WEBROOT®

an opentext™ company

GSM 管理者ガイド

Copyright

GSM 管理者ガイド

目次

第 1 章: グローバル サイト マネージャー管理者ガイド

グローバル サイト マネージャー管理者ガイドを使用するには、次のトピックを参照してください。

コンソールの選択

最初にコンソールにサインインしたとき、次のサイト構成のうち 1 つを選択する必要があります。

- ビジネス用にデバイスを管理しており、すべてのデバイスと請求に使用するキーコードが 1 つである場合は、[ビジネス コンソール] を選択します。詳細については、「 *6{/u}{/color} ページの「ビジネス コンソールについて」*.

- 顧客用にデバイスを管理しており、各顧客のサイトに使用するキーコードと請求が別々である場合は、[マネージド サービス プロバイダー コンソール] を選択します。詳細については、「 *4{/u}{/color} ページの「マネージド サービス プロバイダー コンソールについて」*.


WEBROOT
改良を行いました。
今回の訪問のみ コンソールに移動する前に画面が何度か切り替わります。
お客様の組織に最も当てはまるものを選択してください：
法人向け
• ビジネスのデバイスを管理
• すべてのデバイスと請求に使えるひとつのキーコード
• グループ管理で複数のオフィス拠点をサポート
選択
マネージド サービスプロバイダー
• 顧客のデバイスを管理
• 顧客のサイトごとにキーコード設定、請求。
• 個々のサイト管理について顧客 / 拠点をサポート。
選択

マネージド サービス プロバイダー コンソールについて

マネージド サービス プロバイダー (MSP) コンソールはコンソールの以前のバージョンによく似ています。外観と使用感は変わらず、同じタスクを実行できます。これらのタスクは本管理者ガイドで説明されています。

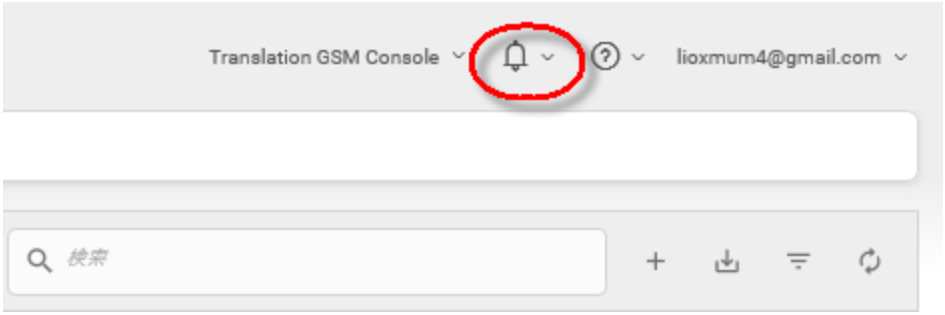
メインのコンソールから次のタブにアクセスできます。

- **ダッシュボード** - エンドポイントを視覚的に解釈するためのさまざまなグラフが表示されます。ここでは、チャートの作成や絞り込み、チャートの削除が可能です。
- **サイト** - すべてのサイトの一覧が、シート数、設定などとともに表示されます。[詳細] ドロップダウン メニューをクリックして、サイトに関する詳細を表示できます。詳細については、「*52{/u}{/color} ページの「管理コンソールの [サイト] タブ概要」*」を参照してください。
- **管理者** - 管理者のリストが表示されます。ここでは、各管理者のサイトごとの権限レベルに関する情報にアクセスすることができます。詳細については、「管理者の操作」セクションを参照してください。
- **グループ** - グループの追加、編集、削除、操作が可能です。
- **ポリシー** - ポリシーの作成、コピー、編集、名前変更が可能です。
- **オーバーライド** - オーバーライドの作成、カスタマイズ、インポートが可能です。
- **警告** - グローバル レベルで警告を作成できます。
- **レポート** - サイトの状態やパフォーマンスに関するレポートを実行できます。
- **設定** - アカウント情報の表示、API クライアント資格情報の作成、データ フィルタの設定が可能です。

- 追加情報については、右上の**はてなマーク (?)** アイコンから、**下向き矢印**をクリックして、次のいずれかにアクセスします。
  - ヘルプ ドキュメント - 多くの場合、操作中のパネルまたはウィンドウに関連してヘルプ情報が表示されます。
  - DNS ヘルプ ドキュメント - ビジネス ドキュメント ポータルを表示します。このポータルから DNS プロテクション ガイドにアクセスできます。

- ウェブルート教育ビデオ - ウェブルート ビデオのプレイリストを表示します。
- サービスの状態 - コンソールの状態ページを表示します。このページで、製品とシステムの状態を確認できます。
- スポットライト ツアー - スポットライト ツアーを表示します。これは、コンソール全体の簡単なツアーです。詳細については、「*9{/u}{/color} ページの「スポットライト ツアーについて」*」を参照してください。
- サポート - リンクをクリックしてヘルプ チケットを入力します。詳細については、「テクニカル サポートを受けるには」を参照してください。

- 警告または通知を確認するには、右上の警告ベル アイコンから、**下向き矢印**をクリックします。



ビジネス コンソールについて

ビジネス コンソールは、次の特徴を持つお客様のために作られました。

- ビジネスのためにデバイスを管理する。
- すべてのデバイスに単一のキーコードと課金制度がある。
- グループを管理することで複数のオフィスの場所をサポートしている。

ビジネス コンソールを選択した場合:

- ビジネスに関する情報を入力する必要があります。詳細については、「*491{/u}{/color} ページの「ビジネス コンソールの設定」*」を参照してください。
- スポットライト ツアーを見る機会が表示されます。このツアーは、オプトアウトして別の機会に見ることもできます。詳細については、「*9{/u}{/color} ページの「スポットライト ツアーについて」*」を参照してください。

ビジネス コンソールには標準コンソールとは異なるタブや機能があります。また、単一サイト ビジネスに特化しており、簡単にデバイスを管理できます。

次のタブと機能には、ビジネス コンソールからアクセスできます。

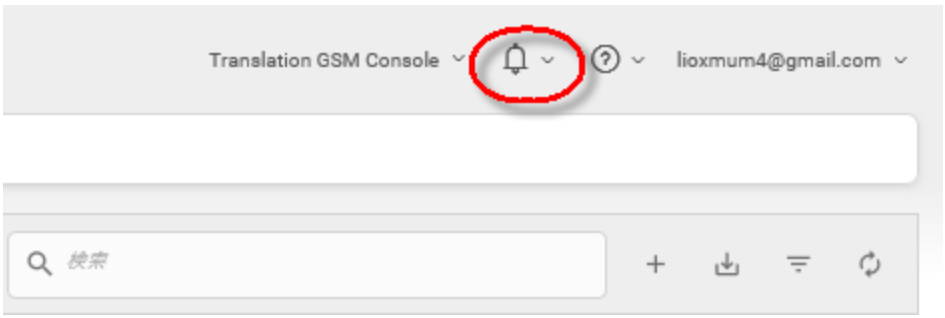
- **ダッシュボード** - エンドポイントを視覚的に解釈するためのさまざまなグラフが表示されます。ここから、エンドポイントの状態に関する情報を含むチャートを確認できます。詳細については、「[ビジネス ダッシュボード] タブ」を参照してください。さらに、DNS プロテクションまたはセキュリティ意識向上トレーニングのいずれかの無料体験版に登録できます。
- **管理者** - 管理者のリストが表示されます。ここでは、各管理者のサイトごとの権限レベルに関する情報にアクセスすることができます。詳細については、「管理者の操作」セクションを参照してください。
- **グループ** - グループの追加、編集、削除、操作が可能です。詳細については、「グループの操作」セクションを参照してください。
- **ポリシー** - ポリシーの作成、コピー、編集、名前変更が可能です。詳細については、「ポリシーの操作」セクションを参照してください。
- **オーバーライド** - オーバーライドの作成、カスタマイズ、インポートが可能です。詳細については、「オーバーライドの操作」セクションを参照してください。
- **警告** - グローバル レベルで警告を作成できます。詳細については、「警告の操作」セクションを参照してください。
- **レポート** - 製品の状態やパフォーマンスに関するレポートを実行できます。詳細については、「レポートの操作」セクションを参照してください。

- **設定** - アカウント情報と詳細設定を表示し、編集できます。詳細については、「*499{/u}{/color} ページの「企業情報の表示と編集」*」と「*501{/u}{/color} ページの「詳細設定の表示および編集」*」を参照してください。
- **DNS プロテクション** - セキュリティ意識向上トレーニングに関する情報を表示し、無料体験版に登録できます。詳細については、「*DNS Protection Trial*」を参照してください。
- **セキュリティ意識向上** - セキュリティ意識向上トレーニングに関する情報を表示し、無料体験版に登録できます。詳細については、「*Security Awareness Training Trial*」を参照してください。

- 追加情報については、右上のヘルプ (?) アイコンから、**下向き矢印**をクリックして、次のいずれかにアクセスします。
  - ヘルプドキュメント - 多くの場合、操作中のパネルまたはウィンドウに関連してヘルプ情報が表示されます。
  - DNS ヘルプドキュメント - ビジネスドキュメント ポータルを表示します。このポータルから DNS プロテクション ガイドにアクセスできます。
  - ウェブルート教育ビデオ - ウェブルート ビデオのプレイリストを表示します。
  - サービスの状態 - コンソールの状態ページを表示します。このページで、製品とシステムの状態を確認できます。
  - スポットライト ツアー - スポットライト ツアーを表示します。これは、コンソール全体の簡単なツアーです。詳細については、「*9{/u}{/color} ページの「スポットライト ツアーについて」*」を参照してください。
  - サポート - リンクをクリックしてヘルプ チケットを入力します。詳細については、「テクニカル サポートを受け

るには」を参照してください。

- 警告または通知を確認するには、右上の警告ベルアイコンから、**下向き矢印**をクリックします。



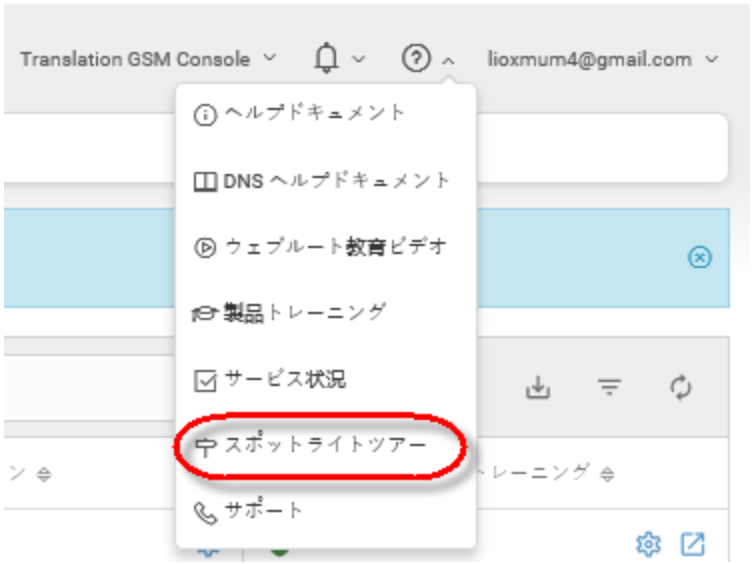
スポットライト ツアーについて

最初にアカウントを設定したときに、スポットライト ツアーが表示されます。ツアーには次に関する簡単な説明が含まれます。

- メイン メニューのタブ
- DNS プロテクションやセキュリティ意識向上トレーニングなどの追加セキュリティ レイヤー
- 必要に応じて、後程再度ツアーを表示できます。

スポットライト ツアーを見るには:

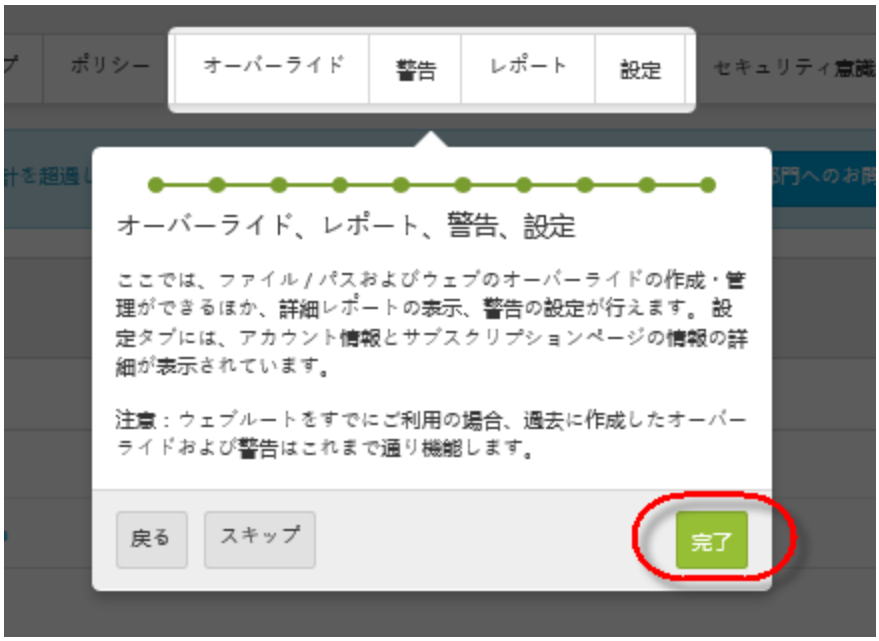
1. **ヘルプ (?)** ドロップダウン メニューから、[**スポットライト ツアー**] を選択します。



   ツアーの最初の画面が表示されます。

2. 必要に応じて、ツアーの視聴が完了するまで [**スキップ**] ボタンまたは [**次へ**] ボタンをクリックします。

3. ツアーの表示が完了したら、[**完了**] ボタンをクリックします。



必要に応じて、ヘルプ (?) ドロップダウン メニューから [スポットライト ツアー] を選択して、いつでもツアーを再度表示できます。

ファイアウォールを介したコミュニケーション

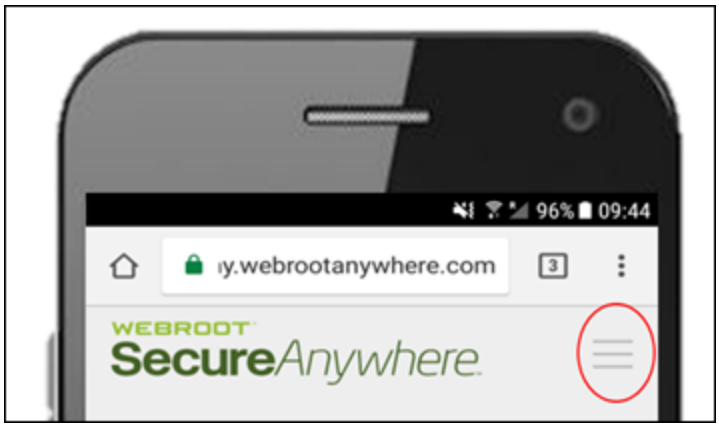
ファイアウォールがある場合、以下の表に記載されたウェブルートのパス マスクを許可してください。

パス	ポート	詳細
***.webrootcloudav.com**	ポート 443 (https)	エージェントのコミュニケーションとアップデート。 **注意:** 一部のファイアウォールはダブルドットを含むサブドメイン名と単一のワイルドカードマスクの使用に対応していません (例: 「g1.p4.webrootcloudav.com」を「*.webrootcloudav.com」で表示)。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。

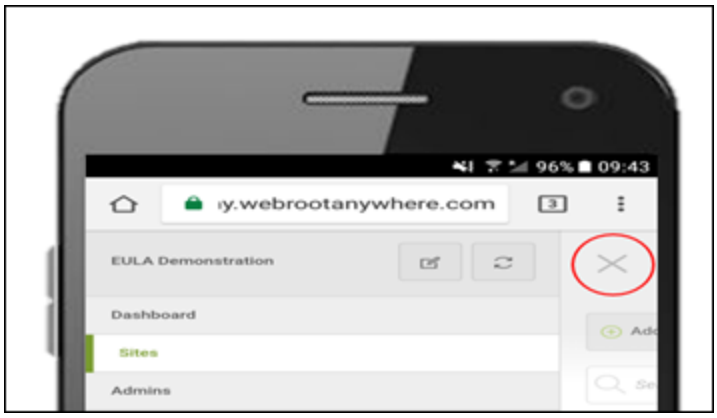
パス	ポート	詳細
https://wrskynet-eu.s3-eu-west-1.amazonaws.com/*	ポート 443 (https)	エージェントのファイルのダウンロードとアップロード。
https://wrskynet-oregon.s3-us-west-2.amazonaws.com/*	ポート 443 (https)	エージェントのファイルのダウンロードとアップロード。
WSAWebFilteringPortal.elasticbeanstalk.com	ポート 80 (http) & 443 (https)	エージェントの Web フィルタリングに必要。elasticbeanstalk は Amazon の AWS ドメインです。
***.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。

強化されたモバイル デバイス表示

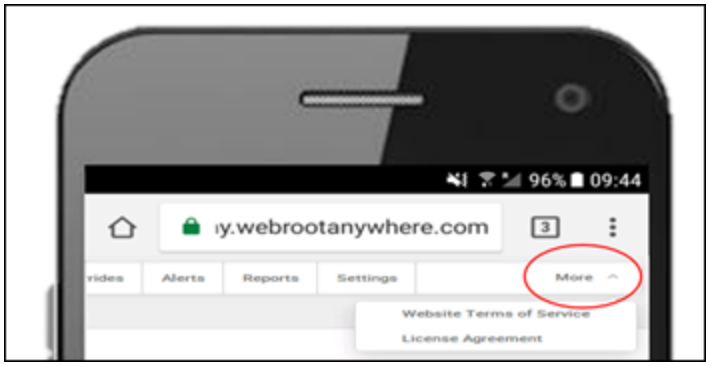
この管理コンソールでは、モバイル デバイスの表示機能が強化されています。モバイルや小型画面の解像度向けに、ナビゲーション バーを非表示にして、画面の右上にハンバーガー型のメニューを表示しました。



このアイコンをクリックするとナビゲーションが左からスライドします。[X] アイコンをクリックすると再度閉じます。



すべての画面において操作性が向上しました。ナビゲーション バーに収まらないナビゲーション アイテムはバーからなくなり、新しい [詳細] ドロップダウン メニューに収まりました。


96% 09:44
y.webrootanywhere.com
3
Alerts
Reports
Settings
More
Website Terms of Service
License Agreement

コンソールの変更

コンソールを切り替えるには、この手順に従います。

注意: このオプションは、複数のコンソールを作成した場合にのみ利用できます。

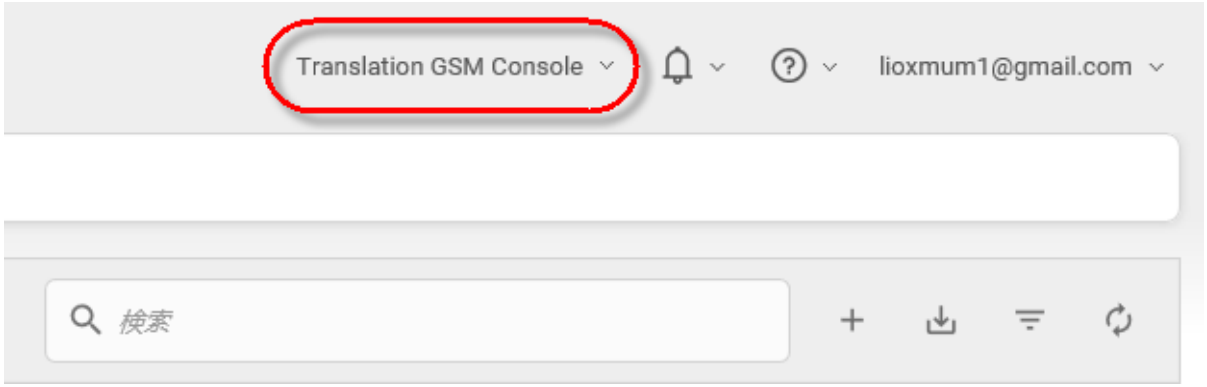
コンソールを変更するには:

1. 管理コンソールにログインします。

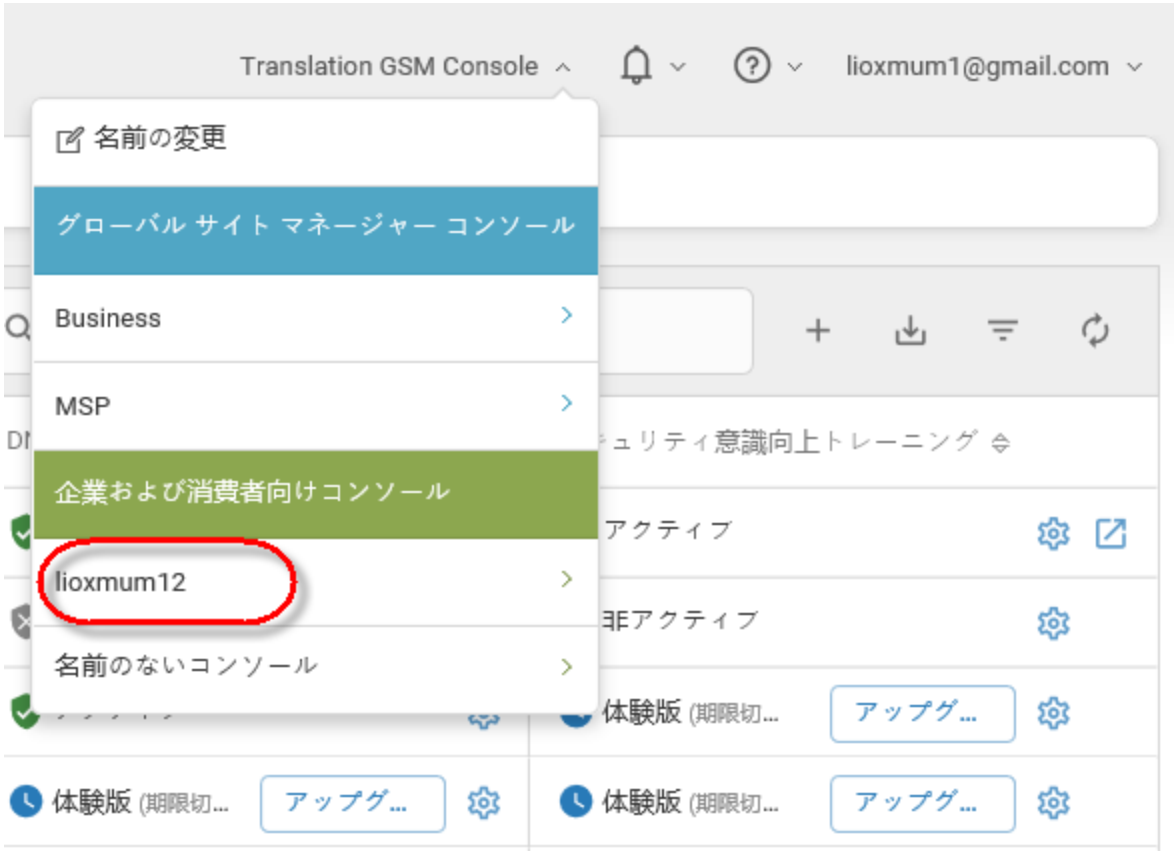
[コンソールの選択] 画面が表示されます。

2. コンソールを選択して開きます。

3. コンソールに入ったら、右上にあるコンソール名に移動して、コンソールを変更します。



4. ドロップダウン メニューから、切り替え先のコンソールの名前を選択します。



[サイト] タブがアクティブになった状態で、選択したコンソールに切り替わります。

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、この手順に従います。

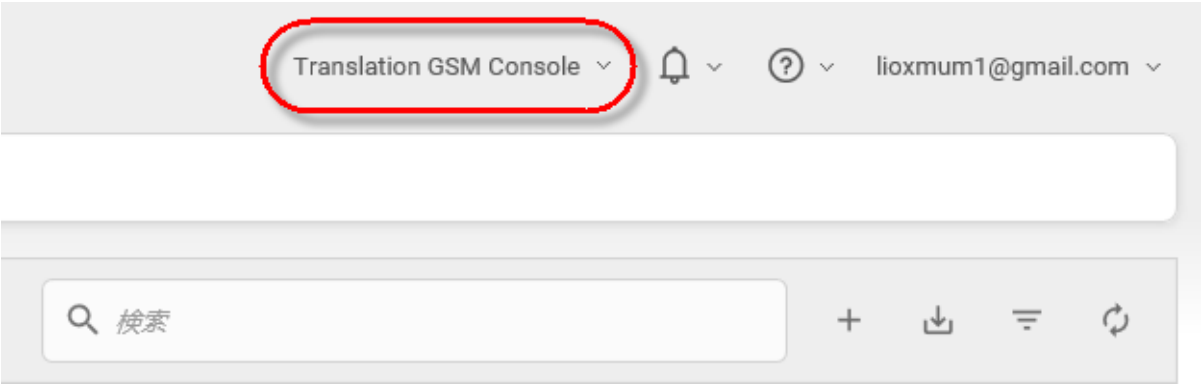
コンソールの名前を変更するには:

1. 管理コンソールにログインします。

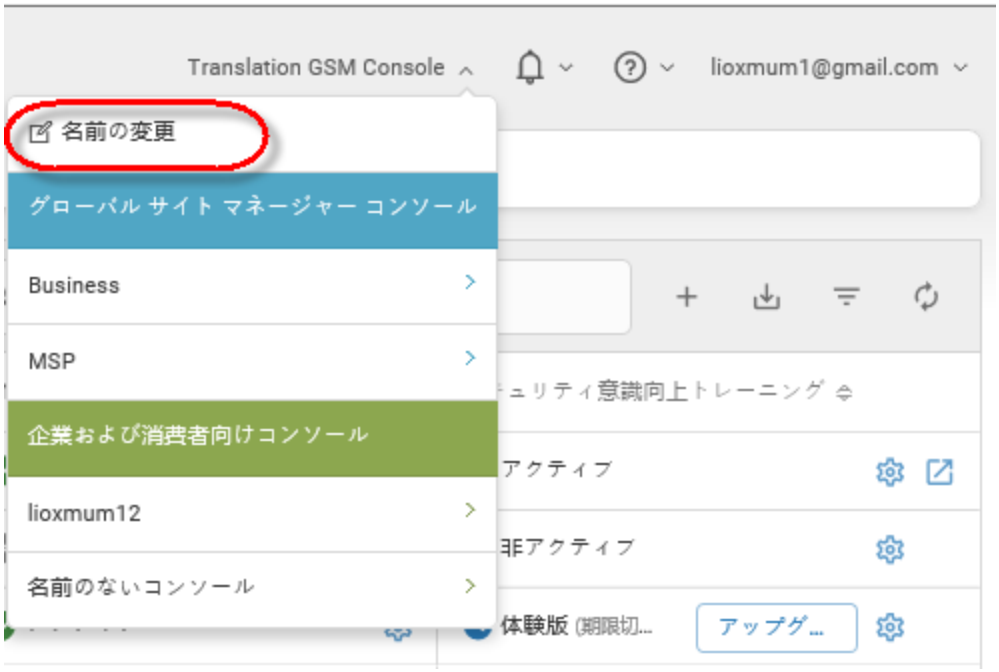
[コンソールの選択] 画面が表示されます。

2. コンソールを選択して開きます。

コンソールに入ったら、右上にあるコンソール名に移動して、コンソールを変更します。



3. ドロップダウン メニューから [**名前変更**] を選択します。



[コンソール名の変更] ウィンドウが表示されます。

4. [名前] フィールドにコンソールの新しい名前を入力します。

5. [**保存**] ボタンをクリックします。

これでコンソール名が変更されました。

エンドポイント コンソールへのアクセス

管理コンソールからエンドポイント コンソールに移動するには、次の手順に従ってください。

エンドポイント コンソールにアクセスするには:

1. 管理コンソールにログインします。

   管理コンソールが表示されます。

2. エンドポイント コンソールにアクセスするサイトの [**管理**] ボタンをクリックします。

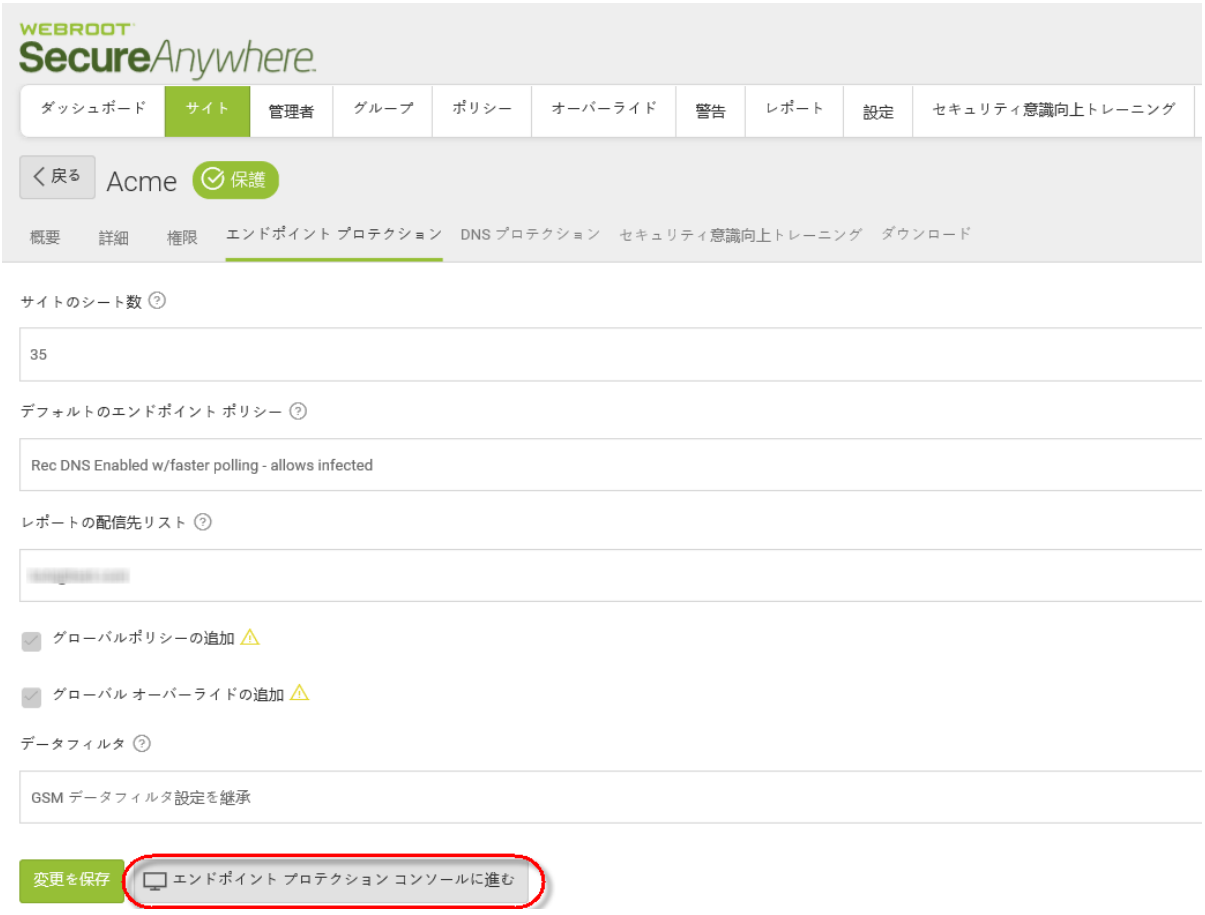
[概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

3. [**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] タブが表示されます。


WEBROOT
SecureAnywhere
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
戻る
Acme
保護
概要
詳細
権限
エンドポイント プロテクション
DNS プロテクション
セキュリティ意識向上トレーニング
ダウンロード
サイトのシート数
35
デフォルトのエンドポイント ポリシー
Rec DNS Enabled w/faster polling - allows infected
レポートの配信先リスト
bob@test.com
グローバルポリシーの追加
グローバル オーバーライドの追加
データフィルタ
GSM データフィルタ設定を継承
変更を保存
エンドポイント プロテクション コンソールに進む

4. ウィンドウ下部にある [**エンドポイント プロテクション コンソールに進む**] ボタンをクリックします。



閲覧していたサイトのエンドポイント プロテクション コンソールが表示されます。

5. 管理コンソールに戻るには、[**サイトへ戻る**] ボタンをクリックします。

グローバル サイト管理のシステム要件

システム要件は次の場所にあります。システム要件は次の場所にあります。サポート対象システムおよびブラウザ.

第 2 章: ダッシュボードの操作

ダッシュボードを操作するには、次のトピックを参照してください。

ダッシュボードのチャートの作成

この手順に従って、ダッシュボードのチャートを作成し、コンソールに追加します。

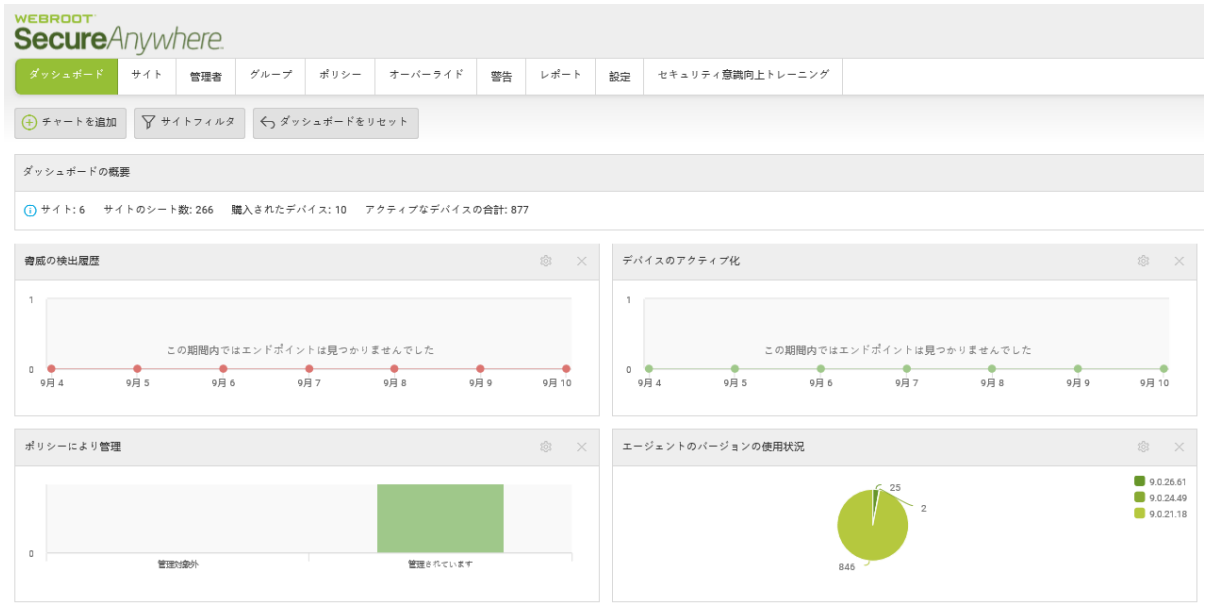
ダッシュボードのチャートを作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。

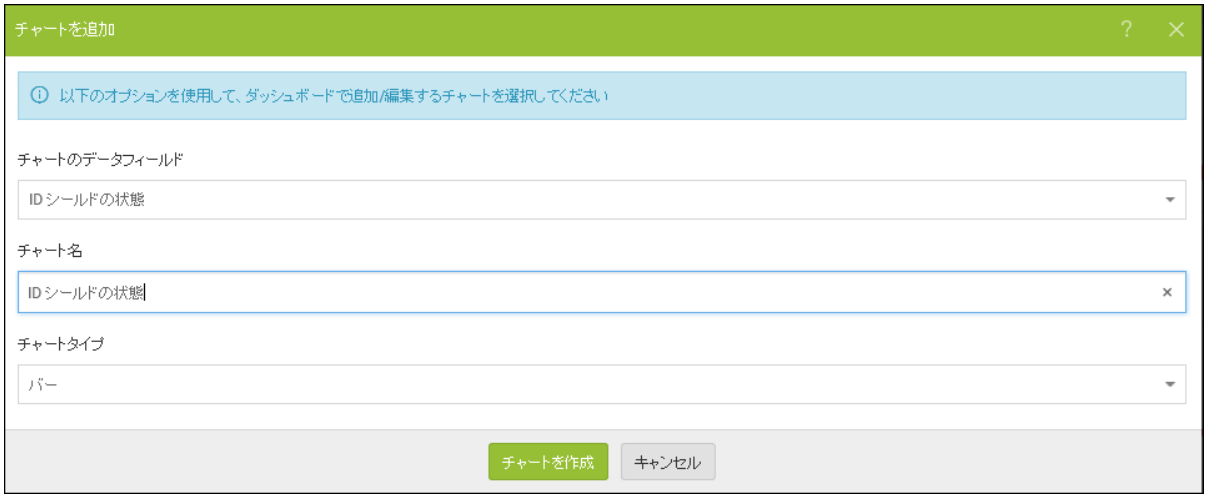
2. メイン メニューから、[**ダッシュボード**] タブをクリックします。

   [ダッシュボード] タブが表示されます。



3. [**チャートを追加**] ボタンをクリックします。

[チャートを追加] ウィンドウが表示されます。



4. [チャートのデータフィールド] ドロップダウン メニューから、次のオプションのいずれかを選択します:

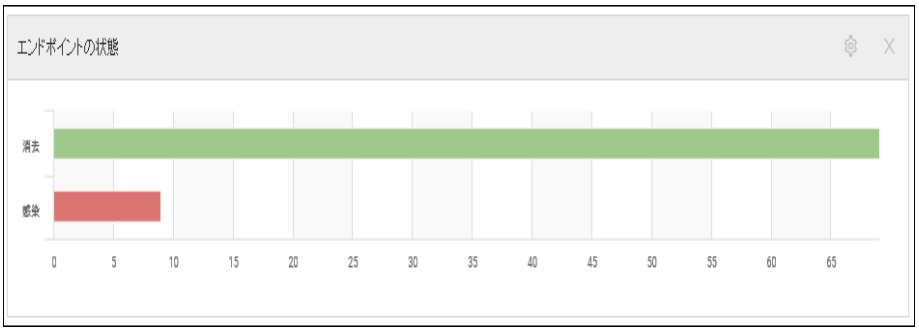
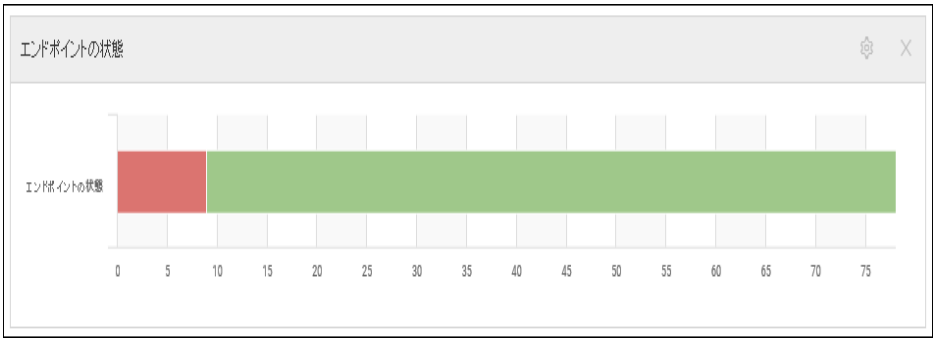
エージェントのバージョンの使用状況	ファイアウォールの状態	オペレーティング システムの言語	ルートキット シールドの状態
注意が必要	ID シールドの状態	オペレーティング システムのプラットフォーム	スケジュール スキャンの状態
デバイスのアクティブ化	Infrared の状態	フィッシング シールドの状態	サイレント モード
デバイスのタイプ	インストールのステータス	プライマリ ブラウザ	脅威の検出履歴
エンドポイントの状態	ポリシーにより管理	リアルタイム シールドの状態	USB シールドの状態
期限切れの状態	オフライン シールドの状態	対応の状態	Web 脅威シールドの状態

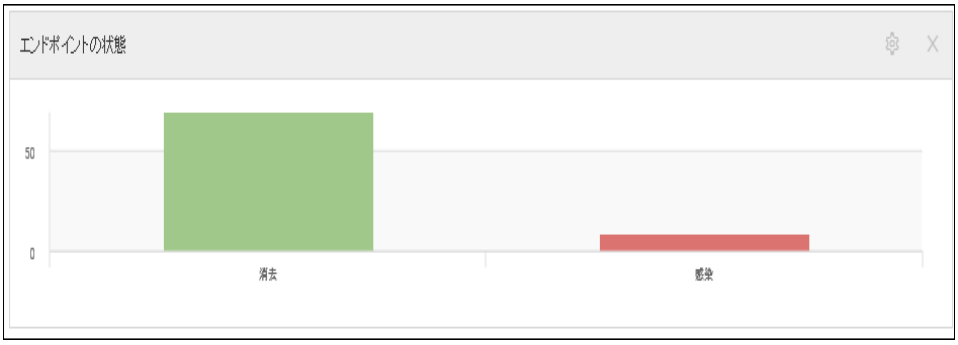
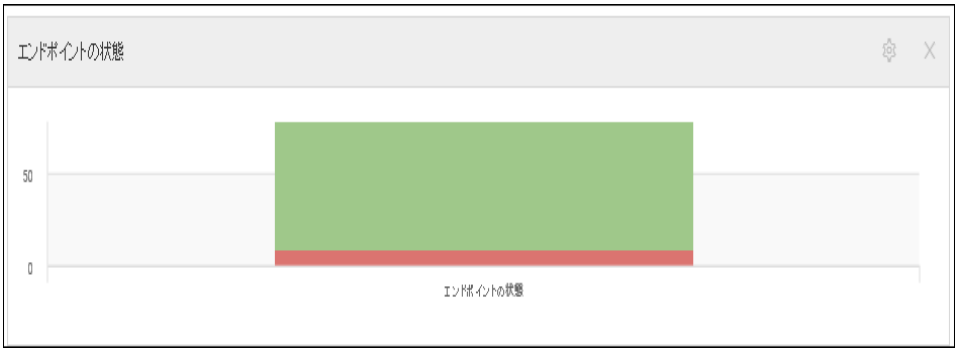
注意: 次のデータポイントは、Mac エージェントでサポートされていません。ファイアウォールの状態、ルートキット シールドの状態、Infrared の状態。 サイレント モード、オフライン シールドの状態。

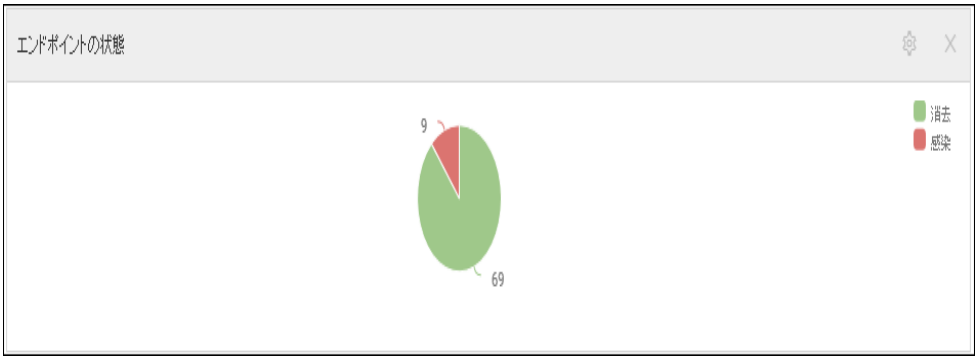
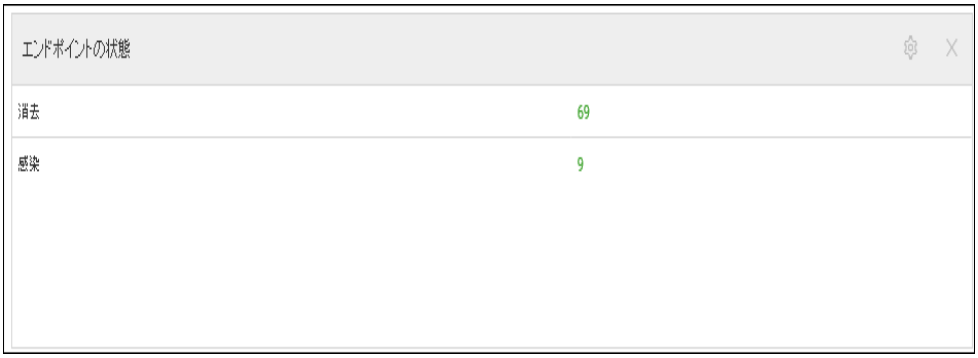
5. [チャート名] フィールドにチャートの名前を入力します。

通常、チャート名はそれに含まれる情報タイプ名を反映しますが、このフィールドは自由入力形式のフィールドですので、必要に応じてチャートに他の名前をつけることができます。

6. [チャート タイプ] ドロップダウン メニューから、次のチャート タイプのいずれかを選択します。

名前	説明
棒グラフ	
積み上げたバー	

名前	説明
カラムチャート	
積み上げた列	

名前	説明
円グラフ	: 
表	

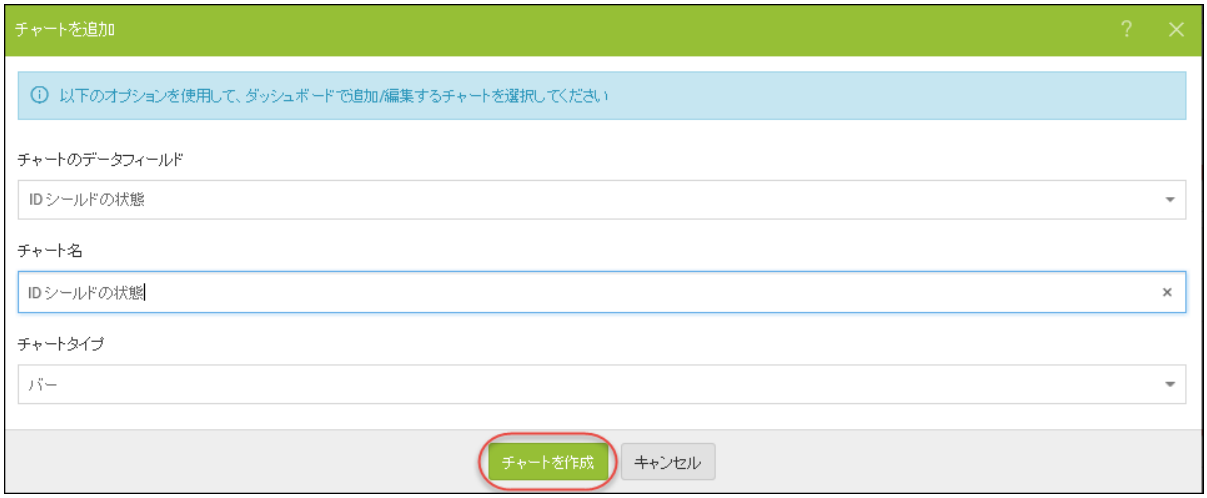
7. 「脅威の検出履歴」または「デバイスのアクティブ化」のダッシュボードチャートを作成する場合、次のチャート タイプの中から選択することができます:
   - エリア
   - スプライン面グラフ
   - カラムチャート
   - 線

- スプライン
- 表

8. 「脅威の検出履歴」または「デバイスのアクティブ化」のダッシュボード チャートを編集する場合、期間を次のいずれかに設定することができます。

24 時間	2 日	3 日	7 日
14 日	30 日	60 日	90 日

9. フィールドへの入力が完了したら、[**チャートを作成**] ボタンをクリックします。



入力された情報でダッシュボードが作成されます。

注意: ダッシュボードのチャートの編集については、「*36{/u}{/color} ページの「ダッシュボードのチャートの編集」*」を参照してください。

ダッシュボードのチャートの編集

ダッシュボードのチャートを作成した後にチャートを編集するには、必要に応じてこの手順を使用することができます。

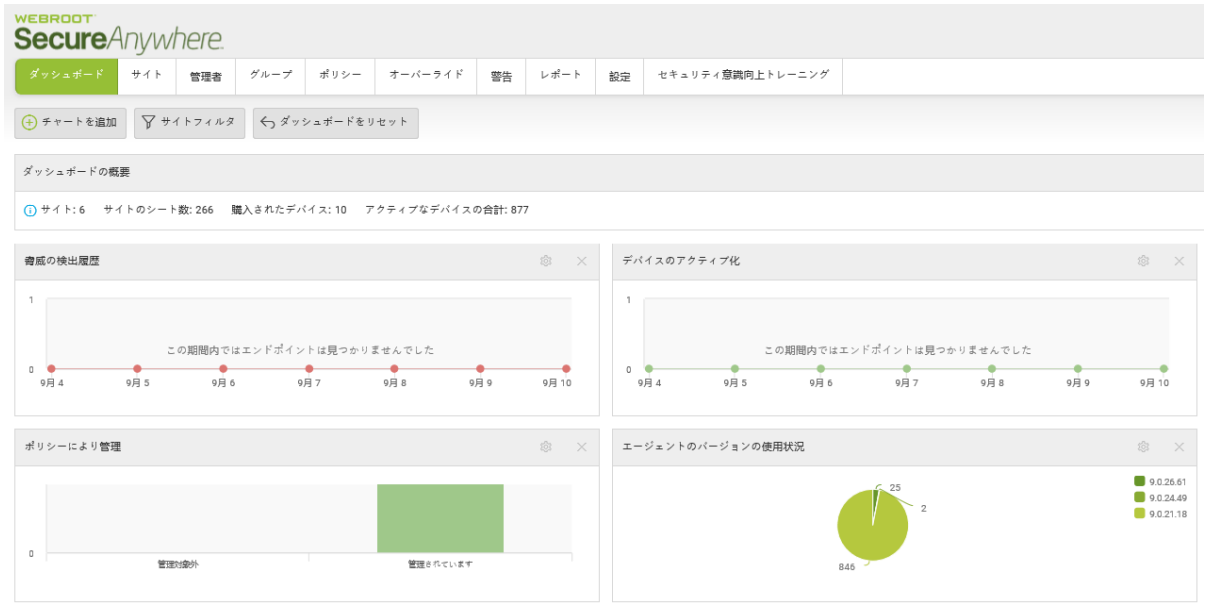
ダッシュボードのチャートを編集するには:

1. 管理コンソールにログインします。

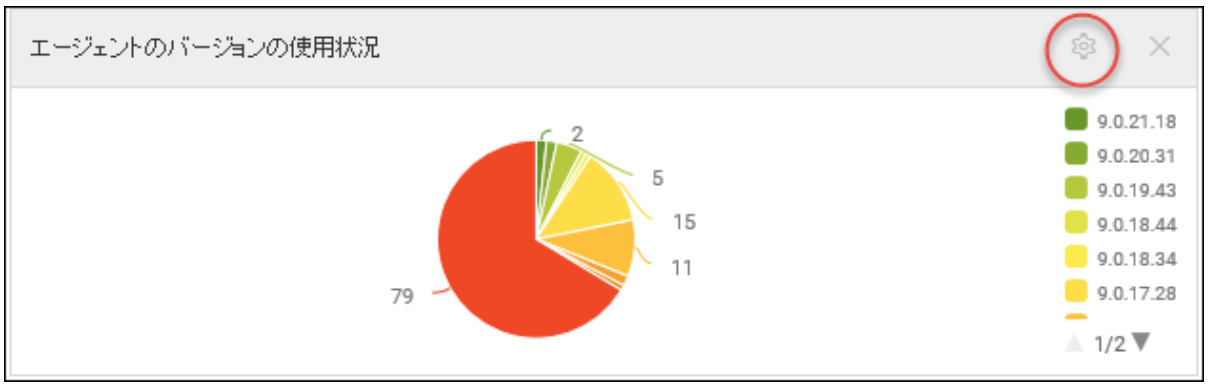
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**ダッシュボード**] タブをクリックします。

   [ダッシュボード] タブが表示されます。



3. 編集するチャートの右上の**歯車**アイコンをクリックします。



[チャートを編集] ウィンドウが表示されます。

4. [チャートのデータフィールド] ドロップダウン フィールドから、次のオプションのいずれかを選択します。

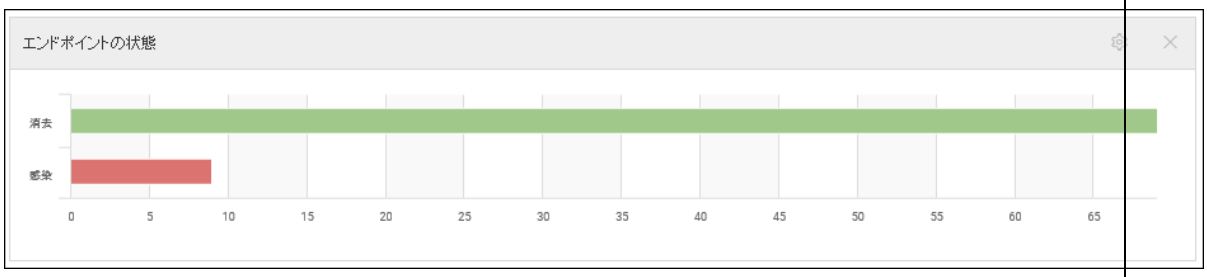
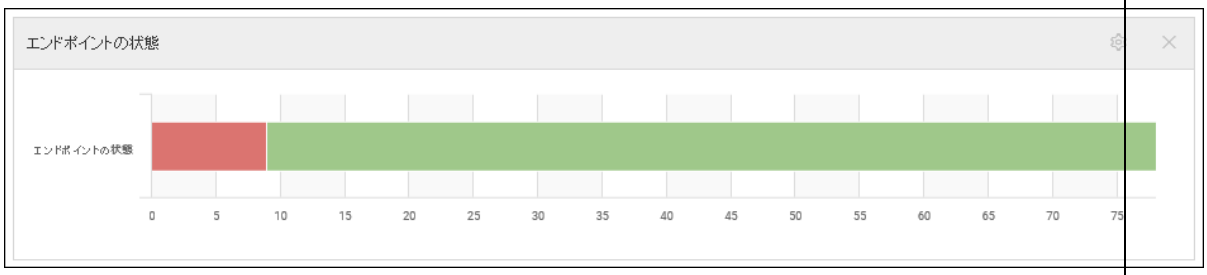
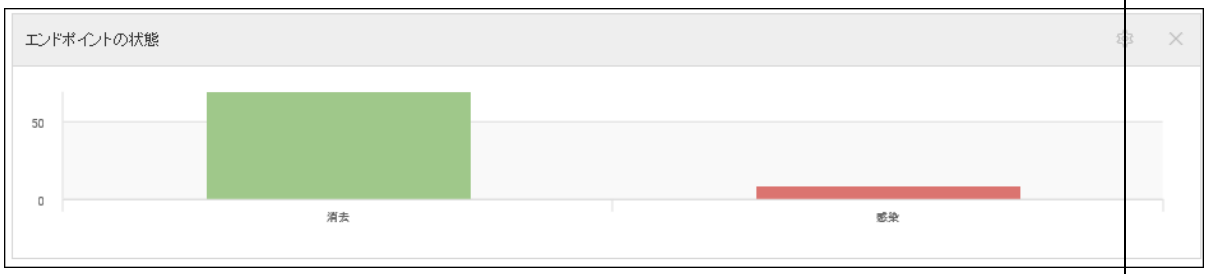
エージェントのバージョンの使用状況	ファイアウォールの状態	オペレーティング システムの言語	ルートキット シールドの状態
注意が必要	ID シールドの状態	オペレーティング システムのプラットフォーム	スケジュール スキャンの状態
デバイスのアクティブ化	Infrared の状態	フィッシング シールドの状態	サイレント モード
デバイスのタイプ	インストールのステータス	プライマリ ブラウザ	脅威の検出履歴
エンドポイントの状態	ポリシーにより管理	リアルタイム シールドの状態	USB シールドの状態
期限切れの状態	オフライン シールドの状態	対応の状態	Web 脅威シールドの状態

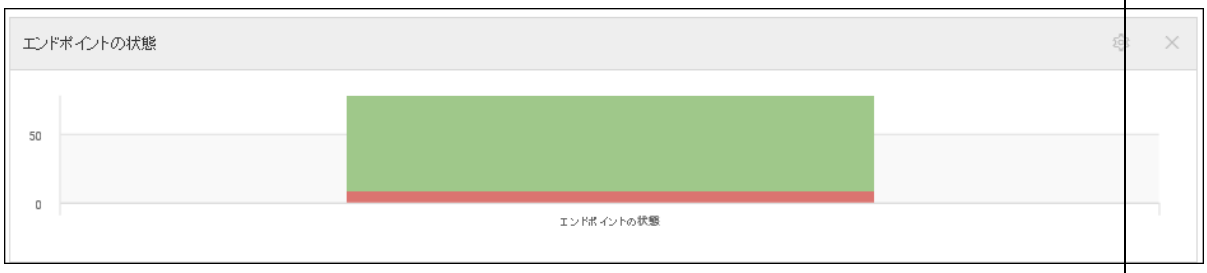
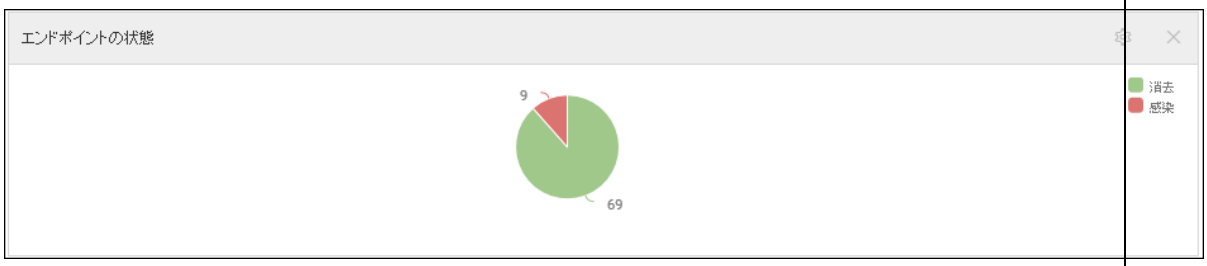
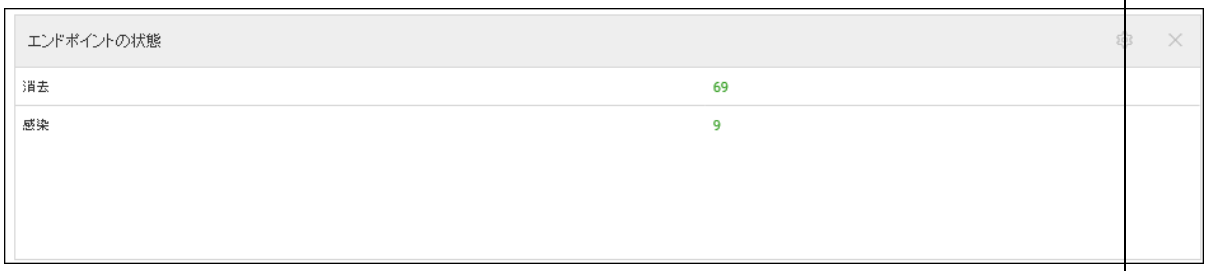
注意: 次のデータポイントは、Mac エージェントでサポートされていません。ファイアウォールの状態、ルートキット シールドの状態、Infrared の状態。 サイレント モード、オフライン シールドの状態。

5. [チャート名] フィールドにチャートの名前を入力します。

通常、チャート名はそれに含まれる情報タイプ名を反映しますが、このフィールドは自由入力形式のフィールドですので、必要に応じてチャートに他の名前をつけることができます。

6. [チャート タイプ] ドロップダウン メニューから、次のチャート タイプのいずれかを選択します。

名前	説明
棒グラフ	
積み上げたバー	
カラムチャート	

名前	説明
積み上げた列	
円グラフ	
表	

7. 「脅威の検出履歴」または「デバイスのアクティブ化」のダッシュボード チャートを編集している場合、次のチャート タイプから選択することができます。

   - エリア
   - スプライン面グラフ
   - カラムチャート

- 線
- 表

8. 「脅威の検出履歴」また「デバイスのアクティブ化」のダッシュボード チャートを編集している場合、[期間] ドロップダウン メニューから次のいずれかを選択します

24 時間	2 日	3 日	7 日
14 日	30 日	60 日	90 日

9. 完了したら、[**チャートを保存**] ボタンをクリックします。

注意: ダッシュボードのチャートの削除については、「*48{/u}{/color} ページの「ダッシュボードのチャートの削除」*」を参照してください。

ダッシュボードのチャートの詳細表示

この手順に従いダッシュボードを絞り込むと、次のような詳細を表示することができます。

- エンドポイントの情報
- 配備の状態

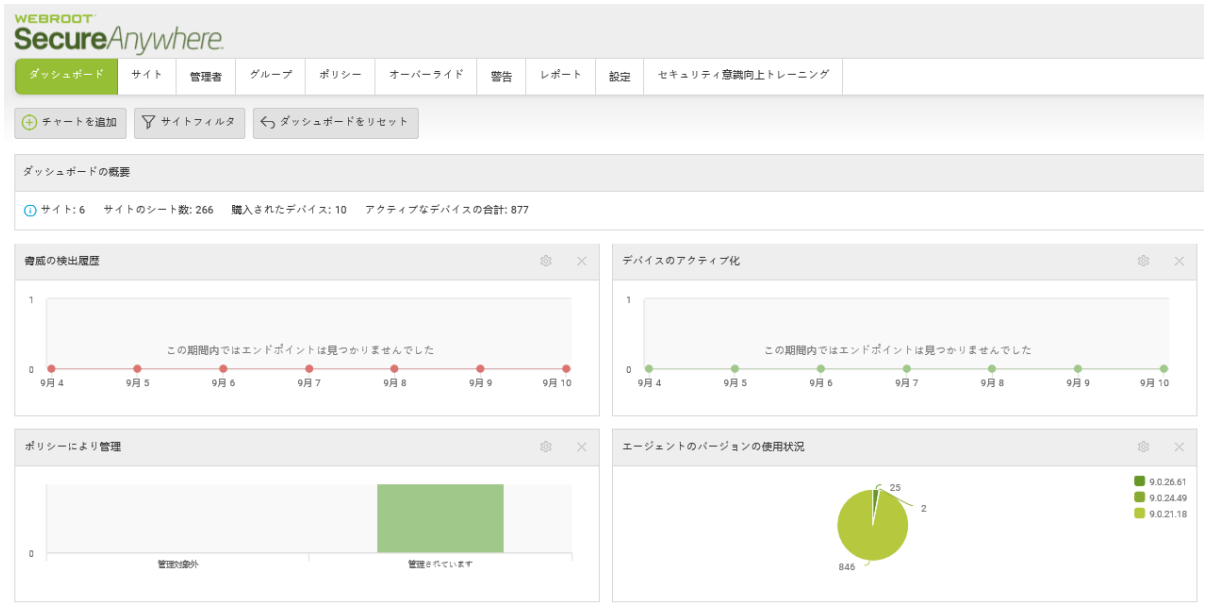
ダッシュボードのチャートを絞り込むには:

1. 管理コンソールにログインします。

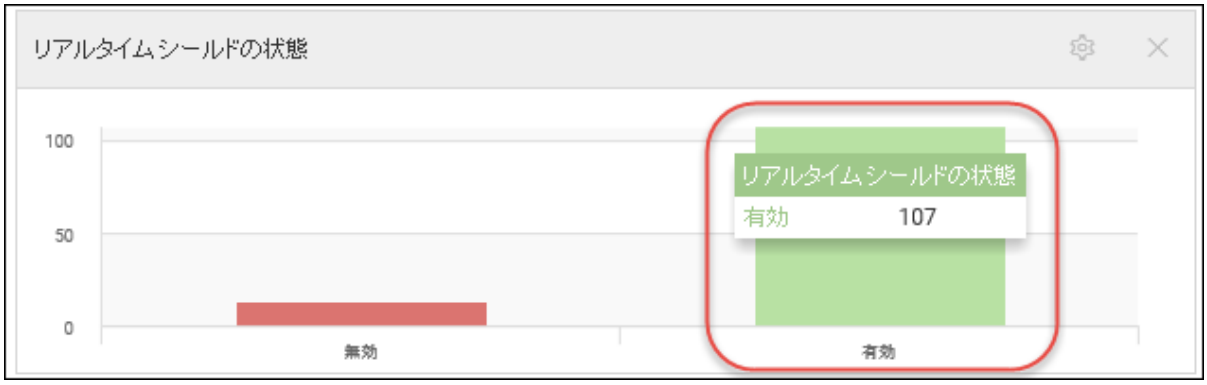
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**ダッシュボード**] タブをクリックします。

   [ダッシュボード] タブが表示されます。

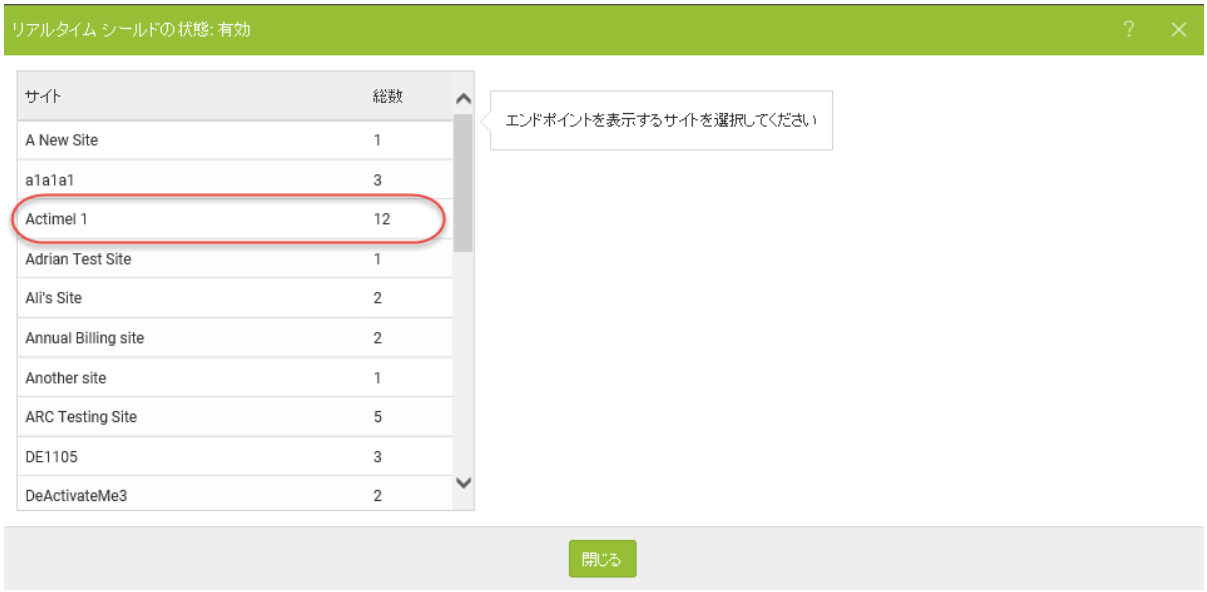


3. 絞り込みたいチャートをクリックします。

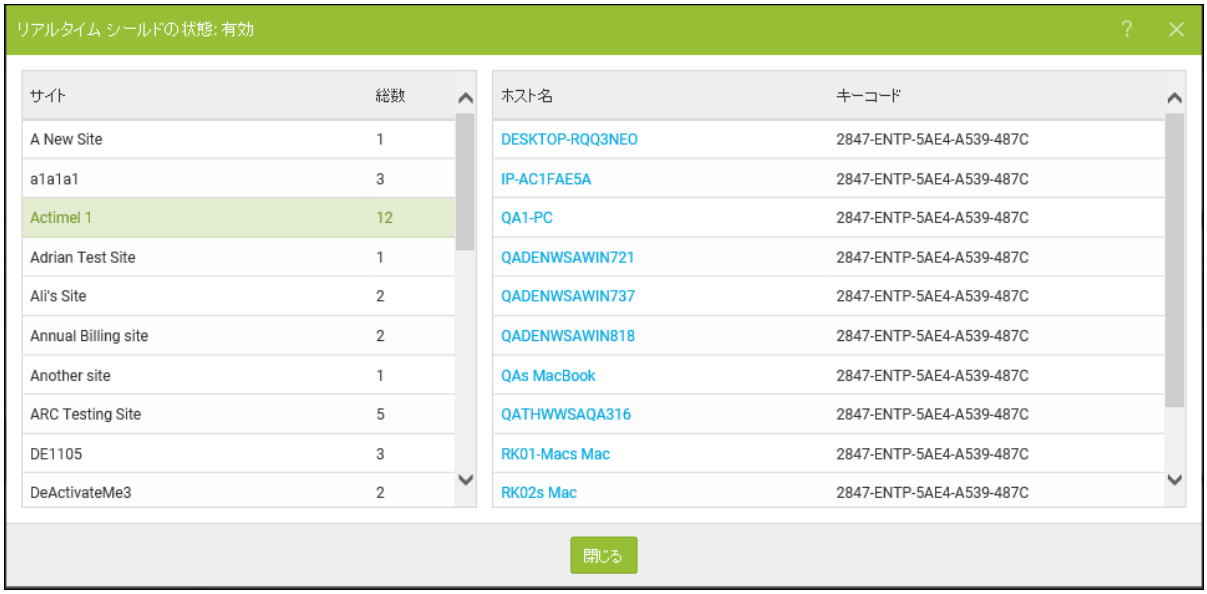


絞り込みの第 1 段階が表示されます。ここには、サイト名やサイトのエンドポイント数に関する情報などが含まれます。

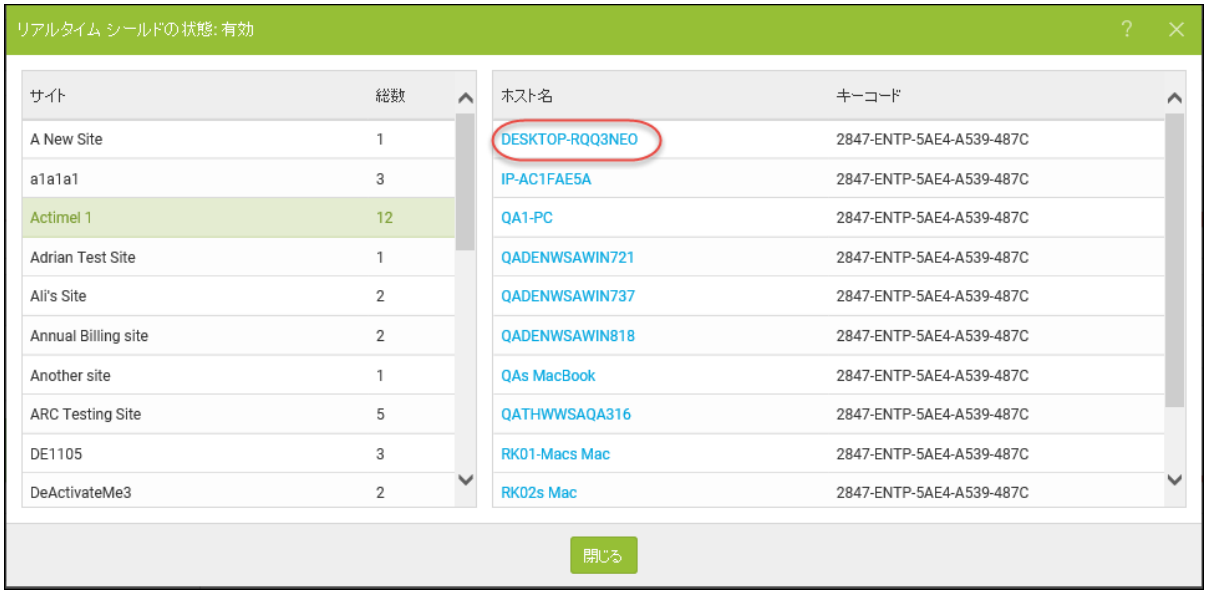
4. サイト コラムでサイト名をクリックすると、絞り込みの第 2 段階が表示されます。



情報がさらに詳細に絞り込まれ、ホスト名や各エンドポイントに関連するキーコードに関する情報が表示されます。



5. ホスト名コラムでホスト名を選択すると、そのホストに関する詳しい情報が表示されます。



[エンドポイント情報] ウィンドウには、次の項目に関する情報が表示されます。

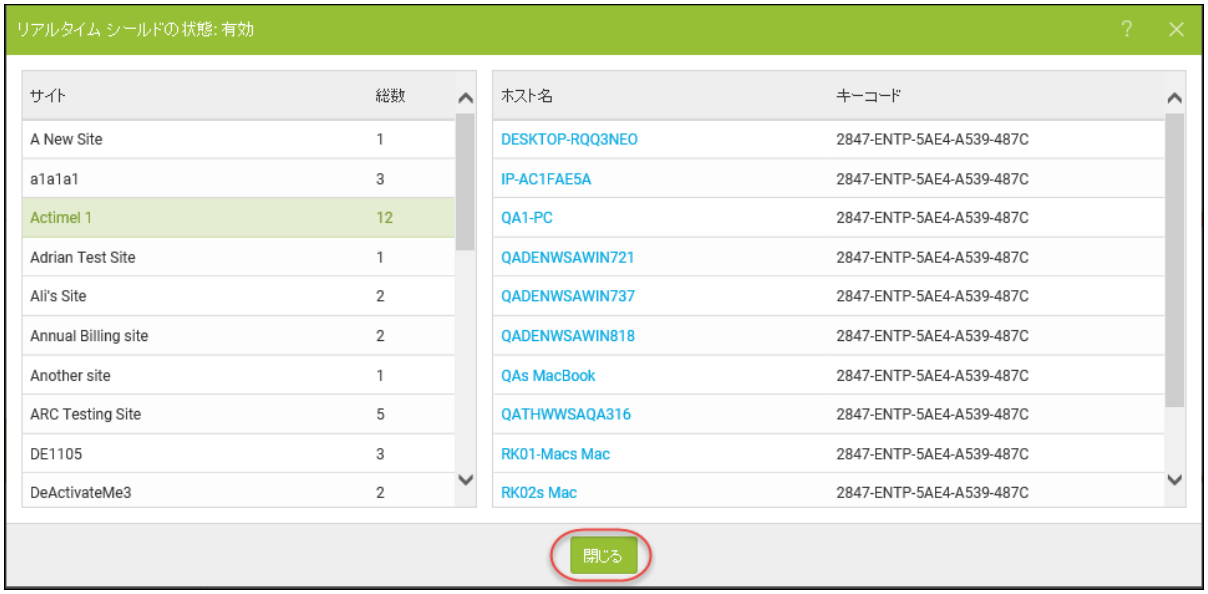
- エンドポイント
- Webroot SecureAnywhere

- スキャン情報
- シールド

注意: 次のデータポイントは、Mac エージェントでサポートされていません。ファイアウォールの状態、ルートキット シールドの状態、Infrared の状態。 サイレント モード、オフライン シールドの状態。

6. 情報を確認したら、[**閉じる**] ボタンをクリックして絞り込みウィンドウに戻ります。

7. その後、絞り込みウィンドウから [**閉じる**] ボタンをクリックして、メインのダッシュボードに戻ります。



ダッシュボードのチャートの削除

この手順に従って、必要なくなったダッシュボードのチャートを削除します。

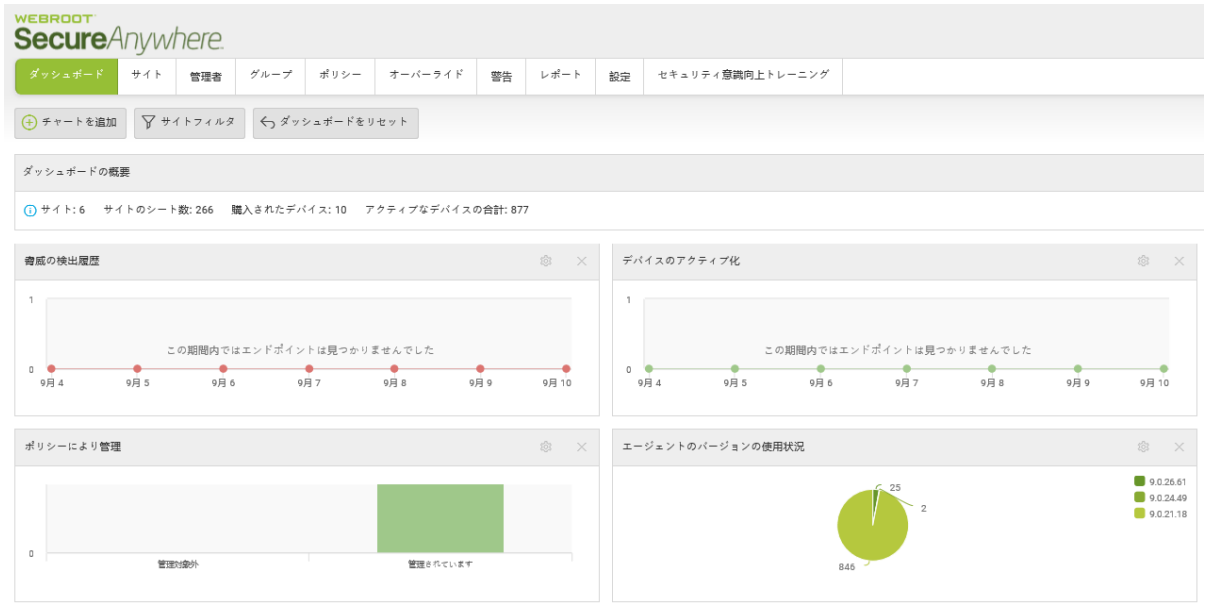
ダッシュボードのチャートを削除するには:

1. 管理コンソールにログインします。

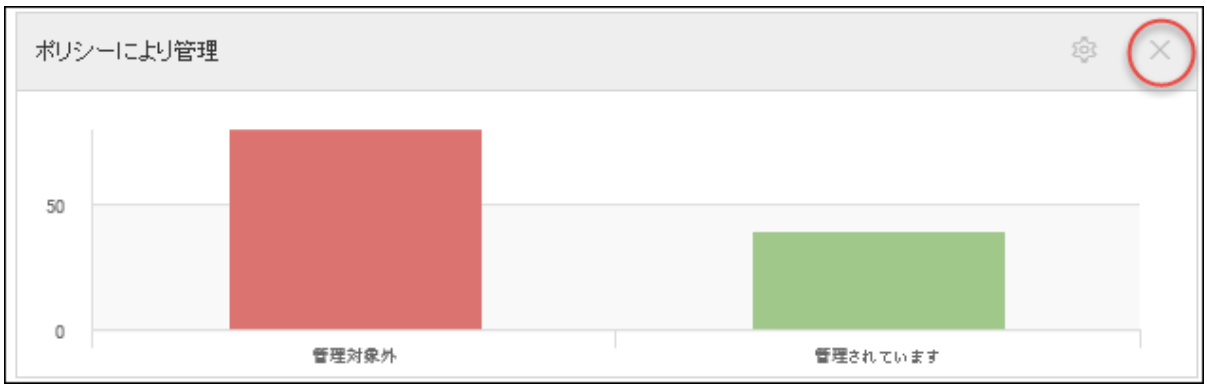
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**ダッシュボード**] タブをクリックします。

   [ダッシュボード] タブが表示されます。



3. 削除するチャートで、チャートの右上にある [X] アイコンをクリックします。



4. 「チャートの削除」メッセージが表示されたら、[OK] ボタンをクリックし、削除を確定します。

システムにより、チャートがダッシュボードから削除されます。

> **注意:** ダッシュボードのチャートの作成と編集については、「*36{/u}{/color} ページの「ダッシュボードのチャートの編集」*.

