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

DNSの品質向上と機能拡張の推進を図るための「DNS flag day」が2019年2月1日に実施。DNSプライバシーの実装が進む一方、BIND以外の脆弱性報告が増加している。

■ルートゾーンKSKロールオーバーの状況

2018年10月11日（協定世界時）、ルートゾーンKSKロールオーバーの作業ステップ「新KSK（以下、KSK-2017）による署名開始」が実施された。

本作業は当初、1年前の2017年10月11日に実施予定であった。しかし、準備が整っていないと考えられるフルリゾルバー（キャッシュDNSサーバー）が想定よりも多いことが調査により判明したため、延期されていたものである。

●ルートゾーンKSKロールオーバーとは

ルートゾーンKSKロールオーバーは、ルートゾーンのDNSSECで使われている鍵署名鍵（KSK）を複数の作業ステップを経て、新しい鍵に更新する作業である。ルートゾーンKSKロールオーバーそのものの概要と必要な作業、作業延期の経緯については『インターネット白書2018』の「DNSの動向」で解説しているので、そちらを参照されたい。

●作業延期後のICANNの対応

ICANNでは問題解決のため、問題となったソフトウェアの調査と特定、未対応のフルリゾルバーが設置されている組織への個別連絡、関係者間の連携や連絡体制の強化、さらなる情報提供[1]などを実施してきた。

それらの活動や、ルートサーバーにおけるトラストアンカーの観測結果[2]を踏まえ、ICANNでは再延期の必要はないと判断。2018年9月16日に開かれた理事会で、KSK-2017による署名開始を当初予定から1年後となる、2018年10月11日午後4時（協定世界時）に実施する旨を決定した[3]。

●作業の状況

2018年10月11日に実施されたKSK-2017による署名開始において、大きな問題の発生は報告されなかった。ICANNでは2018年10月15日に、いくつかの問題の発生が報告されたがそれらは迅速に対応され、KSK-2017への更新は成功したとする旨のプレスリリースを発表した[4]。

なお、.nlのレジストリSIDNが、作業中にRIPE Atlas[5]で観測された、署名の切り替わりの状況を公開している（資料4-2-1）。キャッシュされた署名がTTL値の172800（48時間）に従い、KSK-2010（id: 19036）によるものからKSK-2017（id: 20326）によるものに切り替わっていく状況が、グラフで示されている。

●今後の作業予定

今後、旧KSK（KSK-2010）を失効させる作業が、2019年1月11日から3月22日まで実施される予定である[6]。この作業の期間中、ルートゾーンのDNSKEYリソースレコードの応答サイズが、1425バイトに増大する（資料4-2-2）。

この作業により、今回のルートゾーンKSKロールオーバーの一連の作業ステップは完了となる。

■DNS flag dayの実施

2019年2月1日に「DNS flag day」というイベントが、DNS関係者の間で実施される。本イベントでは、2019年2月1日以降にリリースされる主要なDNSソフトウェアからEDNS0に関するワークアラウンド処理（後述）が削除される。

この動作の変更に伴う名前解決エラーや名前解決の遅延の発生を防ぐため、EDNS0に対応していない権威DNSサーバーやネットワーク機器において、対応作業が必要になる可能性がある。

●DNS flag dayの概要

2018年12月5日現在、資料4-2-3に挙げたオープンソースのDNSソフトウェアベンダーとパブリックDNSサービスの事業者が、DNS flag dayへの参加・サポートを表明している。

【EDNS0の概要とワークアラウンド処理】

DNS flag dayの概要と背景、その影響を知るには、EDNS0の概要と現在の対応状況を知る必要がある。ここでは、それらについて説明する。

EDNS0はRFC 6891で定義される、DNSの機能拡張方式である。DNSSECやDNSのIPv6対応をはじめとするさまざまな機能拡張に対応するため、512バイトを超える大きなDNSメッセージを通信コストの低いUDPで扱えるようにし、応答のフラグや応答コードも拡張する。

EDNS0対応では、フルリゾルバーと権威DNSサーバーの双方がEDNS0に対応している必要がある。また、通信途中のネットワーク機器がEDNS0機能を有効にした問い合わせ／応答を、適切に中継する必要がある。

しかし、送信先の権威DNSサーバーや通信途中のネットワーク機器がEDNS0に対応していないことで、権威DNSサーバーからの応答が得られない場合がある。こうした場合に対応するため、主要なDNSソフトウェアではEDNS0機能を有効にした問い合わせの応答が得られなかった場合、問い合わせた側がEDNS0機能を無効にして同じ内容を再問い合わせする「ワークアラウンド処理」が実行される（資料4-2-4）。

今回のDNS flag dayにより、このワークアラウンド処理が、主要なDNSソフトウェアから削除される。

●DNS flag dayの背景／理由

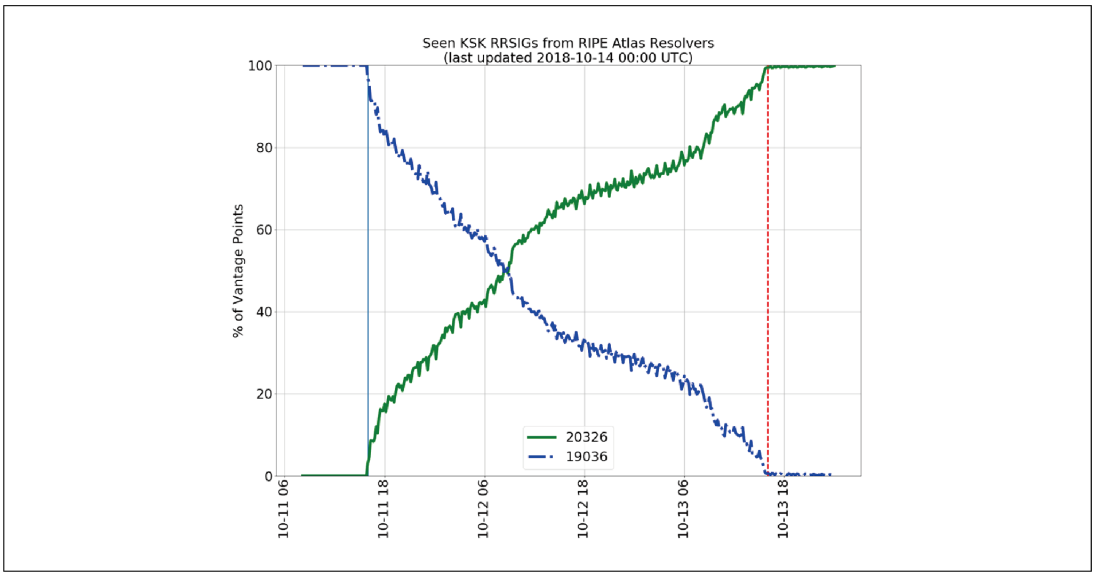
DNS flag dayの実施に至った背景／理由として、以下の2つが挙げられる。

