DNSの不正使用手法に対抗するためのマトリックス
~マトリックス紹介と活用方法~

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とは

DNSとは

DNSは、Domain Name Systemの略で、 インターネット上で ドメイン名 を管理・運用するために開発されたシステムです。 現在、インターネットを利用するときに必要不可欠なシステムの一つとなっています。

郵便で手紙を送る時に住所が必要であるのと同様に、 インターネットでは、 電子メールを送ったりウェブサイトを見たりするために、 相手がインターネット上のどこにいるのかを特定する必要があります。 その際に、例えばnic.ad.jpなどのドメイン名は、 人が覚えやすい「インターネット上の住所」にあたるものとして利用されています。

（引用：JPNIC「DNSとは」https://www.nic.ad.jp/ja/basics/beginners/dns.html)

DNSの使われ方

■ Webサイト閲覧時

https://www.jpcert.or.jp/ ➡ 複雑

```
$ host www.jpcert.or.jp
www.jpcert.or.jp is an alias for d81drv6iivfiw.cloudfront.net.
d81drv6iivfiw.cloudfront.net has address 13.32.50.120
d81drv6iivfiw.cloudfront.net has address 13.32.50.45
d81drv6iivfiw.cloudfront.net has address 13.32.50.11
d81drv6iivfiw.cloudfront.net has address 13.32.50.72
```

■ メール送信時

TO：info@jpcert.or.jp ➡ 以下のいずれかのメールサーバーで受信)

```
jpcert.or.jp. 300 IN MX 20 mx02.jpcert.or.jp.  (210.148.223.19)
jpcert.or.jp. 300 IN MX 10 mx01.jpcert.or.jp.  (210.148.223.3)
```

