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インフラへのDDoS攻撃やDNSクエリによる情報抜き取り、BINDの脆弱性といった脅威が報告されたほか、セキュリティ向上のためにルートゾーンのDNSSEC鍵署名鍵の更新に向けた作業が進められた。

■権威DNSサーバーを標的としたDDoS攻撃

2016年は、DNSにとって重要なサービスであるルートサーバーや、DNSサービスプロバイダー大手の米Dynなど、権威DNSサーバーを標的としたDDoS攻撃が相次いで発生した。日本国内でも、2016年8～9月に発生したDDoS攻撃において、ウェブサーバーと共に権威DNSサーバーが攻撃対象となり、複数のウェブサイトやECサイトが一時的にサービス不能の状態に陥った。

●Dynに対するDDoS攻撃

米国時間2016年10月21日に発生したDynに対するDDoS攻撃では、同社のDNSサービスの顧客である複数の著名なインターネットサービスに影響が及び、世界的に大きな話題となった。

この攻撃には、セキュリティジャーナリストのBrian Krebs氏が運営するブログ「Krebs on Security」に対するDDoS攻撃にも利用された、Miraiと呼ばれる攻撃ツールが使われたことが判明している。Miraiはインターネットに接続されたネットワークカメラや家庭用ルーターなど、さまざまなIoT機器のセキュリティ上の欠陥を突いてそれらの機器を乗っ取り、Botnet[1]を構築することで、極めて大規模なDDoS攻撃[2]を可能にするプログラムである。2016年9月下旬に匿名のインターネットユーザーによってソースコードがインターネット上に公開され、現在では誰でも利用可能な状態になっている。

●有効な対策

こうした権威DNSサーバーに対するDDoS攻撃に対し、インターネットサービスの提供者やウェブサイトの運用者が取り得る有効な対策の一つとして、複数のDNSサービスプロバイダーを併用し、それぞれのDNSサーバーやDNSサービスの停止に備えることが挙げられている。

実際、今回のDynに対するDDoS攻撃では、障害発生時にDynのDNSサービスのみを利用していたウェブサイトは大きな影響を受けたが、複数のDNSサービスを併用していたウェブサイトでは、サービスを継続できていた旨が報告されている。DNSは分散型のプロトコル／サービスであり、普段からこうした冗長化を図っておくことで、サービスの可用性を高めることが可能になる。

■DNSを通信手段として用いるマルウェア

DNSを通信に用いてファイアウォールなど

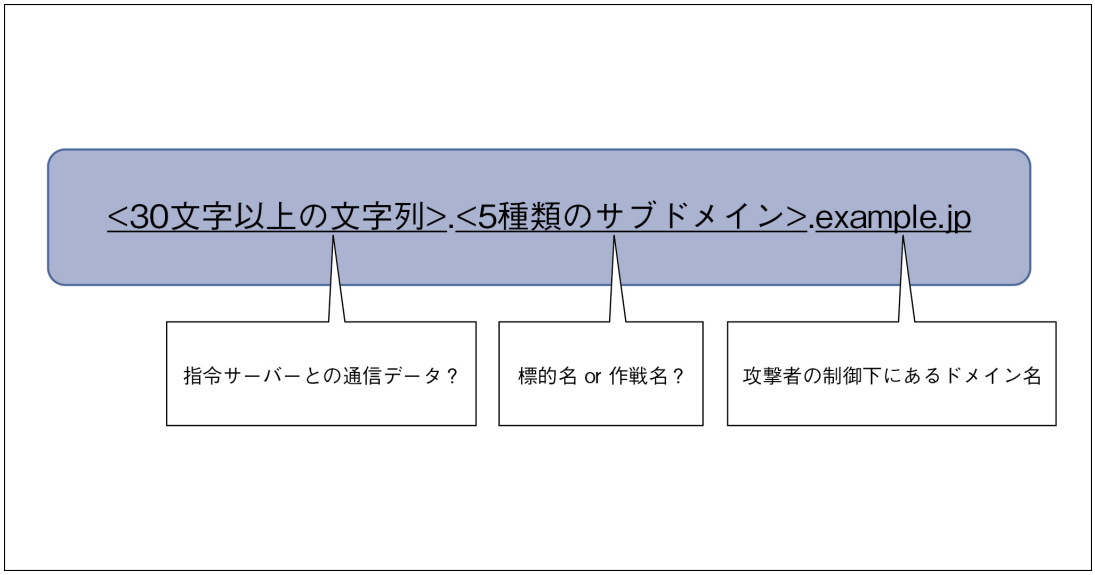
をすり抜ける手法はDNSトンネリング（DNS tunneling）と呼ばれており、従来知られている通信手段の一つである。2016年はDNSクエリの名前情報（QNAME）を通信手段として用いるマルウェアが、相次いで報告された。

