊 test.com	Jun 22nd 2017, 17:58					

# [グループの管理] でのウェブのオーバライドの作成

[グループの管理]タブでウェブのオーバーライドを作成するには、次の手順に従ってください。

### [グループの管理] タブでウェブのオーバーライドを作成するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.								
Home	Endpoint Protection	Support						
Status	Policies Group Managen	nent Repor	ts Overrides	Alerts	Settings	Logs Resources		
🛄 Status		«	Endpoints enco	untering tl	hreats (last 7 d	days)		
We recom endpoint h on the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation ena- igned policy.	on 3 abled						

2. [**グループの管理**] タブをクリックします。

Secure Anywhere.	
Home Endpoint Protection Supp	ort
Status Policies Group Management F	Reports Overrides Alerts Settings Logs Resources
🔛 Status 🔍	Endpoints encountering threats (last 7 days)
We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	

[グループの管理] タブが表示されます。

Secure Anywhere.						
Home Endpoint Pro	tection Supp	ort				
Status Policies Group	Management	Reports Overrides Alerts Settings Logs	Resources			
Groups Views Search	n < 🕫	📑 Endpoints				
🕒 Create   📔 Actions 🗸		Hostname	Policy			
Group Name	No.					
All Endpoints	14					
Deactivated Endpoints	78					
Default Group	9					
Bracknell	0					
Broomfield	0					
Dublin	0					
Mac OS X Systems	0					
RemoteUS	0					
Server	0					
Servers	0					
Sydney	3					
Tokyo	0					
Tradeshow	2					
Workstations	0					

3. [グループ名] カラムで [**すべてのエンドポイント**] を選択します。

Secure Anywhere.									
Home Endpoint Prot	tection Sup	port							
Status Policies Group	Management	Repo	orts O	verrides	Alerts	Settings	Logs	Resources	
Groups Views Search	n  🦑		Endpoi	nts					
🔂 Create   🛐 Actions 🗸				Hostnam	е			Policy	
Group Name	No.								
All Endpoints	14								
Deactivated Endpoints	78								
Default Group	9								
Bracknell	0								
Broomfield	0								
Dublin	0								
Mac OS X Systems	0								
RemoteUS	0								
Server	0								
Servers	0								
Sydney	3								
Tokyo	0								
Tradeshow	2								
Workstations	0								

[すべてのエンドポイント] エリアにすべてのエンドポイントが表示されます。

Secure Anywhere.						
Home Endpoint Pro	tection Supp	oort				
Status Policies Grou	p Management	Reports 0	verrides Alerts Settings Lo	ogs Resources		
Groups Views Searc	h < 🕏	📕 All End	points			
🕒 Create   🗃 Actions 🗸		Rave Ch	anges   🔄 Undo Changes   🌄 Mo	we endpoints to another group   [		
Group Name	No.		Hostname	Policy		
All Endpoints	14	1	AB-WIN10-DEMO	Unmanaged		
Deactivated Endpoints	78	2	TRADE3-7185-BRM	Unmanaged		
Default Group	9	3 🔳	TRADE4-7184-BRM	Unmanaged		
Bracknell	0	4	WRDemoEP01	Demo Policy (Do Not Edit)		
Broomfield	0	5 🔳	WRDemoEP03	Demo Policy (Do Not Edit)		
Dublin	0	6	WRDemoEP04	Demo Policy (Do Not Edit)		
Mac OS X Systems	0	7	WRDEMOEP05	No Remediation		
RemoteUS	0	8	WRDemoEP05	No Remediation		
Server	0	9	WRDemoEP06	Standard Workstation Policy		
Servers	0	10 🔲	WRDemoEP07	Standard Workstation Policy		
Sydney	3	11 🔳	WRDEMOEP11-W8-L	Standard Workstation Policy		
Tokyo	0	12	WRDEMOEP14	No Remediation		
Tradeshow	2	13 🔲	WRDEMOEP15	Standard Workstation Policy		
Workstations	0	14	WRDemoSVR01	Recommended Server Defaults		

4. ウェブのオーバーライドを作成するエンドポイントを選択します。

Secure/	Secure Anywhere.							
Home Endpo	oint Protection Supp	port						
Status Policies	Group Management	Reports Overrides Alerts Settings	Logs Resources					
Groups Views	Search < 🕏	All Endpoints						
🔂 Create   🛐 Actio	ns 🕶	🔚 Save Changes   🔄 Undo Changes	Move endpoints to another group	Apply policy to endpoints   🍧	🛛 Agent Commands 🗸   🖨 Deactivate			
Group Name	No.	Hostname	Policy	Group	Status			
All Endpoints	14	1 🛛 📕 AB-WIN10-DEMO	Unmanaged	Default Group	Protected			
Deactivated Endpoints	s 78	2 TRADE3-7185-BRM	Unmanaged	Tradeshow	Not Seen Recently			
Default Group	9	3 🔲 📕 TRADE4-7184-BRM	Unmanaged	Tradeshow	🐠 Not Seen Recently			
Bracknell	0	4 WRDemoEP01	Demo Policy (Do Not Edit)	Default Group	📀 Not Seen Recently			
Broomfield	0	5 WRDemoEP03	Demo Policy (Do Not Edit)	Sydney	📀 Not Seen Recently			
Dublin	0	6 🔲 📑 WRDemoEP04	Demo Policy (Do Not Edit)	Sydney	🐠 Not Seen Recently			
Mac OS X Systems	0	7 WRDEMOEP05	No Remediation	Default Group	🐠 Not Seen Recently			
RemoteUS	0	8 🔲 📑 WRDemoEP05	No Remediation	Default Group	Needs Attention			
Server	0	9 WRDemoEP06	Standard Workstation Policy	Default Group	📀 Not Seen Recently			
Servers	0	10 🔲 📕 WRDemoEP07	Standard Workstation Policy	Sydney	📀 Not Seen Recently			
Sydney	3	11 WRDEMOEP11-W8-L	Standard Workstation Policy	Default Group	📀 Not Seen Recently			
Tokyo	0	12 WRDEMOEP14	No Remediation	Default Group	🐠 Not Seen Recently			
Tradeshow	2	13 WRDEMOEP15	Standard Workstation Policy	Default Group	🔶 Not Seen Recently			
Workstations	0	14 WRDemoSVR01	Recommended Server Defaults	Default Group	Protected			

