JPRSの技術情報発信（2023年7月～2024年6月）

2024年6月21日

DNS Summer Day 2024

株式会社日本レジストリサービス（JPRS）

森下 泰宏

JPRSの技術情報発信 [1/2]

**JPRSではインターネットの安定運用を目的として、さまざまな形で
ドメイン名・DNS・サーバー証明書に関する技術情報を発信しています。**

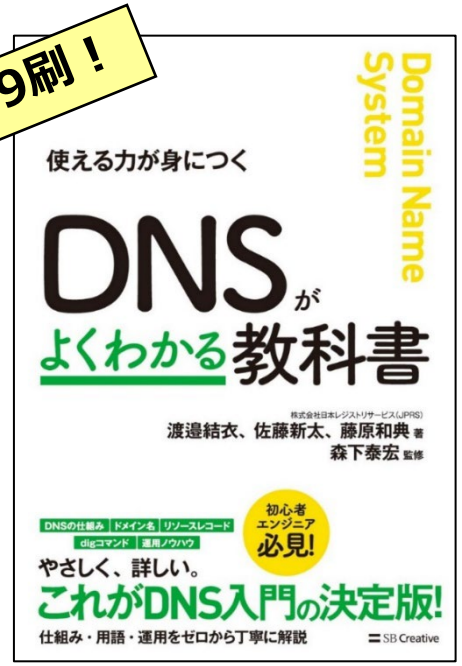
- **公式サイト**
  - JPRS DNS関連技術情報 <https://jprs.jp/tech/>
  - サーバー証明書発行サービス <https://jprs.jp/pubcert/>
  - ドメイン名関連会議報告 <https://jprs.jp/related-info/event/>
  - 技術解説「トピックス&コラム」 <https://jprs.jp/related-info/guide/>
  - 用語辞典 <https://jprs.jp/glossary/>

JPRSの技術情報発信 [2/2]

- **SNS公式アカウント（X、Facebook、YouTube）**

@JPRS_official　　JPRSofficial　　JPRSpress

- **電子メール**
  - メールマガジン「FROM JPRS」<https://jprs.jp/mail/>
  - メーリングリストでの情報提供（DNSOPS.JP、JANOG）
- **書籍「DNSがよくわかる教科書」**
  - 9刷になりました！
- **カンファレンス・イベントなどにおける発表・ブース出展**