DNSの使われ方

悪意をもった利用者によるDNSの使われ方

- フィッシングサイトの稼働
- スパムメールの配信
- マルウェア感染サイトへの誘導手段
- マルウェアの通信手段
- DoS・DDoS攻撃のツール

DNSに係るインシデント対応時の困難・苦労

- 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

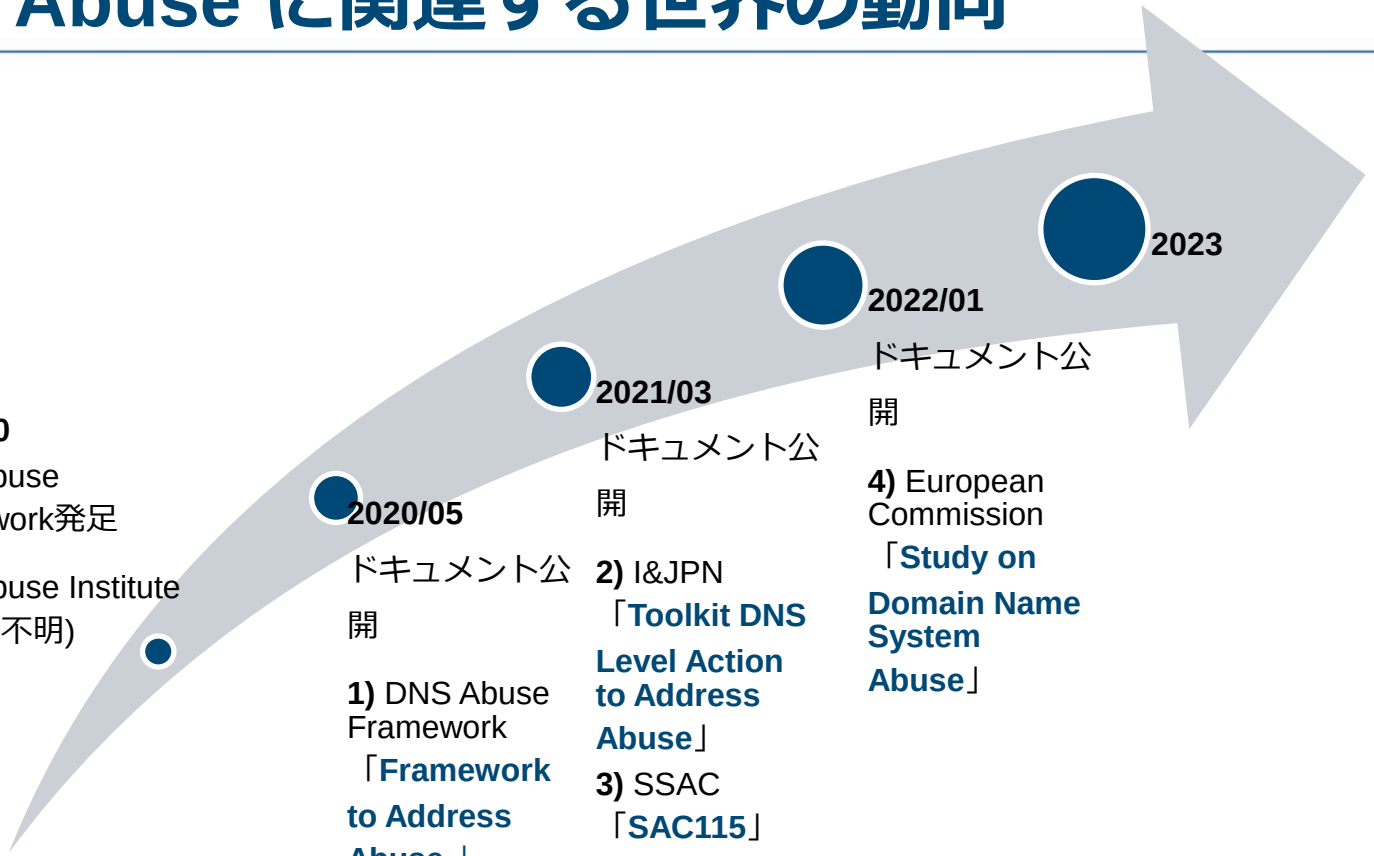
DNS Abuseハンドリング文書化へのモチベーション

DNS Abuseを対応する際に参考にするドキュメントが日本にないのであれば作ればいい

関係事業者間で交わされているノウハウを文書化し残そう

海外で議論されているDNS Abuseの流れに乗って、日本での議論や活動を始めるきっかけを作ろう

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（ヒアリングも含めまとめ） ◘ 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まとめ