5. [**ブロックされた** URL] タブをクリックします。

Secure Anywhere.									
Home Endpoint P	Home Endpoint Protection Support								
Status Policies Gro	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources								
Groups Views Sea	rch < 🕫		All End	dpoints					
🔂 Create   🛐 Actions 🗸			Save C	Changes   🔄 Undo Changes   🌄 Mo	we endpoints to another group   [ 🔼	pply policy	r to endpoints   📢 Ag	gent Commands -	😑 Deactivate
Group Name	No.			Hostname	Policy	Group		Status	
All Endpoints	14	1		AB-WIN10-DEMO	Unmanaged	Default	Group	Protecte	d
Deactivated Endpoints	78	2		TRADE3-7185-BRM	Unmanaged	Trades	how	🔶 Not See	n Recently
Default Group	9	3		TRADE4-7184-BRM	Unmanaged	Trades	how	🕕 Not See	n Recently
Bracknell	0	4		WRDemoEP01	Demo Policy (Do Not Edit)	Default	Group	📀 Not See	n Recently
Broomfield	0	5		WRDemoEP03	Demo Policy (Do Not Edit)	Sydney		🕕 Not See	n Recently
Dublin	0	6		WRDemoEP04	Demo Policy (Do Not Edit)	Sydney		🐠 Not See	n Recently
Mac OS X Systems	0	7		WRDEMOEP05	No Remediation	Default	Group	🐠 Not See	n Recently
RemoteUS	0	8		WRDemoEP05	No Remediation	Default	Group	🕕 Needs A	ttention
Server	0	9		WRDemoEP06	Standard Workstation Policy	Default	Group	🐠 Not See	n Recently
Servers	0	10		WRDemoEP07	Standard Workstation Policy	Sydney		🐠 Not See	n Recently
Sydney	3	11		WRDEMOEP11-W8-L	Standard Workstation Policy	Default	Group	🐠 Not See	n Recently
Tokyo	0	12		WRDEMOEP14	No Remediation	Default	Group	🐠 Not See	n Recently
Tradeshow	2	13		WRDEMOEP15	Standard Workstation Policy	Default	Group	🐠 Not See	n Recently
Workstations	0	14		WRDemoSVR01	Recommended Server Defaults	Default	Group	Protecte	d
	Scan History Blocked URLs								
			Sca	n Start	Status		Scan Type		Area
		1	Jun	27th 2017, 15:31	📀 Clean		Deep Scan		
		2	Jun	15th 2017, 22:31	Clean		Deep Scan		
					-				

## [ブロックされた URL] タブが表示されます。

Sca	Scan History Blocked URLs								
1 c	Treate override								
	URL	Category	Reputation	User Action	Date				
1	https://free-keylogger.en.softonic.com	Keyloggers and Monitoring		Block	Jun 20th 2017, 15:18:44				
2	http://ww1.see-password.com	Keyloggers and Monitoring		Block	Jun 20th 2017, 15:11:44				
з	http://ww1.see-password.com	Keyloggers and Monitoring		Block	Jun 20th 2017, 15:11:40				
4	http://ww1.see-password.com	Keyloggers and Monitoring		Block	Jun 20th 2017, 15:11:31				
5	http://see-password.com	Keyloggers and Monitoring	10 High Risk	Block	Jun 20th 2017, 14:41:56				
6	http://webrootresearch.com	Phishing and Other Frauds	10 High Risk	Block	Jun 20th 2017, 13:49:17				
7	http://webrootresearch.com	Phishing and Other Frauds	10 High Risk	Block	Jun 20th 2017, 13:49:17				
8	http://www.keylogger-test2.com	Keyloggers and Monitoring	10 High Risk	Block	Jun 20th 2017, 13:47:51				

6. ウェブのオーバーライドを作成する URL を選択します。

Sca	Scan History Blocked URLs								
10	Treate override								
	URL	Category	Reputation	User Action	Date				
1	https://free-keylogger.en.softonic.com	Keyloggers and Monitoring		Block	Jun 20th 2017, 15:18:44				
2	http://ww1.see-password.com	Keyloggers and Monitoring		Block	Jun 20th 2017, 15:11:44				
3	http://ww1.see-password.com	Keyloggers and Monitoring		Block	Jun 20th 2017, 15:11:40				
4	http://ww1.see-password.com	Keyloggers and Monitoring		Block	Jun 20th 2017, 15:11:31				
5	http://see-password.com	Keyloggers and Monitoring	10 High Risk	Block	Jun 20th 2017, 14:41:56				
6	http://webrootresearch.com	Phishing and Other Frauds	10 High Risk	Block	Jun 20th 2017, 13:49:17				
7	http://webrootresearch.com	Phishing and Other Frauds	10 High Risk	Block	Jun 20th 2017, 13:49:17				
8	http://www.keylogger-test2.com	Keyloggers and Monitoring	10 High Risk	Block	Jun 20th 2017, 13:47:51				

[オーバーライドの作成] アイコンがアクティブになります。

S	Scan History Blocked URLs							
1	Treate override							
		URL	Category	Reputation				
	1	https://free-keylogger.en.softonic.com	Keyloggers and Monitoring					
	2	http://ww1.see-password.com	Keyloggers and Monitoring					
	3	http://ww1.see-password.com	Keyloggers and Monitoring					
	4	http://ww1.see-password.com	Keyloggers and Monitoring					
	5	http://see-password.com	Keyloggers and Monitoring	10 High Risk				
	6	http://webrootresearch.com	Phishing and Other Frauds	10 High Risk				
	7	http://webrootresearch.com	Phishing and Other Frauds	10 High Risk				
	8	http://www.keylogger-test2.com	Keyloggers and Monitoring	10 High Risk				

7. [オーバーライドの作成] アイコンをクリックします。

Scan History Blocked URLs									
	-	URL	Category	Reputation					
	1	https://free-keylogger.en.softonic.com	Keyloggers and Monitoring						
	2	http://ww1.see-password.com	Keyloggers and Monitoring						
	з	http://ww1.see-password.com	Keyloggers and Monitoring						
	4	http://ww1.see-password.com	Keyloggers and Monitoring						
	5	http://see-password.com	Keyloggers and Monitoring	10 High Risk					
	6	http://webrootresearch.com	Phishing and Other Frauds	10 High Risk					
	7	http://webrootresearch.com	Phishing and Other Frauds	10 High Risk					
	8	http://www.keylogger-test2.com	Keyloggers and Monitoring	10 High Risk					

[ウェブのオーバーライド] ウィンドウが表示されます。[URL] フィールドには選択した URL が表示されています。

Veb Override		
URL:	ww1.see-password.com	
	Save Cancel	

8. 保存] ボタンをクリックします。

W	/eb Override			
	URL:	ww1.see-password.com		
		Save Cancel		

URL が許可リストに追加されます。

ウェブルートエンドポイントプロテクション管理者ガイド

# [レポート] でのウェブのオーバライドの作成

[レポート] タブでウェブのオーバーライドを作成するには、次の手順に従ってください。

### [レポート] タブでウェブのオーバーライドを作成するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.										
Home Endpoint Protection	Support									
Status Policies Group Managen	nent Reports Ov	errides Alerts	Settings Logs	Resources						
E Status	« 🖳 Endpoi	nts encountering t	threats (last 7 days)							
We recommend you check whether this endpoint has automatic remediation end on the assigned policy.	n ibled									
2. [レポート] タブをクリックします。

Secure Anywhere.	
Home Endpoint Protection Supp	ort
Status Policies Group Managemen	Reports Verrides Alerts Settings Logs Resources
🔤 Status	Endpoints encountering threats (last 7 days)
Alert <u>1 Endpoint needs attention</u> We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.	

