共用 DNS 権威サーバの脆弱性

鈴木 常彦[1,a)]

概要：多数の利用者が共用する DNS 権威サーバでは共用であるがゆえの多くの脆弱性が発生しうる。本論文では共用 DNS 権威サーバにおける多様な危険性のある状況 (キャッシュ兼用、親子同居、lame delegation、public suffix ゾーン、放棄された CNAME、sibling domain) に分けて章立てし、それぞれにおける脆弱性 (DDoS, キャッシュポイズニング, ゾーンの乗っ取りなど) について解説、考察し、注意喚起する。

キーワード：DNS，権威サーバ, 共用, 脆弱性, 乗っ取り, ハイジャック, lame delegation

Abstract: Shared DNS authoritative servers used by many users may cause various vulnerabilities by being shared. This paper shows, consider, and alert about each vulnerability - DDoS, cache poisoning, zone hijack - with several risky situations - cache combined, mixed parent/child, lame delegation, public suffix zone, orphaned cname, sibling domain - in each chapter.

Keywords: DNS, shared, authoritative, vulnerability, takeover, hijack, lame delegation

1. はじめに

DNS の権威サーバ (コンテンツサーバ、ゾーンサーバ等とも呼ばれる) を多くの利用者に提供し、多くのゾーンを同居させているサービスは多い。本論文ではそういったサーバを共用 DNS 権威サーバ[*1]と呼ぶ。

本論文で示すように、共用 DNS 権威サーバには多くの利用者が自由に設定したゾーンが同居するがゆえの脆弱性がいくつも存在する。これらは大手の商用サービスにも存在しているが、運営者たち自身の危険性の認識が不十分であったり、コストや利便性と対策の兼ね合いが難しいこともあって、多くの問題の解決がなかなか進まない。未解決なサービスが多いこともあってか、公的な機関からの注意喚起も不十分であり、DNS の利用者たちは長年危険な状態に晒されている。

本論文は共用 DNS 権威サーバの脆弱性 (危険性) の解決が進まない現状を踏まえて、これらを網羅的に解説することで広く注意喚起となることを目的としている。 本章に続き 2. キャッシュ兼用、3. 親子同居、4.lame delegation、5.public suffix ゾーン、6. 放棄された CNAME、7. 共用メールサーバ、8. 兄弟委譲という構成で、危険性を生む状況毎に整理している。なお 7. 共用メールサーバの問題は共用 DNS 権威サーバとセットになっているサービスの問題ではあるが、直接は DNS と関係していない。しかし関係していないがゆえに発生している問題としてあえて取り上げている。

また本論文でとりあげた脆弱性の解決はサービス形態と結びついたビジネス的な問題 (利便性、料金、コスト、信用、コンプライアンスなど) と併せて事業者が考えるべき問題であり、論文として立ち入るのは適切ではないという筆者の考えから、十分な解決方法の提案は行わない。本論文では主としてドメイン名の権利確認の重要性を示すことに止める。 サービスの利用者の立場では問題を理解し、危険な共用サービスの利用を回避することが対策となる。

なお、本論文では、ドメイン名について権利がない他人 (攻撃者) が作成したゾーンへ問い合わせが到達し、応答を返すことができる状態を意図的に作り出すことを乗っ取りあるいはハイジャックと呼んでいる。

2. キャッシュ兼用

権威サーバとキャッシュサーバ (以降 2 種のサーバと呼ぶ) の兼用は多様な害を生み出す。筆者のウェブサイト「キャッシュサーバを権威サーバと兼用すると危ない」[1] に列挙してあるが、主たる問題は以下のようなものである。

(1) キャッシュポイズニング攻撃を受けやすい

[1] 中京大学
Chukyo University, Toyota, Aichi, 470-9393, Japan
[a)] tss@suzuki.sist.chukyo-u.ac.jp

[*1] DNS 権威サーバ：RFC1034 では authoritative name server

(2) DDoS の踏み台になりやすい
(3) NS の移転が困難となる

3 は解説が必要と思われるが本論文の主題ではないので省略する。参考文献に挙げた事例 [2] を参照されたい。これらに加えて本章ではキャッシュ兼用サーバが多くの利用者に共用されている場合の危険性を取り上げて後述（2.2 節) する。

2.1 兼用の歴史

これら多くの問題を抱えながらも DNS の運用の世界においては長らく慣習的に 2 種のサーバの兼用が行われてきた。これは RFC1034[3]、RFC1035[4] がこの 2 種のサーバを明確に分けて説明していなかったこと、長らく独占的なシェアを持っていた実装である BIND がこの 2 種のサーバを兼用できたこと、巷の多くの設定例が兼用を当然のものとして扱っていたこと、そして兼用の害がほとんど認識されていなかったことによると思われる。

