

HSTSおよびピンング証明書エラーのトラブルシューティング

内容

[はじめに](#)

[証明書エラー](#)

[考えられる解決策](#)

[ポリシー管理とローミングクライアント](#)

[証明書例外エラーの無視 \(Chrome for Windowsのみ \)](#)

[Mac OS X用のFirefox、Safari、およびChrome](#)

[Internet Explorerの場合](#)

はじめに

このドキュメントでは、バイパスできない「Your Connection is Untrusted/Not Private」証明書エラーをクリアする方法について説明します。

証明書エラー

.opendns.comまたは.cisco.comの証明書エラーが表示されても、Cisco Umbrellaのドキュメント『[Cisco Umbrellaルート証明書の管理](#)』に記載されている証明書例外を追加してバイパスできない場合は、次の手順を使用して証明書エラーをクリアできるようにします。

例外を追加して証明書エラーをバイパスできない場合、これはHTTP Strict Transport Security(HSTS)の実装または最新のブラウザで事前にロードされた証明書ピンングが原因です。特定のブラウザと特定のWebサイトの間の通信は、HTTPSを使用する要件を含む方法で行われ、バイパスや例外は不可能です。HTTPSページのこの追加のセキュリティは、Webサイトに対して[HSTS](#)がアクティブな場合、Umbrellaブロックページとバイパスブロックページメカニズムが動作しないようにします。

その結果、該当するページには、[ブロックページバイパス](#)(BPB)を使用してアクセスできません (実際には、バイパス画面が表示されない場合があります)。これらの方法では、BPBログインへのアクセスが許可される場合がありますが、ログイン後に証明書エラーが再表示され、アクセスが拒否されます。バイパスできない証明書エラーがGoogle Chrome、Mozilla Firefox、Safariで表示され、バイパスログインにアクセスしようとしている場合は、この記事の残りの部分を確認してください。



注：この問題に対する、すべてのサイトで管理が容易で永続的なソリューションが利用可能になりました。

その結果、この情報は引き続き適用可能ですが、永続的な解決策で回避できます。Cisco Umbrellaのドキュメント「[Manage the Cisco Umbrella Root Certificate](#)」を使用して、CiscoルートCAのインストールを試行します。

重要：ドメインがHSTSの固定リストにある場合、Chrome、Safari、またはFirefoxを実行している場合はリストが事実上バイパスできないため(Internet Explorer(IE)には影響しないため)、例外を追加することはできません。このようなサイトでは、ページバイパスのブロックは機能しません。これら3つのブラウザによるHSTSを使用したサービスの一覧については、[Google Chromium Code Search](#)を参照してください。このリストで注目すべきサービスは次のとおりです。

- Google (およびGmail、Youtube、Google DocsなどのGoogleリソース)
- ドロップボックス
- Twitter
- Facebook

この問題が発生している場合、またはユーザに問題が発生している場合に、この問題を軽減するためにブロックページバイパスに対する変更を確認するには、umbrella-support@cisco.comまたはアカウントマネージャに電子メールを送信して機能要求を提出してください。シスコの製品管理チームおよびエンジニアリングチームは、証明書およびブロックページバイパスの問題を認識し、この機能の代替再設計をテストしています。