本日ご紹介する技術情報発信

1. 脆弱性情報

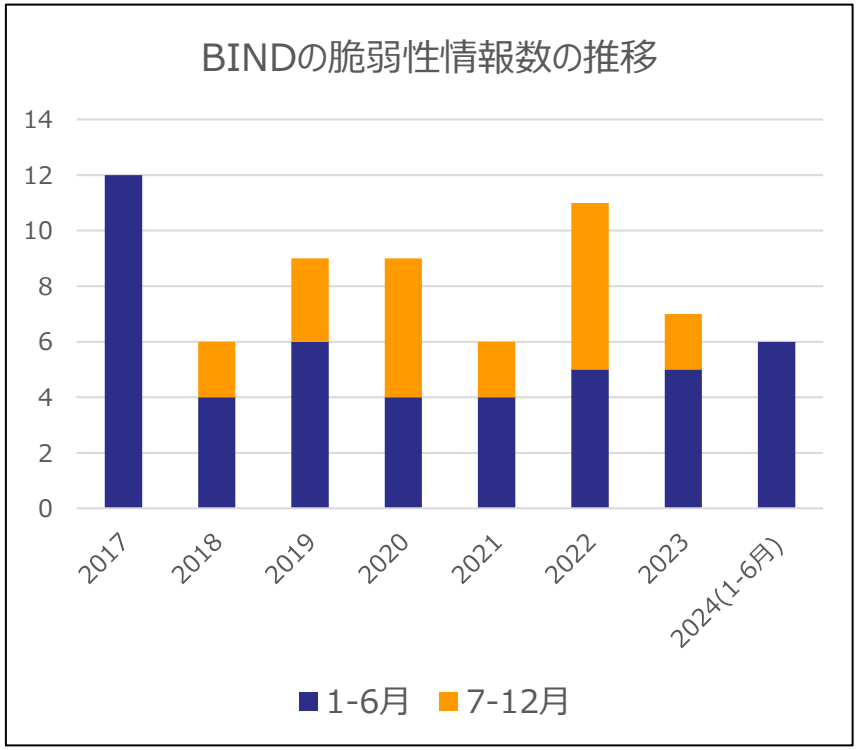
- BIND
- BIND以外

2. DNS運用に関する技術情報

- b.root-servers.net（B-Root）のIPアドレス変更
- RFC日本語訳の追加公開

脆弱性情報

- **BIND（8件（緊急8件））**
  - 2023年7月～12月：2件（前年同期：6件）
  - 2024年1月～6月：6件（前年同期：5件）
- **BIND以外（11件）**
  - Knot Resolver（2件）
  - PowerDNS Recursor（2件）
  - Unbound（3件）
  - Windows DNS（4件）



（カッコ内はJPRSが発信した脆弱性情報の件数）

脆弱性情報（BIND）[1/2]

公開日	タイトル・URL	概要
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）<https://jprs.jp/tech/security/2023-09-21-bind9-vuln-controlchannel.html>	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）<https://jprs.jp/tech/security/2023-09-21-bind9-vuln-dnsovertls.html>	DNS over TLSの実装不具合
2024/2/14	（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2023-5517）<https://jprs.jp/tech/security/2024-02-14-bind9-vuln-nxdomain-redirect.html>	nxdomain-redirectの実装不具合
2024/2/14	（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2023-5679）<https://jprs.jp/tech/security/2024-02-14-bind9-vuln-serve-stale.html>	serve-staleの実装不具合
2024/2/14	（緊急）BIND 9.xの脆弱性（メモリ不足の発生）について（CVE-2023-6516）<https://jprs.jp/tech/security/2024-02-14-bind9-vuln-cache-cleaning.html>	キャッシュクリーニングの実装不具合

脆弱性情報（BIND）[2/2]

公開日	タイトル・URL	概要
2024/2/14	（緊急）BIND 9.xの脆弱性（過剰なCPU負荷の誘発）について（CVE-2023-4408）<https://jprs.jp/tech/security/2024-02-14-bind9-vuln-dnsmessage.html>	計算量が多くなるDNSメッセージを処理させる **※影響大**
2024/2/14	（緊急）BIND 9.xの脆弱性（過剰なCPU負荷の誘発）について（CVE-2023-50387）<https://jprs.jp/tech/security/2024-02-14-bind9-vuln-keytrap.html>	**KeyTrap脆弱性** **※影響大**
2024/2/14	（緊急）BIND 9.xの脆弱性（過剰なCPU負荷の誘発）について（CVE-2023-50868）<https://jprs.jp/tech/security/2024-02-14-bind9-vuln-nsec3.html>	計算量が多くなるNSEC3をDNSSEC検証させる

2024年2月のBIND定期リリース

- **6件の脆弱性情報を公開**
- **運用への影響が大きい脆弱性情報が2件含まれている**
  - CVE-2023-4408
  - KeyTrap（CVE-2023-50387）