また兼用の害が認識されていなければ、あえてサーバを複数台に分けるコストをかける動機もなかったであろう。実際には兼用は運用の困難さが増すことで人的コストを押し上げることになると考えられるのだが。

2001 年には 2 種のサーバを別インスタンスで扱う djbdns1.05 がリリースされたが、BIND ユーザの認識の変化や乗り換えはあまり大きく起きず、権威とキャッシュの分離はあまり進まなかった。

国内では 2003 年のインターネットウィークで株式会社日本レジストリサービス (JPRS) の民田が「サーバーの安全な設定」[5] と題してキャッシュポイズニング対策の観点から分離を訴えたがやはり分離は進まなかった。

2006 年には兼用が一つの大きな要因と思われるオープンリゾルバ (アクセス制限がないキャッシュサーバ) を踏み台とした DDoS が増加していることを受けて、JPRS から「再帰的な問合せを使った DDoS 攻撃の対策について」[6]、JPCERT/CC から「DNS の再帰的な問合せを使った DDoS 攻撃に関する注意喚起」[7] が出されたがやはり分離は進まなかった。

2007 年 5 月の筆者によるサンプリング調査 [11] では 24,214 台の権威サーバ中、83%にあたる 20,001 台がキャッシュ兼用であった。また、1 年後の 2008 年 4 月のサンプリング調査 [12] でも兼用サーバは 77%存在しており、改善はなかなか進んでいなかった。

分離が積極的に進むようになったのは 2008 年の夏頃からだろう。 Mueller[8] や Kaminsky[9] のキャッシュポイズニング手法が公開され、オープンリゾルバの危険性の認識が広まり、JPRS などによりその対策の一部として 2 種のサーバの分離が推奨された [10] ことが大きなきっかけになったと思われる。また NSD と Unbound など、2 種のサーバを分離した実装の普及も大きい。

現在は兼用のサーバを見かけることは少なくなってきたが、2012 年には非常に危険な兼用サーバが商用サービスに見つかっており、次節で解説する。

2.2 共用のキャッシュ兼用サーバ

共用の権威サーバ上に利用者の誰もが任意のドメイン名のゾーンを作れてしまうサービスが世の中に数多く存在している。本論文はその危険性を様々なケースで考察するものであるが、まずはそのサービスが共用のキャッシュサーバを同時に提供しているケースを取り上げる。

BIND のようにキャッシュと権威が同じ IP アドレスとポート番号 (53) でサービスが提供されている場合、キャッシュサーバ利用者からの問い合わせに権威サーバ上に作られた任意のゾーンが応答を返してしまう。また権威サーバへの問い合わせにキャッシュが混入するという問題もある。

権威サーバに上位ゾーンからの委譲の有無を確認して応答する仕組みはないし、キャッシュサーバへの再帰問い合わせ要求 (RD フラグ=1) であっても権威ゾーンが応答してしまう運用が大半である。また、キャッシュと権威のインスタンスや IP アドレスを分離していても、管理ゾーンをキャッシュサーバから権威サーバにフォワーディングしていれば同じ話になる。

こうしたサービスでは、誰もが ”GOOGLE.COM” ゾーンなどを作成しキャッシュサーバの利用者へ応答させることが可能である。実際 2012 年にそのようなサービスを行っていた事業者を筆者が発見し、JPRS が「権威／キャッシュ DNS サーバーの兼用による DNS ポイズニングの危険性について」と題した注意喚起 [14] を行う事態となった。

対策としては権威とキャッシュを完全に分離することや、ゾーン作成、維持においてドメイン名の権利確認をすることが求められる。なお 2 種のサーバの分離ができない事情がある場合に対して、東は BIND において view を用いて権威への問い合わせとキャッシュへの問い合わせを分離する方法 [15] を提案している。

3. 親子同居

キャッシュと権威が分離されても共用の権威サーバに任意のゾーンが作成されることによる問題は大きい。まずは親子同居問題を解説する。なお親子同居はキャッシュポイズニングが容易となる問題 [16][17] を引き起こすが、本論文は共用サーバの問題に特化し、それらはスコープ外として解説しない。

3.1 子ゾーンの乗っ取り

正当に作成されたあるドメイン名のゾーンに対して、同じサーバ上でその子孫のゾーンが正当性なく作成されると問題が発生する。

example.jp が jp から委譲され、あるサーバ上に正

当なゾーンが存在していたとする。そのサーバ上に sub.example.jp ゾーンが作成されると、sub.example.jp は example.jp から委譲を受けなくとも example.jp ゾーン宛のはずの問い合わせに答えてしまう状態となって世界から検索可能となり 、example.jp のサブドメインとして自由に振る舞うことができてしまう。

