

DNSの動向

森下 泰宏 ●株式会社日本レジストリサービス（JPRS） 広報宣伝室 技術広報担当・技術研修センター

複数の大手サービス事業者において、DNSの運用ミスに起因する大規模な障害が発生した。ウェブサービスとの連携の強化や利用者のプライバシー保護を目的とした、新たな技術の導入が図られている。

■DNSの運用ミスに起因する大規模障害

2021年中に複数の大手インターネットサービス事業者において、DNSの運用ミスに起因する大規模な障害が発生した。これらの障害事例はいずれも権威DNSサーバーの運用ミスの影響がそのドメイン名を使うサービスに及び、障害の規模が大きくなったものであった。

本稿では、2021年9月に発生したドコモメール、2021年9月から10月にかけて発生したSlack、および2021年10月に発生したFacebookなどにおける障害の状況について記述する。

●事例：ドコモメール（2021年9月）

2021年9月16日に、NTTドコモが提供するドコモメールとiモードメールにおいて、NTTドコモ以外の宛先に送信されるメールが届きづらくなる状況が発生した¹。

本件は、ドコモメールとiモードメールのメールアドレスとして使われるdocomo.ne.jpゾーンを管理する権威DNSサーバーにおいて、メールの送信元認証技術であるSPF（Sender Policy Framework）のためのTXTレコードが2個設定されたため、当該TXTレコードを用いた送信元認証がメールの受信側でエラーとなり、メールの受

け取り拒否や迷惑メール判定が発生したことによるものである。

SPFの仕様を定義したRFC 7208²は1つのドメイン名に対し、SPFを記述したTXTレコードを複数個設定することを禁止しており、SPFの検証時に当該TXTレコードが複数個見つかった場合、検証エラー（permerror）とする旨が定められている。検証エラーが発生した際の処理はサービスの実装者に委ねられており、メールの受け取り拒否・迷惑メール判定など、サービスごとに異なる処理が実行される。

本件と同様の事例は以前から散発的に発生しており、最近では2021年6月にamazon.comゾーンでも発生している。同様の事例が繰り返される理由として、SPFの設定内容を追加する際にはTXTレコードそのものの追加ではなく、既存のTXTレコードに対するデータの追加が必要になることが挙げられる。

この運用手法はホストに対するIPv4アドレス（Aレコード）やIPv6アドレス（AAAAレコード）の追加とは異なっているため、理解不足による運用ミスを引き起こしやすく、注意が必要である。

●事例：Slack（2021年10月）

2021年9月30日（日本時間10月1日深夜）、ビ

ジネスコラボレーションツールを提供する Slack において、世界的な接続障害が発生した。本件の原因は slack.com ゾーンにおいて、DNSSEC 検証エラーが発生したことによるものである。

2021 年 11 月 30 日に、Slack が本件に関する報告を公開した³。本稿ではその内容に基づき、障害の状況を解説する。

▼障害発生のかきかけ

Slack では slack.com ゾーンの管理に、Amazon が提供する Route 53 を利用している。Route 53 では 2020 年 12 月から DNSSEC をサポートしており⁴、利用者は Route 53 コンソールで自ゾーンの DNSSEC 署名を有効にし、親ゾーンとの信頼の連鎖を構築するための DS レコードを生成・登録することで、DNSSEC に対応できる⁵。

Slack ではこの機能を使用して 2021 年 9 月 30 日に slack.com の DNSSEC 署名を有効にし、com ゾーンに DS レコードを登録した（資料 4-3-14）。その直後、Google Public DNS において、Slack の API サーバーである app.slack.com の IPv4 アドレス（A レコード）が名前解決できなくなる障害が発生した。

この障害は、以下の 5 つの条件が重なったことで発生した。

1：slack.com ゾーンにワイルドカードを用いた A レコードが設定されており、app.slack.com の IPv4 アドレスは、その A レコードで提供されていた。

2：Route 53 における DNSSEC 対応に不具合があった。具体的には、権威 DNS サーバーが応答する DNSSEC の不在応答⁶の NSEC レコードに本来設定されるべき⁷、ワイルドカードを用いた A レコードが存在する旨のタイプビットマップが設定されない状態になっていた（現在は修正済み）。