[レポート] タブが表示されます。

Secure Anywhere.		
Home Endpoint Protection Support		
Status Policies Group Management Reports	Overrides Alerts Settings	Logs Resources
Select your report	All URLs Blocked (Jun 27 10:26)	
Report Type:	😵 All URLs Blocked	
All URLs Blocked 🗸	URL	Category
Policy:		
All		
Group:		
All 👻		
Select time period		
Include deactivated and hidden		
Submit		

3. [レポートの種類]ドロップダウンメニューで [ブロックされたすべての URL]を選択します。

Secu	<b>ire</b> Anywher	e.					
Home	Endpoint Protection	Support					
Status F	Policies Group Managem	ent Repor	ts Overrides				
Select ye	our report	«	? All URL				
Report Type	ə:		😢 All U				
All URLs E	Blocked		✓ UF				
All Threat	All Threats Seen						
All Undete	-						
All URLs E							
Endpoints	with threats on last sean		-				
Endpoints	with undetermined softw	are on last s.					
Threat His	story (Daily)						
Threat His	story (Collated)						
Blocked U	IRL History (Daily)						
Agent Ver	sion Spread						
Agents Ins	stalled						

4. [送信] ボタンをクリックします。

Secu	ireAnywher	2,	
Home	Endpoint Protection	Support	
Status F	Policies Group Managem	ent Reports	Overrides
Select ye	our report	«?	All URLs
Report Type	к.		😢 All URL
All URLs E	Blocked	×	URL
Policy:			
All		×	
Group:			
All		*	
Select tir	ne period		
Include o	leactivated and hidden		
	Submit	)	

[ブロックされたすべての URL] エリアに、ブロックされた URL のリストが表示されます。

Secure Anywhere.							
Home Endpoint Protection Support							
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources							
📄 Select your report 🛛 🔍 ?	All U	JRLs Blocked (Jun 29 09:45) 🛞					
Report Type:	🕲 A	II URLs Blocked					
All URLs Blocked 🗸	📌 Ci	reate override					
Policy:		URL	Category	Reputation			
All	1	http://www.keylogger-test2.com	Keyloggers and Monitoring	10 High Risk			
Group:	2	http://keylogger-test2.com	Keyloggers and Monitoring	10 High Risk			
All	3	http://see-password.com	Keyloggers and Monitoring	10 High Risk			
	4	http://see-password.com	Keyloggers and Monitoring	10 High Risk			
Select time period	5	http://ww1.see-password.com	Keyloggers and Monitoring 10 Hi				
Include deactivated and hidden	6	http://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk			
	7	http://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk			
Submit	8	http://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk			

5. [ブロックされたすべての URL] エリアで、許可する URL を選択します。

Secure Anywhere.				
Home Endpoint Protection S	upport			
Status Policies Group Management	Repor	ts Overrides Alerts Settings	Logs Resources	
Select your report	AII UR	Ls Blocked (Jun 29 09:45) 🛞		
Report Type:	😫 All U	JRLs Blocked		
All URLs Blocked 🗸	📌 Crea	ate override		
Policy:	U	RL	Category	Reputation
All	1 ht	ttp://www.keylogger-test2.com	Keyloggers and Monitoring	10 High Risk
Group:	2 ht	ttp://kevloager-test2.com	Kevloggers and Monitoring	10 High Risk
All	3 ht	ttp://see-password.com	Keyloggers and Monitoring	10 High Risk
	4 ht	ttp://see-password.com	Keyloggers and Monitoring	10 High Risk
Select time period	5 ht	ttp://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk
Include deactivated and hidden	6 ht	ttp://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk
	7 ht	ttp://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk
Submit	8 ht	ttp://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk

[オーバーライドの作成] アイコンがアクティブになります。

A	All URLs Blocked (Jun 29 09:45) 🛞						
0	😵 All URLs Blocked						
1	C	reate override					
		URL	Category	Reputation			
	1	http://www.keylogger-test2.com	Keyloggers and Monitoring	10 High Risk			
	2	http://keylogger-test2.com	Keyloggers and Monitoring	10 High Risk			
	3	http://see-password.com	Keyloggers and Monitoring	10 High Risk			
	4	http://see-password.com	Keyloggers and Monitoring	10 High Risk			
	5	http://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk			

6. [オーバーライドの作成] アイコンをクリックします。

	All URLs Blocked (Jun 29 09:45) 🛞						
E	😵 All URLs Blocked						
C	Create override						
	-	URL	Category	Reputation			
	1	http://www.keylogger-test2.com	Keyloggers and Monitoring	10 High Risk			
	2	http://keylogger-test2.com	Keyloggers and Monitoring	10 High Risk			
	3	http://see-password.com	Keyloggers and Monitoring	10 High Risk			
	4	http://see-password.com	Keyloggers and Monitoring	10 High Risk			
	5	http://ww1.see-password.com	Keyloggers and Monitoring	10 High Risk			

### 選択した URL が表示された状態の[オーバーライドの作成] ウィンドウが表示されます。

leb Override		3
URL:	ww1.see-password.com	
	Save Cancel	

7. 保存]ボタンをクリックします。

URL:	ww1.see-password.com	

URL が許可リストに追加されます。

# ウェブのオーバーライドの編集

ウェブのオーバーライドを編集するには、次の手順に従ってください。

### ウェブのオーバーライドを編集するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere	0_"					
Home Endpoint Protection	Support					
Status Policies Group Managem	ent Reports	Overrides	Alerts	Settings	Logs	Resources
🛄 Status	🔍 🔜 E	Endpoints enco	untering t	threats (last	7 days)	
We recommend you check whether this endpoint has automatic remediation enal on the assigned policy.	n bled					

2. [**オーバーライド**] タブをクリックします。

Seci	Secure Anywhere.						
Home	Endpoint Protection	Support					
Status	Policies Group Manageme	ent Report Overrides Alerts Settings Logs Resources					
🛄 Status		< 🖳 Endpoints encountering threats (last 7 days)					
We recomendpoint hon the ass	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation enab- igned policy.	l Ned					

### [ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。

Secure Anywhere.							
Н	Home Endpoint Protection Support						
Stat	us	Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	S		
File	& F	older Overrides Web Overrides	ł				
Wh	itelis	Blacklist					
Whit	elist						
🔁 C	reate	e   😑 Delete   🔄 Import					
		Override Name	MD5	Path Mask	File Mask		
1	1 Test 4						
2		Test 3		· · · · · · · · · · · · · · · · · · ·			
3		Test 2					
4		Test 1			· · · · · ·		

3. [ウェブのオーバーライド] タブをクリックします。

Secure Anywhere.								
Home Endpoint Protection S	Home Endpoint Protection Support							
Status Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	S					
File & Folder Overrides Whitelist Blacklist	File & Folder Overrides     Web Overrides       Whitelist     Blacklist							
Create   Create								
Override Name	Override Name     MD5     Path Mask     File Mask							
1 🔲 Test 4	1 🔲 Test 4							
2 🔲 Test 3			and a second					
3 🔲 Test 2								
4 🔲 Test 1			· · · · ·					