ここで例えば example.jp ゾーンに www.example.jp の A レコードが存在していたとしよう。そこへ他人 (攻撃者) が無断で www.example.jp ゾーンを同じサーバ上に作成し、ゾーン頂点の www.example.jp に A レコードを設定すると、メジャーな実装の多くは www.example.jp ゾーンのレコードを優先して応答するためドメイン名の乗っ取りが成立する。

下記の設定においては www.example.jp IN A 192.0.2.2 が応答される。 (djbdns の tinydns は両方を応答する)

```
jp ゾーンからの委譲
  example.jp. IN NS ns.example.ad.jp.

example.jp ゾーン
  example.jp. IN NS ns.example.ad.jp.
  www.example.jp. IN A 192.0.2.1

www.example.jp ゾーン
  www.example.jp. IN NS ns.example.ad.jp.
  www.example.jp. IN A 192.0.2.2
```

なお、攻撃者はメジャーな共用サーバにおいて、www.example.jp ゾーンを先んじて登録しておき、jp から example.jp への委譲が向くのを待ち伏せすることも考えられる。

サブドメインの乗っ取りは偽サイトの設置のほか、メールの盗聴や WWW の cookie の悪用につながる。筆者はサブドメインへの DNS 毒入れ疑似体験サイトを用意しているので参照されたい。[18]

このいわゆる親子同居問題は 2012 年に前野 [19] が発見し、徳丸 [20] や筆者 [21] が解説したほか、問題を指摘されたさくらインターネットが「当社 DNS に関するお知らせ」[22] と題して問題と対策の解説を公開している。また JPRS が「サービス運用上の問題に起因するドメイン名ハイジャックの危険性について」[23] と題した注意喚起を行っている。

こうした問題を発生させないためには、共用の権威サーバにおいてはゾーンの作成時のみならず、継続的にそのドメイン名について権利確認を行う必要があるが、権利確認には事業者と利用者双方の手間がかかるうえ、システム開発や運用コストもかかるためか、対策を行っている事業者はなかなか見当たらない。なお、さくらインターネットは作成できるゾーンの条件に制約を課すという対策を行っており上記お知らせ [22] で以下のように説明している。

> ・当社会員 ID に紐づいて管理されているドメインの場合、その所有者以外はネームサーバへ登録できない
> ・登録しようとしているドメインの親ドメインが、別の会員 ID のお客様によって登録されている場合は、登録が出来ない
> ・登録しようとしているドメインの子ドメインが、別の会員 ID のお客様によって登録されている場合は、登録が出来ない
> ・登録しようとしているドメインの親ドメインが当社ネームサーバに委譲されている場合には登録出来ない
> ・登録しようとしているドメインが当社ネームサーバと他のネームサーバの両方に委譲されている場合には登録出来ない (いわゆるセカンダリ設定がされている場合)

しかしこれでは利用者の多様なニーズからは不便も生ずるため権利確認が必要なケースも発生するが、その対応は人間が間に入る形になることが説明されている。また後述の lame delegation への対策の観点からはこれでは不十分であるがここではコメントしない。

他の対策もある。多くのサーバリソースが必要であるが親子ゾーンの同居を許さないポリシーで解決を図ることもできる。AWS の Route53 においては、多数のサーバに利用者のゾーンを分散させ、親子ゾーンを同じサーバに収容しない対策を行っている。 しかし、これもまた後述の lame delegation への対策としては不十分であり、権利確認が必要である。

また、この問題を実装の側から対策しようという提案もある。委譲を受けていないゾーンあるいはリゾルバの意図していないゾーンが問い合わせに応答してしまうことが問題なのだから、リゾルバが委譲を辿って今どのゾーンに問い合わせをしているのかを権威サーバに伝えようという案である。森下による提案「委任にまつわるエトセトラ」[24] の他、東による実装例 [25] もあるが広く採用される動きはみられない。

3.2 親ゾーンの乗っ取り

www.example.jp というドメイン名を公開したい場合、www.example.jp のレコードを持つ example.jp ゾーンを作成し jp から委譲を受けるのが正しい。ところが如何なる理解によるものか、www.example.jp ゾーンのみを作成して example.jp への委譲を受けている例が多く見つかる。これでも www.example.jp ゾーンは機能してそのゾーン頂点の www.example.jp の A レコードを検索することができてしまう。

jp ゾーンからの委譲
```
example.jp. IN NS ns.example.ad.jp.
```

www.example.jp ゾーン
```
www.example.jp. IN NS ns.example.ad.jp.
www.example.jp. IN A 192.0.2.1
```

この状態で example.jp ゾーンを他人 (攻撃者) に作られると www.example.jp 以外の example.jp 以下のドメイン名を乗っ取られてしまう。