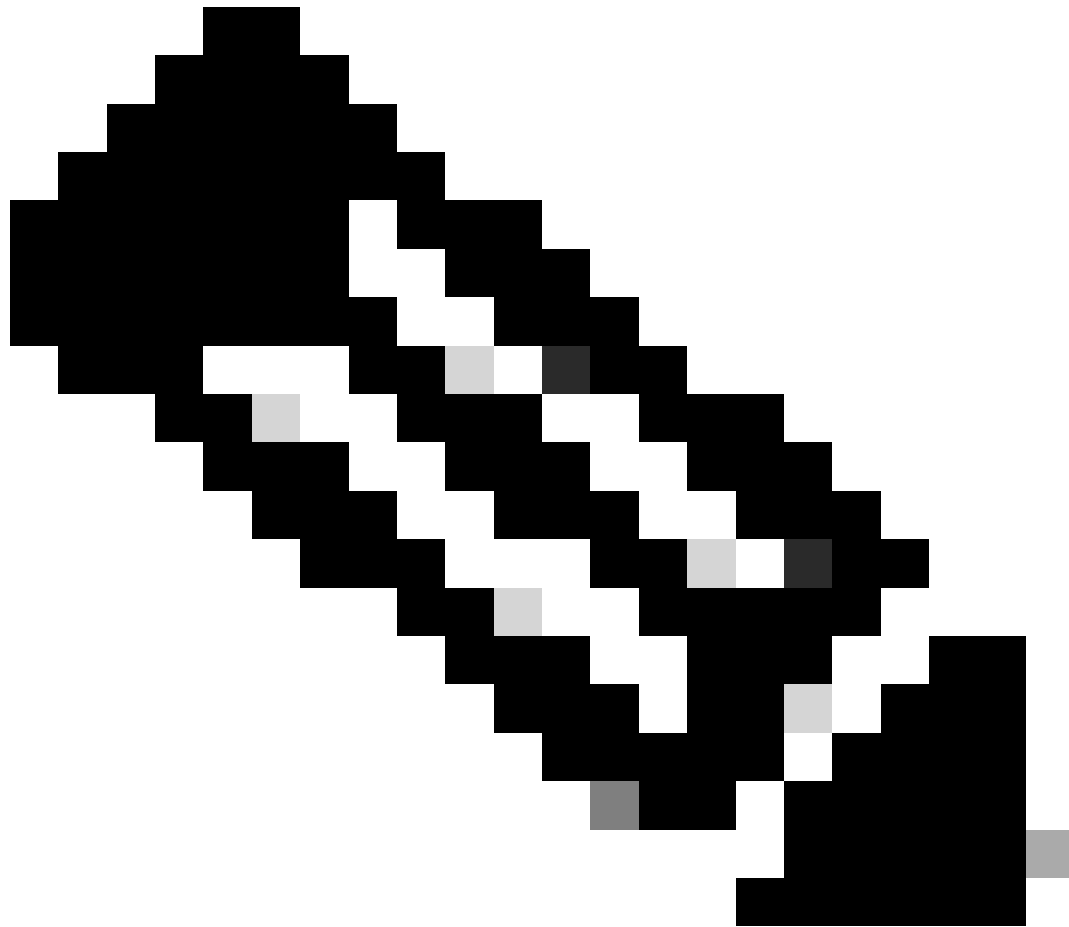
考えられる解決策

これらの問題を解決するには、いくつかの方法があります。最初に、これらのセクションでは、この問題を回避するために、より詳細なポリシーを使用する方法を示します。2つ目は、ブラウザの設定を使用する方法ですが、この問題に該当するブラウザのサブセットのみがブラウザの設定に含まれている点です。

ポリシー管理とローミングクライアント

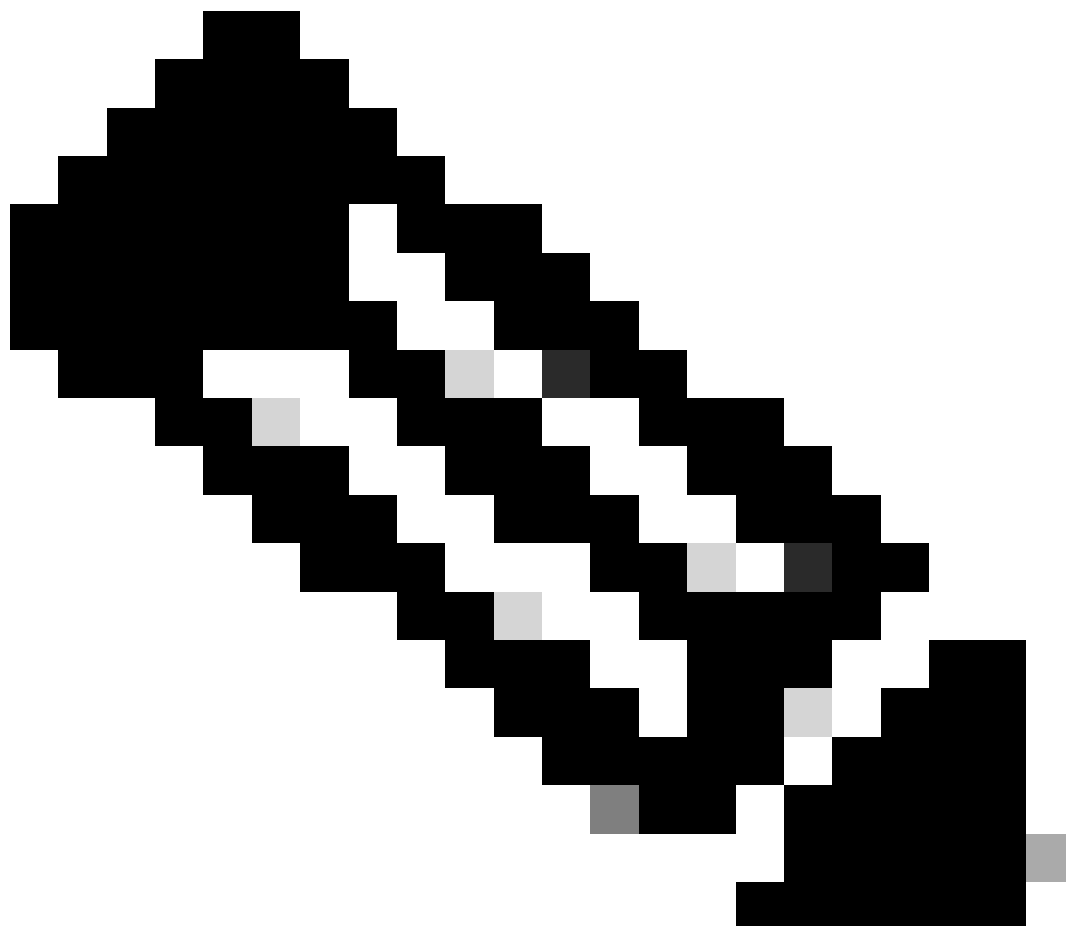
ネットワーク構成またはアクセプタブルユースポリシー(HR)ポリシーに問題があり、このソリューションを妨げている可能性があります。ユーザが特定の時間（昼休みなど）にのみドメインにアクセスすることを許可されている場合、ポリシー管理は効果的なソリューションではありません。Umbrellaは当社のサービスで時間ベースのポリシーアプリケーションを提供できないため、ユーザが常にサイトにアクセスできるようにするだけで問題が発生する可能性があります。パブリック端末などの共有コンピュータでは、Umbrellaローミングクライアントはユーザを区別できず、適切なユーザに適切なドメインを簡単に許可できません。