」を参照してください。

第 3 章: サイトの操作

サイトを操作するには、次のトピックを参照してください。

管理コンソールの [サイト] タブ概要

管理コンソールの [サイト] タブには、すべてのサイトのリストが、シート数、設定などとともに表示されます。

コンソールの右上には次の情報や機能が表示されます。

- **コンソール名** - コンソールの名前が表示され、コンソールの名前を変更したり、表示しているコンソールを変更したりできます。詳細については、「*18{/u}{/color} ページの「コンソールの名前の変更」*」と「*15{/u}{/color} ページの「コンソールの変更」*」を参照してください。
- **ベル アイコン** - アラートやアップデートがある場合に表示されます。
- **はてなマーク アイコン** - 次のオプションを含むドロップダウン メニューが表示されます。
  - **ヘルプドキュメント** - コンソールで閲覧中の内容に関連するトピックのヘルプ情報を表示します。
  - **DNS ヘルプ文書** - DNS 保護のオンライン ガイドを表示します。
  - **Webroot 教育ビデオ** - ウェブルートの YouTube チャンネルへのリンクです。
  - **製品トレーニング** - ウェブルート パートナー認定 Web サイトへのリンクです.
  - **サービスの状態** - 既知の全インシデントの状態が表示される Web サイトへのリンクです.
  - **スポットライト ツアー** - 管理コンソールのツアーを表示できます。詳細については、「*9{/u}{/color} ページの「スポットライト ツアーについて」*」を参照してください。
  - **サポート** - [サポートに連絡] ページを表示します。このページでサポート チケットを入力できます。
- **ユーザー名ドロップダウン** - ログアウト ボタンを含みます。
- **[検索] フィールド** - 検索する情報を入力できます。詳細については、「*68{/u}{/color} ページの「サイトの検索」*」を参照してください。
- **[サイトの追加] ボタン** - ダッシュボードにサイトを追加できます。詳細については、「*56{/u}{/color} ページの「サイトの追加」*」を参照してください。
- **[ダウンロード] ボタン** - CSV ファイルをダウンロードできます。詳細については、「*70{/u}{/color} ページの「CSV ファイルのダウンロード」*」を参照してください。

- **[フィルタ] ボタン** - サイトのフィルタリング条件を指定し、条件に合うサイトのみを表示させることができます。詳細については、「*63{/u}{/color} ページの「サイトのフィルタリング」*」を参照してください。
- **[サイトのリフレッシュ] ボタン** - コンソールに表示されている情報をアップデートします。

最初の行には次の情報や機能が表示されます。

- **結果** - フィルタの設定に基づいて返されたサイトの数を表示します。
- **アクセス可能なサイト** - ログインしたユーザーがアクセスできるサイトの数を表示します。
- **合計** - 現在の管理コンソールでアクティブなサイトの数を表示します。

列には次の情報や機能が表示されます。

- **状態** - 次のいずれかの状態を表示します。
  - 保護
  - 一時停止
  - 期限切れ

  - 要対応
  - 非アクティブ化済み

- **サイト** - 会社名。この情報は、サイトの作成時に入力されます。詳細については、「*56{/u}{/color} ページの「サイトの追加」*」を参照してください。会社名も編集できます。詳細については、「*94{/u}{/color} ページの「サイトの詳細を編集」*」を参照してください。

- **[管理] ボタン** - クリックすると各サイトの追加情報が表示されます。[**管理**] ボタンをクリックしたときに使用可能なアクションに関する詳細については、次のトピックを参照してください。

  - *74{/u}{/color} ページの「サイトの概要を表示」*
  - *88{/u}{/color} ページの「サイト保護の一時停止および再開」*
  - *91{/u}{/color} ページの「サイトの保護を非アクティブ化」*
  - *94{/u}{/color} ページの「サイトの詳細を編集」*
  - *114{/u}{/color} ページの「サイト設定の編集」*
  - *119{/u}{/color} ページの「サイト レベルのデータ フィルタの設定」*
  - *102{/u}{/color} ページの「サイトのタグ付け」*
  - *111{/u}{/color} ページの「サイト管理者権限の更新」*

> **注意:** エンドポイント プロテクション コンソールにアクセスするには、[管理] ボタンをクリックします。詳細については、「*22{/u}{/color} ページの「エンドポイント コンソールへのアクセス」*」を参照してください。

- **キーコード** - サイトのキーコード。キーコードを表示するには、[**キー**] アイコンをクリックします。この情報は、サイトの作成時に入力されます。詳細については、「*56{/u}{/color} ページの「サイトの追加」*」を参照してく

ださい。会社名も編集できます。詳細については、「*94{/u}{/color} ページの「サイトの詳細を編集」*」を参照してください。

- **デバイス** - 対象サイトのデバイス数。この情報は、サイトの作成時に入力されます。詳細については、「*56{/u}{/color} ページの「サイトの追加」*」を参照してください。会社名も編集できます。詳細については、「*94{/u}{/color} ページの「サイトの詳細を編集」*」を参照してください。

  注意: デバイス数の横に感嘆符アイコン (!) が表示されている場合は、[すべてのデータを表示] 以外のデータフィルタが適用されていることを示します。詳細については、「*119{/u}{/color} ページの「サイト レベルのデータ フィルタの設定」*」を参照してください。

- **サイトのシート数** - 対象サイトに割り当てられたシート数。この情報は、サイトの作成時に入力されます。詳細については、「*56{/u}{/color} ページの「サイトの追加」*」を参照してください。会社名も編集できます。詳細については、「*94{/u}{/color} ページの「サイトの詳細を編集」*」を参照してください。
- **DNS プロテクション** - DNS プロテクションが有効になっているかどうかを示します。詳細については、「*About DNS Protection*」を参照してください。
- **セキュリティ意識向上トレーニング** - セキュリティ意識向上トレーニングが有効になっているかどうかを示します。詳細については、「*About Security Awareness Training*」を参照してください。

サイトの追加

管理コンソールにサイトを追加するには、この手順に従ってください。サイト情報の編集に関する詳細は、次のいずれかを参照してください。

- *94{/u}{/color}* ページの「*サイトの詳細を編集*」
- *111{/u}{/color}* ページの「*サイト管理者権限の更新*」
- *114{/u}{/color}* ページの「*サイト設定の編集*」

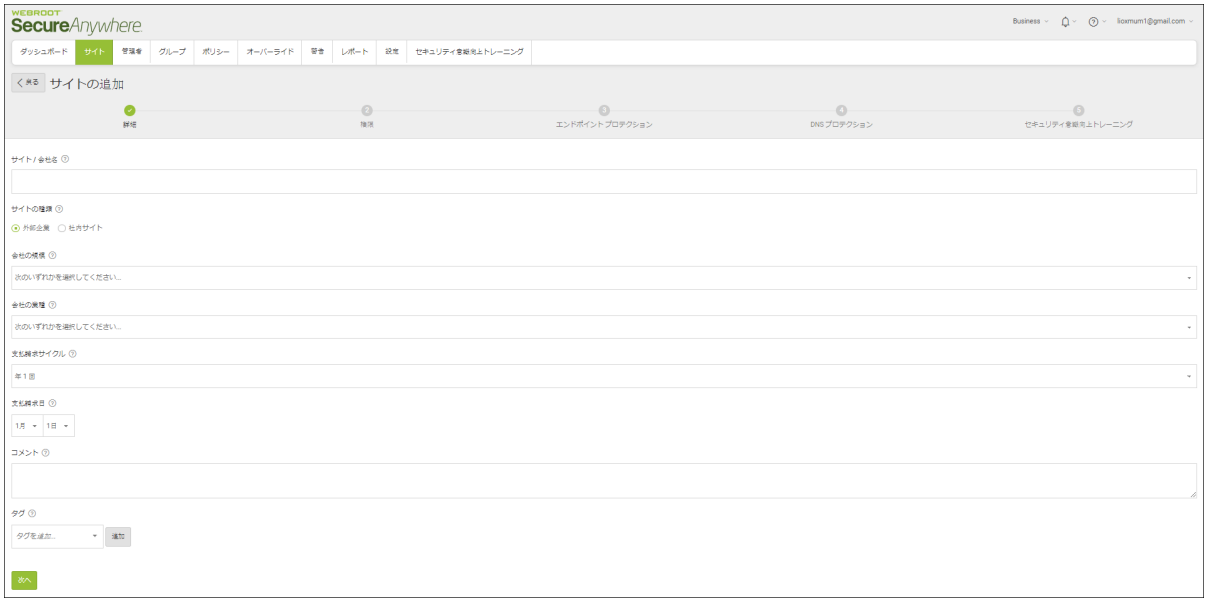
サイトを追加するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**サイトの追加**] ボタンをクリックします。

   [詳細] エリアがアクティブな状態で [サイトの追加] パネルが表示されます。



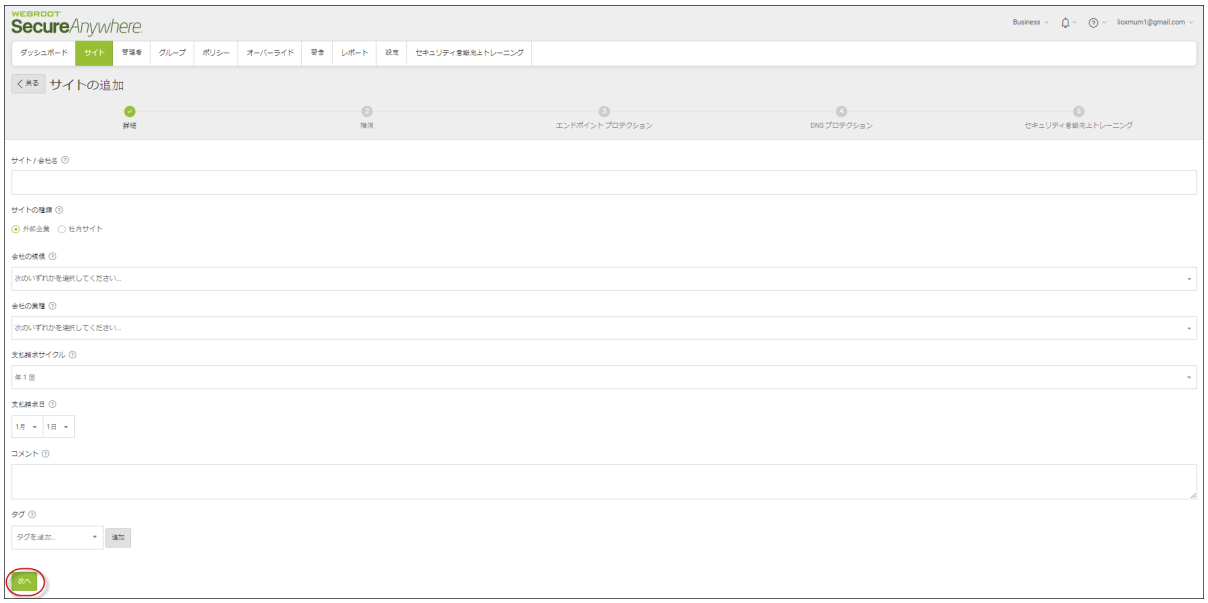
3. [サイト / 会社名] フィールドにサイトの名前を入力します。
4. [サイトの種類] フィールドでは、次のいずれかを行ってください。
   - 作成するサイトが外部の顧客で貴社のサービスを購入するものであれば、[**外部企業**] ラジオ ボタンを選択してステップ 5 に進みます。
   - 作成するサイトがロケーションの追加であったり、同じ会社内のオフィスである場合は、[**社内サイト**] ラジオ ボタンを選択して [**次へ**] をクリックし、ステップ 9 へ進みます。

   注意: [社内サイト] ラジオ ボタンを選択した場合は、[会社の規模]、[会社の業種]、[支払請求サイクル]、[支払請求日] フィールドは表示されないため、内容を指定する必要はありません。

5. [会社の規模] フィールドのドロップダウン メニューで、実際の会社の規模に最も近いものを選択してください。
6. [会社の業種] フィールドのドロップダウン メニューでは、実際の業種に最も近いものを選択します。
7. [支払請求サイクル] フィールドのドロップダウン メニューでは、次の支払請求サイクルのいずれかを選択します。
   - **年 1 回**
   - **四半期ごと**

- **月次**
- **毎週**

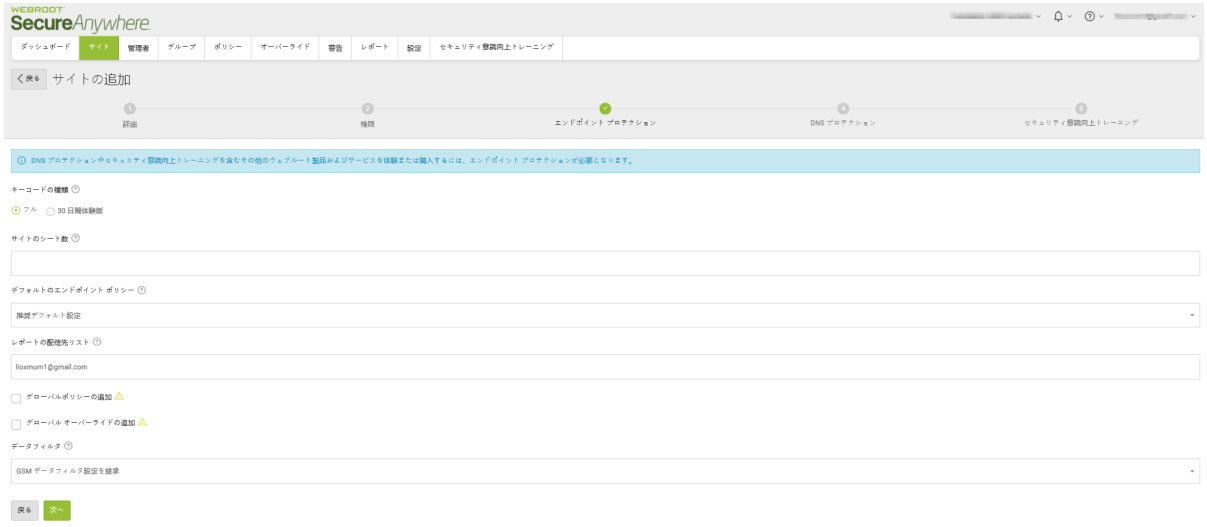
8. [支払請求日] フィールドで、ドロップダウン メニューから支払い請求の月と日を選択します。
9. [コメント] フィールドには、任意の情報を入力します。このフィールドはオプションです。
10. [タグ] ドロップダウン メニューで、このサイトに関連付けるタグを選択するか追加します。このフィールドはオプションです。
11. 設定が完了したら、[**次へ**] ボタンをクリックします。



システムに [権限] エリアが表示されます。

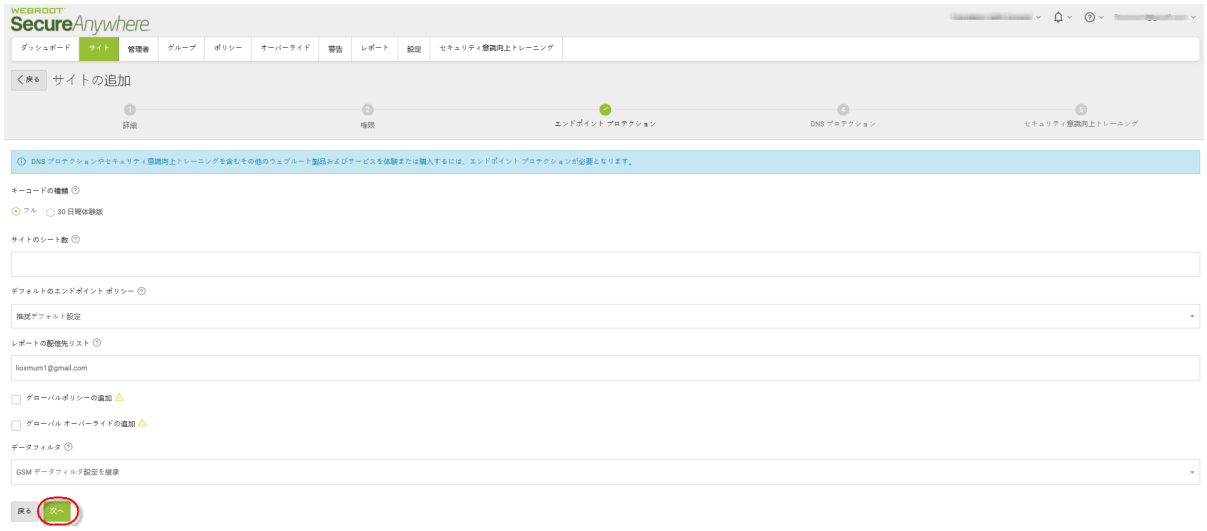
12. サイトの各ユーザーについて、次の権限レベルのいずれかを選択します。
    - **管理者**
    - **表示のみ**
    - **アクセス不可**
13. 設定が完了したら、[**次へ**] ボタンをクリックします。

システムに [エンドポイント保護] エリアが表示されます。



14. [キーコードの種類] エリアで、[フル] または [30 日間体験版] ラジオボタンのいずれかを選択します。
15. [サイトのシート数] フィールドに新しいサイトのシート数を入力します。

16. [デフォルトのポリシー] のドロップダウンで、次のいずれかを選択します。
    - **推奨デフォルト設定**
    - **推奨サーバー デフォルト設定**
    - **サイレント監査**
    - **管理対象外**
17. [グローバル ポリシーの追加] チェックボックスで、次のいずれかを実行します。
    - グローバル ポリシーを含める場合は、このチェックボックスを選択します。
    - グローバル ポリシーを含めない場合は、このチェックボックスを選択しないでください。
18. [グローバル オーバーライドの追加] チェックボックスで、次のいずれかを実行します。
    - グローバル オーバーライドを含める場合は、このチェックボックスを選択します。
    - グローバル オーバーライドを含めない場合は、チェックボックスを選択しないでください。
19. [レポートの配信先リスト] フィールドで、レポートを送信する相手の電子メールアドレスを入力します。
    - 複数の電子メールアドレスを入力する場合は、カンマで区切ります。
    - レポート配信の詳細については、「*396{/u}{/color} ページの「グローバル サイト マネージャー レポート概要」*」を参照してください。
20. [データフィルタ] フィールドのドロップダウン メニューで、いずれかのフィルタを選択して表示するデータの条件を指定します。
21. 設定が完了したら、[**次へ**] ボタンをクリックします。



システムに [DNS プロテクション] エリアが表示されます。

22. DNS プロテクションを有効にする場合、[**SecureAnywhere DNS を有効にする**] チェックボックスを選択します。詳細については、「SecureAnywhere DNS 保護管理者ガイド」を参照してください。
23. 設定が完了したら、[**次へ**] ボタンをクリックします。

システムに [セキュリティ意識向上トレーニング] エリアが表示されます。

24. セキュリティ意識向上トレーニングを有効にする場合、[**セキュリティ意識向上トレーニング**] チェックボックスを選択します。詳細については、「セキュリティ意識向上トレーニング オンライン ガイド」を参照してください。
25. 操作を完了したら、[**完了**] ボタンをクリックします。

以下が実行されます。

- 有効なキーコードの作成
- 必要なコンソールの構築
- コンソールへのキーコードの適用
- ウィンドウを閉じると、サイト コンソールのリストに新しいサイトが表示されます。

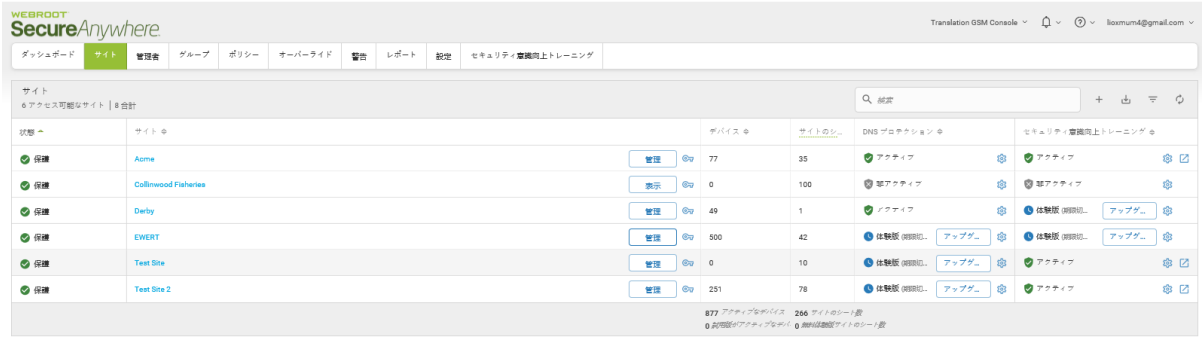
サイトのフィルタリング

フィルタ機能により管理者は、各サイトに割り当てられたタグに基づいて、お客様サイトをフィルタリングすることができます。さらに、サイトの名前やコメントによるサイトのフィルタリングも可能です。

サイトをフィルタリングするには:

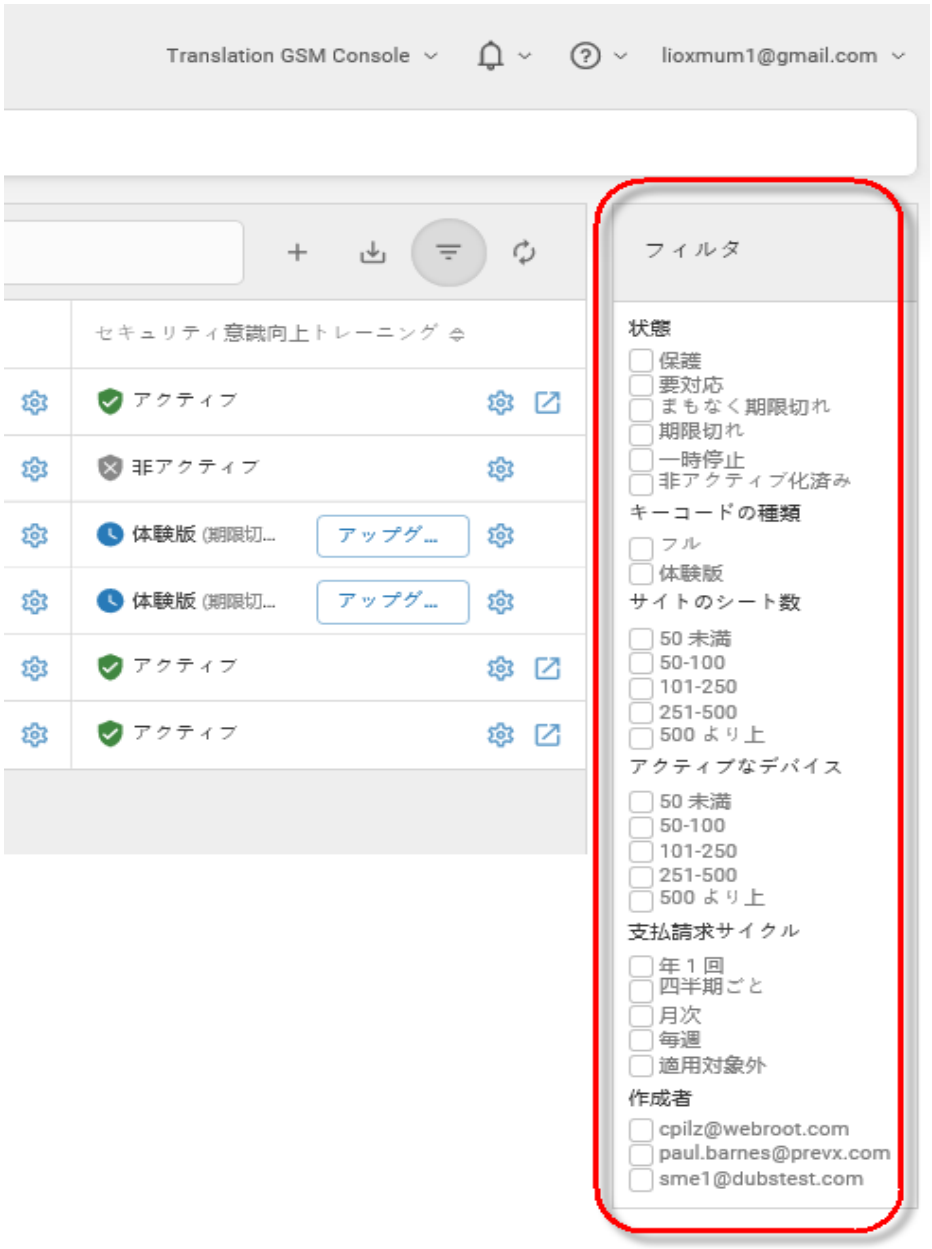
1. 管理コンソールにログインします。

   [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が表示されます。



2. [**フィルタ**] ボタンをクリックします。

システムに [フィルタ] パネルが表示され、適用するフィルタを選択することができます。



注意: [フィルタ] パネルを非表示にするには、[**フィルタ**] アイコンをもう一度クリックします。

3. 次の表の説明に従って、適用するフィルタのボタンをクリックするか情報を入力します。複数のフィルタ

を適用できます。

ボタン	説明
状態	次の状態のいずれか、またはすべてを選択します。 • 保護 • 要対応 • まもなく期限切れ • 期限切れ • 一時停止 • 非アクティブ化済み
キーコードの種類	次のキーコードの種類のいずれか、または両方を選択します。 • フル • 体験版
サイトのシート数	次のサイトのシート数のいずれか、またはすべてを選択します。 • 50 未満 • 50 ～ 100 • 101 ～ 250 • 251 ～ 500 • 500 より上

ボタン	説明
アクティブなデバイス	次のサイトのシート数のいずれか、またはすべてを選択します。 • 50 未満 • 50 ～ 100 • 101 ～ 250 • 251 ～ 500 • 500 より上
支払請求サイクル	次の支払請求サイクルのいずれか、またはすべてを選択します。 • 年 1 回 • 四半期ごと • 月次 • 毎週 • 適用対象外
作成者	サイトを作成したユーザーの電子メールアドレスを選択します。 電子メールアドレスが 7 件以上ある場合は、一覧の右側にスクロール バーが表示されます。
タグ	サイトに対して作成および適用されたタグを選択します。 電子メールアドレスが 7 件以上ある場合は、一覧の右側にスクロール バーが表示されます。

4. 必要に応じて次のいずれか、またはすべてを実行します。
   - [フィルタ] メニューを非表示にするには、[**フィルタ**] ボタンをクリックします。フィルタが適用されている場合は、フィルタの数が青い丸で囲まれて表示されます。
   - すべてのフィルタを表示するには、[**フィルタ**] ボタンをクリックします。

サイトの検索

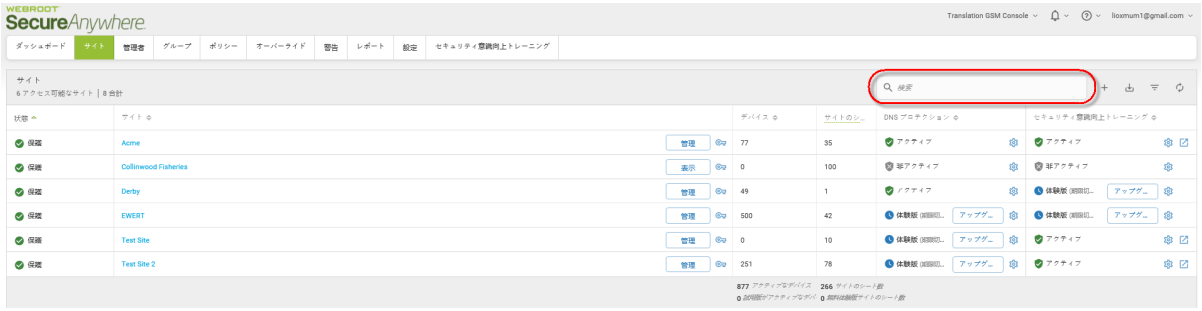
検索機能を使用して、管理者はサイト名でサイトを検索できます。

サイトを検索するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [検索] フィールドに、検索するサイトの名前を入力します。



3. 必要に応じて、名前の一部を入力することもできます。その場合は、条件に一致するすべてのサイトが表示されます。

   たとえば、サイト名に「Hay」という文字が含まれていることが分かっていて、その他の部分が不明な場合は、「**Hay**」と入力します。検索結果には、名前に「Hay」が含まれるすべてのサイトが表示されます。

4. 検索が完了したら、[検索] フィールドの [X] をクリックして入力した文字列を消去します。すると、すべてのサイトが表示されます。

CSV ファイルのダウンロード

サイト名、キーコード、状態などのサイト情報をダウンロードするには、次の手順に従ってください。

CSV ファイルをダウンロードするには:

1. 管理コンソールにログインします。

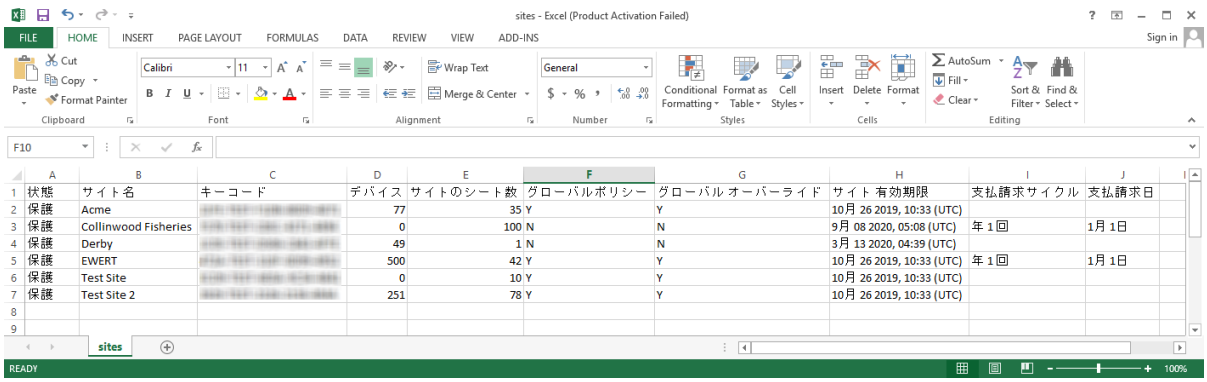
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**ダウンロード**]アイコンをクリックします。

CSV ファイルがダウンロードされます。

注意: ダウンロードしたファイルには、設定したフィルタを反映した情報が含まれています。詳細については、「*63{/u}{/color} ページの「サイトのフィルタリング」*」を参照してください。

3. CSV ファイルをクリックすると、以下の項目に関する情報を確認できます。
   - 状態
   - サイト名
   - キーコード
   - デバイス
   - サイトのシート数
   - グローバルポリシー
   - グローバル オーバーライド
   - サイトの有効期限
   - 支払請求サイクル
   - 支払請求日



	A	B	C	D	E	F	G	H	I	J
1	状態	サイト名	キーコード	デバイス	サイトのシート数	グローバルポリシー	グローバル オーバーライド	サイト 有効期限	支払請求サイクル	支払請求日
2	保護	Acme		77	35	Y	Y	10月 26 2019, 10:33 (UTC)		
3	保護	Collinwood Fisheries		0	100	N	N	9月 08 2020, 05:08 (UTC)	年 1 回	1月 1日
4	保護	Derby		49	1	N	N	3月 13 2020, 04:39 (UTC)		
5	保護	EWERT		500	42	Y	Y	10月 26 2019, 10:33 (UTC)	年 1 回	1月 1日
6	保護	Test Site		0	10	Y	Y	10月 26 2019, 10:33 (UTC)		
7	保護	Test Site 2		251	78	Y	Y	10月 26 2019, 10:33 (UTC)		
8										
9										

サイトの並べ替え

並べ替え機能を使用して、管理者はサイトの見出しに基づいて並べ替えをすることができます。

サイトの並べ替えをするには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. 次のカラムの並べ替えをするには、各見出しの右側にある**上向きの矢印**または**下向きの矢印**をクリックします。
   - 状態
   - サイト
   - デバイス
   - サイトのシート数
   - DNS プロテクション
   - セキュリティ意識向上トレーニング

   注意: 見出しの右側をクリックすると、**上向き**または**下向き**の矢印が表示されます。

各カラムの情報の種類に基づいて、昇順か降順、またはアルファベット順で並べ替えが実行されます。

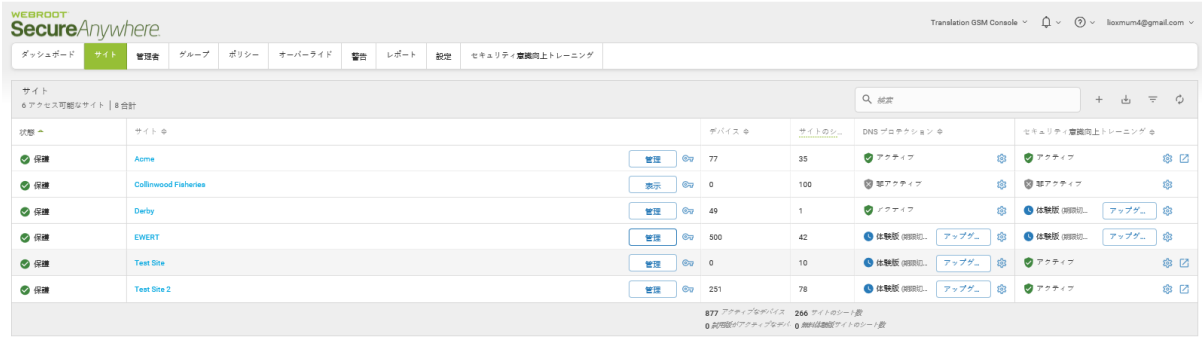
サイトの概要を表示

特定のサイトについて、管理者の名前、支払請求サイクル、コメントなどの追加サイト情報を表示することができます。

追加サイト情報を表示するには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

[管理内] ボタン

[管理内] ボタンには、タブが 6 つあります。

- 概要
- 詳細
- 権限
- エンドポイント プロテクション
- DNS プロテクション
- セキュリティ意識向上トレーニング
- ダウンロード

[概要] タブ

[概要] エリアに、サイトの状態を反映する数字が表示されます。

- 対応が必要なデバイス (現在)
- 対応が必要なデバイス (過去 7 日間)
- インストールされたデバイス (過去 7 日間)

[管理者] エリアには、サイトへのアクセスを付与された管理者が一覧表示されており、また、閲覧のみ権限がある管理者が一覧表示されています。管理者権限レベルの詳細については、「*111{/u}{/color} ページの「サイト管理者権限の更新」*」を参照してください。

[アクション] エリアには以下が含まれます。

- 保護を一時停止したり再開したりする機能について詳細は、「*88{/u}{/color} ページの「サイト保護の一時停止および再開」*」を参照してください。
- サイトを無効にする機能について詳細は、「*91{/u}{/color} ページの「サイトの保護を非アクティブ化」*」を参照してください。

[詳細] タブ

このタブから、次の情報を表示または編集できます。

- サイト / 会社名
- キーコード
- サイトの種類 (内部または外部)。
- サイトに関するコメント。これは自由形式フィールドです。
- サイトを作成した人物の名前。
- サイトをタグでフィルタリングします。

詳細については、「*94{/u}{/color} ページの「サイトの詳細を編集」*」と「*102{/u}{/color} ページの「サイトのタグ付け」*」を参照してください。

[権限] タブ

このタブから、管理者に次のいずれかのレベルでサイト権限を設定できます。

- 管理者
- 表示のみ
- アクセスなし

詳細については、「*111{/u}{/color} ページの「サイト管理者権限の更新」*」を参照してください。

[エンドポイント プロテクション] タブ

このタブから、次の設定を表示または編集できます。

- サイトのシート数
- デフォルトのエンドポイント ポリシー
- グローバル オーバーライドおよびグローバル ポリシーの追加
- レポート配信先リストに電子メールを設定
- データ フィルタを設定
  エンドポイント コンソールに直接移動します。
- 詳細については、「*22{/u}{/color} ページの「エンドポイント コンソールへのアクセス」*」を参照してください。

詳細については、「*114{/u}{/color} ページの「サイト設定の編集」*」を参照してください。

[DNS プロテクション] タブ

このタブから、次の操作を実行できます。

- DNS の保護を有効にする
- DNS の保護を30 日間の体験版からフルライセンスにアップグレード
- ポリシーを編集
- ネットワーク設定をアップグレード

詳細については、「DNS 保護のオンライン ガイド」を参照してください。

[セキュリティ意識向上トレーニング] タブ

このタブから、次の操作のいずれかを実行できます。

- セキュリティ意識向上トレーニングを有効化
- セキュリティ意識向上トレーニングを 30 日間の体験版からフル ライセンスにアップグレード

詳細については、「セキュリティ意識向上トレーニング ガイド」を参照してください。

[ダウンロード] タブ

このタブから、キーコードが自動的に設定された Webroot SecureAnywhere のコピーをダウンロードできます。詳細については、「*124{/u}{/color} ページの「Webroot のダウンロード」*」を参照してください。

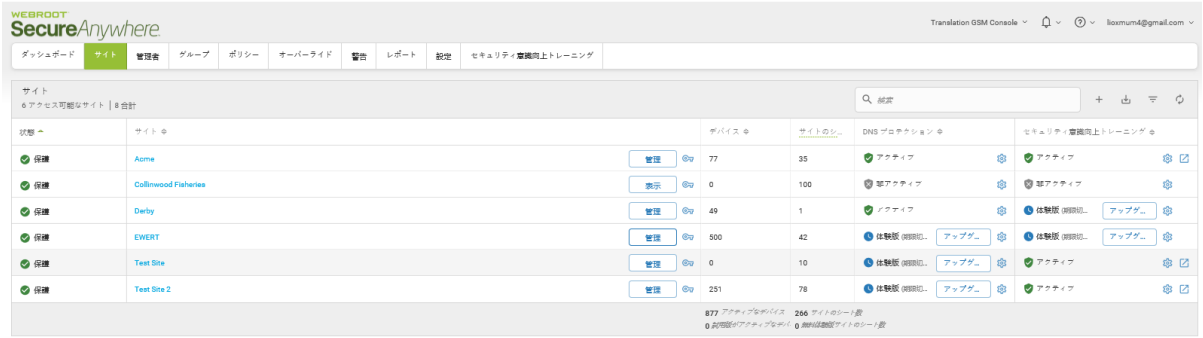
マルチサイトの概要を表示

管理コンソールでは、マルチサイトの配備の概要を確認できます。複数のダッシュボードを同時に表示できるほか、特定のダッシュボードの概要や、特定のサイトに関する追加情報を確認できます。

マルチサイトの概要を表示するには:

1. 管理コンソールにログインします。

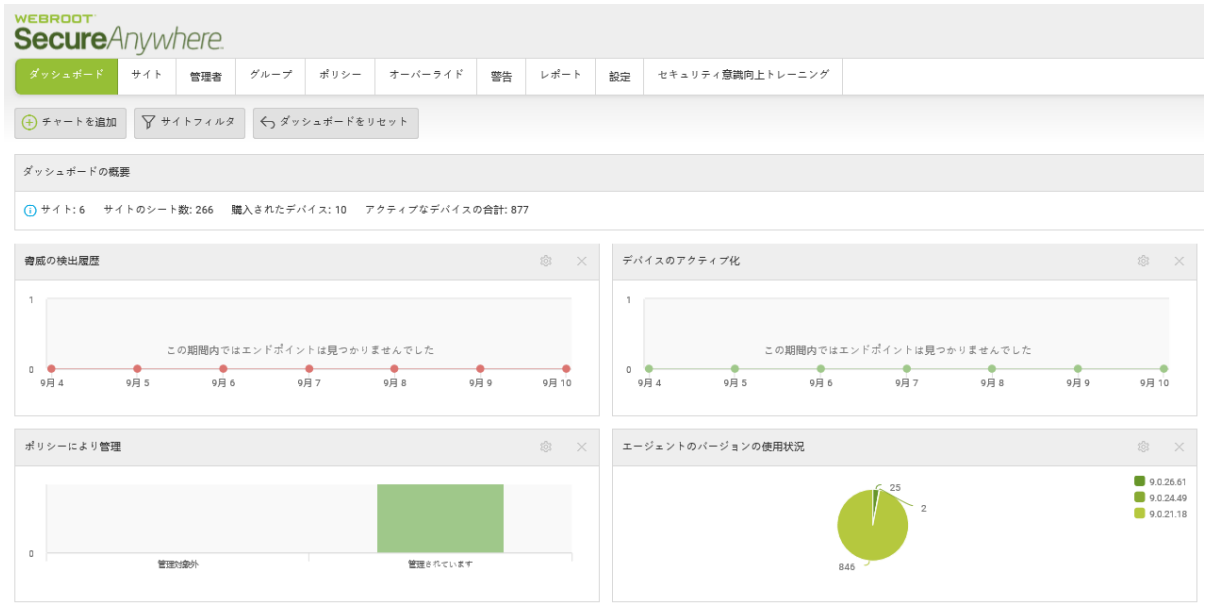
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。



2. [**ダッシュボード**] タブをクリックします。

注意:「脅威の検出履歴」と「デバイスのアクティブ化」のグラフを除き、ダッシュボードの合計では、エージェントのバージョン 8.0.4.134 以降を実行するエンドポイントのみが正確に表示されます。マイグレーションされたキーコードは、このベータ版上のカウントにわずかな異常を引き起こす可能性があります。

[ダッシュボード] タブが表示されます。



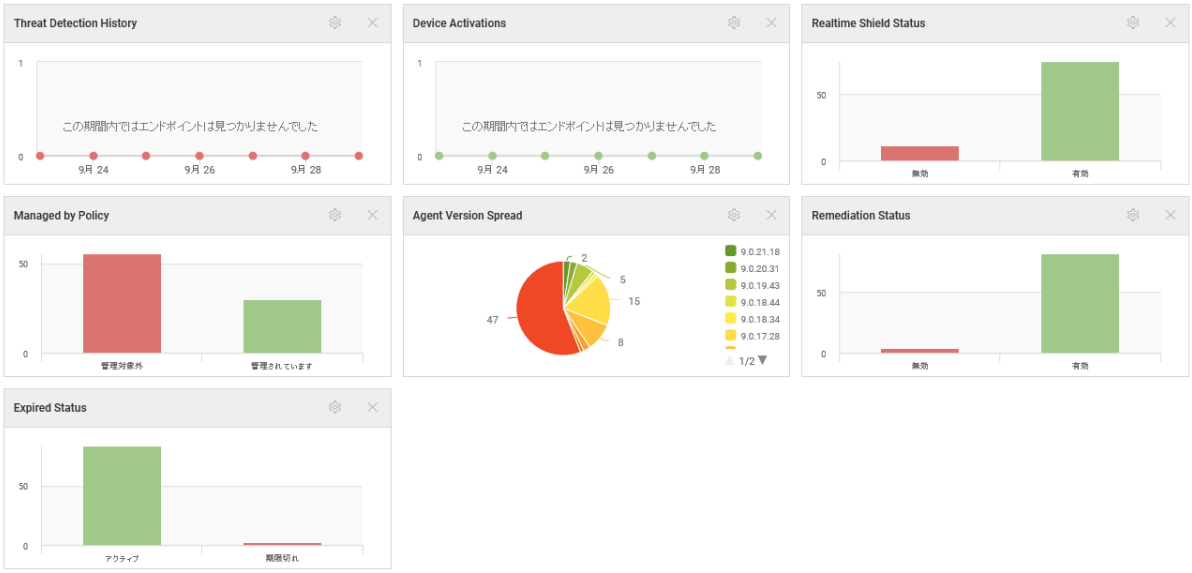
左上に [ダッシュボード概要] バーがあり、全サイトの概要が表示されます。

3. 追加サイト情報を表示するには、[**サイト**] にカーソルを合わせます。

   サイトの概要が表示されます。

[チャート] エリアで、デフォルトで次の各タイプのチャートが表示されます。

- **脅威の検出履歴** - 7 日間に検出されたすべての脅威の履歴。
- **デバイスのアクティブ化** - 7 日間にアクティブ化された新しいデバイスの履歴。
- **ポリシーにより管理** - 管理対象のデバイスと管理対象外のデバイスの数。
- **エージェントのバージョンの使用状況** - WSA エージェント バージョンごとのインストール件数。
- **リアルタイム シールドの状態** - リアルタイム シールドが有効なデバイスと無効なデバイスの数。
- **期限切れの状態** - キーコードが期限切れになっているデバイスの数。
- **対応の状態** - 修復またはクリーンアップ (デフォルトで有効) の状態にあるデバイスの数。



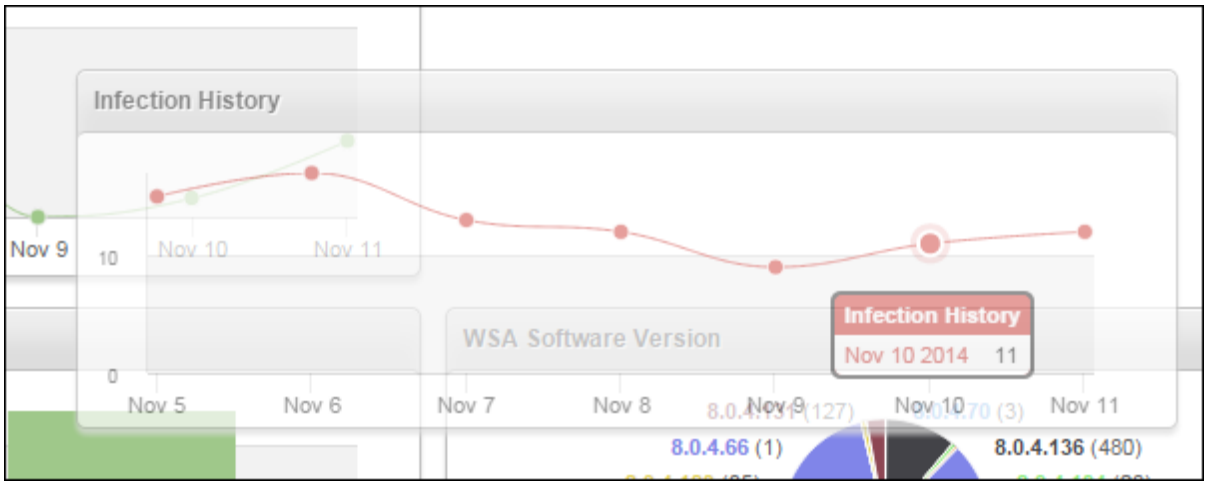
4. ダッシュボードに表示するサイトを設定するには、[**サイトフィルタ**] ボタンをクリックします。

[サイトによりフィルタリング] ウィンドウが表示されます。

5. 以下のいずれかの作業を行ってください。
   - [**すべて**] ラジオボタンを選択してすべてのサイトを表示します。
   - [**サイトの選択**] ラジオボタンを選択して、その後表示されたウィンドウで、表示するサイトを選択します。
     - すべてのサイトを選択するには、[**すべて選択**] ボタンをクリックします。
     - サイトを選択しない場合、[**すべて選択解除**] ボタンをクリックします。

6. 右上で、次のいずれかのトグルボタンをクリックしてダッシュボードのレイアウトを変更します。
   - **1 つのカラム**
   - **2 つのカラム**
   - **3 つのカラム**
   - **4 つのカラム**

7. ダッシュボードをドラッグ アンド ドロップして任意の場所に移動することもできます。



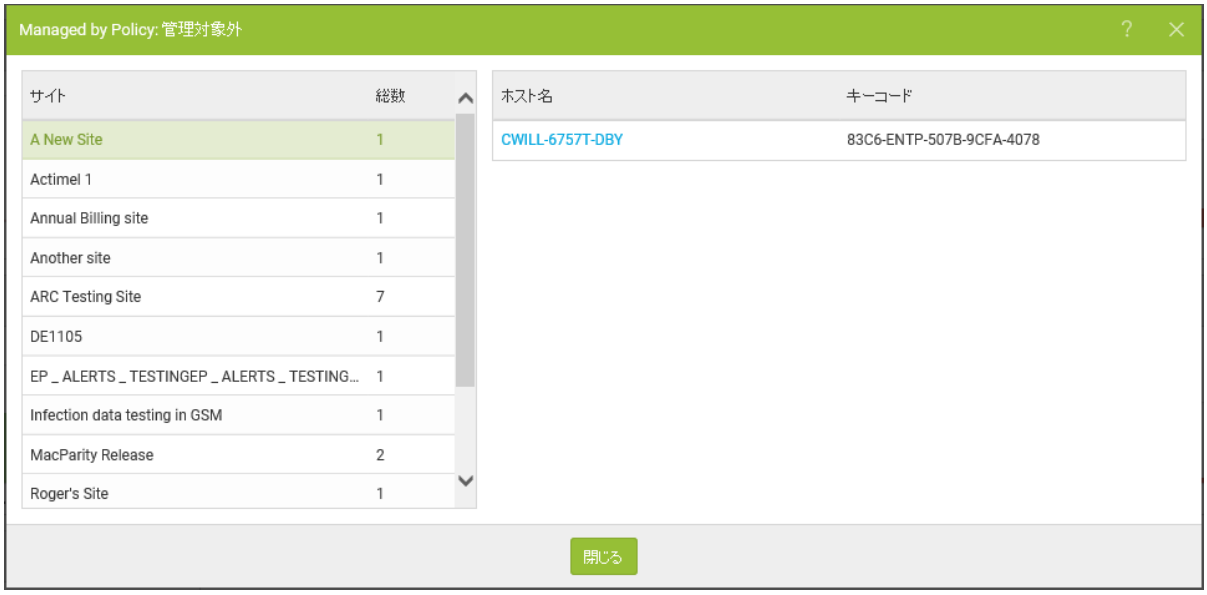
8. ダッシュボードを元の場所に配置するには、[**ダッシュボードをリセット**] ボタンをクリックします。

9. 各サイトの追加情報を表示するには、チャートにカーソルをあてて表示されるウィンドウをクリックします。

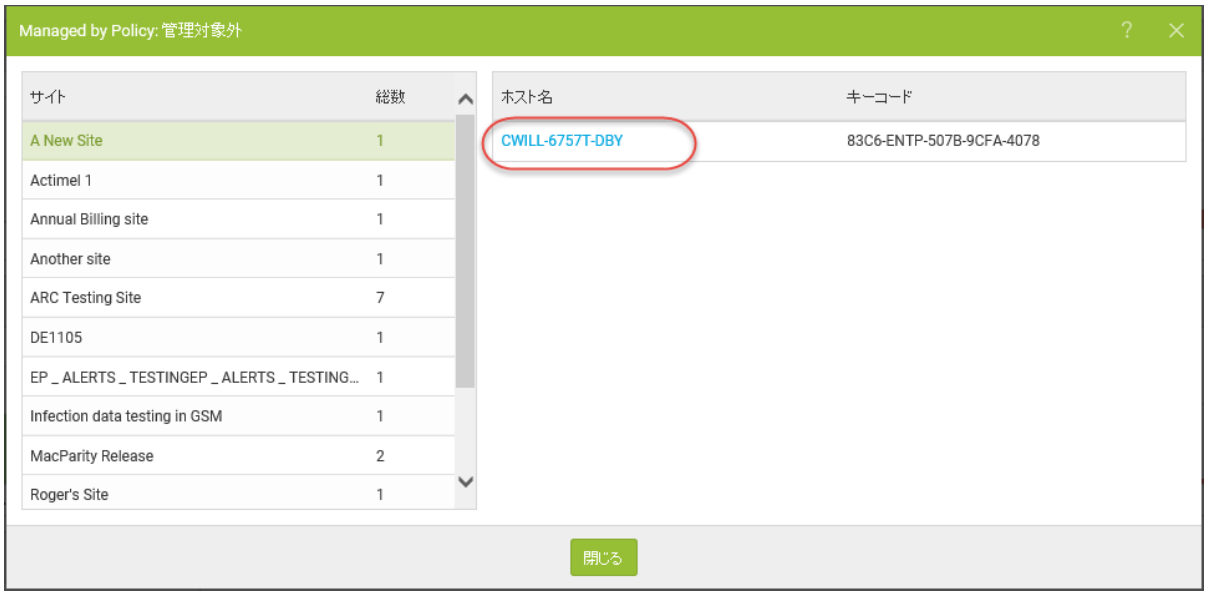
サイトの追加情報が表示されます。

10. 追加情報を表示するには、サイトの名前をクリックします。

ホスト名やキーコード情報が表示されます。

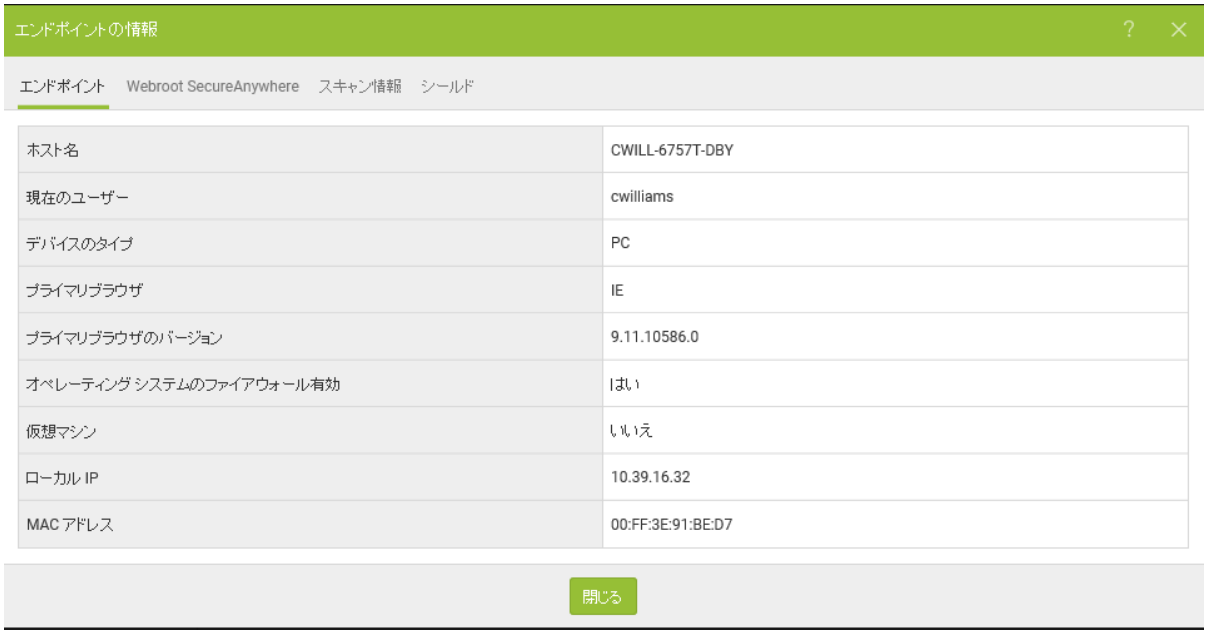


11. [ホスト名] カラムで、リンクをクリックして詳細を表示します。

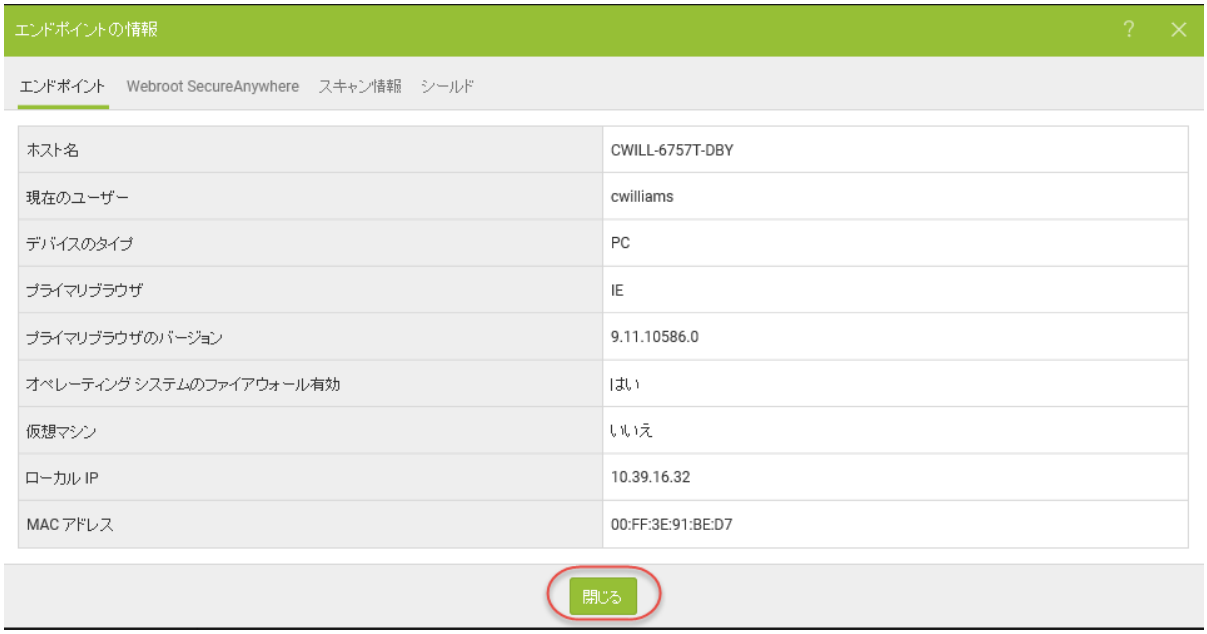


[エンドポイント情報] ウィンドウには、次のタブが表示されます。

- **エンドポイント** - ホスト名、現在のユーザー、デバイスタイプ、内部 IP、MAC アドレスに関する情報を含みます。
- **Webroot SecureAnywhere** - キーコード、バージョン、有効期限、残存日数に関する情報を含みます。
- **スキャン情報** - 最新のスキャン、合計スキャン数、スケジュール済みスキャン時刻に関する情報を含みます。
- **シールド** - 有効にするシールドに関する情報を含みます。



12. 設定が完了したら、[**閉じる**] ボタンをクリックします。



サイト保護の一時停止および再開

あらゆるサイトでサイト保護を一時停止でき、その後、いつでも再開できます。

サイト保護を一時停止または再開するには:

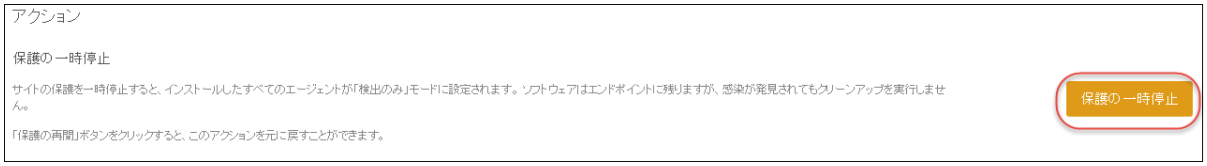
1. 管理コンソールにログインします。

   [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が表示されます。

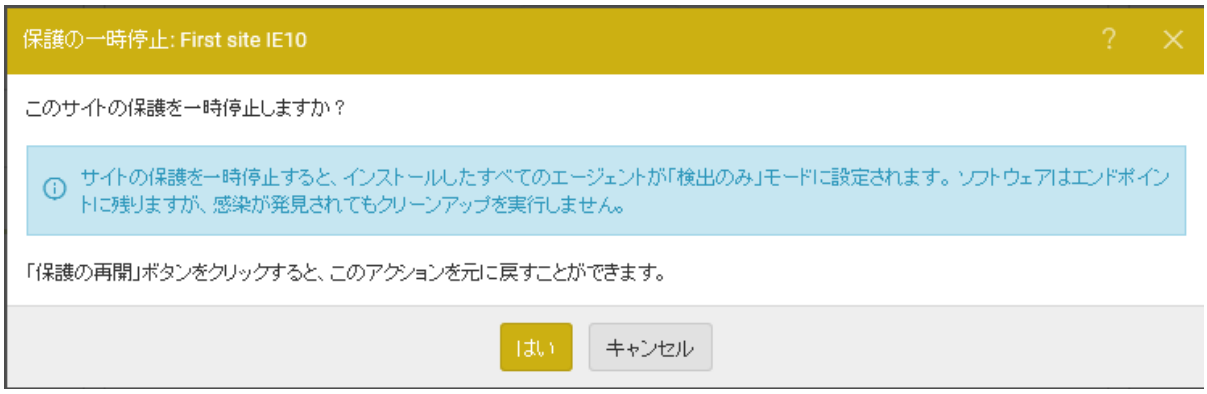
2. 一時停止したいサイトの [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

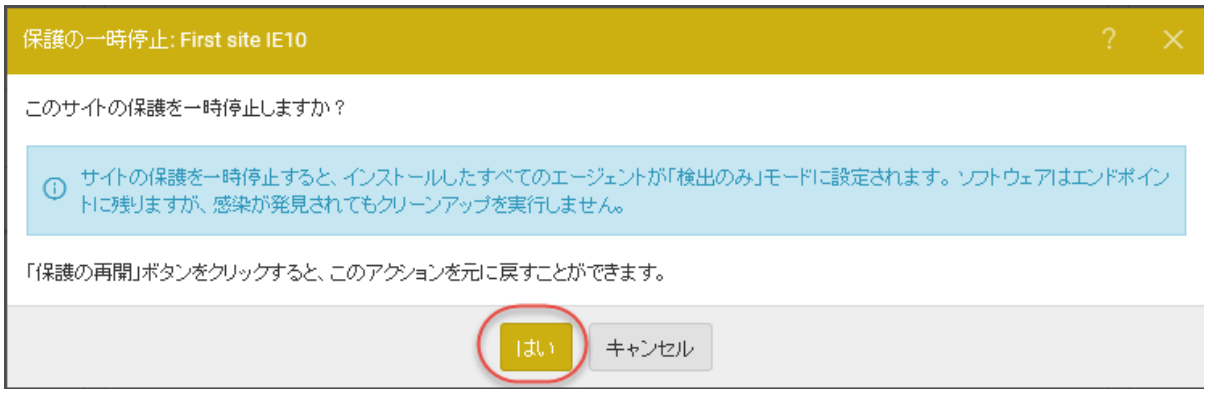
3. サイトの保護を一時停止するには、ページを下方向にスクロールして [**保護の一時停止**] ボタンをクリックします。



保護の一時停止警告メッセージが表示されます。



4. [**はい**] ボタンをクリックして、保護の一時停止に進みます。



サイトが一時停止され、左上に一時停止のアイコンが表示されます。

また、[一時停止] ボタンが [保護の再開] ボタンになります。

5. サイトの保護を再開するには、[**保護の再開**] ボタンをクリックします。

サイトの保護を非アクティブ化

サイトの保護を非アクティブ化するには、次の手順に従ってください。

サイトの保護を非アクティブ化するには:

1. 管理コンソールにログインします。

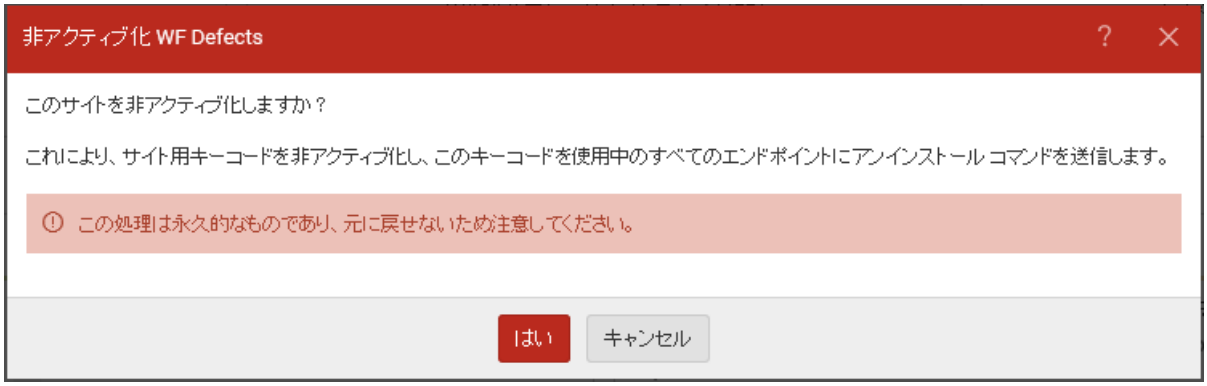
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. 一時停止するサイトの [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

3. 下方向にスクロールして [**非アクティブ化**] ボタンをクリックします。

サイトが非アクティブになり、非アクティブ化警告メッセージが表示されます。



4. [**はい**] ボタンをクリックして継続します。

サイトが非アクティブ化され、サイトのキーコードは失効し、すべてのエンドポイントから Webroot SecureAnywhere がアンインストールされます。

5. 非アクティブになったサイトを表示するには、**サイトの戻る矢印**をクリックして、[**フィルタ**] ボタンをクリックし、[**非アクティブ化**] ボタンを選択します。詳細については、「*63{/u}{/color} ページの「サイトのフィルタリング」*」を参照してください。

サイトの詳細を編集

この手順に従って、サイト名または会社名、シート数などのサイトの詳細を編集したり、サイトに関する情報を追加したりします。

サイトの詳細と編集するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

3. [**詳細**] タブをクリックします。

[詳細] タブが表示されます。


WEBROOT
SecureAnywhere
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
戻る
Acme
保護
概要
詳細
権限
エンドポイント プロテクション
DNS プロテクション
セキュリティ意識向上トレーニング
ダウンロード
サイト / 会社名
Acme
キーコード
サイトの種類
外部企業
社内サイト
会社の規模
次のいずれかを選択してください...
会社の業種
次のいずれかを選択してください...
支払請求サイクル
年1回
支払請求日
1月
1日
コメント
タグ
タグを追加...
追加
変更を保存

4. [サイト / 会社名] フィールドで、必要に応じてサイト名または会社名を更新します。
5. [サイトの種類] エリアで、以下のラジオ ボタンの 1 つを選択します。
   - **外部企業**
   - **社内サイト**

   注意: [社内サイト] ラジオ ボタンを選択した場合は、[会社の規模]、[会社の業種]、[支払請求サイクル]、[支払請求日] フィールドは表示されないため、内容を指定する必要はありません。

6. [会社の規模] フィールドのドロップダウン メニューで、実際の会社の規模に最も近いものを選択してください。
7. [会社の業種] フィールドのドロップダウン メニューでは、実際の業種に最も近いものを選択します。
8. [支払請求サイクル] フィールドのドロップダウン メニューでは、次の支払請求サイクルのいずれかを選択します。
   - **年 1 回**
   - **四半期ごと**
   - **月次**
   - **毎週**
9. [支払請求日] フィールドで、ドロップダウン メニューから支払い請求の月と日を選択します。
10. [コメント] フィールドには、必要に応じてあらゆるコメントやメモを入力します。これは自由形式のフィールドです。
11. [作成者] フィールドで、必要に応じてサイトの作成者を更新します。
12. [タグ] ドロップダウンで、必要な数だけタグを入力します。次のいずれかまたはすべてに基づいてタグを作成することができます。
    - 会社の業種 (医療、建設、輸送など)。
    - タイムゾーン、地理的位置、国、または言語。
    - アカウント マネージャーの名前、IT 担当者の名前、または主な問い合わせ担当者の名前。

    詳細については、「*102{/u}{/color} ページの「サイトのタグ付け」*」を参照してください。

13. 完了したら、[**変更を保存**] ボタンをクリックします。このボタンはタブの最下部にあります。


WEBROOT
SecureAnywhere
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
戻る
Acme
保護
概要
詳細
権限
エンドポイント プロテクション
DNS プロテクション
セキュリティ意識向上トレーニング
ダウンロード
サイト / 会社名
Acme
キーコード
サイトの種類
外部企業
社内サイト
会社の規模
次のいずれかを選択してください...
会社の業種
次のいずれかを選択してください...
支払請求サイクル
年1回
支払請求日
1月
1日
コメント
タグ
タグを追加...
追加
変更を保存

サイトのタグ付け

タグ付け機能を使用して、管理者は、タグと呼ばれる共有属性に基づいてサイトをグループにまとめることができます。タグは各サイトに割り当てられます。

サイトへのタグ付けを行うには:

1. 管理コンソールにログインします。

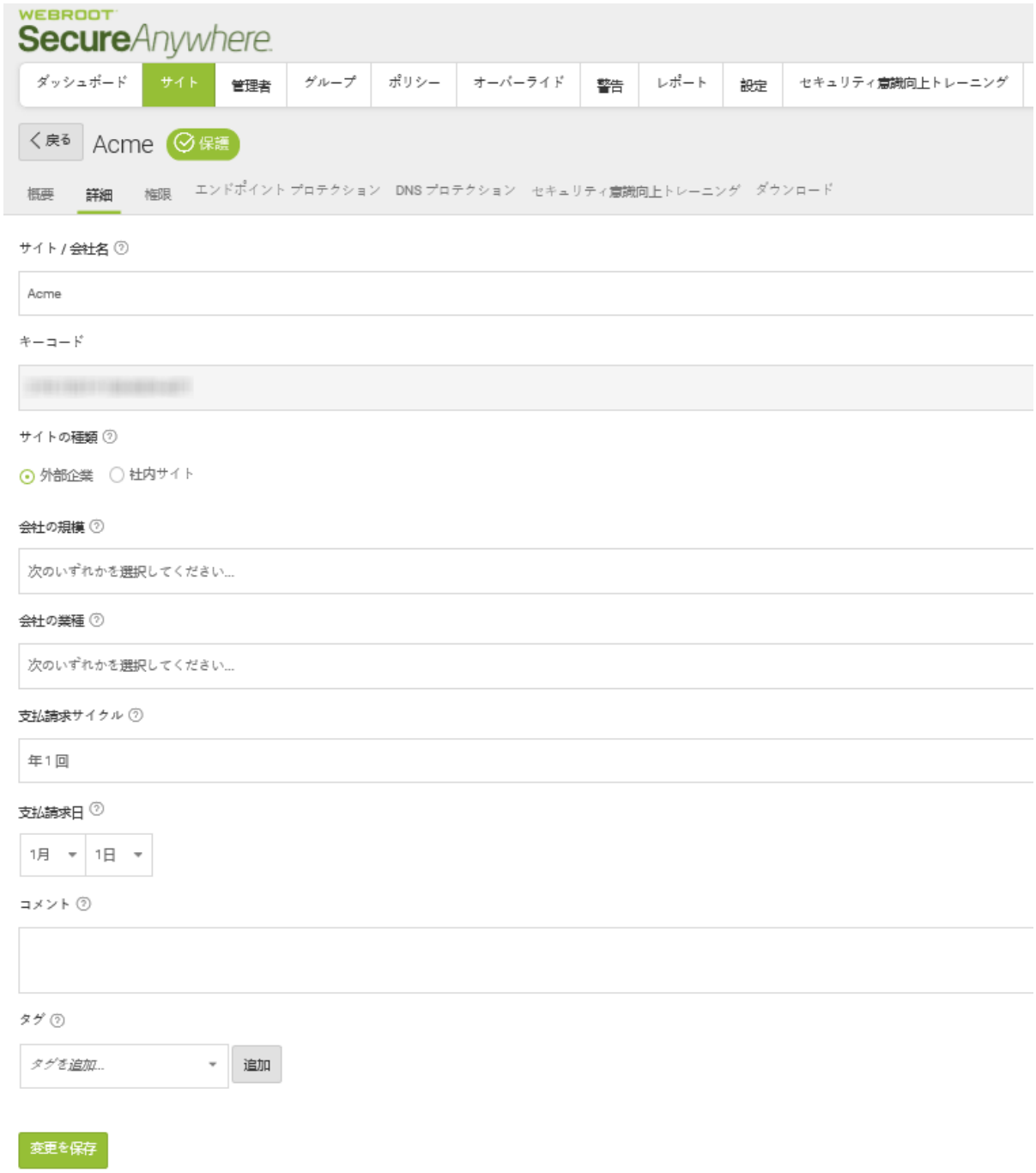
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. タグを追加するサイトを選択して [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

3. [**詳細**] タブをクリックします。

[詳細] タブが表示されます。


WEBROOT
SecureAnywhere
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
戻る
Acme
保護
概要
詳細
権限
エンドポイント プロテクション
DNS プロテクション
セキュリティ意識向上トレーニング
ダウンロード
サイト / 会社名
Acme
キーコード
サイトの種類
外部企業
社内サイト
会社の規模
次のいずれかを選択してください...
会社の業種
次のいずれかを選択してください...
支払請求サイクル
年 1 回
支払請求日
1月
1日
コメント
タグ
タグを追加...
追加
変更を保存

