# DNS のセキュリティと攻撃の防止

DNS 攻撃は、ネットワークの DNS サービスの可用性または安定性を標的とする攻撃です。DNS キャッシュポイズニング、DDoS、DNS スプーフィングなど、さまざまな方法で DNS を攻撃できます。この章では、Cisco Prime Network Registrar で使用可能であり、DNS のセキュリティ関連の脅威と攻撃の防止に役立つ機能について説明します。



# Cisco Prime Network Registrar での DNS 攻撃の防止

Cisco Prime Network Registrar の次の機能は、DNS セキュリティ関連の脅威と攻撃を防止するのに役立ちます。

### キャッシュポイズニング

キャッシュ ポイズニング攻撃は、DNS キャッシュ内の既存のエントリを変更したり、DNS キャッシュに新しい無効レコードを挿入したりすることができます。この攻撃により、ホスト名が誤った IP アドレスを指すようになります。キャッシュポイズニング攻撃の処理の詳細については、DNS キャッシュ ポイズニングの検出と防止を参照してください。

- **UDP ポートのダイナミックな割り当て**

  キャッシング DNSの サーバーは多くの UDP ポート番号を使用します。多くのポート番号を使用することで、誕生日攻撃によるキャッシュ ポイズニングのリスクが軽減されます。詳細については、UDP ポートの動的割り当てを参照してください。

- **DNS トランザクション ID のランダム化**

  DNS 応答の検証に使用される DNS トランザクション ID と送信元ポート番号は、十分にランダムではなく、簡単に予測できるため、攻撃者は DNS クエリに対する偽装応答を作成できます。DNS サーバーは、このような応答を有効と見なします。

- **ランダム化されたクエリ名**

  ドメインのランダム化により、DNS サーバーは、ランダムに生成されたクエリ名を使用し、アップストリームクエリを送信して解決できます。有効なネームサーバーはクエリ名を変更せずに応答するため、この手法を使用して応答が有効であることを確認できます。

DNS のセキュリティと攻撃の防止

Cisco Prime Network Registrar ではアップストリーム クエリのランダム化をサポートしていますが、ランダム化されたケースを維持しないネーム サーバーがいくつかあります。したがって、ケースのランダム化をイネーブルにすると、有効なネーム サーバーをブロックする可能性があります。*randomize-query-case-exclusion* 属性を使用すると、除外リストを作成できます。これにより、ケースのランダム化を引き続き使用できますが、維持されないネームサーバーは除外され、有効な回答で応答を続行します。詳細については、リゾルバ設定の指定を参照してください。

## DDoS 攻撃

分散型サービス妨害攻撃（DDoS 攻撃）では、ターゲットサーバー、サービス、またはネットワークにフラッディングする着信トラフィックが、さまざまな送信元から発信されます。そのため、単一の送信元をブロックするだけでは攻撃を阻止することができません。

- **レート制限**

  レート制限によって、少数のクライアントで DNS サーバーが過負荷になるのを防ぐことができます。また、権威 DNS サーバーに対するアップストリーム クエリ攻撃からも保護します。この機能によって、一部の DDoS 攻撃を軽減し、サーバーが少数のクライアントによって過負荷になるのを防ぐことができます。これにより、悪意のあるトラフィックを制限することができます。詳細については、レート制限のキャッシュ管理を参照してください。

- **スマートキャッシュ**

  権威 DNS サーバーが停止したり、その他の理由でオフラインになったりすると、影響を受ける可能性の低いインターネット サービスにアクセスできるという問題が発生する可能性があります。スマートキャッシングを使用すると、キャッシング DNS サーバーが、権威ネームサーバーに到達できない場合でも期限切れのデータ（最新の既知の応答）を引き続き使用できるようになります。キャッシング DNS サーバーは引き続き権威ネームサーバーに接続し、ネームサーバーが再び機能し始めると期限切れのデータを更新します。スマートキャッシングは、ネットワークの停止や、権威ネームサーバーを使用不能にする可能性のある DDoS 攻撃を軽減するのに役立ちます。詳細については、スマートキャッシュの有効化を参照してください。

- **DNS アンプ攻撃の防止**

  DNS アンプ攻撃は、パブリックアクセスが可能なオープン DNS サーバーを使用してターゲットシステムを DNS 応答トラフィックでフラッディングさせる、一般的な形式の DDoS 攻撃です。主な手法は、攻撃者が DNS 名のルックアップ要求をオープン DNS サーバーに送信し、送信元アドレスをスプーフィングしてターゲットのアドレスにします。DNS サーバーが DNS レコード応答を送信すると、代わりにターゲットに送信されます。攻撃者は通常、アンプ効果を最大化するために、できるだけ多くのゾーン情報の要求を送信します。このタイプのほとんどの攻撃は、攻撃者が送信するスプーフィングされたクエリのタイプは単一の要求で DNS ゾーンに関するすべての既知の情報を返す「ANY」です。応答のサイズは要求よりもかなり大きいため、攻撃者はターゲットに向けられるトラフィックの量を増やすことができます。

