DNSを取り巻く環境

**DNSは多くのアプリケーションで利用されており、インターネットの重要なサービスの1つです。
ここでは最近のTLDの追加で顕在化した名前衝突の問題をはじめ、
DNSを取り巻く環境の最新動向について解説します。**

3.1 DNS最新動向

DNSは問い合わせに対応するレコードを応答してくれるサービスで、主にドメイン名に対応するIPアドレスを検索する名前解決に利用されています。インターネットでは、ほとんどのアプリケーションがDNSによる名前解決を利用しており、とても重要なサービスだと言えます。DNSでは、ゾーンという単位でドメイン名に対応するレコードを保持する権威サーバと、問い合わせを行うクライアントが登場します。ほとんどの場合、クライアントはDNSの面倒な反復問い合わせをISPなどが用意しているDNSキャッシュサーバに依頼して、結果のみを受け取ります。DNSキャッシュサーバは、rootと呼ばれる頂点のゾーン情報を提供する権威サーバのIPアドレスのみを知っており、そこから得られる情報を手がかりにより詳細な情報を保持しているであろう権威サーバをたどって必要なレコードを探します。また、毎回反復問い合わせを行っているとサーバの負荷や遅延が問題となるため、得られたレコードはしばらくキャッシュしておき、再び同じ問い合わせを受けた場合にはそのキャッシュから応答しています。最近はこの他にもブロードバンドルータやファイアウォールなど、通信経路上の機器にもDNS関連の機能が実装されており、DNS問い合わせの中継や制御ポリシーの適用に関わっている場合があります。

ドメイン名の名前空間は重複して登録されることがないように、トップレベルドメイン(TLD)ごとにレジストリと呼ばれる管理組織が指定されて管理しています。rootのゾーン情報はICANNが管理しており、ここから各TLDのレジストリに権威委任されて登録者からのドメイン名登録を処理しています。新規にドメイン名を登録したい場合は、レジストラと呼ばれる仲介業者を通じて登録したいドメイン名に対応するTLDのレジストリに申請しますが、各トップレベルやそのサブドメインの属性ドメインごとに登録ポリシーがあり、誰がどんな目的でドメイン名を登録できるのかが異なっている場合があります。例えば.jpドメインは株式会社日本インターネットレジストリサービス(JPRS)がレジストリを担っており、汎用jpと呼ばれるセカンドレベルドメイン名は日本に連絡のとれる住所を持つ個人・法人であれば誰でも登録できますが、co.jp属性型ドメイン名は日本に登記された会社組織のみが登録できます。また、特に制限を設けず、誰でも登録できるポリシーで運用されているTLDもあります。登録されたドメイン名の管理は登録者に権威委譲されるため、それぞれの登録者が運用ポリシーを持ち、適切に管理運用していく必要があります。

3.2 名前衝突問題

ひとまず動けば良いと、利便のために導入された方式が後々問題を引き起こす場合があります。Name Collision（名前衝突）の問題もこれに該当すると言えます。例えば、社内や家庭内など、管理が明確で特定の人しか利用しない環境では、存在しないTLD（勝手TLD）を用いた独自の内部用ドメイン名空間が利用される場合があります。小規模の場合はhostsファイルなどを利用してホスト名を直接クライアントに登録してしまうこともありますし、クライアント数が増えてくると、社内向けキャッシュサーバやファイアウォールで内部からの勝手TLDの問い合わせに応答するようにDNSを設定し、クライアントを特に設定変更することなく内部用ドメイン名でアクセスできるようにしている場合もあります。設定時には当初の目的を達成し動くように見えるのですが、インターネットは変化し続けており、標準技術を利用して標準以外の設定を行っているとどこかで歪みが生じてしまいます。実は近年、rootゾーンに新規のTLDが追加されており、既にその数は300を越えてまだまだ追加が続いています。ここで内部で利便のために設定していた勝手TLDと追加されたTLDがぶつかると、正規に登録したドメイン名が利用できなかったり意図しないサイトに接続してしまったりといった問題が生じてしまいます。これを名前衝突問題と呼びます（図-1）。問題回避のためには、内部用ドメイン名であっても一意性が担保されたドメイン名を利用することです。既に何らかの登録しているドメイン名があるのならば、そのドメイン名に内部用のサブドメインを設定して利用したり、いっそのこと内部用に新規のドメイン名を登録したりすることで、利用しているドメイン名の一意性が将来にわたって担保できるため安心です。