4. [タグ] フィールドで、必要な数だけタグを入力します。

次のいずれかまたはすべてに基づいてタグを作成することができます。

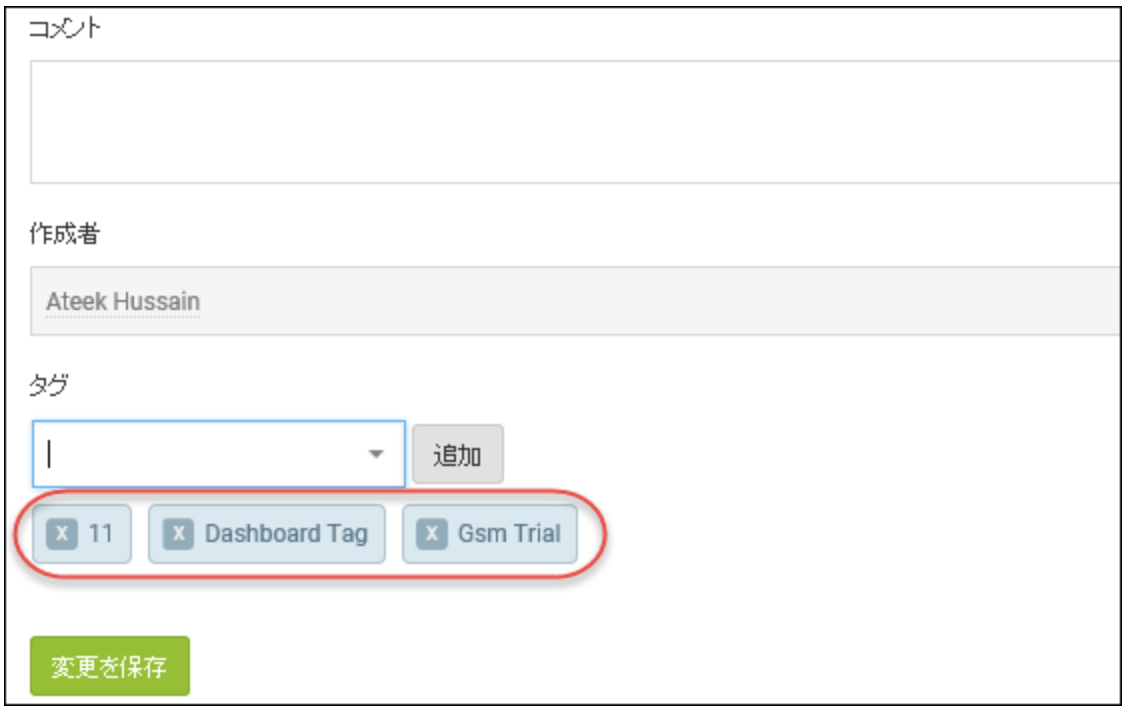
- 会社の業種 (医療、建設、輸送など)。
- タイムゾーン、地理的位置、国、または言語。
- アカウント マネージャーの名前、IT 担当者の名前、または主な問い合わせ担当者の名前。

注意: サイトのタグは必要に応じていくつでも付けることが可能ですが、フィルタリングは 1 つのタグについてのみ実行できます。

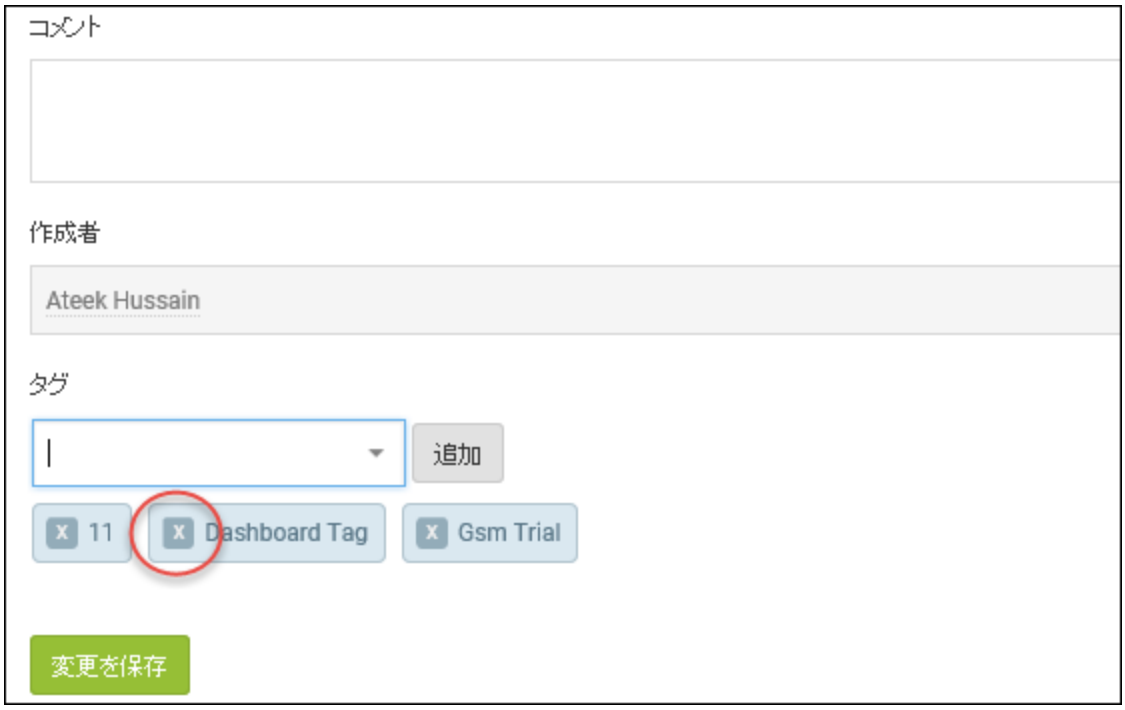
必要に応じて、矢印をクリックして [タグ] ドロップダウン メニューを表示し、以前使用したタグを表示できます。

5. 各タグを追加したら、[**追加**] ボタンをクリックします。

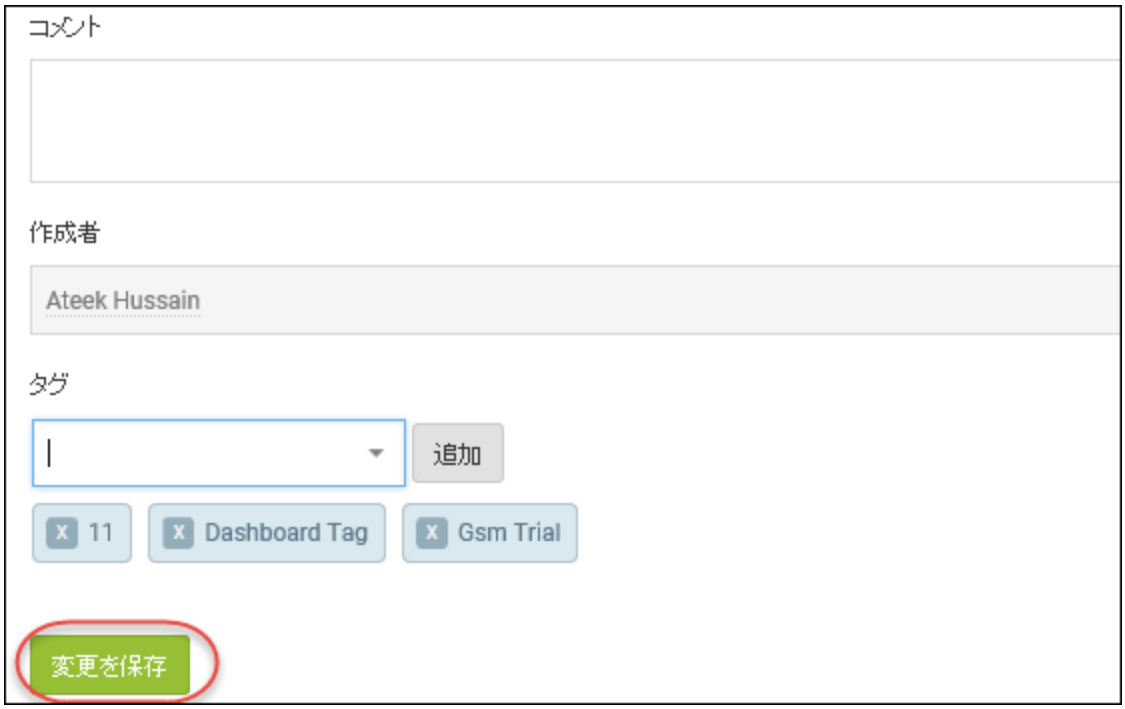
追加されたタグは、[タグ] フィールドの下に表示されます。


コメント
作成者
Ateek Hussain
タグ
追加
11
Dashboard Tag
Gsm Trial
変更を保存

6. タグを削除するには、各タグの左側にある [X] をクリックします。



7. 設定が完了したら、[**変更を保存**] ボタンをクリックします。



サイトにタグ付けした後、この情報を使ってサイトをフィルタリングできます。詳細については、「*63{/u}{/color} ページの「サイトのフィルタリング」*」を参照してください。

サイト管理者権限の更新

サイト管理者権限を更新するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

3. [**権限**] タブをクリックします。

[権限] タブが表示されます。

4. 各管理者に対して、以下のラジオ ボタンの 1 つを選択します。
   - **管理者** - すべてのサイトにアクセスし、管理者の追加、削除、編集をすることができます。
   - **表示のみ** - 管理コンソール サイトの表示のみが可能です。
   - **アクセスなし** - 表示の権限を与えられたサイトを表示することができます。

5. 設定が完了したら、[**変更を保存**] ボタンをクリックします。

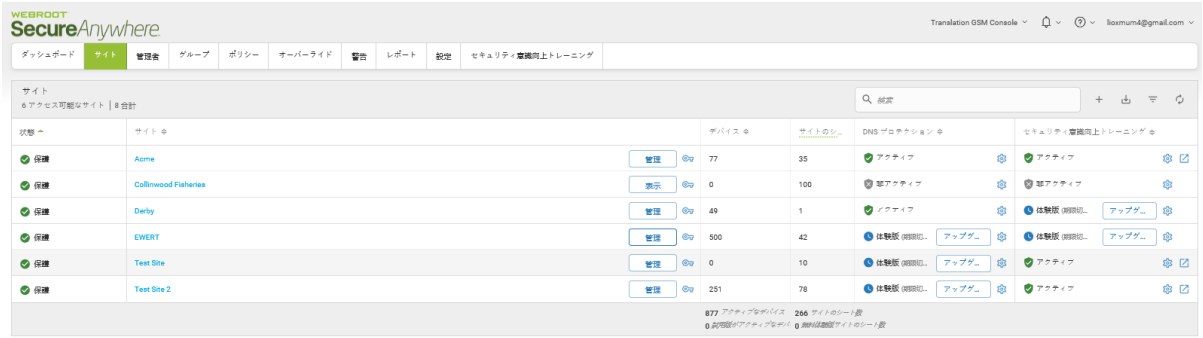
サイト設定の編集

この手順に従って、グローバル ポリシーやグローバル オーバーライド、レポート配信情報、フィルタなど、サイトに関する情報を編集します。

サイトを編集するには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

3. [**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] タブが表示されます。

4. [サイトのシート数] フィールドに、必要に応じてサイトのシート数を入力します。この手順はオプションです。
5. [デフォルトのエンドポイント ポリシー] ドロップダウン メニューで、デフォルトに設定するポリシーをすべて選択します。この手順はオプションです。
6. [グローバルポリシーの追加] チェックボックスについて、以下のいずれか 1 つを実行します。
   - コンソール レベルで作成されたグローバル ポリシーをすべて含めるには、このチェックボックスを選択します。
   - コンソール レベルで作成されたグローバル ポリシーをすべて除外するには、このチェックボックスの選択を解除します。

注意: グローバル ポリシーを含め、一度選択すると、元に戻すことはできません。

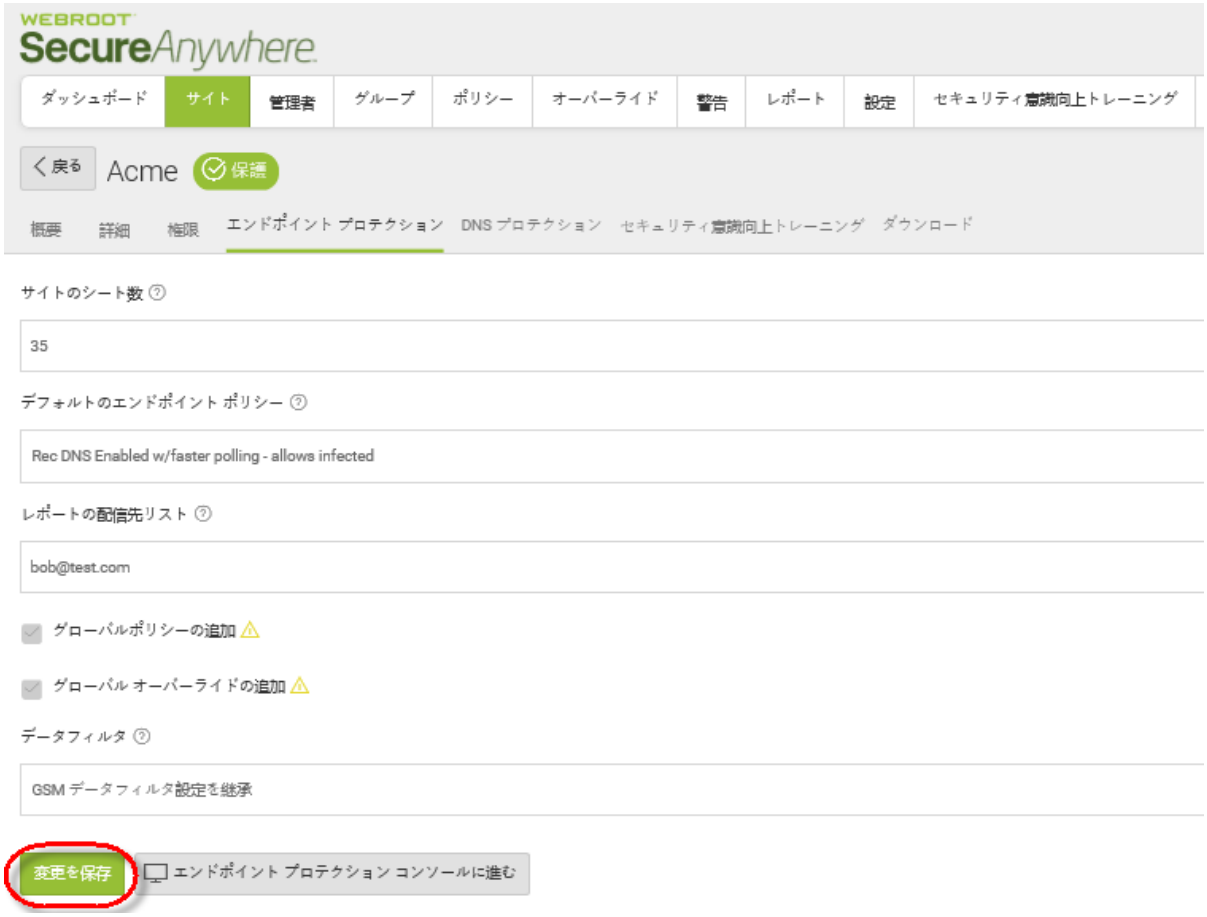
7. [グローバル オーバーライドの追加] チェックボックスについて、以下のいずれか 1 つを実行します。
   - コンソール レベルで作成されたグローバル オーバーライドをすべて含めるには、このチェックボックスを選択します。
   - コンソール レベルで作成されたグローバル オーバーライドをすべて除外するには、このチェックボックスの選択を解除します。

   注意: グローバル オーバーライドを含め、一度選択すると、元に戻すことはできません。

8. [レポートの配信先リスト] フィールドで、レポートを送信する相手の電子メールアドレスを入力します。レポートの詳細については、「*396{/u}{/color} ページの「グローバル サイト マネージャー レポート概要」*」を参照してください。
9. [データ フィルタ] フィールドのドロップダウン メニューで、フィールドをフィルタする設定を選択し、サイトをフィルタリングするデータを入力します。

   詳細については、「*119{/u}{/color} ページの「サイト レベルのデータ フィルタの設定」*」と「*63{/u}{/color} ページの「サイトのフィルタリング」*」を参照してください。

10. 設定が完了したら、[**変更を保存**] ボタンをクリックします。



サイト レベルのデータ フィルタの設定

サイトレベルのデータ フィルタを使用して、データ フィルタをサイトレベルで作成します。マスター設定で選択可能な同じ期間のオプションとともに、特定のサイトについて強制的にマスター設定を適用する追加オプションを選択することができます。

サイト設定の詳細については、「*114{/u}{/color} ページの「サイト設定の編集」*」を参照してください。

サイトレベルのデータフィルタを設定するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. サイトリスト内で、データ フィルタを設定するサイトの [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

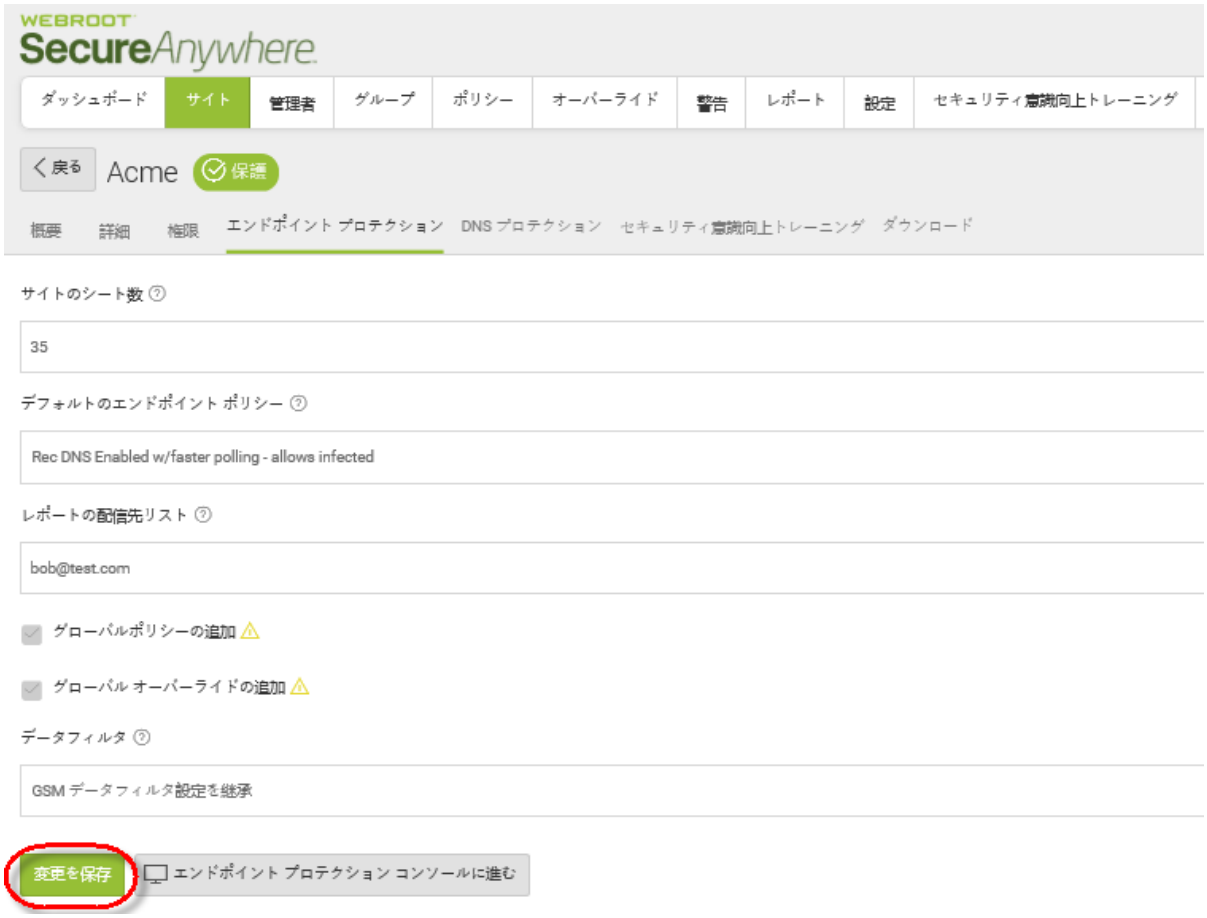
3. [**エンドポイント プロテクション**] タブをクリックします。

[エンドポイント プロテクション] タブが表示されます。

4. [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。
   - **GSM データフィルタ設定を継承**
   - **すべてのデータを表示 (デフォルト設定)**
   - **1 か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 か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 か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 か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 か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**

注意: 限定管理者権限は、サイトを編集する際に [設定] タブへのアクセス権が付与されるようアップデートされました。ここでは、デフォルトのサイト ポリシー、データ フィルタの設定、レポートの配信先リストを変更することができます。

5. 設定が完了したら、[**変更を保存**] ボタンをクリックします。



システムの設定がアップデートされます。

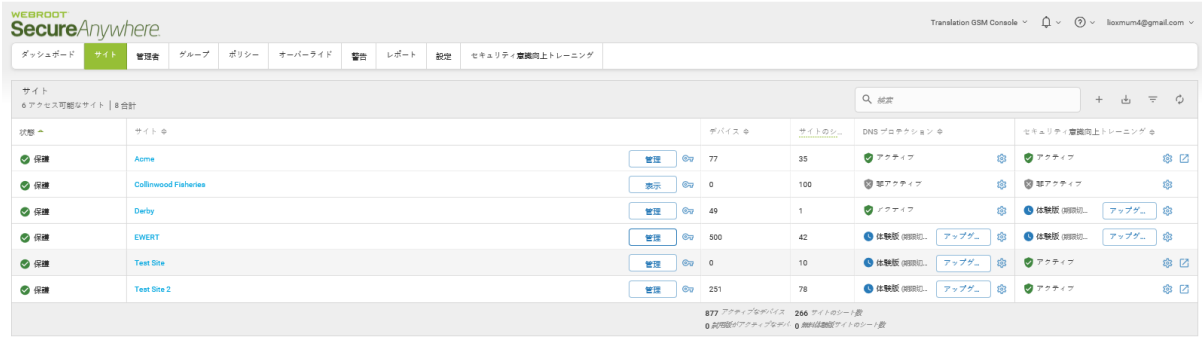
Webroot のダウンロード

選択したデバイスに Webroot SecureAnywhere ソフトウェアを素早く簡単に配備するには、次の手順に従います。

Webroot をダウンロードするには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**管理**] ボタンをクリックします。

   [概要] タブがアクティブな状態で [サイトの管理] パネルが表示されます。

3. [**ダウンロード**] ボタンをクリックします。

[ダウンロード] タブが表示されます。

4. 以下のいずれかを実行します。
   - Windows PC デバイス向けの Webroot をダウンロードするには、[Windows PC 用ダウンロード] カラムで、[**ダウンロード**] リンクをクリックします。
   - Apple Mac デバイス向けの Webroot をダウンロードするには、[Apple Mac 用ダウンロード] カラムで、[**ダウンロード**] リンクをクリックします。
5. ダウンロードしたファイルを実行します。エンドポイントがコンソールに自動的に報告を行います。

第 4 章: 管理者の操作

管理者の追加

異なるサイトに管理者を追加することができます。

管理者を追加するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**管理者**] タブをクリックします。

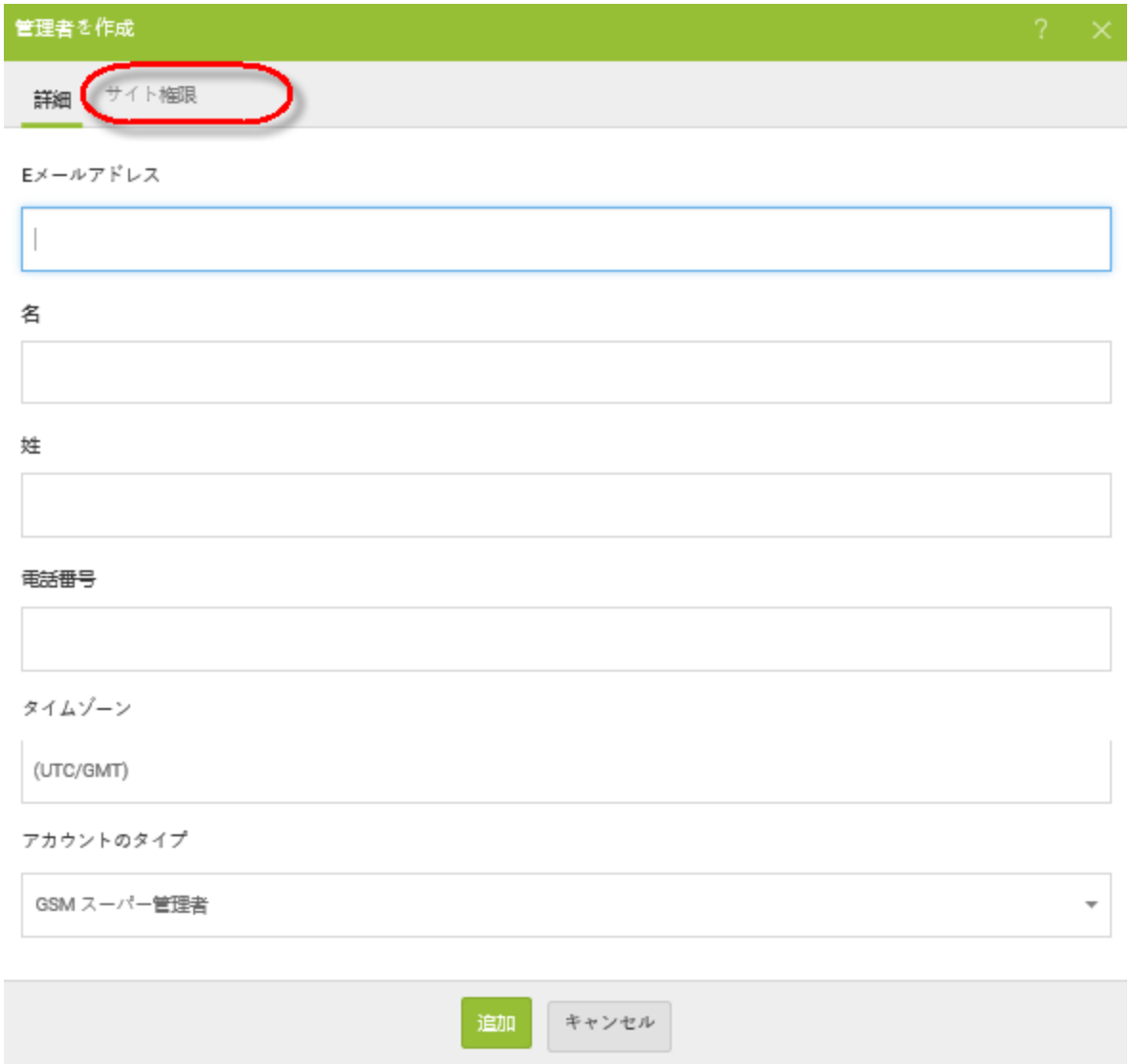
   [管理者] タブが表示されます。

3. [**追加**] ボタンをクリックします。

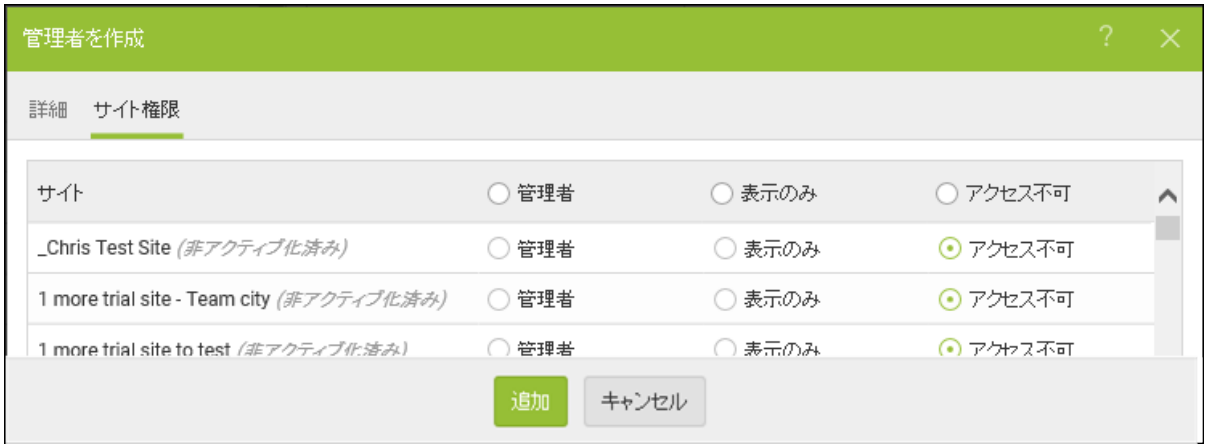
[管理者を作成] ウィンドウが表示されます。

4. [電子メール] フィールドに、追加する管理者の電子メールアドレスを入力します。
5. [名] フィールドに、追加する管理者の名を入力します。
6. [姓] フィールドに、追加する管理者の姓を入力します。
7. [電話番号] フィールドに、追加する管理者の電話番号を入力します。
8. [タイムゾーン] フィールドで**鉛筆**のアイコンをクリックし、追加する管理者の適切なタイムゾーンに該当する国、地域、または主要都市を入力します。

9. [アカウントのタイプ] フィールドで、ドロップダウン メニューから次のいずれかのオプションを選択します。
   - **GSM スーパー管理者** - すべてのサイトにアクセスし、管理者の追加、削除、編集することができます。
   - **GSM 限定管理者** - サイトの表示のみを行うことができます。管理者を追加、削除、または編集することはできません。
   - **サイト管理者のみ (GSM アクセス不可)** - 表示の権限を与えられたサイトを表示することができます。
10. [**サイト権限**] タブをクリックします。



システムに [サイト権限] タブが表示されます。



11. 各サイトについて、次の権限レベルのいずれかを選択します。
    - **管理者**
    - **表示のみ**
    - **アクセス不可**
12. 設定が完了したら [**追加**] ボタンをクリックします。

管理者情報の更新

管理者情報を更新するには、以下の手順に従ってください。以下の*111{/u}{/color} ページの「サイト管理者権限の更新」*の手順に従って、管理者権限を更新することもできます。

管理者の操作を行うには:

1. 管理コンソールにログインします。

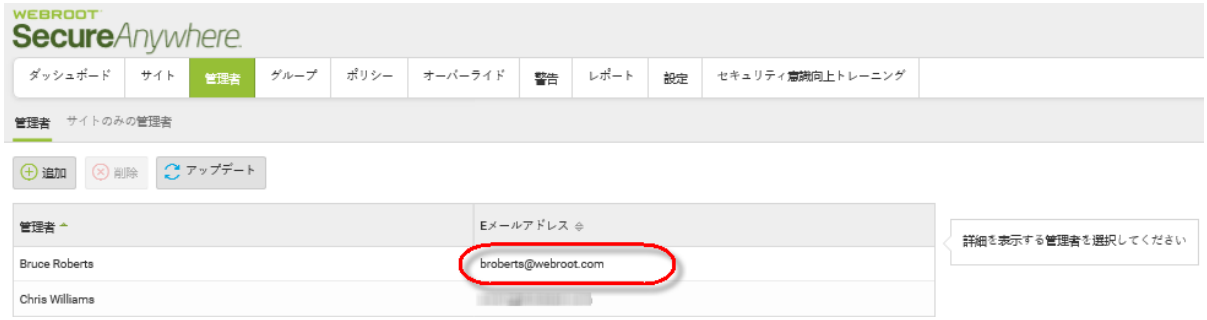
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**管理者**] タブをクリックします。

   次の情報とともに [管理者] パネルが表示されます。

- **名前** - 管理者の名前。
- **電子メール** - 管理者の電子メールアドレス。

3. 追加の管理者情報を表示するには、管理者をダブルクリックします。



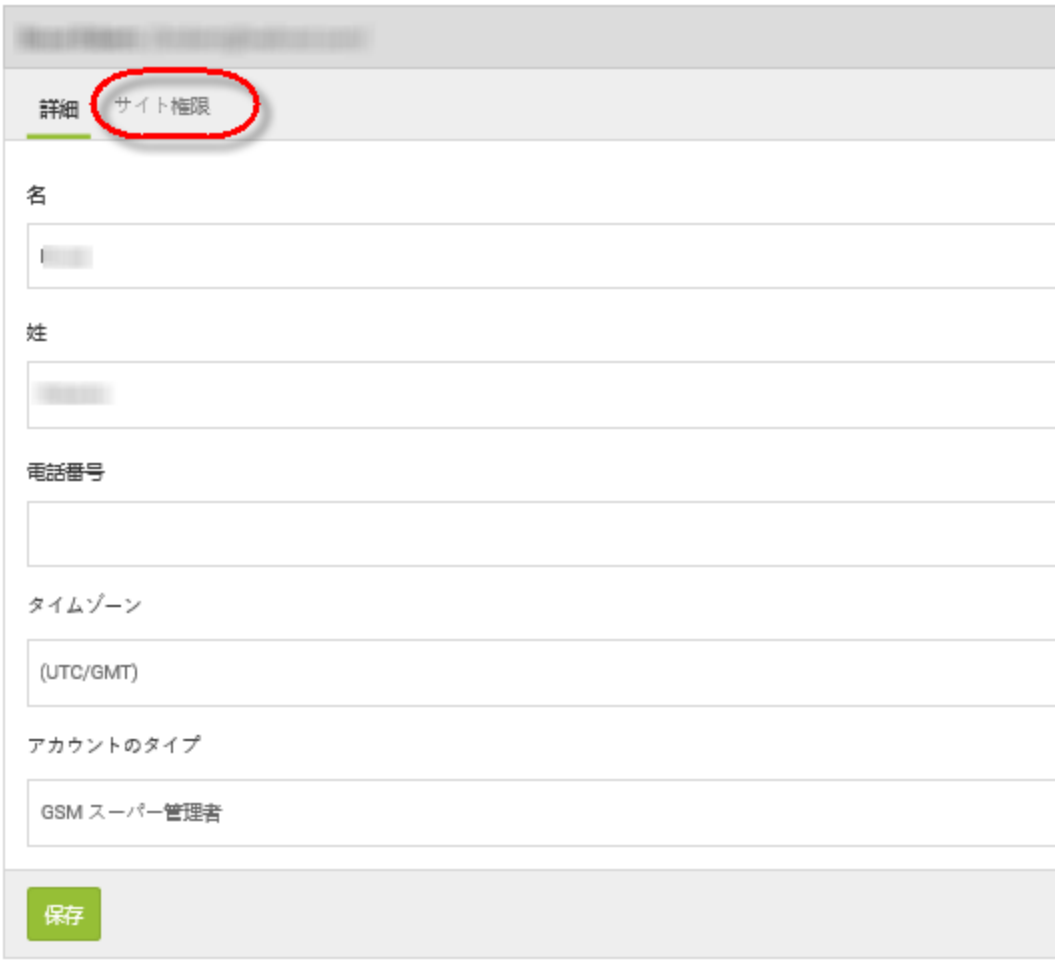
[詳細] タブに管理者情報が表示されます。

4. [詳細] パネルでは、次の項目を表示および編集できます。
   - **名** - フィールドは編集可能です。
   - **姓** - このフィールドは編集可能です。
   - **電話番号** - このフィールドは編集可能です。
   - **タイムゾーン** - 鉛筆のアイコンをクリックして情報を編集します。
   - **アカウントのタイプ** - ドロップダウン メニューから次のいずれかを選択します。
     - **GSM スーパー管理者** - すべてのサイトにアクセスし、管理者の追加、削除、編集することができます。
     - **GSM 限定管理者** - サイトの表示のみを行うことができますが、管理者を追加、削除、または編

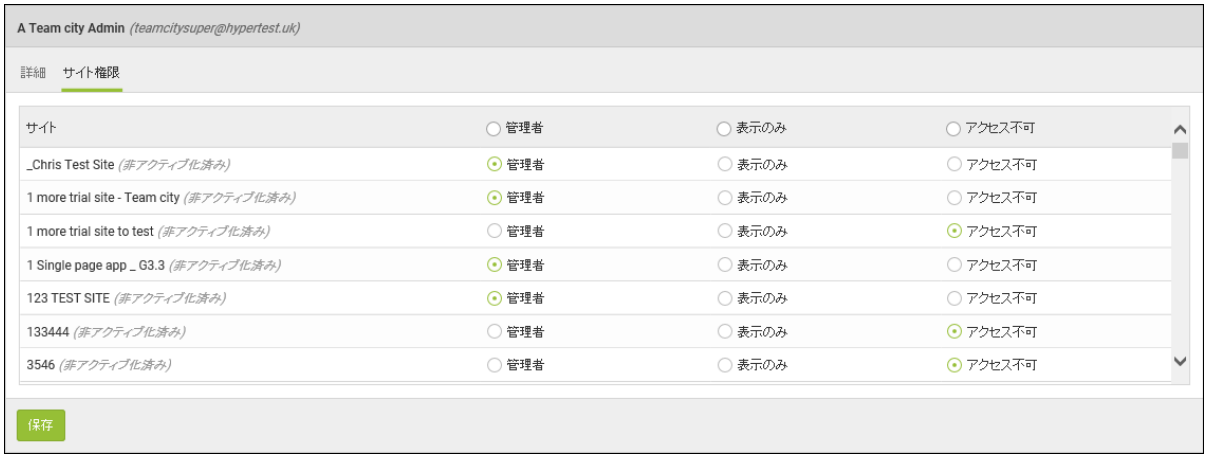
集することはできません。

- **アクセスなし** - 表示の権限を与えられたサイトを表示することができます。

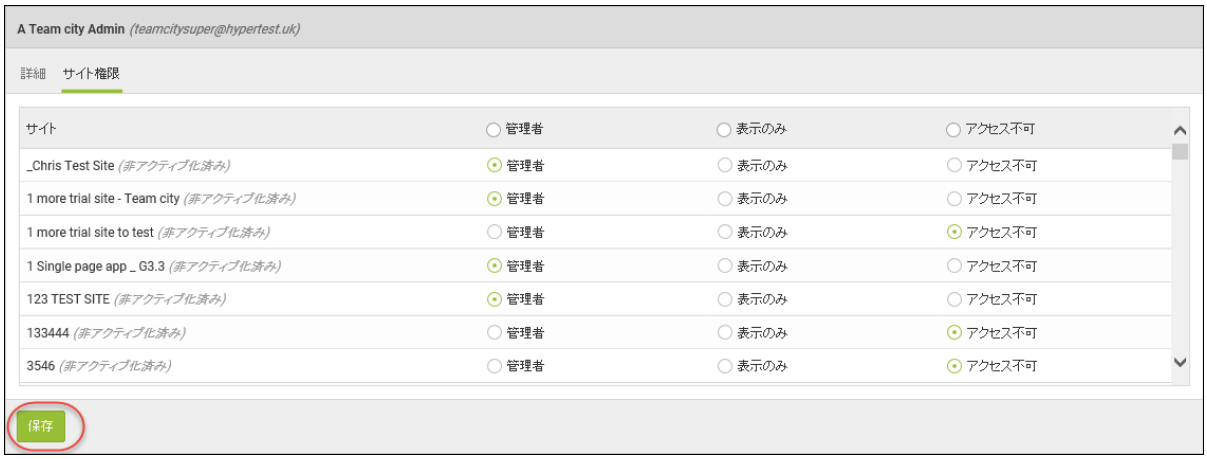
5. [詳細] タブで情報を表示して編集が完了したら、[**サイト権限**] タブをクリックします。



システムに [サイト権限] タブが表示されます。



6. 各サイトについて、次の権限レベルのいずれかを選択します。
   - **管理者**
   - **表示のみ**
   - **アクセス不可**
7. 設定が完了したら [**保存**] ボタンをクリックします。



管理者の削除

この手順に従って、システムから管理者を削除します。

管理者を削除するには:

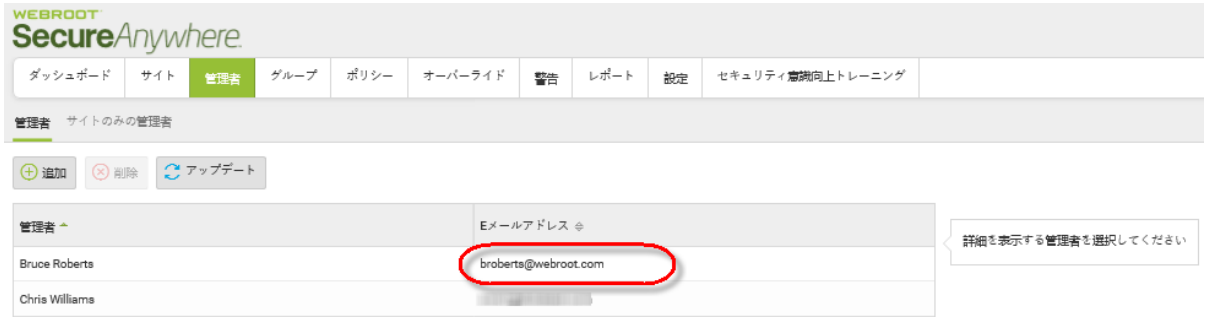
1. 管理コンソールにログインします。

   [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が表示されます。

2. [**管理者**] タブをクリックします。

   [管理者] タブが表示されます。

3. 管理者の詳細を表示するには、その管理者の電子メールアドレスをダブルクリックします。



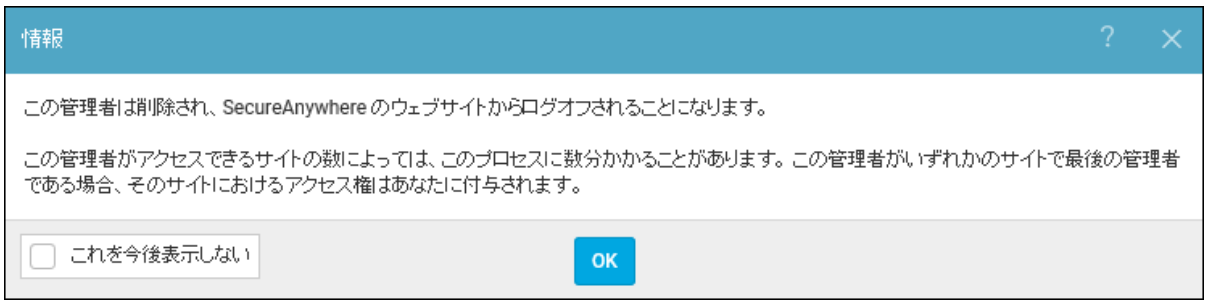
管理者の詳細が表示され、[削除] ボタンがアクティブになります。

4. [**削除**] ボタンをクリックします。

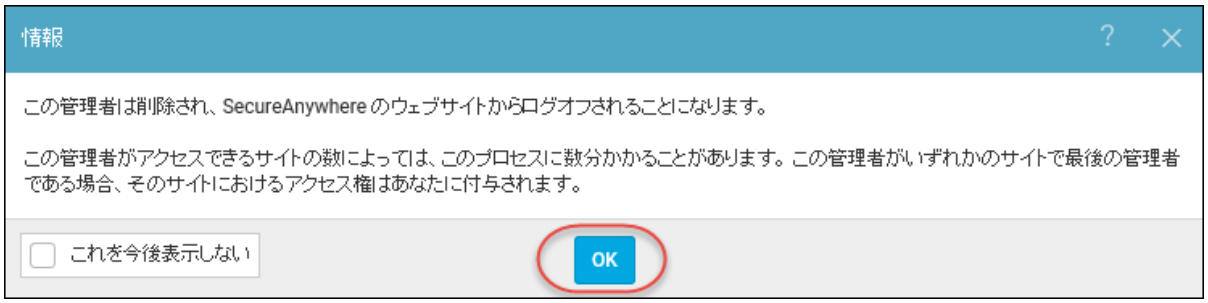
警告メッセージが表示されます。

5. [**削除の確認**] ボタンをクリックします。

情報メッセージが表示されます。



6. [**OK**] ボタンをクリックします。



管理者がシステムから削除されます。

管理コンソール管理者権限について

次の各表で、管理コンソールとエンドポイント プロテクション コンソールの両方に関するさまざまな管理者権限について説明します。

- 管理コンソール プラットフォーム - 管理コンソールへのアクセス
- 管理コンソール プラットフォーム - 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
- SecureAnywhere プラットフォーム - 管理者レベル - エンドポイント プロテクション
- SecureAnywhere プラットフォーム - 基本レベル - エンドポイント プロテクション
- SecureAnywhere プラットフォーム - アクセス不可レベル - エンドポイント プロテクション

注意: アスタリスク (*) が付いている管理者権限は設定可能です。

管理コンソール プラットフォーム - 管理コンソールへのアクセス

スーパー管理者	限定管理者	サイトのみ
ダッシュボード - 可	ダッシュボード - 可	ダッシュボード - アクセス不可
サイト ページ - 可*	サイト ページ - 可*	サイト ページ - アクセス不可
管理者 - 可	管理者 - 表示のみ	管理者 - アクセス不可
グループ - 可	グループ - 可	グループ - アクセス不可
ポリシー - 可	ポリシー - 不可	ポリシー - アクセス不可

スーパー管理者	限定管理者	サイトのみ
オーバーライド - 可	オーバーライド - 不可	オーバーライド - アクセス不可
警告 - 可	警告 - 不可	警告 - アクセス不可
コマンド - 該当なし	コマンド - 該当なし	コマンド - アクセス不可
レポート - 可	レポート - 可	レポート - アクセス不可
DNS - 可	DNS - 可	DNS - 不可
WSAT - 可	WSAT - 可	WSAT - 可
設定 - 可	設定 - 不可	設定 - アクセス不可
ログ - 該当なし	ログ - 該当なし	ログ - アクセス不可
リソース - 該当なし	リソース - 該当なし	リソース - アクセス不可
ダウンロード - 可	ダウンロード - 可	ダウンロード - アクセス不可

管理コンソール プラットフォーム - 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

スーパー管理者	限定管理者	サイトのみ
ダッシュボード - 可	ダッシュボード - 可	ダッシュボード - 可
サイト ページ - 可*	サイト ページ - 可*	サイト ページ - 該当なし
管理者 - 可	管理者 - 可	管理者 - 可
グループ - 可*	グループ - 可*	グループ - 可*
ポリシー - 可*	ポリシー - 可*	ポリシー - 可*
オーバーライド - 可*	オーバーライド - 可*	オーバーライド - 可*
警告 - 可*	警告 - 可*	警告 - 可*
コマンド - 可*	コマンド - 可*	コマンド - 可*
レポート - 可	レポート - 可	レポート - 可
DNS - 不可	DNS - 不可	DNS - 不可
WSAT - 可	WSAT - 可	WSAT - 可
設定 - 可	設定 - 可	設定 - 可

スーパー管理者	限定管理者	サイトのみ
ログ - 可	ログ - 可	ログ - 可
リソース - 可	リソース - 可	リソース - 可
ダウンロード - 可	ダウンロード - 可	ダウンロード - 可

SecureAnywhere プラットフォーム - 管理者レベル - エンドポイント プロテクション

管理者	基本	アクセス不可
状態 - 可	状態 - 可	状態 - 可
管理者 - 可	管理者 - 可	管理者 - 可
グループ - 可*	グループ - 表示のみ	グループ - 不可
ポリシー - 可*	ポリシー - 表示のみ	ポリシー - 不可
オーバーライド - 可*	オーバーライド - 不可	オーバーライド - 不可
警告 - 可*	警告 - 不可	警告 - 不可
コマンド - 可*	コマンド - 不可	コマンド - 不可

管理者	基本	アクセス不可
レポート - 可	レポート - 可	レポート - 不可
DNS - 不可	DNS - 不可	DNS - 不可
WSAT - 可	WSAT - 可	WSAT - 不可
設定 - 可	設定 - 表示のみ	設定 - 不可
ログ - 可	ログ - 可	ログ - 不可
リソース - 可	リソース - 可	リソース - 不可
ダウンロード - 可	ダウンロード - 可	ダウンロード - 可

SecureAnywhere プラットフォーム - 基本レベル - エンドポイント プロテクション

管理者	基本	アクセス不可
状態 - 可	状態	状態 - 不可
管理者 - 不可	管理者 - 不可	管理者 - 不可
グループ - 可*	グループ - 表示のみ	グループ - 不可
ポリシー - 可*	ポリシー - 表示のみ	ポリシー - 不可

管理者	基本	アクセス不可
オーバーライド - 可*	オーバーライド - 不可	オーバーライド - 不可
警告 - 可*	警告 - 不可	警告 - 不可
コマンド - 可*	コマンド - 不可	コマンド - 不可
レポート - 可	レポート - 可	レポート - 不可
DNS - 不可	DNS - 不可	DNS - 不可
WSAT - 可	WSAT - 不可	WSAT - 不可
設定 - 可	設定 - 表示のみ	設定 - 不可
ログ - 可	ログ - 可	ログ - 不可
リソース - 可	リソース - 可	リソース - 不可
ダウンロード - 可	ダウンロード - 可	ダウンロード - 不可

SecureAnywhere プラットフォーム - アクセス不可レベル - エンドポイント プロテクション

管理者	基本	アクセス不可
状態 - 不可	状態 - 不可	状態 - 不可
管理者 - 不可	管理者 - 不可	管理者 - 不可
グループ - 不可	グループ - 不可	グループ - 不可
ポリシー - 不可	ポリシー - 不可	ポリシー - 不可
オーバーライド - 不可	オーバーライド - 不可	オーバーライド - 不可
警告 - 不可	警告 - 不可	警告 - 不可
コマンド - 不可	コマンド - 不可	コマンド - 不可
レポート - 不可	レポート - 不可	レポート - 不可
DNS - 不可	DNS - 不可	DNS - 不可
WSAT - 不可	WSAT - 不可	WSAT - 不可
設定 - 不可	設定 - 不可	設定 - 不可
ログ - 不可	ログ - 不可	ログ - 不可

管理者	基本	アクセス不可
リソース - 不可	リソース - 不可	リソース - 不可
ダウンロード - 不可	ダウンロード - 不可	ダウンロード - 不可

第 5 章: グループの操作

グループを操作するには、次のトピックを参照してください:

グループの追加

初めてエンドポイントに配備する際は、システムによっ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。

グループを追加するには:

1. 管理コンソールにログインします。

   [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が表示されます。

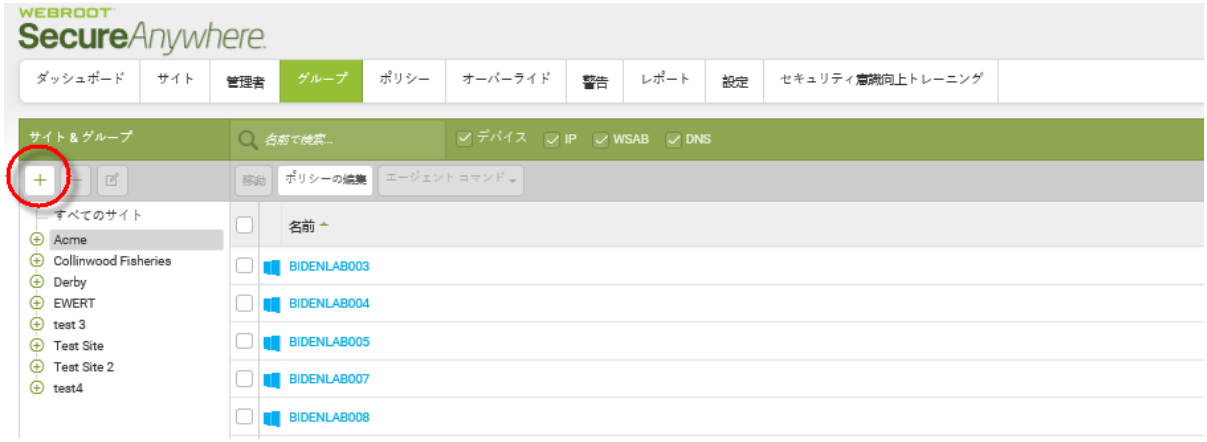
2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. 左のカラムで、このグループを追加する先のサイトを選択します。

[プラス記号 (+)] ボタンがアクティブになります。

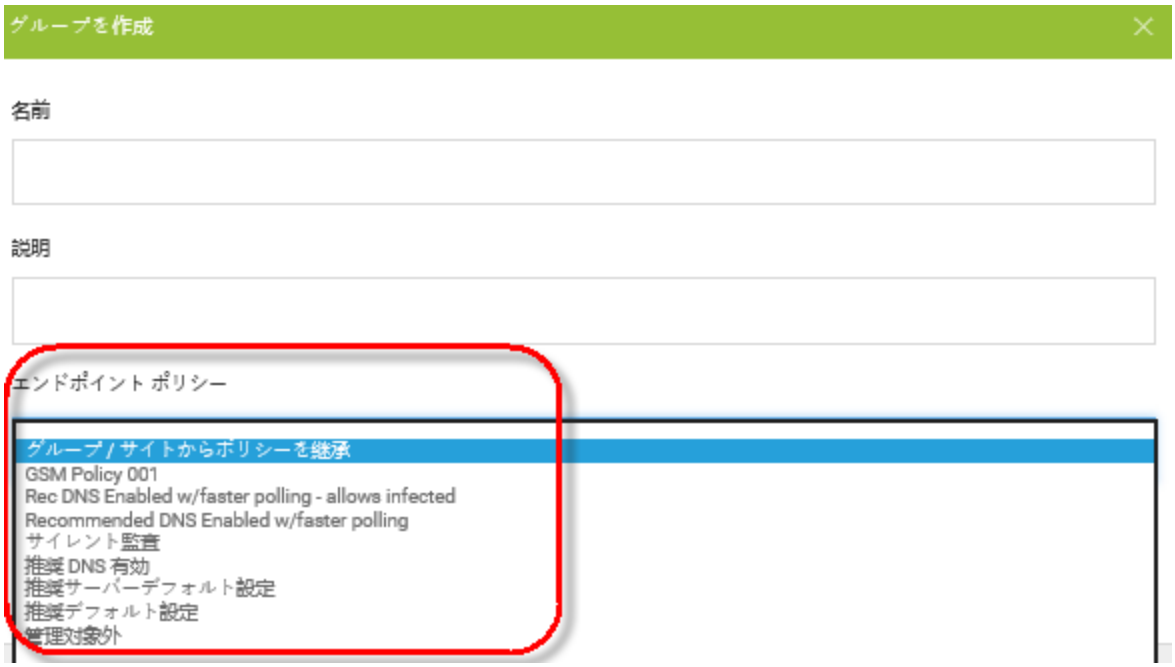
4. [**プラス記号** (+)] ボタンをクリックします。



[グループを作成] ウィンドウが表示されます。

5. [名前] フィールドにグループの名前を入力します。
6. [説明] フィールドにグループについての簡単な説明を入力します。

7. [エンドポイント ポリシー] ドロップダウン メニューで、次のポリシーのいずれかを選択します:
   - **ポリシーなし**
   - **推奨デフォルト設定**
   - **推奨サーバー デフォルト設定**
   - **サイレント監査**
   - **管理対象外**



8. [**作成**] ボタンをクリックします。

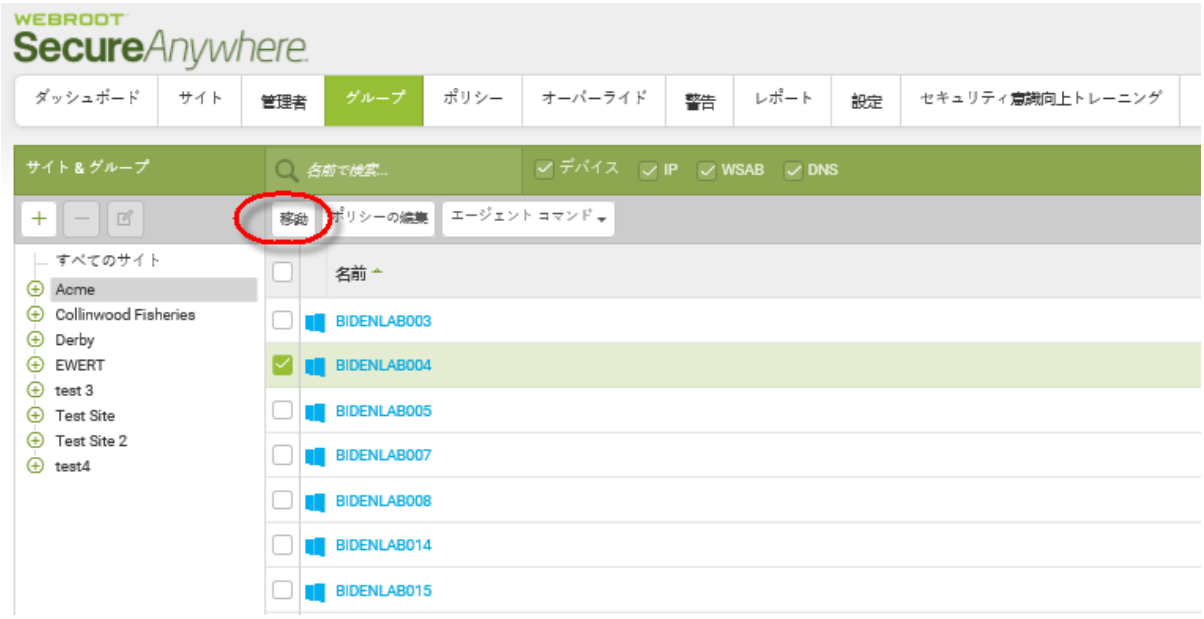
左側の [グループ] パネルに新しいグループが加わります。

9. この新しいグループへエンドポイントを移すには、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。

10. 右側の [デバイス] パネルからひとつ以上のエンドポイントを選択します。

すべてのエンドポイントを選択するには、カラムの一番上にあるチェックボックスを選択します。

11. [**移動**] ボタンをクリックします。



[グループを移動] ウィンドウが表示されます。

12. [次のグループへ移動] ドロップダウン メニューから、エンドポイントを移動する新しいグループを選択します。
13. 以下の [ポリシー管理] ラジオ ボタンのいずれかを選択します:
    - **新しいグループ ポリシーを自動的に継承**
    - **現在のポリシーを変更せずに移動**
14. [**移動**] ボタンをクリックします。

グループは新しいグループに移動されました。

グループの編集

デバイスを編集するには、次の手順に従ってください。

グループを編集するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. 左カラムで、編集するグループを含むサイトを選択します。

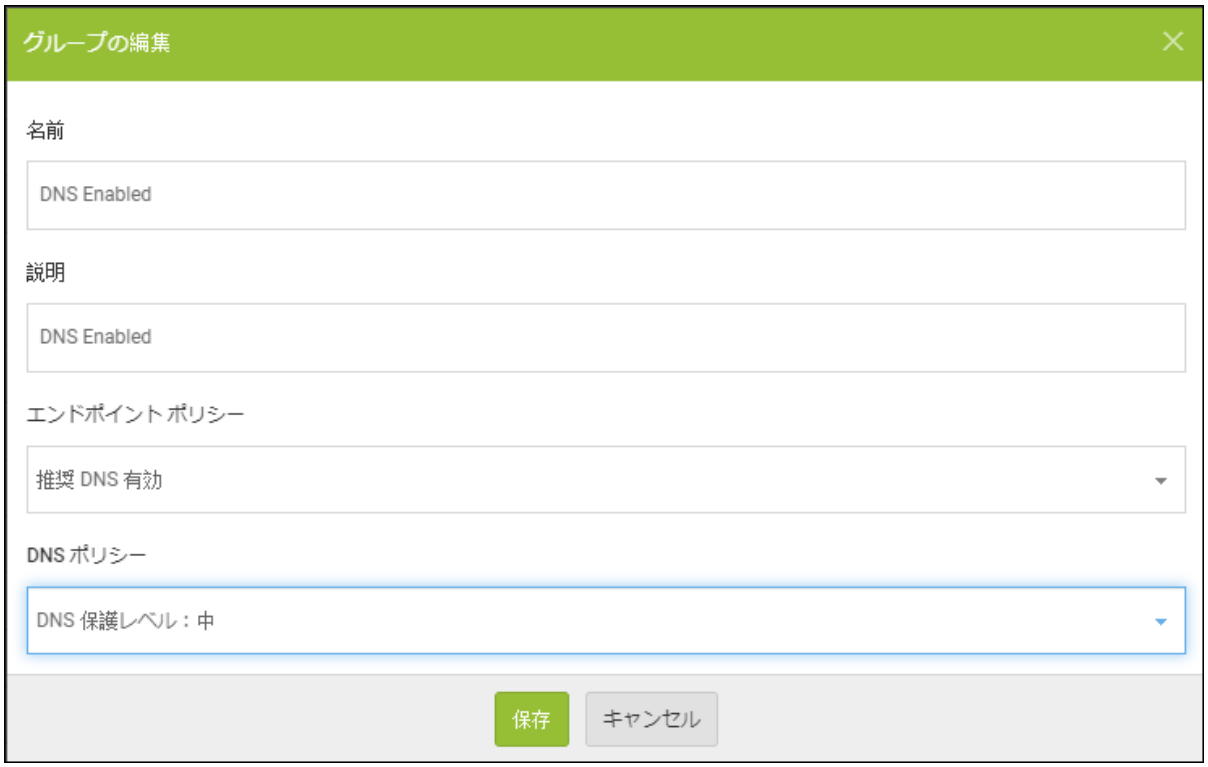
[編集] ボタンがアクティブになります。

4. [**編集**] ボタンをクリックします。

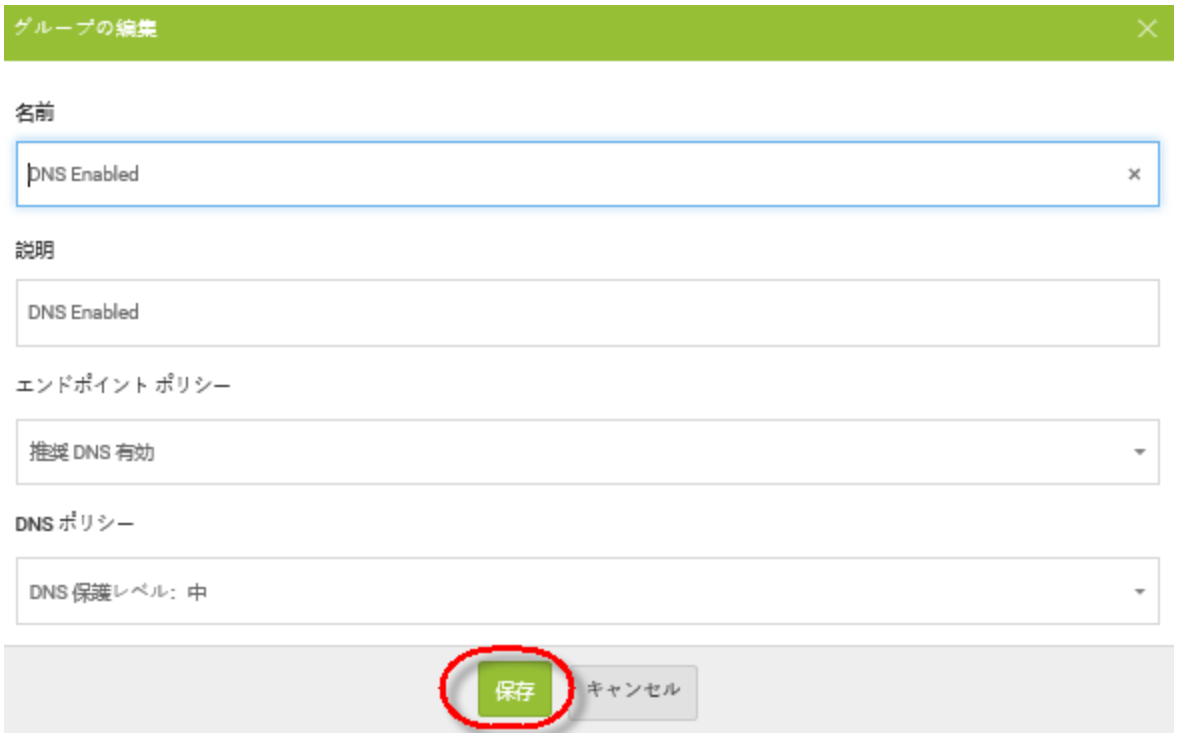
[グループの編集] ウィンドウが表示されます。

5. [名前] フィールドで、グループの名前を編集入力します。この手順はオプションです。
6. [説明] フィールドで、グループの説明を編集します。この手順はオプションです。
7. [エンドポイント ポリシー] ドロップダウン メニューから、グループの他のポリシーを選択します。この手順はオプションです。

8. 以下の [ポリシー管理] ラジオ ボタンのいずれかを選択します。この手順はオプションです。



9. 設定が完了したら [**保存**] ボタンをクリックします。



グループの情報が更新されます。

グループの削除

[グループ] タブからは、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することができます。

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. 管理コンソールにログインします。

   [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が表示されます。

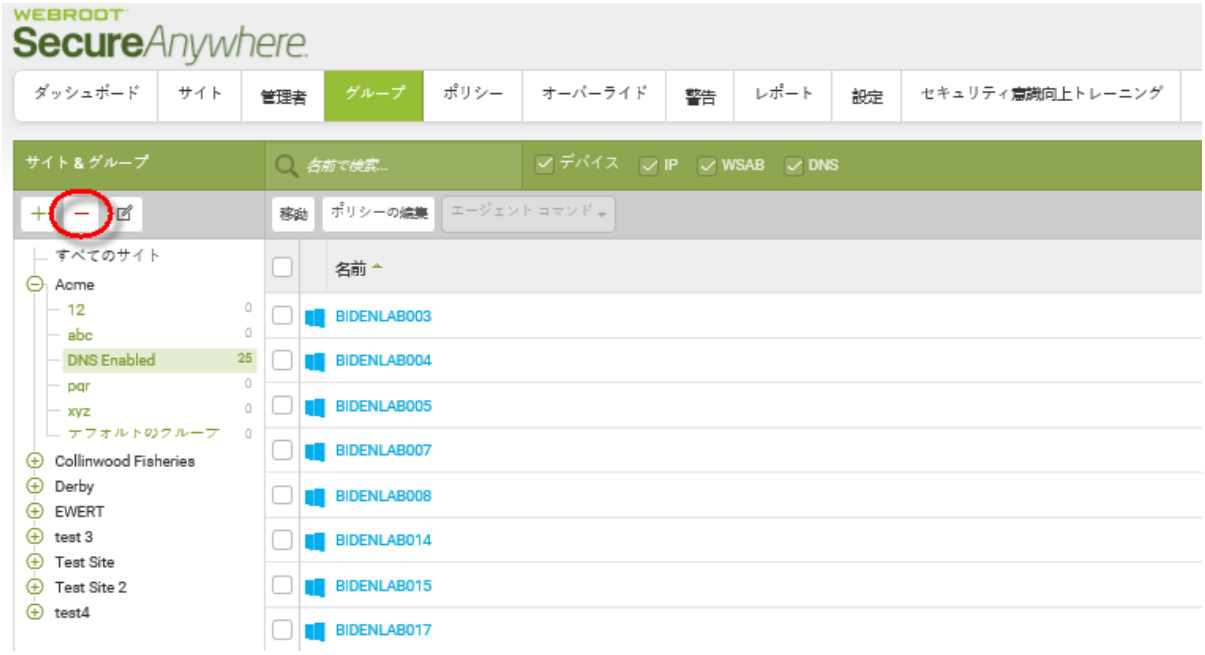
2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. [サイト & グループ] カラムから、削除するグループを選択します。

[マイナス記号 (-)] ボタンがアクティブになります。

4. [**マイナス記号 (-)**] ボタンをクリックします。



[グループの削除] ウィンドウが表示されます。

5. [代替グループの選択] ドロップダウン メニューから、コンテンツを移動する代替グループを選択します。

6. 以下の [ポリシー管理] ラジオ ボタンのいずれかを選択します:
   - **新しいグループ ポリシーを自動的に継承**
   - **現在のポリシーを変更せずに移動**
7. [**削除**] ボタンをクリックします。

グループが削除されます。

第 6 章: デバイスの操作

デバイスを操作するには、次のトピックを参照してください。

デバイス管理の概要

管理コンソールでは、すべてのサイトのすべてのデバイスの概要をひと目で確認することができます。また、管理者は、サイトや状態によるフィルタリング、特定のデバイスを絞り込んで、デバイスの遭遇する脅威情報、ブロックされた URL を表示することができます。また管理者はファイルを復元したり、隔離することができます。

デバイスの管理機能はすべて、管理コンソールの [グループ] タブにあります。

[グループ] タブには 3 つのメインの領域があります。

- フィルタ
- カラム
- ページ移動機能

[グループ] タブのフィルタ

[グループ] タブには 3 つの内蔵フィルタがあり、次のことを行うことができます。

- サイト名によるデバイスのフィルタリング
- 状態によるデバイスのフィルタリング
- グループ内のデバイスのフィルタリング
- グループ内のデバイスの並べ替え
- デバイスの検索

[グループ] タブのカラム

[デバイス] タブのメイン部分では、すべてのデバイスが次のカラムに表示されます。

- **名前** - デバイスの名前を表示します。ここにはデバイスのタイプを示すアイコンが含まれます。

デバイスのアイコン	説明
	デバイスが Windows PC であることを示しています。
	デバイスが Windows サーバー であることを示しています。
	デバイスが Apple Mac であることを示しています。

- **状態** - 次の表のように、デバイスの現在の状態を示します。

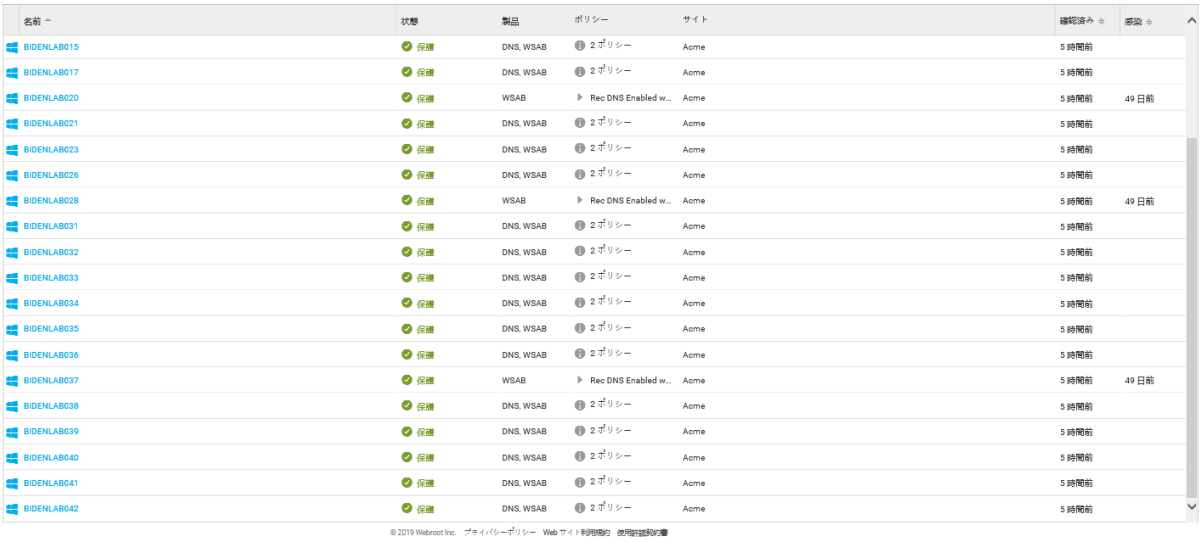
状態アイコン	説明
	**保護** - デバイスが保護されていることを示しています
	**要対応** - デバイスに対応が必要であることを示しています。
	**期限切れ** - デバイスのライセンスの期限が切れており、Webroot SecureAnywhere によって保護されていないことを示しています。
	**対応 & 期限切れ** - 対応が必要であるとともに、デバイスのライセンスの期限が切れており、Webroot SecureAnywhere によって保護されていないことを示しています。
	**最近確認されていません** - デバイスが最近確認されていないことを示しています。

[グループ] タブのページ移動機能

[デバイス] タブ下部にはページ移動機能があります。次の表で各機能について説明します。

機能	説明
	**二重左**矢印をクリックして、リストの最初のページに移動します
	**左**矢印をクリックして、リストの前のページに移動します。
	リストのどのページが表示されているかを示します。
	**右**矢印をクリックして、リストの次のページに移動します。 ドロップダウンメニューから、リストの任意のページを選択して直接そのページに移動します。
	**二重右**矢印をクリックして、リストの最後のページに移動します。
	[アップデート] アイコンをクリックして、ページの情報をアップデートします。

機能	説明
	ページに表示されている行数を示します。ドロップダウン メニューから、次の単位のいずれかを選択できます。 • 50 • 100 • 200 • 500
	リストに表示されるページ数のうち、どのページが表示されているかを数値で表示します。



デバイスに適用されるポリシーの編集

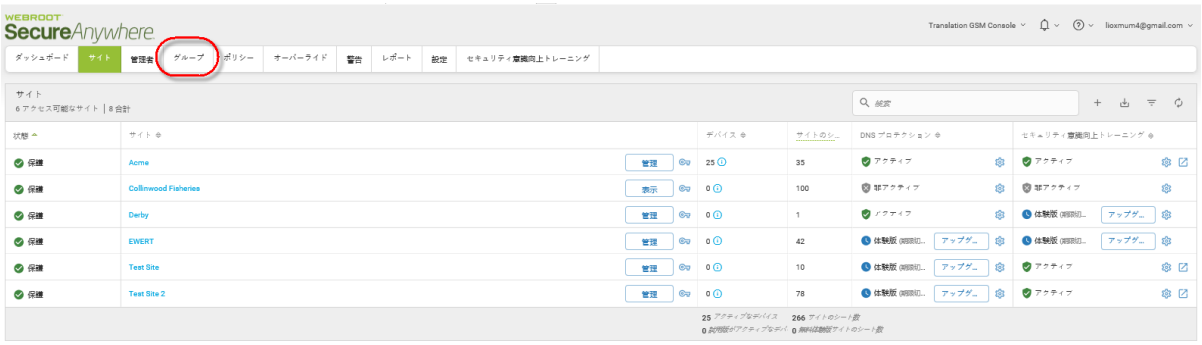
この手順に従って、デバイスに適用されるポリシーを編集します。

ポリシーを編集するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。



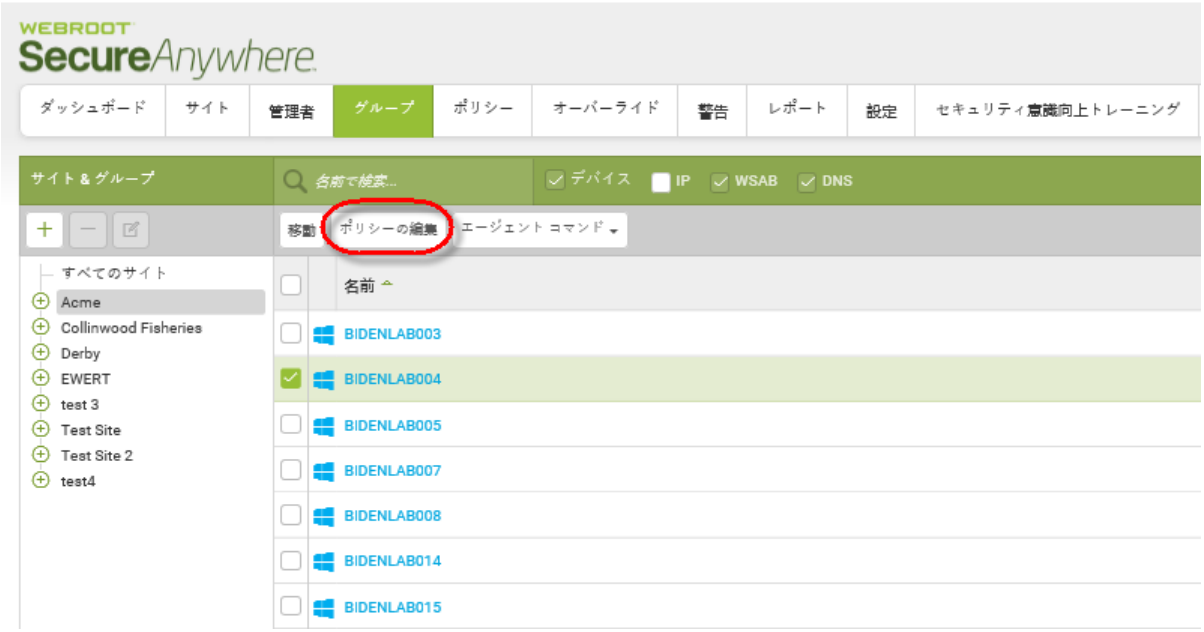
   [グループ] タブが表示されます。

3. 左カラムで、ポリシーを編集するグループとデバイスを含むサイトを選択します。

4. [デバイス] パネルで、ポリシーを編集するデバイスを選択します。

すべてのデバイスを選択するには、カラムの一番上にあるチェックボックスを選択します。

5. [**ポリシーの編集**] ボタンをクリックします。



[ポリシーの編集] ウィンドウが表示されます。

6. [エンドポイント ポリシー] ドロップダウン メニューから、デバイスにポリシーを選択します。
7. [**変更**] ボタンをクリックします。

新しいポリシーがデバイスに追加されます。

デバイスへのウェブのオーバーライドの追加

すべてのデバイスは、状態にかかわらず、ブロックされた URL を持つことができます。この手順に従って、ウェブのオーバーライドをデバイスに追加します。

デバイスにウェブのオーバーライドを追加するには:

