NTP Reflection DDoS Attack
解説ドキュメント

2015/3/13 第 1 版

JANOG NTP 情報交換 WG

ntp-talk-wg@janog.gr.jp

目次

1. 概要

本ドキュメントは、NTP を悪用したサービス妨害攻撃(NTP Reflection DDoS)について問題点と対策を解説するものです。

ネットワークのトラヒック(通信量)を増大させ、回線帯域を占有しサービスを妨害する DoS(サービス妨害)攻撃は、以前より顕在化しているセキュリティ課題の一つです。なかでも、大量の送信元から分散して行われる DDoS(分散型サービス妨害)攻撃は、正常通信と攻撃通信を判別しての防御が困難なこと、防御する設備を保有していても耐えられる規模が限られていることから、対策の困難な課題として知られています。

このような特徴を持つ DDoS 攻撃は定常的に観測されてきましたが、2013 年後半よりネットワーク上で時刻同期を行うためのプロトコルである NTP(Network Time Protocol)を悪用される事例が増えてきました。その背景には、NTP を用いることで効率よく広帯域の DDoS を発生させることができるという情報が、世の中に広く知れわたったことにあると考えられます。攻撃手法は、有効性が広く認知されることで、さらに流行します。このため、今後もさらに流行していく可能性があります。

一方、本事象を根本的に対策するためには、インターネット全体にその対策手法を広く浸透させる必要があります。しかしながら、その対策手法についての情報が十分に整備されているとはいえません。啓発活動を進めていく上で必要な情報の参照先が不十分であり、必要な人に、必要な情報が、伝わる記述で提供されているとは言いがたいのが実情です。

本ドキュメントは、本事象の原因と対策を、企業や組織の情報システムやインターネット接続事業者(ISP)を対象にまとめたものです。そして、情報システム担当や、エンジニアがとるべき対策を整理し紹介するものです。

2. 問題点

2.1. DDoS 攻撃事例から見る脅威

2.1.1. 海外の事例

昨今の DDoS 攻撃事例で有名なものとして、2014 年 2 月に CloudFlare 社が観測し公表した事例[1][2]があります。この事例では、観測史上最高の 400Gbps を超える DDoS 攻撃が観測されたことに加え、ネットワーク上で時刻同期を行う NTP(Network Time Protocol)が悪用されたことで話題となりました。これ以前に最大の事例であった DNS を用いた攻撃事例[3]と比較し、悪用されたサーバ 1 台あたりのトラヒックは 6 倍以上であったと報告されています。本事例では具体的に 4,529 台の NTP サーバが悪用され、平均して 87Mbps の DDoS トラヒックを発生させていたと言及されています。

CloudFlare 社の事例以外にも、オンラインゲームの基盤が攻撃された事例[4]でも、NTP が悪用されたとの報告があります。さらに、Incapsula 社のレポート[5]によれば、2014 年 1 月および 2 月に観測された DDoS 攻撃に悪用された手法のうち、NTP を悪用したサービス妨害攻撃(NTP Reflection DDoS)が最も主要な手法であったと報告されています。

2.1.2. 国内の事例

日本国内では DDoS 攻撃をはじめとするセキュリティインシデントの詳細は世の中に公表されにくい傾向があります。このためか、公式に企業や組織が DDoS 攻撃を受け、その攻撃に NTP を悪用されたことを明らかにしている事例はありません。一方、インターネットを介して発生するセキュリティインシデントについて、日本国内の事例の報告を受け付ける JPCERT/CC では、ntpd の monlist 機能を使った DDoS 攻撃に関するインシデント報告を受けていると報告・注意喚起[6]を行っています。

また、実際に日本の企業や組織が DDoS 攻撃の標的となる事例も出てきています。Symantec 社のブログ[7]によれば、社会的・政治的な主張を目的としてサイバー攻撃を行うハクティビスト集団 Anonymous が、石油関連企業を対象とした DDoS 攻撃を呼びかけたところ、その対象に日本企業も含まれていたことが確認されています。くわえて、国内オンラインゲームの基盤が長期間にわたり DDoS 攻撃を受けた事例[8]もあります。