また、この状況で第三者の作成を制限しなくてはいけないのは親ゾーンだけではない。兄弟ゾーンの作成の制限も必要なことに注意が必要である。子ドメインの乗っ取り同様の対策が、親兄弟ゾーンすべてについて必要なのである。

www ゾーンだけを作るような誤りを避けるため、事業者のゾーン作成の手引きにおいて作成すべきゾーンの名前について誤解を与えない工夫も求められる。

3.3 CNAME 先の同居

以下の実在する応答例は実に奇妙である。

```
% dnsq a c.uecac.jp ns.uecac.jp
1 c.uecac.jp:
(snip), authoritative, nxdomain
query: 1 c.uecac.jp
answer: c.uecac.jp 3600 CNAME www.ipsj.or.jp
authority: ipsj.or.jp 600 SOA ns.ipsj.or.jp (snip)
```

Answer があるのに NXDOMAIN(RCODE3) となっている。しかしこれは DNS 権威サーバの応答としては RFC2308[26] あるいは RFC8020[27] に従った結果生じた規約上正しい応答である。

このからくりは uecac.jp ゾーンのある ns.uecac.jp に偽の ipsj.or.jp ゾーンが同居していることによる。ns.uecac.jp の応答はこの偽ゾーンを参照していて、そこには www.ipsj.or.jp はないため NXDOMAIN となる。

RFC2308 は CNAME の指すゾーンが同じサーバにあればそれを応答に使うことを 2.1 Name Error の全ての例で示しているうえに、QNAME が以下のように定義されている。これらに従えば上述の NXDOMAIN は正しいことになる。

> ”QNAME” - the name in the query section of an answer, or where this resolves to a CNAME, or CNAME chain, the data field of the last CNAME.

しかしこれに対しては Bortzmeyer による Errata [28] が発行されて異議が唱えられた。

> It should say: ”QNAME” - the name in the query section (RFC 1034, section 3.7.1).

かくして、RFC8020 により QNAME は以下のように再定義された。

> ”QNAME”: defined in [RFC1034] and in [RFC1035], Section 4.1.2, but, because [RFC2308] provides a different definition, we repeat the original one here: the QNAME is the domain name in the question section.

しかし、すでに多くの実装が RFC2308 に従って NXDOMAIN を返すようになっている現実に逆らえなかったのか、Section 1.1 Terminology に ” denied domain”という概念が導入され、2.1 Rule に以下の記述が入れられた。

> Warning: if there is a chain of CNAME (or DNAME), the name that does not exist is the last of the chain ([RFC6604]) and not the QNAME. The NXDOMAIN stored in the cache is for the denied name, not always for the QNAME.

従って今なお本節で示した奇妙な例は正規の応答なのである。しかし筆者は例のような偽ゾーンの NXDOMAIN がキャッシュサーバにおいて有効になってしまうと DoS が成立し危険であることに気づき実装を調査した。

BIND、Unbound、PowerDNS Recursor、Knot-resolver、dnscache はこの NXDOMAIN を無視し、CNAME の先は RFC2181[29] の以下の要請に基づいて検索し直すので安全であることを確認した。 またこれらの実装は NXDOMAIN でなく NOERROR で偽の A レコードが返されても当然ながら同様に無視し再検索を行う。

> However when the name sought is an alias (see section 10.1.1) only the record describing that alias is necessarily authoritative. Clients should assume that other records may have come from the server’s cache. Where authoritative answers are required, the client should query again, using the canonical name associated with the alias.

もし、適切に実装されていないキャッシュサーバが存在すると危険であるし、再問い合わせすることになっている権威のないデータを応答に入れるのは無駄であるので、RFC2308 と RFC8020 そして権威サーバ実装はこの奇妙な仕様を改めるべきである。

4. Lame Delegation

Lame delegation とは委譲先のネームサーバがそのゾーンについて権威ある応答を返さない状態を指す (正確には RFC1912[30]、RFC8499[31] 参照) が、本論文では権威サーバが返す NS に含まれるサーバが権威ある応答を返さない場合も同様のリスクがあるものとして扱う。

下記の設定がなされている場合において、ns.example.com

が権威ある応答を返さないものが lame delegation であるが、ns.example.net が権威ある応答を返さないのも同等のリスクがある。(権威からの NS をキャッシュに入れない実装であればこの限りではない)

jp ゾーンからの委譲
```
example.jp. IN NS ns.example.jp.
example.jp. IN NS ns.example.com.
```

example.jp ゾーン
```
example.jp. IN NS ns.example.jp.
example.jp. IN NS ns.example.net.
```