1. 管理コンソールにログインします。

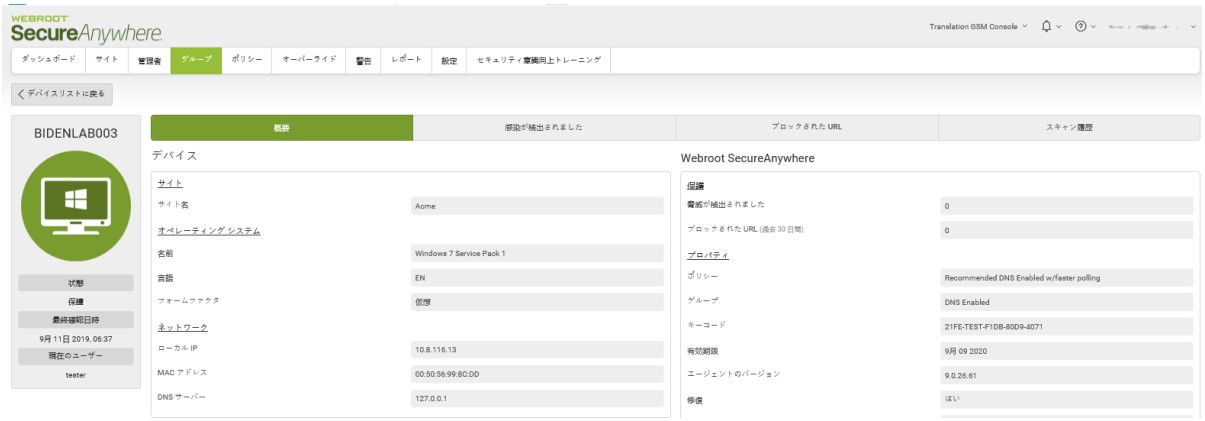
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**グループ**] タブをクリックします。

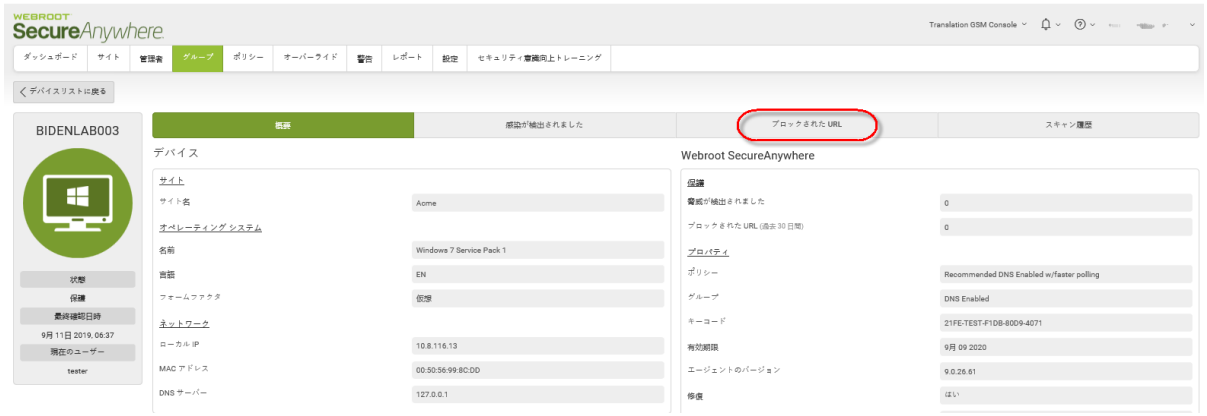
   [グループ] タブが表示されます。

3. オーバーライドする、ブロックされた URL を持つデバイスを選択します。

選択したデバイスの [状態] パネルが表示されます。



4. [**ブロックされた URL**] タブをクリックします。



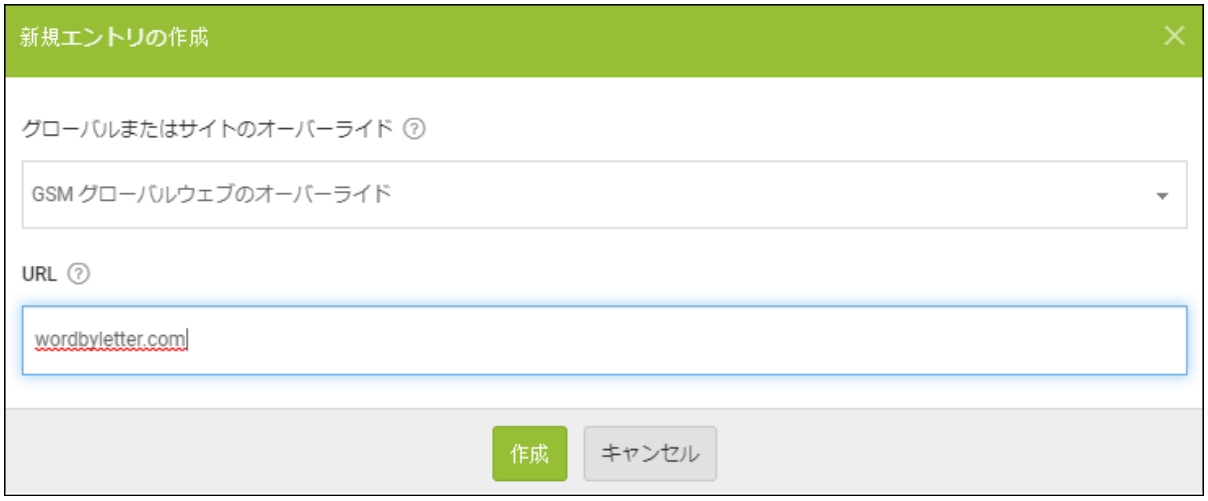
[ブロックされた URL] タブが開いて次の情報が表示されます。

- **URL** - ブロックされた URL。
- **カテゴリー** - ブロックされた URL のタイプ。 Web サイトのカテゴリーの詳細については、「Webroot のカテゴリーの説明」を参照してください。
- **レピュテーション** - ブロックされた URL のレピュテーション。 Web サイトのレピュテーションの詳細については、「Webroot のレピュテーションの説明」を参照してください。
- **ユーザーアクション** - 未定。
- **日付** - URL が最初にリストに表示された日付。
- **アクション** - [新規エントリの作成] ウィンドウを表示します。ここで、ウェブのオーバーライドを作成するための情報を入力できます。

注意: ブロックされた URL がある場合にのみ、追加機能が表示されます。ブロックされた URL がない場合は、URL のカラムのみが表示されます。

5. [**アクション**] アイコンをクリックします。

[新規エントリの作成] ウィンドウが表示されます。



6. URL カラムに、ブロックされた URL が表示されます。また、ウェブのオーバーライドを適用する新しい URL を入力できます。
7. [グローバル] または [サイト オーバーライド] ドロップダウン メニューから、次のいずれかを選択して、管理コンソールまたはサイト レベルでウェブ オーバーライドを作成するかどうかを決定します。
   - **GSM グローバル ウェブのオーバーライド**
   - **サイト名**

8. 設定が完了したら、[**作成**] ボタンをクリックします。

ウェブのオーバーライドが作成されます。

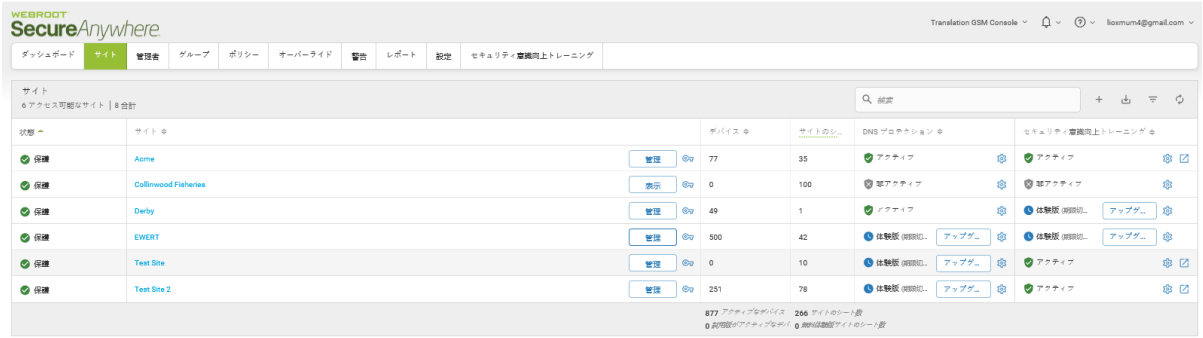
デバイス上のファイルをホワイトリストに記録する

すべてのデバイスには、状態にかかわらず、隔離されたファイルが存在する可能性があります。デバイス上のファイルをホワイトリストに記録するには、この手順に従います。

デバイス上のファイルをホワイトリストに記録するには:

1. 管理コンソールにログインします。

   [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が表示されます。



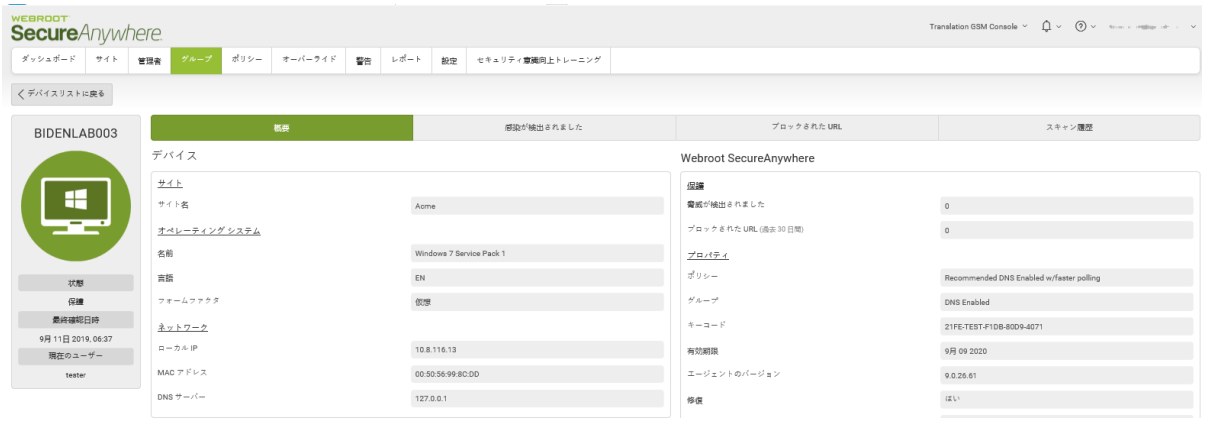
2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

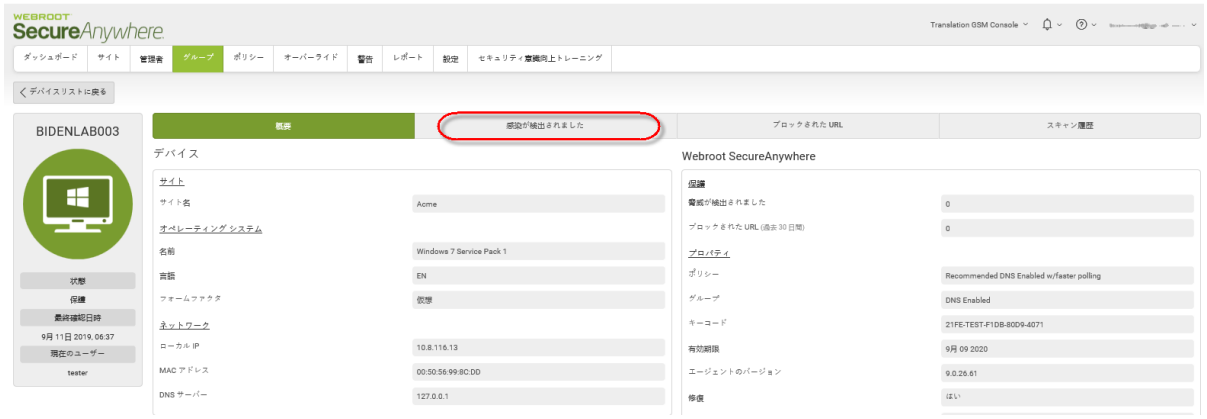
3. オーバーライドする、ブロックされた URL を持つデバイスを選択します。

注意: この例では、保護された状態のデバイスを示していますが、デバイスの状態にかかわらずデバイス上のファイルをホワイトリストに記録できます。

選択したデバイスの [状態] パネルおよび [概要] パネルが表示されます。



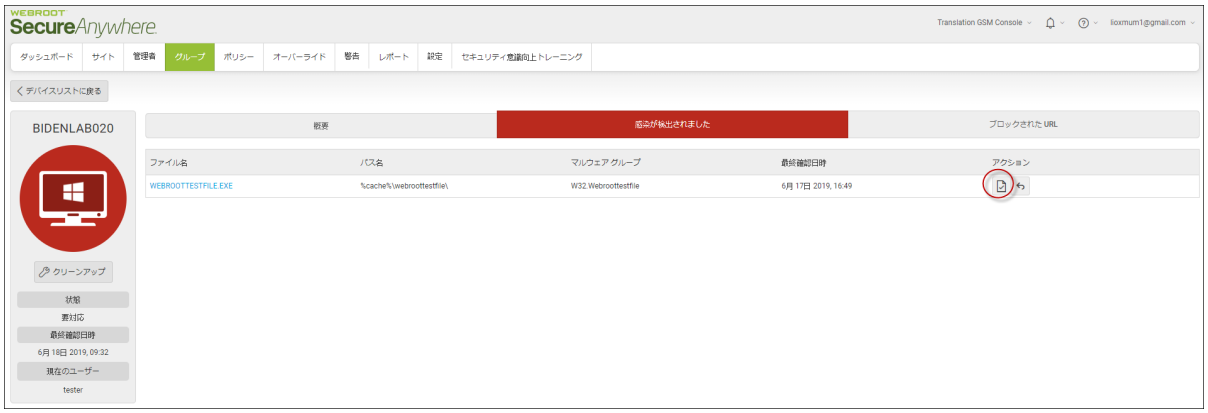
4. [**感染が検出されました**] タブをクリックします。



[感染が検出されました] タブに次のカラムが表示されます。

- **ファイル名** - 感染したファイルの名前。
- **パス名** - 感染したファイルのパス。
- **マルウェア グループ** - ブロックされた URL のレピュテーション。 Web サイトのレピュテーションの詳細については、「Webroot のレピュテーションの説明」を参照してください。
- **最終確認日時** - デバイスがシステムで最後にチェックインした日時。
- **アクション** - ユーザーがデバイス上のファイルを復元したり、ホワイトリストに登録できます。 詳細については、「*188{/u}{/color} ページの「ファイルの隔離からの復元」*」を参照してください。

5. ホワイトリストに登録するファイルで、[**ファイルをホワイトリストに登録する**] アイコンをクリックします。



[新規ホワイトリスト エントリ] ウィンドウが表示されます。

6. [名前 / 説明] フィールドに、ファイルの名前を入力します。
7. [オーバーライドのタイプ] エリアで、以下のラジオ ボタンの 1 つを選択します:
   - **MD5**
   - **フォルダ / ファイル**
8. [MD5] フィールドに MD5 情報が表示されます。

9. 設定が完了したら、[**作成**] ボタンをクリックします。

新規ホワイトリスト エントリが作成されます。

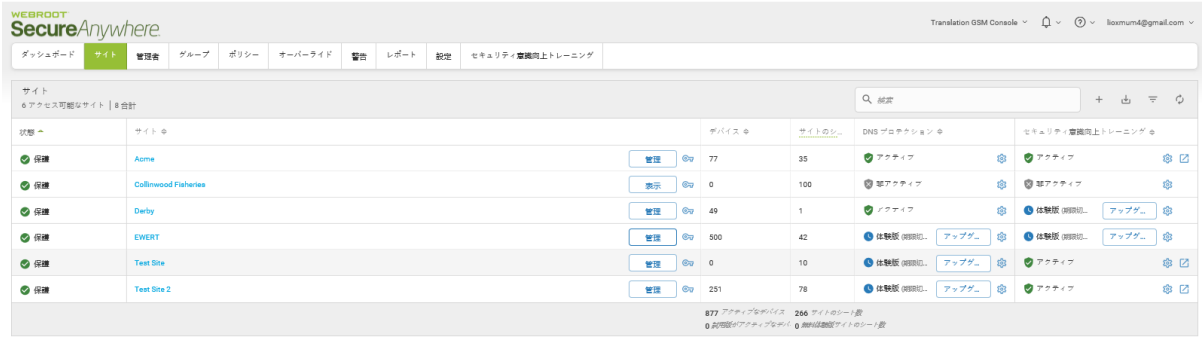
ファイルの隔離からの復元

すべてのデバイスには、状態にかかわらず、隔離されたファイルが存在する可能性があります。隔離先からファイルを復元するには、この手順に従います。

デバイスの隔離先からファイルを復元するには:

1. 管理コンソールにログインします。

   [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が表示されます。



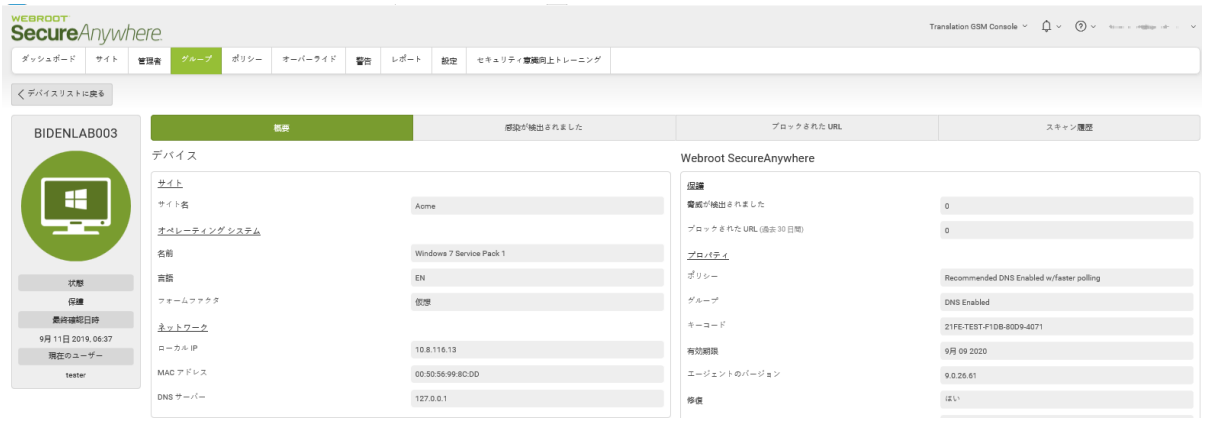
2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

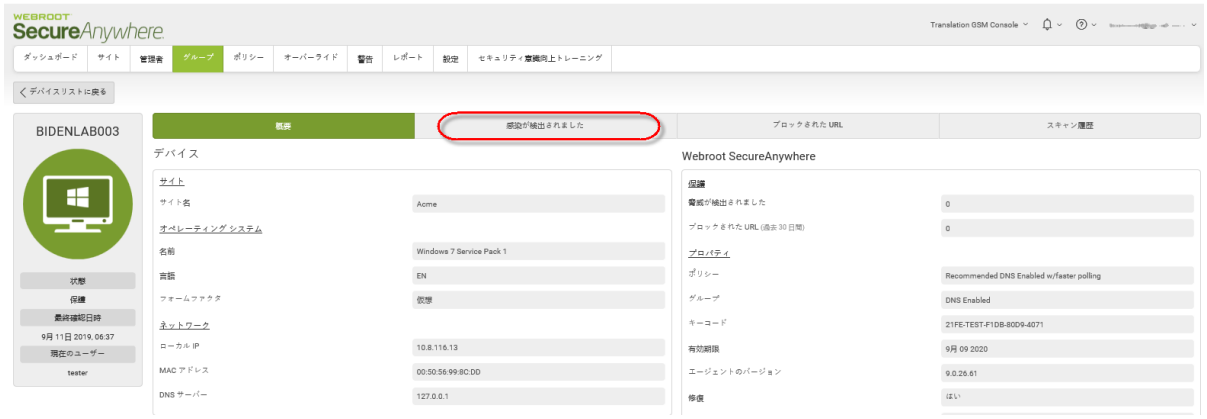
3. オーバーライドする、ブロックされた URL を持つデバイスを選択します。

注意: この例では、保護された状態のデバイスを示していますが、デバイスの状態にかかわらずデバイス上のファイルを復元できます。

選択したデバイスの [状態] パネルが表示されます。



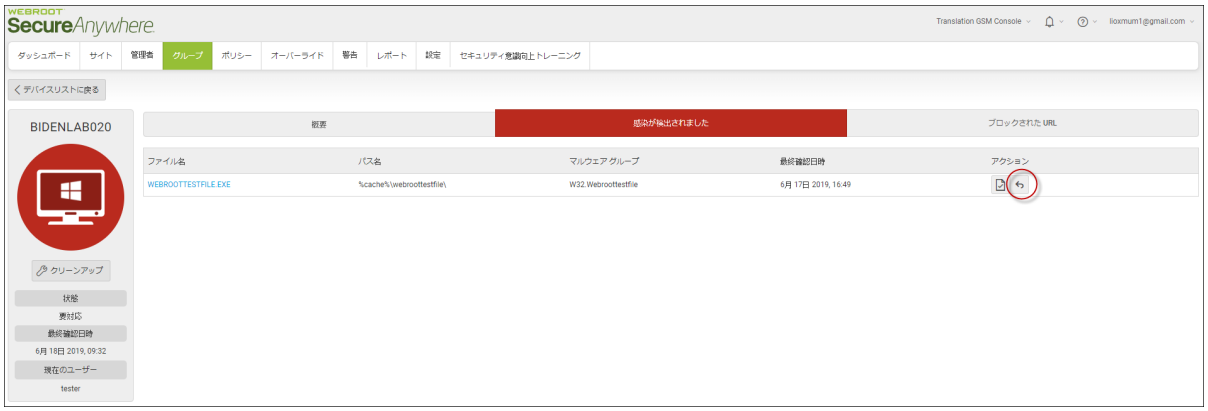
4. [**感染が検出されました**] タブをクリックします。



[感染が検出されました] タブに次のカラムが表示されます。

- **ファイル名** - 感染したファイルの名前。
- **パス名** - 感染したファイルのパス。
- **マルウェア グループ** - ブロックされた URL のレピュテーション。 Web サイトのレピュテーションの詳細については、「Webroot のレピュテーションの説明」を参照してください。
- **最終確認日時** - デバイスがシステムで最後にチェックインした日時。
- **アクション** - ユーザーがデバイス上のファイルを復元したり、ホワイトリストに登録できます。 詳細については、「*183{/u}{/color} ページの「デバイス上のファイルをホワイトリストに記録する」*」を参照してください。

5. [**ファイルの復元**] アイコンをクリックします。



[隔離先から復元する] ウィンドウが表示され、ファイル名と MD5 情報がフィールドに表示されます。

6. ファイルを復元するには、[**復元**] ボタンをクリックします。

システムはファイルをデバイスに復元します。

保護されているデバイスの表示

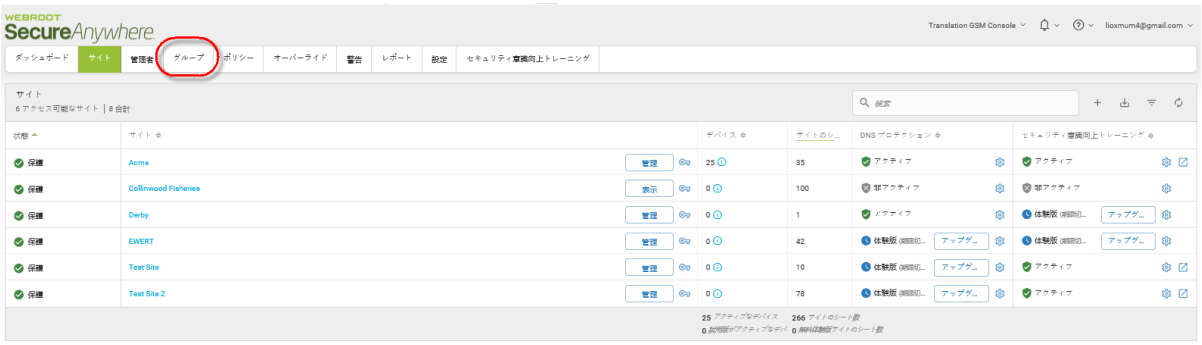
[保護] の状態のデバイスに関する情報を表示するには、以下の手順に従ってください。

保護されているデバイスを表示するには:

1. 管理コンソールにログインします。

   [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が表示されます。

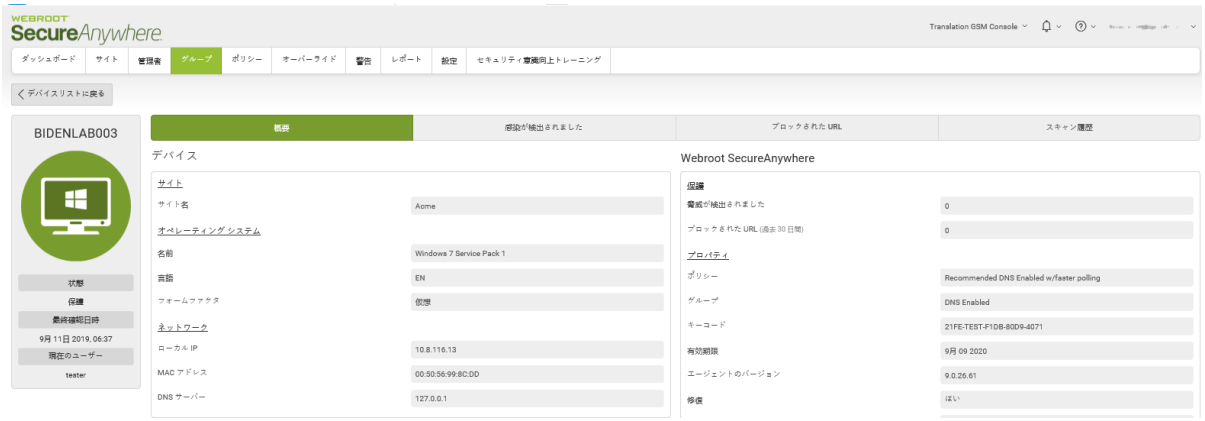
2. [**グループ**] タブをクリックします。



   [グループ] タブが表示されます。

3. 表示する [保護] の状態のデバイスを選択して、ダブルクリックします。

選択したデバイスの [状態] パネルが表示されます。



4. 左側の [デバイス情報] カラムには、デバイスの名前と次の情報が表示されます:
   - **状態** - デバイスの状態。詳細については、「 」を参照してください。*169{/u}{/color} ページの「デバイス管理の概要」*.
   - **最終確認日時** - デバイスがシステムで最後にチェックインした日時。
   - **現在のユーザー** - 現在ログインしている [状態] パネルを表示している管理者の姓。

パネルのメイン部分には、次の情報が表示されます:

- **サイト**
- **オペレーティング システム**
- ネットワーク
- 保護
- プロパティ
- シールド

5. 追加情報については、次の 3 つのタブのいずれかをクリックしてください:
   - 概要 - **デバ**イスに関する情報の概要が表示されます。
   - **感染が検出されました - このデバイスで検出**された感染に関するリストを表示します。
   - **ブロックされた URL** - Web 脅威シールド プログラムによってブロックされた URL のリストを表示します。このタブで、ブロックしたくない URL にウェブのオーバーライドを追加することもできます。詳細については、「」を参照してください。 *178{/u}{/color} ページの「デバイスへのウェブのオーバーライドの追加」*.
   - **スキャン履歴 - 特定の**デバイスで発生したすべてのスキャンと、スキャン中に検出された脅威のリストを表示します。詳細については、「」を参照してください。 *237{/u}{/color} ページの「スキャン履歴の表示」*.
6. 設定が完了したら [**デバイスリストに戻る**] ボタンをクリックします。

最近確認していないファイルの表示

状態が[最近確認されていません] であるデバイスに関する情報を表示するには、以下の手順に従ってください。

最近確認していないデバイスを表示するには:

1. 管理コンソールにログインします。

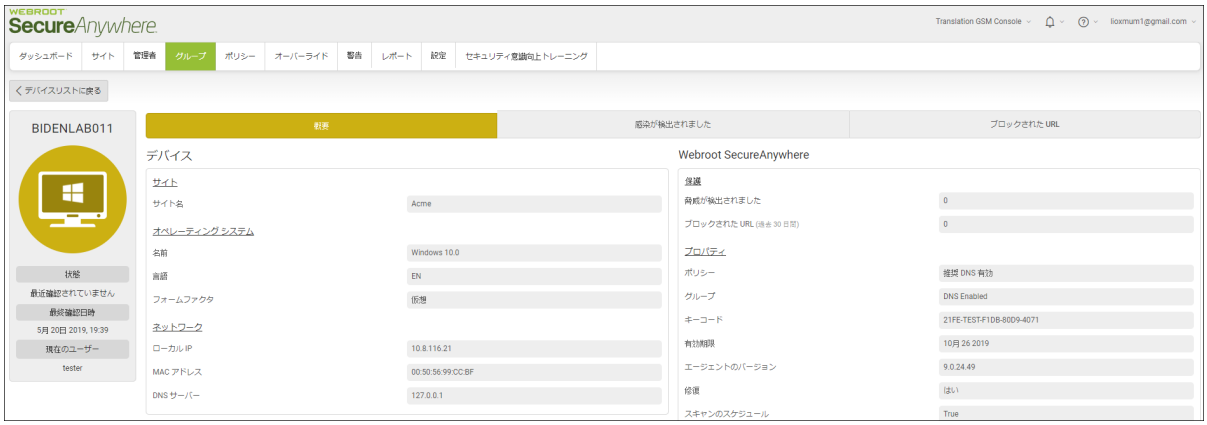
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. 状態が [**最近確認されていません**] の、表示するデバイスを選択して、ダブルクリックします。

選択したデバイスの [状態] パネルが表示されます。

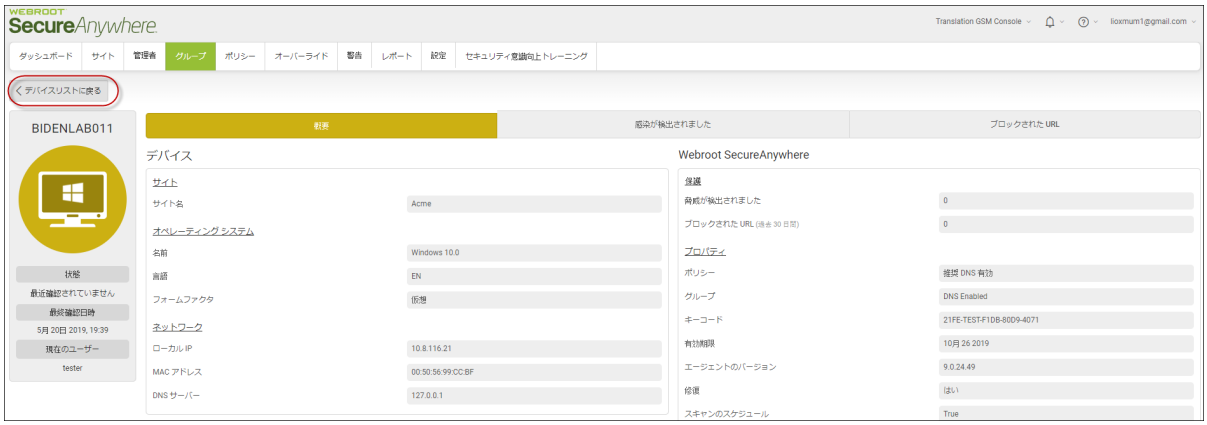


4. 左側の [デバイス情報] カラムには、デバイスの名前と次の情報が表示されます:
   - **状態 - デバイス**の状態。詳細については、「」を参照してください。*169{/u}{/color} ページの「デバイス管理の概要」*.
   - **最終確認日時** - デバイスがシステムで最後にチェックインした日時。
   - **現在のユーザー - 現在**ログインしている [状態] パネルを表示している管理者の姓。

   パネルのメイン部分には、次の情報が表示されます:

   - サイト
   - オペレーティングシステム
   - **ネットワーク**
   - **保護**
   - プロパティ
   - シールド
5. 追加情報については、次の 3 つのタブのいずれかをクリックしてください:
   - **概要 - デバ**イスに関する情報の概要が表示されます。
   - **感染が検出されました - このデバイスで検出**された感染に関するリストを表示します。
   - **ブロックされた URL** - Web 脅威シールド プログラムによってブロックされた URL のリストを表示します。このタブで、ブロックしたくない URL にウェブのオーバーライドを追加することもできます。詳細については、「」を参照してください。*178{/u}{/color} ページの「デバイスへのウェブのオーバーライドの追加」*
   - **スキャン履歴 - 特定の**デバイスで発生したすべてのスキャンと、スキャン中に検出された脅威のリストを表示します。詳細については、「」を参照してください。*237{/u}{/color} ページの「スキャン履歴の表示」*

6. 設定が完了したら [**デバイスリストに戻る**] ボタンをクリックします。



注意の必要なデバイスの表示

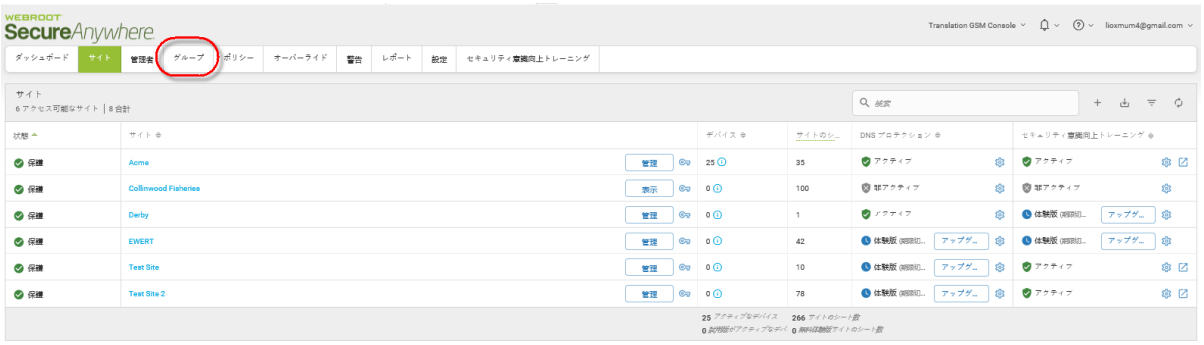
状態が[要対応]であるデバイスに関する情報を表示するには、以下の手順に従ってください。

注意の必要なデバイスを表示するには:

1. 管理コンソールにログインします。

   [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が表示されます。

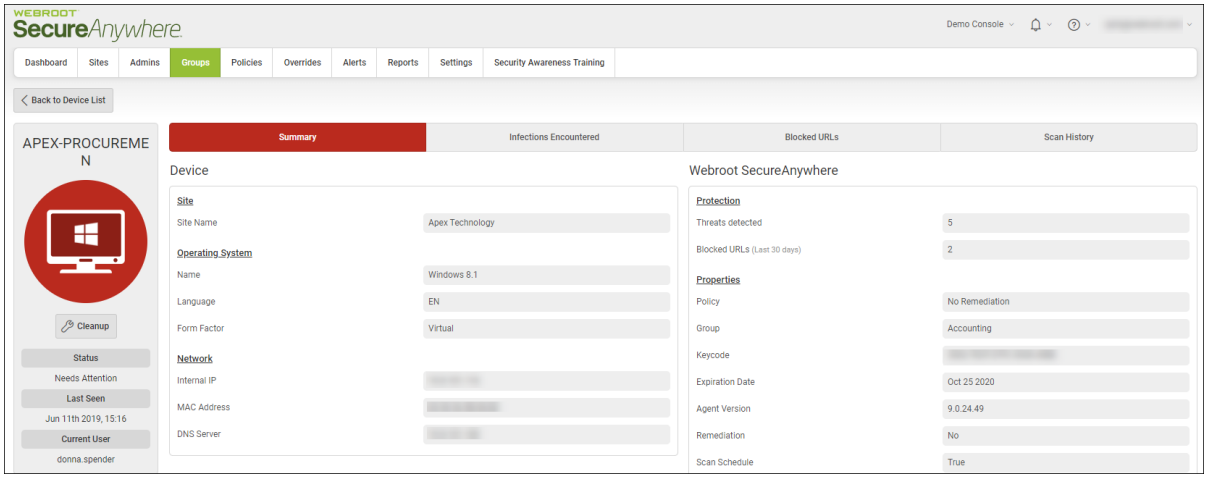
2. [**グループ**]タブをクリックします。



   [グループ]タブが表示されます。

3. 表示する [要対応] の状態のデバイスを選択して、ダブルクリックします。

選択したデバイスの [状態] パネルが表示されます。



4. 左側の [デバイス情報] カラムには、デバイスの名前と次の情報が表示されます:
   - **状態** - デバイスの状態。詳細については、「」を参照してください。*169{/u}{/color} ページの「デバイス管理の概要」*.
   - **最終確認日時** - デバイスがシステムで最後にチェックインした日時。
   - **現在のユーザー** - **現在**ログインしている [状態] パネルを表示している管理者の姓。

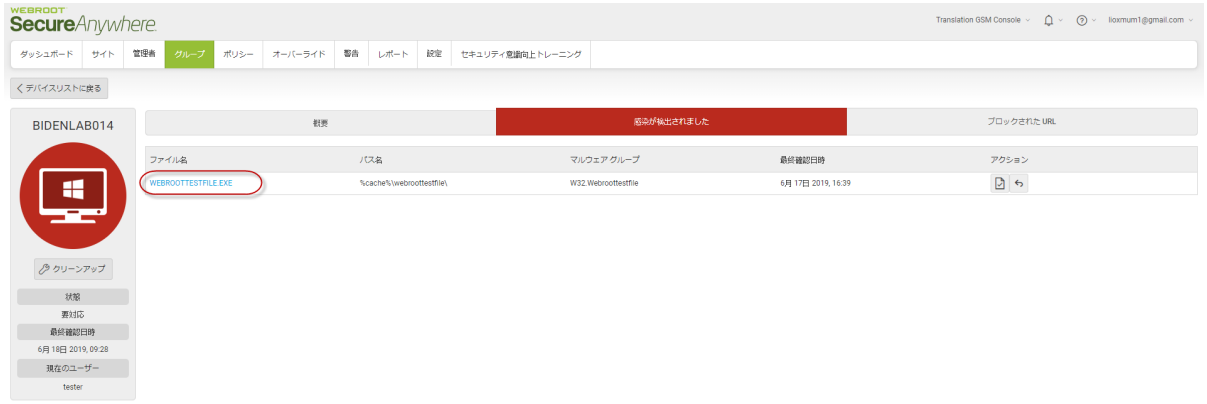
   パネルのメイン部分には、次の情報が表示されます:

   - **サイト**
   - **オペレーティングシステム**
   - **ネットワーク**
   - **保護**
   - プロパティ
   - シールド
5. 追加情報については、次の 3 つのタブのいずれかをクリックしてください:
   - **概要** - **デバ**イスに関する情報の概要が表示されます。
   - **感染が検出されました** - **このデバイスで検出**された感染に関するリストを表示します。
   - **ブロックされた URL** - Web 脅威シールド プログラムによってブロックされた URL のリストを表示します。このタブで、ブロックしたくない URL にウェブのオーバーライドを追加することもできます。詳細に

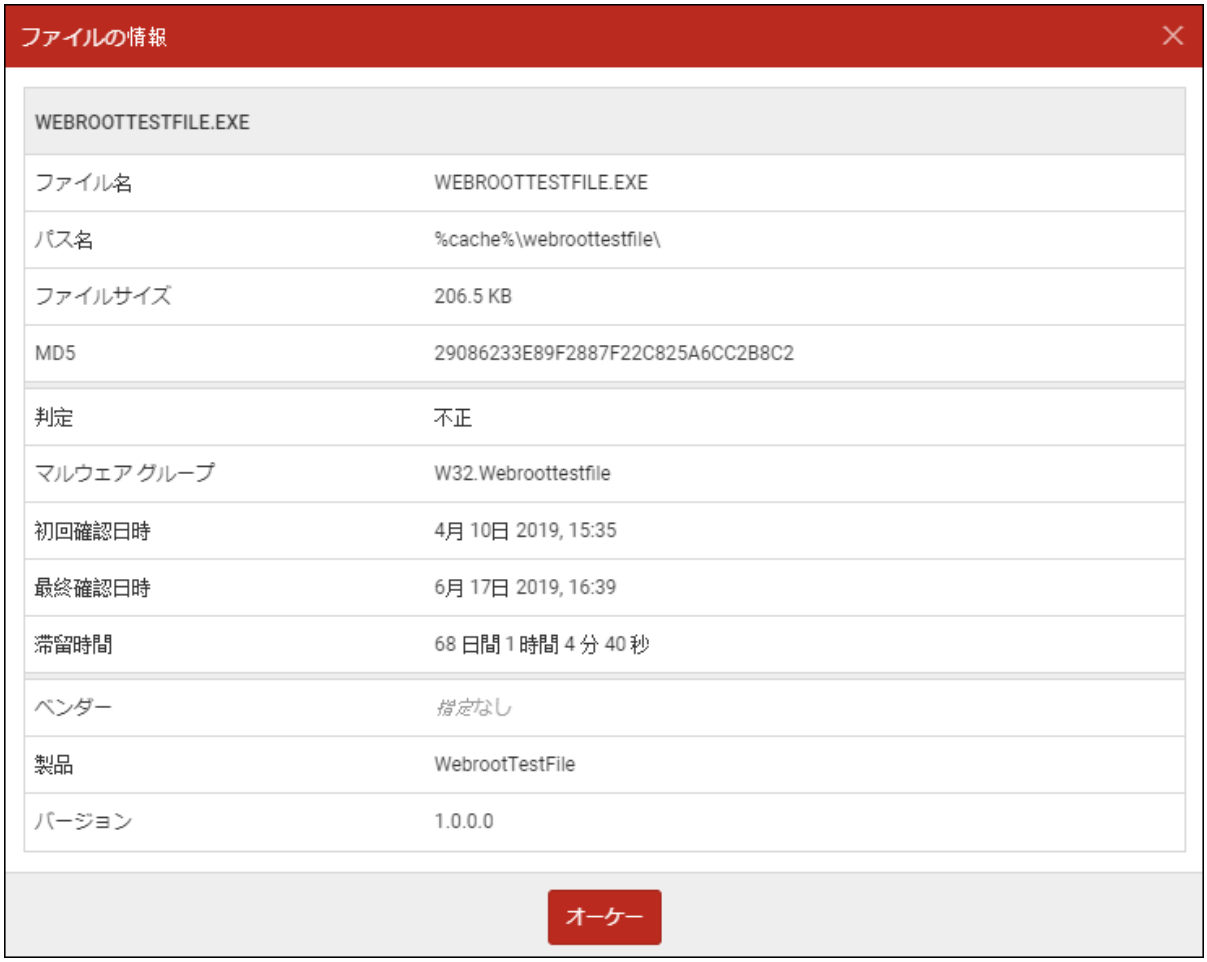
ついては、「」を参照してください。 *178{/u}{/color} ページの「デバイスへのウェブのオーバーライドの追加」*

- **スキャン履歴 - 特定の**デバイスで発生したすべてのスキャンと、スキャン中に検出された脅威のリストを表示します。 詳細については、「」を参照してください。 *237{/u}{/color} ページの「スキャン履歴の表示」*

6. 感染に関する詳細情報を表示するには、[**感染が検出されました**] タブをクリックして、情報を表示する感染をクリックします。

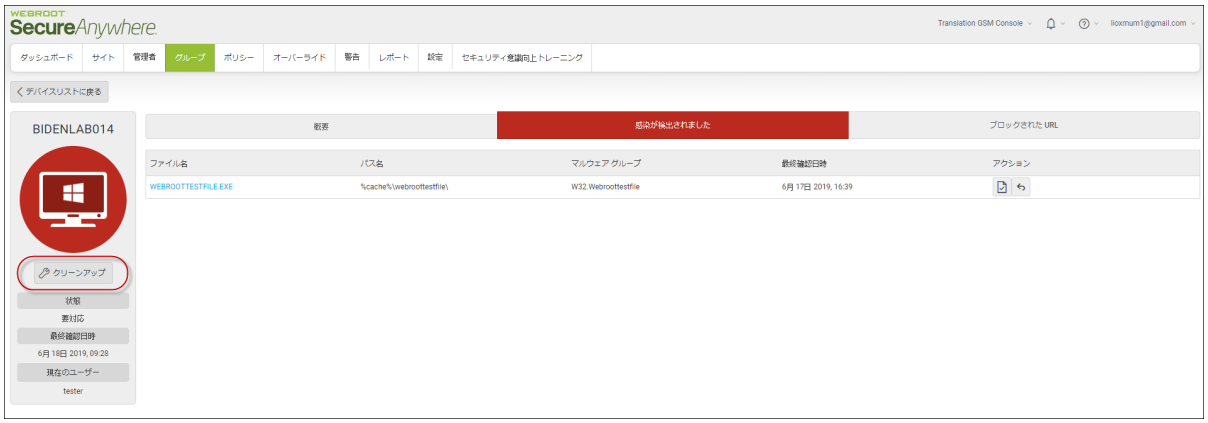


[ファイルの情報] ウィンドウが表示されます。

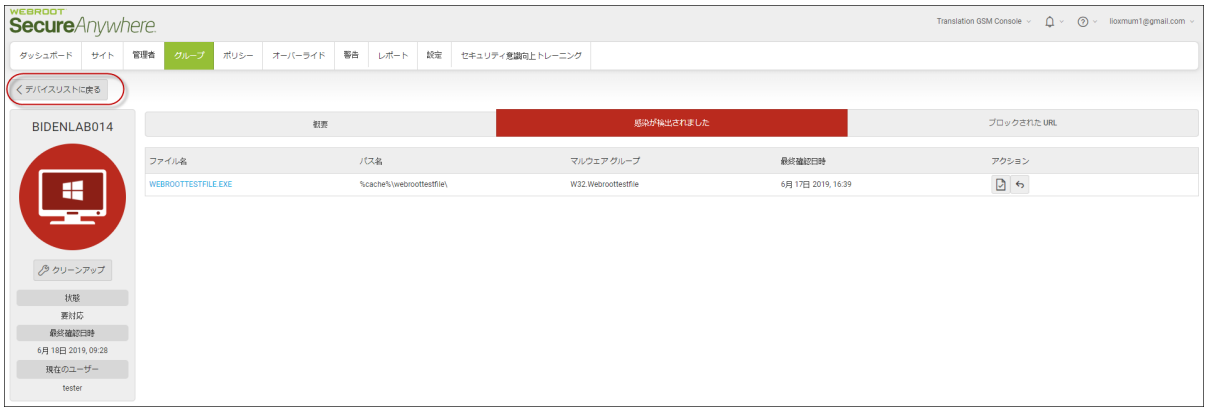


情報の表示が完了したら、[**OK**] ボタンをクリックします。

7. デバイスにクリーン コマンドを送信するには、[**クリーンアップ**] ボタンをクリックします。



8. 設定が完了したら [**デバイスリストに戻る**] ボタンをクリックします。



期限切れのデバイスの表示

[期限切れ] の状態のデバイスに関する情報を表示するには、以下の手順に従ってください。

保護されているデバイスを表示するには:

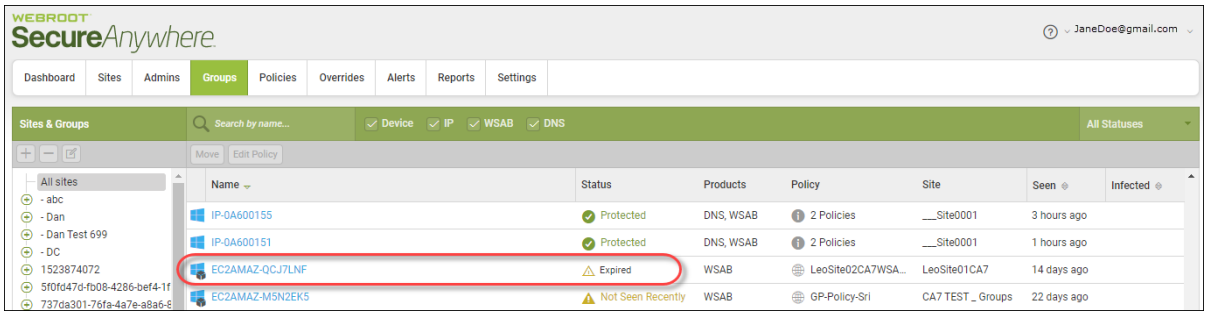
1. 管理コンソールにログインします。

   [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が表示されます。

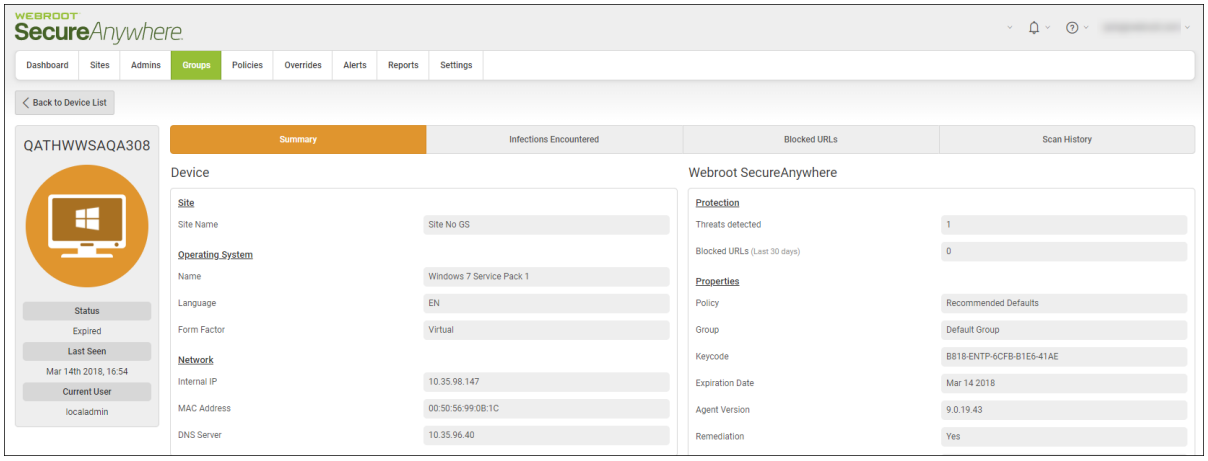
2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. 表示する [期限切れ] の状態のデバイスを選択して、ダブルクリックします。



選択したデバイスの [状態] パネルが表示されます。



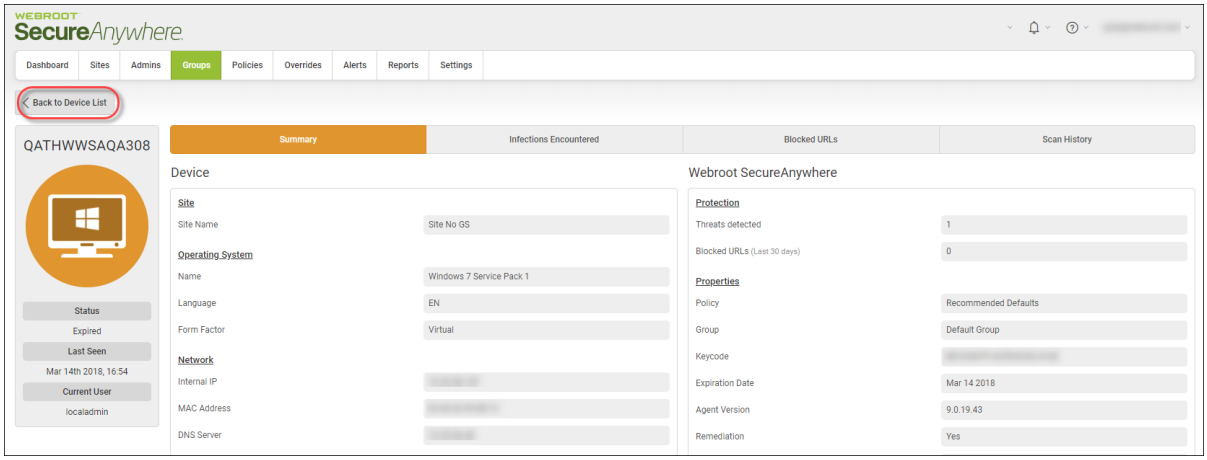
4. 左側の [デバイス情報] カラムには、デバイスの名前と次の情報が表示されます:
   - **状態** - デバイスの状態。詳細については、「」を参照してください。*169{/u}{/color} ページの「デバイス管理の概要」*.

- **最終確認日時** - デバイスがシステムで最後にチェックインした日時。
- **現在のユーザー** - **現在**ログインしている [状態] パネルを表示している管理者の姓。

パネルのメイン部分には、次の情報が表示されます:

- **サイト**
- **オペレーティングシステム**
- **ネットワーク**
- **保護**
- **プロパティ**
- **シールド**

5. 追加情報については、次の 3 つのタブのいずれかをクリックしてください:
   - **概要** - **デバ**イスに関する情報の概要が表示されます。
   - **感染が検出されました** - **このデバイスで検出**された感染に関するリストを表示します。
   - **ブロックされた URL** - Web 脅威シールド プログラムによってブロックされた URL のリストを表示します。このタブで、ブロックしたくない URL にウェブのオーバーライドを追加することもできます。詳細については、「」を参照してください。 *178{/u}{/color}* *ページの「デバイスへのウェブのオーバーライドの追加」*
   - **スキャン履歴** - **特定の**デバイスで発生したすべてのスキャンと、スキャン中に検出された脅威のリストを表示します。詳細については、「」を参照してください。*237{/u}{/color}* *ページの「スキャン履歴の表示」*
6. 設定が完了したら [**デバイスリストに戻る**] ボタンをクリックします。



対応が必要であり、期限が切れているデバイスの表示

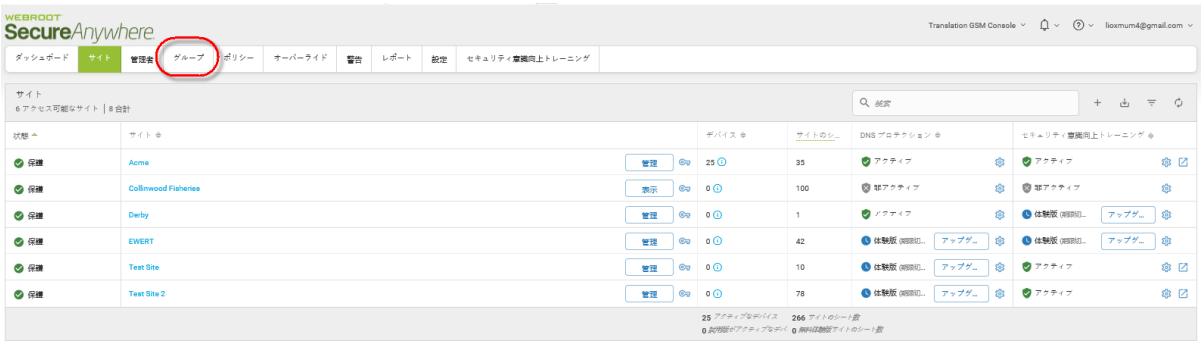
[対応 & 期限切れ] の状態のデバイスに関する情報を表示するには、以下の手順に従ってください。

対応が必要であり、期限が切れているデバイスを表示するには:

1. 管理コンソールにログインします。

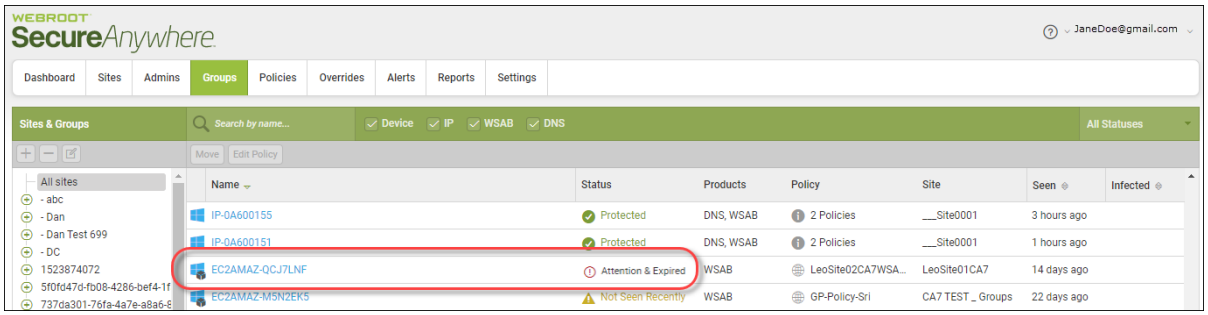
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**デバイス**] タブをクリックします。

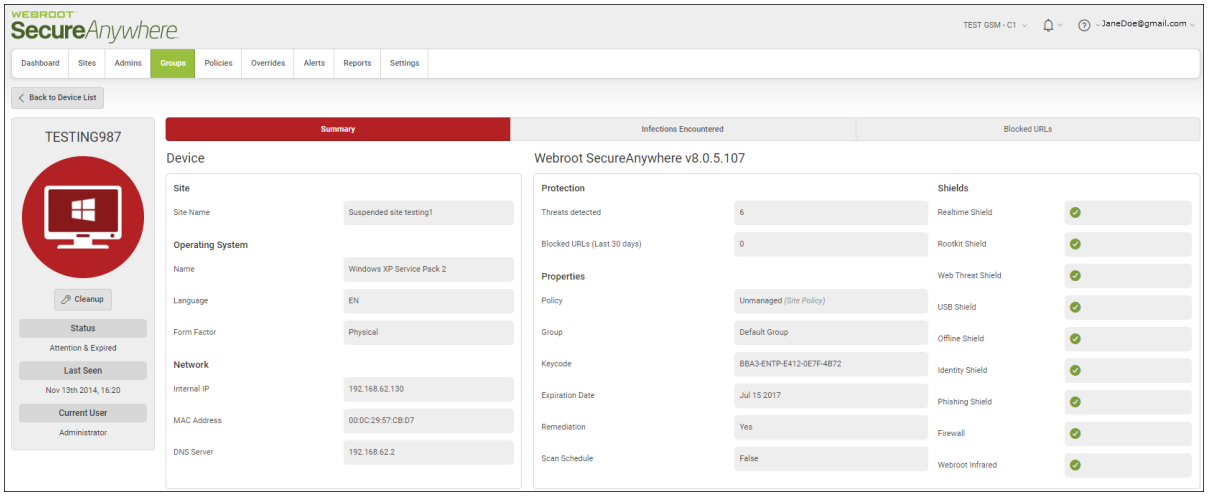


   [グループ] タブが表示されます。

3. 表示する [対応 & 期限切れ] の状態のデバイスを選択して、ダブルクリックします。



選択したデバイスの [状態] パネルが表示されます。



4. 左側の [デバイス情報] カラムには、デバイスの名前と次の情報が表示されます:
   - **状態** - デバイスの状態。詳細については、「」を参照してください。*169{/u}{/color}* *ページの「デバイス管理の概要」*.

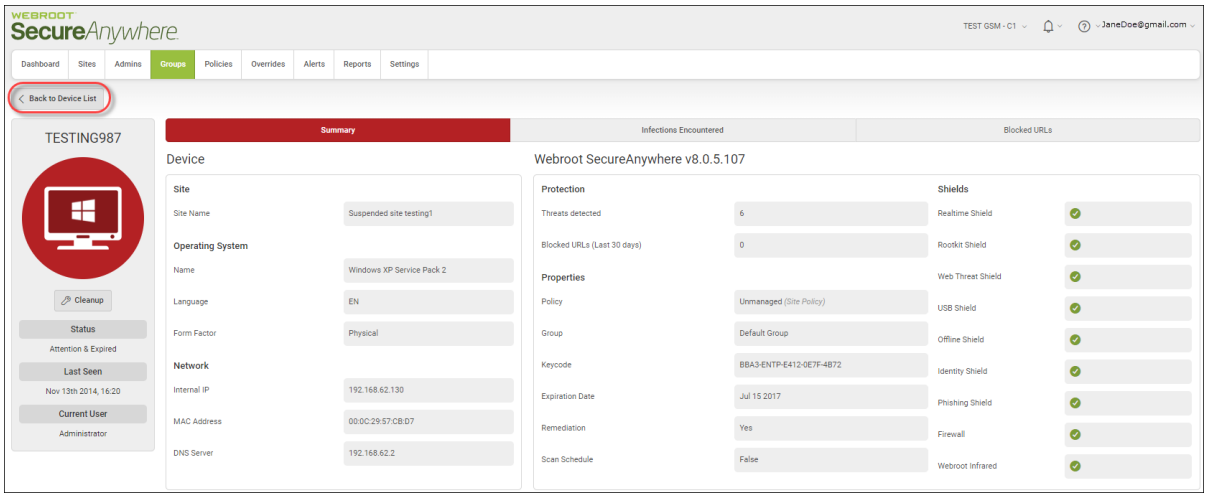
- **最終確認日時** - デバイスがシステムで最後にチェックインした日時。
- **現在のユーザー** - **現在**ログインしている [状態] パネルを表示している管理者の姓。

パネルのメイン部分には、次の情報が表示されます:

- サイト
- **オペレーティング システム**
- **ネットワーク**
- **保護**
- プロパティ
- シールド

5. 追加情報については、次の 3 つのタブのいずれかをクリックしてください:
   - **概要** - **デバ**イスに関する情報の概要が表示されます。
   - **感染が検出されました** - **このデバイスで検出**された感染に関するリストを表示します。
   - **ブロックされた URL** - Web 脅威シールド プログラムによってブロックされた URL のリストを表示します。このタブで、ブロックしたくない URL にウェブのオーバーライドを追加することもできます。詳細については、「」を参照してください。 *178{/u}{/color} ページの「デバイスへのウェブのオーバーライドの追加」*
   - **スキャン履歴** - **特定の**デバイスで発生したすべてのスキャンと、スキャン中に検出された脅威のリストを表示します。詳細については、「」を参照してください。 *237{/u}{/color} ページの「スキャン履歴の表示」*

6. 設定が完了したら [**デバイスリストに戻る**] ボタンをクリックします。



デバイスの概要の表示

グループ内では、1 つまたは複数のエンドポイントを持つことができます。パネル内で、名前、状態、適用されたポリシー、最終確認日時、最近の感染をすばやく表示できます。

この手順に従って、概要、検出された感染、およびブロックされた URL があるかどうかなどのデバイスに関する追加情報を表示します。

デバイスの概要を表示するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。

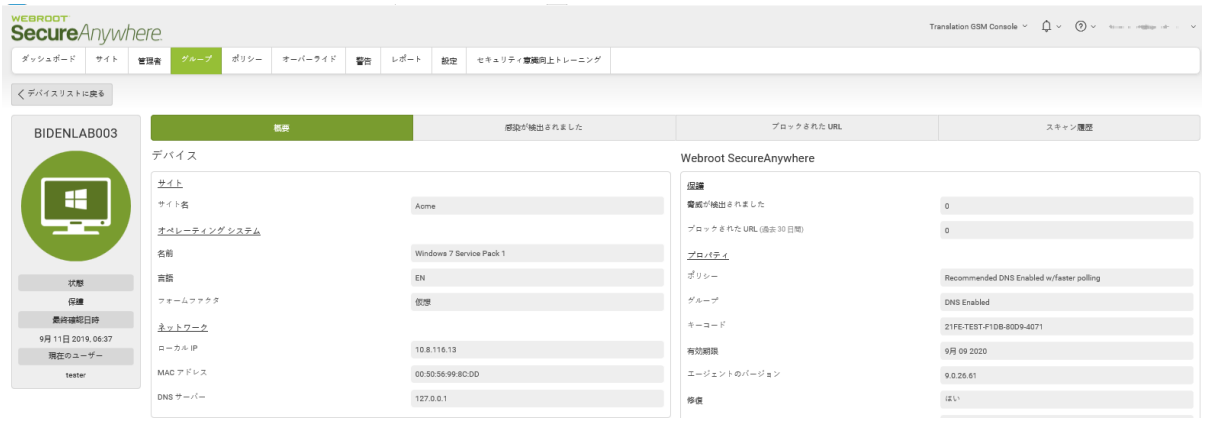
   [グループ] タブが表示されます。

3. 左カラムで、情報を表示するグループとデバイスを含むサイトを選択します。

4. [デバイス] パネルで、情報を表示するデバイスを含むサイトを選択します。

[概要] パネルには、次の情報が表示されます。

- 状態と最終確認日時
- 概要
- 検出された感染
- ブロックされた URL
- スキャン履歴



状態と最終確認日時

左側の [デバイス情報] カラムには、デバイスの名前と次の情報が表示されます:

- エンドポイントの状態を色で示すアイコンを表示します。
  - **状態** - エンドポイントの状態。
  - **最終確認日時** - エンドポイントがシステムで最後にチェックインした日時。

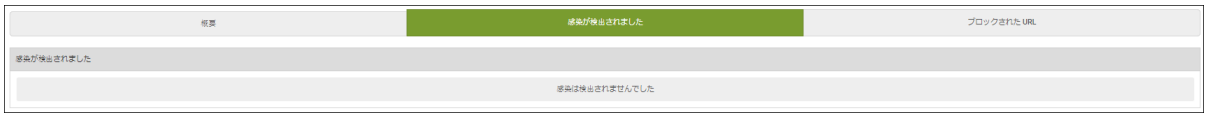
[概要] タブ

- バージョン番号
- サイト情報
- オペレーティング システム
- ネットワーク情報
- 保護
- プロパティ
- シールド

[感染が検出されました] タブ

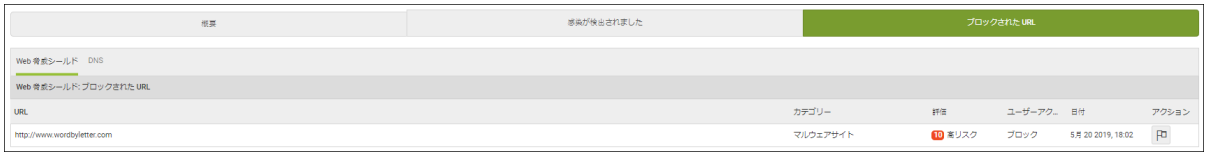
[**感染が検出されました**] タブをクリックして、デバイスが検出した感染に関する情報を表示します。

- ファイル名
- パス名
- マルウェア グループ
- 最終確認日時
- アクション



[ブロックされた URL] タブ

そのエンドポイントからブロックされた URL のリストを含みます。



[スキャン履歴] タブ

発生したすべてのスキャンと、スキャン中に検出された脅威に関する情報を表示します。詳細については、「*237{/u}{/color} ページの「スキャン履歴の表示」*」を参照してください。

デバイスの検索

デバイスを検索するには、次の手順に従ってください。

デバイスを検索するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. 左カラムで、検索するデバイスを含むサイトを選択します。

注意: サイトとグループレベルの両方でデバイスを検索できます。

4. [検索] フィールドに、検索するデバイスの名前を入力します。

必要に応じて、名前の一部を入力することもできます。その場合は、条件に一致するすべてのデバイスが表示されます。たとえば、デバイス名に「Brown」という文字が含まれていることが分かっていて、その他の部分が不明な場合は、「*Brown*」と入力します。

入力した検索条件に一致するデバイスのリストが表示されます。

5. [検索] フィールドをクリアするには、[X] をクリックします。

そのサイト内のすべてのデバイスが表示されます。

サイト名によるデバイスのフィルタリング

この手順に従って、デバイスを所属するサイトの名前で並べ替えます。

サイト名でフィルタリングするには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. [すべてのサイト] ドロップダウン メニューから、フィルタリングするサイトを選択します。

フィルタリングしたデバイスが表示されます。

4. すべてのデバイスをもう一度表示するには、[すべてのサイト] ドロップダウン メニューから、[**すべてのサイト**] を選択します。

デバイスの全リストが表示されます。

サイトの状態によるデバイスのフィルタリング

この手順に従って、デバイスをサイトの状態によってフィルタリングします。

状態によってデバイスをフィルタリングするには:

1. 管理コンソールにログインします。

   [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が表示されます。

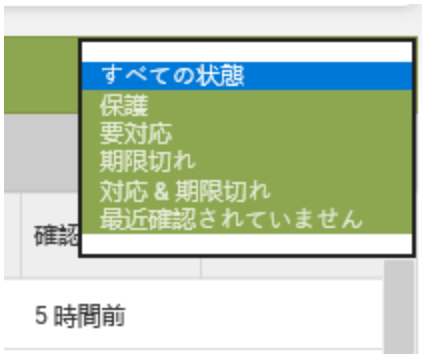
2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. [すべての状態]ドロップダウン メニューから、フィルタリングする状態を選択します。

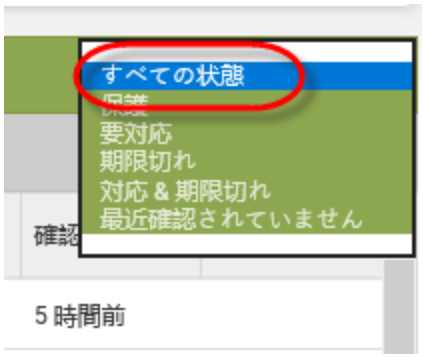
   選択可能な状態は次のとおりです。

   - **保護** - デバイスは Webroot SecureAnywhere によって保護されています。
   - **要対応** - デバイスに対応が必要です。
   - **期限切れ** - デバイスのライセンスの期限が切れており、Webroot SecureAnywhere によって保護されていません。
   - **対応 & 期限切れ** - デバイスへの対応が必要であるとともに、デバイスのライセンスの期限が切れており、Webroot SecureAnywhere によって保護されていないことを示しています。
   - **最近確認されていません** - デバイスは最近 Webroot SecureAnywhere によって確認されていません。



   状態によってフィルタリングしたデバイスが表示されます。

4. すべてのデバイスをもう一度表示するには、[すべての状態] ドロップダウン メニューから、[**すべての状態**] を選択します。



デバイスの全リストが表示されます。

グループ内のデバイスのフィルタリング

この手順に従って、グループ内のデバイスを状態に応じてフィルタリングします。

エンドポイントをフィルタリングするには:

1. 管理コンソールにログインします。

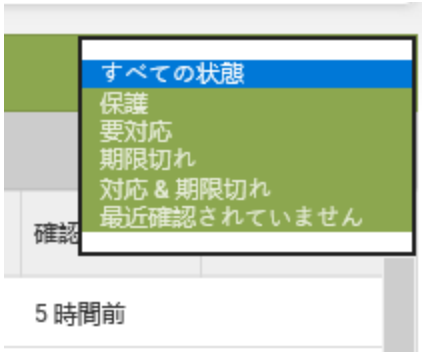
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**グループ**] タブをクリックします。

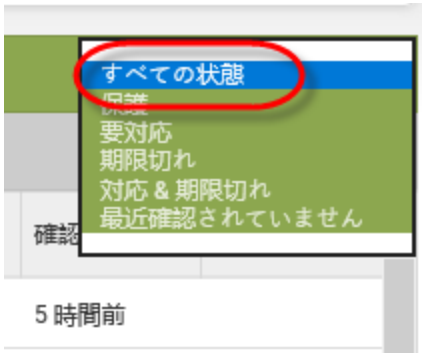
   [グループ] タブが表示されます。

3. 左カラムで、フィルタリングするグループを含むサイトを選択します。

4. [すべての状態] ドロップダウン メニューで、フィルタリングする状態を以下から選択します。
   - **保護** - デバイスは Webroot SecureAnywhere によって保護されています。
   - **要対応** - デバイスに対応が必要です。
   - **期限切れ** - デバイスのライセンスの期限が切れており、Webroot SecureAnywhere によって保護されていません。
   - **対応 & 期限切れ** - デバイスへの対応が必要であるとともに、デバイスのライセンスの期限が切れており、Webroot SecureAnywhere によって保護されていないことを示しています。
   - **最近確認されていません** - デバイスは最近 Webroot SecureAnywhere によって確認されていません。状態によってフィルタリングしたデバイスが表示されます。



5. すべてのデバイスをもう一度表示するには、[すべての状態] ドロップダウン メニューから、[**すべての状態**] を選択します。



デバイスの全リストが表示されます。

グループ間でのデバイスの移動

グループ間でデバイスを移動するには、この手順に従います。

デバイスを移動させるには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。

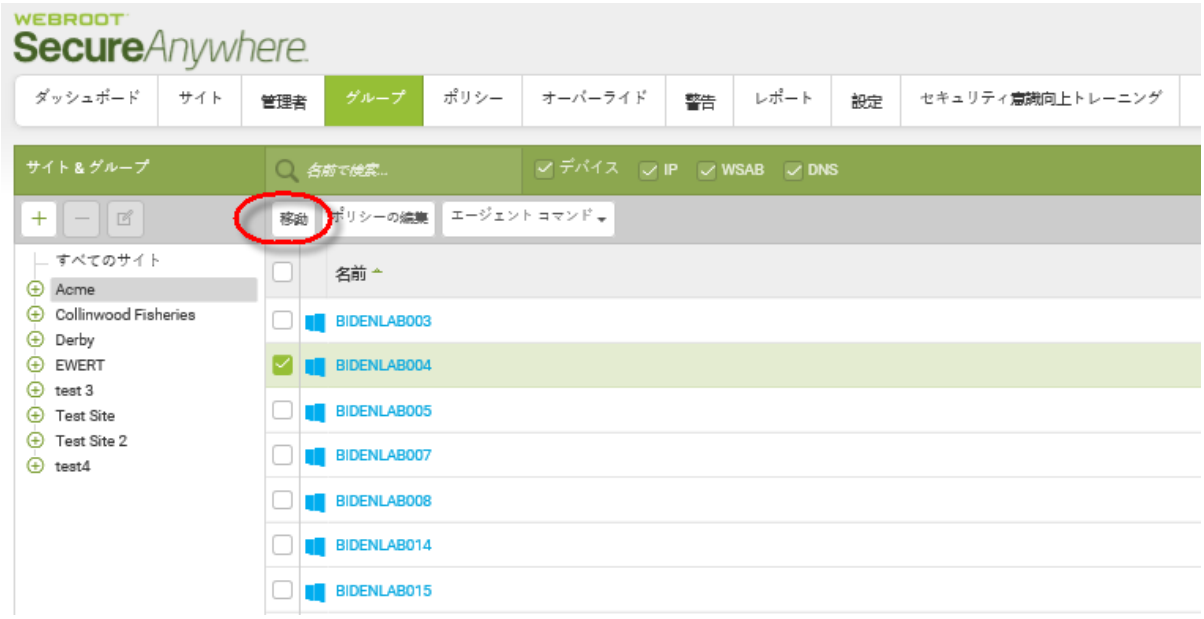
   [グループ] タブが表示されます。

3. 左カラムで、移動するグループを含むサイトを選択します。

4. 右側の [デバイス] パネルからひとつ以上のデバイスを選択します。

すべてのデバイスを選択するには、カラムの一番上にあるチェックボックスを選択します。

5. [**移動**] ボタンをクリックします。



[グループを移動] ウィンドウが表示されます。

6. [次のグループへ移動] ドロップダウン メニューから、デバイスを移動するグループを選択します。
7. 以下の [ポリシー管理] ラジオ ボタンのいずれかを選択します:
   - **新しいグループ ポリシーを自動的に継承**
   - **現在のポリシーを変更せずに移動**
8. [**移動**] ボタンをクリックします。

グループは新しいグループに移動されました。

グループ内のデバイスの並べ替え

グループ間でデバイスを並べ替えるには、この手順に従います。

デバイスを並べ替えるには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. 左カラムで、並べ替えるグループを含むサイトを選択します。

4. [デバイス] パネルで、各見出しの右側にある**上向き**または**下向き**矢印をクリックして次のカラムを並べ替えます。
   - **名前**
   - **確認済み**
   - **感染**

各カラムの情報の種類に基づいて、昇順か降順、またはアルファベット順で並べ替えが実行されます。

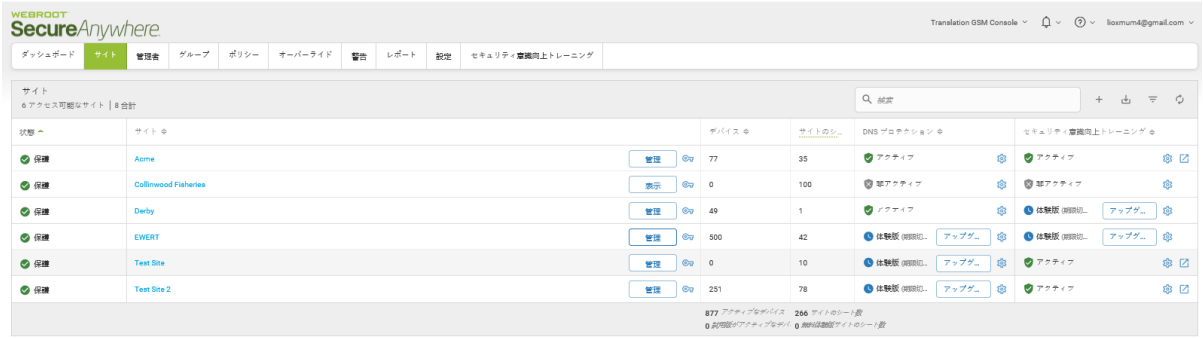
スキャン履歴の表示

特定のデバイスで発生したすべてのスキャンと、スキャン中に検出された脅威のリストを表示するには、以下の手順に従ってください。

スキャン履歴を表示するには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**グループ**] タブをクリックします。

