

# Eicarによるファイル検査のテスト

## 内容

---

[はじめに](#)

[概要](#)

[Eicarの検出プロセスについて](#)

[まとめ](#)

---

## はじめに

このドキュメントでは、Eicarを使用してファイルインスペクションをテストする方法について説明します。

## 概要

現在、eicar.orgテストダウンロードファイルを使用してファイルインスペクション機能が有効になっているかどうかをテストすると、「SSL復号化」が有効または無効の場合に異なる動作が表示されます。Umbrellaファイル検査のみ：SSL復号化が有効な場合、AVスキャンはeicar.orgでダウンロードされます。

## Eicarの検出プロセスについて

eicar.orgのブロックを有効にするには、[SSL復号化を有効](#)にしてください。



注:SSL復号化は、HTTP経由でサイトにアクセスする場合でも必要です。SSL復号化を有効にしていない場合、プロキシはHTTPS経由でトラフィックを処理するドメインをバイパスします。

- Umbrellaインテリジェントプロキシは、DNSレイヤでプロキシにドメインを送信するかどうかを決定します。
- DNS要求はHTTP/HTTPS接続の前に発生します。つまり、ドメインがプロキシの対象である場合、HTTPとHTTPSの両方のトラフィックが常にプロキシされます。
- HTTP/HTTPSトラフィックがインテリジェントプロキシに到達したら、最初にユーザを識別するためのリダイレクトを行います。

このリダイレクトはSSL復号化なしでは不可能です。つまり、一部のシナリオ ( Roaming Usersなど ) ではユーザを正しく識別できない可能性があります。

これらのユーザによるHTTPS要求の切断を防ぐために、Umbrellaでは、SSL復号化が有効でない限り、HTTP/HTTPSトラフィックの両方に対応するプロキシドメイン(eicar.orgなど)を使用しません。

## まとめ

この機能から最高のセキュリティと有効性を得るには、[CiscoルートCA](#)をインストールして、SSL復号化を有効にすることを強くお勧めします。これにより、eicar.orgテストファイルがブロックされ、インテリジェントプロキシを介してファイルインスペクションの対象となるドメイン数が増加します。

予想される動作の要約を次に示します。

- SSL復号化オフ
  - Eicar.orgのサイトは、<https://www.eicar.org/download/eicar.com>ではブロックされません。SSL復号化が無効になっているため、ドメインはまったくプロキシされません。
  - eicarをホストしている当社独自のテストサイトはブロックされています  
: <http://proxy.opendnstest.com/download/eicar.com>
- SSL復号化オン
  - <http://www.eicar.org/download/eicar.com>と<https://www.eicar.org/download/eicar.com>の両方でAVスキャンによってEicarがブロックされる

## 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。