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

2020年はDNSに対する新たな攻撃手法や脆弱性情報が相次いで発表され、対応が進められた年となった。サブドメインテイクオーバーによる被害が国内でも報告され、ドメイン名・DNSの管理の重要性が改めて注目されている。

■NXNSAttackの概要と対応状況

●NXNSAttackの概要

NXNSAttack[1][2]は2020年5月19日にテルアビブ大学の研究者らが論文発表した、DNSに対するDoS攻撃の手法である。攻撃対象のドメイン名を管理する権威DNSサーバーや名前解決を実行するフルリゾルバー（キャッシュDNSサーバー）をサービス不能の状態に陥らせて名前解決ができない状態にし、サービスの提供・利用を妨害することを目的としている。

●NXNSAttackの仕組み

NXNSAttackでは、攻撃にDNSの名前解決の仕組みが使われる。

DNSの名前解決は、クライアントから名前解決要求を受け取ったフルリゾルバーが、権威DNSサーバーの階層構造をたどることで実行される。階層構造をたどれるようにするため、委任元（親）の権威DNSサーバーは委任先（子）を示す委任情報[3]をフルリゾルバーに応答する。委任情報には委任先のゾーンを管理するネームサーバーホスト名（NSレコード）が含まれ、必要に応じてグルーレコードが追加される。

NXNSAttackではこの仕組みを利用し、自身が管理権限を持つドメイン名に、攻撃に使う不適切なNSレコードを設定しておき、そのドメイン名の名前解決を実行するように仕向けることで、攻撃を実行する。

NXNSAttackによる基本的な攻撃例を、資料3-5-1に示す。NXNSAttackにおける登場人物は、クライアント（左上）、攻撃者が準備した権威DNSサーバー（右上）、一般的なフルリゾルバー（中央）の3種類である。

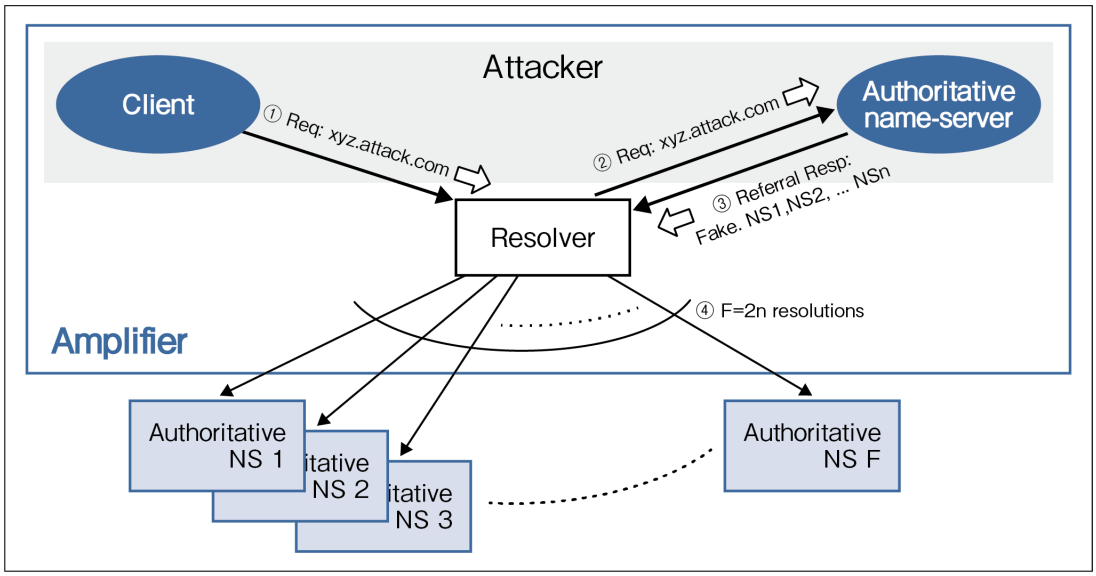
①クライアントは、攻撃者が管理権限を持つドメイン名（xyz.attack.com）に対する名前解決要求をフルリゾルバーに送る。