   [グループ] タブが表示されます。

3. [すべてのサイト] ドロップダウン メニューから、フィルタリングするサイトを選択します。

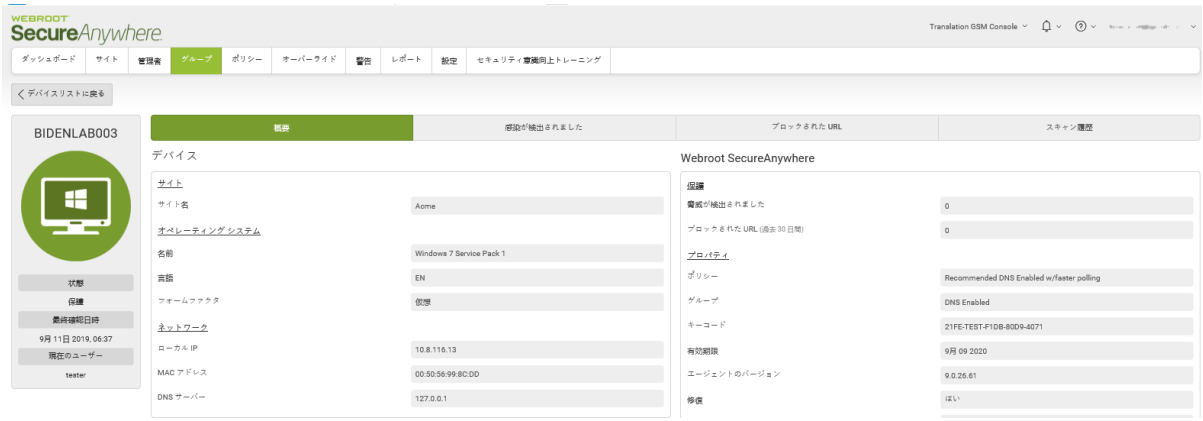
フィルタリングしたデバイスが表示されます。

4. すべてのデバイスをもう一度表示するには、[すべてのサイト] ドロップダウン メニューから、[**すべてのサイト**] を選択します。

デバイスの全リストが表示されます。

5. スキャン履歴を表示する対象のデバイスをクリックします。

[概要] タブがアクティブになった状態で [概要] パネルが表示されます。



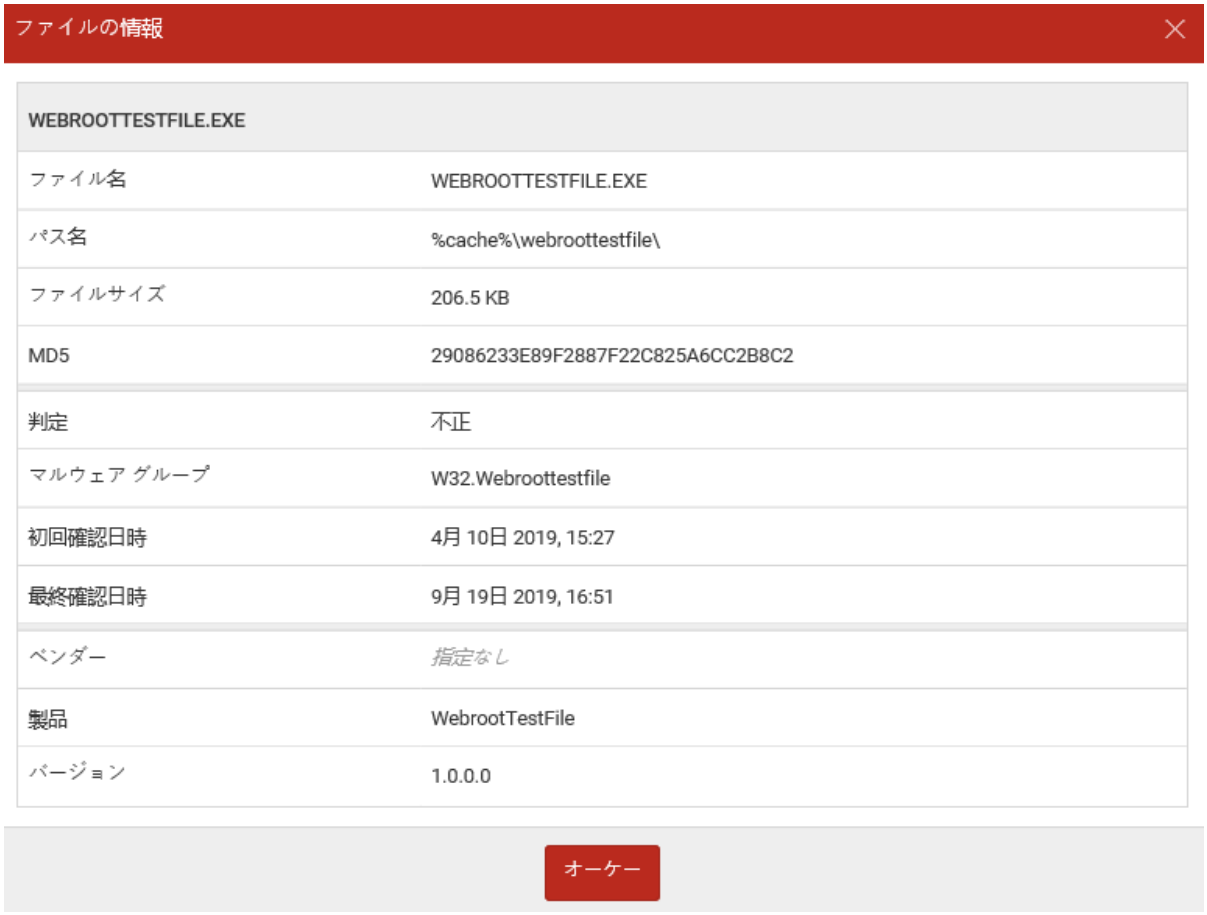
6. [**スキャン履歴**] タブをクリックします。

対象のデバイスのスキャン履歴が表示されます。これには次の情報が含まれます。

- スキャン日
- スキャン結果
- スキャンの種類

脅威が検出された場合は、ファイル名をクリックすると、検出された感染に関する情報を表示できます。

7. 情報の確認を完了した後、[**OK**] ボタンをクリックすると [スキャン履歴] タブに戻ります。



8. 情報を確認した後、[**デバイスリストに戻る**] ボタンをクリックするとデバイスのリストに戻ります。

エージェント コマンドの発行

[グループ] タブでエージェント コマンドを発行するには、以下の手順に従ってください。

注意: [エージェント コマンド] ドロップダウン メニューは、デバイス リストから 1 つ以上のデバイスを選択した後にのみアクティブになります。

エージェント コマンドを発行するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。

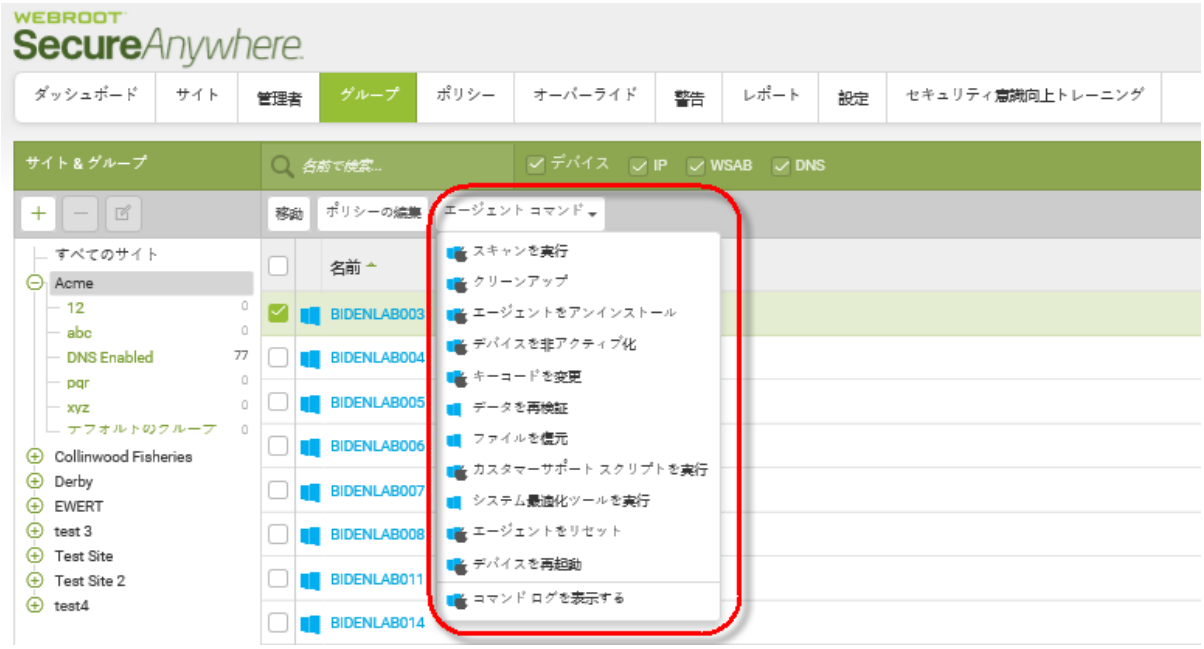
   [グループ] タブが表示されます。

3. 左カラムで、エージェント コマンドを発行する対象のグループとデバイスを含むサイトを選択します。

4. [デバイス] パネルで、エージェント コマンドを発行する対象のデバイスを選択します。

すべてのデバイスを選択するには、カラムの一番上にあるチェックボックスを選択します。

5. [エージェント コマンド] ドロップダウン メニューからポリシーを選択します。



次のような確認ウィンドウが表示されます。[**実行**] または [**キャンセル**] をクリックします。

6. さらに、[エージェント コマンド] ドロップダウン メニューから [**コマンド ログの表示**] を選択することもできます。詳細については、「*247{/u}{/color} ページの「エージェント コマンド ログの表示」*」を参照してください。

エージェント コマンド ログの表示

デバイスに送信したコマンドに関する情報を表示するには、以下の手順に従ってください。

注意: [エージェント コマンド] ドロップダウン メニューは、デバイス リストから 1 つ以上のデバイスを選択した後にのみアクティブになります。

エージェント コマンド ログを表示するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**グループ**] タブをクリックします。

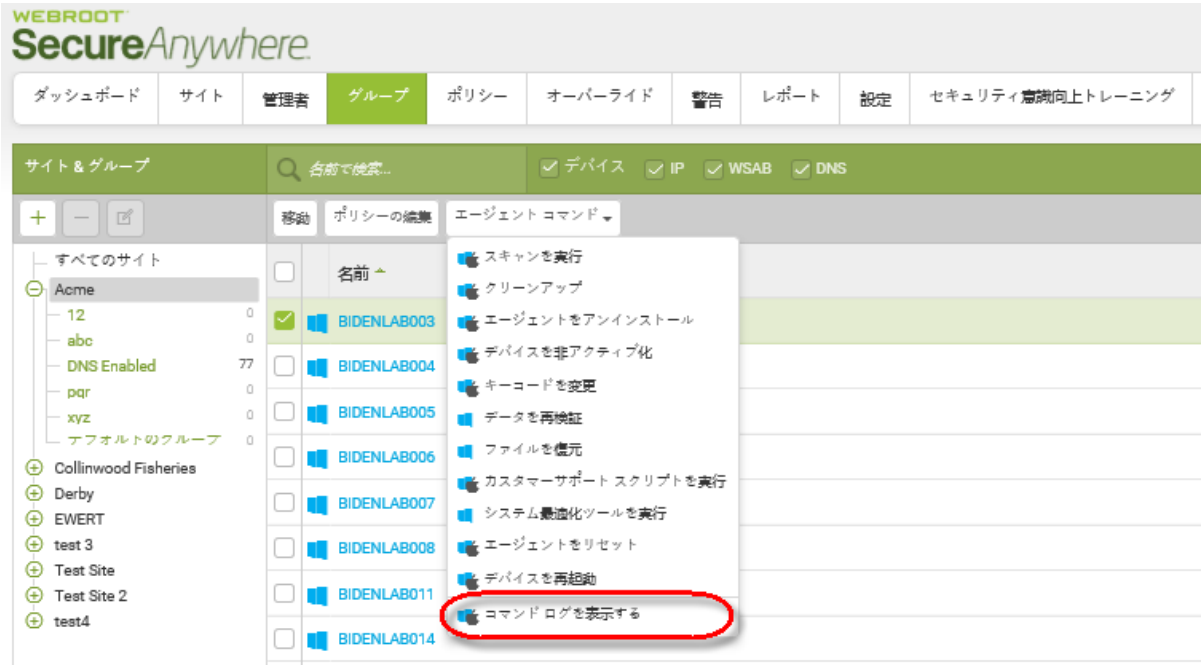
   [グループ] タブが表示されます。

3. 左カラムで、エージェント コマンド ログを表示する対象のグループとデバイスを含むサイトを選択します。

4. [デバイス] パネルで、エージェント コマンド ログを表示する対象のデバイスを選択します。

すべてのデバイスを選択するには、カラムの一番上にあるチェックボックスを選択します。

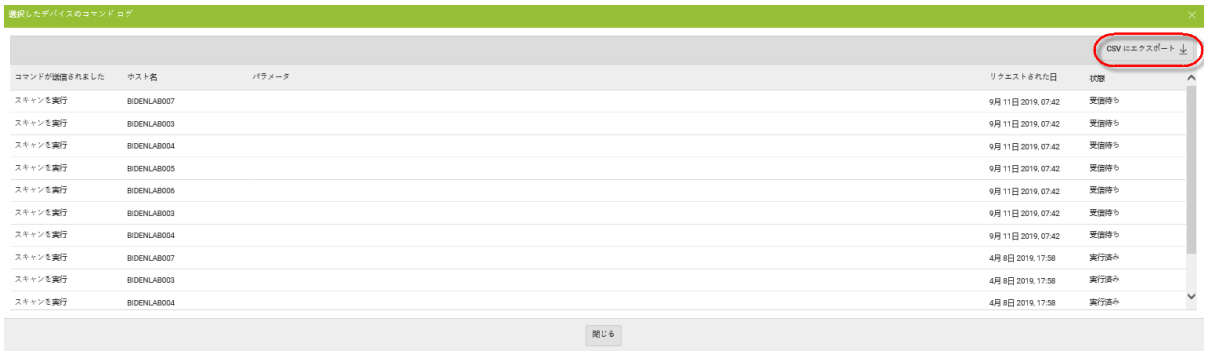
5. [エージェント コマンド] ドロップダウン メニューから [**コマンド ログの表示**] を選択します。



[選択したデバイスのコマンド ログ] ウィンドウが表示されます。これには次の情報が含まれます。

- コマンドが送信されました
- ホスト名
- リクエストされた日
- 状態

6. 必要に応じ、[**CSV にエクスポート**] ボタンをクリックしてエージェント コマンド ログのスプレッド シートをダウンロードすることもできます。



7. 完了したら、[**閉じる**] ボタンをクリックします。

第 7 章: ポリシーの操作

ポリシーを操作するには、次のトピックを参照してください:

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するかの、いずれかの方法をとることができます。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、ポリシー設定を決定できるようになります。詳細は「*260{/u}{/color} ページの「ポリシーの編集」*」を参照してください。

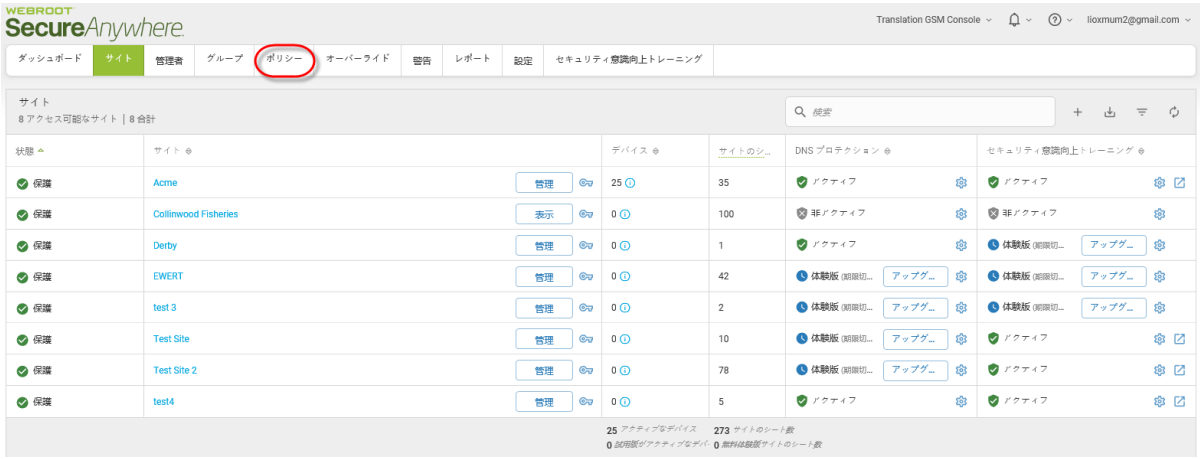
注意: ポリシー名は一意のものである必要があるため、後で競合を起こすことがないよう、事前にポリシー名についての計画を立てておいてください。一度ポリシー名をつけると、そのポリシーを削除した後でも同じ名前を再利用することはできません。

新しいポリシーを作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。

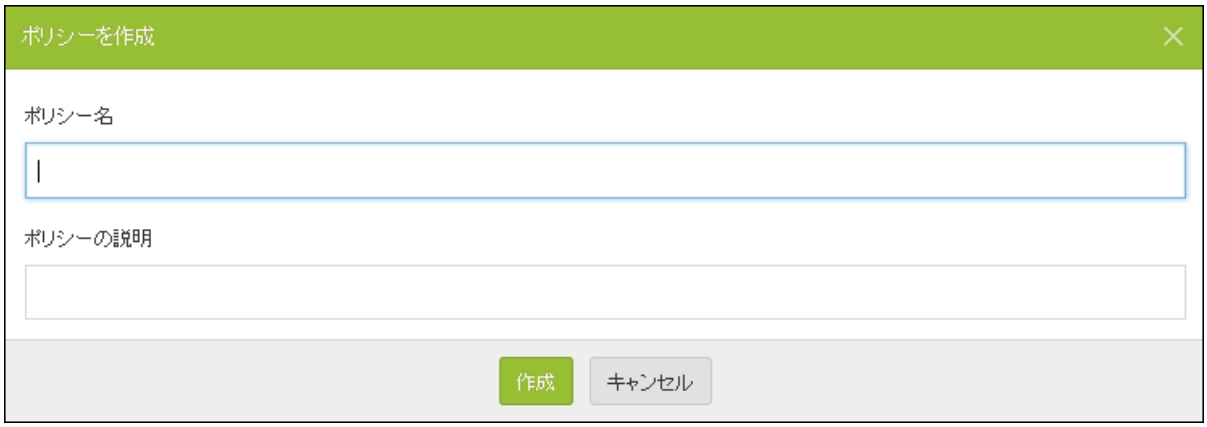
2. [**ポリシー**] タブをクリックします。



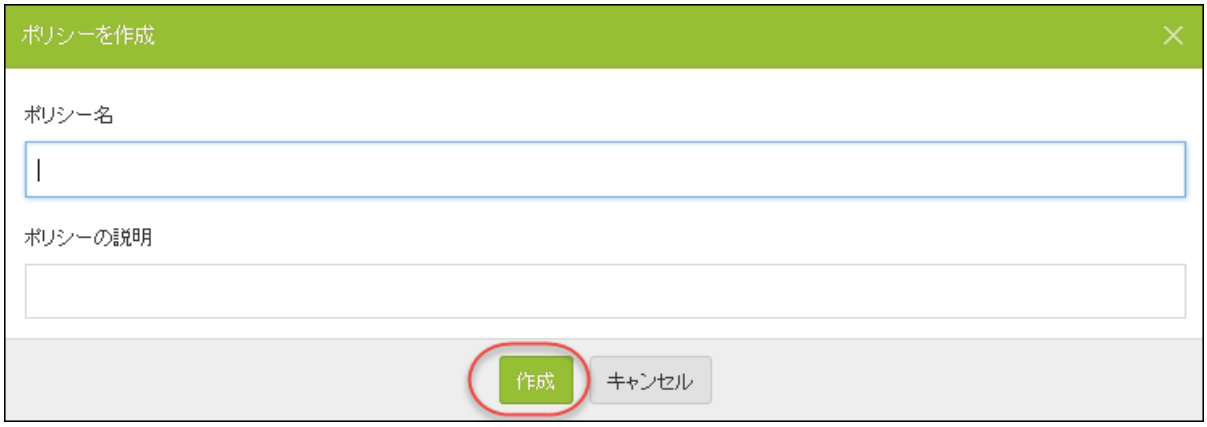
[ポリシー] タブが表示されます。

3. [**追加**] ボタンをクリックします。

[ポリシーを作成] ウィンドウが表示されます。

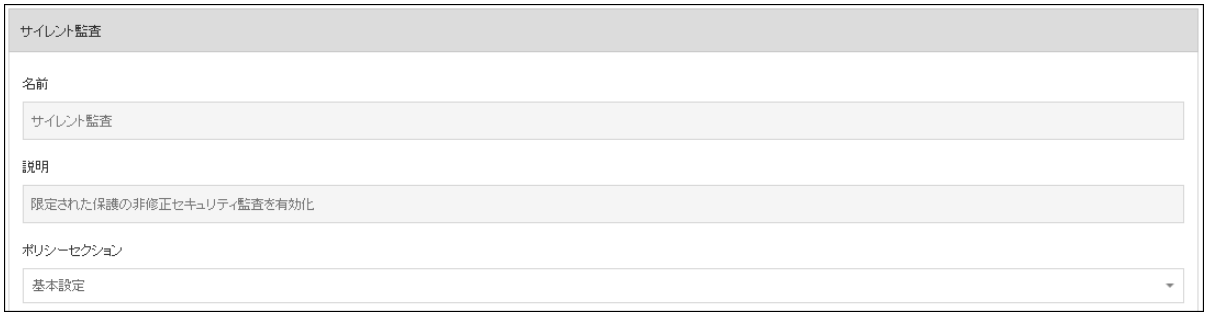


4. [ポリシーを作成] ウィンドウで、50 文字以内の英数字でポリシーの名前と説明を入力し、[**ポリシーを作成**] ボタンをクリックします。



5. [ポリシー] タブで新しいポリシーを確認します。設定を確認および変更するには、作成したポリシーをダブルクリックします。

そのポリシーの設定ウィンドウが表示され、推奨デフォルトが一番上に表示されます。

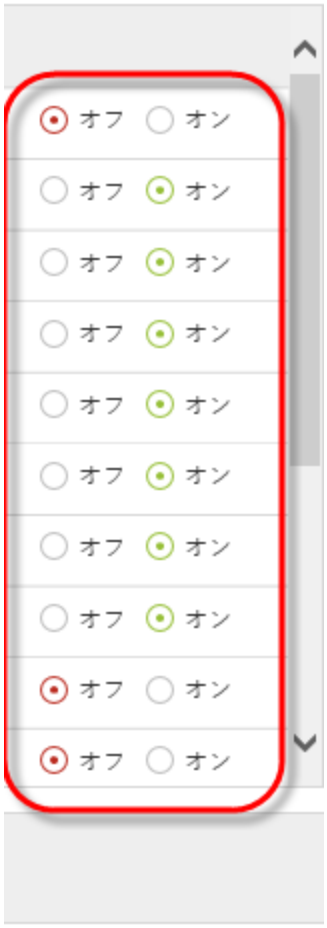


[設定] カラムに、以下に加えてポリシーの名前が表示されます:

- PC のみに適用される設定は、Windows のアイコンで示されます。

- PC と Mac に適用される設定は、Windows アイコンと Mac アイコンの両方で示されます。

[オン / オフ] カラムには、設定が現在エンドポイントでどのように実装されているかが表示されます。


オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン

ポリシーの編集

一度ポリシーを作成すると、ビジネスの目的に合わせてその設定を編集することができます。詳細については、「*253{/u}{/color} ページの「ポリシーの作成」*」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。

管理コンソールのサイトは以下のポリシーで管理されています。

セクション	説明
基本設定	一般設定では、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、また、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。
スキャンのスケジュール	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。
スキャン設定	徹底的なスキャンの実行など、スキャンをより詳細に管理できます。
自己保護	保護を追加して、悪質な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するのを防ぎます。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。

セクション	説明
ヒューリスティック	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。
Web 脅威シールド	ユーザーがインターネットを閲覧および検索結果をクリックする際に、エンドポイントを保護します。
ID シールド	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。
ファイアウォール	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。

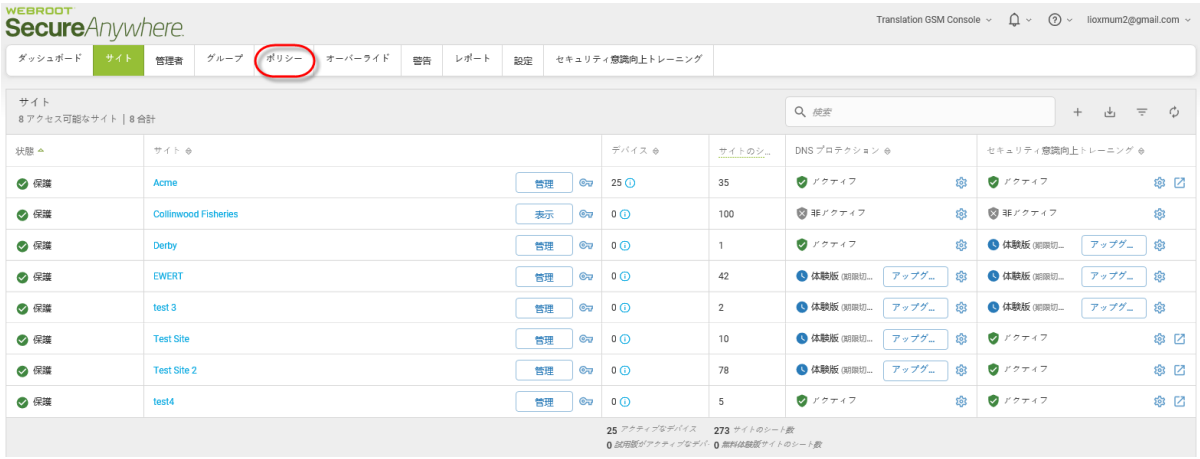
セクション	説明
ユーザー インターフェイス	エンドポイントでの SecureAnywhere プログラムへのユーザー アクセスを設定します。
システム最適化ツール	自動最適化のスケジュール、エンドポイントから削除するファイルや痕跡の種類など、システム最適化ツールの動作を制御します。

ポリシーを編集するには:

1. 管理コンソールにログインします。

   [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が表示されます。

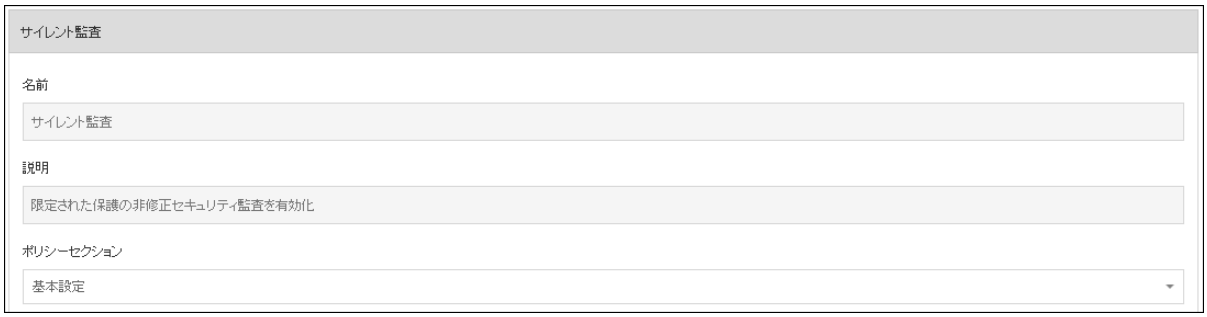
2. [**ポリシー**] タブをクリックします。



[ポリシー] タブが表示されます。

3. [ポリシー] のカラムで、設定を表示するポリシーをクリックします。

基本設定が選択された、ポリシーの設定ウィンドウが表示されます。



[設定] カラムに、以下に加えてポリシーの名前が表示されます:

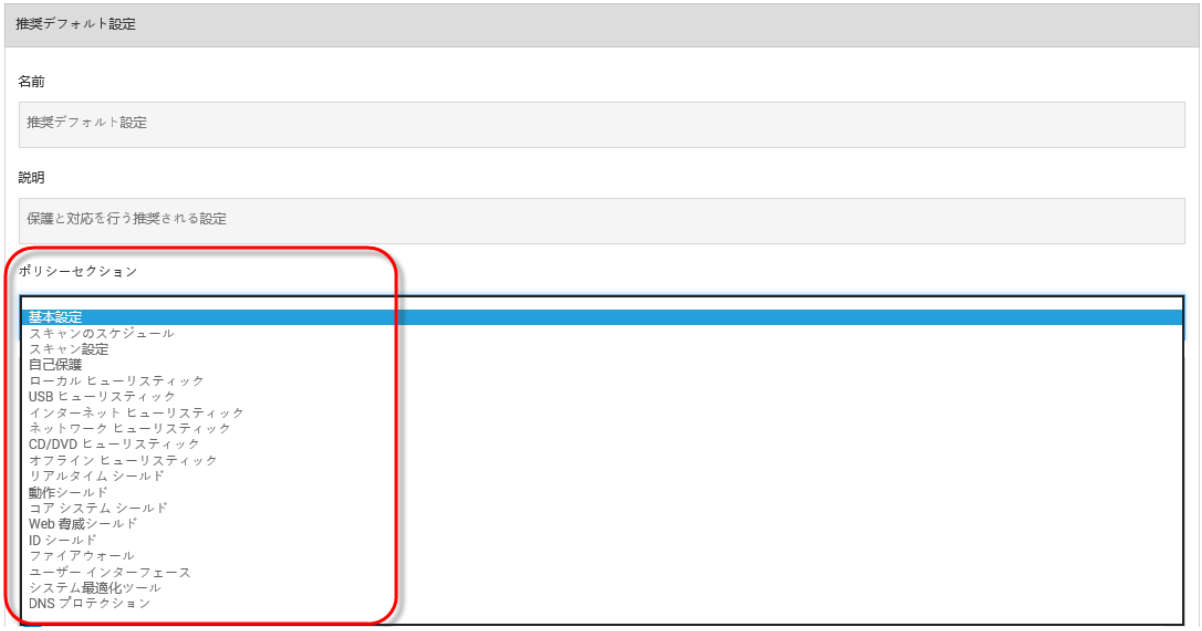
- PC のみに適用される設定は、Windows のアイコンで示されます。

- PC と Mac に適用される設定は、Windows アイコンと Mac アイコンの両方で示されます。

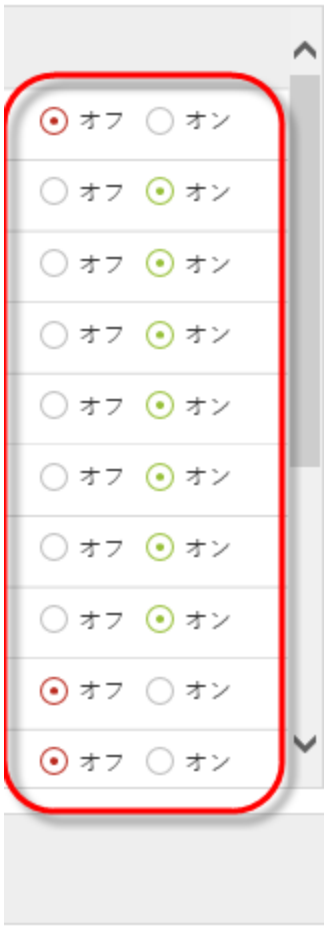
[オン / オフ] カラムには、設定が現在エンドポイントでどのように実装されているかが表示されます。


オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン
オフ オン

4. [ポリシー セクション] ドロップダウン メニューで、編集するカテゴリーを選択します。



5. その設定の [**オン**] または [**オフ**] を選択します。



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。

• 基本設定	• コア システム シールド
• スキャンのスケジュール	• Web 脅威シールド
• スキャン設定	• ID シールド
• 自己保護	• ファイアウォール
• ヒューリスティック	• ユーザー インターフェイス

• リアルタイム シールド	• システム最適化ツール
• 動作シールド	

6. 選択の変更を完了したら、[**保存**] ボタンをクリックします。

基本設定の設定

基本設定は、サイト上での 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 SecureAnywhere 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。
[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 SecureAnywhere 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
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。
詳細なロギングよりも低ディスク使用量を優先する (ログ情報量は少なくなります)	保存する最新のログ アイテムを 4 つに制限することで、ディスク容量を節約します。 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
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	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ションを実行中に、SecureAnywhere の機能を抑制します。 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。
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表示する	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。 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、または 2 時間など。 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

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。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。週 1 回または起動時に指定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	スキャンを実行する時間を指定します: • コンピュータの待機中のスキャン時間には、8:00 AM 前、正午前、5:00 PM 前、または深夜 0:00 AM 前のいずれかを指定できます。 • リソースが使用可能な場合のスキャン時間には、12:00 AM から 11:00 PM までの時刻を 1 時間単位で指定できます。 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。
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、スケジュールされたスキャンを、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 スキャンを実行しない	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徹底した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) スキャンを有効にする	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、それがオペレーティング システム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。
拡張ルー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質な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 エクスプローラーでの「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。
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たい場合は、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 SecureAnywhere 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。

設定	説明
高速スキャ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。
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	ユーザーがある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開きます。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。

設定	説明
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。
バックグラウンドのスキャ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。
高度なサポートを有効にする	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。

設定	説明
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。
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	PUA を検出し、インストールされるのをブロックします。 望ましくない可能性のあるアプリケーション (PUA) とは、必ずしも悪質ではないが、アドウェアやツールバー、あるいはその他の望ましくないツールをシステムに追加するプログラムを指します。一般的に PUA は悪質ではありませんが、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。 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 SecureAnywhere 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。 この設定は PC エンドポイントにのみ適用されます。
ファイルを脅威リサーチに送信することを許可する	ファイルを脅威リサーチに送信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、悪質なソフトウェアが SecureAnywhere プログラムの設定やプロセスを変更するのを防ぎます。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、内部の自己保護状態をアップデートします。

注意: SecureAnywhere 以外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	以下の検出レベルに設定することができます: • **最小** — SecureAnywhere 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。 • **中** — 他のプログラムが保護を無効にするのを防止します。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。 • **最大** — SecureAnywhere のプロセスに対して最高の保護を提供します。この設定を使用する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。

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調整できます:

- **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、新しいプログラムだけではなく、古いプログラムに対しても警告を発します。
- **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質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	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。 • **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。 • **低** — 非常に悪質な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。 • **中** — 一元化されたコミュニティ データベースにおいて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。 • **高** — さまざまなレベルの新しい脅威に対して保護します。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。 • **最大** — 新しい脅威に対して最高レベルの保護を提供します。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。 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
経時ヒューリスティック	コミュニティ内で使用された時間に基づいて、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。 • **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。 • **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。 • **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。 • **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がインストールされることがほとんどなく、システムが比較的安定していると感じる場合にのみお勧めします。この設定では、不明瞭または一般的でないプログラムに対して、誤検出が多くなることがあります。 • **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。 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
頻度ヒューリスティック	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、統計上は一般的ではないとみなされることがあります。 • **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またはベータ プログラムが頻繁にインストールされる場合や、エンドポイントのユーザーが新しいプログラムを頻繁に作成するソフトウェア開発者である場合にお勧めします。 • **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頻繁にインストールすることを許可せず、標準の設定よりもセキュリティを強化する必要がある場合に使用することをお勧めします。 • **高** — コミュニティの一定数で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インストールすることを許可せず、現在感染していると疑われる場合にお勧めします。 • **最大** — コミュニティの大多数で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。 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 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。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 シールド有効	リアルタイム 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。
SecureAnywhere 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	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、エンドポイントがオフラインのときにも保護します。この設定はオンの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。
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	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、またはそのままブロックしたか) を記憶し、同じファイルを発見した場合に次回からはプロンプトを表示しません。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開かれます。 この設定は PC エンドポイントにのみ適用されます。
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。
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。

設定	説明
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、脅威が実行されるのを阻止します。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。
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、管理されている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、その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時に、未分類のプログラムが変更を加えようとすると、警告が発せられます。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	スパイウェアが 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のを阻止し、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、ユーザーがネットサーフィン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使用すると、このシールドは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、またリスクとなりう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 脅威シールド有効	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	ブラウザのエクステンションにより、悪質な 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が提供されます。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。
悪質な 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、既知の悪質な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、サイトが悪質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	悪質な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。

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	悪質な Web サイトが検出された時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。
Web サイトの評価をユーザーがリクエストする機能を無効化	悪質な Web サイトが検出された時に、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。 **注意:** Mac では、これは、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。シールドが悪質な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。
フィッシングの脅威がないか Web サイトを検証する	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、フィッシングの脅威がないか Web サイトを分析します。シールドがフィッシングの脅威を検出した場合、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。
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。

設定	説明
Web サイトの DNS/IP 解決を検証して中間者攻撃を検出する	ユーザーを悪質な 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。
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 が悪質な追跡型 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するのをブロックします (たとえば、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示したりする際にブロック)。 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、SecureAnywhere 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	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、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 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、または許可するかを決定します。

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	• **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する。 • **不明および感染している場合に警告** — エンドポイントが感染している場合、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際に警告する。 • **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際に警告する。 • **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、あらゆるプロセスがインターネットに接続する際に警告する。 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
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、SecureAnywhere により表示される警告を制御します: • **オン** — SecureAnywhere が Windows ファイアウォールがオフであることを検出す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の時で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。

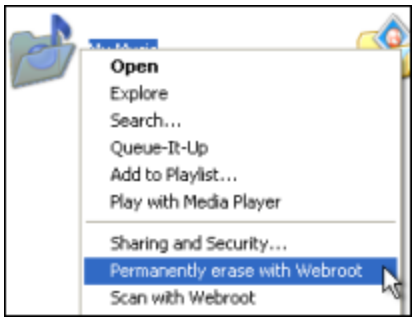
設定	説明
GUI	エンドポイントのユーザーによる SecureAnywhere メイン インターフェイスへのアクセスをブロックまたは許可します。このオプションが [非表示] に設定されている場合にユーザーが SecureAnywhere を開こうとすると、インターフェイスにアクセスするには管理者に問い合わせるよう案内するメッセージが表示されます。 この設定は PC および Mac エンドポイントの両方に適用されます。 **注意:** このオプションはウェブルート システムトレイのアイコンを表示します。ただし、Mac では、このオプションはウェブルート システムトレイのアイコンを表示します。

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、および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。クリーンアップをスケジュールし、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を、スキャンはセキュリティ保護を担当してい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。 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 エクスプローラー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永久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すると、次のメニューアイテムが表示されます:  この設定は PC エンドポイントにのみ適用されます。
Windows 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
最近使ったドキュメント履歴	最近開いたファイルの履歴をクリアします。この履歴には Windows の [スタート] メニューからアクセスできます。 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	[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。この履歴へは [スタート] メニューからアクセスできます。 [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あるアルファベット順に戻します。この一覧は、クリーンアップの実行後、システムを再起動すると、アルファベット順に戻ります。 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	クリップボードの内容をクリアします。Windows のすべてのプログラムでは、[コピー] または [貼り付け] 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)。この一時フォルダは通常 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。
システム一時フォルダ	システム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)。この一時フォルダは通常 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。

設定	説明
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。
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。

設定	説明
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\[ユーザー名]\Local Settings\Application Data\Microsoft\CDBurning または C:\Users\[ユーザー名]\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。
Flash cookie	Adobe Flash によって作成されたデータを削除します。これらのデータはユー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性があります。Flash Cookie は実際には Cookie ではなく、ブラウザの Cookie のプライバシー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。

設定	説明
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。
一時インターネット 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。

設定	説明
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。
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するものとしてマークし、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ます。このオプションは、[Cookie]、[一時インターネット ファイル]、または [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、ファイルを永久に削除します。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。

ポリシーの名前の変更

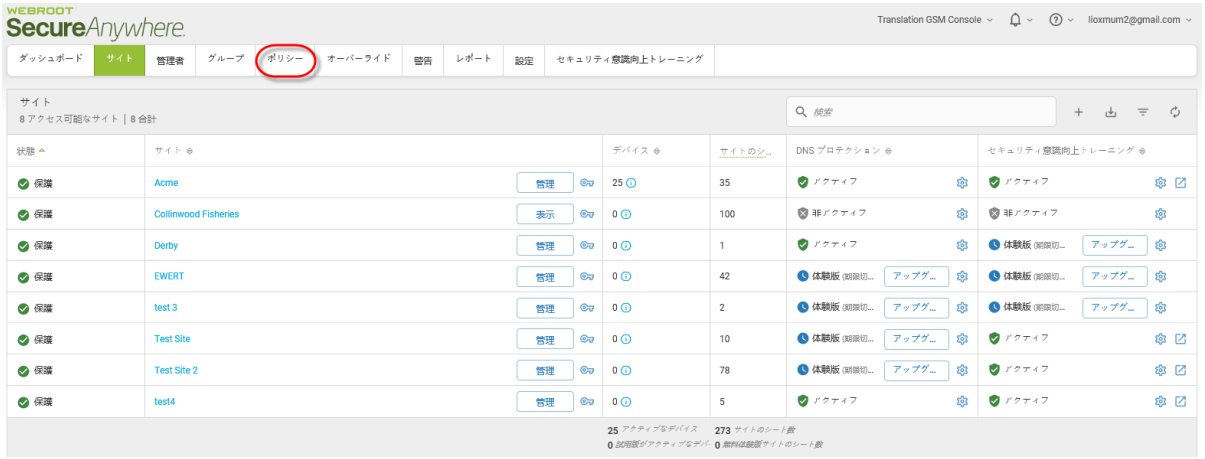
ポリシーの他のセクションを編集することなくポリシーの名前を変更するには、次の手順に従ってください。

ポリシーの名前を変更するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**ポリシー**] タブをクリックします。



   [ポリシー] タブが表示されます。

3. [ポリシー] のカラムで、名前を変更するポリシーを選択します。

注意: デフォルトのウェブルート ポリシーでは、[名前] または [説明] フィールドの情報を編集することはできません。

4. [名前] フィールドに新しい名前を入力します。

5. 設定が完了したら [**保存**] ボタンをクリックします。

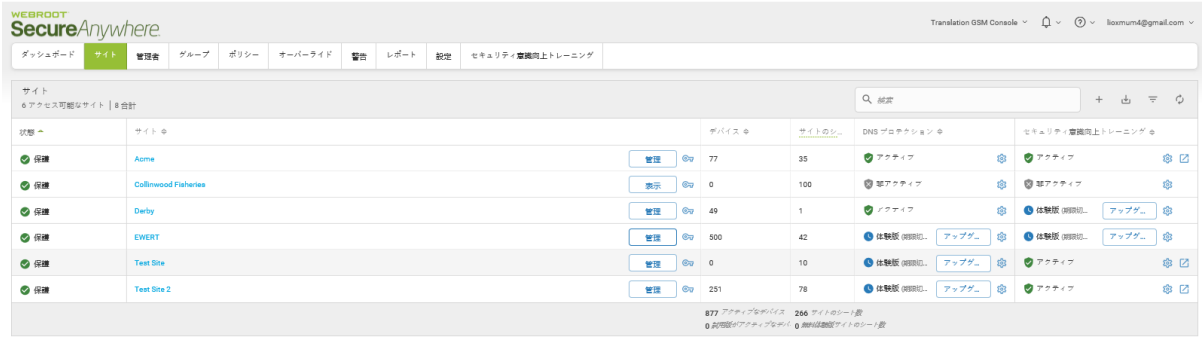
ポリシーのコピー

ポリシーをコピーするには、次の手順に従ってください。これは、既存のポリシーに似た新しいポリシーを作成する場合に便利です。

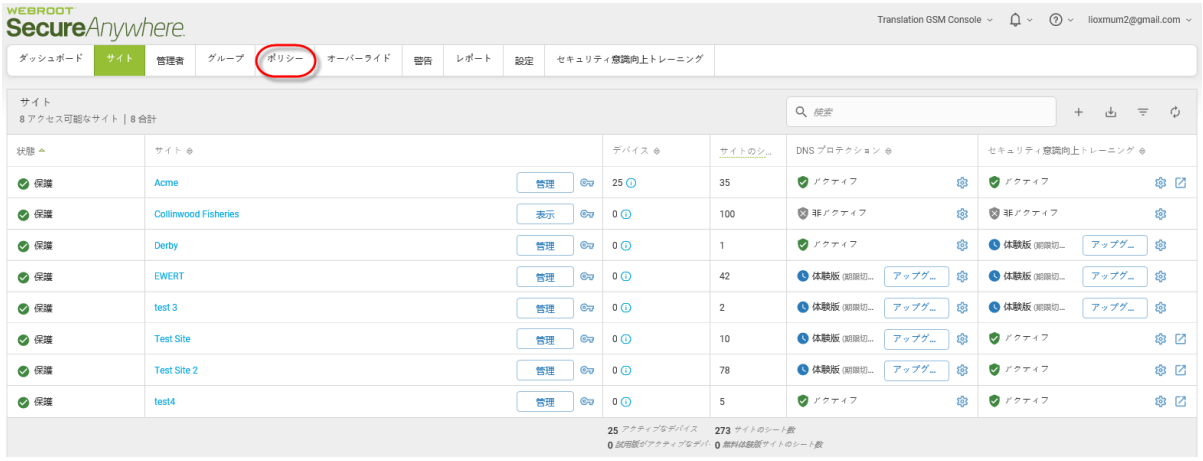
ポリシーの名前を変更するには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**ポリシー**] タブをクリックします。

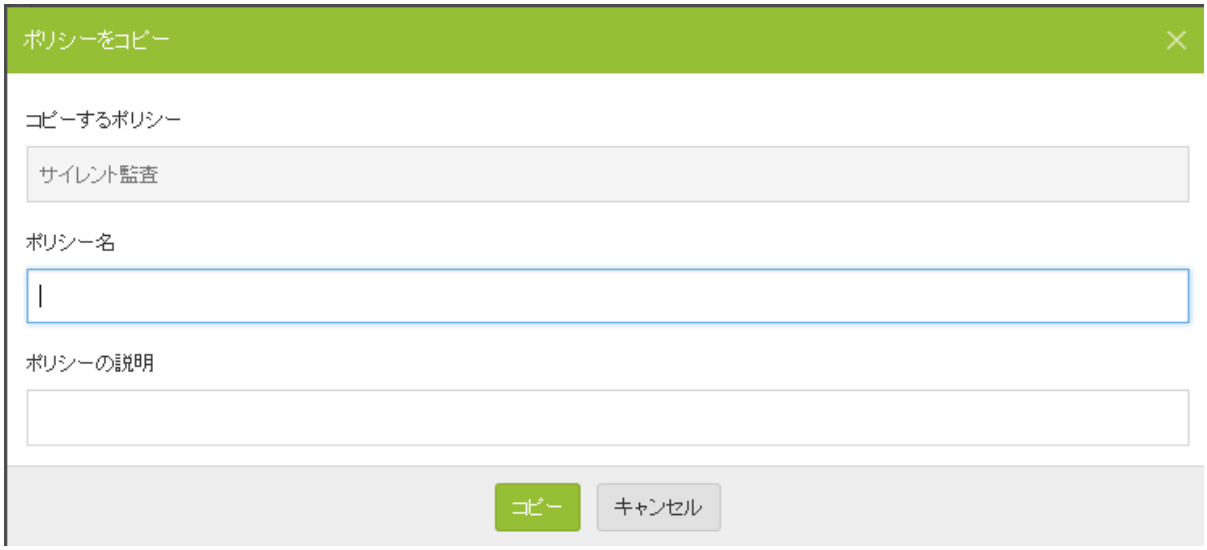


   [ポリシー] タブが表示されます。

3. [ポリシー] のカラムで、コピーするポリシーを選 択します。

4. [**コピー**] ボタンをクリックします。

[ポリシーのコピー] ウィンドウが表示されます。



5. [ポリシー名] フィールドにポリシーの新しい名前を入力します。
6. [ポリシーの説明] フィールドに新しいポリシーについての説明を入力します。

7. 設定が完了したら [**コピー**] ボタンをクリックします。

ポリシーを手動でインポート

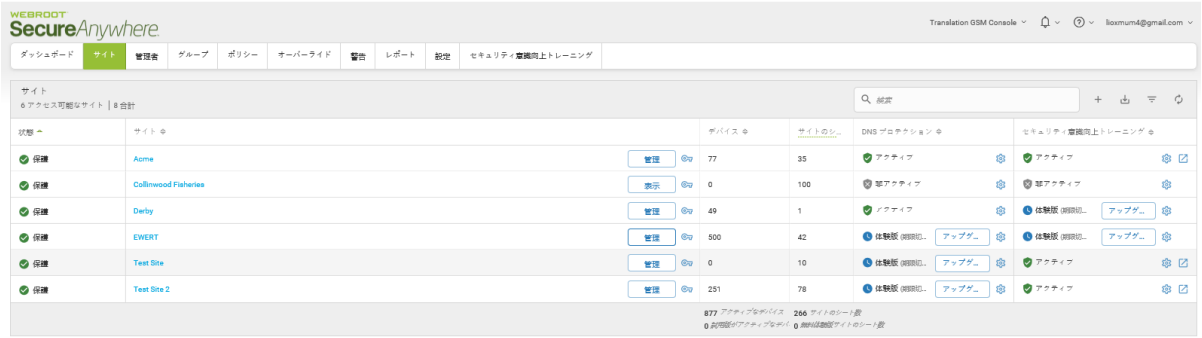
管理者がアクセスできないサイトからポリシーをインポートする場合は、この手順に従って、手動でのみインポートすることができます。

この手順は、管理者が異なる電子メールアドレスで複数のアカウントを持っていたり、転送コードを電子メールで友人に送信し、友人が自身のサイトにインポートできるようにする場合などに便利です。

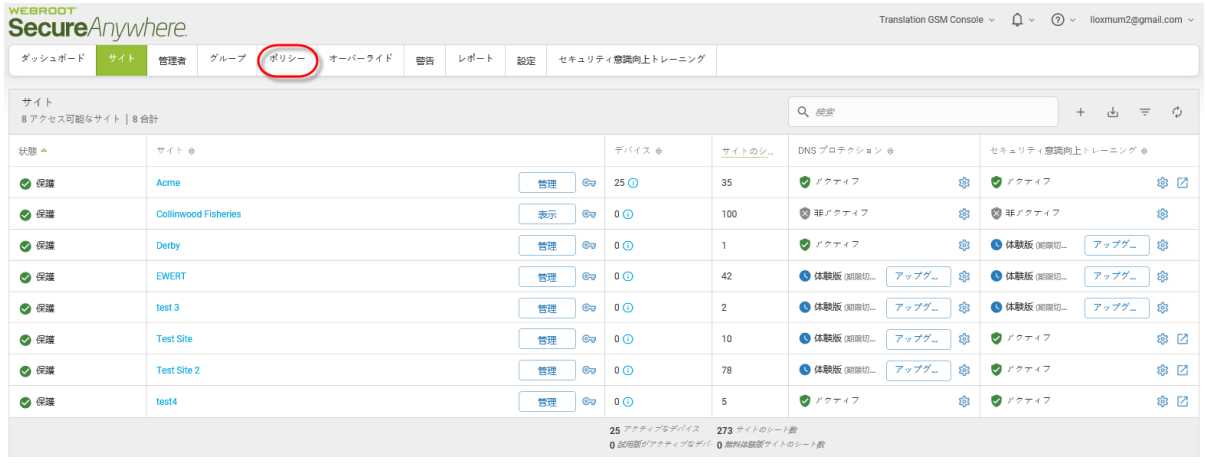
ポリシーを手動でインポートするには:

1. 管理コンソールにログインします。

   [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が表示されます。



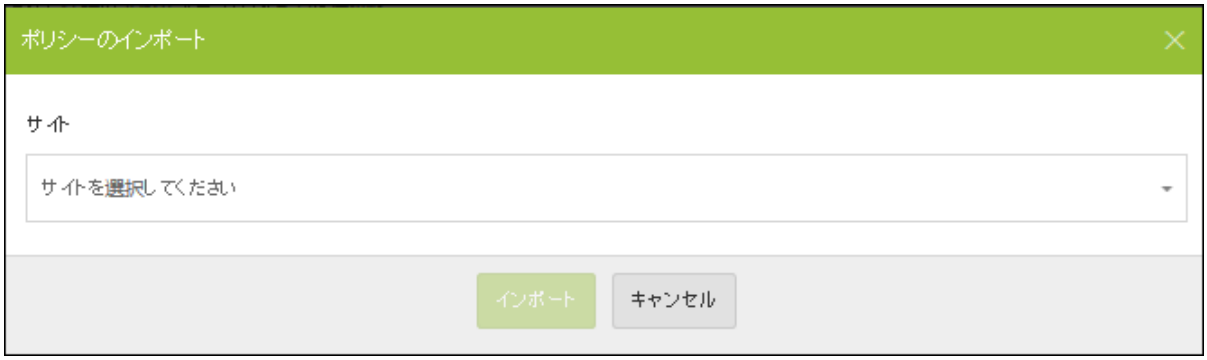
2. [**ポリシー**] タブをクリックします。



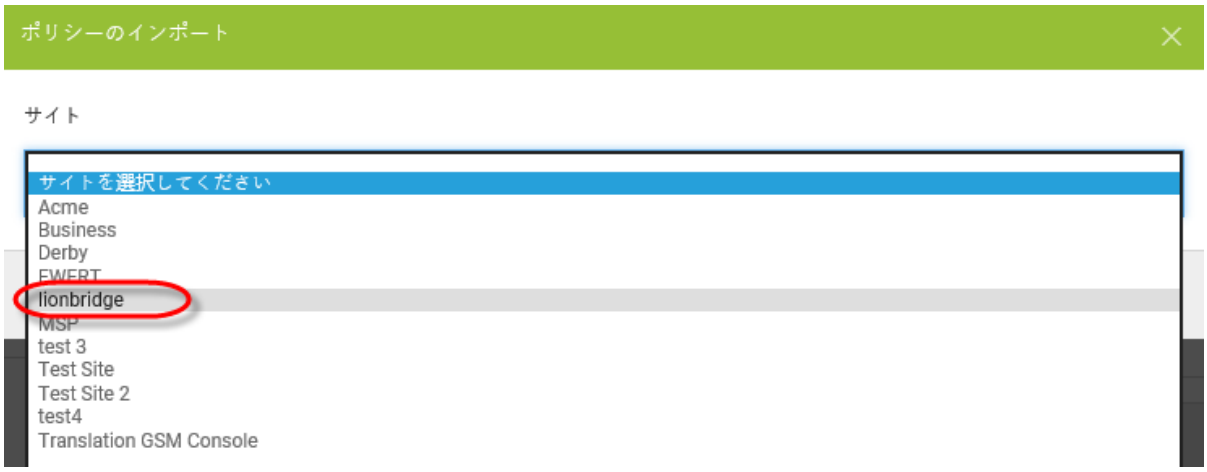
   [ポリシー] タブが表示されます。

3. [**インポート**] ボタンをクリックします。

[ポリシーのインポート] ウィンドウが表示されます。



4. [サイト] ドロップダウン メニューから、ポリシーのインポート元サイトを選択します。



[ポリシー] フィールドがアクティブになります。

5. [ポリシー] ドロップダウン メニューから、インポートするポリシーを選択します。

6. 設定が完了したら、[**インポート**] ボタンをクリックします。

ポリシーが、グローバル ポリシーとして管理コンソールに転送されます。

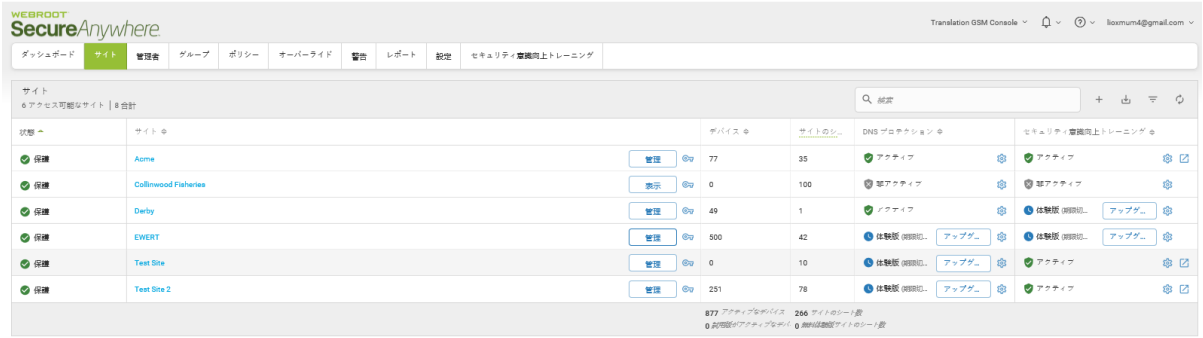
ポリシーの削除

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、そのポリシーはアクティブなポリシーのリストから削除されます。

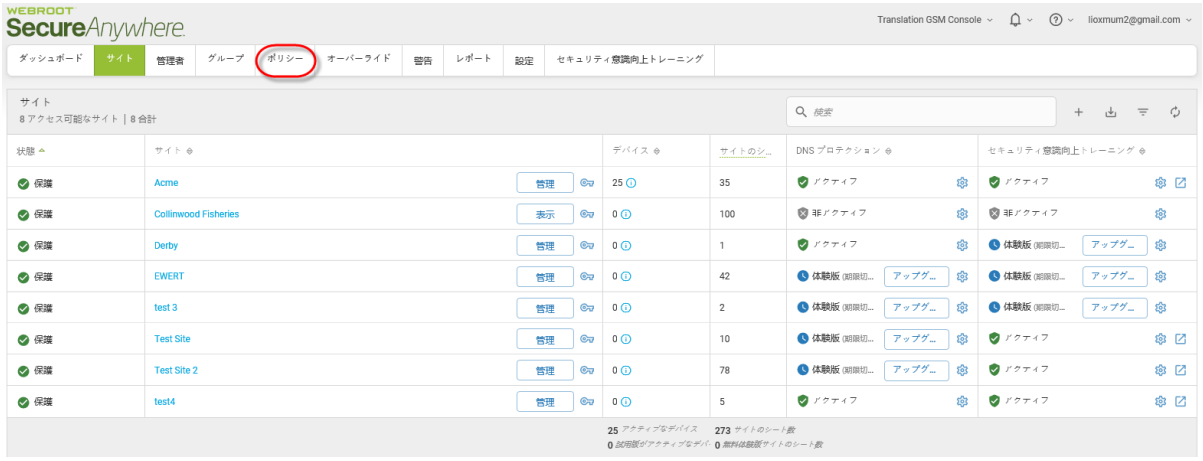
ポリシーを削除するには:

1. 管理コンソールにログインします。

   [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が表示されます。

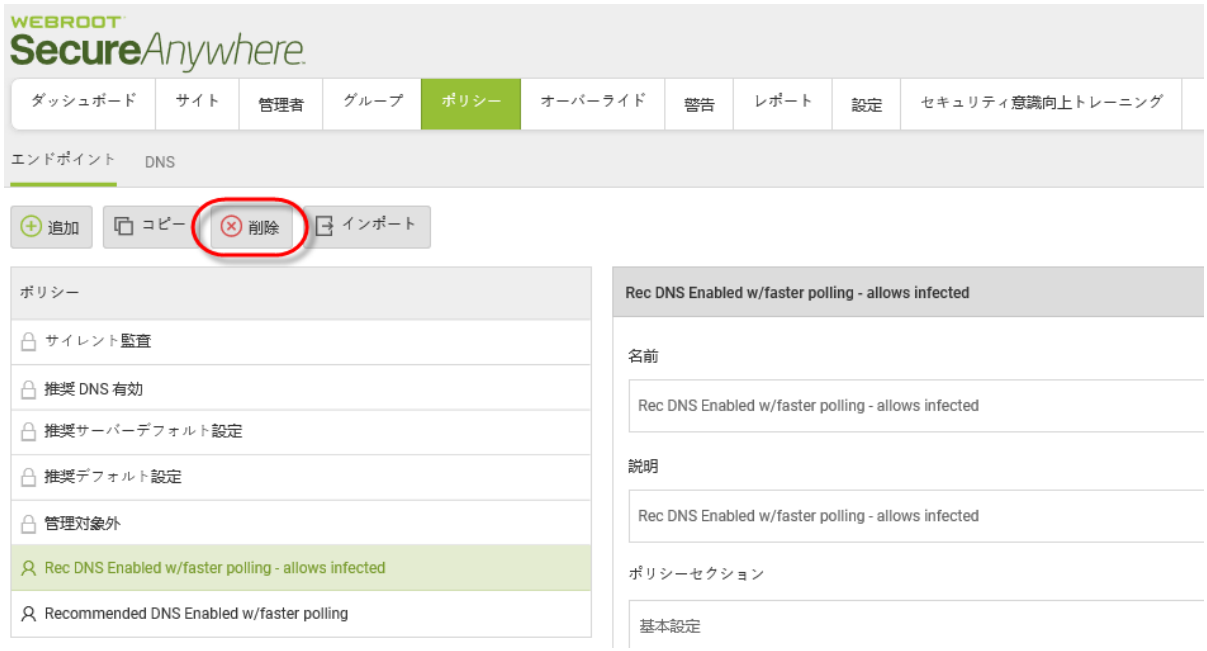


2. [**ポリシー**] タブをクリックします。



   [ポリシー] タブが表示されます。

3. [ポリシー] カラムで、削除するポリシーを選択し、[**削除**] ボタンをクリックします。

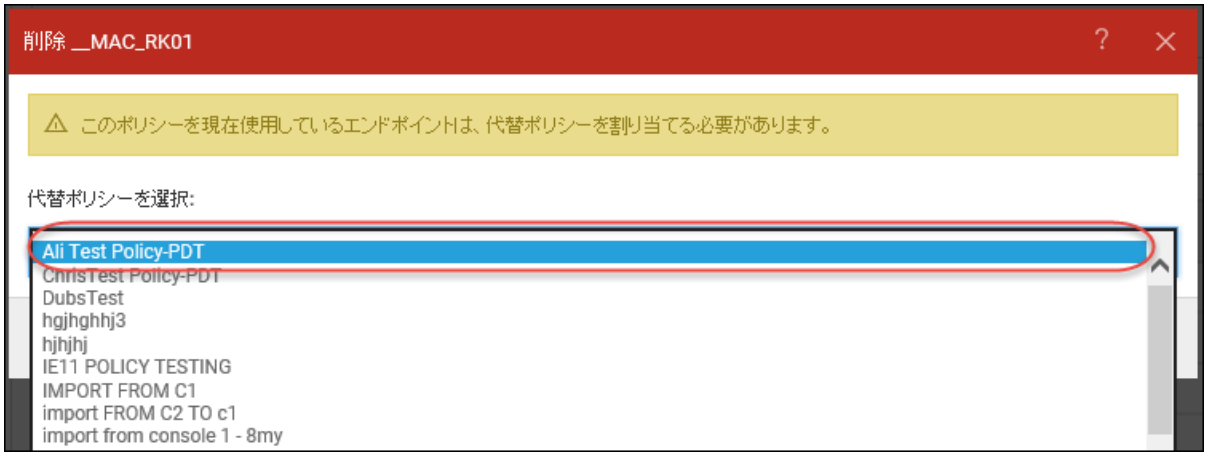


注意: デフォルトのポリシーは削除できません。そのため、クリックしても [削除] ボタンはアクティブになりません。

[標準ポリシーの削除] ウィンドウが表示されます。

注意: このポリシーを現在使用しているエンドポイントは、代替ポリシーを割り当てる必要があります。

4. 必要に応じて、[代替ポリシーの選択] ドロップダウン メニューから新しいポリシーを選択します。



5. [**削除の確認**] ボタンをクリックし、必要なすべての代替ポリシーを割り当てます。

ポリシーが削除されます。

第 8 章: オーバーライドの操作

オーバーライドを操作するには、次のトピックを参照してください:

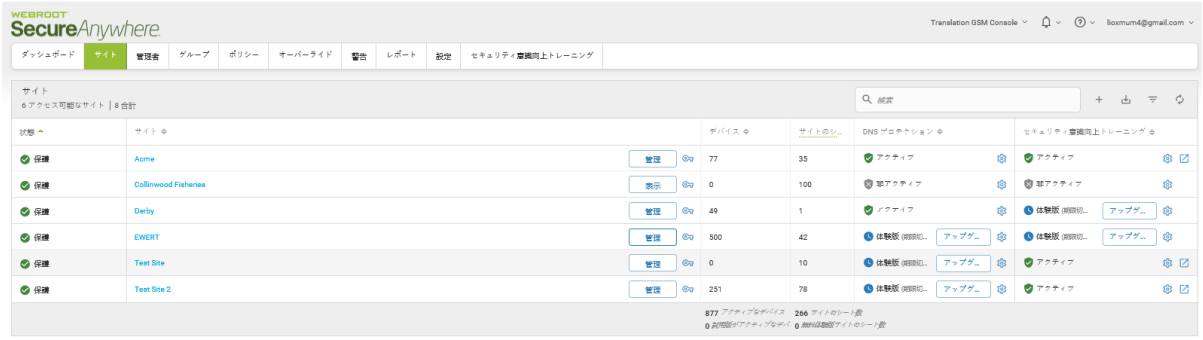
ウェブのオーバーライドの作成

この手順に従って、デフォルトの Web 脅威に対する保護機能のデフォルトの分類をオーバーライドするウェブのオーバーライドを作成します。

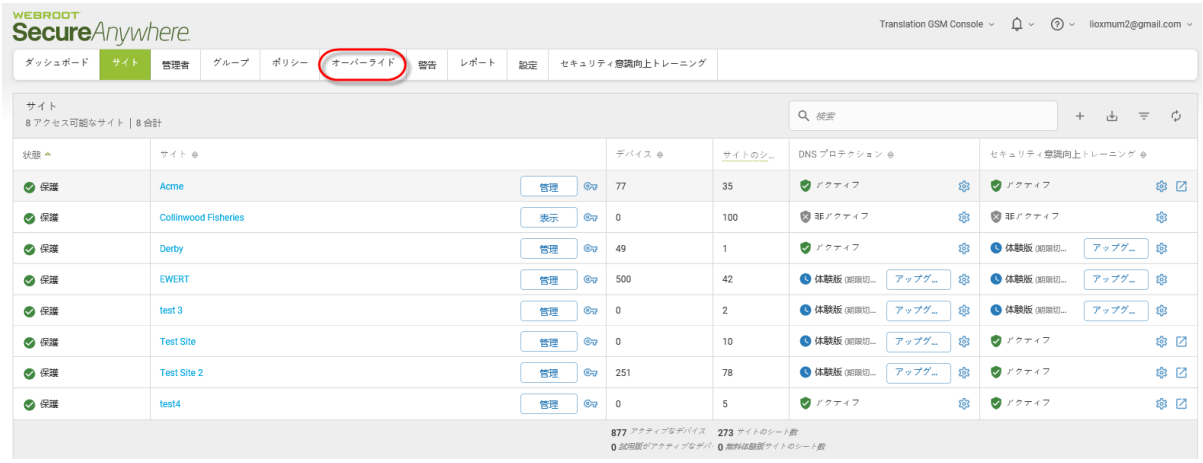
ウェブのオーバーライドを作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**オーバーライド**] タブをクリックします。



   [ファイルのホワイトリスト] 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。

3. [**ウェブのブロック / 許可リスト**] タブをクリックします。

[ウェブのブロック / 許可リスト] タブが表示されます。

4. [**追加**] ボタンをクリックします。

[新規エントリの作成] ウィンドウが表示されます。

5. [ドメイン] フィールドに、ウェブのオーバーライドとして追加する URL を入力します。

   注意: URL を入力する際は、*www*、*http*、または *https* などのプロトコルを入力する必要はありません。また、このフィールドではワイルドカードがサポートされています。

6. [スコープ] で、次のいずれかのラジオ ボタンを選択して、どのサイトでオーバーライドを作成するかを決定します。
   - **グローバル** - このエントリはサイトの設定で [グローバル オーバーライドの追加] チェックボックスが選択されているすべてのサイトで利用することができます。詳細については、「*114{/u}{/color} ページの「サイト設定の編集」*」を参照してください。
   - **サイト** - 選択した特定のサイトにウェブのオーバーライドを適用します。

7. [サイト] ラジオ ボタンを選択した場合は、[サイト] ドロップダウン メニューからサイトを選択します。

注意: サイトに DNS プロテクションが適用されている場合は、「DNS プロテクション管理者ガイド」で、「Working With Block Pages and Overrides」(ブロック ページとオーバーライドの操作) セクションの「DNS プロテクション オーバーライドの作成」を参照してください。

8. 設定が完了したら、[**作成**] ボタンをクリックします。

ホワイトリストのオーバーライドの作成

管理コンソールとサイト レベルの両方のオーバーライド ページでホワイトリストのオーバーライドを作成できるようになりました。

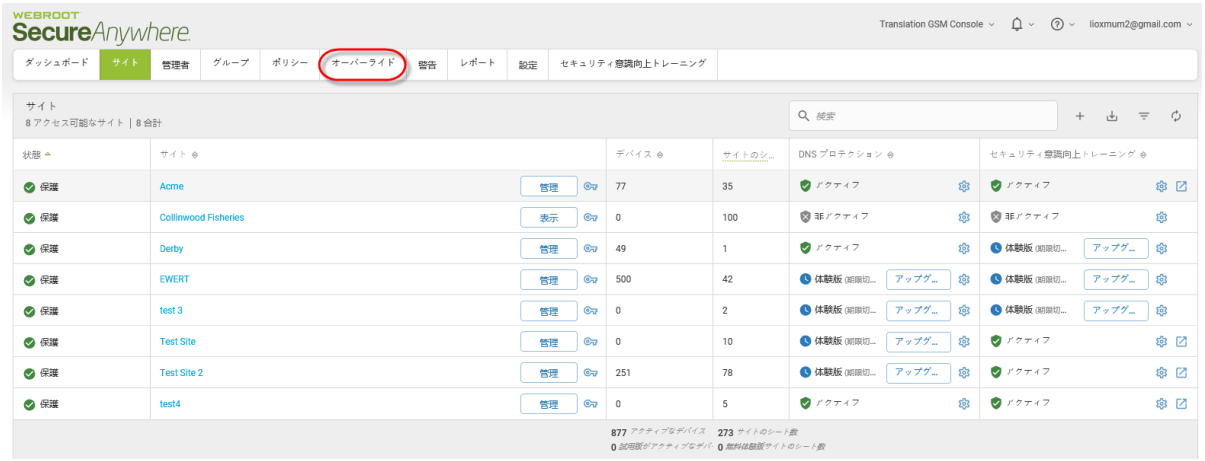
グローバル規模のホワイトリストのオーバーライドは、これまでの MD5 レベルだけでなく、ファイルやフォルダのレベルでも設定できるようになりました。このアップグレードで、より柔軟にオーバーライドを設定できるようになったため、複数の関連する MD5 をオーバーライドする際にも個別にホワイトリストを作成せずに、関連ディレクトリ全体を一括でホワイトリスト化することができます。

ホワイトリストのオーバーライドを作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**オーバーライド**] タブをクリックします。



[ファイルのホワイトリスト] 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。

3. [**追加**] ボタンをクリックします。

4. [新規ホワイトリスト エントリ] ウィンドウが表示されます。

5. MD5 のオーバーライドのタイプを作成するには:
   - [名前 / 説明] フィールドにオーバーライドの名前を入力します。
   - [MD5] ラジオ **ボタン**を選択します。
   - [MD5] フィールドに、ファイルに付けられた 32 英数字の固有識別子を入力してください。
   - [作成] ボタンを
     クリックしま
     す。
6. フォルダ / ファイルのオーバーライドを作成するには、この手順を続けて行います。

> **注意:** ファイル / フォルダのオーバーラードを使用するにはまず、エンドポイントが Webroot SecureAnywhere エンドポイント プロテクションのバージョン 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] のウィンドウで、[**フォルダ / ファイル**] のラジオ ボタンを選択します。

関連フィールドを含む [新規ホワイトリスト エントリ] のウィンドウが表示されます。

8. 次の表を参照してウィンドウの各フィールドに情報を入力してください。

フィールド	説明
名前 / 説明	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。
オーバーライドの種類	[フォルダ / ファイル] のラジオ 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。
パス / フォルダ マスク	オーバーライドの対象となるフォルダです。 絶対パス (例: x:\myfolder\) や、任意パスを持つシステム変数 (例: %SystemDrive%\myfolder) が指定できます。デフォルトでサポートされている環境変数は「%」を入力すると表示されますが、サポートされていないユーザー変数を除き、ターゲット 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。 たとえば「%temp%」は特定のユーザー テンポラリ 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。

フィールド	説明
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はこのチェックボックスを選択します。
悪質な場合は検出	この設定が有効になっていると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。

9. 設定が完了したら、[**作成**] ボタンをクリックします。


新規ホワイトリスト エントリ
注意: フォルダ / ファイルのオーバーライドは、バージョン 9.0.1 以降を実行しているエンドポイントでのみ対応しています。
名前 / 説明
名前または説明を入力してこのエントリを特定
オーバーライドの種類
MD5
フォルダ / ファイル
ファイル マスク (オプション)
例: notepad.exe
パス / フォルダ マスク
サポートしているシステム変数については、% を入力してください。
サブフォルダを含める
悪質な場合は検出
作成
キャンセル

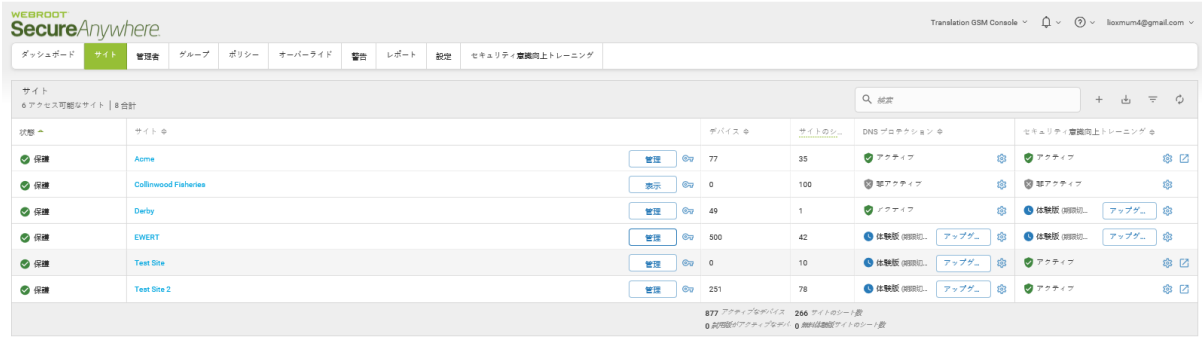
ブラックリストのオーバーライドの作成

管理コンソールとサイト レベルの両方のオーバーライド ページでブラックリストのオーバーライドを作成できるようになりました。

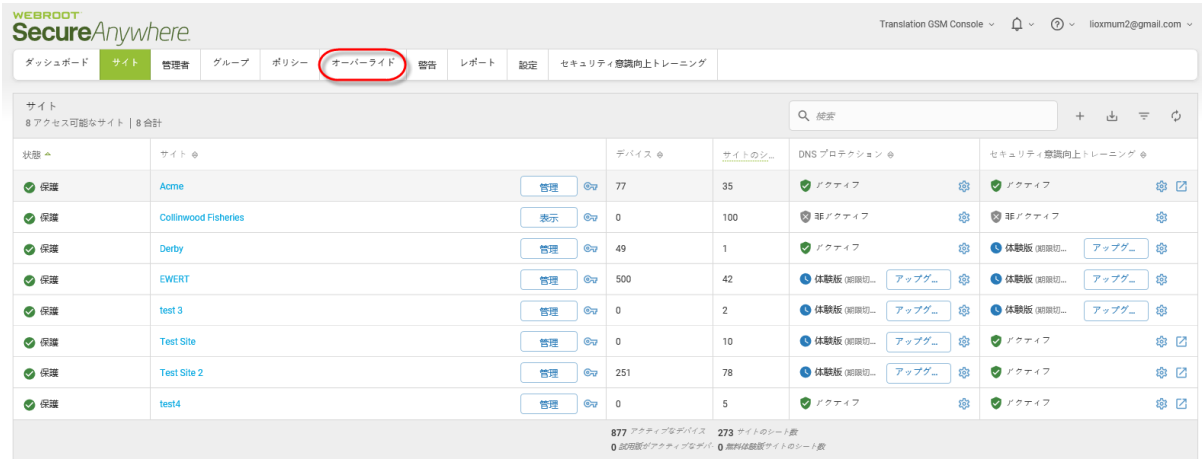
ブラックリストのオーバーライドを作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**オーバーライド**] タブをクリックします。



