DNSの最新動向

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

登録情報の不正書き換えによるドメイン名ハイジャックやDNS水責め攻撃が前年から続く。DNSSECはレジストリでの対応が進むが、各組織での普及が課題。

DNSのセキュリティにおいては、登録情報の不正書き換えによるドメイン名ハイジャックやDNS水責め攻撃の事例が昨年に引き続き話題となった。DNSSECについては、主要なTLDのレジストリで対応が進んでいる一方、各組織の権威DNSサーバーやフルリゾルバー（キャッシュDNSサーバー）における対応は十分とは言えない状況にあり、普及を図っていく上での課題となっている。

■登録情報の不正書き換えによるドメイン名ハイジャック

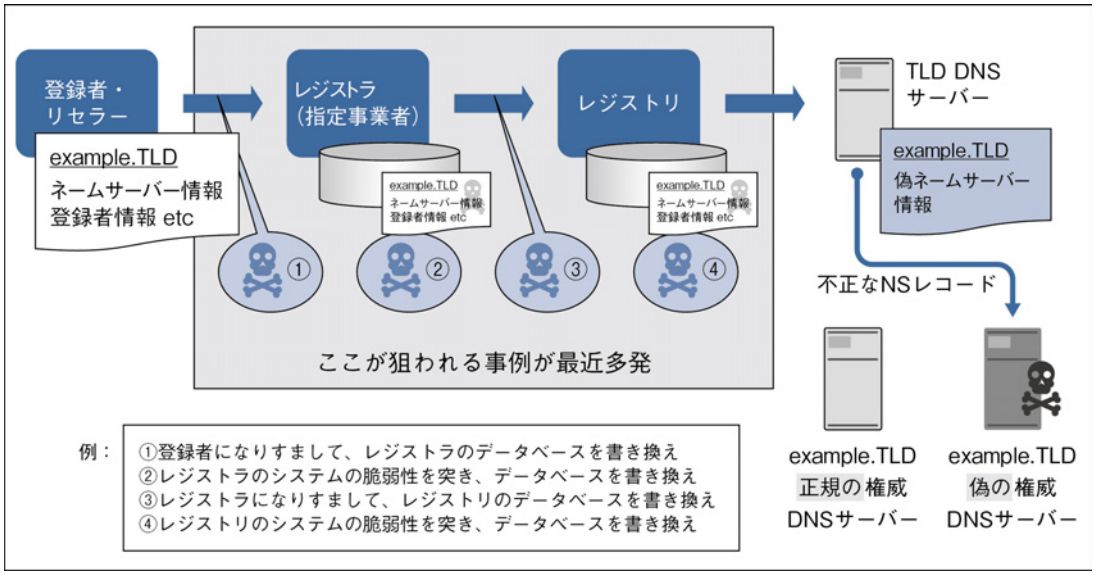
2014年9月から10月にかけ、ドメイン名登録情報の不正書き換えによるドメイン名ハイジャックが、国内の組織が運用する複数の.comサイトに対して実行され、一般メディアでも報道されるなど大きな話題となった。2015年は国内の組織が運用する主なサイトでの被害事例は報告されなかったが、引き続き同攻撃手法による複数の攻撃事例が確認された。

登録情報の不正書き換えによるドメイン名ハイジャックは、レジストリやレジストラに登録されたネームサーバー情報を書き換えることにより、正規のサイトを直接攻撃することなく攻撃者が準備した偽サイトに利用者のアクセスを誘導する手法である。このように、ドメイン名を管理するレジストリやレジストラの登録情報を攻撃対象とすることで、当該サイトを直接攻撃するよりも効率的に攻撃を実現できる場合がある。

登録情報（ネームサーバー情報など）は、登録者→レジストラ→レジストリという流れで申請される[1]。受け取ったネームサーバー情報はレジストリのDNSサーバーに登録・公開される。もし、各システムの脆弱性や認証情報の推定・漏えいなどにより、この流れのどこかで登録情報が不正に書き換えられた場合、偽のネームサーバーに誘導させることができてしまう（資料4-3-14）。