ここで ns.example.com や ns.example.net に example.jp ゾーンがない状態で、example.jp を扱う権利がない他人 (攻撃者) がそれらのサーバに example.jp ゾーンを作ることができてしまうと 1/2 あるいは 1/3 の確率で (キャッシュの実装・状態による) 乗っ取りが成立する。

lame delegation の乗っ取りリスクを抱えたドメインは海外では floating domain と呼ばれており、しばしばバグハンターたちのターゲットにもなっているが日本国内では注意喚起や表立った乗っ取り事例はみられない。

乗っ取りが発生しうる状況には下記のようにいくつかのパターンが存在する。

4.1 全ての NS が lame delegation

この状態ではそのドメイン名は機能していない。 使用が放棄された状態であるが、これを乗っ取ることによって spam をばらまいたり、古い WWW のリンクを乗っ取ることなどが行われる。

4.2 一部の NS が lame delegation

これはネームサーバの移転時、あるいは移転後の不始末によって発生する状態である。一部の NS が機能していれば名前解決はできてしまう場合が多く、不具合は見過ごされがちである。

この状態で一部の NS を乗っ取ると、確率的に悪意ある応答が返せてしまう。そして以下のような設定で悪意ある NS だけをキャッシュさせてしまえば 2 度め以降の問い合わせをすべて乗っ取ることができてしまう。(RFC2181 に従って委譲の NS を権威からの応答で上書きする実装が多い)

本物の example.jp ゾーン
```
example.jp. IN NS ns.example.jp.
example.jp. IN NS ns.example.net.
```
偽の example.jp ゾーン
```
example.jp. IN NS ns.example.net.
```

4.3 キャッシュによる一時的な lame delegation

一般的には lame delegation は恒常的な設定不良を指すが、セキュリティの観点からはごく一時的な lame 状態も危険である。これを指摘している例はみつからず、本論文をもって初めての注意喚起となるだろう。

以下のように ns.example.net から ns.example.com に委譲先を変更したとする。

当初の jp から example.jp への委譲
```
example.jp. 86400 IN NS ns.example.net.
```
当初の example.jp ゾーン
```
example.jp. 600 IN NS ns.example.net.
```
移転後の example.jp への委譲
```
example.jp. 86400 IN NS ns.example.com.
```
移転後の example.jp ゾーン
```
example.jp. 86400 IN NS ns.example.com.
```

ここで問題となるのは ns.example.net である。 この旧サーバにゾーンが残存して以下のように新 NS が設定されていれば古い NS キャッシュに基づいて問い合わせが来ても、ほぼ問題は発生しない。

```
example.jp. 600 IN NS ns.example.com.
```

しかし事業者によっては移転後すぐに旧ゾーンが削除される場合がある。登録者が消してしまうことも考えられる。そこで権利のない他人 (攻撃者) があらためて偽ゾーンを作成すると乗っ取りが成立する。

では旧ゾーンはいつ削除すれば良いのだろうか。多くのキャッシュサーバの実装においては権威サーバの返す TTL で NS がキャッシュされるので、この例では 600 秒まてば良いように思えるかもしれない。しかし、短すぎる TTL を切り上げる運用がしばしば行われ、600 が 3600 程度に切り上げられているサーバから問い合わせが発生するかもしれない。

また委譲元の TTL で NS をキャッシュする実装も存在し、大手 ISP がそれを採用していたりする。したがって少なくとも委譲元の TTL で示された時間は適切に設定されたゾーンを維持する必要がある。論文執筆時点 (2019/10/19) において jp は 1 日 (86400)、com は 2 日 (172800) などとなっている。

権威サーバを提供する事業者はこの問題をよく理解してサービス設計を行う必要がある。移転直後にゾーン削除してしまうサービスはゾーン作成にあたって権利確認をしっかり行わないと危険である。

5. Public Suffix ゾーン

co.jp ゾーンが共用の権威サーバに作られていたらどうなるだろうか。以下のようなドメインがあったとする。

jp ゾーンからの委譲
```
example.co.jp. IN NS ns.example.net.
```

co.jp ゾーン
```
co.jp. IN NS ns.example.net.
*.co.jp. IN A 192.0.2.2
```

example.co.jp ゾーン
```
example.co.jp. IN NS ns.example.net.
example.co.jp. IN A 192.0.2.2
```

ここで ns.example.net から example.co.jp ゾーンが削除されると、example.co.jp への問い合わせについてすべて co.jp ゾーンが応答することになる。 あるいは example.co.jp ゾーンを作成する前に ns.example.net に委譲を向けると co.jp が example.co.jp を乗っ取る。 ただし適切に実装されたキャッシュサーバであれば co.jp の NS がキャッシュとして入るような危険性まではないはずである。

co.jp のように多くのドメイン名で共用されるドメイン名は public suffix (あるいは Effective Top Level Domain) と呼ばれる。 Public suffix のゾーンを登録可能である共用の権威サーバにおいては、広範囲のドメイン名に対して lame delegation を待ち受ける攻撃が可能となる。

