

OpenDNS FamilyShieldについて

内容

[はじめに](#)

[概要](#)

[FamilyShieldを使用するケース](#)

[FamilyShieldの仕組み](#)

[DNSサーバアドレス](#)

[FamilyShieldが使用されていることを確認します。](#)

[制限事項](#)

はじめに

このドキュメントでは、OpenDNS FamilyShieldの概要、機能、およびネットワークでの使用方法について説明します。

概要

OpenDNS FamilyShieldは、DNSベースのコンテンツフィルタリングサービスです。事前定義されたフィルタリング設定を使用して、一般にアダルトコンテンツとして分類されるWebサイトへのアクセスをブロックします。

FamilyShieldを使用するケース

基本的なコンテンツフィルタリングを適用する簡単なDNSベースの方法が必要な場合は、FamilyShieldを使用します。

- ホームネットワーク
- 小規模オフィス環境
- ゲストネットワーク
- 簡素化された制御を必要とするラボまたはキオスクデバイス

FamilyShieldは通常、カスタムフィルタリングポリシーの管理よりもクイックセットアップが優先される場合に使用されます。

FamilyShieldの仕組み

FamilyShieldは、特定のDNSリゾルバアドレスを使用して動作します。ユーザがドメインにアクセスしようとする時、FamilyShieldリゾルバを介してDNSクエリが解決されます。ドメインがFamilyShieldによる制限として分類されている場合、DNS応答はサービスの動作に基づいてブロックまたはリダイレクトされます。



注：これはDNSベースであるため、主にドメイン名解決によってアクセスを制御します。

DNSサーバアドレス

エンドポイントまたはルータ/DHCPのDNS設定で、次のDNSサーバアドレスを設定します。

- 208.67.222.123
- 208.67.220.123

FamilyShieldが使用されていることを確認します。

- デバイスまたはネットワークがFamilyShield DNSサーバアドレスを使用するように設定されていることを確認します。
- 既知の許可されたドメインの名前解決をテストし、通常の解決を確認します。
- コンテンツフィルタリングが機能しない場合は、他のDNS方式によって設定が上書きされないことを確認します (VPN DNS、ブラウザDNS-over-HTTPS、手動で設定されたDNS設定など)。

制限事項

- ユーザがブラウザでDNS設定を変更したり、VPNを使用したり、DNS-over-HTTPS(DoH)を使用したりすると、DNSベースのフィルタリングをバイパスできます。
- フィルタリング動作はカテゴリベースであり、完全なプロキシまたはファイアウォールのコンテンツインスペクションソリューションとは異なります。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。