このように、国内の情報システムにとっても DDoS は身近な脅威であり、その手法の一つとして本ドキュメントのテーマである NTP を用いた手法が悪用される可能性が高い状況となっています。

2.2. 脅威のメカニズム

本節では、脅威のメカニズムを解説するために、まず基本となる UDP パケットの送信元詐称を用いた DDoS 攻撃のメカニズムを解説します。そして次に、NTP が攻撃に悪用されやすい要因を示します。

2.2.1. UDP パケットの送信元詐称を用いた DDoS 攻撃

ネットワークで広く使われている UDP(User Datagram Protocol)はコネクションレスなプロトコルであるため、送信元の詐称が容易であるという特徴があります。この特徴を悪用し、攻撃者は UDP を用いるサービスのリクエストパケットを、送信元アドレスを標的システムのものに詐称しサーバ(踏み台、リフレクタ)に送信します。すると、サーバは攻撃者ではなく詐称された標的システムにレスポンスを返します。このとき、レスポンスサイズが大きく、大量であれば、標的システムのネットワーク帯域を溢れさせることができます。これが、UDP パケットの送信元詐称を用いた DDoS 攻撃(UDP-based Amplification Attacks[9])の基本的な仕組みです。

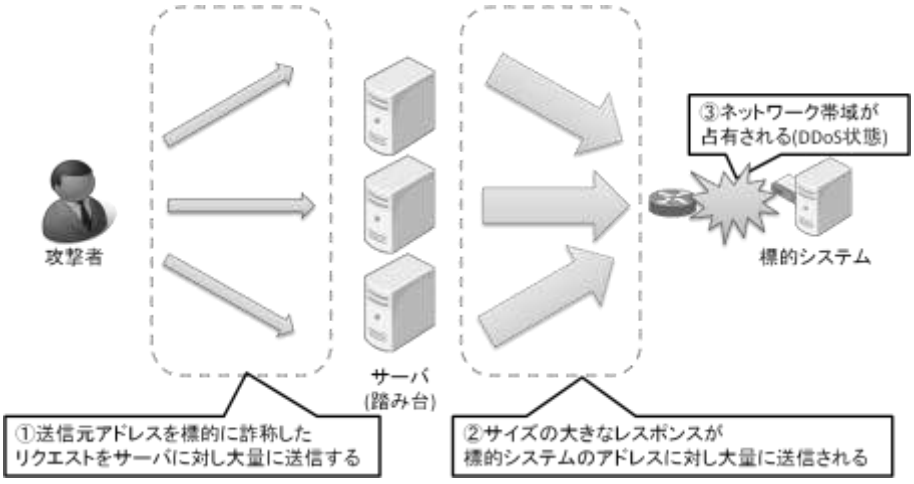

図 1 UDP パケットの送信元詐称を用いた DDoS 攻撃

2.2.2. NTP が悪用される要因

これまでにも DNS や SNMP などが DDoS 攻撃に悪用されてきましたが、数ある UDP サービスの中から特に NTP が悪用される理由には、増幅率が高い、踏み台の数が多いという攻撃者にとって都合のよい背景があります。表 1 は、DDoS 攻撃に悪用されやすいサービスの、増幅率と悪用されやすいコマンドをまとめたものです。NTP の monlist コマンドを悪用した場合、増幅率は最大で 556.9 倍、平均でも 200 倍程度の増幅率となります。これ

は他のサービスに比べ、抜群に高い増幅率であり、1Gbps のトラヒックを発生させるために必要な帯域はわずか 5Mbps、10Gbps の攻撃であっても 50Mbps にすぎないことを示しています。

Protocol	Amplification Factor(増幅率)	Vulnerable Command
NTP	556.9	monlist
DNS	28 to 54	Any ほか
SNMP	6.3	GetBulk request

表 1 悪用されやすいプロトコル/サービスの例([9]より翻案)