完成までの流れ

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チェック

ドキュメント完成

DNSの不正使用手法に対抗するためのマトリックスの完成・公開

本日のプレゼンテーションの内容

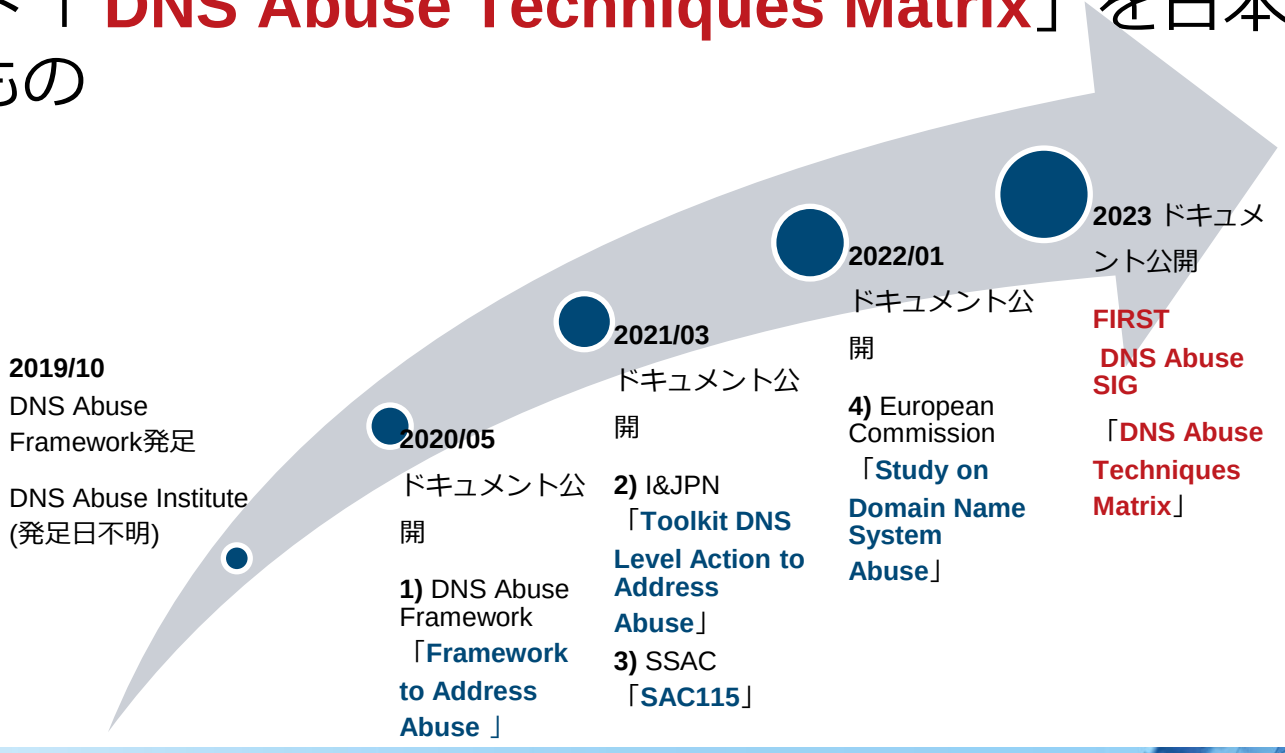
1. DNSの不正使用手法に対抗するためのマトリックスとは
2. ドキュメントの構成
3. マトリックスの見かた
4. 活用方法（ケーススタディ）
5. 課題点

本日のプレゼンテーションの内容

1. DNSの不正使用手法に対抗するためのマトリックスとは
2. ドキュメントの構成
3. マトリックスの見かた
4. 活用方法（ケーススタディ）
5. 課題点

DNSの不正使用手法に対抗するためのマトリックスとは

- 2023年にFIRST DNS Abuse SIGから公開されたドキュメント「**DNS Abuse Techniques Matrix**」を日本語訳したもの



DNSの不正使用手法に対抗するためのマトリックスの特徴

これまでのDNS Abuse関連ドキュメントは、一般的なカテゴリーであるフィッシングやDDoSなど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。

- 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の不正使用手法に対抗するためのマトリックスの特徴

■ 例えば、フィッシング

> フィッシング とは実在する組織を騙って、ユーザネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった個人情報を詐取することです。
>
> （引用：フィッシング対策協議会「フィッシングとは」(https://www.antiphishing.jp/consumer/abt_phishing.html)

フィッシング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の不正使用手法に対抗するためのマトリックスとは

カテゴリーではなく、テクニック（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する
- 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

範囲対象外

DNS が関与する攻撃と並行して使われるその他の手法

- BGP ハイジャック
- TLS 証明書のなりすましといったもの

マルウェアなど不正プログラムによるDNSの不正使用に係る範囲

- DGAドメイン生成に使われるマルウェアへの対処などは対象外

本日のプレゼンテーションの内容

1. DNSの不正使用手法に対抗するためのマトリックスとは
2. ドキュメントの構成
3. マトリックスの見かた
4. 活用方法（ケーススタディ）
5. 課題点

ドキュメントの構成

ドキュメントは22枚（気軽に読めるボリューム）

- 用語の説明
  - ステークホルダー
  - 手法
  - 行為
    - 検知
    - 緩和
    - 抑止
- 不正手法の例
- マトリックス

用語の説明

ステークホルダー	15関係事業者・組織・人で構成 各ステークホルダーの説明を記載
手法	21種類の手法で構成 各手法の説明を記載
行為	フェーズごとに行為を3パターンに分けて記載 • Detect（検知） • Mitigate（緩和） • Prevent（抑止）

