DNS Abuse ハンドリングブックの必要性について

JPCERTコーディネーションセンター
インシデント ハンドリング グループ
中井 尚子

DNS Abuseハンドリングブックは必要なのか

- DNS Abuseハンドリングブックの前に DNS Abuse とは
  - 国内ではDNS Abuseを定義したものは見当たらない
  - 海外でも共通認識のもとで定義したものは見当たらない
  - 欧州連合政策執行機関向けに纏められたドキュメント (Study on Domain Name System (DNS) Abuse) では以下の内容が提案された

> Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.

European Commission
Study on Domain Name System (DNS) abuse
https://op.europa.eu/en/publication-detail/-/publication/d9804355-7f22-11ec-8c40-01aa75ed71a1

DNS Abuseハンドリングブックは必要なのか

DNS Abuse ハンドリングブックを考えたきっかけ

DNS Abuseを対応する際に参考にするドキュメントが日本にはない

関係事業者間で交わされているノウハウを文書化し残す

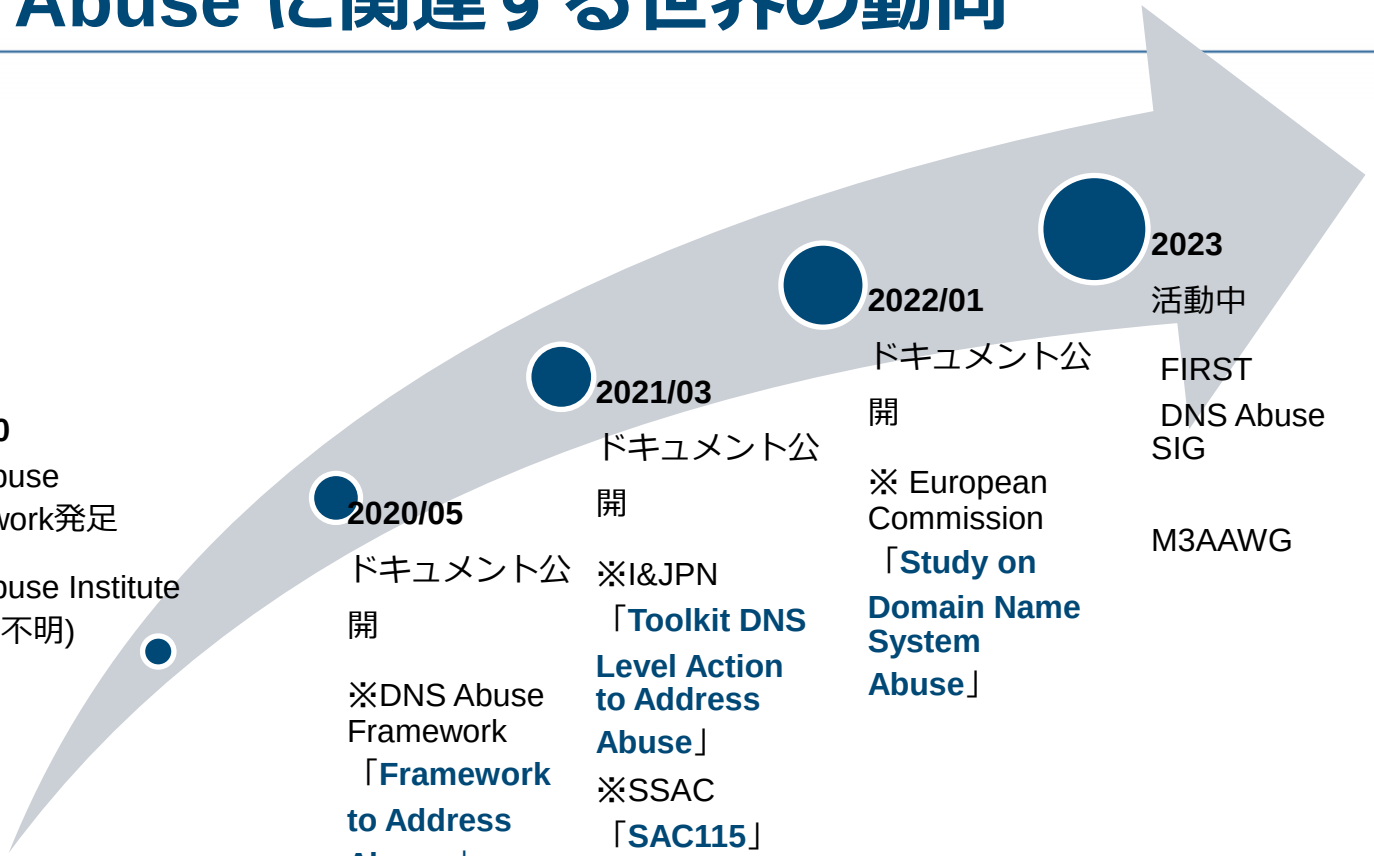
海外で議論されているDNS Abuseの流れに乗って日本でも議論や活動を始めるきっかけにする