また、ネットワークに接続されるサーバやネットワーク機器だけでなく、ネットワークプリンタやネットワークカメラなどの多種多様のデバイスが時刻同期機能を持っており、NTP を利用しています。それら数多くの機器が一部分であるとはいえ不適切な状態で運用されていることから、攻撃者が悪用しやすく、大規模の攻撃を発生させやすい状況となっています。

これは NTP の仕様に基づく構成と密接に関わっています。NTP は図 2 に示すとおり Stratum0 と呼ばれる精度の高い NTP サーバを頂点とする階層構造をとります。そして、NTP デーモンは他の機器で稼働する NTP サービスを参照するクライアントでもあり、同時に他の機器に NTP サービスを提供するサーバとしても動作します。このため、各々の NTP デーモンで適切に制限しなければ、不特定多数にサービスを提供してしまいます。なかでも DDoS 攻撃に悪用される monlist コマンドは、本来不特定多数に提供する必要の無いサービスですが、このような特性に基づく構成と、システム管理者の理解不足、不適切なデフォルト設定などの要因により、不適切な状態の機器が多数存在する状況となっています。

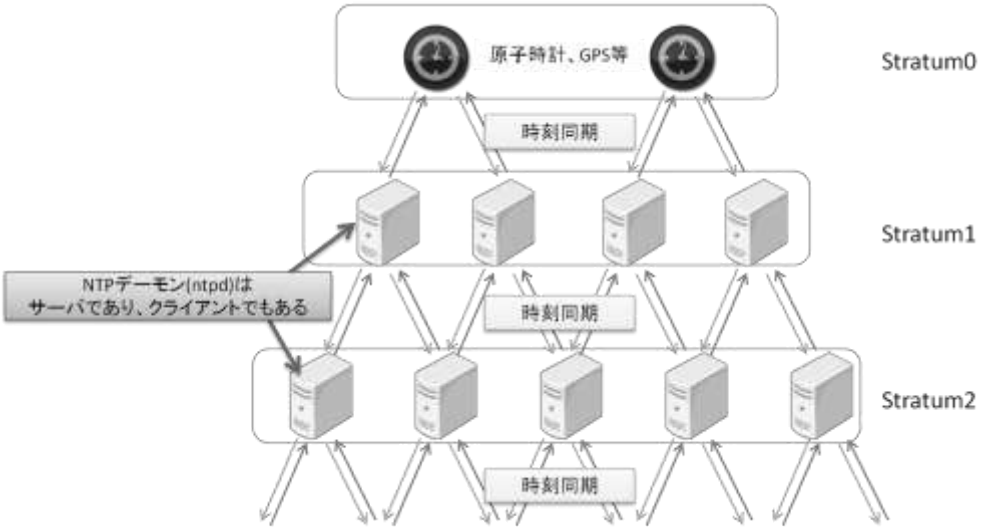
原子時計、GPS等
Stratum0
時刻同期
Stratum1
NTPデーモン(ntpd)は
サーバであり、クライアントでもある
時刻同期
Stratum2
時刻同期

図 2 NTP の階層構造

3. 対策

本章では、NTP を悪用したサービス妨害攻撃(NTP Reflection DDoS)について、企業の情報システムやインターネット接続事業者(ISP)の設備を対象とした技術的な対策を紹介します。基本的な考え方として、攻撃は元から絶つことが望ましいといえますが、各々の立場によってできる対策が異なるため、全体像を図 3 に示し、各々の立場を踏まえ、とるべき対策を紹介していきます。自社の設備やサービスを守るための、踏み台(リフレクタ)からの攻撃への対策については 3.1 節、自社や顧客が加害者とならないための、攻撃者と踏み台(リフレクタ)の間の悪用を防ぐ対策については 3.2 節に示します。