3：Google Public DNS では DNSSEC の不在応答

の内容を積極的に利用して、パフォーマンスの向上を図っていた⁸。

4：app.slack.com は IPv6 に対応していなかったため AAAA レコードが設定されておらず、AAAA レコードが問い合わせされた際、不在応答である NODATA（そのレコードタイプは存在しない）を返す状態になっていた。

5：多くのクライアントは IPv6 アドレスでの接続を優先するため、app.slack.com においても、AAAA レコードを A レコードよりも先に問い合わせる状態であった。

これらの条件が重なり、Google Public DNS はクライアントからの app.slack.com の IPv4 アドレス（A レコード）の問い合わせに対し、権威 DNS サーバーに問い合わせることなく、IPv6 アドレス（AAAA レコード）を問い合わせた際の NODATA 応答のキャッシュを利用し、当該レコードタイプ（この例では A レコード）が存在しない旨を応答する状態となった。

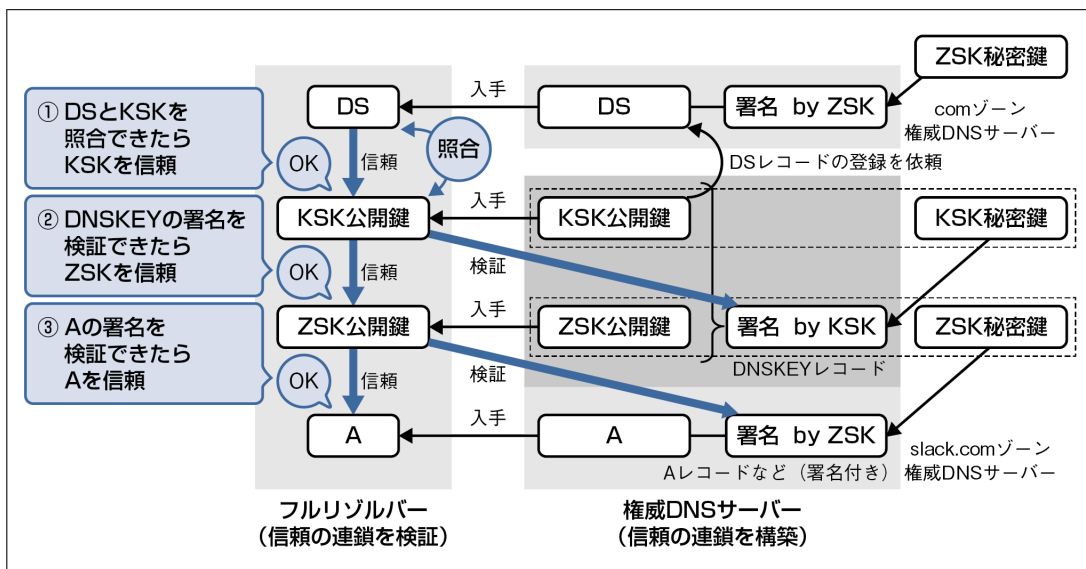
▼大規模障害になった理由

Slack では前述の障害に対応するため、有効にした slack.com ゾーンの DNSSEC を無効に戻す作業を実施した。

有効にした DNSSEC を無効にする場合、キャッシュの影響を回避するため、以下の手順を実施する必要がある。

- 1：親ゾーンに登録した DS レコードを削除する。
- 2：DS レコードの削除を確認後、設定されていた DS レコードの TTL が満了するまで待機する。
- 3：自ゾーンの DNSSEC 設定（DNSKEY レコードと署名）を削除する。

しかし Slack では slack.com ゾーンの DNSSEC を無効にする際に手順 2 を実施しなかったため、インターネット上のフルリゾルバー（キャッシュ DNS サーバー）では com ゾーンに設定された



出所：筆者作成

slack.com の DS レコードがキャッシュに残ったまま、slack.com ゾーンの DNSSEC 設定 (DNSKEY レコードと RRSIG レコード) が削除された状態となった。これにより、それらのフルリゾルバーにおいて slack.com の DNSSEC 検証エラーが発生し、障害が大規模化した (資料 4-3-15)。

com ゾーンの DS レコードの TTL は 86400 (1 日) であったため、障害が長期に及んだ。Slack では緊急回避策としてフルリゾルバーのキャッシュのクリアと、比較的早期に障害から回復した (理由は後述) Google Public DNS への一時的な変更を呼び掛けた⁹。