登録情報の不正書き換えを狙ったレジストリやレジストラへの攻撃はこれまでもあったが、誘導先の偽サイトにおいて攻撃者が準備した特定のメッセージや政治的スローガンなどを表示する、いわゆる示威行為にとどまっていた。しかし、前述の国内サイトが被害を受けた事例では、誘導先の偽サイトから特定の利用者に対しマルウェアの注入を図る行為が実行されており、Webサイトのみにとどまらず、その閲覧者も直接の攻撃対象となっていた。そのため、JPCERT/CCやJPRSが、本件に関する緊急の注意喚起を2014年11月5日に公開している[2][3]。

資料4-3-14　ネームサーバー情報の不正書き換え



出典：筆者作成

■ドメイン名ハイジャックの対策

この攻撃手法はレジストリ・レジストラモデルを採用するすべてのTLDに適用可能であり、登録情報を取り扱う関係者それぞれにおいて、適切な対策を考慮・実施する必要がある。対策としては次のものが挙げられる。

●各システムにおける脆弱性対策・情報漏えい対策

登録情報を取り扱う登録者・リセラー・レジストラ・レジストリにおいて、不正アクセスの防止や、不正なコード実行の防止、登録済IPアドレス以外からのアクセスの制限など、適切な脆弱性対策や情報漏えい対策を実施する。

●アカウント管理の適正化によるなりすましの防止

登録者やリセラー、レジストラが申請先のシステムを利用する際のなりすまし防止の手段として、安易なパスワードを利用しないことやパスワードの使い回しをしないことに加え、申請を受け付ける側は二段階認証やクライアント証明書などの高度な認証手段を提供し、申請する側でそれを利用するなどの対策を実施する。

●レジストリロックの設定

一部のTLDのレジストリでは、レジストラに対するオプションサービスとして、レジストリロックを提供している場合がある[4]。登録者、リセラーまたはレジストラがロックの設定をレジストリに依頼することにより、情報の書き換えの際に、電話での確認など、ロックの解除のための特別な手続きを要求する。これにより、登録情報の意図しない書き換えを防止できる。JPRSでも、2015年1月より指定事業者向けにレジストリロックサービスの提供を開始している。

■DNS水責め攻撃

2014年初頭から世界的に観測されているDNS水責め攻撃[5]と呼ばれる攻撃手法についても、引

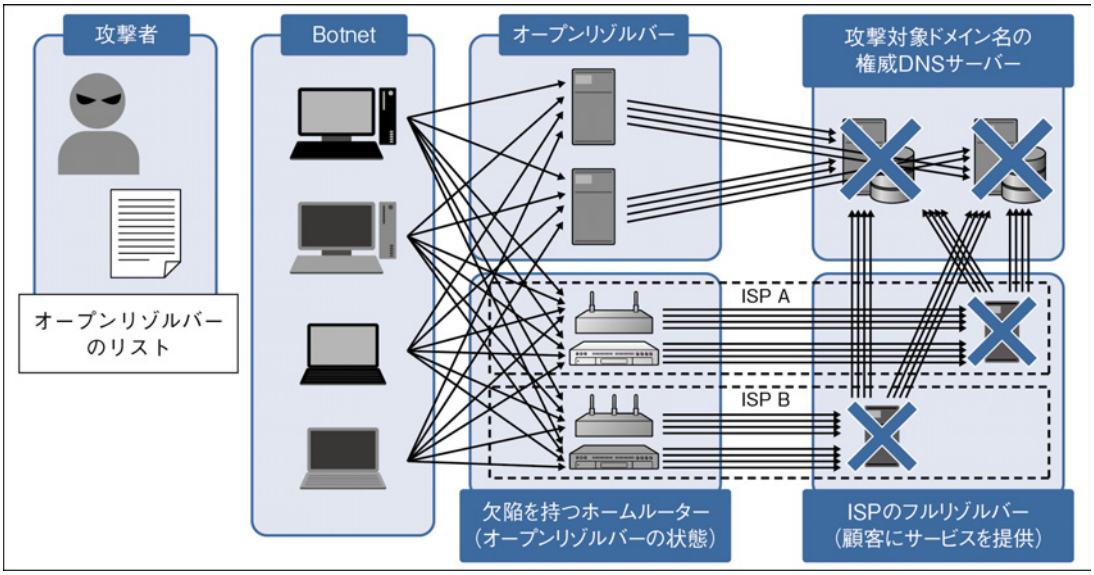
き続き事例が確認されている状態にあり、2015年のDNSのセキュリティにおいて話題となった。