1つは、DNSソフトウェア／サービスの品質とパフォーマンスの向上である。

ワークアラウンド処理は例外処理であり、バグや脆弱性の要因となる。また、再送処理により全体のパフォーマンスも低下する。こうした処理を減らして、DNSの安定性と効率の向上を図る狙いがある。

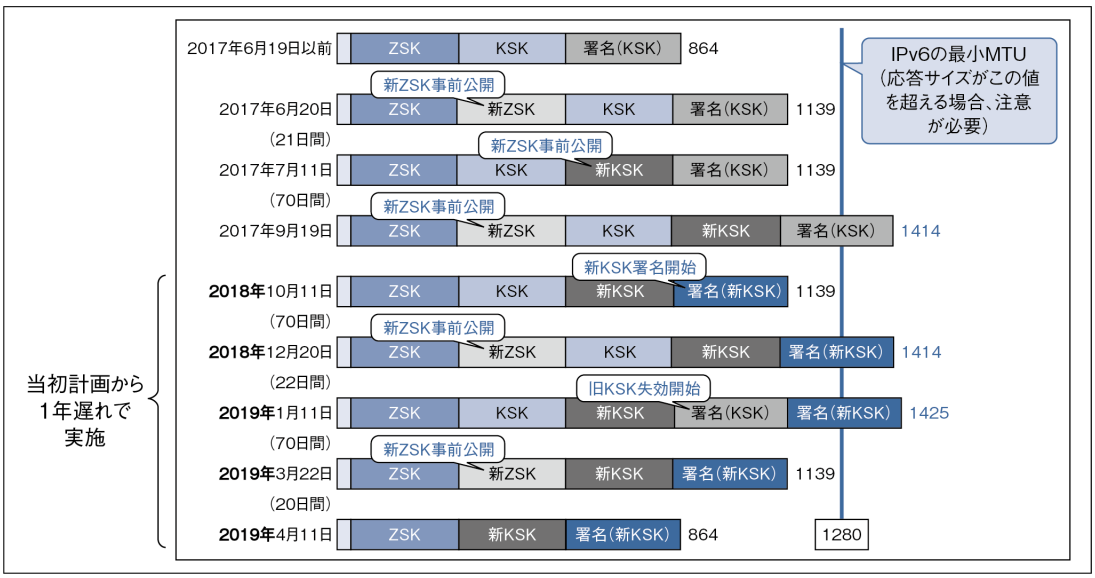
もう1つは、DNSにおける新機能の導入・機能拡張の推進である。ワークアラウンド処理は短期的な問題解決手段としては有効であるが、EDNS0を用いた新機能の導入や機能拡張を図る上での障害となる。ワークアラウンド処理を取りやめることでEDNS0への対応を進め、新機能の導入・機能拡張の推進を図る狙いがある。

資料4-2-1　RIPE Atlasにおける署名鍵の変化の状況（SIDN Labsの調査）



出典：SIDN：A successful root KSK rollover: a brief look back　https://www.sidnlabs.nl/a/weblog/a-successful-root-ksk-rollover-a-short-look-back?language_id=2

資料4-2-2　ルートゾーンKSKロールオーバーの作業ステップと実施時期



出典：筆者作成

●DNS flag dayの影響

ワークアラウンド処理が削除されるため、EDNS0に対応していない権威DNSサーバーからの応答が得られなくなる可能性がある。その結果、特定のドメイン名の名前解決エラーや、名前解決の遅延が発生する可能性がある（資料4-2-5）。DNS flag dayでは、通信途中のネットワーク機

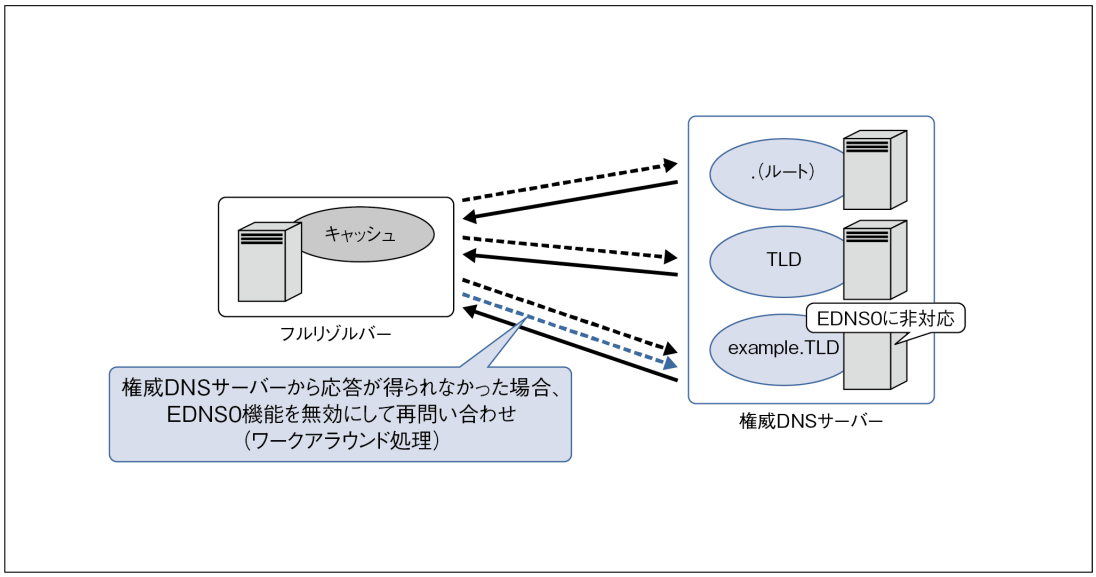
資料4-2-3　DNS flag dayへの参加・サポートを表明しているオープンソースDNSソフトウェアベンダー・パブリックDNSサービス事業者（2018年12月5日現在）

オープンソースDNSソフトウェアベンダー	開発しているソフトウェア
CZ.NIC	Knot DNS / Knot Resolver
Internet Systems Consortium	BIND
NLnet Labs	NSD / Unbound
PowerDNS.COM	PowerDNS Authoritative Server / PowerDNS Recursor

