

## DNS サーバの現状調査

### 1 はじめに

DNS(Domain Name System)は、コンピュータのホスト名と IP アドレスを対応付けるサービスであり、インターネットの基幹システムの一つである。DNS サーバのうち、外部から再帰的な問い合わせが可能なのは様々な攻撃に悪用される可能性がある。(図1)

警察庁サイバーフォースセンターでは、この問題について分析レポート「DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について」(「6 参考文献」の[1]を参照)を 2006 年に公開し、注意喚起を行ってきたところである。今回、DNS サーバの現状を調査するため、本年 4 月から 5 月にかけて日本国内の主要なサイトを対象として各種調査を実施した。

調査の結果、外部から再帰的な問い合わせに応じる DNS サーバは、全体の約半数にあたる 49%であった。また、DNS サーバソフトウェアのバージョン情報調査によると、脆弱性のあるバージョンを使用していると疑われる DNS サーバが存在した。

その他、2008 年 7 月には、複数の DNS サーバソフトウェアにキャッシュポイズニングが成立する脆弱性が公表されている(「6 参考文献」の[2]、[3]を参照)。

これらの DNS サーバは、キャッシュポイズニング攻撃や DDoS 攻撃の踏み台として悪用される可能性が懸念されるため、早急な対策が求められる。

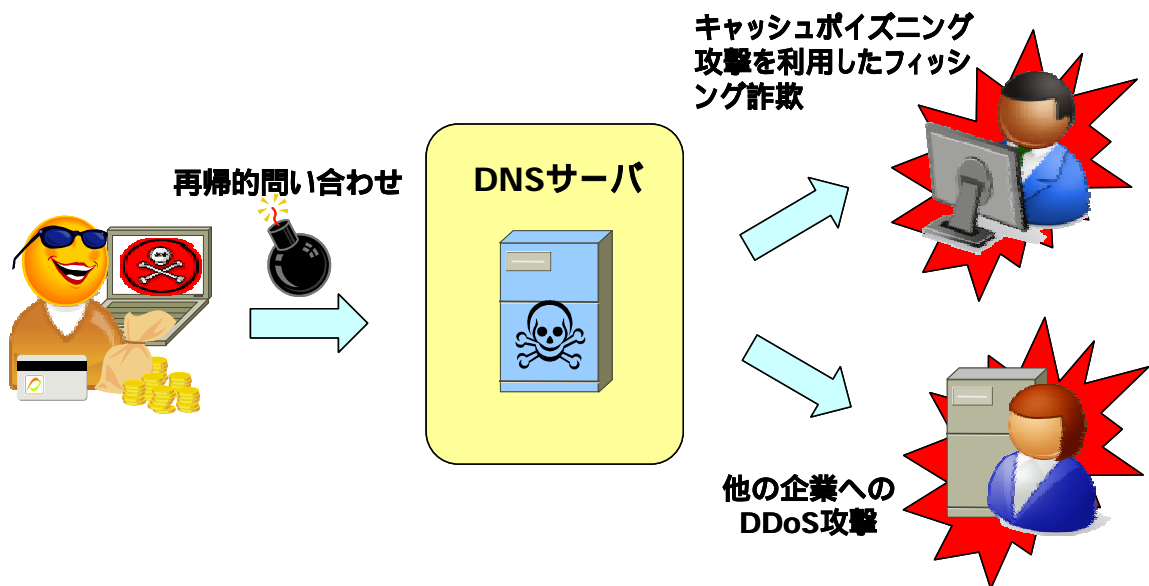


図1 DNS の再帰的な問い合わせを悪用した攻撃の例

## 2 再帰的な問い合わせの悪用

DNS サーバの機能である再帰的な問い合わせとは、利用者からの名前解決要求を受けた DNS サーバが、要求された情報を持っていない場合、他の DNS サーバに対して問い合わせを行い、得られた結果を利用者のコンピュータに回答する機能である。DNS サーバは、他の DNS サーバから得た情報を一定期間キャッシュし、同様の問い合わせに対して、このキャッシュ情報を使用する。

