

アクティビティレポートの異常なDNSクエリの特定と理解

内容

[はじめに](#)

[ランダムDNS要求の例](#)

[ランダムDNS要求の説明](#)

[なぜこのような要求が発生するのでしょうか。](#)

[原因としてChromeを特定する方法](#)

はじめに

このドキュメントでは、アクティビティレポートに表示される可能性のあるランダムなDNS要求の性質と原因、およびその発生源を特定する方法について説明します。

ランダムDNS要求の例

これらの要求の例は、通常は異常な、または一見ランダムな文字列として表示されます。

```
iafkbge  
nwvkqoogx  
uefakmvidzao  
claeedov  
cjkcmrh  
cjemikołwaczyb  
ccshpypwddmro  
cdsvmfjgvfcnbob  
cegzauxjexfrk  
ceqmhxowbcys  
cewigwgvfd  
cexgxhwgt
```

ランダムDNS要求の説明

すべてのインターネットサービスプロバイダーがDNS応答に関するRFCルールに準拠しているわけではありません。アクティビティ検索レポートに表示されるこれらの不明瞭なDNS要求は、エンドユーザーを保護するために一意の要求を送信するGoogle Chromeの方法に起因します。

なぜこのような要求が発生するのでしょうか。

- 一部のインターネットサービスプロバイダーは、存在しないドメインに対するDNSクエリ

に、プロバイダー所有のアドレスを指すAレコードで応答します。結果として表示されるランディングページには、通常、「did you mean...」などのアドバタイズメントとメッセージが表示されます。このタイプの操作と関連する結果の概要については、[DNS/ハイジャックに関するWikipediaの記事](#)を参照してください。

- RFC標準によれば、存在しないドメインに対するDNS要求の正しい応答はNXDOMAINです。広告是一般に不要であるため、Googleはこの動作をテストする方法を開発しました。起動時に、Chromeは3つの要求を送信し、応答が何であることを確認します。テストドメインがNXDOMAINに解決されるのではなく同じAレコードに解決される場合、Chromeはこの動作を検出し、エンドユーザからのアドバタイズメントを非表示にします。
- この手法は、ランダムに見えるDNS要求の唯一の原因ではありませんが、最も一般的なシナリオの1つを表しています。

原因としてChromeを特定する方法

- 同じ内部ホストから送信された3つの異常なDNSクエリのグループを探します。このパターンは、Chromeがテストクエリを生成していることを示します。

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。