パブリックDNSサービス事業者	サービス名
Cleanbrowsing	Cleanbrowsing DNS
CleanerDNS	Quad9 DNS
Cloudflare / APNIC	1.1.1.1
Google	Google Public DNS

出典：https://dnsflagday.net/

資料4-2-4　フルリゾルバーにおけるワークアラウンド処理



出典：筆者作成

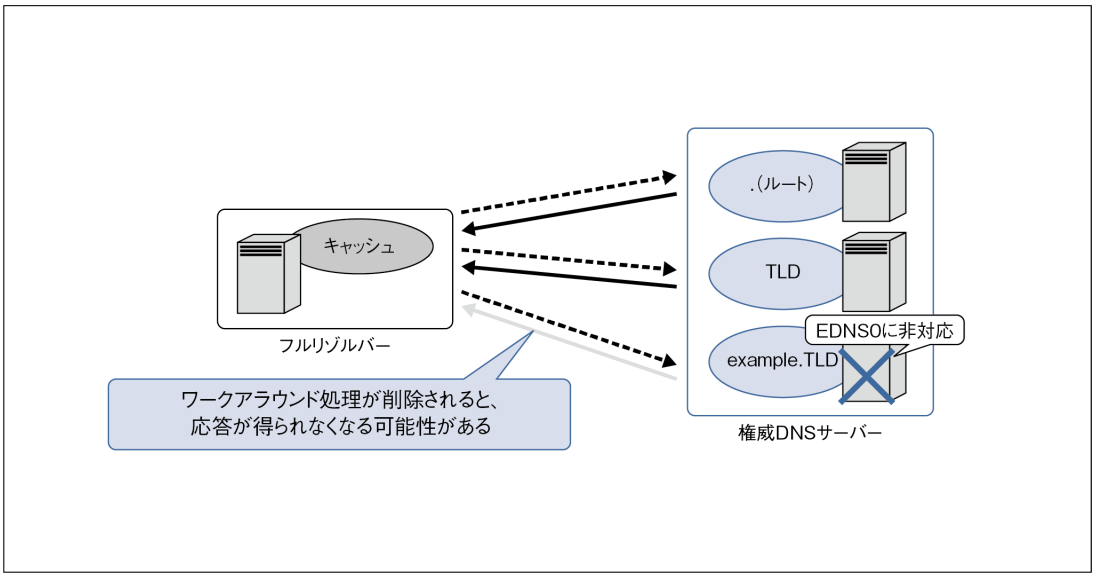
器のEDNS0対応にも注意が必要である。通信途中にEDNS0に対応していないネットワーク機器があった場合、前述したケースと同様、名前解決エラーや名前解決の遅延が発生する可能性がある(資料4-2-6)。

該当する機器の例として、EDNS0機能を有効にしたパケットがドロップされる場合や、IPフラグメンテーション[7]により断片化されたパケットの処理が適切でない場合などが挙げられる。

●影響が出る時期

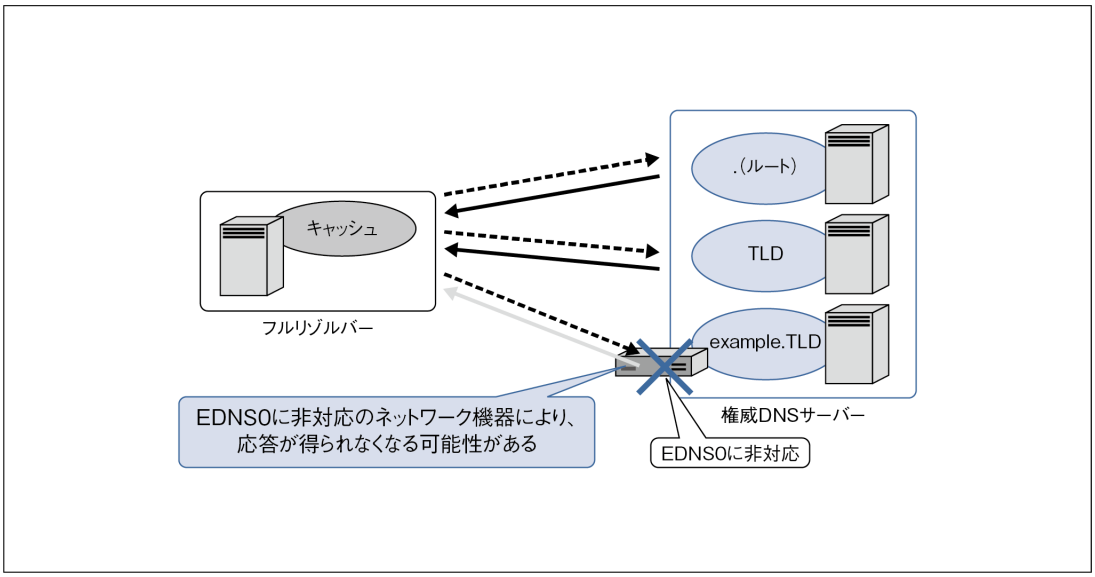
DNS flag dayで動作が変更されるのは、2019年2月1日以降にリリースされるDNSソフトウェアである。そのため、各組織のフルリゾルバーにおいてDNS flag dayの影響が出るのは、2019年2月1日以降にリリースされたバージョンにフル

資料4-2-5　DNS flag dayの影響（1）



出典：筆者作成

資料4-2-6　DNS flag dayの影響（2）



出典：筆者作成

リゾルバーを更新後、EDNS0に対応していない権威DNSサーバーが管理するドメイン名を名前解決しようとしたタイミングとなる。

【DNSソフトウェアの更新の必要性】

ソフトウェアを適切に更新してシステムを最新の状態に保つことは、セキュリティレベルの維持やシステムの安定運用における必須項目である。DNS flag dayの影響を回避するために古いバー

ジョンのDNSソフトウェアを使い続けることは、セキュリティやシステム運用における大きなリスクとなるため、推奨されない。

●対応状況の確認方法

DNS flag dayの公式サイト[8]で、指定したドメイン名がDNS flag dayの影響を受けるかどうかを確認可能である（資料4-2-7）。「Test your domain」の入力フォームにドメイン名を入力し、「Test」ボタンをクリックすると、テスト結果が表示される。

結果は、「GO」「！」「SLOW」の3種類のアイコンで表示される。「SLOW」アイコンが表示された場合、そのドメイン名を管理する権威DNSサーバーや、その権威DNSサーバーが接続されているネットワーク機器において、確認・対応作業が必要になる。

