

# 包括フィルタリングの使用中のブラウザ証明書失効エラーのトラブルシューティング

## 内容

---

[はじめに](#)

[問題](#)

[原因](#)

[解決方法](#)

---

## はじめに

このドキュメントでは、Umbrellaフィルタリングを使用しているときにブラウザ証明書失効エラーを解決する方法について説明します。

## 問題

[許可のみモード]または[カテゴリの制限]の設定を使用している場合、サイトを正しく読み込むには、許可リストに複数のドメインを追加しなければならないことがよくあります。

具体的な問題の1つは、HTTPS/SSL Webサイトの証明書失効リスト(CRL)をブロックでき、その結果、一部のブラウザでエラーが生成されることです。これらのCRLをブロックすると、ブラウザが検証を行おうとする間に遅延が発生する場合があります。

## 原因

CRL(Certificate Revocation Lists)および新しいOCSP(Online Certificate Status Protocol)は、SSL証明書が何らかの理由で失効したかどうかを認証局に問い合わせるために使用されます。これは通常、HTTPS Webサイトに接続する際にバックグラウンドで透過的に行われます。

これは、証明書/CAが侵害された場合に証明書が失効すると、ブラウザがユーザのWebサイトへのアクセスを停止するという概念です。CRLへのアクセスを許可することをお勧めします。

Allow-Onlyモードでは、ブロックを明示的に解除しない限り、ほとんどのCRLがブロックされます。この影響は、使用されているWebブラウザによって異なります。

- Internet Explorer 7では、次のようなエラーを含むポップアップ警告が表示されます。  
Revocation information for the security certificate for this site is not available.
- 新しいバージョンのInternet Explorerでは、[特定のレジストリキーフラグが設定されていない限り、エラーは表示されません。](#)
- Google Chromeのアドレスバーの横に警告が表示されます。警告をクリックすると、次のエラーが表示されます。証明書が失効しているかどうかを確認できません
- Firefoxでは、about:configでsecurity.OCSP.require設定が設定されていない場合、エラーは

表示されません

## 解決方法

1. Webブラウザで証明書を表示して、証明書のCRLを検索します（手順はブラウザによって異なります）。
2. [詳細]タブを使用して、次の情報を探します。
  - CRL配布ポイント
  - 権限アクセス情報
3. URL情報（次の例）をメモし、Umbrellaダッシュボードの許可リストに追加します。

## 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。