### [ウェブのオーバーライド] タブが表示されます。

Secure Anywhere.							
Н	Home Endpoint Protection Support						
Stat	us	Policies Group Management Reports Overrides Alerts Settings Logs Resources					
File	& Fo	Ider Overrides Web Overrides					
Allov	v Lis	t					
🔁 C	reat	e 😑 Delete					
	URL Date Last Modified 👻						
1	1 👔 test3.com Jun 29th 2017, 15:52						
2		test2.com	Jun 29th 2017, 15:52				
3	3 🗍 test1.com Jun 29th 2017, 15:52						

4. [許可リスト] で、編集するウェブのオーバーライドを選択し、ダブルクリックします。

Secure Anywhere.						
Home Endpoint Protection Support						
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
File & Folder Overrides Web Overrides						
Allow List						
🔂 Create 🤤 Delete						
URL	Date Last Modified 👻					
1 📄 test3.com	Jun 29th 2017, 15:52					
2 📄 test2.com	Jun 29th 2017, 15:52					
3 test1.com	Jun 29th 2017, 15:52					

[ウェブのオーバーライド] ウィンドウが表示されます。

Web Override		×
URL:	test.com	
	Save Cancel	

- 5. 必要に応じて、ウェブのオーバーライドを編集します。
- 6. 設定が完了したら[保存]ボタンをクリックします。

Web Override		×
URL:	test.com	
(	Save Cancel	

編集内容が保存されます。

# ウェブのオーバーライドの削除

ウェブのオーバーライドを削除するには、次の手順に従ってください。

### ウェブのオーバーライドを削除するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。

Secure Anywhere.						
Home Endpoint Protection	Support					
Status Policies Group Managem	ent Reports	Overrides	Alerts	Settings	Logs	Resources
🛄 Status	🔍 🔜 E	Endpoints enco	untering t	threats (last	7 days)	
We recommend you check whether this endpoint has automatic remediation enal on the assigned policy.	n bled					

2. [**オーバーライド**] タブをクリックします。.

Secure Anywhere.						
Home	Endpoint Protection	Support				
Status	Policies Group Manageme	t Report Overrides Alerts Settings Logs Resources				
🖳 Status		Key Endpoints encountering threats (last 7 days)				
We recommendpoint ha	Alert <u>1 Endpoint needs attention</u> mend you check whether this as automatic remediation enable	ed				
on the assi	igned policy.					

[ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。

Se	Secure Anywhere.						
Но	Home Endpoint Protection Support						
Stat	us	Policies Group Management	Reports Overrides Alert	ts Settings Logs Resource	es		
File	& F	older Overrides Web Overrides	1				
Whi	telis	Blacklist					
White	elist						
🔁 C	reat	e   😑 Delete   🔁 Import					
		Override Name	MD5	Path Mask	File Mask		
1	1 🔲 Test 4						
2	2 🔲 Test 3			· · · · · · · · · · · · · · · · · · ·			
3		Test 2					
4		Test 1					

3. [ウェブのオーバーライド] タブをクリックします。

Secure Anywhere.								
Home Endpoint Protection S	Home Endpoint Protection Support							
Status Policies Group Management	Reports Overrides Alerts	Settings Logs Resource	S					
File & Folder Overrides Web Overrides Whitelist Blacklist	File & Folder Overrides     Web Overrides       Whitelist     Blacklist							
Create   😑 Delete   🖓 Import								
Override Name	Override Name     MD5     Path Mask     File Mask							
1 🔲 Test 4	1 Test 4							
2 🔲 Test 3								
3 🔲 Test 2								
4 🔲 Test 1			_ · · · · ··					

### [ウェブのオーバーライド] タブが表示されます。

Secure Anywhere.							
Н	Home Endpoint Protection Support						
Stat	us	Policies Group Management Reports Overrides Alerts Settings Logs Resources					
File	& Fo	Ider Overrides Web Overrides					
Allov	v Lis	t					
🔁 C	reat	e 😑 Delete					
	URL Date Last Modified 👻						
1	1 👔 test3.com Jun 29th 2017, 15:52						
2		test2.com	Jun 29th 2017, 15:52				
3	3 🗍 test1.com Jun 29th 2017, 15:52						

4. [許可リスト] エリアで、削除するウェブのオーバーライドを選択します。

Secure Anywhere.							
Home Endpoint Protection Support							
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources	Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
File & Folder Overrides Web Overrides	File & Folder Overrides Web Overrides						
Allow List							
🕒 Create 😑 Delete							
URL	Date Last Modified 👻						
1 📄 test3.com	Jun 29th 2017, 15:52						
2 📄 test2.com	Jun 29th 2017, 15:52						
3 test1.com	Jun 29th 2017, 15:52						

[削除]アイコンがアクティブになります。

Secure Anywhere.			
Home Endpoint Protection Support			
Status Policies Group Management Reports Overrides Aler	ts Settings Logs Resources		
File & Folder Overrides Web Overrides			
Allow List			
🔂 Create 🤤 Delete			
URL	Date Last Modified 👻		
1 📄 test3.com	Jun 29th 2017, 15:52		
2 📑 test2.com	Jun 29th 2017, 15:52		
3 📄 test1.com	Jun 29th 2017, 15:52		

5. [削除] アイコンをクリックします。

Secure Anywhere.		
Home Endpoint Protection Support		
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources		
File & Folder Overrides Web Overrides		
Allow List		
URL	Date Last Modified 👻	
1 📄 test3.com	Jun 29th 2017, 15:52	
2 📋 test2.com	Jun 29th 2017, 15:52	
3 📄 test1.com	Jun 29th 2017, 15:52	

#### 確認メッセージが表示されます。

Confirm	Confirm Delete				
?	Are you sure you wish to delete the selected overrides?				
	Yes No				

6. [はい] ボタンをクリックします。



#### ウェブのオーバーライドがシステムから削除されます。

# 第12章:設定の管理

設定の管理方法については、以下のトピックを参照してください。

# データフィルタの設定

エンドポイントプロテクションの管理コンソールでは、一定の期間中に確認されていないエンドポイントをデータ から削除して、サイトの現状について最も正確なデータを表示することができます。

1 カ月、2 カ月、3 カ月、6 カ月、または 12 カ月確認されていないすべてのエンドポイントをデータセットで非表示にするか、EP コンソールが GSM で管理されている場合は GSM データフィルタ設定を継承できます。すべてのデータを表示するよう選択することもできます。

#### データフィルタを設定するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのパネルが表示されます。



2. [設定]タブをクリックします。



#### [設定] パネルが表示されます。

Secure Anywhere.					
Home Endpoint Protection	Home Endpoint Protection				
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources					
tie Settings					
Data Filter:         Hide all data for endpoints not seen for more than 1 month					
Save					
Home     Endpoint Protection       Status     Policies     Group Management     Repoint Rep	ports Overrides Alerts Settings Logs Resources Hide all data for endpoints not seen for more than 1 month				

