JPRS トピックス＆コラム

■DDoSにあなたのDNSサーバーが使われる
～DNSリフレクター攻撃の脅威と対策～

インターネットに接続されている他人の機器をDDoS攻撃の踏み台として悪用する「リフレクター攻撃」について、その概要とDNSにおける事例・対策について解説します。

■ネットワークにおけるリフレクター

リフレクター（reflector）の本来の意味は**反射板**です。例えば、自動車に積まれる三角停止表示板や写真撮影で用いるレフ板は、光を反射するリフレクターです。

インターネット上でサービスを提供しているサーバーは、利用者からの問い合わせに対応する形で応答を返します。つまり、それらのサーバーはネットワークにおけるリフレクターの一種であると言えます（図 1）。

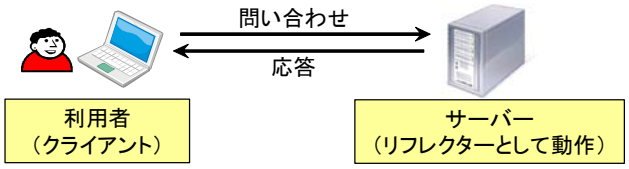

図 1: インターネット上の通信

■リフレクターを攻撃に悪用

リフレクター攻撃では、インターネットに接続されているリフレクター（サーバーなど）が攻撃に悪用されます。具体的には、攻撃者が**送信元の IP アドレスを偽装した問い合わせ**をリフレクターに送りつけることで攻撃目標に応答を誘導し、**攻撃を間接的に実行**します（図 2）。

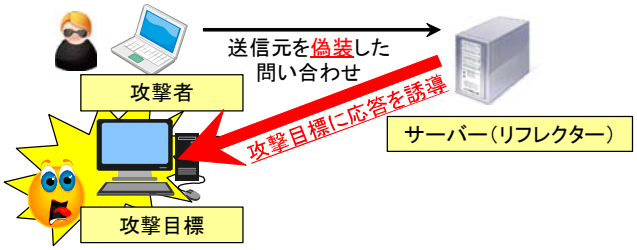

図 2: リフレクター攻撃

■攻撃者から見たリフレクター攻撃のメリット

リフレクター攻撃には、目標を直接攻撃する場合に比べ、二つのメリットが存在します。

① **真の攻撃者を特定しにくくできる**

間接的な攻撃形態であることから、真の攻撃者を特定しにくくなります[1]。

② **攻撃を大規模化できる**

増幅率（問い合わせに対する応答のサイズ）の高いリフレクターを用いる、インターネット上の多数のリフレクターを同時に用いるといった手法により、攻撃を大規模化できます。

■リフレクター攻撃成立の条件

攻撃者がリフレクター攻撃を効率良く実行するためには、以下の条件を満たしている必要があります。

① **送信元 IP アドレスの詐称が可能である**

通信プロトコルとして **UDP を用いている**場合、TCP の場合に比べ、送信元 IP アドレスの詐称が容易になります。

② **リフレクターが多数存在している**

そのプロトコルが**インターネット上で広く利用**されていればいるほど、悪用可能なリフレクターを発見できる可能性が高くなります。

③ **リフレクターによる増幅率が高い**

応答のサイズが問い合わせのサイズに対し大きい程、攻撃時の効率を高くできます。

■リフレクター攻撃に利用されやすいプロトコル

DNS や NTP[2]は前述した三つの条件をすべて満たしており、**リフレクター攻撃に利用されやすいプロトコル**であると言えます。そのため、それらの機能を持つサーバーや機器をインターネットに接続する場合、リフレクター攻撃の踏み台とならないように**適切に設定・運用**する必要があります。

---

1 特定が不可能になるわけではなく、2013 年 3 月に発生した Spamhaus/CloudFlare を標的とした大規模なリフレクター攻撃では、攻撃の首謀者が逮捕・起訴されています。

2 Network Time Protocol: インターネットにおける時刻同期プロトコルとして、RFC 5905 で定義されています。

※掲載内容は2014年3月現在のものです。

■DNS リフレクター攻撃

DNS サーバーには**キャッシュ DNS サーバー**と**権威 DNS サーバー**の二種類がありますが、これらはいずれもリフレクター攻撃に悪用される可能性があります。

▼オープンリゾルバーによる攻撃

キャッシュ DNS サーバーは組織内からの DNS 問い合わせを受け付けてインターネット上の権威 DNS サーバーを検索する、名前解決機能を提供します（図 3）。