共用の権威サーバは公開されている Public Suffix のリスト (PSL) `https://publicsuffix.org/` を用いてこれらのゾーンを登録できないようにするべきである。しかし public suffix が登録できてしまうサービスは存在する。

6. 放棄された CNAME

DNS のリソースレコードの指す先が適切に管理されていない問題は NS レコード以外にも存在する。 特に使われなくなった CNAME の指す先が乗っ取られる事例が世界中で多発している。

例えば CDN (Content Delivery Network) を利用するために以下の CNAME が設定されたとする。

```
old-service.example.jp.\
  IN CNAME orphan.cdn.example.com.
```

ここで old-service.example.jp が不要となり、CDN を解約して orphan が cdn.example.com から抹消されたとする。ここで CNAME だけがまだ残っている状態で他人 (攻撃者) があらためて CDN 事業者と契約し、ドメイン名として orphan.cdn.example.com を指定してコンテンツを置くと乗っ取りが成立する。

事例としては、fan.football.sony.net の CNAME であった fanfootballsony.s3-us-west-2.amazonaws.com が乗っ取られたケース [32] や Windows のデスクトップで用いられていた notifications.buildmypinnedsite.com が乗っ取られたケース [33] などがあげられる。

これらは Subdomain takeover attack と呼ばれ、floating domain と同様にバグハンターたちのターゲットとなっており、乗っ取り可能なドメイン名を探すツールがいくつもネット上に公開されている。対策としては使わなくなったリソースレコードは直ぐに削除することが求められる。

7. 共用メールサーバ

DNS 権威サーバは直接関係しないが、関係しないがゆえの問題がある。ドメイン名を自由に設定できる共用のメールサーバをサービスしている事業者は多い。それらのサービスではドメイン名を登録すると共用の DNS 権威サーバにゾーンが作成されるとともにメールサーバの配送設定がなされる。想定されている利用方法は設定後にその権威サーバに上位ゾーンからの委譲が向けられて利用が始まるというものであろう。

しかし上位からの委譲が向くのをまたず、メールサーバを共用するドメイン間においては、ドメイン名が設定された時点で内部配送が始まるサービスが存在する。広く用いられているメールサーバ実装ではいちいち DNS で MX を引くことなく内部配送を行う仕組み [34] が提供されているため、あえてこれを回避する仕組みを用意しない限り同様の状況となる。

このようなサービスではメールサーバの移転が困難 (事前準備で内部配送が始まってしまう) となるばかりでなく、ドメイン名の権利確認もない多くのサービスでは内部配送の乗っ取りが発生しメールが盗聴される危険性がある。

筆者がある大手のレンタルサーバの DNS 権威サーバの挙動を確認するために chukyo-u.ac.jp ゾーンを作成したところ、該当ドメインへメールを送れなくなったので設定を解除して欲しい旨の連絡を事業者から頂くに至った。メールサーバが使うキャッシュサーバが権威サーバへフォワーディングを行っているのか確認したがそうした挙動はなく、単純にメールサーバの内部配送であることが判明した。こうした挙動はいくつかの大手サービスでも同様に確認できている。

この件は 2019 年 4 月に JPCERT/CC へ報告するとともに、セキュリティ関連の勉強会で注意喚起のプレゼン [35] を実施した。

このようなサービスにおいて問題を解消するには内部配送において MX を参照するなどの構造に設計変更をする必要があり、コストとの関係で解決には時間がかかると思われる。こうした状況下における注意喚起のあり方も問題提起をしたい。

8. 兄弟委譲 (sibling glue)

サブドメインを不特定多数に貸し出している (委譲している) サービスが存在する。そして TLD (Top Level Domain) のレジストリも自ずと大量のドメイン名の委譲を共存させているサービス事業者である。これらにおいて発生する問題をここに提起する。

jp ゾーンから以下の委譲が行われていたとする。

```
example.jp. IN NS ns.example.jp.
```

```
example.jp. IN NS ns.example.ad.jp.
```

このとき本来の glue の定義とその必要性からは、example.jp に関する問い合わせに対して、jp サーバの応答は以下のようになるはずである。

```
Authority Section
  example.jp. IN NS ns.example.jp.
  example.jp. IN NS ns.example.ad.jp.
Additional Section
  ns.example.jp. IN A 192.0.2.1
```

ところが実際の応答が以下のようなものになる場合がある。

```
Authority Section
  example.jp. IN NS ns.example.jp.
  example.jp. IN NS ns.example.ad.jp.
Additional Section
  ns.example.jp. IN A 192.0.2.1
  ns.example.ad.jp. IN A 192.0.2.2
```

