DNS Abuse ハンドリング ブックに関するアップデート

JPCERTコーディネーションセンター
インシデントレスポンスグループ
中井 尚子

DNS Summer Day 2022 振り返り

前回のDNS Summer Day2022では、DNS Abuseハンドリングブックの必要性と世界のDNS Abuse に関する動向を説明。

- 日本にはDNS abuse をハンドルする際のマテリアルがない
- 日本でDNS abuse の議論を活発に行うためのきっかけ作り

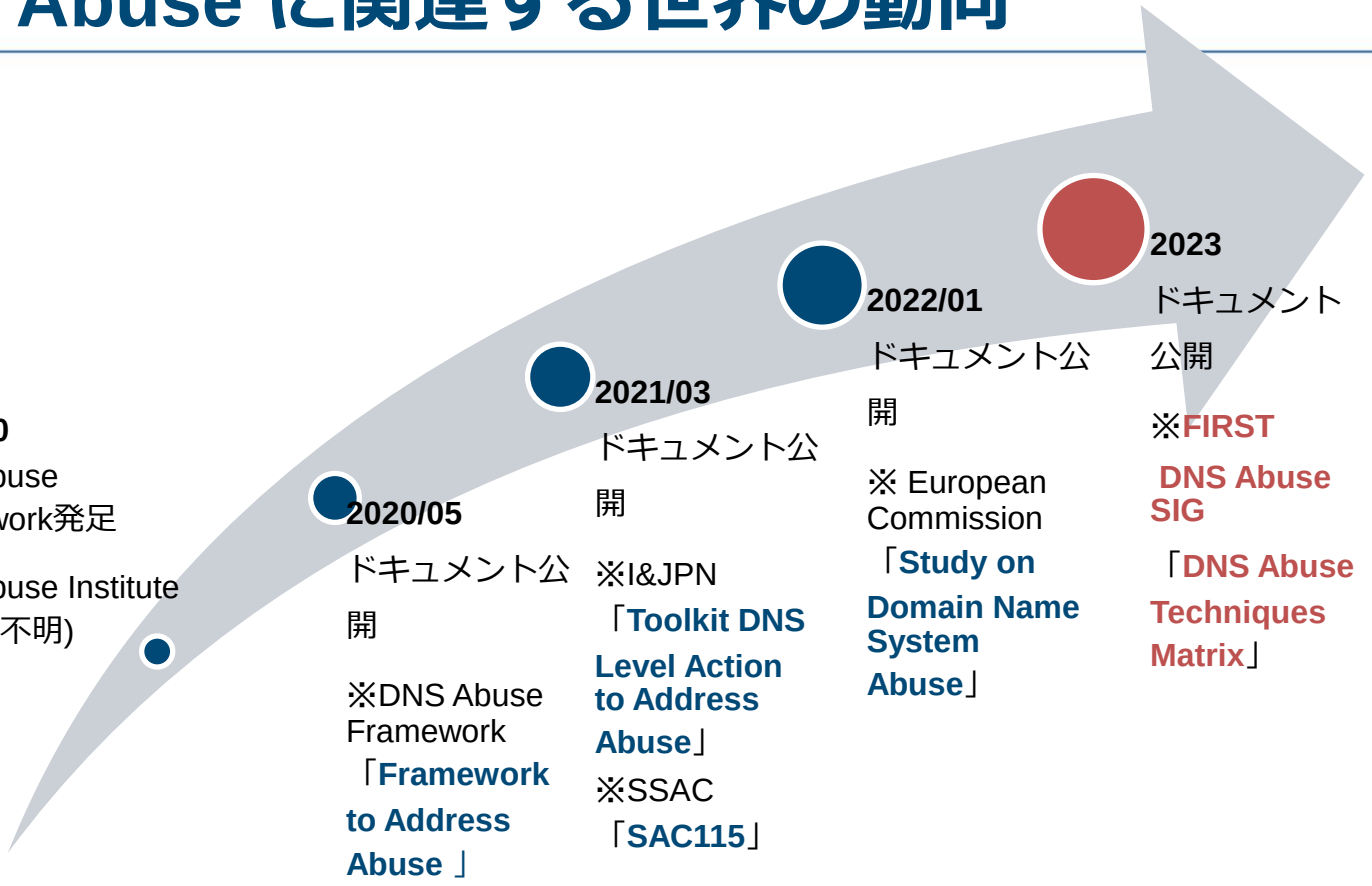
その後2023年、世界のDNS Abuse に関する動きに次のドキュメントが新しく追加されます。

FIRST DNS Abuse SIG

「DNS Abuse Techniques Matrix」

FIRST DNS Abuse SIG https://www.first.org/global/sigs/dns/

DNS Abuse に関連する世界の動向



DNS Abuse Techniques Matrix の特徴

これまでのDNS Abuseドキュメントは、最終的な被害である
フィッシングやDDoSなどのカテゴリーでまとめられるケースが
散見されるが、実際の要因や対処すべき箇所は実はもっと細かい。