名前衝突問題はサーバの電子証明書にも関わってきます。電子証明書を発行するパブリック認証局は、これまで組織内部のサーバでも電子証明書を利用できるように、勝手TLDの内部用ドメイン名であっても電子証明書を発行してきました。通常のサーバ用電子証明書であれば、電子メールやWebサイトへの特定文字列の登録などでドメイン名保持の確認ができるのですが、勝手TLDではそのような確認ができないので、特段の確認なく電子証明書が取得できていました。すると、新規に追加されたTLDでドメイン名を登録した場合、過去に誰かがそのドメイン名に対応する電子証明書を取得している可能性が出てきてしまいます。電子証明書関連の任意団体であるCA/Browser Forumでは、この名前衝突問題を受け、今後は段階的に内部用ドメイン名向けの電子証明書を制限する運営基準を策定しました。既に現状で発行されている内部用ドメイン名向けの電子証明書は、有効期限が2015年11月1日以降とならないように設定されています。また、新規TLDが追加された場合は、120日以内に関連する電子証明書が失効されるほか、2016年10月には、これまで発行された電子証明書を含め、勝手TLDやインターネットから存在が確認できないドメイン名を用いた内部用ドメイン名に対するすべての電子証明書が失効される予定です。

クライアントには、DNSで名前解決する際にドメイン名を補うサーチリストや、DNSサフィックスといった機能を実

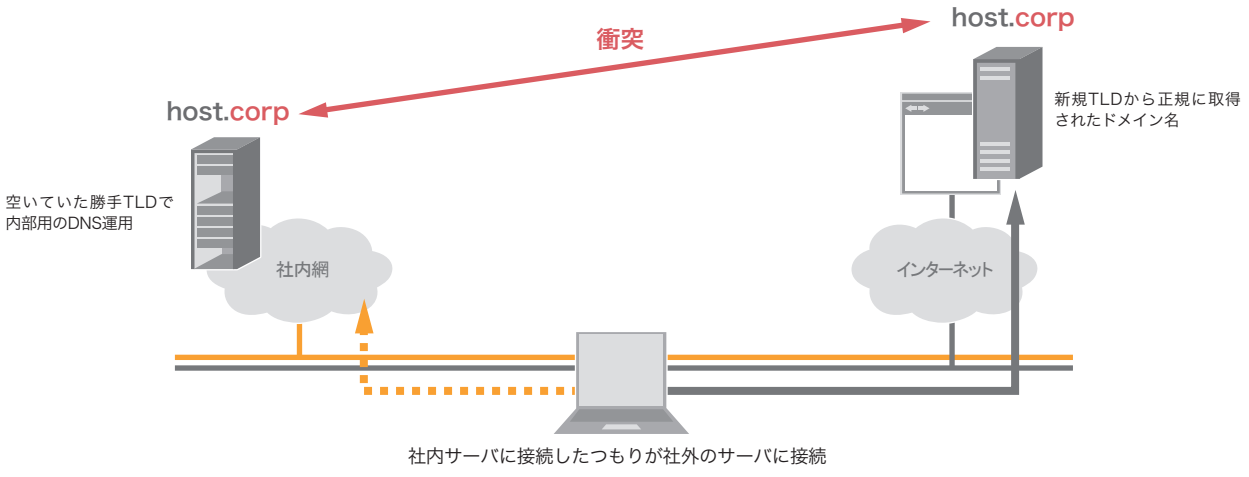

図-1 名前衝突の例

装している場合があります。これはユーザが完全なドメイン名(FQDN)を指定しなくても、その先頭部分を入力すれば意図するドメイン名を指定できるようにする機能です。組織内部ではドメイン名部分が共通の場合が多く、複数のサーバや機器に接続するのに何度も同じドメイン名を入力しなくても済むように利用されています。しかし、これもまた名前衝突問題と関わってきます。クライアントの実装に因るところが大きいのですが、「.」が1つでも含まれたドメイン名がアクセス先に指定されると、ひとまずそのドメイン名をDNSで問い合わせ、レコードが存在しなければサーチリストのドメイン名を補って再度問い合わせる挙動が多いようです。そうすると、これまでは初回の問い合わせに対応するドメイン名が存在しなかったために、ドメイン名が補完され意図したドメイン名で名前解決できていたものが、その後の環境変化で初回の問い合わせに応答が得られた場合、意図しないサイトに接続してしまう可能性があります。新たに登録されたTLDにはtokyoやnycといった地域名も含まれており、サブドメインでこれらの地域名を利用して運用している場合には特に注意が必要です。無論、実際にはすべての追加されるTLDと内部でのサブドメイン運用、DHCPなどで配布するDNSのサーチリストを総合的に見て影響を考える必要があります。利用者にはできるだけ完全なドメイン名でアクセスするように誘導しておくのが将来にわたって安心です。

