# Webroot法人向け製品 - 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

*管理者ガイド*

# お知らせ

Webroot法人向け製品の管理者ガイド 改正 2025年3月12日。

本書に記載されている情報は、以下の製品に関するものです:

- Webrootエンドポイントプロテクション
- Webroot DNSプロテクション
- Webroot Security Awareness Training

# コンテンツ

# 概要

この管理者ガイドでは、**Webrootエンドポイントプロテクション**の使用方法について詳しくご説明します。**Webroot DNSプロテクション**および**Webrootセキュリティ意識向上トレーニング**は**Webrootエンドポイントプロテクション**と連携しているため、これらの製品を使用している場合は、このガイドも参照してください。

**Webrootエンドポイントプロテクション**は小規模のビジネスを経営する個人管理者、および顧客のセキュリティを管理するマネージドサービスプロバイダー(MSP)向けの製品ですが、さまざまな場所にオフィスを持つ大規模な企業にも適したソリューションです。

- **Webrootエンドポイントプロテクション**は、企業やその顧客をウイルス、ランサムウェア、フィッシング、マルウェア、その他のサイバー攻撃から保護するために設計されています。**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**のいずれかを使用する前に、エンドポイントプロテクションをインストールし、設定する必要があります。
- **Webroot DNSプロテクション**はネットワークおよびデバイスレベルでDNSリクエストをフィルタリングして管理する、強力かつ使いやすいセキュリティソリューションです。この製品は個別に購入でき、単独で動作するほか、**Webrootエンドポイントプロテクション**とも連携します。詳細は「*DNSプロテクション* ページ 101」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**は、セキュリティのベストプラクティスに関する理解を深め、実践できるようになることを目的に設計されたホスト型のプログラムです。このプログラムには、フィッシングシミュレータとトレーニングコース、およびその他のツールが含まれます。この製品は個別に購入でき、単独で動作するほか、**Webrootエンドポイントプロテクション**とも連携します。詳細は「*Security Awareness Training* ページ 115」を参照してください。

**管理コンソール**と呼ばれるオンラインポータルから、すべての法人向け製品にアクセスできます。管理コンソールとは、Webrootの法人向け製品にログインして管理を行う、一元化されたWebサイトです。

このガイドではまず、Webrootエンドポイントプロテクションのインストールと設定方法について説明します。その後、**DNSプロテクション**と**セキュリティ意識向上トレーニング**について別の章で説明します。

権限によっては、このガイドで説明している機能の一部を利用できない場合があります。

# 基本的な用語

はじめに、Webroot Endpoint Protectionとサイバーセキュリティ全般に関する基本的な用語をいくつかご説明します。

**Webroot Endpoint Protectionに関する用語:**

- **事業体**は管理コンソールを使用して管理できるデバイスやグループです。
    - **デバイス**はエージェントインストールです。
    - **グループ**はデバイスをまとめて管理できる組織単位です。たとえば、特定のポリシーをデバイスのグループに適用できます。
- **サイト**を使用すると部署や会社の地域やオフィスの場所を表すことができます。マネージドサービスプロバイダー(MSP)や大企業にとって、サイトは顧客ごとにエンドポイントの集合を集約して対応するための手段です。
- **ポリシー**はエージェントの動作を定義するものです。エンドポイントプロテクションとDNSプロテクションのシステムポリシーは編集できません。エンドポイントプロテクションの管理対象外ポリシーでは、エージェント側で独自の設定を選択して管理できます。
- **エージェント**: エンドポイントデバイス上で動作するソフトウェアです。インストールされているコンピュータに対して一意のIDを持ち、管理者に代わってバックグラウンドのセキュリティ操作を実行します。

**サイバーセキュリティ全般に関する用語:**

- **マルウェア**: 悪意のあるソフトウェア(malicious software)の略称で、危険なプログラムやコードを意味します。マルウェアによる攻撃は通常、電子メール内の感染した添付ファイルをクリックすることで行われます。これには以下の手口が使われる可能性があります。
    - **ウイルス**: 自身を複製できるプログラムです。一般的には独自のコードを挿入してコンピュータプログラムを感染させます。
    - **スパイウェア**: コンピュータのアクティビティを監視するプログラムです。
    - **ランサムウェア**: データへのアクセスをブロックしたり、身代金が支払われなかった場合にデータを公開すると脅したりするプログラムです。
- **ソーシャルエンジニアリング**: ユーザーを欺いて機密情報を提供させる行動の総称です。これには悪意のある添付ファイルをダウンロードさせようとする他、フィッシング、おとり、電子メールハッキングなどの巧みな戦術が含まれます。
    - **フィッシング**: 電子メールの受信者に購入をさせたり機密情報を漏洩させたりする目的で、有効に見せかけた不正な電子メールを送信する行為です。特定の受信者を標的としたフィッシングを**スピアフィッシング**と呼びます。
    - **おとり**: ターゲットの欲望や好奇心を引き付けるために仕掛けられる罠です。よく見られるおとりには、マルウェアに感染したフラッシュドライブを目立つ場所に置く、魅力的なオンライン広告や宣伝によって悪意のあるWebサイトに誘導する、あるいはマルウェアに感染したファイルをダウンロードするように仕向けたりするなどの手口が挙げられます。
    - **電子メールハッキング**: 電子メールアカウントやメッセージの不正操作です。
- エンドポイントの一般的な保護に関する**セキュリティ**のベストプラクティスには、以下が含まれます。
    - **パスワードセキュリティ**: ハッカーの総当たり攻撃にも対応できるよう、パスワードは複雑なものにすることが重要です。パスワードは定期的に、またセキュリティ侵害が考えられる場合に更

新する必要があります。2要素認証を追加すると、セキュリティレイヤーが強化されます。Webrootではこれらのベストプラクティスを1つでも多く採用することを強く推奨しています。

- **エンドポイント/デバイスのセキュリティ**: すべてのエンドポイントにパッチを適用し、最新の状態にする必要があります。Webrootでは、ユーザーが各自のセキュリティ基準に沿って、パッチを常に最新の状態に保つことを強く推奨しています。
- **WiFiセキュリティ**: ワイヤレス接続は、セキュアなネットワークに制限する必要があります。Webrootでは、WiFiのセキュリティを可能な限り維持することを強く推奨しています。
- **モバイルデバイスのセキュリティ**: モバイルデバイスの紛失や盗難の可能性を最小限に抑え、安全なネットワーク内で業務のみに使用するようにします。Webrootでは、ユーザーが可能な限り各自のモバイルデバイスを保護することを強く推奨しています。
- **物理的セキュリティ**: 物理的セキュリティには、ポータブルデバイス(ノートパソコン、タブレット、スマートフォン)の物理的な認識の向上の重要性だけでなく、物理的なオフィスとそのセキュリティの重要性も含まれます。Webrootでは、物理的セキュリティのベストプラクティスを最大限実践することを強く推奨しています。
- **出張時のセキュリティ**: 出張時にも上記と同じセキュリティのベストプラクティスに留意する必要があります。Webrootではこれらのベストプラクティスを1つでも多く採用することを強く推奨しています。

# 要件

このセクションで説明する製品は、**管理コンソールで**管理されます。管理コンソールは、以下のブラウザーの3つの最新バージョンをサポートしています:

• Google Chrome

• Microsoft Edge

• Firefox

• Safari

**エンドポイント保護**は、ほとんどの最新のWindowsおよびMacコンピュータをサポートしています。Windowsサーバーと VMの組み合わせも保護されています。ご不明な点は詳細リストをご覧ください。

デスクトップ、サーバー、VMプラットフォーム、およびブラウザーのシステム要件は、エンドポイント保護製品ページに記載されています。

注:MacデバイスでWebroot SecureAnywhere 9.5.10以降にアップグレードするには、macOS 11 (Big Sur®) またはそれ以降のバージョンを実行している必要があります。macOS 10.15( Catalina®) またはそれ以前のバージョンのmacOSを使用している場合、バージョン9.5.8以降のエージェントのアップグレードを受け取ることはできません。製品の機能性と機能の可用性を向上させるには、オペレーティングシステムのmacOS 11 (Big Sur®)以降へのアップグレードをご検討ください。

**ポートとファイアウォール**のシステム要件一覧は、ナレッジベースで確認できます。

**DNSプロテクション**については、DNSプロテクションエージェントは通信の大部分にポート443を使用し、DNSプロテクションのリゾルバーではDNS解決にDNS (ポート53)およびDoH (ポート443)をサポートします。

特定のファイアウォールの設定については、ナレッジベース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**の要件は、以下のとおりです。

- フィッシングシミュレーションの電子メールを受信するには、対象ドメイン内に有効な電子メールが必要です。
- トレーニングコースの表示には、最新のWebブラウザのほとんどがサポートされています。
- • お使いのメールサーバーが、ナレッジベースで指定されているセキュリティ入門トレーニングのメールサーバーをブロックしていない必要があります。これらのメールサーバーはナレッジベースで規定されています。
- MicrosoftまたはGoogleを使用している場合は、電子メールのヘッダーでも電子メールを送信できるよう、追加の推奨手順を実行することをお勧めします。
    - Microsoft ExchangeおよびOffice 365で、Webrootセキュリティ意識向上トレーニングの電子メールを許可する方法
    - G Suite Gmailで、Webrootセキュリティ意識向上トレーニングの電子メールを許可する方法
    - Proofpoint Essentialsで、Webrootセキュリティ意識向上トレーニングの電子メールを許可する方法

上記のリンクは米国の英語サイトのものです。国と言語のオプションを変更するには、Webサイトの上部で国旗をクリックして国を選択します。

# を使用するには

こののセクションでは、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使用を開始するための基本的な手順を説明します。製品の設定時は、自社独自のネットワークトポロジーとセキュリティ要件を常に考慮するようにしてください。

Webroot管理コンソールは、Webrootエンドポイントプロテクション、Webroot DNSプロテクション、Webrootセキュリティ意識向上トレーニングの基盤となるコンソールです。いずれの製品を使い始める場合も、初期設定が必要です。

**Webroot管理コンソール:**

- ステップ1: 体験版を**登録**するか、Webrootのビジネス製品を**購入**します。このステップは、本ガイドを受け取る前に済んでいるはずです。
    - 日本国内での利用をご検討の場合は弊社営業にお問合せください。オンライン購入の場合は日本語でのサポートが受けられない場合がありますので、予めご了承ください。体験版利用の詳細は『』の「*製品の購入または体験版への登録* ページ 11」を参照してください。
- ステップ2: Webroot管理コンソールの設定を行います。これにはWebrootアカウントの作成とアクティブ化、2要素認証の設定(必要な場合)、管理コンソール表示の選択が含まれます。
    - アカウントの作成の詳細については、『』の「*アカウントの作成とアクティブ化* ページ 11」を参照してください。
    - 2要素認証の詳細については、『』の「*2要素認証(2FA)の設定* ページ 13」を参照してください。
    - 管理コンソール表示の詳細については、『』の「*管理コンソールの表示の選択* ページ 12」を参照してください。
    - サイトの作成の詳細については、『』の「*サイトの作成(MSPのみ)* ページ 14」を参照してください。

**エンドポイントプロテクション:**

- Webroot管理コンソールの設定手順のステップ1と2を完了すると、コンソールが登録および設定されます。
- エンドポイントプロテクションエージェントをデバイスに配備します。
- 保護対象とするコンピュータごとにエージェントをインストールします。インストールが完了すると、エージェントが管理コンソールを通じて、エンドポイントのアクティビティを登録、報告するようになります。
    - 詳細は『』の「*エージェントのダウンロードとインストール* ページ 17」を参照してください。

**DNSプロテクション:**

- Webroot管理コンソールの設定手順のステップ1と2を完了すると、コンソールが登録および設定されます。
- DNSプロテクションの有効化とインストールを行います。
    - 詳細は『』の「*DNSプロテクションの有効化と設定* ページ 101」を参照してください。
- 保護対象とするコンピュータごとにエージェントをインストールします。インストールが完了すると、エージェントが管理コンソールを通じて、DNSのアクティビティを登録、報告するようになります。
    - 詳細は『』の「*ネットワーク証明書とライセンスのインストール* ページ 113」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:**

- Webroot管理コンソールの設定手順のステップ1と2を完了すると、コンソールが登録および設定されます。
- セキュリティ意識向上トレーニングの有効化と対象ユーザーの選択を行います。
  - セキュリティ意識向上トレーニングの有効化の詳細については、『』の「*Security Awareness Trainingの有効化* ページ 116」を参照してください。
  - 対象ユーザーの選択の詳細については、『』の「*トレーニング対象のユーザーの選択* ページ 116」を参照してください。

これらのステップを完了すると、すべてのWebroot製品で管理コンソールを使った作業を開始できます。

# ステップ1: 登録/購入

すでに製品を購入済み、または体験版に登録済みの場合は、このステップをスキップできます。

## 製品の購入または体験版への登録

1. https://www.webroot.com/jp/ja/businessに移動します。国名リストから現在地を確認します。
2. [**ビジネス向け**]メニューで[**製品**]セクションを確認し、関心のある製品をクリックします。
3. [**購入方法**]をクリックします。
   - **エンドポイントプロテクション**を購入するには[**今すぐ購入**]または[**無料で試す**]をクリックし、画面に表示される手順に従います。日本国内での購入をご検討の場合は営業にお問合せください。また、大量のサブスクリプションや複数の製品を購入される場合は、営業担当者にお問い合わせください。オンラインでのご購入ですと日本語でのサポート対応ができない場合がございますので予めご了承ください。
   - DNSプロテクションとセキュリティ意識向上トレーニングの場合は、[**無料で試す**]または[**デモをリクエスト**]を選択できます。次のページで必要な情報を入力し、[**送信**]をクリックします。

ISPまたはパブリックドメイン(gmail.comなど)の電子メールアドレスは制限されているため、使用できません。電子メールアドレスは、有効な企業または組織のアドレスである必要があります。

# ステップ2: 設定

このステップでは、法人向けの管理コンソールの使用を開始できるよう、設定に関する以下のタスクについて説明します。

- アカウントの作成とアクティブ化
- 管理コンソールの表示の選択
- 2要素認証の設定
- サイトの作成(MSPのみ)

## アカウントの作成とアクティブ化

製品を購入または体験版に登録すると、登録確認メールが届きます。

1. 電子メールを開封します。
2. 登録用リンクをクリックします。

3. 登録ページで、電子メールに記載されている一時パスワードを入力します。
4. フォームの以下の情報を入力します。
    - パスワード要件:
        - 9文字以上、30文字以内である必要があります。
        - 数字が3つ以上、その他の文字が6文字以上含まれている必要があります。
        - 文字列をnullまたは空にすることはできません。
        - 特殊文字、<、>は使用できません。
        - セキュリティコードと同じ値は使用できません。
    - セキュリティコード要件:
        - セキュリティコードは、パスワードを入力した後の追加のセキュリティ対策として使用される文字または数字です。
        - このコードからランダムな2文字を入力する必要があるため、覚えやすい値を使用することが推奨されます。
        - 大文字と小文字は区別されます。
        - 6文字以上である必要があります。
        - 連続した数字や文字は使用できません(1 2 3 4 5 6など)。
        - 一般的な単語は使用できません。

## 管理コンソールの表示の選択

管理コンソールの表示は2種類のオプションから選択できます。

- **マネージドサービスプロバイダー(MSP)向けの表示**: 企業だけでなく、複数の顧客のセキュリティを管理する組織にも使用できます。
- **ビジネス向けの表示**: 単一のサイトで独自にセキュリティを管理する小規模な企業向けに設計されています。

管理コンソールの表示は、初回アクセス時に決定します。**ビジネス向けの表示**を選択した場合は、必要に応じて後から**MSP向けの表示**にアップグレードできます。

**管理コンソールの表示を選択するには、以下の手順に従います。**

1. my.webrootanywhere.comから管理コンソールにログインします。
2. コンソールへの初回アクセス時は、表示の選択を促すプロンプトが表示されます。
    - [**マネージドサービスプロバイダー**]を選択すると、サイトごとに製品を管理できる管理コンソールが設定されます。
        - サイトは、部署、オフィスの場所、顧客、または管理対象のその他の組織単位を表します。
        - 必要に応じて、サイトごとに異なる請求とキーコードを使用できます。
        - この表示は、**ビジネス向けの表示**に変更できません。

- [**ビジネス**]を選択すると、管理コンソールが単一のサイトとして設定され、より小規模な企業のセキュリティのみに焦点を当てることができます。
    - すべてのデバイスと請求に単一のサイトとキーコードを使用します。
    - サイトごとに異なる請求とキーコードを使用できます。
    - この表示は、後から**マネージドサービスプロバイダー向けの表示**に変更できます。

3. 希望する表示で[**選択**]をクリックします。
4. **ビジネス向けの表示**を選択した場合は、会社の情報を入力します。
    - [**サイト/会社名**]: サイトまたは会社の一意の名前です。
    - [**デバイスの数**]: 管理するデバイスの数を指定します。
    - [**会社の業種**]: 会社の業種を選択します。
    - [**会社の規模**]: 会社の規模を表す範囲を選択します。
5. 完了したら、[**選択**]をクリックします。

**法人向けの表示**を選択した場合、後から**マネージドサービスプロバイダー向けの表示**に変換できます。ただし、**マネージドサービスプロバイダー向けの表示**を選択した場合は、後から**法人向けの表示**に変換することはできません。

**コンソールを「法人向けの表示」から「MSP向けの表示」に変更するには、以下の手順に従います。**

1. ナビゲーションペインで[**設定**]に移動します。
2. [**詳細設定**]タブをクリックします。
3. [**マネージドサービスプロバイダーコンソールに変換**]で、[**変換**]をクリックします。

## 2要素認証(2FA)の設定

アカウントをアクティブにした後は、2要素認証(2FA)のオプションを設定することで、アカウントへの不正アクセスを防止できます。

2要素認証の設定は任意ですが、設定することを強く推奨します。

**2要素認証を設定するには、以下の手順に従います。**

1. AndroidまたはiOSのモバイルデバイスかタブレットで、Google Authenticator、Microsoft Authenticator、LastPass Authenticator、Authy2要素認証などの認証アプリを開くかインストールします。
2. https://my.webrootanywhere.comから管理コンソールにログインします。
3. [**2FAを設定する**]をクリックします。
    - 2FAを後で設定する場合は、[**今はスキップする**]をクリックします。
    - その場合、後で2FAを設定するには、コンソールの[**管理者**]セクションに移動します。管理者のリストで名前をクリックします。[**ログイン設定**]ボックスで[**2FAを有効にする**]をクリックします。
4. セキュリティの質問に答えて[**続行**]をクリックします。
    - セキュリティコードは大文字と小文字が区別されます。

5. モバイルデバイスまたはタブレットで、認証用アプリを開き、管理コンソールに表示されているQRコードをスキャンします。
    - コードをスキャンできない場合は、[**QRコードをスキャンできない場合**]をクリックし、認証用アプリからコードを入力します。
    - コードの大文字と小文字は区別されます。
6. コードを入力すると、認証コードが表示されます。コードを入力し、[**認証コードを確認する**]をクリックします。
7. 認証が成功したことを確認します。
    - 認証に失敗した場合は、認証用アプリから新しいコードを入力します。コードの有効期間は30秒間です。
8. 成功したら、[**コンソールに進む**]をクリックして再度ログインします。

2要素認証では、個人のセキュリティコードではなく認証用アプリのコードをログインのたびに使用します。

**法人向けの表示**を選択した場合は、「*エンドポイントプロテクション* ページ 16」に進みます。

**マネージドサービスプロバイダー向けの表示**を選択した場合は、「*サイトの作成(MSPのみ)* ページ 14」に進みます。

## サイトの作成(MSPのみ)

管理コンソールで[**マネージドサービスプロバイダー向けの表示**]を選択した場合は、サイトを作成して初期設定を完了する必要があります。

**サイトを作成するには、以下の手順に従います。**

1. [**サイトリスト**]、[**サイトを追加**]の順にクリックします。[**サイトの追加**]ウィザードが開きます。
2. [**詳細**]でサイトの詳細を入力します。
    - [**サイト/会社名**]: サイトまたは会社の一意の名前です。
    - [**サイトの種類**]:
        - [**外部企業**]: 管理している外部企業です。
        - [**社内サイト**]: 店舗やオフィスなど、自社内にあるサイトです。
    - [**会社の規模**] (外部企業のみ): 会社の規模を表す範囲を選択します。
    - [**会社の業種**] (外部企業のみ): 会社の業種を選択します。
    - [**支払請求サイクル**] (外部企業のみ): このサイトで必要に応じて定義および使用する支払請求サイクルです。これは参考用で、Webrootアカウントには関連付けられていません。
    - [**支払請求日**] (外部企業のみ): このサイトで必要に応じて定義および使用する支払請求日です。これは参考用で、Webrootアカウントには関連付けられていません。
    - [**配信先リスト**]: スケジュールレポートを受け取れる電子メールアドレスをコンマで区切って最大10個指定します。新しいレポートをスケジュールする場合は、[**各サイトの配信先リストに送信**]を選択して、関連するすべての電子メールアドレスがレポートを受信できるようにします。
    - [**グローバルポリシーの追加**]:

- 有効にすると、このサイトですべてのグローバルポリシーを使用できます。一度有効にすると、このオプションは変更できません。
- 無効にする場合は、サイトごとに個別のポリシーを作成する必要があります。

- [**グローバルオーバーライドの追加**]:
  - 有効にすると、グローバルオーバーライドがこのサイトに適用されます。たとえば、あるサイトで特定のファイルを許可し、それをグローバルオーバーライドとして設定すると、このオプションが有効になっているすべてのサイトがそのファイルを許可します。一度有効にすると、このオプションは変更できません。
  - 無効にする場合は、サイトごとに個別のオーバーライドを作成する必要があります。
- [**コメント**] (オプション): サイトまたは会社を説明するコメントです。
- [**タグ**] (オプション): 検索のフィルタリングに便利なラベルです。サイトにカスタムタグを追加すると、そのタグを使用して[**サイトリスト**]をフィルタリングできます。サイトにカスタムタグを適用するには、各タグの後ろの[**タグ**]ボックスにタグ名を入力してEnterを押します。

3. [**次へ**]をクリックして続けます。
4. [**管理者権限**]ステップで、このサイトに付与する権限を選択します。サイトを作成したアカウントにはデフォルトで完全な管理者権限が与えられるため、そのアカウントはリストに表示されません。他のすべてのアカウントがリストに表示され、デフォルトで[**アクセス不可**]に設定されます。
   - [**管理者**]: サイトへのフルアクセスが許可されます。
   - [**表示のみ**]: サイトの表示のみが許可されます。
   - [**アクセス不可**]: サイトへのアクセスが拒否されます。
5. [**次へ**]をクリックして続けます。
6. 3番目のステップでは、Endpoint Protectionのオプションが表示されます。Endpoint Protectionは常に有効ですが、他の製品のみを使用する場合は、エンドポイントエージェントの配備は任意であることに注意してください。
   - **キーコードの種類**
     - 製品を購入した場合: フル
     - 30日間の無料体験に登録した場合: 体験版
   - [**サイトのシート数**]: 設定するサイトのエンドポイント数を指定します。この設定は配備されるシート数を制限するものではなく、請求に使用されることもありません。
   - [**デフォルトのエンドポイントポリシー**]: グループ、サイト、または会社からのポリシーを継承してポリシーが割り当てられていない限り、このサイトにインストールされたすべての新しいデバイスに使用されます。インストール後に、デバイスが使用するポリシーを変更することができます。Webrootでは、デフォルトのエンドポイントポリシーのコピーを作成し、ベストプラクティスと特定のニーズに合わせて変更することを推奨しています。詳細は『』の「*Endpoint Protectionのポリシーのベストプラクティス* ページ 42」を参照してください。
     - [**推奨デフォルト設定**]: デスクトップおよびノートパソコンが対象です。
     - [**推奨DNS有効**]: [**推奨デフォルト設定**]と同様、デスクトップおよびノートパソコンが対象です。また、DNSプロテクションエージェントを自動インストールします。

- [**推奨サーバーデフォルト設定**]: サーバー環境が対象です。リソースの使用率とサーバーへの影響の最小化に重点を置いています。
- [**サイレント監査**]: エンドポイントプロテクションを透過的に使用できます。検出事項を報告しますが、感染を修復しません。ポリシーのテスト用として、本番環境への影響を最小限に抑えるようにできています。Webrootではこのポリシーの使用を、本番環境における潜在的な誤検出や競合の特定、および不明なソフトウェアの発見を目的として、初期設定中のような短時間に限定することを推奨しています。
- [**管理対象外**]: ユーザーが各自の設定をエージェントのユーザーインターフェイスで編集できるようにします。それまで適用されていたポリシーや設定は継承されますが、ユーザーインターフェイスを表示するかどうかを除いて特に設定はありません。
    - テクニカルサポートやトラブルシューティングで、またポリシー管理が不要な場合に使用します。
    - エンドユーザーが直接制御できるローカルの非管理アプリケーションにエージェントを変換します。
    - 本番環境では使用しないでください。
- ポリシー名の最初に[**レガシー**]の付いたポリシーには以前推奨されていたポリシー設定が含まれています。

- ***データフィルタ***
    - コンソールに表示されるデータを表示または非表示にするには、データフィルタを適用します。
    - たとえば、[**2か月**]を選択すると、2か月間接続されていないすべてのデバイスが、このサイトに表示されるデータから除外されます。
    - データフィルタを適用すると、ページの読み込みのパフォーマンスは向上する場合がありますが、表示される内容は制限されます。
    - フィルタを適用または削除する場合、配備サイズと表示するデータの量によっては、データの更新に数分かかることがあります。
    - [**親設定を継承**]を選択すると、コンソールレベルで設定されたフィルタが継承されます。この設定は、[**設定**] > [***データフィルタ***] > [***データフィルタ***]ドロップダウンで確認できます。

7. [**次へ**]をクリックして続けます。
8. 必要に応じて、**DNS Protection**を有効にします。詳細は『』の「*DNSプロテクション* ページ 101」を参照してください。
9. [**次へ**]をクリックして続けます。
10. 必要に応じて、**Security Awareness Training**を有効にします。詳細は『』の「*Security Awareness Training* ページ 115」を参照してください。
11. [**保存**]をクリックしてサイトの設定を完了し、キーコードをサイトに割り当てます。

# エンドポイントプロテクション

Webrootエンドポイントプロテクションの設定を行う際の次の手順は、エージェントの配備です。これにより、デバイスを潜在的な問題から保護するだけでなく、その問題に関するフィードバックが提供されます。今後すべてのデバイスに簡単に適用できるよう、最初にカスタムポリシーを作成することをお勧めします。

- カスタムポリシーの作成
- エージェントのダウンロードとインストール
- キーコードを確認する方法

## カスタムポリシーの作成

Webrootではエンドポイントを保護するため、ベストプラクティスを活用したカスタムポリシーの作成を推奨しています。現時点でポリシーを作成しておくと、今後すべてのエンドポイントに簡単に適用できます。

以下の手順は、Endpoint Protectionのカスタムポリシーを作成する一例です。自社独自の要件を常に優先してください。

**カスタムポリシーを作成するには、以下の手順に従います。**

1. ナビゲーションペインにある[**管理**]の下部で、[**ポリシー**]をクリックします。
    - 推奨されるデフォルトポリシーに基づくカスタムポリシーを新規で作成するには、[**ポリシーを追加**]をクリックします。
    - 既存のポリシーに基づくカスタムポリシーを作成するには、コピー対象のポリシーの行を特定し、[**アクション**]の下にある[**コピー**]をクリックします。
2. 新規で作成されたポリシーは推奨されるデフォルトポリシーに基づいており、大半のワークステーションのユースケースに対応するように設定されています。ベストプラクティスを適用し、特定の要件を適用しながらポリシーをカスタマイズしてください。
    - [**名前**]: ポリシー名です。
    - [**説明**]: ポリシーの意図や目的の説明です。
    - 以下は一般的に設定が変更されることの多い項目です。
        - **基本設定**
            - [**システムトレイアイコンを表示する**] (デフォルト: オン)
        - **ユーザーインターフェイス**
            - [**GUI**] (デフォルト: 表示)
        - **Evasion Shield**
            - [**スクリプト保護**]: [**検出と修復**]に設定すると、脅威が特定された場合にすぐにアクションを実行できます。
        - **USBシールド**
            - [**USBストレージデバイスをブロック**] (デフォルト: オフ)

## エージェントのダウンロードとインストール

Webrootエンドポイントプロテクションは、エージェントがインストールおよび実行されているPCとMacを保護します。Webrootエージェントはインストールされているコンピュータごとに一意のIDを持ち、ユーザーによる制御を必要とせず、管理者に代わってセキュリティ操作を実行します。

エンドポイントプロテクションエージェントはクラウドベースで機能します。そのため、インターネットアクセスが大幅に制限されたネットワークにエージェントをインストールする場合は、エージェントが正常に機能するよう、ファイアウォールの設定で特定のURLを許可する必要があります。

許可する必要のあるURLのリストについては、ナレッジベースを参照してください。

**エージェントをダウンロードしてインストールするには、以下の手順に従います。**

1. 管理コンソールで、エージェントをインストールするためのダウンロードリンクを見つけます。
   - **法人向けの表示**の場合:
     a. [**設定**] > [**ダウンロード**]をクリックし、インストールファイルのダウンロードリンクを見つけます。
     b. 対象のデバイスで使用されているOSの下部に表示された[**ダウンロード**]リンクをクリックします。
   - **MSP向けの表示**の場合:
     a. [**サイトリスト**]をクリックします。
     b. リストでサイトを特定し、名前をクリックします。
     c. [**エンドポイントプロテクション**]タブを開きます。
     d. [**ソフトウェアのダウンロード**]ボックスで、[**Windows (.exe) をダウンロード**]、[**Windows (.msi) をダウンロード**]、または[**Macをダウンロード**]リンクをクリックし、対象のデバイスに適したファイルをダウンロードします。
2. 今後の参考のため、会社またはサイトの**キーコード**をコピーします。詳細は「*キーコードの確認* ページ 18」を参照してください。
3. エージェントをインストールするデバイスに、インストールファイルを移動します。
4. エージェントをインストールします。

インストールが完了すると、エージェントが脅威のスキャンを開始します。初期スキャンが完了してエージェントが管理コンソールでチェックインすると、[**事業体**]ページの[**名前**]列に情報が入力されます。このプロセスは通常は15 ~ 30分程度で完了しますが、最大で24時間かかる場合もあります。

エンドポイントプロテクションとDNSプロテクションを使用する場合、エンドポイントポリシーでDNSプロテクションを有効化する必要があります。サイトでDNSプロテクションが有効化され、エンドポイントポリシーでDNSプロテクションが有効になっている場合、デバイスが[**事業体**]にリストされるとDNSフィルタリングが開始されます。DNSプロテクションの詳細については、『』の「*DNSプロテクション* ページ 101」を参照してください。

## キーコードの確認

エージェントのインストール時にはキーコードが必要です。サイトごとに一意のキーコードがあり、インストール中に参照されるか、コマンドラインで指定する必要があります。デフォルトでは、キーコードは.exeのインストーラーのファイル名として割り当てられます。変更しない場合はデフォルトのキーコードが使われます。ただし、MSIを使用した場合やファイル名を変更した場合は、コマンドラインからキーコードを指定するか、インストーラーGUIから入力する必要があります。エージェントの配備に関する詳細については、『』の「*エージェントの配備* ページ 84」を参照してください。

キーコードは、以下のいずれかの方法で確認できます。

**法人向けの表示の場合:**

1. ナビゲーションペインで[**設定**]をクリックします。
2. [**ダウンロード**]タブを選択します。

**MSP向けの表示の場合:**

1. [**サイトリスト**]タブをクリックします。
2. サイト名の横にある[**キー**]ボタン( )をクリックします。

# エンドポイントプロテクションの使用の開始

おめでとうございます! エンドポイントプロテクションの設定が完了しました。

- エージェントによる脅威の初回スキャンは、通常15 ~ 30分以内に完了します。24時間が経過しても管理コンソールにデバイスが表示されない場合は、カスタマーサポートにお問い合わせください。
- Webrootではクラウドベースで脅威を検出しているため、Windowsエンドポイント用定義ファイルのダウンロードやインストールは不要です。特定された新しい脅威はすべてクラウドで情報が更新され、即座に保護されます。
- Macエージェントでは、特定のバージョンのファイルが使用されます。バージョン番号は、エージェントのバージョンの末尾に付加されます。
- エンドポイントプロテクションは、他のセキュリティ製品と競合することなく使用できます。

エンドポイントエージェントがコンソールにチェックインすると、[デバイス]列に表示されるデバイス数が増加します。脅威が検出された場合は、[状態]が[**要対応**]に変わります。

## 詳細

それぞれの製品でグローバルナビゲーションバーの[**ヘルプ**]ボタン( )をクリックすると、オンラインヘルプを利用できます。

オンラインでは以下のとおり、より多くの情報も参照できます。

- Webrootサポートナレッジベース: answers.webroot.com
- Business Endpoint Protection (Webrootコミュニティ)

## スポットライトツアー

初めてコンソールを開いたときに、製品案内のためのスポットライトツアーが起動します。ツアーには、以下の項目に関する簡単な説明が含まれます。

- ダッシュボード
- 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、追加のセキュリティレイヤー
- 管理者の管理
- グループとポリシー
- オーバーライド、レポート、警告、設定

スポットライトツアーを後から再度表示するには、以下の手順に従います。

1. グローバルナビゲーションバーで[**リソース**]ボタン( )をクリックします。
2. ドロップダウンメニューで[**スポットライトツアー**]を選択します。

# Webroot製品のナビゲーション

管理コンソールと呼ばれるオンラインポータルから、すべての法人向け製品にアクセスできます。Webrootの法人向け製品にログインし、管理を行う場所が管理コンソールです。

管理コンソールのURLは、https://my.webrootanywhere.com/です。

管理コンソールには2つの表示形式があり、Webrootエンドポイントプロテクションを最初に開いたときに設定します。

- **法人向けの表示**: 管理コンソールを単一のサイトとして利用し、企業のサイバーセキュリティのみに焦点を当てることができます。
    - すべてのデバイスと請求に単一のキーコードを使用できます。
    - **グループ**を利用すると、デバイスを整理しやすくなります。
    - 表示は後から**マネージドサービスプロバイダー(MSP)向けの表示**に変更できます。
- **マネージドサービスプロバイダー(MSP)向けの表示**: 複数のサイトを管理できます。
    - サイトは企業、部署、地域、オフィスの場所、または管理対象のその他の組織単位を表します。
    - サイトごとに異なる請求とキーコードを使用できます。