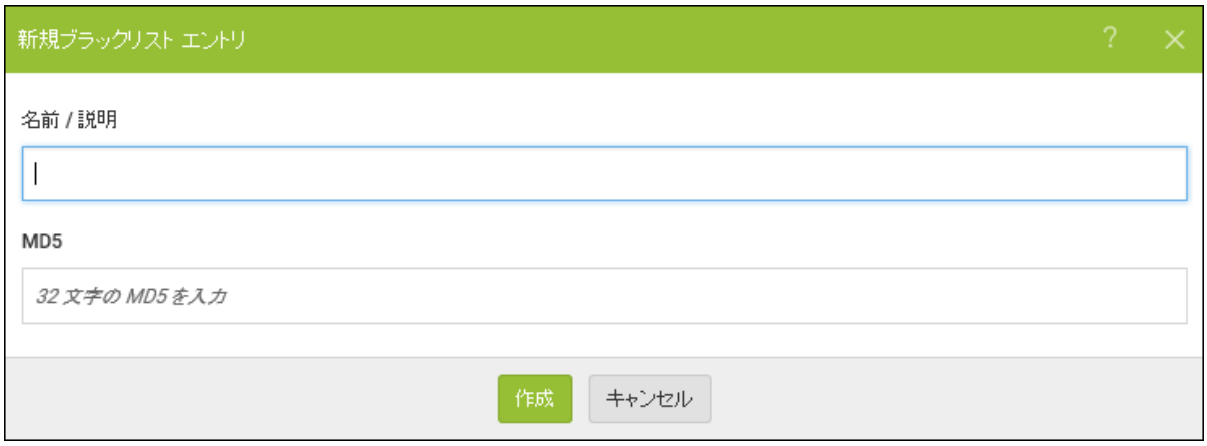
   [ファイルのホワイトリスト] タブがアクティブになった [オーバーライド] タブが表示されます。

3. [**ファイルのブラックリスト**] タブをクリックします。

[ファイルのブラックリスト] が表示されます。

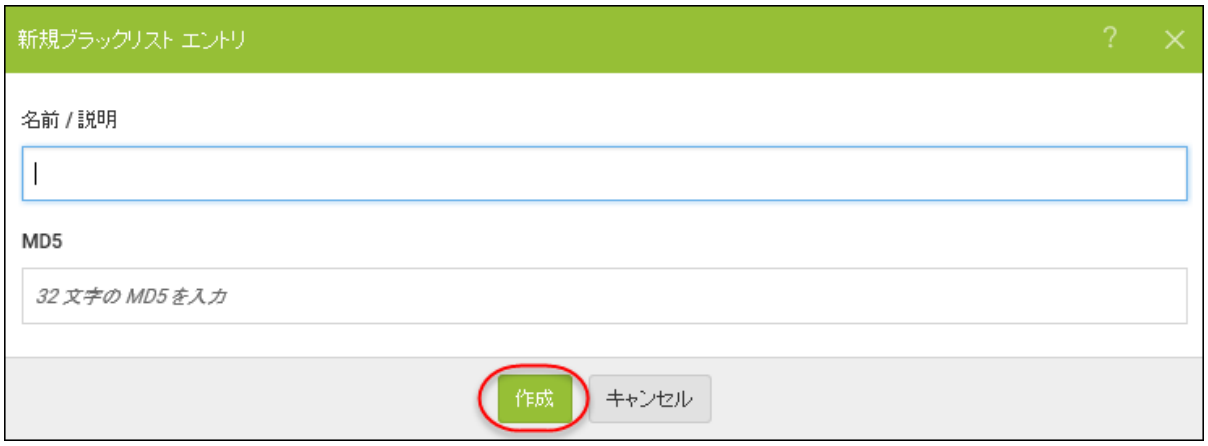
4. [**追加**] ボタンをクリックします。

[新規ブラックリスト エントリ] ウィンドウが表示されます。



5. [名前 / 説明] フィールドにオーバーライドの名前を入力します。
6. [MD5] フィールドに、ファイルに付けられた 32 英数字の固有識別子を入力してください。

7. 設定が完了したら、[**作成**] ボタンをクリックします。



ウェブのオーバーライドの編集

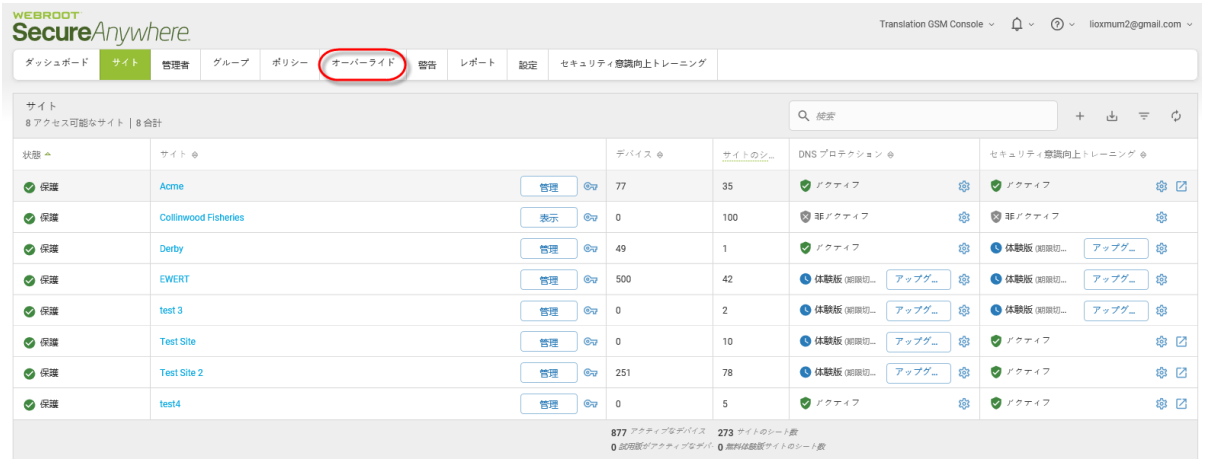
ウェブのオーバーライドを編集するには、次の手順に従ってください。

ウェブのオーバーライドを編集するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**オーバーライド**] タブをクリックします。



   [ファイルのホワイトリスト] 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。

3. [**ウェブのブロック / 許可リスト**] タブをクリックします。

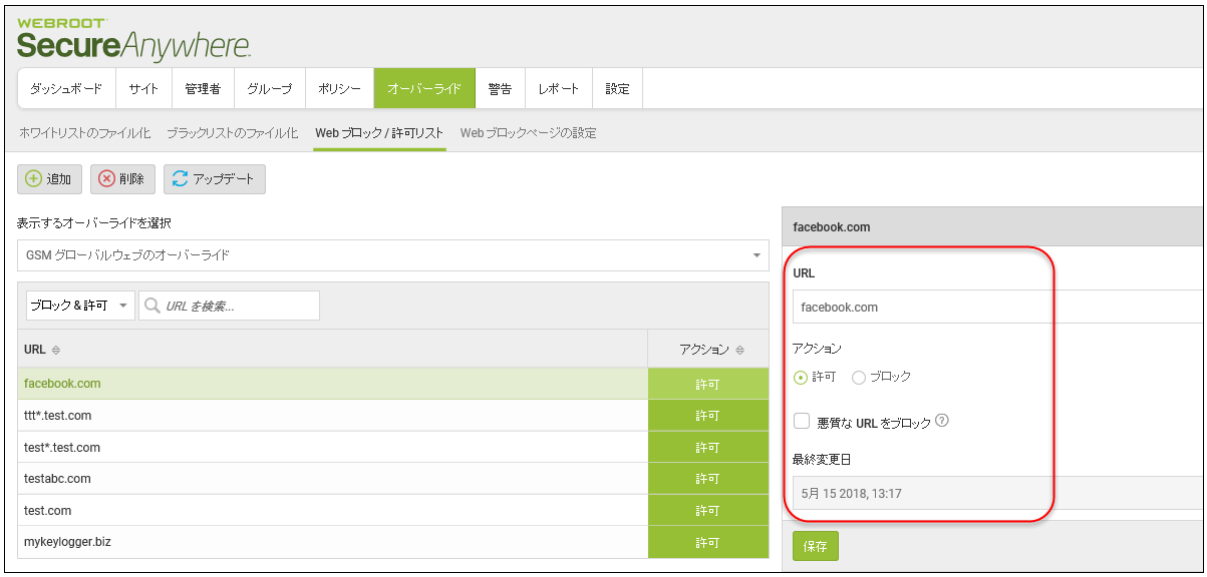
[ウェブのブロック / 許可リスト] タブが表示されます。

4. 編集するオーバーライドについて、[アクション] 列の 3 つのドットをクリックし、[**オーバーライドの編集**] を選択します。

[オーバーライドの編集] ウィンドウが表示されます。


オーバーライドを編集
ドメイン
ワイルドカードはドメイン内でサポートされています (e.g. *.subdomain.com)。
スコープ
グローバル
サイト
ポリシー
関連ポリシー
DNS 保護レベル：中
ブロック / 許可
ブロック
許可
悪質な URL をブロック
最終変更日
3月 19 2019, 12:32
編集
キャンセル

5. 必要に応じて、フィールドを編集します。



注意: URL を入力する際は、*www*、*http*、または*https* などのプロトコルを入力する必要はありません。

6. 設定が完了したら [**編集**] ボタンをクリックします。

設定がアップデートされます。

オーバーライドのインポート

管理コンソールとサイト レベルの両方のオーバーライド ページで、既存のサイトからオーバーライドをインポートできるようになりました。この手順は、管理者が同じオーバーライドを各サイトで手動で作成するのではなく、別のサイトへコピーする場合に便利です。

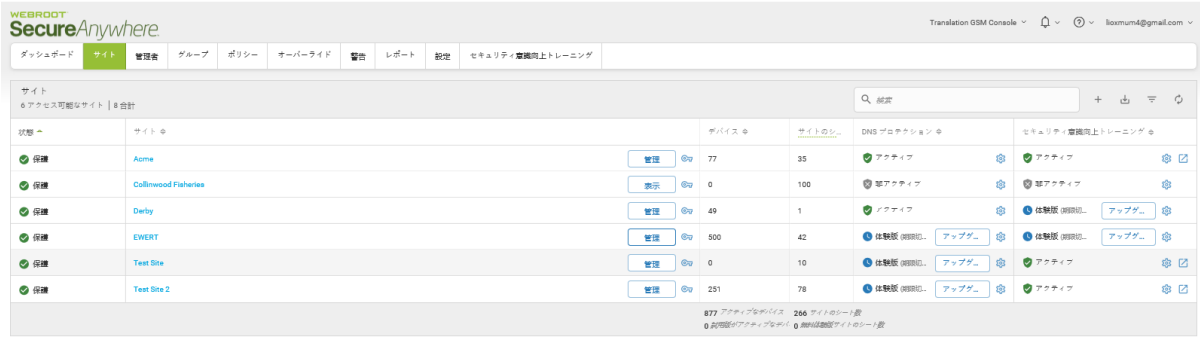
スーパー管理者は、サイトのオーバーライドをグローバルに設定し、グローバル オーバーライドのオプションが選択された他のすべてのサイトに適用することもできます。

この手順に従って、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インポートします。

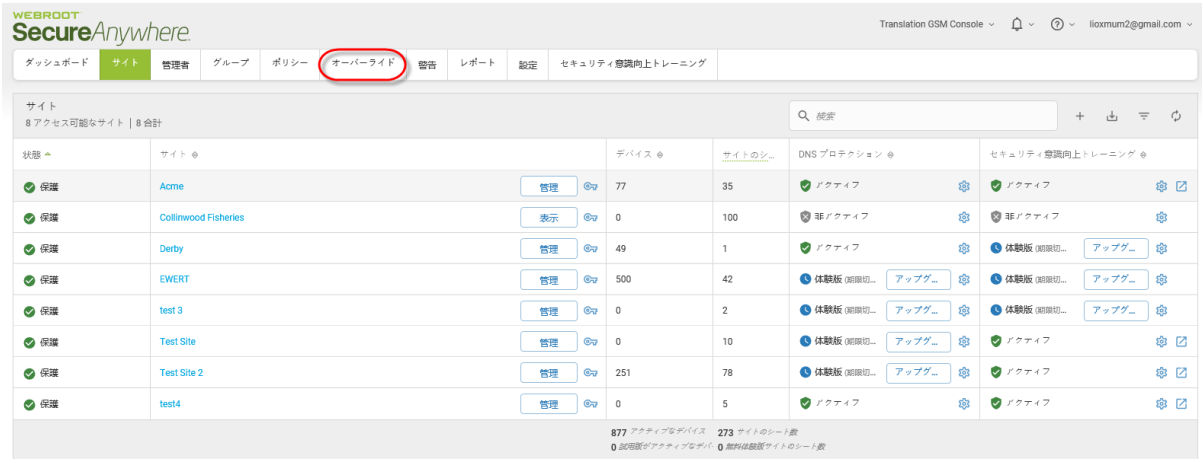
オーバーライドをインポートするには:

1. 管理コンソールにログインします。

   [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が表示されます。



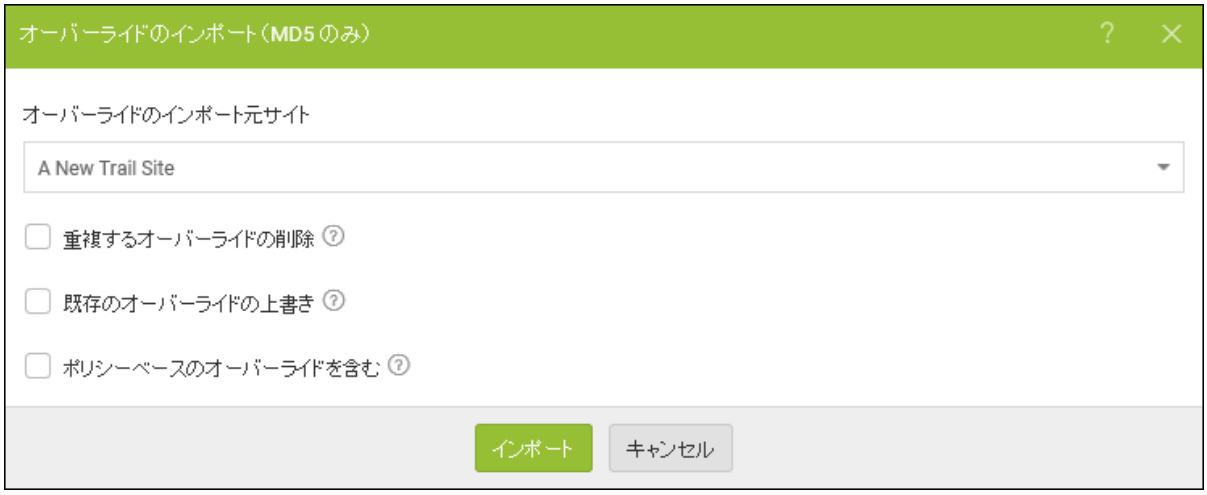
2. [**オーバーライド**] タブをクリックします。



[ファイルのホワイトリスト] 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。

3. [**インポート**] ボタンをクリックします。

[オーバーライドをインポート] ウィンドウが表示されます。



4. [オーバーライドのインポート元サイト] のドロップダウンメニューで、オーバーライドをインポートするサイトを選択します。

5. 必要に応じて、次のチェックボックスを選択します:
   - **重複するオーバーライドの削除** - **このチェックボックス**を選択した場合は、オーバーライドがファイルの判定に一致すると(MD5 のホワイトリスト エントリで「正当」の判定が既に出ているものなど)、オーバーライドがインポートされません。
   - 既存のオーバーライドの上書き — **このチェックボックスを選**択すると、インポートしたリスト内で重複するオーバーライドにより既存のオーバーライドを上書きすることが決定されます。
   - **ポリシーベースのオーバーライドを含む** - **標準コンソールで作成**され、選択されたインポート元サイト/コンソール内の特定のポリシーのみに割り当てられたオーバーライドをインポートできます。オーバーライドをポリシーに割り当てる機能は標準コンソールのみで使用できます。

6. 設定が完了したら、[**インポート**] ボタンをクリックします。

指定したサイトから、すべてのオーバーライドが現在選択されているサイトにインポートされます。

ウェブのオーバーライドの表示

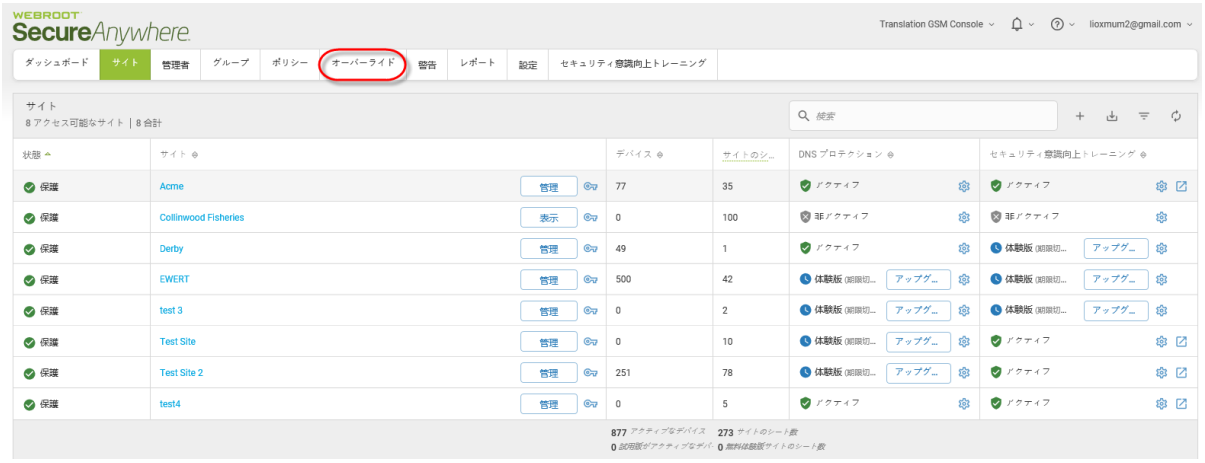
作成したウェブのオーバーライドに関する追加情報を表示するには、以下の手順に従ってください。

ウェブのオーバーライドを表示するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**オーバーライド**] タブをクリックします。



   [ファイルのホワイトリスト] 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。

3. [**ウェブのブロック / 許可リスト**] タブをクリックします。

[ウェブのブロック / 許可リスト] タブが表示されます。

4. 特定のオーバーライドを見つける場合や、スコープ、関連ポリシー、ブロック/許可の状態に基づいてオーバーライドを並び替える場合は、以下のいずれかを実行します。
   - [ドメイン] フィールドに、検索するドメインの名前を入力します。
   - [スコープ] ドロップダウン メニューから、スコープに基づくポリシーを選択します。たとえば、グローバル ポリシーのみをフィルタリングするには、[*グローバル*] を選択します。
   - [関連ポリシー] ドロップダウン メニューから、関連するポリシーに基づくドメインを選択します。
   - [ブロック / 許可] ドロップダウン メニューで、以下の項目ようにフィルタリングを実行できます。
     - ブロックおよび許可
     - ブロック
     - 許可
   - さらに、カラムの一番上で上向きまたは下向き矢印をクリックして以下の列のフィルタリングを行うこともできます。
     - **ドメイン** - アルファベット順でフィルタリングを行います。
     - **最終変更** - 日付によるフィルタリングを行います。

オーバーライドの削除

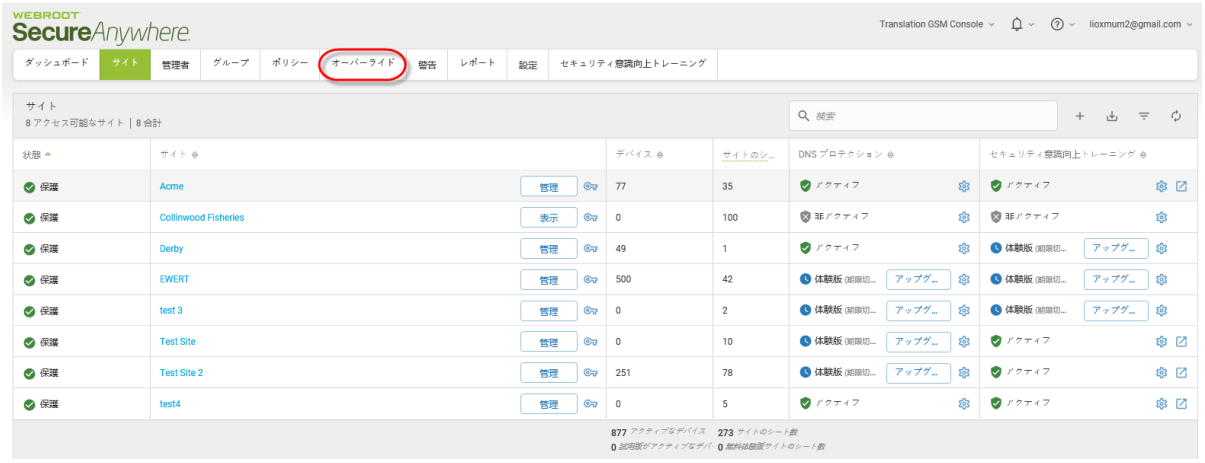
この手順に従って、ホワイトリストまたはブラックリストのオーバーライドを削除します。

オーバーライドを削除するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**オーバーライド**] タブをクリックします。



   [ファイルのホワイトリスト] 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。

3. [ホワイトリスト] または [ブラックリスト] タブのどちらかで、削除するオーバーライドをハイライトします。

選択したオーバーライドが強調表示され、[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。

[ホワイトリスト / ブラックリストのエントリ削除] の確認ウィンドウが表示されます。

5. [**削除の確認**] 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。

ウェブのオーバーライドの削除

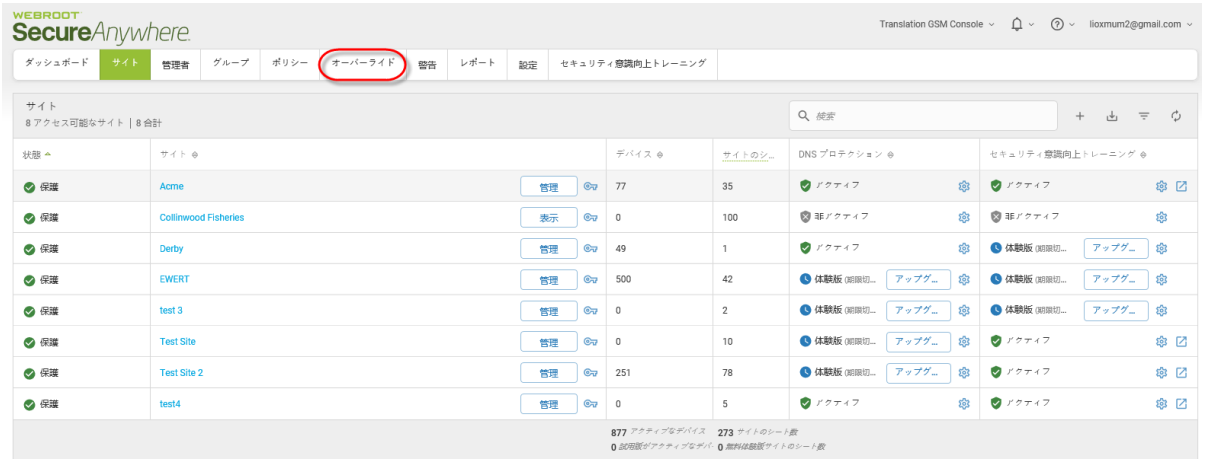
この手順に従って、必要なくなったウェブのオーバーライドを削除します。

ウェブのオーバーライドを削除するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**オーバーライド**] タブをクリックします。



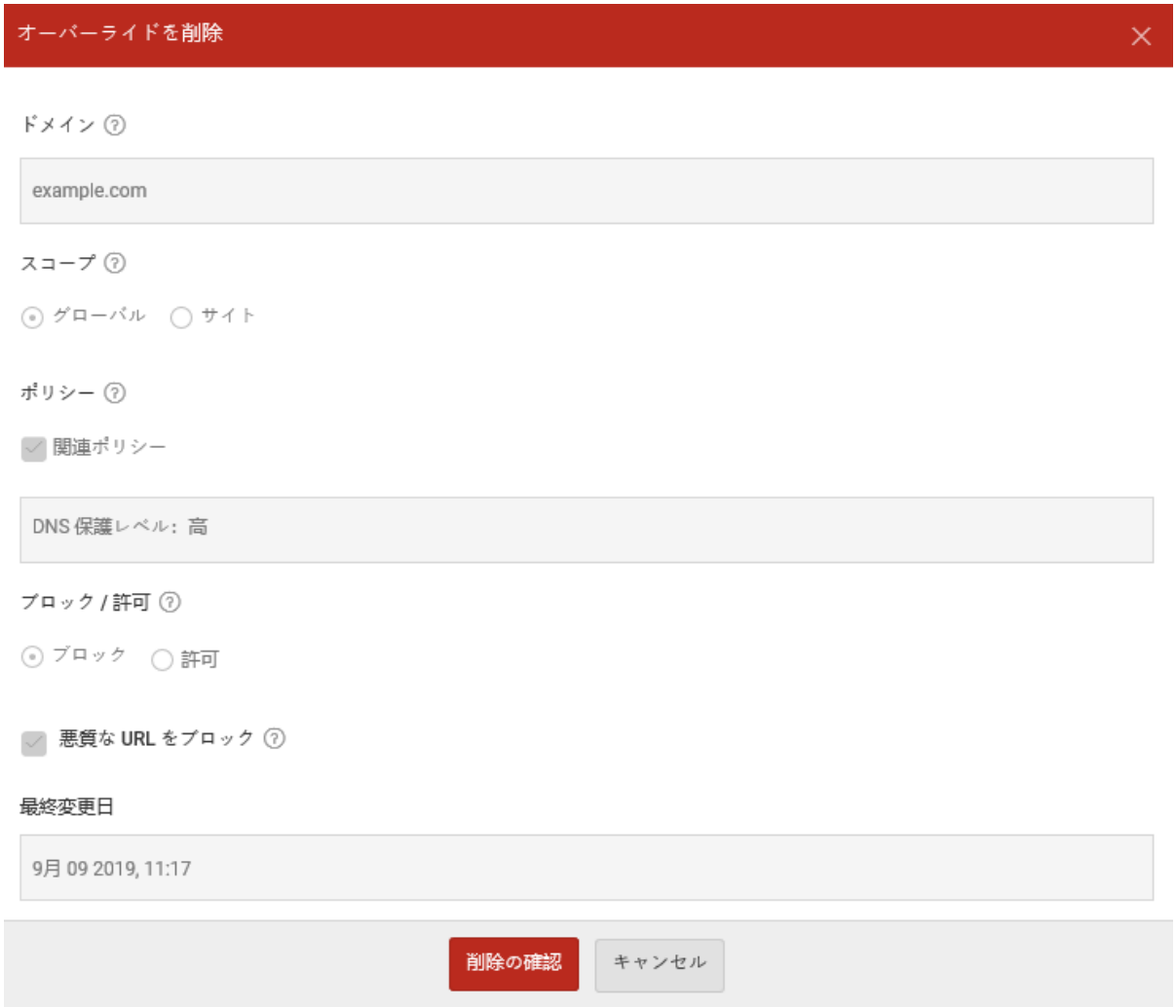
   [ファイルのホワイトリスト] タブがアクティブになった [オーバーライド] タブが表示されます。

3. [**ウェブのブロック / 許可リスト**] タブをクリックします。

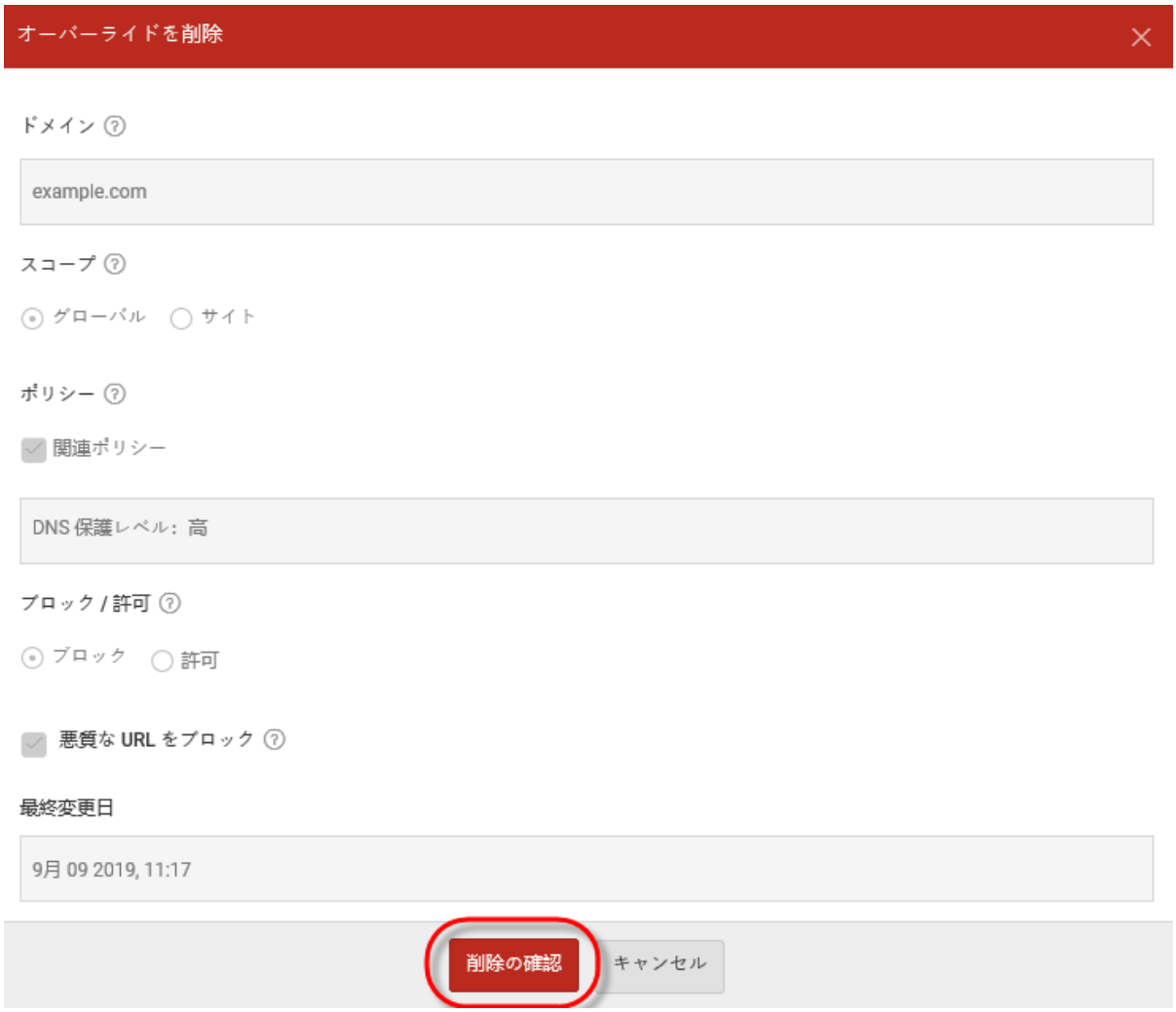
[許可リスト] タブがアクティブになった [ウェブのオーバーライド] タブが表示されます。

4. 削除するウェブのオーバーライドについて、[アクション] 列の 3 つのドットをクリックし、[**削除**] を選択します。

選択したウェブのオーバーライドの URL を含む [削除] ウィンドウが表示されます。


オーバーライドを削除
ドメイン
example.com
スコープ
グローバル
サイト
ポリシー
関連ポリシー
DNS 保護レベル：高
ブロック / 許可
ブロック
許可
悪質な URL をブロック
最終変更日
9月 09 2019, 11:17
削除の確認
キャンセル

5. [**削除の確認**] ボタンをクリックします。



ウェブのオーバーライドが削除されます。

ブロック ページのカスタマイズ

ブロック ページは、各管理コンソールごとにカスタマイズすることができます。これにより、管理者は詳細な情報をユーザーに通知できます。

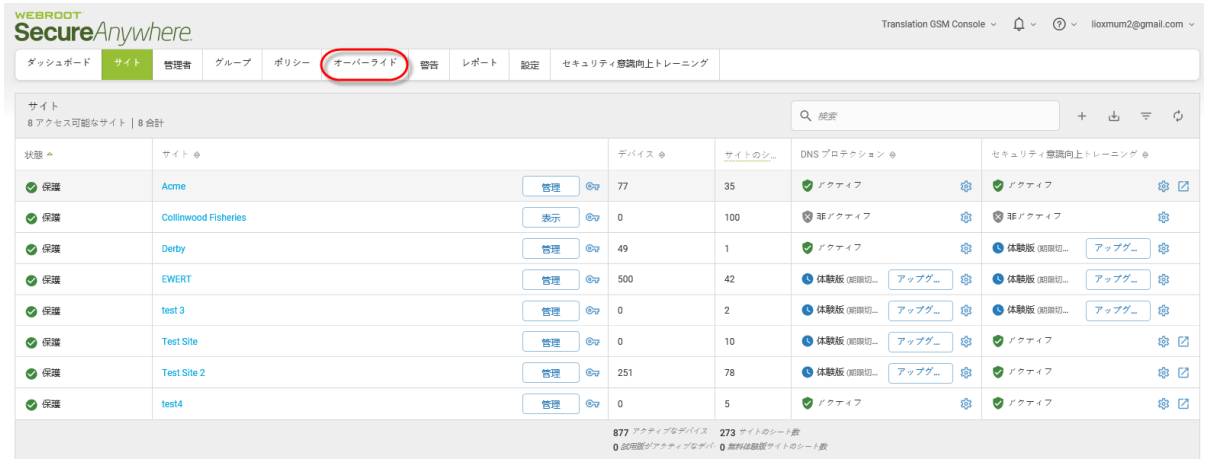
- 管理者は、企業ベースのロゴを含めることができます。
- [コンテンツ] フィールドは、電話番号、Web サイト、リンクなどのカスタム テキストに使用できます。たとえば、*「質問がある場合はネットワーク管理者に連絡してください」*などの情報を入力し、希望する連絡方法を含めることができます。

ブロック ページをカスタマイズするには:

1. 管理コンソールにログインします。

   [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が表示されます。

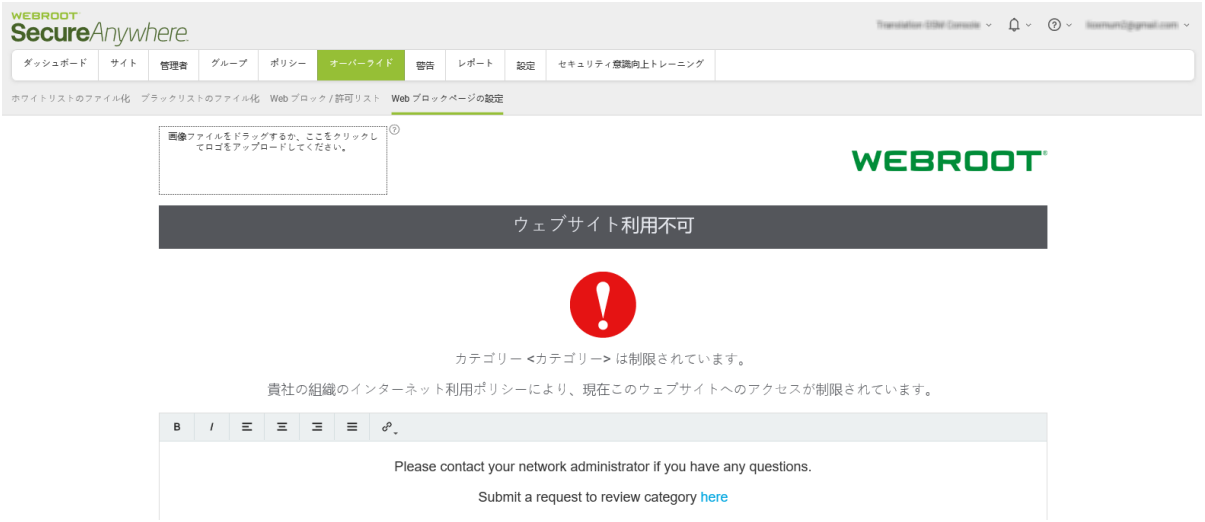
2. [**オーバーライド**] タブをクリックします。



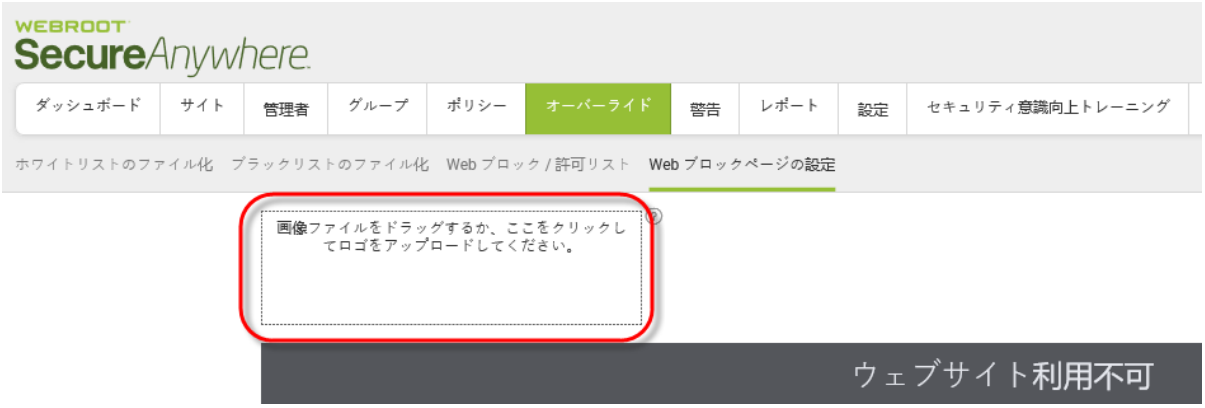
[ファイルのホワイトリスト] タブがアクティブになった [オーバーライド] タブが表示されます。

3. [**ウェブ ブロック ページの設定**] タブをクリックします。

[ウェブ ブロック ページの設定] タブが表示されます。



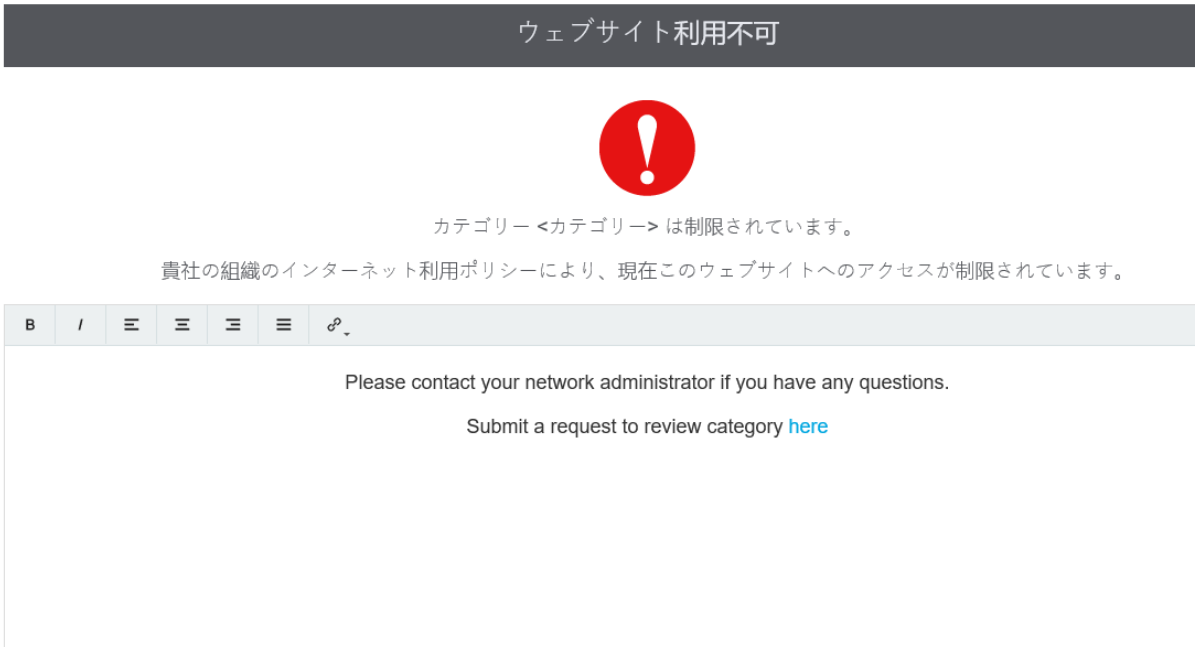
4. 左上で、以下のどちらかを選んで実行してください。
   - 画像ファイルをドラッグするか、領域内をクリックしてロゴをアップロードしてください。
   - [**現在の画像を削除**] をクリックして、ロゴのスペースを削除します。



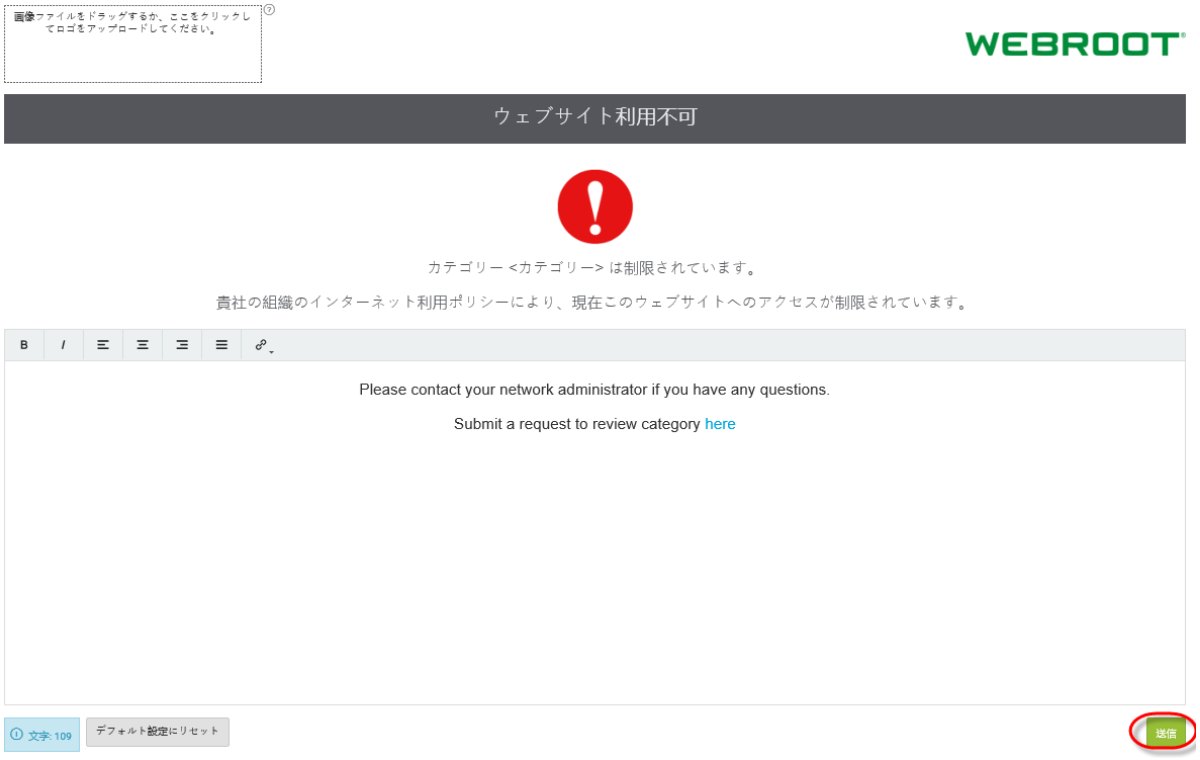
注意: ロゴは 1 MB 以下で、最大高さは 50 ピクセル、最大幅は 500 ピクセルです。

5. 自由形式のフィールドに、制限された Web サイトにアクセスしようとするたびにユーザーに表示されるメッセージを入力します。

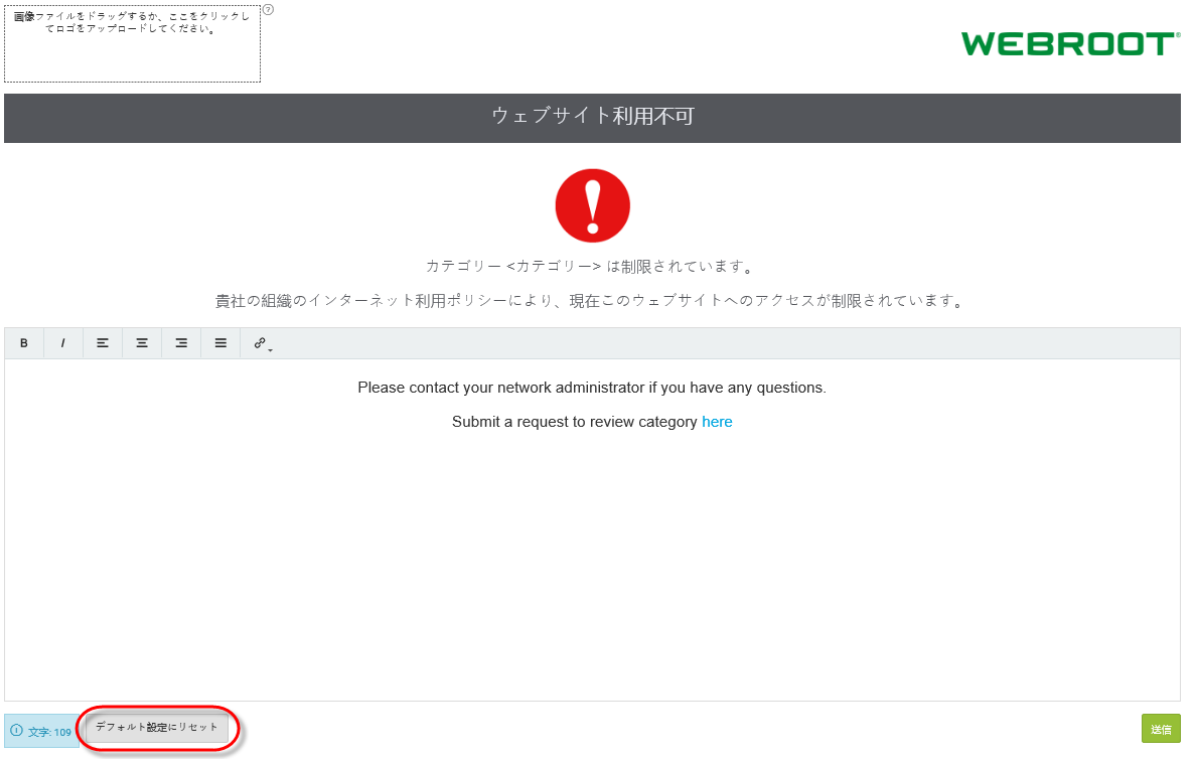
- 画面の左下にある青色のボックスには、使用されている文字数が表示されます。
- デフォルトのメッセージは、*「質問がある場合はネットワーク管理者に連絡してください」*です。必要に応じて変更することができます。
- 必要に応じて、WYSIWYG 編集メニューを使用してメッセージをフォーマットします。



6. 設定が完了したら、[**送信**] ボタンをクリックします。



7. 必要に応じて、[**デフォルト設定にリセット**] ボタンをクリックします。



第 9 章: 警告の操作

警告を操作するには、次のトピックをご覧ください。

警告の作成

グローバルレベルで警告を作成できるようになりました。個別のサイトの警告を手動で管理するのではなく、すべて 1 か所の共有ロケーションから処理できるため、メンテナンス費用を大幅に削減することができます。

感染に関する警告、インストールに関する警告、感染の概要、またはインストールの概要など送信する警告の種類や、警告を送信する頻度を選択することにより、警告を集中的に設定および管理することが可能です。それから、子エンドポイント保護サイトに警告を適用することができます。

注意: 管理コンソールレベルで作成されたグローバル警告は、サイトレベルの「表示のみ」モードで表示されます

警告を作成するには:

1. 管理コンソールにログインします。

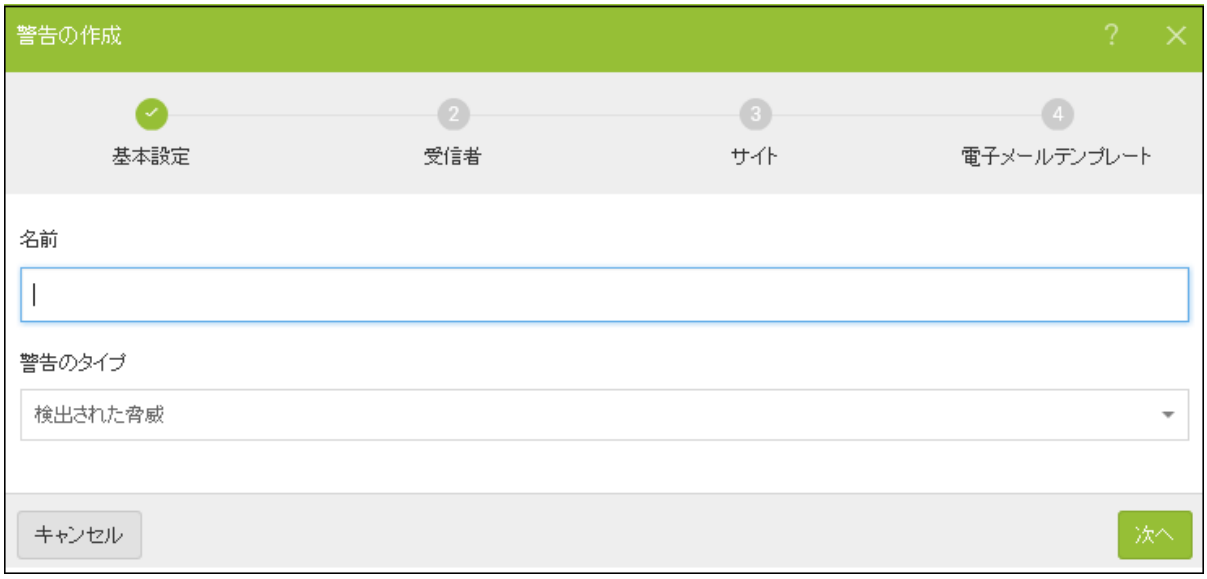
   [サイト] タブがアクティブになった状態で管理コンソールが表示されます。

2. [**警告**] タブをクリックします。

[警告リスト] タブがアクティブな状態で [警告] タブが表示されます。

3. [**追加**] ボタンをクリックします。

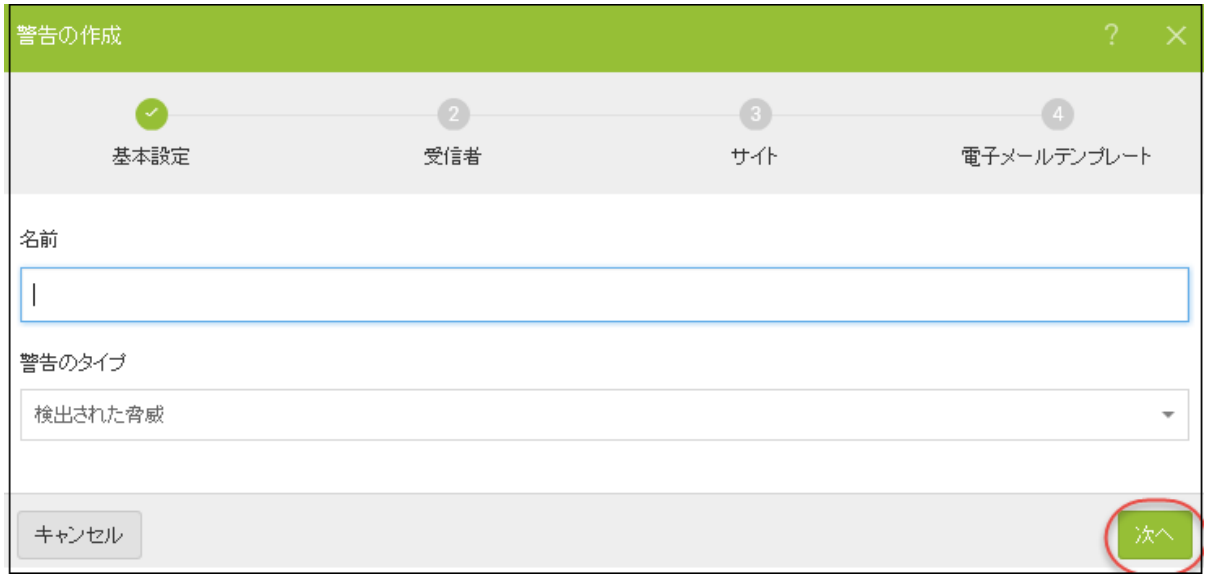
[警告の作成] ウィンドウが表示されます。



4. [名前] フィールドで以下のいずれかを実行します。
   - システムが生成した警告の名前を受け入れます。
   - 警告の新しい名前を入力します。
5. [警告のタイプ] ドロップダウン メニューから次のいずれかを選択して警告のタイプを決定します。
   - **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**

6. [**次へ**] ボタンをクリックします。



[受信者] パネルが表示されます。

7. 次のいずれかの [警告の受信者] ラジオ ボタンを選択します。
   - **既存のリストを使用**
   - **新規リストの作成**
8. [新規リストの作成] を選択した場合は、次のすべての手順を実行します。それ以外の場合は次のステップに進みます。
   - [配信先リストの名前] フィールドに新しい配信先リストの名前を入力します。
   - [電子メールアドレス] フィールドに、新しい配信先リストの受信者の電子メールアドレスを入力します。
9. [配信先リストを選択] ドロップダウン メニューから、以前に作成した配信先リストを選択します。

   詳細については、「法人向け WSA エンドポイント プロテクション管理者ガイド」の「*配信先リストの作成*」を参照してください。

10. [**次へ**] ボタンをクリックします。

[サイト] パネルが表示されます。

11. 次のいずれかの [この警告を使用するサイト] ラジオ ボタンを選択します。
    - **すべてのサイト**
    - **選択したサイト**
12. [**次へ**] ボタンをクリックします。

[電子メールテンプレート] パネルが表示されます。

13. [電子メールの件名] フィールドに電子メールの件名を入力します。
14. [電子メールメッセージの本文] フィールドに、送信するメッセージの本文を入力します。
15. データ入力を使用する場合は、テキストにカーソルを合わせ、任意のタグをクリックして、テキスト内の位置にデータを挿入します。

    次のデータポイントが、Mac エージェントでサポートされていません。

    - ワークグループ
    - アクティブ ディレクトリ

16. 設定が完了したら、[**終了**] ボタンをクリックします。

警告の削除

警告を削除するには、次の手順に従ってください。

警告を削除するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**警告**] タブをクリックします。

   [警告リスト] タブがアクティブな状態で [警告] タブが表示されます。

3. 削除する警告をクリックします。

   その警告に関する情報が表示され、[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。

[警告メッセージの削除] ウィンドウが表示されます。

5. [**削除の確認**] ボタンをクリックします。

警告が削除されます。

警告の一時停止または再開

この手順に従って、警告を一時停止または再開します。

警告の一時停止または再開方法:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**警告**] タブをクリックします。

   [警告リスト] タブがアクティブな状態で [警告] タブが表示されます。

3. 一時停止または再開する警告をクリックします。

   その警告に関する情報が表示され、[一時停止 / 再開] ボタンがアクティブになります。

注意: 警告がアクティブ化されている場合は、ボタンで一時停止できます。警告が一時停止されている場合は、ボタンを使用して警告を再開できます。

4. 以下のいずれかを実行します。
   - [**一時停止**] ボタンをクリックして、警告を一時停止します。

   - [**再開**] ボタンをクリックして、警告を再開します。

[状態] 列には、警告がアクティブであるか一時停止状態であるかが反映されます。


WEBROOT
SecureAnywhere
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ
警告リスト
配信先リスト
追加
削除
再開
名前
種類
配信先リスト
状態
abcAlert 1
検出された脅威
Distribution List 1
一時停止
Webroot System Messages
システムメッセージ
システムメッセージ リスト
アクティブ

配信先リストの作成

[警告] タブでは、警告メッセージを受信するユーザーの配信先リストを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を作成する場合などに使用します。

配信先リストを作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**警告**] タブをクリックします。

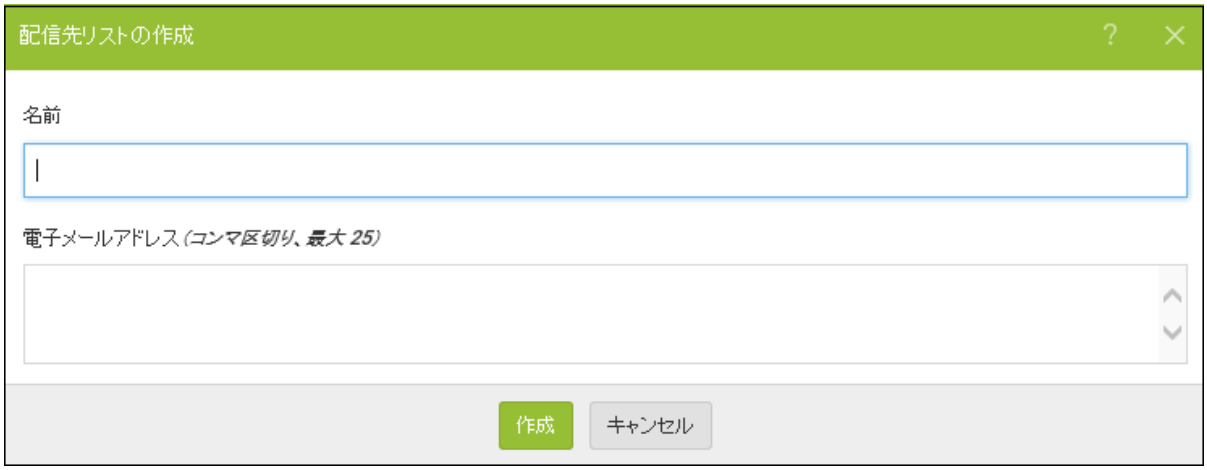
   [警告リスト] タブがアクティブな状態で [警告] タブが表示されます。

3. [**配信先リスト**] タブをクリックします。

[配信先リスト] タブが表示されます。

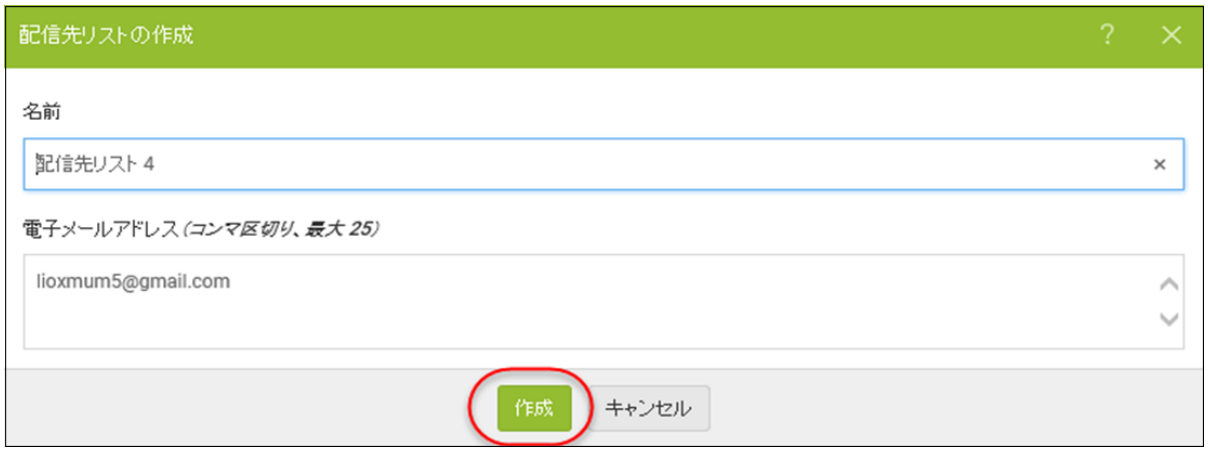
4. [**追加**] ボタンをクリックします。

[配信先リストの作成] ウィンドウが表示されます。



5. [名前] フィールドで以下のいずれかを実行します。
   - システムが生成した警告の名前を受け入れます。
   - 警告の新しい名前を入力します。
6. [電子メールアドレス] フィールドに、新しい配信先リストの受信者の電子メールアドレスを入力します。

7. 設定が完了したら、[**作成**] ボタンをクリックします。



第 10 章: レポートの操作

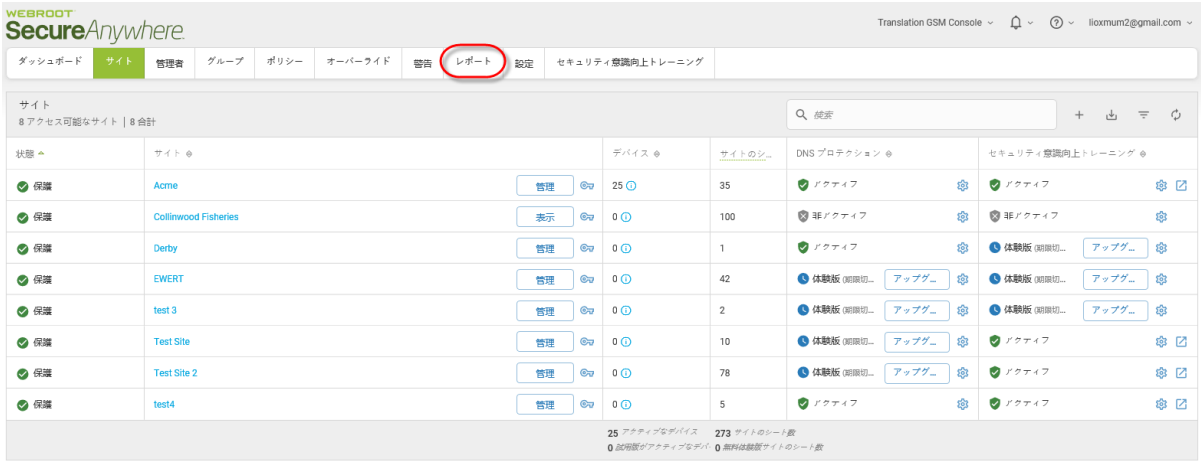
レポートを操作するには、次のトピックを参照してください:

グローバル サイト マネージャー レポート概要

管理サイト コンソールのレポート機能を使用すると、必要な時に必要な情報をレポートできるよう、各サイトまたは配備全体の状態やパフォーマンスについて、詳細な各種ツールによるレポートを作成することができます。

カスタム レポートは一定の間隔で定期的に出力したり、送信する相手の個々の要件にポイントを絞った内容を特別に作成したりすることができます。レポートのスケジューリングを利用すれば、自分自身や顧客にとって重要な情報を見逃すことがなくなります。

レポート機能はすべて、管理サイト コンソールの [レポート] タブにあります。



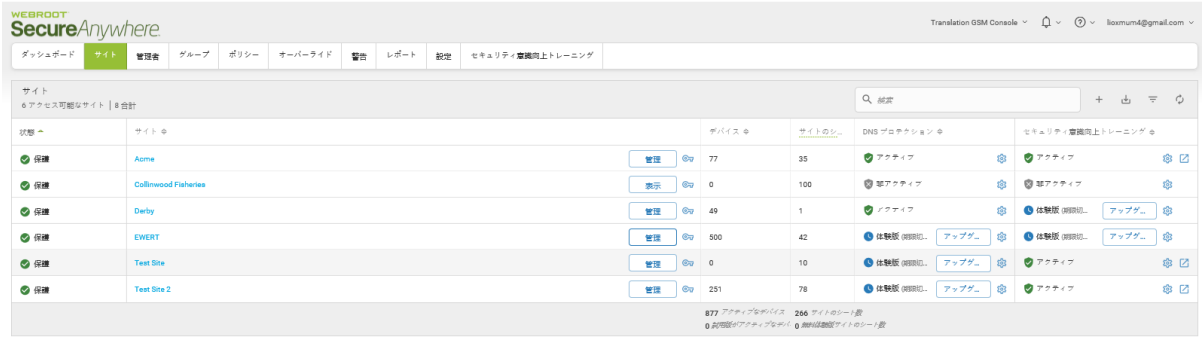
レポートの作成

カスタマイズ可能なデータ、スケジュール、宛先および言語を備えたレポートのスケジューリング機能によって、利害関係者への十分な情報の伝達に必要な情報と柔軟性が提供されます。

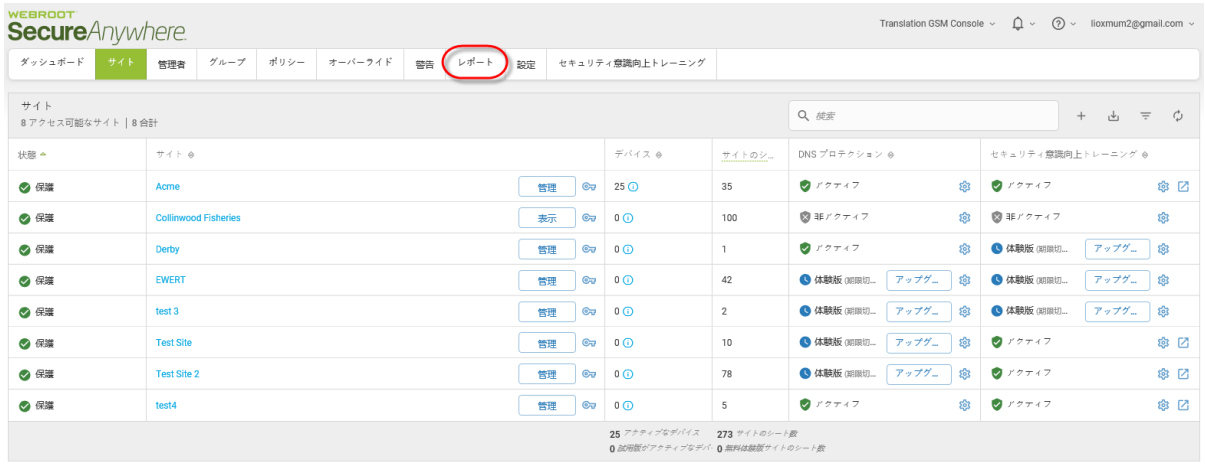
レポートを作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**レポート**] タブをクリックします。



   [オンデマンド] タブがアクティブな状態で [レポート] タブが表示されます。

3. [**スケジュールされたレポート**] タブをクリックします。

[スケジュールされたレポート] タブが表示されます。

4. [**追加**] ボタンをクリックします。

[レポートを作成] ウィンドウが表示されます。

5. [レポート名] フィールドにレポートの識別子を入力します (例: *週別概要レポート*)。
6. [配送予定] ドロップダウン メニューで定期的にレポートを実行するスケジュールを作成し、関係者に配信します。または、情報が必要な場合にレポートを実行して配信するよう設定することもできます。
   - **毎日** — 毎日指定した時刻に実行されます。
   - **毎週** — 毎週指定した曜日と時刻に実行されます。
   - **毎月** — 毎月指定した日と時刻に実行されます。

注意: スケジュールで選択する時間は UTC (協定世界時) であり、ユーザーのタイムゾーンとは関連がありません。

7. [作成方法] フィールドで、対象となる受信者に情報を配信するためのレポートの作成方法を指定します。選択されたサイトを集約するか、または個別のサイトごとに作成するかを選択できます。次のいずれかを選択してください:
   - **選択されたサイトごとに 1 つのレポートを作成**
   - **選択されたすべてのサイトのデータを組み合わせた 1 つのレポートを作成**
8. [受信者] ドロップダウン メニューから、次のいずれかを選択して、通常のサイト受信者のリストを設定するか、または特定の電子メールアドレスを配信先として追加するかを指定します:
   - **各サイトのレポート配信先リストに電子メールを送信**
   - **手動で入力された固定のアドレスに電子メールを送信**
   - **上記の両方を実行**

注意: レポートの配信先リストは新しいフィールドです。このフィールドは、サイトのページで各サイトの編集を選択すると変更できます。既存のすべてのサイトでは、各サイトですでに設定されているすべての管理者の電子メールアドレスがあらかじめ入力されています。

9. [テンプレート] ドロップダウン メニューから、レポートに含めるデータのテンプレートを選択します。
10. [サイト] フィールドをクリックして、レポートに含めるサイトを選択します。
11. [言語] フィールドをクリックして、作成するレポートの言語を選択します。

    グラフの軸やタイトルなどのデフォルトのテキストが、選択された言語で表示されます。複数の言語を選択した場合、言語ごとに 1 つのレポートが作成されます。英語に加えて、言語のオプションは次のとおりです。

ドイツ語	トルコ語	スペイン語
フランス語	イタリア語	日本語
韓国語	オランダ語	ポルトガル語
ロシア語	中国語 (簡体字)	中国語 (繁体字)

12. 設定が完了したら、[**作成**] ボタンをクリックします。


レポートを作成
レポート名
配送予定
毎週
月曜
09:00
UTC +00:00
作成方法
サイトごとに 1 つのレポートが作成されました
受信者
各サイトのレポート配信先リストに電子メールを送信
テンプレート
abc
サイト
1 of 8 選択済み
言語
1 of 13 選択済み
作成
キャンセル

レポートの生成

[今すぐレポートを実行する] ツールを使用すると、スケジュールに含まれていないレポートにいつでもアクセスすることができます。このツールを使用すると、作成方法および配信先リストに対して一回に限りオーバーライドを適用できる機能を用いて、レポートのスケジュールをすぐに設定することができます。

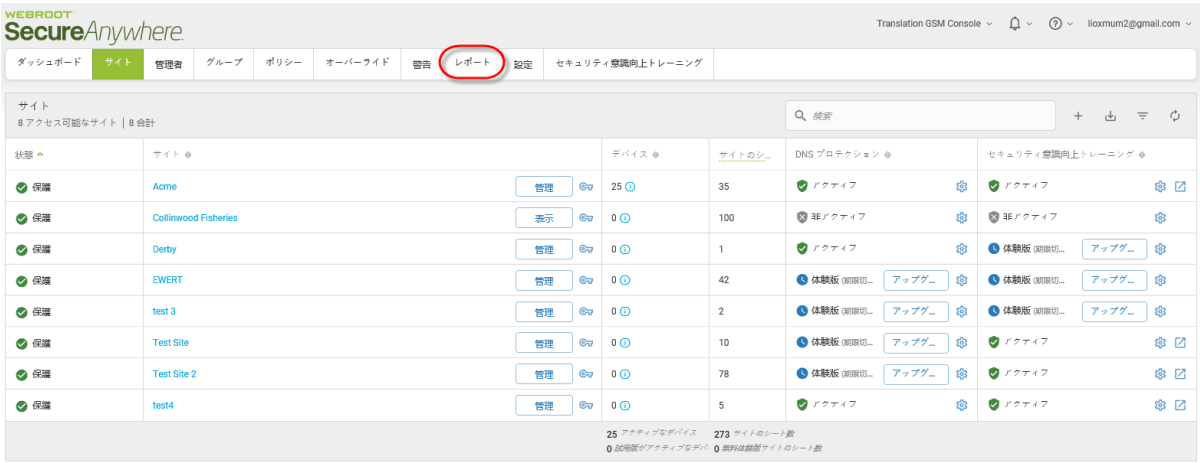
現在のスケジュールに永続的な変更を加えることなく、サイト全体の情報を集約するようにレポートを変更したり、各サイトについてそれぞれレポートを作成して受信者をカスタマイズしたりできます。または、スケジュール通りにレポートを実行することも可能です。

レポートを生成するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**レポート**] タブをクリックします。



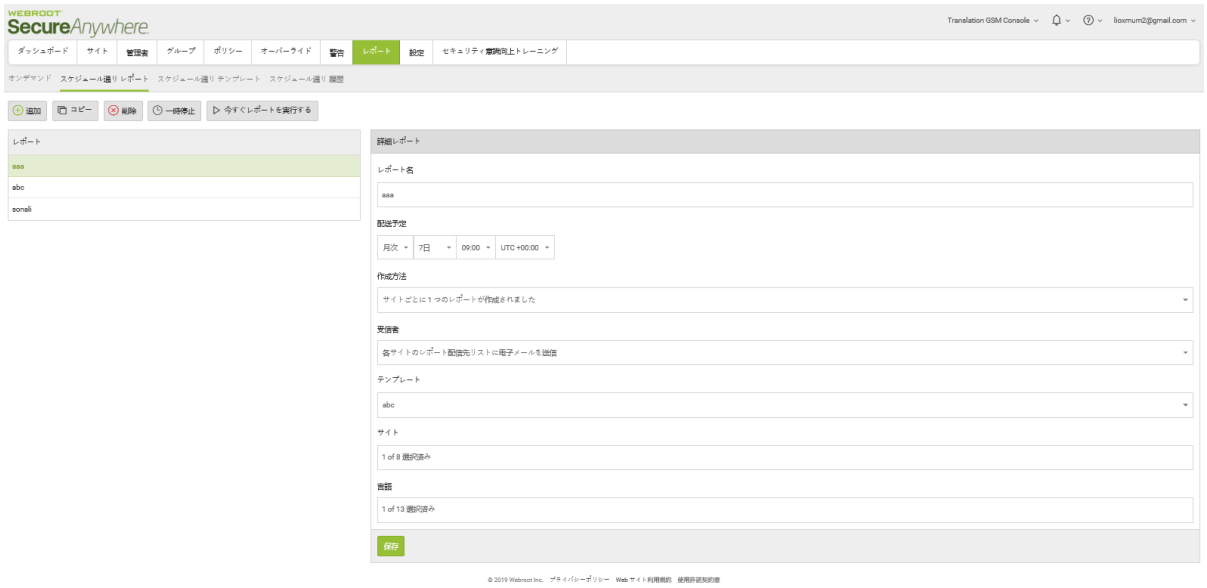
[オンデマンド] タブがアクティブな状態で [レポート] ペインが表示されます。