ICANNでは名前衝突問題を早くから認識しており、影響を軽減するために対策を重ねてきました。先に挙げたCA/Browser Forumの運営基準はICANNとの対話による成果ですし、実際のDNSの問い合わせ状況に基づき、新規のTLD導入の危険性評価もしてきました。調査には主にDNS-OARCのA Day in the Life of the Internet(DITL)プロジェクト[*1]で収集された主要な権威サーバからのデータが利用されました。内部用ドメイン名は組織内などで利用されているはずですが、設定ミスやモバイル端末が外部で接続試行した場合などにDNS問い合わせが外部に漏れ出します。これはrootサーバなどでも検知できるため、勝手TLDの利用を推定することができます。この調査では特にhomeとcorpという勝手TLDを利用した問い合わせが格段に多いことが判明し、これらを新規TLDとして認めると問題が多すぎるということで、この2つに関しては無期限に委任保留する旨を決定しました[*2]。また、それ以外の新規TLDに関してもDITLなどのデータへの出現頻度に基づき、名前衝突の可能性が高い一部のセカンドレベルのドメイン名については、登録を禁止する制限付きで委任されることとなりました。

日本国内でもJPNICで新gTLD大量導入に伴うリスク検討・対策提言専門家チームを設立して、名前衝突問題に関する検討を行い提言を文章としてまとめています[*3]。名前衝突の問題は思わぬ所で影響が出てしまう可能性があるため、組織内の設定や文章に記載したURLなど、今までは問題なく動いていたものも含めて見直し、実は危うい前提に成り立っていないかを今一度確認してみてることをお勧めします。

＊1　https://www.dns-oarc.net/oarc/data/ditl
＊2　https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-1-07oct13-en.pdf
＊3　https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/

3.3 DNSと通信制御

DNSは、Webサイトへの誘導やメールの配送制御など、利用者の通信を制御する機能をもち、また閲覧することもできます。つまり、DNSの応答を変化させることにより、クライアントの通信を制御することができます(図-2)。例えば、世界規模でコンテンツ配信を行っている事業者ではクライアントからのDNS問い合わせに対して遅延の低減や配信の効率化を目的に、クライアント近傍の配信サーバのIPアドレスを応答するように実装している場合もあります。実際には利用者の多くは、ISPなどの提供するDNSキャッシュサーバを利用しているため、コンテンツ事業者の管理する権威サーバではこのDNSキャッシュサーバ単位で利用者をグループ化し、最も適切だと思われるIPアドレスを応答するようにしているようです。一方で攻撃者に悪用された例もあります。攻撃者の管理するDNSキャッシュサーバを参照させて、悪意あるコンテンツをダウンロードさせる場合が多いようです。DNS Changerの事例では端末のDNS参照先を書き換えていますし、更に、ブロードバンドルータのDNS参照先も攻撃者のものに書き換えていたと報告されています。このような悪意あるデータを参照させられないように、DNSの設定には注意を払わなければなりませんが、DNSを取り巻く環境は複雑になってきています。

