DNSの動向

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

DNSSECの仕組みを利用した攻撃手法「KeyTrap」が発表され、対応が進められた。ICANNがプライベート利用のためのTLD「.internal」の予約と、2回目のルートゾーンKSKロールオーバーの作業日程を発表。

■DNSの役割とその重要性

DNSはドメイン名とIPアドレスの対応など、インターネットに接続されたコンピューターの情報を得るための仕組みである。インターネット上のほとんどのサービスはDNSの利用を前提として構築・運用されているため、その機能に支障が生じた場合、サービスの利用・提供に重大な影響を及ぼす。

DNSは名前解決を要求するスタブリゾルバー、問い合わせと応答を転送するフォワーダー、名前解決を実行するフルリゾルバー、階層構造を構成し、情報を管理・提供する権威DNSサーバーという、役割の異なる構成要素が連携して動作する、分散システムを採用している。

近年、DNSはメールの送信元認証やサーバー証明書発行時の権限確認など、さまざまな用途に使われており、その重要性はますます高まっている。

■KeyTrap脆弱性の公開

2024年2月13日にドイツの国立応用サイバーセキュリティ研究センターATHENEの研究者チームが、KeyTrapという新しいサイバー攻撃手法を発表した[1]。KeyTrapはDNSの構成要素の一つであるフルリゾルバーを主な標的としており、脆弱性に付与される共通の識別番号（CVE-ID）として、CVE-2023-50387が割り当てられている[2]。

●攻撃の手法

KeyTrapでは、攻撃用のゾーンデータを設定した権威DNSサーバーを準備し、名前解決によりフルリゾルバーに注入することで意図しない動作をさせる、という手法が用いられている。この手法による攻撃の流れを図4-3-15に示す。

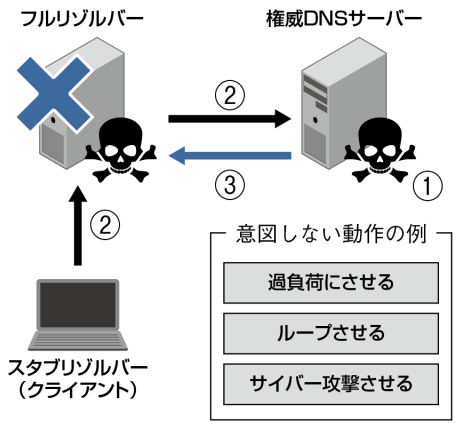
この攻撃手法は2014年に公開されたiDNS Attack[3]、2020年に公開されたNXNSAttack[4]、2021年に公開されたtsuNAME[5]など、既存のサイバー攻撃でも用いられている。

●攻撃の仕組み

KeyTrapはDNSSECの仕組みを利用し、負荷の高いDNSSEC検証処理をフルリゾルバーに強制させることでリソースの枯渇を図り、サービスの提供を妨害する。

DNSSECではゾーン署名鍵（ZSK）と鍵署名鍵（KSK）の分離、鍵の更新（ロールオーバー）、RFC 8901で定義される複数のDNS運用者によるマルチ署名者DNSSECなどを実現するため、1つのゾーンに複数の鍵を設定でき、かつ、1つのリソースレコードセット（RRSet）に複数の署名を追加

資料4-3-15　KeyTrap：攻撃の流れ



① 攻撃用のゾーンデータを設定した権威 DNS サーバーを準備する
② そのデータを応答するドメイン名を名前解決させるように仕向ける
③ フルリゾルバーに応答を注入することで意図しない動作をさせる

出所：筆者作成

できるように設計されている。

鍵の識別を容易にするため、DNSSECでは鍵に対応する鍵タグが付与される。鍵タグはDNSKEYレコードからチェックサム計算される、16ビットの数値である。

KeyTrapの攻撃パターンの例を資料4-3-16に示す。例1では鍵タグを衝突させた多数のZSKと検証に失敗する多数の署名を権威DNSサーバーに準備し、検証させることで多数の署名検証処理を、例2ではハッシュ値照合エラーになる多数のDSレコードと鍵タグを衝突させた多数のKSKを権威DNSサーバーに準備し、照合させることで多数のハッシュ値照合処理を、それぞれフルリゾルバーに強制している。

