

WEBROOT®

ウェブルート セキュアエニウェア ビジネス

-エンドポイント プロテクション

管理コンソール画面操作ガイド

Table of Contents

文書情報	3
更新履歴.....	3
コンソール利用の準備	4
Webroot アカウントの登録.....	4
確認メール.....	5
コンソール名の変更.....	6
タイムゾーンの変更.....	6
表示言語.....	7
利用規約とプライバシーポリシー.....	8
パスワードまたはセキュリティコードを忘れた場合.....	9
管理コンソール機能	11
アカウント設定.....	12
ユーザーの管理.....	13
アクセス権.....	15
キーコードの管理.....	18
新しいコンソールの追加方法.....	19
ダウンロード.....	21
ヘルプ.....	21
サポート.....	22
ログアウト.....	22
エンドポイントプロテクション	23
初めてアクセスする場合.....	23
状態.....	24
ポリシー.....	27
あらかじめ用意されているポリシー.....	37
ポリシーの編集.....	38
使用するグループとエンドポイント.....	39
グループの管理.....	40
エンドポイント一覧.....	41
コマンド.....	43
スキャン履歴.....	54
非アクティブ化.....	54
レポート.....	55
インストールされたエージェント.....	55
エージェントのバージョンの使用状況.....	55
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.....	55
最新のスキャンで脅威が検出されたエンドポイント.....	56
発見されたすべての未判定のソフトウェア.....	56
発見されたすべての脅威.....	56
脅威の履歴(日単位).....	57
脅威の履歴(内訳).....	57
警告.....	57
オーバーライド.....	60
ログ.....	62
変更ログ.....	62
コマンドログ.....	62

文書情報

更新履歴

Date	Author	Position	Version	Change Reference
2012/6/25	Tatsunobu Murata		0.1	New
2012/6/28	Tatsunobu Murata		0.2	Revised for Silent Policy etc.
2012/9/12	Taki Nakamura		1.0	Revised minor changes and etc
2013/7/12	Taki Nakamura		1.1	Updated screen captures and adding alert
2013/11/06	Taki Nakamura		1.2	Updated screenshots and some minor changes

コンソール利用の準備

Webroot アカウントの登録

まだ Webroot アカウントを作成していない場合、<http://my.webrootanywhere.com> にアクセスします。ブラウザの言語設定に応じて適切な言語を表示するサイトにリダイレクトするので、[今すぐ登録する]をクリックします。

アカウントを作成するために必要な情報を入力する画面が表示されます。セキュアエニウェアのキーコードを[ウェブルート製品のキーコード]に登録し、その他のフィールドに必要な情報を入力します。

- 入力した電子メールアドレスにアカウント作成用の確認メールが送信されますので、間違いのないように入力してください。
- 指定したパスワードとセキュリティコードは作成されたアカウントにログインする際に必要です。忘れないようにしてください。

全フィールドに入力したら、[今すぐ登録]ボタンをクリックします。

ご登録ありがとうございます

キーコードをご登録いただきありがとうございます。コンソールを有効にするためのリンクを記載した確認の電子メールを送信しました。

確認メール

上記のメッセージが表示されたら指定したメールアドレスに確認用メールが送信されてきます。

ウェブルート コンソールの確認 (アクションが必要)

受信トレイ x

Webroot Console Confirmation noreply@webroot.com 18:25 (3分前) ☆

To 自分

キーコードをご登録いただきありがとうございます。登録を完了し、ウェブルート コンソールをアクティブにするには、次の確認のリンクをクリックしてください:

<https://ja-my.webrootanywhere.com/regconfirm.asp?LEX=077FADF0-8D0A-4AA0-9038-9522E16CE75A&L=6&EM=tatsu56u.antiv@gmail.com&FL=Y&AP=N>

今後ともご愛顧のほどよろしくお願い申し上げます。ウェブルート株式会社

アカウント登録メールにしたがって登録処理を完了しないと、セキュアエニウェアのメイン画面には以下のようなメッセージが表示されます。



アカウントのアクティブ化が必要

セキュアエニウェア アカウントが作成されましたが、アクティブ化するには電子メールアドレスを確認する必要があります。

アカウント開設のサポート

メールに含まれている URL をクリックしてアカウント登録を完了すると、セキュリティコード入力画面が表示されるので、アカウント作成時に指定したセキュリティコードから指定されている位置の文字を入力し、[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の 3 番目と 6 番目の文字を入力してください

今すぐ登録確認する

正しく設定されていれば、以下のような画面が表示されます。



コンソール名の変更

アカウントを登録すると、デフォルトで[名前のないコンソール]が作成されます。右上のコンソール名の右にある鉛筆アイコンをクリックすることでコンソール名を変更できます。



コンソール名を入力したら緑のチェックアイコンをクリックします。



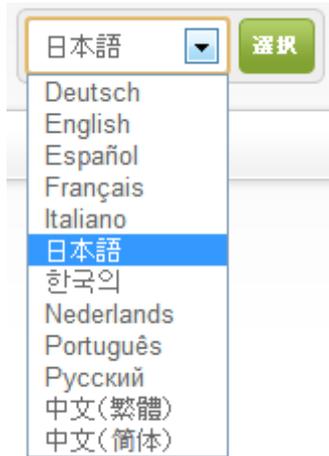
タイムゾーンの変更

アカウント登録をした状態ではデフォルトでタイムゾーンは GMT に設定されています。タイムゾーンを日本時間に変更することでコンソール上で表示される時間が日本時間になります。

タイムゾーンの変更方法については「[アカウント設定](#)」を参照してください。

表示言語

<https://my.webrootanywhere.com> にアクセスすれば、ブラウザの言語設定に応じて適切な言語を表示する URL にリダイレクトされます (日本語であれば <https://ja-my.webrootanywhere.com>)。ブラウザの言語設定とは異なる言語で表示したい場合は、ログイン画面にある言語選択ドロップダウンリストから選択します。



希望の言語を選択後、[選択]をクリックすることで、以降管理コンソールにアクセスする際に使用される言語を指定できます。

利用規約とプライバシーポリシー

<http://my.webrootanywhere.com> の下部に利用規約とプライバシーポリシーへのリンクがあります。

日本 マイアカウント サポート

WEBROOT®

個人向け 法人向け パートナー向け お客様向け

ウェブルートからの法律上のお知らせ

Webroot, Inc. (ウェブルート) は、本サイトにおいて以下の条件に従い、情報と製品を提供いたします。このサイトを使用される方 (以下「皆様」といいます) は、本サイトにアクセスすることにより、この条件に同意したことになります。ウェブルートはいつでも、予告なしに、適宜この条件を変更する権利を留保いたします。ウェブルートは、この条件の違反につき、法令上可能なあらゆる権利を行使することができます。以下において、特に付与されない権利は、ウェブルートに留保されます。

著作権

本サイトに記載の情報は著作権により保護されています。特に許された場合を除き、方法、形式のいかんにかかわらず、本サイトのいかなる部分も、ウェブルートの事前の書面による許可なしに、複製または譲渡することはできません。

著作権表示

© 2013 – Webroot Inc. All rights reserved.

責任の排除

本サイトを通じて提供される一切の情報 (製品またはサービスの企画、ソフトウェア・プログラム、ソフトウェア・コード、提供物、プログラム、将来の方針の記述、ホワイト・ペーパー、その他の技術上もしくは販売上の資料を含みますが、これらに限定されません) (以下「掲載情報」といいます) は、情報提供の目的のためにのみ掲載されており、ウェブルートは、適宜、予告なしに変更することがあります。ウェブルートは、掲載情報の正確性や完全性については何ら責任を負いません。掲載情報は、商品性や特定目的への適合性、権利非侵害に関する黙示の保証その他の一切の保証なしに、現状のまま提供されています。ウェブルートは、本ウェブサイトおよびここで提供される掲載情報に関し、一切の責任を排除いたします。管轄地域によっては、黙示の保証の排除が許されない場合がありますが、その場合には、以上の責任の排除は適用されません。いかなる場合でも、ウェブルートは、どなたに対しても、また、損害発生の可能性

日本 マイアカウント サポート

WEBROOT®

個人向け 法人向け パートナー向け お客様向け



ウェブルートは、欧州連合およびその構成国ならびにスイスから取得した個人データの収集、転送、使用および保持に関して、米国商務省が推挙する米国・欧州連合セーフハーバーフレームワークおよび米国・スイスセーフハーバーフレームワークを遵守しています。ウェブルートは、通知、選択、転送、セキュリティ、安全性、データの完全性、アクセスおよび執行のセーフハーバー プライバシー原則を堅持することを証明いたしました。セーフハーバー原則につき更にお知りになりたい場合及びウェブルートの証明の閲覧をされる場合は、[HTTP://WWW.EXPORT.GOV/SAFEHARBOR/](http://WWW.EXPORT.GOV/SAFEHARBOR/) にアクセスしてください。

発効日: 2002年1月1日

最新の更新日: 2013年8月8日

ウェブルートは、2013年8月8日に本プライバシーポリシーをアップデートし、パブリック・フォーラムに関する情報を含めました。詳しくは、以下の1項目をご覧ください。

プライバシーポリシー

ウェブルートにとって、お客様のプライバシーの保護は非常に重要な課題です。つまるところ、オンラインのプライ



Webroot

Software, Inc. は、TRUSTe からプライバシーマークを授与されています。これは、このプライバシーポリシーと情報の取扱いがTRUSTeによって審査され、お客様の個人情報の収集と使用に関する透明性、説明責任、選択の提供などを含むTRUSTeのプログラム要件 (TRUSTe's program requirements) に遵守していることを示すものです。TRUSTe プログラムは、当社 Web サイト (www.webroot.com/jp/la) を通じて収集された情報のみを対象とし、当社のモバイルアプリケーションやダウンロードしたソフトウェアによって収集される情報は対象には含まれません。TRUSTe の使命は、独立したサードパーティとして、プライバシー信頼マークと革新的な信頼ソリューションを通して、世界中の企業およびお客様の間のインターネットにおける信頼を推進することであり

リセット用のメールに含まれる URL をクリックします。

お客様のウェブルート コンソール パスワード

受信トレイ x



Webroot Console Password noreply@webrootclo 0:48 (1分前) ☆

To 自分

当社製品をご利用いただき誠にありがとうございます。ご請求いただいた、パスワードをリセットするリンクは次のとおりです：

<https://ja-my.webrootanywhere.com/resetpassword.asp?LEX=54B0245B-15BB-4D80-91F4-D6A6A8C7BF74>

今後ともご愛顧のほどよろしくお願い申し上げます。ウェブルート株式会社

パスワードもしくはセキュリティコードリセット画面が表示されるので、新しく入力して保存します。

[詳細のリセット](#)

以下に詳細を入力してください：

新しいパスワードを作成 *

強度： 中

新しいパスワードを再入力 *

新しいパスワードを保存

リセット処理が完了します。

[詳細のリセット](#)

完了しました

変更が適用されました。ログインできます。

ログイン

管理コンソール機能

ログイン後画面右上に表示されているメールアドレスをクリックすると、ユーザー管理機能がドロップダウンリストで表示されます。



ユーザーの管理

ユーザーの管理

新規ユーザーの作成

名前	電子メール	権限		
		セキュアエニウェア	エンドポイント プロテクション	
	 (アクティブ)	管理者	管理者	
	 (アクティブ)	基本	基本	
村田	 (アクティブ)	管理者	管理者	

コンソールにアクセスできるユーザーを追加することができます。ユーザーの追加は以下の手順に従います。

1. 右上のドロップダウンより[新規ユーザーの作成]をクリックします。
2. [新規ユーザーの作成]画面に電子メールとタイムゾーンを入力します。

新規ユーザーの作成

新規ユーザーを作成するには以下に詳細を入力してください

電子メールアドレス

タイムゾーン 

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? はい

タイムゾーンは鉛筆アイコンをクリック後、日本と入力し、表示された[日本、東京、京都、大阪、横浜]を選択後、緑色のチェックアイコンをクリックします。

3. [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?]をチェックすると以下の入力フィールドが表示されるので、必要なアクセス権を設定します。

