DNSの動向

森下 泰宏 ●株式会社日本レジストリサービス（JPRS） 技術広報担当・技術研修センター

WindowsとChromiumの組み合わせでDNSのTCPクエリが増加する事例が発生し、対応が進められた。2014〜2015年に流行したランダムサブドメイン攻撃が再流行し、国内での被害事例も報告された。

■ WindowsとChromiumの組み合わせによるTCPクエリの増加

2022年11月ごろから、Windows版のChromiumベースのウェブブラウザー（Google Chrome、Microsoft Edge）においてウェブサイトが閲覧しづらい状況が発生する旨が、利用者から散発的に報告されるようになった[1]。

本件は、WindowsのUDPの挙動とChromiumに新たに組み込まれた非同期DNSリゾルバー（AsyncDNS）の挙動の組み合わせによってTCPによるDNSクエリ（以下、TCPクエリ）が増加し[2]、その対応が十分でない一部のホームルーターにおいて接続障害が発生することで引き起こされたことが判明している[3]。

●TCPクエリが増加する仕組み

以下、DNS Summer Day 2023で発表されたインターネットイニシアティブ（IIJ）の山口崇徳氏の資料[4]と草場健氏の資料[5]に基づき、TCPクエリが増加する仕組みについて解説する。

1：Windows版ChromiumにおけるAsyncDNSの有効化

2022年11月2日に、Windows版のChromiumにおいて、AsyncDNSをデフォルトで有効にする旨のコミットが実施された[6]。このコミットは2023年1月10日にリリースされた、Chrome 109に組み込まれている。この状況は、2022年11月ごろから今回の事例が報告され始め、2023年1月ごろから報告数が増加したという状況と符合している。

2：AsyncDNSの挙動

AsyncDNSは一般的なDNSクライアントと同様、当初はUDPでDNSクエリを送信する。ただし、システムが割り当てるUDPソースポート番号のエントロピーが低いと判断した場合、キャッシュポイズニングに対する安全性確保の観点から、TCPクエリに切り替えるようになっている[7]。

3：WindowsのUDPの挙動

Windows 10/11のUDPの挙動を調査した結果、システムが割り当てるUDPソースポート番号はランダムになっておらず、少し前に割り当てられたポート番号と同じ番号が複数回にわたり割り当てられる場合があることが判明している。

なお、この挙動の理由として、Windows 11がUDPポートの枯渇に対応するためにソケットキャッシング（socket caching）という機能を導入したためである旨が海外の技術者から報告され

ているが[8]、マイクロソフトは本件に関する公式見解を公開しておらず、詳細は不明である。

4：TCPクエリの増加に伴う接続障害の発生

2の挙動と3の挙動が重なることで、Windows版のChromiumベースのウェブブラウザーからのTCPクエリが増加し、その対応が十分でない一部のホームルーターやファイアウォールなどを使っている環境において、接続障害が発生する。

●本件に関する対応状況

TCPクエリへの対応が十分でなかった一部のホームルーターにおいて、ファームウエアの更新による対応が実施されている[9]。

またChromiumにおいても、UDPソースポートの重複判定の条件を直近256回のうち2回から256回のうち3回に変更し、TCPクエリへの切り替えの発生頻度を減らす緩和策が実施され、2023年5月にリリースされたChrome 113に適用されている。

■ランダムサブドメイン攻撃の再流行

2023年3月ごろから、DNSを狙った攻撃手法であるランダムサブドメイン攻撃と考えられる事例が世界的に増加し、わが国の行政機関や地方自治体などを含む複数のウェブサイトで具体的な被害も発生している旨が、複数の研究者[10]や事業者[11]から報告されている。

●ランダムサブドメイン攻撃の仕組み

ランダムサブドメイン攻撃は、攻撃対象のドメイン名を管理する権威DNSサーバーに大量のDNSクエリを集中させることでサービスの利用・提供を妨害する、DDoS攻撃の一つである[12]。

ランダムサブドメイン攻撃の仕組みを資料1に示す。攻撃者（①）は別途作成・入手したインターネット上のオープンリゾルバー[13]のリストを持っており、乗っ取られた多数の機器で構成されたBotnet（②）を遠隔操作できる。この状況において攻撃者はBotnetに対し、攻撃対象のドメイン名にランダムなサブドメインを追加した名前で、リストに掲載されているオープンリゾルバー（③、④）に名前解決要求を送るように指令を出す[14]。