用語の説明：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

ステークホルダーの説明（一部紹介）

- レジストラー – TLD 下位へのドメイン登録を許可する組織 - 詳細については https://www.icann.org/en/icann-acronyms-and-terms/registrar-en 参照。

- レジストリ – TLD に関するドメインのデータベースを維持する責任を負う組織 - 詳細については https://www.icann.org/en/icann-acronyms-and-terms/registry-en 参照。

- ネットワーク運用者 – AS の運用組織。この能力を持つ組織は、再帰 DNS サーバーを稼働させていない ものと想定する。この列は、ネットフローの情報(送信元/宛先 IP アドレス、L3 プロトコル、送信元/宛先ポ ート番号など)や BGP ルーティングデータを意味し、パッシブ DNS は除外する(明確化のため)。

- ホスティングプロバイダー - インターネットホスティングサービスを提供する会社。インターネットホスティン グサービスとは、インターネットに接続されたサーバーを運営し、組織や個人がインターネットに接続され たコンテンツを提供したり、サービスをホストしたりできるようにするサービスである。詳しくは、 https://en.wikipedia.org/wiki/Internet_hosting_service 参照。

留意：ホスティングプロバイダーが防弾ホスティングである場合や攻撃インフラの提供に加担している場 合、連絡したとしても、よくて何も得るものはなく、最悪の場合チームが報復に晒されることになる。

用語の説明：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			

手法の説明（一部紹介）

- DGA (ドメイン生成アルゴリズム) – 詳細については https://attack.mitre.org/techniques/T1568/002/ 参 照。

- ドメイン名の侵害 – ドメイン名の正当な保有者から管理権限を不当に奪う。侵害されたドメインは、さまざ まな悪意ある行為、例えば SPAM の送信、フィッシング、マルウェアの配布、ボットネットのコマンド＆コン トロール(C2)などに使用される可能性がある。詳細については https://www.icann.org/groups/ssac/documents/sac-007-en 参照。

- lame delegation（レイムデレゲーション）– ネームサーバーのドメインの有効期限が切れると lame delegation が発生する。攻撃者は期限が切れたネームサーバーのドメインを再登録することにより、その ドメインの管理権限を得られる。詳細については https://blog.apnic.net/2021/03/16/the-prevalence-persistence-perils-of-lame-nameservers/ 参照。

- DNS キャッシュポイズニング – DNS スプーフィングとも呼ばれる。サイバー攻撃の一種で、攻撃者が偽の DNS レコードを注入することによって DNS リゾルバーのキャッシュを汚染し、攻撃者に制御されたレコー ドをリゾルバーに保存させる。詳細については https://capec.mitre.org/data/definitions/142.html 参照。

用語の説明：行為

フェーズごとに行為を3パターンに分けて記載

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

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

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

不正手法の例

- JPCERT/CC

ドメイン生成アルゴリズム(DGA)や、セカンドレベルドメインの悪意ある登録などの手法を紹介

Phishing URL dataset from JPCERT/CC

- 米国歳入庁(IRS)

悪意ある登録やなりすましを利用した手法を紹介

IRS reports significant increase in texting scams; warns taxpayers to remain vigilant

