DNS界のできごと（2018年7月～2019年6月）
- JPRSが発信した技術情報から -

2019年6月28日

DNS Summer Day 2019

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

JPRSではインターネットの安定運用を目的として、さまざまなメディアで
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/>
- 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）
- 人（技術広報担当）
  - 各種イベント・ミーティングでの発表、ブース出展

本日紹介するDNS界のできごと

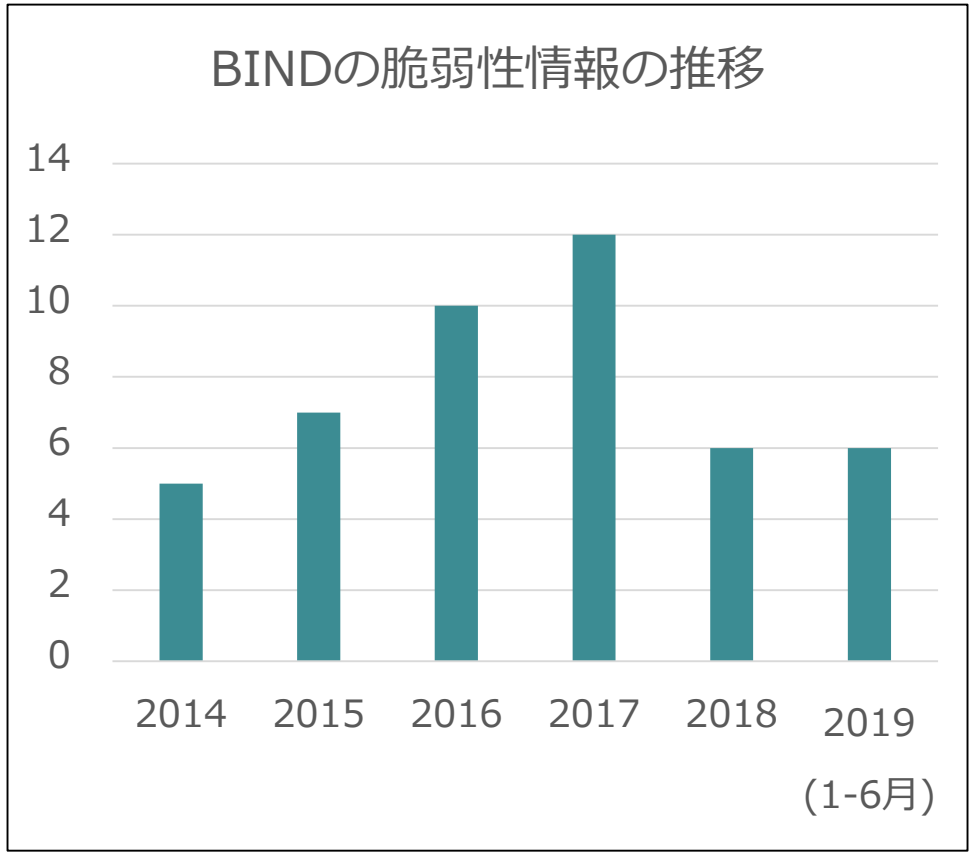
- 脆弱性情報の公開（21件）
  - BIND（8件）[*1]
  - BIND以外のDNS実装（13件）
- ルートゾーンKSKロールオーバー（新規3件、更新3件）
- DNS flag day（新規3件、更新3件）
- その他（2件）

（カッコ内はJPRSが発信した技術情報の件数）

[*1]Supported Preview Editionのみを対象とした脆弱性情報1件は含まない

脆弱性情報

- BIND（8件（緊急2件））
  - 2018年7月～12月：2件（前年同期：0件）
  - 2019年1月～6月：6件（前年同期：4件）
- BIND以外のDNS実装（13件）
  - NSD（1件）
  - PowerDNS Authoritative Server（3件）
  - PowerDNS Recursor（3件）
  - Knot DNS（1件）
  - Knot Resolver（2件）
  - Windows DNS（3件）



Knot Resolverの**重大な脆弱性**が修正（以降で説明）

脆弱性情報（BIND）[1/2]

公開日	タイトル・URL	対象
2018/8/9	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2018-5740） <https://jprs.jp/tech/security/2018-08-09-bind9-vuln-deny-answer-aliases.html>	9.12.0-9.12.2 9.11.0-9.11.4 9.10.0-9.10.8 9.9.0-9.9.13
2018/9/20	■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-2018-5741） <https://jprs.jp/tech/security/2018-09-20-bind9-vuln-krb5-subdomain.html>	9.12.0-9.12.2-P1 9.11.0-9.11.4-P1 9.0.0-9.10.8-P1
2019/2/22	■（緊急）BIND 9.xの脆弱性（メモリリークの発生）について（CVE-2018-5744） <https://jprs.jp/tech/security/2019-02-22-bind9-vuln-edns-options.html>	9.12.0-9.12.3-P1 9.11.3-9.11.5-P1 9.10.7-9.10.8-P1
2019/2/22	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2018-5745） <https://jprs.jp/tech/security/2019-02-22-bind9-vuln-managed-keys.html>	9.12.0-9.12.3-P1 9.11.0-9.11.5-P1 9.9.0-9.10.8-P1
2019/2/22	■BIND 9.xの脆弱性（アクセス制限の不具合によるゾーンデータの流出） について（CVE-2019-6465） <https://jprs.jp/tech/security/2019-02-22-bind9-vuln-dlz.html>	9.12.0-9.12.3-P2 9.11.0-9.11.5-P2 9.9.0-9.10.8-P1