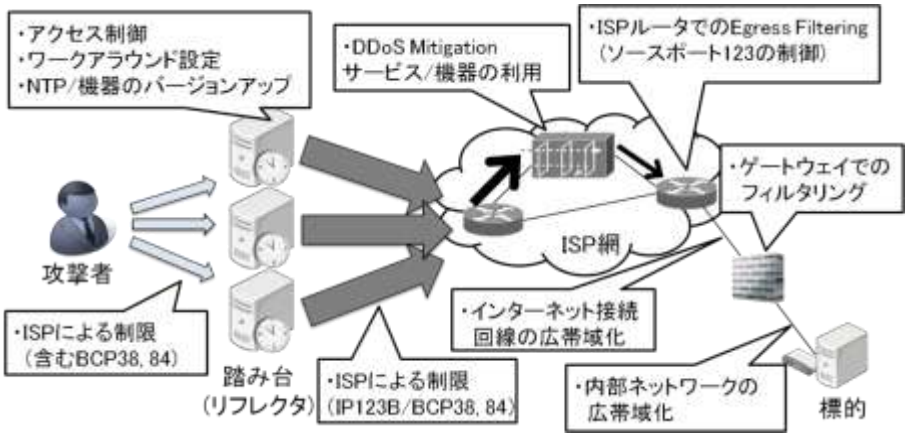

図 3 NTP を悪用したサービス妨害攻撃への対策(全体像)

3.1.攻撃から守る対策 - 設備やサービスを守るために

3.1.1. 企業の情報システムを守るために担当者がとるべき対策

DDoS は回線帯域という資源に対し、それを量で埋め尽くす攻撃手法であるため、資源を上回る量の攻撃トラヒックに対して対抗できる対策はありません。このため、ボトルネックを洗い出し、緩和策により攻撃への耐性を高めることが対策となります。一般的な情報システムにおいては、入り口となるインターネット接続回線がボトルネックになりますが、それ以外にも考慮し対策すべき点があります。これらを順に紹介していきます。

・インターネット接続回線/内部ネットワークの広帯域化

根本的な対策にはならないものの、より広帯域なネットワークを用意することで、より広帯域の攻撃に耐えられるようになることが期待できます。インターネット接続回線においては、1Gbps や 10Gbps といった高速回線も以前と比

較して低価格で提供されるようになっているため、これらのサービスにアップグレードすることで耐性を高めることができます。

また、情報システム内のネットワークについても見直す必要があります。最近では 1Gbps 以上のインターフェイスを持つサーバやネットワーク機器が一般的ですが、数年前まではそれ未満の機器が多く存在していました。ネットワークを構成するケーブルについても 100Mbps までしか対応していないケースが見受けられます。インターネット接続回線を広帯域化したとしても、内部ネットワークが新たなボトルネックとなるケースがあるため、対策の一環として情報システム内部のネットワーク帯域も確認・増強することが求められます。

・ゲートウェイおよび ISP ルータでのフィルタリング

情報システムへの攻撃トラヒックの流入を防ぐ対策として、時刻同期先として参照している NTP サーバ以外からの NTP 通信をインターネット境界のゲートウェイで破棄することが挙げられます。具体的には UDP123 番ポート宛の通信をフィルタリングすることになりますが、設定によってはインターネット上の不特定な NTP サーバと通信できなくなる、外部に向けて NTP サービスを提供できなくなる、といった可能性があるため影響がないか確認することが必要です。

また、そもそもインターネット接続回線に大量の NTP トラヒックが流れないよう ISP へ依頼し、ISP ルータにおいてもフィルタリングを実施する方法も対策として有効です(Egress Filtering)。この手法は ISP のサービスポリシーやサービスメニューによって実施可否が異なりますが、事前に対策として実施しておくほか、実際に DDoS 攻撃を受けた場合の対処手法の一つになるため、予め ISP の担当者と会話をし、良好な関係性を築いておくことを推奨します。

・DDoS 軽減(Mitigation)サービスの導入

契約している ISP によっては DDoS 対策専用の機器を用いて、DDoS トラヒックを選別し軽減(mitigation)するサービスを提供している場合があります。これは、インターネット接続回線に入る前の、より広帯域な ISP のバックボーンで対処するため、インターネット接続回線以上の攻撃トラヒックに対しても対処できることが期待できます。このようなサービスは申込から実際のサービス開始までに時間を要する場合もあり、また平常時に学習した正常なトラヒックパターンに基づいて、DDoS トラヒックの選別を行うため、予めサービスを導入しておくことが必要です。

