インターネット 10分 講座

ICANNにおけるDNS Abuse（DNS不正利用）とは ～ 議論と対策の現状 ～

1 はじめに

インターネット上のセキュリティ脅威は日に日に高度化、凶悪化しており、収まることがありません。システム侵入やサービス妨害などの技術的な被害だけでなく、人権や財産権の侵害につながる攻撃も後を絶たず、対策は後追いになりがちです。近年ICANN会議で盛んに議論されているキーワード「DNS Abuse（DNS不正利用）」は、このようなセキュリティ脅威に関する議論の一つです。

言葉の組み合わせから、DNSの仕組みを通じた、あるいはDNSを利用した不正利用、といった意味合いであることは想像できますが、さまざまなステークホルダーを擁するICANNでは、さまざまな主張がなされており、DNS Abuseという言葉の定義もなかなか一義に定まりません。本稿ではこのDNS Abuseに関して、ICANNでの議論の状況や、対策の現状に関して解説します。

2 DNS Abuseに関するICANNの責務

ICANNが、インターネットの一意な識別子の調整に責任を持っている団体だという概要的な理解はある程度浸透していますが、本件の議論の前に、厳密に言ってどこからどこまでがICANNの責任範囲か、明確にしておく必要があります。ICANNの付属定款第1章※1を引用します。

> 1.1項：使命
>
> (a) ICANNの使命は、インターネットの一意な識別子の体系の安定しセキュアな運用を堅持することである。特に、
>
> (i) DNSのルートゾーンにおけるドメイン名の割り当てを調整し、gTLDの第2レベルのドメイン名の登録に関するポリシーの策定と実施を調整する。この役割において、ICANNの活動範囲は以下のようなポリシー策定および実施の調整である。
>
> ・DNSの開放性、相互接続性、回復性、セキュリティ、安定性を推進するために合理的に必要な、統一された、または調整された決定に関するもので、gTLDのレジストラとレジストリに関しては、付属定款付録G-1およびG-2に記述される領域のポリシーを含む
> ・ボトムアップでコンセンサスベースのマルチステークホルダープロセスを通じて策定され、インターネットの一意なドメイン名体系の安定でセキュアな運営を確かにするべく設計されたもの
>
> ⋮
>
> (b) ICANNはミッション外の活動は行わないものとする。
>
> (c) ICANNは1.1項(a)の範囲外において、インターネットの一意な識別子を用いたサービスやそのようなサービスが提供するコンテンツを規制(例えばルールや制限を課す)しないものとする。

このように、ICANNが活動できる範囲は、識別子としてのドメイン名の機能と、DNSの機能を健全に保つことであり、ドメイン名が指し示すサービスやコンテンツの規制は行わない、ということが明言されています。

※1 BYLAWS FOR INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
https://www.icann.org/resources/pages/governance/bylaws-en/#article1

3 ICANNがレジストリ・レジストラに課している縛り

ICANNはgTLDに関して、定款で定められたミッションを遂行するために、ポリシーに関しては支持組織によるボトムアップなプロセスを経た勧告に従って定め、ポリシーに加え、運用上必要な措置や守るべき条件を課して、レジストリやレジストラの運営を許可します。これらの条件は契約書の条項としてまとめられ、レジストリとの間ではレジストリ契約（Registry Agreement, RA）※2、レジストラの間ではレジストラ認定契約（Registrar AccreditationAgreement, RAA）※3を結びます。以下にRA、RAAにおける、DNS Abuseに関連する条項を示します。

RA:　仕様11.3(a)　レジストラが登録者との契約の際に、不法・不正利用を禁じ利用停止を含む罰則を盛り込むよう、レジストリ・レジストラ契約に規定する
　　仕様11.3(b)　登録されているドメイン名に対して、セキュリティ脅威がないか定期的な技術的分析を行い、統計情報を記録維持する

RAA: 3.18: レジストラの不正利用窓口および不正利用申告に関する調査の義務
　3.18.1:不正利用窓口を置き、不正利用の申告を適正に取り扱う
　3.18.2:法執行機関、消費者保護団体等に対する窓口を24時間365日設ける
　3.18.3:不正利用申告の受付以降の処理プロセスを明快に示してWebで公開。申告と回答の履歴を2年間以上保持する

※2 Base Registry Agreement - Updated 31 July 2017　https://www.icann.org/en/registry-agreements/base-agreement
※3 2013 Registrar Accreditation Agreement　https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

4 RAPWG報告書とCCTレビュー報告書

近年の盛り上がり以前の検討成果としてRAPWG（Registration Abuse Policies Working Group、登録不正利用ポリシー作業部会）報告書を、そして近年の盛り上がりに繋がる検討成果としてCCTレビュー報告書を押さえておきます。