▼ Google Public DNS が早期に回復した理由

Google Public DNS は DNSSEC 検証を実施しており、当該時間に slack.com の DNSSEC 検証エラーが発生した。しかし、Google Public DNS では利用者が外部からキャッシュをフラッシュ (クリア) できる仕組みを提供しており¹⁰、障害発生

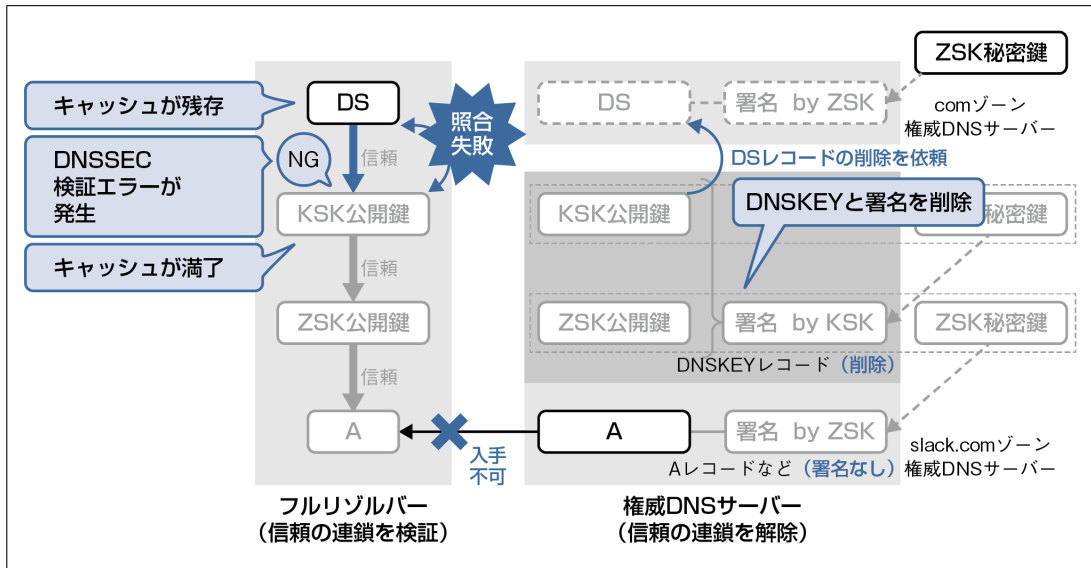
時に複数の利用者が slack.com の DS レコードのキャッシュクリアを実施したため、他のフルリゾルバーよりも早期に回復したことが、Google Public DNS の管理者から報告されている¹¹。

●事例：Facebook、Instagram など (2021 年 10 月)

2021 年 10 月 4 日 (日本時間 10 月 5 日深夜)、Facebook (現 Meta) が運営する Facebook、Instagram、WhatsApp、Messenger において、世界的な接続障害が発生した。

本件の原因は、同社における通常メンテナンス時の操作ミスのため同社の各地のデータセンターが孤立し、その影響により同社の DNS インフラネットワークの経路広告が停止されたことで、同社の DNS インフラに外部から接続できない状態に陥ったことによるものである旨、同社から報告されている¹²。

同社からは障害復旧に時間を要した理由とし



出所：筆者作成

て、DNSインフラへの到達性が失われたことが同社の社内システムにも影響し、データセンターへの入室とハードウェア・ルーターの設定変更に時間を要した旨が報告されている¹³。

本件については、パブリックDNSサービス1.1.1.1を運営するCloudflareからも、1.1.1.1において観測された状況が報告されている¹⁴。

報告によると、facebook.comのすべての権威DNSサーバーにアクセスできなくなった際にスマートフォンのFacebookアプリから大量のDNSトラフィックが送信され続ける状態となり、Facebookのサービスに関する問い合わせ数が通常時の約30倍に達したとのことで、急増したDNSトラフィックがインターネット上のフルリゾルバーの名前解決全体に影響を及ぼした可能性がある旨が示唆されている（資料4-3-16）。