また、公式サイトではDNS管理者向けに、ednscomp[9]を用いた確認を呼びかけている。ednscompはBINDの開発元のISCが公開しているEDNS0の対応状況を調べるツールで、実行すると、詳細な調査結果が表示される。

■DNSプライバシーの概要と実装状況

プライバシー保護に対する意識の高まりを受け、DNSにおいてもプライバシー保護のための技術が注目されている。2018年には主要なパブリックDNSサービス、スマートフォン、ウェブブラウザーなどのコンシューマー向けの環境において、DNSプライバシー関連技術の実装・普及が進んだ。

また、この技術はいわゆるDNSブロッキングの回避手段としても利用可能である。そのため、DNSブロッキングに対する関心の高まりと共に、インターネット利用者の関心も高まっている。

本節では、DNSプライバシーを実現する要素技術の概要と、現在の実装状況について解説する。

●DNSにおけるプライバシー上の懸念点とその解決方法

DNSにおけるプライバシー上の懸念点を、資料4-2-8に示す。

従来のDNS通信は暗号化されておらず、ネットワーク上を平文でやりとりされる。そのため、スタブリゾルバー（クライアント）からフルリゾルバーへの通信をモニターすることで、どのホストが、いつ、何を問い合わせたのかという情報を得ることができる（懸念点1）。また、フルリゾルバー上でアクセスログを収集することでも、同様の情報を得ることができる（懸念点2）。

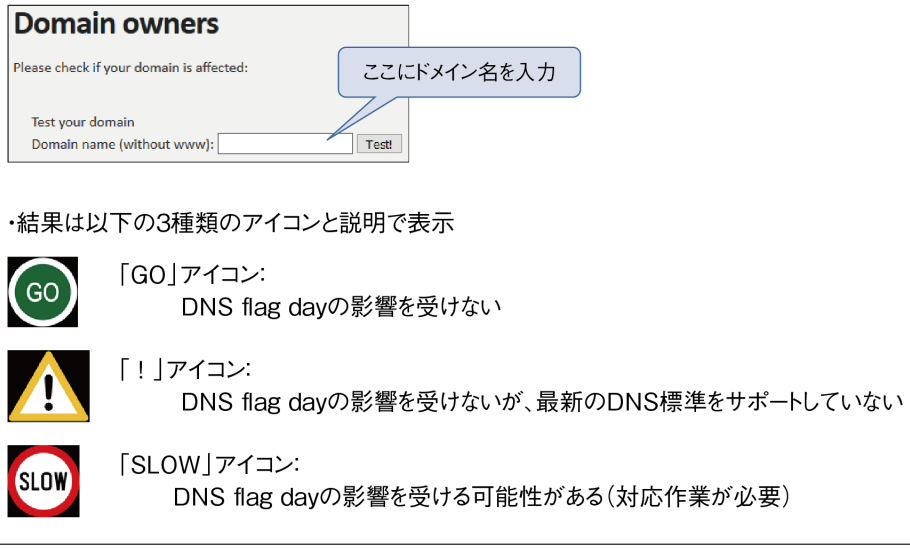
また、フルリゾルバーはスタブリゾルバーから受け取った問い合わせ内容（ドメイン名／タイプ）を、権威DNSサーバーにそのまま問い合わせる。そのため、ルートサーバーやTLDの権威DNSサーバーではフルリゾルバーを介して、クライアントが問い合わせた内容を、ある程度得られることになる（懸念点3）。

そのため、これらの懸念点に対応するための活動がIETFで進められることとなった。その結果、懸念点1については、スタブリゾルバーとフルリゾルバーの間の通信を暗号化するための方式が標準化された。また、懸念点3については、名前解決のアルゴリズムを変更し、フルリゾルバーが権威DNSサーバーに必要最低限の情報のみを送るようにするための方式が標準化された。

懸念点2については、日本のISPでは憲法／電気通信事業法における、通信の秘密の保護の対象となっている。ただし、会社や学校などの組織は電気通信事業者ではないため、独自のモニタリングや、その結果を利用した独自のブロッキング、フィルタリングを実施している場合がある。

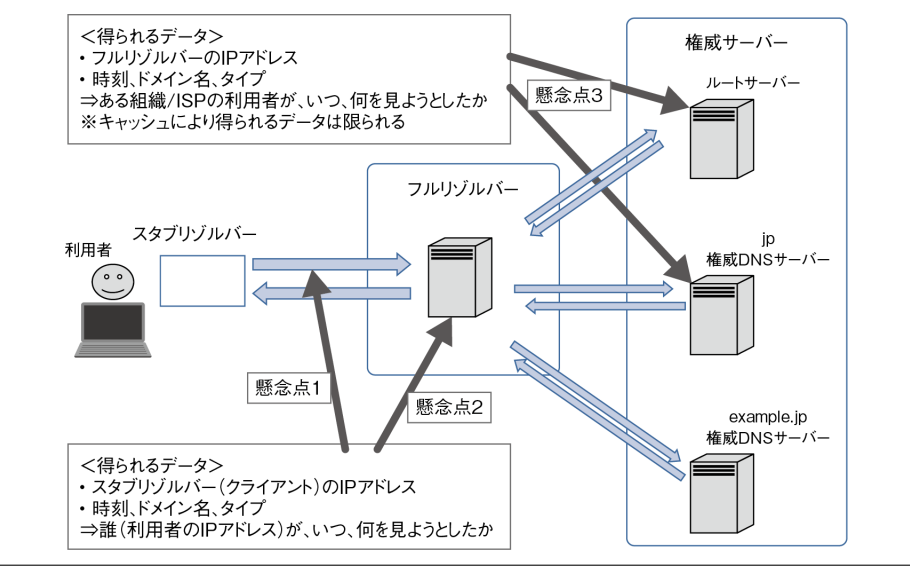
なお、パブリックDNSサービスにおけるアク

資料4-2-7　DNS flag day公式サイトでの確認結果とその意味



出典：筆者作成

資料4-2-8　DNSにおけるプライバシー上の懸念点



出典：筆者作成

セスログの取り扱いについては、別途後述する。

●DNS over TLSの概要と実装状況

【DNS over TLSの概要】

DNS over TLSは、DNSの通信をTLS[10]で保護／暗号化するための技術である。

DNS over TLSの通信には、TCPのポート853番が割り当てられている。通信の内容は従来の

TCPのDNSと同じものを、TLSで保護／暗号化したものである。

DNS over TLSは、スタブリゾルバーとフルリゾルバーの間の通信に使うことが想定されている。DNS over TLSを使うことでスタブリゾルバーとフルリゾルバーの間の通信が保護され、通信内容を傍受することができなくなる。