管理者がそのネットワークのすべてのユーザに同じアクセス権を与えることを好まない場合を除き、サイトやネットワークなどの非詳細なアイデンティティを検討する際には、ポリシー管理はそれほど効果的ではありません。ポリシー管理は、ネットワークの他の部分ではサイトにアクセスできないときにサイトにアクセスできるユーザのサブセットに適用し、マシンにローミングクライアントをインストールして適切なポリシー階層を適用することで、それらのユーザを除外する場合に最も効果的です。



注：シスコは2024年4月2日にUmbrella Roamingクライアントのサポート終了を発表しました。Umbrella Roaming Clientのサポート終了日は2025年4月2日です。Umbrella Roaming Clientのすべての機能は、現在Cisco Secure Clientで使用できます。シスコは、Cisco Secure Clientのみで将来のイノベーションを提供します。移行の計画とスケジュールを今すぐ開始することをお勧めします。UmbrellaローミングクライアントからCisco Secure Clientに移行する方法については、[このサポート技術情報](#)の記事を参照してください。

ブラウザが最初に失敗した検証応答を受信しないため、適切なポリシー管理がこの問題に対する最善のソリューションです。一部のユーザーが、通常はブロックページバイパスを使用してアクセスする必要があるサイトへのアクセスを許可されている場合、これらのユーザーに対して個別のポリシーを構成し、使用を許可するドメインを許可リストに追加できます。ユーザの要求がブロックされることはないため、ブラウザは証明書が一致しないドメインからの要求を受信することはありません。[Umbrella Roaming Client](#)を使用すると、これらの特定のポリシーを提供できます。これは、特定のドメインを許可リストに入れ、特定のユーザが常にこれらのエラーを回避できるようにしていることを意味します。



注:Umbrellaローミングクライアントは、特定のポリシーを複数のユーザに配布する効果的な方法ですが、Active Directory(AD)統合を有効にしている場合は、これらの許可されたポリシーを特定のADユーザにも適用できます。

証明書例外エラーの無視 (Chrome for Windowsのみ)

証明書例外エラーを無視するように設定できるのは、Chrome for Windowsだけです。これにより、このエラーは軽減されます。ブラウザはエラーを無視するように指示され、代わりに通常のUmbrellaブロックページが表示されます。

重要：この方法では、証明書のエラーを無視するようにブラウザが設定されているため、ポリシー管理を調整するよりもリスクが高くなります。その結果、ブラウザが中間者(MiTM)攻撃を受ける可能性があります。したがって、このエラーに対処するための安全なアプローチとしてこれを推奨することはできませんが、回避策となります。

これらの設定変更はコンピュータ単位で行う必要があるため、大規模な環境では困難ですが、機能します。

Mac OS X用のFirefox、Safari、およびChrome

Mac OS X用のFirefox、Safari、およびChromeは、ピンングされたドメインの証明書例外エラーを無視するように設定できません。また、常にHSTSリストを順守します。このエラーに対する既知の回避策はありません。

Internet Explorerの場合

Internet Explorer(IE)には、HSTSの制限は実装されていません。その結果、IEを設定する必要がなくなり、このエラーは表示されません。MicrosoftがブラウザにHSTSを実装することを選択した場合、これはIEの将来のバージョンで変更される可能性があります。

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。