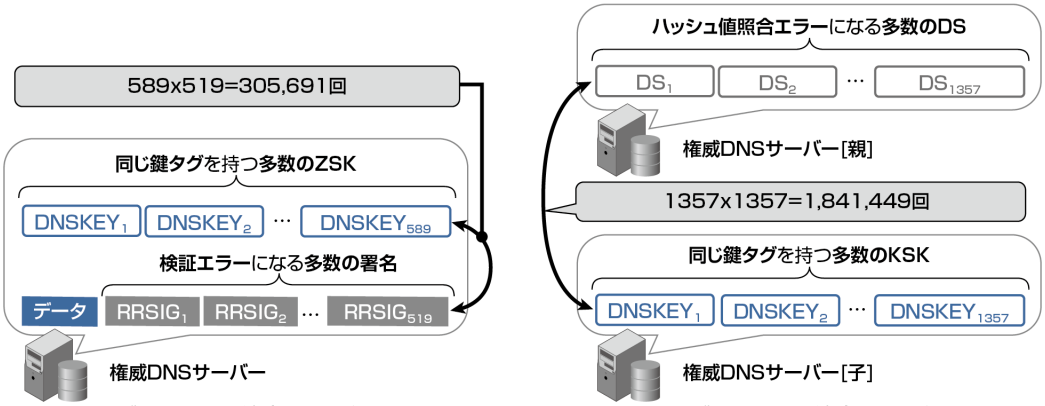
●攻撃の効果と開発者の後悔

DNSSECの仕様を定めているRFC 4035とRFC 6840では、すべての署名の検証に失敗した場合のみ検証失敗（Bogus）と判定すべきであり（SHOULD）、かつ、一致する公開鍵の候補がなくなるまで検証を試さなければならない（MUST）と定められている。

KeyTrapはこの仕様を利用し、鍵タグを意図的に衝突させた多数の鍵や、検証・照合に失敗する多数の署名・ハッシュを処理させることで、攻撃を成立させる。実装の種類やサーバーの性能などにより攻撃の効果は異なるが、実験環境において1度の応答でBIND 9のフルリゾルバーを16時間以上にわたってサービス停止可能であった旨が、研究者から報告されている。

なお、DNSの基本仕様を定めているRFC 1034には、名前解決において無限ループに陥ったり、リクエストや問い合わせの連鎖反応が引き起こされたりしないように作業量を抑制することが、リゾルバーに推奨される最優先事項である旨が記述されている。ISCでBIND 9の開発に携わるペトル・シュパチェック氏はKeyTrapの公開時にこの記述を引用する形で、「我々は聞く耳を持たな

資料4-3-16　KeyTrap：攻撃パターンの例



出所：筆者作成

かった（We did not listen）」という後悔を同社の公式ブログで発表している[6]。

●実装・サービスにおける対応の状況

KeyTrapはDNSSECの仕組みを利用した攻撃手法であるため、さまざまなDNS実装・サービスが脆弱性の対象となった。対象となった主な実装・サービスの一覧を資料4-3-17に示す。

KeyTrapの対策は、脆弱性を報告した研究者と実装・サービスの開発者が連携する形で進められた。2023年11月2日に研究者から関係者に情報が限定公開され、主な実装・サービスにおける対策の完了を研究者が確認した後、2024年2月13日に情報が公開されている[7]。

実装・サービスにおける対策はいずれも、名前解決におけるDNSSEC検証の作業量を抑制する形で実施されている。

■.internal TLDの予約

2024年7月29日のICANN理事会で、組織内で利用するプライベート利用のためのトップレベルドメイン（TLD）として、.internalを予約することが決議された[8]。

●本件の背景

IPv4ではプライベート利用のためのIPアドレスとして、プライベートIPアドレスが定義されている[9]。そのIPアドレスブロックは10.0.0.0/8、172.16.0.0/12、192.168.0.0/16の3つであり、ホームルーターのLAN側IPv4アドレスのデフォルト設定など、さまざまな場面で広く利用されている。

一方、DNSにはプライベート利用のための名前空間は定義されておらず、一部の組織や通信機器ベンダーがそうした用途のドメイン名として、ルートゾーンに存在しないTLDをアドホックに割り当てて使うことが半ば常態化している。こうした状況はルートサーバーに送られる無駄なDNS問い合わせの増加の原因の一つとなっており、かつ、2012年のgTLD追加募集において、組