●遠隔操作ウイルスの制御

セキュリティ企業のラックは2016年2月1日、遠隔操作ウイルスの制御にDNSクエリの名前情報を利用するマルウェアに関する注意喚起を公開した[3]。

この事例では、暗号化された通信データや標的名／作戦名と推察される文字列をサブドメインに設定したDNSクエリを、Botと指令サーバー間の通信に利用していたことが判明している（資料4-2-1）。

資料4-2-1　DNSクエリによる遠隔操作ウイルスの制御



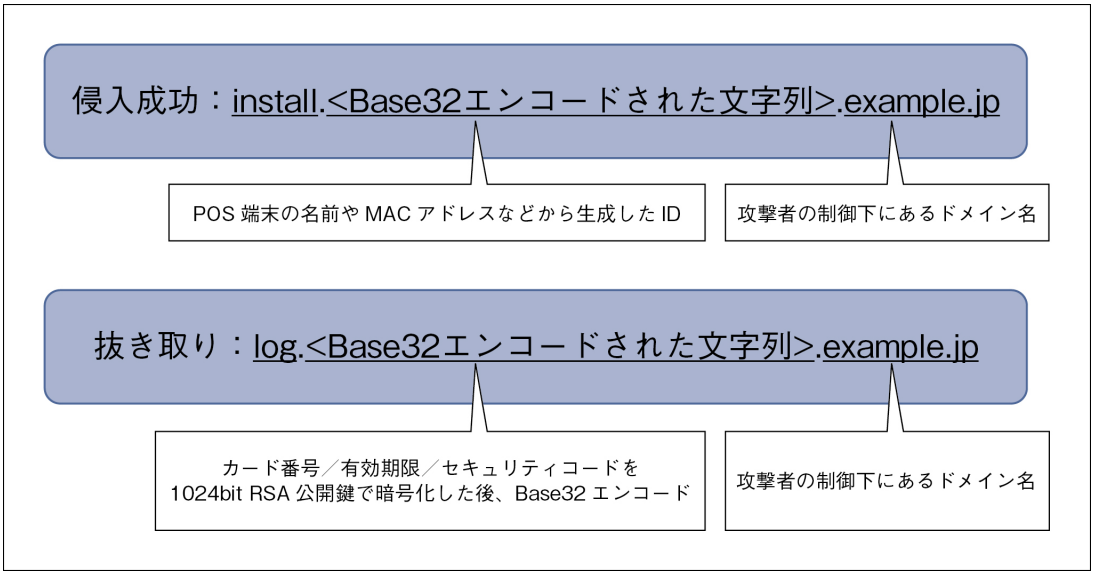
出典：著者作成

●クレジットカード情報の抜き取り

米国のセキュリティ企業FireEyeは2016年4月19日、感染したPOS端末からDNSクエリの名前情報を通信手段としてクレジットカード情報を抜き取る、MULTIGRAINと呼ばれる新種のマルウェアに関する注意喚起を公開した[4]。

