JPRSの技術情報発信（2020年7月～2021年6月）

2021年6月25日

DNS Summer Day 2021

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！

- **5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）**
- 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/>

5刷での変更点

1. 新gTLDの追加募集に関する状況の変化を反映
2. DMARCのサンプルを追加
3. DNSVizのURIを変更（http → https）
4. 引用先の記述更新（IPv6逆引きに関するG Suiteのヘルプ）を反映
5. BIND 9.14.0でQNAME minimisationが標準になったことを反映
6. DMARC、TSIGに関する付録A（DNS関連のRFC）の更新
7. 索引にDMARCを追加

『DNSがよくわかる教科書』第5刷での変更点について
<https://www.sbcr.jp/support/4815607374/>

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、YouTube）
- カンファレンス・イベントなどにおける発表・ブース出展

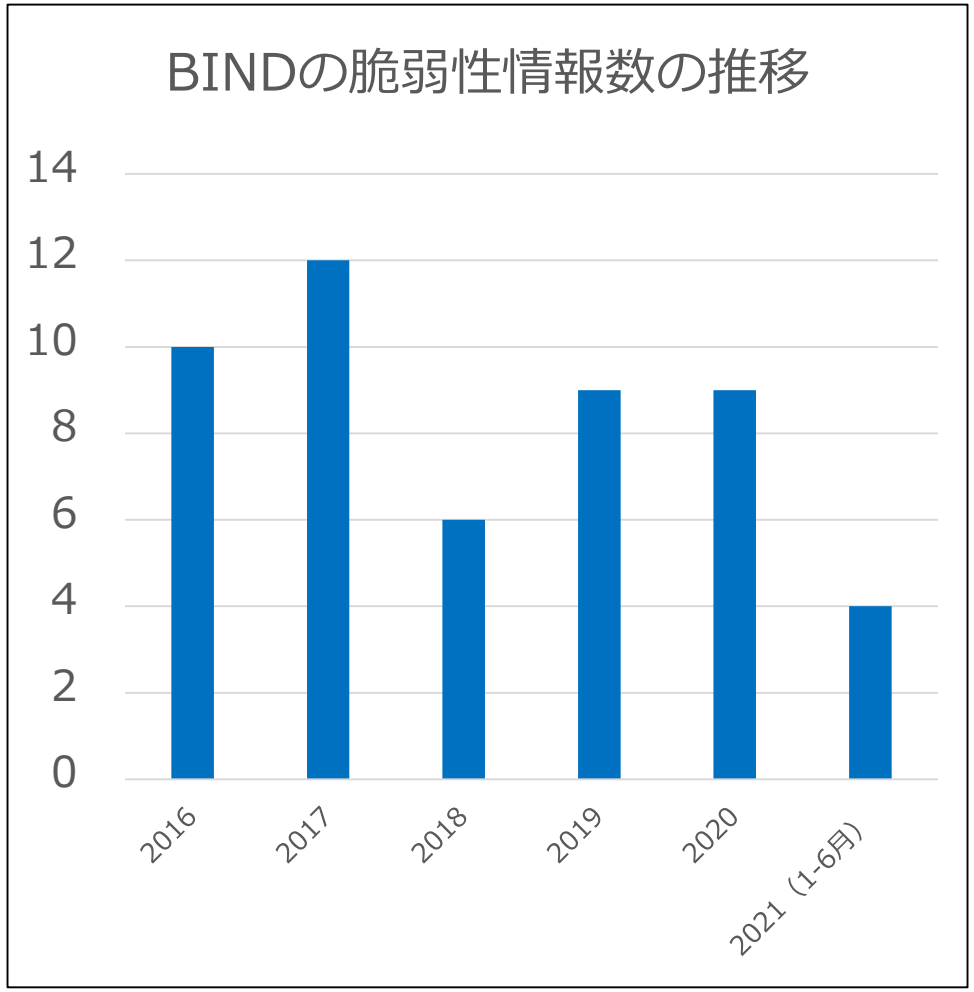
本日ご紹介する技術情報発信

1. 脆弱性情報
   - BIND（9件）
   - BIND以外のDNS実装（16件）
2. 攻撃手法・イベント・インシデントに関する技術情報
   - サブドメインテイクオーバー
   - DNS flag day 2020
   - SAD DNS・DNSpooq・tsuNAME