### (1) DNS キャッシュポイズニング攻撃

DNS キャッシュポイズニング攻撃とは、DNS サーバの脆弱性等を悪用し、偽の情報を DNS サーバへキャッシュさせる攻撃である。攻撃が成功した場合、DNS サーバの利用者を攻撃者の意図するサイトへ誘導することができる。

DNS サーバが外部に対して再帰的な問い合わせを許可している場合、攻撃者はキャッシュポイズニング攻撃の成功・失敗を容易に確認できるため、キャッシュポイズニング攻撃を受ける可能性が高まることが懸念される。

### (2) DDoS 攻撃の踏み台

再帰的な問い合わせを悪用した DDoS 攻撃の概要を図 2 に示す。攻撃者は最初に、用意した DNS サーバから、巨大なデータを再帰的問い合わせ可能な DNS サーバにキャッシュさせる(図 2 の ①)。攻撃者は、発信元を攻撃対象に詐称した問い合わせを DNS サーバに送信することにより(図 2 の ②)、DNS サーバから攻撃対象に対してキャッシュした巨大なデータが送信される(図 2 の ③)。これを大量に行うことにより、DDoS 攻撃を行うことができる(図 2 の ④)。

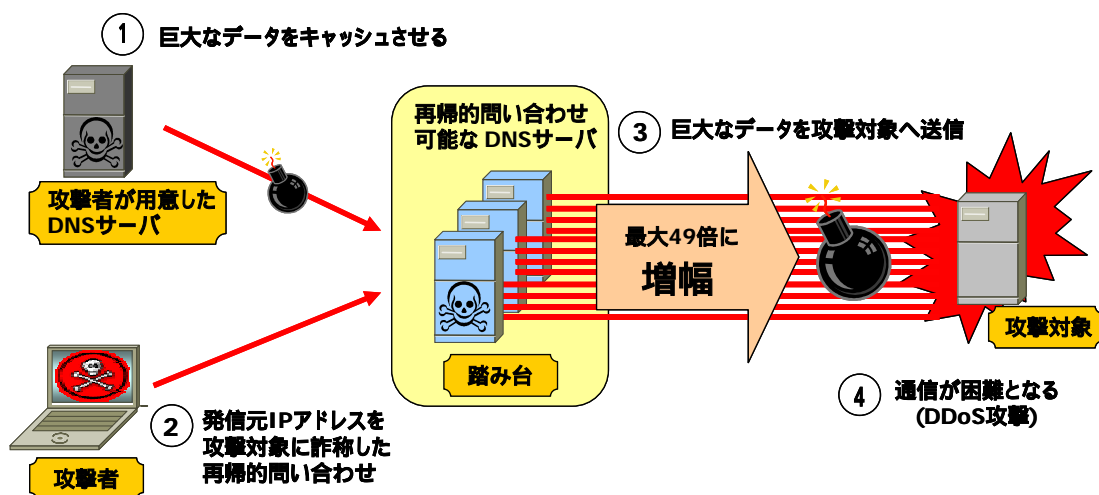


図 2 DNS サーバに対する再帰的な問い合わせを悪用した DDoS 攻撃

### 3 DNS サーバの調査

重要インフラ事業者等のサイトの DNS サーバについて、以下のとおり調査を実施した。

表 1 DNS サーバの調査条件

調査対象	: 重要インフラ事業者等のサイトの DNS サーバ
サーバ数	: 2,022
調査期間	: 2008 年 4 月 1 日から 2008 年 5 月 31 日

#### (1) 再帰的な問い合わせに関する調査

外部からの再帰的な問い合わせに応じる DNS サーバは、調査対象の 49%を占めた。(図 3)

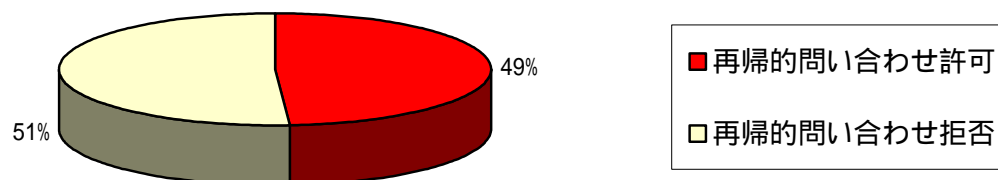


図 3 外部から再帰的な問い合わせが可能な DNS サーバの割合

## (2) サーバソフトウェアとバージョン情報調査

DNS サーバには、使用しているソフトウェアのバージョン情報を外部から取得できるものがある。特に DNS サーバソフトウェアとして広く利用されている BIND は、初期設定でバージョン情報を取得可能である。