MULTIGRAINでは、DNSクエリによってPOS端末への感染（侵入成功）の伝達や入手したクレジットカード情報の抜き取りを実行している（資料4-2-2）。

資料4-2-2　DNSクエリによるクレジットカード情報の抜き取り

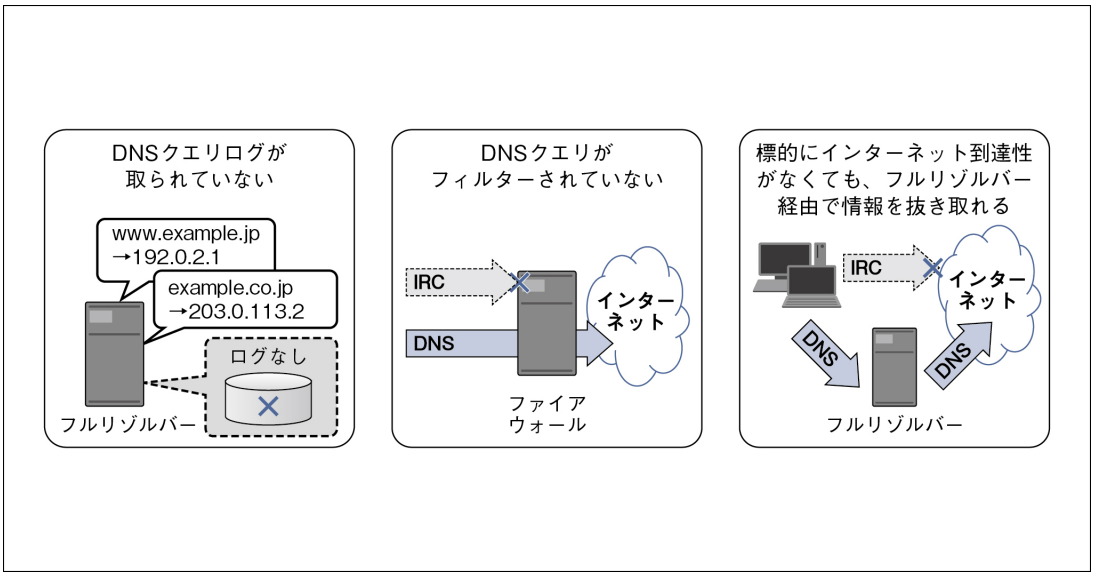


出典：著者作成

●DNSクエリが通信に利用される背景

DNSクエリを通信手段として用いるマルウェアが出現した背景として、攻撃者から見た場合に、以下のようなメリットがあることが挙げられる（資料4-2-3）。

資料4-2-3　DNSクエリが通信に利用される背景



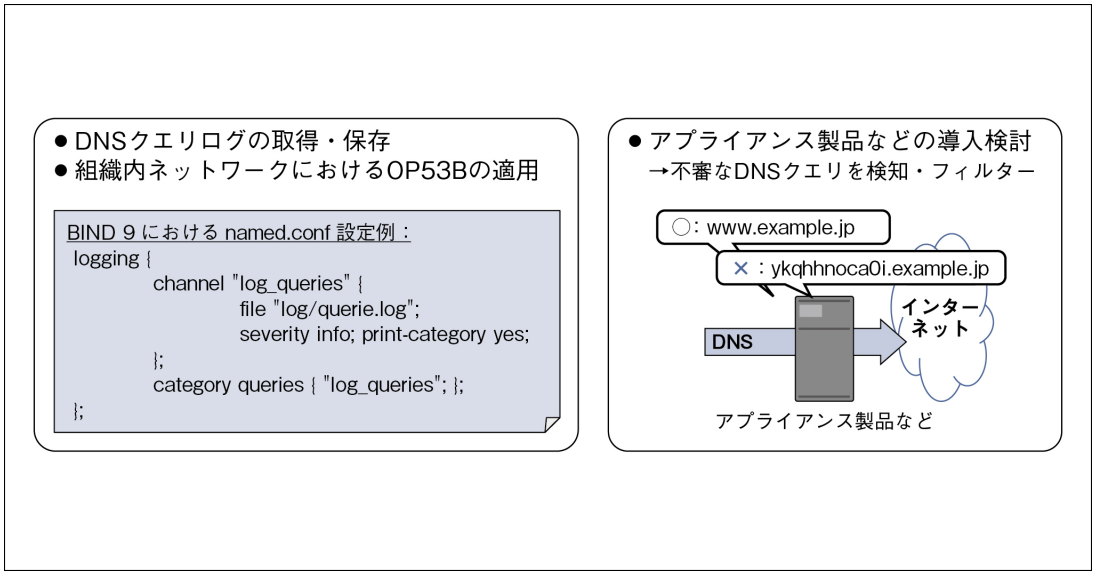
出典：著者作成

・組織内ネットワークにおいてDNSクエリログが取られていないことが多く、マルウェアの活動状況を把握されにくい。
・外部に対するDNSクエリはフィルターされていないことが多く、情報伝達や情報の抜き取りに利用しやすい。
・情報収集に用いるドメイン名を頻繁に変更することで、DNSクエリに対するフィルターの回避や、活動状況の隠ぺいを図れる。
・マルウェアを感染させる標的そのものにインターネット到達性がなくても、フルリゾルバー（キャッシュDNSサーバー）経由で情報を抜き取れる可能性が高い。

●有効な対策

こうしたマルウェアに対する有効な対策として、以下の項目が挙げられる（資料4-2-4）。