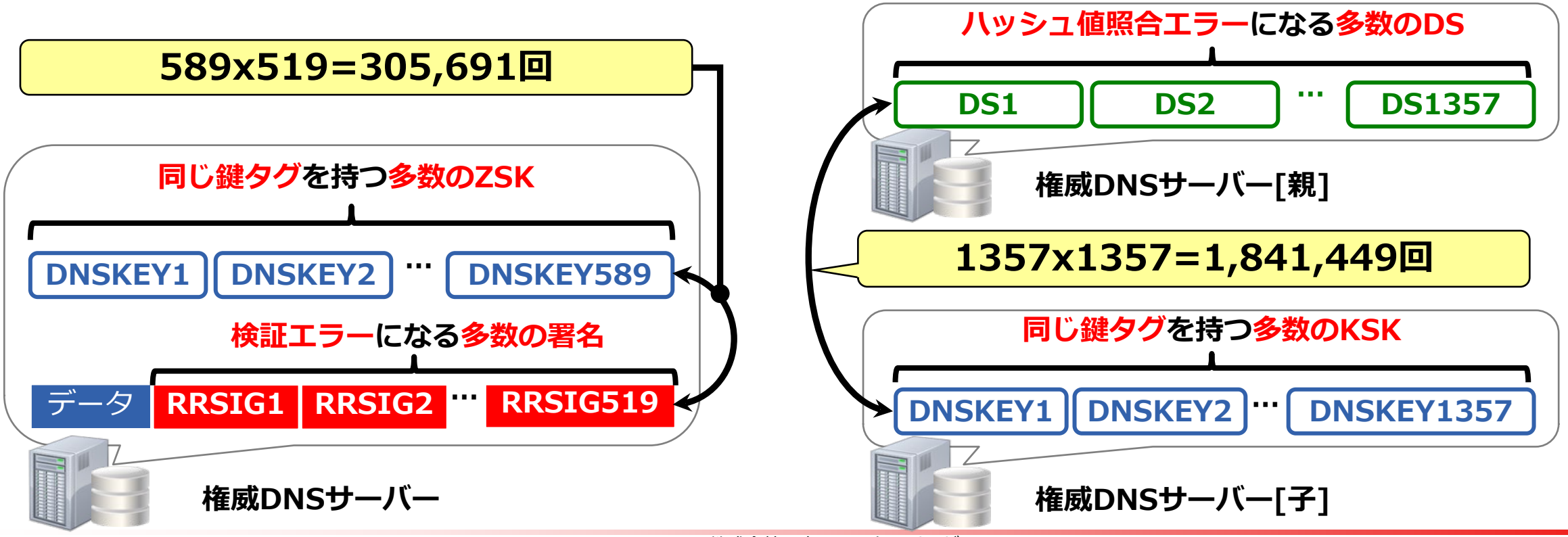
CVE-2023-4408

- **以下の4条件をすべて満たしている**
  - **フルリゾルバーと権威DNSサーバーの双方**が対象
  - **9.0.0以降のすべてのバージョン**のBIND 9が対象
  - リモートからの**問い合わせと応答の双方**で脆弱性をトリガー可能
  - namedの**設定やオプションの変更**では**影響を回避・軽減できない**

公開直後に、**PoCを作成・検証できた**旨が報告されています。
まだの場合、すぐに対応しましょう。

KeyTrap（CVE-2023-50387）

- フルリゾルバーをだまして、負荷の高い処理をさせる（以下は例）
  - ポステルの法則の「受信では寛容に」を過剰に適用してしまった事例の一つ



脆弱性情報（BIND以外）[1/2]

公開日	タイトル・URL	概要
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）<https://jprs.jp/tech/security/2023-07-14-windowsdns.html>	**RCE脆弱性4件**
2023/8/25	Knot Resolverの脆弱性情報が公開されました<https://jprs.jp/tech/security/2023-08-25-knotresolver.html>	特定のケースで過剰なTCP再接続を実行してしまう
2023/12/15	Windows DNSの脆弱性情報が公開されました（CVE-2023-35622）<https://jprs.jp/tech/security/2023-12-15-windowsdns.html>	DNSスプーフィングが可能になる
2024/3/12	Unboundの脆弱性情報が公開されました（CVE-2024-1931）<https://jprs.jp/tech/security/2024-03-12-unbound.html>	拡張DNSエラー（EDE）の内部処理で無限ループが発生
2024/2/14	Windows DNSサーバーの脆弱性情報が公開されました（CVE-2024-26221、他6件）<https://jprs.jp/tech/security/2024-04-12-windowsdns.html>	**RCE脆弱性7件**