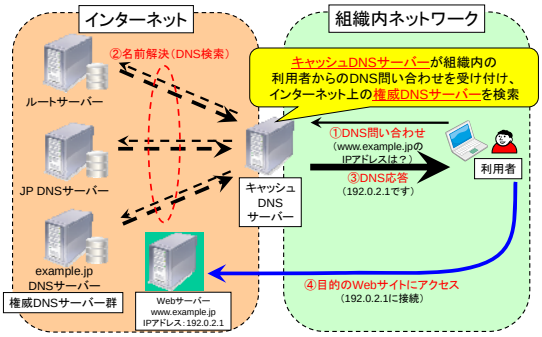

図 3: キャッシュ DNS サーバーの役割

しかし、インターネット上には本来制限すべき外部の利用者からの DNS 問い合わせも処理してしまう、**オープンリゾルバー**が多数存在しています[3]（図 4）。

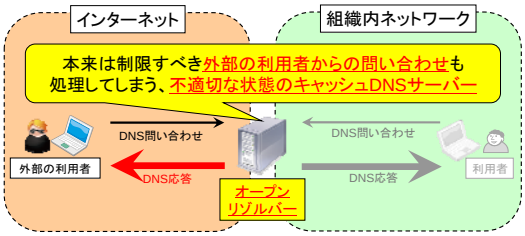

図 4: オープンリゾルバー

オープンリゾルバーは DNS リフレクター攻撃の踏み台となりやすく、**きわめて危険な存在**です（図 5）。

▼オープンリゾルバーの種類

オープンリゾルバーには**本来不要な名前解決機能が有効にされてしまっている権威 DNS サーバー**や、**WAN 側からの DNS 問い合わせも処理してしまうホームルーターなど**も含まれています。これらはいずれも不適切な状態であり、**設定の修正など**が必要になります。

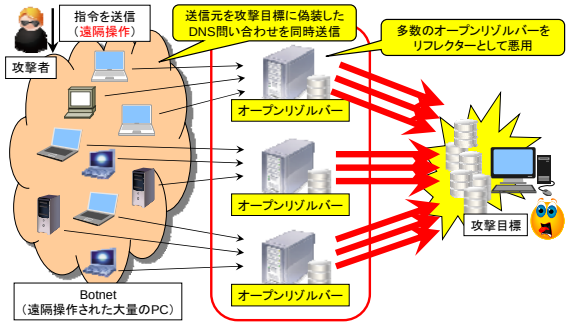

図 5: オープンリゾルバーによる DNS リフレクター攻撃

▼権威 DNS サーバーによる攻撃

2012 年頃から、権威 DNS サーバーを DNS リフレクター攻撃に悪用する事例が報告され始めています（図 6）。権威 DNS サーバーはキャッシュ DNS サーバーと異なり事前のアクセスコントロールの適用が難しく[4]、**オープンリゾルバーの場合とは異なる対策**が必要になります。

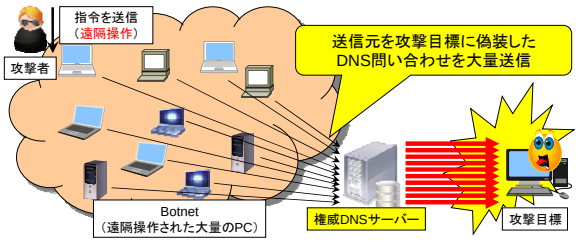

図 6: 権威 DNS サーバーによる DNS リフレクター攻撃

■攻撃対策

DNS リフレクター攻撃への対策には、以下の三つが有効です。

① **ネットワークにおける送信元検証の適用**
送信元を詐称したデータがインターネット上に送られないように、ネットワーク側で設定する。

② **キャッシュ DNS サーバーにおける設定修正**
設定を修正し、オープンリゾルバーでなくす。

③ **権威 DNS サーバーにおける DNS RRL[5]の導入**
防御技術である DNS RRL を導入する。

対策の詳細については JPRS Web で公開している技術解説「**DNS Reflector Attacks（DNS リフレクター攻撃）について**」をご参照ください。

---

3 2014 年 3 月時点で、世界中に 2,300 万台以上のオープンリゾルバーが存在していると報告されています（openresolverproject.org 調べ）。

4 サービス対象がインターネット全体となるため。

5 Response Rate Limiting