- 3. [データフィルタ]ドロップダウンメニューで、次のいずれかを選択します。
  - •1カ月間確認されていないエンドポイントのデータをすべて非表示にする
  - 2カ月間確認されていないエンドポイントのデータをすべて非表示にする
  - 3 カ月間確認されていないエンドポイントのデータをすべて非表示にする6カ月間確認されていない エンドポイントのデータをすべて非表示にする
  - ・12カ月間確認されていないエンドポイントのデータをすべて非表示にする
  - ・ すべてのテータを表示 (デフォルト設定)

• GSM データフィルタ設定を継承

Home Endpoint Protection	n
Status Policies Group Managemen	nt Reports Overrides Alerts Settings Logs Resources
Data Filter: Save	Hide all data for endpoints not seen for more than 3 months         Hide all data for endpoints not seen for more than 1 month         Hide all data for endpoints not seen for more than 2 months         Hide all data for endpoints not seen for more than 3 months         Hide all data for endpoints not seen for more than 6 months         Hide all data for endpoints not seen for more than 1 months         Hide all data for endpoints not seen for more than 3 months         Hide all data for endpoints not seen for more than 1 months         Show all data         Inherit the GSM data filter setting (Currently: Show all data)

4. 保存]ボタンをクリックします。

Secure Anywhere.	
Home Endpoint Protection	
Status Policies Group Management Rep	orts Overrides Alerts Settings Logs Resources
Settings	
Data Filter:	Hide all data for endpoints not seen for more than 3 months

保存が完了したことを示すメッセージが表示されます。

Save Su	Save Successful				
•	Your console data will now be updated, with endpoints and their associated data shown or hidden depending on your selection. Please note that dependent on deployment size, it may take a few minutes until all data has been filtered.				
	ок				

#### 5. [OK] ボタンをクリックします。



設定が更新され、ログエントリが作成されます。詳細については、「<u>データフィルタログの表示 ページ</u> 524」を参照してください。

# 第13章:ログの表示

ログの表示方法については、以下のトピックを参照してください。

変更ログの表示	
コマンドログの表示	
データフィルタログの表示	

## 変更ログの表示

変更ログでは、次の各タイプのイベントがいつ発生したのかを確認することができます。

- ログオン 管理者の管理ポータルへのログイン。
- ポリシー ポリシーの作成、変更、削除。
- エージェントコマンド コマンドの開始。
- オーバーライド オーバーライドの作成、変更、削除。
- グループ グループの作成、変更、削除。
- エンドポイント エンドポイントの名前の変更、または別のグループへの移動。
- レポート レポートの生成。

変更ログは、日付範囲、イベントのタイプ、ユーザー、グループ、ポリシー別にフィルタリングできます。

#### 変更ログを表示するには

1. エンドポイントのポータルで [ログ] タブをクリックします。

デフォルトで [変更ログ] が表示されます。このログには変更イベントが一覧表示され、リストを絞り込む ためのフィルタが用意されています。

WEBROOT*       Buy now         SecureAnywhere.       Buy now         Status       Policies       Group Management       Reports       Alerts       Overrides       Logs       Resources         Change Log       Command Log				
C	E Change Log			
	Date	Event Type	Description *	
1	Jul 7th 2014, 08:30	Logon	swilson@emailaddress.com logged on	
2	Jul 4th 2014, 08:25	Logon	swilson@emailaddress.com logged on	
3	Jun 28th 2014, 10:30	Logon	swilson@emailaddress.com logged on	
4	Jun 25th 2014, 03:16	Logon	swilson@emailaddress.com logged on	
5	Jul 6th 2014, 23:48	Group	swilson@emailaddress.com deleted Marketing	
6	Jul 11th 2014, 00:34	Group	swilson@emailaddress.com created Sales	
7	Jul 8th 2014, 10:12	Policy	swilson@emailaddress.com created Recommended Server Defaults	
8	Jul 10th 2014, 21:07	Policy	swilson@emailaddress.com created Recommended Defaults	
9	Jun 30th 2014, 12:36	Logon	jsmith@emailaddress.com logged on	
10	Jul 10th 2014, 13:32	Override	jsmith@emailaddress.com added Override MD5:bf114e3f508900299acc16541353e	
11	Jun 26th 2014, 13:20	Endpoint	djones@emailaddress.com moved NancyJackson_PC74 (Policy: Recommended D	
12	Jul 12th 2014, 16:35	Endpoint	djones@emailaddress.com moved ArthurMartinez_PC48 (Policy: Recommended S	
13	Jun 24th 2014, 13:19	Override	djones@emailaddress.com added Override MD5:a743dfbdeb6afa862e22967af1ec	

- 2. 左側のペインの [変更ログをフィルタリング] のオプションを使用して、データを絞り込みます。データのフィ ルタリングの条件は次のとおりです。
  - [開始日] および [終了日] これら 2 つのフィールドに mm/dd/yyyy形式で日付を入力するか、カレン ダーのアイコンをクリックして日付を指定します。
  - イベントの種類 ドロップダウンリストでイベントを選択します。イベントには、グループ、エンドポイント、ポリシーの変更や、オーバーライド、ユーザーのログオンなどがあります。
  - ユーザーの選択 ドロップダウンリストからユーザーを選択します。
  - グループの選択 ドロップダウンリストからグループを選択します。
  - ポリシーの選択 ドロップダウンリストからポリシーを選択します。
- 3. フィルタリング条件を選択したら、[送信]をクリックします。

- 4. 次のいずれか、または両方の操作を行います。
  - データが 50 アイテムを超える場合は、下の左向き矢印と右向き矢印をクリックしてページ間を移動します。



Z

• データをアップデートするには、[**更新**] アイコンをクリックします。

## コマンドログの表示

コマンドログでは、最近処理したコマンドと未処理のコマンドに関する情報を確認できます。ログには次のデータが含まれています。

- ホスト名 -コマンドを受信したエンドポイントの名前。
- コマンド エンドポイントに対して発行されたコマンド。
- ・パラメータ-ファイルの完全なパス名など、コマンドの実行に使用された追加のパラメータ。
- リクエストされた日 管理ポータルからコマンドが送信された日付。
- •ステータス-[時間切れ]または[実行済み]。24時間で時間切れとなります。

#### コマンドログを表示するには

1. エンドポイントのポータルで [ログ] タブをクリックします。

Secure Anywhere.	Buy now
Status Policies Group Management	Reports Alerts Overrides Logs Resources
E Status	K Endpoints encountering threats (last 7 days)