セキュアエニウェア

エンドポイント プロテクション

アクセス権の詳細は「[アクセス権](#)」を参照してください。

4. [ユーザーを作成]ボタンをクリックします。

該当ユーザーが新規の Webroot アカウントである場合、作成したユーザーのメールアドレスに確認用のメールが送信され、以下のメッセージが表示されます。

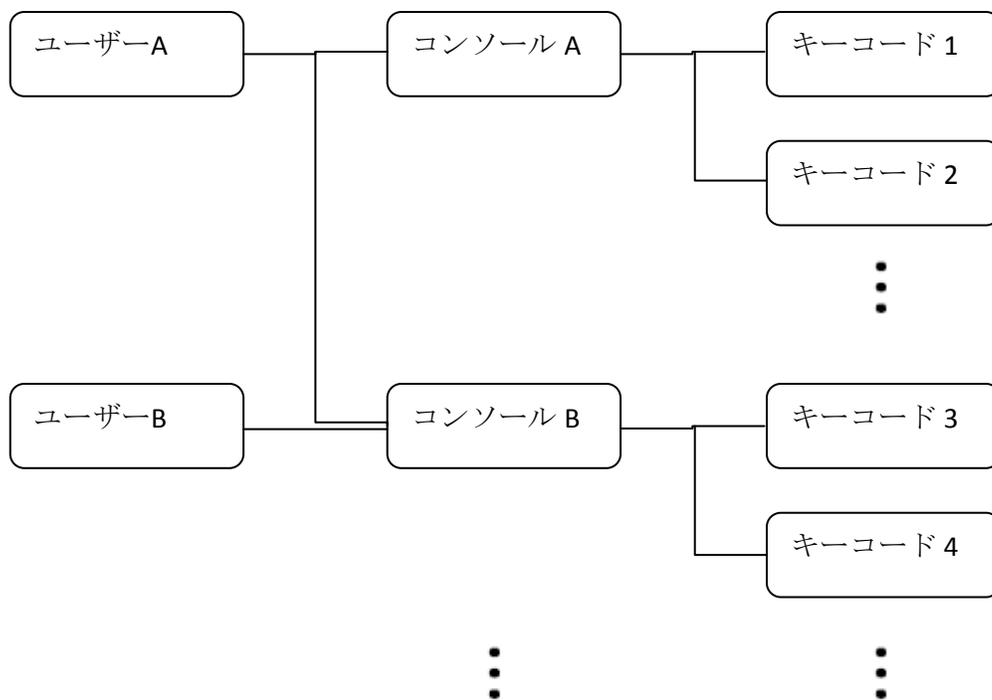
アクセス権が付与されました

新しいユーザーにコンソールへのアクセス権について通知する電子メールが送信されます。これを確認するとログインできるようになります。

[ユーザーの管理に戻る](#)

アクセス権

セキュアエニウェアのコンソールにおけるユーザーの概念は以下のようになっています。



1ユーザーは複数のコンソールに対するアクセス権を付与することができ、1つのコンソールには複数のキーコードを割り当てることができます。また、1つのコンソールに複数のユーザーを割り当てることができます。ただし、1つのキーコードを複数のコンソールに割り当てることはできません。

アクセス権とは、コンソールにログインしたユーザーが、自分が割り当てられている各コンソールに対してどのようなアクセスが許されるかを設定するものです。たとえば、上記の図では、ユーザーAはコンソールAとコンソールBに対してそれぞれ個別にアクセス権を設定することになります。

ユーザーがコンソールにアクセスするには、コンソールに対して[セキュアエニウェア]へのアクセス権が必要です。コンソールに対して一度割り当てたユーザーは削除することはできないので、特定ユーザーに対してコンソールへのアクセスを止めたい場合には、該当ユーザーの[セキュアエニウェア]へのアクセス権を[不可]に変更します。一方、コンソールへのアクセスを許可するユーザーには、[セキュアエニウェア]に対して以下のいずれかのアクセス権を設定します。

- 基本
アカウント設定だけが利用できます。ただしアクセス権の変更はできません。
- 管理者
アカウント設定の他、ユーザーの管理、キーコードの管理を利用できます。

また、[エンドポイントプロテクション]コンソールに対してもアクセス権を設定することができます。ユーザーに[エンドポイントプロテクション]コンソールへのアクセスを許可する場合は、以下のいずれかのアクセス権を設定します。

- 基本
コンソールが提供する情報にアクセスすることができますが、設定などを変更することはできません。たとえば、セキュリティポリシーの設定などを変更することはできません。また、コマンド発行も一切できません。
- 管理者
コンソールが提供する情報にアクセスするだけでなく、設定されている権限に応じて設定を変更することができます。

管理者のアクセス権

[エンドポイントプロテクション]に対して管理者のアクセス権を与えると、更に以下の詳細権限の詳細画面が表示されます。

グループ	
作成	<input type="checkbox"/>
エンドポイントの非アクティブ化	<input type="checkbox"/>
グループへのエンドポイントの割り当て	<input type="checkbox"/>
ポリシー	
作成・編集	<input type="checkbox"/>
エンドポイントへのポリシーの割り当て	<input type="checkbox"/>
オーバーライド	
MD5	<input type="checkbox"/>
コマンド	
なし	<input type="radio"/>
シンプル	<input type="radio"/>
アドバンス	<input type="radio"/>
エキスパート	<input type="radio"/>
警告	
他のユーザーへの警告を受信	<input type="checkbox"/>

設定した詳細権限を該当ユーザー自身が変更できないようにするには、[セキュアエニウェア]に対して[基本]権限を付与します。

詳細権限で設定されるコマンド実行権と実行可能なコマンドの関係は以下の通りです。

- シンプル
 - 以下のコマンドを実行可能
 - エージェント
 - データを消去
 - 選択したエンドポイントのコマンドを表示
- アドバンスト
 - シンプルに加えて以下のコマンドを実行可能
 - 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
 - ID シールド
- エキスパート
 - アドバンストに加えて以下のコマンドを実行可能
 - アドバンスト

キーコードの管理

キーコードの管理

製品キーコードを追加

キーコードを今すぐ購入

キーコード	エディション	デバイス	有効期限までの日数	更新	アップグレード
SAE◆◆◆◆◆EBBF	エンドポイントプロテクション	10	223 (2013年1月25日)	更新	アップグレード

コンソールに対して新しいキーコードを追加することができます。

[製品キーコードを追加]

キーコードの追加

キーコードを追加する

製品キーコード

製品キーコードに追加するキーコードを入力して[追加]をクリックすることでコンソールにキーコードが追加されます。

既に他のコンソールに割り当てられているキーコードを追加しようとすると以下のようなメッセージが表示され、キーコードは追加されません。

エラー (UAL043): このキーコードは既に登録されています

新しいコンソールの追加方法

新しいコンソールを追加したい場合は、コンソールのログイン画面で[今すぐ登録する]をクリックします。

ログイン

電子メールアドレス

パスワード

[ログインできない場合](#)

アカウントを作成する

セキュリティと利便性

アカウントを作成すると、複数のデバイスでウェブルート製品を使用してセキュリティを管理できます。また、簡単な操作で新しいデバイスを追加し、他のユーザーのデバイスを保護できるようになります。

アカウントを作成するための情報入力ページで、新しいコンソールを作成するためのキーコードと新しいコンソールを割り当てる既存の Webroot アカウントのメールアドレスを入力します。

アカウントを作成する:

ウェブルート製品のキーコード *

電子メールアドレス *

電子メールアドレスを再入力 *

パスワード *

パスワードの繰り返し *

個人用セキュリティコード *

セキュリティの質問 * 母親の出生地

セキュリティの回答 * サンフランシスコ

既存のメールアドレスを入力

指定したメールアドレスに該当するアカウントが検出され、以下の画面が表示されます。

以前に登録されたことがありますか？

お客様の詳細の一部が既存の記録と一致し、お客様がすでに所有しているウェブルート セキュアエニウェア コンソールが確認されました。

次の2つのオプションのいずれかを選択してください。

このキーコードに新しいコンソールを追加する

このオプションが選択された場合:

- 今後のログインでは、元のログイン詳細を使用してください。
- 今回のシングルログインが終了するまでは、所有しているどのコンソールにもアクセスできます。

選択

このキーコードを既存のコンソールに追加する

手順:

1. 既存のアカウントにログインします
2. [キーコードの管理] をクリックします
3. [製品キーコードを追加] ボタンをクリックします
4. キーコードをボックスに入力して [追加] をクリックします
5. 既存のコンソールにキーコードが正しく追加されます

ログイン



サポートにご連絡いただく必要がある場合は、次の参照番号をお申し出ください:

危険 (URFL301): このキーコードに対して新しいコンソールを作成しますか？

[このキーコードに新しいコンソールを追加する] を選択します。

ご登録ありがとうございます

コンソールが作成されました。次回のログイン時に使用できるようになります。

ログイン

既存のアカウントに対して新しいコンソールが作成され、該当ユーザーでログインするとコンソール選択画面が表示されます。

表示するコンソールを選択してください:

コンソール名	作成日	キーコード	許可されたデバイス	期限切れのキーコード
ブランクエンドポイントプロテクション	2012年6月16日 11:08	-	-	-
Sales Demo Account	2012年1月27日 0:37	2 表示	70	0
ウェブルートデモ	2012年1月26日 23:34	1 表示	10	0

新規に作成されたコンソールはデフォルトで[名前のないコンソール]になっているので、必要に応じてコンソール名を編集します。

一度コンソールを選択後、表示するコンソールを切り替える場合はコンソール名の横のディスプレイアイコンをクリックします。

ブルームフィールド コンソールを変更する エンドポイントの検索...

ダウンロード

ホーム
エンドポイント プロテクション
ブルームフィールド

状態
ポリシー
グループの管理
レポート
警告
オーバーライド
ログ
リソース

リソース

簡易配備オプション

コンソールにエンドポイントを登録するための最も迅速かつ簡単な方法は、キーコードが自動で適用されるウェブルート セキュアエニウェアのコピーをダウンロードして実行することです。その後、このファイルをユーザーが実行するだけで、エンドポイントのコンソールに自動的にレポートが表示されます。

ご使用になれるキーコード / ダウンロード:

SAE6TESTD3DA25C9E8BF	Windows 用ダウンロード	Windows 用電子メールテンプレート
----------------------	-----------------	----------------------

Mac ユーザーはこちらからウェブルート セキュアエニウェア ソフトウェアをダウンロードできます: [Mac 用ダウンロード](#)

高度な配備オプション: (Windows のみ)

コマンドラインからバックグラウンドでインストーラーを実行

- エンドポイントで、ウェブルート セキュアエニウェアのインストーラーをダウンロードします。ダウンロードするには[こちらをクリックしてください](#)。
- 配備のヘルプに記載されたコマンドを使用して、コマンドラインからインストーラーを実行します。表示するには[こちらをクリックしてください](#)。

MSI を使用してインストール

- ウェブルート セキュアエニウェア MSI インストーラーをダウンロードします。ダウンロードするには[こちらをクリックしてください](#)。
- 配備のヘルプに記載されたコマンドを使用して、コマンドラインからインストーラーを実行します。表示するには[こちらをクリックしてください](#)。