②名前解決要求を受け取ったフルリゾルバーは、攻撃者が準備した権威DNSサーバーに、xyz.attack.comに対する問い合わせを送る。

③権威DNSサーバーは攻撃用に準備された委任情報を応答する。委任情報には多数のNSレコード（NS1、NS2、…、NSn）が含まれている。

④委任情報を受け取ったフルリゾルバーは、NSレコードで指定されたネームサーバーホスト名に対する名前解決を実行する。名前解決はAレコードとAAAAレコードに対して実行され、問い合わせの数がNSレコードの数の2倍（2n）に増幅される（増幅率はフルリゾルバーの実装や設定など

資料3-5-1　NXNSAttackによる攻撃例



出典：https://cyber-security-group.cs.tau.ac.il/dns-ns-paper.pdf から引用

に依存する）。

この例において、NSレコードにfake-1.victim.com、fake-2.victim.com、…、fake-n.victim.comのように、攻撃対象のドメイン名（victim.com）に存在しないサブドメインを付加したNSレコードを指定することで、攻撃対象の権威DNSサーバーに問い合わせを集中させることが可能になる[4]。また、極めて多数のNSレコードを指定することで、フルリゾルバーの処理を溢れさせる攻撃も可能になる。

●NXNSAttackの対応状況

NXNSAttackの公開と同時に、主なフルリゾルバー実装・DNS製品に対する修正版がリリースされた。いずれの実装・製品においても、名前解決における問い合わせの処理に一定の制限を設け、過負荷にならないようにする対策が図られている。修正版へのアップデート以外の回避策は準備されていないため、早急なアップデートが必要になる。

■SIGRedの概要と対応状況

●SIGRedの概要

SIGRed[5]は2020年7月14日にCheckpoint Softwareの研究者が発表した、Windows DNS Serverの脆弱性である。Windows DNS Serverの開発元であるマイクロソフトでは深刻度を「緊急」、影響度を「リモートでコードが実行される（RCE）」としており、自己増殖による拡散が可能（wormable）であるとしている[6]。

こうした内容から、脆弱性の深刻度を示すCVSSスコアは最高点の10.0となっており、発表から2日後の2020年7月16日に米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）が、即時のパッチ適用を呼び掛ける緊急指令を公開している[7]。

●SIGRedの仕組み

SIGRedは脆弱性を持つWindows DNS Server

がSIGレコードを含む応答を受け取った際の処理により、バッファオーバーフローを引き起こすことで発生する。

SIGレコードは1999年に発行されたDNSSECの旧仕様（RFC 2535）で定義されたリソースレコードであり、2005年に発行された現行のDNSSEC（RFC 4033〜4035）によってRRSIGレコードに置き換えられ、廃止されている。しかし、Windows DNS ServerにはSIGレコードの処理が残っており、Checkpoint Softwareの研究者が攻撃方法（アタックベクター）を発見したことで、脆弱性が顕在化することとなった。

アタックベクターのポイントは、以下の2点である。

①DNSのメッセージ圧縮／展開機能により受け取ったDNS応答を伸長させ、バッファオーバーフローを引き起こさせる。

②https://標的のDNSサーバー:53/というURLにアクセスさせ、Webブラウザー経由で不正なデータを注入することにより、一般利用者や内部の利用者を攻撃に加担させる[8]。

●SIGRedの対応状況

SIGRedの公開と同時に、マイクロソフトから脆弱性を修正するパッチがリリースされており、Windows Updateで適用可能である。Windows Updateが利用できない場合、パッチを別途ダウンロード・インストールする必要がある。

