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

「はじめに」ガイド

お知らせ

Webroot法人向け製品の「はじめに」ガイド 改正 2025年3月13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

この文書に記載されている情報は、予告なしに変更されることがあります。本書に記載されているソフトウェアは、ライセンス契約または秘密保持契約に基づいて提供されています。本ソフトウェアは、これらの契約の条件に従ってのみ使用または複製することができます。本書のいかなる部分も、Webrootの書面による許可なく、購入者の個人的な使用以外の目的で、複写および録音を含む、電子的または機械的ないかなる形式または手段によっても、複製、検索システムへの保存、転送を行うことはできません。

コンテンツ

概要

この「はじめに」ガイドでは、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法人向け製品の設定および実行方法について詳しく説明します。

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『Webrootエンドポイントプロテクション管理者ガイド』の「DNSプロテクション」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『Webroot法人向け製品の管理者ガイド』の「セキュリティ意識向上トレーニング」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。

エンドポイントプロテクションおよび、すべての製品に共通する機能の詳細については、『Webroot法人向け製品の管理者ガイド』を参照してください。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。

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。

Webroot管理コンソールを使用するには

この「はじめに」ガイドでは、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『Webroot法人向け製品の管理者ガイド』の「*製品の購入または体験版への登録* ページ 7」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、『Webroot法人向け製品の管理者ガイド』の「*アカウントの作成とアクティブ化* ページ 8」を参照してください。
    - 2要素認証の詳細については、『Webroot法人向け製品の管理者ガイド』の「*2要素認証(2FA)の設定* ページ 9」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、『Webroot法人向け製品の管理者ガイド』の「*管理コンソールの表示の選択* ページ 8」を参照してください。
    - サイトの作成の詳細については、『Webroot法人向け製品の管理者ガイド』の「*サイトの作成(MSPのみ)* ページ 10」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『Webroot法人向け製品の管理者ガイド』の「*エージェントのダウンロードとインストールページ 14*」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『Webroot法人向け製品の管理者ガイド』の「*DNSプロテクションの有効化と設定* ページ 16」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『Webroot法人向け製品の管理者ガイド』の「ネットワーク証明書とライセンスのインストール」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、『Webroot法人向け製品の管理者ガイド』の「*Security Awareness Trainingの有効化* ページ 25」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、『Webroot法人向け製品の管理者ガイド』の「*トレーニング対象のユーザーの選択* ページ 25」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 13」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 10」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『Webroot法人向け製品の管理者ガイド』の「Endpoint Protectionのポリシーのベストプラクティス」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『Webroot法人向け製品の管理者ガイド』の「DNSプロテクション」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『Webroot法人向け製品の管理者ガイド』の「Security Awareness Training」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 15」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、『Webroot法人向け製品の管理者ガイド』の「DNSプロテクション」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、『Webroot法人向け製品の管理者ガイド』の「エージェントの配備」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。

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「*Webroot管理コンソールを使用するには* ページ 6」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『Webroot法人向け製品の管理者ガイド』『Webroot法人向け製品の管理者ガイド』の「ネットワークの設定」を参照してください。
    - ネットワークを保護します。詳細は『Webroot法人向け製品の管理者ガイド』の「ネットワークの設定」を参照してください。

DNSプロテクションの設定に関する詳細については、『Webroot法人向け製品の管理者ガイド』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 18」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。

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「*Webroot管理コンソールを使用するには* ページ 6」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 25」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 25」を参照してください。

Security Awareness Trainingの設定に関する詳細については、『Webroot法人向け製品の管理者ガイド』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。