30分間操作を行わないと、管理コンソールから自動的にサインアウトされますのでご注意ください。セッションの有効期限が切れる前にセッションをアクティブに保つには、管理コンソール内で何らかのアクションを実行します。セッションの残り時間が2分になると、サインインを維持するよう促されます。セッションを更新するには、**サインイン**または**ログイン**をクリックしてください。

## ナビゲーション

管理コンソールの**ナビゲーションペイン**では、ナビゲーションリンクからさまざまなコンソールページにアクセスできます。ナビゲーションペインの下部にある**<**または**>**のアイコンを使用すると、ナビゲーションリンクを展開したり折りたたんだりすることができます。

- [**コンソールスイッチャー**]: コンソール間を移動できます。割り当てられたコンソールが1つのみの場合は、静的なコンソール名が表示されます。複数のコンソールで作業している場合は、選択可能なコンソール名のリストがドロップダウンリストに表示されます。コンソールスイッチャーを使うとコンソール名を変更でき、変更後の名前は、そのコンソールを使用するすべてのユーザーに表示されます。
- [**サイトリスト**] (**MSP向けの表示**のみ): アクセス可能なすべてのサイトが表示されます。このページから個々のサイトを表示および管理できます。詳細は『』の「*サイト(MSPのみ)* ページ 25」を参照してください。
- [**ダッシュボード**]: このタブには保護の概要が表示されます。**法人向けの表示**は単一の組織向け、**マネージドサービスプロバイダー(MSP)向けの表示**は複数サイトを管理する組織向けに設計されているため、**ダッシュボード**の表示はコンソールの種類ごとに異なります。詳細は『』の「*ダッシュボード* ページ 22」を参照してください。
- [**管理**]: このタブには3つのサブタブがあります。
    - [**事業体**]: このページでは、すべてのデバイスとグループを表示、整理、管理できます。詳細は『』の「*事業体* ページ 31」を参照してください。

        - **デバイス**はエンドポイントです。
        - **グループ**は、デバイスをまとめて管理できる組織単位です。たとえば、特定のポリシーをデバイスのグループに適用できます。
    - [**ポリシー**]: このページでは、ポリシーを作成、管理できます。詳細は『』の「*ポリシー* ページ 42」を参照してください。
        - ポリシーは、スキャンの実行方法、スキャンの頻度、およびその他の指示に関する設定を含めたエージェントの動作を定義します。
        - **エンドポイントプロテクション**と**DNSプロテクション**のシステムポリシーは編集できません。
        - **エンドポイントプロテクション**の管理対象外ポリシーでは、エージェント側で独自の設定を選択して管理できます。
    - [**オーバーライド**]: ポリシー設定やWebrootによるファイルやURLの定義方法にかかわらず、許可またはブロックする必要のあるファイルやURLを指定できます。詳細は『』の「*エンドポイントプロテクションのオーバーライド* ページ 71」を参照してください。
- [**DNSプロテクション**] (**法人向けの表示**のみ): **DNSプロテクション**が有効かどうか、また有効になっている場合はその設定が表示されます。詳細は『』の「*DNSプロテクション* ページ 101」を参照してください。
    - **MSP向けの表示**では、**DNSプロテクション**はサイトごとに設定されます。詳細は『』の「*サイト (MSPのみ)* ページ 25」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**のキャンペーン、コンテンツ、ユーザー、および設定(**法人向けの表示**のみ)が表示されます。詳細は『』の「*Security Awareness Training* ページ 115」を参照してください。
    - **MSP向けの表示**の場合、セキュリティ意識向上トレーニングの設定はサイトページに表示されます。
- [**レポート**]: **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**の詳細な情報が記載されます。レポートは必要に応じて作成することも、定期的な間隔でスケジュールすることもできます。詳細は『』の「*レポート* ページ 74」を参照してください。
- [**警告**]: 脅威が検出されたとき、またはWebrootエージェントがデバイスにインストールされたときに通知される電子メール通知です。警告の配信先リストは、警告の送信先となる1つ以上の電子メールアドレスのリストです。詳細は『』の「*警告と警告の配信先リスト* ページ 90」を参照してください。
- [**管理者**]: コンソールに存在する管理者またはアカウントが表示されます。詳細は『』の「*管理タスク* ページ 92」を参照してください。
- [**設定**]: 設定のセクションが含まれ、内容は選択した表示形式によって異なります。詳細は『』の「*設定* ページ 95」を参照してください。

# よく使用される機能

画面上部には、よく使用される機能にアクセスするためのアイコンが表示されています。

- [**リソース**]ボタン(): お知らせ、スポットライトツアー、サービス状況、パートナートレーニング、ドキュメント、法律、その他の製品情報へのリンクにアクセスできます。
- [**ヘルプ**]ボタン(): ヘルプドキュメントとカスタマーサポートへのリンクにアクセスし、新規のサポートチ

ケットを送信できます。

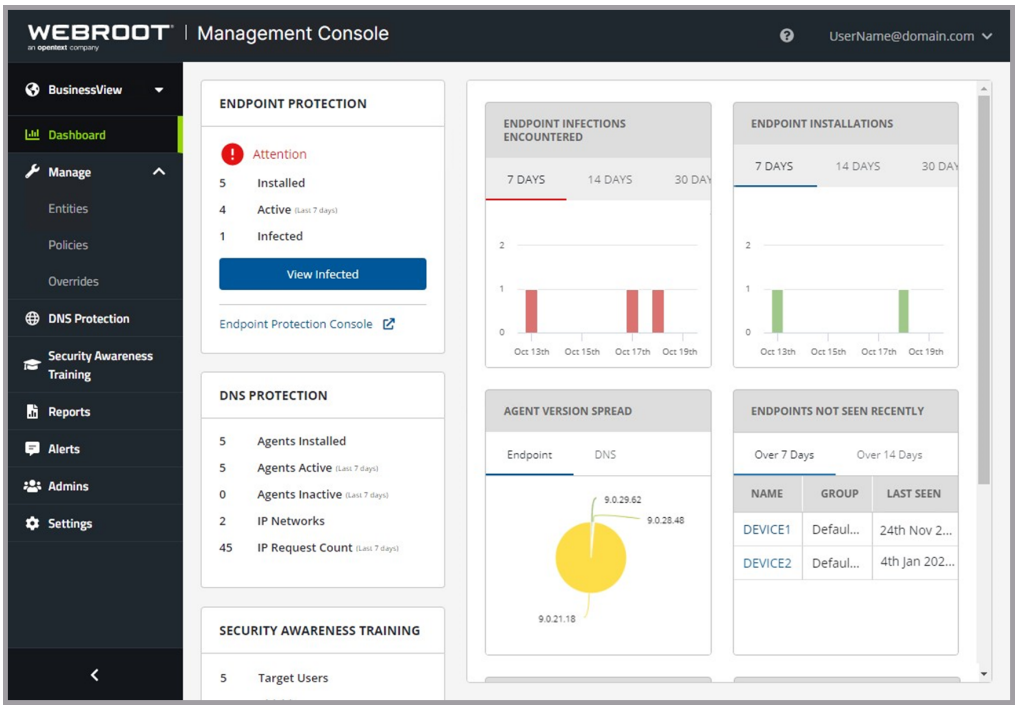
- [**ログイン名**]: クリックするとコンソールからログアウトするオプションが表示されます。

## ダッシュボード

**ダッシュボード**には、保護の概要が表示されます。ダッシュボードは管理コンソールの表示によって異なります。

- あるサイトから別のサイトにデバイスを移動したときにキーコードを移行した場合、デバイス数に不一致が生じる可能性があります。

**法人向けの表示のダッシュボード**には、統計タイルと状態を示すチャートが表示されます。




ページの左側の3つのタイルには、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統計情報の概要が表示されます。これらの統計情報により、各コンポーネントを一目で分析することができます。

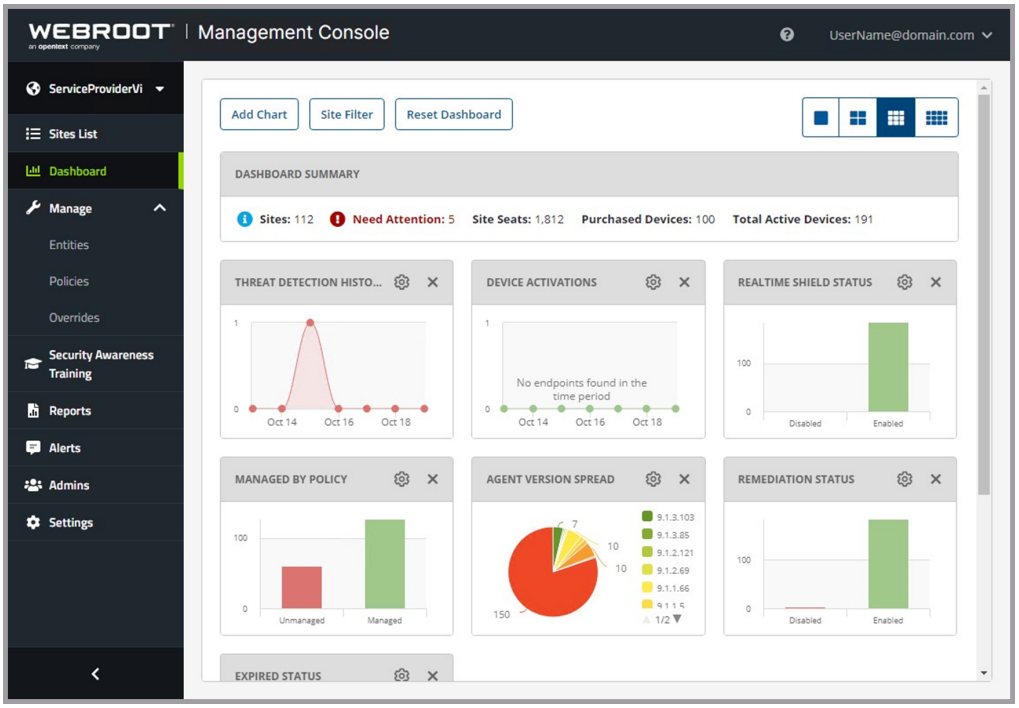
- [**エンドポイントプロテクション**]には、スキャン対象であるデバイスの統計情報の概要が表示されます。感染したデバイスを表示するには、[**感染したものを表示**]をクリックします。
- [**DNSプロテクション**]には、DNSプロテクションの対象であるエージェントとネットワークの状態が表示されます。有効になっていない場合は[**DNS Protectionを有効にする**]をクリックして有効にします。
- [**セキュリティ意識向上トレーニング**]には、ターゲットユーザーとキャンペーンに関する情報が表示されます。

タイル内のボタンとハイパーリンクを使用すると、コンソールの特定のページに移動したり、使用していない製品を有効にしたりできます。

コンポーネントタイルの隣には、アクティビティの詳細を示すさまざまなチャートが表示されます。チャートのデータやマシン名をクリックすると、チャートのコンポーネント内で絞り込むことができます。

- チャートのコンポーネント内で絞り込むには、チャートのデータをクリックします。
- 場合によっては、表示された詳細の内容をさらに絞り込むことができます。
- [**編集**]ボタン(⚙)をクリックすると、チャートを修正できます。
- [**削除**]ボタン(×)をクリックすると、チャートを削除できます。

**MSP向けの表示のダッシュボード**には、サイトの概要と状態を示すチャートが表示されます。




ページ上部の[**ダッシュボード概要**]には、サイト、シート、デバイスの統計情報の概要が表示されます。

- [**サイト**]にカーソルを合わせると、統計の内訳が表示されます。
- [**対応が必要**]または[**期限が切れるサイト**]をクリックすると[**サイトリスト**]ページに移動し、個々のサイトの詳細を表示できます。

[ダッシュボード概要]の下部には、アクティビティの詳細を示すさまざまなチャートが表示されます。

- チャートのコンポーネント内で絞り込むには、チャートのデータをクリックします。
- 場合によっては、表示された詳細の内容をさらに絞り込むことができます。
- [**編集**]ボタン(⚙)をクリックすると、チャートを修正できます。
- [**削除**]ボタン(×)をクリックすると、チャートを削除できます。

このダッシュボードでは、以下のアクションも実行できます。

- [**チャートを追加**]をクリックすると、別のチャートを作成できます。必要なオプションを選択します。チャートを定義したら、[**チャートを追加**]をクリックします。
- [**サイトフィルタ**]をクリックすると、チャートに含めるサイトを決定するフィルタを設定またはクリアできます。

    - [**すべて**]: チャートにすべてのサイトが表示されます。
    - [**サイトの選択**]: 選択したサイトのみがチャートに表示されます。
- [**ダッシュボードをリセット**]をクリックすると、チャートのレイアウト、表示、フィルタがデフォルトにリセットされます。
- [**レイアウト**]ボタンをクリックすると、チャートの表示を1行あたり1 ~ 4個のチャートに変更できます。チャートをドラッグ&ドロップして、希望する表示方法でチャートを並べ替えることもできます。

# サイト(MSPのみ)

**サイト**を使用すると部署や会社の地域やオフィスの場所を表すことができます。マネージドサービスプロバイダー(MSP)や大企業にとって、サイトは顧客ごとにエンドポイントの集合を集約して対応するための手段です。

管理コンソールから、サイトの表示、追加、管理を行うことができます。

サイトを追加するには、『』の「*サイトの作成(MSPのみ)* ページ 14」を参照してください。

## すべてのサイトの表示(MSP向けの表示のみ)

[**サイトリスト**]をクリックすると、アクセスできるサイトの概要が表示されます。

[**サイトリスト**]ページの上部で、以下のコントロールを使用できます。

- [**サイトリスト**]: デフォルトでは、すべての製品についての情報がこの表に表示されます。[**表示**]ドロップダウンメニューをクリックすると、製品のリスト、または[**列のカスタマイズ**]ボタン( )をクリックして定義できるカスタマイズ表示を選択できます。
- [**検索**]: このボックスに入力した検索テキストを含む行のみを、リストに表示できます。
    - 検索では、表示されている行だけでなく表全体が対象になります。
    - フィルタが適用されている場合、検索範囲はフィルタによって表示される行のみに制限されます。
    - 適用された検索語、フィルタ、並べ替え設定は、手動でリセットするかコンソールからログアウトするまで、コンソール内の他のページに移動しても保持されます。
- [**サイトを追加**]: 新しいサイトを作成します。サイトの作成の詳細については、『』の「*サイトの作成(MSPのみ)* ページ 14」を参照してください。
- [**エクスポート**]: サイトのリストに現在適用されている検索とフィルタに基づいて、サイトのリストをコンマで区切られたファイル(.csv)でダウンロードします。
- [**更新**]: サイトのリストを更新します。指定した検索とフィルタは更新後もサイトのリストに適用されます。
- [**フィルタ**]: フィルタパネルが開きます。
    - [**フィルタ**]ボタンにある緑色の円に囲まれた数値は、現在適用されているフィルタの数を示します。
    - フィルタパネルでセクションを展開すると、利用可能なフィルタが表示されます。
    - フィルタの横にある[**除外**]リンクをクリックすると、そのフィルタが除外され、グループ内の残りのフィルタが選択されます。
    - 適用したフィルタは手動でリセットするかコンソールからログアウトするまで、コンソール内の他のページに移動しても保持されます。
    - 1つのフィルタグループの選択をすべて手動で削除するには、[**リセット**]をクリックします。
    - すべてのフィルタを削除するには、パネル下部の[**フィルタをリセット**]をクリックします。

**[サイトリスト]の表の表示をカスタマイズするには、以下の手順に従います。**

1. [**カラムのカスタマイズ**]ボタン(  )をクリックします。
2. [**カラムのカスタマイズ**]パネルが開きます。このパネルで各データポイントの横にあるチェックボックスを選択し、[**サイトリスト**]の表に含めるか除外するかを決定します。
3. 表示される列の順序を並べ替えるには、各データポイントの横にある二重線のアイコン( ═ )をドラッグします。
4. [**適用**]をクリックして変更を保存します。

カスタマイズした表示は、別のページに移動したり、コンソールからログアウトした後も保持されます。表をデフォルトの表示にリセットするには、[**カラムのカスタマイズ**]パネルで、[**デフォルトにリセット**]をクリックします。

[**サイトリスト**]の表では、サイトを以下のとおり表示および管理できます。

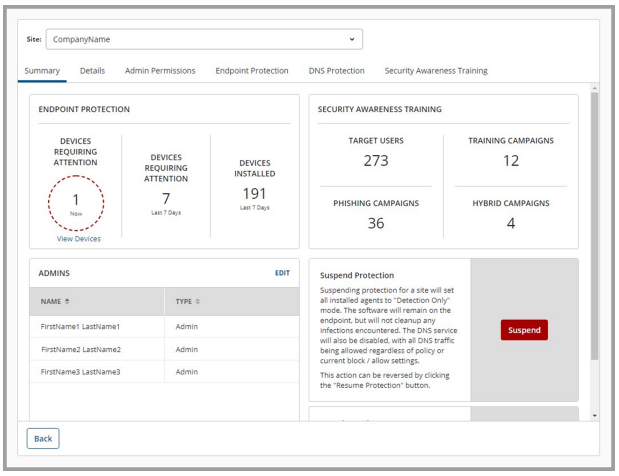
- **製品のサブスクリプションの状態**は、青い線を展開することで表示されます。行の上部にある青い矢印をクリックすると、情報を展開したり折りたたんだりすることができます。
    - **アクティブな有料**サブスクリプション: 白文字を含む青で塗りつぶされた円で示されます。
    - **アクティブな体験版**サブスクリプション: 青文字を含む白で塗りつぶされた円で示されます。
    - **期限切れの体験版**サブスクリプション: 青文字と青のスラッシュを含む白で塗りつぶされた円で表示されます。
    - **期限切れの有料**サブスクリプション: 白文字を含む赤で塗りつぶされた円に白いスラッシュで示されます。
    - **非アクティブ**なサブスクリプション: 黒文字を含む灰色で塗りつぶされた円で表示されます。
    - **一時停止**中のサブスクリプション: 白文字を含む黒で塗りつぶされた円で示されます。
- [**サイト名**]のリンクをクリックすると、そのサイトが開きます。該当のサイトの管理または表示が可能かどうかは、権限によって異なります。
- **鍵**のアイコン(🔑)をクリックすると、サイトに割り当てられているキーコードが表示されます。[**コピー**]をクリックすると、コードがクリップボードにコピーされます。
- **アクション**ボタン(⋮)をクリックすると、サブスクリプションを管理する方法を選択できます。
    - [**設定**]ボタン(⚙): サブスクリプションの設定を変更できます。
    - [**試用を開始する**]: このオプションは、サイトで当該のサブスクリプションを有効にしたことがない場合に表示されます。クリックすると、本製品と機能が同じで30日間無料の体験版の試用を開始できます。
    - [**アップグレード**]: このオプションは、体験版のサブスクリプションを試用している場合に表示されます。クリックすると、有料サブスクリプションにアップグレードされます。
    - [**購入**]: このオプションは、サブスクリプションが期限切れの場合に表示されます。クリックすると、サブスクリプションが更新されます。
    - [**再有効化**]: このオプションは、サブスクリプションが無効になっている場合に表示されます。クリックすると、サブスクリプションが再び有効化されます。
    - [**レガシーコンソール**]ボタン(🔗): **Endpoint Protection**または**Security Awareness Training**のサブスクリプションで、Endpoint Protectionのレガシーコンソールにアクセスできる場

合に表示されます。[開く]をクリックすると、レガシーコンソールが開きます。レガシーコンソールで[**サイトに戻る**]をクリックすると、最新のインターフェイスに戻ることができます。

- 列を**並べ替える**には、その列の見出しをクリックします。
- [**行と改ページ**]コントロールを使用すると、1ページの表示を増減したり、ページ間を移動したりできます。

# 特定のサイトの表示

1. [**サイトリスト**]ページを開きます。
2. [**サイト名**]のリンクをクリックします。タブの付いたサイトページが開きます。




- サイトページでは、上部のサイトスイッチャーを使用してサイトを切り替えることができます。
- [**概要**]タブには、このサイトに関連するデバイス、状態、管理者の概要が表示されます。
  - [**対応が必要なデバイス**]: このタイルの[**デバイスを表示**]リンクは、対応が必要なデバイスが少なくとも1つある場合にのみ表示されます。リンクをクリックすると、[**事業体**]ページが開きます。詳細は『』の「*事業体* ページ 31」を参照してください。
  - [**管理者**]: このタイルで[**編集**]をクリックすると、サイトの管理者を変更できます。詳細は『』の「*管理タスク* ページ 92」を参照してください。
  - [**保護の一時停止**]: このタイルで[**一時停止**]をクリックすると、サイトのすべての保護が一時停止されます。
    - この操作を行うと、エージェントはインストールされたままになりますが、感染は解決されません。
    - DNSプロテクションエージェントを使用している場合、エージェントはDNSリクエストのフィルタリングを停止し、すべてのDNS設定が元の設定に戻されます。
    - Webroot DNSリゾルバーは、そのサイトで登録されたIPアドレスからのDNSリクエストへの応答を停止します。
    - エンドポイントプロテクションの一時停止したサイトへの請求は、エージェントがアンインストールまたは非アクティブ化されない限り、アクティブなサイトと同様に継続されます。DNSプロテクションの場合、請求は継続されません。

- [**保護の再開**]: このタイルで[**再開**]をクリックすると、一時停止された保護が再開されます。
    - 感染の解決が開始されます。
    - DNSプロテクションを使用している場合、フィルタリングが再開し、エージェントが有効になります。またDNSサーバーが登録されたIPアドレスからのリクエストを解決し、ポリシー設定に従ってDNSトラフィックが処理されます。
- [**サイトの非アクティブ化**]: このタイルで[**サイトの非アクティブ化**]をクリックすると、サイトのキーコードが非アクティブ化されます。
    - この処理は恒久的なものであり、元に戻せないことに注意してください。
    - このアクションにより、そのキーコードを使用するすべてのデバイスにアンインストールコマンドが送信されます。
    - 非アクティブ化したサイトへの請求は行われません。
- [**サイトを削除**]: このタイルで[**サイトを削除**]をクリックすると、非アクティブ化されたサイトがコンソールから削除されます。
    - この処理は恒久的なものであり、元に戻せないことに注意してください。
    - このサイトのデータは表示できなくなります。

- [**詳細**]タブには、サイトの作成時に設定したサイトの詳細が表示されます。必要に応じて設定を変更します。
    - [**サイト/会社名**]: サイトまたは会社の一意の名前です。
    - [**サイトの種類**]:
        - [**外部企業**]: 管理している外部企業です。
        - [**社内サイト**]: 店舗やオフィスなど、自社内にあるサイトです。
    - [**会社の規模**] (外部企業のみ): 会社の規模を表す範囲を選択します。
    - [**会社の業種**] (外部企業のみ): 会社の業種を選択します。
    - [**支払請求サイクル**] (外部企業のみ): このサイトで必要に応じて定義および使用する支払請求サイクルです。これは参考用で、Webrootアカウントには関連付けられていません。
    - [**支払請求日**] (外部企業のみ): このサイトで必要に応じて定義および使用する支払請求日です。これは参考用で、Webrootアカウントには関連付けられていません。
    - [**配信先リスト**]: スケジュールレポートを受け取れる電子メールアドレスをコンマで区切って最大10個指定します。新しいレポートをスケジュールする場合は、[**各サイトの配信先リストに送信**]を選択して、関連するすべての電子メールアドレスがレポートを受信できるようにします。
    - [**グローバルポリシーの追加**]:
        - 有効にすると、このサイトですべてのグローバルポリシーを使用できます。一度有効にすると、このオプションは変更できません。
        - 無効にする場合は、サイトごとに個別のポリシーを作成する必要があります。

- [**グローバルオーバーライドの追加**]:
    - 有効にすると、グローバルオーバーライドがこのサイトに適用されます。たとえば、あるサイトで特定のファイルを許可し、それをグローバルオーバーライドとして設定すると、このオプションが有効になっているすべてのサイトがそのファイルを許可します。一度有効にすると、このオプションは変更できません。
    - 無効にする場合は、サイトごとに個別のオーバーライドを作成する必要があります。
- [**コメント**] (オプション): サイトまたは会社を説明するコメントです。
- [**タグ**] (オプション): 検索のフィルタリングに便利なラベルです。サイトにカスタムタグを追加すると、そのタグを使用して[**サイトリスト**]をフィルタリングできます。サイトにカスタムタグを適用するには、各タグの後ろの[**タグ**]ボックスにタグ名を入力してEnterを押します。

- [**管理者権限**]タブには、サイトにアクセスできるユーザーが表示されます。
    - 管理者のリストには、サイトへのアクセス権限([**管理者**]、[**表示のみ**]、[**アクセス不可**]のいずれか)が付与されているユーザーが表示されます。
    - 必要に応じて、各管理者の権限を変更します。
- [**エンドポイント保護**]タブには、サブスクリプションの状態とデフォルトのサイト設定が表示されます。また、エージェントのインストールファイルのダウンロードリンクも含まれています。
    - [**サイトのシート数**]: 設定するサイトのエンドポイント数です。この設定は請求には使用されません。
    - [**デフォルトのエンドポイントポリシー**]: グループ、サイト、または会社からのポリシーを継承してポリシーが割り当てられていない限り、このサイトにインストールされたすべての新しいエンドポイントプロテクションデバイスに使用されます。インストール後に、デバイスが使用するポリシーを変更することができます。Webrootでは、デフォルトのエンドポイントポリシーのコピーを作成し、ベストプラクティスと特定のニーズに合わせて変更することを推奨しています。詳細は『』の「*Endpoint Protectionのポリシーのベストプラクティス* ページ 42」を参照してください。
        - [**推奨デフォルト設定**]: デスクトップおよびノートパソコンが対象です。
        - [**推奨DNS有効**]: [**推奨デフォルト設定**]と同様、デスクトップおよびノートパソコンが対象です。また、DNSプロテクションエージェントを自動インストールします。
        - [**推奨サーバーデフォルト設定**]: サーバー環境が対象です。リソースの使用率とサーバーへの影響の最小化に重点を置いています。
        - [**サイレント監査**]: エンドポイントプロテクションを透過的に使用できます。検出事項を報告しますが、感染を修復しません。ポリシーのテスト用として、本番環境への影響を最小限に抑えるようにできています。Webrootではこのポリシーの使用を、本番環境における潜在的な誤検出や競合の特定、および不明なソフトウェアの発見を目的として、初期設定中のような短時間に限定することを推奨しています。
        - [**管理対象外**]: ユーザーが各自の設定をエージェントのユーザーインターフェイスで編集できるようにします。それまで適用されていたポリシーや設定は継承されますが、ユーザーインターフェイスを表示するかどうかを除いて特に設定はありません。

        - テクニカルサポートやトラブルシューティングで、またポリシー管理が不要な場合に使用します。
        - エンドユーザーが直接制御できるローカルの非管理アプリケーションにエージェントを変換します。
        - 本番環境では使用しないでください。
      - ポリシー名の最初に[**レガシー**]の付いたポリシーには以前推奨されていたポリシー設定が含まれています。
    - ***データフィルタ***
      - コンソールに表示されるデータを表示または非表示にするには、データフィルタを適用します。
      - たとえば、[**2か月**]を選択すると、2か月間接続されていないすべてのデバイスが、このサイトに表示されるデータから除外されます。
      - データフィルタを適用すると、ページの読み込みのパフォーマンスは向上する場合がありますが、表示される内容は制限されます。
      - フィルタを適用または削除する場合、配備サイズと表示するデータの量によっては、データの更新に数分かかることがあります。
      - [**親設定を継承**]を選択すると、コンソールレベルで設定されたフィルタが継承されます。この設定は、[**設定**] > [***データフィルタ***] > [**データフィルタ**]ドロップダウンで確認できます。
    - [**エンドポイントプロテクションコンソールに進む**]: エンドポイントプロテクションのレガシーコンソールを開きます。レガシーコンソールで[**サイトに戻る**]をクリックすると、最新のインターフェイスに戻ることができます。
    - [**ソフトウェアのダウンロード**]: このセクションには、エンドポイントプロテクションエージェントのインストールファイルのリンクが含まれます。これらのリンクとファイルはサイトとキーコードに固有のものです。詳細は『』の「*エージェントの配備* ページ 84」を参照してください。
- [**DNSプロテクション**]タブで、DNSプロテクションを有効または無効にできます。
  - 有効にすると、そのサイトのDNSプロテクションの設定を行うことができます。詳細は『』の「*DNSプロテクション* ページ 101」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**]タブで、Security Awareness Trainingを有効または無効にできます。
  - 有効にすると、トレーニング対象とするユーザー(電子メールアドレス)を含むドメインを特定することで、ユーザーをトレーニングの対象にすることができます。
  - ドメインの識別にはAzure Active Directory統合または手動プロセスを使用できます。詳細は『』の「*Security Awareness Training* ページ 115」を参照してください。

# 事業体

**事業体**は管理コンソールを使用して管理できるデバイスやグループです。

- **デバイス**はエージェントインストールです。
- **グループ**はデバイスをまとめて管理できる組織単位です。たとえば、特定のポリシーをデバイスのグループに適用できます。

## 使用可能な事業体の表示

[**事業体**]タブでは、デバイスおよびグループを表示、整理、管理できます。

使用可能な管理者を表示するには、[**管理者**] > [**事業体**]をクリックします。

- **法人向けの表示**の場合、事業体の表には、グループのリストや各グループ内のデバイスが表示されます。
- **MSP向けの表示**の場合、事業体の表には、サイトのリストが表示されます。サイトを展開すると、グループやデバイスを表示できます。

サイトまたはグループを選択すると、各デバイスの概要を表示できます。

- デバイスが保護されているかどうかをすばやく確認できます。
- 過去7日以内にチェックインされていないデバイスは、最近確認されていないデバイスとして識別されます。
- 非アクティブにされているデバイスは、別の**非アクティブ化済みデバイス**のグループに表示されます。
    - デバイスを再アクティブ化し、以前のグループに復元するには、デバイス名の横にあるチェックボックスをオンにしてから[**再アクティブ化**]をクリックします。また、エージェントも再インストールする必要があります。
- グループ内のデバイスを表示する場合、[**デバイス名**]の横にある以下のアイコンで、デバイスの種類をすばやく特定できます。
    - **Windows**のアイコン( ): Windowsデスクトップ
    - **サーバー**のアイコン( ): Windowsサーバー
    - **Apple**のアイコン( ): MacOSデスクトップ
    - **ロケーション**のアイコン( ): IPアドレス
- ポリシー名の横にあるアイコンによって、デバイスに割り当てられているポリシーを識別できます。このアイコンにカーソルを合わせると、完全なポリシー名と割り当て方法が表示されます。
    - **モニター**のアイコン( ): ポリシーはデバイスに直接割り当てられます。
    - **建物**のアイコン( ): ポリシーは、サイトポリシーを使用しているデバイスに割り当てられます。
    - **接続ボックス**のアイコン( ): ポリシーは、グループポリシーを使用しているデバイスに割り当てられます。
    - **Iの文字付きの円**のアイコン( ): デバイスに複数のポリシーが割り当てられています。
- デバイス名の上にカーソルを合わせると、鉛筆のアイコン( )が表示されます。

    - デフォルトでは、デバイスのホスト名が表示されます。[**編集**]アイコン(  )をクリックすると、割り当てられたデバイス名を、より直感的でユーザーフレンドリーな名前に変更できます。
    - これにより、[**事業体**]ページとコンソール内の他のすべての場所に表示されるデバイス名が変更されます。
- デバイスの隔離ステータスは、デバイス名の後に表示されます。
    - **隔離は**ロックアイコン  で示されます。
    - **隔離保留と隔離解除保留は、**砂時計のアイコン  で示されます。

[**事業体**]ページの上部から、以下のアクションを利用できます。

- **MSP向けの表示**の場合、[**検索**]ボックスに検索テキストを入力すると、そのテキストを含む行のみをリストに表示できます。
    - 検索では、表示されている行だけでなく表全体が対象になります。
    - 適用された検索語、フィルタ、並べ替え設定は、手動でリセットするかコンソールからログアウトするまで、コンソール内の他のページに移動しても保持されます。
- [**エージェントコマンド**]をクリックすると、選択したデバイスで特定の機能を実行できます。[エージェントコマンド]は、デバイスに割り当てられているポリシーで定義されたポーリング間隔に基づいて実行されます。
    - WindowsとAppleのアイコンは、それぞれのOSに適用されるコマンドであることを示しています。
    - エンドポイントプロテクションの[**最も人気**]コマンドは、リストの一番上に表示されます。
        - [**スキャン**]: コマンドの受信後、選択したデバイスのスキャンを開始します。
        - [**クリーンアップ**]: コマンドの受信後、デバイスのスキャンを開始して悪意のあるファイルを隔離します。スキャンが完了すると、[**スキャン履歴**]に結果が表示されます。
        - [**アンインストール**] (エンドポイントプロテクションとDNSプロテクション): 選択したデバイスからエージェントを削除します。デバイスが、DNSプロテクションをインストールするように設定されたエンドポイントプロテクションのポリシーを使用している場合、次回のデバイスのチェックイン時にDNSプロテクションがインストールされます。
        - [**デバイスを非アクティブ化**] (エンドポイントプロテクションおよびDNSプロテクション): 選択したデバイスからエージェントをアンインストールします。また、デバイスは割り当てられたグループから[**非アクティブ化済みデバイス**]に移動されます。
        - [**キーコードを変更**]: 選択したデバイスのキーコードを、入力されたキーコードに変更します。
        - [**すべてのファイルとプロセスを再検証する**]: 次回のスキャン実行時に、選択したデバイスのすべてのファイルとプロセスを検証します。このオプションは、手動のオーバーライドを作成し、選択したデバイスを強制的に変更する場合に便利です。
        - [**ファイルを復元**]: 許可する必要があるファイルが誤検出された場合などに、隔離されているファイルを復元します。
        - [**カスタマーサポートスクリプトを実行**]: デバイスを更新または感染を除去するため、カスタマーサポートから提供されたスクリプトを実行します。

- [**システム最適化ツール**]: コマンドの受信後、システム最適化ツールのプロセスを開始します。
- **デバイスの再起動**は、選択したデバイスに再起動コマンドを送信します。デバイスがコマンドを受信すると、ユーザーに通知することなく即座に再起動が行われます。
- **デバイスの隔離**は、管理コンソールとの通信を除き、デバイスへのすべての内部および外部ネットワークトラフィックがブロックされます。マルウェアに感染している可能性のあるデバイスをすべてのネットワークから切り離し、感染の可能性を最小限に抑えるのにこのコマンドを使用します。詳しくは、*デバイスの隔離と隔離解除* ページ 81を参照してください。
    - **デバイスの隔離**コマンドを送信するには、デバイスがPC Agent 9.0.36.40以降、またはMac Agent 9.6.4以降を実行している必要があります。
- **デバイスの隔離解除**は、デバイスへの内部および外部ネットワークトラフィックのブロックをすべて解除します。
    - **デバイスの隔離解除**コマンドを送信するには、デバイスがPC Agent 9.0.36.40以降、またはMac Agent 9.6.4以降を実行している必要があります

- [**すべてのコマンドを表示**]をクリックすると、利用可能なすべてのコマンドが表示されます。特定のコマンドを検索するには、**検索**ボックスを使用します。
    - [**アプリケーションを許可**]: 選択したデバイスでアプリケーションを実行できます。
    - [**ファイアウォールによりブロックされたプロセスを許可**]: ファイアウォールのポリシー設定によりブロックされたすべてのプロセスについて通信を許可します。詳細は「*ファイアウォール* ページ 63」を参照してください。
    - [**スキャン時間を変更**]: 選択したデバイスでエージェントが日次スキャンを実行する時刻を変更します。
    - [**ログファイルを消去**]: 現在のログファイルを消去して、選択したデバイス上の領域を解放します。
    - [**すべてのアイテムを正当と見なす/拒否されているすべてのアプリケーションを許可**]: 選択したデバイスで検出されたすべてのファイルを安全であるとタグ付けし、以前はブロックされていたすべてのアプリケーションを実行できるようにリセットします。
    - [**カスタマーサポートの診断**]: ユーティリティを実行して、感染したデバイスに関する情報を収集し、結果をWebrootサポートチームに送信します。
    - [**アプリケーションを拒否**]: 選択したデバイスでアプリケーションを実行できないようにブロックします。
    - [**プロキシ設定を無効化**]: 選択したデバイスで有効になっていたプロキシ設定をすべて無効にします。インターネットアクセスがプロキシサーバーを介したものだけである場合、デバイスはインターネットと通信できなくなります。
    - [**エンドポイントをロック**]: ログイン画面を起動して、選択したデバイスをロックします。再びログインする際は、ユーザー名とパスワードを入力する必要があります。
    - [**ログオフ**]: セッションを終了し、現在のアカウントからユーザーをログオフします。
    - [**アプリケーションを保護**]: 選択したデバイスで実行されている特定のアプリケーションにセキュリティレイヤーを追加します。

- [**パスワード保護を削除**]: インストール時にWebrootのアンインストールパスワードが設定されている場合、そのパスワードを解除します。
- [**デスクトップの壁紙をリセット**]: デスクトップの壁紙をデフォルト設定にリセットします。この変更を適用するにはデバイスを再起動する必要があります。このオプションは、デバイスが最近マルウェアに感染したことでデスクトップの壁紙が変更された場合に便利です。
- [**スクリーンセーバーをリセット**]: スクリーンセーバーをデフォルト設定にリセットします。この変更を適用するにはデバイスを再起動する必要があります。このオプションは、デバイスが最近マルウェアに感染したことでデスクトップのスクリーンセーバーが変更された場合に便利です。
- [**システムポリシーをリセット**]: タスクマネージャーを開くなど、Windowsの管理機能を使用できないようにする可能性のあるレジストリのシステムポリシーをリセットします。このオプションは、デバイスが最近マルウェアに感染したことで設定が変更された場合に便利です。
- [**[セーフモードとネットワーク]で再起動する**]: 選択したセーフモードのデバイスをネットワークで再起動します。
- [**フォルダをスキャン**]: 選択したデバイスの特定のフォルダをスキャンします。
- [**シャットダウン**]: 選択したデバイスを次回のレポート時にシャットダウンします。
- [**信頼できないプロセスの強制終了**]: 許可されていないプロセスすべてを終了させます。このオプションは、通常のスキャンでマルウェアと疑われるすべての痕跡を完全に削除できなかった場合に便利です。
- [**アプリケーションの保護を解除**]: 以前に保護したアプリケーションから追加のセキュリティを解除します。

- **コマンドログ**は、実行されたエージェントコマンドの履歴を表示します。コマンドログをCSV(カンマ区切り)ファイルにエクスポートできます。コマンドログでは、最近のコマンドや未処理のコマンドに関する情報を確認することができます。ログには以下のデータが含まれています:
  - **デバイス名** — コマンドを受信したエンドポイントの名前。
  - **コマンド** — エンドポイントに発行されたコマンド。
  - **パラメーター** — コマンドを実行するための追加パラメーター(フルパス名など)。
  - **送信日** — コマンドが管理コンソールから送信された日付。
    - **ステータス** — 以下のいずれかです:
    - **キャンセル済み** — 管理者がコマンドをキャンセルしました。
    - **保留中** — エージェントはまだコマンドを受信していません。
    - **期限切れ** — コマンドをエージェントに配信できませんでした。
    - **配信済み** — コマンドはエージェントに配信されました。
  - **アクション** — 以下のいずれかのアクションを実行できます:

        - **キャンセル**—「保留」ステータスのコマンドをキャンセルします。
        - **再試行** — 同じコマンドを再度送信します。これは、「キャンセル済み」「期限切れ」「完了」ステータスのコマンドにのみ利用できます。
- [**移動**]により、選択したデバイスを別のグループに移動できます。
    - **MSP向けの表示**を使用している場合は、グループが同じサイト内にある必要があります。
    - デバイスのポリシーを、移動先のグループに割り当てられたポリシーに更新するか、現在使用しているポリシーを維持するかを指定します。
- [**ポリシーを変更**]: 選択したデバイスに割り当てられているポリシーを変更できます。
- **エクスポート**は、**エンティティ**テーブルの現在のビューを含む.CSVレポートをダウンロードするためのリンクを含むメールを送信するので、ローカルでデータを扱うことができます。
- **フィルター**は、フィルターパネルを開きます。
    - **フィルター**ボタン上の緑色の丸と数字は、現在適用されているフィルターの数を示しています。
    - [**フィルタ**]ボタンにある緑色の円に囲まれた数値は、現在適用されているフィルタの数を示します。
    - フィルタパネルでセクションを展開すると、利用可能なフィルタが表示されます。
    - フィルタの右側にある[**除外**]リンクをクリックすると、そのフィルタが除外され、グループ内の残りのフィルタが選択されます。
    - 適用したフィルタは手動でリセットするかコンソールからログアウトするまで、コンソール内の他のページに移動しても保持されます。
    - 1つのフィルタグループの選択をすべて手動で削除するには、[**リセット**]をクリックします。
    - すべてのフィルタを削除するには、パネル下部の[**フィルタをリセット**]をクリックします。
- **列のカスタマイズ**ボタン  では、**エンティティ**テーブルの列のビューをカスタマイズできます。*テーブルビューのカスタマイズ* ページ 36を参照してください。

## テーブルビューのカスタマイズ

**列 のカスタマイズ**ボタン  では、**エンティティ**テーブルの列 のビューをカスタマイズできます。

**「エンティティ」テーブルビューをカスタマイズするには:**

1. **列 のカスタマイズ**ボタン  をクリックします。
2. 開いた**列 のカスタマイズ**パネルで、各 データポイント の横 にあるチェック ボックスを選 択して、そのデータポイントを**エンティティ**テーブルに含 めるかどうかを選 択します。
3. 各 データポイント の横 にある二 重 線 ＝ アイコンをドラッグすると、表 に表 示 される列 の順 序 を並 べ替えることができます。
4. **適 用**をクリックして変 更 を保 存します。

カスタムビューは、他 のページに移 動したり、コンソールからログアウトした後 も保 持 されます。テーブルビューをデフォルトビューに戻 すには、**列 のカスタマイズ**パネルで**デフォルト にリセット**をクリックします。

# 特定の事業体の表示

1. [**管理**] > [**事業体**]をクリックします。
    - **MSP向けの表示**の場合、管理するデバイスを含むサイトを選択します。
    - **法人向けの表示**の場合、管理するデバイスを含むグループを選択します。
2. **名前**列で、デバイスをクリックします。タブ付きページからデバイス**サマリー**タブが開きます。

    デバイス**サマリー**タブでは、選択したデバイスの上位レベルの情報を表示し、以下のアクションを実行できます:

    - デフォルトでは、デバイスのホスト名が表示されます。割り当てられたデバイス名をより直感的な、またはユーザーフレンドリーなものに変更するには、デバイス名の後にある**編集**をクリックします。
        - これにより、[**事業体**]ページとコンソール内の他のすべての場所に表示されるデバイス名が変更されます。
        - • デバイス名を元の名前に戻すには**元のホスト名に戻す**をクリックします。
    - [**エージェントコマンド**]は、デバイスに割り当てられているポリシーで定義されたポーリング間隔に基づいて実行されます。
        - WindowsとAppleのアイコンは、それぞれのOSに適用できる固有のコマンドであることを示しています。
        - エンドポイントプロテクションの[**最も人気**]コマンドは、リストの一番上に表示されます。
            - [**スキャン**]: コマンドの受信後、選択したデバイスのスキャンを開始します。
            - [**クリーンアップ**]: コマンドの受信後、デバイスのスキャンを開始して悪意のあるファイルを隔離します。スキャンが完了すると、[**スキャン履歴**]に結果が表示されます。
            - [**アンインストール**] (エンドポイントプロテクションとDNSプロテクション): 選択したデバイスからエージェントを削除します。
            - [**デバイスを非アクティブ化**] (エンドポイントプロテクションおよびDNSプロテクション): 選択したデバイスからエージェントをアンインストールします。また、デバイスは割り当てられたグループから[**非アクティブ化済みデバイス**]に移動されます。
            - [**キーコードを変更**]: 選択したデバイスのキーコードを、入力されたキーコードに変更します。
            - [**すべてのファイルとプロセスを再検証する**]: 次回のスキャン実行時に、選択したデバイスのすべてのファイルとプロセスを検証します。このオプションは、手動のオーバーライドを作成し、選択したデバイスを強制的に変更する場合に便利です。
            - [**ファイルを復元**]: 許可する必要があるファイルが誤検出された場合などに、隔離されているファイルを復元します。
            - [**カスタマーサポートスクリプトを実行**]: デバイスを更新または感染を除去するため、カスタマーサポートから提供されたスクリプトを実行します。

- [**システム最適化ツール**]: コマンドの受信後、システム最適化ツールのプロセスを開始します。
- [**リセット**]: テクニカルサポートが特定の状況下で使用するツールです。このコマンドは、サポートなしでは実行しないでください。
- [**デバイスを再起動**]: 選択したデバイスに再起動のコマンドを送信します。デバイスがコマンドを受信すると、ユーザーに通知されることなく再起動が直ちに実行されます。

- [**すべてのコマンドを表示**]をクリックすると、利用可能なすべてのコマンドが表示されます。特定のコマンドを検索するには、検索ボックスを使用します。
  - [**アプリケーションを許可**]: 選択したデバイスでアプリケーションを実行できます。
  - [**ファイアウォールによりブロックされたプロセスを許可**]: ファイアウォールのポリシー設定によりブロックされたすべてのプロセスについて通信を許可します。詳細は「*ファイアウォール* ページ 63」を参照してください。
  - [**スキャン時間を変更**]: 選択したデバイスでエージェントが日次スキャンを実行する時刻を変更します。
  - [**ログファイルを消去**]: 現在のログファイルを消去して、選択したデバイス上の領域を解放します。
  - [**すべてのアイテムを正当と見なす/拒否されているすべてのアプリケーションを許可**]: 選択したデバイスで検出されたすべてのファイルを安全であるとタグ付けし、以前はブロックされていたすべてのアプリケーションを実行できるようにリセットします。
  - [**カスタマーサポートの診断**]: ユーティリティを実行して、感染したデバイスに関する情報を収集し、結果をWebrootサポートチームに送信します。
  - [**アプリケーションを拒否**]: 選択したデバイスでアプリケーションを実行できないようにブロックします。
  - [**プロキシ設定を無効化**]: 選択したデバイスで有効になっていたプロキシ設定をすべて無効にします。インターネットアクセスがプロキシサーバーを介したものだけである場合、デバイスはインターネットと通信できなくなります。
  - [**エンドポイントをロック**]: ログイン画面を起動して、選択したデバイスをロックします。再びログインする際は、ユーザー名とパスワードを入力する必要があります。
  - [**ログオフ**]: セッションを終了し、現在のアカウントからユーザーをログオフします。
  - [**アプリケーションを保護**]: 選択したデバイスで実行されている特定のアプリケーションにセキュリティレイヤーを追加します。
  - [**パスワード保護を削除**]: インストール時にWebrootのアンインストールパスワードが設定されている場合、そのパスワードを解除します。
  - [**デスクトップの壁紙をリセット**]: デスクトップの壁紙をデフォルト設定にリセットします。この変更を適用するにはデバイスを再起動する必要があります。このオプションは、デバイスが最近マルウェアに感染したことでデスクトップの壁紙が変更された場合に便利です。

- [**スクリーンセーバーをリセット**]: スクリーンセーバーをデフォルト設定にリセットします。この変更を適用するにはデバイスを再起動する必要があります。このオプションは、デバイスが最近マルウェアに感染したことでデスクトップのスクリーンセーバーが変更された場合に便利です。
- [**システムポリシーをリセット**]: タスクマネージャーを開くなど、Windowsの管理機能を使用できないようにする可能性のあるレジストリのシステムポリシーをリセットします。このオプションは、デバイスが最近マルウェアに感染したことで設定が変更された場合に便利です。
- [**[セーフモードとネットワーク]で再起動する**]: 選択したセーフモードのデバイスをネットワークで再起動します。
- [**フォルダをスキャン**]: 選択したデバイスの特定のフォルダをスキャンします。
- [**シャットダウン**]: 選択したデバイスを次回のレポート時にシャットダウンします。
- [**信頼できないプロセスの強制終了**]: 許可されていないプロセスすべてを終了させます。このオプションは、通常のスキャンでマルウェアと疑われるすべての痕跡を完全に削除できなかった場合に便利です。
- [**アプリケーションの保護を解除**]: 以前に保護したアプリケーションから追加のセキュリティを解除します。
- [**コマンドログ**]: 実行されたエージェントコマンドの履歴を表示します。コマンドログはCSV (コンマ区切りファイル)にエクスポートできます。

- [**ポリシーを変更**]: 選択したデバイスに割り当てられているポリシーを変更できます。

他のタブをクリックすると、デバイスの詳細をドリルダウンできます。

- [**検出された脅威**]: このタブには、脅威を特定する2つの表があります。
  - [**ファイル脅威の検出**]: この表には、検出した脅威ファイルが表示されます。ファイル名をクリックすると、ファイルおよび検出されたマルウェアの詳細が表示されます。
  - [**Evasion Shieldスクリプト検出**]: この表には、回避シールドで検出されたスクリプト脅威が表示されます。スクリプト名をクリックすると、検出したスクリプトの詳細が表示されます。
  - [**アクション**]をクリックすると、特定のファイルを以下のとおり変更できます。
    - [**許可リストにファイルを追加**]: 選択したファイルを許可リストの項目として新たに追加できます。
    - [**隔離先から復元**]: 隔離先からファイルを削除し、元の場所に復元します。
  - [**実行可能検出ノート**]は、ポリシー設定に従って、脅威が検出および修復された場合に表示されます。
    - 次回のスケジュールスキャン後、ステータスは自動的に[保護]に更新されます。
    - [**クリーンアップ**]をクリックすると、デバイスのスキャンが直ちに開始され、悪意のあるファイルが隔離されます。
    - スキャンが完了すると、[**スキャン履歴**]に結果が表示されます。
- [**Web Threat Shieldのブロック**]: このタブには、Web脅威シールドによってブロックされたURLが表示されます。

        - [**アクション**]をクリックし、[**許可リストにURLを追加**]を選択すると、Webオーバーライドリストに新しい事業体が作成されます。
    - [**DNSプロテクション**] (DNSプロテクションが有効な場合): このタブには、ブロックされたドメイン、ユーザー、およびブロックされた理由に関する情報が表示されます。
        - [**アクション**]をクリックし、[**許可リストにURLを追加**]を選択すると、Webオーバーライドリストに新しい事業体が作成されます。
    - [**スキャン履歴**]: このタブには、デバイスのスキャンの履歴が表示されます。スキャン中に脅威が検出された場合は、表の行を展開して脅威の詳細を表示します。
        - [**ファイル名**]をクリックすると、ファイルおよび検出されたマルウェアの詳細が表示されます。
        - [**アクション**]をクリックすると、特定のファイルを以下のとおり変更できます。
            - [**許可リストにファイルを追加**]: このファイルを許可されたファイルとして指定します。
            - [**隔離先から復元**]: 隔離先からファイルを削除し、元の場所に復元します。
    - **プロセスログ**は、指定した時間枠内にログに記録されたエンドポイントイベントに関する上位レベルの情報を表示します。

## グループの管理

グループは、デバイスをまとめて管理できる組織単位です。たとえば、特定のポリシーをデバイスのグループに適用できます。

エージェントが配備されると、すべてのデバイスは[**デフォルトのグループ**]に自動的に割り当てられます。グループを作成してカスタマイズすることで、それぞれのデバイスを異なる方法で管理できます。

[**サイト&グループ**](**マネージドサービスプロバイダー (MSP) 向けの表示**)または[**グループ**](**ビジネス向けの表示**)のリストの上部から以下のアクションを利用できます。

- [**グループを作成**]ボタン  をクリックすると、選択したサイトに対して新しいグループを作成できます。**マネージドサービスプロバイダー (MSP) 向けの表示**では、新しいグループを作成するためにサイトを選択する必要があります。
- [**グループを削除**]ボタン  をクリックすると、選択したグループを削除できます。削除するグループに存在するデバイスを移動するには、新しいグループを指定する必要があります。
- [**グループを編集**]ボタン  をクリックすると、グループの名前またはグループに割り当てられたポリシーを変更できます。
- [**このグループにデバイスをインストール**]ボタン  をクリックすると、選択したグループに直接デバイスを配備する方法を確認できます (エンドポイントプロテクションのみ)。画面の指示に従ってインストーラーをダウンロードして実行します。デバイスは、選択したグループに割り当てられているポリシーを自動的に継承します。

**デバイスを新しいグループに移動させるには、以下の手順に従います。**

1. ナビゲーションペインで[**事業体**]をクリックします。
2. [**事業体**]ページで、新しいグループに移動させるデバイスを1つ以上選択します。

3. [**移動**]をクリックします。
    - **MSP向けの表示**を使用している場合は、グループが同じサイト内にある必要があります。
    - デバイスのポリシーを、移動先のグループに割り当てられたポリシーに更新するか、現在使用しているポリシーを維持するかを指定します。

# ポリシー

**ポリシー**はエージェントの動作を定義するものです。エンドポイントプロテクションとDNSプロテクションのシステムポリシーは編集できません。エンドポイントプロテクションの管理対象外ポリシーでは、エージェント側で独自の設定を選択して管理できます。

- [**グローバル**]および[**サイト**]ポリシーは編集、コピー、削除できます。ポリシーの[**名前**]の横に[**編集可能**]アイコンがあるポリシーは編集できます。
- [**システム**]ポリシーは表示またはコピーできます。

ポリシーの設定時には、推奨されるベストプラクティスを確認することをお勧めします。詳細は「*Endpoint Protectionのポリシーのベストプラクティス* ページ 42」を参照してください。

## Endpoint Protectionのポリシーのベストプラクティス

Endpoint Protectionのデフォルトのポリシーは全体的な基本ポリシーと見なされますが、ポリシーの割り当て先であるグループの特定のニーズを満たすために、これらのポリシーを変更する必要があります。自社独自の要件を常に優先してください。

必要なポリシーを作成する際には、以下のベストプラクティスを検討してください。

- **名前**: ポリシーの名前がわかりやすいものであることを確認します。複数のポリシーがある場合、各ポリシーで有効になっている設定の種類をすばやく特定できるようなわかりやすい名前を付けると便利です。また、ブロックされているアプリケーションやWebサイトを含めることもできます。
- **論理グループと特殊な状況**: 主な論理グループは何か。一部のグループをより小さなグループに分割する必要があるか。異なるポリシー設定が必要な役割は何か。シャットダウンを許可するマシンとシャットダウンできないマシンでは異なるポリシー設定が必要か。また、一部の論理グループについて、アプリケーションやWebサイトをブロックする必要があるかどうかを確認します。
- **人とコンピュータ**: 経営幹部と経営幹部でない従業員、ワークステーションとサーバー、さまざまな部門、部門内のさまざまな役職に対して、異なるポリシーが必要になる場合があります。

さまざまな種類の事業体に推奨されるベストプラクティスを以下に示します。繰り返しになりますが、自社独自の要件を常に優先してください。

- **ワークステーション**: 組織内のワークステーションのポリシーを作成する場合は、[**推奨デフォルト設定**]のポリシーのコピーを作成し、以下の設定をそれぞれ変更します。
    - **スキャン設定**
        - [**学習スキャンで検出された脅威を自動的に削除する**]を[**オン**]にすると、学習スキャン中に検出された脅威を削除することで、クリーンなベースラインが作成されます。マシンがクリーンになると、Endpoint Protectionでは変更されたものだけをすばやくチェックできます。
- **サーバー**: 直接アクセスされないサーバーのポリシーを作成する場合は、[**推奨サーバーデフォルト設定**]のポリシーのコピーを作成し、以下の各設定を変更します。
    - **スキャン設定**
        - [**学習スキャンで検出された脅威を自動的に削除する**]を[**オン**]にすると、学習スキャン中に検出された脅威を削除することで、クリーンなベースラインが作成されます。マシン

がクリーンになると、Endpoint Protectionでは変更されたものだけをすばやくチェックできます。

- **リアルタイムシールド**
  - [**書き込みまたは変更時にファイルをスキャンする**]オプションを[**オン**]に設定します。このオプションを使用すると、特にバックドアの脅威(安全なドキュメントファイルと思われるファイルに埋め込まれた悪意のあるマクロなど)の侵入を防ぐことができます。

- **RDS/ターミナルサーバー**: 直接アクセスされるサーバーのポリシーを作成する場合は、[**推奨サーバーデフォルト設定**]のポリシーのコピーを作成し、以下のそれぞれの設定を変更します。
  - **基本設定**
    - [**SecureAnywhereをスタートメニューに表示する**]を[**オフ**]に設定します。このオプションを無効にすると、[**スタート**]メニューからのアクセスに対するEndpoint Protectionの保護が強化されます。この設定は、複数名がサーバーにアクセスする場合に特に重要です。
    - [[**プログラムの追加と削除**]パネルに**SecureAnywhereを表示する**]を[**オフ**]に設定します。このオプションを無効にすると、アンインストールに対するEndpoint Protectionの保護が強化されます。この設定は、複数名がサーバーにアクセスする場合に特に重要です。
  - **スキャン設定**
    - [**アーカイブファイルをスキャンする**]を[**オン**]に設定します。これにより、サーバーをより完全に保護できます。
    - [**学習スキャンで検出された脅威を自動的に削除する**]を[**オン**]にすると、学習スキャン中に検出された脅威を削除することで、クリーンなベースラインが作成されます。マシンがクリーンになると、エンドポイントプロテクションでは変更されたものだけをすばやくチェックできます。
  - **リアルタイムシールド**
    - [**書き込みまたは変更時にファイルをスキャンする**]オプションを[**オン**]に設定します。このオプションを使用すると、特にバックドアの脅威(安全なドキュメントファイルと思われるファイルに埋め込まれた悪意のあるマクロなど)の侵入を防ぐことができます。

# 使用可能なポリシーの表示

エンドポイントプロテクションおよびDNSプロテクションのポリシーを操作するには、[**管理**] > [**ポリシー**]をクリックします。

**MSP向けの表示**で作業している場合、ポリシーは**グローバル**レベルまたは**サイト**レベルのいずれかで作成できます。

- [**グローバル**]および[**サイト**]ポリシーは編集、コピー、削除できます。ポリシーの[**名前**]の横に[**編集可能**] アイコンがあるポリシーは編集できます。
- [**システム**]ポリシーは表示またはコピーできます。

[**エンドポイントプロテクション**]タブおよび[**DNSプロテクション**]タブの[**ポリシー**]ページの上部から、以下のアクションボタンを使用できます。

- [**ポリシー**]ドロップダウンメニューをクリックすると、[**ポリシー**]の表に以下のとおり表示される結果の範囲を選択できます。
    - グローバルポリシーは、アクセスできるすべてのサイトに適用されます。
    - [**サイト**]リストで特定のサイトを選択すると、そのサイトに関連付けられたポリシーを表示および管理できます。
- 表の結果をさらに絞り込むには[**検索**]ボックスを使用します。
- 新しいポリシーを作成するには、[**ポリシーを追加**]をクリックします。詳細は「*新しいポリシーの追加* ページ 45」を参照してください。
- 別のサイトまたはコンソールから既存のポリシーをインポートするには、[**ポリシーをインポート**]をクリックします。詳細は「*別のサイトからの既存ポリシーのインポート* ページ 46」を参照してください。

画面上部のタブはポリシーのタイプによって分類されます。

- [**エンドポイントプロテクション**]: このタブには、デフォルトのエンドポイントプロテクションシステムポリシーと、作成済みのすべてのグローバルポリシーが表示されます。
    - [**推奨デフォルト設定**]: デスクトップおよびノートパソコンが対象です。
    - [**推奨DNS有効**]: [**推奨デフォルト設定**]と同様、デスクトップおよびノートパソコンが対象です。また、DNSプロテクションエージェントを自動インストールします。
    - [**推奨サーバーデフォルト設定**]: サーバー環境が対象です。リソースの使用率とサーバーへの影響の最小化に重点を置いています。
    - [**サイレント監査**]: エンドポイントプロテクションを透過的に使用できます。検出事項を報告しますが、感染を修復しません。ポリシーのテスト用として、本番環境への影響を最小限に抑えるようにできています。Webrootではこのポリシーの使用を、本番環境における潜在的な誤検出や競合の特定、および不明なソフトウェアの発見を目的として、初期設定中のような短時間に限定することを推奨しています。
    - [**管理対象外**]: ユーザーが各自の設定をエージェントのユーザーインターフェイスで編集できるようにします。それまで適用されていたポリシーや設定は継承されますが、ユーザーインターフェイスを表示するかどうかを除いて特に設定はありません。
        - テクニカルサポートやトラブルシューティングで、またポリシー管理が不要な場合に使用します。
        - エンドユーザーが直接制御できるローカルの非管理アプリケーションにエージェントを変換します。
        - 本番環境では使用しないでください。
    - ポリシー名の最初に[**レガシー**]の付いたポリシーには以前推奨されていたポリシー設定が含まれています。
- [**DNSプロテクション**]: このタブには、DNSプロテクションがまだ有効になっていない場合、DNSプロテクションを有効にするためのスイッチが表示されます。DNSプロテクションが有効になっている場合は、デフォルトのDNSプロテクションポリシーと作成済みのすべてのグローバルポリシーが表示されます。
    - [**DNS保護レベル: 高**]: すべてのセキュリティカテゴリーおよび、人材の保護、問題あり/リーガルのコンテンツがブロックされます。
    - [**DNS保護レベル: 中**]: すべてのセキュリティカテゴリーおよび、人材の保護のコンテンツがブロッ

クされます。

- 詳細は「*DNSプロテクションのポリシーの管理* ページ 103」を参照してください。

[**エンドポイントプロテクション**]タブおよび[**DNSプロテクション**]タブの[**ポリシー**]ページから、以下の機能を利用できます。

- [**ポリシー名**]のリンクをクリックすると、ポリシー名を表示または編集できます。ユーザーが作成したポリシーのみ編集可能です。
- [**アクション**]列では、ポリシーを以下の方法で管理できます。
  - [**表示**]: デフォルトのポリシーに割り当てられているポリシー設定を確認できます。
  - [**コピー**]: 既存のポリシーをコピーできます。詳細は「*既存のポリシーのコピー* ページ 45」を参照してください。
  - [**編集**]: 作成、コピー、またはインポートしたポリシーに割り当てられているポリシー設定を編集できます。詳細は「*ポリシーの編集* ページ 46」を参照してください。
  - [**削除**]: ユーザーが作成したポリシーを削除できます。詳細は「*ポリシーの削除* ページ 47」を参照してください。
- ページの下部には[**ポリシーの使用状況**]指標が表示されます。

## 新しいポリシーの追加

1. [**管理**] > [**ポリシー**]を開きます。
2. [**エンドポイントプロテクション**]タブまたは[**DNSプロテクション**]タブで[**ポリシーを追加**]をクリックします。
   - 一意の**名前**と**説明**を入力します。各フィールドの文字数は最大50文字(英数字)です。
   - [**スコープ**]を選択し、**グローバル**ポリシーを含めるように設定されているサイトにポリシーを適用するか、選択した**サイト**だけに適用するかを指定します。設定した**スコープ**は後で変更できないことにご注意ください。
   - キャレット(^)をクリックすると、各セクションの設定を展開したり折りたたんだりすることができます。
   - 必要に応じて、デフォルトのポリシー設定を変更します。
3. 完了したら、[**保存**]をクリックします。

## 既存のポリシーのコピー

1. [**管理**] > [**ポリシー**]を開きます。
2. [**エンドポイントプロテクション**]または[**DNSプロテクション**]タブから、コピーするポリシーを選択します。
3. [**アクション**]の下にある[**コピー**]をクリックします。
   - 一意の**名前**と**説明**を入力します。各フィールドの文字数は最大50文字(英数字)です。
   - [**スコープ**]を選択し、**グローバル**ポリシーを含めるように設定されているサイトにポリシーを適用するか、選択した**サイト**だけに適用するかを指定します。設定した**スコープ**は後で変更できないことにご注意ください。

- キャレット (^)をクリックすると、各セクションの設定を展開したり折りたたんだりすることができます。
- 新しいポリシーは、コピーしたポリシーの設定に基づきます。
- 必要に応じて、ポリシーの設定を変更します。

4. 完了したら、[**保存**]をクリックします。

## ポリシー名の変更

1. [**管理**] > [**ポリシー**]を開きます。
2. [**エンドポイントプロテクション**]または[**DNSプロテクション**]タブから、名前を変更するポリシーを開きます。
3. [**名前**]フィールドに新しい名前を入力します。
   - 新しい名前は一意である必要があります。
4. 完了したら、[**保存**]をクリックします。

## 別のサイトからの既存ポリシーのインポート

別のサイトまたはコンソールから既存のエンドポイントプロテクションポリシーをインポートできます。

1. [**管理**] > [**ポリシー**]を開きます。
2. [**ポリシーをインポート**]をクリックします。
   - [**インポート**]ダイアログで、インポートするポリシーが含まれているコンソールまたはサイトを指定します。
   - インポートするポリシーを選択します。選択したサイトのポリシーのみがリストに表示されます。
   - ポリシーのインポート先となるコンソールまたはサイトを選択します。
   - インポートしようとするポリシーの名前がすでに存在する場合、ポリシーをインポートすることはできません。
3. [**ポリシーをインポート**]をクリックします。

インポート後のポリシーは、必要に応じて編集できます。

## ポリシーの編集

作成、コピー、またはインポートしたポリシーは編集できます。デフォルトのポリシーは編集できません。

1. [**管理**] > [**ポリシー**]を開きます。
2. [**エンドポイントプロテクション**]タブまたは[**DNSプロテクション**]タブで、[**ポリシー名**]のリンクをクリックします。
3. [**名前**]、[**説明**]、または[**ポリシー設定**]のいずれかを変更します。
   - キャレット (^)をクリックすると、各セクションの設定を展開したり折りたたんだりすることができます。
   - 各セクションを保存しながら作業します。
4. 各セクションの編集が完了したら、[**保存**]をクリックします。

## ポリシーの削除

作成、コピー、またはインポートしたポリシーは削除できます。デフォルトのポリシーは削除できません。削除するポリシーを使用しているデバイスは、別のポリシーに再割り当てする必要があります。

1. [**管理**] > [**ポリシー**]を開きます。
2. [**エンドポイントプロテクション**]または[**DNSプロテクション**]タブから、削除するポリシーを選択します。
3. [**アクション**]の下部にある[**削除**]をクリックします。
4. プロンプトが表示されたら、[**代替ポリシー**]を選択します。削除するポリシーを使用しているすべてのデバイスには、**代替ポリシー**が割り当てられます。
5. [**ポリシーを削除**]をクリックします。

## エンドポイントプロテクションのポリシー設定

ポリシーの最適な設定方法を判断するには、「*Endpoint Protectionのポリシーのベストプラクティス* ページ 42」を参照してください。

**エンドポイントプロテクションのポリシーを確認または変更するには、以下の手順に従います。**

1. [**管理**] > [**ポリシー**]を開きます。
2. [**エンドポイントプロテクション**]タブから、確認または変更するポリシーを選択します。
    - ポリシーを確認する場合、ページの下部に[**ポリシーの使用状況**]が表示されます。
    - ポリシーはすべてWindowsデバイスの操作時に使用できます。アスタリスク(*)が付いているポリシーは、Appleデバイスにも適用されます。

## 基本設定

基本設定のポリシーにより、エージェントの基本動作を制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| SecureAnywhereへのショートカットをデスクトップ上に表示する | Endpoint Protectionデスクトップショートカットをデスクトップで使用できます。 | Endpoint Protectionデスクトップショートカットはデスクトップで使用できません。 |
| システムトレイアイコンを表示する | Endpoint Protectionアイコンをシステムトレイ(タスクトレイ)で使用できます。 | Endpoint Protectionアイコンはシステムトレイ(タスクトレイ)で使用できません。 |
| 起動時にスプラッシュ画面を表示する | システムの起動時にEndpoint Protection画面が表示されます。 | システムの起動時にEndpoint Protection画面が表示されません。 |
| SecureAnywhereをスタートメニューに表示する | [**スタート**]メニューからEndpoint Protectionを利用できます。 | [**スタート**]メニューからEndpoint Protectionを利用できません。 |
| [プログラムの追加と削除]パネルにSecureAnywhereを表示する | Windowsのバージョンに応じて、Endpoint Protectionが[**プログラムの追加と削除**]または[**プログラムと機能**]に表示されます。 | Endpoint Protectionは[**プログラムの追加と削除**]にも[**プログラムと機能**]にも表示されません。 |
| Windowsアクションセンターに SecureAnywhereを表示する | Endpoint Protectionは、[**アクションセンター**]の[ウイルス対策]と[脅威に対する防止]に表示されます。 | Endpoint Protectionは、[**アクションセンター・セキュリティセンター**]に表示されません。 |
| 更新を自動的にダウンロードして適用する* | エージェントは、エンドユーザーに通知することなく、アップデートを自動的にダウンロードして適用します。 | エージェントはアップデートを自動的にダウンロードまたは適用しません。 |
| 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* | 非スキャン機能は、CPUリソースを節約するためにバックグラウンドで実行されます。 | すべてのEndpoint Protection機能はフォアグラウンドで実行されます。 |
| 詳細なロギングよりも低ディスク使用量を優先する | Endpoint Protectionのログは、最後の4つのログアイテムのみを保持します。 | Endpoint Protectionのログはすべてのログアイテムを保持します。 |
| 大量のリソースを使用する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* | エンドユーザーがゲームをしているとき、動画を見ているとき、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しているときに、Endpoint Protectionの機能が見送られます。 | Endpoint Protectionの機能は見送られません。 |

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| SecureAnywhereの手動シャットダウンを許可する* | システムトレイ(タスクトレイ)アイコンからEndpoint Protectionをシャットダウンできます。 | システムトレイ(タスクトレイ)からEndpoint Protectionをシャットダウンするオプションは使用できません。 |
| 重要でない通知をバックグラウンドに表示する | Endpoint Protectionの重要メッセージのみがシステムトレイ(タスクトレイ)に表示されます。情報メッセージは非表示になります。 | 重要メッセージと情報メッセージの両方がシステムトレイ(タスクトレイ)に表示されます。 |
| 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(タスクトレイ)のEndpoint Protectionのメッセージが、数秒後に自動的に表示されなくなります。 | エンドユーザーがシステムトレイ(タスクトレイ)のEndpoint Protectionのメッセージを閉じる必要があります。 |
| 実行履歴の詳細を保存する | データは[**実行履歴**]ログに保存されます。 | データは[**実行履歴**]ログに保存されません。 |
| ポーリング間隔* | エージェントがアップデートを確認する頻度を指定します。デフォルトの設定は1時間です。推奨設定は15分です。 | |

* Appleデバイスにも適用されます。

## スキャンのスケジュール

スキャンのスケジュールのポリシーにより、スキャンを実行するタイミングを制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| スケジュールスキャンを有効にする* | スキャンは定義されたスケジュールを使用して実行されます。 | スキャンは1日1回、ソフトウェアをインストールした時刻とほぼ同じ頃に実行されます(インストール時に実行し、次は約24時間後に実行します)。 |
| スキャン頻度* | デバイスをスキャンする頻度を指定します。 | |
| 時間* | デバイスをスキャンする時刻を指定します。時間間隔を選択するか、特定の時刻を選択できます。ランダム化の設定を有効にすると、選択した時間の前後にさらに1時間を追加できます。 | |
| 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* | スキャンがスケジュールされた時刻に実行されなかった場合、起動後1時間以内に実行されます。 | スキャンがスケジュールされた時刻に実行されなかった場合、スキャンはスキップされます。 |
| 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。 | スキャンの進捗状態がウィンドウに表示されます。 |
| 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 | 警告は、脅威が検出された場合のみに表示されます。 | 脅威が検出されなくても、スキャンが完了するとステータスウィンドウが表示されます。 |
| 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* | バッテリ電源のみを使用している場合、スキャンはスキップされます。 | スキャンはどの電源を使用しても実行されます。 |
| フル画面のアプリケーションまたはゲーム実行中はスケジュール スキャンを実行しない* | 映画やゲームなど、全画面表示のアプリケーションを使用しているときは、スキャンがスキップされます。 | 全画面表示のアプリケーションを使用しているときでも、スキャンが実行されます。 |
| 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 | スケジュールされた時刻から前後1時間以内にスキャンが実行されます。 | スキャンはスケジュールされた時刻に実行されます。スキャンを正確な時刻にスケジュールする必要がある場合は、この設定をオフにします。 |
| ディープスキャンではなくスケジュールされたクイックスキャンを実行する | メモリのクイックスキャンのみが実行されます。 | スキャンにより、マシン全体がチェックされます。 |

* Appleデバイスにも適用されます。

## スキャン設定ポリシー

スキャン設定ポリシーにより、スキャンの対象と実行方法を制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| 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 | OSの前に読み込まれるマスターブートレコードがスキャンされます。 | マスターブートレコードはスキャンされません。 |
| 拡張ルートキット検出を有効化する | エンドポイントプロテクションは、ディスクや保護されたシステム領域に隠されているルートキットおよびその他悪意のあるソフトウェアをスキャンします。これらはスパイウェアの開発者が検出と削除を回避するために作成したものです。 | エンドポイントプロテクションは、ルートキットおよびその他悪意のあるソフトウェアをスキャンしません。 |
| 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 | ファイルをすぐにスキャンするために、Windowsエクスプローラーで右クリックメニューを使用できます。 | 右クリックメニューは使用できません。 |
| 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 | ファイルがスキャンされるたびにエンドポイントプロテクションの表示が更新されます。 | エンドポイントプロテクションの表示は定期的に更新され、最後の更新以降にスキャンされたすべてのファイルが表示されます。 |
| 高速スキャンよりも低メモリ使用量を優先する | スキャンの実行に使用されるメモリは少なくなりますが、スキャンの実行速度が遅くなる場合があります。 | スキャンの実行により多くのメモリが使用されるため、スキャンの実行速度が速くなります。 |
| 高速スキャンよりも低CPU使用量を優先する | スキャンの実行に使用されるプロセッサの使用量は少なくなりますが、スキャンの実行速度が遅くなる場合があります。 | スキャンの実行により多くのプロセッサが使用されるため、スキャンの実行速度が速くなります。 |
| 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 | エンドユーザーが初めてファイルを実行したときに、スキャンを示すダイアログボックスが表示されます。 | エンドユーザーが初めてファイルを実行したときには何も表示されませんが、ファイルはスキャンされます。 |

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| 非実行可能ファイルの詳細をスキャンログに保存する | すべてのファイルデータがスキャンログに保存されるため、ログファイルのサイズが大きくなります。 | 実行可能ファイルデータのみがスキャンログに保存されるため、ログファイルのサイズが小さくなります。 |
| アーカイブファイルをスキャンする* | .zip、.rar、.cab、7-zipのファイル形式がスキャンされます。 | .zip、.rar、.cab、7-zipのファイル形式はスキャンされません。 |
| 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 | クリーンアップしてマルウェアを削除すると、自動的に再起動されます。 | クリーンアップしてマルウェアを削除すると、ユーザーに再起動を促すプロンプトが表示されます。 |
| マルウェアのクリーンアップ中に再起動しない | マルウェアを削除するためのクリーンアップ中に、マシンが再起動することはありません。 | マルウェアを削除するためのクリーンアップ中に、再起動が妨げられることはありません。クリーンアップが不完全である可能性があります。 |
| バックグラウンドスキャン中に発見された脅威を自動的に除去する | バックグラウンドスキャン中に検出された脅威は、自動的に隔離されます。 | 脅威はスケジュールスキャン時に隔離されます。 |
| 学習スキャンで発見された脅威を自動的に除去する | デバイスの最初のスキャン中に検出された脅威は、自動的に隔離されます。 | 脅威はスケジュールスキャン時に隔離されます。 |
| 高度なサポートを有効にする | Webrootカスタマーサポートにログが送信されます。 | ログはWebrootに送信されません。 |
| 感染しているスキャン結果を表示する | Webrootカスタマーサポートにログが送信されます。 | ログはWebrootに送信されません。 |

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
| --- | --- | --- |
| 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 | 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(悪意はないが、好ましくない動作をする可能性がある、またはアドウェアやツールバーなどのセキュリティ上の問題を引き起こす可能性があるプログラム)は、インストールがブロックされるか、可能な場合はマシンから削除されます。されるデフォルト設定は[**オン**]です。 | これらのアプリケーションはブロックまたは削除されません。 |
| 脅威の調査用にファイルを送信することを許可 | ファイルは、脅威調査のためにWebrootに送信されます。 | ファイルはWebrootに送信されません。 |

* Appleデバイスにも適用されます。

## 自己保護

自己保護のポリシーにより、エージェントが自身を保護する方法を制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| 自己保護応答のクローキングを有効にする | 別の製品がエンドポイントプロテクションの機能に干渉しようとしている場合、エンドポイントプロテクションは保護のためのスキャンを開始して自己を保護しようとします。 | エンドポイントプロテクションは自己を保護しようとしません。 |
| 自己保護のレベル | 自己保護検出レベルを指定します。<br>• [**最小**]: エンドポイントプロテクションの設定が保護されます。他のサイバーセキュリティ製品がインストールされている場合は、このレベルを使用します。<br>• [**中**]: 他のプログラムでエンドポイントプロテクションを無効にすることはできません。他のサイバーセキュリティ製品との互換性を最大限に高めるには、このレベルを使用します。<br>• [**最大**]: エンドポイントプロテクションのプロセスが保護されます。他のセキュリティ製品がインストールされていない場合は、このレベルが推奨されます。 | |

## ヒューリスティック

一連のヒューリスティックのポリシーによって、ローカルドライブ、インターネット、ネットワーク、CD/DVDドライブ、およびマシンがオフラインの場合の動作を制御できます。サポートによるご案内がない限り、デフォルト設定は変更しないでください。

## リアルタイムシールド

リアルタイムシールドのポリシーにより、疑わしい脅威や既知の脅威に対するブロックと警告の動作を制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| リアルタイムシールド有効* | 疑わしい脅威や既知の脅威は直ちにブロックされます。 | 脅威はブロックされず、ユーザーには通知されません。この設定を無効にすると、保護の強度が減少します。 |
| 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 | 脅威定義ファイルはデバイスにダウンロードされ、デバイスがオフラインのときに保護に使用されます。 | 脅威定義ファイルはダウンロードされず、オフラインのデバイスは保護されません。 |
| 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 | エンドポイントプロテクションは、エンドユーザーが警告にどのように応答したか(許可したか、またはブロックしたか)を記憶し、同じファイルについてはプロンプトを再度表示しません。 | エンドポイントプロテクションは同じファイルに対して毎回警告を表示します。 |
| ブロックされたファイルを自動的に隔離する* | 以前に隔離されたファイルは、自動的に隔離されます。たとえば、ファイルが再度ダウンロードされた場合です。 | 以前に隔離されたファイルは、次回の定期スキャンでは隔離されません。 |
| 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* | 疑わしい脅威や既知の脅威は、実行時に自動的にブロックされます。 | 疑わしいまたは既知の脅威が検出されたときは、エンドユーザーに許可またはブロックするよう警告します。 |
| 書き込みまたは変更時にファイルをスキャンする* | 新規または変更されたファイルは、保存またはインストール時にスキャンされます。 | 新規または変更されたファイルは、保存またはインストール時にスキャンされません。 |
| 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* | ユーザーがログインしていないときに、疑わしい脅威や既知の脅威の実行が自動的にブロックされます。 | ユーザーがログインしていないときに、ファイルの実行はブロックされません。 |
| リアルタイムイベントの警告を表示する | 不審なアクティビティが検出されると直ちに警告が表示されます。 | 警告は表示されません。 |

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
| --- | --- | --- |
| リアルタイム ブロック モードの警告を表示する | マルウェアが検出されると直ちに警告が表示されます。ヒューリスティックスのオプションのいずれかが、[**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、このオプションをオンにします。 | 警告は表示されません。 |
| リアルタイムブロックのお知らせを表示する | マルウェアが検出されると直ちにトレイに警告の通知が表示されます。 | トレイに警告の通知は表示されません。 |

* Appleデバイスにも適用されます。

## 動作シールド

動作シールドのポリシーにより、デバイスで実行されているアプリケーションおよびプロセスの分析を制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| 動作シールド有効 | 疑わしい脅威についてプロンプトが表示されると、既知の脅威は即座にブロックされて隔離されます。 | 脅威は警告もブロックもされません。 |
| 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 | Endpoint Protectionでは、実行が許可される前にプログラムのアクティビティが検査されます。安全であると思われる場合は、Endpoint Protectionによって実行が許可され、そのアクティビティが継続的に監視されます。 | プログラムは検査されません。 |
| 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 | Endpoint Protectionがプログラムを検査し、その目的を判断します。たとえば、マルウェアによってレジストリエントリが変更され、電子メールが送信される可能性があります。 | プログラムは検査されません。 |
| 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 | Endpoint Protectionは、安全または脅威として分類されていないプログラムだけを検査します。 | プログラムは検査されません。 |
| 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 | Endpoint Protectionによって脅威を許可するかブロックするかが決定されます。 | 脅威を許可するかブロックするかを決定するよう、エンドユーザーにプロンプトが表示されます。 |
| 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 | 未分類のプログラムでは、デバイスがオフラインのときにプログラムがデバイスに変更を加えようとすると警告が表示されます。 | デバイスがオフラインのときにプログラムがデバイスに変更を加えようとしても、警告は表示されません。 |

* Appleデバイスにも適用されます。

## コアシステムシールド

コアシステムシールドのポリシーにより、コンピュータシステムの構造を監視および保護できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| コアシステムシールド有効 | 疑わしい脅威についてプロンプトが表示されると、既知の脅威は即座にブロックされて隔離されます。 | 脅威は警告もブロックもされません。 |
| 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、システムを変更しようとするすべての試みをEndpoint Protectionが阻止します。 | システムを変更しようとするすべての試みは、Endpoint Protectionによって阻止されません。 |
| 破損したシステムコンポーネントを検出して修復する | Endpoint Protectionは、破損したコンポーネントまたはファイルを検出して復元します。 | Endpoint Protectionは、破損したコンポーネントまたはファイルを検出または復元しません。 |
| 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の場合、カーネルメモリの変更がブロックされます。 | 未分類のプログラムの場合、カーネルメモリの変更はブロックされません。 |
| 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の場合、システムプロセスの変更がブロックされます。 | 未分類のプログラムの場合、システムプロセスの変更はブロックされません。 |
| LSPチェーンと他のシステム構造の整合性を検証する | Endpoint Protectionは、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破損しないように監視します。 | Endpoint Protectionは、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破損しないように監視することはありません。 |
| どのプログラムもHOSTSファイルを変更できないようにする* | hostsファイルを変更しようとすると、Endpoint Protectionの警告が表示されます。 | hostsファイルを変更しようとしても、Endpoint Protectionの警告は表示されません。 |

* Appleデバイスにも適用されます。

## Web脅威シールド

Web脅威シールドのポリシーにより、インターネットの閲覧と検索エンジンの動作を制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| Webシールドを有効化* | エンドポイントプロテクションは、インターネットの閲覧を監視し、疑わしいサイトに対して警告を表示します。また、検索エンジンの検索結果リンクも分析します。 | インターネット閲覧の監視や検索エンジンの分析は行われません。 |
| ブラウザのエクステンションを有効にする | ウェブの検索結果を表示すると、アイコンが表示されます。アイコンにカーソルを合わせると、サイト評価のレビューを見ることができます。 | ウェブの検索結果を表示しても、評価のアイコンは表示されません。 |
| 悪質なWebサイトをブロック* | エンドポイントプロテクションは、既知の悪質なウェブサイトをブロックします。 | ウェブサイトはブロックされません。 |
| リアルタイムフィッシング対策を有効にする* | エンドポイントプロテクションは、これまで検出されたことがなく、未分類のサイトであるゼロデイフィッシングサイトに対して警告を表示します。 | ゼロデイフィッシングサイトでは、警告は表示されません。 |
| 検索エンジンを使用する際に安全評価を表示する* | 検索エンジンの結果リンクでは、信頼できるサイトは緑のチェックマーク、疑わしいサイトは赤のX印で区別されます。 | 検索エンジンの結果は識別されません。 |
| Webフィルタリングドライバを有効化 | ブラウザ拡張機能が無効になっている場合など、悪意のある接続に対する追加の保護が行われます。 | 悪意のある接続に対する追加の保護は行われません。 |
| 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* | エンドユーザーは、既知の悪意のあるWebサイトが検出されたときに表示されるブロックページを回避できません。 | ユーザーはブロックページを回避できます。 |
| 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* | エンドユーザーは、既知の悪意のあるWebサイトが検出されたときに表示されるブロックページからWebサイトのレビューのリクエストを送信することはできません。 | ユーザーはブロックページからウェブサイトのレビューをリクエストすることができます。 |

* Appleデバイスにも適用されます。

## IDシールド

IDシールドのポリシーにより、オンライントランザクション中のデータの保護方法を制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| IDシールド有効* | エンドポイントプロテクションはオンライントランザクションを監視します。MacOSでは、このオプションは[**セキュアキーボード入力モード**]の設定を制御します。 | オンライントランザクションは監視されません。 |
| オンライン上の個人情報に対する脅威を探す | 悪意のあるコンテンツが検出されると、エンドポイントプロテクションが分析して警告を表示します。 | コンテンツは分析されません。 |
| アクセス時にWebサイトを検証して正当性を判別する | エンドポイントプロテクションは、ウェブサイトのIPアドレスがリダイレクトされたとき、または脅威として識別されたときに、分析を行って警告を表示します。 | ウェブサイトのIPアドレスは分析されません。 |
| WebサイトのDNS/IP解決を検証して中間者攻撃を検出する | エンドポイントプロテクションは、中間者攻撃など、ウェブサイトがリダイレクトされたときに分析を行って警告を表示します。 | ウェブサイトのリダイレクトは分析されません。 |
| Webサイトが危険度の高い追跡情報を作成しないようブロックする | サードパーティのCookieが悪意のあるサイトから送信された場合、エンドポイントプロテクションはサードパーティのCookieをブロックします。 | サードパーティのCookieはブロックされません。 |
| 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 | エンドポイントプロテクションでは、ユーザー名とパスワードを入力した場合や、ウェブサイトの認証情報の保存を選択した場合などに、プログラムによる認証情報へのアクセスがブロックされます。 | プログラムによる認証情報へのアクセスはブロックされません。 |
| 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 | エンドポイントプロテクションは、プログラムがデータにアクセスしようとしたときに警告を表示します。 | データにアクセスするプログラムに対して警告は表示されません。 |
| 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 | 信頼できる画面キャプチャプログラムは、画面に表示されるコンテンツに関係なく機能します。 | 画面キャプチャプログラムは、保護された画面のコンテンツにアクセスできません。 |

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
| --- | --- | --- |
| IDシールド対応モードを有効にする | 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について、その実行が許可されます。たとえば、デバイスでアプリケーションの実行に問題がある場合は、このオプションを有効にする必要があります。このオプションを有効にした場合も、IDシールドのコア機能によってデバイスの保護が継続されます。 | IDシールドは、悪意があると判断したすべてのアプリケーションのブロックを継続します。 |
| 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 | エンドポイントプロテクションは、日本語や中国語など、アルファベット以外の文字を使用するデバイスをキーロガーから保護します。 | キーロガーに対する保護はありません。 |

* Appleデバイスにも適用されます。

## ファイアウォール

ファイアウォールのポリシーにより、エンドポイントプロテクションのファイアウォールを制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| 有効 | エンドポイントプロテクションのファイアウォールがアウトバウンド通信を監視し、Windowsファイアウォールがインバウンド通信を監視します。エンドポイントプロテクションのファイアウォールは、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。ファイアウォールが疑わしい通信を検出すると、エンドユーザーに警告が表示されます。 | アウトバウンド通信は監視されません。 |
| ファイアウォールのレベル | このオプションは、ファイアウォール保護のレベルを指定します。<br>• [**デフォルトで許可**]: エージェントによって明示的にブロックされない限り、すべてのプロセスがインターネットに接続できます。<br>• [**不明および感染している場合に警告**]: インターネットに接続している信頼できない新しいプロセス、またはデバイスが感染しているかどうかを検索します。<br>• [**不明の場合に警告**]: インターネットに接続している信頼できない新しいプロセスを検索します。<br>• [**デフォルトでブロック**]: エージェントによって明示的にブロックされていない限り、インターネットに接続しているプロセスを検索します。 | |
| 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の場合、警告が表示されます。 | Windowsファイアウォールがオフの場合、警告が表示されません。 |
| ファイアウォールプロセスの警告を表示する | ファイアウォールレベルの警告が表示されます。 | 警告は表示されず、プロセスは許可されます。 |

* Appleデバイスにも適用されます。

## ユーザーインターフェイス

ユーザーインターフェイスのポリシーにより、エンドユーザーのWindowsまたはAppleデバイスでエンドポイントプロテクションを利用できるかどうかを制御できます。

- [**表示**]に設定すると、ユーザーはデバイス上でエンドポイントプロテクションを表示し、アクセスできます。スキャンは実行できますが、エージェントの管理や設定の変更はできません。
- [**非表示**]に設定すると、ユーザーがエンドポイントプロテクションにアクセスしようとした場合、管理者への連絡を促すプロンプトが表示されます。MacOSで[非表示]を選択した場合はシステムトレイのアイコンも非表示になります。

## システム最適化ツール

システム最適化のポリシーにより、不要なファイルやデータの削除といったWindowsの一般的なクリーンアップタスクを制御できます。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| システム最適化ツールを集中管理 | [システム最適化ツール]のコントロールを表示します。 | [システム最適化ツール]のコントロールは表示されません。 |
| 曜日 | システム最適化ツールは選択した曜日に実行されます。 | システム最適化ツールは選択した曜日に実行されません。 |
| 指定時間での実行 - 時 | システム最適化ツールを実行する時刻を指定します。 | |
| 指定時間での実行 - 分 | システム最適化ツールを実行する選択時刻の分を指定します。 | |
| 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 | スケジュールされた実行時間にマシンの電源がオフになっている場合、システム最適化ツールは起動時に実行されます。 | システム最適化ツールは、スケジュールされた実行時間にのみ実行されます。 |
| 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 | Windowsエクスプローラーに、ファイルをごみ箱に移動せずに消去できる右クリックメニューのオプションが表示されます。 | このオプションは、Windowsエクスプローラーに表示されません。 |
| ごみ箱 | システム最適化ツールが実行されると、ごみ箱内のすべてのファイルが削除されます。 | ごみ箱からは何も削除されません。 |
| 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が[**スタート**]メニューから削除されます。履歴だけが削除され、実際のファイルは削除されません。 | [**スタート**]メニューからは何も削除されません。 |
| スタートメニューのクリック履歴 | 最近開いたプログラムへのショートカットの履歴が[スタート]メニューから削除されます。履歴だけが削除され、実際のショートカットは削除されません。 | 履歴は削除されません。 |
| 実行履歴 | [**実行**]ダイアログボックスからコマンドの履歴が削除されます。すべてのコマンドをクリアするには、再起動が必要な場合があります。 | 履歴は削除されません。 |
| 検索履歴 | コンピュータの検索履歴が削除されます。履歴だけが削除され、検索中に見つかったファイルやプログラムは削除されません。 | 履歴は削除されません。 |

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| スタートメニューの並べ替え履歴 | 再起動が行われると、[**スタート**]メニューの順序の変更はすべて元に戻され、メニューはデフォルトの設定であるアルファベット順になります。 | [**スタート**]メニューの順序は元に戻りません。 |
| クリップボードの内容 | クリップボードの内容は消去されます。 | クリップボードの内容は消去されません。 |
| Windows一時フォルダ | Windows一時フォルダ(通常は `C:\Windows\Temp\`)内のすべてのデータは、ファイルが使用中でない限り削除されます。 | データは削除されません。 |
| システム一時フォルダ | システム一時フォルダ内のすべてのデータは、ファイルが使用中でない限り削除されます。フォルダの場所はWindowsのバージョンによって異なります。 | データは削除されません。 |
| Windows Update一時フォルダ | Windows Update一時フォルダ内のすべてのデータは、ファイルが使用中でない限り削除されます。 | データは削除されません。 |
| Windowsレジストリストリーム | Windowsレジストリの変更履歴が削除されます。履歴のみが削除され、レジストリへの変更やキーは削除されません。 | 履歴は削除されません。 |
| デフォルトログオンユーザー履歴 | コンピュータに最後にログインしたユーザーを格納するレジストリキーが削除されます。ユーザーは、コンピュータを起動するたびにユーザー名を入力する必要があります。この設定は、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適用されません。 | レジストリキーは削除されません。 |
| メモリダンプファイル | すべてのメモリダンプファイル(特定のWindowsエラーに対して自動的に作成されるファイル)が削除されます。 | ダンプファイルは削除されません。 |
| 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は、ファイルが使用中でない限り削除されます。フォルダの場所はWindowsのバージョンによって異なります。 | プロジェクトファイルは削除されません。 |
| Flash Cookie | Adobe Flashのデータは削除されます。これはブラウザのCookieプライバシー制御によって制御される実際の「Cookie」ではありません。 | データは削除されません。 |
| アドレスバー履歴 | アクセスしたWebサイトの履歴がInternet Explorerから削除されます。 | 履歴は削除されません。 |

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| Cookie | すべてのCookieが削除されます。ユーザーは、パスワードやショッピングカートのアイテムなど、Cookieに保存されているエントリを再入力する必要があります。 | Cookieは削除されません。 |
| インターネット一時ファイル | ブラウザの一時ファイルがすべて削除されます。 | ファイルは削除されません。 |
| URL履歴 | Internet Explorerの履歴ペインがクリアされます。 | 履歴ペインのエントリは削除されません。 |
| 設定ログ | Internet Explorerのアップデートログファイルは削除されます。 | ファイルは削除されません。 |
| Microsoftダウンロードフォルダ | Internet Explorerのダウンロードフォルダ内のファイルは削除されます。 | ファイルは削除されません。 |
| MediaPlayerバー履歴 | Internet Explorerの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が削除されます。ファイルそのものは削除されず、最近開いたファイルのリストだけが削除されます。 | 最近開いたファイルの一覧は削除されません。 |
| オートコンプリートフォーム情報 | Internet Explorerのオートコンプリートデータは削除されます。ユーザーはフォームにデータを再入力する必要があります。 | データは削除されません。 |
| Index.datの消去 | 再起動すると、Webアドレス、検索クエリ、最近開いたファイルなどのWindows情報が保存される`index.dat`ファイルが削除されます。 | `index.dat`ファイルは削除されません。 |
| 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 | 削除されたファイルの処理方法を指定します。<br>• [**標準**]: ファイルは削除されますが、ごみ箱からは削除されません。データ復元ユーティリティを使用すると、これらのファイルを復元できる場合があります。このオプションは、最速のクリーンアッププロセスです。<br>• [**中**]: ファイルは削除されますが、ごみ箱からは削除されず、データが保存されていた場所は3回上書きされます。データ復元ユーティリティでは、これらのファイルの復元が困難になります。このクリーンアッププロセスは、通常のクリーンアッププロセスよりも時間がかかります。<br>• [**最大**]: ファイルは削除されますが、ごみ箱からは削除されず、データが保存された場所は、データの場所の周囲の領域を含めて7回上書きされます。これらのファイルは、データ復元ユーティリティでは復元が最も困難です。これはまた、最も時間がかかるクリーンアッププロセスです。 | |

## DNSプロテクションのポリシー設定

DNSプロテクションのポリシーは、DNSプロテクションがエージェントとともにインストールされるかどうかを制御します。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| DNSプロテクションをインストール | DNSプロテクションがエンドポイントプロテクションエージェントとともにインストールされます。 | DNSプロテクションはインストールされません。 |

## 回避シールド

回避シールドのポリシーにより、ファイルベースの攻撃、ファイルレスの攻撃、難読化または暗号化攻撃を含む回避型攻撃を検出してブロックできます。バージョン9.0.29.00以降を実行しているエージェントが必要です。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| スクリプト保護 | この設定は、スクリプト保護のレベルを指定します。<br>• [**オフ**]: スクリプト保護が無効になります。<br>• [**検出と報告**]: スクリプトの脅威が見つかると、検出されて警告が表示されます。<br>• [**検出と修復**]: スクリプトの脅威が見つかると、検出されて警告が表示され、隔離されます。 | |

## USBシールド

以下の設定により、USBストレージデバイスの検出とこれらのデバイスへのアクセスを制御できます。バージョン9.0.31.84以降を実行しているエージェントが必要です。

| ポリシー設定 | ポリシー設定が有効な場合 | ポリシー設定が無効な場合 |
|---|---|---|
| USBシールドを有効化 | USBストレージデバイスで疑わしい脅威や既知の脅威が実行された場合、即座にブロックされます。 | 脅威はリアルタイムでブロックされません。コンテキストメニューの**[ウェブルートでスキャン]**オプションを使用すると、USBドライブをスキャンできます。 |
| USBストレージデバイスをブロック | USBストレージデバイスへの読み取り、書き込み、実行のアクセスはすべてブロックされます。エンドユーザーがUSBストレージデバイスを挿入すると、メッセージが表示されます。 | USBストレージデバイスにフルアクセスできます。 |

# エンドポイントプロテクションのオーバーライド

[**オーバーライド**]: ポリシーやドメインのカテゴリにかかわらず許可またはブロックする必要のあるファイルやドメインを指定できます。

**マネージドサービスプロバイダー (MSP) 向けの表示**において、グローバルファイルのオーバーライドはサイトの[**詳細**]タブで[**グローバルオーバーライドの追加**]が有効になっているすべてのサイトに適用されます(推奨)。

サイトオーバーライドはグローバルオーバーライドより常に優先されます。

ポリシーオーバーライドはサイトオーバーライドより常に優先されます。

オーバーライドの変更は適用から15分以内に複製されます。

DNSオーバーライドにアクセスするには、[**管理**] > [**オーバーライド**]に移動し、[**ウェブのオーバーライド**]タブを選択します。

## ファイルの許可とブロック

ファイルのオーバーライドでは、エンドポイントプロテクションを使用する場合に実行できるファイルとブロックされるファイルを管理者が定義できます。フォルダ/ファイルのオーバーライドは、Webrootエージェントのバージョン9.0.1以降でのみサポートされています。

[**管理**] > [**オーバーライド**]の順に移動し、[**ファイルのオーバーライド**]タブをクリックすると、許可およびブロックされたファイルを表示および管理できます。[**オーバーライド**]ドロップダウンメニューをクリックして、[**オーバーライド**]の表に以下のとおり表示される結果の範囲を選択します。

- [**グローバル**]オーバーライドは、アクセスできるすべてのサイトに適用されます。
- [**サイト**]リストで特定のサイトを選択すると、そのサイトに関連するオーバーライドが表示されます。

表の結果をさらに絞り込むには[**検索**]ボックスを使用するか、[**フィルタ**]をクリックします。適用された検索語、フィルタ、並べ替え設定は、手動でリセットするかコンソールからログアウトするまで、コンソール内の他のページに移動しても保持されます。

**ファイルのオーバーライドを追加するには、以下の手順に従います。**

1. [**オーバーライドを追加**]をクリックします。
2. [**ファイルのオーバーライドの追加**]ページで、ファイルのオーバーライドの種類として[**許可**]または[**ブロック**]を選択します。
    - [**許可**]: ファイルのオーバーライドでは、Webrootのクラウド判定にかかわらず、ファイルの実行を許可します。
    - [**ブロック**]: ファイルのオーバーライドでは、Webrootのクラウド判定にかかわらず、ファイルの実行をブロックします。
3. [**オーバーライドの種類**]を選択して、ファイルをフォルダ/ファイルの場所で識別するか、MD5ハッシュ値で識別するかを指定します。
    - **フォルダ/ファイル**
        - フォルダ/ファイルに基づいてブロックすることはできません。フォルダ/ファイルは許可のみ可能です。

- [**フォルダ**]フィールドに、絶対ファイルパス、またはシステム変数(例: `%SystemDrive%`)を使用したファイルパスを指定します。サポートしている変数のリストを表示するには、「%」を入力します。
- [**ファイル**]フィールドに、特定のファイル名またはワイルドカードを入力します。空白のままにすると、指定したフォルダ内のすべてのファイルが許可されます。
- 指定したパスのサブフォルダを含める場合は、[**サブフォルダを含める**]を選択します。
- 割り当てられたポリシーに従ってファイルを検出して修復するには、[**悪質な場合は検出**]を選択します。監視とジャーナリングは無効になります。このオプションを無効にすると、検出と修復のポリシー設定はファイルに適用されません。
- オーバーライドの**名前**を入力します。
- [**スコープ**]を選択して、**グローバル**設定を含めるように設定されているすべてのサイトに規則を適用するか、選択した**サイト**だけに適用するかを選択します。
- オーバーライドの[**スコープ**]に[**サイト**]を選択した場合、オーバーライドをポリシーに関連付けて、個々のサイト、グループ、またはデバイスに適用できます。

- **MD5**ハッシュ
  - MD5ハッシュ値に基づくファイルを許可またはブロックできます。
  - MD5を選択した場合は、32文字のハッシュを指定します。

4. 終了したら、[**保存**]をクリックします。

**別のコンソールまたはサイトで定義済みのオーバーライドをインポートするには、以下の手順に従います。**

1. [**オーバーライドのインポート**]をクリックします。
2. [**インポート元のコンソール/サイト**]のドロップダウンメニューで、インポート元のオーバーライドを含むコンソール/サイトを選択します。
3. [**インポート先のコンソール/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コンソール/サイトを選択します。
4. 以下のいずれかのオプションの横にある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**]: 重複する項目がオーバーライドのインポートリストから削除され、すでに設定されているオーバーライドが維持されます。選択しない場合、重複する項目は削除されません。
   - [**既存のオーバーライドの上書き**]: 削除されない重複する項目によって既存の項目が上書きされます。選択しない場合、重複する項目はインポート後も維持されます。
   - [**ポリシーベースのオーバーライドを含む**]: インポート元のサイトで使用されているポリシーに割り当てられたオーバーライドがインポートされます。これらのオーバーライドは**グローバル**オーバーライドに変換されます。選択しない場合、サイトからのポリシーのオーバーライドはインポートされません。
5. 終了したら、[**インポート**]をクリックします。

**オーバーライドを編集するには、以下の手順に従います。**

1. 表でオーバーライドを検索し、[アクション]列の下にある[**編集**]をクリックします。
2. オーバーライドの仕様を変更します。選択された許可/ブロックの値がWebrootクラウド判定とすでに一致している場合、[**重複するオーバーライド**]の警告が表示されます。
3. [**保存**]をクリックします。

**オーバーライドを削除するには、以下の手順に従います。**

1. [**オーバーライド**]の表で、削除するオーバーライド名の横にあるチェックボックスを選択します。
2. [**削除**]をクリックします。

## ウェブサイトへのアクセスの許可とブロック

エンドポイントプロテクションのみを使用している場合、[**ウェブのオーバーライド**]タブで許可された設定は、Web脅威シールドの任意のポリシー設定に関連するものになります。

DNSプロテクションを使用している場合、ドメインの許可とブロックの両方を[**ウェブのオーバーライド**]タブで設定できます。

**許可またはブロックするドメインを指定するには、以下の手順に従います。**

1. [**追加**]をクリックして、許可またはブロックするドメインを指定します。
    - [**ドメイン**]ボックスでは、規則を設定するために、ドメインのリストをコンマ区切りで入力します。プロトコル(httpsやwwwなど)は必要ありません。たとえば、「domain.com」のように指定できます。ワイルドカード(*.domain.com)はサポートされています。
    - [**スコープ**] (**MSP向けの表示**のみ)を選択すると、グローバル設定を含めるように設定されているすべてのサイトに規則を適用するか、選択したサイトだけに適用するかを指定できます。
    - [**ポリシー**] (**MSP向けの表示**のみ)を選択すると、ポリシーを指定して、この規則を関連付けることができます。ポリシーを指定しない場合、オーバーライドはサイトに関連付けられます。
    - [**ブロック/許可**]を選択すると、特定のドメインをブロックするか許可するかを指定できます。
    - [**悪質なURLをブロック**] (Web脅威シールドのみ)を選択すると、既知のマルウェアが含まれるドメインなど、悪意のあるURLはWeb脅威シールドのポリシーによってブロックされます。
2. [**アップデート**]をクリックして表を更新します。

[**フィルタ**]は、[フィルタ]行にある上下の矢印を使用すると表示できます。表示されるリストをスコープ別、ポリシー別、またはURLがブロック/許可されているかどうかで、[ドメイン]を含む行のみに絞り込むことができます。

**並べ替え**は、列の見出しをクリックすると、その列を基準に表が並べ替えられます。

[**アクション**]列で[ **オーバーライドを編集**]または[**オーバーライドを削除**]を選択できます。

# レポート

レポートには、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詳細な情報が記載されます。レポートは必要に応じて作成することも、定期的な間隔でスケジュールすることもできます。

ナビゲーションペインで[**レポート**]をクリックすると、すべてのレポートオプションが表示されます。

**MSP向けの表示**の場合、[**APIレポート**]タブを開いて、スタンドアロンのUniversal Reporterツールの情報を取得すると、顧客向けにカスタマイズしたレポート作成に使用できます。

# レポートの種類

オンデマンドのレポートやスケジュールされたレポートには、次のレポートを使用できます。

- **DNSプロテクション**レポートは、DNSプロテクションを有効にしている場合にのみ利用できます。詳細は「*DNSプロテクションレポート* ページ 114」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**レポートは、セキュリティ意識向上トレーニングを有効にしている場合にのみ利用できます。詳細は「*セキュリティ意識向上トレーニングレポート* ページ 127」を参照してください。

## デバイスレポート

- [**エージェントのバージョンの使用状況**]: インストールされたエージェントのバージョンを表示
- [**デバイスのアクティブ化**]: ドロップダウンメニューで指定できる期間内のアクティブ化を表示
- [**デバイスのタイプ**]: WindowsまたはMacOSデバイスを表示
- [**エンドポイントの状態**]: クリーンなデバイスと感染したデバイスを表示
- [**期限切れの状態**]: アクティブなデバイスと期限切れのデバイスを表示
- [**インストールの状態**]: アクティブなデバイスとアンインストールされたデバイスを表示
- [**ポリシーにより管理**]: ポリシー管理対象のデバイスと管理対象外のデバイスを表示
- [**オペレーティングシステムのファイアウォールの状態**]: 有効、無効、サポート未対応のOSのファイアウォールを表示
- [**オペレーティングシステムの言語**]: OSの言語を表示
- [**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、または不明なOSのアーキテクチャを表示
- [**プライマリブラウザ**]: デフォルトのブラウザを表示
- [**対応の状態**]: 有効および無効の対応の状態を表示
- [**スケジュールスキャンの状態**]: 有効および無効のスケジュールスキャンを表示
- [**サイレントモード**]: 有効、無効、サポート未対応のサイレントスキャンを表示
- [**仮想マシン**]: 仮想マシンとして分類されたデバイスを表示

### ファイル脅威に関するレポート

- [**確認されたすべての脅威**]: ファイル名で特定された脅威を表示
- [**確認されたすべての未判定のソフトウェア**]: ファイル名で未判定の脅威を表示
- [**注意が必要**]: 注意が必要なサイトを表示
- [**対応の必要なデバイス**]: 対応が必要なデバイスを表示
- [**最新のスキャンで脅威が確認されたデバイス**]: デバイス別に特定された脅威を表示
- [**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**]: デバイスによる未判定の脅威を表示
- [**脅威の検出履歴**]: カウント別に特定された脅威を表示

### シールドレポート

- [**Evasion Shield - スクリプト保護ステータス**]: 無効/サポート未対応の回避シールド保護の検出とレポート、検出と修復のすべてのステータスを表示
- [**Evasion Shield - スクリプト検出**]: 回避シールドで検出された脅威を表示
- [**ファイアウォールの状態**]: 有効、無効、サポート未対応のエンドポイントプロテクションのファイアウォールの状態を表示
- [**IDシールドの状態**]: 有効および無効なIDシールドの保護を表示
- [**Infraredの状態**]: 有効、無効、サポート未対応のInfrared設定を表示
- [**オフラインシールドの状態**]: 有効、無効、サポート未対応のオフラインシールド保護を表示
- [**フィッシングシールドの状態**]: 有効および無効なフィッシングシールドの保護を表示
- [**リアルタイムシールドの状態**]: 有効および無効なリアルタイムシールドの保護を表示
- [**ルートキットシールドの状態**]: 有効、無効、サポート未対応のルートキットシールド保護を表示
- [**USBシールドの状態**]: 有効、無効、サポート未対応のUSBシールド保護を表示
- [**Web脅威シールドによってブロックされた URL履歴**]: ブロックされたURLを日付別に表示
- [**Web脅威シールドによってブロックされたURL**]: ブロックされたURLを表示
- [**Web脅威シールドの状態**]: 有効および無効なWeb脅威シールドの保護を表示

## レポートの作成と実行

必要に応じて新しいレポートを作成し、実行できます。また、既存のスケジュールレポートを、スケジュールされた時間外に実行することもできます。

1. [**レポート**]をクリックし、[**オンデマンド**]タブを開きます。
2. レポートの実行対象とする**サイト**を指定します。すべてのサイトに対してレポートを実行することもできます。
3. 作成する**レポート**を指定します。
4. 該当する場合は、レポートデータの**期間**を指定します。

5. [**送信**]をクリックすると、レポートが作成、表示されます。レポートの種類によっては、レポートで以下のタスクやコントロールを1つ以上使用できる場合があります。
    - チャートのデータをクリックすると、そのデータのサブセットの詳細を表示できます。チャートによっては、より細かなレベルで詳細情報が表示されます。
    - 表のレイアウトで行をクリックすると、その行のエントリに関する詳細が表示されます。
    - ファイル名をクリックすると、詳細が表示されます。
    - [**CSVにエクスポート**]をクリックすると、レポートのデータをコンマ区切りのファイル(.csv)にダウンロードできます。CSVへのエクスポートは、以下のレポートでのみ利用できます。
        - 確認されたすべての脅威
        - 確認されたすべての未判定のソフトウェア
        - 最新のスキャンで脅威が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
        - DNS: アクティブなホスト
        - Evasion Shield
        - 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
    - [**アクション**]をクリックすると、以下の機能の一部にアクセスできます。
        - [**このファイルを許可リストに追加**]: 以下のレポートを許可されたファイルに指定します。
            - 確認されたすべての脅威
            - 確認されたすべての未判定のソフトウェア
            - 最新のスキャンで未判定のソフトウェアが検出されたデバイス
            - Evasion Shield – スクリプト検出
            - 最新のスキャンで脅威が確認されたデバイス
            - 脅威の検出履歴
        - [**このファイルをブロックリストに追加**]: 以下のレポートをブロックされたファイルに指定します。
            - 確認されたすべての未判定のソフトウェア
            - 最新のスキャンで未判定のソフトウェアが検出されたデバイス
        - [**このファイルを隔離先から復元する**]: 隔離先からファイルを削除し、元の場所に復元します。
        - [**このデバイスでクリーンアップを開始する**]: デバイスのスキャンを直ちに開始し、悪意のあるファイルを隔離します。
        - [**オーバーライドの作成**]: URLのオーバーライドを作成します。
    - [**ドメイン**]ボックスでは、規則を設定するために、ドメインのリストをコンマ区切りで入力します。プロトコル(httpsやwwwなど)は必要ありません。たとえば、「domain.com」のように指定できま

す。ワイルドカード(*.domain.com)はサポートされています。この機能は以下のレポートに適用されます。

- Web脅威シールドによってブロックされたURL
- Web脅威シールドによってブロックされたURL履歴

- [**範囲**] (**MSP向けの表示**のみ)を選択すると、グローバル設定を含めるように設定されているすべてのサイトに規則を適用するか、選択したサイトだけに適用するかを指定できます。この機能は以下のレポートに適用されます。
  - Web脅威シールドによってブロックされたURL
  - Web脅威シールドによってブロックされたURL履歴
- [**ポリシー**] (**MSP向けの表示**のみ)を選択すると、ポリシーを指定して、この規則を関連付けることができます。ポリシーを指定しない場合、**オーバーライド**はサイトに関連付けられます。この機能は以下のレポートに適用されます。
  - Web脅威シールドによってブロックされたURL
  - Web脅威シールドによってブロックされたURL履歴
- [**ブロック/許可**]を選択すると、特定のドメインをブロックするか許可するかを指定できます。この機能は以下のレポートに適用されます。
  - Web脅威シールドによってブロックされたURL
  - Web脅威シールドによってブロックされたURL履歴
- [**悪質なURLをブロック**]を選択すると、既知のマルウェアが含まれるドメインなど、悪意のあるURLは規則にかかわらずブロックされます。この機能は以下のレポートに適用されます。
  - Web脅威シールドによってブロックされたURL
  - Web脅威シールドによってブロックされたURL履歴

# スケジュールレポート

スケジュールされたレポートを使用すると、定期的にサイトの詳細情報をレポートとして取得できます。電子メールで提供される、スケジュールされたレポートへのリンクの有効期限は48時間です。期限を過ぎたレポートを表示する必要がある場合は、スケジュールされたレポートの履歴を参照してください。

スケジュールレポートを作成するには、いずれも既存のスケジュールテンプレートの設定が必要です。

## スケジュールレポートのテンプレートの作成

デフォルトでは2つのレポートのテンプレートを利用でき、必要に応じて独自のテンプレートを作成できます。

使用可能なスケジュールされたレポートのテンプレートを表示するには、[**レポート**]をクリックし、[**スケジュールテンプレート**]タブを選択します。

[**スケジュールテンプレート**]タブの上部に表示された以下のボタンを利用できます。

- [**追加**]: スケジュールされたレポートの新しいテンプレートを追加します。
- [**コピー**]: スケジュールされた既存のレポートのテンプレートをコピーします。新しいテンプレートを選択して、変更を加えます。

- [**削除**]: スケジュールされたレポートのテンプレートを削除します。テンプレートを削除した場合は、代わりのテンプレートを割り当てる必要があります。

**スケジュールされたレポートのテンプレートを作成するには、以下の手順に従います。**

1. [**レポート**]をクリックし、[**スケジュールテンプレート**]タブを選択します。
2. [**追加**]をクリックします。[**テンプレートの作成**]ダイアログが表示されます。
    - [**名前**]: テンプレートの一意の名前を指定します。
    - [**タイトルページのテキスト**]: このテンプレートで生成されるレポートのタイトルに使用するテキストを指定します。
    - [**ファイル形式**]: PDFまたはCSVから選択します。
3. レポートに含めるデータの種類を選択して配置し、レポートのテンプレートを生成します。
    - [**ページを追加**]: テンプレートにレポートの種類を追加できます。ドロップダウンメニューから、指定するレポートの種類をページごとに選択します。
    - [**データフィールド**]: 表示されるデータの種類を表示します。
    - [**チャートタイプ**]: データに使用するチャートのタイプをドロップダウンから選択します(該当する場合)。
    - [**期間**]: データの期間をドロップダウンから選択します(該当する場合)。
    - [**ページを削除**]: クリックすると、選択した行がテンプレートから削除されます。
    - **上下矢印**: 行を並べ替える場合に使用します。
4. 完了したら、[**作成**]をクリックします。

## スケジュールレポートの作成

スケジュールされたレポートを新規で作成するには、スケジュールレポートの既存のテンプレートが必要です。詳細は「*スケジュールレポートのテンプレートの作成* ページ 77」を参照してください。

**既存のスケジュールレポートを表示するには、以下の手順に従います。**

1. [**レポート**]をクリックし、[**スケジュールレポート**]タブを選択します。レポートの表の上部にある、以下のボタンを利用できます。
    - [**追加**]: スケジュールレポートを新規で作成します。
    - [**コピー**]: 既存のスケジュールレポートをコピーします。新しいレポートを選択して、変更を加えます。
    - [**削除**]: スケジュールレポートを削除します。
    - [**一時停止**]: レポートの作成を一時停止します。再開されるまでレポートを生成したり、電子メールで送信したりすることはできません。
    - [**再開**]: 一時停止されたレポートを再開します。レポートの生成と電子メールでの送信が、スケジュールレポートの設定で指定した間隔で開始されます。
2. スケジュールレポートを即時に生成して送信するには、[**今すぐレポートを実行する**]をクリックします。レポートの**作成方法**と**受信者**を変更して即時に実行することもできますが、これらの変更は定期的にスケジュールされたレポートには適用されません。

**スケジュールレポートを設定するには、以下の手順に従います。**

1. [**レポート**]をクリックし、[**スケジュールレポート**]タブを選択します。
2. [**追加**]をクリックします。[**レポートを作成**]ダイアログボックスが開きます。
    - [**レポート名**]: レポートの一意の名前を指定します。
    - [**配送予定**]: レポートを生成するタイミングを選択します。タイムゾーンをUTC (協定世界時) で指定します。
    - [**作成方法**]: サイトごとに1つのレポートを生成するか、すべてのサイトに対して1つのレポートを生成するかをこのドロップダウンで指定します。
    - [**受信者**]: このオプションは、作成方法によって異なります。
        - 選択したすべてのサイトのデータで単一のレポートを生成する場合は、電子メールアドレスをコンマで区切って指定します(最大25個)。
        - サイトごとに1つのレポートを生成する場合は、以下から選択します。
            - [**各サイトの配布リストに送信**]: 各サイトに関連付けられたレポート配信先リストを使用するには、このオプションを選択します。
                - **法人向けの表示**の場合、これは[**設定**]タブで指定したレポート配信先リストです。
                - **MSP向けの表示**の場合、[**サイトリスト**]タブに移動し、**サイト名**のリンクをクリックして、[**詳細**]タブに移動します。
            - [**以下の電子メールアドレスに電子メールを送信**]: 電子メールアドレスのコンマ区切りリスト(最大25個)を入力して送信するには、このオプションを選択します。
            - [**両方に送信**]: 上記の両方のオプションを使用するには、このオプションを選択します。
        - [**テンプレート**]を選択して、レポートに使用するテンプレートを指定します。
    - [**サイト**]: レポートを生成するサイトを選択します。
    - [**言語**]: 生成されるレポートのデフォルトのテキストを指定します。選択した言語ごとに1つのレポートが生成されます。
3. レポートを設定したら、[**作成**]をクリックします。

## スケジュールされたレポートの履歴の表示

過去90日以内に生成されたスケジュールされたレポートを表示するには、[**レポート**]をクリックし、[**スケジュール履歴**]タブを選択します。

過去90日以内に生成された各レポートが表形式で表示されます。

[**サイト**]列で、青い円の疑問符の上にカーソルを置くと、レポートに含まれるサイトが表示されます。

[**ダウンロード**]をクリックすると、レポートのコピーをローカルマシンにダウンロードできます。サイトごとに1つのレポートを選択し、複数のサイトを選択した場合は、ダウンロードするサイトのレポートを指定する必要があります。

必要に応じて、[**履歴を更新**]をクリックして表を更新します。

## プロセスログ

エンドポイント保護のプロセスログ機能は、より多くのエンドポイントイベントデータを公開し、ほぼリアルタイムの脅威対応を可能にすることで、MSPのエンドポイント可視性を高めます。

**レポート**の**プロセスログ**タブで、指定した時間枠内にログに記録されたエンドポイントイベントに関する上位レベルの情報を含む表を表示します。

**「プロセスログ」テーブルに表示されるプロセスをカスタマイズするには、以下の方法があります:**

- **プロセスログ**ドロップダウンリストをクリックして、特定のサイトまたはすべてのサイトで発生したプロセスをフィルターで絞り込みます。
- 特定の日付範囲内で発生したプロセスをフィルターで絞り込むには、カレンダードロップダウンリストを使用します。
- フィルターパネルを開くには、**フィルター**をクリックします。
    - 各セクションを展開すると、各フィルターグループで使用可能なフィルターが表示されます。
    - **フィルター**ボタン上の緑色の丸と数字は、現在適用されているフィルターの数を示しています。
    - **決定**のファイルを選択します。
    - 特定の**プロセス名**、**プロセスパス**、または**ユーザー名**で結果を絞り込むには、それぞれのフィールドに値の一部、または値を全部入力します。
    - 特定の**MD5**、または**SHA256**ハッシュで結果を絞り込むには、それぞれのフィールドに値を全部入力します。
    - **リセット**をクリックすると、1つのフィルターグループの選択項目を手動でクリアできます。
    - **フィルターのリセット**をクリックすると、すべてのフィルターがクリアされます。
    - 適用したフィルターは手動でリセットするかログアウトするまで管理コンソール内の他のページに移動しても保持されます。

「プロセスログ」テーブル内のデータを.csvファイルとしてダウンロードするには、**エクスポート**をクリックします。エクスポートされたレポートには、適用された日付範囲とフィルターのみが含まれます。

プロセスツリービューを使用して、特定のプロセスの詳細情報を表示したり、そのプロセスのオーバーライドを作成したりすることもできます。詳細については、*プロセスツリービューの使用* ページ 80を参照してください。

## プロセスツリービューの使用

**プロセスログ**タブでは、プロセスツリーまでドリルダウンして、特定のプロセスと関連するイベントの視覚的な表示と詳細情報を見ることができます。また、デバイスを隔離または隔離解除し、ファイル決定のオーバーライドを作成することもできます。詳細は、*プロセスオーバーライドの作成* ページ 82を参照してください。

**プロセスの詳細を表示するには:**

- **プロセスログ**テーブルで、**プロセス名**列のリンクをクリックすると、プロセスツリービューにドリルダウンできます。**プロセスの詳細**ウィンドウには、選択したプロセスに関する情報が表示されます。

  注:プロセスツリー内の関連イベントをクリックして、その詳細を表示することもできます。

- **プロセス名** — デバイスのオペレーティング・システムによって識別されるプロセス名。
- **判定** — ファイルの判定値(良い、未決定、悪い)。
- **コマンド引数** — プロセス実行時に渡されたコマンド引数。
- **昇格** — 実行中のプロセスの昇格特権(ユーザー、限定、管理者、システム)。
- **MD5** — プロセスに関連付けられたファイルのMD5ハッシュ。
- **正規化されたプロセスパス** — プロセスの正規化されたファイルパス。
- **親プロセスguid** — 親プロセスデータの一意GUID。このGUIDは、実行ライフサイクルを通じてプロセスを追跡します。
- **PID** — 実行時にデバイス・オペレーティング・システムによってプロセスに割り当てられるID。
- **プロセスパス** — プロセスに関連付けられたファイルのシステムパスとファイル名。
- **タイムスタンプ** — プロセス実行イベントの受信に関連付けられた日時。
- **ユーザー名** — プロセスを実行したユーザーまたはシステムアカウント。
- **SHA256** — プロセスに関連付けられたファイルのSHA256ハッシュ。

**プロセスツリービューは、以下のいずれかの方法でカスタマイズできます:**

- ビューエリア内でマウスまたはスクロールホイールを使用して、ドラッグ、縮小、拡大します。
- プロセスツリーのナビゲーションバーにあるコントロールのいずれかを選択します。
  -  をクリックすると、拡大します。
  -  をクリックすると、縮小します。
  -  をクリックすると、プロセスツリーがビューエリア内の中央に表示されます。
  -  をクリックすると、プロセスツリーがデフォルトビューにリセットされます。
  - 異なるプロセスツリービューに切り替えます。
    - 水平ビュー  は、プロセスツリーを横に配置します(デフォルト)。
    - 垂直ビュー  は、プロセスツリーを縦に配置します。
    - 極ビュー  は、中央の親プロセスから派生するすべての関連プロセスが表示されます。

## デバイスの隔離と隔離解除

デバイスを隔離すると、管理コンソールとの通信を除き、デバイスへのすべての内部および外部ネットワークトラフィックがブロックされます。マルウェアに感染している可能性のあるデバイスをすべてのネットワークから切り離し、感染の可能性を最小限に抑えたい場合に有用です。また、デバイスの隔離を解除して、すべてのネットワークに復元することもできます。

デバイスを隔離または隔離解除するには、PC Agent 9.0.36.40以降、またはMac Agent 9.6.4以降を実行している必要があることに注意してください。

**ベストプラクティス:**

- デバイスを可能な限り迅速に隔離および隔離解除できるようにするには、ポリシーで「SecureAnywhereを手動でシャットダウンすることを許可する」設定をオフにします。「エンドポイント保護」がデバイス上でシャットダウンされた場合、エンドポイント保護が再び開始されるまで、デバイスを隔離または隔離解除することはできません。
- デバイスを隔離する必要がある場合は、デバイスをVPNからも切断することをお勧めします。マルウェアに感染している可能性のあるデバイスは、VPNに接続しないでください。

**デバイスを隔離するには:**

1. プロセスツリービューで、**デバイスを隔離**をクリックします。
2. デバイスは、無効化されたボタンで示されるように、**隔離保留**ステータスであることを示します。
3. 隔離保留の期間が終了すると、デバイスは**隔離済み**と表示されます。

**隔離されたデバイスを隔離解除するには:**

1. プロセスツリービューで、**デバイスを隔離解除**をクリックします。
2. しばらくの間、デバイスは**隔離解除保留**ステータスであることを示します。

## プロセスオーバーライドの作成

オーバーライドを使用すると、ポリシーのルールに関係なく許可またはブロックされるファイルやプロセスを特定できます。

**プロセスツリーに表示されているファイルのオーバーライドを作成するには:**

1. プロセスツリーで、プロセスをクリックします。
2. **プロセスの詳細**ウィンドウで、**オーバーライドの作成**をクリックします。
3. **オーバーライドの作成**ダイアログボックスが開くので、以下の情報を入力します:
    - 以下の**許可/ブロック**オプションのいずれかを選択します:
        - **許可** - ファイルオーバーライドは、Webrootのクラウド分類に関係なく、ファイルの実行を許可します。
        - **ブロック** - ファイルオーバーライドは、Webrootのクラウド分類に関係なく、ファイルの実行をブロックします。
    - オーバーライド**タイプ**を選択して、ファイルをフォルダ/ファイルの場所で識別するか、MD5ハッシュ値で識別するかを指定します。
        - **フォルダ/ファイル**
            - フォルダ/ファイルに基づいてブロックすることはできません。フォルダ/ファイルを許可することのみができます。
            - **フォルダ**ボックスに、絶対ファイルパスまたは指定するシステム変数 ( %SystemDrive%など) を使用したファイルパスを入力します。%を入力すると、サポートされている変数のリストが表示されます。

- **ファイル**ボックスに、特定のファイル名またはワイルドカードを入力します。空白のままだと、指定したフォルダ内のすべてのファイルが許可されます。
- 指定したパスのサブフォルダを含めるには、**サブフォルダを含める**チェックボックスを選択します。
- **悪意のあるか検出**チェックボックスを選択すると、割り当てられたポリシーに従ってファイルが検出され、修復されます。モニタリングとジャーナリングは無効です。このチェックボックスをオフにすると、検出および修復ポリシーの設定はファイルに適用されません。

- **名前**ボックスに、オーバーライドの名前を入力します。
- **適用範囲**では、**グローバル**をクリックして、グローバル設定を含めるように構成されているすべてのサイトに適用するルールを指定するか、**サイト**をクリックして、選択したサイトだけに適用するルールを指定します。
  - **サイト**を選択すると、オーバーライドをポリシーに関連付けることができ、個々のサイト、グループ、またはデバイスに適用できます。
- このオーバーライドをデフォルトまたは保存されたポリシーに適用するには、**ポリシーと関連付ける**チェックボックスを選択します。

# エージェントの配備

エージェントは、各デバイスで実行されるソフトウェアです。Webrootエージェントはインストールされているコンピュータごとに一意のIDを持ち、ユーザーによる制御を必要とせず、管理者に代わってセキュリティ操作を実行します。

Webrootの法人向け製品では、2種類のエージェントを使用します。

- **エンドポイントプロテクション**
    - クラウドベースで実行されます。
    - エージェントのインストール後は、定義ファイルをインストールまたはアップデートする必要はありません。
    - エンドポイントプロテクションの脅威が新たに特定された場合、エージェントがクラウド上で更新され、エンドポイントプロテクションの対象のデバイスが直ちに保護されます。
- **DNSプロテクション**
    - DNSプロテクションを購入した場合にのみ利用できます。
    - DNSプロテクションエージェントのインストールは、提供されたMSIを使用して、または既存のエンドポイントプロテクションエージェントを介して実行できます。
    - インストールはWindowsエンドポイントにのみ可能です。
    - Macエンドポイントの保護は、DNSプロテクションで保護されたネットワークを通じて、VPN経由またはオンサイトで実行できます。
    - DNSプロテクションサーバーへのアクセスが可能な場合、DNSプロテクションエージェントがDNSリクエストをフィルタリングおよび管理します。
    - 詳細は「*DNSプロテクションエージェントのインストール* ページ 109」を参照してください。

エージェントはさまざまな方法でデバイスに配備できます。これにはローカルマシンへの手動インストールから、RMMソリューションまたはGPOを使用したリモート配備、SCOM、PDQ Deploy、AutoMoxなどのサードパーティのツールまで、さまざまな選択肢が挙げられます。

どの方法を選択する場合でも、配備戦略が適切に機能していることを確認できるまで、最初は少数のデバイスを作業対象とする必要があります。適切に機能していることを確認できたら、より多くのデバイスに対して防御策を実装します。

次のセクションでは、よく使用される配備方法の一部について説明します。

## インストールウィザードを使用した、WindowsまたはMacOSへのエンドポイントプロテクションのインストール

**インストールウィザードを使用してWindowsまたはMacOSにエンドポイントプロテクションエージェントをインストールするには、以下の手順に従います。**

1. 管理コンソールで、エージェントをインストールするためのダウンロードリンクを見つけます。
    - **法人向けの表示**の場合:
        a. [**設定**] > [**ダウンロード**]をクリックし、インストールファイルのダウンロードリンクを見つけます。
        b. 対象のデバイスで使用されているOSの下部に表示された[**ダウンロード**]リンクをクリックします。
    - **MSP向けの表示**の場合:
        a. [**サイトリスト**]をクリックします。
        b. リストでサイトを特定し、名前をクリックします。
        c. [**エンドポイントプロテクション**]タブを開きます。
        d. [**Windows (.exe) をダウンロード**]、[**Windows (.msi) をダウンロード**]、または[**Macをダウンロード**]リンクをクリックし、対象のデバイスに適したファイルをダウンロードします。
2. 今後の参考のため、会社またはサイトの**キーコード**をコピーします。
3. エージェントをインストールするデバイスに、インストールファイルを移動します。
4. エージェントをインストールします。

インストールが完了すると、エージェントが脅威のスキャンを開始します。初期スキャンが完了してエージェントが管理コンソールでチェックインすると、[**事業体**]ページの[**デバイス**]列に情報が入力されます。このプロセスは通常は15 ~ 30分程度で完了しますが、最大で24時間かかる場合もあります。

DNSプロテクションが有効な場合、DNSプロテクションエージェントはエンドポイントプロテクションエージェントを介してインストールされます。

## コマンドラインからのWindowsまたはMacOSへのエンドポイントプロテクションのインストール

**コマンドラインからWindowsまたはMacOSにエンドポイントプロテクションをインストールするには、以下の手順に従います。**

1. 管理コンソールで、エージェントをインストールするためのダウンロードリンクを見つけます。
    - **法人向けの表示**の場合:
        - [**設定**] > [**ダウンロード**]をクリックし、インストールファイルのダウンロードリンクを見つけます。
        - 対象のデバイスで使用されているOSの下部に表示された[**ダウンロード**]リンクをクリックします。
    - **MSP向けの表示**の場合:
        - [**サイトリスト**]をクリックします。
        - リストでサイトを特定し、名前をクリックします。
        - [**エンドポイントプロテクション**]タブを開きます。
2. Windowsのダウンロードのリンクを選択して、ファイルをダウンロードします。

3. デバイスに対応するいずれかのコマンドオプションを使用して、エージェントをインストールします。明示的な記載がない限り、下記のオプションはWindowsマシン用です。

    - /key=keycodeまたは-keycode =: (Mac)指定したキーコードを使用してエージェントのソフトウェアをインストールします。ハイフンの有無は問いません。
    - /silentまたは-silent: (Mac)エージェントをバックグラウンドでインストールします。画面上の操作はありません。
    - /nostart: エージェントをインストールしますが、起動はしません。
    - /lockautouninstall=password: エージェントをインストールしますが、Windowsのコントロールパネルのプログラムリストには追加しません。これにより、指定したパスワードを使用して、後からバックグラウンドでアンインストールできます。/lockautouninstallを使用する場合、コントロールパネルの[**プログラムの追加と削除**]にエンドポイントプロテクションは表示されません。エンドポイントプロテクションを[**プログラムの追加と削除**]に含めるには、/exeshowaddremoveコマンドを使用します。
    - /autouninstall=password: /lockautouninstallで指定したパスワードを使用してエージェントをアンインストールします。デフォルトでは、管理対象外の状態でユーザーがソフトウェアを削除できないようにするため、コントロールパネルの[**プログラムの追加と削除**]にエンドポイントプロテクションは表示されません。
    - -clone: クローン作成であるため一意のホスト名を持たないデバイスにエージェントをインストールした際に、一意のIDをマシンに割り当てます。ホスト名に一意のIDが含まれるため、このマシンを識別しやすくなります。
    - -uniquedevice: 一意のマシンIDを持たないが固有のホスト名を持つデバイスにエージェントをインストールした際に、一意のIDをマシンに割り当てます。このマシンの識別にはホスト名が使用されます。
    - /exeshowaddremove: エージェントのソフトウェアをWindowsのコントロールパネルのプログラムリストに追加します。エンドユーザーは、管理対象外のエージェントソフトウェアをアンインストールできます。
    - /group=groupcode: エージェントのインストール中に、指定したグループにデバイスを割り当てます。グループは管理コンソールにすでに存在し、かつマシンにエージェントソフトウェアがインストールされていない必要があります。
    - /proxyhost=IPaddressまたは-proxy_host=: (Mac)エージェントのインストール時に、指定したプロキシサーバーを使用します。

    エンドポイントプロテクションではプロキシ設定が自動的に検出されるため、自動検出を使用したくない場合はコマンドラインのオプションを優先的に使用できます。

    プロキシサーバーを指定する場合は、すべてのプロキシ設定を使用し、指定しないオプションにはNULL値を渡します。

    - /proxyport=portnumberまたは-proxy_port=: (Mac)指定したポート番号をプロキシサーバーに使用します。
    - /proxyuser=nameまたは-proxy_user=: (Mac)指定したユーザー名をプロキシサーバーに使用します。
    - /proxypass=passwordまたは-proxy_pass=: (Mac)指定したパスワードをプロキシサーバーに使用します。

- `/proxyauth=authtype`または`-proxy_auth=`: (Mac)以下の認証タイプのいずれかをプロキシサーバーに使用します。
  - `0`: すべての認証タイプを検索します。このオプションを指定すると時間がかかり、プロキシサーバーで不必要なエラーが発生する可能性があります。
  - `1`: 基本認証を使用します。
  - `2`: ダイジェスト認証を使用します。
  - `3`: Negotiate認証を使用します。
  - `4`: NTLM認証を使用します。
- `/lang=languagecode`または`-language=`: (Mac)以下の言語コードのいずれかを使用してエージェントをインストールします。
  - `de`:ドイツ語
  - `en`: 英語
  - `es`: スペイン語
  - `fr`: フランス語
  - `it`: イタリア語
  - `ja`: 日本語
  - `ko`: 韓国語
  - `nl`: オランダ語
  - `pt`: ポルトガル語(ブラジル)
  - `ru`: ロシア語
  - `tr`:トルコ語
  - `zh-cn`: 簡体字中国語
  - `zh-tw`: 繁体字中国語

インストールが完了すると、エージェントが脅威のスキャンを開始します。初期スキャンが完了してエージェントが管理コンソールでチェックインすると、[**事業体**]ページの[**デバイス**]列に情報が入力されます。このプロセスは通常は15 ~ 30分程度で完了しますが、最大で24時間かかる場合もあります。

DNSプロテクションが有効な場合、DNSプロテクションエージェントはエンドポイントプロテクションエージェントを介してインストールされます。

# Msiexecを使用した、Windowsへのエンドポイントプロテクションのインストール

MsiexecはWindowsのコマンドラインベースのプログラムで、ソフトウェアインストールパッケージを解釈してインストールします。Misexecを使用してエンドポイントプロテクションをインストールできます。このインストール方法は通常、リモート配備ツールを使用してソフトウェアをプッシュする場合に使用します。

**Msiexecを使用してWindowsにエンドポイントプロテクションエージェントをインストールするには、以下の手順に従います。**

1. 管理コンソールで、エージェントをインストールするためのダウンロードリンクを見つけます。
    - **法人向けの表示**の場合:
        a. [**設定**] > [**ダウンロード**]をクリックし、インストールファイルのダウンロードリンクを見つけます。
        b. 対象のデバイスで使用されているOSの下部に表示された[**ダウンロード**]リンクをクリックします。
    - **MSP向けの表示**の場合:
        a. [**サイトリスト**]をクリックします。
        b. リストでサイトを特定し、名前をクリックします。
        c. [**エンドポイントプロテクション**]タブを開きます。
2. `.msi`ファイルをダウンロードします。
3. 以下の構文を使用して、エンドポイントプロテクションでMsiexecを使用します。GUILICのキーコードを実際のキーコードに置き換えます。ハイフンの有無は問いません。

    ```
    msiexec /i wsasme.msi GUILIC=キーコード CMDLINE=SME,quiet /qn /l*v install.log
    ```

    コマンドで`ARPNOREMOVE`を指定して、エンドユーザーがエンドポイントプロテクションをアンインストールできないようにすることもできます。

インストールが完了すると、エージェントが脅威のスキャンを開始します。初期スキャンが完了してエージェントが管理コンソールでチェックインすると、[**事業体**]ページの[**デバイス**]列に情報が入力されます。このプロセスは通常は15 ~ 30分程度で完了しますが、最大で24時間かかる場合もあります。

DNSプロテクションが有効な場合、DNSプロテクションエージェントはエンドポイントプロテクションエージェントを介してインストールされます。

# グループポリシーを使用した、Windowsへのエンドポイントプロテクションのインストール

グループポリシーは、`.msi`インストーラーでソフトウェア配備ツールとして使用できます。この方法を使用するには、MicrosoftのActive DirectoryおよびGPOエディタに精通している必要があります。

**グループポリシーを使用してWindowsにエンドポイントプロテクションエージェントをインストールするには、以下の手順に従います。**

1. 管理コンソールでインストールファイルのダウンロードリンクを見つけます。
    - **法人向けの表示**の場合:
        a. [**設定**] > [**ダウンロード**]をクリックし、インストールファイルのダウンロードリンクを見つけます。
        b. 対象のデバイスで使用されているOSの下部に表示された[**ダウンロード**]リンクをクリックします。
    - **MSP向けの表示**の場合:

a. [**サイトリスト**]をクリックします。

b. リストでサイトを特定し、名前をクリックします。

c. [**エンドポイントプロテクション**]タブを開きます。

2. `.msi`ファイルをダウンロードします。
3. ドメインコントローラーで、GPOエディタを使用して配備グループのポリシーを作成します。
4. グループポリシーを作成する組織単位に属するすべてのデバイスに、エンドポイントプロテクションを割り当てます。グループ内のデバイスを再起動すると、エンドポイントプロテクションがインストールされます。

インストールが完了すると、エージェントが脅威のスキャンを開始します。初期スキャンが完了してエージェントが管理コンソールでチェックインすると、[**事業体**]ページの[**デバイス**]列に情報が入力されます。このプロセスは通常は15～30分程度で完了しますが、最大で24時間かかる場合もあります。

DNSプロテクションが有効な場合、DNSプロテクションエージェントはエンドポイントプロテクションエージェントを介してインストールされます。

## スクリプトを使用した、エンドポイントプロテクションエージェントのインストール

エージェントのインストールに使用するスクリプトは、実行前に必ず十分なテストを行ってください。Webrootではスクリプトのトラブルシューティングやサポートは提供していません。またスクリプト関連の質問にはお答えできません。

Macへのインストールに使用するサンプルスクリプトについては、ナレッジベースの「Mac端末へインストールする方法(コマンドラインおよびスクリプト)」を参照してください。

# 警告と警告の配信先リスト

警告は、脅威が検出されたとき、またはWebrootエージェントがデバイスにインストールされたときに送信される電子メール通知です。脅威とインストールの概要を示す警告を生成することもできます。警告の配信先リストは、警告の送信先となる1つ以上の電子メールアドレスのリストです。

## 警告と警告の配信先リストの管理

利用可能な警告を表示するには、[**警告**]をクリックします。このページは、警告リストと配信先リストの2つのタブに分かれています。各リストには、警告または警告の配信先リストに関する概要が表示されます。

- ドロップダウンメニューで範囲を選択すると、以下のとおり、確認および管理できる警告が[**警告**]の表に表示されます。
    - グローバル警告は、アクセスできるすべてのサイトに適用されます。
    - [**サイト**]リストで特定のサイトを選択すると、そのサイトに関連付けられた警告を表示および管理できます。
- いずれかのタブの[**追加**]をクリックすると、警告や警告の配信先リストを追加できます。
- いずれかのタブの[**削除**]をクリックすると、選択した警告や警告の配信先リストを削除できます。
    - 警告を割り当て済みの配信先リストを削除した場合、同じ範囲の配信先リストと置き換える必要があります。
- [**一時停止**]をクリックすると、選択した警告を一時停止できます。警告基準が満たされた場合も、警告の配信先リストに電子メールは送信されません。
- [**再開**]をクリックすると、選択した警告を再開できます。警告基準が満たされた場合、警告の配信先リストに電子メールが送信されます。

表の行をクリックすると、その表の行にある項目の詳細を表示および編集できます。

## 警告の追加

**警告を追加するには、以下の手順に従います。**

1. [**警告**]をクリックし、[**警告リスト**]タブを開きます。
2. [**追加**]をクリックします。
3. [**警告の作成**]ウィザードの最初のステップでは、警告の基本設定を行います。
    - [**名前**]をクリックして、警告の一意の名前を指定します。
    - [**警告のタイプ**]をクリックして、作成する警告の種類を選択します。
4. [**次へ**]をクリックして続けます。
5. [**警告の作成**]ウィザードの2番目のステップでは、この警告を使用するサイトを選択します。
    - スコープの選択
        - [**グローバル**]: 複数のサイトで警告を作成できます。
        - [**サイト**]: 特定のサイトで警告を作成できます。
    - サイトの選択

- [**すべてのサイト**]: すべてのサイトにこの警告を設定できます。
- [**選択したサイト**]: 選択したサイトにこの警告を設定できます。

6. [**次へ**]をクリックして続けます。
7. [**警告の作成**]ウィザードの3番目のステップでは、警告を受信するユーザーを指定します。
   - 既存の配信先リストを使用するには、[**既存のリストを使用**]をクリックし、ドロップダウンから配信先リストを選択します。
   - 新しい配信先リストを作成するには、[**新規リストの作成**]を選択します。
     - [**配信先リストの名前**]で、新しい警告配信先リストに一意の名前を指定します。
     - [**電子メールアドレス**]ボックスで、警告の通知先の電子メールアドレスをコンマで区切って指定します(最大25個)。
8. [**次へ**]をクリックして続けます。
9. [**警告の作成**]ウィザードの4番目のステップでは、警告の生成時に送信される電子メールを設定します。
   - [**電子メールのタイトル**]で、送信する電子メールのメッセージのタイトルを指定します。
   - [**電子メールメッセージの本文**]で、送信する電子メールのメッセージの本文を指定します。
   - [**データ入力**]は、警告の生成時に特定のデータが入力される変数です。カーソルをタイトルフィールドまたは本文フィールドに置くと、データ入力ボタンが青色(有効)になります。有効になった変数をクリックして、タイトルまたは本文に追加します。
     - [**脅威の一覧**]のデータ入力を選択した場合、リストから追加のデータ入力を選択し、含める脅威を指定する必要があります。
     - [**Workgroup**]および[**Active Directory**]のデータ入力は、MacOSには適用されません。
10. [**終了**]をクリックして、警告を作成します。

# 警告の配信先リストの追加

**警告の配信先リストを追加するには、以下の手順に従います。**

1. [**警告**]をクリックし、[**配信先リスト**]タブを開きます。
2. [**追加**]をクリックします。
3. スコープを選択します。
   - [**グローバル**]: 複数のサイトで配信先リストを作成できます。
   - [**サイト**]: 特定のサイトで配信先リストを作成できます。
4. 警告の配信先リストを設定します。
   - [名前]をクリックして、警告の一意の名前を指定します。
   - [**電子メールアドレス**]ボックスで、警告の通知先の電子メールアドレスをコンマで区切って指定します(最大25個)。
5. [**作成**]をクリックして、警告の配信先リストを作成します。

# 管理タスク

各ユーザーアカウントには、以下の3種類の権限のいずれかが付与されます。

- [**スーパー管理者**]アカウント: 管理コンソール上のすべてのタスクを完全に参照および実行できます。
- [**限定管理者**]アカウント: 管理コンソール上の特定の領域のみを参照できます。
- [**アクセス不可**]アカウント: 管理コンソールの使用が禁じられています。

**MSP向けの表示**の場合、ユーザーアカウントを使用してサイトへのアクセスを制御することもできます。

- [**管理者**]: サイトへのフルアクセスが許可されます。
- [**表示のみ**]: サイトの表示のみが許可されます。
- [**アクセス不可**]: サイトへのアクセスが拒否されます。この場合、[**サイトリスト**]ページにサイトは表示されません。

## 使用可能な管理者の表示

使用可能な管理者を表示するには、[**管理者**]ページに移動します。

- スーパー管理者および限定管理者は、[**管理者**]タブのリストに表示されます。
- サイトのみの管理者(**MSP向けの表示**のみ)は、[**サイト限定管理者**]タブのリストに表示されます。
    - **サイトのみの管理者**タブで管理者の追加または編集ができなくなりました。代わりに、**管理者**タブを使用して管理者を管理することをお勧めします。

管理者の管理には以下のコントロールが利用できます。ユーザーアカウントに付与されたアクセス権や、どのタブにいるかに応じて、これらのアクションのいくつかを実行できない場合があります。

- **管理者の追加**をクリックして、新しい管理者を追加します。単一サイトコンソールの場合、この機能は**管理者**タブでのみ利用可能です。
- **管理者名**のリンク: アカウント情報を表示または編集するには、このリンクをクリックします。
- [**アクション**]: 以下の機能を実行できます。
    - [**確認の電子メールを再送信**]: アカウントの電子メールアドレスに確認の電子メールを再送信できます。
    - **編集**は、アカウント情報を表示または編集することができます。単一サイトコンソールの場合、この機能は**管理者**タブでのみ利用可能です。
    - [**削除**]: 管理者を削除できます。
- 列の見出しをクリックすると、その列を基準に表が並べ替えられます。

## 管理者の追加

1. [**管理者**]、[**管理者を追加**]の順にクリックします。
2. [**管理者を追加**]ウィザードの最初のステップでは、管理者の詳細を設定します。
    - [**名**]: ユーザーの名を指定します。
    - [**姓**]: ユーザーの姓を指定します。

- [**電子メール**]: ユーザーの電子メールアドレスを指定します。このアドレスは、ユーザーのログイン時に使用するものです。
- [**電話**]: (オプション)ユーザーの電話番号を指定します。
- [**タイムゾーン**]: ユーザーのタイムゾーンを指定します。
- [**アカウントの種類**]: このユーザーに付与する管理コンソールのアクセス権の種類を決定します。

| 管理コンソールの項目 | スーパー管理者 | 限定管理者 |
|---|---|---|
| サイトリスト(**MSP向けの表示**のみ) | サイト権限に基づく | X |
| ダッシュボード | X | X |
| 事業体 | X | |
| オーバーライド | X | |
| DNSプロテクション | X | |
| セキュリティ意識向上トレーニング | X | |
| レポート | X | |
| 警告 | X | |
| 管理者 | X | 表示のみ |
| 設定 | X | X |

3. **ビジネス向けの表示**の場合、[**保存**]をクリックして管理者を追加します。
4. **MSP向けの表示**の場合、[**次へ**]をクリックしてサイトの管理者権限の割り当てを続行します。
5. この管理者がアクセスできるサイトを選択します。
   - [**管理者**]: サイトへのフルアクセスが許可されます。
   - [**表示のみ**]: サイトの表示のみが許可されます。
   - [**アクセス不可**]: サイトへのアクセスが拒否されます。この場合、[**サイトリスト**]ページにサイトは表示されません。
6. [**保存**]をクリックして管理者を追加します。

# 管理者の編集

**管理者を編集するには、以下の手順に従います。**

1. [**管理者**]ページに移動します。
2. **管理者名**のリンクをクリックします。選択した管理者の設定が表示されます。

3. 必要に応じて、[**詳細**]タブまたは[**サイト権限**] (**MSP向けの表示**のみ)タブの設定を変更します。
4. 完了したら、[**保存**]をクリックします。

# 管理者の削除

削除した管理者は再度追加できます。コンソールごとに少なくとも1人の管理者が必要なため、管理者が1人の場合は削除できません。

**管理者を削除するには、以下の手順に従います。**

1. [**管理者**]ページに移動します。
2. [**アクション**]の下部にある[**削除**]をクリックします。
3. [**管理者を削除**]をクリックして、管理者の削除を確定します。

# 設定

[**設定**]タブには、さまざまな設定のセクションが含まれます。**法人向けの表示**または**MSP向けの表示**では、利用できる設定が異なります。

## 法人向けの表示の設定

[**エンドポイント**]タブには、一般的なサイトまたは会社の情報が含まれます。

- [**サイト/会社名**]: サイトまたは会社の一意の名前です。
- [**キーコード**]: 読み取り専用のフィールドで、サイトまたは会社に割り当てられるキーコードが表示されます。キーコードが体験版の場合は、試用期間の残り日数も表示されます。これはEndpoint Protectionのインストールで使用されるキーコードです。このキーコードは[**ダウンロード**]タブにも表示されます。
- [**会社の規模**]: 会社の規模を表す範囲です。
- [**会社の業種**]: 会社の業種です。
- [**コメント**]: (オプション)サイトまたは会社を説明するコメントを入力します。
- [**サイトのシート数**]: 設定するサイトのエンドポイント数です。この設定は請求には使用されません。
- [**デフォルトのエンドポイントポリシー**]: グループ、サイト、または会社からのポリシーを継承してポリシーが割り当てられていない限り、このサイトにインストールされたすべての新しいEndpoint Protectionエージェントに使用されます。インストール後に、デバイスが使用するポリシーを変更することができます。Webrootでは、このポリシーのコピーを作成し、ベストプラクティスと特定のニーズに合わせて変更することを推奨しています。
    - [**推奨デフォルト設定**]: デスクトップおよびノートパソコンが対象です。
    - [**推奨DNS有効**]: [**推奨デフォルト設定**]と同様、デスクトップおよびノートパソコンが対象です。また、DNSプロテクションエージェントを自動インストールします。
    - [**推奨サーバーデフォルト設定**]: サーバー環境が対象です。リソースの使用率とサーバーへの影響の最小化に重点を置いています。
    - [**サイレント監査**]: エンドポイントプロテクションを透過的に使用できます。検出事項を報告しますが、感染を修復しません。ポリシーのテスト用として、本番環境への影響を最小限に抑えるようにできています。Webrootではこのポリシーの使用を、本番環境における潜在的な誤検出や競合の特定、および不明なソフトウェアの発見を目的として、初期設定中のような短時間に限定することを推奨しています。
    - [**管理対象外**]: ユーザーが各自の設定をエージェントのユーザーインターフェイスで編集できるようにします。それまで適用されていたポリシーや設定は継承されますが、ユーザーインターフェイスを表示するかどうかを除いて特に設定はありません。
        - テクニカルサポートやトラブルシューティングで、またポリシー管理が不要な場合に使用します。
        - エンドユーザーが直接制御できるローカルの非管理アプリケーションにエージェントを変換します。
        - 本番環境では使用しないでください。

        - ポリシー名の最初に[**レガシー**]の付いたポリシーには以前推奨されていたポリシー設定が含まれています。
- [**レポートの配信先リスト**]: 生成されたレポートの送信先の電子メールアドレスをコンマで区切って指定します(最大10個)。

[**サブスクリプション**]タブでは、Webroot製品の詳細を確認し、アップグレードや更新を行うことができます。RMMパートナーを通じて購入した場合は、パートナーのサイトにリダイレクトされることがあります。

[**アカウント情報**]: このタブにはメインのアカウントの所有者に関する情報が表示されます。

- [**サイト/会社名**]: コンソールの定義に使用する会社名です。コンソール名を編集するには、[**名前の変更**]をクリックします。
- [**会社住所**]: アカウントの作成時に会社の住所が自動的に指定されます。住所を変更する必要がある場合はWebrootにお問い合わせください。
- [**連絡先の電子メール**]: 選択したコンソールのメインアカウントの電子メールです。電子メールを変更する必要がある場合はWebrootにお問い合わせください。
- [**連絡先電話番号**]: アカウントの作成時に電話番号が自動的に指定されます。電話番号を変更する必要がある場合はWebrootにお問い合わせください。
- [**親のキーコード**]: 選択したコンソールに割り当てられているキーコードです。このキーコードはインストールに使用しないでください。インストールには([**エンドポイント**]タブにある)サイトに割り当てられたキーコードを使用する必要があります。サブスクリプションを更新するには[**更新/アップグレード**]をクリックしてください。
- [**使用状況を表示**]: 前年の使用状況を確認できる独立したコンソールが開きます。[**使用状況**]をクリックし、プロンプトが表示されたらログインし、プロンプトが表示されたらコンソールを選択します。ログインすると、使用状況と請求に関するタブが表示されます。
    - [**使用状況**]: このタブのレポートは[**使用状況**]ページで選択した日付から30日間分を合計したものです。
        - [**CSVをダウンロード**]リンクをクリックすると、使用状況のデータをエクスポートできます。
        - [**サイトの使用状況**]ボタンをクリックすると、サイトの使用状況を絞り込んで表示できます。そのサイトの利用状況データをエクスポートすることもできます。
- [**請求書の支払い**]: 支払い履歴を確認できる独立したコンソールが開きます。[**請求書**]をクリックし、プロンプトが表示されたらログインし、プロンプトが表示されたらコンソールを選択します。ログインすると、使用状況と請求に関するタブが表示されます。
    - Webrootに直接支払う場合は、[**請求書**]タブでオンラインの支払い機能を使用できます。サービスプロバイダーまたはサードパーティに支払う場合、オンライン支払い機能は使用できません。
        - 請求ページでアカウントを選択します。必要に応じて、画面の指示に従ってアカウントを作成し、受信した電子メールを確認します。
        - 請求書を確認し、必要に応じて支払いを実行できます。
        - 自動支払を設定し、保存したクレジットカードを使用して自動的に支払うこともできます。画面の指示に従ってクレジットカード情報を保存してください。自動支払を中止する場合は、wrAccountsReceivable@opentext.comまたは営業担当者にお問い合わせください。

- [**ログイン設定**]: このセクションでは、**パスワード**の変更、**セキュリティの質問**の変更、**2FAの有効化**、**セキュリティコード**の変更を行うことができます。

[**ダウンロード**]タブには、WindowsおよびMacOSエージェントのインストール用のリンクがあります。また、インストールに適用される組み込みのキーコードのコピーもあります。これらのインストールファイルを使用して、デバイスに手動でインストールします。詳細は「*エージェントの配備* ページ 84」を参照してください。

[**Webブロックページの設定**]: このタブでは、DNS ProtectionまたはWeb Threat Shieldによってウェブサイトがブロックされたときに表示される通知ページをカスタマイズできます。

- 通知ページに独自のロゴを表示する場合は、点線のボックスにロゴをドラッグ&ドロップします。点線のボックスをクリックしてロゴを選択することもできます。
    - ロゴファイル名の拡張子は`.png`、`.gif`、または`.jpeg`でなければなりません。
    - ロゴの最大高さは50ピクセルです。
    - 幅はロゴの縦横比が維持されるよう自動的に調整されます。
    - ファイルサイズの上限は1MBです。
    - ロゴを追加すると、Webrootのロゴが「powered by Webroot」というロゴに変わります。
    - アップロードしたロゴを削除するには、点線のボックスの上にカーソルを移動し、[**現在の画像を削除**]をクリックします。「powered by Webroot」のロゴが標準のWebrootのロゴに戻ります。
- [**ウェブサイト利用不可**]: ロゴと書式ツールバーとの間にあるテキストとグラフィックが通知ページに自動的に表示されます。テキストとグラフィックの変更や削除はできません。
- [**追加情報**]: 書式バーの下にあるこの自由形式のフィールドに追加情報を入力します。
    - このテキストは変更または削除できます。
    - 500文字以下で入力してください。
- [**デフォルト設定にリセット**]: ロゴと追加情報をデフォルトの設定にリセットするには、このボタンをクリックします。

[**Unity APIアクセス**]: このタブからUnity APIにアクセスできます。

- これは、請求やレポートなどのWebrootサービスおよび情報へのアクセスを自動化する場合に使用できるREST APIです。
- 使用を開始するには[**新しいクライアント認証情報を作成する**]をクリックします。3ステップのプロセスを実行し、クライアントシークレットをメモします。情報へのアクセスやアクションの実行を目的としたこのAPIでの認証では、クライアントIDとクライアントシークレットを使用する必要があります。
- また、通知APIを有効することもできます。通知APIを使用すると、さまざまなドメインレベルで登録できる一連のイベントに基づき、Unity API通知をほぼリアルタイムで受信できます。
- 一意のクライアント認証情報は最大20個作成できます。クライアント認証情報を1つでも作成すると、そのUnity API設定をUnity APIアクセステーブルから管理できます。そこから以下のアクションを利用できます。
    - [**新規**]: [**新しいクライアント認証情報を作成する**]ダイアログボックスが開きます。
    - [**編集**]: **クライアント認証情報を編集する**]ダイアログボックスが開きます。選択したクライアント認証情報の名前、説明、Unity APIの使用目的を変更できます。API通知は、ステップ2の[イベント通知APIを使用する予定はありますか]に対して[はい]か[いいえ]で答えることで有効または無効にできます。

- [**削除**]: 選択したクライアント認証情報の記録を削除します。
- [**シークレットを更新する**]: 選択した認証情報に対するクライアント認証情報のシークレットを更新します。実行すると、以前に設定されたシークレットが失効し、今後この古いシークレットを使用した認証情報で行われるリクエストはすべて取り消されます。
- [**一時停止**]: クライアントのAPIアクセスを一時的に取り消します。選択したクライアント認証情報によるアクセスを再び有効にするには[**再開**]をクリックします。

[**詳細設定**]タブには2つの詳細設定があります。

- [**編集**]をクリックすると、フィルタを設定または削除したり、データフィルタの変更履歴を表示できます。コンソールに表示されるデータを制限するには、[データフィルタ]を適用します。このオプションを適用すると、読み込まれるデータの量によってはページの読み込みのパフォーマンスが向上する場合がありますが、表示される内容は制限されます。フィルタを適用または削除する場合、配備サイズと表示するデータの量によっては、データの更新に数分かかることがあります。
- [**変換**]をクリックすると、**マネージドサービスプロバイダー向けの表示**に変更できます。これにより、複数のサイト(会社、ビジネス、組織単位など)を管理コンソールに設定できます。キーコードや請求はサイトごとに異なります。マネージドサービスプロバイダーコンソールへの変換は不可逆的の操作で、元に戻すことはできません。

# マネージドサービスプロバイダー向けの表示の設定

[**サブスクリプション**]タブでは、Webroot製品の詳細を確認し、アップグレードや更新を行うことができます。RMMパートナーを通じて購入した場合は、パートナーのサイトにリダイレクトされることがあります。

[**アカウント情報**]: このタブにはメインのアカウントの所有者に関する情報が表示されます。

- [**サイト/会社名**]: コンソールの定義に使用する会社名です。コンソール名を編集するには、[**名前の変更**]をクリックします。
- [**会社住所**]: アカウントの作成時に会社の住所が自動的に指定されます。住所を変更する必要がある場合はWebrootにお問い合わせください。
- [**連絡先の電子メール**]: 選択したコンソールのメインアカウントの電子メールです。電子メールを変更する必要がある場合はWebrootにお問い合わせください。
- [**連絡先電話番号**]: アカウントの作成時に電話番号が自動的に指定されます。電話番号を変更する必要がある場合はWebrootにお問い合わせください。
- [**親のキーコード**]: 選択したコンソールに割り当てられているキーコードです。このキーコードはインストールに使用しないでください。インストールには([**エンドポイント**]タブにある)サイトに割り当てられたキーコードを使用する必要があります。サブスクリプションを更新するには[**更新/アップグレード**]をクリックしてください。
- [**使用状況を表示**]: 前年の使用状況を確認できる独立したコンソールが開きます。[**使用状況**]をクリックし、プロンプトが表示されたらログインし、プロンプトが表示されたらコンソールを選択します。ログインすると、使用状況と請求に関するタブが表示されます。
    - [**使用状況**]: このタブのレポートは[**使用状況**]ページで選択した日付から30日間分を合計したものです。

        - [**CSVをダウンロード**]リンクをクリックすると、使用状況のデータをエクスポートできます。
        - [**サイトの使用状況**]ボタンをクリックすると、サイトの使用状況を絞り込んで表示できます。そのサイトの利用状況データをエクスポートすることもできます。
- [**請求書の支払い**]: 支払い履歴を確認できる独立したコンソールが開きます。[**請求書**]をクリックし、プロンプトが表示されたらログインし、プロンプトが表示されたらコンソールを選択します。ログインすると、使用状況と請求に関するタブが表示されます。
    - Webrootに直接支払う場合は、[**請求書**]タブでオンラインの支払い機能を使用できます。サービスプロバイダーまたはサードパーティに支払う場合、オンライン支払い機能は使用できません。
        - 請求ページでアカウントを選択します。必要に応じて、画面の指示に従ってアカウントを作成し、受信した電子メールを確認します。
        - 請求書を確認し、必要に応じて支払いを実行できます。
        - 自動支払を設定し、保存したクレジットカードを使用して自動的に支払うこともできます。画面の指示に従ってクレジットカード情報を保存してください。自動支払を中止する場合は、wrAccountsReceivable@opentext.comまたは営業担当者にお問い合わせください。
- [**ログイン設定**]: このセクションでは、**パスワード**の変更、**セキュリティの質問**の変更、**2FAの有効化**、**セキュリティコード**の変更を行うことができます。

[**データフィルタ**]タブでは、時間ベースのフィルタをすべてのサイトに適用できます。適用する期間を選択して[**保存**]をクリックします。この設定は個々のサイト内でオーバーライドできます。また、データフィルタの変更履歴も表示されます。

[**Webブロックページの設定**]: このタブでは、DNS ProtectionまたはWeb Threat Shieldによってウェブサイトがブロックされたときに表示される通知ページをカスタマイズできます。

- 通知ページに独自のロゴを表示する場合は、点線のボックスにロゴをドラッグ&ドロップします。点線のボックスをクリックしてロゴを選択することもできます。
    - ロゴファイル名の拡張子は.png、.gif、または.jpegでなければなりません。
    - ロゴの最大高さは50ピクセルです。
    - 幅はロゴの縦横比が維持されるよう自動的に調整されます。
    - ファイルサイズの上限は1MBです。
    - ロゴを追加すると、Webrootのロゴが「powered by Webroot」というロゴに変わります。
    - アップロードしたロゴを削除するには、点線のボックスの上にカーソルを移動し、[**現在の画像を削除**]をクリックします。「powered by Webroot」のロゴが標準のWebrootのロゴに戻ります。
- [**ウェブサイト利用不可**]: ロゴと書式ツールバーとの間にあるテキストとグラフィックが通知ページに自動的に表示されます。テキストとグラフィックの変更や削除はできません。
- [**追加情報**]: 書式バーの下にあるこの自由形式のフィールドに追加情報を入力します。
    - このテキストは変更または削除できます。
    - 500文字以下で入力してください。
- [**デフォルト設定にリセット**]: ロゴと追加情報をデフォルトの設定にリセットするには、このボタンをクリックします。

[**Unity APIアクセス**]: このタブからUnity APIにアクセスできます。

- これは、請求やレポートなどのWebrootサービスおよび情報へのアクセスを自動化する場合に使用できるREST APIです。
- 使用を開始するには[**新しいクライアント認証情報を作成する**]をクリックします。3ステップのプロセスを実行し、クライアントシークレットをメモします。情報へのアクセスやアクションの実行を目的としたこのAPIでの認証では、クライアントIDとクライアントシークレットを使用する必要があります。
- また、通知APIを有効することもできます。通知APIを使用すると、さまざまなドメインレベルで登録できる一連のイベントに基づき、Unity API通知をほぼリアルタイムで受信できます。
- 一意のクライアント認証情報は最大20個作成できます。クライアント認証情報を1つでも作成すると、そのUnity API設定をUnity APIアクセステーブルから管理できます。そこから以下のアクションを利用できます。
    - [**新規**]: [**新しいクライアント認証情報を作成する**]ダイアログボックスが開きます。
    - [**編集**]: **クライアント認証情報を編集する**]ダイアログボックスが開きます。選択したクライアント認証情報の名前、説明、Unity APIの使用目的を変更できます。API通知は、ステップ2の[イベント通知APIを使用する予定はありますか]に対して[はい]か[いいえ]で答えることで有効または無効にできます。
    - [**削除**]: 選択したクライアント認証情報の記録を削除します。
    - [**シークレットを更新する**]: 選択した認証情報に対するクライアント認証情報のシークレットを更新します。実行すると、以前に設定されたシークレットが失効し、今後この古いシークレットを使用した認証情報で行われるリクエストはすべて取り消されます。
    - [**一時停止**]: クライアントのAPIアクセスを一時的に取り消します。選択したクライアント認証情報によるアクセスを再び有効にするには[**再開**]をクリックします。

# DNSプロテクション

DNSプロテクションは、エージェントを介して個々のデバイスを保護するDNSフィルタリングサービスとして、またDNSリクエストをWebroot DNSリゾルバーに転送することで、ネットワーク上のすべてのデバイスを保護するサービスとしても機能します。

[**設定**]でDNSプロテクションを有効にした場合、Webroot管理コンソールにはDNSプロテクションに特有のタブや設定が表示されるようになります。これらはDNSプロテクションが無効の場合は表示されません。

## DNSプロテクションを使用するには

1. Webroot管理コンソールに登録します。詳細は「*を使用するには* ページ 10」を参照してください。
2. DNSプロテクションの有効化と設定を行います。詳細は「DNSプロテクションの有効化と設定」を参照してください。
3. エンドポイントが**DNSプロテクション**で保護されていることを確認します。
    - DNSプロテクションエージェントを配備します。詳細はの「*ネットワークの設定* ページ 112」を参照してください。
    - ネットワークを保護します。詳細は『』の「*ネットワークの設定* ページ 112」を参照してください。

### DNSプロテクションの有効化と設定

また、Webroot管理コンソールで有効化する必要があります。

**DNSプロテクションの有効化と設定を行うには、以下の手順に従います。**

1. ナビゲーションペインで[**設定**]タブをクリックします。
2. [**サブスクリプション**]タブで、DNSプロテクションの無料体験版をアクティブ化するか、サブスクリプションを有効にします。
3. 目的のサイトのDNSプロテクションを有効にします。
    - **マネージドサービスプロバイダー向けの表示**を使用している場合は、ナビゲーションペインで[**サイトリスト**]タブに移動します。次に、DNSプロテクションを有効にするサイトを選択し、[**DNSプロテクション**]タブをクリックします。
    - **ビジネス向けの表示**を設定している場合は、ナビゲーションペインで[**DNSプロテクション**]タブをクリックします。
4. スライダーコントロールを使用して、**DNSプロテクション**を有効にします。
5. 必要に応じて、キーコードのタイプを選択します。
    - [**フルバージョン**]: 制限のない完全版の製品です。このサービスは有料です。
    - [**体験版**]: 完全版の製品ですが、30日間限定の無料体験版です。
6. [**エージェント設定**]で、デフォルトのDNSサイトポリシーを選択します。新しいエージェントがインストールされた場合、このポリシーが常にデフォルトで割り当てられます。
    - [**DNS保護レベル: 高**]: 推奨されている開始時のポリシーです。すべてのセキュリティカテゴリーおよび、人材の保護、問題あり/規制関連のコンテンツがブロックされます。

- [**DNS保護レベル: 中**]: [**DNS保護レベル: 高**]と同等のセキュリティを提供しますが、問題あり/リーガルのコンテンツはブロックされません。
- カスタムポリシーも簡単に作成できます。詳細は「*DNSプロテクションのポリシーの管理* ページ 103」を参照してください。

7. [**エージェント設定**]の[**ドメインバイパス**]設定は、Active Directoryドメインなどのローカル DNSリゾルバーで検索する必要があるドメインに使われます。
   - リストに設定されたドメインはローカルDNSリゾルバーによって解決され、フィルタリング対象とはなりません。
   - 解決に関して発生し得る問題を回避するために、使用中のアクティブディレクトリドメインを追加することを推奨します。
   - ワイルドカードを使用して、「*.webroot.com」などのサブドメインを含めることができます。
   - [**ドメインバイパスリスト**]はDNSプロテクションエージェントにのみ適用されます。
8. [**ネットワーク設定**]では、ゲストデバイスやIoTデバイスなど、ネットワーク上のすべてのデバイスを保護するための詳細を入力できます。エージェントがインストールされていない場合も入力は可能です。
   - [**静的IP**]: インターネットアクセスに使用するパブリックIPv4アドレスを特定します(WAN IP)。
   - [**動的IP**]: 静的IPアドレスが使用できない場合、動的DNSサービスに関連するドメインを入力できます。ドメインを入力すると、現在対応しているIPアドレスが[**ドメイン/IPアドレス**]ボックスの横に表示されます。
   - このIPアドレスに関連付けるポリシーを選択します。このIPアドレスから受信したDNSリクエストは、このポリシーに基づいて解決されます。
   - [**ネットワークの追加**]を選択して、このネットワークへのIPアドレスの追加を完了します。この変更は、[**保存**]をクリックするまで有効にはならないことにご注意ください。
   - 複数のネットワークまたは回線を追加する必要がある場合は、追加する**ドメイン/IPアドレス**を入力して[**ネットワークの追加**]をクリックしてください。
9. [**DNSリゾルバールックアップ**]の[ネットワークの場所]メニューから、その地域に適切なWebroot DNSリゾルバーを特定します。これは設定ではなく、最も適切なリゾルバーを特定するためのメカニズムです。
   - DNSプロテクションを有効にしたサイトに適したネットワークの場所を選択します。
   - 最適なプライマリおよびセカンダリWebroot DNSサーバーが表示されます。
   - 最適なリゾルバーを特定した後は、お使いのルーターのDNSサーバーのDNSフォワーダー(AD)として、これらのIPアドレスを使用できます。
   - ネットワーク設定を変更する前に、このサーバーへのDNS解決をテストすることを強く推奨します。たとえば、nslookupコマンド(`nslookup www.webroot.com 35.226.80.229`)を使用できます。サーバーが応答しない場合は、ネットワーク設定を更新する前に、手順8で入力したIPアドレスを確認します。
10. [**高度な設定**]で、エージェントをサーバーで有効にするかどうかを選択します。
    - 選択すると、DNSプロテクションエージェントがサーバー上で有効化され、フィルタリングを実行するようになります。

- DNSプロテクションエージェントはAzureサーバーや、DNS解決を提供する他のサービスと競合するため、通常はこの方法は推奨されません。
- DNSサーバーを保護するには、手順8と9で説明されているように、ネットワークフィルタリングを使用するためにネットワークを登録し、Webrootリゾルバーを DNSフォワーダーとして追加することを推奨します。
- [**サーバーでエージェントを有効にする**]チェックボックスを選択した場合、RDS/ターミナルサービスのサーバーや、DNSの役割を持たないその他のサーバーでDNSプロテクションエージェントが有効化され、フィルタリングを行います。

11. 完了したら、[**保存**]をクリックします。

## DNSプロテクションのポリシーの管理

DNSプロテクションのポリシーを確認または変更するには、以下の手順に従います。

1. [**管理**] > [**ポリシー**]を開きます。
2. [**DNSプロテクション**]タブから、確認または変更するポリシーを選択します。

   [**ポリシー**]のページは複数のセクションに分かれています。

   - [**プライバシー設定**]では、ユーザーのプライバシー設定とログに記録される情報を制御できます。
     - [**ユーザー情報の非表示**]: プライバシー改善のため、リクエストされたユーザー名とドメインがログ内で「非表示」という語に置き換えられます。リクエストがセキュリティリスクカテゴリーに分類される場合は、可視性を維持するためにそのドメインがログに記録されます。
     - [**ローカルエコー**]: DNSプロテクションエージェントによるDNSリクエストをローカルネットワークのDNSリゾルバーにエコーし、ファイアウォールまたはDNSサーバーでこれらのリクエストを認識できるようにします。DNSリゾルバーはプライバシー改善のために指定することが可能で、リクエストはそのリゾルバーを利用できる場合のみにエコーされます。
     - [**フェールオープン**]: Webroot DNSリゾルバーを利用できない場合に発生し得るDNS中断を回避するため、DNS解決はローカルリゾルバーに延期されるか、フィルタリングなしで返されます。
   - **リーク防止**は、DNS解決の代替ソースをブロックし、すべてのDNSリクエストがフィルタリングされ、ログに記録されるようにします。この機能にはAgentバージョン4.2以降が必要で、Windows 10以降でのみサポートされています。
     - **標準DNSリクエスト** – 有効にすると、ポート53のTCPおよびUDP経由の通信がブロックされます。
     - **DoHリクエスト** – 有効にすると、既知のDoHプロバイダーに対してポート443TCPを介した通信がブロックされます。
     - **DoTリクエスト** – 有効にすると、ポート853 TCP経由の通信がブロックされます。
     - **除外** – このフィールドを使用して、通信をブロックすべきでないDNSサーバーのIPアドレスを入力します。入力されたIPは、**標準DNSリクエスト**、**DoHリクエスト**、**DoTリクエスト**のDNSリーク防止によってブロックされません。
   - [**セキュリティ設定**]では、特定のドメインをブロックするか許可するかを指定できます。

- **キーロガーおよび監視**: キーストロークやウェブサイト閲覧行動を追跡するソフトウェアエージェント用のダウンロードとディスカッションが含まれるドメイン。
- **マルウェアサイト**: 実行ファイル、ドライブバイ感染サイト、悪意のあるスクリプト、ウイルス、トロイの木馬など、悪意のあるコンテンツが含まれていることがわかっているサイト。
- **フィッシングおよびその他の詐欺行為**: 信頼できるサイトを装っていることが知られているドメイン。通常、ユーザーから個人情報を入手することを目的としています。これらのサイトは通常、すぐに消滅してしまうため、このようなサイトの例もすぐに使えなくなります。
- **プロキシ回避とアノニマイザー**: プロキシサーバーまたはその他の方法を使用して、URLフィルタリングまたは監視機能を回避するドメイン。
- **スパイウェアおよびアドウェア**: ユーザーに知られず、あるいは明確な同意なく行われる情報収集または追跡を提供、もしくは促すスパイウェアまたはアドウェアが含まれていることがわかっているドメイン。このポリシーには、迷惑な広告ポップアップや、ユーザーのコンピュータにインストールされる可能性のあるプログラムを含むサイトも含まれます。
- **ボットネット**: ネットワーク攻撃の発信源となるボットネットワークの一部であることがわかっているドメイン。攻撃には、スパムメッセージ、サービス拒否(DOS)攻撃、SQLインジェクション、プロキシジャッキング、またその他の迷惑な接触などが含まれます。
- **スパムURL**: スパムメッセージに含まれるドメイン。

- [**コンテンツ設定**]には、利用可能なコンテンツを制御するためのカテゴリーが含まれます。
  - **人材の保護**
    - **乱用薬物**: 非合法薬物、違法薬物、乱用薬物に関連するドメイン。危険ドラッグ、シンナー遊び、処方薬の誤用、その他合法薬物の乱用などがあります。
    - **アダルトおよびポルノ**: 性的関心を喚起することを目的として性的に露骨なコンテンツを扱うドメイン。アダルト玩具やビデオなどのアダルト商品を扱うサイトなどがあります。このカテゴリーには、性的に露骨なオンライングループのドメイン、性的な話や性的行為に関する記述があるサイト、ビデオ通話、エスコートサービス、ストリップクラブなどの成人向けサービスのサイト、および性的に露骨なアートを扱うサイトも含まれます。
    - **デート**: 出会い系サイトなど、個人的な関係を確立することを目的としたドメイン。
    - **性教育**: 生殖、性的発育、安全な性行為の実践、性感染症、性的区別、避妊、避妊薬、より良い性生活に対するヒント、性的機能を高める製品に関する情報が掲載されたドメイン。
    - **水着および下着**: 水着、ランジェリー、その他の挑発的な衣類が表示されるドメイン。
    - **グロテスク**: 血液または嘔吐などの身体機能が表示されるドメイン。
    - **ヌード**: 人体のヌードまたはセミヌードの描写を扱うドメイン。性的意図がない場合がありますが、ヌーディストや裸体主義者のサイト、ヌードの絵画、芸術的な性質を持つフォトギャラリーなどが含まれます。

- **アルコールおよびタバコ**: アルコール飲料や、たばこ製品とその関連品の販売に関する情報を提供、宣伝、または支援するドメイン。

- **問題あり/リーガル**
  - **カルトおよびオカルト**: 占星術(星占いを含む)、まじない、呪文、魔力、または超自然的な存在を介して、実際の出来事に作用または影響を与えようとする方法、手段、その他のリソースを提供するドメイン。
  - **ギャンブル**: 現金または仮想マネーを使用するドメイン。賭け事、宝くじへの参加、ギャンブル、ナンバー賭博の運営に関する情報とアドバイスを含むドメイン、オンラインカジノや国外のギャンブル事業、スポーツくじおよびプール賭博、大きな報酬を提供するあるいは多額の賭け金が必要なバーチャルスポーツおよびファンタジーリーグが含まれます。ドメイン上でギャンブルができないホテルやリゾートのドメインは、「ライフスタイル」、「旅行」、「一般情報」、「ローカル情報」に分類されます。
  - **マリファナ**: マリファナの使用、栽培、歴史、文化、または法的問題を扱うドメイン。
  - **ハッキング**: 通信機器/ソフトウェアへの違法あるいは疑わしいアクセスまたは使用のためのドメイン、またはネットワークおよびシステムに侵入する可能性のあるプログラムを開発および配信するためのドメイン。コンピュータプログラムやその他システムのライセンス取得および使用料金を回避するためのドメインも含まれます。
  - **武器**: 銃器、ナイフ、格闘技用の道具といった武器の販売、レビュー、説明を提供するドメイン。アクセサリや他の改造に関する情報を提供するドメインも含まれます。
  - **リードメール**: 電子メールまたはWebページ内の特定のリンクをクリックして閲覧すると、現金または賞品の形でユーザーに支払いがされるドメイン。
  - **問題あり**: ユーザーのブラウザ操作またはクライアントを独特な、予想外な、あるいは疑わしい方法で制御するドメイン。一攫千金をアピールするドメインも含まれます。
  - **嫌悪および差別**: 憎悪犯罪や人種差別的なコンテンツまたは言動を擁護するドメイン。
  - **暴力**: 暴力、暴力描写、または暴力的な方法を推奨するドメイン。ゲーム/マンガにおける暴力および自殺も含まれます。
  - **不正行為**: 不正行為を助け、無料で使用できるエッセーや試験のコピー、盗作などのコンテンツを含むドメイン。
  - **違法**: 逮捕を免れるための方法、著作権および知的財産権の侵害など、犯罪行為を扱うドメイン。
  - **中絶**: 妊娠中絶への賛同または反対を主張するドメイン。
- **ソーシャルメディア/インターネットコミュニケーション**
  - **ソーシャルネットワーキング**: SNSなど、ユーザー同士の交流や、メッセージおよび画像の投稿、その他の方法でコミュニケーションが行われるユーザーコミュニティ

を持つドメイン。

- **個人サイトおよびブログ**: 個人またはグループによって投稿されるコンテンツを持つドメイン。ブログも含まれます。
- **オンライングリーティングカード**: 電子カードを提供するドメイン。
- **検索エンジン**: キーワードまたは語句を使用して、テキスト、Webサイト、画像、動画、ファイルを含む検索結果を表示するドメイン。
- **インターネットポータル**: インターネット上のより幅広いコンテンツやトピックを集めたドメイン。
- **Web広告**: 広告、メディアコンテンツ、バナーを含むドメイン。
- **ウェブベースの電子メール**: ウェブベースの電子メールおよび電子メールクライアントを提供するドメイン。
- **インターネットコミュニケーション**: インターネット電話、メッセージの送受信、VoIPサービス、WiFi、および関連ビジネスを提供するドメイン。
- **動的に生成されたコンテンツ**: URLに渡された引数、あるいはジオロケーションといったその他の情報をもとにコンテンツを動的に生成するドメイン。
- **パークドメイン**: ホストエンティティに収益を生む可能性があるが、通常はユーザーにとって有益なコンテンツが含まれない限定コンテンツやクリックスルー広告をホストするドメイン。
- **プライベートIPアドレス/URL**: プライベートネットワーク用にIPアドレスを配布する組織によって確保されたIPアドレスやプライベートドメインに割り当てられたドメイン。

- **ショッピング**
  - **オークション**: 個人間でのサービスや商品の購入の支援を主な目的としたドメイン(案内広告を除く)。
  - **ショッピング**: デパート、小売店、会社カタログ、および消費者または企業によるオンラインショッピングや物品およびサービスの購入が可能なその他のドメイン。
  - **シェアウェアおよびフリーウェア**: スクリーンセーバー、アイコン、壁紙、ユーティリティ、着信音など、フリーソフトウェア、オープンソースコード、または寄付を要求するダウンロードが可能なドメイン。
- **エンターテインメント**
  - **エンターテインメントおよびアート**: 映画、ビデオ、テレビ、音楽および番組ガイド、本、マンガ、映画館、ギャラリー、アーティスト、またはエンターテインメントに関するレビュー、舞台芸術(演劇、寄席演芸、オペラ、交響楽団など)、博物館、ギャラリー、図書館、アーティストのサイト(彫刻や写真など)を含むドメイン。
  - **ストリーミングメディア**: 音声または動画コンテンツの販売、配信、ストリーミングに関するドメイン。視聴者向けにこのようなダウンロードを提供するドメインも含まれます。
  - **ピアツーピア**: ピアツーピア(P2P)のクライアントおよびアクセスを提供するドメイン。トレントおよび音楽ダウンロードプログラムも含まれます。

- **ゲーム**: ゲームプレイやダウンロード、ビデオゲーム、コンピュータゲーム、電子ゲーム、ゲームに関するヒントやアドバイス、隠しコマンドの取得方法に関するドメイン。ボードゲームの販売に特化したドメイン、ゲームプレイに特化したジャーナルや雑誌、オンラインの懸賞や景品配布の主催、ゲームまたはゲームプレイを主催するファンタジースポーツのドメインも含まれます。
- **音楽**: 楽曲の販売、配信、ストリーミング、また音楽グループやパフォーマンス、歌詞、音楽ビジネスについての情報に関するドメイン。

- **ライフスタイル**
  - **旅行**: 航空会社および航空券予約代理店、旅行の計画、予約、車両レンタル、旅先の説明、ホテルやカジノの宣伝に関するドメイン。
  - **ホームおよびガーデン**: 家のメンテナンス、ホームセキュリティ、装飾、料理、ガーデニング、家電、デザインなどの家庭の話題や家庭用製品に関するドメイン。
  - **宗教**: 教会、集会場(シナゴーグ)、またはその他の礼拝所を含む、従来型または非従来型の宗教的または準宗教的なテーマを扱うドメイン。
  - **狩猟および釣り**: スポーツハンティング、銃関連の団体、釣りに関するドメイン。
  - **社会**: 一般大衆に関するさまざまなトピックやグループ、つながり、および安全や子供、社会、慈善団体といった、さまざまな人々に影響を及ぼす幅広い問題に関するドメイン。
  - **スポーツ**: チームや連盟のWebサイト、国外、国内、大学、プロのスポーツ関連スコアおよびスケジュール、スポーツ関連のオンライン雑誌またはニュースレターに関するドメイン。
  - **ファッションおよび美容**: ファッション雑誌、美容、衣服、化粧品、スタイルに関するドメイン。
  - **レクリエーションおよび趣味**: 模型飛行機の収集、野外活動(ハイキング、キャンピング、ロッククライミングなど)、特殊な芸術作品やクラフト、技術、動物およびペット関連の情報、トレーニング、ショー、動物愛護協会などのレクリエーションの娯楽に関する情報やつながり、フォーラム、および出版物についてのドメイン。

- **企業/公的機関/サービス**
  - **不動産**: 不動産または有形固定資産の賃借、購入、または売却、家の売買に関するヒント、不動産業者、賃貸業または引っ越しサービス、および物件の改善に関するドメイン。
  - **コンピュータおよびインターネット セキュリティ**: コンピュータおよびインターネット セキュリティ、セキュリティを主題とするディスカッショングループに関するドメイン。
  - **金融サービス**: 銀行業務と、貸付や会計業務、保険、銀行、住宅ローン、損害保険会社といったその他の財務情報を提供するドメイン(市場情報、仲介業務、取引サービスを提供するドメインは除く)。
  - **ビジネスおよび経済**: 企業、企業のウェブサイト、ビジネス情報、経済、マーケティング、管理、起業家精神に関するドメイン。
  - **コンピュータおよびインターネットの情報**: 技術的な情報を含む一般的なコンピュータ情報およびインターネット情報に関するドメイン。SaaS (サービスとしての

ソフトウェア)、およびインターネットサービスを提供するその他のドメインも含まれます。

- **軍**: 軍事、軍部門、軍隊、および軍事史に関するドメイン。
- **個別の株に関するアドバイスおよびツール**: 金融投資の戦略、相場、ニュースなどの市場情報を含む、証券取引および投資資産の管理を促進または支援するドメイン。
- **トレーニングおよびツール**: 遠隔学習および職業専門学校、オンライン講座、職業訓練、ソフトウェアのトレーニング、技能研修に関するドメイン。
- **パーソナルストレージ**: オンラインストレージのサービスや、ファイル、音楽、画像やその他データの投稿サービスを提供するドメイン。
- **公的機関**: 各地方自治体および中央政府と政府機関、また主税局、公共サービス、救急サービスといった公的機関のサービスに関するドメイン。さまざまな公的機関に関する法律について考察または説明するドメインも含まれます。
- **コンテンツ配信ネットワーク**: 広告、メディア、ファイル、画像、ビデオなど、第三者向けのコンテンツおよびデータ配信に関するドメイン。
- **自動車**: 自動車のレビュー、車の購入または販売に関するヒント、部品カタログ、中古車売買、写真、およびオートバイやボート、自動車、トラック、RV車に関する話題、自動車の改造についての定期刊行物および雑誌に関するドメイン。
- **ウェブホスティング**: ウェブページや、ウェブサイトの開発、公表、プロモーションに関する情報を扱う無料または有料のホスティングサービスを提供するドメイン。

- **一般情報**
  - **リーガル**: 法務・法律関係のトピック、法律事務所、法律問題に関するディスカッションや分析を扱うドメイン。
  - **ローカル情報**: レストラン、エリア/地域の情報、お勧めの場所に関する情報を含む市町村ガイドおよび観光情報に関するドメイン。
  - **求人検索**: 職探しの支援、有望な雇用主(従業員を募集している雇用主)を探すためのツールの提供、採用情報検索および学校の就職あっせんを行うドメイン。
  - **翻訳**: ユーザーがさまざまな言語でページを閲覧できるようにする言語翻訳サイトを参照しているドメイン。これらのドメインでは、翻訳サイトのURLのコンテキスト内に閲覧対象ページのコンテンツが表示されるため、フィルタリングを回避することができます。
  - **参照資料および研究**: オンライン辞書、地図、人口調査、年鑑、図書目録、家系図、科学的情報を含む私的、専門的、または教育的な参考資料に関するドメイン。
  - **哲学的および政治的主張**: 政治、哲学、議論、および主義主張を推進するための具体的な視点や立場の奨励に関するドメイン。
  - **教育機関**: 幼稚園、小学校、中学校、高校、短大、大学、専門学校やその他教育的内容に関する情報(入学案内や授業料、講義摘要を含む)に関す

るドメイン。

- **キッズ**: 子供とティーンのために設計されたドメイン。
- **ニュースおよびメディア**: ラジオ放送局や雑誌、オンライン新聞、ヘッドラインニュースサイト、ニュース配信サービス、カスタマイズできるニュースサービス、気象情報関連のドメインなど、時事、またはその日の最新のトピックが掲載されているドメイン。
- **健康および医薬品**: 全般的な健康、フィットネス、健康維持に関する伝統的および非伝統的な方法とトピックに関するドメイン。病気、さまざまな健康状態、歯科、精神科、眼科や、その他専門医に関する医療関連情報、病院や診療所、医療保険、美容整形に関する情報が掲載されているドメインも含まれます。
- **画像およびビデオの検索**: 写真および画像の検索、オンラインフォトアルバム、デジタルフォトエクスチェンジ、および画像ホスティングを提供するドメイン。

- **未分類のドメイン**: Webrootによって前述のいずれのカテゴリーにも分類されていないドメイン。未分類(Uncategorized)のドメインを分類付けするにはサポートにお問合せください。

- **追加のフィルタリング**: 多くの検索エンジンでは、露骨なコンテンツ、成人向けコンテンツ、不適切なコンテンツを制限するフィルタリングオプションを適用できます。これは、フィルタに関連付けられた対応IPアドレスを返すことで、DNSを介して行われます。
  - [**Google SafeSearchを有効にする**]: www.google.comに対するDNSリクエストはforcesafesearch.google.comに解決され、検索結果から露骨なコンテンツがフィルタリングされます。
  - [**DuckDuckGoセーフサーチを有効にする**]: www.duckduckgo.comに対するDNSリクエストがsafe.duckduckgo.comに解決され、検索結果から成人向けコンテンツが除外されます。
  - [**Bingセーフサーチを有効にする**]: www.bing.comに対するDNSリクエストがstrict.bing.comに解決され、検索結果から不適切なコンテンツが除外されます。
  - [**YouTube制限付きモードを有効にする] (標準モード)**: www.youtube.comに対するDNSリクエストがrestrictmoderate.youtube.comに解決されます。
  - **[YouTube制限付きモードを有効にする] (厳格モード)**: www.youtube.comに対するDNSリクエストがrestrict.youtube.comに解決されます。

## DNSプロテクションエージェントのインストール

DNSプロテクションエージェントのインストールには、以下の2つのオプションを利用できます。

- MSIをダウンロードしてインストール: このオプションは、DNSプロテクションエージェントをWebrootエンドポイントプロテクションなしで使用する場合に利用されます。提供されたMSIを使ってWebroot管理コンソールに事業体を追加することで、コンソールの設定と管理ができるようになります。詳細は「*MSIを使用した、DNSプロテクションエージェントのインストール* ページ 110」を参照してください。
- Webrootエンドポイントプロテクションを使用したインストール: このオプションは、DNSプロテクションエージェントをWebrootエンドポイントプロテクションと組み合わせて使用する場合に使われます。詳細は「*エンドポイントプロテクションを介したDNSプロテクションエージェントのインストール* ページ 110」を参照してください。

## MSIを使用した、DNSプロテクションエージェントのインストール

**MSIを使用してDNSプロテクションエージェントをインストールするには、以下の手順に従います。**

1. Webroot管理コンソールで、[**DNSプロテクション**]タブに移動します。
    - DNSプロテクションが有効になっていることを確認します。詳細は「*DNSプロテクションの有効化と設定* ページ 101」を参照してください。
    - **マネージドサービスプロバイダー向けの表示**を使用している場合は、ナビゲーションペインで[**サイトリスト**]タブに移動します。次に、DNSプロテクションを有効にするサイトを選択し、[**DNSプロテクション**]タブをクリックします。
    - **ビジネス向けの表示**を設定している場合は、ナビゲーションペインで[**DNSプロテクション**]タブをクリックします。
2. [**DNSプロテクション**]タブの[**エージェントのインストール**]ボックスで、[**MSIによるDNSプロテクションエージェントの配備**]リンクをクリックします。
3. MSIを実行します。
    - MSIをシステム上で直接実行する場合、キーコードの入力を促すプロンプトが表示されます。[**DNS Protectionエージェントのインストール**]ボックスに表示された、DNSプロテクションのインストール先のサイトに対応するキーコードを入力します。
    - MSIは、コマンドライン、スクリプト、またはActive Directoryを通じて起動することもできます。[**DNS Protectionエージェントのインストール**]ボックスに表示されたキーコードを使用します。エージェントを正常にインストールするには、`keycode=`に以下のとおり記述します。

      ```
      Msiexec /i wrdnsp.msi /quiet keycode=xxxx-xxxx-xxxx-xxxx-xxxx
      ```

MSIの制限のため、MSIの名前を`wrdnsp.msi`から変更することは推奨されません。

インストール後の再起動は不要です。

## エンドポイントプロテクションを介したDNSプロテクションエージェントのインストール

Webroot エンドポイントプロテクションとDNSプロテクションの両方を使用する場合、DNSプロテクションエージェントはエンドポイントプロテクションを介してインストールする必要があります。エンドポイントプロテクションを使用しているシステムでMSIが使用されている場合、あるいはDNSプロテクションを使用しているシステムにエンドポイントプロテクションを追加する場合、DNSプロテクションエージェントはエンドポイントプロテクションの設定によって管理されます。

**エンドポイントプロテクションのポリシーを使用してDNSプロテクションエージェントを配備するには、以下の手順に従います。**

1. ナビゲーションペインで、[**管理**] > [**ポリシー**]に移動します。
2. [**エンドポイントプロテクション**]タブで、DNSプロテクションエージェントをインストールする事業体を使用しているポリシーを選択します。
    - このポリシーはコピーを作成しておくことが推奨されます。編集が完了したら、この新しいポリシーを、DNSプロテクションエージェントをインストールする事業体に適用できます。
    - あるいは、このポリシーを編集して(システムポリシーを除く) DNSプロテクションエージェントをインストールすることもできます。影響を受けるシステムについては、[**ポリシーの使用状況**]セクションで確認できます。

3. [**DNSプロテクション**]セクションで、[**DNSプロテクションをインストール**]のオプションを[**オン**]に設定します。
4. [**保存**]をクリックします。

この新しいポリシーをデフォルトとして、グループや個々の事業体に適用できるようになりました。

このポリシーを使用する事業体が次回チェックインする際に、DNSプロテクションエージェントがインストールされます。

DNSプロテクションエージェントがエンドポイントにインストールされると、以下が行われます。

- DNSプロテクションエージェントが、キーコードおよび関連するDNSプロテクションライセンスを検証します。
- エージェントが、利用可能な最新バージョンに自動的に更新されます。
- 新たに「Webroot DNS Protection Agent」という名のサービスが作成および開始されます。
- サービスが開始すると、アクティブディレクトリなどの内部DNS解決のため、アクティブなネットワークアダプタのDNS設定が識別されます。
- このサービスは続けて、DNSリクエストがエージェントにリダイレクトされるように、ネットワークアダプタのDNS設定(IPv4とIPv6の両方)をループバックアドレス(127.0.0.1と::1)に設定します。
- すべての外部DNSリクエストはDoH (DNS over HTTPS)を介してWebroot DNSリゾルバーに送信され、高速でフィルタリングされて解決されます。
- すべてのActive Directoryとローカルドメインリクエストは、事前に識別されたアクティブなネットワークアダプタ用のDNSリゾルバーによって解決されます。
- DNS Protection Agentサービスの実行中は、ネットワークアダプタのDNSを変更しても、直ちにループバックに戻されます。
- サービスが停止するかエージェントがアンインストールされた場合、ネットワークアダプタのDNS設定が元の設定に戻ります。

以下の場合、DNSプロテクションエージェントはアンインストールされます。

- エンドポイントプロテクションをDNSプロテクションの体験版と併用していて体験版の有効期限が切れた場合。次回のデバイスのチェックイン時にDNSプロテクションエージェントが自動的にアンインストールされます。
- DNSプロテクションをインストールしないようにエンドポイントプロテクションのポリシーが変更された場合。次回のデバイスのチェックイン時にDNSプロテクションが自動的にアンインストールされます。
- DNSプロテクションを実行しているデバイスに、エージェントのアンインストールコマンドが送信された場合。
- [**プログラムの追加と削除**]でDNSプロテクションエージェントがアンインストールされた場合。ただし、そのエージェントがエンドポイントプロテクションエージェントによってインストールされた場合は、自動的に再インストールされます。
- サイトが非アクティブにされた場合。DNSプロテクションエージェントは自動的にアンインストールされます。

DNSプロテクションエージェントがエンドポイントプロテクションを介さずMSIで直接インストールされ、ライセンスや体験版の期限が切れた場合、DNSプロテクションエージェントはDNSリクエストのフィルタリングと管理を停止します。また、DNSプロテクションエージェントのDNS設定は元の値に戻り、再度ライセンスが認証さ

れた場合にのみフィルタリングを再開します。**アンインストール**エージェントコマンドを実行すると、DNSプロテクションエージェントがその事業体から削除されることにご注意ください。

# ネットワークでのDNSプロテクションの利用

DNSプロテクションは、ネットワークに関連付けられたIPアドレスまたはドメインを登録し、ルーターとDNSフォワーダーを設定することで、ネットワーク上のすべてのデバイスを保護します。これにはDNSプロテクションエージェントを実行していないデバイスも含まれます。Wi-FiやゲストネットワークなどのあらゆるネットワークのDNSを制御できると同時に、VPN経由で接続したデバイスも保護できます。

## ネットワークの設定

**ネットワークをDNS Protection用に設定するには、以下の手順に従います。**

1. Webroot管理コンソールで、[**DNS Protection**]タブに移動します。
    - **マネージドサービスプロバイダー向けの表示**を使用している場合は、ナビゲーションペインで[**サイトリスト**]タブに移動します。次に、DNSプロテクションを有効にするサイトを選択し、[**DNSプロテクション**]タブをクリックします。
    - **ビジネス向けの表示**を設定している場合は、ナビゲーションペインで[**DNSプロテクション**]タブをクリックします。
2. [**ネットワーク設定**]セクションで、保護対象のネットワークの[**ドメイン/IPアドレス**]を入力します。
    - [**静的IP**]: インターネットアクセスに使用するパブリックIPv4アドレスを入力します(WAN IP)。
    - [**動的IP**]: 静的IPアドレスを使用できない場合、ダイナミックDNSサービスに関連するドメインを入力します。ドメインを入力すると、現在対応しているIPアドレスが[**ドメイン/IPアドレス**]ボックスに表示されます。
    - このIPアドレスに関連付けるポリシーを選択します。このIPアドレスから受信したDNSリクエストは、このポリシーに基づいて解決されます。
    - [**ネットワークの追加**]をクリックして、このネットワークへのIPアドレスの追加を完了します。この変更は、[**保存**]をクリックするまで有効にはならないことにご注意ください。
    - 複数のネットワークまたは回線を追加する場合は、追加する**ドメイン/IPアドレス**を入力して[**ネットワークの追加**]をクリックしてください。
3. [**DNSリゾルバールックアップ**]セクションで[**ネットワークの場所**]リストからネットワークの場所を選択すると、その地域に適切なWebroot DNSリゾルバーを特定できます。これは設定ではなく、最も適切なリゾルバーを特定するための表示のみの機能です。
    - DNS Protectionを有効にしたサイトに適したネットワークの場所を選択します。最適なプライマリおよびセカンダリWebroot DNSサーバーが表示されます。
    - 最適なリゾルバーを特定した後は、お使いのルーターのDNSサーバーのDNSフォワーダー(AD)として、これらのIPアドレスを使用できます。
    - ネットワーク設定を変更する前に、このサーバーへのDNS解決をテストすることを推奨します。たとえば、次のコマンドを使用できます。`nslookup`:

```
nslookup www.webroot.com 35.226.80.229
```

    - サーバーが応答しない場合は、DNSフォワーダーのルーターを更新する前に、IPアドレスを確認します。
4. ルーターまたはDNSフォワーダーを更新して、Webroot DNS Protectionサーバーを使用できるようにします。

- たとえば、Windows DNSサーバーの場合、[**サーバーマネージャー**] > [**ツール**] > [**DNS**]の順に移動します。
- お使いのDNSサーバーを右クリックし、[**プロパティ**]を選択します。
- [**フォワーダー**]タブで、フォワーダーのリストの一番上にWebroot DNS Protectionサーバーを追加します。

### ネットワーク証明書とライセンスのインストール

ドメインがブロックされたときに表示される通知ページを「**ブロックページ**」と呼びます。

ブロックされたドメインにアクセスしようとしたときにブロックページを適切に表示するには、信頼されたルート証明機関ストア(通常は `..\Certificates - Current User\Trusted Root Certification Authorities\Certificates`)にWebroot証明書をインストールすることが推奨されます。

DNSプロテクションエージェントを使用している場合、この作業は必要ありません。

証明書がなくてもデバイスは保護されますが、その場合は**ブロックページ**ではなく証明書のエラーが表示されるため、このページは単にユーザーへの便宜的な表示となります。証明書は、次のように手動でインストールすることも、`certinstaller.exe`ツールを使用してインストールすることもできます。

- 証明書インストーラー:

  https://download.webroot.com/DNS/certinstaller.exe

- 証明書:

  https://download.webroot.com/DNS/certificates/webroot-certificate.p7b

  https://download.webroot.com/DNS/certificates/webroot-certificate.pem

## DNSプロテクションのオーバーライド

[**オーバーライド**]: ポリシーやドメインのカテゴリにかかわらず許可またはブロックする必要のあるファイルやドメインを指定できます。

**マネージドサービスプロバイダー (MSP) 向けの表示**において、グローバルファイルのオーバーライドはサイトの[**詳細**]タブで[**グローバルオーバーライドの追加**]が有効になっているすべてのサイトに適用されます(推奨)。

サイトオーバーライドはグローバルオーバーライドより常に優先されます。

ポリシーオーバーライドはサイトオーバーライドより常に優先されます。

オーバーライドの変更は適用から15分以内に複製されます。

DNSオーバーライドにアクセスするには、[**管理**] > [**オーバーライド**]に移動し、[**ウェブのオーバーライド**]タブを選択します。

### DNSプロテクションのドメインの許可とブロック

**DNSプロテクション**を使用していない場合、**ウェブのオーバーライド**はエンドポイントプロテクションの機能のWeb脅威シールドに適用され、許可された機能のみが効力を持ちます。

**DNSプロテクション**を使用している場合、[**ウェブのオーバーライド**]タブで指定した**Webオーバーライド**は、お使いのDNSプロテクションのオーバーライドです。

# DNSプロテクションレポート

ナビゲーションペインで[**レポート**]をクリックすると、すべてのレポートオプションが表示されます。

DNSプロテクションレポートは、DNSプロテクションを使用している場合にのみ適用されます。

- [**DNS: アクティブなホスト**]: 完全な閲覧履歴とインターネットの使用状況を表示
- [**DNS: ブロックされたボットネットのコマンド&制御**]: コマンド&制御のソフトウェアを使用してボットネットに分類され、ブロックされたドメインを表示
- [**DNS: 最もブロックされたカテゴリー**]: 最も頻繁にブロックされたドメインをカテゴリー別に表示
- [**DNS: 最もブロックされたドメイン**]: 最も頻繁にブロックされたドメインを上位12ドメインまで表示
- [**DNS: 最もリクエストの多かったカテゴリー**]: 最も頻繁にリクエストされたドメインをカテゴリー別に表示
- [**DNS: リクエスト数別サイト順位**]: リクエストされた上位ドメインに対する日別のリクエスト数を表示

# Security Awareness Training

Webroot Security Awareness TrainingはWebroot Endpoint Protectionとも連携しますが、個別に購入することになります。Security Awareness Trainingは、サイバーセキュリティのベストプラクティスに関する理解を深め、実践できるようになることを目的に設計されたホスト型のプログラムです。このプログラムには、フィッシングシミュレータとトレーニングコース、およびその他のツールが含まれます。

Security Awareness Trainingのモジュールはキャンペーンを介して管理されます。キャンペーンとは、対象ユーザーのグループに送信される単一のフィッシングシミュレーションまたは一連のトレーニングコースを意味します。キャンペーンにはセキュリティ意識向上プログラムのレポートや管理も含まれます。