現状では多くの端末がDHCPの情報に基づいて参照先のDNSキャッシュサーバを設定しています。DHCP機能は組織内の管理者が意識的に運用している場合や、コンシューマ用途ではブロードバンドルータで標準的に提供されている場合があります。ブロードバンドルータでは、DNSの問い合わせをISPなどのDNSキャッシュサーバに単純に中継する機能を実装し、宅内の端末にはルータ自身をDNSの参照先として参照させるものが多いようです。ただしこの実装はDNSの仕様からすると、かなり限定された機能のみが提供されている場合があり、TCPでの問い合わせに対応していなかったり、EDNS0に対応しきれていないものがあるようです。この状況を踏まえて、RFC5625/BCP152[*4]としてブロードバンドルータなどにDNS中継機能を実装する際のガイドラインが公開されています。このガイドラインでは、DNS中継機能を将来にわたって問題なく利用し続けられるように、透過性に注意して実装することが推奨されています。

ブロードバンドルータの一部には、端末の参照先DNS設定に関わらず、通過するすべてのDNS問い合わせをブロードバンドルータに設定されたDNSキャッシュサーバ宛にねじ曲げる機種も存在します。この場合、端末にどんなIPアドレスを参照先DNSとして登録しても、端末からのDNS

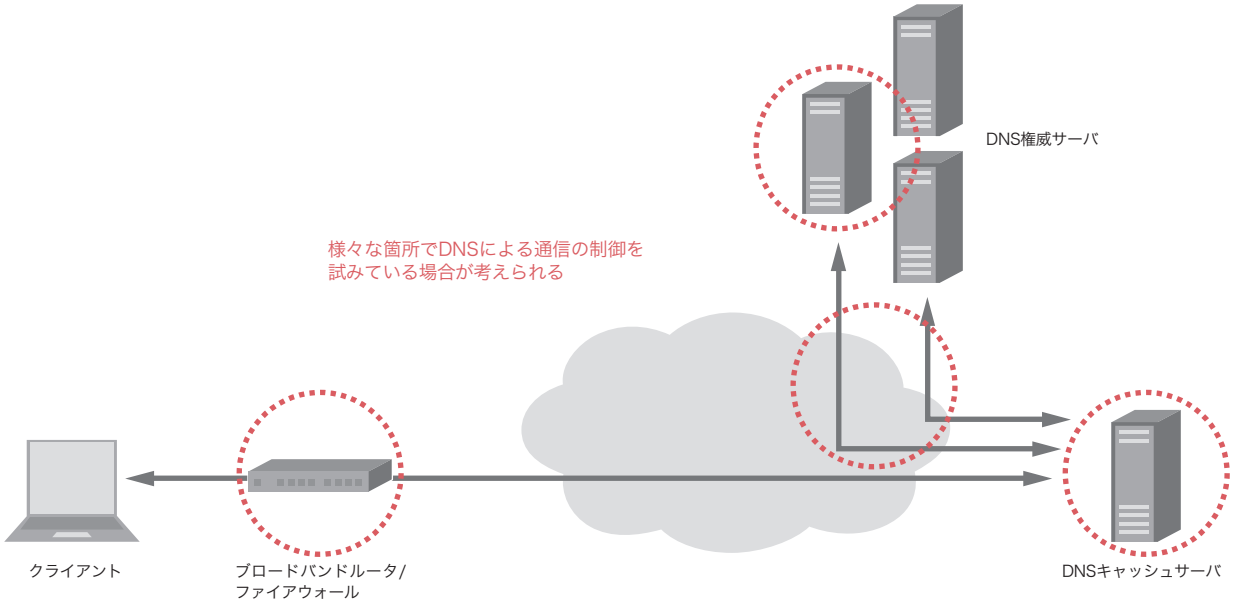

図-2 DNSと通信制御

*4 https://tools.ietf.org/html/rfc5625

問い合わせはブロードバンドルータを経由した瞬間に特定のDNSキャッシュサーバへの問い合わせとして書き換えられてしまうため、端末のDNS設定を見ただけでは実際にどのDNSキャッシュサーバを参照しているか判別できません。これは特定のDNSキャッシュサーバを強制する運用ポリシーの実装には便利な機能かもしれませんが、ひとたび問題が発生すると、利用者もその状態に気が付きにくいので切り分けがとても困難な仕様です。