本脆弱性は既に実証コード（PoC）が公開されており、公知となっている。サーバーを外部に公開しているか否かによらず、即時のパッチ適用が必須となっている。

■SAD DNSの概要と対応状況

●SAD DNSの概要

SAD DNS[9][10]は2020年11月11日にカリフォルニア大学リバーサイド校と清華大学の研究者らが論文発表した、キャッシュポイズニング[11]の手法である。SAD DNSではTCP/IPの実装の特性を利用したサイドチャネル攻撃[12]によって問い合わせポート番号を外部から推測することで、攻撃成功の確率向上を図っている。

▼攻撃成功の確率と各要素との関係

SAD DNSで用いられた攻撃手法を理解するために必要な前提知識として、キャッシュポイズニングが成功する確率と、DNSの通信における各要素との関係について説明する。

攻撃対象のフルリゾルバーにキャッシュポイズニングが成功する確率Psと、DNSの通信における各要素との関係式を資料3-5-2に示す。この式において確率Psの値を増やすためには、この式の分子の値を増やすか、分母の値を減らす必要がある。

2008年に発表されたカミンスキー型攻撃手法[13]の対策として普及したソースポートランダマイゼーション[14]では、問い合わせに使われるUDPポートをランダム化することでNpの実効値を増やし、確率Psの減少を図っている。

▼SAD DNSで用いられた攻撃手法

問い合わせポート番号を外部から推測して絞り込むことでNpの実効値を減らし、確率Psの増加を図ることが、SAD DNSのコンセプトである。論文では、IDとソースポートランダマイゼーションによる効果（2の32乗＝約43億）を、2の16乗の2倍（13万1072）に減らすことが可能である旨が記載されている。

ただし、その特性上、論文の方法による問い合わせポート番号の推測には一定の時間を要する。そのため、SAD DNSでは権威DNSサーバーに大量の問い合わせを送信してDNS RRL[15]を発動さ

資料3-5-2　キャッシュポイズニングの成功確率の関係式

攻撃対象のフルリゾルバーにキャッシュポイズニングが
成功する確率Psと各要素との相関関係

$$Ps \propto \frac{R \cdot t}{Ns \cdot Np \cdot Ni}$$

R：攻撃パケットの送信頻度（パケット/秒）
t ：攻撃可能時間（正規の応答を受け取るまで）（秒）
Ns ：攻撃対象ゾーンの権威DNSサーバーの数
Np：問い合わせに使われるUDPポートの数
Ni：ID（16ビット）

出典：筆者作成

せることで攻撃可能時間tの値を増やし、確率Psの増加を図る方法も併用している。

SAD DNSで発表されたサイドチャネル攻撃は、ICMPのプロトコル仕様とRate Limitingの実装の特性を利用した高度なものである。具体的な内容については、研究者らが公開した論文[16]を参照いただきたい。

●SAD DNSの対応状況

LinuxのTCP/IPの実装はSAD DNSに対して脆弱であったことが判明しており、ICMP Rate Limitingの実装を改良することで送信元ポート番号の推測を困難にする緊急パッチが、SAD DNSの公開と同時にリリースされている[17]。

SAD DNSはキャッシュポイズニングの手法であり、対策の基本はこれまでのキャッシュポイズニングへの対策と同様である。有効な対策としてDNSSECの適用や、攻撃を検知した際のTCPでの再問い合わせなどが挙げられる。

■サブドメインテイクオーバーの概要と対策

サブドメインテイクオーバー[18]は、CDN（Content Delivery Network）サービスやWebサービスの利用開始時に設定したサブドメインのDNS設定がサービスの利用終了後も残ったままになっていることを利用し、ドメイン名の管理権限を持たない第三者が、そのサブドメインの乗っ取り（テイクオーバー）を図る攻撃手法である。