なお、本件については2021年11月に開催されたInternet Week 2021のDNS DAYにおいてNTTコミュニケーションズの小坂良太氏からも、当該

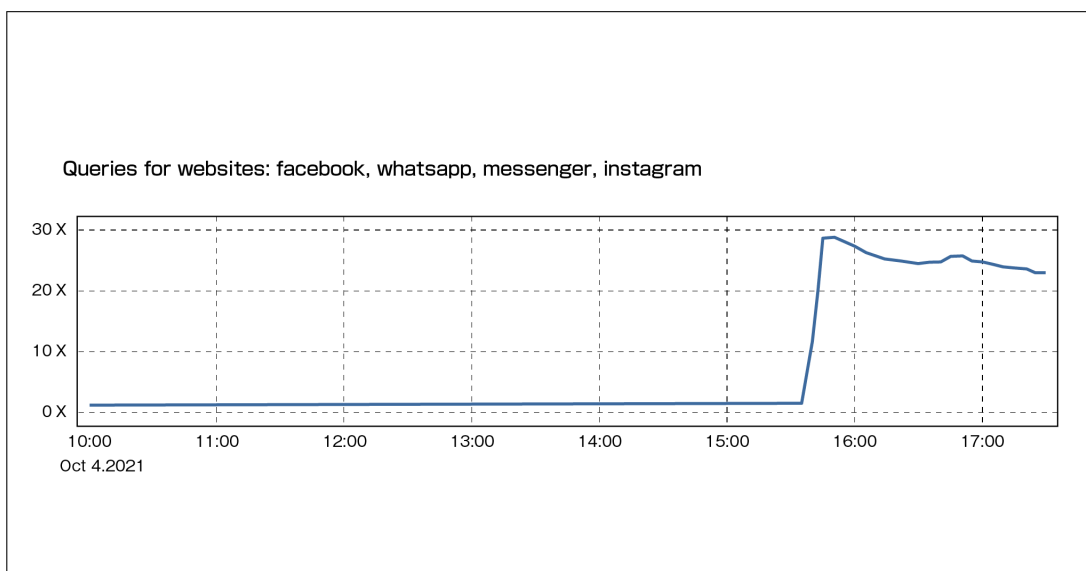
時刻に同社が運用するOCNのフルリゾルバーにおいて、同様のDNSトラフィックの上昇が観測された旨が報告されている¹⁵。また、comゾーンを管理するVerisignからも、com/netの権威DNSサーバーにおいてDNSトラフィックの大幅な上昇が観測された旨が報告されている¹⁶。

■HTTPSレコードの概要と利用状況

IETFにおいて、HTTPSサービスを提供するための新しいリソースレコードである「HTTPSレコード」の標準化が進められている¹⁷。本稿執筆時点においてIETF dnsop ワーキンググループでの議論は終了しており、IESG¹⁸における最終レビューを経た後、RFCとして発行される予定となっている。

●HTTPSレコードの概要

HTTPSレコードにはウェブサーバーのホスト名、サーバーごとの優先度、HTTPS接続に必要な情報など、HTTPSサービスの提供に関するさま



出所： <https://blog.cloudflare.com/ja-jp/october-2021-facebook-outage-ja-jp> の図に基づき筆者作成

ざまな情報を設定・記述する。

資料 4-3-17 に、外部の CDN (Content Delivery Network) サービスを利用し、<https://example.com/> という URL でウェブサイトを開示する場合の、HTTPS レコードの設定例を示す。このように、HTTPS レコードは外部サービスの利用者・提供者双方のゾーンの権威 DNS サーバーで設定される。

HTTPS レコードは従来の CNAME レコードでは不可能であった、ゾーン頂点¹⁹にも設定可能である。

●HTTPS レコードの利用状況

本稿執筆時点において、HTTPS レコードのサポートは主要なウェブブラウザ (Chrome、Firefox、Safari) で実装済みとなっており、Safari ではデフォルトで有効に設定されている。そのため 2020 年以降、HTTPS レコードの DNS 問い合わせは、既にインターネット上で観測されるように