【DNS over TLSの実装状況】

NLnet Labsが開発しているUnboundが、DNS over TLSを実装している。パブリックDNSサービスでは、CleanerDNSが運用するQuad9やCloudflareとAPNICが共同運用する1.1.1.1が、DNS over TLSを実装しており、Google Public DNSも2019年1月9日から、DNS over TLSのサービスを開始している[11]。

スタブリゾルバーではgetdns API[12]が、DNS over TLSを実装している。また、Android 9.0以降のスタブリゾルバーにはDNS over TLSが標準で組み込まれており、指定されたフルリゾルバーでDNS over TLSが利用可能な場合、自動的に有効に設定されるようになっている（資料4-2-9）。

●DNS over HTTPSの概要と実装状況

【DNS over HTTPSの概要】

DNS over TLSでは、TCPのポート853番が通信に使われる。しかし、制限されたネットワーク環境ではこのポートへの通信がブロックされている場合があり、DNS over TLSを使えないことになる。

そうした背景から、DNSの通信にウェブの通信で使われるHTTPSを使うアイデアが提案された。このための技術が、DNS over HTTPSである。DNS over HTTPSでは、DNSの通信はウェブの通信と同様、HTTPSで保護／暗号化される。

RFC 8484で定義されているDNS over HTTPSではGET/POSTメソッドにより、DNSパケットをそのフォーマットのままで取り扱う。たとえば、GETで資料4-2-10のようなリクエストを送ると、DNSパケットのフォーマットで応答が返る。

【DNS over HTTPSの実装状況】

前述した1.1.1.1が、DNS over HTTPSを実装している。1.1.1.1ではRFC 8484方式のDNS over HTTPSに加え、データをJSON[13]で表現した独自方式のDNS over HTTPSを実装している。なお、Google Public DNSも、独自方式のDNS over HTTPSを実装している。

スタブリゾルバーではウェブブラウザーのFirefoxが、DNS over HTTPSを実装している。ただし、デフォルトでは無効に設定されており、使用する場合、ネットワーク設定のメニューで有効にする必要がある（資料4-2-11）。

また、Alphabet（Googleの持株会社）の子会社のJigsawが、DNS over HTTPSを実装したAndroid用アプリ「Intra」を公開しており、無償で利用可能である[14]。Intraでは問い合わせ先としてGoogle Public DNS、1.1.1.1、それ以外を指定できる。

Intraはオープンソースソフトウェアであり、GitHubでソースが無償公開されている[15]。ソースコードによるとGoogle Public DNSを指定した場合、前述した独自方式のDNS over HTTPSが使われるようになっている。

●QNAME minimisationの概要と実装状況

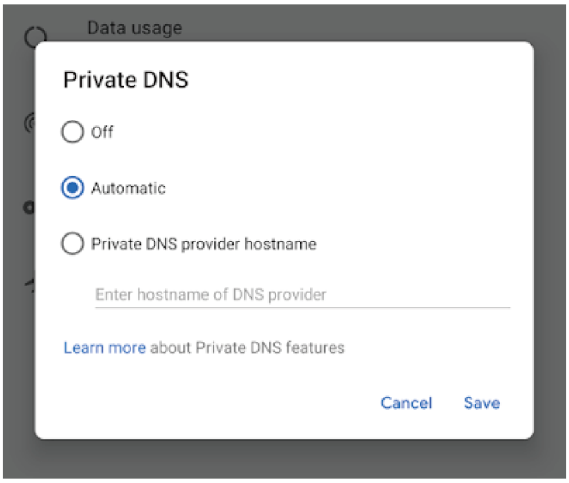
【QNAME minimisationの概要】

QNAME minimisationは、フルリゾルバーの名前解決アルゴリズムを変更し、ルートサーバーやTLDの権威DNSサーバーには名前解決に必要な最低限の情報のみを問い合わせるようにする技術である。

従来のフルリゾルバーの動作とQNAME minimisationの比較を、資料4-2-12に示す。

QNAME minimisationにより、フルリゾルバー

資料4-2-9　Android 9.0のDNS over TLS設定画面



出典：https://developers-jp.googleblog.com/2018/05/dns-over-tls-support-in-android-p.html

資料4-2-10　DNS over HTTPSのリクエストの例

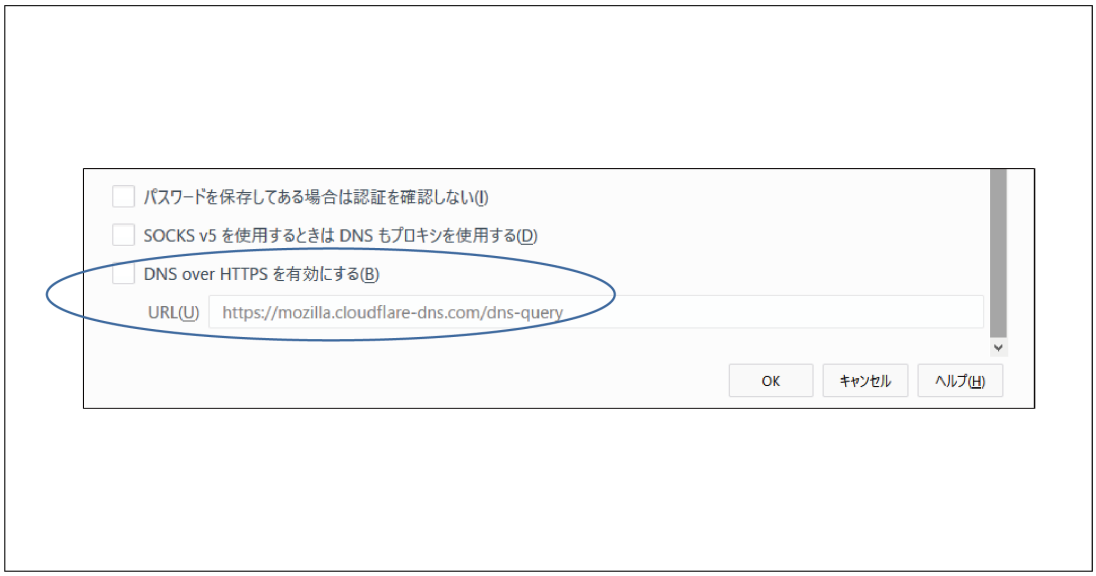
```
:method = GET
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
accept = application/dns-message
```