●サブドメインテイクオーバーが発生する流れ

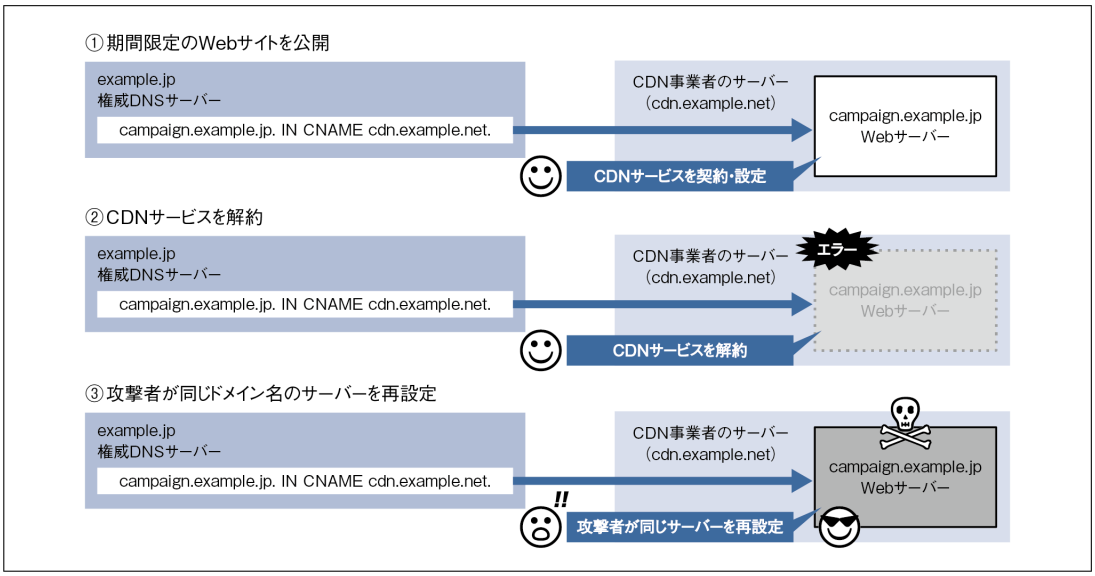
サブドメインテイクオーバーが発生する流れを資料3-5-3に示す。

この例では、CDNサービスの利用者のドメイン名をexample.jp、CDNサービス事業者のドメイン名をcdn.example.netとしている。

①期間限定のWebサイトを公開

キャンペーンの運営のため、example.jpの管理者がcdn.example.netで運営されるCDNサービス上にサイトを構築し、事業者から

資料3-5-3　サブドメインテイクオーバーが発生する流れ



出典：筆者作成

指定されたCNAMEレコードを設定して、campaign.example.jpというドメイン名で期間限定のWebサイトを公開する。

②CDNサービスを解約

公開期間の終了に伴い、CDNサービスを解約する。これによりCDNサービス上からWebサイトが削除され、アクセスできない状態になる。

③攻撃者が同じドメイン名のサーバーを再設定

攻撃者がこの状態のサブドメインを発見し[19]、CDNサービス側に同じドメイン名のサーバーを再設定することで、サブドメインテイクオーバーを実行する。

●サブドメインテイクオーバーの事例

2020年に発生したサブドメインテイクオーバーの事例を2件紹介する。サブドメインテイクオーバーの事例は本稿執筆時点においても報告され続けており、CDNサービスの普及に伴い、増加傾向にある。