DNS Abuse Techniques Matrix は一般的なカテゴリーではなく、
Techniques（手法）に着目しまとめたもの。

- インシデントで分類される一般的なカテゴリー
  - フィッシング
  - 改ざん
  - DDoS
  - スパム

DNS Abuse Techniques Matrix の特徴

- 例えば、フィッシング

情報を窃取する目的のコンテンツをインターネット上で稼働させ、認証情報や機密情報を窃取する行為であるが、行為を遂行するまでに多くの手法が絡む。

- 考えられる手法
  - 不正ドメインの登録
  - 不正サブドメインの登録
  - Webサーバー立ち上げ・コンテンツ準備
  - DNS情報書き換えによる誘導
  - フィッシングメール用ドメイン準備
  - なりすましメールの送信

DNS Abuse Techniques Matrix とは

DNS Abuse Techniques Matrix とは、Techniques（手法）に着目しまとめたもの。

- DNSの不正使用(DNS Abuse)を伴うインシデントに対応するインシデント対応チームに向けたアドバイスとなる
- DNSの不正使用の調査・研究における既存の取組を補完することを目標

DNS Abuse Techniques Matrix

ステークホルダー	15関係事業者・組織・人を掲載
手法	21種類の手法を掲載
行動	マトリックスはフェーズごとに行動を分けて整理 □ **Detect（検知）** 　□ インシデントの可能性がある事象を特定する 　□ 監視と検知、インシデント報告の受理 □ **Mitigate（緩和）** 　□ インシデントを封じ込め、安全な運用を回復させる 　□ 緩和と復旧 □ **Prevent（抑止）** 　□ DNS固有の作業手順を適用し、将来におけるこの種のインシデントの発生確率を下げる 　□ 組織内ITチームへの共有、脆弱性対応

DNS Abuse Techniques Matrix（ステークホルダー）

15関係事業者・組織・人		
レジストラー	レジストリ	権威DNSサーバー運用者
ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク管理者
アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー
機器・OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー
法執行機関および公安機関	CSIRTs / ISACs	インシデント対応者

DNS Abuse Techniques Matrix（手法）

21種類の手法			
DGA (ドメイン生成アルゴリズム)	ドメイン名の侵害	lame delegation（レイムデレゲーション）	DNSキャッシュポイズニング
DNSリバインディング	DNSサーバーの侵害	スタブリゾルバーのハイジャック	ローカルな再帰リゾルバーのハイジャック
オンパス(on-path)のDNS攻撃	DNSに対するDoS	DoSを目的としたDNSサーバーの不正使用	動的なDNS解決による検知の難化
動的なDNS解決(Fast flux)による隠ぺい	DNSを介した情報の不正な持ち込みおよび持ち出し	(実効的)セカンドレベルドメインの悪意ある登録	ダイナミックDNSプロバイダーを介した悪意あるサブドメインの作成
DNSの不正使用を目的としたDNS以外のサーバーの侵害	未登録ドメイン名を介したなりすまし	登録されたドメイン名のなりすまし	DNSトンネリング
DNSビーコン			

実際のマトリックス（Detection:検知）

FIRST

Version 1.1 (Feb 9, 2023)

TLP:CLEAR

Detection

✓ : The entity has the capability to detect

✗ : The entity lacks the capability to detect

	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrants	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
DGAs	✓ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✓ (eSLDs only)	✓ (eSLDs only, w/ analysis of customer domains)	✓ (eSLDs only)	✓ (Logs/ Passive DNS logging & analysis)	✗	✓	✗	✓	✗	N/A (Registrant is Threat Actor itself)	✗	✓ (Can engage registries and/or PSWG GAC)	✗	✓ (if outgoing queries logged)
Domain name compromise	✓	✓	✗	✓	✓ (DNS RPZ + threat intelligence feeds)	✗	✗	✗	✓	✗	✓ (w/ proactive monitoring)	✗	✓	✗	✗ (Assuming external domain)
Lame delegations	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✓ (w/ proactive monitoring)	✗	✗	✗	✗ (without historical delegation info)
DNS cache poisoning	✗	✗	✗	✗	✓ (Validating DNSSEC at the recursive and enabling extended errors - RFC 8914)	✓ (Flow analysis - NetFlow, Zeek)	✗	✗	✓	✗	✓ (w/ proactive monitoring)	✗	✗	✗	✗ (Assuming external resolver is poisoned)
DNS rebinding	✗	✗	✗	✗	✓ (pDNS analysis - DNS responses varying from	✓ (Flow analysis -	✗	✗	✓	✗	✓ (w/ proactive monitoring)	✗	✗	✗	✓

実際のマトリックス（Mitigation:緩和）

Version 1.1 (Feb 9, 2023)