ウェブルートセキュアエニウェアのインストールに必要なファイルのダウンロードとその使い方に関する説明が表示されます。

ヘルプ

コンソールサイト利用に関するオンラインヘルプを開きます。

WEBROOT®
SecureAnywhere.
tatsunobu.murata@webroot.com

ホーム
エンドポイント プロテクション

はじめに

- [セキュアエニウェア エンドポイント プロテクションについて](#)
- [ウェブルート アカウントの作成](#)
- [セキュアエニウェア エンドポイント プロテクションへのログイン](#)
- [セットアップ ウィザードの使用](#)
- [管理されているエンドポイントの状態の表示](#)
- セキュアエニウェアの実装**
- [実装の方法](#)
- [セキュアエニウェア インストーラーのダウンロードと実行](#)
- [インストーラーをバックグラウンドで実行](#)
- [MSIを使用したインストール](#)
- [GPOを使用したインストール](#)
- [セキュアエニウェア リモート実装ツールの使用](#)
- アカウントの操作**
- [アカウント設定の編集](#)
- [アカウントへのコンソールの追加](#)
- [警告の設定](#)

ウェブルートセキュアエニウェア エンドポイント プロテクションについて

ウェブルート エンドポイント プロテクションは、エンタープライズ全体のウェブルート セキュアエニウェア ソフトウェアを管理するための管理者向けポータルです。次の2つの管理モードを使用できます。

- 管理モード:**ウェブルート セキュアエニウェア エンドポイント プロテクションの一元的なポリシーにより、エンドポイントのウェブルート セキュアエニウェア ソフトウェアが管理されます。エンドユーザーがローカルで設定を行うことはできません。
- 非管理モード:**エンドユーザーがウェブルート セキュアエニウェア ソフトウェアを設定でき、セキュアエニウェア エンドポイント プロテクションでスキャン結果を表示できます。一元的なポリシーは強制されません。

ウェブルート セキュアエニウェア エンドポイント プロテクションに初めて登録する際に、セットアップ ウィザードが開き、エンドポイントに実装するポリシーをすばやく指定できます。詳細については「[セットアップ ウィザードの使用](#)」を参照してください。

登録後、キーコードを使用してアカウントを作成します。詳細については「[ウェブルート アカウントの作成](#)」および「[セキュアエニウェア エンドポイント プロテクションへのログイン](#)」を参照してください。

アカウントの作成および登録を済ませ、ログインすると、管理するエンドポイントにウェブルート セキュアエニウェアを実装できます(詳細は[実装の方法](#)をご覧ください)。その後、エンドポイントの動作を定義するポリシーとグループを追加できます。

セキュアエニウェア エンドポイント プロテクションのホーム ページには、管理されているエンドポイントの概要が表示されます。また、エンドポイント プロテクションのタブを開くと、管理されているエンドポイントの状態を確認できます。詳細については「[管理されているエンドポイントの状態の表示](#)」を参照してください。

サポート



The screenshot shows a web browser window with the URL `ja-detail.webrootanywhere.com/howcanwehelpbusiness.asp?FOUR=Y&CMD=UBERSUPPORT&SOURCE=ENTERPRISESAPSEC`. The page features the Webroot logo and the heading "企業・法人向け製品サポート". Below this, it highlights "SecureAnywhere » Endpoint Protection" and provides a brief description of the support service. A search bar is present, followed by a "ウェブルートに質問する" button. At the bottom, there are links for "よくあるご質問", "ウェブルートセキュアエニウェア エンドポイント プロテクション ガイド", "サポートチケットを送信する", and "サポートチケットの確認". A "サポートに連絡" link is also visible in the bottom right corner.

ログアウト

現在ログインしているユーザーをログアウトします。

ログアウト

ログオフしました

ホームに戻る

エンドポイントプロテクション

コンソールに表示されている[エンドポイントプロテクション]タブか[エンドポイントプロテクションに進む]ボタンをクリックすることでエンドポイントプロテクションに進むことができます。

The screenshot shows the Webroot SecureAnywhere dashboard. At the top, there's a navigation bar with 'ホーム' (Home) and 'エンドポイント プロテクション' (Endpoint Protection) tabs. Below the navigation bar, there's a summary card for 'エンドポイント プロテクション' (Endpoint Protection) with the following statistics:

- 7 台のエンドポイントが保護されています
- 0 台のエンドポイントが現在感染しています
- 0 台のエンドポイントが感染しています (過去 24 時間)

At the bottom of the card, there is a button labeled 'エンドポイント プロテクションに進む' (Go to Endpoint Protection).

初めてアクセスする場合

エンドポイントプロテクションコンソールに初めてアクセスする場合、エンドポイントに適用されるデフォルトのセキュリティポリシーを選択する画面が表示されます。

The screenshot shows the 'セットアップ ウィザード' (Setup Wizard) screen. It prompts the user to select a default policy for the endpoint during installation. The text reads: 'インストール時にエンドポイントに適用されるデフォルトのポリシーを選択してください。' (Please select the default policy to be applied to the endpoint during installation.)

Below this, it states: 'これらのポリシーは初期設定用にウェブルート セキュアエニウェア エンドポイントプロテクションに用意されています。インストール後に新しいポリシーを作成して、管理対象のエンドポイントに適用することもできます。' (These policies are prepared for initial setup in Webroot SecureAnywhere Endpoint Protection. After installation, you can also create a new policy and apply it to managed endpoints.)

The user is asked to 'デフォルトの設定を選択してください *' (Select the default settings *). A dropdown menu is set to '推奨デフォルト設定' (Recommended default settings). A '送信' (Send) button is visible below the dropdown.

A note at the bottom says: '注意：デフォルトのポリシーは、インストール後に変更できます。' (Note: The default policy can be changed after installation.)

まだ1つもエンドポイントを登録していないコンソールではエンドポイントの配布方法に関する情報が表示されます。

The screenshot shows the 'リソース' (Resources) section of the console. It provides instructions on how to register endpoints:

コンソールにエンドポイントを登録するための最も迅速かつ簡単な方法は、キーコードが自動で適用されるウェブルート セキュアエニウェアのコピーをダウンロードして実行することです。その後、このファイルをユーザーが実行するだけで、エンドポイントのコンソールに自動的にレポートが表示されます。

ご使用になれるキーコード / ダウンロード:

- SABQJTESD473356A367B (Windows 用ダウンロード) (Windows 用電子メールテンプレート)

Mac ユーザーはこちらからウェブルート セキュアエニウェア ソフトウェアをダウンロードできます: (Mac 用ダウンロード)

高度な配備オプション:(Windows のみ)

コマンドラインからバックグラウンドでインストーラーを実行

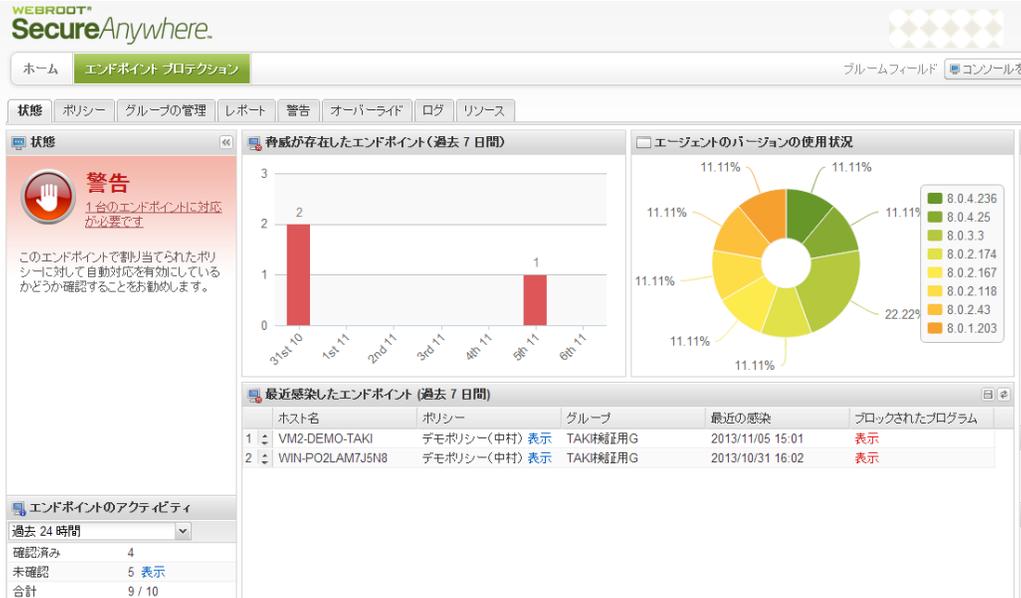
- エンドポイントで、ウェブルート セキュアエニウェアのインストーラーをダウンロードします。ダウンロードするにはこちらをクリックしてください。
- 配備のヘルプに記載されたコマンドを使用して、コマンドラインからインストーラーを実行します。表示するにはこちらをクリックしてください。

MSI を使用してインストール

- ウェブルート セキュアエニウェア MSI インストーラーをダウンロードします。ダウンロードするにはこちらをクリックしてください。
- 配備のヘルプに記載されたコマンドを使用して、コマンドラインからインストーラーを実行します。表示するにはこちらをクリックしてください。

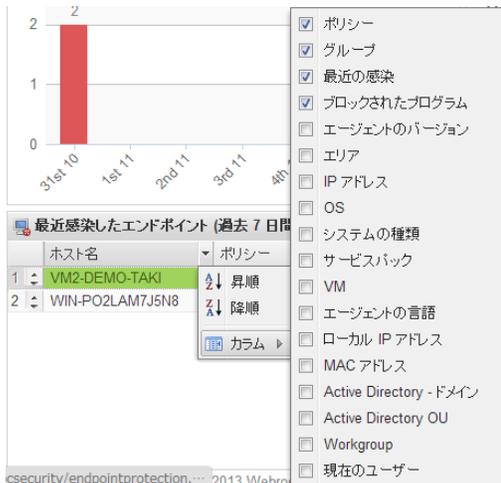
状態

監視されている全エンドポイントの概況を表示します。



エンドポイントプロテクションコンソールでは をクリックすることで表示されている情報をリフレッシュできます。また、 をクリックすることで表示されている情報を CSV 形式で出力できます。

また、一覧表示でカラムの上にマウスをホバーした際に表示される ▼ をクリックすることで、データをソートしたり表示するカラムの選択を行うことができます。



[状態]に警告表示がされている場合、[対応が必要です]リンクをクリックすると以下の画面が表示されます。

対応が必要なエンドポイント

脅威が存在するエンドポイント

	ホスト名	ポリシー	エージェントのバージョン	エリア
1	TMURATA-503DD9C	#営業部門ポリシー 表示	8.0.1.193	

このエンドポイントで発見された脅威

オーバーライドを作成

	ファイル名	パス名	マルウェアグループ	最近の観測
1	TROJAN.PROXY.WIN32.GEN_1...	%temp%\testvirus.zip E381AEE...	W32.Trojan.Mitglieder	2012/06/18 10:50

[未確認]の[表示]をクリックすると以下の画面が表示され、状態の確認が取れていないエンドポイントの一覧を表示することができます。

未確認のエンドポイント: 過去 24 時間

	ホスト名	グループ	最終確認日時	エージェントのバージョン
1	VM-WIN7PRO-EN01	fuji-test-group	2013/11/01 18:02	8.0.4.25
2	TAK-VM-2	TAK試験証用G	2013/08/28 13:07	8.0.2.167
3	LH-A6YUXRDE8PFT	fuji-test-group	2013/03/29 16:59	8.0.2.118
4	WIN-7U989MA5TEE	デフォルトのグループ	2012/11/15 03:24	8.0.2.43
5	WIN-M9K4KIQCJHP	マーケティング部門	2012/07/22 01:13	8.0.1.203

[脅威が発見されたエンドポイント]に赤い棒グラフが表示されている場合、棒グラフ部分をクリックすることで該当期間に脅威が発見されたエンドポイントの詳細を表示することができます。