これは jp ゾーンに以下のように example.ad.jp の glue が登録されていて、権威サーバの実装がこれを example.jp の応答へも提供してしまうためである。

```
example.ad.jp. IN NS ns.example.ad.jp.
ns.example.ad.jp. IN A 192.0.2.2
```

ns.example.ad.jp の A レコードは example.ad.jp の内部名ではあっても example.jp の内部名ではないため glue ではなく、これを example.jp に関する委譲応答で提供する必要性はない。

しかしメジャーな実装 (BIND,NSD で確認) では兄弟関係にあるサブドメイン (sibling domain) への委譲の glue を応答に提供してしまう。これらは俗に sibling glue と呼ばれており、DNS 用語集である RFC8499[31] の”Bailiwick” の説明では ”Glue records for sibling domains are allowed, but not necessary” と容認されている。(なお RFC8499 に sibling glue という用語はない)

example.jp が ns.example.ad.jp の A レコードを提供しない場合、キャッシュサーバはどのみち jp ゾーンへ問い合わせ直すのだから一度に提供してしまえば良いだろうという考えなのだろうが、キャッシュポイズニングの観点からこれが危険であるという筆者の考察を以下に述べる。(実装では未検証)

jp から example.jp への委譲応答が以下だったとする。

```
Authority Section
  example.jp. IN NS longname1.example.jp.
  example.jp. IN NS longname2.example.jp.
  example.jp. IN NS longname3.example.jp.
  (たくさん省略)
  example.jp. IN NS longnameN.example.jp.
  example.jp. IN NS nsa.dns.jp.
Additional Section
  longname1.example.jp. IN A 192.0.2.1
  longname2.example.jp. IN A 192.0.2.2
  longname3.example.jp. IN A 192.0.2.3
  (たくさん省略)
  longnameN.example.jp. IN A 192.0.2.N
  nsa.dns.jp. IN A 203.119.1.4

;; MSG SIZE rcvd: 1600 (フラグメントするサイズ)
```

このとき DNS 第一フラグメント便乗攻撃 [36] が行われると Additional Section の nsa.dns.jp が偽物にすり替えられる可能性がある。

glue が厳格な定義 (RFC8499 の in-domain) を採用したキャッシュサーバであれば nsa.dns.jp の A は捨てられるが、sibling domain まで in-bailiwick(内部名) 扱いした実装 (RFC8499 がこれを追認) ではキャッシュが汚染される。

なお、これは理論上の話であり、ここで例にあげた jp サーバやキャッシュサーバでの第一フラグメント便乗攻撃に対する各種対策によって回避しうる。

第一フラグメント便乗攻撃への対策によらずこれを避けるには sibling domain を除いた本来の in-domain な内部名だけを glue として受け入れる実装が必要である。

9. まとめ

共用 DNS 権威サーバの脆弱性 (危険性) について網羅的に解説した。どの問題も数多くのサービス、ドメインに残存し、頻繁に多くのドメインに危険な状態が発生している。この論文で公表した Sibling domain へのキャッシュポイズニングの考察を含め、すべての問題は既公表の問題であり DNS の利用者たちは危険に晒されている状況である。被害が出るまで、あるいは対策が行き渡るまで注意喚起しないというスタンスは DNS 利用者 (つまり一般のネット利用者) たちの利益にならない。本論文をきっかけに各所から広く注意喚起がなされ、利用者が声をあげ、サービス事業者において対策が進むことに期待したい。

謝辞 何年にも渡って共用サーバの問題を考察してきたが、その過程にあたっては qmail.jp の前野年紀氏にさまざまなご教示を頂いてきた。特に親子同居問題は前野氏の発見によるものである。前野氏には本論文草稿へのご意見も頂きここに感謝を記す。また色々な場で JPRS の森下泰宏氏と意見交換させて頂き、一部の問題については JPRS から注意喚起をして頂いたことに感謝する。JPCERT/CC においては共用メールサーバなど一部の問題について注意喚起を検討頂いており感謝する。また愛知県警察においては愛知県内の事業者に諸々の注意喚起をして頂いており感謝する。

