

JPRSの技術情報発信 (2022年7月～2023年6月)

2023年6月23日

DNS Summer Day 2023

株式会社日本レジストリサービス (JPRS)

森下 泰宏

「DNSがよくわかる教科書」増刷！

- **7刷**になりました！

- 2018年11月22日 発売（1刷）
- 2018年12月（2刷）
- 2019年7月（3刷）
- 2020年6月（4刷）
- 2021年2月（5刷）
- 2021年12月（6刷）
- **2023年4月（7刷）**

- 出版社サポートページに更新情報を随時掲載

- 増刷時に書籍（紙・電子版）に反映



DNSがよくわかる教科書 | SBクリエイティブ
<<https://www.sbcr.jp/product/4797394481/>>

7刷での変更点

1. G Suite → Google Workspaceへの名称変更と、
内容更新への対応
2. QNAME minimisationに関するコラムを追加
3. DNS over QUICに関するコラムを追加
4. 付録Aに新しいRFCを追加

『DNSがよくわかる教科書』第7刷での変更点について
<<https://www.sbcr.jp/support/4815617742/>>

本日より紹介する技術情報発信

1. 脆弱性情報

- BIND (11件)
- BIND以外のDNS実装 (12件)

2. 解説動画

- Internet Week Basicオンデマンド
- JPRS YouTube公式チャンネル

3. 予告：b.root-servers.netのIPアドレス変更

脆弱性情報

- BIND (11件 (緊急9件))
 - 2022年7月～12月：6件 (前年同期：2件)
 - 2023年1月～6月：5件 (前年同期：5件)
- BIND以外のDNS実装 (12件)
 - Knot Resolver (2件)
 - PowerDNS Recursor (3件)
 - Unbound (2件)
 - Windows DNS (5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
2022/9/22	<ul style="list-style-type: none"> ■ (緊急) BIND 9.18.xの脆弱性 (メモリアリークの発生) について (CVE-2022-2906) <https://jprs.jp/tech/security/2022-09-22-bind9-vuln-tkey.html> 	TKEY共通鍵 処理時のメモリ リーク
2022/9/22	<ul style="list-style-type: none"> ■ BIND 9.xの脆弱性 (パフォーマンスの低下) について (CVE-2022-2795) <https://jprs.jp/tech/security/2022-09-22-bind9-vuln-large-delegations.html> 	特殊な委任情報 の処理の不具合
2022/9/22	<ul style="list-style-type: none"> ■ BIND 9.18.xの脆弱性 (不適切なメモリの読み取りまたはDNSサービスの停止) について (CVE-2022-2881) <https://jprs.jp/tech/security/2022-09-22-bind9-vuln-bufferoverread.html> 	statistics channelの実装 不具合
2022/9/22	<ul style="list-style-type: none"> ■ (緊急) BIND 9.xの脆弱性 (DNSサービスの停止) について (CVE-2022-3080) <https://jprs.jp/tech/security/2022-09-22-bind9-vuln-serve-stale.html> 	serve-staleの 実装不具合
2022/9/22	<ul style="list-style-type: none"> ■ (緊急) BIND 9.xの脆弱性 (メモリアリークの発生) について (CVE-2022-38177) <https://jprs.jp/tech/security/2022-09-22-bind9-vuln-ecdsa.html> 	ECDSA検証時 のメモリアリーク
2022/9/22	<ul style="list-style-type: none"> ■ (緊急) BIND 9.xの脆弱性 (メモリアリークの発生) について (CVE-2022-38178) <https://jprs.jp/tech/security/2022-09-22-bind9-vuln-eddsa.html> 	EdDSA検証時 のメモリアリーク

月間の脆弱性情報数の最高記録を更新 (2022年9月、6件)

脆弱性情報 (BIND) [2/2]