この攻撃はDDoS攻撃の一種であり、DNSリフレクター（DNS amp）攻撃と同様、第三者のオープンリゾルバーやホームルーターを攻撃の踏み台として悪用するが、DNSの応答ではなく、攻撃対象にランダムなサブドメインを付加したDNS問い合わせが直接攻撃に使われる。この問い合わせのパターンはキャッシュポイズニング攻撃の手法であるカミンスキー型攻撃手法[6]で用いられるものに類似している（資料4-3-15）。

DNS水責め攻撃ではカミンスキー型攻撃手法と異なり、キャッシュポイズニングを目的とした攻撃パケット（偽のDNS応答）が検出されないため、この攻撃が最初に観測された段階では、攻撃者の目的が判然としなかった。その後、2014年5月から7月にかけて、数多くのドメイン名がこの攻撃の被害を受け、アクセス不能の状態に陥った。その際の攻撃パターンや攻撃対象の分析結果から、攻撃対象のドメイン名を管理する権威DNSサーバーに大量のDNS問い合わせを送り付けることでサービス不能の状態にし、そのドメイン名をアクセス不能の状態に陥らせることが攻撃者の目的であったと考えられている。

前述した2014年5月から7月の攻撃では権威DNSサーバーに加え、日本国内の複数のISPを含む数多くのフルリゾルバーも過負荷の状態となり、一時的にサービス不能の状態に陥った。

資料4-3-15　DNS水責め攻撃



出典：筆者作成

■DNS水責め攻撃の仕組みと対策

DNS水責め攻撃では、DNS問い合わせにランダムなラベルを付加することでキャッシュ機能を無効化し、DNSの仕組みを攻撃にそのまま利用している。DNSリフレクター攻撃と異なり、問い合わせ元のIPアドレスを詐称する必要がなく、根本的な対策を実施しにくいことが特徴であるが、現時点におけるDNS水責め攻撃の代表的な対策としては次のものが挙げられる。

●フルリゾルバーにおける対策

フルリゾルバーにおいて、攻撃対象ドメイン名の問い合わせに対するフィルタリングの実施、攻撃対象のゾーンをローカルに保持、攻撃対象のゾーンの処理に対する特別なルールの記述などの対策が実施されている[7]。しかし、これらは攻撃発生後の事後対策となること、また、対策により対象ドメイン名に対するDoS自体は成立してしまうことに注意が必要である。

●ISPにおけるIP53Bの実施

IP53B（Inbound Port 53 Blocking）は、顧客側のDNS通信を行うポートである53/udp（DNS）へのアクセスをISP側でブロックすることにより、ホームルーターの欠陥を外部から利用できなくするものである。DNSリフレクター攻撃の対策としても有効であることから、IP123B（NTP）と共に国内外のISPにおいて、導入が進められている。

なお、ISPにおいて本対策を実施する際には通信の秘密の保護の観点から、慎重な検討が必要である。JAIPAなど5団体がまとめた「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」[8]では本対策について、ISPの管理下にある動的IPアドレスに対する場合にのみ、正当業務行為として違法性が阻却されると考えられるとしている[9]。

■DNSSECの状況

DNSSECは、DNSのセキュリティ拡張方式であり、公開鍵暗号方式を用いてDNS応答に電子署名を付加し、受信側でそれを検証することにより応答の出自と完全性を保証するための技術である。DNSSECにより、攻撃者が偽のDNS応答を外部から注入して偽サイトへの誘導を図るDNSキャッシュポイズニング攻撃を検知・防止することができる。

DNSSECを利用するためには、登録情報を管理するレジストリおよびレジストラ、DNS情報を管理・公開する権威DNSサーバー、DNS情報を検索するフルリゾルバーのすべてにおいて、DNSSECへの対応が完了している必要がある。

●レジストリやレジストラにおけるDNSSEC対応状況

ルートゾーンでは2010年7月からDNSSECの運用が開始されており、.jpや.com、.netなど主要なTLDのレジストリでは、DNSSECへの対応を既に完了している。また、2012年に開始された新gTLDプログラムではICANNがレジストリとの契約によりDNSSECへの対応を義務づけていることから、すべての新gTLDのレジストリは運用開始当初からDNSSECに対応している。

レジストラ（.jpでは指定事業者）におけるDNSSEC対応では、ドメイン名登録者から受け取ったDSレコードのレジストリへの取り次ぎや、登録システムにおけるDNSSEC関連情報への対応などが必要であり、一部のレジストラにおける対応にとどまっている。なお、ICANNは新gTLDプログラムにおいてレジストリと同様、新gTLDのレジストラにもDNSSEC対応を義務づけている。

●逆引きゾーンにおけるDNSSEC対応状況

逆引きゾーンについては、地域ごとのIPアドレスの割り振り管理を行うRIR（Regional Internet Registry：地域インターネットレジストリ）、および国ごとのIPアドレスの割り振り管理を行うNIR（National Internet Registry：国別インターネットレジストリ）におけるDNSSEC対応が必要になる。

アジア太平洋地域のRIRであるAPNICをはじめ、五つのRIRでは既にDNSSEC対応を完了して

いる。日本のNIRであるJPNICでもDNSSEC対応を完了し、2015年11月に正式運用（DSレコード登録の受け付け）を開始した[10]。

● DNSサーバー・DNSサービスにおけるDNSSEC対応状況

DNSSECでは権威DNSサーバー側におけるDNSSEC署名、フルリゾルバー側におけるDNSSEC検証のサポートが必要になる。DNSSECに対応している主なDNSサーバーやDNSサービスを示す（資料4-3-16）。

資料4-3-16　DNSSECに対応している主なDNSサーバーソフトウェアやDNSサービス

ソフトウェア／サービスの名称	開発元	権威DNSサーバーにおけるDNSSEC署名	フルリゾルバーにおけるDNSSEC検証
BIND	Internet Systems Consortium, Inc.	○	○
NSD	NLnet Labs	○	−
Unbound	NLnet Labs	−	○
PowerDNS Authoritative Server	PowerDNS.COM BV	○	−
Knot DNS	CZ.NIC z.s.p.o.	○	−
Yadifa	EURid	○	−
Microsoft Windows DNS	Microsoft Corp.	○	○
Nominum Vantio AuthServe	Nominum, Inc.	○	−
Nominum Vantio CacheServe	Nominum, Inc.	−	○
Infoblox Secure DNS	Infoblox Inc.	○	○
CloudFlare Virtual DNS	CloudFlare Inc.	○	−
Google Public DNS	Google Inc.	−	○

出典：筆者作成

●DNSSECの普及に向けた課題

運用の難しさやコストの高さなどから各組織の権威DNSサーバーやフルリゾルバーにおけるDNSSEC対応は十分には進んでいない[11][12]。それらにおける対応を進めていくことがDNSSECの普及を図る上で重要である。

■DNSSECに関する最近の話題

DNSSECに関する最近の話題として、ネガティブトラストアンカーの標準化とルートゾーンにおけるKSKロールオーバーの検討状況について紹介する。

●ネガティブトラストアンカーの標準化

DNSSEC署名されたドメイン名において運用上の事故や設定ミスが発生した場合、DNSSEC検証を有効に設定しているフルリゾルバーでは、そのドメイン名の名前解決そのものができなくなってしまう場合がある。

こうした場合にフルリゾルバー側でそのドメイン名のDNSSEC検証を一時的に無効にし、DNSサービスの継続を可能にするための仕組みであるネガティブトラストアンカー（Negative Trust Anchors）が、2015年9月にRFC 7646として発行された[13]。

RFCには主な実装におけるネガティブトラストアンカーの設定例が記述されており、本機能の標準化により、大手ISPなどにおけるDNSSECの導入障壁が下がることが期待される。

●ルートゾーンにおけるKSKロールオーバーの検討

前述の通り、ルートゾーンでは2010年7月にDNSSECの運用が開始された。DNSSECではセキュリティ上の理由により、署名に用いる鍵（ゾーン署名鍵ZSKと鍵署名鍵KSK）を定期的に更新（ロールオーバー）する必要がある。

鍵のロールオーバー、特にKSKのロールオーバーはDNSSEC運用における重要なイベントであり、過去いくつかのTLDにおいて、KSKのロールオーバーの失敗によるサービスの中断が発生している。また、ルートゾーンのKSKロールオーバーではDNSSECバリデーター[14]に設定されたトラストアンカー[15]の更新も必要になるため、特に慎重な検討が必要になる。