選択した期間に脅威が発見されたエンドポイント

エンドポイント

	ホスト名	ポリシー	最新のスキャン時間	エージェントのバージョン
1	TMURATA-503DD9C	#営業部門ポリシー	2012/06/18 10:50	8.0.1.193

このエンドポイントでブロックされたプログラム

オーバーライドを作成

	ファイル名	パス名	マルウェアグループ	最近の観測
1	TROJAN.PROXY.WIN32.GEN_1...	%temp%\testvirus.zip E381AEE...	W32.Trojan.Mitglieder	2012/06/18 10:50

[エージェントのバージョンの使用状況]に表示されている円グラフをダブルクリックすることで、該当バージョンを使用しているエンドポイントの一覧を表示することができます。

エージェント バージョンを実行するエンドポイント 8.0.1.193

	ホスト名	初めての観測	最近の観測
1	???XP???-2D9EC769	2012/06/16 12:48	2012/06/16 13:12
2	TMURATA-503DD9C	2012/06/14 14:31	2012/06/18 14:40
3	TMURATA-503DD9C-2D9EC769	2012/06/16 10:02	2012/06/17 03:56
4	TMURATA-503DD9C-9919A232	2012/06/16 13:40	2012/06/17 03:36
5	TMURATA-D600	2011/10/16 03:05	2012/06/17 09:31

[最近感染したエンドポイント]のポリシーの[表示]をクリックすることで感染したエンドポイントに適用されているセキュリティポリシーの詳細を表示できます。また、[ブロックされたプログラム]の[表示]をクリックすることで、該当エンドポイントで発見した脅威の一覧を表示できます。

このエンドポイントでこれまでに発見されたすべての脅威

オーバーライドを作成

	<input type="checkbox"/> ファイル名	パス名	マルウェアグループ	最近の観測
1	<input type="checkbox"/> TROJAN.PROXY.WIN32.G...	%temp%\testvirus.zip E38...	W32.Trojan.Mitglieder	2012/06/18 10:50

ポリシー

セキュリティポリシーの管理を行います。

The screenshot shows the Webroot SecureAnywhere management interface. At the top, there's a navigation bar with 'ホーム' and 'エンドポイントプロテクション'. Below that, a menu includes 'ポリシー', 'グループの管理', 'レポート', '警告', 'オーバーライド', 'ログ', and '資料'. The main area displays a table of policies with columns for 'ポリシー名', 'ポリシーの説明', '作成日', and '下書きの変更'.

ポリシー名	ポリシーの説明	作成日	下書きの変更
サイレント監査	秘出のみを実行するセキュリティ監査		
営業第二部門	営業2	2012/08/17 02:53	いいえ
営業第一部門	営業1	2012/08/17 02:53	いいえ
推奨されるデフォルト設定	保護と対応を行う推奨される設定		
管理対象外	ユーザーが管理するすべての PC で、このポリシーを...		
セミナーポリシー	セミナーA	2012/11/01 16:27	いいえ
デモポリシー(中村)	test	2012/07/05 11:29	いいえ
Recommended Server Defaults	Recommended setup for servers, protection enabled		
マーケティングポリシー	Marketing	2012/07/05 11:26	いいえ
#営業部門ポリシー	GUI非表示/未知なアプリ実行不可	2012/02/05 15:38	いいえ
#開発部門ポリシー	GUI表示可	2012/06/16 15:35	いいえ

[作成]をクリックすることで新しいポリシーを作成することができます。

The dialog box titled 'ポリシーを作成' contains two input fields: 'ポリシー名:' and 'ポリシーの説明:'. Below the fields are two buttons: 'ポリシーを作成' and 'キャンセル'.

ポリシー名とポリシーの説明を入力して[ポリシーを作成]をクリックします。ポリシーの説明には「GUI 表示可」など、ポリシー設定の特徴を書いておくとう便利です。新規に作成されるポリシーは[推奨されるデフォルト設定]がベースになります。ポリシーを選択し[削除]をクリックすることで該当ポリシーを削除することができます。[削除]をクリック後確認画面が表示されるので、削除する場合には[はい]をクリックします。

The dialog box titled 'ポリシーの削除' features a question mark icon and the text '削除しますか "#開発部門ポリシー"?' Below the text are two buttons: 'はい' and 'いいえ'.

※ システムに最初から用意されている[サイレント監査]、[推奨デフォルト設定]、[管理対象外]、[推奨サーバーデフォルト設定]については削除できません。

[削除したポリシーを表示]をチェックすると、削除したポリシーを表示することができます。

企画部門セキュリティ設定	企画用	2012/06/16 15:27	いいえ	削除済み
--------------	-----	------------------	-----	------

削除したポリシーはグレーアウトして表示されますが、[削除]以外の操作が可能ですので、削除したポリシーを基にして新しいポリシーを作成する必要がある場合などに便利です。

ポリシーを選択し[名前の変更]をクリックすることで該当ポリシーの名前を変更することができます。新しい名前を設定する画面が表示されるので、新しい名前を入力して[ポリシーの名前を変更]をクリックします。

※ システムに最初から用意されている[サイレント監査]、[推奨デフォルト設定]、[管理対象外]、[推奨サーバーデフォルト設定]については名前を変更できません。

ポリシーを選択し[コピー]をクリックすることで該当ポリシーを基に新しいポリシーを作成することができます。作成する新しいポリシーに関する設定画面が表示されるので、新しい名前と説明を入力して[ポリシーを作成]をクリックします。

※ システムに最初から用意されている[管理対象外]についてはコピーできません。

ポリシーを選択し[CSVにエクスポート]をクリックすることで、該当ポリシーの設定内容を CSV にエクスポートできます。データは UTF-8 でエクスポートされます。

ポリシーを選択し[デフォルトに設定]を選択することで、該当コンソールに新たに接続されるエンドポイントにデフォルトで適用されるポリシーを指定することができます。

ポリシーをダブルクリックすることでポリシー設定の詳細を表示することができます。表示される設定項目はエージェント側の設定画面に表示されるものと基本的に同じですが、コンソールからだけ設定できる特殊なパラメータがいくつかあります。

[基本設定]

セクション	設定	ライブ
基本設定	セキュアエニウェアへのショートカットをデスクトップ上に表示する	オフ
スキャンのスケジュール	システムトレイアイコンを表示する	オン
スキャン設定	起動時にスプラッシュ画面を表示する	オン
自己保護	セキュアエニウェアをスタートメニューに表示する	オン
ヒューリスティック	[プログラムの追加と削除] パネルにセキュアエニウェアを表示する	オン
リアルタイム シールド	Windows アクション センターにセキュアエニウェアを表示する	オン
動作シールド	セキュアエニウェアのキーコードを画面上に表示しない	オン
コア システム シールド	更新を自動的にダウンロードして適用する	オン
Web 脅威シールド	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	オフ
ID シールド	詳細なロギングよりも低ディスク使用量を優先する (ログ情報は少なくなります)	オフ
ファイアウォール	フル画面アプリケーションまたはゲームの検出時にリソース使用量を低減する	オン
ユーザー インターフェース	セキュアエニウェアの手動シャットダウンを許可する	オフ
システム クリーナ	重要でない通知をバックグラウンドに表示する	オン
	警告メッセージを自動的にフェードアウトする	オン
	実行履歴の詳細を保存する	オン
	ポーリング間隔	毎日

キャンセル

コンソール上で行われた設定変更はエージェントにプッシュされることはなく、すべてエージェントからのポーリングにより通知されます。ポーリング間隔は、エージェントがコンソールに対してポーリングを行う時間間隔を設定します。ポーリング間隔のデフォルトは[毎日]です。設定可能な間隔は毎日/12時間/6時間/4時間/3時間/2時間/1時間/30分/15分です。通常、コンソールからは頻繁に設定変更が行われることはないので、無駄なネットワークアクセスを軽減するにはデフォルトの[毎日]で問題ありません。

コンソールで行った変更をただちにエージェントに反映するには、エンドポイントのシステムトレイで  アイコンを右クリックし、[設定のリフレッシュ]を実行します。

今すぐスキャン

コンソールを開く

ヘルプとサポート

情報

設定のリフレッシュ

スキャン ログの保存

[スキャンのスケジュール]

推奨デフォルト設定		
セクション	設定	ライブ
基本設定	スケジュール スキャンを有効にする	オン
スキャンのスケジュール	スキャン頻度	毎日
スキャン設定	時間	スキャン...
自己保護	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...	オン
ヒューリスティック	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	オン
リアルタイム シールド	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	オン
動作シールド	バッテリー電源の場合はスケジュール スキャンを実行しない	オン
コア システム シールド	フル画面のアプリケーションまたはゲーム実行中はスケジュール スキャンを実行...	オン
Web 脅威シールド	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	オン
ID シールド	ディープ スキャンではなく、スケジュールされたクイックスキャンを実行する	オフ
ファイアウォール		
ユーザー インターフェース		
システム クリーナ		

キャンセル

[スキャン設定]

推奨デフォルト設定		
セクション	設定	ライブ
基本設定	リアルタイム マスター ブートレコード(MBR) スキャンを有効にする	オン
スキャンのスケジュール	拡張ルートキット検出を有効化する	オン
スキャン設定	Windows エクスプローラーでの「右クリック」スキャンを有効にする	オン
自己保護	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	オン
ヒューリスティック	高速スキャンよりも低メモリ使用量を優先する	オン
リアルタイム シールド	高速スキャンよりも低 CPU 使用量を優先する	オフ
動作シールド	非実行可能ファイルの詳細をスキャン ログに保存する	オフ
コア システム シールド	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	オフ
Web 脅威シールド	アーカイブ ファイルをスキャンする	オン
ID シールド	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	オフ
ファイアウォール	マルウェアのクリーンアップ中に再起動しない	オフ
ユーザー インターフェース	バックグラウンド スキャン中に発見された脅威を自動的に除去する	オン
システム クリーナ	学習スキャンで発見された脅威を自動的に除去する	オフ
	高度なサポートを有効にする	オン
	感染しているスキャン結果を表示する	オフ
	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)を悪質なものとして検知する	オフ

キャンセル

※ 学習スキャン = インストール後の初回スキャン

※ 高度なサポート = システム情報の自動アップロード

[自己保護]

推奨デフォルト設定

セクション	設定	ライブ
基本設定	自己保護応答のクローキングを有効にする	オン
スキャンのスケジュール	自己保護のレベル	最大
スキャン設定		
自己保護		
ヒューリスティック		
リアルタイム シールド		
動作シールド		
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 インターフェース		
システム クリーナ		

キャンセル

[ヒューリスティック]

推奨デフォルト設定

セクション	設定	ライブ
基本設定	リアルタイム マスター ブート レコード (MBR) スキャンを有効にする	オン
スキャンのスケジュール	拡張ルートキット検出を有効化する	オン
スキャン設定	Windows エクスプローラーでの「右クリック」スキャンを有効にする	オン
自己保護	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	オン
ヒューリスティック	高速スキャンよりも低メモリ使用量を優先する	オン
リアルタイム シールド	高速スキャンよりも低 CPU 使用量を優先する	オフ
動作シールド	非実行可能ファイルの詳細をスキャン ログに保存する	オフ
コア システム シールド	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	オフ
Web 脅威シールド	アーカイブ ファイルをスキャンする	オン
ID シールド	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	オフ
ファイアウォール	マルウェアのクリーンアップ中に再起動しない	オフ
ユーザー インターフェース	バックグラウンド スキャン中に発見された脅威を自動的に除去する	オン
システム クリーナ	学習スキャンで発見された脅威を自動的に除去する	オフ
	高度なサポートを有効にする	オン
	感染しているスキャン結果を表示する	オフ
	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) を悪質なものとして検知する	オフ

キャンセル

[リアルタイムシールド]