3.1.2. インターネット接続事業者(ISP)が顧客システムや設備を守るために可能な対応策

インターネット接続事業者には、電気通信事業法 4 条で定められた通信の秘密の保護の制約があり、対策はその範囲内に限られます。その基本的な考え方については「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン[10]」に整理されており、まずこれを参照することが必要です。

該当ガイドラインでは、NTP で利用される UDP123 番ポートに対する通信遮断の事例が紹介され、その妥当性について一定の解釈が与えられています。しかしながら、ガイドライン全体として個々の判断は実際の状況に応じて個別になされるべきものであり、「迷う場合には監督官庁である総務省に照会することが好ましい」とデリケートな対応を求めています。このため、実施の是非について個別調整、もしくは業界内でのコンセンサスをとっていくことが技術的な対策の前に必要となります。

3.2. 悪用を防ぐ対策 - 自社や顧客が加害者にならないために

3.2.1. ネットワーク内の状況把握

具体的な対策を講じる前に、まずは、管理するネットワークの状況の把握が必要となります。具体的な状況把握の手法としては、ネットワーク内における UDP 123 番ポートの稼動状況のスキャンや、Open NTP Project[11]の調査結果の活用などが挙げられます。このプロジェクトでは、指定したネットワーク内に存在する不適切な状態の NTP デーモンを確認できる無償のサービスを提供しています。

NTP デーモンは、ネットワーク機器などにおいて意図せずデフォルト設定で有効化されている場合もありますので、NTP サーバとして稼動させているホストに限らず、広くネットワーク全体にわたる状況把握が対策として有効です。

しかし、自社の管理するネットワーク内であったとしても、顧客のアドレス帯域に対してスキャンをかけることの妥当性・適法性はこのドキュメント編集時において明らかになっていません。スキャン対象については慎重に選定する必要があります。対象や手法の適法性について迷う場合には、都度総務省に照会するのがよいでしょう。

3.2.2. 企業の情報システム担当がとるべき対策

管理する機器やシステムが加害者とならないためには、NTP デーモンの設定や、Firewall などで制限をし、不特定の送信元からリクエストを受け付けなくする設定変更が対策となります。管理するネットワークの状況を確認し、悪用されてしまう可能性のあるサーバやネットワーク機器があれば、その製品仕様に従った対処が望まれます。

本対策の難しい点は、対象のバリエーションが多く、対策手法も多岐にわたることです。具体的な対策手法は各メーカより提供されていますが、なかには、サポートが終了した製品もあり、そもそもファームウェアの更新などの根本的な対策を行えないケースもあります。サポートが提供されている製品への更新が望まれますが、暫定策としてパケット

フィルタリングなどで NTP の通信先を制限する方法もあります。TEAM CYMRU による NTP に関する設定のテンプレート集 SECURE NTP TEMPLATE[12]には Cisco IOS, Juniper JUNOS, UNIX ntpd やフィルタについての考察があり参考になります。

また、VPS サービスやクラウドサービスを利用している場合には、運用しているサーバが踏み台の一つとなってしまう可能性が考えられます。基本的な対策は変わりませんが、事業者自身が状況を把握し、対策を推進しているケースがありますので、これに従って対処することが望ましいといえます。

3.2.3. インターネット接続事業者がとるべき対策

NTP Reflection DDoS をはじめとする、UDP パケットの送信元を詐称する攻撃は、送信元を詐称したパケットがネットワーク上に流れなければそもそも成立しません。そのため、送信元を詐称したパケットのフィルタリング(遮断)が対策になります。この取り組みは、様々な理由により望ましいと言われながらもこれまでなかなか普及してきませんでしたが、昨今の状況から送信元を詐称したパケットをインターネット上に流さないようにする必要性が増しており、世界的に対応を進めていく機運が高まっています。基本的な考え方については、インターネット標準を規定する IETF が策定している RFC2827 (BCP 38)[13]として公開されており、実際にどのように実施していくかは、パケットフィルタや、RFC 3704 [14]として公開されている uRPF(Unicast Reverse Path Forwarding)などの手法が有効です。JANOG においては、JANOG 18 および 31.5 の松崎氏の発表[15][16]が参考になります。