資料4-3-17　KeyTrap：攻撃パターンの例

種類	対象となった主な実装・サービス
フルリゾルバー	Akamai CacheServe、BIND 9、Knot Resolver、PowerDNS Recursor、Unbound、Windows DNS Server
パブリック DNS サービス	1.1.1.1、Google Public DNS、Quad9、OpenDNS
DNS ツール	delv、DNSViz、ldns-verify-zone、kzonecheck
DNS ライブラリ	dnspython、getdns、ldns、libunbound

出所：KeyTrap の論文を基に筆者作成

織内で使用中の名前がインターネットのドメイン名と衝突する、名前衝突の問題として顕在化するに至っている[10]。

今回の予約はそうした状況を改善するため、セキュリティと安定性に関する問題を取り扱うICANNの諮問委員会であるSSACがまとめた、SAC113[11]勧告に基づいて実施されたものである。

●特殊用途ドメイン名への登録に関する状況

.exampleや.testなど、通常のインターネットの利用以外の特殊な用途に使われるドメイン名として、特殊用途ドメイン名（Special-Use Domain Names）が設定・予約されている[12]。本稿の執筆時点でIANAに登録されている特殊用途ドメイン名の例を、資料4-3-18に示す。

今回予約された.internalもその用途から、特殊用途ドメイン名に登録すべきドメイン名となる。特殊用途ドメイン名の登録にはIETFでの標準化、またはIESGの承認が必要であるため、2024年8月2日にIANAのキム・デイビーズ氏とICANNのアンドリュー・マッコナキー氏がプライベート利用のためのTLDに関するインターネットドラフトを、IETFに提出している[13]。

●今後の展望と運用における最善策

本稿執筆時点で、特殊用途ドメイン名に関するICANNとIETF間の連携のプロセスは定められておらず[14]、.internalの特殊用途ドメイン名への登録には、ある程度の時間を要する見込みである。

なお、前述したSAC113勧告には、プライベート利用のためのドメイン名には当該組織やネットワークで使用中のドメイン名のサブドメインを使うことが最善策であり、プライベート利用のためのTLDの予約後もその点に変化がないことが記述されている。

■ルートゾーンKSKロールオーバーの状況

DNSSECではセキュリティ上の理由により、定期的な鍵の更新が必要になる。ルートゾーンKSKロールオーバーはルートゾーンのDNSSEC鍵署名鍵（KSK）を更新するための、一連の作業手続きである。

●ルートゾーンKSKロールオーバーの手順

ルートゾーンKSKロールオーバーはいくつかの手順を経て実施される。主な手順を以下に示す。

1：新しいKSK（新KSK）の生成
2：ルートゾーンで新KSKを事前公開
3：新KSKへの切り替え
4：旧KSKの失効

初回となる前回の新KSKへの切り替えは、2018年10月11日に実施されている[15]。ICANNはソフトウエアやデバイスにおける十分な対応期間を

資料4-3-18　特殊用途ドメイン名の例

ドメイン名	定義される RFC	用途
alt	RFC 9476	DNS でない名前空間
example.com	RFC 6761	例示用ドメイン名（example.net、example.org も同様）
home.arpa	RFC 8375	家庭用ネットワーク
local	RFC 6762	マルチキャスト DNS と DNS の共存
onion	RFC 7686	Tor ネットワーク上のサービス識別
resolver.arpa	RFC 9462	暗号化リゾルバーの検出
test	RFC 6761	テスト用ドメイン名

出所：筆者作成

確保するため、2回目となる今回のルートゾーンKSKロールオーバーにおける新KSKの事前公開期間、すなわち2から3までの期間を、2年間とする旨を発表している。

●HSMの切り替えに伴う作業中断

ICANNは2023年3月2日に発表したスケジュールで、2023年4月27日に新KSKを生成し、2024年1月からルートゾーンで事前公開することを予告していた[16]。

しかし、ルートゾーンの鍵の生成に使っているハードウエアセキュリティモジュール（HSM）のベンダーが製造・サポートの終了を発表し、代替ベンダーへの切り替えが必要になったことから手順の再設計が必要になり、作業が中断されていた[17]。

●作業日程の決定

手順が再設計され、HSMに関する問題が解消されたことを受け、ICANNは2024年2月28日に、2024年4月26日のルートKSKセレモニー[18]で新KSKを生成することと、2025年1月から新KSKをルートゾーンで事前公開することを発表した[19]。