- Nominet

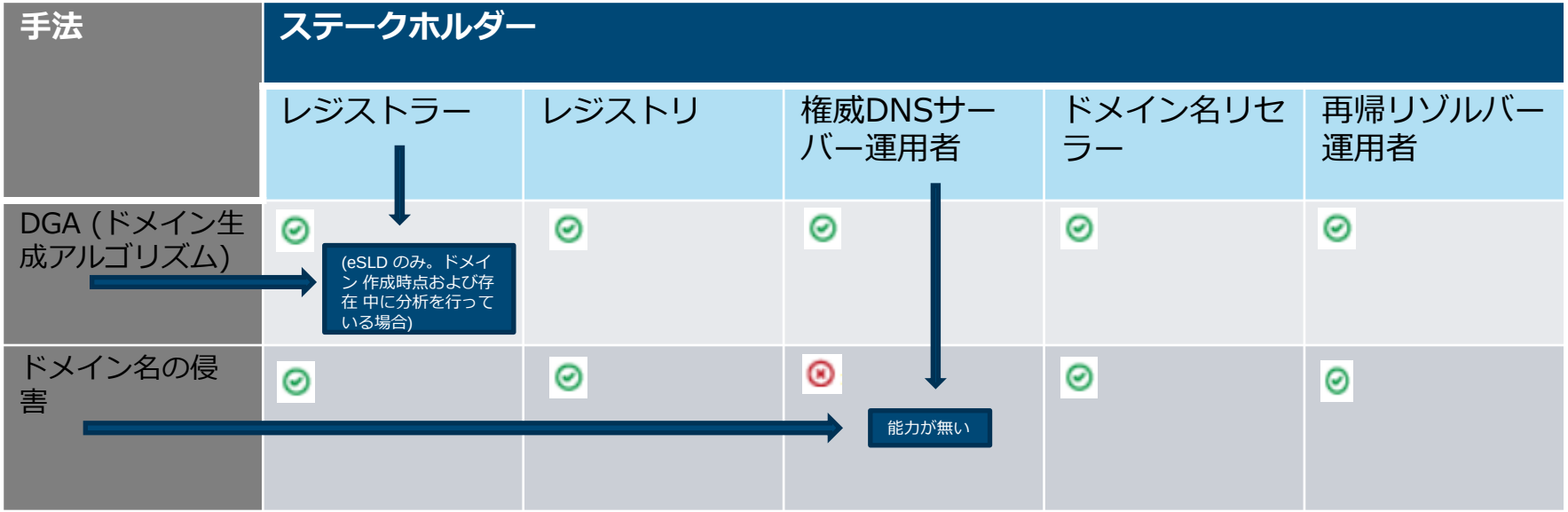
DNS の dangling エントリーがどのように lame delegation やオンパスの DNS 攻撃といった手法につながる脆弱性をもたらすかを紹介