ISPのDNSキャッシュサーバでも様々な制御が実装されてきています。IPv6閉域網に接続した端末がIPv4のみでインターネット側のサーバと通信する場合、IPv6での接続に失敗し、IPv6/IPv4フォールバックによる遅延や接続障害が発生する場合があります。IPv6でもインターネット接続があれば問題なく通信できるのですが、申し込みが必要であったりルータの更新が必要であったりするため、導入に時間がかかることが懸念されます。このようなユーザ環境での問題を軽減するため、DNSキャッシュサーバでIPv6のレコードであるAAAAレコードに対して応答しない、AAAAフィルタと呼ばれる機能が実装されている場合があります。また、児童ポルノの流通を防止するために、DNSキャッシュサーバで特定ドメイン名の応答を遮断する児童ポルノブロッキング[*5]が実装されている場合もあります。

一部の国や地域によっては、望ましくないコンテンツへのアクセスを遮断するために政府主導でDNSの制御を導入している場合があります。その地域でサービスを提供する各ISPのDNSキャッシュサーバで遮断している場合や、ネットワーク上にDNSの問い合わせを監視する機能を実装し、特定のドメイン名への問い合わせを遮断したり、偽の内容を応答する場合があるようです。ユーザからは通信障害なのか意図された遮断なのか分からない上に遮断ポリシーが明示されることは少ないため、問題なのかどうかも含めて切り分けが困難です。しかし、国や地域によって遮断されるコンテンツに傾向があるため、恐らく意図された遮断であろうとの推測は可能です。このように、DNSでは様々な箇所で制御が実装されている可能性があるため、問題を切り分ける際にはそれらを考慮して障害箇所を見つける必要があります。

3.4 DNSと攻撃

DNSは多くの機器に実装されており、多くのアプリケーションが実質的に依存しているため、攻撃に悪用されたり攻撃の対象となったりすることがあります。主にオープンリゾルバと呼ばれる、誰からの問い合わせにも応答するDNSキャッシュサーバを踏台にしたDNS増幅攻撃は、その増幅効率と攻撃分散の良さから広く悪用されてきました。多くのDNSキャッシュサーバが、何ら対策されないままに誰からの問い合わせにも応答する状態だったために踏台として悪用されました。国内のISPのDNSキャッシュサーバは近年徐々に設定を変更し、そのユーザからのみDNS問い合わせを受け付けるようになってきています。ただし、ブロードバンドルータに実装されいてる一部のDNS中継機能は標準でインターネットからのDNS問い合わせにも制限なく応答してしまうため、踏台として悪用されてしまいます。これらは個別のユーザによる対応が必要となるため、継続的な注意喚起が必要です。

DNSの権威サーバに対する攻撃やその悪用も発生しています。通常のDDoSと同じく、大量のトラフィックを権威サーバ宛に送信して輻輳によるサービス妨害を狙った攻撃や、DNSのプロトコルとしては正常な問い合わせを権威サーバに大量に投げつけてDNS増幅攻撃の踏台に悪用される事例が発生しています。単純な妨害トラフィックであれば適当なパケットフィルタなどで防御できますが、増幅攻撃の踏台として悪用された場合は攻撃を意図した問い合わせを単純に見分けることができないため、対応に検討が必要です。JP DNSを含むいくつかの権威DNSでは、Response Rate Limiting(RRL)と呼ばれる、連続した同一応答を抑制する機能を実装し、影響の軽減に努めています[*6]。ただし、この対策も万能ではないため、引き続き攻撃手法に注視し、適切な対応を模索していく必要があります。