また、すでに自社のユーザがすでに踏み台となってしまっている場合にはこれを撲滅していく対応策も必要です。実際に一部の家庭用ブロードバンドルータが実際に NTP Reflection DDoS 攻撃の踏み台となり、外部に攻撃をしてしまったケースが国内でも相当数観測されています。一般的に、家庭用ブロードバンドルータはユーザの所有物であり、具体的な対策は多くの場合ユーザの手に委ねる形にならざるを得ません。このため、ISP においては、ユーザに対する啓発活動への取り組みが必要となってきています。

4. インシデント対応

3 章では NTP Reflection DDoS に対する具体的な対策手法を述べてきました。一方で、実際に DDoS 攻撃に直面した際には、先述の対策手法の実装以外にも数多くの対応が必要となります。本章ではこれをインシデント対応と位置づけ、必要となる対応をまとめます。具体的には、自社もしくは顧客のシステムが攻撃を受けた場合、自社もしくは顧客のシステムが攻撃に悪用されている場合に分けて、実施すべき対応を紹介します。

4.1. 自社もしくは顧客のシステムが攻撃を受けた場合

4.1.1. 事前準備

なにごとも準備していない対応はできません。3 章の内容をふまえ、問題発生時の対応を決め、予め備えておくことが必要です。なかでも、インターネット接続回線の帯域を上回るトラヒックが発生した場合は、ISP の協力なしには対処できません。このため予め ISP の担当者との関係性を構築しておくことが特に重要となります。

4.1.2. 検知と対応

検知はユーザの申告による場合もありますが、迅速に対応するためには、トラヒックモニタリングやサービス監視などにより検知する方が望ましいといえます。

検知した攻撃トラヒックがインターネット接続回線の帯域内に収まる場合は、システムの担当者で一定の対応が可能です。たとえば、接続元が限定的である場合には、攻撃トラヒックの発生元に連絡を取り、対処を要請することも有効な対応手法の一つとなります。具体的な連絡先については WHOIS 情報を参照することが一般的です。

しかしながら、インターネット接続回線の帯域を上回るトラヒックに対しては、ISP 側で対応してもらうほかありません。ISP 担当者と連携し、3 章で述べた ISP でのフィルタリングや、DDoS 軽減(mitigation)といった対策を粛々と進めていきます。

4.2. 自社または顧客システムが攻撃に悪用されている場合

4.2.1. 事前準備

状況把握のために、トラヒックの可視化や検知システムの導入が前提となります。また、実際の攻撃に悪用されてしまった場合には、WHOIS 情報の技術管理者情報を元にして連絡が行われるケースが多いため、予め WHOIS 情報を適切に更新しておく必要があります。

4.2.2. 検知と対応

自らモニタリングにより検知するほか、外部からの申告によって認知するケースが一般的です。外部からの申告の場合は、管轄のシステムに問題があり余所に迷惑を掛けていることになりますので、申告内容を真摯に受け止め、申告内容を元に対象機器を割り出して「適切な状態であるか？」を改めて確認する対応策が必要です。

今回のような UDP パケットの送信元詐称を用いた手法の場合、「詐称元」となっていて「実際は自分が被害者」となるケースも考えられますが、まずは「自分が攻撃元になっていないか」の確認が重要となってきます。その上で対象が自社システムである場合には自ら対策を、顧客システムであった場合には顧客とメール・電話等で連絡をとり、対応してもらうよう伝えます。この際、必要であれば顧客からの相談にのる位の気構えと体制が必要になります。

さらに、申告者に対する対応も必要となります。基本的に「申告者も人」ですから「申告に対して返事すら無い」と受け取られる場合、全体的なマイナスイメージとなりますので極力避けることが必要です。初回は「申告内容を元に該当機器の状態を確認します」の一報だけでも十分です。くわえて、問題点が判明し問題解決に向かっての対応状況「申告のあった該当機器」によってはファームウェア対応待ちの可能性も有りますので申告から 1 週間を目処に対応状況報告をすると申告を行った側や被害に遭われた方は多少安心するかと考えられます。最後に対応完了報告(予定含む)にて「対応完了」または「対応完了予定時期」に関しても報告を行ったほうが良いと考えられます。