推奨デフォルト設定		
セクション	設定	ライブ
基本設定	リアルタイム シールド有効	オン
スキャンのスケジュール	セキュアエニウェアの中央データベースに基づくオフライン保護を有効にする	オン
スキャン設定	ブロックされたファイルに対するアクションを記憶する	オン
自己保護	ブロックされたファイルを自動的に隔離する	オン
ヒューリスティック	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	オン
リアルタイム シールド	書き込みまたは変更時にファイルをスキャンする	オン
動作シールド	ログインしているユーザーがない場合に自動的に脅威をブロックする	オン
コア システム シールド	リアルタイム イベントの警告を表示する	オフ
Web 脅威シールド	リアルタイム ブロック モードの警告を表示する	オフ
ID シールド	リアルタイム ブロックのお知らせを表示する	オフ
ファイアウォール		
ユーザー インターフェース		
システム クリーナ		

キャンセル

[リアルタイムブロックモードの警告を表示する]をオンにした場合、マルウェアの検出時に以下のダイアログが表示され、ユーザーが該当ファイルをブロックするかどうかを指定できます。この設定がオフの場合、プログラムは自動的にブロックされます。



※ 管理対象外ポリシーではこの設定は常にオンになります。

[動作シールド]

推奨デフォルト設定		
セクション	設定	ライブ
基本設定	動作シールド有効	オン
スキャンのスケジュール	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	オン
スキャン設定	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	オン
自己保護	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	オン
ヒューリスティック	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	オフ
リアルタイム シールド	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...	オン
動作シールド		
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 クリーナ		

キャンセル

[コアシステムシールド]

推奨デフォルト設定		
セクション	設定	ライブ
基本設定	コア システム シールド有効	オン
スキャンのスケジュール	システム変更を実行する前にシステム変更を評価する	オン
スキャン設定	破損したシステムコンポーネントを検出して修復する	オン
自己保護	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	オン
ヒューリスティック	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	オン
リアルタイム シールド	LSP チェーンと他のシステム構造の整合性を検証する	オン
動作シールド	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	オフ
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 クリーナ		

キャンセル

[Web 脅威シールド]

推奨デフォルト設定		
セクション	設定	ライブ
基本設定	Web 脅威シールド有効	オン
スキャンのスケジュール	検索エンジンの結果を分析し、アクセスする前に悪質な Web サイトを識別する	オン
スキャン設定	新しくインストールされたブラウザを自動的に保護	オン
自己保護	アクセスする前に Web サイト上に悪意のあるソフトウェアがないか調べる	オン
ヒューリスティック	アクセスする前に Web サイトコンテンツ内にエクスプロイトがないか調べる	オン
リアルタイム シールド	ユーザーがローカルに Web 脅威シールドをオーバーライドする機能を無効にする	オン
動作シールド	新規ブラウザがインストールされた際、ブラウザのアドオンを自動的にインストール	オン
コア システム シールド	Web フィルタリング ドライバのみインストール (Web フィルタリング ブラウザのア...	オフ
Web 脅威シールド		
ID シールド		
ファイアウォール		
ユーザー インターフェース		
システム クリーナ		

キャンセル

[ユーザーがローカルに Web 脅威シールドをオーバーライドする機能を無効にする]が[オン]の場合、ユーザーが Web 脅威シールドが脅威とみなしたサイトにアクセスすることはできなくなります。

[ID シールド]

推奨デフォルト設定		
セクション	設定	ライブ
基本設定	ID シールド有効	オン
スキャンのスケジュール	オンライン上の個人情報に対する脅威を探す	オン
スキャン設定	フィッシングの脅威がないか Web サイトを分析する	オン
自己保護	アクセス時に Web サイトを検証して正当性を判別する	オン
ヒューリスティック	Web サイトの DNS/IP 解決を検証して中間者攻撃を検出する	オン
リアルタイム シールド	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	オン
動作シールド	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	オン
コア システム シールド	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...	オフ
Web 脅威シールド	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...	オン
ID シールド	ID シールド対応モードを有効にする	オフ
ファイアウォール	非ラテン語のシステム上でキーロギング保護機能を有効にする	オフ
ユーザー インターフェース		
システム クリーナ		

キャンセル

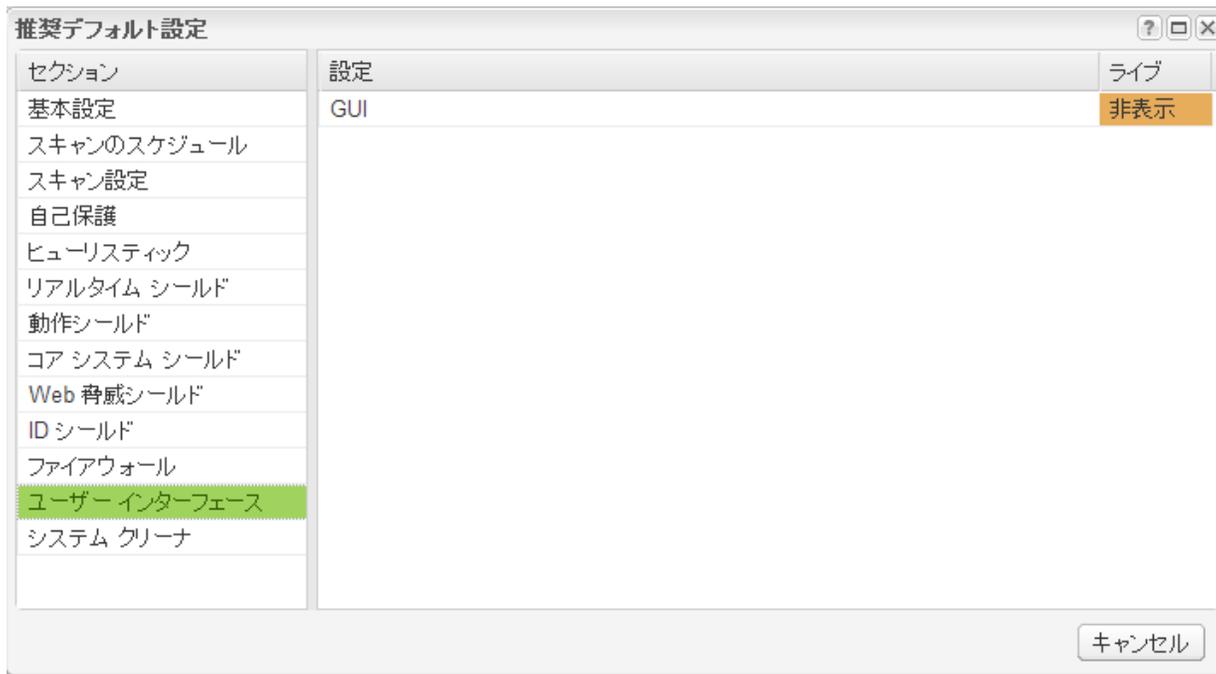
[ファイアウォール]



ファイアウォールレベル

- デフォルトで許可(すべてのプロセスがインターネット接続するのを許可)
- 不明および感染している場合に警告(感染時、未知のプロセスがインターネット接続するのを防止)
- 不明の場合に警告(未知のプロセスがインターネット接続するのを防止)
- デフォルトでブロック(明示的に許可しない限りインターネット接続させない)

[ユーザーインターフェース]



エンドポイントにおいてセキュアエニウェアのメイン画面を表示させるかどうかを設定します。

[システムクリーナ]



ゴミ箱やキャッシュなど、不要なファイルをスケジュールに従いクリーンアップします。

あらかじめ用意されているポリシー

システムにはあらかじめ以下のポリシーが用意されています。

- サイレント監査

システムトレイやスタートメニューにも表示されず、バックグラウンドでスキャンとシールドが動きますが、脅威を検出しても何もしません。検出した脅威に関してはコンソール上に表示されますので、コンソールからコマンドを発行して駆除を行います。

シールドにおいても脅威のブロックを行わないので、他の AV 製品と組み合わせて WSA の有効性を検証するような場合や、ユーザーの作業への介入を極力抑えて必要な対応は管理者からのコマンドで対処したい場合に有効です。

- 推奨デフォルト設定

一般的な環境に推奨されるポリシー設定です。本資料上記ポリシー設定のスクリーンショットは推奨されるデフォルト設定から採取したものです。

- 管理対象外

現在エンドポイントに設定されているセキュリティポリシーを、エンドポイント側で編集できるようにするためのポリシーです。

- 推奨サーバーデフォルト設定

サーバーOS で最適に動作するよう設定されているポリシーです。

ポリシーの編集

システムに最初から用意されている[サイレント監査]、[推奨されるデフォルト設定]、[管理対象外]、[推奨サーバーデフォルト設定]以外のポリシーはダブルクリックすることで編集することができます。

編集する場合は[下書き]をクリックして表示された値を選択します。



下書きに設定した値を保存するには[変更を保存]をクリックします。取り消すには[変更をリセット]をクリックします。

保存した下書きを実際のポリシーに反映するには[下書きの変更をライブに昇格]をクリックします。



昇格するまでは[下書きの変更]に[はい]が表示されます。

ポリシー名	ポリシーの説明	作成日	下書きの変更
#営業部門ポリシー	GU非表示/未知なアプリ実行不可	2012/02/05 15:38	いいえ
#開発部門ポリシー	GU表示可	2012/06/16 15:35	いいえ
demo テストポリシー	テストのためのポリシー	2012/06/19 00:17	はい

使用するグループとエンドポイント

選択されたポリシーを適用しているグループの一覧が表示されます。

① 使用するグループとエンドポイント #開発部門ポリシー

変更を保存 | 変更を取り消す | 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 | 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

グループ名	エンドポイントの数	説明
開発部門	2 表示	

グループ名をダブルクリックすることで、該当エンドポイントを移動するグループを指定できます。

グループ名	エンドポイントの数
営業部門	1 表示
営業部門	1 表示

新たなグループを指定して[変更を保存]をクリックすると該当エンドポイントが新しいグループに移動されます。[変更を取り消す]をクリックすると変更したグループが元のグループに戻ります。

[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]をクリックすることで、該当ポリシーが適用されているすべてのエンドポイントに別なポリシーを適用できます。

すべてのエンドポイントを別のポリシーに移動

ポリシー:

保存 キャンセル

[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]をクリックすることで、該当ポリシーが適用されているすべてのエンドポイントを一覧表示できます。

次を使用するすべてのエンドポイント: (ポリシー: #開発部門ポリシー, グループ: 開発部門)

	ホスト名	グループ	状態	最近の観測
1	TMURATA-503DD9C-9919A...	開発部門	✔ 保護	2012/06/17 03:36
2	TMURATA-D600	開発部門	✔ 保護	2012/06/19 02:24

グループの管理

管理対象のエンドポイントを任意のグループに分けることができます。

The screenshot shows the Webroot SecureAnywhere management interface. The main content area displays a table of endpoints for the selected group 'TAKI検証用G'.

ホスト名	ポリシー	状態	初回確認日時	最...	エージェント...	デバイス MID	インスタンス MID
1: NAKATA-VM-1	管理対象外	期	2012/07/05 1...	201...	8.0.1.233	79AEFDC2DB8FE2AF480...	33118c080bbdab934d5e0084fa2ef8bd...
2: TAKI-VM-2	デモポリシー(中村)	保護	2012/07/10 2...	201...	8.0.2.155	2C0FF5DC0C0349CA50E8...	3d20bd4cd275b5e5b988e05ac9430...

Below the table, the policies applied to the group are listed:

ポリシー名	このポリシーを使用するエンドポイント	ポリシーの説明
デモポリシー(中村)	1	test
管理対象外	1	ユーザーが管理するすべての PC で、このポリシーを使用します

[作成]をクリックすることで新しいグループを作成できます。

グループを作成

グループ名:

説明:

グループを選択し[削除]をクリックすることで、該当グループを削除することができます。[削除]をクリック後確認画面が表示されるので、削除する場合には[はい]をクリックします。

グループを削除しますか?