出典：RFC 8484

はクライアントが問い合わせたドメイン名・タイプをルートサーバーやTLDの権威DNSサーバーに送信しなくなる。そのため、ルートサーバーやTLDの権威DNSサーバーでは、クライアントが問い合わせたドメイン名、タイプを知ることができなくなる。

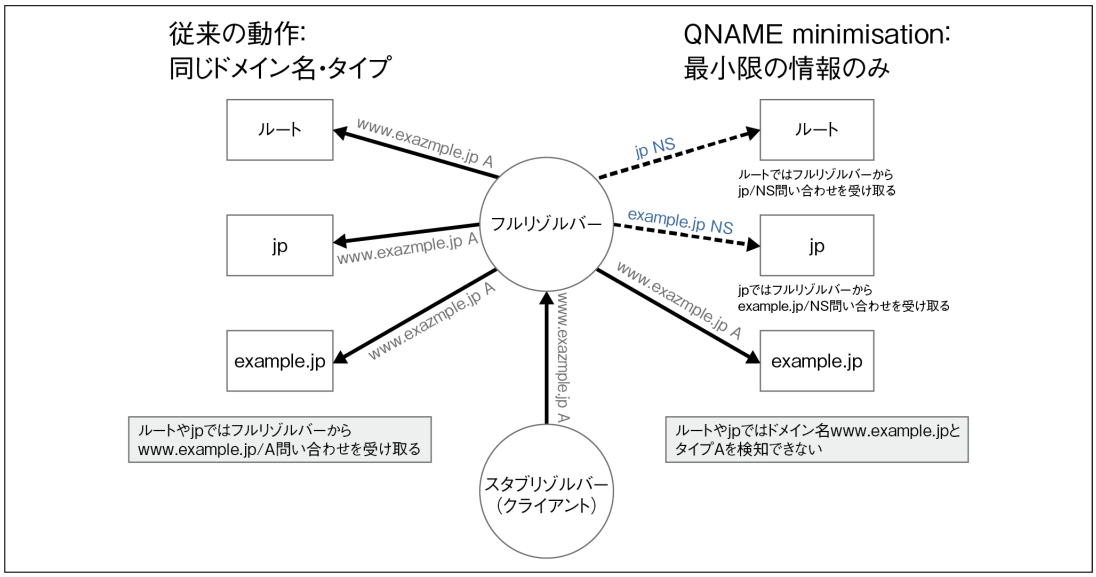
ただし、DNSではドメイン名のラベルの区切りとゾーンの境界（ゾーンカット）は、必ずしも一

資料 4-2-11　Firefox 63.0.3 の DNS over HTTPS 設定画面



出典：筆者作成

資料 4-2-12　従来の動作（左）と QNAME minimisation（右）の比較



出典：筆者作成

致していない。そのため、QNAME minimisation を適用した場合、フルリゾルバーから権威 DNS サーバーに対し、無駄な問い合わせが発生する可能性がある。

【QNAME minimisation の実装状況】

CZ.NIC が開発している Knot Resolver や前述した Unbound など、複数のフルリゾルバーが QNAME minimisation を実装しており、標準で

有効になっている。また、BINDも開発版のバージョン9.13.2で、QNAME minimisationを実装している。

パブリックDNSサービスでは前述した1.1.1.1がQNAME minimisationを実装しており、標準で有効になっている。

●パブリックDNSサービスにおけるアクセスログの取り扱い

パブリックDNSサービスではそれぞれの運用元により、アクセスログとして取得・保存する情報の内容や取り扱いが異なっている。

Google Public DNSはDDoS攻撃の検知や問題の修正のため、送信元のIPアドレスをアクセスログに一時的に保存している。また、保存用のログには送信元の都市レベルの位置情報が含まれており、ランダムサンプリングで抽出・保存される[16]。

一方、1.1.1.1は送信元のIPアドレスをアクセスログに保存しておらず、保存用のログには位置情報が含まれていない[17]。

また、Cloudflareでは1.1.1.1から得られたデータを、共同運用するAPNIC以外の第三者に提供しないことを表明しており、APNICが利用可能なデータの用途を、共同研究契約に基づく非営利の運用研究に限定している。

■ドメイン名ハイジャックの状況

ドメイン名ハイジャックは、ドメイン名の管理権限を持たない第三者が、不正な手段で他者のドメイン名を自身の支配下に置く行為である。

ドメイン名ハイジャック自体は、以前から知られている攻撃手法である。しかし、最近の事例では攻撃の目的が、従来よく見られた示威行為や主義・主張のアピールから、実利の獲得を狙ったものに変化している。

本節では、ドメイン名ハイジャックの目的の変化と、2017年から2018年にかけて発生した2つの特徴的な事例を紹介するとともに、ドメイン名ハイジャックに備えるための、各組織における対策について解説する。

●ドメイン名ハイジャックの目的の変化

実利の獲得を狙った目的の具体例としては、アカウント情報の不正入手、仮想通貨の不正送金、計算機資源の不正使用（例：仮想通貨のマイニング）などが挙げられる。

以下で紹介する2つの事例も、実利の獲得を図ったものである。いずれも、2017年から2018年にかけて発生した。

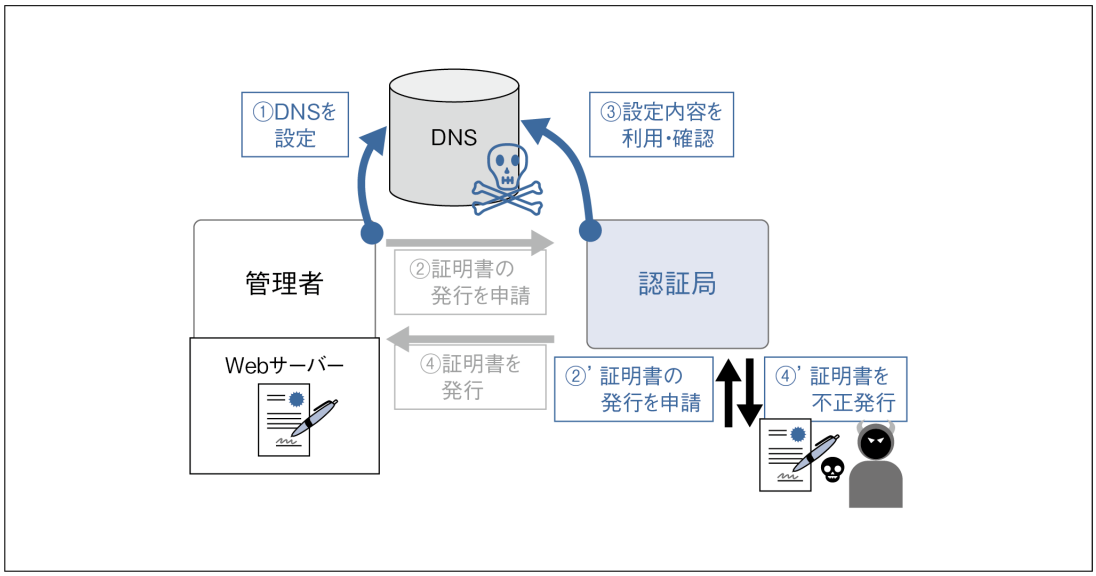
事例1：Fox-IT社

2017年12月に、オランダのセキュリティ企業であるFox-ITが、自社の顧客向けポータルサイトがドメイン名ハイジャックの被害を受けた際の経過と対応をまとめた、レポートを公開した[18]。

