Distributed via @police http://www.npa.go.jp/cyberpolice/

平成 26 年1月 17 日

Topic

NTP[1]サーバを踏み台としたリフレクター攻撃（NTP リフレクター攻撃）に対する注意喚起について

適切な設定がされないままインターネットに公開されている NTP サーバは、リフレクター攻撃の踏み台として悪用される可能性があります。

1 NTP リフレクター攻撃の原理

NTP サーバを踏み台として実行されるリフレクター攻撃（NTP リフレクター攻撃）は、平成25 年中に広く認識されるようになった DNS リフレクター攻撃[2]と同様の原理で実行されます。DNSリフレクター攻撃では、インターネット上から任意の問い合わせが可能となっているDNSサーバ（オープンリゾルバ）が踏み台となります。これと同様に NTP リフレクター攻撃では、インターネット上からの問い合わせが可能な NTP サーバが攻撃の踏み台として悪用されます。

攻撃者が、踏み台となる NTP サーバに対して発信元を攻撃対象に偽装して問い合わせを行うと、踏み台となった NTP サーバは、偽装された問い合わせ元、つまり攻撃対象に対して問い合わせ結果を回答します（図1）。この際に、問い合わせのデータサイズと比較して、NTP サーバからの回答のサイズが大きくなり、攻撃者からの攻撃パケットが、あたかも NTP サーバで反射増幅されて攻撃対象に届くかのように動作します。このため、この種の攻撃は「リフレクター（反射器）攻撃」と呼ばれます。

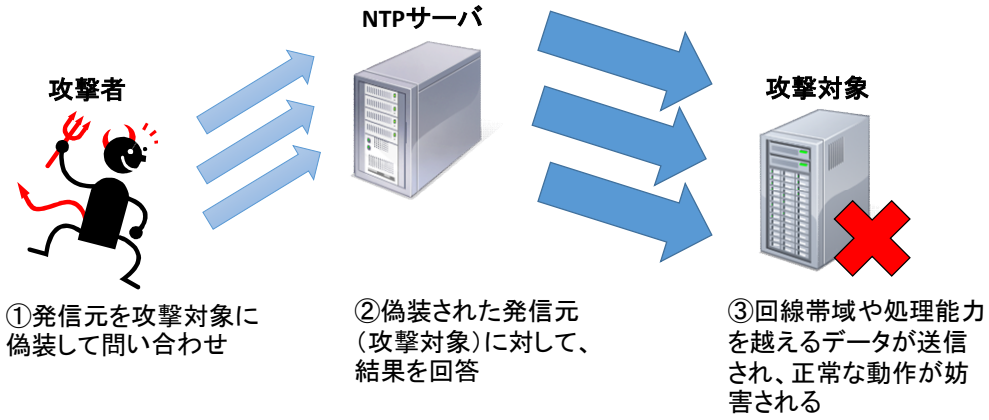

図1 NTP リフレクター攻撃の原理

NTP サーバから返される回答のデータサイズが大きいほど、リフレクター攻撃の増幅率は大きくなります。NTP サーバのモニタリングに使用されるコマンド「monlist」の回答は、そのサ

[1] NTP とは、「Network Time Protocol」の略であり、ネットワーク経由でコンピュータ等の時刻同期を行うプロトコルです。

[2] DNS リフレクター攻撃（DNS リフレクション攻撃）については、次の資料を参照してください。
「DNS リフレクション攻撃に対する注意喚起について」（平成 25 年4月 11 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130411.pdf

イズが非常に大きくなるため、特にその危険性が指摘されています。「monlist」は過去にやりとりした最大 600 件のアドレスを回答するため、その増幅率は数十倍から数百倍となる可能性があります。NTP のサーバプログラム「ntpd」においては、このコマンドの動作は脆弱性[1]として扱われており、最新の開発バージョンでは無効とされています。

2　定点観測システムにおける観測状況

定点観測システムにおいては、NTP で使用されるポート 123/UDP に対するアクセス件数が、平成 25 年 11 月から断続的に増加している状況となっています（図2）。これらのアクセスは、インターネット上からの問い合わせが可能なNTPサーバの探索又はNTPリフレクター攻撃の試行である可能性が考えられます。

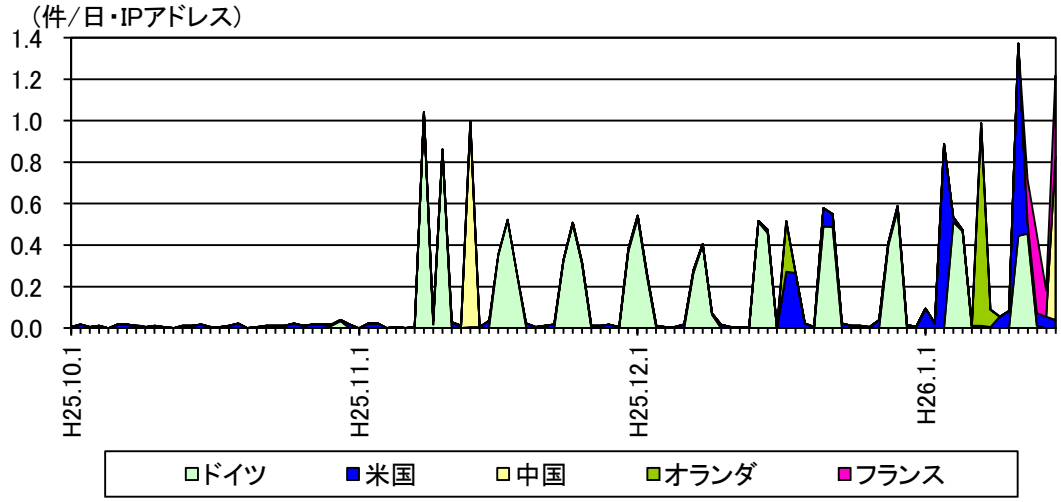

図2　宛先ポート 123/UDP に対する発信元国・地域別アクセス件数の推移
（H25.10.1～H26.1.15）

3　国内外における注意喚起等の状況

(1) 平成 25 年 12 月 26 日以降、米国のセキュリティ対策企業、SANS 及び US-CERT 等から注意喚起が実施されています。

(2) 米国の複数のゲームサイトに対して、最大 100Gbps に及ぶ NTP リフレクター攻撃が実行され運営が妨害された旨が、平成 26 年1月 14 日に報道されています。

(3) 平成 26 年1月 15 日に、一般社団法人 JPCERT/CC からも日本語による注意喚起[2]が実施されています。

[1] 「JVNVU#96176042 NTP が DDoS 攻撃の踏み台として使用される問題」（CVE-2013-5211）
https://jvn.jp/cert/JVNVU96176042/index.html

[2] 「ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起」（平成 26 年1月 15 日）
http://www.jpcert.or.jp/at/2014/at140001.html

４　NTP リフレクター攻撃の踏み台とならないために推奨する対策

各組織が管理する機器が、NTP リフレクター攻撃の踏み台として悪用されないために、次の対策を実施することを推奨します。

(1) NTP サーバを外部に公開する必要がない場合には、適切なアクセス制限を実施して、インターネットからの通信を遮断する。

(2) ルータ等のインターネットに接続されているネットワーク機器においても、意図せずに外部へ NTP サーバの機能を公開していないか確認する。

(3) 外部に NTP サーバを公開する必要がある場合には、設定により「monlist」機能を無効とするか、「monlist」機能が無効となっている最新の開発バージョンの「ntpd」にアップデートする。