脆弱性情報（BIND）[2/2]

公開日	タイトル・URL	対象
2019/4/25	**■（緊急）BIND 9.xの脆弱性（ファイル記述子の過度な消費）について（CVE-2018-5743）<https://jprs.jp/tech/security/2019-04-25-bind9-vuln-tcp-clients.html>**	9.14.0 9.12.0-9.12.4 9.11.0-9.11.6 9.9.0-9.10.8-P1
2019/4/25	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2019-6467）<https://jprs.jp/tech/security/2019-04-25-bind9-vuln-nxdomain-redirect.html>	9.14.0 9.12.0-9.12.4
2019/6/20	■BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2019-6471）<https://jprs.jp/tech/security/2019-06-20-bind9-vuln-malformed-packets.html>	9.14.0-9.14.2 9.12.0-9.12.4-P1 9.11.0-9.11.7

CVE-2018-5743（2019年4月公開）

- 設定値の制限を超えるTCP接続を受け入れてしまう不具合
  - 修正ミスによりパッチが取り下げられ、一般公開に時間を要した
  - ISCの脆弱性情報の「Document revision history」の内容と日付から、対応状況をある程度読み取れる

Document revision history:

1.0 Advance Notification, 16 January 2019
1.1 Recall due to error in original fix, 17 January 2019
1.3 Replacement fix delivered to Advance Notification customers, 15 April 2019
1.4 Corrected Versions affected and Solution, 16 April 2019
1.5 Added reference to BIND 9.11.6-S1
2.0 Public disclosure, 24 April 2019

修正ミスによりパッチを取り下げ

差し替え版のパッチを事前配布

事前通知から一般公開まで3カ月以上

脆弱性情報（BIND以外）[1/2]

公開日	タイトル・URL	対象
2018/7/5	■Knot Resolverの脆弱性情報が公開されました <https://jprs.jp/tech/security/2018-07-05-knotresolver.html>	2.3.0及びそれ以前
2018/7/12	■Windows DNSの脆弱性情報が公開されました（CVE-2018-8304） <https://jprs.jp/tech/security/2018-07-12-windowsdnsapi.html>	2018年7月以前にリリースされたWindows DNSAPI
2018/8/1	■NSDの脆弱性情報が公開されました <https://jprs.jp/tech/security/2018-08-01-nsd.html>	2.2.0-4.1.22
2018/8/6	**■Knot Resolverの脆弱性情報が公開されました（CVE-2018-10920） <https://jprs.jp/tech/security/2018-08-06-knotresolver.html>**	2.4.0及びそれ以前
2018/8/8	■Knot DNSの脆弱性情報が公開されました <https://jprs.jp/tech/security/2018-08-08-knotdns.html>	2.6.9及びそれ以前
2018/10/11	■Windows DNSの脆弱性情報が公開されました（CVE-2018-8320） <https://jprs.jp/tech/security/2018-10-11-windowsdns.html>	2018年10月以前にリリースされたWindows DNS
2018/11/8	■PowerDNS Recursorの脆弱性情報が公開されました （CVE-2018-10851、CVE-2018-14626、CVE-2018-14644） <https://jprs.jp/tech/security/2018-11-08-powerdns-recursor.html>	3.2-4.1.4 (CVE-2018-10851) 4.0.0-4.1.4 (CVE-2018-14626、 CVE-2018-14644)

CVE-2018-10920（2018年8月公開）

- Knot Resolverの重大な脆弱性
  - 不適切なCNAME応答の受け入れ
    - **[ある文字列].*TLD*の権限があれば、**
      [任意の文字列].*TLD*に対するキャッシュポイズニングが可能[*1]

[*1]layer/iterate: fix cache injection via CNAME · CZ-NIC/knot-resolver@d2dd680 · GitHub <https://github.com/CZ-NIC/knot-resolver/commit/d2dd680d54c1753c1ad1f973be733d879cea1a73>

- PoCが公開済
  - 2.4.1以降（最新は4.0.0）への更新必須

脆弱性情報（BIND以外）[2/2]