削除しますか "#検証用"?

※ システムに最初から用意されている[すべてのエンドポイント]、[デフォルトのグループ]、[非アクティブ化されたエンドポイント]を削除することはできません。

グループを選択し[名前の変更]をクリックすることで、該当グループ名を変更することができます。[名前の変更]をクリック後確認変更画面が表示されるので、新しい名前を入力して[グループ名を変更]をクリックします。

グループ名を変更

グループ名:

説明:

※ システムに最初から用意されている[すべてのエンドポイント]、[デフォルトのグループ]、[非アクティブ化されたエンドポイント]は名前を変更できません。

エンドポイント一覧

グループペインでグループを選択することで、エンドポイントペインにグループに該当するエンドポイントの一覧を表示することができます。

エンドポイントの場所: 開発部門

変更を保存 | 変更を取り消す | エンドポイントを別のグループに移動 | ポリシーをエンドポイントに適用 | エージェント コマンド ▾ | >>

	<input type="checkbox"/> ホスト名	ポリシー	状態	最近の観測	最近の感染	エージェント...
1	<input type="checkbox"/> TMURATA-503DD9C-9919A232	#開発部門ボ...	✔ 保護	2012/06/17 03:36		8.0.1.193
2	<input type="checkbox"/> TMURATA-D600	#開発部門ボ...	✔ 保護	2012/06/19 02:40		8.0.1.193

同時に[使用されているポリシー一覧]に該当グループが使用しているポリシーの一覧が表示されます。

ポリシーの使用場所: 開発部門

変更を保存 | 変更を取り消す

ポリシー名	このポリシーを使用するエンドポイント	ポリシーの説明
管理対象外	1	ユーザーが管理するすべての PC で、このポリ...
#開発部門ポリシー	1	GUI表示可

エンドポイント一覧のカラムをマウスでホバーして表示される▼をクリックすることでソート順や表示するカラムを設定することができます。

- プラットフォーム
- 現在のユーザー
- ポリシー
- グループ
- 状態
- 初回確認日時
- 最終確認日時
- 最近の感染
- エージェントのバージョン
- キーコード
- Windows OS
- デバイス MID
- インスタンス MID
- VM
- エージェントの言語
- IP アドレス
- ローカル IP アドレス
- MAC アドレス
- Active Directory - ドメイン
- Active Directory OU
- Workgroup

エンドポイント一覧で[ホスト名]もしくは[ポリシー]をダブルクリックすることで[ホスト名]もしくは[ポリシー]を変更することができます。変更された内容を保存するには[変更を保存]をクリックします。変更された内容を元に戻すには[変更を取り消す]をクリックします。

エンドポイントを選択して[エンドポイントを別のグループに移動]をクリックすることで、該当エンドポイントを別なグループに移動できます。

エンドポイントをどのグループに移動しますか？

グループ:

エンドポイントを選択して[ポリシーをエンドポイントに適用]をクリックすることで、グループに適用されているポリシーとは別なポリシーを該当エンドポイントに設定することができます。

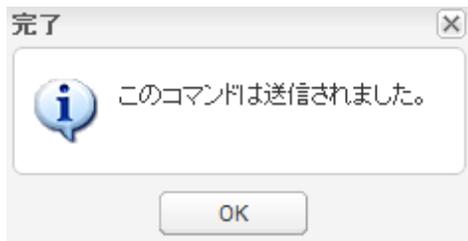
ポリシーを適用

ポリシー:

コマンド

ユーザーに設定されているアクセス権限に応じて、エンドポイントを選択してコマンドを実行することができます。アクセス権限の設定と実行可能なコマンドの関係は「[管理者のアクセス権](#)」を参照してください。

コマンドを発行するには対象のエンドポイントを選択(複数選択可)し、[エージェントコマンド]をクリックします。コンソールから発行されたコマンドはすぐにエンドポイントで実行されるのではなく、次のエージェントのポーリングタイミングでコンソールから取得されエンドポイントで実行されます。それまでコマンドはコンソールにキューイングされます。正しくキューに格納された場合、以下のメッセージが表示されます。



※「送信されました」と表示されますが、内部的にはキューイングされた状況なので、次回エージェントがポーリングするまでは受信されませんので注意してください。

特定のエンドポイントに発行されたコマンドの状況は[エージェントコマンド]⇒[選択したエンドポイントのコマンドを表示]を実行して確認できます。

最近処理済みまたは未処理のコマンド							
	ホスト名	コマンド	パラメータ	リクエストされた日	終了日	開始日	状態
1	VM2-DEMO-TAKI	再起動		2013/07/19 14:28	2013/07/2...	2013/07/1...	実行済み
2	VM2-DEMO-TAKI	リセット		2013/09/03 15:00	2013/09/0...	2013/09/0...	実行済み
3	VM2-DEMO-TAKI	リセット		2013/09/03 14:39	2013/09/0...	2013/09/0...	実行済み
4	VM2-DEMO-TAKI	リセット		2013/09/02 17:42	2013/09/0...	2013/09/0...	実行済み
5	VM2-DEMO-TAKI	リセット		2013/09/02 17:39	2013/09/0...	2013/09/0...	実行済み
6	VM2-DEMO-TAKI	リセット		2013/09/02 17:28	2013/09/0...	2013/09/0...	実行済み
7	VM2-DEMO-TAKI	リセット		2013/09/02 17:18	2013/09/0...	2013/09/0...	実行済み
8	VM2-DEMO-TAKI	キーコードを変更	SAA9TESTB6A79D8A52E6	2013/09/20 17:17	2013/09/2...	2013/09/2...	実行済み
9	VM2-DEMO-TAKI	キーコードを変更	SAE6TESTD3DA25C9E8BF	2013/08/28 17:04	2013/08/3...	2013/08/2...	実行済み
10	VM2-DEMO-TAKI	アンインストール		2013/10/24 16:50	2013/10/2...	2013/10/2...	実行済み

コマンドを送信後、エージェントからのポーリング間隔により、コマンドはエンドポイントに受信されます。

[エージェント]

- スキャン



コマンドから実行されるスキャンはクイックスキャンとなります。

- スキャン時間を変更



- フォルダをスキャン



フォルダスキャンは[カスタム／右クリックスキャン]となります。

- クリーンアップ



クイックスキャンにより脅威を隔離します。

- システムクリーナ



- アンインストール



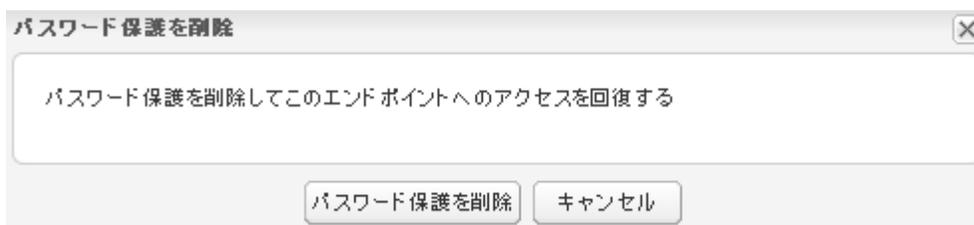
アンインストールを行っても非アクティブ化はされません。

- リセット



エンドポイントに管理ポリシーを設定しなおします。エンドポイントの VM をロールバックするなどしてコンソールの設定と異なるポリシー設定になった場合などに有効です。

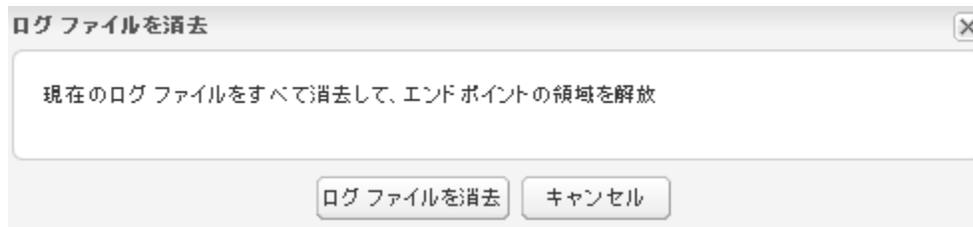
- パスワード保護を解除



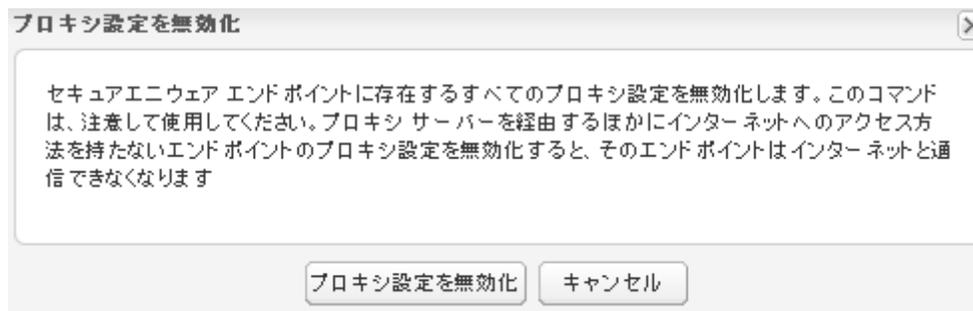
管理対象外のエンドポイントのアクセス制御に設定されているパスワードが分からなくなった場合に使用します。

[データを消去]

- ログファイルを消去



- プロキシ設定を無効化



エージェントに設定されているプロキシ設定を無効にします。このコマンドを誤って発行するとエージェントがコンソールに接続できなくなるので注意が必要です。

[キーコード]

- キーコードを変更

キーコードを変更

このエンドポイントに別のキーコードを指定します。たとえば、会社での変更によって新しいキーコードを使用しなければならない場合などに、別のキーコードを使用する必要があります

キーコード:

キーコードを変更 キャンセル

- キーコードを一時的に変更

キーコードを一時的に変更

ドロップダウン リストからキーコードを選択し、セキュアエニウェアで使用する日付を指定します。このオプションは、一時的なキーコードを使用してテストのために特別な機能を有効にする場合などに使用できます。

キーコード:

指定した期間内にコマンドを実行

開始時間:

終了時間:

キーコードを変更 キャンセル

[電源 & ユーザーアクセス]

- エンドポイントのロック

エンドポイントのロック ✕

このエンドポイントをロックする

エンドポイントのロック キャンセル

エンドポイントの画面をロックします。解除するにはログオン中のユーザーパスワードが必要です。

- ログオフ

ログオフ ✕

現在のアカウントからユーザーをログオフします

ログオフ キャンセル

- 再起動

再起動 ✕

レポートが生成された時にこのエンドポイントを再起動します

再起動 キャンセル

- [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。

[セーフモードとネットワーク]で再起動する キャンセル

- シャットダウン

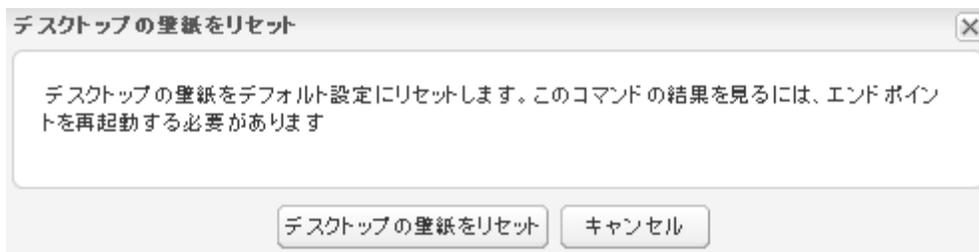
シャットダウン ✕

レポートが生成された時に、このエンドポイントをシャットダウンします。

シャットダウン キャンセル

[マルウェア対策ツール]