T[変更ログ] タブがアクティブになった状態で [ログ] パネルが表示されます。

we Se	Secure Anywhere. Buy now			
Stat	Status Policies Group Management Reports Alerts Overrides Logs Resources			
Cha	nge Log Command Log			
	ingo Log			
_ 🔣 C	hange Log			
	Date	Event Type	Description -	
1	Jul 7th 2014, 08:30	Logon	swilson@emailaddress.com logged on	
2	Jul 4th 2014, 08:25	Logon	swilson@emailaddress.com logged on	
з	Jun 28th 2014, 10:30	Logon	swilson@emailaddress.com logged on	
4	Jun 25th 2014, 03:16	Logon	swilson@emailaddress.com logged on	
5	Jul 6th 2014, 23:48	Group	swilson@emailaddress.com deleted Marketing	
6	Jul 11th 2014, 00:34	Group	swilson@emailaddress.com created Sales	
7	Jul 8th 2014, 10:12	Policy	swilson@emailaddress.com created Recommended Server Defaults	
8	Jul 10th 2014, 21:07	Policy	swilson@emailaddress.com created Recommended Defaults	
9	Jun 30th 2014, 12:36	Logon	jsmith@emailaddress.com logged on	
10	Jul 10th 2014, 13:32	Override	jsmith@emailaddress.com added Override MD5:bf114e3f508900299acc16541353e	
11	Jun 26th 2014, 13:20	Endpoint	djones@emailaddress.com moved NancyJackson_PC74 (Policy: Recommended D	
12	Jul 12th 2014, 16:35	Endpoint	djones@emailaddress.com moved ArthurMartinez_PC48 (Policy: Recommended S	
13	Jun 24th 2014, 13:19	Override	djones@emailaddress.com added Override MD5:a743dfbdeb6afa862e22967af1ec:	

2. [**コマンドログ**] タブをクリックします。

Secure Anywhere. Buy now				
State	us Policies Group Man	agement Reports	s Alerts Overrides Logs Resources	
Cha	nge Log Command Log			
C	hange Log			
20	Date	Event Type	Description -	
1	Jul 7th 2014, 08:30	Logon	swilson@emailaddress.com logged on	
2	Jul 4th 2014, 08:25	Logon	swilson@emailaddress.com logged on	
3	Jun 28th 2014, 10:30	Logon	swilson@emailaddress.com logged on	
4	Jun 25th 2014, 03:16	Logon	swilson@emailaddress.com logged on	
5	Jul 6th 2014, 23:48	Group	swilson@emailaddress.com deleted Marketing	
6	Jul 11th 2014, 00:34	Group	swilson@emailaddress.com created Sales	
7	Jul 8th 2014, 10:12	Policy	swilson@emailaddress.com created Recommended Server Defaults	
8	Jul 10th 2014, 21:07	Policy	swilson@emailaddress.com created Recommended Defaults	
9	Jun 30th 2014, 12:36	Logon	jsmith@emailaddress.com logged on	
10	Jul 10th 2014, 13:32	Override	jsmith@emailaddress.com added Override MD5:bf114e3f508900299acc16541353e	
11	Jun 26th 2014, 13:20	Endpoint	djones@emailaddress.com moved NancyJackson_PC74 (Policy: Recommended D	
12	Jul 12th 2014, 16:35	Endpoint	djones@emailaddress.com moved ArthurMartinez_PC48 (Policy: Recommended S	
13	Jun 24th 2014, 13:19	Override	djones@emailaddress.com added Override MD5:a743dfbdeb6afa862e22967af1ec	

## [コマンドログ] パネルが表示されます。

Se	BROOT Buy now	Interactiv	your@emailaddress.com ↓				
Stat	us Policies Group Management Reports Alerts Overrides	Logs Resources					
Cha	Change Log Command Log						
() R	Recent & Outstanding Commands						
	Hostname	Command	Date Requested - Status				
1	Metro Dev Laptop	Change keycode	Jul 12th 2014, 17:16 Elapsed				
2	Sophia's PC 1	Change keycode	Jul 12th 2014, 01:57 Executed				
3	Elizabeth's PC 2	Clear Log Files	Jul 11th 2014, 20:27 Elapsed				
4	Mac Mini	Log off	Jul 10th 2014, 10:54 Elapsed				
5	Mac Mini	Scan	Jul 7th 2014, 05:28 Elapsed				
6	Sophia's PC 1	Change keycode	Jul 5th 2014, 08:40 Executed				

3. データが 50 アイテムを超える場合は、下のナビゲーションボタンを使用してページ間を移動します。

|4 4 | Page 1 of 7 ▶ ▶| 2

4. データをアップデートするには、[更新] アイコンをクリックします。

I	-	
I	21	1
I	- Martin	
I	-	

# データフィルタログの表示

データフィルタの設定に加えられたすべての変更は、データフィルタログに記録されます。

### データフィルタログを表示するには

1. エンドポイントプロテクションのコンソールにログインします。

[状態] タブがアクティブになった状態でエンドポイントプロテクションのパネルが表示されます。



2. [**ログ**] タブをクリックします。



T[変更ログ] タブがアクティブになった状態で [ログ] パネルが表示されます。

Secure Anywhere.						
Home Endpoint Protection						
Status Policies Group Management	Rep	orts Overrides Alerts Settings Logs Resources				
Change Log Command Log Data Filter Log						
T Filter Change Log						
Between:		Date				
	1 Nov 11th 2015, 13:30					
And:	2 Nov 11th 2015, 13:27					
	3 Nov 11th 2015, 12:35					
	4 Nov 11th 2015, 12:34					
Event Type:	5	Nov 11th 2015, 11:23				
No Filter		⁸ Nov 11th 2015, 10:48				
Involving User:	7	Nov 11th 2015, 10:37				
No Filter		Nov 11th 2015, 10:35				
		Nov 11th 2015, 10:24				
No Filter	10	Nov 11th 2015, 10:16				
Involving Policy:	11	Nov 11th 2015, 08:21				
No Filter	12	Nov 11th 2015, 08:13				
Normer		Nov 11th 2015, 08:10				
Submit	14	Nov 11th 2015, 04:56				
Cubinic	15	Nov 11th 2015, 04:55				

3. [**データフィルタログ**] タブをクリックします。

Secure Anywhere.						
Home Endpoint Protection						
Status Policies Group Management Reports Overrides Alerts Settings Logs Resources						
Change Log Command Log Data Filter Log						
Tilter Change Log						
Between:			Date			
	•	1	Nov 11th 2015, 13:30			
And [.]	nd:	2	Nov 11th 2015, 13:27			
·		3	Nov 11th 2015, 12:35			
		4	Nov 11th 2015, 12:34			
Event Type:		5	Nov 11th 2015, 11:23			
No Filter	*	6	Nov 11th 2015, 10:48			
Involving User:		7	Nov 11th 2015, 10:37			
No Filter	*	8	Nov 11th 2015, 10:35			
Involving Group:		9	Nov 11th 2015, 10:24			
No Filter	¥	10	Nov 11th 2015, 10:16			
Involving Policy:		11	Nov 11th 2015, 08:21			
No Filter	¥	12	Nov 11th 2015, 08:13			
		13	Nov 11th 2015, 08:10			
Submit		14	Nov 11th 2015, 04:56			
		15	Nov 11th 2015, 04:55			