DNS Abuseハンドリングブックは必要なのか

JPCERT/CC での状況を振り返る

- DNS Abuseの知見やノウハウが個々で蓄積しレベルに差異がある
- DNS Abuseのノウハウを共有する機会が少ない
- 対応時に発生するミスコミュニケーション
- 海外事業者との連携時に感じるDNS Abuseに対する考えの相違

DNS Abuse に関連する世界の動向



1）ドキュメント

タイトル	**Framework to Address Abuse**
組織	DNS Abuse Framework
概要	◘ 6ページ ◘ DNS Abuse を 5 つのカテゴリーに分け解説 　◘ Malware, Botnets, Phishing, Pharming, Spam(Spam は Phishing Email 配布に関わる場合） ◘ Webサイトコンテンツに対する見解（human life に悪影響を及ぼす場合は対応） ◘ Webサイトコンテンツに対する対応フローの説明 ◘ レジストリ、レジストラーでの信頼される通知者の役割について説明

2）ドキュメント

タイトル	**Toolkit DNS Level Action to Address Abuse**
組織	INTERNET & JURISDICTION POLICY NETWORK（I&JPN)
概要	◘ 48ページ ◘ General Level とTechnical Levelに分け紹介 ◘ General Level 　◘ 不正内容の特定と連絡に関して 　◘ 不正内容に沿ったDNSレベルでの対応の評価に関して、また対応することでの影響などの解説（LOCK, HOLD, REDIRECT,TRANSFER) ◘ Technical Level 　◘ 報告元の確認、報告内容の評価、要望の評価の説明 　◘ 事業者内の対応プロセス評価・判断方法の説明 　◘ DNS AbuseごとのDNSレベル対応のマッピング ◘ DNS Abuse ワークフロー

3）ドキュメント

タイトル	**（SAC115）SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS**
組織	ICANN Security and Stability Advisory Committee (SSAC)
概要	◘ 39ページ ◘ DNS Abuse の定義やWebサイトコンテンツについて 　◘ The Framework to Address Abuse を参照 ◘ Abuse 対応での適切な時期・対応フロー・エスカレーションについて ◘ Abuse のエビデンスについて 　◘ Website screenshot(phishingなど) 　◘ MX records/ A, AAAA DNS records 　◘ Malware の挙動(botnets, ransomwareなど) ◘ DNS Abuse 連絡先について ◘ Appendix：（DNS ecosystem,対応事業者,関係組織グループ)

4）ドキュメント

タイトル	**Study on Domain Name System (DNS) abuse**
組織	European Commission
概要	◘ 173ページ ◘ ドメイン空間の市場、DNS ecosystem の概要 ◘ DNS Abuse の定義 ※Abuseとして以下3つに焦点 1. 不正登録ドメインでの事象 2. DNS運用での事象 3. Webサイトコンテンツに係る事象（不正登録・侵害ドメイン含め） ◘ DNS Abuse 被害状況（ヒアリングも含め纏め） ◘ IoT , 5G がDNS Abuse にもたらす影響 ◘ DNS Abuse に対する規制の枠組み ◘ 世界レベル、EU、ICANN, Others ◘ Others(I&JPN, DNS Abuse Framework) ◘ TLD(gTLD, ccTLD)での対策の事例 ◘ DNS Abuseに向けたソリューション纏め

その他の活動中コミュニティー

- FIRST
  - Forum of Incident Response and Security Teams
  - DNS Abuse SIG

- M3AAWG
  - Messaging, Malware and Mobile Anti-Abuse Working Group

DNS Abuseハンドリングブック作成までの流れ

海外ドキュメントの精査

日本語に訳す

日本語文書をDNS事業者や関係者内で議論
（DNSOPS,その他関係者）

ブック作成

必要に応じて内容を改定しつつ、DNS Abuseハンドリングの履歴を残す

日本語版DNS Abuseハンドリングブックがあるとよい点

世界で公開されるドキュメントをベースに日本語版を作成することで、日本でも世界共通認識に沿ったDNS Abuse対応が可能となる

日本でも世界共通認識に沿った対応をしていると世界にアピールできる

DNS Abuse対応フローに取り入れ扱いやすいドキュメントとなる

新しいテクノロジーが登場した際、更新対象となるドキュメントが存在する

事業者・調整機関・関係組織において共通言語を意識させる

最後に

日本語版DNS Abuse ハンドリングブックは必要だと思うのですが、皆さまどう思われましたか

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

ご清聴ありがとうございました

海外で公開されたドキュメント

- DNS Abuse Framework
  - Framework to Address Abuse
  - https://dnsbuseframework.org
- ICANN Security and Stability Advisory Committee (SSAC)
  - 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
- INTERNET & JURISDICTION POLICY NETWORK
  - Toolkit DNS Level Action to Address
  - https://www.internetjurisdiction.net/domains/toolkit
- European Commission
  - Study on Domain Name System (DNS) abuse
  - https://op.europa.eu/en/publication-detail/-/publication/d9804355-7f22-11ec-8c40-01aa75ed71a1