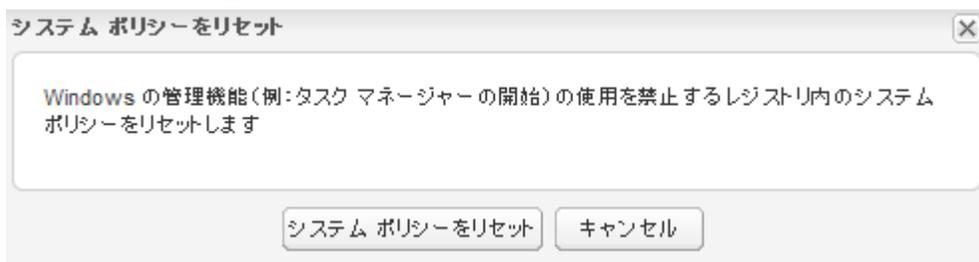
- デスクトップの壁紙をリセット



- スクリーンセーバーをリセット



- システムポリシーをリセット

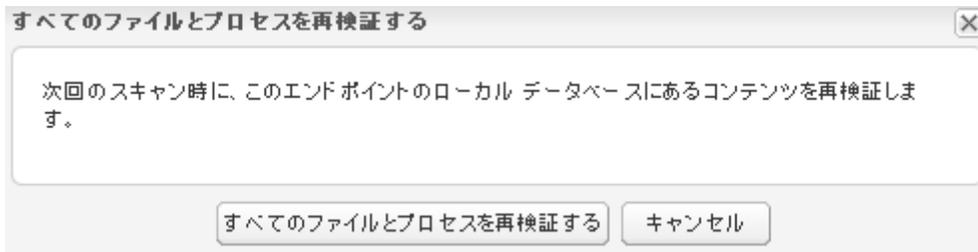


- ファイルを復元



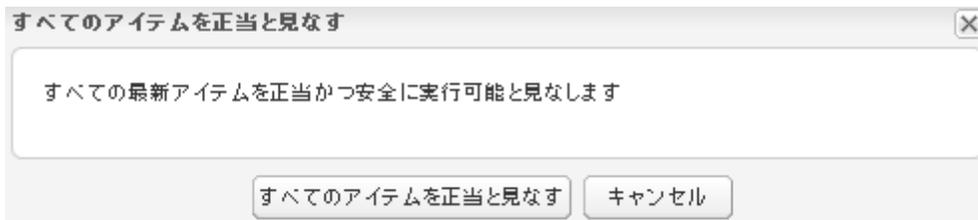
[ファイル&プロセス]

- すべてのファイルとプロセスを再検証する



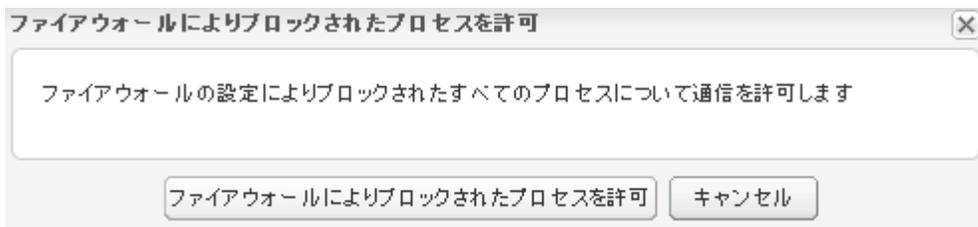
ローカルにキャッシュされているクラウドの判定結果を再検証します。

- すべてのアイテムを正当と見なす

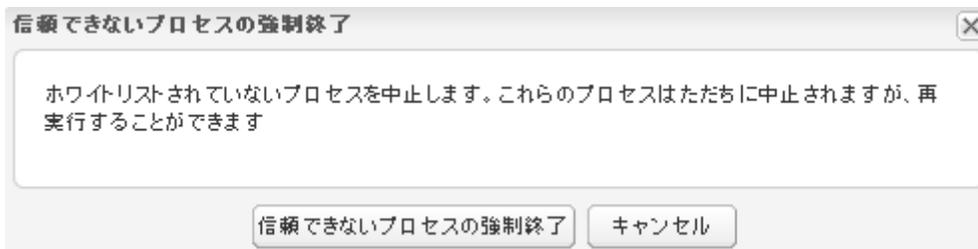


エンドポイントで現在実行中のプロセスを正当なプログラムと見なします。設定はローカル上に保存されます。

- 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



- 信頼できないプロセスの強制終了



[IDシールド]

- アプリケーションを許可

アプリケーションを許可

許可するアプリケーションの MDS を入力します

MDS:

送信 キャンセル

- アプリケーションを拒否

アプリケーションを拒否

拒否するアプリケーションの MDS を入力します

MDS:

送信 キャンセル

- 拒否されているすべてのアプリケーションを許可

拒否されているすべてのアプリケーションを許可

「拒否」と設定されているアプリケーションを「許可」に変更します。

拒否されているすべてのアプリケーションを許可 キャンセル

- アプリケーションを保護

アプリケーションを保護

保護するアプリケーションの MDS を入力します

MDS:

送信 キャンセル

- アプリケーションの保護を解除

アプリケーションの保護を解除

保護を解除するアプリケーションの MDS を入力します

MDS:

送信 キャンセル

[アドバンス]

- カスタマーサポートスクリプトを実行

クリーンアップ スクリプトを実行

カスタマーサポートから提供されたクリーンアップ用スクリプトを実行します

クリーンアップ スクリプト:

- カスタマーサポートの診断

カスタマーサポートの診断

カスタマーサポートの診断

URL:

電子メールアドレス:

詳細設定(オプション)

- ファイルをダウンロードして実行

ファイルをダウンロードして実行

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

URL:

コマンドライン オプション(オプション):

- DOS コマンドを実行

DOS コマンドを実行

実行する DOS コマンドを指定します。このコマンドは、コマンドレベルでの変更をリモートで実行する必要がある場合に便利です。

DOS コマンド:

- レジストリコマンドを実行

レジストリコマンドを実行

実行するレジストリコマンドを指定します。注意:このコマンドは `reg.exe` と同じ構文を使用しますが、`reg.exe` は呼び出しません。ローカルの レジストリ ハイブのパス(HKLM\ Software\ など)を直接参照することのみ可能で、コンピュータ名をパスに含めることはできません。

レジストリコマンド:

レジストリコマンドを実行 キャンセル

スキャン履歴

エンドポイント一覧からエンドポイントを選択することで、該当エンドポイントの[スキャン履歴]を表示することができます。

次のスキャン履歴: TMURATA-503DD9C

このエンドポイントで発見されたすべての脅威を表示

	スキャン開始	状態	スキャンの種類	エリア	IP アドレス	およそのスキャン時間
1	2012/06/18 10:50	⚠ 脅威が検出され...	ディープ スキャン	●	183.73.131.50	18 秒
2	2012/06/18 04:27	✔ 消去	クイックスキャン	●	210.2.217.194	5 秒

スキャン履歴一覧では以下のカラムを設定できます。

- 状態
- スキャンの種類
- エリア
- IP アドレス
- およそのスキャン時間
- Windows フル OS
- ローカル IP アドレス
- MAC アドレス
- Active Directory - ドメイン
- Active Directory OU
- Workgroup
- 現在のユーザー

脅威が検出されたスキャンをクリックすると検出された脅威の詳細を表示することができます。

脅威が検出されました

オーバーライドを作成

	<input type="checkbox"/> ファイル名	パス名	ファイルサイズ	マルウェア グループ	
1	<input type="checkbox"/>	TROJAN.PROXY.WIN32.G...	%temp%\testvirus.zip E38...	17,920	W32.Trojan.Mitglieder

脅威の詳細では以下のカラムを設定できます。

- パス名
- ファイルサイズ
- マルウェア グループ
- 最終確認日時
- 初回確認日時
- ベンダー
- 製品
- バージョン
- クラウド判定
- MD5

非アクティブ化

選択したエンドポイントを非アクティブな状態にし、キーコードを 1 つ解放します。

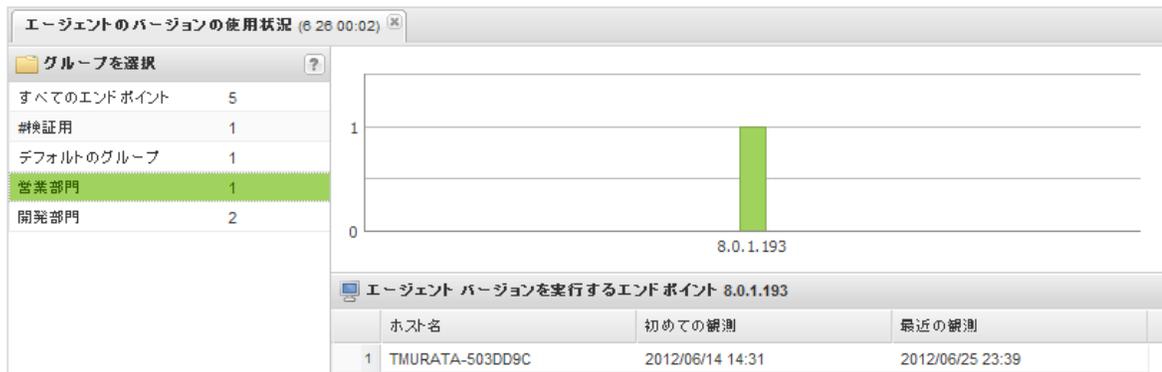
レポート

管理対象のエンドポイントに関するレポートを生成することができます。

インストールされたエージェント



エージェントのバージョンの使用状況



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

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 (6 26 00:07) [X]

未判定のソフトウェアが検出されたエンドポイント [?] [?]

	ホスト名	エージェントのバ...	OS	システムの種類	サービスパック	エリア	IPアドレス
1	???XP???-2D9EC769	8.0.1.193	WinXP	32ビット	3	●	210.2.217.194
2	TMURATA-503DD9C	8.0.1.193	WinXP	32ビット	3	●	210.2.217.194
3	TMURATA-503DD9C-2D9EC769	8.0.1.193	WinXP	32ビット	3	●	210.2.217.194
4	TMURATA-503DD9C-9919A232	8.0.1.193	WinXP	32ビット	3	●	210.2.217.194
5	TMURATA-D600	8.0.0.40	WinXP	32ビット	3	●	219.113.27.14

このエンドポイントで発見されたすべての未判定のソフトウェア [?]