RAPWGは、GNSO（分野別ドメイン名支持組織）で2009年に組成されたWGです。ドメイン名の利用だけでなく、サイバースクワッティングをはじめとする登録自体の不正なども視野に入れて検討を行い、報告書は、2010年5月に公開されました。※4 この報告書の中には「DNS Abuse」というフレーズは出てきませんが、Abuse（不正利用）の定義を

- 実質的な害を与える、あるいはそのような害を引き起こす行動
- 不法、違法、あるいは公開された正当な目的の意図あるいは計画に反していると考えられる行動

とし（同報告書4.1項）、具体的な不正利用の例として、スパム、マルウェア配送、児童ポルノ、フィッシング、Botnetのコマンド・コントロールなどを挙げています（同6.1項）。

ICANNのテーマ別レビューの一つであるCCT（Competition, Consumer Trust, and Consumer Choice：競争、消費者信頼および消費者選択）レビューは、2018年9月に最終報告書を公開しました。※5この最終報告書では、「児童虐待、知的財産権侵害、詐欺などの不正不法行為を引き起こすドメイン名の不正利用」などもDNS Abuseとなり得るが、定義は各国の管轄法に大きく依存すること、「マルウェア、フィッシング、BotnetなどDNSインフラに対するセキュリティ脅威」が、DNS Abuseの中で特に、DNS Security Abuseとして広く認識されていることを示した（同報告書P.88）上で、DNS Abuseに関して以下の3項目を勧告しました。

14: DNS Abuseに対して積極的な不正利用対策を組み入れられるインセンティブをレジストリ契約に組み込む

15: 特定のレジストリ・レジストラ事業者の組織的な不正利用を防ぐ方策の実施

16: DNS Abuse対策に資する客観データの収集と提供

ICANN理事会は2019年3月に、CCTレビュー最終報告書の35勧告のうち6勧告を受諾、14勧告を再検討依頼に帰して、17勧告を理事会における継続検討としました。分割した上で再検討依頼と継続検討に分類された勧告があるため、このような数字となっています。この再検討の結果は2020年10月の理事会決議に示され、上の三つのうち勧告14,15 はDNS Abuseの定義の明確化が必要として、継続検討としました。勧告16は、既にDAAR（Domain Name Abuse Activity Reporting）として実施中であったため、受諾としました。DAARの内容に関しては後述します。

※4 Registration Abuse Policies Working Group Final Report
　https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf
※5 COMPETITION, CONSUMER TRUST, AND CONSUMER CHOICE REVIEW Final Report
　https://www.icann.org/en/system/files/files/cct-final-08sep18-en.pdf

5 各ステークホルダーの姿勢：レジストリ・レジストラの場合

近年のDNS Abuse議論の盛り上がりは、あらゆる支持組織や諮問委員会でこのキーワードに関する議論が行われ、明示的に名称に掲げるサブグループが作られていることから分かります。

2019年にCPH（Contracted Party House、契約者会議）の関係者を中心とした活動として、DNS Abuse Framework※6というものが立ち上がり、同名の枠組み文書※7を採択するとともに、定期的なレビューと改版を行っています。枠組み文書は、不正利用の内容、被害へ

の対策や関係者の役割などを概説するとともに、DNS Abuseの定義を以下のように行っています。

- DNS Abuseは有害な行いのうちDNSに関連するもので、次の五つの大きなカテゴリーからなる：マルウェア、Botnet、フィッシング、ファーミング、スパム（ただし他のDNS Abuseの配送機構となる場合）

そして、これらDNS Abuseに対しては、レジストリ・レジストラに対処を求め、ICANNとの契約で課せられている不正利用窓口に対して申告があった場合には直ちに申告内容を確認して対処するべき、としています。その一方で、不正利用だと確認された場合に、それに対する対処として現実的なものがそのドメイン名全体の削除（テイクダウン）しかなく、それでも大きなプラットフォームになるほど影響が過大となると指摘しています。

また、.orgのレジストリであるPIR（Public Interest Registry）[※8]は、自社のプロジェクトとして DNS Abuse Institute[※9]というものを立ち上げ、研究、協調、普及啓発などを行っています。

CPHはレジストリとレジストラからなり、ドメイン名登録に関わる不正利用対策を行う主体となる関係者です。そのため、不正利用対策は商材であるドメイン名の品質向上に寄与するものの、エスカレートする要請には対応することはできず、対応対象をICANNの責務であるDNSセキュリティ脅威に留めたいという意向を、一般的に持ちます。また、DNS Abuse対応をはじめとする検討や対策は、それが直接事業収益に繋がるものではないことから、積極的に対応に応じる事業者、まったく関与しようとしない事業者など、濃淡が大きく分かれており、後者にあたる事業者に対する働きかけが重要だと考えられます。