[データフィルタログ] パネルが表示され、追加した変更ごとに以下の情報を提示します。

- 設定 選択されたフィルタのオプション。
- ユーザー-変更を行ったユーザーの名前。
- •日付-変更が加えられた日付。

Secure Anywhere.							
Home Endpoint Protection							
Status         Policies         Group Management         Reports         Overrides         Alerts         Settings         Logs         Resources							
Char	Change Log Command Log Data Filter Log						
🔣 Data Filter Log							
	Setting	User	Date				
1	Hide all data for endpoints not seen for more than 6 months	JaneDoe@webroot.com	Nov 11th 2015, 13:36				
2	Hide all data for endpoints not seen for more than 3 months	JaneDoe@ webroot.com	Nov 11th 2015, 12:44				
3	Hide all data for endpoints not seen for more than 1 month	JaneDoe@webroot.com	Nov 11th 2015, 10:34				
4	Inherit the GSM data filter setting	JaneDoe@ webroot.com	Nov 11th 2015, 10:34				
5	Show all data	JaneDoe@webroot.com	Nov 5th 2015, 09:18				
6	Hide all data for endpoints not seen for more than 1 month	JaneDoe@webroot.com	Nov 5th 2015, 09:17				

# 第 14 章: 使用状況データへのアクセス

使用状況データへのアクセスの詳細については、以下のトピックを参照してください。

# 使用状況データへのアクセスについて

使用状況コンソールには、ウェブルートの製品とサービスに関する詳細な情報が表示されます。このコンソールで、セキュリティ意識向上のためのトレーニングの使用状況データにアクセスできるようになりました。

詳細については、<u>GSM 管理者ガイド</u>の「<u>設定の操作</u>」セクションのトピック「<u>使用状況データへのアクセス</u>」を 参照してください。
# 第15章:WSA Business エンドポイントプロテク ションのサポート

ウェブルートのサポートオプションおよびその他のリソースの詳細については、以下のトピックを参照してください。

# テクニカル サポートを受けるには

ウェブルートではさまざまなサポートオプションを提供しています。次のいずれかの方法をご利用ください。

- <u>ナレッジベースで回答を探す</u>。
- オンライン文書で回答を探す。
- <u>ヘルプチケットを送信する</u>。
- <u>ウェブルートのオンラインビジネスフォーラムを利用する</u>。

# 索引

# [

[IP 範囲] タブ、使用 334
[アクティブ ディレクトリ] タブ、使用 332
[インストールされたエージェント] レポート、生成 395
[エージェントのバージョンの使用状況] レポート、生成 390
[オーバーライド] タブ、オーバーライドの適用 439
[ブロックされた URL の履歴 (日単位)] レポート、生成 386
[ブロックされたすべての URL] レポート、生成 356
[ワークグループ] タブ、使用 336
[確認されたすべての春威] レポート、生成 342
[確認されたすべての春國] レポート、生成 377
[脅威の履歴 (日単位)] レポート、生成 369
[最新のスキャンで希威が存在したエンドポイント] レポート、生成 361
[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポート、生成 365

С

CSV ファイル、エクスポート 216

# G

GPO、SecureAnywhere のインストール 131

# I

ID シールド コマンド 156 設定 284

#### Μ

Mac の SecureAnywhere メニュー 169 Mac のツールドロップダウンメニュー 170 Mac、SecureAnywhere インストーラーの使用 118 Mac、SecureAnywhere を開く 167 MSI、SecureAnywhere のインストール 130

#### S

```
SecureAnywhere

GPO でのインストール 131

Mac 版のインストーラー、使用 118

MSI を使用したインストール 130

VM へのインストール 132

Windows 版のインストーラー、使用 117

アンインストール 202

インストーラー、使用 116

ターミナル RDS サーバーへのインストール 132

配備 112

複製 イメージへのインストール 132

SecureAnywhere のアンインストール 202

SecureAnywhere の配備 112
```

#### V

VM、SecureAnywhere のインストール 132

# W

Web 脅威シールドの設定 281 Windows SecureAnywhere インストーラーの使用 117 SecureAnywhere を開く 165

# あ

```
アカウント
アップグレード 91
更新 91
アカウントのアップグレード 91
アカウントの更新 91
アカウント設定、編集 55
アクセス
テクニカルサポート 532
管理コンソール 52
使用状況データ 530
製品情報 43
アップデート
ダウンロード 177
強制実行 177
```

い

```
インストーラーのオプション 132
インストール
SecureAnywhere、GPO の使用 131
SecureAnywhere、MSI の使用 130
SecureAnywhere、VM 132
SecureAnywhere、ターミナル RDS サーバー 132
SecureAnywhere、複製イメージ 132
```

# う

```
ウェブのオーバーライド
[グループの管理]タブでの作成 485
[レポート]での作成 494
作成 480
削除 506
編集 502
ウェブルートアカウント、作成 11
```

# え

```
エージェントコマンド 147
エージェントのバージョンの概要、表示 212
エクスポート
 CSV 7r1u 216
 オーバーライド、スプレッドシートへの 471
 データ、スプレッドシートへの 41
エンドポイント
 サブネットへの移動 162
 ハードウェアの変更 162
 再アクティブ化 200
 非アクティブ化 199
エンドポイント、キーコードの変更 135
エンドポイント、グループに整理 330
エンドポイント、グループ間での移動 328
エンドポイント、コマンドの発行 144
エンドポイント、ポリシー間での移動 307
エンドポイント、検索 139
エンドポイント、名前の変更 138
エンドポイントキーコード、変更 135
エンドポイントでのコマンドの実行 194
エンドポイントのアップデート、管理 162
エンドポイントの移動
 グループ間 328
 サブネット への 162
```

ポリシー間 307 エンドポイントの検索 139 エンドポイントの再アクティブ化 200 エンドポイントの状態、表示 204 エンドポイントの非アクティブ化 199 エンドポイントプロテクションのタブの説明 37 エンドポイントプロテクションのメニュー、開く 38 エンドポイントプロテクションのレポート、生成 340 エンドポイントプロテクションの概要 2 エンドポイントプロテクションの概要 1 エンドポイントプロテクションの概要 3

#### お

#### オーバーライド スプレッドシートへのエクスポート 471 導入 424 表示 466 オーバーライドの適用 [オーバーライド] タブから 439 グループから 446 レポートから 454 滞留時間のポップアップから 459 オプション、インストーラー 132

#### か

カスタムの警告、作成 408

# き

キーコード、追加 81

# <

グループ オーバーライドの適用 446 ポリシーの適用 324 削除 338 追加 319 名前変更 321

# C

コアシステムシールドの設定 279

コマンド ID シールド 156 エージェント 147 エンドポイントで実行中 194 エンドポイントへの発行 144 ファイル 155

ファイル 155 プロセス 155 マルウェア対策 154 ユーザーアクセス 153 詳細 158 電源 153 コマンドログ、表示 520 コンソール 切り替え 90 追加 84 名前変更 90 コンソールの切り替え 90