この事例では、ドメイン名ハイジャックがサーバー証明書の不正発行・不正使用のために使われ、HTTPSに対する攻撃が行われた。攻撃者はレジストラのログインID・パスワードをクラックして、ドメイン名fox-it.comの設定を書き換える権限を入手した後、以下の2段階の手順により、HTTPSへの攻撃を成功させた。

1. メール関連のDNS設定を不正変更した後、メール認証を用いてサーバー証明書の発行を認証局に申請、正規の手順でサーバー証明書を不正発行／不正入手した（資料4-2-13）。
2. 不正入手したサーバー証明書をインストールして顧客向けポータルサイトの偽サイトを作成、当該サイトのIPアドレスを変更して、顧客のアクセスを偽サイトに誘導した。なお、この偽サイトは受け付けた入力を、本物のポータルサイトにリダイレクトするように設定されていた（資料

資料4-2-13　メール関連のDNS設定を変更後、正規の手順でサーバー証明書を不正発行



出典：筆者作成

4-2-14)。

この結果、

・URLのドメイン名は正しいが、接続先は偽サイトである

・HTTPS接続の際、Webブラウザーが警告を表示しない

という状況となり、偽サイトであると気付かずにログインを試みた複数の顧客のアカウント情報が、攻撃者に流出した。

事例2：MyEtherWallet

2018年4月に、仮想通貨イーサリアムのウォレット（保管所）を提供するMyEtherWalletが、ドメイン名ハイジャックの被害を受けた。この事例では攻撃手法として、MyEtherWalletが当時、ドメイン名 myetherwallet.comの管理に使用していたAmazon Route 53を標的とした、経路ハイジャックが用いられた。

本件では、Google Public DNSからのDNSクエリが経路ハイジャックによって攻撃者が準備した偽の権威DNSサーバーに誘導された。その結果、Google Public DNSに偽のDNS応答が注入され、被害が拡大した[19]。

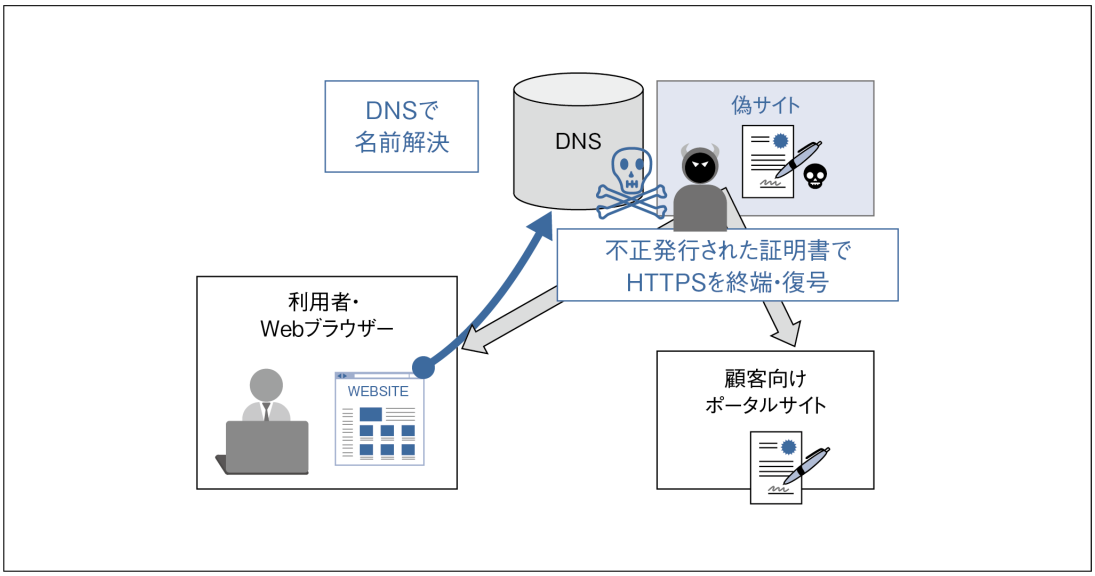
●ドメイン名ハイジャックの対策

前述したように、ドメイン名ハイジャックの主な目的が示威行為や主義・主張のアピールから、実利の獲得にシフトしている。そのため、著名企業やポータルサイトのドメイン名に加え、顧客向けポータルサイトや仮想通貨の保管・取引に使うドメイン名なども、攻撃の標的となっている。

一方、ドメイン名ハイジャックに用いられる手法は従来と同様、レジストリの登録情報の不正書き換えによるものが中心である。それに加え、経路ハイジャック、サーバー証明書に対する攻撃との併用・攻撃の隠蔽など、これまであまり見られなかった手法や、手法の洗練も見られるようになってきている。

こうした状況に対応するためには、ドメイン名

資料4-2-14　HTTPSを終端・復号後、正規のサイトに転送



出典：筆者作成

／DNS単体での対策ではなく、組織そのもののリスクマネジメントの一環としてとらえ、対策することが重要である。具体的な対策としては、自組織で使っているドメイン名の状況把握、信頼できる事業者やサービスの利用、事業者が提供するロックサービスや認証サービスの利用、監視サービスの導入・利用などが挙げられる。

なお、経路ハイジャックについてはDNS運用者における対策は困難であり、AS運用者における対策が必要である。その1つとして、Amazon Route 53ではMyEtherWalletの事例の後、経路ハイジャックの影響を最小限に抑えるための対策[20]を実施している。