▼iPhone当選詐欺

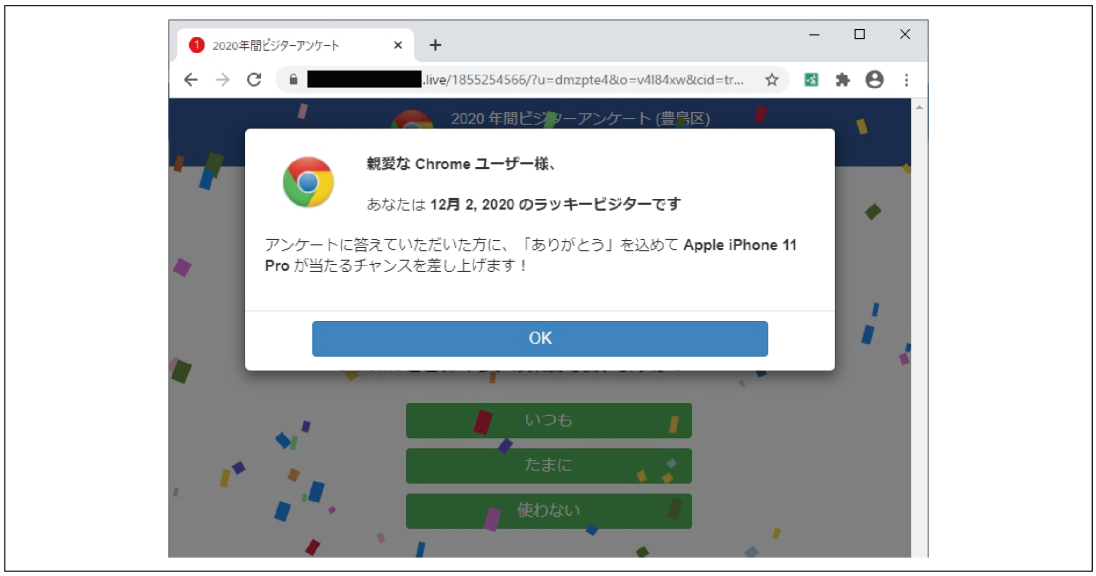
検索結果のリンクをクリックした際に突然「iPhoneが当選した」という画面が表示され、アンケートと共にアカウント情報・クレジットカード情報などの入力を促して情報の窃取・悪用を図る詐欺行為である（資料3-5-4）。

iPhone当選詐欺では、検索で表示されたおとりサイトから詐欺サイトへの誘導を図る手口が用いられており、このおとりサイトの作成にサブドメインテイクオーバーが用いられていることが判明している。著名企業や自治体など、検索で上位に表示されやすいドメイン名が標的になっており、2020年7月までに国内の上場企業のドメイン名を含む、100件以上の被害事例が確認されている。

▼偽サイトの作成

徳島県のLG.JPドメイン名（demo.pref.tokushima.lg.jp）がサブドメインテイクオーバーされ、

資料3-5-4　iPhone当選詐欺の画面



ポケモン徹底攻略（https://yakkun.com/）の偽サイトの作成に使われた。攻撃者は本物のコンテンツをコピーし、リンクをアフィリエイト付きのものに差し替えた偽サイトを作成・公開していたことが判明している。

本事例では、ゲームに登場する主なキャラクターの名前でGoogle検索した際、一時的に偽サイトを本物よりも上位に表示させることに成功している。

●サブドメインテイクオーバーの防止策

サブドメインテイクオーバーの根本的な対策は、外部サービスの利用終了時に、不要になったDNS設定を削除することである。

なお、事例の多発を受け、CDNサービスやWebサービスの利用時に利用者が設定するドメイン名に関する管理権限の確認を必須とする対策を実施している事業者も存在する[20]。こうした事業者を利用することで、自身のドメイン名に対してサブドメインテイクオーバーが実行される危険性を軽減できる。

■DNS flag dayの状況

DNS flag dayは、DNSに関する重要な変更について歩調を合わせて実施する日として、準備を進めている関係者により名付けられたものである。

●DNS flag day 2020の実施状況

2019年2月1日に実施されたDNS flag day 2019に引き続き、2020年10月1日にDNS flag day 2020が実施された。DNS flag day 2020の目的、推奨される設定内容については、『インターネット白書2020』pp.166-169を参照されたい。