5. まとめ

NTP Reflection DDoS Attack は、古くから知られる DDoS 攻撃の一種であるためか、まだまだ一般の認知度や危機感は低い状況です。一方、実際にトラヒックを観測した人や、調査や検証を通じて実態を把握した人は、その重大性を認識し、対策を始めています。NTP は、本ドキュメントで述べてきた DDoS 攻撃に悪用される主要なプロトコルの一つとして猛威を振るっています。

攻撃手法はその有効性が広く認知されることでさらに流行します。本手法の容易性や効率性を鑑みると、今後さらに流行していく危険性があり、DDoS 対策の必要性はますます高まっていくと考えられます。

本ドキュメント記載の内容が、各組織、ひいてはインターネット全体で対策を進める上での参考となれば幸いです。

6. 謝辞

本ドキュメントの執筆にあたりご協力くださった JANOG NTP 情報共有 WG のみなさま、活動について有用なコメントをいただいた多くの JANOG メンバのみなさまにこの場を借りて感謝の意を表します。本当にありがとうございました。

7. 参考文献・URL

[1] CloudFlare, “Technical Details Behind a 400Gbps NTP Amplification DDoS Attack,” 2013. [Online]. Available: http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack.

[2] CloudFlare, “The DDoS That Almost Broke the Internet,” 2014. [Online]. Available: http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet.

[3] CloudFlare, “The DDoS That Knocked Spamhaus Offline (And How We Mitigated It),” [Online]. Available: http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho.

[4] S. Khandelwal, “100Gbps DDoS attack took down Gaming servers with NTP Servers,” 2014. [Online]. Available: http://thehackernews.com/2014/01/ddos-attack-NTP-server-reflection-protection.html.

[5] Incapsula, “Report: 2014 DDoS Trends - Botnet Activity is up by 240%.,” 2014. [Online]. Available: http://www.incapsula.com/blog/ddos-threat-landscape-report-2014.html.

[6] JPCERT コーディネーションセンター, “ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起,” 2014. [Online]. Available: https://www.jpcert.or.jp/at/2014/at140001.txt.

[7] Symantec, “Emerging Threat - Anonymous - Operation Petrol,” 2014. [Online]. Available: http://www.symantec.com/connect/blogs/emerging-threat-anonymous-operation-petrol-june-20-2014.

[8] “DDoS 攻撃で停止の「ファンタシースターオンライン 2」、再開できず 「攻撃規模、極めて大きい」,” 2014. [Online]. Available: http://www.itmedia.co.jp/news/articles/1406/23/news078.html.

[9] US-CERT, “Alert (TA14-017A) UDP-based Amplification Attacks,” 2013. [Online]. Available: http://www.us-cert.gov/ncas/alerts/TA14-017A.

[10] 一般社団法人日本インターネットプロバイダー協会ほか, “電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン,” 2014. [Online]. Available: http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf.

[11] Open NTP Project, “OpenNTPProject.org - NTP Scanning Project,” [Online]. Available: http://openntpproject.org/.

[12] TEAM CYMRU, “SECURE NTP TEMPLATE,” [オンライン]. Available: http://www.team-cymru.org/secure-ntp-template.html.

[13] D. S. P. Ferguson, “BCP38 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” 2000. [Online]. Available: https://tools.ietf.org/html/bcp38.

[14] P. S. F. Baker, “Ingress Filtering for Multihomed Networks,” 2004. [Online]. Available: https://tools.ietf.org/html/bcp84.

[15] M. Yoshinobu, “DNS amplification attacks,” 14 7 2006. [Online]. Available: http://www.janog.gr.jp/meeting/janog18/files/DNSamp_Maz.pdf.

[16] M. Yoshinobu, “BCP38,” 19 04 2013. [Online]. Available: http://www.janog.gr.jp/meeting/janog31.5/doc/janog31.5_dns-open-resolver-maz.pdf.