公開日	タイトル・URL	概要
2023/1/26	<ul style="list-style-type: none"> ■ (緊急) BIND 9.xの脆弱性 (DNSサービスの停止) について (CVE-2022-3924) <https://jprs.jp/tech/security/2023-01-26-bind9-vuln-serve-stale-softquota.html> 	serve-staleの実装不具合
2023/1/26	<ul style="list-style-type: none"> ■ (緊急) BIND 9.xの脆弱性 (DNSサービスの停止) について (CVE-2022-3736) <https://jprs.jp/tech/security/2023-01-26-bind9-vuln-serve-stale-rrsig.html> 	serve-staleの実装不具合
2023/1/26	<ul style="list-style-type: none"> ■ (緊急) BIND 9.xの脆弱性 (メモリ不足の発生) について (CVE-2022-3094) <https://jprs.jp/tech/security/2023-01-26-bind9-vuln-dynamic-update.html> 	dynamic updateの実装不具合
2023/6/22	<ul style="list-style-type: none"> ■ (緊急) BIND 9.xの脆弱性 (メモリ不足の発生) について (CVE-2023-2828) <https://jprs.jp/tech/security/2023-06-22-bind9-vuln-cache-cleaning.html> 	キャッシュクリーニングの実装不具合
2023/6/22	<ul style="list-style-type: none"> ■ (緊急) BIND 9.xの脆弱性 (DNSサービスの停止) について (CVE-2023-2911) <https://jprs.jp/tech/security/2023-06-22-bind9-vuln-serve-stale.html> 	serve-staleの実装不具合

「serve-staleの実装不具合」

serve-staleとは？

- RFC 8767で定義
- 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、名前解決を継続する機能**
 - デフォルトでは、1800ms待った後にstale answerを返す
- 権威DNSサーバーへのDDoS攻撃や事故などを想定
 - “stale bread is better than no bread.” (RFC 8767)
(参考訳：**賞味期限切れのパンでも、ないよりまし**)

実装が面倒で、他の機能とも衝突しやすい

ただし、現時点では
デフォルトでoff

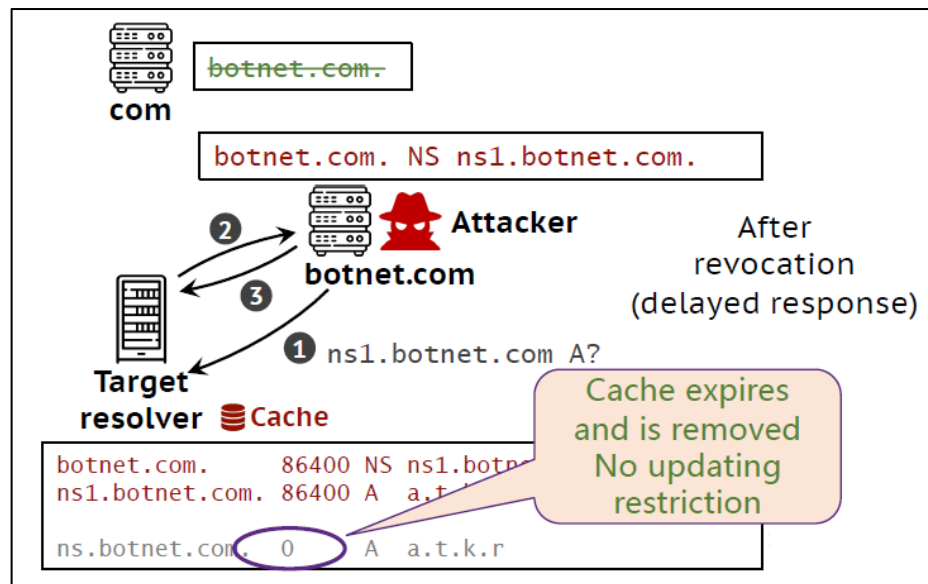
脆弱性情報（BIND以外） [1/2]

公開日	タイトル・URL	概要
2022/7/15	■ Windows DNSサーバーの脆弱性情報が公開されました（CVE-2022-30214） < https://jprs.jp/tech/security/2022-07-15-windowsdns.html >	実装の不具合によるRCE
2022/8/4	■ Unboundの脆弱性情報が公開されました（CVE-2022-30698、CVE-2022-30699） < https://jprs.jp/tech/security/2022-08-04-unbound.html >	Phoenix Domain脆弱性
2022/8/26	■ PowerDNS Recursorの脆弱性情報が公開されました（CVE-2022-37428） < https://jprs.jp/tech/security/2022-08-26-powerdns-recursor.html >	protobufログインの実装不具合
2022/9/16	■ Windows DNSサーバーの脆弱性情報が公開されました（CVE-2022-34724） < https://jprs.jp/tech/security/2022-09-16-windowsdns.html >	実装の不具合によるDoS
2022/9/27	■ Knot Resolverの脆弱性情報が公開されました（CVE-2022-40188） < https://jprs.jp/tech/security/2022-09-27-knotresolver.html >	実装の不具合によるDoS
2023/1/25	■ PowerDNS Recursorの脆弱性情報が公開されました（CVE-2023-22617） < https://jprs.jp/tech/security/2023-01-25-powerdns-recursor.html >	実装の不具合によるDoS

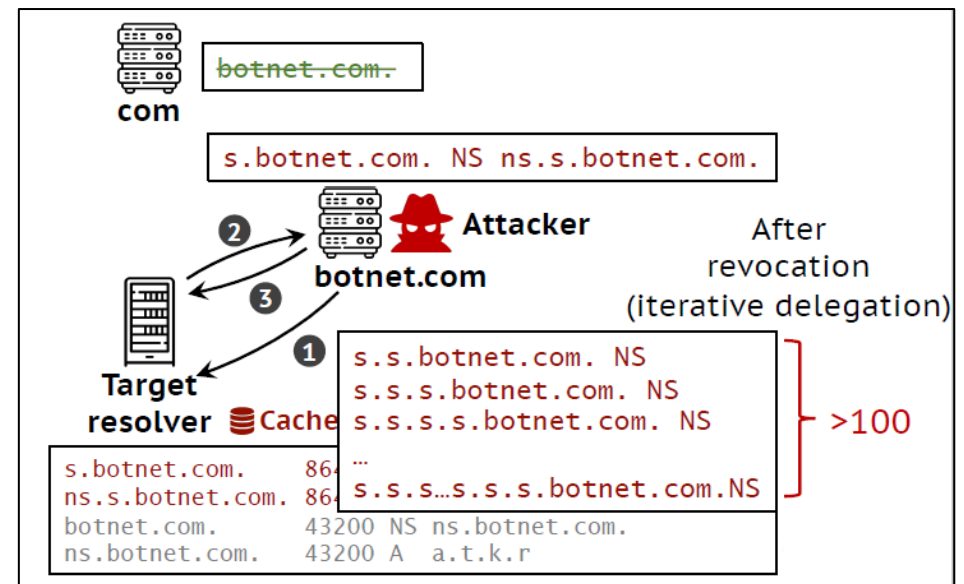
Phoenix Domain脆弱性

Phoenix Domain脆弱性とは？

- 2023年3月に発表された、**幽霊ドメイン名脆弱性の変種**
 - 二つの方法で、幽霊ドメイン名脆弱性を発生させる



方法1：キャッシュが満了するタイミングを狙う



方法2：子ゾーンの名前を延々と問い合わせ続ける

引用元：<<https://lixiang521.com/publication/ndss23/ndss23-li-phoenix-slides.pdf>>


脆弱性情報（BIND以外） [2/2]

公開日	タイトル・URL	原因
2023/1/25	■ PowerDNS Recursorの脆弱性情報が公開されました（CVE-2023-22617） < https://jprs.jp/tech/security/2023-01-25-powerdns-recursor.html >	実装の不具合によるDoS
2023/2/3	■ Knot Resolverの脆弱性情報が公開されました < https://jprs.jp/tech/security/2023-02-03-knotresolver.html >	特定のケースでの過剰なTCP再接続を回避
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） < https://jprs.jp/tech/security/2023-03-17-windowsdns.html >	実装の不具合によるRCE
2023/4/3	■ PowerDNS Recursorの脆弱性情報が公開されました（CVE-2023-26437） < https://jprs.jp/tech/security/2023-04-03-powerdns-recursor.html >	実装の不具合によるDoS
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） < https://jprs.jp/tech/security/2023-04-14-windowsdns.html >	RCE9件 、 情報漏えい1件
2023/6/16	■ Windows DNSの脆弱性情報が公開されました（CVE-2023-32020） < https://jprs.jp/tech/security/2023-06-16-windowsdns.html >	実装の不具合によるDNSスプーフィング脆弱性

「他9件」 「RCE9件」

MS月例セキュリティ更新プログラムでの 大量報告（2023年4月）

- **RCE9件、情報漏えい1件**
- 発見者は同じ人
 - George Hughey氏、MSRC勤務
- 2021年7月・2022年4月にも
同様の事例あり
 - 同じ人による大量のRCE脆弱性
報告

 **George Hughey**
@ecthr0s

Yesterday's Patch Tuesday saw the release of 10 CVEs I found in DNS! These could potentially allow an authenticated attacker to gain remote code execution. A huge thank you to the DNS team who worked through and fixed these.

msrc.microsoft.com/update-guide/v...

ツイートを翻訳

Microsoft Windows DNS	CVE-2023-28256	Windows DNS Server Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28278	Windows DNS Server Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28307	Windows DNS Server Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28306	Windows DNS Server Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28223	Windows Domain Name Service Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28254	Windows DNS Server Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28305	Windows DNS Server Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28308	Windows DNS Server Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28255	Windows DNS Server Remote Code Execution Vulnerability	Important
Microsoft Windows DNS	CVE-2023-28277	Windows DNS Server Information Disclosure Vulnerability	Important

午前2:26 · 2023年4月13日 · 2.4万 件の表示

引用元：<<https://twitter.com/ecthr0s/status/1646203249895284737>>

解説動画（Internet Week Basicオンデマンド）

● DNSを学べる解説動画を公開

- 1時間で学び直すDNSの仕組みのキホン（2022年11月）
- DNSに対するサイバー攻撃とその対策（理論編）（2023年2月）
- DNSに対するサイバー攻撃とその対策（実践編）（2023年2月）

Internet Week Basicオンデマンド - JPNIC

<<https://www.nic.ad.jp/ja/materials/iw/ondemand/>>

1時間で学び直すDNSの仕組みのキホン【Internet Week Basic オンデマンド】

まとめ：DNSの役割

- DNSの役割は、大きく二つに分けられる
 - ① 名前と対象（IPアドレスなど）を、あらかじめ対応付けておく
 - ② 名前と対象の対応付けを調べて、問い合わせ先に返す
- DNSを理解するためには、二つの役割を区別して理解することが重要
- パート2では、①と②を実現するためのDNSの構成要素と、分散管理の仕組みについて解説する

Copyright © 2022 株式会社日本レジストリサービス

8:39 / 1:00:24 ・ DNSの役割 > スクロールして詳細を表示

DNSに対するサイバー攻撃とその対策（理論編）【Internet Week Basic オンデマンド】

理論編のまとめ

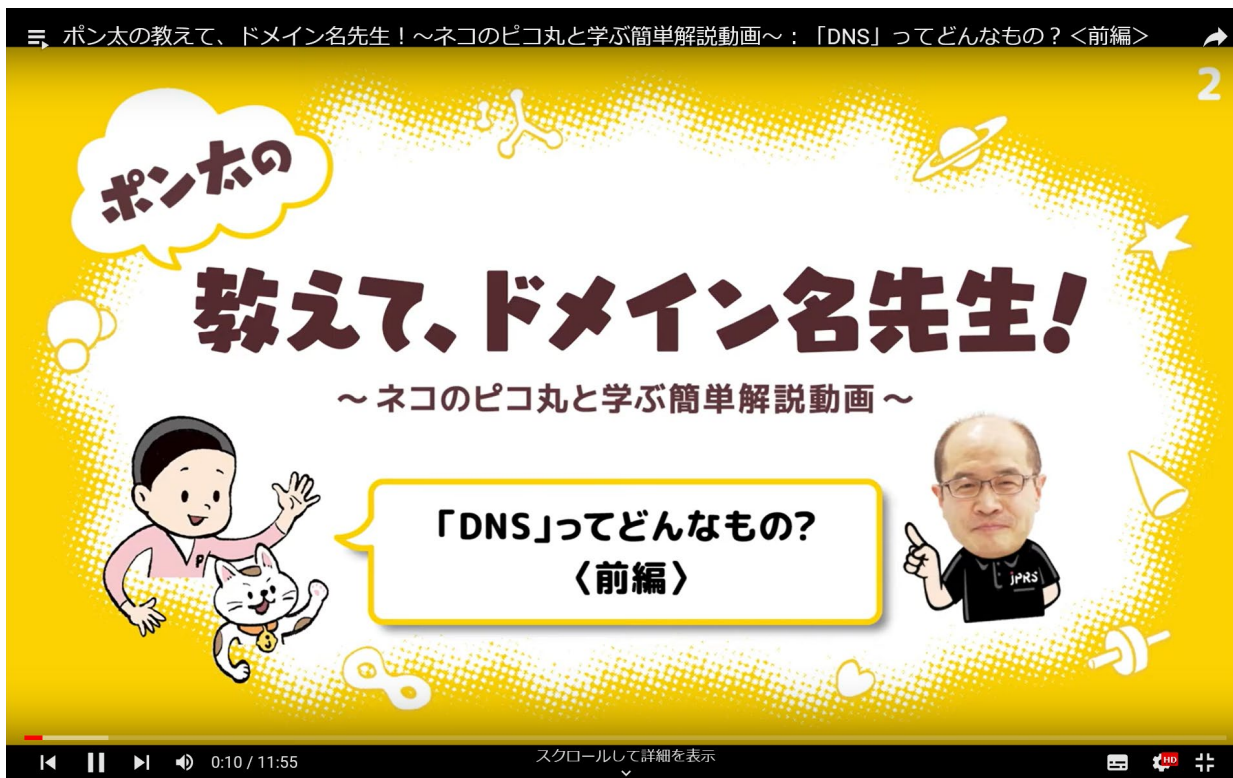
- この動画では「DNSに対するサイバー攻撃とその対策（理論編）」と題し、攻撃対象と攻撃手法・守る対象と対策の効果に注目して、攻撃を6種類、対策を4種類に分類しました。
- その上で、DNSの構成要素が攻撃を受け、サービスに影響が及んだ場合の影響範囲を整理し、DNSが備える特性が攻撃に及ぼす影響について解説しました。
- 実践編では、DNSに対する代表的な攻撃手法とその対策の概要について、理論編で解説した分類と影響範囲を踏まえた形で解説します。

Copyright © 2023 株式会社日本レジストリサービス

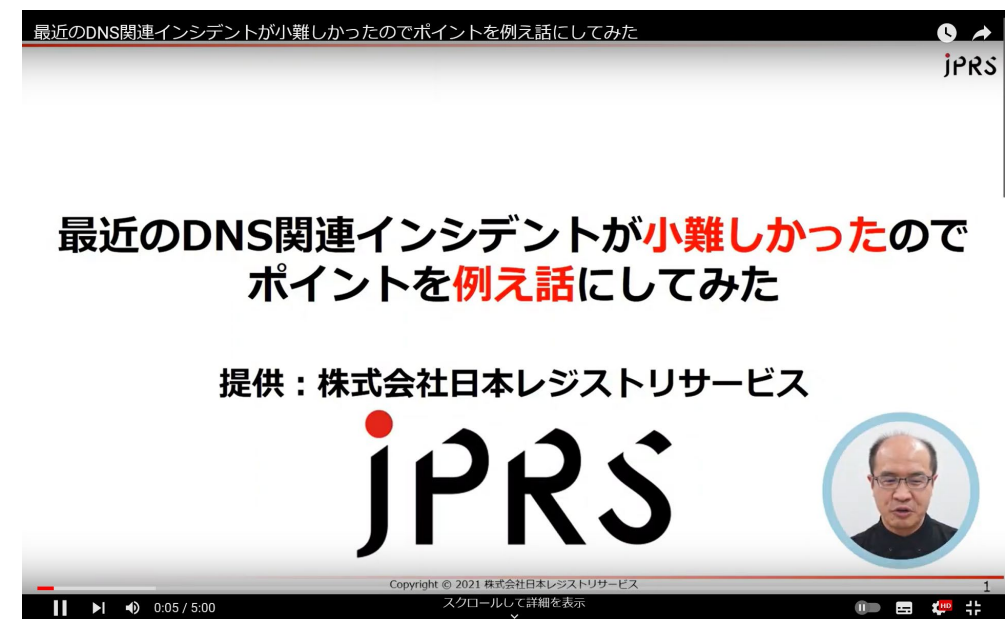
32:14 / 33:55 ・ 理論編のまとめ > スクロールして詳細を表示

解説動画（YouTube公式チャンネル）

- ポン太のインターネット教室でおなじみの「**教えて、ドメイン名先生！**」シリーズや、**JANOG Meeting**の**休憩時間動画**を公開



JPRSpres - YouTube
<<https://www.youtube.com/user/JPRSpres>>



予告：b.root-servers.net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る予定

ルートサーバーのIPアドレス変更は2017年10月24日以来、6年ぶり

- IPアドレスの変更後、フルリゾルバー（キャッシュDNSサーバー）において、ルートヒントの更新作業が必要になる

重要：あわてて更新する必要はありません！

- 主なDNSソフトウェア・ディストリビューション・パッケージではバージョンアップや脆弱性対応の際に、**ルートヒントも併せて更新される**
- かつ、少なくとも1年間は現在のIPアドレスでサービスが継続されるため、**手動で更新する場合もゆっくりやればよい**
- 権威DNSサーバーでは、**何もする必要はない**

**JPRSではB-RootのIPアドレス変更を確認後、
改めてお知らせする予定です**

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！

jPRS

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



@JPRS_official



JPRSofficial



JPRSpress