

JPRSの技術情報発信（2019年7月～2020年6月）

2020年6月26日

DNS Summer Day 2020

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」が4刷に！

- 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）**

ご購入、ありがとうございます！



JPRSの技術情報発信

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。

- Web
 - 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/>>
 - 技術解説「JPRS トピックス & コラム」 <<https://jprs.jp/related-info/guide/>>
 - メディアへの寄稿
- 電子メール
 - メールマガジン「FROM JPRS」（登録は <<https://jprs.jp/mail/>> から）
 - 技術コミュニティのメーリングリストにおける情報提供
- SNS公式アカウント（[Twitter](#)、[Facebook](#)）
- カンファレンス・イベントなどにおける発表、ブース出展

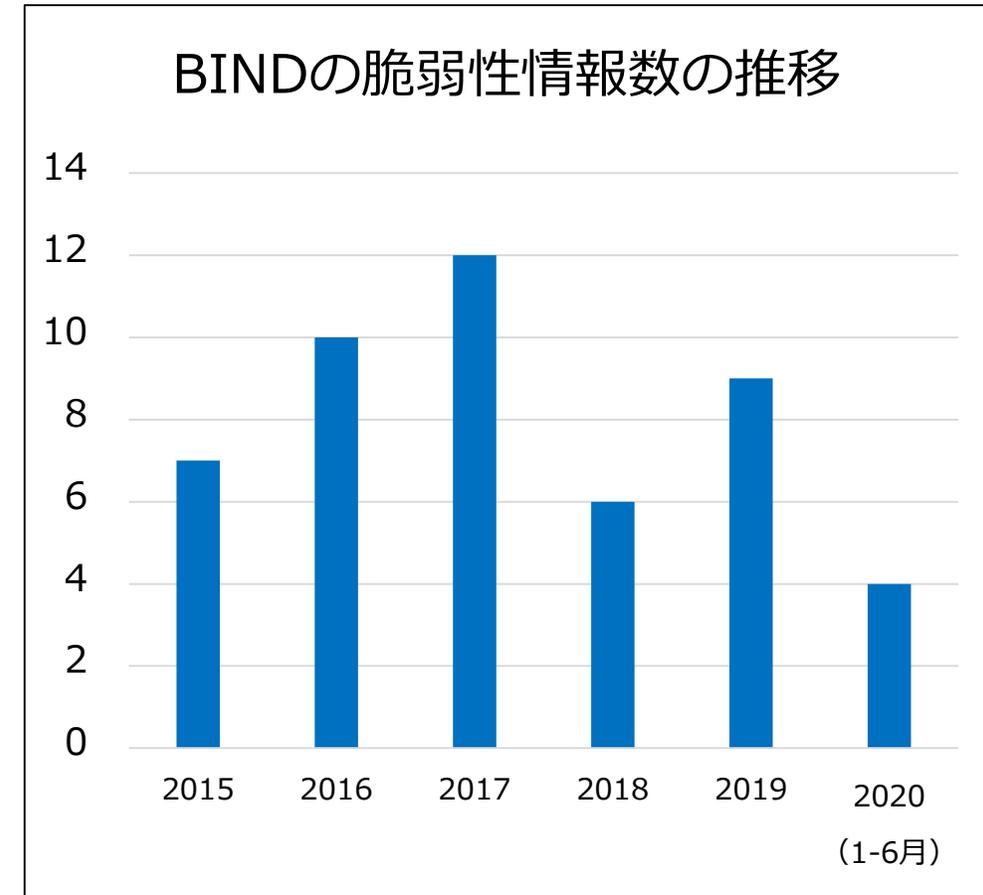
本日より紹介する技術情報発信

- 脆弱性情報 (19件)
 - BIND (7件)
 - BIND以外のDNS実装 (12件)
- NXNSAttackに関する情報発信
- DNS関連RFCの日本語訳公開