資料4-2-4　有効な対策例



出典：著者作成

〈DNSクエリログの取得・保存と内容の調査〉

状況を把握し、問題が発生した際の調査を可能にするため、各組織で運用されているフルリゾルバーにおいてDNSクエリログを取得・保存しておくことが必要になる。また、取得したログをある程度の期間保存しておくことで、何らかのイベント発生を把握した際には、さかのぼって調査することが可能になる。

不審なDNSクエリを見つける際に利用可能な名前情報の特徴としては、ランダムな文字列のラベルや、異常に長いラベルなどが挙げられる。

ログの取得方法としては、DNSサーバーソフトウェアのクエリログ機能を利用する、サーバーを接続しているネットワークのトラフィックを監視して流れているDNSデータの内容を記録するなどの方法が考えられる。

〈組織内ネットワークにおけるOP53Bの適用〉

前述したDNSクエリログの取得・保存に加え、組織外のリゾルバーやパブリックDNSサービス

の利用を制限するため、組織内ネットワークに対しOP53B（Outbound Port 53 Blocking）を適用する[5]。

組織内ネットワークにおけるOP53Bの適用は、DNS Changer[6]のような、利用するフルリゾルバーを攻撃者が用意した別のサーバーに差し替えるタイプのマルウェアによる被害の防止にも有効である。