ISPのDNSキャッシュサーバでは、2014年初旬から断続的にいくつかのドメイン名に関する大量のDNS問い合わせを観測しています。意図は不明ですが、恐らく該当ドメイン名の権威サーバに対する分散攻撃であろうと推測しています。ただし、この攻撃に付随した該当権威サーバとの通

*5 http://www.netsafety.or.jp/blocking/
*6 http://www.redbarn.org/dns/ratelimits

信が大量に発生するため、DNSキャッシュサーバでも過負荷になり、DNSキャッシュサーバ利用者の名前解決に遅延が生じるなどの障害が発生する場合があります。攻撃者がこれを意図しているかは別にして、利用者に影響が出てしまうようなら何らかの対策が必要ですが、オープンリゾルバになっているブロードバンドルータが踏台に利用されたり、ユーザの端末に感染したbotからのDNS問い合わせであったりと、ユーザからの通常のDNS問い合わせと同様に見えてしまうため、汎用的な対策が難しい攻撃です。異常な頻度の問い合わせ形式を注視して、都度状況に応じた対策が必要となります。

DNSでは問い合わせプロトコルとして主にUDPが利用されています。UDPはTCPと比べて通信の成りすましが容易で、攻撃者が偽の応答を注入できる可能性があります。偽の応答の注入に成功するには、問い合わせとIPアドレス、ポート番号、DNS ID、QNAMEの情報が一致する必要があります。防御側では問い合わせの該当情報が偽の応答と一致しないように努力する必要があります。DNS IDが既に十分乱数から生成されているとすると、残るは送信元ポート番号に良い乱数を利用することが必須です。送信元ポート番号を固定している古いDNS実装を利用している場合には最新のDNS実装に更新するなどして、推測しにくい問い合わせを送出できるように対策が必要です。また、一部ファイアウォールやNAPT機器では、せっかく問い合わせ元でDNS IDや送信元ポート番号に乱数を利用しても、これらの情報を上書きしてしまうものもあるため、併せて注意が必要です。

多くのDNS関連の攻撃には、送信元IPアドレスの偽装が利用されています。各ネットワークでBCP38[*7]を実装して、送信元IPアドレスの偽装ができない環境が整えば、現在のDNSを悪用した攻撃はほとんどが根絶可能です。BCP38を容易に実装できるようにとuRPF check機能も各社ルータに実装されているため、特に端末が接続しているようなネットワークでは送信元IPアドレスを偽装した攻撃の送出を未然に防げるように、積極的に送信元IPアドレスの検証導入をご検討ください。

3.5 まとめ

DNSはインターネットで多くのアプリケーションが依存する重要なサービスです。これが健康的な状態を維持して利用可能であるためには、権威サーバを始めとして名前解決を行うクライアントやDNSキャッシュサーバ、その他のDNSを仲介する機器が適切な協調のもとに管理、運用されている必要があります。DNSの名前空間は、昨今の新規TLD追加に伴って大きく変化しつつあります。勝手TLDを利用した内部向けのドメイン名や、サーチリストに依存した名前解決を利用している場合には、名前衝突の問題が発生する可能性があります。また、DNSは制御系としても広く利用されており、様々な箇所で制御を試みている可能性があるために複雑さが増してきています。複雑さはそれ自体問題の発生原因となるほか、問題解決の障害にもなるので注意が必要です。DNSに限りませんが、潤沢な帯域やCPU資源を背景に攻撃手法は変化しています。攻撃手法の変化に注視しつつ、時代に即した運用ができるように日々の情報収集や情報交換を心がけることをお勧めします。IIJでも自社の設備の適切な運用はもちろんのこと、必要に応じた情報共有や議論などを通じてインターネットの健康な発展に寄与していきたいと考えています。

執筆者:

松崎 吉伸（まつざき よしのぶ）
IIJ ネットワーク本部 ネットワークサービス部 技術開発課 シニアエンジニア。

*7 http://tools.ietf.org/html/bcp84