(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 (7件 (緊急3件))
 - 2019年7月～12月：3件 (前年同期：2件)
 - 2020年1月～6月：4件 (前年同期：6件)
- BIND以外のDNS実装 (12件)
 - NSD (1件)
 - Unbound (3件)
 - PowerDNS Authoritative Server (1件)
 - PowerDNS Recursor (1件)
 - Knot Resolver (3件)
 - Windows DNS (3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	対象
2019/10/17	■ BIND 9.xの脆弱性 (DNSサービスの停止) について (CVE-2019-6476) < https://jprs.jp/tech/security/2019-10-17-bind9-vuln-qname-minimisation.html >	9.14.0-9.14.6
2019/10/17	■ BIND 9.xの脆弱性 (mirror zones機能におけるDNSSEC検証のバイパス) について (CVE-2019-6475) < https://jprs.jp/tech/security/2019-10-17-bind9-vuln-mirror-zones.html >	9.14.0-9.14.6
2019/11/21	■ (緊急) BIND 9.xの脆弱性 (システムリソースの過度な消費) について (CVE-2019-6477) < https://jprs.jp/tech/security/2019-11-21-bind9-vuln-tcp-pipelining.html >	9.14.1-9.14.7 9.12.4-P1-9.12.4-P2 9.11.6-P1-9.11.12

- CVE-2019-6477 : CVE-2018-5743対応に伴う不具合
 - 2019年4月に公開されたCVE-2018-5743への対応により、TCP同時接続数の制限がバイパスされてしまう不具合が発生したものの

ISCのセキュリティポリシー変更 (2019年10月)

- 2019年10月のセキュリティポリシー変更

ISC Security Vulnerability Policy Updated
<<https://www.isc.org/blogs/vulnerability-policyupdate/>>

- “Beginning this year, **to the extent possible** we will avoid scheduling disclosure of non-emergency security issues during the period beginning November 1 and ending December 31.”
 - 訳：「今年から、11月1日から12月31日までの期間に緊急でないセキュリティ問題の開示をスケジュールすることを、**可能な限り回避する**」
- このアナウンスの後、CVE-2019-6477が**2019年11月20日**に公開
 - JPRSでも、2019年11月21日に脆弱性情報を公開

脆弱性情報 (BIND) [2/2]

公開日	タイトル・URL	対象
2020/5/20	■ (緊急) BIND 9.xの脆弱性 (パフォーマンスの低下・リフレクション攻撃の踏み台化) について (CVE-2020-8616) https://jprs.jp/tech/security/2020-05-20-bind9-vuln-processing-referrals.html	9.0.0-9.16.2 ※全バージョン
2020/5/20	■ (緊急) BIND 9.xの脆弱性 (DNSサービスの停止・異常な動作) について (CVE-2020-8617) https://jprs.jp/tech/security/2020-05-20-bind9-vuln-tsig.html	9.0.0-9.16.2 ※全バージョン
2020/6/18	■ BIND 9.xの脆弱性 (DNSサービスの停止) について (CVE-2020-8618) https://jprs.jp/tech/security/2020-06-18-bind9-vuln-zone-transfer.html	9.16.0-9.16.3
2020/6/18	■ BIND 9.xの脆弱性 (DNSサービスの停止) について (CVE-2020-8619) https://jprs.jp/tech/security/2020-06-18-bind9-vuln-asterisk.html	9.16.0-9.16.3 9.14.9-9.14.12 9.11.14- 9.11.19

- CVE-2020-8616 : NXNSAttack
- CVE-2020-8617 : TSIGに関する実装上の不具合
 - TSIGを明示的に設定していない場合も対象

ISCのセキュリティポリシー変更 (2020年5月) [1/2]

- 2020年5月のセキュリティポリシー変更

Update to ISC's Security Policy

<<https://www.isc.org/blogs/security-policy-update/>>

- “we here at ISC have decided to amend our security policy to allow, **at our discretion**, limited pre-announcement of pending security vulnerability disclosures.”
 - 訳：「私たちISCは、**私たちの裁量で**、保留中のセキュリティ脆弱性開示の限られた事前アナウンスを許可するようにセキュリティポリシーを修正することを決定した」
- 2020年5月は事前アナウンスあり、2020年6月は事前アナウンスなし
 - 事前アナウンスの基準は？

ISCのセキュリティポリシー変更 (2020年5月) [2/2]

ISC Software Defect and Security Vulnerability Disclosure Policy
<<https://kb.isc.org/docs/aa-00861>>

- “When ISC at our own discretion believe that **the issue could have a significant impact on many or all users of the Software**, we may notify the product-specific announcement”
 - 訳：「問題がそのソフトウェアの多く、またはすべてのユーザーに重大な影響を与える可能性がある」と判断した場合」
- 要は「ほっとくとやばいやつ」

脆弱性情報 (BIND以外) [1/2]

公開日	タイトル・URL
2019/7/12	<p>■ Knot Resolverの脆弱性情報が公開されました (CVE-2019-10190、CVE-2019-10191)</p> <p><https://jprs.jp/tech/security/2019-07-12-knotresolver.html></p>
2019/7/12	<p>■ Windows DNS Serverの脆弱性情報が公開されました (CVE-2019-0811)</p> <p><https://jprs.jp/tech/security/2019-07-12-windowsdnserver.html></p>
2019/7/12	<p>■ Windows DNSキャッシュリゾルバーサービスの脆弱性情報が公開されました (CVE-2019-1090)</p> <p><https://jprs.jp/tech/security/2019-07-12-windowsdnrsrvr.html></p>
2019/8/8	<p>■ PowerDNS Authoritative Serverの脆弱性情報が公開されました (CVE-2019-10203)</p> <p><https://jprs.jp/tech/security/2019-08-06-powerdns-auth.html></p>
2019/8/22	<p>■ NSDの脆弱性情報が公開されました (CVE-2019-13207)</p> <p><https://jprs.jp/tech/security/2019-08-22-nsd.html></p>
2019/10/4	<p>■ Unboundの脆弱性情報が公開されました (CVE-2019-16866)</p> <p><https://jprs.jp/tech/security/2019-10-04-unbound.html></p>

脆弱性情報 (BIND以外) [2/2]

公開日	タイトル・URL
2019/11/20	■ Unboundの脆弱性情報が公開されました (CVE-2019-18934) < https://jprs.jp/tech/security/2019-11-20-unbound.html >
2019/12/6	■ Knot Resolverの脆弱性情報が公開されました (CVE-2019-19331) < https://jprs.jp/tech/security/2019-12-06-knotresolver.html >
2020/4/17	■ Windows DNSの脆弱性情報が公開されました (CVE-2020-0993) < https://jprs.jp/tech/security/2020-04-17-windowsdns.html >
2020/5/21	■ Unboundの脆弱性情報が公開されました (CVE-2020-12662 、CVE-2020-12663) < https://jprs.jp/tech/security/2020-05-21-unbound.html >
2020/5/21	■ PowerDNS Recursorの脆弱性情報が公開されました (CVE-2020-10995 、CVE-2020-12244、CVE-2020-10030) < https://jprs.jp/tech/security/2020-05-21-powerdns-recursor.html >
2020/5/21	■ Knot Resolverの脆弱性情報が公開されました (CVE-2020-12667) < https://jprs.jp/tech/security/2020-05-21-knotresolver.html >

- CVE-2020-12662、CVE-2020-10995、CVE-2020-12667はいずれも、NXNSAttackに関するもの

NXNSAttackに関する情報発信

- 2020年5月19日：論文・脆弱性情報が関係者から一斉公開
- 2020年5月20～21日：JPRSから各DNS実装の脆弱性情報を公開
 - 5月20日：BIND
 - 5月21日：Unbound・PowerDNS Recursor・Knot Resolver
- 2020年5月22日：JPRS用語辞典に「NXNSAttack」掲載

JPRS用語辞典 | NXNSAttack (エヌエックスエヌエスアタック)
<<https://jprs.jp/glossary/index.php?ID=0262>>

- 2020年6月5日：Internet Watchに寄稿原稿掲載

名前解決の仕組みを使ってDNSを攻撃、「NXNSAttack」とは
<<https://internet.watch.impress.co.jp/docs/news/1257030.html>>

- 2020年6月26日：DNS Summer Day 2020でJPRS阿波連が発表

DNS関連RFCの日本語訳公開

- インターネットコミュニティへの貢献・DNSに関する理解の促進のため、DNS関連のRFCを日本語に翻訳・公開

JPRS DNS 関連技術情報 - DNS関連のRFC
<<https://jprs.jp/tech/index.html#dns-rfc-info>>

- 現在、54本のRFCを公開中

期間中に新規公開したRFC

- JPRS社員が共著者となっているRFC：4本
 - RFC 4074、RFC 7719、RFC 8499（公開日：2020年3月27日）
 - RFC 8198（公開日：2020年3月31日）
- その他のDNS関連RFC：14本
 - RFC 2181、RFC 2308（公開日：2020年3月31日）
 - RFC 5625、RFC 6891、RFC 8020（公開日：2020年4月8日）
 - RFC 1122、RFC 1123、RFC 5452（公開日：2020年4月17日）
 - RFC 6840、RFC 6895、RFC 7129（公開日：2020年4月24日）
 - RFC 1034、RFC 1035、RFC 3901（公開日：2020年5月15日）

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](https://twitter.com/JPRS_official)



[JPRSofficial](https://www.facebook.com/JPRSofficial)