（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（9件（緊急3件））
  - 2020年7月～12月：5件（前年同期：3件）
  - 2021年1月～6月：4件（前年同期：4件）
- BIND以外のDNS実装（16件）
  - NSD（1件）
  - Unbound（1件）
  - PowerDNS Authoritative Server（2件）
  - PowerDNS Recursor（2件）
  - Knot Resolver（1件）
  - Windows DNS（9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
2020/8/21	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8620）<https://jprs.jp/tech/security/2020-08-21-bind9-vuln-libuv.html>	9.16.0以降
2020/8/21	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8621）<https://jprs.jp/tech/security/2020-08-21-bind9-vuln-forwarding.html>	9.14.0以降
2020/8/21	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8622）<https://jprs.jp/tech/security/2020-08-21-bind9-vuln-tsig.html>	9.0.0以降 ※全バージョン
2020/8/21	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8623）<https://jprs.jp/tech/security/2020-08-21-bind9-vuln-pkcs11.html>	9.10.0以降
2020/8/21	■BIND 9.xの脆弱性（サービス提供者が意図しないDynamic Updateの許可）について（CVE-2020-8624）<https://jprs.jp/tech/security/2020-08-21-bind9-vuln-updatepolicy.html>	9.9.12以降

- 2020年8月の定期リリースで、5件の脆弱性が公開
  - 一度に公開された数としては史上最多
  - ISCから予告あり

脆弱性情報（BIND）[2/2]

公開日	タイトル・URL	対象
2021/2/18	■（緊急）BIND 9.xの脆弱性（DNSサービスの停止・**リモートコード実行**） について（CVE-2020-8625）<https://jprs.jp/tech/security/2021-02-18-bind9-vuln-gsstsig.html>	9.5.0以降
2021/4/30	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2021-25214）<https://jprs.jp/tech/security/2021-04-30-bind9-vuln-ixfr.html>	9.8.5/9.9.3以降
2021/4/30	■（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2021-25215）<https://jprs.jp/tech/security/2021-04-30-bind9-vuln-dname.html>	9.0.0以降 ※全バージョン
2021/4/30	■（緊急）BIND 9.xの脆弱性（DNSサービスの停止・**リモートコード実行**） について（CVE-2021-25216）<https://jprs.jp/tech/security/2021-04-30-bind9-vuln-gsstsig.html>	9.5.0以降

- CVE-2020-8625とCVE-2021-25216は共に、GSS-TSIGのSPNEGO実装のバグに起因する脆弱性（有効に設定されている場合のみ対象）
  - 32ビットアーキテクチャではリモートコード実行（RCE）が可能
  - CVE-2021-25216の公開後、ISCはSPNEGOの実装をBINDから削除

2021年4月の脆弱性情報公開について

- ISCは当初、2021年4月21日の公開を事前アナウンス
  - 日本時間では2021年4月22日
- 脆弱性の修正に時間を要したため、公開を1週間延期
  - 日本時間では2021年4月29日（祝日）
- 脆弱性情報の内容・緊急度に基づき、JPRSで取り扱いを検討
  - 検討の結果、翌営業日である2021年4月30日に脆弱性情報を公開

参考：休日に脆弱性情報を公開した事例

- 2013年7月27日（土）に脆弱性情報を緊急公開

> ■（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2013-4854）
> <https://jprs.jp/tech/security/2013-07-27-bind9-vuln-malformed-rdata.html>

- 「BINDコロリ（①～④）」+ゼロデイ（⑤）の合わせ技

> ① リモートからのDNS問い合わせ一発でnamedを落とせる
> ② 多くのバージョンのBINDが対象となる
> ③ 権威DNSサーバー・フルリゾルバーの双方が対象となる
> ④ namedの設定やオプションでは回避できない
> ⑤ 脆弱性を悪用した攻撃事例が観測され、**ISCの公開日が前倒し**された

脆弱性情報（BIND以外）[1/3]

公開日	タイトル・URL
2020/7/7	■PowerDNS Recursorの脆弱性情報が公開されました（CVE-2020-14196）<https://jprs.jp/tech/security/2020-07-07-powerdns-recursor.html>
2020/7/16	■**Windows DNS** Serverの脆弱性情報が公開されました（CVE-2020-1350）<https://jprs.jp/tech/security/2020-07-16-windowsdns.html>
2020/8/14	■**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-2020-1584）<https://jprs.jp/tech/security/2020-08-14-windowsdnsrslvr.html>
2020/9/17	■**Windows DNS**の脆弱性情報が公開されました（CVE-2020-0836、CVE-2020-1228）<https://jprs.jp/tech/security/2020-09-17-windowsdns.html>
2020/9/17	■**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-2020-0839）<https://jprs.jp/tech/security/2020-09-17-windowsdnsrslvr.html>
2020/9/25	■PowerDNS Authoritative Serverの脆弱性情報が公開されました （CVE-2020-17482）<https://jprs.jp/tech/security/2020-09-25-powerdns-auth-leaking.html>
2020/9/25	■PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2020-24696、CVE-2020-24697、CVE-2020-24698）<https://jprs.jp/tech/security/2020-09-25-powerdns-auth-gss-tsig.html>