■DNSサーバーソフトウェアの脆弱性の状況

●BINDの脆弱性の状況

これまで数多くの脆弱性が報告されてきたBINDであるが、2018年は脆弱性の報告件数は6件と、昨年の12件に比べ減少した。

資料4-2-15に、2018年中にJPRSが注意喚起したBINDの脆弱性の一覧を示した。これらのうち緊急のものは1件であり、こちらも昨年の5件に比べ減少している。

●BIND以外のDNSソフトウェアの状況

BINDの脆弱性報告数が減少した一方、BIND以外のDNSソフトウェアの脆弱性がコンスタントに報告されるようになった。資料4-2-16に、2018年中にJPRSが注意喚起したBIND以外のDNSソフトウェアの脆弱性の一覧を示した。

脆弱性の報告件数が増加した背景として、BIND以外のソフトウェアの開発が進み、それらのソフトウェアの利用者や、利用機会が増加したことが挙げられる。

資料 4-2-15　2018 年に JPRS が注意喚起した BIND の脆弱性

公開・更新日	タイトル
2018 年 1 月 17 日	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2017-3145）
2018 年 5 月 21 日	BIND 9.12.x の脆弱性（サービス性能の劣化及び DNS サービスの停止）について（CVE-2018-5737）
2018 年 5 月 21 日	BIND 9.12.x の脆弱性（DNS サービスの停止）について（CVE-2018-5736）
2018 年 6 月 13 日	BIND 9.x の脆弱性（サービス提供者が意図しないアクセスの許可）について（CVE-2018-5738）
2018 年 8 月 9 日	BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2018-5740）
2018 年 9 月 20 日	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）

出典：筆者作成

資料 4-2-16　2018 年に JPRS が注意喚起した BIND 以外の DNS ソフトウェアの脆弱性

公開・更新日	タイトル
2018 年 1 月 23 日、1 月 24 日 (更新)	Unbound の脆弱性情報が公開されました（CVE-2017-15105）
2018 年 1 月 24 日	PowerDNS Recursor の脆弱性情報が公開されました（CVE-2018-1000003）
2018 年 1 月 24 日	Knot Resolver の脆弱性情報が公開されました（CVE-2018-1000002）
2018 年 4 月 25 日	Knot Resolver の脆弱性情報が公開されました（CVE-2018-1110）
2018 年 5 月 11 日	PowerDNS Authoritative Server の脆弱性情報が公開されました（CVE-2018-1046）
2018 年 6 月 14 日	Windows DNS の脆弱性情報が公開されました（CVE-2018-8225）
2018 年 7 月 5 日	Knot Resolver の脆弱性情報が公開されました
2018 年 7 月 12 日	Windows DNS の脆弱性情報が公開されました（CVE-2018-8304）
2018 年 8 月 1 日	NSD の脆弱性情報が公開されました
2018 年 8 月 6 日	Knot Resolver の脆弱性情報が公開されました（CVE-2018-10920）
2018 年 8 月 8 日	Knot DNS の脆弱性情報が公開されました
2018 年 10 月 11 日	Windows DNS の脆弱性情報が公開されました（CVE-2018-8320）
2018 年 11 月 8 日	PowerDNS Authoritative Server の脆弱性情報が公開されました（CVE-2018-10851、CVE-2018-14626）
2018 年 11 月 8 日	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）
2018 年 11 月 28 日	PowerDNS Recursor の脆弱性情報が公開されました（CVE-2018-16855）
2018 年 12 月 13 日	Windows DNS Server の脆弱性情報が公開されました（CVE-2018-8626）

出典：筆者作成

1. ICANN、KSK ロールオーバーにおける注意事項についての包括的なガイドを発行– ICANN
https://www.icann.org/news/announcement-2018-08-27-ja
2. RFC 8145 Root Trust Anchor Reportshttp://root-trust-anchor-reports.research.icann.org/
3. ニュースリリース：KSK のロールに関する理事会の承認– ICANN
https://www.icann.org/resources/press-material/release-2018-09-18-ja
4. 最初のルート KSK ロールオーバーが正常に完了– ICANN
https://www.icann.org/news/announcement-2018-10-19-ja
5. RIPE NCC が進めているプロジェクトの 1 つ。世界中に設置されたプローブ（測定のために設置される専用の機器）からデータを収集し、さまざまな調査・研究に活用することを目的としている。
https://atlas.ripe.net/
6. The Recent KSK Rollover: Summary and Next Steps – ICANN
https://www.icann.org/news/blog/the-recent-ksk-rollover-summary-and-next-steps
7. サイズの大きな IP パケットを、その IP パケットのサイズより小さな最大転送単位（MTU）を持つネットワークを通して中継す

る際に必要となる仕組み。MTUを超えるIPパケットはMTUを超えないサイズに分割され、分割されたIPパケットは、以降、そのままの形で転送される。

8. DNS flag day　https://dnsflagday.net/
9. EDNS Compliance Tester　https://ednscomp.isc.org/ednscomp/
10. TCPのようなコネクション型の通信を保護するためのプロトコル。以前はSSLという名前で開発されていたが、したが、IETFでの標準化の際、TLSという名称に変更された。
11. Google Public DNS now supports DNS-over-TLS https://security.googleblog.com/2019/01/google-public-dns-now-supports-dns-over.html
12. Welcome to getdns!https://getdnsapi.net/
13. JavaScript Object Notation。JavaScriptのオブジェクト表記方法に由来する、簡便なデータ記述方法。
14. Intra - Google Play のアプリ https://play.google.com/store/apps/details?id=app.intra
15. GitHub - Jigsaw-Code/Intra: An experimental tool that allows you to test new DNS-over-HTTPS services on Android https://github.com/Jigsaw-Code/Intra
16. Your Privacy/Public DNS/Google Developers https://developers.google.com/speed/public-dns/privacy
17. Cloudflare 1.1.1.1 CLOUDFLARE RESOLVER PRIVACY FREQUENTLY ASKED QUESTIONS https://developers.cloudflare.com/1.1.1.1/commitment-to-privacy/privacy-policy/privacy-policy/
18. Lessons learned from a Man-in-the-Middle attack – Fox-IT International blog https://blog.fox-it.com/2017/12/14/lessons-learned-from-a-man-in-the-middle-attack/
19. Official statement regarding DNS spoofing of MyEtherWallet domain – MyEtherWallet https://www.reddit.com/r/MyEtherWallet/comments/8eloo9/official_statement_regarding_dns_spoofing_of/
20. 広告する経路を、グローバルな経路広報が可能な最小サイズである/24に変更。

インターネット白書 ARCHIVES

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が1996年～2019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（株式会社インプレスR&D）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（初期は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的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 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp