

DNS への攻撃と対策

藤原和典 ((株) 日本レジストリサービス)

応
般



DNS への攻撃

ドメイン名システム (Domain Name System, DNS) はインターネットで用いられる名前システムである。インターネットの利用が広まり、重要性が高まるにつれ、DNS への攻撃は増大している。DNS への攻撃は、大きく分けると可用性に対する攻撃 (サービス不能攻撃) と完全性に対する攻撃 (応答を改変) の 2 種類が考えられる。ユーザ視点では、前者は名前解決の失敗のために「インターネットが使えない」や「あるサイトが閲覧できない」というクレームが出る影響となり、後者はユーザが気付かないうちに偽サイトへ誘導されたり、メールなどを奪われるという影響がある。

DNS の概要

ドメイン名はルートを起点とし、63 文字以下のラベルをドットで連結したもので、ラベルごとに階層をなすドメイン名空間を構成する。ドメイン名空間は、ルートを根とし、ルートの子ノードにラベルが 1 つのトップレベルドメイン名 (TLD)、TLD の子ノードに一般組織のドメイン名などが存在する木構造である。DNS では、ドメイン名の階層ごとに階層以下の管理主体を変更でき、それを委任と呼ぶ。委任された単位をゾーンと呼ぶ。主な委任点は、ルート、TLD、一般組織のドメイン名などである。委任する側を親と呼び、委任される側を子と呼ぶ。図 -1 にドメイン名空間の例と DNS の概要を示す。

DNS には、利用者端末に含まれるスタブリゾルバ、名前解決を行うフルリゾルバ、各ドメイン名のデータを保持する権威 DNS サーバという構成要素がある。フ

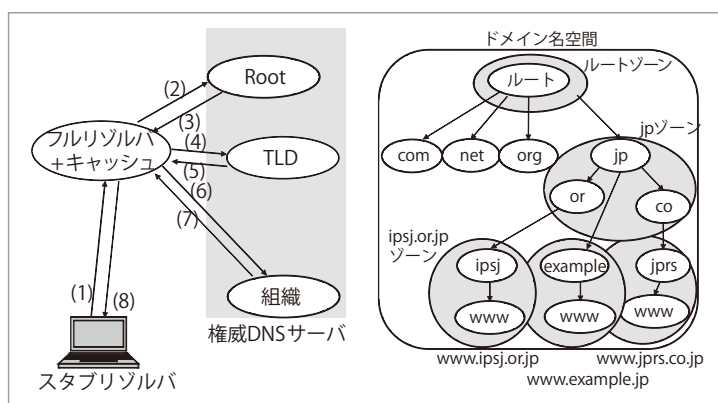


図 -1 ドメイン名と DNS の概要

ルリゾルバ機能を、キャッシュ機能に着目してキャッシュサーバと記述する文献が多いが、本稿では RFC 1035 に書かれている用語である full resolver を用いた。

www.ipsj.or.jp というドメイン名の場合、ルートから jp への委任と or.jp から ipsj.or.jp という委任があり、ルート DNS サーバ、jp TLD DNS サーバ、ipsj.or.jp DNS サーバの 3 つの権威 DNS サーバを用いて名前解決できる。

DNS はドメイン名、タイプ、クラスの組をキーとするデータベースであり、タイプごとに決められた形式の値を保持する。キーと値の組をリソースレコード (RR) と呼ぶ。タイプには、IPv4 アドレスを示す A や、IPv6 アドレスを示す AAAA、委任情報を示す NS、別名変換での正式名を示す CNAME、メールサーバ情報を示す MX などがある。インターネットではクラス IN を用いる。

利用者がブラウザなどにドメイン名を入力すると、図 -1 に示すように、端末からのクエリは ISP^{☆1} などが提供するフルリゾルバに送られ、フルリゾルバがルート、TLD、各組織の権威 DNS サーバに問い合わせ

☆1 Internet Service Provider (プロバイダ)。

名前解決を行い、結果をユーザに返す。図中 (1) (2) (4) (6) は同じドメイン名・タイプのクエリであり、www.ipsj.or.jp タイプ A というクエリの場合、(3) は jp への委任情報を、(5) は ipsj.or.jp への委任情報を、(7) は www.ipsj.or.jp A の情報を返す。フルリゾルバは検索途中の情報と検索結果をキャッシュし、次回の名前解決で使用する。

さらに、DNS に署名検証を追加する DNS セキュリティ拡張 (DNSSEC) が実装されている。

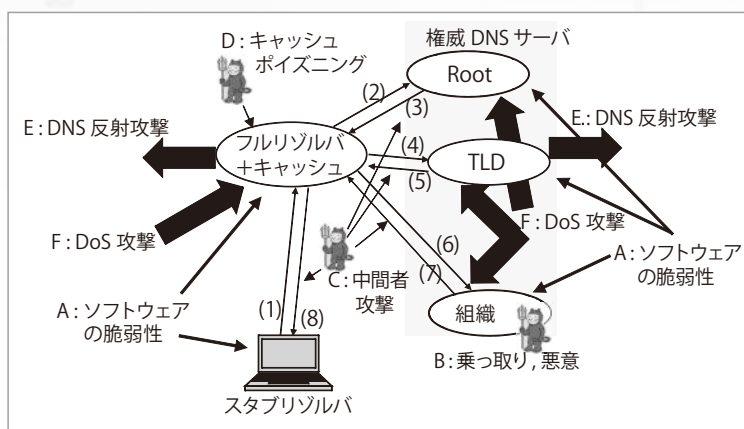


図-2 DNS への攻撃

DNS への攻撃の分類

DNS では、図-1のそれぞれの構成要素と、各要素間の通信路に攻撃が向けられる可能性がある。図-2に考えられる攻撃を示す。(B)、(C)、(D)が完全性に対する攻撃（応答を改変）であり、(F)が可用性に対する攻撃（サービス不能攻撃）、(E)がサービス不能攻撃の加害者になる場合である。また(A)はソフトウェアの脆弱性である。

ソフトウェアの脆弱性

OS やアプリケーション、DNS 関連のソフトウェアには脆弱性が存在することがある。その脆弱性により、キャッシュポイズニングや乗っ取りの原因となることや、サービスを停止することでサービス不能攻撃の原因となることがある。ソフトウェアの脆弱性が公表された場合には影響を考慮した上で遅滞なく修正する必要がある。

ソフトウェア脆弱性への対策は、遅滞なく脆弱性情報を入手し、脆弱性情報に記された対策を行うことである。ソフトウェアや OS の開発元は、脆弱性情報を配布するメーリングリストを運用していることが多く、そこに登録しておくことで公開される脆弱性情報を入手できる。

もう1つの対策として、複数の実装を用いたシステムを構築することで多様性を確保し、ある実装に脆弱性が見つかった場合、システム全体のサービス停止を回避する手法がある。

権威 DNS サーバの乗っ取り・悪意

図-2 (B) は DNS サーバの管理権限を奪われた場合である。権威 DNS サーバを動かすサーバそのものを乗っ取られたり、悪意を持って運用されると、ユーザを悪意のあるサイトに誘導したり、メールを盗むことが容易に可能である。サーバそのものの管理権限を奪われた場合、そのドメイン名を閲覧する一般利用者からは対策ができない。

* 登録情報の不正書き換え

jp や com などの TLD へのドメイン名登録はレジストラと呼ばれる登録代行業者を通じて行うが、登録代行業者での登録者の認証は ID パスワード認証のところが多い。これまで何度も、登録者のアカウントの不正使用やシステムの脆弱性の悪用によるドメイン名の管理権限盗難が報告されている。ドメイン名登録情報を書き換えられると、そのドメイン名の管理権限そのものを奪われる。

中間者攻撃

図-2 (C) は中間者攻撃である。攻撃者は通信路を流れるパケットの中身を監視し、応答の書き換えや偽応答の注入で、正規ではない応答をユーザやフルリゾルバに返すことができる。具体的には、ワイヤレスネットワークの傍受やワイヤタッピング、ファイアウォール機器への機

能追加で実装する。中間者攻撃では確実に応答を改変できるため、攻撃の効果が大きい。

これを国家規模で実装しているところが存在する。巨大なファイアウォールを運用し、通過するパケットを監視し、都合が悪いドメイン名へのアクセスを別のアドレスに誘導する実装例を図-3に示す。すべてのパケットはファイアウォールを通過するため、特定のクエリに対する応答の書き換えや、偽応答の注入で、利用者に書き換えた応答を返す。この例では、利用者が意図した接続先ではない、偽のサーバへ誘導させている。なお、この例では利用者が直接ルート DNS サーバなどの権威 DNS サーバにクエリを送っても書き換えられることがあり、別の環境と応答を比較することで書き換えを推定できる。

多くのネットワークでは盗聴の可能性を否定できないが、特に公衆 Wi-Fi などの暗号化されていない無線ネットワークでは、誰でも通信を傍受でき、DNS クエリを抽出し、偽の応答を(別経路から)容易に注入できる。

対策には、信頼できない通信路を使わない、通信路の暗号化、TSIG^{☆2}によるDNS通信の認証、エンドノードでのDNSSEC検証などがある。また、厳密には中間者攻撃とは異なるが、フルリゾルバ運用者がDNSの応答を改変し、利用者が望まないアドレスへ誘導できる。実装例としては、ISPによる児童ポルノサイトへのアクセス遮断や、2014年春に起きたトルコ政府によるtwitterへのアクセス遮断などがある。

キャッシュポイズニング

図-2(D)をキャッシュポイズニング(キャッシュ汚染)といい、権威DNSサーバからの応答を偽装したパケットなどで、フルリゾルバのキャッシュに偽造したデータを注入する。キャッシュ汚染攻撃は簡単ではないことが多いが、一度注入できるとキャッシュ保持期間にわたり効果が持続する。

1990年代にはNS RRやCNAME RR、MX RRなどの値に含まれるドメイン名の情報を応答に添付する

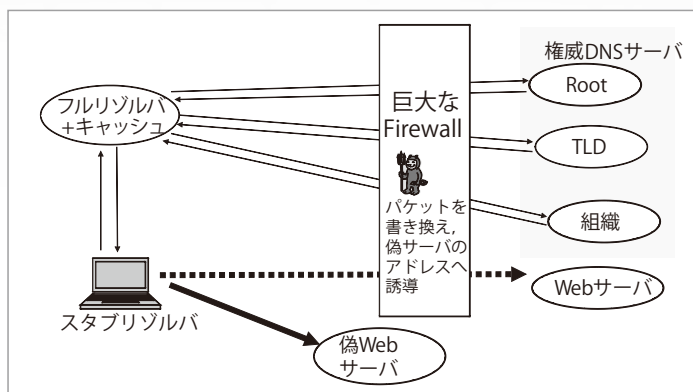


図-3 中間者攻撃の例

タイプの攻撃が行われ、クエリ名に対応する応答以外を捨てるフィルタを実装するという改良をフルリゾルバに実施することで対策された。

現在のキャッシュ汚染攻撃は、図-2の権威DNSサーバからの応答(3)(5)(7)を偽装し、フルリゾルバのキャッシュを汚染する。(3)はTLDへの委任情報、(5)は登録ドメイン名への委任情報であり、(7)は管理権限のある応答か、下位ドメイン名への委任である。フルリゾルバから権威DNSサーバへの通信のパケットの概要を図-4に示す。クエリと応答で、送信元アドレス・ポート番号、宛先アドレス・ポート番号が入れ替わり、QRビット(クエリ/レスポンス:応答)が異なる。IDフィールドと、クエリセクションは同じである。

フルリゾルバは応答パケットを受信すると、同じであるべき項目を検査し、一致した場合クエリに対応する応答パケットとして受け入れる。キャッシュ汚染攻撃では、これらを一致させ、応答セクションや委任情報セクションに注入すべきデータを追加する。フルリゾルバは、正規の応答よりも前に条件が一致した偽装応答を受け取ると正規の応答と区別できないため、偽装応答を受け入れ、キャッシュ汚染が成功する。

キャッシュ汚染攻撃を行う立場に立つと、フルリゾルバが権威DNSサーバに送るクエリに対応する偽装応答を作りたいが、IDフィールドを事前に知ることは困難である。また、ソースポートランダムマイゼーション(SPR)という技術でフルリゾルバが権威DNSサーバに送るクエリのポート番号をランダムに変化させる場合、ポート番号の推定も困難である。攻撃者はIDフィールドとポート番号、(複数ある場合の)権威DNSサーバを事前

☆2 RFC 2845で定義される、共有鍵を使用したDNSトランザクションの認証技術。

に知ることはできず、ランダムな値を指定して大量に送ること、確率的な成功を狙う。そのため、フルリゾルバは送っていないクエリに対する応答を大量に受け取ることになる。

偽装応答を長期にわたって少しずつ、多くのサーバに送るものを“Birthday Attack”といい、試行期間を長くするに従い、成功確率が上がる。短時間に多くのパケットを与えて汚染するものの代表が2008年に公開された Dan Kamin-sky 氏による連続攻撃手法と、Bernhard Müller氏によるノード委任攻撃である。

* 連続攻撃手法

存在しないドメイン名の情報を問い合わせると、権威 DNS サーバはその名前が存在しないという応答を返す。そこで、あるドメイン名（以下、トリガドメイン名とする）にランダムラベルを前置したものをフルリゾルバに送る。フルリゾルバは、そのクエリ名を権威 DNS サーバに問い合わせる。トリガドメイン名の管理権限を持つ権威 DNS サーバは、ランダムラベルがついているドメイン名に対して、通常は名前エラーを返すため、フルリゾルバはランダムラベルがついた名前エラー情報だけをキャッシュし、トリガドメイン名の情報をキャッシュしない。ランダムラベルの変更で、トリガドメイン名に対する攻撃を繰り返すことができる。なお、応答を返す権威 DNS サーバは、トリガドメイン名の管理権限を持つサーバである。

* ノード委任攻撃

図-1のドメイン名空間の例では、ホスト名 www.example.jp は example.jp ゾーン内にあり、委任ではないが、www.example.jp に委任を作る設定は可能で

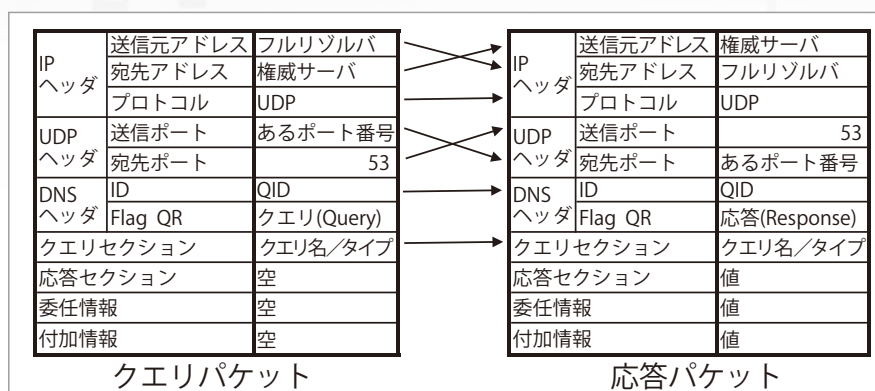


図-4 フルリゾルバと権威 DNS サーバの通信

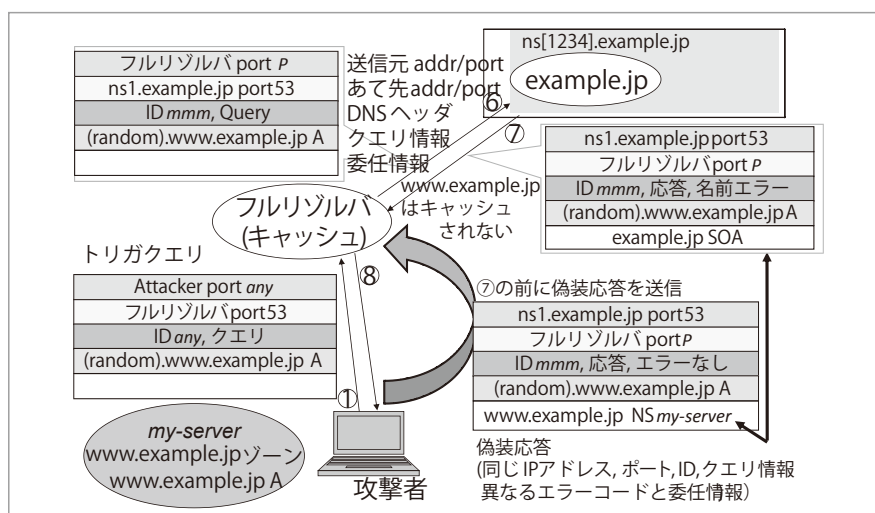


図-5 ノード委任攻撃

ある。つまり、random.www.example.jp というクエリを送った場合に、example.jp の DNS サーバが www.example.jp の委任情報を返すことがある。そこで偽の委任応答を注入するものがノード委任攻撃である。攻撃は図-2の権威 DNS サーバからの応答である(3) (5) (7) のどれに対しても成立する。

図-2の(6) (7)に着目すると、すべての NS RR を持たないホスト名は委任の可能性があり、偽の委任応答を注入できる。注入方法を図-5に示す。www.example.jp には A RR が登録されているとし、example.jp ゾーンの権威 DNS サーバは4台あるとする。利用者が www.example.jp A を検索(図-2の(1))すると、フルリゾルバは example.jp の4台ある権威 DNS サーバのうち、たとえば ns1.example.jp を選択して www.example.jp A クエリを送り、その権威 DNS サーバは www.example.jp A の情報を返す。ここで、www.example.jp をトリガドメイン名とし、ランダムラベルを

前置するクエリを攻撃者が送るとする。フルリゾルバは図-5のトリガクエリを受け取ると、*random.www.example.jp* A クエリを *ns1.example.jp* に送る。*ns1.example.jp* はエラー応答を返すが、攻撃ツールから送信元 IP アドレスを *ns1.example.jp* にした偽装応答を正規の応答の前に送る。送信元ポート番号、ID、クエリセクションなどが一致すればフルリゾルバは受け入れ、委任情報セクションに書かれている情報 (*www.example.jp* は *my-server* に委任する) をキャッシュする。その後、フルリゾルバが *www.example.jp* A クエリを受け取ると、*www.example.jp* は *my-server* に委任されているという情報がキャッシュされているため、*my-server* に対して *www.example.jp* A クエリを送ることになり、*my-server* は *www.example.jp* A に対して任意のアドレスを返すことができる。この攻撃に先立ち、*my-server* に *www.example.jp* ゾーンを準備し、誘導先の *www.example.jp* A を設定しておく。

ノード委任攻撃では、何度でも攻撃を試行できるため、そのうち攻撃が成功する。攻撃成功までの時間の期待値 T は、

$$T = \frac{\text{ID数} \times \text{ポート番号数} \times \text{DNSサーバ数}}{\text{偽装応答送出レート}}$$

となり、偽装応答送出レートが 10 万クエリ/秒で、権威 DNS サーバ数が 4 の場合、SPR しない場合 $T = 65536 * 1 * 4 / 100000 = \text{約 } 2.62 \text{ 秒}$ であり、している場合で $T = 65536 * 64000 * 4 / 100000 = 167772 \text{ 秒}$ (約 2 日) となる。

キャッシュ汚染の対策としては、先述の SPR が有効である。現在のフルリゾルバは、明示的に停止しない限り、SPR を標準で使用する。連続攻撃型のノード委任攻撃では、送信していないクエリに対応する応答が大量にフルリゾルバに到達するため、フルリゾルバの入出力パケットを数えるだけで異常を検知できる。キャッシュ汚染攻撃を受け、偽装応答をキャッシュに注入された場合には、それをキャッシュから消した上でフルリゾルバにそのドメイン名のクエリを送り、別のフルリゾルバの応答と比較して再度の注入を受けていないことを確認する必要がある。

これまで確実にキャッシュ汚染攻撃と分かる攻撃の

報告を聞いたことはなく、SPR している場合には大量の偽装応答を長時間送り続ける必要があるため、現実的には攻撃は困難である。

なお、DNSSEC で攻撃を検知できるが、DNSSEC 対応のドメイン名が少なく、効果が限定的である。

DNS 反射攻撃

図-2 (E) に示す DNS 反射攻撃は、DNS サーバを加害者にするものである。DNS にはクエリよりも応答のほうが大きいことと、トランスポートとして UDP (User Datagram Protocol) を使うという性質があり、UDP には IP アドレスの詐称に弱いという性質がある。詐称した IP アドレスからクエリを送ると、フルリゾルバは詐称された IP アドレスに応答を返すため、詐称されたアドレスに攻撃パケットを送ることになる。フルリゾルバでの対策は、顧客からのアクセスだけを許すようなアクセス制限であるが、顧客から攻撃を受ける可能性は残る。

フルリゾルバや、クエリを中継するフォワードのうち、適切なアクセス制限を行っていないものをオープンリゾルバと呼ぶ。オープンリゾルバに送信元 IP アドレスを偽装した DNS クエリパケットを送ると、クエリパケットの 10 倍以上の大きさの応答パケットを送信元アドレスに送る。

また、権威 DNS サーバもクエリパケットの数倍の応答パケットを返すため、送信元 IP アドレスを偽装することで攻撃に使用できる。権威 DNS サーバでの対策として、応答レートを制限する DNS Response Rate Limiting (DNS RRL) という技術が開発された。

自分が加害者になることを避けるためには、フルリゾルバに適切なアクセス制限を適用し、権威 DNS サーバに DNS RRL を適用する。

サービス不能攻撃

図-2 (F) で示すサービス不能 (Denial of Service, DoS) 攻撃は、サーバソフトウェアの脆弱性を利用してサービスを停止させたり、権威 DNS サーバやフルリゾルバの負荷を上げて応答を得られなくなったり、通信路を溢れさせて応答が戻らないようにする。DoS による効

果は、対象とするドメイン名の名前解決の失敗や、フルリゾルバを使えなくなることである。サーバの脆弱性を原因とする攻撃の場合は脆弱性対策を行うことで攻撃を回避できるが、大量のパケットを送る攻撃の場合は完全な対策は不可能で、攻撃発生後にフィルタなどで絞る対策が主に行われている。