脆弱性情報（BIND以外）[2/2]

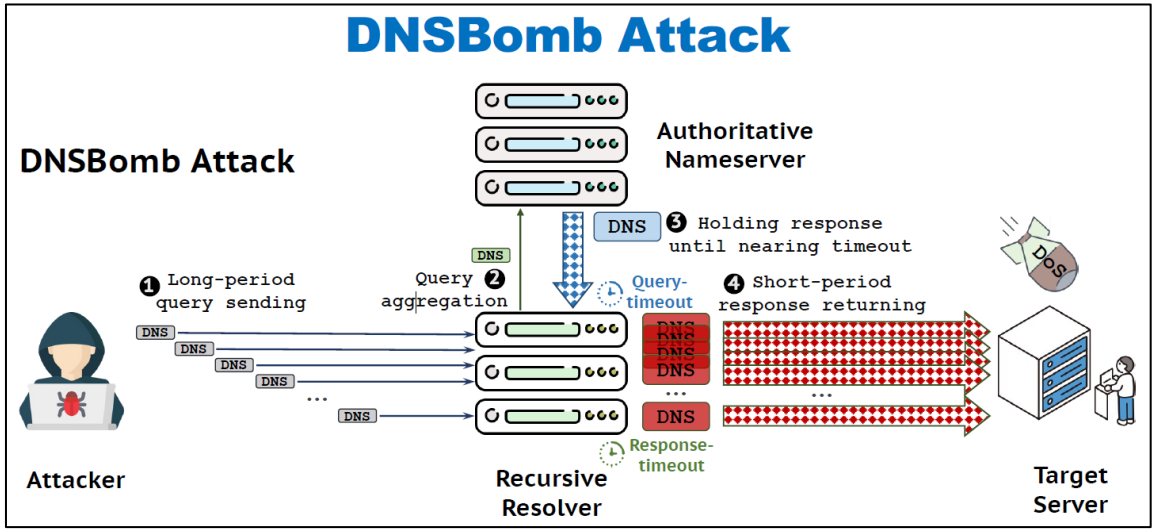
公開日	タイトル・URL	概要
2024/2/16	Knot Resolverの脆弱性情報が公開されました（CVE-2023-50387、CVE-2023-50868）<https://jprs.jp/tech/security/2024-02-16-knotresolver.html>	**KeyTrap脆弱性**・NSEC3脆弱性
2024/2/16	PowerDNS Recursorの脆弱性情報が公開されました（CVE-2023-50387、CVE-2023-50868）<https://jprs.jp/tech/security/2024-02-16-powerdns-recursor.html>	**KeyTrap脆弱性**・NSEC3脆弱性
2024/2/16	Unboundの脆弱性情報が公開されました（CVE-2023-50387、CVE-2023-50868）<https://jprs.jp/tech/security/2024-02-16-unbound.html>	**KeyTrap脆弱性**・NSEC3脆弱性
2024/2/16	Windows DNSの脆弱性情報が公開されました（CVE-2023-50387、CVE-2024-21342、CVE-2024-21377）<https://jprs.jp/tech/security/2024-02-16-windowsdns.html>	**KeyTrap脆弱性**、ほか2件の実装バグ
2024/4/30	PowerDNS Recursorの脆弱性情報が公開されました（CVE-2024-25583）<https://jprs.jp/tech/security/2024-04-30-powerdns-recursor.html>	フォワーダーとして設定している場合に特定の応答でDoS可能
2024/5/13	Unboundの脆弱性情報が公開されました（CVE-2024-33655）<https://jprs.jp/tech/security/2024-05-13-unbound.html>	**DNSBombの高効率な踏み台**として利用可能

Windows DNSサーバーのRCE脆弱性

- **MSの月例更新で、同じ人物が報告した複数のRCE脆弱性がまとめて公開される傾向が続いている**
  - 2021年7月（10件）・2022年4月（17件）
    - 報告者：Yuki Chen（陳雪斌）氏
  - 2023年4月（9件）・2023年7月（4件）
    - 報告者：George Hughey氏
  - 2024年4月（7件）
    - 報告者：Rajesh Kumar氏

DNSBomb（CVE-2024-33655など）

- **2024年5月22日に論文が公開された、パルス型DoS攻撃の手法**
  - **DNSリフレクター攻撃**の一種
  - 発表者は攻撃の流れを、**“Ka-me”**、**“Ha-me”**、**“HA!!!”**と説明している
    - **送信元を偽装した同じ内容の問い合わせ**を、踏み台のフルリゾルバーに**少しずつ送って溜め込み**（①：**Ka-me**）、権威DNSサーバーへの問い合わせを**一つに集約する**（②）
    - 権威DNSサーバーで、応答を**タイムアウトの直前まで保留した後で返す**（③：**Ha-me**）
    - **多数の大きな応答**が標的に**一気に返される**（④：**HA!!!**）



引用元：<https://lixiang521.com/publication/oakland24-2/sp2024-dnsbomb-slides.pdf>

Unboundにおける先行対応

- **踏み台としての効率が特に高かったため、論文公開の2週間前に効率を下げるためのパッチが先行公開された（5月8日）**
  - JPRSでは5月13日にUnboundの脆弱性情報を公開

Software	Practical Attack Bandwidth			
	Attacker -side	Victim -side	Nameserver -side	BAF
BIND	140.6Kb/s	92.5Mb/s	155.5Kb/s	673.9x
Unbound	140.6Kb/s	2.9Gb/s	140.6Kb/s	21,881.1x
PowerDNS	562.5Kb/s	230.4Mb/s	70.3Kb/s	419.5x
Knot	421.9Kb/s	925.4Mb/s	70.3Kb/s	2,246.3x
Microsoft	210.9Kb/s	274.5Mb/s	70.3Kb/s	1,332.4x

2.1万倍以上

引用元：<https://lixiang521.com/publication/oakland24-2/sp2024-dnsbomb-slides.pdf>

技術情報（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（B-Root）のIPアドレスが変更された**
  - JPRSでは11月28日に**技術情報**を公開

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>

  - 2023年7月のJANOG52で、**変更の背景と必要な対応**について情報発信
    - 幕間動画のアーカイブをJPRS公式YouTubeチャンネルで公開

b.root-servers.netのIPアドレス変更とDNS運用者における対応について4分でまとめてみた
<https://www.youtube.com/watch?v=xOThYczeZGk>

ゆっくり確実に更新すればOK！

- **フルリゾルバー（キャッシュDNSサーバー）の運用者**
  - ルートヒントの更新が必要
  - しかし、**慌てる必要はない**
    - 少なくとも1年間（～2024年11月27日）、**旧IPアドレスでサービスが継続**される
    - 主なDNSソフトウェア・ディストリビューション・パッケージでは更新の際に、**ルートヒントも併せて更新**される
- **権威DNSサーバーの運用者**
  - **何もする必要はない**

技術情報（RFC日本語訳の追加公開）

- **公式サイトで、DNS･DNSSECに関する主なRFCの日本語訳を公開**
  - 1034･1035･2181･4033･4034･4035･5155など、**55本**
- **2024年2月16日に、RFC 7583を追加公開**

RFC 7583：DNSSECにおける鍵のロールオーバーのタイミングに関する考慮点
<https://jprs.jp/tech/material/rfc/RFC7583-ja.txt>

  - 総務省「令和5年度ISPにおけるネットワークセキュリティ技術の導入及び普及促進に関する調査の請負事業DNSSECガイドライン作成チーム」の活動の成果物として作成されたもの
    - 総務省の許諾のもと、ご提供いただいた形で無償公開

JPRSでは今後もさまざまな形で技術情報発信を続けていきます！

<https://jprs.jp/tech/>

@JPRS_official　JPRSofficial　JPRSpress