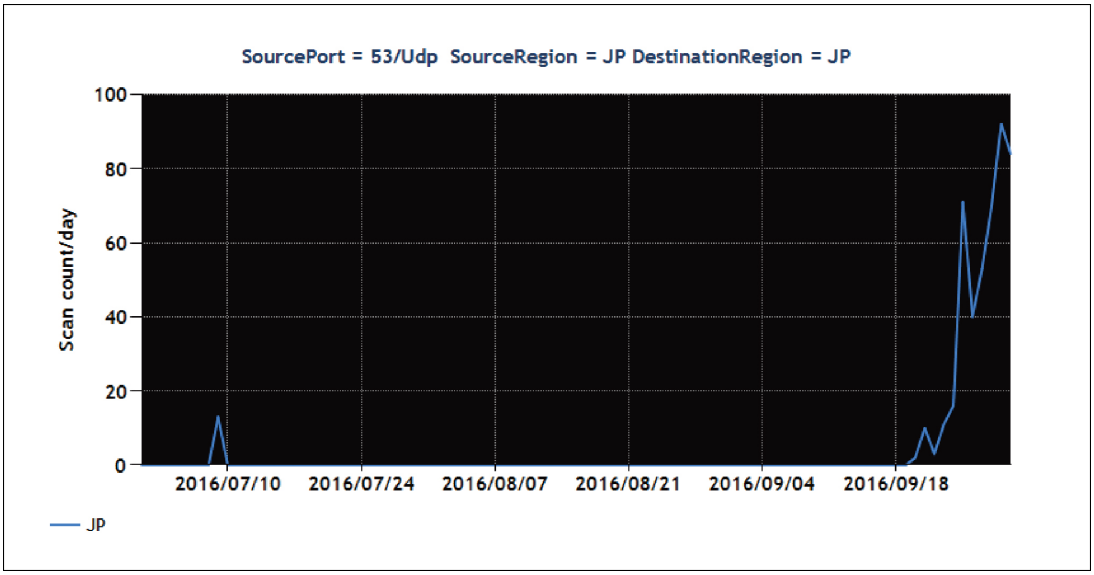
〈不審なDNSクエリを検知・ブロック可能な製品の導入検討〉

不審なDNSクエリを検知・ブロックする機能を備えたアプライアンス製品やサービスが、複数のベンダーから発表・提供されている。こうした製品を導入・活用することにより、被害の発生を防止できる場合がある。

■ランダムサブドメイン攻撃の状況

2014年初頭から世界的に観測され始め、以降、継続的に観測されていたランダムサブドメイン攻撃[7]が、2016年5月25日からほとんど観測されない状態になっていた（資料4-2-5）[8]。しかし、2016年9月20日から再び観測されるようになり[9]、本稿執筆時点の2016年11月下旬現在も継続している。

資料4-2-5　ランダムサブドメイン攻撃の発生状況



出典：インターネット定点観測レポート（2016年7〜9月）（https://www.jpcert.or.jp/tsubame/report/report201607-09.html）

■DNSソフトウェアの脆弱性

●BINDの脆弱性の状況

代表的なDNSソフトウェアであるBINDについて、2016年は、年間最多となる9件の脆弱性が報告された。2016年中にJPRSが注意喚起したBINDの脆弱性の一覧を資料4-2-6に示す。

資料4-2-6　2016年にJPRSが注意喚起したBINDの脆弱性

公開・更新日	注意喚起のタイトル
1月20日	（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2015-8704） - フルリゾルバー（キャッシュDNSサーバー）／権威DNSサーバーの双方が対象、バージョンアップを強く推奨 -
1月20日	BIND 9.10.xの脆弱性（DNSサービスの停止）について（CVE-2015-8705） - フルリゾルバー（キャッシュDNSサーバー）／権威DNSサーバーの双方が対象、バージョンアップを強く推奨 -
3月10日	（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-1285） - フルリゾルバー（キャッシュDNSサーバー）／権威DNSサーバーの双方が対象、バージョンアップを強く推奨 -
3月10日	（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-1286） - DNSSEC検証を実施していない場合も対象、バージョンアップを強く推奨 -
3月10日	BIND 9.10.xの脆弱性（DNSサービスの停止）について（CVE-2016-2088） - DNS cookie機能を有効にしている場合のみ対象、バージョンアップを強く推奨 -
7月19日	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-2775） - lightweight resolverプロトコルを有効にしている場合のみ対象、バージョンアップを推奨 -
9月28日・10月3日	（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-2776） - フルリゾルバー（キャッシュDNSサーバー）／権威DNSサーバーの双方が対象、バージョンアップを強く推奨 -
10月21日	（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-2848） - フルリゾルバー（キャッシュDNSサーバー）／権威DNSサーバーの双方が対象、 対象となるディストリビューション・バージョンに要注意 -
11月2日	（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2016-8864） - バージョンアップを強く推奨 -

出典：JPRSの発表を基に作成

これらの脆弱性のうち、2016年9月に公開されたCVE-2016-2776では、日本国内のサービスプロバイダーにおける被害事例[10]や、網羅的なスキャンによる無差別攻撃[11]が観測されている。

■DNSSECに関する最近の話題

●ルート/arpaゾーンにおけるDNSSEC署名有効期間の変更

2016年9月6日にルートゾーンおよびarpaゾーンのDNSSEC署名の有効期間が、従来の10日間から13日間に変更された。この設定変更は、ICANNの諮問委員会の一つであるルート・サーバー・システム諮問委員会（Root Server System Advisory Committee：RSSAC）が発行したRSSAC003文書[12]における推奨値に従ったものである。

今回の設定変更は、RSSAC003文書が想定する最悪のシナリオ（a worst-case scenario）に対応するための予防措置であり、設定変更の影響は特に観測されておらず、現在まで本件に関する障害は報告されていない。