DoS 攻撃を受けた場合は、アクセス制限の徹底と DNS サーバの増強、上流の接続 ISP によるフィルタの適用などを行うぐらいしか対策がない。

* ランダムサブドメイン攻撃

DoS 攻撃の1つとして、2014 年 4 月ごろからランダムサブドメイン攻撃や、DNS 水責め攻撃と呼ばれる攻撃が続いている。図-6 にランダムサブドメイン攻撃の模式図を示す。この攻撃は、クエリ名として攻撃対象のドメイン名にランダムプリフィクスを付けたクエリ名を用い、多くの IP アドレスからフルリゾルバにクエリを送るもので、おそらく攻撃対象の権威 DNS サーバを標的とし、攻撃対象ドメイン名の名前解決の妨害を意図したと考えられる。ところが、ランダムプリフィクスをつけたドメイン名の情報はフルリゾルバのキャッシュに存在しないため、必ず権威 DNS サーバへクエリを送る。権威 DNS サーバが応答しない場合や、応答が遅い場合、フルリゾルバで処理中のクエリが増えてリソースが消費され、名前解決の失敗などが発生する。その結果、「インターネットへのアクセスができない」というクレームが利用者から発生し、一般の新聞でも報道される障害となった^{☆3}。

ISP のフルリゾルバは顧客からのアクセスだけ受け付けるように設定されているが、顧客のマシンが Bot となって攻撃元になった場合や、顧客のブロードバンドルータ (CPE) がオープンリゾルバになっている場合には、顧客の CPE 経由で ISP のフルリゾルバに大量のクエリが到達し、フルリゾルバの負荷が上がることとなる。

ランダムサブドメイン攻撃への根本的な対策はオー

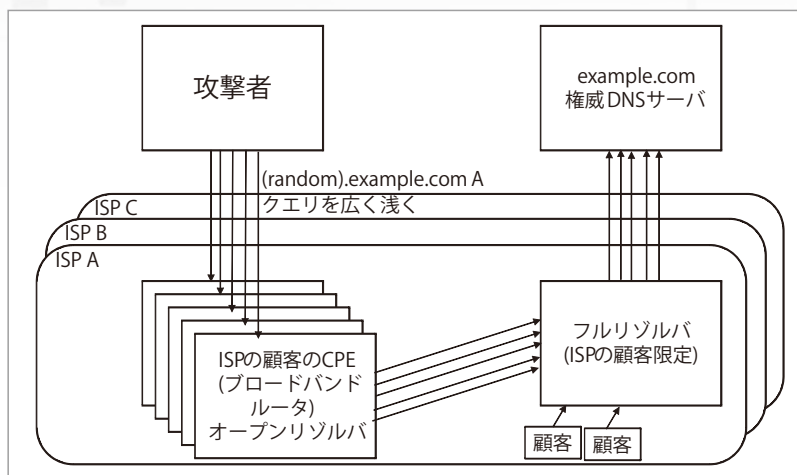


図-6 ランダムサブドメイン攻撃

ンリゾルバをなくすことであるが、困難であり、対症療法的な対策がとられている。さらに、顧客のアドレスへの DNS クエリの多くはオープンリゾルバによる攻撃を目論むものであるとし、フィルタ (Inbound Port 53 Blocking: IP53B) することが検討され、一部実装されている。

前述したノード委任攻撃とランダムサブドメイン攻撃にはランダムプリフィクスを持つクエリを攻撃に使用する共通点があることが興味深い。

対策の整理

本稿では、DNS への攻撃を分類し、対策を紹介した。一般のドメイン名登録者、フルリゾルバ運用者が取り得る対応は限られるが、以下の対策を行うことが重要である。

- 適切なアクセス制限
- 権威 DNS サーバへの DNS RRL の導入
- ソフトウェアの脆弱性対策
- ソースポートランダムマイゼーションなどの標準で有効にされている機能の使用
- 定常的な監視と、異常時の調査

(2015 年 1 月 20 日受付)

藤原和典（正会員）fujiwara@jprs.co.jp

1991 年早稲田大学大学院理工学研究科修士課程修了。1992～96 年早稲田大学情報科学研究教育センター助手。2002 年より (株) 日本レジストリサービス勤務。2010 年より筑波大学大学院博士後期課程在籍。DNS および関連技術の研究開発、標準化に従事。

☆3 2014 年 8 月 2 日 読売新聞（一面）。