公開日	タイトル・URL	対象
2018/11/8	■PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2018-10851、CVE-2018-14626）<https://jprs.jp/tech/security/2018-11-08-powerdns-auth.html>	3.3.0-4.1.4 (CVE-2018-10851) 4.1.0-4.1.4 (CVE-2018-14626)
2018/11/28	■PowerDNS Recursorの脆弱性情報が公開されました（CVE-2018-16855）<https://jprs.jp/tech/security/2018-11-28-powerdns-recursor.html>	4.1.0-4.1.7
2018/12/13	■Windows DNS Serverの脆弱性情報が公開されました（CVE-2018-8626）<https://jprs.jp/tech/security/2018-12-13-windowsdnsserver.html>	2018年12月以前にリリースされたWindows DNS
2019/1/23	■PowerDNS Recursorの脆弱性情報が公開されました（CVE-2019-3806、CVE-2019-3807）<https://jprs.jp/tech/security/2019-01-23-powerdns-recursor.html>	4.1.4-4.1.8 (CVE-2019-3806) 4.1.0-4.1.8 (CVE-2019-3807)
2019/3/20	■PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2019-3871）<https://jprs.jp/tech/security/2019-03-20-powerdns.html>	4.1.6及びそれ以前
2019/6/24	■PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2019-10162、CVE-2019-10163）<https://jprs.jp/tech/security/2019-06-24-powerdns-auth.html>	4.1.9及びそれ以前 (CVE-2019-10162) 4.1.8及びそれ以前 (CVE-2019-10163)

ルートゾーンKSKロールオーバー

公開・更新日	タイトル・URL
2018/9/19	■ICANNが新KSKでの署名開始の日程を決定 <https://jprs.jp/tech/notice/2018-09-19-rootzonekskrollover-update.html>
2018/10/25	■ICANNが新KSKへの切り替え成功と、今後の予定を発表 <https://jprs.jp/tech/notice/2018-10-25-rootzonekskrollover-update.html>
2018/10/4、2018/10/25、2019/1/16（更新）	■ルートゾーンKSKロールオーバーによる影響とその確認方法について <https://jprs.jp/tech/notice/2017-07-10-root-zone-ksk-rollover.html>
2018/10/4、2018/10/25、2019/1/16（更新）	■ルートゾーンKSKロールオーバーの概要と影響の確認方法 <https://jprs.jp/tech/notice/2017-07-10-root-zone-ksk-rollover.pdf>
2018/10/4、2019/1/16（更新）	■ルートゾーンKSKロールオーバーについてのご質問とその回答 <https://jprs.jp/tech/notice/2017-08-10-root-zone-ksk-rollover-qa.html>
2019/3/8	■ICANNがルートゾーンKSKロールオーバーの全体状況をまとめた文書を公開 <https://jprs.jp/tech/notice/2019-03-08-rootzonekskrollover-review.html>

- 初めてのルートゾーンKSKロールオーバーは無事に完了

DNS flag day

公開・更新日	タイトル・URL
2019/1/21、 2019/1/28（更新）	■DNS flag dayに関する文書の公開と対応状況の確認について <https://jprs.jp/tech/notice/2019-01-21-dns-flag-day.html>
2019/1/21、 2019/1/28（更新）	■DNS flag dayの概要・影響と対応状況の確認方法 <https://jprs.jp/tech/notice/2019-01-21-dns-flag-day.pdf>
2019/1/21、 2019/1/28（更新）	■DNS flag dayについてのご質問とその回答 <https://jprs.jp/tech/notice/2019-01-21-dns-flag-day-qa.html>

- “The 2019 DNS flag day was a very successful event.”（公式サイトより）
  - 「2019年のDNS flag dayはとてもうまくいったイベントだった」

それって本当？

- 現在、DNSからのIPフラグメンテーションの排除を主な目的とした「**DNS flag day 2020**」が計画中
  - 正確な日付は未定（is not yet determined）

- BINDは9.14.0から
- Unboundは1.9.0から

その他の注意喚起・技術情報

- BINDの不具合に関する注意喚起
  - 巨大なゾーンデータのゾーン転送により引き起こされる不具合について

公開・更新日	タイトル・URL
2018/7/10	■BIND 9.xのゾーン転送における巨大なゾーンデータの取り扱いの不具合について <https://jprs.jp/tech/notice/2018-07-10-bind9-zonetransfer.html>

- 米国国土安全保障省の緊急指令公開に関する注意喚起
  - さまざまな手法によるドメイン名ハイジャックが米国で多発している件

公開・更新日	タイトル・URL
2019/1/28	■（緊急）米国国土安全保障省によるDNS設定の改ざんに関する緊急指令の公開について <https://jprs.jp/tech/security/2019-01-28-cisa-emergency-directive.html>

宣伝タイム：JPRSブースのご紹介

JPRSブースのご紹介

- 書籍「DNSがよくわかる教科書」見本誌
- 配布物
  - JPRSトピックス&コラム
  - サーバー証明書関連パンフレット
  - Software Design × JPRS（抜き刷り）
  - JPRSオリジナルグッズ

Visit Us!☺

JAPAN REGISTRY SERVICES

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

@JPRS_official

JPRSofficial