脆弱性情報（BIND以外）[2/3]

公開日	タイトル・URL
2020/10/16	■PowerDNS Recursorの脆弱性情報が公開されました（CVE-2020-25829）<https://jprs.jp/tech/security/2020-10-16-powerdns-recursor.html>
2020/12/3	■NSDの脆弱性情報が公開されました（CVE-2020-28935）<https://jprs.jp/tech/security/2020-12-03-nsd.html>
2020/12/8	■Unboundの脆弱性情報が公開されました（CVE-2020-28935）<https://jprs.jp/tech/security/2020-12-08-unbound.html>
2020/12/11	■**Windows DNS**に関するセキュリティアドバイザリが公開されました<https://jprs.jp/tech/security/2020-12-11-windowsdnsresolver.html>
2021/1/15	■**Windows DNS**の脆弱性情報が公開されました（CVE-2021-1637）<https://jprs.jp/tech/security/2021-01-15-windowsdns.html>
2021/2/12	■**Windows DNS**の脆弱性情報が公開されました（CVE-2021-24078）<https://jprs.jp/tech/security/2021-02-12-windowsdns.html>
2021/3/12	■**Windows DNS**サーバーの脆弱性情報が公開されました（CVE-2021-26877、CVE-2021-26893、CVE-2021-26894、CVE-2021-26895、CVE-2021-26896、CVE-2021-26897、CVE-2021-27063）<https://jprs.jp/tech/security/2021-03-12-windowsdns.html>

脆弱性情報（BIND以外）[3/3]

公開日	タイトル・URL
2021/4/16	■**Windows DNS**の脆弱性情報が公開されました（CVE-2021-28323、 CVE-2021-28328） <https://jprs.jp/tech/security/2021-04-16-windowsdns.html>
2021/5/10	■Knot Resolverの脆弱性情報が公開されました <https://jprs.jp/tech/security/2021-05-10-knotresolver.html>

- Windows DNSの脆弱性が多数報告・修正
  - Windows DNSサーバーの脆弱性に加え、キャッシュリゾルバーサービス（スタブリゾルバー）の脆弱性も報告・修正
  - スタブリゾルバーの脆弱性では、コンシューマー向けWindowsもパッチの適用が必要
    - Windows Updateで適用可能

攻撃手法・イベント・インシデントに関する技術情報

【期間中にJPRSから技術情報を発信した項目】

- サブドメインテイクオーバー
- DNS flag day 2020
- SAD DNS
- DNSpooq
- tsuNAME

サブドメインテイクオーバー

- JPRS用語辞典に解説を掲載

JPRS用語辞典｜Subdomain Takeover（サブドメインテイクオーバー）
<https://jprs.jp/glossary/index.php?ID=0267>

- 以下のカンファレンス・イベントで解説
  - Internet Week 2020（ランチタイムウェビナー）
  - JANOG47（休憩時間動画・バーチャルブース動画）
  - 第1回フィッシング対策勉強会（オンライン講演）
  - Interop 2021 Tokyo（展示ブースにおけるセミナー・動画）
    - 動画はYouTube公式チャンネルでも配信

DNS flag day 2020

- JPRS DNS関連技術情報に解説を掲載

DNS flag day 2020の実施について
<https://jprs.jp/tech/notice/2020-09-24-dns-flag-day-2020.html>

- 公式サイトが日本語に対応していたため、実施日・概要・呼びかけ対象を簡潔に記載し、公式サイトを案内

SAD DNS・DNSpooq・tsuNAME

- 情報の公開後なるべく早く、JPRS用語辞典に解説を掲載

JPRS用語辞典｜SAD DNS（サドディーエヌエス）
<https://jprs.jp/glossary/index.php?ID=0270>

JPRS用語辞典｜DNSpooq（ディーエヌエススプーク）
<https://jprs.jp/glossary/index.php?ID=0273>

JPRS用語辞典｜tsuNAME（ツネーム）
<https://jprs.jp/glossary/index.php?ID=0275>

- DNSpooqはさまざまな機器が対象となるため、DNS関連技術情報にも掲載

dnsmasqにおける「DNSpooq」脆弱性の公開について
- バージョンアップ・ファームウェアの更新など、適切な対応を強く推奨 -
<https://jprs.jp/tech/security/2021-01-25-dnspooq.html>

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