●ルートゾーンのゾーン署名鍵の鍵長変更

2016年10月1日にルートゾーンのゾーン署名鍵（ZSK）の鍵長が、1024ビットから2048ビットに変更された。この設定変更は米国国立標準技術研究所（National Institute of Standards and Technology：NIST）の勧告[13]に従ったものであると考えられており、ルートゾーンにおいてDNSSECの運用が2010年に開始されて以来、初の鍵長変更となった。

今回の変更によってルートサーバーが返すDNS応答のサイズが増大したが、現在まで本件に関する障害は報告されていない。

●ルートゾーンの鍵署名鍵の更新（KSKロールオーバー）

2017年7月から2018年3月にかけて、ルートゾーンの鍵署名鍵の更新（KSKロールオーバー）が実施される予定である。ルートゾーンのKSKの運用について定めたDPS（DNSSEC Practice Statement）[14]では、KSKロールオーバーの実施を

運用開始の5年後以降と定めており、今回がルートゾーンにおけるDNSSECの運用開始後、初の実施となる。

本件に関する作業はすでに開始されており、2016年10月27日に実施されたキーセレモニーにおいて、新しいKSKが生成された。ICANNが公開したKSKロールオーバーの作業工程の予定を資料4-2-7に示す。

資料4-2-7　KSKロールオーバーの作業工程予定

予定日	内容
2016年10月27日	新しいKSK（KSK-2017）の生成（実施済み）
2017年2月	KSK-2017の運用準備完了
2017年3月	KSK-2017をIANAのウェブサイトで公開
2017年7月11日	KSK-2017をルートゾーンで公開
2017年9月19日	ZSKロールオーバーによってルートゾーンのDNS応答サイズが増大
2017年10月11日	KSK-2017をルートゾーンのDNSKEY RRの署名に使用
2018年1月11日	現在のKSK（KSK-2010）の失効をルートゾーンに設定
2018年3月22日	KSK-2010をルートゾーンから削除
2018年8月	KSK-2010をすべてのHSMから削除
2018年8月31日	KSKロールオーバープロセスが完了

HSM：Hardware Security Module。公開鍵暗号に用いる秘密鍵などの秘密情報を生成・管理するために使われる専用の機器。

出典：ICANNの公開文書「2017 KSK Rollover Operational Implementation Plan Version: 2016-07-22」（https://www.icann.org/en/system/files/files/ksk-rollover-operational-implementation-plan-22jul16-en.pdf）を基に作成）

〈考慮すべき事項①：応答サイズの増大によるIPフラグメントの発生〉

KSKロールオーバーによってルートサーバーが返すDNS応答サイズが増大し、IPフラグメントが発生する。もし、IPフラグメントを正しく処理できないネットワーク機器やファイアウォールが使われていた場合、ルートサーバーからのDNS応答を正しく受け取れなくなる可能性がある。

現在、多くのフルリゾルバーではDNSSEC検証を有効にしていない場合もDNSSEC署名付きの応答を受け取っているため、今回のKSKロールオーバーによる影響を、該当するすべてのフルリゾルバーにおいて考慮する必要がある。

なおDNS-OARCと米Verisignが、KSKロールオーバー実施中の大きなDNS応答を正しく処理できるかを確認するためのテストページを公開している[15]。

〈考慮すべき事項②：トラストアンカーの自動更新〉

KSKロールオーバーに伴い、トラストアンカー[16]の更新が必要になる。DNSSECではトラストアンカーを自動更新するための仕組みがRFC 5011で定義されており、RFC 5011をサポートしているフルリゾルバーであれば、手動での更新は不要である。

ただし、ルートゾーンのトラストアンカーの自動更新はこれまで運用実績がなく、かつ、過去に本機能に関するバグ[17]や脆弱性[18]が報告されたバージョンのBINDが運用されている可能性がある。予期せぬトラブルを防止するため、DNSSEC検証を有効にしているフルリゾルバーの運用者は、前述したバグや脆弱性が報告されていないバージョンであることの確認やトラストアンカーの自動更新における動作の理解など[19]、KSKロールオーバーの際にトラストアンカーの自動更新が正しく実施されるかについて留意する必要がある。