DNS flag day 2020の実施に起因すると考えられる大規模なトラブルは、本稿執筆時点で確認されていない。

●公式サイトのテスト結果に関する注意点

DNS flag day 2020の公式サイト[21]ではDNS flag day 2019と同様、運用中の権威DNSサー

バー・フルリゾルバーのテストが可能である。結果表示の形式はDNS flag day 2019と同様であり、交通標識を模したアイコンにより、対応状況が表示される。

ただし、テスト結果の「GO」の意味が、DNS flag day 2019とDNS flag day 2020では異なっている。それぞれの「GO」の意味を、以下に示す。

①DNS flag day 2019における「GO」の意味

「対象の権威DNSサーバー・フルリゾルバーは現在の設定で問題なく、設定の追加や変更は不要である」

②DNS flag day 2020における「GO」の意味

「対象の権威DNSサーバー・フルリゾルバーはDNS flag day 2020に対応する準備ができている。対応のための設定を追加しても、問題は起こらない」

すなわち、DNS flag day 2020では、テストで「GO」と表示された場合も、対応のための設定の確認と追加（EDNSバッファサイズを1232バイトに設定）が別途必要になる点に注意が必要である。

●今後の予定

本稿執筆時点において、2021年以降のDNS flag dayの実施は未定である。今後の状況は、公式サイトで公開される見込みである。

■DNSサーバーソフトウエアの脆弱性の状況

●BINDの脆弱性の状況

資料3-5-5に、2020年中に日本レジストリサービス（JPRS）が注意喚起したBINDの情報を示す。

▼脆弱性情報の事前アナウンスを開始

BINDの開発元のInternet Systems Consortium（ISC）が2020年5月19日にセキュリティポリシーを更新し、脆弱性情報の事前アナウンスを開始した[22]。事前アナウンスされるのは脆弱性情報の公開日と件数のみで、内容は従来と同様、当日まで秘匿される。

ISCでは事前アナウンスの理由について、BIND運用者の脆弱性対応を支援するためであるとしている。また、ISCでは事前アナウンスの基準を「問題がそのソフトウエアの多く、あるいはすべてのユーザーに重大な影響を与える可能性があると判断した場合」としており、影響が軽微であると判断した場合は事前公開されないこともある。

●BIND以外のDNSソフトウエアの状況

資料3-5-6に、2020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示す。

脆弱性情報はBINDに限らず、他のDNSソフトウエアでも随時公開されている。こうした情報を入手して迅速に対応することはDNSに限らず、システムの運用管理における必須事項の1つである。

1. NXNSAttack
   https://cyber-security-group.cs.tau.ac.il/
2. JPRS用語辞典｜NXNSAttack（エヌエックスエヌエスアタック）
   https://jprs.jp/glossary/index.php?ID=0262
3. PRS用語辞典｜委任情報
   https://jprs.jp/glossary/index.php?ID=0192
4. この「存在しない（Non-eXistent）NS」が、NXNSAttackという名前の由来となっている。
5. SIGRed - Resolving Your Way into Domain Admin: Exploiting a 17 Year-old Bug in Windows DNS Servers - Check Point Research
   https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/

資料3-5-5　2020年にJPRSが注意喚起したBINDの情報

公開・更新日	タイトル
2020/5/20	（緊急）BIND 9.xの脆弱性（パフォーマンスの低下・リフレクション攻撃の踏み台化）について（CVE-2020-8616）
2020/5/20	（緊急）BIND 9.xの脆弱性（DNSサービスの停止・異常な動作）について（CVE-2020-8617）
2020/6/18	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8618）
2020/6/18	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8619）
2020/8/21	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8620）
2020/8/21	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8621）
2020/8/21	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8622）
2020/8/21	BIND 9.xの脆弱性（DNSサービスの停止）について（CVE-2020-8623）
2020/8/21	BIND 9.xの脆弱性（サービス提供者が意図しないDynamic Updateの許可）について（CVE-2020-8624）