BIND8 又は BIND9 と回答するサーバは全体の 29%（BIND9 が 23%、BIND8 が 6%）、その他の文字列を回答するサーバは 45%であった。バージョン情報の問い合わせに対して回答しないサーバは 26%であった。（図 4）

ただし、BIND はバージョン情報の問い合わせに対して、その他の文字列を回答又は回答しない設定にすることが可能である。

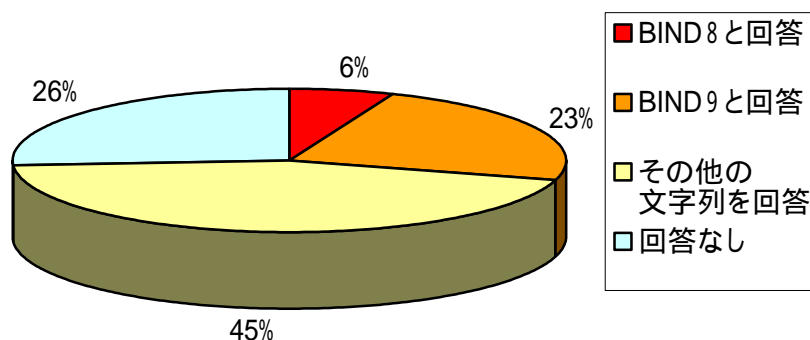


図 4 BIND のバージョン情報問い合わせに対する回答結果

## (3) DNS の TTL の設定状況

DNS の TTL(Time To Live)とは、DNS のキャッシュサーバ等がキャッシュした情報を保持する期間について参考にする設定値のことである。TTL が短い設定値のサイトが攻撃対象となった場合、キャッシュポイズニング攻撃が成功する危険性が増大するため、注意が必要である（「6 参考文献」の[3]を参照）。DNS サーバの TTL 値について調査したところ、以下のとおりであった（図 5）。

TTL 値が 1 日に設定されているサーバが最も多く 44%を占めた。1 日より長く設定されているサーバが 3%ある一方で、10 分未満の短い TTL 値のサーバが全体の 8%存在した。

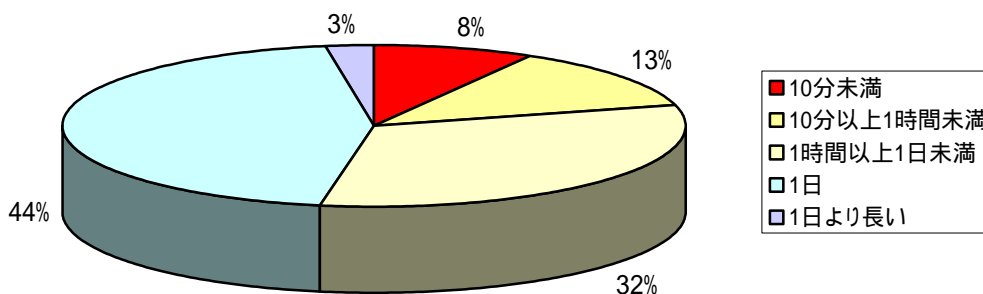


図 5 TTL 値の調査結果

#### (4) サーバソフトウェアのバージョンと外部からの再帰的問い合わせ状況

サーバソフトウェアのバージョン情報と外部からの再帰的問い合わせに対する応答状況について分類した結果を図6に示す。

外部からの再帰的問い合わせを許可するものはBIND8と回答したものが80%、BIND9と回答したものが68%と非常に多い。これは、BINDの初期設定が外部からの再帰的問い合わせを許可していたことが原因である可能性が高い。