オーバーライドを作成

	ファイル名	パス名	ファイルサイズ	最近の観測
1	HELLOC.EXE	%desktop%	52,775	2012/06/25 21:12
2	VICTIM.EXE	%temp%\vmwarendnd\9a2bd0e3\	52,775	2012/06/25 21:12

最新のスキャンで脅威が検出されたエンドポイント

最新のスキャンで脅威が検出されたエンドポイント (6/28 00:31)					
脅威が存在するエンドポイント					
	ホスト名	ポリシー	エージェントのバージョン	エリア	
1	TMURATA-503DD9C	#営業部門ポリシー 表示	8.0.1.193	日本	

このエンドポイントで発見された脅威					
オーバーライドを作成					
	ファイル名	パス名	マルウェアグループ	初めての観測	最近の観測
1	TROJAN.PROXY.WIN32.G...	%temp%\testvirus.zip E38...	W32.Trojan.Mitglieder	2012/06/17 05:11	2012/06/26 00:19

発見されたすべての未判定のソフトウェア

発見されたすべての未判定のソフトウェア (6/28 00:20)					
すべての未判定のソフトウェア					
オーバーライドを作成					
	ファイル名	パス名	ファイルサイズ	最近の観測	ホスト名
1	VICTIM.EXE	%desktop%	52,775	2012/06/25 23:11	TMURATA-503DD9C
2	HELLOC.EXE	%desktop%	52,775	2012/06/25 21:12	TMURATA-503DD9C
3	VICTIM.EXE	%temp%\vmwarend19a2...	52,775	2012/06/25 21:12	TMURATA-503DD9C
4	HELLOC.EXE	%desktop%	52,775	2012/06/25 21:12	TMURATA-503DD9C-2D9...
5	VICTIM.EXE	%desktop%	52,775	2012/06/25 21:12	TMURATA-503DD9C-2D9...
6	HELLOC.EXE	%desktop%	52,775	2012/06/25 21:12	TMURATA-503DD9C-991...
7	VICTIM.EXE	%desktop%	52,775	2012/06/25 21:12	TMURATA-503DD9C-991...
8	GUITRN.DLL	%windir%\system32\dlca...	132,096	2012/06/17 05:12	TMURATA-503DD9C
9	FXSOCM.DLL	%windir%\system32\dlca...	132,608	2012/06/17 05:12	TMURATA-503DD9C
10	WRENTMTWZRD.EXE	%programfiles%\wsadep...	1,398,192	2012/06/16 12:48	TMURATA-503DD9C-2D9...
11	WRENTMTWZRD.EXE	%programfiles%\wsadep...	1,398,192	2012/06/16 12:48	???XP???-2D9EC769

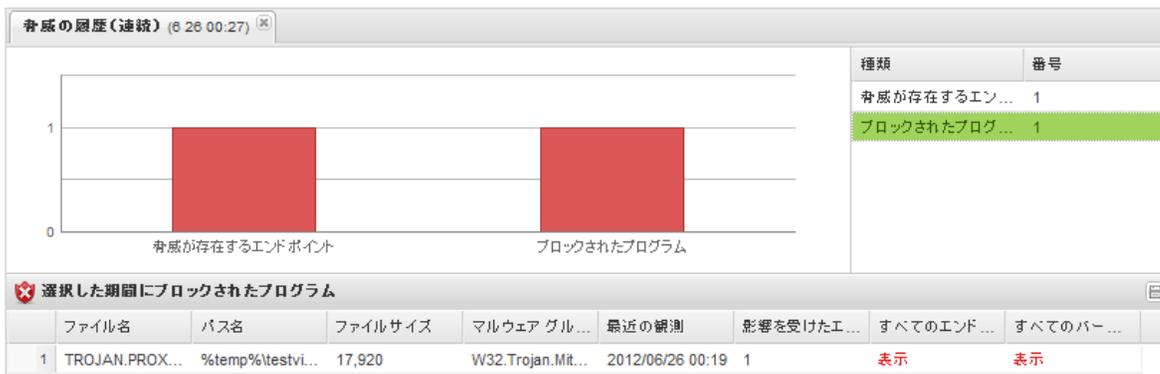
発見されたすべての脅威

発見されたすべての脅威 (6/26 00:21)					
発見されたすべての脅威					
オーバーライドを作成					
	ファイル名	パス名	ファイルサイズ	最近の観測	ホスト名
1	TROJAN.PROXY.WIN32.G...	%temp%\testvirus.zip E38...	17,920	2012/06/21 01:39	TMURATA-503DD9C

脅威の履歴(日単位)



脅威の履歴(内訳)



警告

警告通知メッセージをカスタマイズして設定することができます。

Webroot SecureAnywhereの警告管理画面のスクリーンショット。左側のメニューには「警告」が選択されています。中央には警告のリストが表示されており、右側には「配信先リスト」が設定されています。

警告の名前	警告のタイプ	配信先リスト	作成日	作成者	編集日	編集者	状態
感染に関する警告	感染が検出されました	感染リスト	2013/0...	nori@webroot...	2013/0...	taki.na...	アクティブ
ウェブライト システムメッセージ	システムメッセージ	システムメッセージ...	2013/0...	nori@webroot...	2013/0...	taki.na...	アクティブ
感染の概要	感染の概要	感染の概要リスト	2013/0...	a@webroot.com	2013/0...	taki.na...	アクティブ
インストールの概要	インストールの概要	インストールの概要...	2013/0...	nori@webroot...	2013/0...	hideka...	アクティブ
インストールに関する警告	エンドポイントがインストールされました	インストールのリスト	2013/0...	a@webroot.com	2013/0...	taki.na...	アクティブ

配信先リスト	電子メールアドレス
インストールのリスト	camura@we...
インストールの概要リ...	ss@vccorp.net
システムメッセージ...	zu.fujimori@...
感染の概要リスト	camura@we...
感染リスト	zu.fujimori@...

作成できる通知メッセージは以下の4つです。

- 感染通知
- インストール通知
- 感染通知
- 感染概要通知

警告通知を作成するには、作成をクリックし、4つのメッセージの中から選択し、名前を指定します。

警告の作成

ステップ 1: この警告に名前を付けた後、警告のタイプを選択します

警告のタイプ:

警告の名前:

キャンセル

- 感染が検出されました
- エンドポイントがインストールされました
- 感染の概要
- インストールの概要

警告の作成

ステップ 1: この警告に名前を付けた後、警告のタイプを選択します

警告のタイプ:

警告の名前:

キャンセル 戻る 次へ

警告メッセージを送信する宛先リストを新規で作成するか、既存の宛先リストを選択します。

警告の作成

ステップ 2: 既存の配信先リストを選択するか、またはこの警告を送信する電子メールのリストを新規に作成します

警告の受信者: 既存のリストを使用 新規リストの作成

配信先リストを選択:

キャンセル

- インストールのリスト
- システムメッセージリスト
- 感染の概要リスト
- 感染リスト

警告の作成

ステップ 2: 既存の配信先リストを選択するか、またはこの警告を送信する電子メールのリストを新規に作成します

警告の受信者: 既存のリストを使用 新規リストの作成

リストの名前:

電子メールアドレス(コンマで区切る、最大 10):

キャンセル 戻る 次へ

デフォルトのメッセージにデータを追加するには、右側のプルダウンより選択し追加します。

メッセージをカスタマイズする場合も、ここで編集してください。

警告の作成

ステップ 3: 電子メールの作成

電子メールの件名: 感染に関する警告[hostname][currentuser] データ入力 ▾

電子メールメッセージの本文: 1 件の感染がエンドポイントにより最近検出されました:
 ホスト名: [hostname]
 グループ名: [groupname]
 ポリシー名: [policyname]
 キーコード: [keycode]
 感染リスト:
 [infectionlist.filename,malwaregroup,pathname]

ホスト名
 グループ名
 ポリシー名
 キーコード
 現在のユーザー
 コンソール名

キャンセル 戻る プレビュー 終了

警告の作成

ステップ 3: 電子メールの作成

電子メールの件名: 感染に関する警告 データ入力 ▾

電子メールメッセージの本文: 1 件の感染が検出されました:
 ホスト名: [hostname]
 グループ名: [groupname]
 ポリシー名: [policyname]
 キーコード: [keycode]
 IP アドレス: [ip]
 ログインユーザー: [currentuser]

ホスト名
 グループ名
 ポリシー名
 初回確認日時
 最終確認日時
 最近の感染
 オペレーティング システム
 エージェントのバージョン
 IP アドレス
 MAC アドレス
 国コード
 キーコード
 現在のユーザー
 作業グループ
 アクティブなディレクトリ
 コンソール名
 感染リスト

✕ キャンセル ← 戻る

オーバーライド

未知のソフトウェアまたは検出された脅威に対してオーバーライドを作成し、判定を上書きすることができます。オーバーライドを作成するには、未知のソフトウェアもしくは検出された脅威の一覧から上書き対象を選択後、

 をクリックします。

オーバーライドをグローバルに適用すると、すべてのポリシーに有効な上書き設定になります。

オーバーライドを作成

判定:

このオーバーライドをグローバルに適用しますか?

保存 キャンセル

グローバルに適用しない場合には対象とするポリシーを選択します。

オーバーライドを作成

判定:

このオーバーライドをグローバルに適用しますか?

ポリシー:

保存 キャンセル

※ 判定には、ユーザーの権限に応じて[正当]もしくは[不正]が設定できます。

設定されているオーバーライドは、[オーバーライド]タブから確認できます。

オーバーライド						
+ 作成 - 削除 CSV にエクスポート						
	MD5	共通のファイル名	共通のパス名	手動判定	作成日	ポリシー
1	5626DA23E4618AF4...	HELLOC.EXE	%desktop%	正当	2012/06/26 00:42	#開発部門ポリシー

上書き設定する対象ファイルの MD5 が分かれば、[作成]ボタンをクリックして上書き設定を行うことも可能です。

オーバーライドを作成

MD5:

判定:

このオーバーライドをグローバルに適用しますか?

保存 キャンセル

オーバーライドで[不正]と指定されたファイルは、スキャン時に以下のように Win32.LocalInfect として検出されます。

スキャン結果: **1 脅威 検出**

削除	脅威	感染
<input checked="" type="checkbox"/>	victim.exe 場所 c:\documents and settings\administrator\デスクトップ	Win32.LocalInfect.2

ログ

変更ログ

ユーザーによる管理コンソールへのログインや、設定変更などの操作履歴を確認できます。

日付	イベントの種類	説明
2012/06/25 23:39	エンドポイント	a@webroot.com が次を移動: TMURATA-503DD9C (ポリシー: demo テストポリシー) 現在のグループ: 営業部門
2012/06/25 22:44	ポリシー	a@webroot.com が次を変更: demo テストポリシー
2012/06/25 22:44	ポリシー	a@webroot.com が次を変更: demo テストポリシー
2012/06/25 21:59	エンドポイント	a@webroot.com が次を移動: TMURATA-503DD9C (ポリシー: demo テストポリシー) 現在のグループ: 営業部門
2012/06/25 21:51	エンドポイント	a@webroot.com が次を移動: TMURATA-503DD9C (ポリシー: demo テストポリシー) 現在のグループ: 営業部門
2012/06/25 21:51	ポリシー	a@webroot.com が次を変更: demo テストポリシー
2012/06/25 21:51	ポリシー	a@webroot.com が次を変更: demo テストポリシー
2012/06/25 21:31	エンドポイント	a@webroot.com が次を移動: TMURATA-503DD9C (ポリシー: demo テストポリシー) 現在のグループ: 営業部門

ログに対して以下のフィルタをかけることができます。

- 日付
ログを参照する日付を指定することができます。
- イベント
操作の対象をグループ、エンドポイント、ポリシー、オーバーライド、ログオンから選択することができます。
- ユーザー
操作を行ったユーザーを選択することができます。
- グループ
操作対象のグループを選択することができます。
- ポリシー
操作対象のポリシーを選択することができます。

コマンドログ

発行されたエージェントコマンドの一覧を確認できます。

ホスト名	コマンド	パラメータ	リクエストされた日	状態
TMURATA-503DD9C	DOS コマンドを実行	dir	2012/06/25 23:43	実行済み
TMURATA-503DD9C	カスタマーサポートの診断	http://download.webroot.com/wsabl...	2012/06/25 23:38	実行済み
TMURATA-D600	カスタマーサポートの診断	http://download.webroot.com/wsabl...	2012/06/25 23:38	受信待ち
TMURATA-503DD9C-9919A232	カスタマーサポートの診断	http://download.webroot.com/wsabl...	2012/06/25 23:38	受信待ち
TMURATA-503DD9C	カスタマーサポートの診断	http://download.webroot.com/wsabl...	2012/06/25 23:22	実行済み
TMURATA-503DD9C	信頼できないプロセスの強制終了		2012/06/25 23:17	実行済み
TMURATA-503DD9C	信頼できないプロセスの強制終了		2012/06/25 23:17	実行済み
TMURATA-503DD9C	ファイアウォールによりブロックされた...		2012/06/25 23:14	実行済み
TMURATA-503DD9C	すべてのファイルとプロセスを再検証...		2012/06/25 23:11	実行済み