出典：筆者作成

資料3-5-6　2020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
2020/4/17	Windows DNS Serverの脆弱性情報が公開されました（CVE-2020-0993）
2020/5/21	Unboundの脆弱性情報が公開されました（CVE-2020-12662、CVE-2020-12663）
2020/5/21	PowerDNS Recursorの脆弱性情報が公開されました（CVE-2020-10995、CVE-2020-12244、CVE-2020-10030）
2020/5/21	Knot Resolverの脆弱性情報が公開されました（CVE-2020-12667）
2020/7/7	PowerDNS Recursorの脆弱性情報が公開されました（CVE-2020-14196）
2020/7/16	Windows DNS Serverの脆弱性情報が公開されました（CVE-2020-1350）
2020/8/14	Windows DNSキャッシュリゾルバーサービスの脆弱性情報が公開されました（CVE-2020-1584）
2020/9/17	Windows DNSの脆弱性情報が公開されました（CVE-2020-0836、CVE-2020-1228）
2020/9/17	Windows DNSキャッシュリゾルバーサービスの脆弱性情報が公開されました（CVE-2020-0839）
2020/9/25	PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2020-17482）
2020/9/25	PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2020-24696、CVE-2020-24697、CVE-2020-24698）
2020/10/16	PowerDNS Recursorの脆弱性情報が公開されました（CVE-2020-25829）
2020/12/3	NSDの脆弱性情報が公開されました（CVE-2020-28935）
2020/12/8	Unboundの脆弱性情報が公開されました（CVE-2020-28935）
2020/12/11	Windows DNSに関するセキュリティアドバイザリが公開されました

出典：筆者作成

6. Windows DNSサーバーの脆弱性情報CVE-2020-1350に関する注意喚起- Microsoft Security Response Center
https://msrc-blog.microsoft.com/2020/07/14/20200715-dnsvulnerability/
https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/
7. Emergency Directive (ED 20-03) Windows DNS Server Vulnerability | CISA
https://www.cisa.gov/blog/2020/07/16/emergency-directive-ed-20-03-windows-dns-server-vulnerability
8. この方法はWebブラウザーがInternet ExplorerやEdge Legacyである場合に可能となる。FirefoxやChrome、EdgeではHTTPSのポート番号として53を指定できないため、この方法による攻撃は不可能である。
9. SAD DNS
https://www.saddns.net/
10. JPRS用語辞典｜SAD DNS（サドディーエヌエス）
https://jprs.jp/glossary/index.php?ID=0270
11. JPRS用語辞典｜DNSキャッシュポイズニング
https://jprs.jp/glossary/index.php?ID=0171
12. 装置・機器などの動作状況を外部から観察し、内部の機密情報を取得しようとする攻撃手法の総称
13. JPRS用語辞典｜カミンスキー型攻撃手法（The Dan Kaminsky

attack）
https://jprs.jp/glossary/index.php?ID=0228

14. JPRS用語辞典｜ソースポートランダマイゼーション
https://jprs.jp/glossary/index.php?ID=0167
15. 技術解説：「DNS Reflector Attacks（DNSリフレクター攻撃）」について
https://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html
16. DNS Cache Poisoning Attack Reloaded | Proceedings of the 2020、ACM SIGSAC Conference on Computer and Communications Security
https://dl.acm.org/doi/10.1145/3372297.3417280
17. CVE - CVE-2020-25705
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25705
18. JPRS用語辞典｜Subdomain Takeover（サブドメインテイクオーバー）
https://jprs.jp/glossary/index.php?ID=0267
19. DNSの設定は公開情報であり、サブドメインテイクオーバー可能な状態は、外部からの総当たり検索により発見可能である。
20. Amazon CloudFrontがディストリビューションに代替ドメイン名を追加する際のセキュリティを強化
https://aws.amazon.com/jp/about-aws/whats-new/2019/04/amazon-cloudfront-enhances-the-security-for-adding-alternate-domain-names-to-a-distribution/
21. 020 | DNS flag day
https://dnsflagday.net/2020/index-ja.html
22. Update to ISC's Security Policy
https://www.isc.org/blogs/security-policy-update/

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～2021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