参考文献

[1] 鈴木常彦: キャッシュサーバを権威サーバと兼用すると危ない, http://www.e-ontap.com/dns/weirdra/
[2] ohesotori: DNS 移転失敗体験談, https://www.slideshare.net/ohesotori/dns-23491023
[3] IETF: RFC1034 DOMAIN NAMES - CONCEPTS AND FACILITIES , https://tools.ietf.org/html/rfc1034
[4] IETF: RFC1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, https://tools.ietf.org/html/rfc1035
[5] 民田雅人: サーバーの安全な設定, https://jprs.jp/tech/material/IW2003-DNS-DAY-secure-dns-minda.pdf
[6] JPRS: 再帰的な問合せを使った DDoS 攻撃の対策について, https://jprs.jp/tech/notice/2006-03-29-dns-cache-server.html
[7] JPCERT/CC: DNS の再帰的な問合せを使った DDoS 攻撃に関する注意喚起, https://www.jpcert.or.jp/at/2006/at060004.html
[8] Bernhard Mueller: Improved DNS spoofing using node re delegation, https://sec-consult.com/wp-content/uploads/files/whitepapers/SEC-Consult_Whitepaper_whitepaper-dns-node-redelegation.pdf, 2008
[9] Dan Kaminsky: It's The End Of The Cache As We Know It, https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf, 2008
[10] JPRS: 新たなＤＮＳキャッシュポイズニングの脅威, https://jprs.jp/related-info/guide/009.pdf
[11] 鈴木常彦: DNS の危機的状況,FIT2007（第 6 回情報科学技術フォーラム）一般講演論文集，第 4 分冊，pp.29-31, 2007
[12] Rikitake, K., Suzuki, T. and Nakao, K.: DNS Security: Now and The Future, IEICE Technical Report ICSS2007-01, pp.3-8, 2007
[13] 鈴木常彦: オープンリゾルバの状況, IEICE Technical Report ICM2008-16,pp89-91, 2008
[14] JPRS: 権威／キャッシュ DNS サーバーの兼用による DNS ポイズニングの危険性について, https://jprs.jp/tech/security/2012-07-04-risk-of-auth-and-recurse.html
[15] 東大亮: キャッシュ・権威 兼用型浸透問題への対処, https://www.slideshare.net/hdais/auth-cachebindconfig
[16] JPRS: Security Issues への取り組みと対応, https://www.janog.gr.jp/meeting/janog34/doc/janog34-dnsvl-morishita-1.pdf
[17] 鈴木常彦: DNS 毒入れの真実, http://www.e-ontap.com/dns/poisoning_spa/
[18] 鈴木常彦: DNS 毒入れ疑似体験, http://www.e-ontap.com/dns/mimic-hijack/
[19] 前野年紀: qmail.jp,https://moin.qmail.jp/
[20] 徳丸浩: さくら DNS にサブドメインハイジャックを許す脆弱性,https://blog.tokumaru.org/2012/06/sakura-dns-subdomain-hijacking.html
[21] 鈴木常彦:「さくら DNS にサブドメインハイジャックを許す脆弱性」ってのは過小評価, http://www.e-ontap.com/blog/20120614.html
[22] さくらインターネット株式会社: 当社 DNS に関するお知らせ, https://www.sakura.ad.jp/information/announcements/2012/06/29/653/,2012
[23] JPRS: サービス運用上の問題に起因するドメイン名ハイジャックの危険性について, https://jprs.jp/tech/security/2012-06-22-shared-authoritative-dns-server.html,2012
[24] JPRS: 委任にまつわるエトセトラ, https://dnsops.jp/event/20120901/20120901-DNS_Summer_Days_2012-the-delegation-v1.4-after.pdf#page=18, 2012 東大亮:
[25] ends-query-tagete-info, https://github.com/hdais/edns-query-target-info
[26] IETF: RFC2308 Negative Caching of DNS Queries (DNS NCACHE), https://tools.ietf.org/html/rfc2308
[27] IETF: RFC8020 NXDOMAIN: There Really Is Nothing Underneath, https://tools.ietf.org/html/rfc8020
[28] IETF: Errata ID: 4983, https://www.rfc-editor.org/errata/eid4983
[29] IETF: RFC2181 Clarifications to the DNS Specification, https://tools.ietf.org/html/rfc2181
[30] IETF: RFC1912 Common DNS Operational and Configuration Errors,https://tools.ietf.org/html/rfc1912
[31] IETF: RFC8499 DNS Terminology, https://tools.ietf.org/html/rfc8499
[32] Sony Subdomain Takeover, https://canyoupwn.me/en-sony-subdomain-takeover
[33] Microsoft verliert Kontrolle über Windows-Kacheln, https://www.golem.de/news/subdomain-takeover-microsoft-verliert-\\kontrolle-ueber-windows-kacheln-1904-140709.html
[34] How Postfix delivers mail, http://www.postfix.org/OVERVIEW.html
[35] 黒塗りの DNS (萎縮編)〜共用サービスの闇〜, https://www.e-ontap.com/dns/ssmjp/
[36] 太田健也, 鈴木常彦: DNS 第一フラグメント便乗攻撃の追検証と対策の検討, 第 81 回全国大会講演論文集 2019(1), 443-444, 2019-02-28