3. [**スケジュールされたレポート**] タブをクリックします。

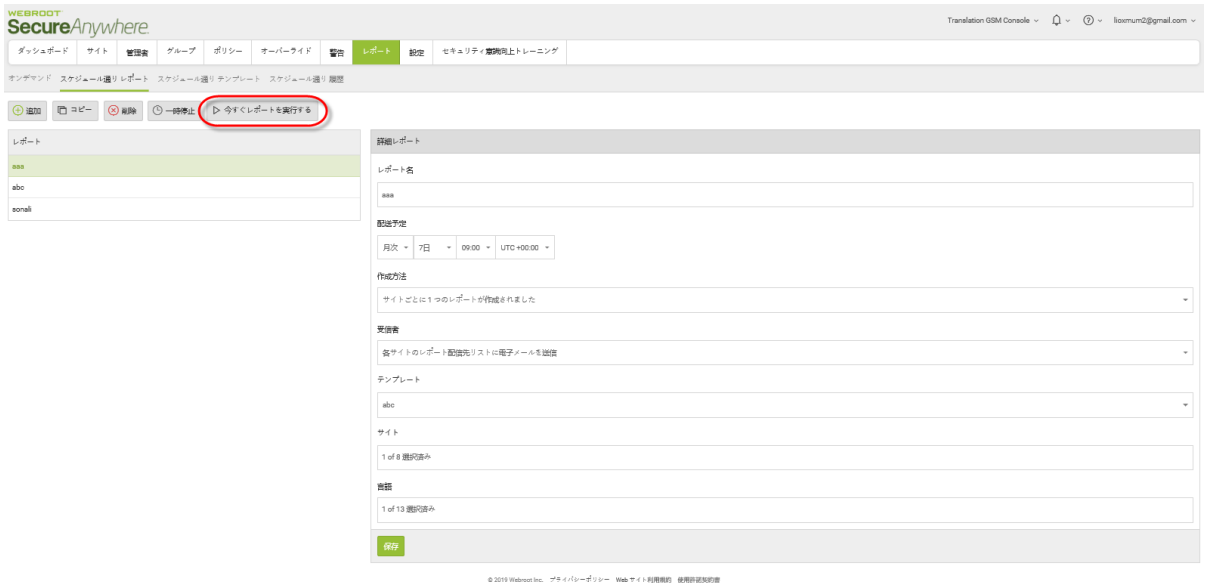
[スケジュールされたレポート] タブが表示されます。

4. 実行するレポートの名前をクリックします。

[詳細レポート] ペインが表示されます。



5. 必要に応じてレポートの詳細をアップデートしてから、[**今すぐレポートを実行する**] ボタンをクリックします。



[今すぐレポートを実行] ウィンドウが表示されます。

6. 以下のいずれかの作業を行ってください:
   - 変更なしでレポートを実行する場合は、[実行] ボタンをクリックします。

   - 変更を加えてからレポートを実行する場合は、[変更なしでレポートを実行] チェックボックスの

   選択を解除し、作成方法を選択した後、レポートの受信者の名前を入力してから [実行] ボタンをクリックします。

オンデマンド レポートの生成

レポートを実行してその情報を管理コンソール使用中に画面に表示するには、次の手順に従ってオンデマンド レポートを生成します。

レポートを生成して CSV ファイルや PDF を作成する方法については、「*403{/u}{/color} ページの「レポートの生成」*」をご覧ください。

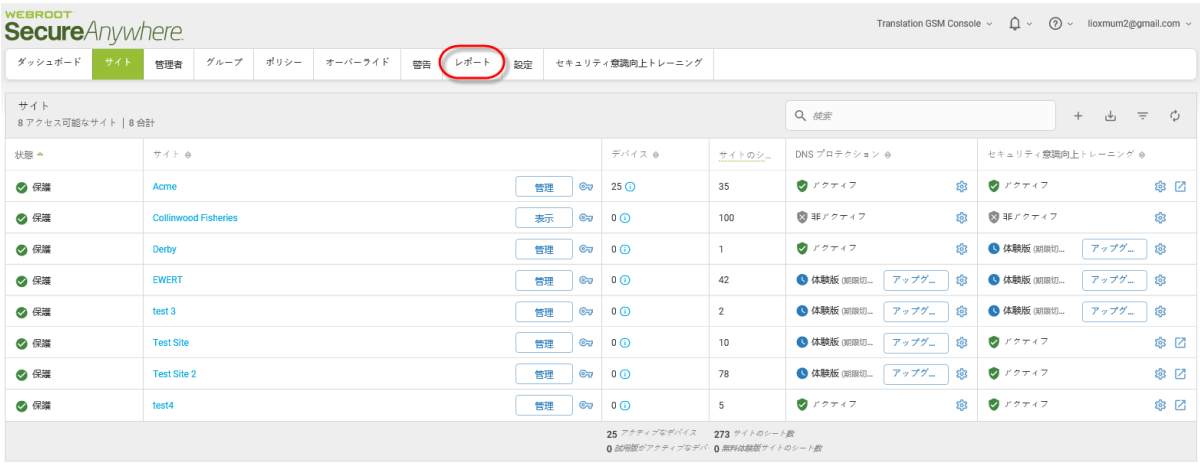
注意: 限定管理者は、アクセス権のあるサイトについてオンデマンド レポートを実行できます。

オンデマンド レポートを生成するには:

1. 管理コンソールにログインします。

   [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が表示されます。

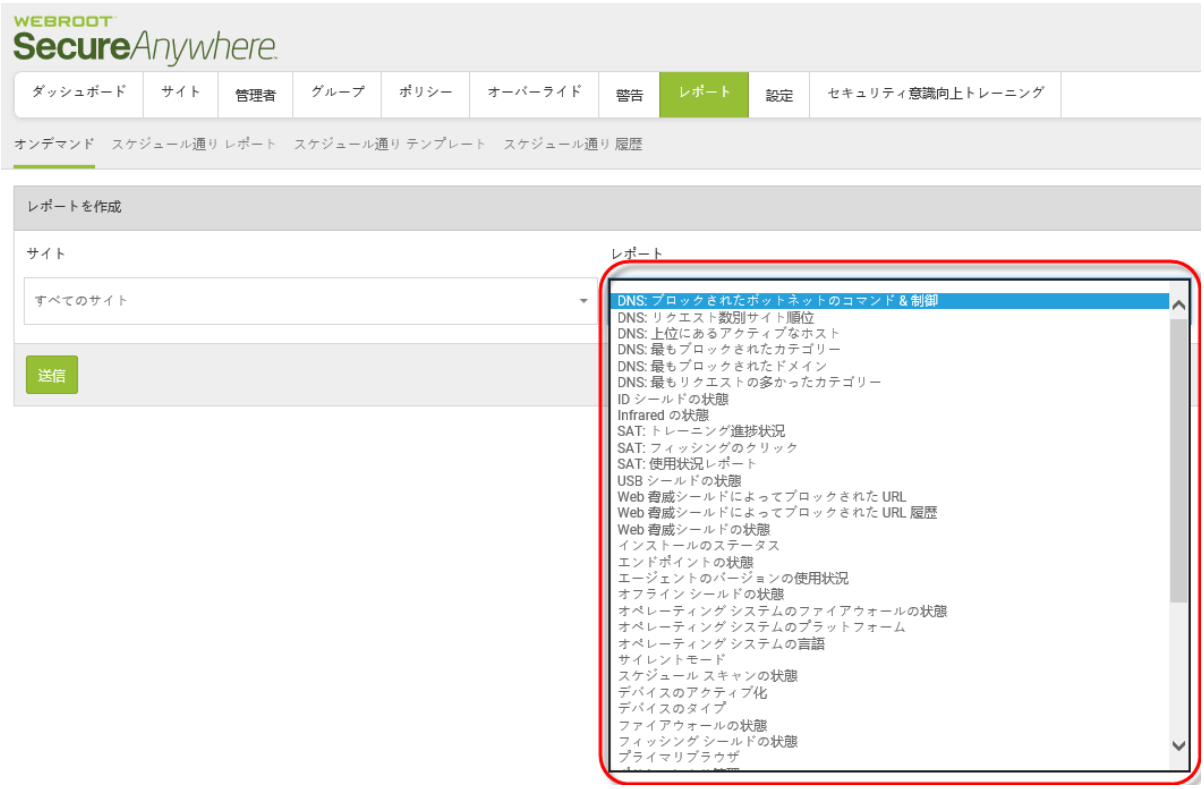
2. [**レポート**] タブをクリックします。



[オンデマンド] タブがアクティブな状態で [レポート] ペインが表示されます。

3. ドロップダウン メニューから、レポートを生成するサイトを選択します。

4. レポートのドロップダウン メニューから、生成するレポートを選択します。



レポートのすべてのオプションについては以下の表をご覧ください。

データ フィールド	レポート 説明	チャート タイプ	期間
エージェントのバージョンの使用状況	各エンドポイント デバイスが使用している Webroot Secure Anywhere エージェントのバージョンを表示します。	棒グラフ、カラム チャート、円グラフ	なし
確認されたすべての脅威	検出された脅威を特定します。このレポートには脅威がファイル名でリストされ、SecureAnywhere で脅威を検出された時と場所が表示されます。	スプレッドシート	[期間] ドロップダウン メニューから [日付取得] を使用して日付範囲を選択します。指定できる範囲は過去 7 日間から過去 90 日間までです。さらに、カスタムの日付範囲を作成することもできます。
確認されたすべての未判定のソフトウェア	「未判定」と分類されたファイルを特定します。これに該当するのは、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であり、安全なファイルにもマルウェアにも分類できない実行可能ファイルであることが一般的です。	スプレッドシート	[期間] ドロップダウン メニューから [日付取得] を使用して日付範囲を選択します。指定できる範囲は過去 7 日間から過去 90 日間までです。さらに、カスタムの日付範囲を作成することもできます。

データ フィールド	レポート 説明	チャート タイプ	期間
注意が必要	安全であると判断されたすべてのエンドポイント デバイス、および対応が必要と判断されたすべてのエンドポイント デバイスのリストを表示します。	棒グラフ、カラム チャート、円グラフ	なし
デバイスのアクティブ化	選択した期間にアクティブ化されたすべてのエンドポイント デバイスのリストを表示します。	面グラフ、スプライン面グラフ、棒グラフ、カラム チャート、折れ線グラフ、スプライン グラフ	24 時間、1 日、2 日、3 日、7 日、14 日、30 日、60 日、90 日
デバイスのタイプ	PC または Mac のエンドポイント デバイス数のリストを表示します。	棒グラフ、カラム チャート、円グラフ	なし
注意の必要なデバイス	「要対応」状態であるデバイスのリストを表示します。	リスト	24 時間、1 日、2 日、3 日、7 日、14 日、30 日、60 日、90 日

データ フィールド	レポート 説明	チャート タイプ	期間
最新のスキャンで脅威が確認されたデバイス	脅威をエンドポイントの場所別に表示します。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が行えます。	スプレッドシート	[期間] ドロップダウン メニューから [日付取得] を使用して日付範囲を選択します。指定できる範囲は過去 7 日間から過去 90 日間までです。さらに、カスタムの日付範囲を作成することもできます。
最新のスキャンで未判定のソフトウェアが検出されたデバイス	「未判定」と分類されたファイルのあるデバイスを特定します。これに該当するのは、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であり、安全なファイルにもマルウェアにも分類できない実行可能ファイルであることが一般的です。	スプレッドシート	[期間] ドロップダウン メニューから [日付取得] を使用して日付範囲を選択します。指定できる範囲は過去 7 日間から過去 90 日間までです。さらに、カスタムの日付範囲を作成することもできます。
エンドポイントの状態	サイト上のクリーンなエンドポイント デバイスおよび感染したエンドポイント デバイスの数を表示します。	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
期限切れの状態	アクティブなエンドポイント デバイス、および状態が「期限切れ」のエンドポイント デバイスの数を表示します。	棒グラフ、カラム チャート、円グラフ	なし
ファイアウォールの状態	ファイアウォールの各オプションがどのエンドポイント デバイスに設定されているかを表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
ID シールドの状態	ID シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
Infrared の状態	Webroot Infrared の各オプションがどのエンドポイント デバイスに設定されているかを表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
インストールの状態	Webroot Secure Anywhere 製品がインストールされているエンドポイント デバイス、およびこれまでに Webroot Secure Anywhere 製品がアンインストールされたことのあるエンドポイント デバイスを表示します。	棒グラフ、カラム チャート、円グラフ	なし
ポリシーにより管理	作成したポリシーにより管理されているエンドポイント デバイス、および管理されていない状態のエンドポイント デバイスの数を表示します。	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
オフライン シールドの状態	オフライン シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
オペレーティング システムのファイアウォールの状態	オペレーティング システムのファイアウォールの各オプションがどのエンドポイント デバイスに設定されているかを表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
オペレーティング システムの言語	エンドポイント デバイスで使用されているオペレーティング システムの言語を表示します。	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
オペレーティング システムのプラットフォーム	エンドポイント デバイスで使用されているオペレーティング システムのプラットフォーム (32 ビット、64 ビット、または不明) を表示します。	棒グラフ、カラム チャート、円グラフ	なし
フィッシング シールドの状態	フィッシング シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし
プライマリ ブラウザ	各エンドポイント デバイスで使用されているプライマリ ウェブ ブラウザを表示します。	棒グラフ、カラム チャート、円グラフ	なし
リアルタイム シールドの状態	リアルタイム シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
対応の状態	対応の状態の各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効 対応の状態を無効化するには、[ブロックされたファイルを自動的に隔離する]オプションを**オフにする必要があります**。	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
概要レポート	サイトまたは配備に関する情報の概要を全体の合計値で表示します: • アクティブなデバイスの数 • エンドポイントが現在注意を必要としている利用可能なシートの数 • 脅威にさらされたエンドポイント (過去 n 日間) • 確認された脅威の総数 (過去 n 日間) • 確認されたエンドポイントの数 (過去 n 日間) • 確認されていないエンドポイントの数 (過去 n 日間) • 確認されたエンドポイントの数 (累計)	棒グラフ、カラム チャート、円グラフ	なし

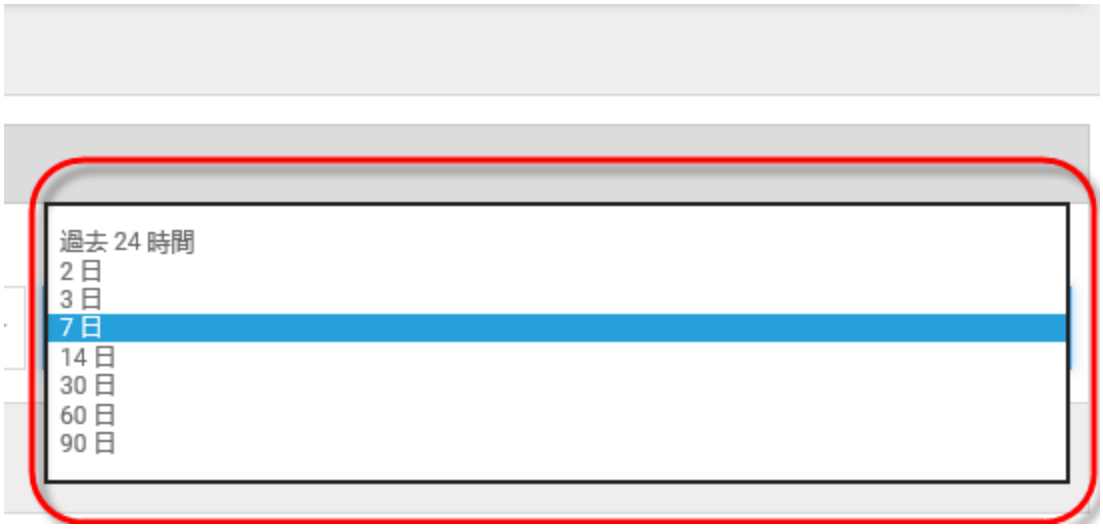
データ フィールド	レポート 説明	チャート タイプ	期間
ルートキット シールドの状態	ルートキット シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
スケジュール スキャンの状態	スケジュール スキャンの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし
サイレント モード	サイレント監査の各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
脅威の検出履歴	選択した期間内にエンドポイント デバイスで検出されたすべての脅威の履歴を表示します。	面グラフ、スプライン面グラフ、棒グラフ、カラム チャート、折れ線グラフ、スプライン グラフ	24 時間、1 日、2 日、3 日、7 日、14 日、30 日、60 日、90 日
USB シールドの状態	USB シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
仮想マシン	仮想マシン (VM) に分類されたエンドポイント デバイスの数を表示します。	棒グラフ、カラム チャート、円グラフ	なし
Web 脅威シールドによってブロックされた URL 履歴	ウェブルートの Web 脅威シールドによってブロックされた URL の履歴を表示します。	スプレッドシート	[期間] ドロップダウン メニューから [日付取得] を使用して日付範囲を選択します。指定できる範囲は過去 7 日間から過去 90 日間までです。さらに、カスタムの日付範囲を作成することもできます。

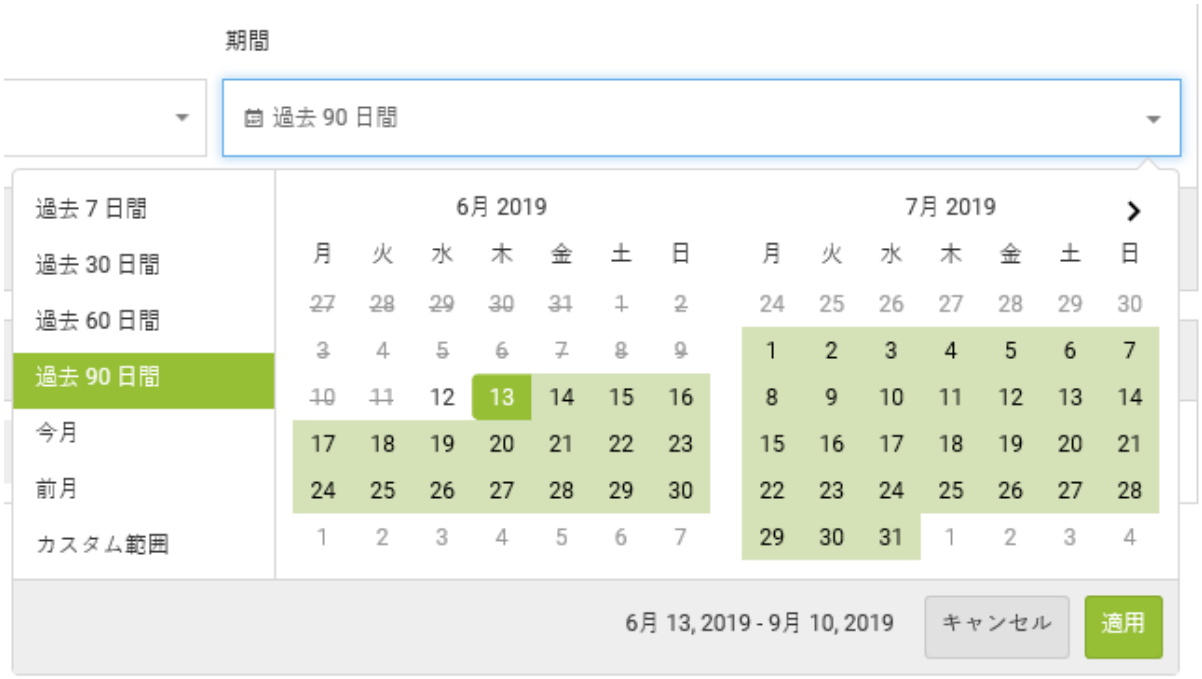
データ フィールド	レポート 説明	チャート タイプ	期間
Web 脅威シールドによってブロックされた URL	ウェブルートの Web 脅威シールドによってブロックされた URL のリストを表示します。	スプレッド シート	[期間] ドロップダウン メニューから [日付取得] を使用して日付範囲を選択します。指定できる範囲は過去 7 日間から過去 90 日間までです。さらに、カスタムの日付範囲を作成することもできます。
Web 脅威シールドの状態	Web 脅威シールド オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし

5. レポートの生成期間が選べる場合は、[期間] のドロップダウン メニューから 1 つ選択してください:

   - 過去 24 時間
   - 2 日
   - 3 日
   - 14 日
   - 30 日 - これはデフォルト設定です。
   - 60 日
   - 90 日

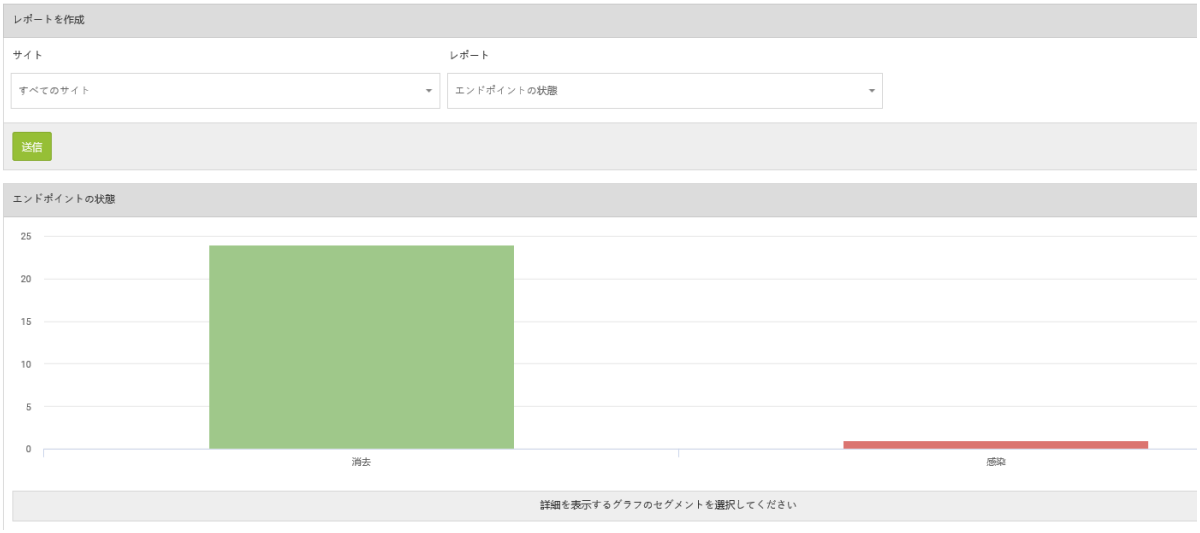


6. レポートで日付取得機能を試用できる場合は、[期間] のドロップダウン メニューから次のいずれかの日付範囲を選択して、[**適用**] ボタンをクリックします。

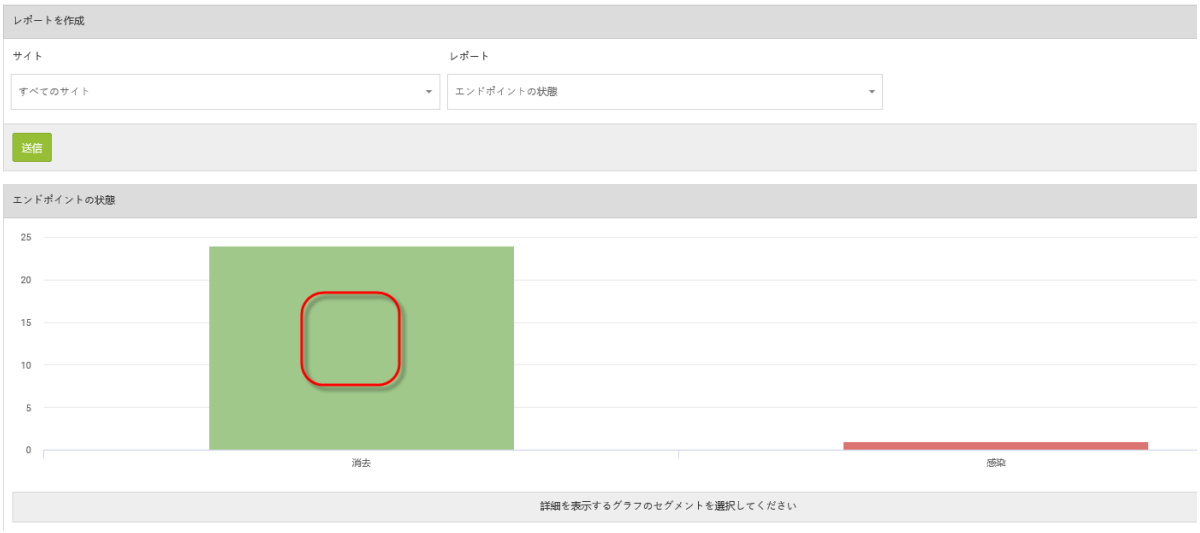


7. 設定が完了したら、[**送信**] ボタンをクリックします。

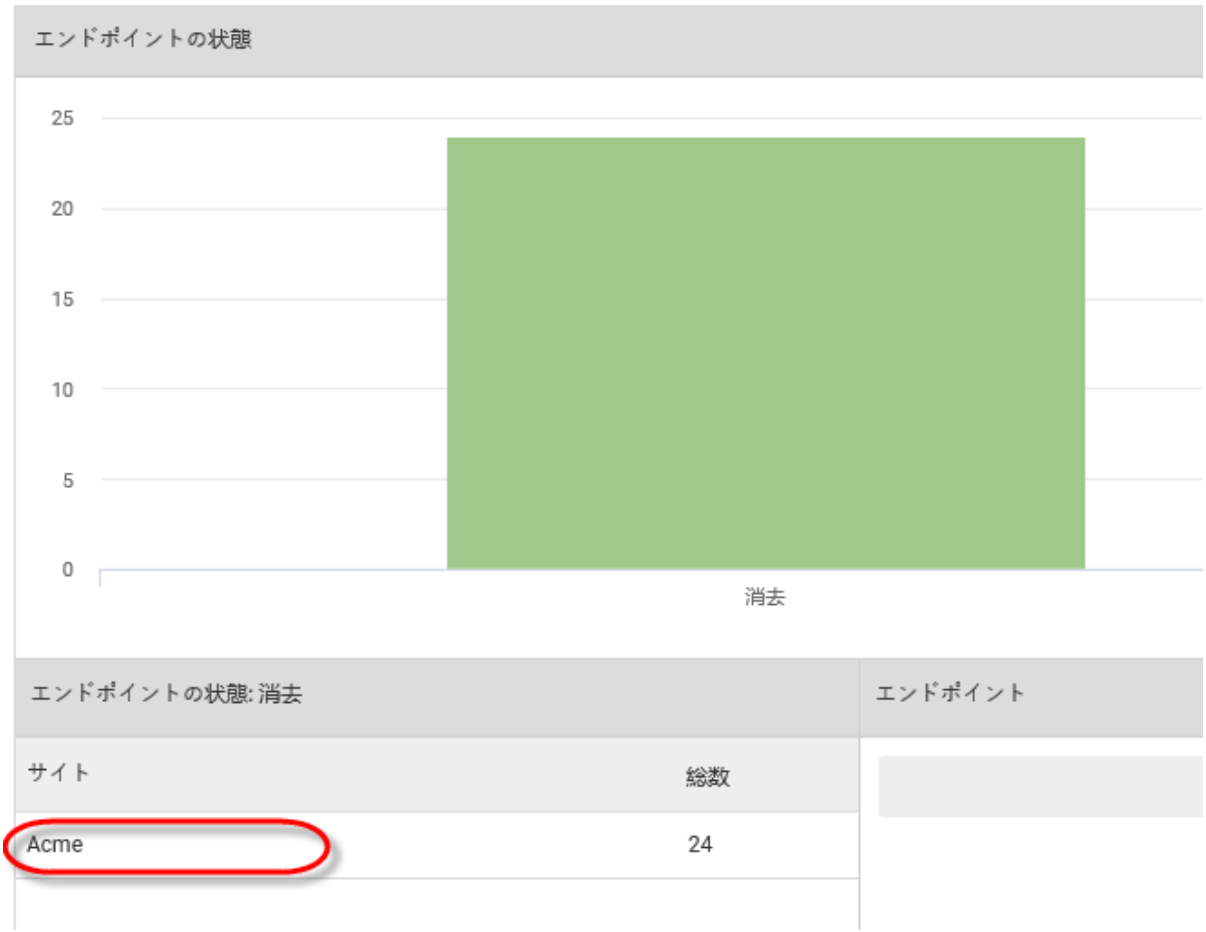
レポートがグラフィック形式でコンソールに表示されます。



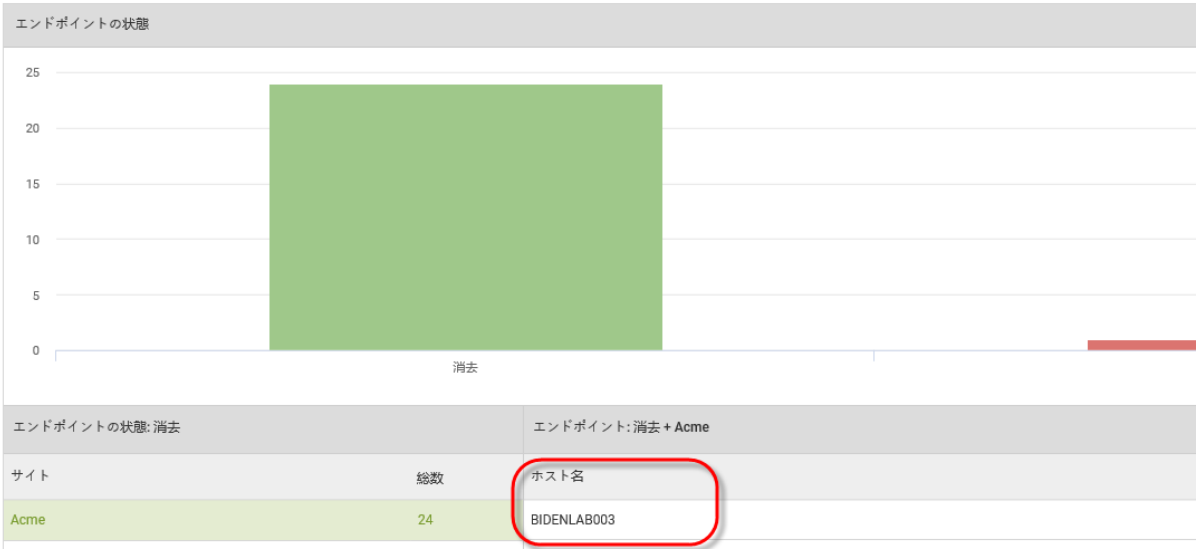
8. 情報を表示するには、各部をクリックします。



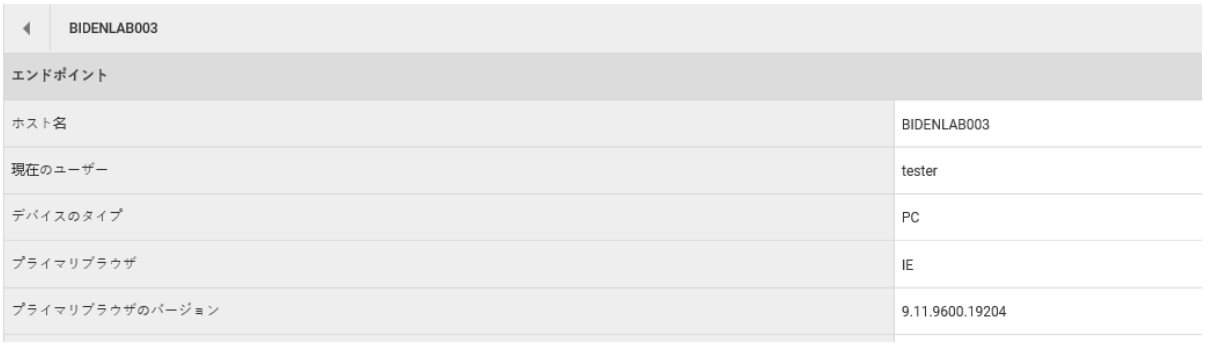
9. 左側のパネルでいずれかのサイトをクリックすると、特定のサイトについて詳細な情報を表示することができます。



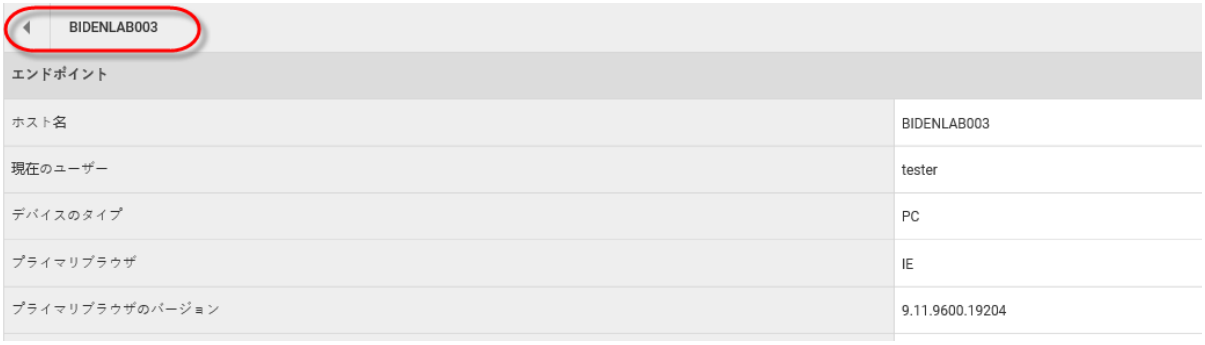
以下のように、そのサイトについての詳細な情報が表示されます。



10. [ホスト名] カラムでいずれかのホスト名をクリックすると、そのホストについてのより具体的で詳細な情報が表示されます。右側のスクロールバーを使うとすべての情報を見ることができます。



11. 終了後は**左**矢印をクリックして前の画面に戻ります。



レポート テンプレートの作成

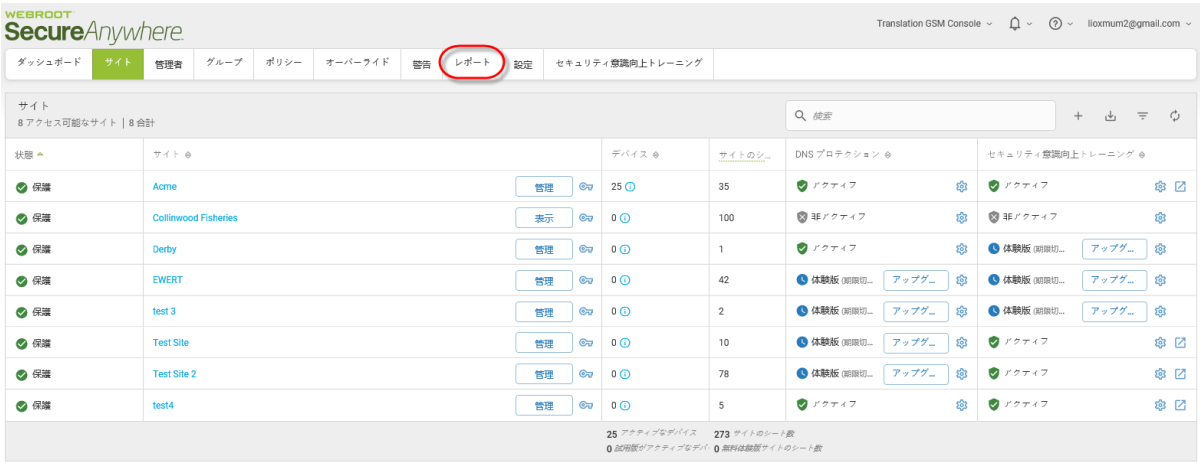
レポートのスケジューリング機能では、カスタマイズ可能なテンプレートを使用します。必要なコンテンツを含むレポートを作成する際に、ページの追加や削除、データや期間の選択を簡単に行うことができます。デフォルトのテンプレートが含まれており、必要に応じて変更、コピー、削除できます。または、新しいテンプレートを作成することもできます。

レポートのテンプレートを作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**レポート**] タブをクリックします。



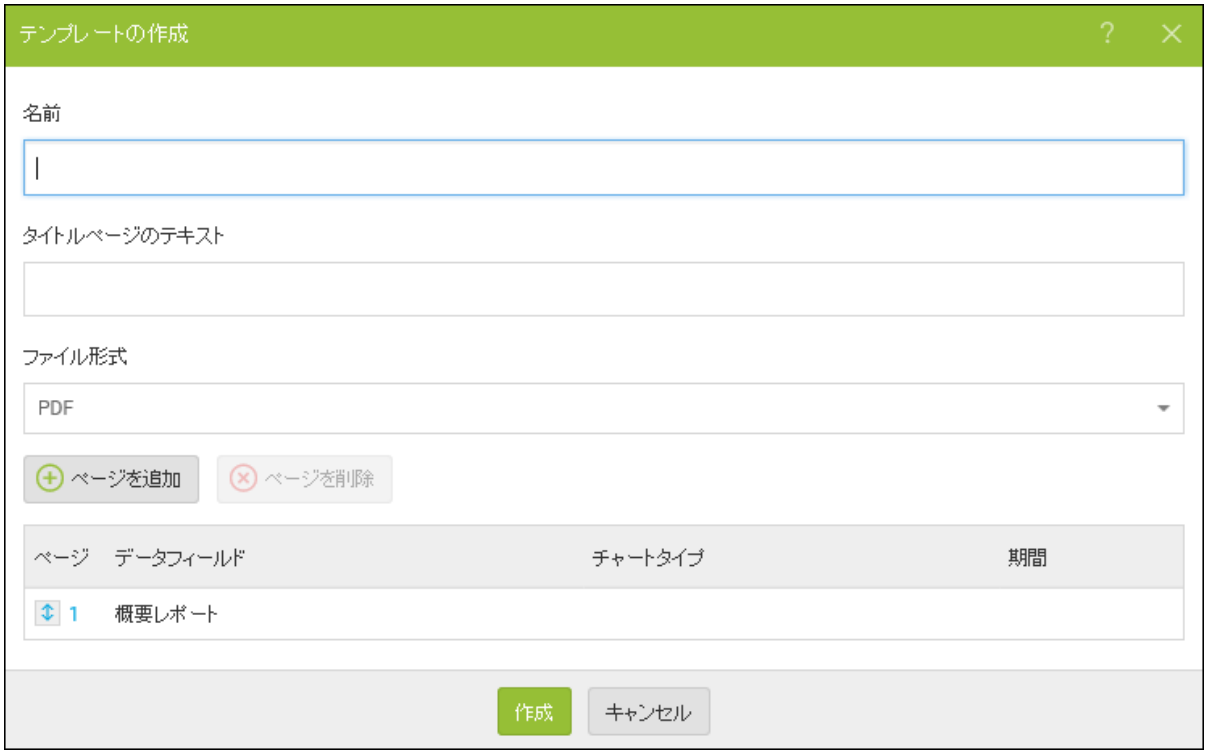
   [オンデマンド] タブがアクティブな状態で [レポート] ペインが表示されます。

3. [**スケジュールされたテンプレート**] タブをクリックします。

[スケジュールされたテンプレート] タブが表示されます。

4. [**追加**] ボタンをクリックします。

[テンプレートの作成] ウィンドウが表示されます。



5. [名前] フィールドにテンプレートの識別子を入力します (例: *概要テンプレート*)。
6. [タイトルページのテキスト] フィールドに、レポートのカバー ページに表示されるテキストを入力します。
7. [ファイル形式] フィールドのドロップダウン メニューから次のいずれかの形式を選択します:
   - **PDF**
   - **CSV**
8. [ページ] カラムで、**上矢印**と**下矢印**を使用して、テンプレートに含むページの数を指定します。
9. [データフィールド] カラムのドロップダウン メニューから、各ページに含むデータの種類を選択します。
10. [チャート タイプ] カラムで、レポート結果を表示するチャートのタイプを選択します (例: *棒グラフ*、*カラム チャート*、*円グラフ*)。

    [デバイスのアクティブ化] と [脅威の検出履歴] では、他のチャート タイプを選択することができます。

11. 必要に応じて、レポートで使用する期間を [期間] カラムで選択します。

> **注意:** 特定の期間を選択できるのは [デバイスのアクティブ化] と [脅威の検出履歴] についてのみです。

12. レポートのすべてのオプションについては以下の表をご覧ください。

データ フィールド	レポート 説明	チャート タイプ	期間
エージェントのバージョンの使用状況	各エンドポイント デバイスが使用している Webroot Secure Anywhere エージェントのバージョンを表示します。	棒グラフ、カラム チャート、円グラフ	なし
注意が必要	安全であると判断されたすべてのエンドポイント デバイス、および対応が必要と判断されたすべてのエンドポイント デバイスのリストを表示します。	棒グラフ、カラム チャート、円グラフ	なし
デバイスのアクティブ化	選択した期間にアクティブ化されたすべてのエンドポイント デバイスのリストを表示します。	面グラフ、スプライン面グラフ、棒グラフ、カラム チャート、折れ線グラフ、スプライン グラフ	24 時間、1 日、2 日、3 日、7 日、14 日、30 日、60 日、90 日

データ フィールド	レポート 説明	チャート タイプ	期間
デバイスのタイプ	PC または Mac のエンドポイント デバイス数のリストを表示します。	棒グラフ、カラム チャート、円グラフ	なし
エンドポイントの状態	サイト上のクリーンなエンドポイント デバイスおよび感染したエンドポイント デバイスの数を表示します。	棒グラフ、カラム チャート、円グラフ	なし
期限切れの状態	アクティブなエンドポイント デバイス、および状態が「期限切れ」のエンドポイント デバイスの数を表示します。	棒グラフ、カラム チャート、円グラフ	なし
ファイアウォールの状態	ファイアウォールの各オプションがどのエンドポイント デバイスに設定されているかを表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
ID シールドの状態	ID シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし
Infrared の状態	Webroot Infrared の各オプションがどのエンドポイント デバイスに設定されているかを表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
インストールのステータス	Webroot Secure Anywhere 製品がインストールされているエンドポイント デバイス、およびこれまでに Webroot Secure Anywhere 製品がアンインストールされたことのあるエンドポイント デバイスを表示します。	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
ポリシーにより管理	作成したポリシーにより管理されているエンドポイント デバイス、および管理されていない状態のエンドポイント デバイスの数を表示します。	棒グラフ、カラム チャート、円グラフ	なし
オフライン シールドの状態	オフライン シールドの各オプションが設定されているエンドポイント デバイスの数を表示します。 • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
オペレーティング システムのファイアウォールの状態	オペレーティング システムのファイアウォールの各オプションがどのエンドポイント デバイスに設定されているかを表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
オペレーティング システムの言語	エンドポイント デバイスで使用されているオペレーティング システムの言語を表示します。	棒グラフ、カラム チャート、円グラフ	なし
オペレーティング システムのプラットフォーム	エンドポイント デバイスで使用されているオペレーティング システムのプラットフォーム (32 ビット、64 ビット、または不明) を表示します。	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
フィッシング シールドの状態	フィッシング シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし
プライマリ ブラウザ	各エンドポイント デバイスで使用されているプライマリ ウェブブラウザを表示します。	棒グラフ、カラム チャート、円グラフ	なし
リアルタイム シールドの状態	リアルタイム シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
対応の状態	対応の状態の各オプションが設定されているエンドポイント デバイスの数を表示します。 • 無効 • 有効 対応の状態を無効化するには、[**ブロックされたファイルを自動的に隔離する**] オプションをオフにする必要があります。	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
概要レポート	サイトまたは配備に関する情報の概要を全体の合計値で表示します: • アクティブなデバイスの数 • エンドポイントが現在注意を必要としている利用可能なシートの数 • 脅威にさらされたエンドポイント (過去 n 日間) • 確認された脅威の総数 (過去 n 日間) • 確認されたエンドポイントの数 (過去 n 日間) • 確認されていないエンドポイントの数 (過去 n 日間) • 確認されたエンドポイントの数 (累計)	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
ルートキット シールドの状態	ルートキット シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
スケジュール スキャンの状態	スケジュール スキャンの各オプションが設定されているエンドポイント デバイスの数を表示します。 • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし

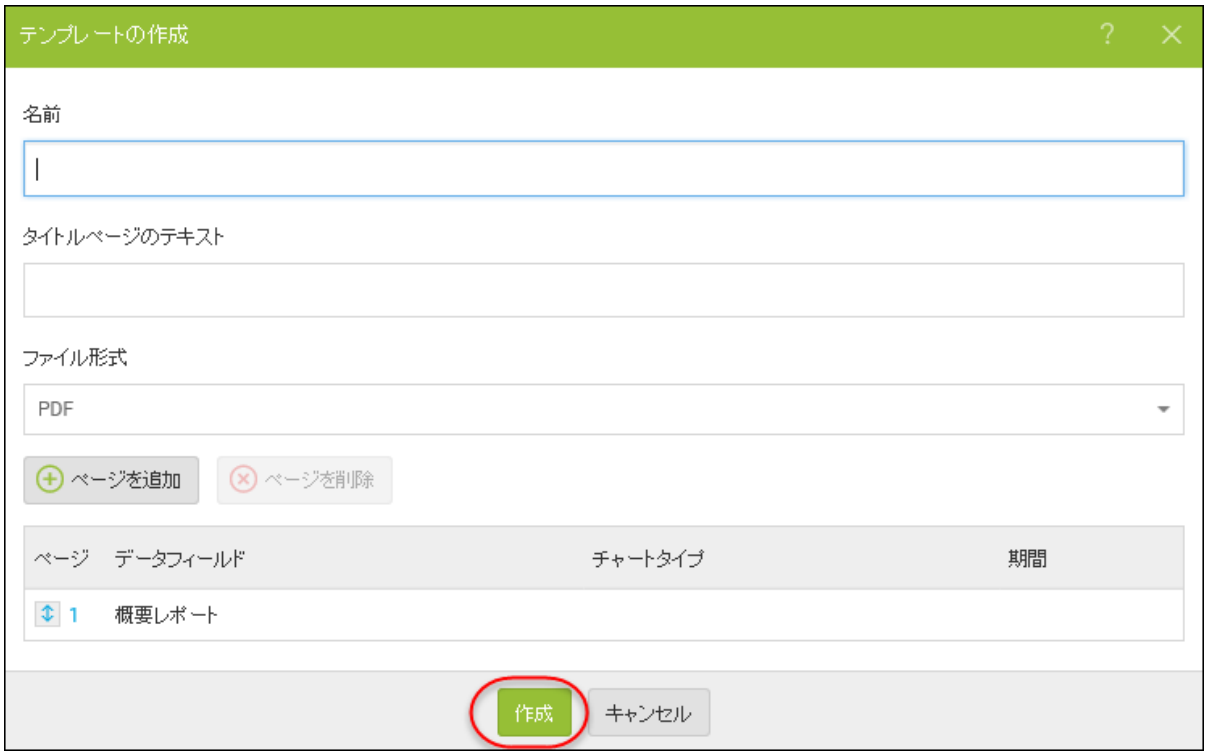
データ フィールド	レポート 説明	チャート タイプ	期間
サイレント モード	サイレント監査の各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし
脅威の検出履歴	選択した期間内にエンドポイント デバイスで検出されたすべての脅威の履歴を表示します。	面グラフ、スプライン面グラフ、棒グラフ、カラム チャート、折れ線グラフ、スプライン グラフ	24 時間、1 日、2 日、3 日、7 日、14 日、30 日、60 日、90 日
USB シールドの状態	USB シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効 • サポートされていません	棒グラフ、カラム チャート、円グラフ	なし

データ フィールド	レポート 説明	チャート タイプ	期間
仮想マシン	仮想マシン (VM) に分類されたエンドポイント デバイスの数を表示します。	棒グラフ、カラム チャート、円グラフ	なし
Web 脅威シールドの状態	USB シールドの各オプションが設定されているエンドポイント デバイスの数を表示します: • 無効 • 有効	棒グラフ、カラム チャート、円グラフ	なし

複数のサイトの統計データを 1 つのレポートで列記する場合は、次の情報も含まれます:

- サイト総数
- アクティブなサイト
- 体験版サイト
- 一時停止したサイト
- 非アクティブ化したサイト
- 期限切れのサイト
- 14 日以内に期限が切れるサイト
- 対応が必要なエンドポイントのあるサイト

13. 設定が完了したら、[**作成**] ボタンをクリックします。



レポート履歴へのアクセス

リクエストされた日や受信者の概要を含む過去 90 日間に実行されたすべてのレポートの履歴レコードにアクセスできるほか、スケジュールの一部として送信された内容そのものをダウンロードする機能が使用できます。ダウンロードをリクエストすると、元の生成時に含まれていたテンプレート、サイト、および言語が選択可能になり、配信先リスト上の関係者に送信された内容と同じものを見ることができます。

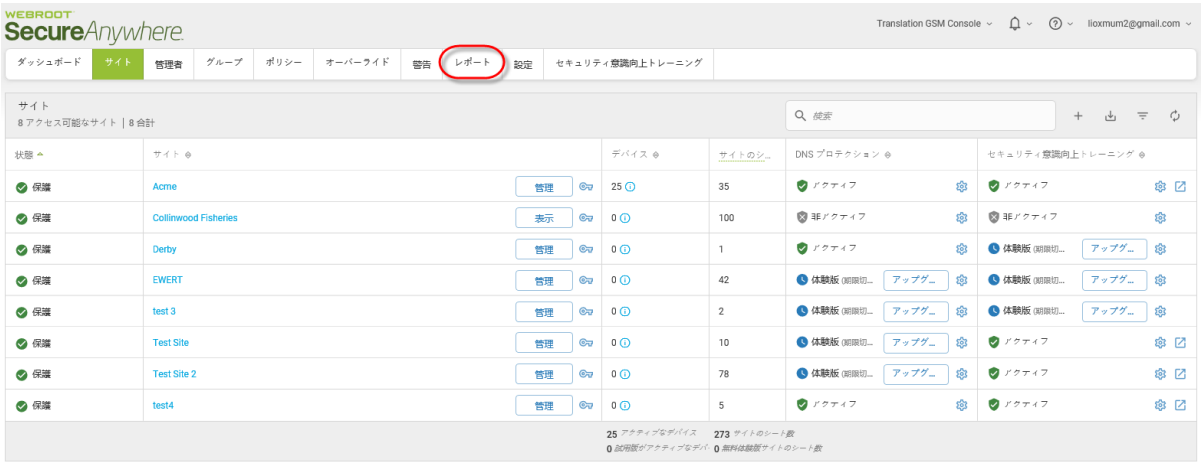
注意: レポートは、PDF 形式でのみ入手可能です。レポートはダウンロード用履歴を通じて 90 日間入手できます。メールで届いたレポートのダウンロード用リンクは 48 時間のみ有効です。

レポートの履歴にアクセスするには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**レポート**] タブをクリックします。



[オンデマンド] タブがアクティブな状態で [レポート] タブが表示されます。

3. [スケジュールされた履歴] タブをクリックします。

[履歴] ペインに次の情報が表示されます:

- レポート名
- 作成タイプ
- 受信者
- サイト
- リクエストされた日
- 状態
- PDF をダウンロード

レポートのダウンロード

スプレッドシート形式で表示されるレポートは、CSV 形式にエクスポートできます。

この操作が可能なレポートは次のとおりです。

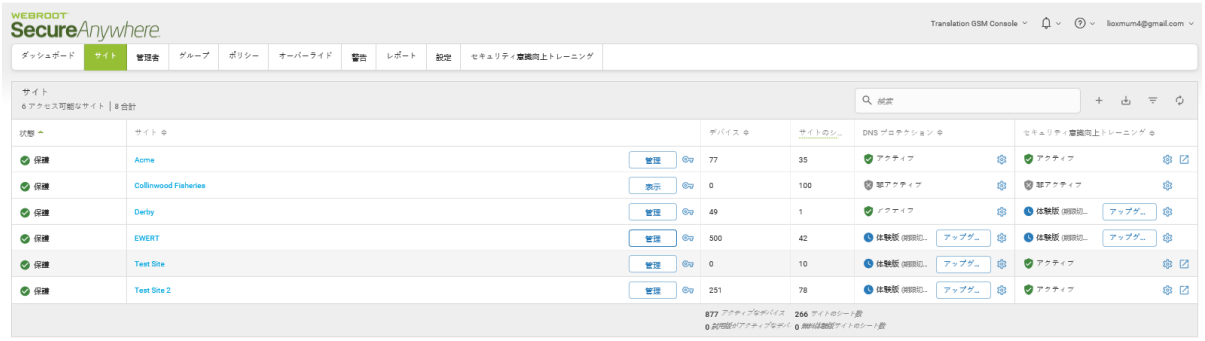
- 確認されたすべての脅威
- 確認されたすべての未判定のソフトウェア
- 最新のスキャンで脅威が確認されたデバイス
- 最新のスキャンで未判定のソフトウェアが検出されたデバイス
- Web 脅威シールドによってブロックされた URL 履歴
- Web 脅威シールドによってブロックされた URL

詳細については、「*408{/u}{/color} ページの「オンデマンド レポートの生成」*」を参照してください。

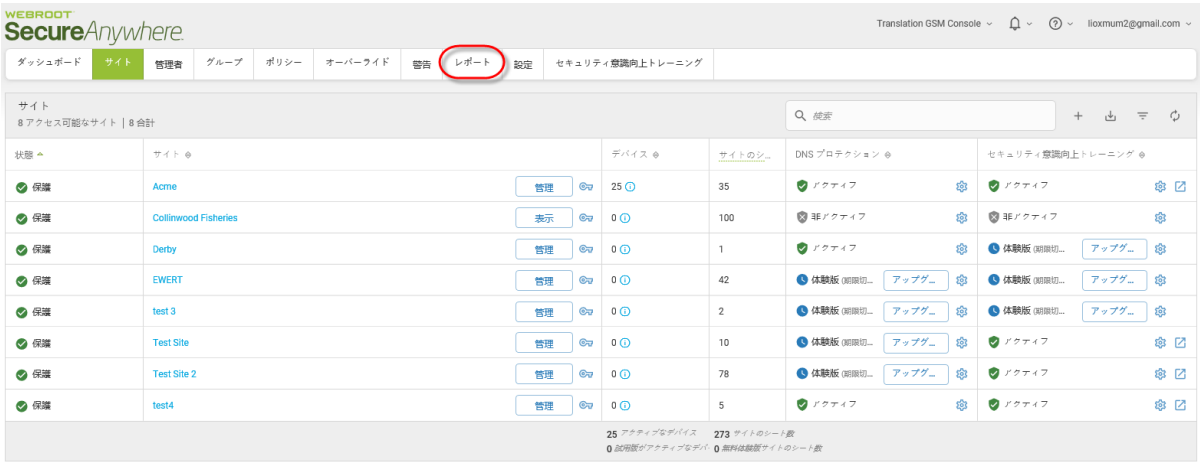
レポートをダウンロードするには:

1. 管理コンソールにログインします。

   [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が表示されます。



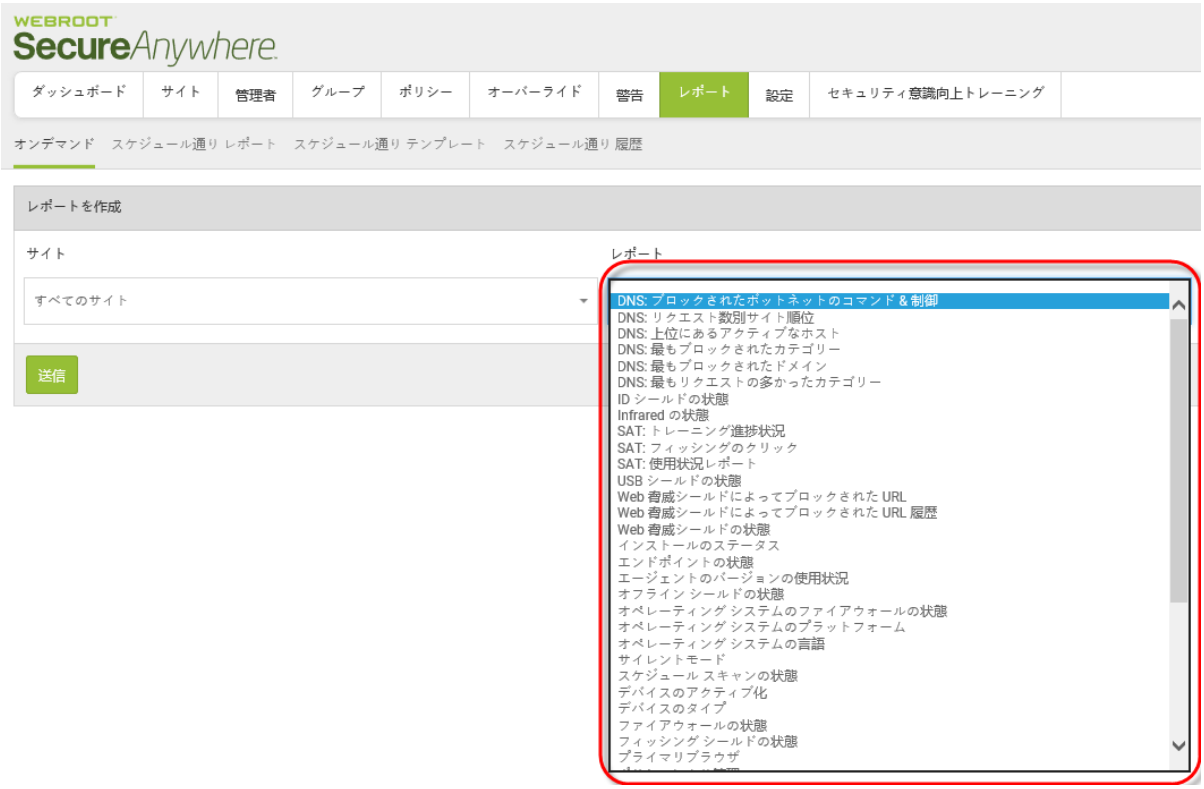
2. [**レポート**] タブをクリックします。



[オンデマンド] タブがアクティブな状態で [レポート] ペインが表示されます。

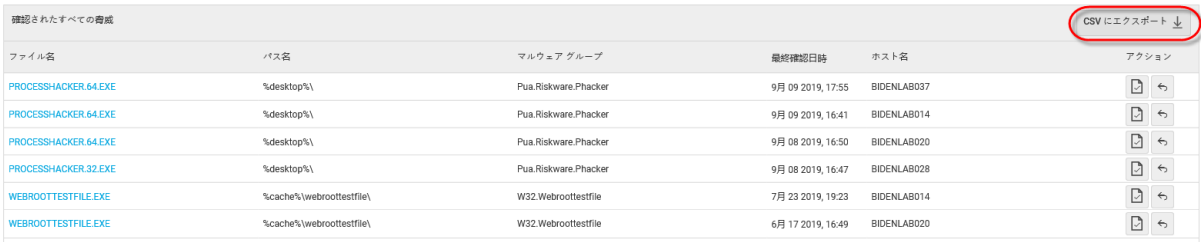
3. ドロップダウン メニューから、レポートを生成するサイトを選択します。

4. レポートのドロップダウン メニューから、生成するレポートを選択します。



レポートがスプレッドシート形式で表示されます。

5. [**CSV にエクスポート**] ボタンをクリックします。



「*CSV ファイルがリクエストされました。ファイルはアカウントに登録された電子メールアドレス宛てに送信されます。*」というメッセージが表示されます。

6. レポートのスプレッドシートに戻るには、[**OK**] ボタンをクリックします。

第 11 章: 設定の操作

設定を操作するには、次のトピックを参照してください:

設定概要

[設定] タブには次の機能があります:

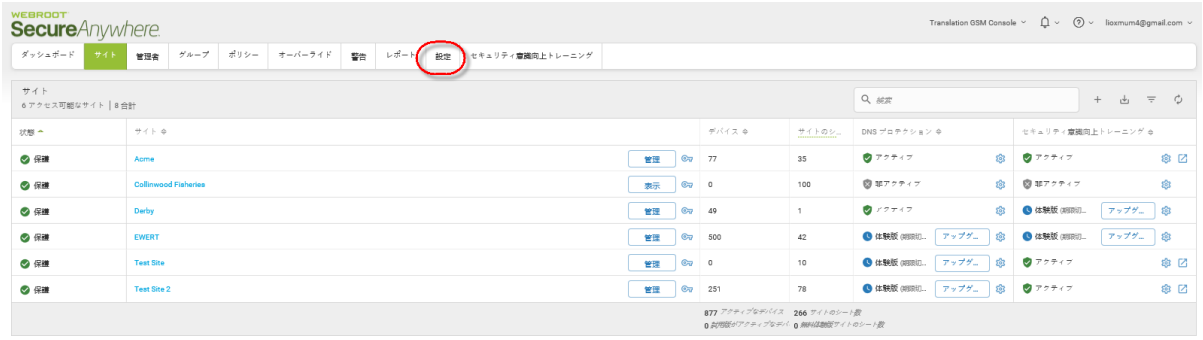
- *DNS プロテクションのサブスクリプションのアクティブ化*
- *セキュリティ意識向上トレーニングのサブスクリプションのアクティブ化*
- *アカウント情報の表示*
- *474{/u}{/color} ページの「GSM レベルのデータフィルタの設定」*
- *480{/u}{/color} ページの「API クライアント認証情報の作成」*

[設定] タブにアクセスするには:

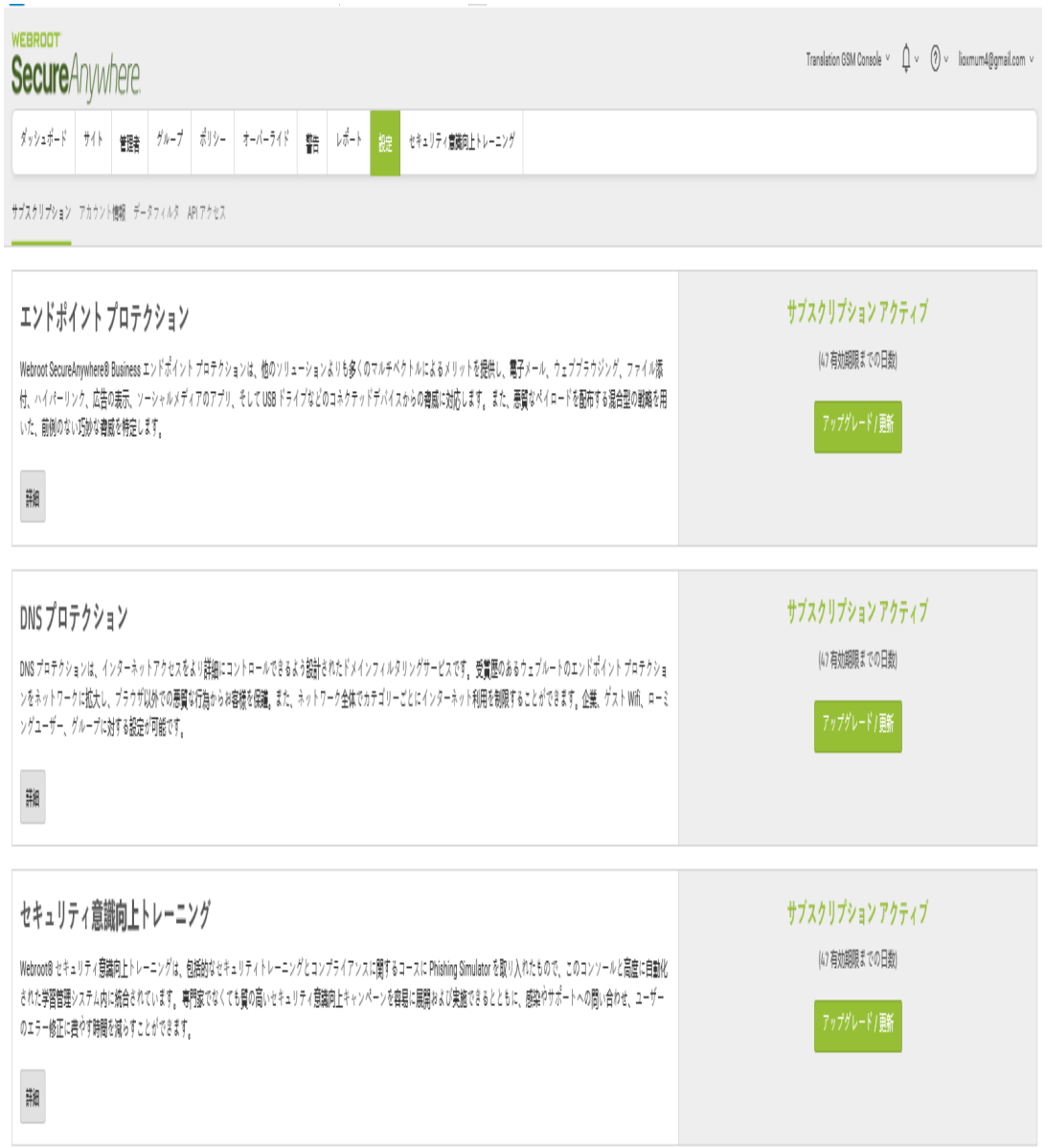
1. 管理コンソールにログインします。

   [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が表示されます。

2. [**設定**] タブをクリックします。



   [サブスクリプション] タブがアクティブな状態で [設定] タブが表示されます。



3. [設定] タブで使用可能な機能の詳細は、各項目をクリックしてください:
   - *DNS プロテクションのサブスクリプションのアクティブ化*
   - *セキュリティ意識向上トレーニングのサブスクリプションのアクティブ化*
   - *474{/u}{/color} ページの「GSM レベルのデータフィルタの設定」*

- 456{/u}{/color} ページの「アカウント情報の表示」
- 480{/u}{/color} ページの「API クライアント認証情報の作成」

アカウント情報の表示

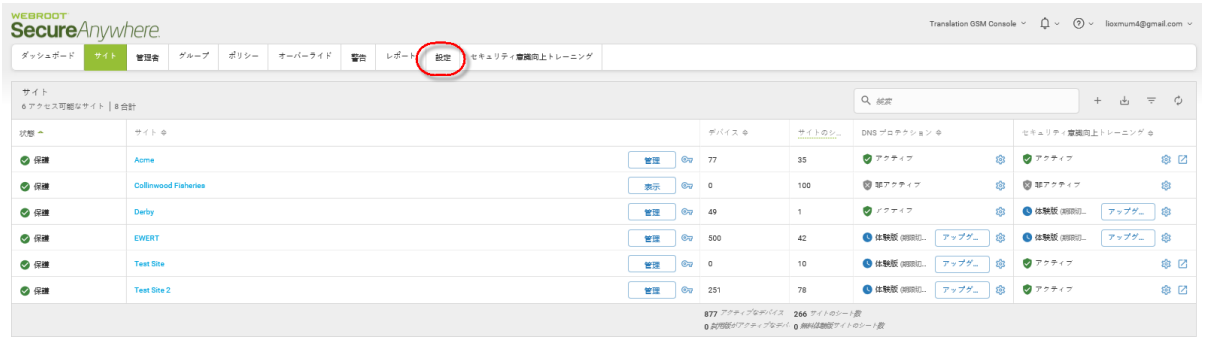
連絡先や支払請求サイクルなど、複数のアカウントについての情報を表示することができます。

アカウント情報を表示するには:

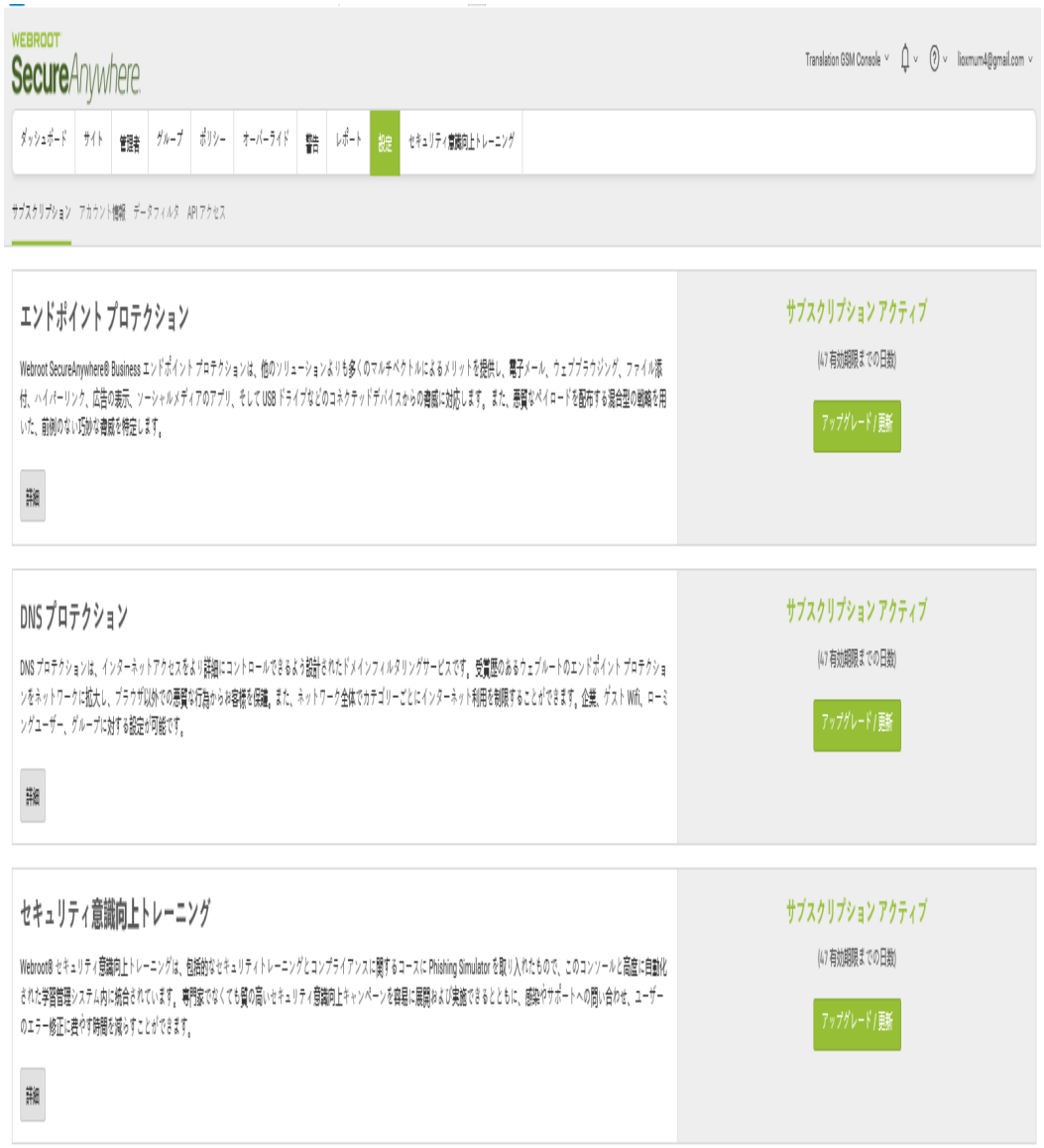
1. 管理コンソールにログインします。

   [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が表示されます。

2. [**設定**] タブをクリックします。



   [サブスクリプション] タブがアクティブな状態で [設定] タブが表示されます。


WEBROOT
SecureAnywhere
Translation GSM Console
liuxmum4@gmail.com
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
サブスクリプション
アカウント情報
データフィルタ
API アクセス
エンドポイント プロテクション
Webroot SecureAnywhere® Business エンドポイント プロテクションは、他のソリューションよりも多くのマルチベクトルによるメリットを提供し、電子メール、ウェブブラウジング、ファイル添付、ハイパーリンク、広告の表示、ソーシャルメディアのアプリ、そして USB ドライブなどのコネクテッドデバイスからの脅威に対応します。また、悪質なペイロードを配布する混合型の戦略を用いた、前例のない巧妙な脅威を特定します。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新
DNS プロテクション
DNS プロテクションは、インターネットアクセスをより詳細にコントロールできるよう設計されたドメインフィルタリングサービスです。受賞歴のあるウェブルートのエンドポイント プロテクションをネットワークに拡大し、ブラウザ以外での悪質な行為からお客様を保護。また、ネットワーク全体でカテゴリーごとにインターネット利用を制限することができます。企業、ゲスト Wifi、ローミングユーザー、グループに対する設定が可能です。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新
セキュリティ意識向上トレーニング
Webroot® セキュリティ意識向上トレーニングは、包括的なセキュリティトレーニングとコンプライアンスに関するコースに Phishing Simulator を取り入れたもので、このコンソールと高度に自動化された学習管理システム内に統合されています。専門家でなくても質の高いセキュリティ意識向上キャンペーンを容易に展開および実施できるとともに、感染やサポートへの問い合わせ、ユーザーのエラー修正に費やす時間を減らすことができます。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新

3. [アカウント情報] タブをクリックします。

[アカウント情報] タブが開いて次の情報が表示されます:

- サイト / 会社名
- 会社住所
- 連絡先の電子メール
- 連絡先電話番号
- 親キーコードは更新またはアップグレードできます。[更新 / アップグレード] ボタンをクリックすると、チャネル パートナーとウェブルートのアカウント マネージャーの情報が表示されます。どちらも更新やアップグレード時のサポートを行っています。
- 使用状況データ。詳細については、「*460{/u}{/color} ページの「使用状況データへのアクセス」*」と「」を参照してください。*468{/u}{/color} ページの「使用状況データ レポートのダウンロード」*


WEBROOT
SecureAnywhere
Console
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
サブスクリプション
アカウント情報
データフィルタ
API アクセス
アカウントの詳細
サイト / 会社名
Console
名前の変更
会社住所
連絡先の電子メール
連絡先電話番号
鍵のキーコード
更新 / アップグレード
このキーコードは、インストールには使用できません。Webroot ソフトウェアをインストールするには、サイト キーコードを正しく入力してください。
使用状況データ
このアカウントの使用状況データを表示するには、下のボタンをクリックし、Webroot 使用状況コンソールを新しいウィンドウで起動します。ウィンドウを閉じると、このコンソールに戻ります。
使用状況コンソール

使用状況データへのアクセス

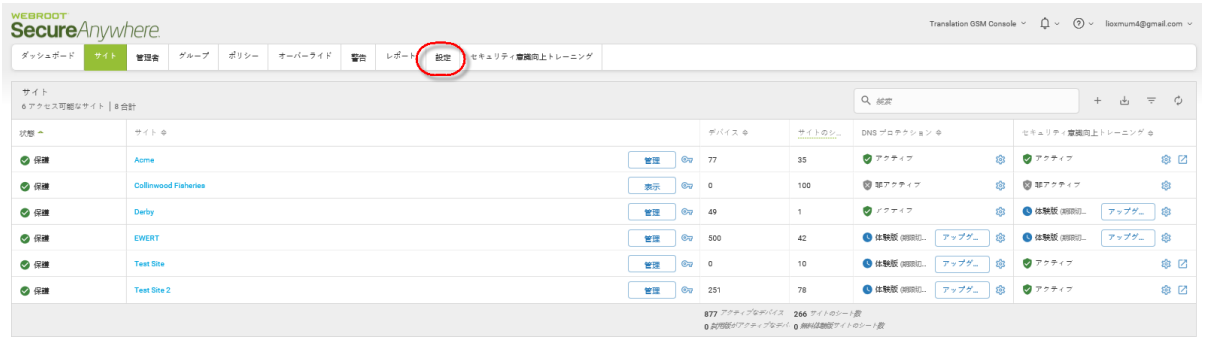
ウェブルートの製品およびサービスの詳細な内訳が含まれた使用状況コンソールを使用して、エンドポイントプロテクション、DNS プロテクション、セキュリティ意識向上トレーニングに関する使用状況データにアクセスできるようになりました。

使用状況データにアクセスするには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**設定**] タブをクリックします。



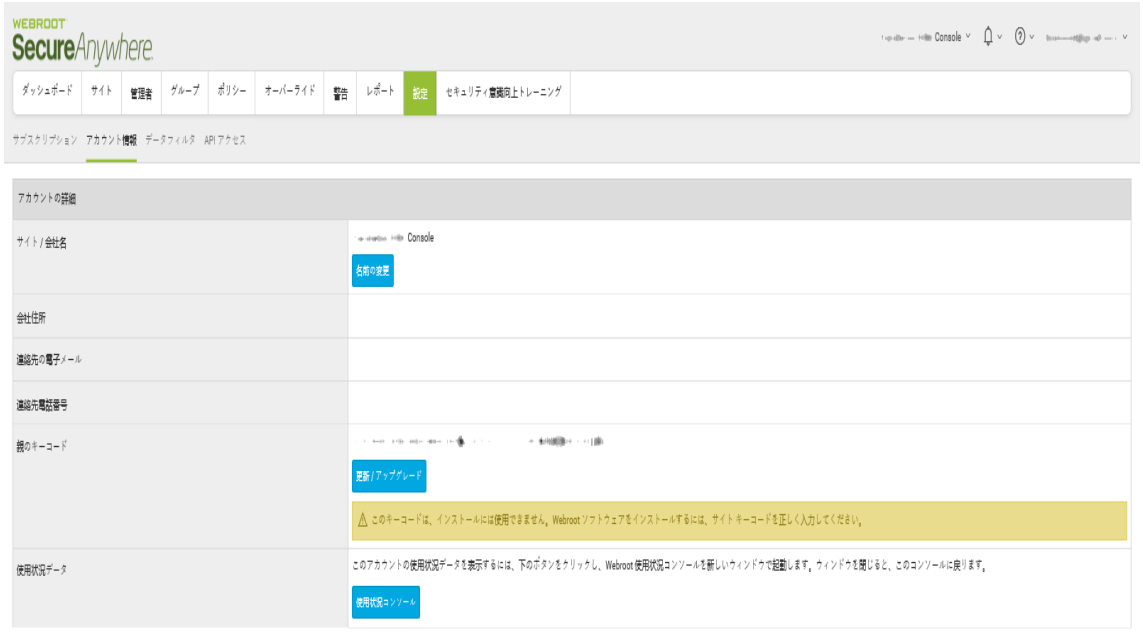
   [サブスクリプション] タブがアクティブな状態で [設定] タブが表示されます。