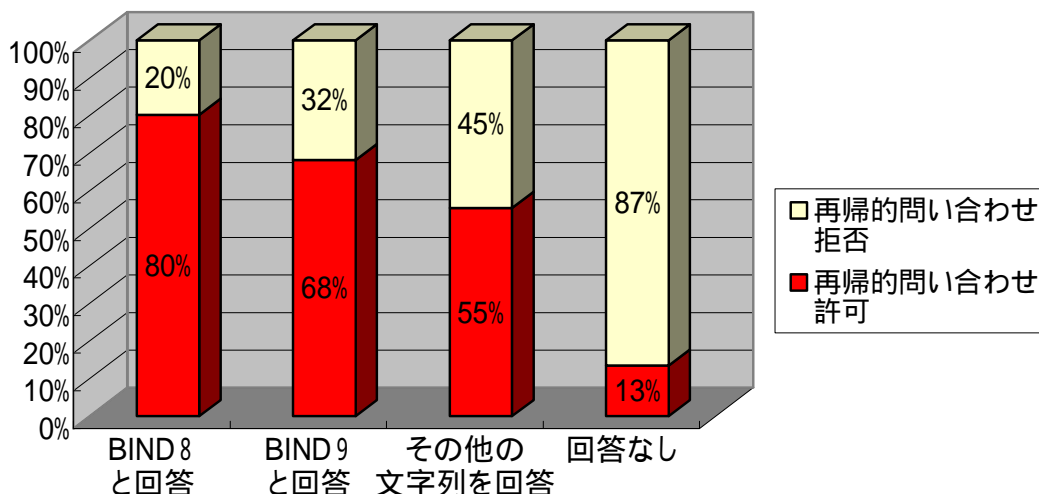


図6 バージョン情報毎の再帰的問い合わせ可否の割合

## 4 対策

DNSサーバの設定等について、以下の対策をとることを推奨する。

### (1) 再帰的問い合わせに関する設定

キャッシュサーバとして使用しているDNSサーバでは、信頼できる利用者以外からの再帰的問い合わせを受け付けないようにする。

### (2) バージョン情報の回答に関する設定

外部からの問い合わせに対して、脆弱性のあるソフトウェアのバージョン情報を回答した場合、悪意のある第三者の攻撃対象になる可能性がある。このため、バージョン情報をその他の文字列で回答するか、回答を返さないようにするのが望ましい。

### (3) TTLに関する設定

TTLが適切な設定値になっていることを再確認する。

### (4) サーバソフトウェアの更新

サーバソフトウェアを利用するアプリケーションへの影響を考慮した上で、脆弱性のないバージョンに更新する。

## 5 まとめ

今回の調査で、国内主要サイトの多数の DNS サーバが、外部からの再帰的な問い合わせを許可していることを確認することができた。これらの DNS サーバは、DDoS 攻撃の踏み台として悪用されたり、キャッシュポイズニング攻撃の被害に遭う可能性が高いと考えられる。

サーバソフトウェアと DNS の再帰的な問い合わせの関係によると、BIND を使用しているとみられる DNS サーバの多くは、外部からの再帰的な問い合わせを許可しているものが多かった。古いバージョンの BIND は、初期設定で外部からの再帰的な問い合わせを許可するため、DNS サーバを構築・運用する際は注意する必要がある。

DNS はインターネットにおいて基盤となる重要なサービスであり、被害を未然に防止するためにも、DNS サーバの適切な運用に向け、セキュリティ対策の確認をお願いしたい。

警察庁サイバーフォースセンターでは今後とも情報セキュリティ対策に資する情報があれば、警察庁セキュリティポータルサイト@police を通じて、情報の提供を行なう予定である。

## 6 参考文献

[1] @police

DNS の再帰的な問い合わせを悪用したDDoS 攻撃手法の検証について

[http://www.cyberpolice.go.jp/server/rd\\_env/pdf/20060711\\_DNS-DDoS.pdf](http://www.cyberpolice.go.jp/server/rd_env/pdf/20060711_DNS-DDoS.pdf)

[2] Multiple DNS implementations vulnerable to cache poisoning

<http://www.us-cert.gov/cas/techalerts/TA08-190B.html>

[3] 複数のDNSソフトウェアにおけるキャッシュポイズニングの脆弱性について

<http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning.html>