TLP:CLEAR

Mitigation

✓ : The entity has the capability to mitigate

✗ : The entity lacks the capability to mitigate

	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrants	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
DGAs	✓ (updating status to onHold or changing name servers)	✓	✗	✓ (updating status to onHold or changing name servers)	✓ (dns rpz)	✗	✗	✗	✗	✗	N/A (Registrant is Threat Actor itself)	✗	✓ (Defensive registration, generate domains and share with registries)	✗	✓ (blocking)
Domain name compromise	✓ (if compromise at the registrar level)	✓	✓	✓ (if compromise is at the reseller level)	✓	✗	✗	✗	✗	✗	✓ (w/ appropriate clean up)	✗	✗	✗	✓ (blocking)
Lame delegations	✗	✗	✗	✗	✗	✗	✗	✗	✗		✓ (updating name servers)	✗	✗	✗	✗ (contact registrar, etc.)
DNS cache poisoning	✗	✗	✓	✗	✓ (DNSSEC)	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗ (contact authoritative operator, etc.)
DNS rebinding	✗	✓	✗	✗	✗	✓ (BCP38, BGP blackhole attacker's IP netblock)	✗	✗	✗	✗	✗	✗	✗	✗	✓

実際のマトリックス（Prevention:抑止）

Version 1.1 (Feb 9, 2023)

TLP:CLEAR

Prevention

✓ : The entity has the capability to prevent the threat

✗ : The entity lacks the capability to prevent the threat

	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrants	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
DGAs	✓ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✓ (eSLDs only)	✓ (if DG algorithm is known)	✓ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✓ (if DG algorithm is known, DNS RPZ + threat intelligence)	✓ (if DG algorithm is known)	✗	✗	✗	✗	N/A (registrant is threat actor itself)	✗	✓	✓ Investigating DG Algorithm)	✗
Domain name compromise	✓ (measures to prevent compromise of registrant account)	✗	✗	✓ (measures to prevent compromise of registrant account)	✗	✗	✗	✗	✗	✗	✓ (proactive measures to prevent compromise of registrant account)	✗	✓	✓ (contact relevant stakeholders)	✗
Lame delegations	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓ (good practices managing domain portfolio)	✗	✓	✓ (contact relevant stakeholders)	✗
DNS cache poisoning	✗	✗	✗	✗	✓ (DNSSEC validation enabled in the recursive)	✗	✗	✗	✗	✗	✗	✗	✓	✓ (contact recursive operator or network operator clear/refresh cache)	✗ (assuming cache is external to the org)

日本語版公開に向けて

- FIRSTのDNS Abuse Techniques Matrix の日本語版を公開します。

Version 1.1 (Feb 9, 2023)

TLP:CLEAR

検知

✓ : エンティティは検知する能力を保持している

✗ : エンティティは検知する能力が無い

	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DGA（ドメイン生成アルゴリズム）	✓ (eSLD のみ。ドメイン作成時点および存在中に分析を行っている場合)	✓ (eSLD のみ)	✓ (eSLD のみ。顧客のドメインの分析を行っている場合)	✓ (eSLD のみ)	✓ (再帰リゾルバーでロギングまたは pDNS によるロギングと分析を行っている場合)	✗	✓	✗	✓	✗	該当なし（登録者が脅威アクターそのもの）	✗	✓ (レジストリか、PSWG および GAC のどちらかあるいは両方に関与を要請可能)	✗	✓ (送出される問合わせがロギングされている場合)
ドメイン名の侵害	✓	✓	✗	✓	✓ (DNS RPZ を使用し、脅威インテリジェンスを反映している場合)	✗	✗	✗	✓	✗	✓ (事前防御的監視を行っている場合)	✗	✓	✗	✗ (組織外のドメインを想定)
lame delegation（レイムデレゲーション）	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✓ (事前防御的監視を行っている場合)	✗	✗	✗	✗ (組織外のドメインを想定)
DNS キャッシュポイズニング	✗	✗	✗	✗	✓ (再帰リゾルバーで DNSSEC 署名検証を行い RFC 8914 規定の拡張エラーを有効にしている場合)	✓ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✗	✗	✓	✗	✓ (事前防御的監視を行っている場合)	✗	✗	✗	✗ (外部のリゾルバーが汚染されたと想定)
DNS リバインディング	✗	✗	✗	✗	✓ (pDNS 分析により、パブリック IP アドレスから RFC 1918 アドレスに変化した DNS 応答を検知可能)	✓ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✗	✗	✓	✗	✓ (事前防御的監視を行っている場合)	✗	✗	✗	✓

今後のチャレンジ

Matrix Version2

- ポリシーメーカー側の行動も検討
- 手法が十分であるか
- 係るステークホルダーの意見を基に補完

日本語版ハンドリングブック

- 日本語版を公開し、取り扱いやすいハンドリングブックを制作

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/reference.html

インシデントレスポンスグループ

- Email：ir-info@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