- **Allow ANY Query ACL**

DNS のセキュリティと攻撃の防止

Cisco Prime Network Registrar では、[サーバーの管理（Manage Servers）] ページの *allow-any-query-acl* 属性が応答のサイズを最小化するのに役立ちます。この属性は、権威 DNS サーバーページとキャッシング DNS サーバーページの両方に存在し、デフォルト値は「none」です。

- **最小限の応答**

  Cisco Prime Network Registrar は、権限と追加のセクションが応答で省略される *minimal-responses* をサポートしています。これによりクエリの応答サイズが小さくなるため、サービス拒否をある程度遅らせることができます。Cisco Prime Network Registrar 11.0 以降、*minimal-responses* は キャッシング DNS サーバー でデフォルトで有効になっており、権威 DNS サーバーではデフォルトで無効になっています。

## データの認証と許可

- **DNSSEC**

  DNSSECにより、データ出自の認証、データの完全性の確認、および認証による存在否定が可能になります。DNSSEC を使用すると、DNS プロトコルが特定のタイプの攻撃（特に DNS スプーフィング攻撃）の影響を受けにくくなります。Cisco Prime Network Registrar は、権威 DNS サーバーとキャッシング DNS サーバーの両方で DNSSEC をサポートしています。

  権限 DNS サーバーでの DNSSEC サポートの詳細については、権威 DNSSEC の管理を参照してください。

  キャッシング DNS サーバーでの DNSSEC サポートの詳細については、DNSSEC の管理を参照してください。

- **DNS ファイアウォール**

  キャッシング DNS ファイアウォールは、ネットワーク上で機能することが許可されているドメイン名、IP アドレス、およびネームサーバーを制御します。また、DNS ファイアウォールルールは、RPZ を使用して権威 DNS サーバー上の特別に指定されたゾーンに対しても設定できます。RPZ と RR データを DNS リゾルバと組み合わせることにより、DNS サーバーの不正使用を防ぐ有効な DNS ファイアウォールを構成できます。詳細については、DNS ファイアウォールの管理を参照してください。

- **Cisco Umbrella**

  Cisco Umbrella は、フィッシングやマルウェアなどのインターネット上の脅威に対する防御の最前線となります。Umbrella を解決に使用するようにキャッシング DNS を設定することにより、シスコの Umbrella のクラウドサービスで、要求されたドメイン/ホストに関する最新の応答を提供することが可能になります。詳細については、Umbrella を使用するためのキャッシュ DNS の設定を参照してください。

- **ACL を使用したセキュアな DNS サーバーアクティビティ**

  ACL に基づいて特定のゾーンのみを照会するようにクライアントを制限できます。

  - ゾーンクエリの制銀：権威 DNS サーバーの属性 *restrict-query-acl* は、サーバーが受け入れる必要があるデバイスクエリを制限します。キャッシング DNS サーバーの属性

DNS のセキュリティと攻撃の防止

*acl-query* と *acl-do-not-query* では、それぞれ、照会される IP アドレスと照会されないサブネットを指定します。

- ゾーン転送要求の制限：*restrict-xfer-acl* 属性を使用して、既知のセカンダリサーバーへのゾーン転送要求をフィルタリングします。
- DDNS 更新の制限：*update-acl* 属性を使用して、既知の DHCP サーバーからの DDNS パケットをフィルタリングします。
- 悪意のあるクライアントのブロック：*acl-blocklist* 属性は、アクセスコントロールリストに登録されているクライアントからの要求をブロックします。このリストには、ホスト、ネットワークアドレス、およびその他の ACL を含めることができます。リストの ACL と一致するクライアントからの要求はドロップされます。

- **TSIG または GSS-TSIG を使用したセキュアゾーン転送と DNS の更新**

  セキュア モードでのゾーン転送は、HMAC MD5 ベースの TSIG と GSS-TSIG の両方をサポートします。オプションの TSIG キーまたは GSS-TSIG キー（『*Cisco Prime Network Registrar 11.0 DHCP User Guide*』の「*Transaction Security*」の項または「*GSS-TSIG*」の項を参照）をプライマリサーバーアドレスに追加できます。それには、エントリを *address–key* の形式でハイフンでつなぎます。

- **DoT によるセキュアなクエリ**

  DNS over TLS （DoT）は、TLS プロトコルを介して DNS クエリと応答を暗号化およびラップするためのセキュリティプロトコルです。これにより、クライアントとリゾルバ間のプライバシーとセキュリティが向上します。基本的な接続プロトコルとして TCP を使用し、TLS 暗号化と認証を介したレイヤを使用します。

  権威 DNS サーバーの TLS 設定の詳細については、「権威 DNS サーバーの管理」の章の、「TLS の設定の指定」の項を参照してください。

  キャッシング DNS サーバーの TLS 設定の詳細については、「キャッシング DNS サーバーの管理」の章の、「TLS の設定の指定」の項を参照してください。