その後、2024年11月5日のroot-dnssec-announceメーリングリストへの投稿で[20]、生成された新KSK（KSK-2024）の情報と、具体的な作業日程を発表した。発表された日程は以下の通りである（タイムゾーンはいずれもUTC）。

・新KSKの事前公開：2025年1月11日
・新KSKへの切り替え：2026年10月11日
・旧KSKの失効：2027年1月11日

■DNSソフトウエアの脆弱性の状況

●BINDの状況

2024年中にJPRSが注意喚起したBINDの情報を資料4-3-19に示す。

2024年は本稿で解説したKeyTrapのほか、権威DNSサーバーとフルリゾルバーの双方が対象となるため、影響が広範囲に及ぶCVE-2023-4408、CVE-2024-0760が公開されており、適切な対応が必要である。

●BIND以外のDNSソフトウエアの状況

2024年中にJPRSが注意喚起したBIND以外のDNSソフトウエアの情報を資料4-3-20に示す。

2024年はKeyTrapに関する複数の注意喚起を実施したほか、Unboundにおける影響が特に大きかったDNSBomb（CVE-2024-33655など）に関する注意喚起を公開している[21]。

資料 4-3-19　2024 年に JPRS が注意喚起した BIND の情報

公開・更新日	タイトル	概要
2024 年 2 月 14 日	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2023-5517）	nxdomain-redirect の実装不具合
2024 年 2 月 14 日	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2023-5679）	serve-stale の実装不具合
2024 年 2 月 14 日	（緊急）BIND 9.x の脆弱性（メモリ不足の発生）について（CVE-2023-6516）	キャッシュクリーニングの実装不具合
2024 年 2 月 14 日	（緊急）BIND 9.x の脆弱性（過剰な CPU 負荷の誘発）について（CVE-2023-4408）	計算量が多くなる DNS メッセージを処理させる
2024 年 2 月 14 日	（緊急）BIND 9.x の脆弱性（過剰な CPU 負荷の誘発）について（CVE-2023-50387）	KeyTrap 脆弱性
2024 年 2 月 14 日	（緊急）BIND 9.x の脆弱性（過剰な CPU 負荷の誘発）について（CVE-2023-50868）	計算量が多くなる NSEC3 を検証させる
2024 年 7 月 24 日	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2024-4076）	serve-stale の実装不具合
2024 年 7 月 24 日	（緊急）BIND 9.x の脆弱性（過剰な CPU 負荷の誘発）について（CVE-2024-1975）	SIG(0) の実装不具合
2024 年 7 月 24 日	（緊急）BIND 9.x の脆弱性（パフォーマンスの低下）について（CVE-2024-1737）	リソースレコードの処理の実装不具合
2024 年 7 月 24 日	（緊急）BIND 9.x の脆弱性（named の動作不安定）について（CVE-2024-0760）	DNS メッセージの受け付け処理の実装不具合
2024 年 12 月 24 日	BIND 9.20.x の QPzone の実装における不具合について	インメモリデータベース QPzone の実装不具合

出所：筆者作成

1. KeyTrap – ATHENE
https://www.athene-center.de/en/keytrap
2. CVE-2023-50387 | CVE
https://www.cve.org/CVERecord?id=CVE-2023-50387
3. The Infinitely Delegating Name Servers (iDNS) Attack | ANSSI
https://cyber.gouv.fr/publications/infinitely-delegating-name-servers-idns-attack
4. NXNSAttack - NXNSAttack by Lior Shafir, New DNS DDoS vulnerability
https://www.nxnsattack.com/
5. tsuNAME - Vulnerability that can be used to DDoS DNS
https://tsuname.sidnlabs.nl/
6. BIND 9 Security Release and Multi-Vendor Vulnerability Handling, CVE-2023-50387 and CVE-2023-50868 – ISC
https://www.isc.org/blogs/2024-bind-security-release/
7. [2406.03133] The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC
https://arxiv.org/abs/2406.03133
8. Approved Resolutions | Special Meeting of the ICANN Board | 29 July 2024
https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-special-meeting-of-the-icann-board-29-07-2024-en#section2.a
9. RFC 1918: Address Allocation for Private Internets
https://www.rfc-editor.org/rfc/rfc1918
10. Name Collision Resources & Information – ICANN
https://www.icann.org/resources/pages/name-collision-2013-12-06-en
11. SAC113 SSAC Advisory on Private-Use TLDs
https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-113-en.pdf
12. Special-Use Domain Names
https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml
13. draft-davies-internal-tld-01 - A Top-level Domain for Private Use
https://datatracker.ietf.org/doc/draft-davies-internal-tld/
14. RFC 8244: Special-Use Domain Names Problem Statement
https://www.rfc-editor.org/rfc/rfc8244.html
15. 最初のルート KSK ロールオーバーが正常に完了
https://www.icann.org/en/announcements/details/first-root-ksk-rollover-successfully-completed-15-10-2018-ja
16. ICANN Announces Schedule to Generate New Keys for KSK Key Rollover
https://www.icann.org/en/announcements/details/icann