この名前はキャッシュされていないため、クエリを受け付けたフルリゾルバー（③、⑤）は攻撃対象ドメイン名の権威DNSサーバー（⑥）にDNSクエリを送る。その結果、DNSクエリが権威DNSサーバーに集中し、サーバーやネットワークの処理能力を超えることで、攻撃が成立する。

●パブリックDNSサービスを用いた攻撃

本件について、Google Public DNSやクラウドサービス大手のCloudflareが運用する1.1.1.1などの大手パブリックDNSサービスを攻撃に利用する事例が報告されている[15]。パブリックDNSサービスは意図的なオープンリゾルバーとして運用されているため攻撃元を選択的にブロックすることが難しく、かつ攻撃者はその高いパフォーマンスを攻撃の効率向上に利用することが可能になる。

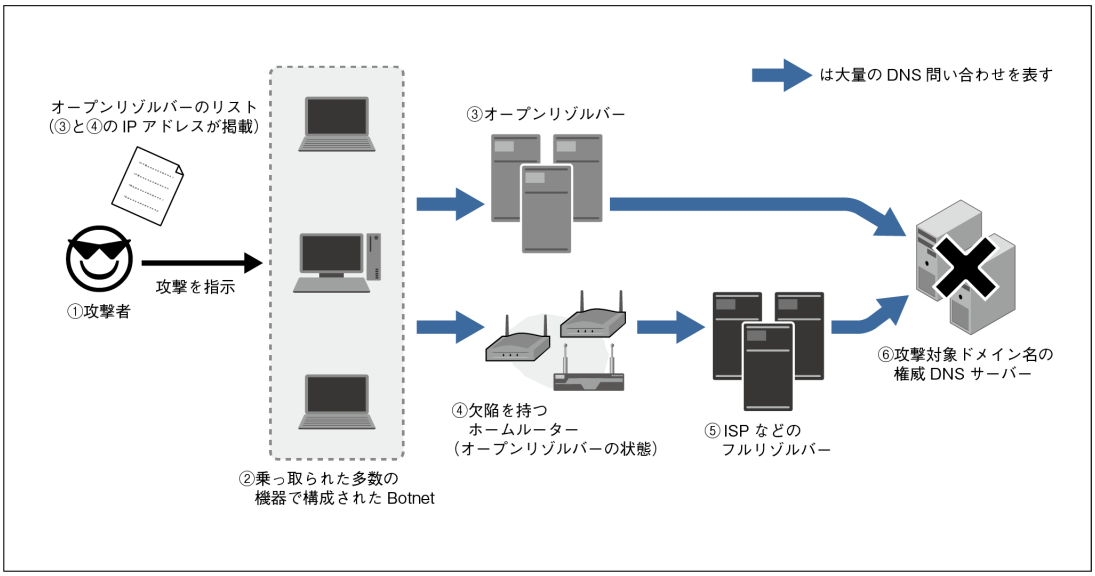
●攻撃の目的・意図

ランダムサブドメイン攻撃は2014年から2015年にかけ、世界的に流行した。当時の攻撃対象は主に中国語圏のカジノサイト・ECサイト・ニュースサイトなどで、対象となる組織やサービスに、一定の傾向が見られた[16]。しかし、今回の攻撃ではそうした傾向が判明しておらず、攻撃の目的は現在まで明らかになっていない。

●攻撃への対策

ランダムサブドメイン攻撃の代表的な対策とし

資料4-3-16　ランダムサブドメイン攻撃の仕組み



出所：筆者作成

て、サーバーやネットワークの攻撃耐性を高めることと、攻撃の巻き添えによるサービス全断のリスクの低減を図ることの2点が挙げられる。

前者の例としては権威DNSサーバーそのものの強化に加え、ロードバランサーやIP Anycast[17]の導入によるサーバーやネットワークのスケールアップ・スケールアウトが挙げられる。また、高負荷に耐える外部DNSサービスの利用や複数の外部DNSサービスの併用も、有効な対策となる。

後者の例としては、権威DNSサーバーを複数のグループに分けることで収容するドメイン名を分散する、サーバーのグループ化が挙げられる。資料2の例では権威DNSサーバーを3グループに分けて収容するドメイン名を分散し、攻撃の巻き添えによるDNSサービスの全断を回避している。

■ルートゾーンへのZONEMDの追加

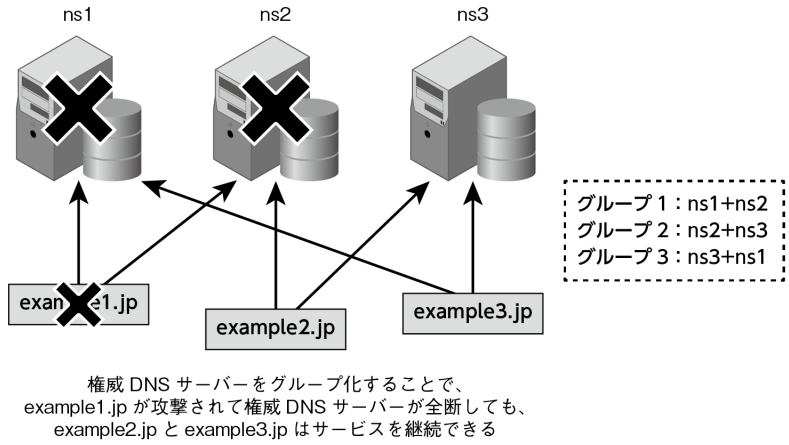
2023年9月21日（協定世界時）、ルートゾーンにZONEMDリソースレコード（以下、RR）が追加された[18]。本稿ではZONEMD RRの概要と、ルートサーバーの運用における取り扱いについて記述する。

●ZONEMDとは

ZONEMDはRFC 8976で定義される、ゾーンデータ全体のメッセージダイジェスト[19]を記述するためのRRである。ZONEMD RRのフォーマットと記述例を資料3に示す。

ZONEMDをDNSSECと併用することで、ゾーンデータの受信者はその内容を検証し、データの完全性と発信元の真正性を確認できるようになる。これにより受信者は、受信したゾーンデータと公開されたゾーンデータが同一であることを検証できる。なお、ZONEMDをDNSSECなしで使った場合はチェックサムとしてのみ機能し、送信エラーや切り捨てなどの偶発的な破損からゾーンデータを保護する。

資料4-3-17　権威DNSサーバーのグループ化



出所：筆者作成

資料4-3-18　ZONEMDリソースレコードのフォーマットと記述例

ZONEMDのフォーマット

```
ドメイン名 TTL　IN ZONEMD シリアル スキーム ハッシュアルゴリズム (
                    ダイジェスト )
```

ZONEMDの記述例

```
$ORIGIN .
@    86400 IN ZONEMD 2023121500 1 1 (
              9C2028B2E9FB3675CA39E707E401687D55A37FC107C9
              B889EE563230FBB1FFEAF72AE6913199BF6072987860
              6481C12B )
```

出所：筆者作成

●ルートサーバーにおけるZONEMDの取り扱い

ZONEMDの追加に先立ち、2022年8月2日にルートサーバー運用者（Root Server Operators、以下RSO）が、その取り扱いに関する声明を発表した[20]。その内容を以下に示す。

1：ルートサーバーシステムの安定性と信頼性確保のため、初期導入・テストの期間中、各自のシ

ステムがZONEMD RRを含むルートゾーンを受信・提供できるかを検証する。

2：ZONEMD RRの追加後少なくとも1年間、その有効性にかかわらず受け取ったゾーンデータをそのまま配布する。また、期間中にZONEMD RRの正当性を評価し、ZONEMDによる検証を有効にする前に、その結果を報告する。

3：その後、個々のRSOは、各自のシステムにおけるZONEMDの検証失敗への対応方法の理解と、不正なルートゾーンを受け取った際のIANAとルートゾーンメンテナー（注：現在はVerisign）への連絡手順の文書化を前提として、ZONEMDの検証を有効にできる。

4：RSOはルートゾーンメンテナーとIANA機能の運用者（注：現在はPTI）に対し、ZONEMD RRをルートゾーンに追加する日の2か月前に連絡する旨を要請する。

●正式運用の開始

段階的な導入を図るため、2023年9月21日のZONEMD RRの追加ではハッシュアルゴリズムとしてプライベート領域（241）が設定された。その後、2023年12月6日にハッシュアルゴリズムが本来の値であるSHA-384（1）に変更され、ゾーンデータの検証が可能になった[21]。

●1.1.1.1における名前解決障害の発生

ZONEMD RRの追加から2週間後の2023年10月4日7時から11時（協定世界時）にかけ、パブリックDNSサービス1.1.1.1においてZONEMD RRの追加に起因する名前解決障害が発生していた旨を、運営元のCloudflareが発表した[22]。

同社では本件について、パフォーマンス向上のために1.1.1.1に導入していたルートゾーンをローカルに保持するシステムがZONEMD RRを解析できなかったためにゾーンデータが更新されない状態になり、2週間後の2023年10月4日にDNSSEC署名の有効期間の満了による検証エラーが発生したことが障害の原因であった旨を公表し、陳謝を表明している。