Dangling DNS is no laughing matter

本日のプレゼンテーションの内容

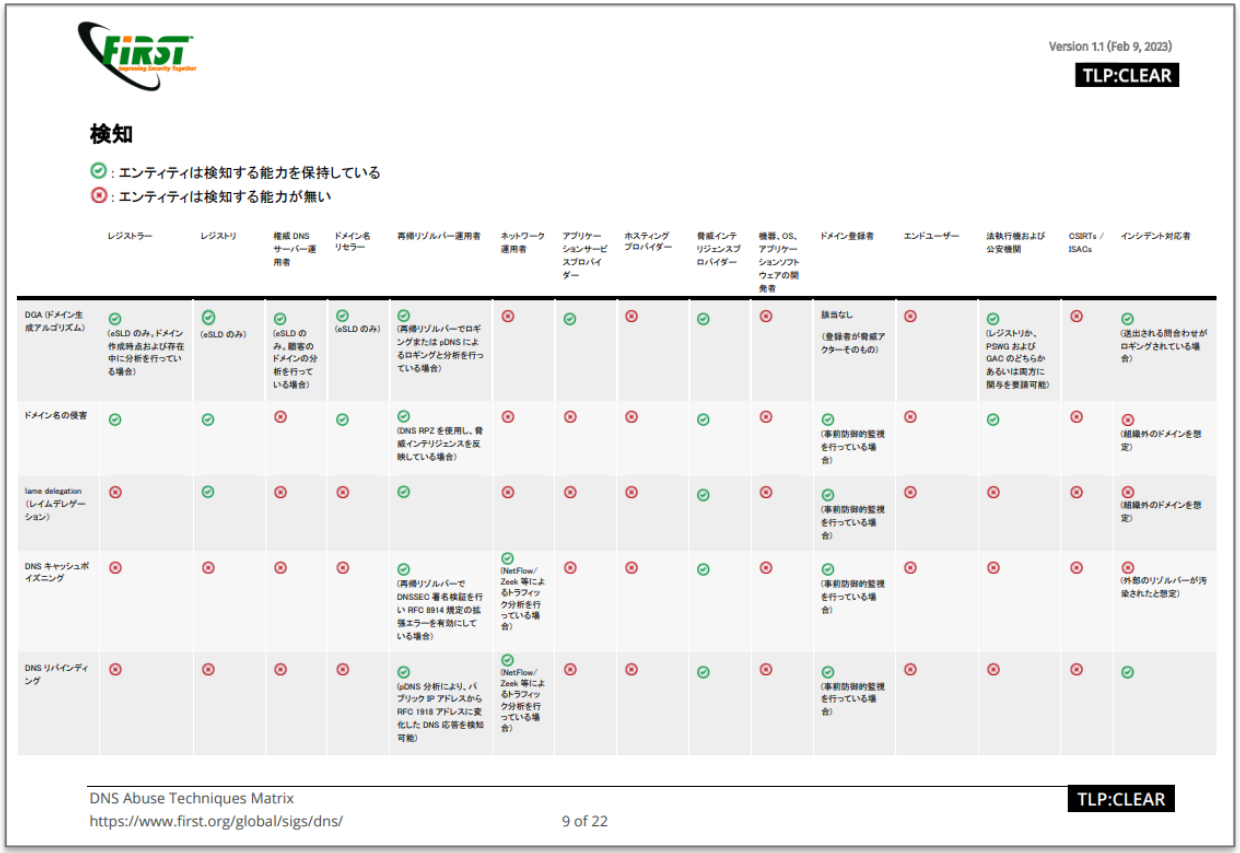
1. DNSの不正使用手法に対抗するためのマトリックスとは
2. ドキュメントの構成
3. マトリックスの見かた
4. 活用方法（ケーススタディ）
5. 課題点