なっている²⁰。

CDN サービスでは Cloudflare が HTTPS レコードの設定をサポートしており²¹、今後、標準化の進行に伴い、他の CDN サービスやマネージド DNS サービスなどにおいてもサポートが進んでいくものと考えられる。

■Oblivious DoH の概要と利用状況

Oblivious DoH は、DNS 問い合わせに関するプライバシーを保護するための仕組みである。その仕様は実験プロトコル (Experimental) として、IETF に提案されている²²。

●Oblivious DoH の概要

Oblivious DoH ではクライアントとリゾルバーの間に DNS 問い合わせ・応答を中継するプロキシを追加し、かつ、クライアントとリゾルバーがエンドツーエンドで DNS データを暗号化・復号することで、リゾルバーの運用者が IP アドレスと DNS 問い合わせの内容を同時に入手できないよ

◆CDNサービスの利用者（example.com）のゾーンでの設定例（エイリアスモード）

```
@      7200 IN HTTPS 0 pool.svc.example.net.
```

<設定の意味>

- example.comのHTTPS サービスはpool.svc.example.netで提供
(注：CNAME を設定できないゾーン頂点にも設定可能)

◆CDNサービスの提供者（svc.example.net）のゾーンでの設定例（サービスモード）

```
pool    7200 IN HTTPS 1 h3pool alpn=h2,h3 ech="123..."
        7200 IN HTTPS 2 . alpn=h2 ech="abc..."
```

<設定の意味>

- pool.svc.example.netのHTTPSサービスは、h3pool（優先度1）とpool（優先度2）で提供
- h3poolはHTTP/2とHTTP/3に、poolはHTTP/2に対応
- サーバーにHTTPS接続するためのECH（Encrypted Client Hello）情報

出所：筆者作成

うにしている。

Oblivious DoHにおけるDNS問い合わせ・応答の流れを資料4-3-18に示す。プロキシではクライアントのIPアドレス、リゾルバーではDNS問い合わせの内容のみを入手可能になる。

●Oblivious DoHの利用状況

Oblivious DoHはAppleが提供する iCloud Private Relayで使われており、iOS 15、iPadOS 15、macOS Monterey以降のOSでサポートされている²³。なお当該OSのiCloud Private Relayは本稿執筆時点ではベータ版となっており、デフォルトでは無効に設定されている。

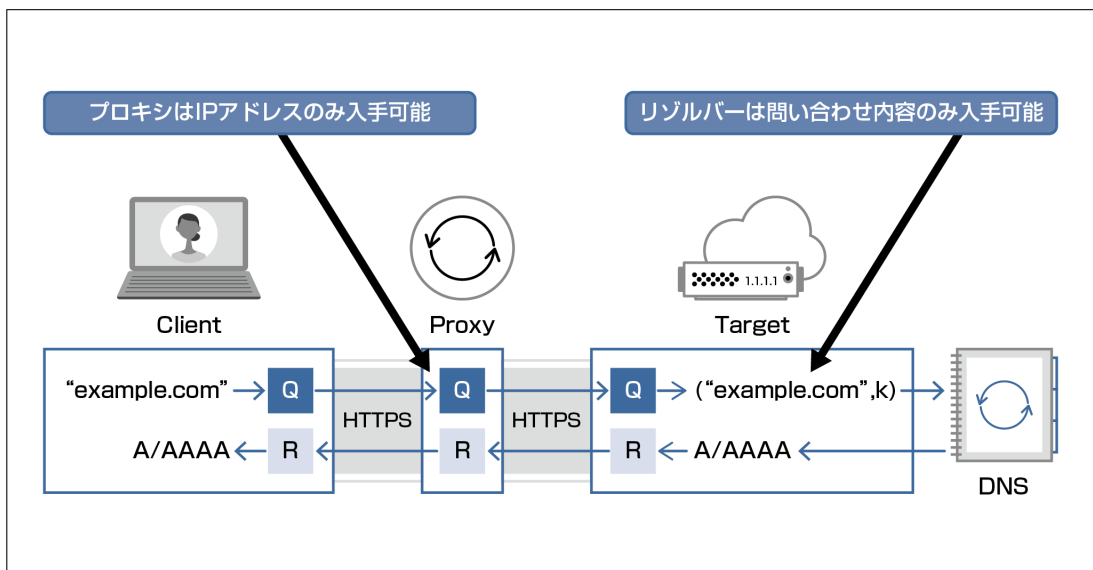
■arpaゾーンのルートサーバーからの分離

2021年10月29日に、arpaゾーンをルートサーバーから分離することを定めた、RFC 9120が発行された²⁴。本RFCはarpaを管理するIAB²⁵が、今後の方針として公開したものである²⁶。

