# MacOSにおけるDNSペナルティおよび内部ドメインのアクセス問題の解決

## 内容



## はじめに

このドキュメントでは、DNS解決に影響を与える新しいバージョンのMacOS Big Surの問題を解決する方法について説明します。

## 背景説明

### 対象範囲

- ネットワーク上のAnyConnect Roamingセキュリティモジュールまたは Umbrella（VAまたは転送など）
  - Umbrellaスタンドアロンローミングクライアントは影響を受けません。シングルDNS環境が存在し、すべてのDNSが127.0.0.1で上書きされます)。
- 複数のネットワークインターフェイスがある環境で発生しますが、内部アドレスを解決できるのは1つだけです。例：
  - VPNおよびオフVPN
  - 複数のNIC - 1つの企業および1つの非企業

### 症状

- パブリックドメインへのアクセス機能を維持しながら、ローカルドメインにアクセスできない（または断続的な機能）
  - nslookupは特に影響を受けず、引き続き機能します
    - ping、tracerouteなどが正しく解決しないか、内部ドメインが見つからない

## 問題

この問題は、複数のDNSサーバが存在する場合にDNS解決を管理する方法を処理するMacOSのコ

ードが原因で発生します。1つのネットワークアダプタ上に複数のリゾルバを置くことも、異なるネットワークアダプタ上に複数のリゾルバを置くこともできます。REFUSEDで応答したDNSサーバは、60秒間「ペナルティを科される」ことになります。この場合、この期間中に発生したDNSクエリは、ペナルティを課されていない代替DNSサーバで試行されます。

たとえば、DHCPがAとBという1つのネットワークに関する2つのDNSサーバをアドバタイズし、AがREFUSEDで応答した場合、Bがペナルティを受けない限り、BはAよりも60秒間優先されます。

すべてのDNSサーバがペナルティを受けている場合、MacOSは最もペナルティの低いサーバを優先します。 たとえば、Aがすでにペナルティを課されているのにBがペナルティを科された場合、MacOSはBよりもAを優先します。

これは、MacOS 11以降でDoH(DNS over HTTPS)をアサートしようとする方法によって複雑になります。 MacOSは、可能な場合はユーザセットのDoHプロバイダーを優先するようにプログラムされています。これにより、Umbrella DNSセキュリティが回避されます。つまり、MacOSがDoH要求を開始すると、(RFCに従った)REFUSED応答が返されます。DNSのペナルティが設定されているため、内部ドメインが正しく解決されない可能性があります。この問題の詳細については、「iOS 14およびmacOS 11でのDNSリゾルバの選択」を参照してください。

# 解決方法

Appleがこの動作を変更する予定なのか、Umbrellaがこの問題を回避するために動作を変更できるのか、まだ把握していません。現時点では、回避策として次の2つのオプションがあります。

## オプション 1

グループポリシーでsplit-DNSを有効にし、内部ドメインがトンネル経由でのみ解決可能になるように、split-DNS設定に内部ドメインを追加します。これにより、これらのドメインはネイティブOSリゾルバによってのみトンネル経由で解決可能であるのに対し、他のドメインはトンネル外でのみ解決可能になります。

## オプション 2

グループポリシーでtunnel-all-DNSを有効にして、DNSトラフィックがトンネルの外部に送信されないようにします。

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。