マトリックスの見かた



- エンティティは能力を保持している
- エンティティは能力が無い

マトリックス：検知



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

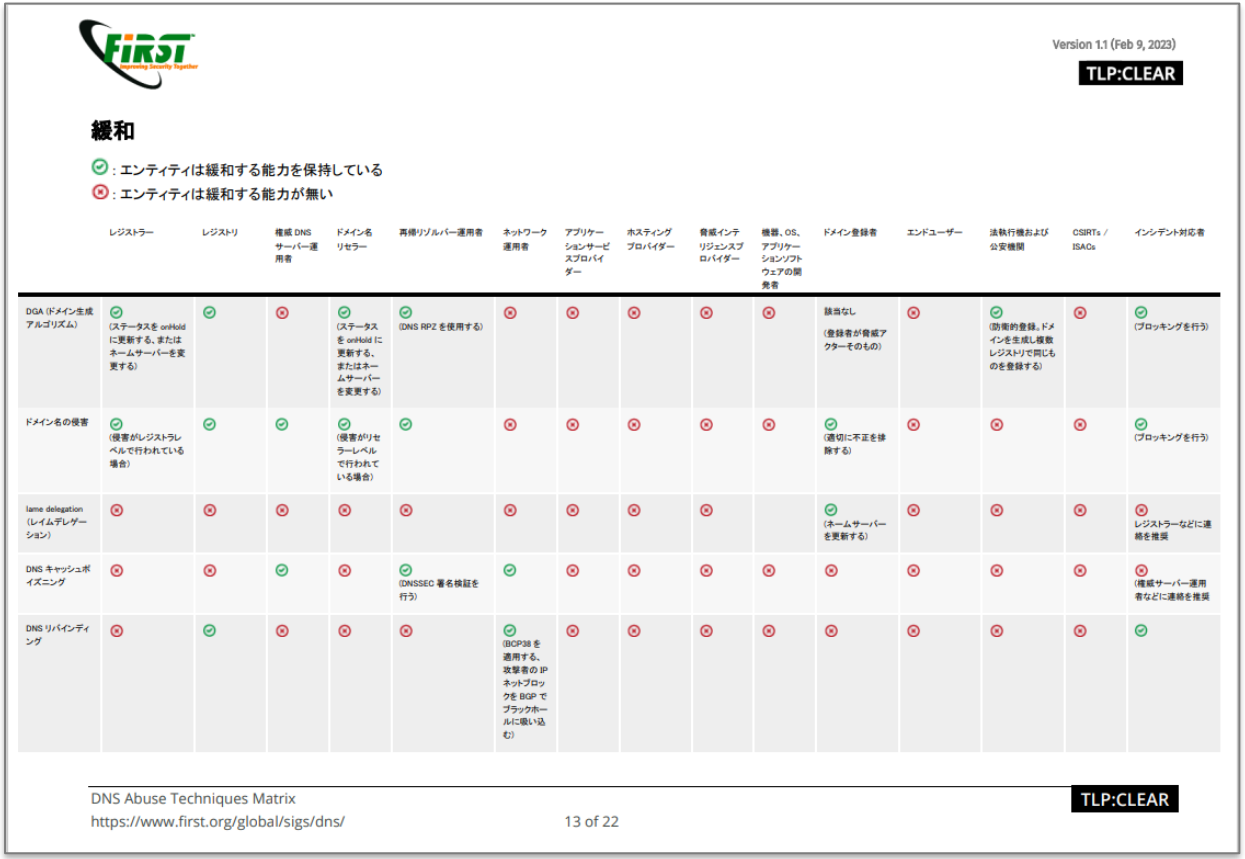
	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
DGA (ドメイン生成アルゴリズム)	(eSLD のみ。ドメイン作成時点および存在中に分析を行っている場合)	(eSLD のみ)	(eSLD のみ。顧客のドメインの分析を行っている場合)	(eSLD のみ)	(再帰リゾルバーでロギングまたは 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)				

DNS Abuse Techniques Matrix
https://www.first.org/global/sigs/dns/

9 of 22

TLP:CLEAR

マトリックス：緩和



Version 1.1 (Feb 9, 2023)

TLP:CLEAR

緩和

✓ : エンティティは緩和する能力を保持している

✗ : エンティティは緩和する能力が無い

	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)	✓ (ステータスを onHold に更新する、またはネームサーバーを変更する)	✓	✗	✓ (ステータスを onHold に更新する、またはネームサーバーを変更する)	✓ (DNS RPZ を使用する)	✗	✗	✗	✗	✗	該当なし (登録者が脅威アクターそのもの)	✗	✓ (防衛的登録。ドメインを生成し複数レジストリで同じものを登録する)	✗	✓ (ブロッキングを行う)
ドメイン名の侵害	✓ (侵害がレジストラレベルで行われている場合)	✓	✓	✓ (侵害がリセラーレベルで行われている場合)	✓	✗	✗	✗	✗	✗	✓ (適切に不正を排除する)	✗	✗	✗	✓ (ブロッキングを行う)
lame delegation (レイムデレゲーション)	✗	✗	✗	✗	✗	✗	✗	✗	✗		✓ (ネームサーバーを更新する)	✗	✗	✗	✗ レジストラーなどに連絡を推奨
DNS キャッシュポイズニング	✗	✗	✓	✗	✓ (DNSSEC 署名検証を行う)	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗ (権威サーバー運用者などに連絡を推奨
DNS リバインディング	✗	✓	✗	✗	✗	✓ (BCP38 を適用する、攻撃者の IP ネットブロックを BGP でブラックホールに吸い込む)	✗	✗	✗	✗	✗	✗	✗	✗	✓

DNS Abuse Techniques Matrix

https://www.first.org/global/sigs/dns/

13 of 22

TLP:CLEAR

マトリックス：抑止

Version 1.1 (Feb 9, 2023)