arpaはARPANET²⁷からの移行用のTLDとして、1985年に創設された。その後、2001年に発行されたRFC 3172²⁸で、通信プロトコルの内部で使われるインフラストラクチャドメインとして再定義され、現在に至っている。

arpaゾーンは歴史的理由により、j.root-servers.net（J-Root）を除く、12のルートサーバーに委任されている²⁹。RFC 9120ではarpaゾーンを管理する権威DNSサーバーをa.ns.arpa、b.ns.arpa…という形で準備し、ルートサーバーから分離することで、ルートサーバーの管理ポリシーに影響されない形でarpaゾーンを管理可能にする旨の方針を定めている。

本提案が公開された背景として、RFC 9120ではルートサーバー・ルートゾーンの運用に影響するとして、arpaゾーンに関するIETFで検討された一部の提案が却下された旨を挙げている。なお、本稿執筆時点では分離に関する具体的なスケジュールや手順は公開されておらず、今後決定さ



出所： <https://blog.cloudflare.com/oblivious-dns/> の図に基づき筆者作成

れる予定となっている。

■ DNSソフトウェアの脆弱性の状況

● BINDの脆弱性の状況

資料4-13-19に、2021年中に JPRSが注意喚起した BINDの情報を示す。

● BIND以外のDNSソフトウェアの状況

資料4-3-20に、2021年中に JPRSが注意喚起した BIND以外のDNSソフトウェアの情報を示す。

2021年はWindows DNSに関する多数の脆弱性が報告された。脆弱性にはWindows DNSサーバーに加え、Windowsの名前解決ライブラリを対象としたものも含まれている。これらはWindows 10/11のようなコンシューマー向けOSも対象となるため、注意が必要である。

Windows Updateの確実な実施とMicrosoftからリリースされる脆弱性情報の確認・対応が、本件における有効な脆弱性対策となる。

1. ドコモメールアドレスからの送信メールが一部宛先に届きづら
い事象について
https://www.nttdocomo.co.jp/service/docomo_mail/
2. RFC 7208: Sender Policy Framework (SPF) for Authoriz-
ing Use of Domains in Email, Version 1
<https://www.rfc-editor.org/rfc/rfc7208.html>
3. The Case of the Recursive Resolvers - Slack Engineering
<https://slack.engineering/what-happened-during-slack-s-dnssec-rollout/>
4. DNSSECでAmazon Route 53のサポートを開始
<https://aws.amazon.com/jp/about-aws/whats-new/2020/12/announcing-amazon-route-53-support-dnssec/>

5. DNSSEC 署名を有効にし、信頼チェーンを確立します。 -
Amazon Route 53
https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/dns-configuring-dnssec-enable-signing.html
6. DNSにおいて、問い合わせのドメイン名・タイプ（型）に一致
するリソースレコードが存在しないことを示す応答。
7. RFC 7129: Authenticated Denial of Existence in the DNS
<https://www.rfc-editor.org/rfc/rfc7129.html>
8. Security Benefits | Public DNS | Google Developers
<https://developers.google.com/speed/public-dns/docs/security>
9. Status Site - Incident: Less than 1% of users may be ex-

資料 4-3-19 2021 年に JPRS が注意喚起した BIND の情報

公開・更新日	タイトル
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)
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)
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)
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)
2021/8/19	(緊急) BIND 9.16.19 の脆弱性 (DNS サービスの停止) について (CVE-2021-25218)
2021/10/28	BIND 9.x の脆弱性 (パフォーマンスの低下) について (CVE-2021-25219)