※6 DNS Abuse Framework https://dnsabuseframework.org/
※7 DNS Abuse Framework - 2020年5月29日版枠組み文書 https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf
※8 Public Interest Registry https://pir.org/
※9 DNS Abuse Institute https://dnsabuseinstitute.org/

6 レジストリ・レジストラ以外

一方、GNSOの中でも、NCPH（非契約者会議）の関係者はドメイン名のユーザーであり、自分たちが使うドメイン名の品質や安全性としてDNS Abuseを捉えています。それに加えて、IPC（知的財産権部会）の関係者は、ドメイン名における商標権だけでなく、コンテンツの著作権などの財産権にも関心が高いので、DNSへのセキュリティ脅威に加えて、財産権もDNS Abuseの議論に含めるべきだという意見が多く見られます。

諮問委員会ではどうでしょうか。At-Largeは強い関心で議論を推進しており、ICANN会議ごとにDNS Abuseに関するセッションを、他のグループの関係者や有識者を交えて開催していますし、At-Large Webサイトの中に特設ページを設けて[※10]、過去のセッションの資料や各種リファレンスを集積しています。

GAC（政府諮問委員会）ではPSWG（公共安全作業部会）[※11]において、主に消費者保護の観点からの議論が展開されています。また、上に示したDNS Abuseの定義には必ずしも適合しないのですが、日本政府が海賊版対策の観点からの問題提起を、ICANN70、ICANN71の場で展開しています。これに関しては後述します。

SSACは、セキュリティや安定性の維持の観点から、技術的検討を進めていました。その成果は、2021年3月と最近になって公表されました。こちらは最後に紹介します。

※10 At-Large and DNS Abuse https://atlarge.icann.org/policy/at-large-and-dns-abuse-en
※11 GAC Public Safety Working Group (PSWG) https://gac.icann.org/working-group/gac-public-safety-working-group-pswg

7 gTLD Subpro PDPでの検討

gTLDでは、2012年に続く次のラウンドの新gTLD募集に関して、gTLD Subpro PDP（新gTLD次ラウンド検討ポリシー策定プロセス）を通じて検討を行い、2021年1月に最終報告書[※12]を公表しました。DNS Abuseに関して、以下のような勧告が含まれます。

9.15：コミュニティで継続中のDNA Abuseに関する議論を認識し、新ラウンド導入に関わらず、DNS Abuseに対して全体的な対策が必要

全体的な対策が必要としながら、具体的な勧告には至っておらず、DNS Abuseの定義に関しても既存の議論に委ねる形となっています。これらは前述のCCTレビュー最終報告書の三つの勧告を十分検討した上で、と脚注に示されています。（同報告書P.42）

※12 Final Report on the new gTLD Subsequent Procedures Policy Development Process
https://gnso.icann.org/sites/default/files/file/field-file-attach/final-report-newgtld-subsequent-procedures-pdp-20jan21-en.pdf

8 ICANN事務局における対応

DNS Abuseに関する議論がコミュニティで盛んに行われているところですが、ICANN事務局でのDNS Abuse対応は二つあります。一つは、客観的な統計データでDNS Abuseに関する実状を情報提供すること、もう一つは、レジストリ・レジストラが、RA、RAAで定められた対応を行っていることを確認すること、です。

統計データの提供は、前述のDAAR[※13]という名称で、ICANN事務局のCTOオフィス（Office of CTO: OCTO）が実施しています。これは、すべてのgTLDと希望するccTLDの登録ドメイン名に対して、Reputation Block List（RBL）と呼ばれる外部レピュテーションデータを照合して、各TLDにおける不正利用の存在を統計的に分析するものです。その結果は、月次レポートとしてDAAR Webページで公開されています。

レジストリ・レジストラが契約に沿った運営を行っているかに関しては、ICANN事務局のコンプライアンス部門が確認を行っています。コ

ンプライアンス部門は、一般ユーザーからの、レジストリ・レジストラの契約事項不履行疑いの申し立てを受け付けていますが[※14]、加えて定期的な監査も実施します。直近では2021年1月に、DNSセキュリティ脅威に関する義務の履行状況に関して監査が行われました。[※15]

※13 Domain Abuse Activity Reporting https://www.icann.org/octo-ssr/daar/
※14 Submitting a Complaint to ICANN Contractual Compliance https://www.icann.org/compliance/complaint
※15 ICANN Org Launches Audit of Registrar Compliance with DNS Security Threat Obligations
https://www.icann.org/en/announcements/details/icann-org-launches-audit-of-registrar-compliance-with-dns-security-threat-obligations-15-1-2021-en