ICANNではKSKのロールオーバーについて、キーセレモニーが必要になった場合[16]または運用開始から5年目以降に実施するとしており[17]、運用開始から5年目を迎えた2015年、KSKのロールオーバーに関する本格的な検討が開始された。

2015年2月にICANNの募集によりデザインチームが組織され、ロールオーバーの計画検討が開始されている。検討結果をまとめた最初の草案が2015年8月に公開され[18][19]、草案に対するパブリックコメントが実施された。現在はパブリックコメントの結果を受けた、デザインチームにおける検討作業が継続されている。

1. 登録者とレジストラの間にリセラー（再販業者）が入る場合もある。
2. 登録情報の不正書き換えによるドメイン名ハイジャックに関する注意喚起（JPCERT/CC）
   https://www.jpcert.or.jp/at/2014/at140044.html
3. （緊急）登録情報の不正書き換えによるドメイン名ハイジャックとその対策について（2014年11月5日公開）（JPRS）
   http://jprs.jp/tech/security/2014-11-05-unauthorized-update-of-registration-information.html
4. オプションサービスであり、有償であることがある。また、サービスを提供しているTLDのすべてのリセラー・レジストラが対応しているわけではない。
5. 本攻撃手法は「DNS水責め攻撃」「ランダムDNSクエリー攻撃」「ランダムサブドメイン攻撃」など、さまざまな名称で呼ばれている。本稿では2014年2月にこの攻撃について報告した米国Secure64 Softwareによる命名「Water Torture」（https://blog.secure64.com/?p=377）に由来する「DNS水責め攻撃」という名称を使用した。
6. DNSキャッシュポイズニング攻撃をより効率的に成立させるための攻撃方法。2008年7月に、セキュリティ研究者のダン・カミンスキー氏が発見した。プロトコル上の脆弱性に起因しており、根本的な対策としてDNSSECの導入が有効である。
7. BIND 9.10.3/9.9.8において、本攻撃の対策のための機能が実装された（ただしデフォルトでは無効に設定）。詳細についてはBINDのソースに付属のマニュアルのfetches-per-serverおよびfetches-per-zoneの項目を参照。
8. 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン 第4版 2015年11月30日
   https://www.jaipa.or.jp/other/mtcs/guideline_v4.pdf
9. 2015年12月に発生した国内ISPにおける障害事例では緊急対策として、同ISPが管理する固定IPアドレスを含むIP53Bが実施された。なお、同ISPでは固定IPアドレスの利用者からの申請により、IP53Bを個別に解除する対応を実施している。
10. 逆引きDNSへのDNSSEC署名の追加と上位ゾーンへのDSレコード登録について
    https://www.nic.ad.jp/ja/topics/2015/20151016-01.html
11. .com、.net、.eduのDNSSEC対応済ドメイン名の数はDNSSEC Scoreboard（http://scoreboard.verisignlabs.com/）で確認できる。
12. クエリタイプDSおよびDNSKEYのDNSクエリーをJP DNSサーバーに送ってくるIPアドレス、つまり、配下にDNSSEC検証を実施しているクライアント／フォワーダーが存在する、あるいは自身DNSSECバリデーターであると判断できるIPアドレスの割合は年に2％程度の割合で増加しているものの、依然としてIPアドレス全体の10％以下にとどまっている。
13. Definition and Use of DNSSEC Negative Trust Anchorshttps://www.ietf.org/rfc/rfc7646.txt
14. DNSSEC検証を実施する主体。通常はフルリゾルバーがバリデーターを担当する。
15. DNSSECにおいて、信頼の連鎖を構築する際の起点となる情報。
16. たとえば秘密鍵の漏洩など、事故が発生した場合。
17. DNSSEC Practice Statement for the Root Zone KSK Operator
    https://www.iana.org/dnssec/icann-dps.txt
18. Root Zone KSK Rollover Plan
    https://www.icann.org/en/system/files/files/root-zone-ksk-rollover-plan-draft-04aug15-en.pdf
19. ルートゾーンKSKロールオーバー計画
    https://www.icann.org/ja/system/files/files/root-zone-ksk-rollover-plan-draft-04aug15-ja.pdf

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～2016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。

http://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