■B-RootのIPアドレス変更

2023年11月27日に、ルートサーバーの一つであるb.root-servers.net（以下、B-Root）のIPv4/IPv6アドレスが変更された[23]。ルートサーバーのIPアドレス変更は2017年10月24日のB-RootのIPv4アドレスの変更以来、6年ぶりとなる。

●IPアドレス変更の目的

B-Rootを運用する南カリフォルニア大学情報科学研究所（USC/ISI）は今回のIPアドレス変更の目的として、IPアドレスを割り当てるRIRを多様化し、ルートサーバーシステムの耐久性を高めることを挙げている。

今回のB-RootのIPアドレスは、USC/ISIと中南米地域を担当するRIRであるLACNICが契約を締結し、LACNICが割り当てている。本件はLACNICとして初の、ルートサーバーへのIPアドレス割り当てとなる[24]（資料4-3-19）。

なお、今回割り当てられたIPアドレスの経路情報はLACNICが提供するRPKI[25]による送信元検証が可能になっており、信頼性の向上が図られている。

●DNS運用への影響

ルートサーバーのIPアドレスが変更された場合、運用中のフルリゾルバーにおいてルートヒントの更新作業が必要になる[26]。運用元のUSC/ISIは更新作業のための移行期間を少なくとも1年

資料4-3-19　RIRと割り当て先ルートサーバーの状況

RIR	担当地域	割り当て先ルートサーバー
ARIN	北米	A, C, D, E, F, G, H, J, L
RIPE NCC	欧州・中東・中央アジア	I, K
APNIC	アジア・太平洋	M
LACNIC	中南米・カリブ海	B
AFRINIC	アフリカ	（なし）

（2023年11月27日現在）

出所：筆者作成

間、2024年11月27日まで設定する旨を発表している。

■DNSソフトウエアの脆弱性の状況

●BINDの状況

資料4-3-20に、2023年中にJPRSが注意喚起したBINDの脆弱性情報を示す。

2023年中に公開された7件の脆弱性のうち3件が、RFC 8767で定義されるserve-stale機能の実装不具合に起因するものとなっている。serve-staleは権威DNSサーバーから所定の時間内に応答が得られなかった場合に期限切れのキャッシュデータを活用して、名前解決を継続する機能である。なお、2023年12月現在、本機能はデフォルトで無効に設定されている。

●BIND以外のDNSソフトウエアの状況

資料4-3-21に、2023年中にJPRSが注意喚起したBIND以外のDNSソフトウエアの脆弱性情報を示す。

2023年4月のマイクロソフトのセキュリティ更新プログラム（月例パッチ）で、Windows DNSサーバーの脆弱性が10件公開されている。うち9件はリモートコード実行（RCE）が可能になる重大な脆弱性であるため、速やかなパッチの適用が必要である。

1. サイトに接続できないと頻繁に表示されるようになりました。- Google Chrome コミュニティ、https://support.google.com/chrome/thread/188653227/
2. DNSの現在の仕様では、すべてのリゾルバーと権威DNSサーバーはTCPとUDPの双方でのサービス提供が必須であり、クライアントはTCPとUDPのどちらでクエリを送ってもよいと定められている。
3. WindowsのChromeやEdgeでネットにつながりにくくなる現象、一部の家庭用ルーターが原因かも？【DNS Summer Day 2023】- INTERNET Watch、https://internet.watch.impress.co.jp/docs/event/1520427.html
4. ChromeのTCPクエリ問題、https://dnsops.jp/event/20230623/20230623-yamaguchi.pdf
5. Chromeはなぜ TCPクエリを出したのか、https://dnsops.jp/event/20230623/20230623-kusaba.pdf
6. 他のOS（Android、Linux、macOS）ではAsyncDNSが既に有効にされていたが、Windows版とはUDPソケットの取り扱いが異なっており、当該事例は発生しなかった。
7. TCPクエリが送信される状態になった場合、当該ウェブブラウザーを再起動するまでその状態が継続する。
8. Increase in DNS over TCP from Chrome Browser on Windows 11、https://lists.dns-oarc.net/pipermail/dns-operations/2023-March/021979.html
9. WindowsのChromeだとネットにつながらない、特定のISPで起こった怪現象| 日経クロステック（xTECH）、https://xtech.nikkei.com/atcl/nxt/column/18/02538/072700001/
10. 2023年春に起きたDNS水責め絨毯爆撃の観察記録- 情報処理学会電子図書館、http://id.nii.ac.jp/1001/00226666/
11. ランダムサブドメイン攻撃において事業者として行なった対策と解析について、https://internetweek.jp/2023/archives/program/c10
12. JPRS用語辞典｜ランダムサブドメイン攻撃（DNS水責め攻撃）、https://jprs.jp/glossary/index.php?ID=0137
13. JPRS用語辞典｜オープンリゾルバー（Open Resolver）、https://jprs.jp/glossary/index.php?ID=0184
14. 例えば、攻撃対象のドメイン名がexample.jpであった場合、攻