キャンペーンを計画および実行する際は、以下の点を考慮してください。

- 全員に参加してもらいます。すべての部門で、新規採用者と既存の従業員を含めるようにしてください。あらゆるレベルの従業員を含め、サービスプロバイダーのスタッフもトレーニングを受ける必要があります。
- 特定の脅威やリスク、業界の規制やコンプライアンスの観点から、キャンペーンを受けるグループにとってこのトレーニングが適切であることを確認します。
- 技術的な知識については特定のレベルを想定しないでください。基本的なことから始めて、より具体的な内容に進みます。
- トレーニングを受けるすべての人に、明確な参加ガイドラインを提供します。
- 行動の変化には時間がかかります。
- セキュリティのトレーニングは定期的に改善する必要があります。
- フィッシングシミュレーションとトレーニングキャンペーンを毎月実施することを検討します。
- 測定、評価、報告を定期的に行います。
- フィッシングテストに関する話題が従業員やスタッフに広まると、結果の精度が損なわれる可能性があることに注意します。
- テスト結果を全員に伝え、参加への感謝の意を伝えます。
- 新しいリスクを定期的に周知します。

## Security Awareness Trainingを使用するには

始める前に、電子メールサーバーが、フィッシングシミュレーションやトレーニングでユーザーに送信される電子メールをブロックしないことを確認します。

**Security Awareness Trainingを使用するには、以下の手順に従います。**

1. **Endpoint Protection**の登録と設定を行います。**Security Awareness Training**を使用するためにエージェントを配備する必要はありません。詳細は「*を使用するには* ページ 10」を参照してください。
2. **Security Awareness Training**の有効化と設定を行います。詳細は「*Security Awareness Trainingの有効化* ページ 116」を参照してください。
3. トレーニング対象のユーザーを選択します。詳細は「*トレーニング対象のユーザーの選択* ページ 116」を参照してください。

## Security Awareness Trainingの有効化

**Security Awareness Trainingを有効にするには、以下の手順に従います。**

1. [**セキュリティ意識向上トレーニング**]に移動します。
    - **ビジネス向けの表示**の場合、ナビゲーションペインで[**セキュリティ意識向上トレーニング**]をクリックし、[**設定**]タブを開きます。
    - **マネージドサービスプロバイダー (MSP) 向けの表示**の場合、ナビゲーションペインで[**サイトリスト**]をクリックし、サイトを開き、[**セキュリティ意識向上トレーニング**]タブを開きます。
2. [**セキュリティ意識向上トレーニング**]スイッチを有効にします。
3. 必要に応じて、キーコードのタイプを選択します。
    - [**フルバージョン**]: 制限のない完全版の製品を使用できるキーコードです。このサービスは有料です。
    - [**体験版**]: 完全版の製品ですが、30日間限定の無料体験版を使用できるキーコードです。
4. [**保存**]をクリックします。

Security Awareness Trainingが有効になると、機能を管理するための2つのインターフェイスが表示されます。

キャンペーンを管理するには、ナビゲーションペインで[**セキュリティ意識向上トレーニング**]をクリックします。

**Security Awareness Trainingの設定を行うには、以下の手順に従います。**

- **ビジネス向けの表示**の場合、ナビゲーションペインで[**セキュリティ意識向上トレーニング**]をクリックし、[**設定**]タブを開きます。
- **マネージドサービスプロバイダー (MSP) 向けの表示**の場合、ナビゲーションペインで[**サイトリスト**]をクリックし、サイトを開き、[**セキュリティ意識向上トレーニング**]タブを開きます。

## トレーニング対象のユーザーの選択

Security Awareness Trainingを有効にした後は、トレーニング対象のユーザーを選択する必要があります。そのために、対象とするユーザーを含むドメインを特定します。**MSP向けの表示**を使用している場合は、各サイトのドメインを特定する必要があります。

**トレーニング対象のユーザーを選択するには、以下の手順に従います。**

1. Security Awareness Trainingの設定に移動します。
    - **ビジネス向けの表示**の場合、ナビゲーションペインで[**セキュリティ意識向上トレーニング**]をクリックし、[**設定**]タブを開きます。
    - **マネージドサービスプロバイダー (MSP) 向けの表示**の場合、ナビゲーションペインで[**サイトリスト**]をクリックし、サイトを開き、[**セキュリティ意識向上トレーニング**]タブを開きます。
2. ユーザーの選択に使用するドメインを設定します。
    1. **ビジネス向けの表示**の場合、[**セキュリティ意識向上トレーニング**]タブ、[**設定**]タブの順に移動した先のオプションを使用します。

2. **MSP向けの表示**の場合、ナビゲーションペインで[**サイトリスト**]をクリックしてサイトを開き、[**セキュリティ意識向上トレーニング**]タブを開きます。

3. Active Directoryの統合を使用して自動的にドメインを設定するか、ドメイン認証を使用して手動で設定するかを選択します。

   - [**Active Directoryの統合**]: Azure Active Directoryと同期してドメインを識別します。また、セキュリティトレーニングの対象となるドメイン内のユーザーのリストも同期されます。詳細は、ナレッジベース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の設定**]ページで同期の状況を確認できます。必要に応じて、[**無効**]をクリックしてAzureからの同期を停止することもできます。

   - [**ドメインの検証**]: 検証用の電子メールでドメインを識別した後、ユーザーを追加できます。ISPまたはパブリックドメイン(gmail.comなど)の電子メールアドレスは制限されているため、使用できません。電子メールアドレスは、有効な企業または組織のアドレスである必要があります。

     - [**新しいドメインの追加**]ボックスに電子メールアドレスを入力します。
       - 入力した電子メールアドレスが**ドメインメンバー**である場合、キャンペーンを作成および実行できますが、侵害レポートにはアクセスできません。
       - 入力した電子メールアドレスがシステムレベルの**ドメイン管理者**(admin、administrator、info、postmaster、root、system、webmasterなど)である場合、キャンペーンを作成および実行でき、侵害レポートにアクセスできます。
     - [**認証リクエストを送信**]をクリックして、指定した電子メールアドレスに認証用の電子メールを送信します。
     - 認証のメールが届いたら、メッセージ内の認証用リンクをクリックして、そのドメインへのアクセスを確認します。
     - ドメインへのアクセスが確認されたら、ナビゲーションペインで[**セキュリティ意識向上トレーニング**]をクリックして[**ユーザー**]タブを開きます。
     - サイトを選択します(**MSP向けの表示**のみ)。
     - [**サイトにユーザーを追加**]をクリックします。
       - [**ユーザーを手動で入力**]: トレーニング対象とする各ユーザーの名前と電子メールを手動で入力するには、このオプションを選択します。
       - [**Active Directoryの統合を設定**]: Azure Active Directoryを使用して同期するには、このオプションを選択します。詳細は、ナレッジベースを参照してください。
       - [**ファイルからユーザーをアップロードする**]: トレーニングの対象とするユーザーをインポートする場合はこのオプションを選択します。このファイルに含めることができるレコードは最大1万5,000件です。
         - [**CSV**]: コンマで区切られた`.csv`ファイルのユーザーリストを使用できます。このファイルにはユーザーの名、姓、電子メールアドレスが含まれている必要があります。必要に応じて一意のIDとタグを含めることができます。
         - [**LDIF**]: LDAP/アクティブディレクトリからエクスポートした`.ldif`ファイルを使用できます。次のフィールドを使用してトレーニング対象のユーザーを追加します。

- [**givenname**] (入力必須): ユーザーの名として使用されるエントリです。
- [**sn**] (入力必須): ユーザーの姓として使用されるエントリです。
- [**mail**] (入力必須): ユーザーの電子メールアドレスとして使用されるエントリです。
- [**objectGUID**] (任意): ユーザーの一意のIDとして使用されるエントリです。
- [**ou**] (任意): タグとして使用される組織単位です。

## ユーザーの管理

サイト内で、ユーザーを追加、編集、削除できます。

**ユーザーを管理するには、以下の手順に従います。**

1. ナビゲーションペインで[**セキュリティ意識向上トレーニング**]をクリックし、[**ユーザー**]タブを開きます。
2. 管理するサイトをクリックします(**MSP向けの表示**のみ)。
3. [**サイトにユーザーを追加**]をクリックします。
    - [**ユーザーを手動で入力**]: トレーニング対象とする各ユーザーの名前と電子メールを指定できます。
    - [**ファイルからユーザーをアップロードする**]: トレーニングの対象とするユーザーをインポートする場合はこのオプションを選択します。このファイルに含めることができるレコードは最大1万5,000件です。
        - [**CSV**]: コンマで区切られた`.csv`ファイルのユーザーリストを使用できます。このファイルにはユーザーの名、姓、電子メールアドレスが含まれている必要があります。必要に応じて一意のIDとタグを含めることができます。
        - [**LDIF**]: LDAP/アクティブディレクトリからエクスポートした`.ldif`ファイルを使用できます。次のフィールドを使用してトレーニング対象のユーザーを追加します。
            - [**givenname**] (入力必須): ユーザーの名として使用されるエントリです。
            - [**sn**] (入力必須): ユーザーの姓として使用されるエントリです。
            - [**mail**] (入力必須): ユーザーの電子メールアドレスとして使用されるエントリです。
            - [**objectGUID**] (任意): ユーザーの一意のIDとして使用されるエントリです。
            - [**ou**] (任意): タグとして使用される組織単位です。
    - [**Active Directoryの統合を設定**]: Azure Active Directoryを使用して同期するには、このオプションを選択します。
        - [**今すぐ設定**]をクリックします。
        - 表示された**シークレットトークン**をコピーし、画面の指示に従ってAzure Active Directoryのテナントを設定します。

サイトからユーザーを**削除**する場合は、ユーザー名の横にあるチェックボックスを**オン**にして、[**選択したユーザーを削除**]をクリックします。

## 配信先リストの作成と管理

Security Awareness Trainingの配信先リストを作成して、ユーザーをグループに編成できます。この設定は、フィッシングシミュレーションやトレーニングコースを一部のユーザーに送信して目的のトレーニングを行う場合に役立ちます。

**配信先リストを作成して管理するには、以下の手順に従います。**

1. ナビゲーションペインで[**セキュリティ意識向上トレーニング**]をクリックし、[**ユーザー**]タブを開きます。
2. 対象のサイトをクリックします(**MSP向けの表示**のみ)。対象のサイトはSecurity Awareness Trainingが有効になっており、1人以上のユーザーが割り当てられている必要があります。
3. [**配信先リストの作成**]ボタン( )をクリックして、Security Awareness Trainingの新しい配信先リストを作成します。
    - [**配信先リストの名前**]: Security Awareness Trainingの配信先リストの名前を指定します。
    - [**会社**]: このリストには、使用可能なユーザーが表示されます。このリスト内のユーザーをクリックすると、[**配布リストメンバー**]のリストに移動します。
    - [**検索**]: このボックスを使うと、いずれかのリストを検索条件を満たすサイトだけに絞り込むことができます。検索条件をクリアするには[x]をクリックします。
    - [**全て追加する**]: クリックすると、会社のリストに表示されているすべてのユーザーを[**配布リストメンバー**]リストに追加できます。検索フィルタを適用した場合は、[**会社**]リストに表示されているエントリのみが追加されます。
    - [**配布リストメンバー**]: このリストには、配信先リストに含まれるすべてのユーザーが表示されます。表示されているリストには、検索フィルタの結果にかかわらず、リスト内のすべてのユーザーが表示されます。ユーザーを削除する場合、ユーザー名をクリックすると会社名のリストに戻ります。
    - [**すべて削除**]: クリックすると、[**配布リストメンバー**]リストからすべてのアイテムが削除され、そのアイテムが会社名リストに戻ります。
    - [**保存**]: クリックすると、Security Awareness Trainingの新しい配信先リストが保存されます。

既存の配信先リストを編集するには、対象の配信先リスト名を選択して[**配信先リストの編集**]ボタン( )をクリックします。

既存の配信先リストを削除するには、対象の配信先リスト名を選択して[**配信先リストの削除**]ボタン( )をクリックします。

## 新しいキャンペーンの作成

始める前に、あなたのメールサーバーがユーザーに送信されるフィッシングシミュレーションやトレーニングメールをブロックしていないことを確認してください。また、キャンペーンを作成するには、少なくとも1つのサイトで管理者権限を持っている必要があります。

1. ナビゲーションペインで[**セキュリティ意識向上トレーニング**]をクリックし、[**キャンペーン**]タブが選択されていることを確認します。
2. [**新しいキャンペーン**]をクリックします。[新しいキャンペーン]ダイアログが表示されます。
3. セクション1でキャンペーンを構築します。

- [**キャンペーン名**]で、わかりやすいキャンペーン名を指定します。これは管理者のみに表示されます。
- [**キャンペーンタイプ**]で、作成するキャンペーンのタイプを選択します。
    - [**フィッシング**]: テストを実行し、フィッシングリンクをクリックしたユーザーの数をレポートする電子メールベースのフィッシングシミュレーションです。
    - **トレーニング**は、学習コンテンツを使ってユーザーを教育し、何人のユーザーがトレーニングを完了したかを報告するキャンペーンです。トレーニングを選択すると、オプションでトレーニングキャンペーンのタイトルとランディングページのメッセージを指定することができます。
    - [**電子メールのテンプレートを選択**] (トレーニングのみ)では、サムネイルからトレーニングの招待状メールのテンプレートを選択できます。このテンプレートはさまざまなカスタマイズが可能です。
    - **トレーニング・リメディエーション**は、フィッシングシミュレーション・キャンペーンに失敗したユーザーを自動的にトレーニングに参加させるために使用されます。「トレーニング・リメディエーション」キャンペーンは「フィッシング」キャンペーンとは別に管理されているため、すべてのフィッシングキャンペーンで再利用することができます。

      **重要**:現在、「トレーニング・リメディエーション」キャンペーンの管理はスーパー管理者に制限されています。このオプションは、スーパー管理者に指定されていない管理者には表示されません。
- すべてのキャンペーンタイプで、メールテンプレートをカスタマイズすることができます。**テンプレートのカスタマイズ**のリンクをクリックして、メールの配信方法や表示方法をカスタマイズします。これらのフィールドの意図は、フィッシングやトレーニング用にメールをカスタマイズする場合によって異なります。例えば、フィッシング用は、ユーザーをテストするので、情報を本物のように見せかけたいです。トレーニング用は、ユーザーがフィッシングだと思い、トレーニングの招待を削除しないように、情報を本物のように見せかけたいです。
    - **送信者名**は、あなたがメールを送信させたい個人、エイリアス、グループ、または組織の名前です。
    - **送信者アドレス**は、あなたがメールの送信元にしたいアドレスです。
    - **メール件名**は、メールの件名です。
    - **メール本文**はメールの本文です。テンプレート画像を編集したり、自分の画像にリンクすることもできます。カスタムテンプレートに画像を追加する方法については、「カスタムテンプレートから画像をリンクする」を参照してください。
    - **新規作成として保存**をクリックすると、カスタマイズした内容に基づいて新しいテンプレートが作成されます。
    - **編集の適用**をクリックすると、カスタマイズ中のテンプレートを変更します。
- フィッシングキャンペーンの場合:
    - メールテンプレートを選択して、メールのテンプレートを指定します。検索テキストを入力するか、カテゴリーフィルターを選択することで、表示されるサムネイルを絞り込むことができます。

- ランディングページURLをクリックしてドメインを選択します。これはフィッシング・メールからユーザーに送られるURLです。URLをサブドメインでカスタマイズすることで、フィッシングメールやユーザーに関連したものにすることができます。
- ランディングページのセクションでは、ランディングページのURLがクリックされたときに表示させたい内容を選択します。
  - [**インフォグラフィック**]: Webベースのトレーニングページを表示します。フィッシングシミュレーションをクリックしたことをユーザーに即座に把握させます。このオプションは、シミュレーションが進行中であることをユーザーに警告します。
    - [**インフォグラフィックのテンプレートを選択**]で、表示するインフォグラフィックを選択できます。
    - インフォグラフィックページの本文を変更する場合は、[**テンプレートをカスタマイズ**]をクリックします。
  - [**壊れたリンク**]: 404タイプのエラーページを表示します。これを選択した場合、ユーザーに状況を即座に把握させることはできません。シミュレーションが進行中であることを警告することなく、ユーザーをテストします。
    - [**404タイプ**]で、表示されるリンク切れエラーのタイプを選択できます。
  - [**ルアーページ**]: ユーザーをWebページに移動させ、情報を入力するかどうかをテストしてシミュレーションを拡張します。ユーザーが情報を入力すると、Webベースのトレーニングページにリダイレクトされます。このページでは、フィッシングシミュレーションをクリックしたことをユーザーに即座に把握させます。この段階に達すると、ユーザーに対してシミュレーションが進行中であることが警告されます。
    - [**ルアーページのテンプレートを選択**]: 表示するルアーページを選択できます。
    - [**テンプレートをカスタマイズ**]: ルアーページの本文を変更できます。
    - [**データ転記先**]: ユーザーがルアーページに情報を入力した場合に表示されるインフォグラフィックを選択します。
    - [**テンプレートをカスタマイズ**]: インフォグラフィックページの本文を変更できます。
- 「**トレーニング**」キャンペーンおよび「**トレーニング・リメディエーション**」キャンペーンの場合:
  - **ランディングページのコンテンツ**を指定することで、キャンペーン登録時に送信されるトレーニング招待メールをクリックした際のエンドユーザーの体験をコントロールすることができます。
  - **メールテンプレートの選択**では、トレーニング招待メールテンプレートを選択するためのサムネイルが表示されます。これらのテンプレートは完全にカスタマイズ可能です。
  - **トレーニングコースの選択**では、サムネイルをスクロールするか、名前で検索のボックスを使用してコース名で絞り込むことにより、トレーニングキャンペーンごとに最大10コースを選択することができます。また、トレーニングキャンペーンの言語を選択し、選択リストの異なる位置にコースをドラッグすることで、ランディングページの表示順序を指定することができます。

4. セクション2でキャンペーンに含めるサイトを選択します。見出しをクリックすると展開されます。

- **サイト選択**テーブルには、利用可能なサイトが一覧表示されます。期限切れのサイト、ユーザーのいないサイト、現在の管理者に十分な権限がないサイトは含まれません。このリストでサイトをクリックすると、「選択したサイト」のリストに移動します。
    - [**検索**]: このボックスを使うと、いずれかのリストを検索条件を満たすサイトだけに絞り込むことができます。検索条件をクリアするには[x]をクリックします。
    - [**配布リストを表示**]: クリックすると、Security Awareness Trainingのすべての配信先リストを表示できます。配信先リストでは、サイト内のすべてのユーザーではなく、リスト内のユーザーにのみキャンペーンが送信されます。
    - [**全て追加する**]: クリックすると、現在[**サイトを選択**]リストに表示されているすべてのサイトと配信先リストが、[**選択済みのサイト**]リストに追加されます。検索フィルタを適用した場合、またはSecurity Awareness Trainingの配信先リストが表示されていない場合は、[**サイトを選択**]リストに表示されているエントリだけが追加されます。
- [**選択済みのサイト**]の表には、キャンペーンに含まれるすべてのサイトとSecurity Awareness Trainingの配信先リストが表示されます。表示されているリストには、検索フィルタの結果にかかわらず、リスト内のすべてのアイテムが表示されます。このリスト内のサイトをクリックすると、[**選択済みのサイト**]リストからアイテムを削除し、そのアイテムを[**サイトを選択**]リストに戻します。
- [**すべて削除**]をクリックすると、[**選択済みのサイト**]リストからすべてのアイテムを削除し、そのアイテムを[**サイトを選択**]リストに戻します。

5. 次のセクションでキャンペーンのスケジュールを決めます。セクションを選択すると展開されます。

   *注*: 現在、「トレーニング・リメディエーション」キャンペーンでは、自動登録、開始日、期間、配信時間は必要ありません。

   - [**自動登録**]を選択すると、新しいユーザーがキャンペーン用に選択したサイトまたは配信先リストに追加された場合に、このキャンペーンに自動的に追加されます。キャンペーンがアクティブである限り、新しいユーザーにはキャンペーンが提供されます。
       - [**開始日**]: ユーザーを自動的に登録する場合は、キャンペーンを開始する日付を指定します。
   - [**期間**]フィールドは、ユーザーを自動的に登録するかどうかによって異なります。キャンペーンの終了後にキャンペーンにアクセスしようとすると、キャンペーンが無効になったことを示すメッセージが表示されます。
       - ユーザーを自動的に登録する場合は、登録したユーザーがキャンペーンに留まる期間を選択します。キャンペーンは、最終日の午後11:59に自動的に終了します。[**無期限**]を選択すると、手動でキャンペーンを終了するまで、ユーザーはキャンペーンに登録されたままになります。
       - ユーザーを自動的に登録しない場合は、キャンペーンを実行する期間を選択します。終了日を設定しない場合、キャンペーンを手動で終了しない限り、キャンペーンは期限切れになりません。終了日を設定すると、キャンペーンは最終日の午後11:59に自動的に終了します。
   - [**配信時間**]は、キャンペーンの電子メールを送信する時刻です。キャンペーンのスケジュール時間は、ローカルコンピュータのタイムゾーンに従って指定されます。たとえば、コンピュータで東部標準時を使用している場合に午前10:00を選択すると、太平洋標準時を使用してコンピュータで表示したときに、時刻が自動的に午前7:00に調整されます。

- [**始動時に電子メールを送信する**]: キャンペーンの開始と同時にすべての電子メールが送信されるように指定します。
- [**独自に設定した時刻に電子メールを送信する**]: 指定した時刻にすべての電子メールを送信します。
- [**メールの配信をある一定の日数にわたって行う**]: 指定した日数にわたって電子メールの配信を行います。

- 「**キャンペーン終了後、自動的にキャンペーンサマリーレポートを送信**」を選択すると、キャンペーン終了後に自動的にキャンペーンサマリーレポートを送信します。

6. 最終セクションでキャンペーンを確認します。セクションをクリックすると展開されます。このセクションではキャンペーンの設定を確認することができます。不完全なキャンペーン構成設定はすべて識別されます。このセクションでは、単一のメールアドレスを入力し、**送信プレビュー**をクリックすることもできます。複数のメールアドレスの場合はこれを繰り返します。各メールアドレスには、キャンペーンの外観と機能のプレビューが表示されます。
7. 以下のいずれかのボタンをクリックしてください。
   - **キャンセル**を選ぶと、保存せずにキャンペーン作成を終了します。設定したキャンペーン設定は失われます。
   - **保存 & 閉じる**を選ぶと、キャンペーンを終了し、構成したキャンペーン設定を保存します。キャンペーンは下書きステータスのままで、指定された開始日になっても開始されません。
   - [**キャンペーンを開始する**]: キャンペーンの作成が終了し、指定したキャンペーン設定が保存されます。指定した開始日に達するとキャンペーンが開始されます。開始日が即時の場合、キャンペーンは即時に開始されます。

## カスタムテンプレートからの画像のリンク

カスタムテンプレートの画像をリンクすることで、電子メールテンプレートを任意で独自の画像にカスタマイズできます。キャンペーンで画像を使用する場合、Webrootの条件に従って、関連するすべての著作権および利用規約を遵守する必要があります。

電子メールのテンプレートに画像を追加してカスタマイズする場合は、下記を考慮してください。

- 画像のアドレスはインターネットでホストされている有効なURLである必要があります。
- URLはWebブラウザで誰でもアクセスできるものである必要があります。
- 画像はホットリンク保護されていないものである必要があります。
- 画像はサードパーティのWebサイトに埋め込み可能なものである必要があります。

## オートパイロットの有効化

Security Awareness Trainingのオートパイロットプログラムを利用すると、事前にスケジュールされたトレーニングやフィッシングキャンペーンを、対象のユーザーに月次で実施できます。

**SATのオートパイロットにユーザーを登録するには、以下の手順に従います。**

1. 管理コンソールの[**セキュリティ意識向上トレーニング**]セクションで、[**オートパイロット**]タブをクリックします。
2. [**オートパイロットキャンペーンスケジュールを表示**]をクリックして、プログラムの内容を確認します。

3. [**オートパイロット**]スイッチを有効にします。
4. (オプション)各キャンペーンの終了後にキャンペーン概要レポートを自動的に送信するため、宛先の電子メールアドレスを1つ入力します。メッセージには単一のzipファイルへのリンクが記載されます。そのzipファイルには、キャンペーンの対象サイト別のレポートが格納されます。
5. オートパイロットキャンペーンに登録するサイトまたは配信先リストを選択します。
6. [**保存**]をクリックします。

**オートパイロットキャンペーンを無効にするには、以下の手順に従います。**

1. [**オートパイロット**]スイッチを無効にします。
2. スケジュールされたオートパイロットキャンペーンを無効化するため、[**キャンペーン**]タブに移動します。
3. 選択したオートパイロットキャンペーンの[**アクション**]メニューで、[**キャンペーンを終了**]をクリックします。

SATのオートパイロットの詳細については、「よくあるご質問」を参照してください。

# 使用可能なキャンペーンの表示と管理

使用可能なキャンペーンを表示するには、ナビゲーションペインから[**セキュリティ意識向上トレーニング**]を開き、[**キャンペーン**]タブが表示されていることを確認します。このページには、Security Awareness Trainingを使用しているサイト数と過去90日間のキャンペーン数の概要が表示されます。

表示されるのは自分のキャンペーンだけではありません。他の管理者が作成したキャンペーンの下書きも表示され、編集、開始することができます。

[**キャンペーン管理**]の表では以下のコントロールを使用できます。

- [**検索**]: このボックスに入力した検索テキストを含む行のみをリストに絞り込んで表示できます。検索では、表示されている行だけでなく表全体が対象になります。
- [**新しいキャンペーン**]: 新しいキャンペーンを作成するには、このボタンをクリックします。詳細は「*新しいキャンペーンの作成* ページ 119」を参照してください。
- [**フィルタ**]: フィルタパネルを開いたり閉じたりするには、このボタンをクリックします。適用するフィルタを1つ以上選択します。
- 列を**並べ替える**には、その列の見出しをクリックします。
- [**キャンペーン名**]のリンク: アクティブなキャンペーン、スケジュールされたキャンペーン、または完了したキャンペーンの名前をクリックすると、そのキャンペーンの概要レポートを表示できます。
- [**サイト名**]のリンク: クリックすると、**Security Awareness Training**のレガシーコンソールに移動できます。このレガシーコンソールは今後廃止される予定です。
- [**アクション**]: 以下の機能を実行できます。
    - [**キャンペーンを終了**]: キャンペーンを直ちに終了します。キャンペーンの終了後にキャンペーンにアクセスしようとすると、エラーメッセージが表示されます。
    - [**今すぐリマインダーを送信**]: トレーニングキャンペーンを修了していないユーザーに電子メールでリマインダーが送信されます。
    - [**キャンペーンを編集**]: キャンペーンを編集できます。このオプションは、キャンペーンの下書きのみで使用できます。

- [**キャンペーンをアーカイブ**]: 完了して無効になったキャンペーンを保持できます。アーカイブされたキャンペーンを確認できます。
- [**キャンペーンを削除**]: 下書きのキャンペーンを削除できます。削除されたキャンペーンを確認することはできません。
- [**キャンペーンをコピー**]: キャンペーンのコピーを作成します。

- [**行と改ページ**]: キャンペーン管理表の下部にある制御機能で、1ページの表示を増減したり、ページ間を移動したりできます。

## 使用可能なトレーニングコースの表示

使用可能なトレーニングコースを確認するには、[**セキュリティ意識向上トレーニング**]に移動し、[**コンテンツライブラリ**]タブを選択します。

使用可能なトレーニングコースはタブ別に分類されています。タブにはそのカテゴリーのコースが表示され、コース名、説明、時間の長さなども記載されています。トレーニングコースをクリックすると、コースの評価方法やコースの発行元を確認できます。詳細なコース表示から[**コースのプレビュー**]をクリックしてコースを確認するか、[**キャンペーンに追加**]をクリックして選択したトレーニングコースで新しいキャンペーンを作成できます。

[**検索**]ボックスにテキストを入力すると、その検索テキストを含むコースのみが表示されます。必要に応じて、[**コースリストをCSVとしてダウンロード**]をクリックして、各コースの概要を.csvファイルで表示することもできます。

## キャンペーン概要レポートの表示

キャンペーンがまだ開始されていない場合、状態は[**スケジュール済み**]となります。キャンペーンの状態が[**スケジュール済み**]となっている間、データは生成されません。ただし、[**キャンペーン名**]のリンクをクリックすると、キャンペーンの設定を表示できます。

キャンペーンがアクティビティを生成した後は、キャンペーン概要レポートを表示できます。[**セキュリティ意識向上トレーニング**]タブに移動し、[**キャンペーン名**]のリンクをクリックすると、そのキャンペーンの概要レポートを表示できます。レポートは以下のとおり、複数のセクションに分かれています。

- 最上部のセクション: 開始時刻、時間、登録ユーザーなどのキャンペーンの概要が記載されます。
- 「トレーニング・リメディエーション」キャンペーンが使用されている場合、トップセクションにはリンクされたキャンペーンセクションも表示され、リメディエーション(是正)の関係が示され、リンクされたキャンペーン間で結果を簡単に相互参照することができます。
- マルチサイトキャンペーンの場合、サマリーレポートには、キャンペーンに含まれるサイトのリストと主要指標が表で表示されます。各サイトの個別レポートを表示するには、**配信レポート**をクリックします。
- 個々のサイトのサマリーレポートビューでは、選択内容に応じて、**サンキー**または**棒グラフ**形式で**結果**が表示されます。グラフの下には、各ターゲットユーザーの詳細な結果が表示されています。
    - [**サンキー**]: 各ユーザーのログに記録されたすべてのイベントを表示できるため、キャンペーンの詳細情報を評価するのに最適なオプションです。各バケットにおける濃い縦棒の高さは、そのタイプのイベントで記録されたユーザーの総数を表します。ユーザーがリンクを複数回クリックした場合も、各ユーザーが記録されるイベントのインスタンスは1つのみです。キャンペーンイベントの詳細な情報については、「*キャンペーンイベントの解釈* ページ 127」を参照してください。

    - [**棒グラフ**]: 各ユーザーのログに記録された最新の優先イベントのみが表示されるため、結果をすぐに参照するのに最適なオプションです。
- データ可視化グラフの下にある「詳細結果」テーブルには、キャンペーンでアクティブなユーザーの最新のイベントと是正状況(トレーニング・リメディエーションを使用している場合)が表示されます。
- マルチサイトおよびシングルサイトのサマリービューでは、キャンペーンで使用されたコンテンツが最後のセクションに表示されます。
    - **使用メール**はキャンペーンに使用されたメールです。
    - **ランディングページ**(フィッシングキャンペーンのみ)は、キャンペーンに指定されたルアー、インフォグラフィック、リンク切れを表示します。
    - **トレーニングコース**(トレーニングキャンペーンのみ)は、キャンペーンに指定されたコースを表示します。
- [**PDFをエクスポート**]または[**CSVをエクスポート**]をクリックすると、選択したファイル形式の概要レポートをダウンロードできます。CSVファイルの場合、電子メールの配信コードといった詳細なアクティビティデータも追加で参照できます。

## キャンペーンイベントの解釈

Security Awareness Trainingの以下のイベントは、キャンペーン概要レポートに表示されるサンキー図に直接マッピングされます。

- **登録済み**: 対象のユーザーはキャンペーンに登録されています。
- **処理済み**: 電子メールメッセージは認証され、配信キューに格納されています。
- **遅延配信**: 通常、受信サーバーが配信を後日に延期したことを意味します。このイベントは受信サーバーに負荷がかかり、現時点でメッセージを受信できない場合に発生する可能性があります。メッセージは最初の送信から最大で72時間、再送信が試行されます。
- **配信済み**: 受信者の電子メールシステムが正常に「配信済み」メッセージで応答しました。ただし、電子メールは受信者のネットワーク内に到達した後、内部のスパムフィルタによってフィルタリングされていたり、非表示となっている場合があります。
- **開封**: このイベントは、電子メールの追跡用のピクセルをロードすることで記録されます。ピクセルがロードされていない場合、電子メールクライアントによって非表示となっている場合があります。
- **クリック**: このイベントは、スパムシステムが電子メールのURLを探索することで「実際にはクリックされていないクリック」イベントとして記録される可能性があります。
- **学習ページへのアクセス**: 対象ユーザーが学習ページ(インフォグラフィック)にアクセスしました。このイベントはフィッシングメールまたはルアーページ(有効な場合)からの直接アクセスで発生する場合があります。
- **ルアーへのアクセス**: 対象ユーザーがフィッシングのルアーページにアクセスしました。ユーザーがフィッシングメールのリンクをクリックするとルアーページに誘導され、クリックイベントが記録されます。
- **トレーニングへのアクセス**: 対象ユーザーがコースの開始ページにアクセスしました。このイベントは、トレーニング招待メールまたはフィッシングメール(ハイブリッドキャンペーンの場合)からの直接アクセス、またはハイブリッドフィッシングキャンペーンのルアーページ(有効な場合)でのやり取りから発生する場合があります。
- **キャンペーン完了**: 対象ユーザーが、1つのキャンペーンで割り当てられたすべてのアクティビティを正常に完了しました。

これ以外のキャンペーンイベントは、以下のとおりマッピングと集計が行われます。

- **バウンス**: このイベントは、ターゲットへの電子メールがすべて配信できなかった(バウンスした)場合にのみ集計されます。
- **破棄済み**: このイベントは、ターゲットへの電子メールがすべて破棄された場合にのみ集計されます。
- **トレーニング開始済み**: このバケットには、「トレーニング試行済み」、「コース試行済み」、「トレーニング合格」、「トレーニング完了」、「コース修了」イベントが含まれます。ユーザーが少なくとも1つのコースを試行した場合にのみ集計されます。

## セキュリティ意識向上トレーニングレポート

ナビゲーションペインで[**レポート**]をクリックすると、すべてのレポートオプションが表示されます。

セキュリティ意識向上トレーニングレポートは、セキュリティ意識向上トレーニングを使用している場合にのみ適用されます。

- [**SAT: フィッシングのクリック**]: サイト別のクリック率
- [**SAT: トレーニング進捗状況**]: サイト別のトレーニング率
- [**SAT: 使用状況レポート**]: 使用状況の統計情報