1. 遠隔操作可能な多数のコンピューター（Bot）で構成された、仮想ネットワーク。
2. Dyn に対する攻撃では、10万台以上の機器が攻撃に利用されたといわれている。
3. 遠隔操作ウイルスの制御に DNS プロトコルを使用する事案への注意喚起（ラック）
   http://www.lac.co.jp/security/alert/2016/02/01_alert_01.html
4. MULTIGRAIN - Point of Sale Attackers Make an Unhealthy Addition to the Pantry（FireEye）
   https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html
5. US-CERT が公開した設定ガイドにおいて、OP53B の適用が推奨されている。
   Alert (TA15-240A) Controlling Outbound DNS Access（US-CERT）
   https://www.us-cert.gov/ncas/alerts/TA15-240A
6. 感染した機器が利用するフルリゾルバーの設定を、攻撃者が設定した DNS サーバーを利用するように書き換えることで、フィッシングなどの不正行為に悪用しようとするマルウェア。
7. 本攻撃手法は「ランダムサブドメイン攻撃」「DNS 水責め攻撃」などさまざまな名称で呼ばれているが、本稿では「ランダムサブドメイン攻撃」を使用している。
8. DNS 水責め（Water Torture）攻撃対策と動向について 2016（九州通信ネットワーク）
   http://dnsops.jp/event/20160624/DNS_Summer_Days_2016_suematsu.pdf
   インターネット定点観測レポート（2016 年 4〜6 月）（JPCERT/CC）
   https://www.jpcert.or.jp/tsubame/report/report201604-06.html
9. インターネット定点観測レポート（2016 年 7〜9 月）（JPCERT/CC）
   https://www.jpcert.or.jp/tsubame/report/report201607-09.html
10. ［障害報告］DNS 名前解決のサービス障害につきまして（シーズ）
    https://www.seeds-std.co.jp/mente/2016/10/04/2263/
11. BIND の脆弱性（CVE-2016-2776）を標的とした無差別な攻撃活動の観測について（警察庁）
    http://www.npa.go.jp/cyberpolice/topics/?seq=19301
12. RSSAC003 - RSSAC Report on Root Zone TTLs
    https://www.icann.org/en/system/files/files/rssac-003-root-zone-ttls-21aug15-en.pdf
13. 暗号強度強化に関する勧告（NIST SP 800-57）では、RSA 暗号における 1024 ビットの使用を非推奨とし、2048 ビットへの移行を推奨している。
    Recommendation for Key Management Part 3: Application-Specific Key Management Guidance（NIST）
    http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
14. 管理対象ドメイン名における DNSSEC サービスの安全性や運用のポリシー、考え方、手順などについて網羅的にまとめた文書で、そのドメイン名の DNSSEC 運用者が必要に応じて作成・公開する。
    DNSSEC Practice Statement for the Root Zone KSK Operator
    https://www.iana.org/dnssec/icann-dps.txt
15. OARC's DNS Reply Size Test Server
    https://www.dns-oarc.net/oarc/services/replysizetest/
    DNSSEC Key Size Test
    http://keysizetest.verisignlabs.com/
16. DNSSEC 検証における信頼の連鎖の起点としてバリデーターに設定される情報。トラストアンカーには通常、ルートゾーンの KSK またはそのハッシュが設定される。
17. BIND 9.7.x/9.8.x のトラストアンカー自動更新機能の実装上のバグについて - バージョンアップを推奨 -（JPRS）
    https://jprs.jp/tech/notice/2011-09-01-bind9-bug-rfc5011-trust-anchor-updates.html
18. BIND 9.x の脆弱性（DNS サービスの停止）について（2015 年 2 月 19 日公開）- DNSSEC 検証を実施している DNS サーバーのみ対象、バージョンアップを強く推奨 -（JPRS）
    https://jprs.jp/tech/security/2015-02-19-bind9-vuln-managed-trust-anchors.html
19. 東京大学の石原知洋氏の発表資料が参考になる。
    Root KSK 更新に対応する方法
    https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/t5/t5-ishihara.pdf

［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～2017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