資料 4-3-20　2023 年に JPRS が注意喚起した BIND の情報

公開・更新日	タイトル	概要
2023/1/26	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2022-3924）	serve-stale の実装不具合
2023/1/26	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2022-3736）	serve-stale の実装不具合
2023/1/26	（緊急）BIND 9.x の脆弱性（メモリ不足の発生）について（CVE-2022-3094）	dynamic update の実装不具合
2023/6/22	（緊急）BIND 9.x の脆弱性（メモリ不足の発生）について（CVE-2023-2828）	キャッシュクリーニングの実装不具合
2023/6/22	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2023-2911）	serve-stale の実装不具合
2023/9/21	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2023-3341）	制御チャンネルの入力処理の実装不具合
2023/9/21	（緊急）BIND 9.18.x の脆弱性（DNS サービスの停止）について（CVE-2023-4236）	DNS over TLS の実装不具合

出所：筆者作成

資料 4-3-21　2023 年に JPRS が注意喚起した BIND 以外の DNS ソフトウエアの情報

公開・更新日	タイトル
2023/1/25	PowerDNS Recursor の脆弱性情報が公開されました（CVE-2023-22617）
2023/1/25	PowerDNS Recursor の脆弱性情報が公開されました（CVE-2023-22617）
2023/2/3	Knot Resolver の脆弱性情報が公開されました
2023/3/17	Windows DNS サーバーの脆弱性情報が公開されました（CVE-2023-23400）
2023/4/3	PowerDNS Recursor の脆弱性情報が公開されました（CVE-2023-26437）
2023/4/14	Windows DNS の脆弱性情報が公開されました（CVE-2023-28223、他 9 件）
2023/6/16	Windows DNS の脆弱性情報が公開されました（CVE-2023-32020）
2023/7/14	Windows DNS サーバーの脆弱性情報が公開されました（CVE-2023-35310、他 3 件）
2023/8/25	Knot Resolver の脆弱性情報が公開されました
2023/12/15	Windows DNS の脆弱性情報が公開されました（CVE-2023-35622）

出所：筆者作成

撃には{ランダムな文字列}.example.jp という名前が使われる。

15. 2023 年第 2 四半期 DDoS 脅威レポート、https://blog.cloudflare.com/ddos-threat-report-2023-q2-ja-jp
16. 当時進行していた香港の反政府デモを支持する報道機関がデモの記事を掲載した直後、その報道機関のドメイン名が大規模なランダムサブドメイン攻撃を受けた事例が、複数回報告されている。
17. JPRS 用語辞典｜IP Anycast（アイピーエニーキャスト）、https://jprs.jp/glossary/index.php?ID=0108
18. [dns-operations] Root zone operational announcement: introducing ZONEMD for the root zone、https://lists.dns-oarc.net/pipermail/dns-operations/2023-September/022286.html
19. JPRS 用語辞典｜ハッシュ値（ダイジェスト値）、https://jprs.jp/glossary/index.php?ID=0230
20. Statement on adding ZONEMD to the root zone、https://root-servers.org/media/news/2022-08-Statement_on_ZONEMD.pdf
21. [dns-operations] Root zone operational announcement: introducing ZONEMD for the root zone、https://lists.dns-oarc.net/pipermail/dns-operations/2023-December/022388.html
22. 2023 年 10 月 4 日の 1.1.1.1 ルックアップ障害、https://blog.cloudflare.com/ja-jp/1-1-1-1-lookup-failures-on-october-4th-2023-ja-jp/
23. New addresses for b.root-servers.net、https://b.root-servers.org/news/2023/05/16/new-addresses.html
24. LACNIC Assigns Number Resources to the USC/ISI DNS Root Server、https://www.lacnic.net/6869/2/lacnic/lacnic-assigns-number-resources-to-the-usc_isi-dns-root-server
25. リソース PKI (RPKI; Resource Public Key Infrastructure) –

JPNIC、https://www.nic.ad.jp/ja/rpki/

26. b.root-servers.net（B-Root）のIPアドレス変更に伴う設定変更について、https://jprs.jp/tech/notice/2023-11-28-b.root-servers.net-ip-address-change.html

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2024年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | インプレス・サステナブルラボ | ✉ iwp-info@impress.co.jp