# さ

サイト管理者 削除 107 設定、編集 98 追加 93

# し

システム、移行 162 システムの移行 162 システム最適化ツールの設定 290 システム要件 4

# す

スキャンのスケジュールの設定 262 スキャン結果 確認 171 スキャン結果の確認 171 スキャン設定 264 スキャン履歴 表示 171 スプレッドシート、データのエクスポート 41

# せ

セットアップ、準備 5

```
セットアップの準備 5
た
ターミナル RDS サーバー、SecureAnywhere のインストール 132
ダウンロード
アップデート 177
レポートのスプレッドシート 402
```

#### っ

ツールドロップダウンメニュー、Mac 170

# τ

データの並べ替え レポート内 45 表内 45 データフィルタ、設定 512 データフィルタログ、表示 524 テクニカルサポート、受ける 532 テストインストール、実行 29 デストインストールの実行 29 デフォルトのポリシー、選択 27,227 デフォルトのポリシーの選択 27,227

#### は

ハードウェアの変更、エンドポイント上 162 パネル 開く 40 折りたたみ 40 パネルの折りたたみ 40

# ひ

ビデオチュートリアル、開く 41 ヒューリスティックの設定 270

# ふ

ファイアウォール、通信 6,163 ファイアウォールの設定 287 ファイアウォールを介した通信 6,163 ファイルコマンド 155 ファイルのオーバーライド、設定 174 ファイルの隔離、復元 173 ファイルの隔離からの復元 173 ブラックリストのオーバーライド、作成 426 プロキシバイパス、入力 8 プロキシ情報、インストーラー内での入力 8 プロキシ情報、エンドポイントでの入力 9 プロセスコマンド 155

ゝ

ヘルプファイル、開く 41

ほ

ポータルユーザー 管理 68 作成 68 ポータルユーザーの権限、設定 75 ポリシー コピー 237 作成 233 削除 312 導入 222 名前変更 242 ポリシーに割り当てられたエンドポイント、表示 301 ポリシーのコピー 237 ポリシーの適用 1 つのエンドポイントへ 325 グル**ー**プへ 324 ホワイトリストのオーバーライド、作成 432

# ま

マルウェア対策コマンド 154

# め

א=ם- Mac  $\mathcal{O}$  SecureAnywhere 169

#### Þ

ユーザーアクセスコマンド 153 ユーザーインターフェイスの設定 289 ユーザー情報、編集 72

# り

リアルタイムシールドの設定 274

#### れ

レポート インストールしたエージェント 395 エージェントのバージョンの使用状況 390 オーバーライドの適用 454 ブロックされたすべての URL 356 確認されたすべての脅威 342 確認されたすべての未判定のソフトウェア 349 脅威の履歴 (内訳) 377 最新のスキャンで脅威が存在したエンドポイント 361 最新のスキャンで未判定のソフトウェアが検出されたエンドポイント 365 生成 340 日単位のブロックされた URL の履歴 386 日単位の脅威の履歴 369 レポートのスプレッドシート、ダウンロード 402 レポートのデータ、並べ替え 45

# ろ

ログイン、初回 24

# 漢字

#### 開く

SecureAnywhere, Mac 167 SecureAnywhere, Windows 165 エンドポイントプロテクションのメニュー 38 パネル 40 ビデオチュートリアル 41 ヘルプファイル 41 概要 使用状況データへのアクセス 530 概要、エンドポイントプロテクション 2 環境、設定 5 環境設定 5 管理 エンドポイントのアップデート 162 ポータルユーザー 68 脅威 171 管理コンソール、アクセス 52 管理ポータル、使用 33

基本設定 259 強制実行 **アップデート** 177 即時のアップデート 180 脅威、管理 171 脅威の最新状況、表示 208 警告 一時停止 422 削除 422 導入 405 警告の一時停止 422 高度なコマンド 158 作成 [グループの管理] でのウェブのオーバライド 485 [レポート] でのウェブのオーバライド 494 ウェブのオーバーライド 480 ウェブルートアカウント 11 カスタムの警告 408 ブラックリストのオーバーライド 426 ポータルユーザー 68 ポリシー 233 ホワイトリストのオーバーライド 432 配信先リスト 406 削除 ウェブのオーバーライド 506 グループ 338 サイト管理者 107 ポリシー 312 警告 422 使用 [IP 範囲] タブ 334 [アクティブディレクトリ] タブ 332 [ワークグループ] タブ 336 Mac 版 SecureAnywhere インストーラー 118 SecureAnywhere のインストーラー 116 Windows 版 SecureAnywhere インストーラー 117 管理ポータル 33 自己保護の設定 269 初回のログイン 24 生成 [インストールされたエージェント] レポート 395 [エージェントのバージョンの使用状況] レポート 390 [ブロックされた URL の履歴 (日単位)] レポート 386 [ブロックされたすべての URL] レポート 356 [確認されたすべての脅威] レポート 342 [確認されたすべての未判定のソフトウェア] レポート 349

[脅威の履歴 (内訳)] レポート 377 [脅威の履歴 (日単位)]レポート 369 [最新のスキャンで脅威が存在したエンドポイント] レポート 361 [最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポート 365 エンドポイントプロテクションのレポート 340 レポート 340 製品情報、アクセス 43 設定 ID シールド 284 Web 脅威シールド 281 コアシステムシールド 279 システム最適化ツール 290 スキャン 264 スキャンのスケジュール 262 データフィルタ 512 ヒューリスティック 270 ファイアウォール 287 ファイルのオーバーライド 174 ポータルユーザーの権限 75 ユーザーインターフェイス 289 リアルタイムシールド 274 基本設定 259 自己保護 269 動作シールド 277 説明 エンドポイントプロテクションのタブ 37 即時のアップデート、強制実行 180 滞留時間、概要 214 滞留時間について 214 滞留時間のポップアップ、オーバーライドの適用 459 単一のエンドポイント、ポリシーの適用 325 追加 キーコード 81 グループ 319 コンソール 84 サイト管理者 93 定義された警告メッセージ、表示 420 電源コマンド 153 動作シールドの設定 277 導入 オーバーライド 424 ポリシー 222 警告 405 入力 プロキシバイパス 8 プロキシ情報、インストーラー内 8

プロキシ情報、エンドポイント上 9 配信先リスト、作成 406 配備方法、選択 29 配備方法の選択 29 表のデータ、並べ替え 45 表示 エージェントのバージョンの概要 212 エンドポイントの状態 204 オーバーライド 466 コマンドログ 520 スキャン履歴 171 データフィルタログ 524 ポリシーに割り当てられたエンドポイント 301 脅威の最新状況 208 定義された警告メッセージ 420 変更ログ 517 複製イメージ、SecureAnywhere のインストール 132 変更 エンドポイントのキーコード 135 エンドポイントのハードウェア 162 変更ログ、表示 517 編集 アカウント設定 55 ウェブのオーバーライド 502 サイト管理者設定 98 ユーザー情報 72 名前変更 エンドポイント 138 グループ 321 コンソール 90 ポリシー 242 要件、システム 4