9 日本政府のGACにおける働きかけ

総務省は、2020年12月に「インターネット上の海賊版対策に係る総務省の政策メニュー」[※16]を公表し、その中で「海賊版サイトのドメイン名に関し、ドメイン名の管理・登録を行う事業者による事後的対応の強化について、国際的な場（ICANN等）において議論を推進」する、としました（同文書P.1）。海賊版対策の局面では、海賊版運営事業者のドメイン名に関する登録情報から、事業者特定がタイムリーに行われることが求められます。しかし日本国内の出版社からの登録者情報請求への対応が芳しくないレジストラが海外に一部存在し、この問題に関する懸念から、日本国政府では2021年3月に開催されたICANN70会議（バーチャル開催）のGACのセッションにおいて発表時間を確保し、契約遵守によって登録者情報開示が円滑になるよう、働きかけました[※17]。同様の働きかけは、2021年6月のICANN71会議（バーチャル開催）でも実施されました。

これは、DNS Abuseというキーワードで近年盛んに議論されている、DNS基盤へのセキュリティ脅威の問題とは異なりますが、不正・不法行為に際して、ドメイン名という識別子の登録情報から登録者の特定を行うという、レジストリの基本機能のあり方を問うものとして、GAC内では複数のメンバーから支持が明言されたとのことです。

※16 インターネット上の海賊版対策に係る総務省の政策メニュー https://www.soumu.go.jp/main_content/000725629.pdf
※17 第60回ICANN報告会・政府諮問委員会報告・発表資料 https://www.nic.ad.jp/ja/materials/icann-report/20210513-ICANN/icann60-3-ouchi.pdf
ICANN71の報告資料は執筆時点ではまだありませんでした。

10 最後に - SAC115の紹介とともに

ここまで、ICANNにおけるDNS Abuseの議論を、時間の経過とともに説明しました。DNS Abuseの定義が定まらないために、議論が見通せないような局面があることを説明しましたが、明確な定義を試みているのは、DNSセキュリティ脅威に対象を限定することで、テイクダウンのような思い切った対策が取れるようにする、といった意味合いのように思えます。しかし、最後に示した日本政府からの働きかけのように、海賊版のような財産権（この場合知的財産権）の侵害の対策に関しても、IPアドレスや接続事業者からの情報と同様に、ドメイン名の登録情報から登録者を同定する情報を得て、その事業者に働きかけられるようにすることは、インターネットの識別子のレジストリとしては当然提供するべき機能であると言えます。総務省からの働きかけが、多くのコミュニティメンバーに支持され、議論や対策が進んでいくことを期待します。

本稿の最後となりますが、SSACの検討成果である、SAC115[※18]を紹介します。SAC115は“SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS（DNSで取り扱われる不正利用対策のための相互運用可能なアプローチに関するSSAC報告書）”と題され、DNSを中心にインターネット基盤の事業者たちを視野に入れて、DNS不正利用への対処方法に関して提言されています。2021年3月に公表されました。

この文書では、DNS Abuseの定義として、前述のDNS Abuse Frameworkによるものを一旦参照していますが、「しかし現存する、報告された、あるいはサービス事業者によって対応されたすべての形態のDNS Abuseを代表せず」、「網羅的なリストというものは存在しえない」（同文書P.13）として、改めてこれを定義することを留保しています。それに替えて、広くDNSを通じた不正利用に関する対処方法案として、下記の別表7項目を提唱しています。そして、これらの段階を通じて、多くの関係者にわたる不正利用対応を推進する「Common Abuse Response Facilitator（共通不正利用対応推進者）」という役割を設けるという草案を示し、この草案に検討を重ねて詰めていくことを勧告としています。

レジストリやレジストラにおける、不正利用の認定が困難であるという問題を、この認定を行うNotifierという役割を関係者で広く認定して対策にあたることをはじめ、不正利用対策に取り組むために有用で、これまでに必ずしも存在しなかった機能をいくつか提言しています。勧告の言葉遣いからも伺えますが、文書の末尾には、検討の過程で得られた異論も記録されているように、議論がまだ成熟していないようです。しかし、DNSに関わる不正利用の対策は、ICANN事務局とレジストリ・レジストラだけで完結せず、さまざまな関係者が関与する必要があるのは確かです。今後のDNS Abuseの議論が、こういった具体的な機構論を含め、実践的な形で進むことを願っています。

別表7項目
（1）不正利用の標準定義の策定
（2）不正利用の認定と通知を担う Notifier Programの構築
（3）不正利用解決の適切な主要担当者の決定
（4）標準的立証方法の策定とベストプラクティスの収集
（5）不正利用解決の標準エスカレーションパスの確立
（6）不正利用レポートに対する合理的な対応時間の決定
（7）報告者が不正利用種別を特定し正しい対応者に報告できるようにする判定機関の創設

（JPNIC インターネット推進部 前村昌紀）

※18 SAC115 - SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS https://www.icann.org/en/system/files/files/sac-115-en.pdf