資料 4-3-20　2024 年に JPRS が注意喚起した BIND 以外の DNS ソフトウエアの情報

公開・更新日	タイトル	概要
2024 年 2 月 16 日	Knot Resolver の脆弱性情報が公開されました（CVE-2023-50387、CVE-2023-50868）	KeyTrap 脆弱性・NSEC3 脆弱性
2024 年 2 月 16 日	PowerDNSRecursor の脆弱性情報が公開されました（CVE-2023-50387、CVE-2023-50868）	KeyTrap 脆弱性・NSEC3 脆弱性
2024 年 2 月 16 日	Unbound の脆弱性情報が公開されました（CVE-2023-50387、CVE-2023-50868）	KeyTrap 脆弱性・NSEC3 脆弱性
2024 年 2 月 16 日	Windows DNS の脆弱性情報が公開されました（CVE-2023-50387、CVE-2024-21342、CVE-2024-21377）	KeyTrap 脆弱性、ほか 2 件の実装バグ
2024 年 3 月 12 日	Unbound の脆弱性情報が公開されました（CVE-2024-1931）	拡張エラー（EDE）内部処理の不具合
2024 年 4 月 12 日	Windows DNS サーバーの脆弱性情報が公開されました（CVE-2024-26221、他 6 件）	リモートコード実行（RCE）脆弱性 7 件
2024 年 4 月 30 日	PowerDNSRecursor の脆弱性情報が公開されました（CVE-2024-25583）	フォワーダー機能の実装不具合
2024 年 5 月 13 日	Unbound の脆弱性情報が公開されました（CVE-2024-33655）	DNSBomb の高効率な踏み台として利用可能
2024 年 8 月 16 日	Windows DNS の脆弱性情報が公開されました（CVE-2024-37968）	DNS スプーフィング可能
2024 年 10 月 7 日	PowerDNSRecursor の脆弱性情報が公開されました（CVE-2024-25590）	特別に細工された応答で DoS 攻撃可能
2024 年 10 月 7 日	Unbound の脆弱性情報が公開されました（CVE-2024-8508）	特別に細工された応答でパフォーマンスが大幅に低下
2024 年 11 月 15 日	Windows DNS の脆弱性情報が公開されました（CVE-2024-43450）	DNS スプーフィング可能

出所：筆者作成

-announces-schedule-to-generate-new-keys-for-ksk-key-rollover-02-03-2023-en

17. Root Zone KSK HSM Update - root-dnssec-announce - lists.icann.org
https://lists.icann.org/hyperkitty/list/root-dnssec-announce@icann.org/thread/IBFBNNHBKSXQ5HRNJMEFLE6NKSDKCJQA/

18. ルートゾーンの DNSSEC 鍵を生成する、一連の手続き

19. I CANN to Generate New DNS Cryptographic Key at April 2024 Ceremony
https://www.icann.org/en/announcements/details/icann-to-generate-new-dns-cryptographic-key-at-april-2024-ceremony-28-02-2024-en

20. Upcoming changes to the DNSSEC root trust anchor - root-dnssec-announce - lists.icann.org
https://lists.icann.org/hyperkitty/list/root-dnssec-announce@icann.org/thread/6FJBYQQGCJM3KV6ZOZKDOFURCXXPEU3D/

21. DNSBomb
https://dnsbomb.net/

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および株式会社インプレスが1996年～2025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 | インプレス・サステナブルラボ | ✉ iwp-info@impress.co.jp