WEBROOT
SecureAnywhere
Translation GSM Console
liaxmum4@gmail.com
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
サブスクリプション
アカウント情報
データフィルタ
API アクセス
エンドポイント プロテクション
Webroot SecureAnywhere® Business エンドポイント プロテクションは、他のソリューションよりも多くのマルチベクトルによるメリットを提供し、電子メール、ウェブブラウジング、ファイル添付、ハイパーリンク、広告の表示、ソーシャルメディアのアプリ、そして USB ドライブなどのコネクテッドデバイスからの脅威に対応します。また、悪質なペイロードを配布する混合型の戦略を用いた、前例のない巧妙な脅威を特定します。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新
DNS プロテクション
DNS プロテクションは、インターネットアクセスをより詳細にコントロールできるよう設計されたドメインフィルタリングサービスです。受賞歴のあるウェブルートのエンドポイント プロテクションをネットワークに拡大し、ブラウザ以外での悪質な行為からお客様を保護。また、ネットワーク全体でカテゴリーごとにインターネット利用を制限することができます。企業、ゲスト Wifi、ローミングユーザー、グループに対する設定が可能です。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新
セキュリティ意識向上トレーニング
Webroot® セキュリティ意識向上トレーニングは、包括的なセキュリティトレーニングとコンプライアンスに関するコースに Phishing Simulator を取り入れたもので、このコンソールと高度に自動化された学習管理システム内に統合されています。専門家でなくても質の高いセキュリティ意識向上キャンペーンを容易に展開および実施できるとともに、感染やサポートへの問い合わせ、ユーザーのエラー修正に費やす時間を減らすことができます。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新

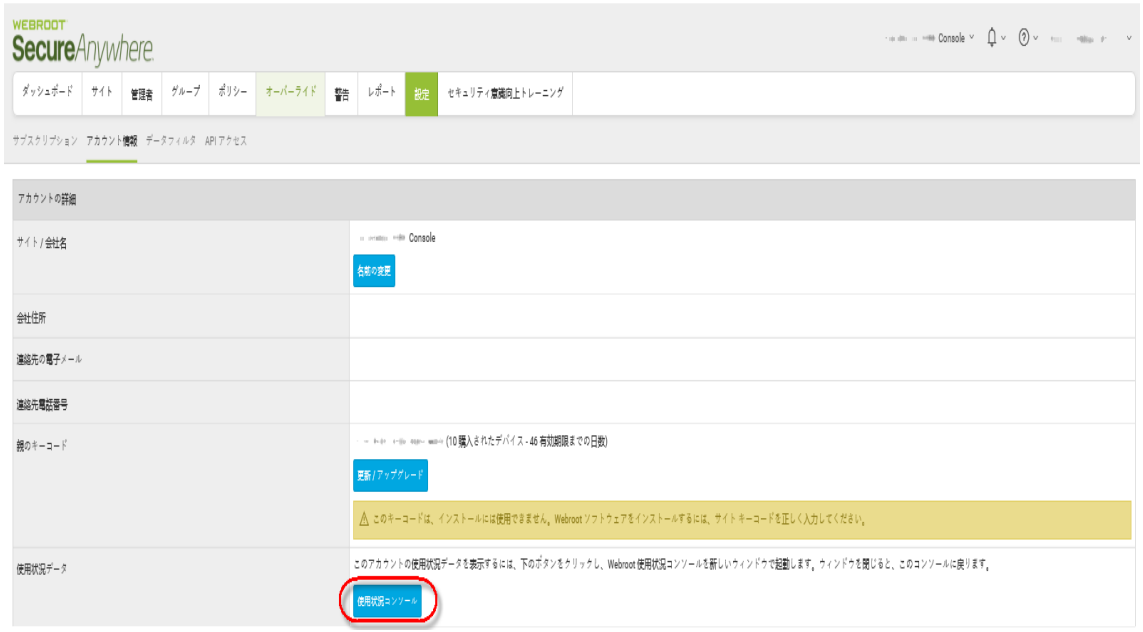
3. [アカウント情報] タブをクリックします。

[アカウント情報] タブが開いて次の情報が表示されます:

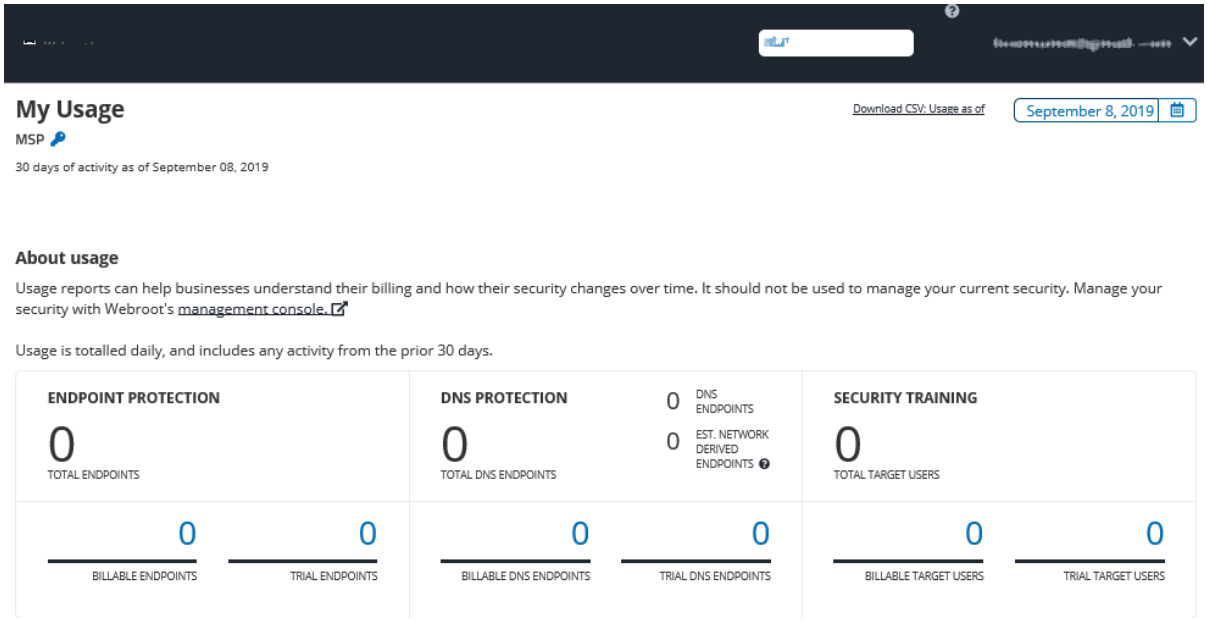
- サイト / 会社名
- 会社住所
- 連絡先の電子メール
- 連絡先電話番号
- 親キーコードは更新またはアップグレードできます。 更新 / アップグレードボタンをクリックすると、チャネル パートナーとウェブルートのアカウント マネージャーの情報が表示されます。どちらも更新やアップグレード時のサポートを行っています。



4. [**使用状況コンソール**] ボタンをクリックします。



使用状況コンソールが表示されます。



使用状況コンソールの上部に、次の情報が表示されます。

- エンドポイント プロテクション、DNS プロテクション、セキュリティ意識向上トレーニングの請求可能なエンドポイント数。
- エンドポイント プロテクション、DNS プロテクション、セキュリティ意識向上トレーニングの試用中エンドポイント数。

注意: 使用状況は、[日付取得] フィールドに指定された日付の 30 日前からのアクティビティを対象に、毎日集計されます。

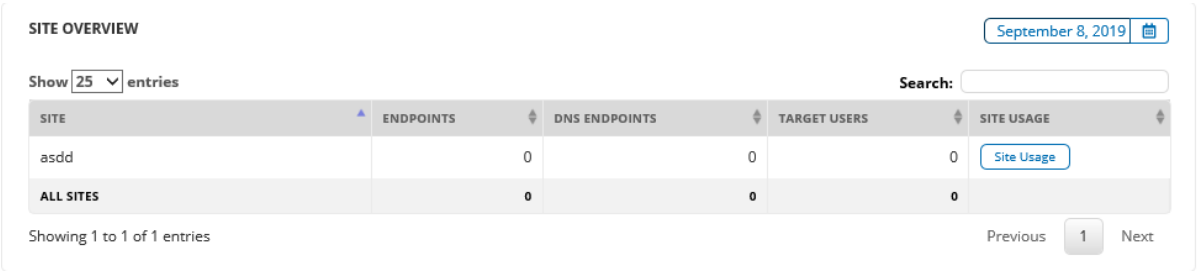
5. 必要に応じて、以下の両方を実行できます:

- [選択] ドロップダウン メニューから別の管理コンソールを選択して使用状況を確認することもできます。

- 表示対象の日付範囲を変更するには、[日付取得] を使用します。

注意: レポートのダウンロードについては、「*468{/u}{/color} ページの「使用状況データレポートのダウンロード」*」を参照してください。

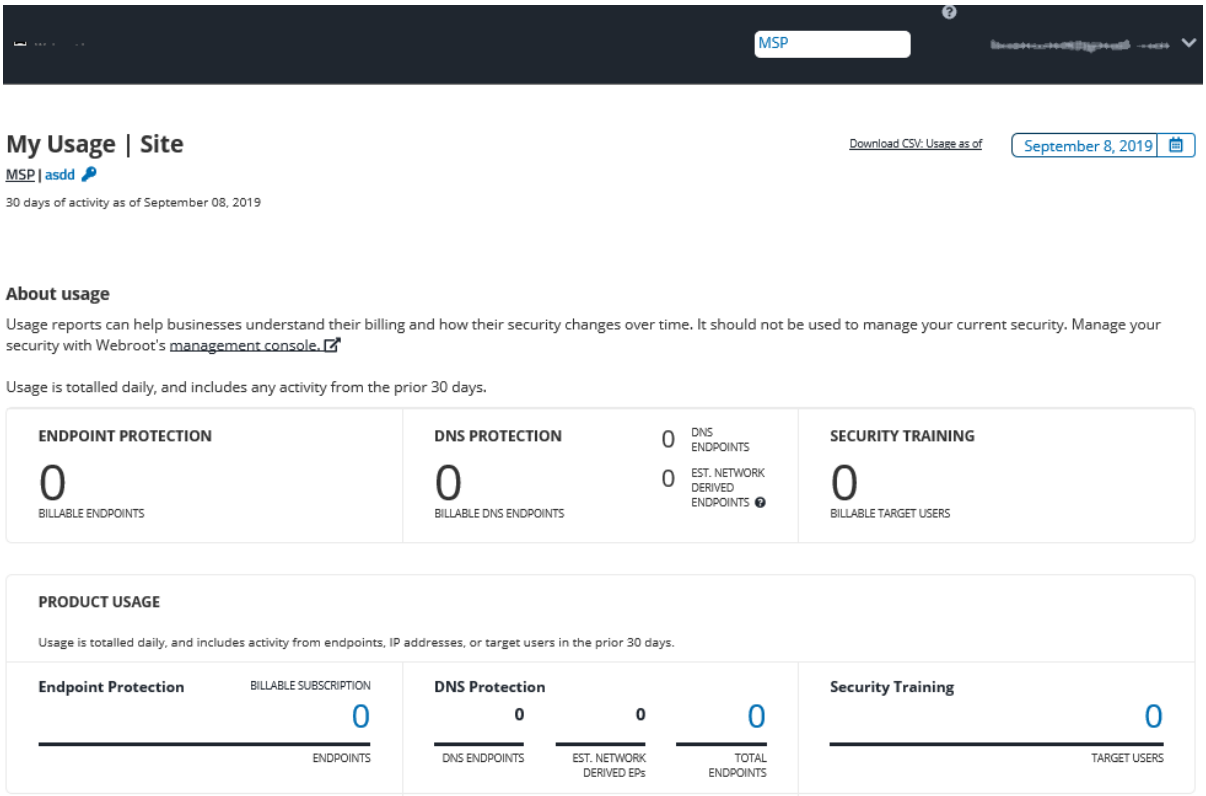
使用状況コンソールの下部に、サイト概要のスプレッドシートが表示されます。



このスプレッドシートには、以下のカラムが含まれています。

- **サイト** - サイト名が表示されます。
- **エンドポイント** — 請求可能なエンドポイント数が表示されます。この数は、このページの上部の [エンドポイント プロテクション] エリアに示されている数を反映しています。
- **DNS エンドポイント** — 請求可能な DNS プロテクション エンドポイント数が表示されます。この数は、このページの上部の [DNS プロテクション] エリアに示されている数を反映しています。
- **ターゲット ユーザー** — セキュリティ意識向上トレーニングの請求可能なターゲット ユーザー数が表示されます。この数は、このページの上部の [セキュリティ意識向上トレーニング] エリアに示されている数を反映しています。
- **サイトの使用状況** — そのサイトの使用状況データを表示するには、[**Site Usage**] (サイトの使用状況) ボ

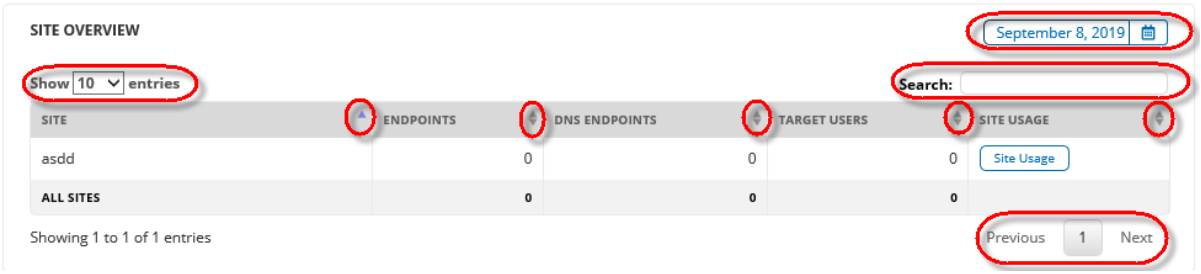
タンをクリックします。



必要に応じて、以下のいずれかを実行できます:

- 表示対象の日付範囲を変更するには、[日付取得] を使用します。
- 情報を並べ替えるには、各カラムで**上向き**または**下向き**の矢印をクリックします。
- 特定のサイトを検索するには、[検索] フィールドにサイト名を入力します。
- 表示するエントリ数を増やすには、表示エントリ数のドロップダウン メニューで数を調整します。
- さらに多くのエントリがある場合は、[**戻る**] または [**次へ**] の矢印をクリックして前または次のページを表示し

ます。


SITE OVERVIEW
September 8, 2019
Show 10 entries
Search:
SITE
ENDPOINTS
DNS ENDPOINTS
TARGET USERS
SITE USAGE
asdd
0
0
0
Site Usage
ALL SITES
0
0
0
Showing 1 to 1 of 1 entries
Previous
1
Next

使用状況データ レポートのダウンロード

使用状況データを確認した後、CSV ファイルをダウンロードするには、次の手順に従ってください。

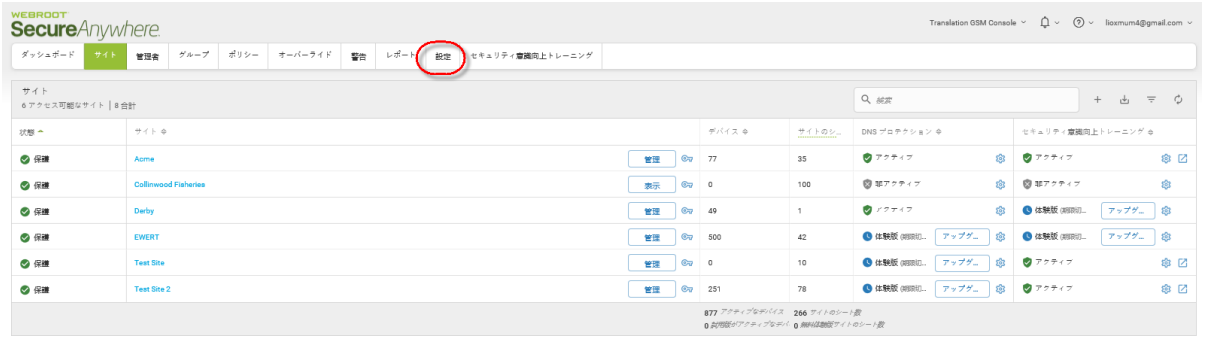
注意: 使用状況データの詳細については、「*460{/u}{/color} ページの「使用状況データへのアクセス」*」を参照してください。

使用状況データにアクセスするには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**設定**] タブをクリックします。



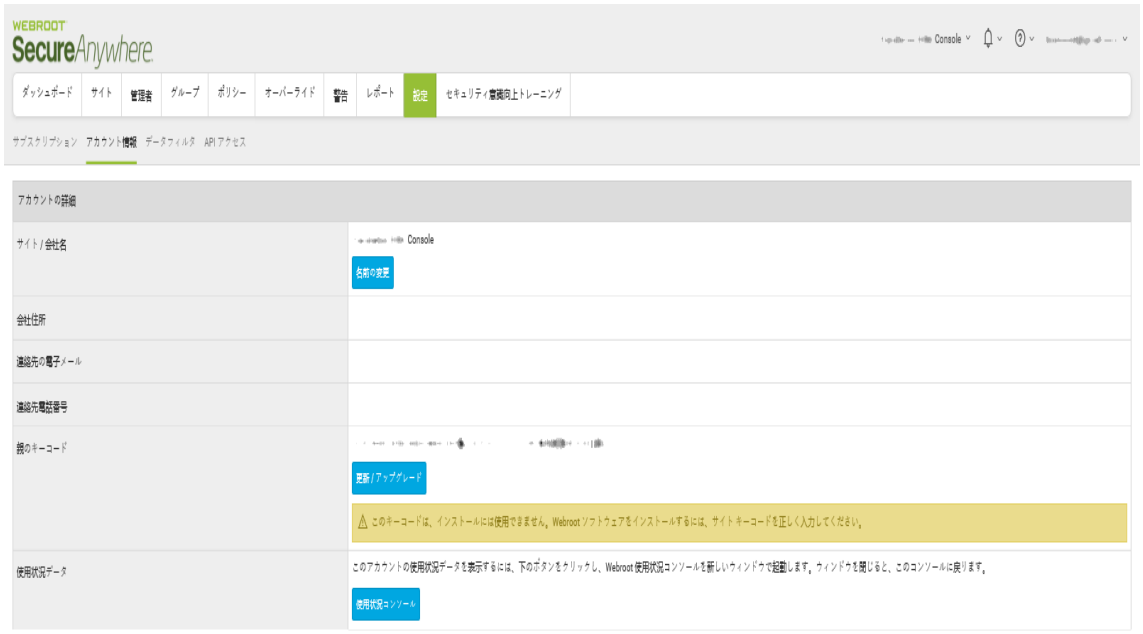
   [サブスクリプション] タブがアクティブな状態で [設定] タブが表示されます。


WEBROOT
SecureAnywhere
Translation GSM Console
liaxmum4@gmail.com
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
サブスクリプション
アカウント情報
データフィルタ
API アクセス
エンドポイント プロテクション
Webroot SecureAnywhere® Business エンドポイント プロテクションは、他のソリューションよりも多くのマルチベクトルによるメリットを提供し、電子メール、ウェブブラウジング、ファイル添付、ハイパーリンク、広告の表示、ソーシャルメディアのアプリ、そして USB ドライブなどのコネクテッドデバイスからの脅威に対応します。また、悪質なペイロードを配布する混合型の戦略を用いた、前例のない巧妙な脅威を特定します。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新
DNS プロテクション
DNS プロテクションは、インターネットアクセスをより詳細にコントロールできるよう設計されたドメインフィルタリングサービスです。受賞歴のあるウェブルートのエンドポイント プロテクションをネットワークに拡大し、ブラウザ以外での悪質な行為からお客様を保護。また、ネットワーク全体でカテゴリーごとにインターネット利用を制限することができます。企業、ゲスト Wifi、ローミングユーザー、グループに対する設定が可能です。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新
セキュリティ意識向上トレーニング
Webroot® セキュリティ意識向上トレーニングは、包括的なセキュリティトレーニングとコンプライアンスに関するコースに Phishing Simulator を取り入れたもので、このコンソールと高度に自動化された学習管理システム内に統合されています。専門家でなくても質の高いセキュリティ意識向上キャンペーンを容易に展開および実施できるとともに、感染やサポートへの問い合わせ、ユーザーのエラー修正に費やす時間を減らすことができます。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新

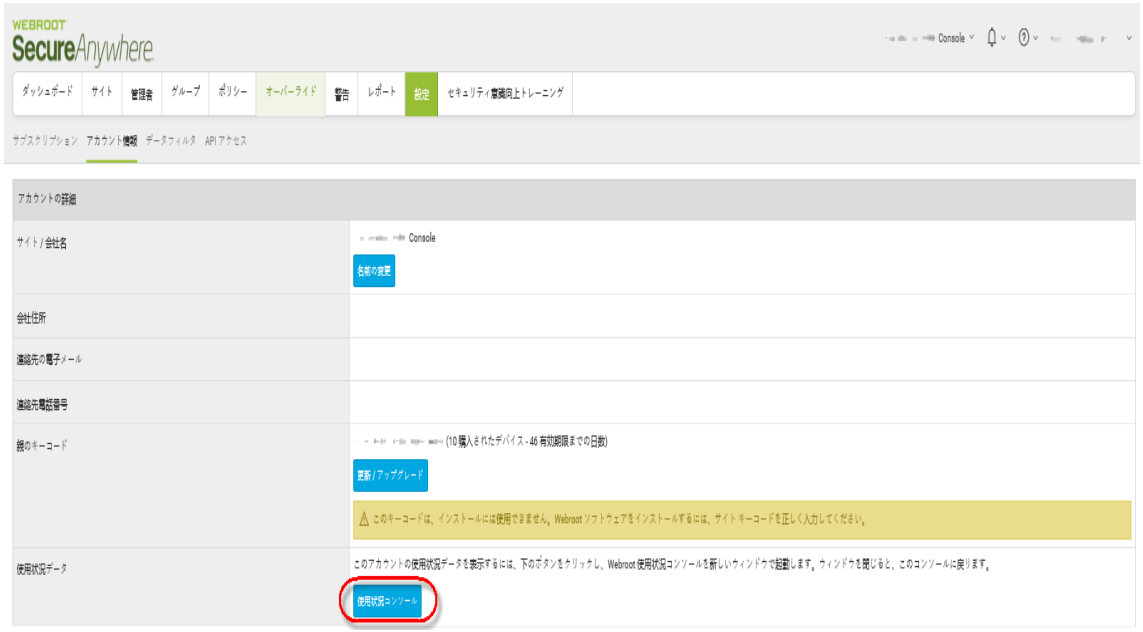
3. [アカウント情報] タブをクリックします。

[アカウント情報] タブが開いて次の情報が表示されます:

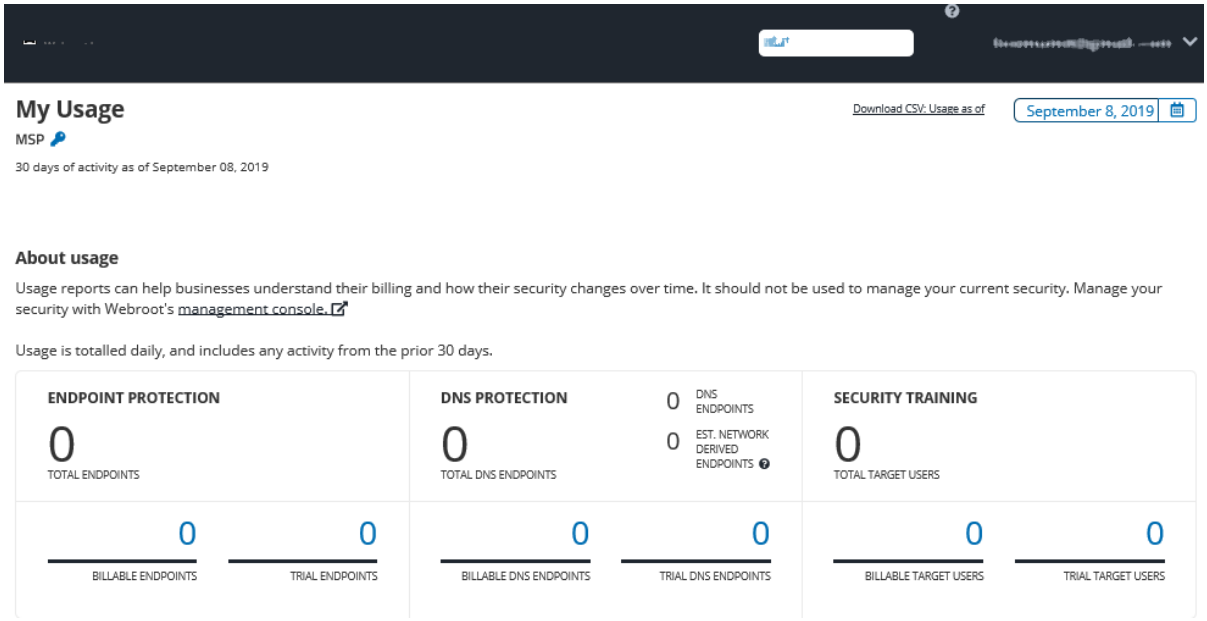
- サイト / 会社名
- 会社住所
- 連絡先の電子メール
- 連絡先電話番号
- 親キーコードは更新またはアップグレードできます。 更新 / アップグレードボタンをクリックすると、チャネル パートナーとウェブルートのアカウント マネージャーの情報が表示されます。どちらも更新やアップグレード時のサポートを行っています。



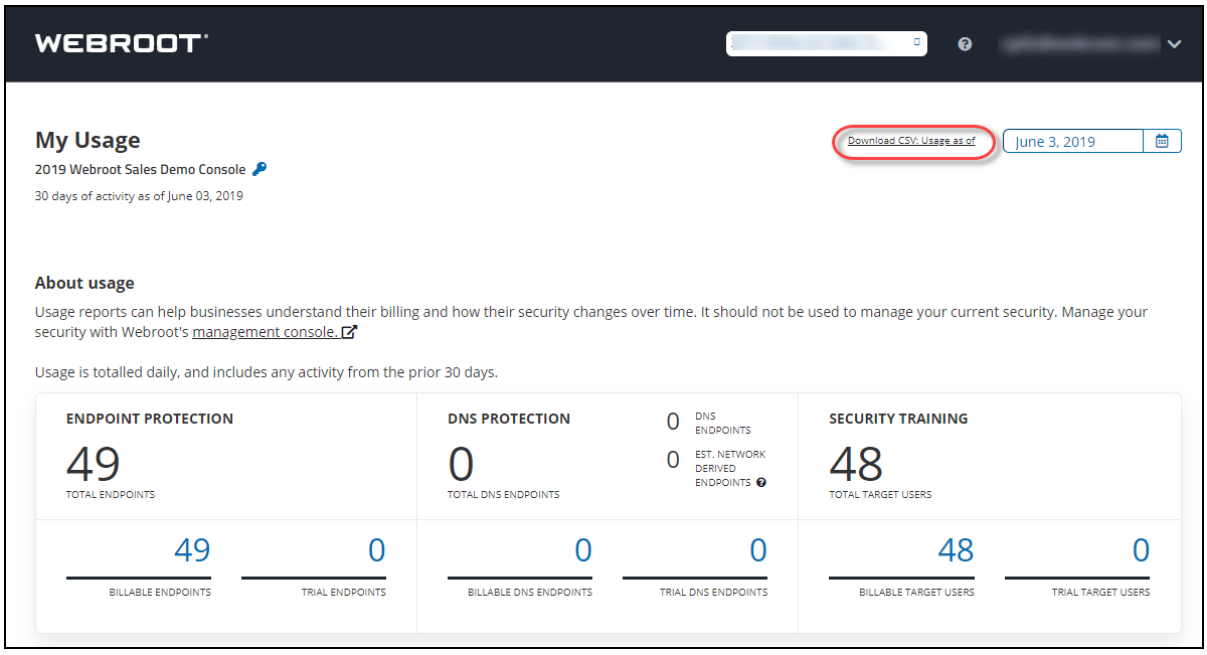
4. [**使用状況コンソール**] ボタンをクリックします。



使用状況コンソールが表示されます。



5. [日付取得] で日付範囲を選択した後、[**Download CSV Usage as of**] (使用状況の CSV ファイルをダウンロード) リンクをクリックします。



ウェブルートにより CSV ファイルがお使いのコンピュータにダウンロードされます。

6. ダウンロードをクリックすると、ファイルを開いて情報を確認できます。このスプレッドシートには、以下の情報が含まれています。
   - GSM キー
   - 使用日
   - サイト キー
   - サイト名
   - サイトの状態
   - SAEP エンドポイントの総数
   - DNSP 有効
   - DNSP ライセンスの種類
   - 実際の DNSP デバイス合計
   - DNSP EST ネットワーク由来のエンドポイント
   - DNSP エージェント数合計
   - WSAT 有効
   - WSAT ライセンスの種類
   - WSAT ユーザー数合計

GSM レベルのデータフィルタの設定

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、配備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。

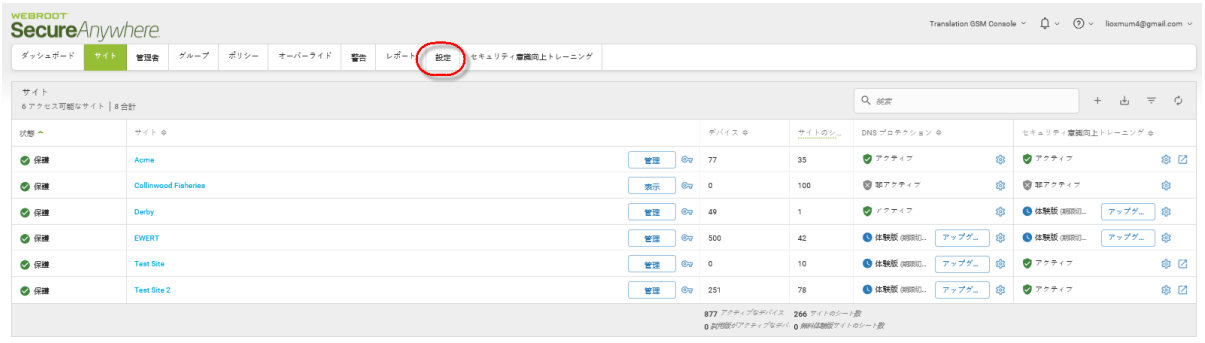
管理コンソールのマスター設定は、その管理コンソールのすべてのサイトで継承することも、サイトごとに設定することもできます。ダッシュボードとスケジュールされたレポートには、選択した期間中に検出されたエンドポイントのみが表示されます。

管理コンソール レベルのデータ フィルタを設定するには:

1. 管理コンソールにログインします。

   [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が表示されます。

2. [**設定**] タブをクリックします。



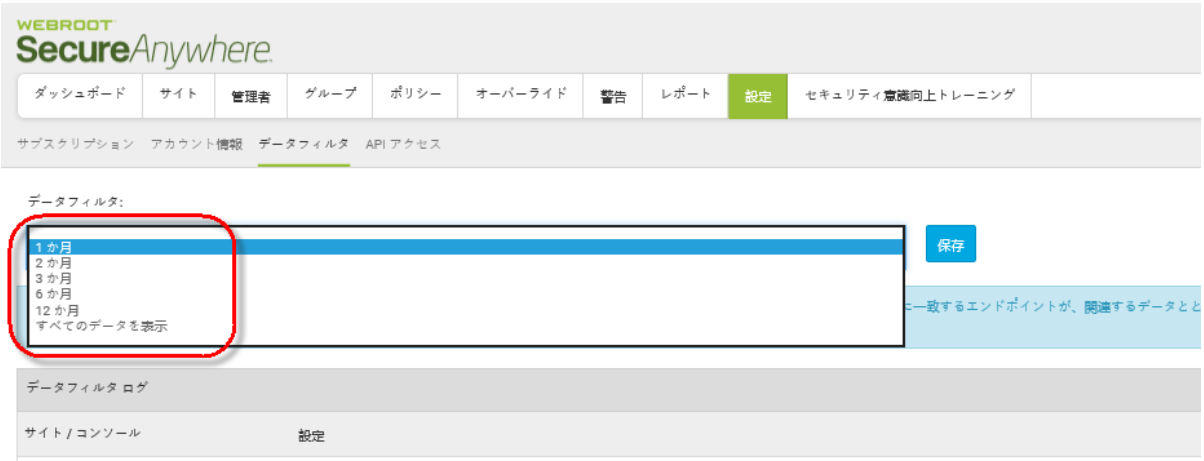
   [サブスクリプション] タブがアクティブな状態で [設定] タブが表示されます。


WEBROOT
SecureAnywhere
Translation GBM Console
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
サブスクリプション
アカウント情報
データフィルタ
API アクセス
エンドポイント プロテクション
Webroot SecureAnywhere® Business エンドポイント プロテクションは、他のソリューションよりも多くのマルチベクトルによるメリットを提供し、電子メール、ウェブブラウジング、ファイル添付、ハイパーリンク、広告の表示、ソーシャルメディアのアプリ、そして USB ドライブなどのコネクテッドデバイスからの脅威に対応します。また、悪質なペイロードを配布する混合型の脅威を用いた、前例のない巧妙な脅威を特定します。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード/更新
DNS プロテクション
DNS プロテクションは、インターネットアクセスをより詳細にコントロールできるよう設計されたドメインフィルタリングサービスです。悪質度のあるウェブルートのエンドポイント プロテクションをネットワークに拡大し、ブラウザ以外での悪質な行為からお客様を保護。また、ネットワーク全体でカテゴリーごとにインターネット利用を制限することができます。企業、ゲスト Wifi、ローミングユーザー、グループに対する設定が可能です。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード/更新
セキュリティ意識向上トレーニング
Webroot® セキュリティ意識向上トレーニングは、包括的なセキュリティトレーニングとコンプライアンスに関するコースに Phishing Simulator を取り入れたもので、このコンソールと高度に自動化された学習管理システム内に統合されています。専門家でなくても質の高いセキュリティ意識向上キャンペーンを容易に展開および実施できるとともに、感染のサポートへの問い合わせ、ユーザーのエラー修正に費やす時間を減らすことができます。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード/更新

3. [**データ フィルタ**] タブをクリックします。

[データ フィルタ] タブが表 示されます。

4. [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:
   - **すべてのデータを表示 (デフォルト設定)**
   - **1 か月**
   - **2 か月**
   - **3 か月**
   - **6 か月**
   - **12 か月**



注意: **データ フィルタ**の設定を使用する際、データは削除されるのではなく、表示されているデータセットからオプションに基づいて非表示になっているだけです。異なる期間を選択、またはすべてのデータが表示されるよう選択すると、選択内容に関連したすべてのエンドポイント情報が常に表示されます。

5. 設定が完了したら [**保存**] ボタンをクリックします。

変更が保存されたことを示すメッセージが表示されます。

6. [**OK**] ボタンをクリックします。

注意: 次回から [保存が完了しました] のメッセージが表示されないようにするには、[**これを今後表示しない**] チェックボックスを選択します。

[設定] パネルの下の部分に [データ フィルタ] ログが表示されます。このログには、データフィルタの設定に加えられたすべての変更が記録されます。ログには以下の詳細が含まれます:

- **サイト / コンソール** — 変更が適用されたサイトまたは親設定が変更された管理コンソール。
- **設定** — 選択されたオプション。
- **ユーザー** — 変更を行ったユーザーの名前。
- **日付** — 変更した日時。

データフィルタ ログ

サイト / コンソール	設定	ユーザー	日付
GSM コンソール	3 か月	lioxmum4@gmail.com	9月 10日 2019, 05:59
GSM コンソール	すべてのデータを表示	jthoming@webroot.com	7月 23日 2019, 19:22
GSM コンソール	1 か月	lioxmum1@gmail.com	3月 13日 2019, 14:03
GSM コンソール	2 か月	lioxmum1@gmail.com	3月 13日 2019, 14:02
GSM コンソール	1 か月	lioxmum1@gmail.com	3月 13日 2019, 14:02

API クライアント認証情報の作成

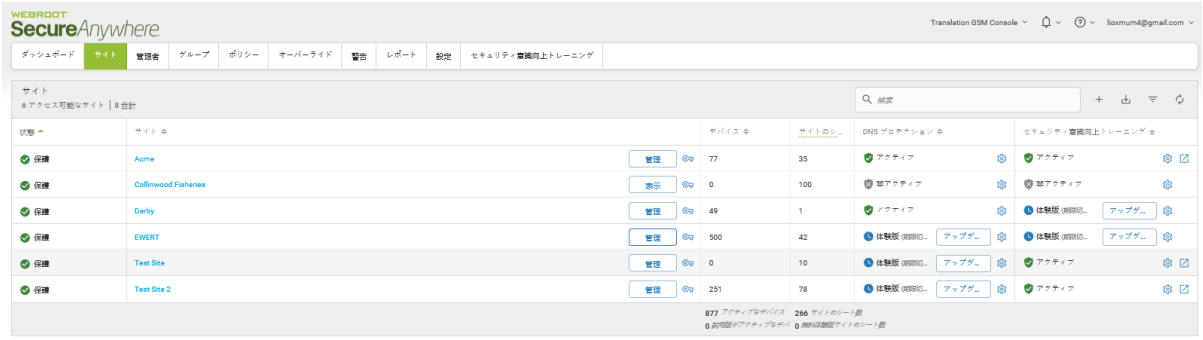
API クライアント認証情報を作成すると、SecureAnywhere とご利用中の管理型システムとの間で安全な認証接続方式を用いて、Unity API システムに接続できるようになります。それによって請求、レポート、配備およびその他のプロセスを自動化することができます。

API の詳細については、「ウェブルート Unity API」を参照してください。

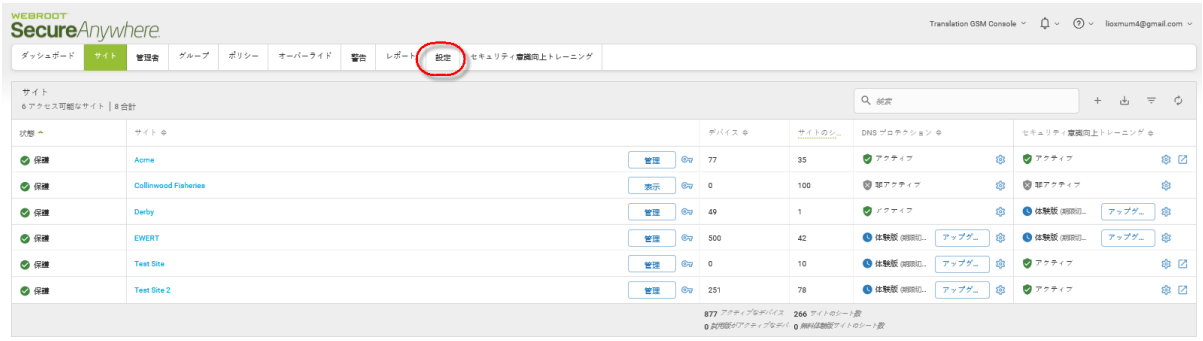
API クライアント認証情報を作成するには:

1. 管理コンソールにログインします。

   [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が表示されます。



2. [**設定**] タブをクリックします。



   [サブスクリプション] タブがアクティブな状態で [設定] タブが表示されます。


WEBROOT
SecureAnywhere
Translation GSM Console
liaxmum4@gmail.com
ダッシュボード
サイト
管理者
グループ
ポリシー
オーバーライド
警告
レポート
設定
セキュリティ意識向上トレーニング
サブスクリプション
アカウント情報
データフィルタ
API アクセス
エンドポイント プロテクション
Webroot SecureAnywhere® Business エンドポイント プロテクションは、他のソリューションよりも多くのマルチベクトルによるメリットを提供し、電子メール、ウェブブラウジング、ファイル添付、ハイパーリンク、広告の表示、ソーシャルメディアのアプリ、そして USB ドライブなどのコネクテッドデバイスからの脅威に対応します。また、悪質なペイロードを配布する混合型の戦略を用いた、前例のない巧妙な脅威を特定します。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新
DNS プロテクション
DNS プロテクションは、インターネットアクセスをより詳細にコントロールできるよう設計されたドメインフィルタリングサービスです。受賞歴のあるウェブルートのエンドポイント プロテクションをネットワークに拡大し、ブラウザ以外での悪質な行為からお客様を保護。また、ネットワーク全体でカテゴリーごとにインターネット利用を制限することができます。企業、ゲスト Wifi、ローミングユーザー、グループに対する設定が可能です。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新
セキュリティ意識向上トレーニング
Webroot® セキュリティ意識向上トレーニングは、包括的なセキュリティトレーニングとコンプライアンスに関するコースに Phishing Simulator を取り入れたもので、このコンソールと高度に自動化された学習管理システム内に統合されています。専門家でなくても質の高いセキュリティ意識向上キャンペーンを容易に展開および実施できるとともに、感染やサポートへの問い合わせ、ユーザーのエラー修正に費やす時間を減らすことができます。
詳細
サブスクリプション アクティブ
(47 有効期限までの日数)
アップグレード / 更新

3. [**API アクセス**] タブをクリックします。

[API アクセス] タブが表示されます。

4. [**新規**] ボタンをクリックします。

[新しいクライアント認証情報を作成する] ウィンドウが表示されます。

5. [名前] フィールドに認証情報の名前を入力します。
6. [説明] フィールドに認証情報の簡単な説明を入力します。
7. [**Webroot SecureAnywhere ビジネス ソリューション契約書の内容を表示するにはこちらをクリックしてください**] リンクをクリックして、Webroot Unity SDK および Unity API 契約書のサービス利用条件を確認します。

8. 設定が完了したら、[**作成**] ボタンをクリックします。

[クライアント認証情報の記録] ウィンドウが表示されます。このウィンドウでは、入力した認証情報の名前と説明がクライアント ID ([クライアント ID] カラム内) と合わせて表示されます。

重要な点は、同じウィンドウにクライアント シークレットが表示されることです。これはコンソールでは表示されません。必ずこのクライアント シークレットをメモし、そのうえで [**クライアント シークレットをメモしました**] ボタンをクリックしてください。

9. 必要に応じて、クライアントの行項目をハイライトすれば次のことができます:note
   - クライアント認証情報の編集 - [編集] ボタンをクリックしてフィールドの情報を**更新し**ます。設定が完了したら、[変更を保存] ボタンをクリックします。
   - クライアント認証情報の削除 - [削除] ボタンをクリックします。もう一度 [削除] ボタンをクリックして削除を確定します。
   - 新しいクライアント シークレットの作成 - [シークレットを更新する] ボタン**をクリックし、新しいクラ**イアント シークレットをメモします。続いて [クライアント シークレットをメモしました] ボタンをクリックしてください。
   - クライアントの一時停止 - [一時停止] ボタンをクリックします。もう一度 [一時停止] ボタンをクリックして一時停止を確定します。

- 関連ドキュメントへのアクセス - [Unity API] ボタンをクリックします。
- 関連ドキュメントへのアクセス - [開発者] ボタンをクリックします。

第 14 章: ビジネス コンソールの操作

ビジネス コンソールについての詳細は、次のトピックを参照してください。

ビジネス コンソールの概要

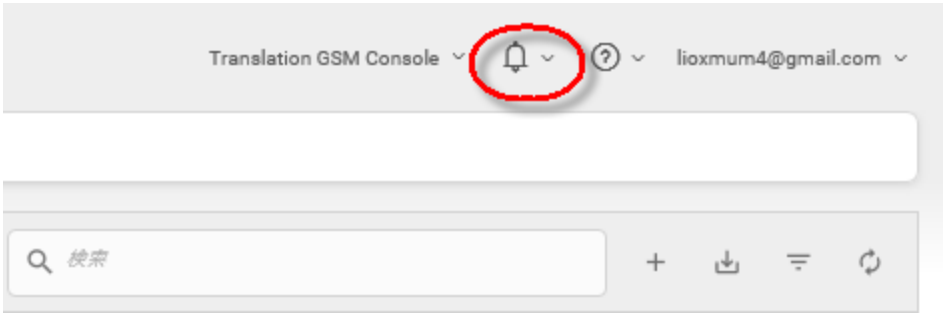
ビジネス コンソールを使用すると、簡単にデバイスを管理できます。次のタブと機能には、ビジネス コンソールからアクセスできます。

- **ダッシュボード** - エンドポイントを視覚的に解釈するためのさまざまなグラフが表示されます。ここから、エンドポイントの状態に関する情報を含むチャートを確認できます。詳細については、「[ビジネス ダッシュボード] タブ」を参照してください。さらに、DNS プロテクションまたはセキュリティ意識向上トレーニングのいずれかの無料体験版に登録できます。
- **管理者** - 管理者のリストが表示されます。ここでは、各管理者のサイトごとの権限レベルに関する情報にアクセスすることができます。詳細については、「管理者の操作」セクションを参照してください。
- **グループ** - グループの追加、編集、削除、操作が可能です。詳細については、「グループの操作」セクションを参照してください。
- **ポリシー** - ポリシーの作成、コピー、編集、名前変更が可能です。詳細については、「ポリシーの操作」セクションを参照してください。
- **オーバーライド** - オーバーライドの作成、カスタマイズ、インポートが可能です。詳細については、「オーバーライドの操作」セクションを参照してください。
- **警告** - グローバル レベルで警告を作成できます。詳細については、「警告の操作」セクションを参照してください。
- **レポート** - 製品の状態やパフォーマンスに関するレポートを実行できます。詳細については、「レポートの操作」セクションを参照してください。
- **設定** - アカウント情報と詳細設定を表示し、編集できます。詳細については、「*499{/u}{/color} ページの「企業情報の表示と編集」*」と「*501{/u}{/color} ページの「詳細設定の表示および編集」*」を参照してください。
- **DNS プロテクション** - セキュリティ意識向上トレーニングに関する情報を表示し、無料体験版に登録できます。詳細については、「*DNS Protection Trial*」を参照してください。
- **セキュリティ意識向上** - セキュリティ意識向上トレーニングに関する情報を表示し、無料体験版に登録できます。詳細については、「*Security Awareness Training Trial*」を参照してください。

- 追加情報については、右上のヘルプ (?) アイコンから、**下向き矢印**をクリックして、次のいずれかにアクセスします。
  - ヘルプ ドキュメント - 多くの場合、操作中のパネルまたはウィンドウに関連してヘルプ情報が表示されます。

- DNS ヘルプドキュメント - ビジネスドキュメント ポータルを表示します。このポータルから DNS プロテクション ガイドにアクセスできます。
- ウェブルート教育ビデオ - ウェブルート ビデオのプレイリストを表示します。
- サービスの状態 - コンソールの状態ページを表示します。このページで、製品とシステムの状態を確認できます。
- スポットライト ツアー - スポットライト ツアーを表示します。これは、コンソール全体の簡単なツアーです。詳細については、「*9{/u}{/color} ページの「スポットライト ツアーについて」*」を参照してください。
- サポート - リンクをクリックしてヘルプ チケットを入力します。詳細については、「テクニカル サポートを受けるには」を参照してください。

- 警告または通知を確認するには、右上の警告ベル アイコンから、**下向き矢印**をクリックします。



ビジネス コンソールの設 定

ビジネス コンソールを選 択した後 、企 業 の情 報を入 力する必 要 があります。

ビジネス コンソールを設 定するには:

1. コンソールにログインします。
2. [ビジネス] で、[**選 択**] ボタンをクリックします。

ビジネス情 報 ページが表 示されます。

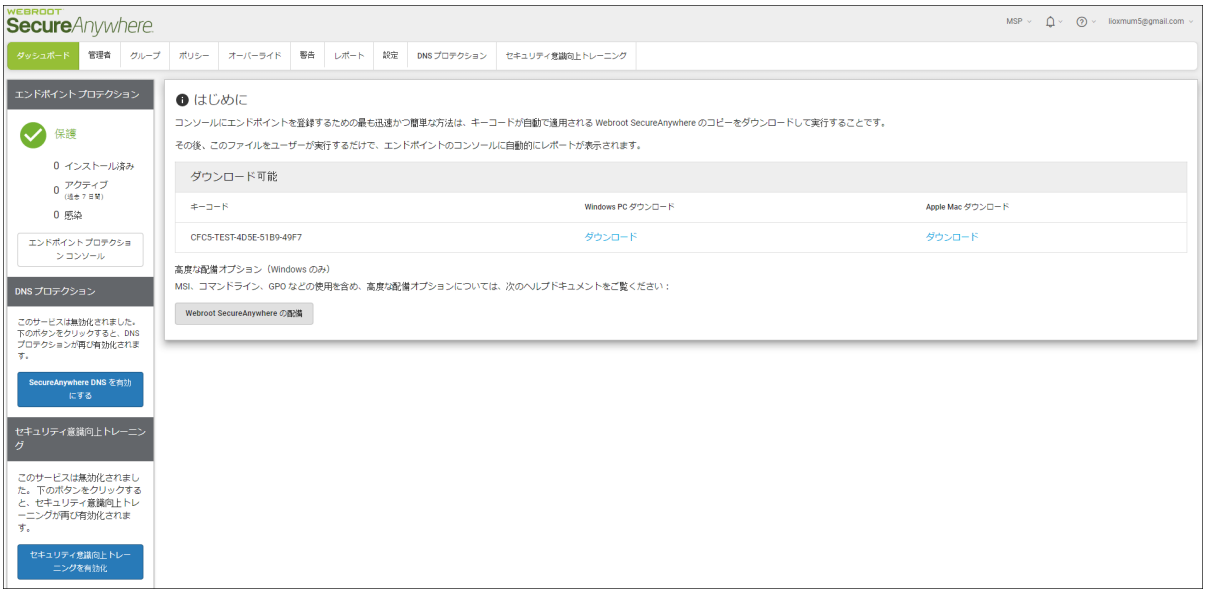
3. [サイト / 会社名] フィールドにサイトまたは会社の名前を入力します。
4. [デバイスの数] フィールドに管理するデバイスの数を入力します。
5. [会社の業種] フィールドのドロップダウンメニューから、実際の業種のタイプに最も近いものを選択します。
6. [会社の規模] フィールドのドロップダウンメニューから、実際の会社の従業員数に最も近いものを選択してください。

7. 設定が完了したら、[**選択**] ボタンをクリックします。

会社のダッシュボードが表示されます。このダッシュボードで次を実行できます。

- ビジネス スポットライト ツアーを表示する。ヘルプ (?) ドロップダウン メニューから、いつでも表示できます。詳細については、「*507{/u}{/color} ページの「ビジネス コンソールのスポットライト ツアーについて」*」を参照してください。
- エンドポイント プロテクションに進む。
- セキュリティ意識向上トレーニングの無料体験版を開始する - [**無料体験版を開始**] ボタンをクリックして [セキュリティ意識向上] タブに移動します。ここで、セキュリティ意識向上トレーニングの詳細を確認したり、登録したりできます。詳細については、「セキュリティ意識向上トレーニング管理者ガイド」を参照してください。
- DNS プロテクションの無料体験版を開始する - [**無料体験版を開始**] ボタンをクリックして [DNS] タブに移動します。ここで、DNS プロテクションの詳細を確認したり、登録したりできます。詳細については、「DNS プロテクション管理者ガイド」を参照してください。

- ウェブルート プロテクションをダウンロードして使用を開始します。



8. 必要に応じて、企業の情報を編集できます。詳細については、「*499{/u}{/color} ページの「企業情報の表示と編集」*」を参照してください。

[ビジネス ダッシュボード] タブ

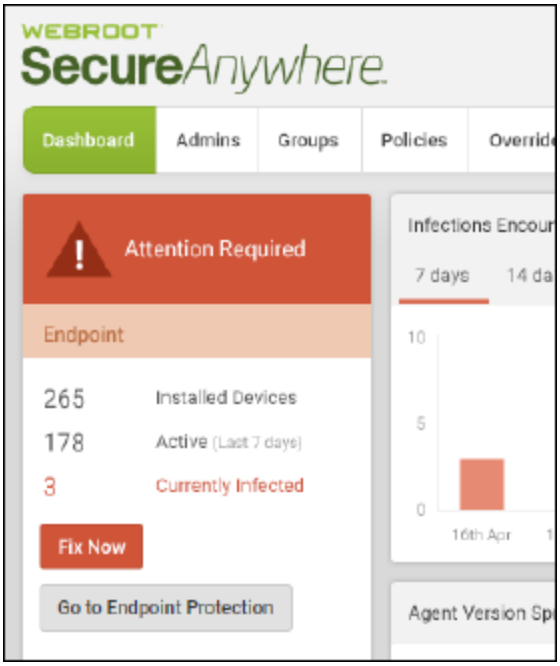
コンソールを有効にし、デバイスがレポート作成を開始すると、左パネルの上部で次に関する簡単な概要が分かります。

- エンドポイント プロテクション
- DNS プロテクション
- セキュリティ意識向上トレーニング
- ダッシュボードのチャート

エンドポイント プロテクション

このエリアでは、次を確認できます。

- インストールされたデバイスの数。
- 有効なデバイスの数。
- 感染しているデバイスの数。



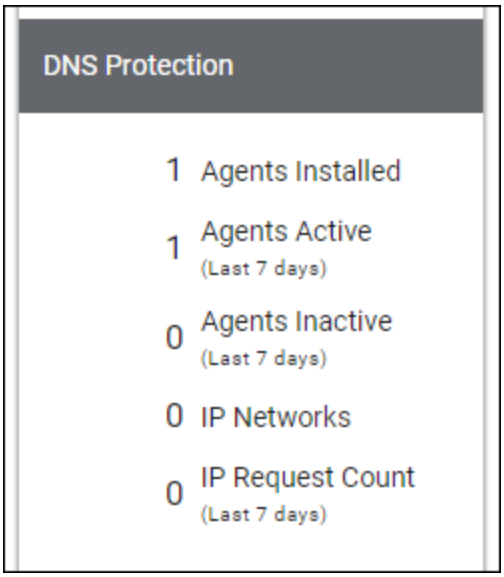
問題がある場合、以下のいずれかを実行できます。

- [**感染デバイスを表示**] 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 コンソール**] ボタンをクリックします。詳細については、「エンドポイント プロテクション管理者ガイド」を参照してください。

DNS プロテクション

このエリアでは、サービスが有効であるときに、次の情報を確認できます。

- インストールされたデバイスの数。
- 有効なデバイスの数
- 過去 7 日間に確認されていないデバイスの数。
- 過去 7 日間に作成されたリクエストの数。
- さらに、サブスクリプションの残存日数を確認できます。



DNS プロテクションの詳細については、「*DNS Protection Trial*」および「DNS プロテクション管理者ガイド」を参照してください。

セキュリティ意識向上トレーニング

このエリアでは、サービスが有効であるときに、次の情報を確認できます。

- 現在実行中のアクティブ キャンペーンの合計数。
- 現在実行中のフィッシング キャンペーンの合計数。
- 現在実行中のトレーニング キャンペーンの合計数。
- 現在実行中のハイブリッド キャンペーンの合計数。

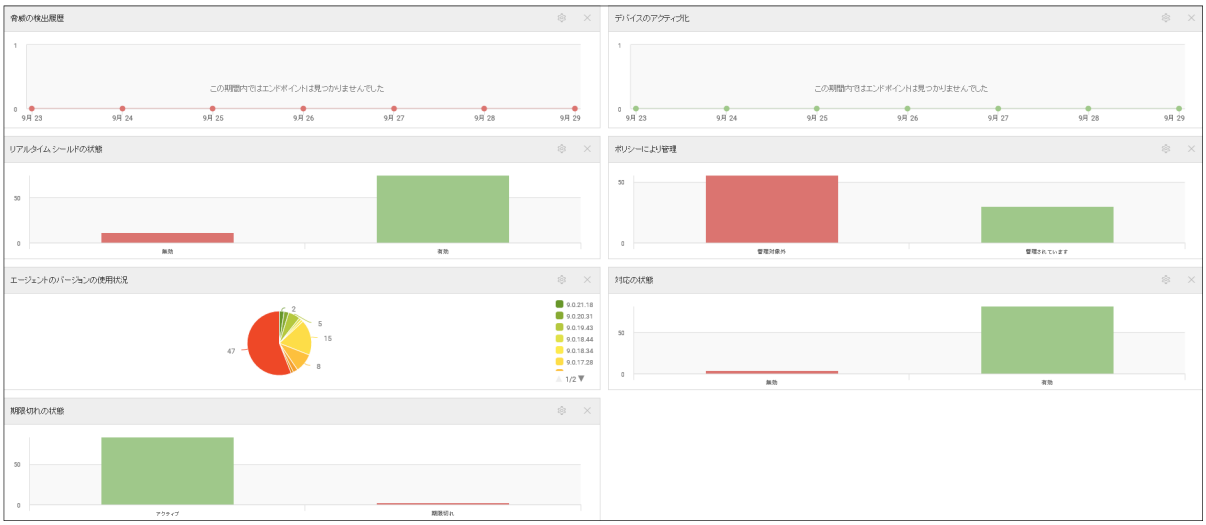
必要に応じて、[セキュリティ意識向上トレーニングに移動] ボタンをクリックして、セキュリティ意識向上トレーニング コンソールにログインできます。 詳細については、「セキュリティ意識向上トレーニング トライアル」および「セキュリティ意識向上トレーニング管理者ガイド」を参照してください。

ダッシュボードのチャート

[ビジネス ダッシュボード] タブには次の標準レポートが表示され、エンドポイントに関する情報を簡単に確認できます。

- 検出された感染
- インストール
- エージェントのバージョンの使用状況
- 最近確認していないエンドポイント
- 最近検出された悪質なファイル

- 最もブロックされた Web カテゴリー



必要に応じて、次のいずれかを実行できます。

- *42{/u}{/color}* ページの「*ダッシュボードのチャートの詳細表示*」
- *36{/u}{/color}* ページの「*ダッシュボードのチャートの編集*」

注意: [ビジネス ダッシュボード] タブのレイアウトは他の標準 [ダッシュボード] タブのものと異なりますが、機能はほぼ同じです。

企業情報の表示と編集

[エンドポイント] タブで企業情報を表示して編集できます。これは、サイトを作成したときに入力した情報です。

企業情報を表示して編集するには:

1. 管理コンソールにログインします。
2. [**設定**] タブをクリックします。

[エンドポイント] タブがアクティブな状態で [設定] タブが表示されます。

3. 必要に応じて、次のフィールドを編集できます。
   - 会社名
   - 会社の規模
   - 会社の業種
   - コメント。このフィールドはオプションです。
   - サイトのシート数
   - デフォルトのエンドポイント ポリシー
   - レポート配信先リスト

> **注意:** [キーコード] フィールド内の情報は編集できません。

加えた変更は自動的に保存されます。

詳細設定の表示および編集

[詳細設定] タブでは、次を表示して編集できます。

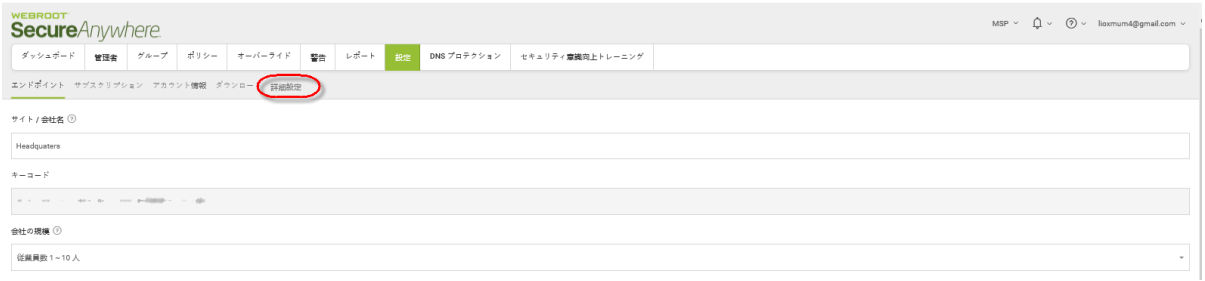
- **データ フィルタ** - 一定の期間中に確認されていないエンドポイントのデータを表示するかどうかを決定します。
- **コンソールの変換** - コンソールを、複数のサイトを管理するコンソールに変換します。詳細については、「*4 {/u}{/color} ページの「マネージド サービス プロバイダー コンソールについて」*」を参照してください。

企業情報を表示して編集するには:

1. 管理コンソールにログインします。
2. [**設定**] タブをクリックします。

[エンドポイント] タブがアクティブな状態で [設定] タブが表示されます。

3. [**詳細設定**] タブをクリックします。



[詳細設定] タブが表示されます。

4. 確認されていないエンドポイントのデータを非表示にするには、[**編集**] ボタンをクリックします。この情報は毎日更新されます。

5. コンソールを、複数のサイトまたはマネージド サービス プロバイダーに変更するには、[**変換**] ボタンをクリックします。

6. [コンソールを変換] ウィンドウが表示されたら、次を実行します。
   - コンソールを変換するときに起きる事柄に関する情報を確認します。
   - [**確認**] チェックボックスを選択して、情報をよく読み、理解したことを示します。

- [**コンソールを変 換**] ボタンをクリックします。

注 意: 一 度 、コンソールを複 数 サイトのコンソールに変 換したら、単 一 サイトのコンソールに戻すことはできません。

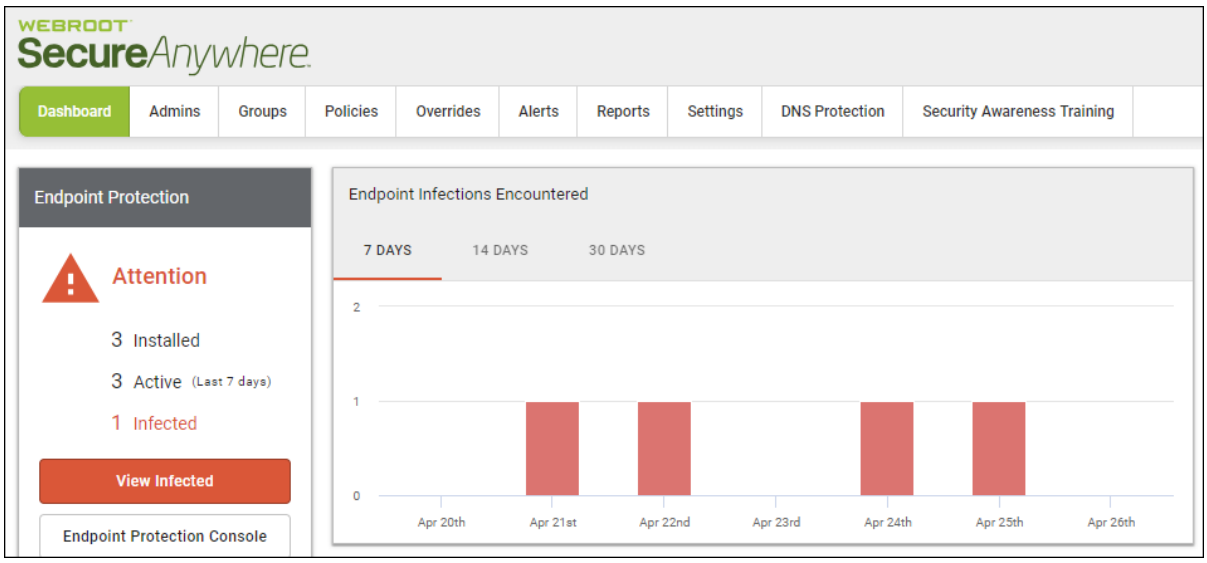
サイトのシート数の追加購入

サポートに連絡することなくサイトのシート数を追加購入するには、次の手順に従ってください。

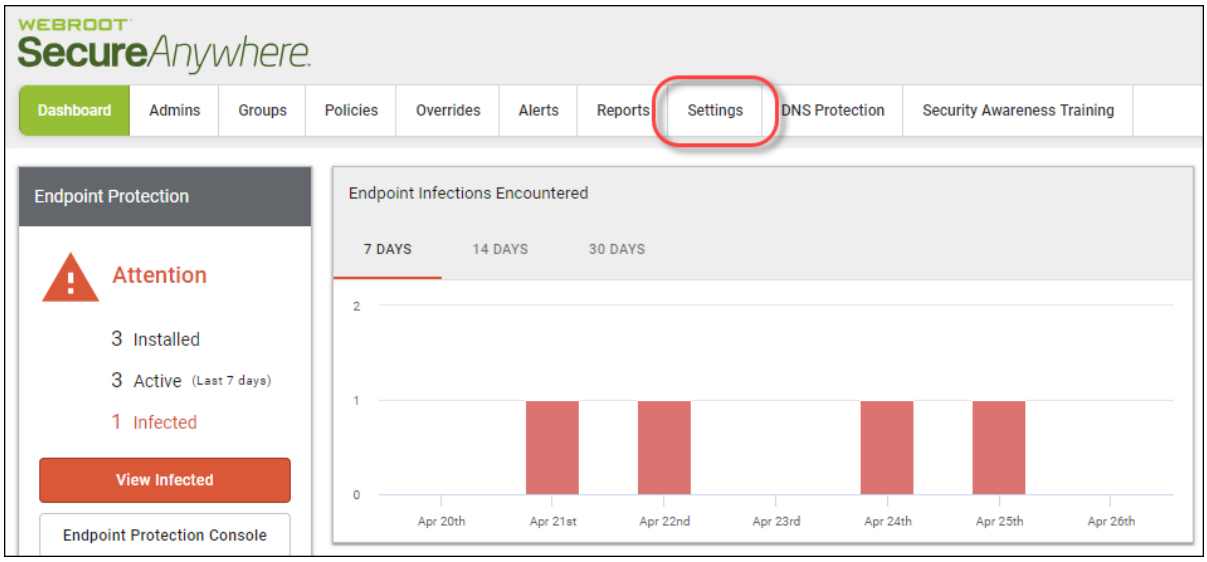
サイトのシート数を追加購入するには:

1. 管理コンソールにログインします。

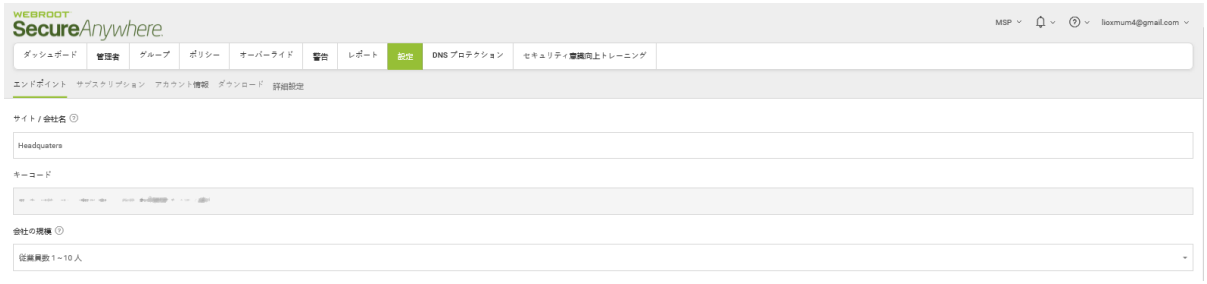
   管理コンソールが表示されます。



2. [**設定**] タブをクリックします。



[エンドポイント] タブがアクティブな状態で [設定] タブが表示されます。



3. [**サブスクリプション**] タブをクリックします。

[サブスクリプション] タブが表示されます。

4. [サブスクリプション] タブで、エンドポイント、DNS プロテクション、またはセキュリティ意識向上トレーニングのシート数を追加できます。

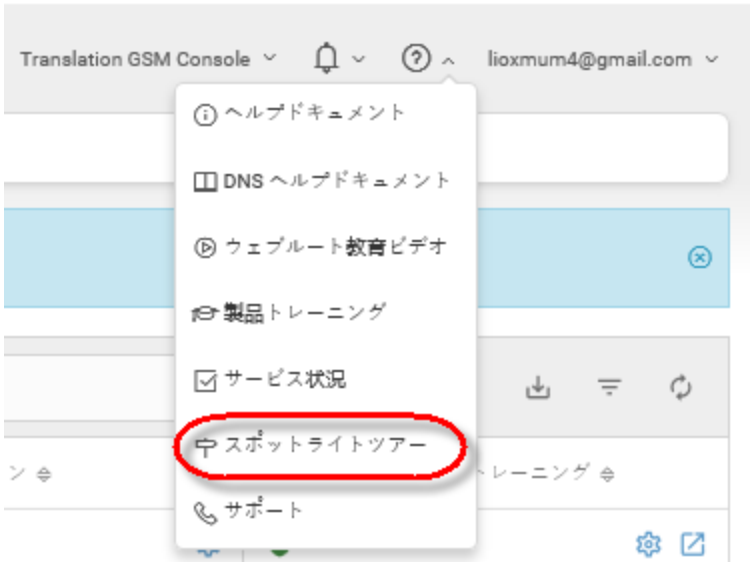
ビジネス コンソールのスポットライト ツアーについて

最初にアカウントを設定したときに、スポットライト ツアーが表示されます。ツアーには次に関する簡単な説明が含まれます。

- メイン メニューのタブ
- DNS プロテクションやセキュリティ意識向上トレーニングなどの追加セキュリティ レイヤー
- 必要に応じて、後程再度ツアーを表示できます。

スポットライト ツアーを見るには:

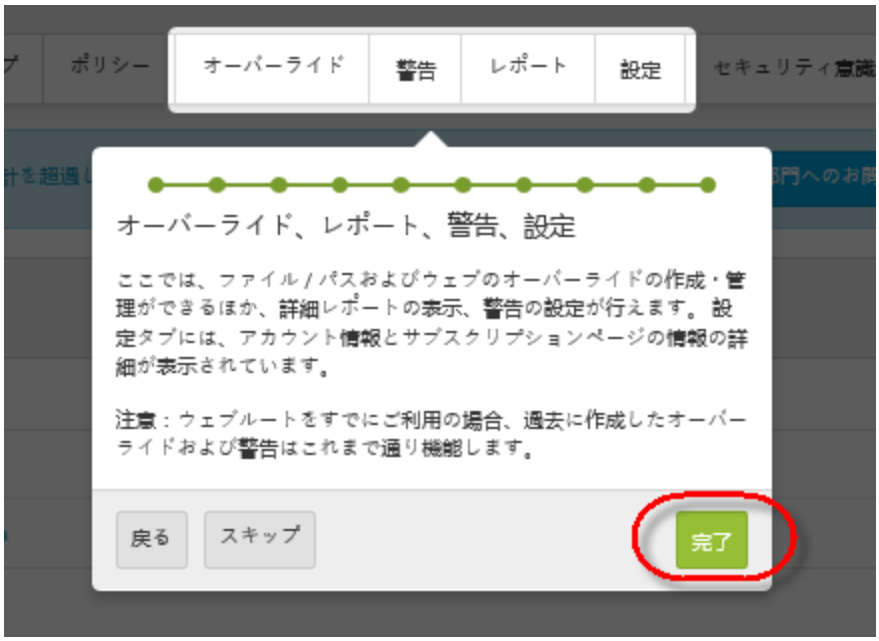
1. **ヘルプ (?)** ドロップダウン メニューから、[**スポットライト ツアー**] を選択します。



   ツアーの最初の画面が表示されます。

2. 必要に応じて、ツアーの視聴が完了するまで [**スキップ**] ボタンまたは [**次へ**] ボタンをクリックします。

3. ツアーの表示が完了したら、[**完了**] ボタンをクリックします。



必要に応じて、ヘルプ (?) ドロップダウン メニューから [スポットライト ツアー] を選択して、いつでもツアーを再度表示できます。

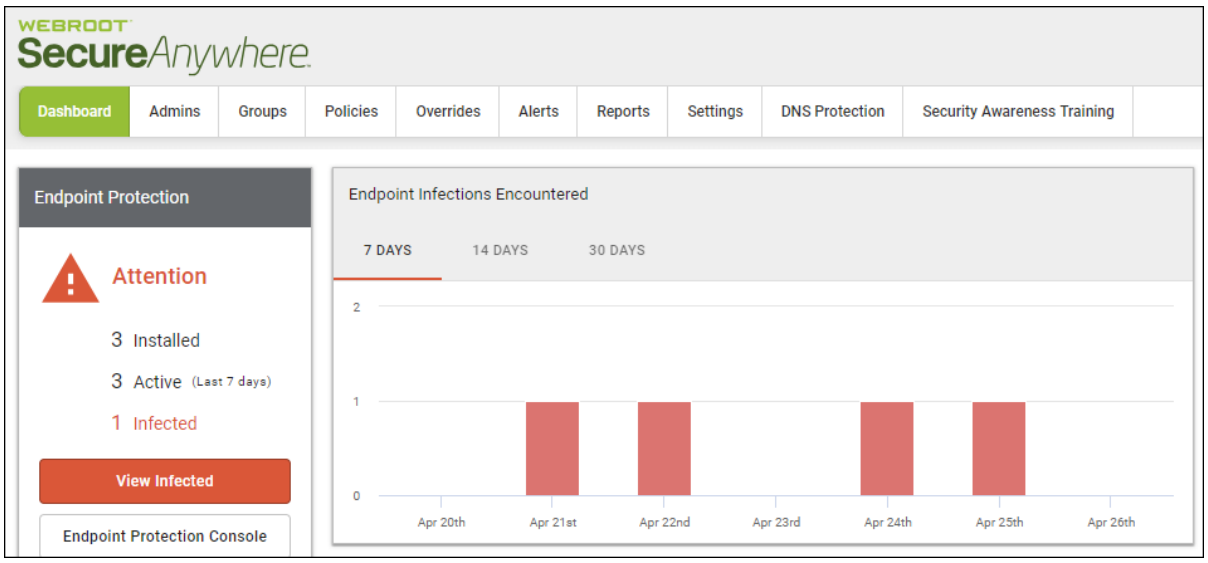
エンドポイント コンソールへの移動

管理コンソールからエンドポイント コンソールに移動するには、次の手順に従ってください。

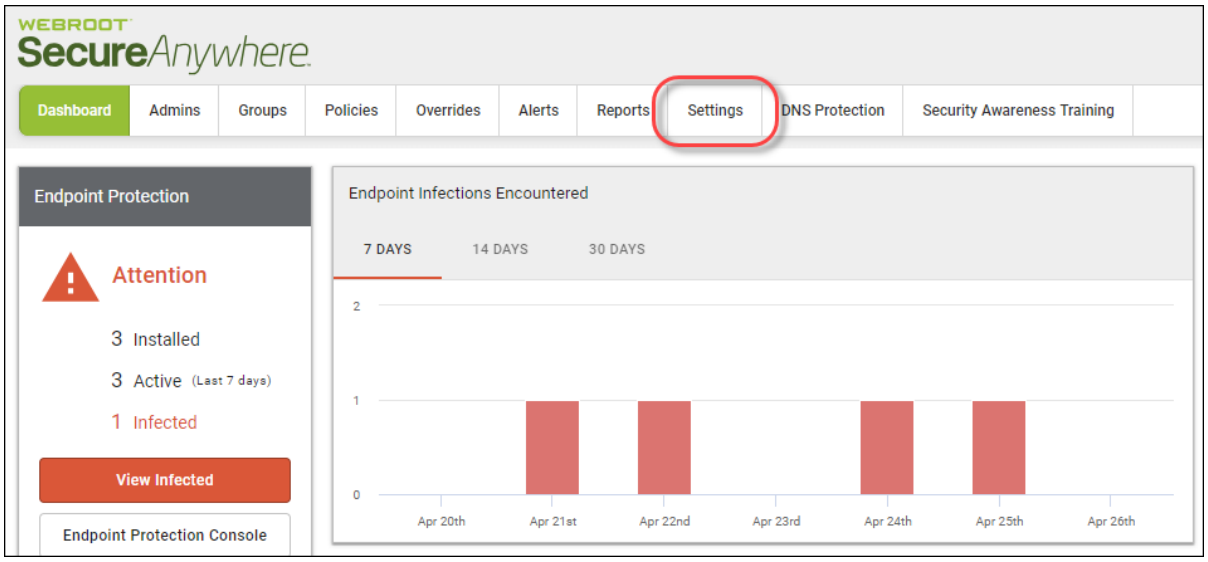
エンドポイント コンソールに移動するには:

1. 管理コンソールにログインします。

   管理コンソールが表示されます。



2. [**設定**] タブをクリックします。



[エンドポイント] タブがアクティブな状態で [設定] タブが表示されます。

3. 下 方 向 にスクロールして [**エンドポイント プロテクション コンソールに進む**] ボタンをクリックします。

第 15 章: グローバル サイト マネージャー サポート

サポートの詳細については、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選択します。

- ナレッジベースで回答を探す。
- オンライン文書で回答を探す。
- ヘルプ チケットを送信する。
- 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。

索引

こ

さ

し

す

ふ

へ

ほ

ま

も

れ

漢字