出所：筆者作成

資料 4-3-20 2021 年に JPRS が注意喚起した BIND 以外の DNS ソフトウェアの情報

公開・更新日	タイトル
2021/1/15	Windows DNS の脆弱性情報が公開されました (CVE-2021-1637)
2021/1/25	dnsmasq における「DNSpooq」脆弱性の公開について
2021/2/12	Windows DNS の脆弱性情報が公開されました (CVE-2021-24078)
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)
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)
2021/5/10	Knot Resolver の脆弱性情報が公開されました
2021/7/16	Windows DNS の脆弱性情報が公開されました (CVE-2021-33745、他 12 件)
2021/7/29	PowerDNS Authoritative Server の脆弱性情報が公開されました (CVE-2021-36754)
2021/9/17	Windows DNS の脆弱性情報が公開されました (CVE-2021-36968)
2021/10/15	Windows DNS サーバーの脆弱性情報が公開されました (CVE-2021-40469)

出所：筆者作成

- periencing trouble connecting to Slack
<https://status.slack.com/2021-09/06c1e17de93e7dc2>
10. Flush Cache | Public DNS | Google Developers
<https://developers.google.com/speed/public-dns/cache?hl=ja>
11. [dns-operations] slack.com bogus
<https://lists.dns-oarc.net/pipermail/dns-operations/2021-October/021369.html>
12. Update about the October 4th outage - Engineering at Meta
<https://engineering.fb.com/2021/10/04/networking-traffic/outage/>
13. More details about the October 4 outage - Engineering at Meta
<https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/>
14. フェイスブックがインターネットから消えた事件を説明する
<https://blog.cloudflare.com/ja-jp/october-2021-facebook-outage-ja-jp/>
15. プログラム詳細- IW2021
<https://www.nic.ad.jp/iw2021/program/detail/>
16. Observations on Resolver Behavior During DNS Outages - Verisign Blog
<https://blog.verisign.com/security/facebook-dns-outage/>
17. Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)
<https://datatracker.ietf.org/doc/draft-ietf-dnsop-svcb-https/>
18. IETF の活動と標準化プロセスを管理し、議論の方向性をガイドする役割を担う組織。
19. 委任により分割された、子ゾーンの頂点のドメイン名。ゾーン頂点には SOA レコードと NS レコードが設定されるため、他のレコードとの併存が許可されない CNAME レコードは設定できない。
20. New SVCB & HTTPS Resource Records in the wild
https://community.akamai.com/customers/s/article/NetworkOperatorCommunityNewSVCBHTTPSResourceRecordsinthewild2021128135350?language=en_US
21. Managing DNS records in Cloudflare - Cloudflare Help Center
<https://support.cloudflare.com/hc/en-us/articles/360019093151-Managing-DNS-records-in-Cloudflare>
22. Oblivious DNS Over HTTPS
<https://datatracker.ietf.org/doc/draft-pauly-dprive-oblivious-doh/>

23. iCloud Private Relay に向けたネットワークやWeb サーバの準備- サポート- Apple Developer
<https://developer.apple.com/jp/support/prepare-your-network-for-icloud-private-relay/>
24. RFC 9120: Nameservers for the Address and Routing Parameter Area ("arpa") Domain
<https://www.rfc-editor.org/rfc/rfc9120.html>
25. IETF の活動方針とインターネット標準化プロセスを監督し、RFC 編集者を任命する機関。IETF のプロトコルパラメーターレジストリの管理も担当。
26. RFC 9120 on Nameservers for the Address and Routing Parameter Area ("arpa") Domain | Internet Architecture Board
<https://www.iab.org/2021/10/29/rfc-9120-on-nameservers-for-the-address-and-routing-parameter-area-arpa-domain/>
27. 1969 年に米国防総省の高等研究計画局（ARPA）が創設したネットワーク。1990 年まで運用され、現在のインターネットの原型の一つとなった。
28. RFC 3172: Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")
<https://www.rfc-editor.org/rfc/rfc3172.html>
29. [dns-operations] What is the reason of J-Root doesn't serve the arpa zone?
<https://lists.dns-oarc.net/pipermail/dns-operations/2021-December/021486.html>



1996, 1997, 1998, 1999, 2000, ...

[インターネット白書ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2022年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<https://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

インプレス・サステナブルラボ

✉ iwp-info@impress.co.jp