TLP:CLEAR

抑止

: エンティティは抑止する能力を保持している

: エンティティは抑止する能力が無い

	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う)	(eSLD のみ)	(DGA が既知の場合)	(eSLD のみ。ドメイン作成時点および存在中に分析を行う)	(DGA が既知であれば、DNS RPZ を使用し脅威インテリジェンスを反映する)	(DGA が既知の場合)					該当なし (登録者が脅威アクターそのもの)			(DGA の調査)	
ドメイン名の侵害	(登録者アカウントの侵害を抑止する対策を講じる)			(登録者アカウントの侵害を抑止する対策を講じる)							(登録者アカウントの侵害を抑止する事前防御策を講じる)			(関連するステークホルダーに連絡する)	
lame delegation (レイムデレゲーション)											(ドメインポートフォリオを管理するための優れた実践を導入する)			(関連するステークホルダーに連絡する)	
DNS キャッシュポイズニング					(再帰リゾルバーで DNSSEC 署名検証を有効にする)									(再帰リゾルバー運用者またはネットワーク運用者に連絡し、キャッシュのクリア/リフレッシュを確認)	(キャッシュは組織外にあると想定)

DNS Abuse Techniques Matrix
https://www.first.org/global/sigs/dns/ 17 of 22

TLP:CLEAR

本日のプレゼンテーションの内容

1. DNSの不正使用手法に対抗するためのマトリックスとは
2. ドキュメントの構成
3. マトリックスの見かた
4. 活用方法（ケーススタディ）
5. 課題点

DNSの不正使用手法に対抗するためのマトリックスの活用方法

フィッシング

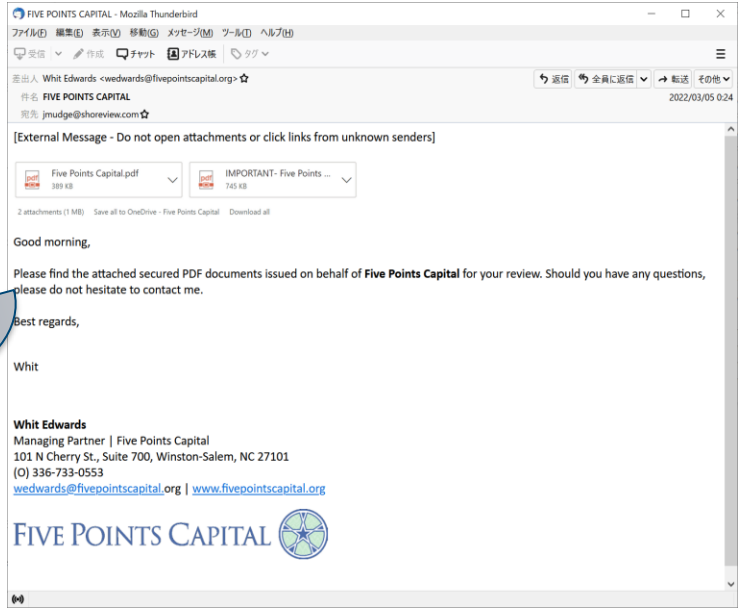
- フィッシングメール
- フィッシングサイトの稼働
- フィッシング活動の準備

フィッシングメール

- Five Points Capital になりすましたフィッシングメール
- 対象ドメイン名
  - 正）fivepointscapital.com
  - 偽）fivepointscapital.org

フィッシングメールヘッダー

```
Received: from 223404411203 named unknown by gmailapi.google.com with
 HTTPREST; Fri, 4 Mar 2022 07:24:49 -0800
From: Whit Edwards <wedwards@fivepointscapital.org>
Date: Fri, 4 Mar 2022 07:24:49 -0800
Message-ID:
<CALYXdvkVcj3ttxy34VqKEgz_tmwEExjdLB1smvTjopMbU2zwaQ@mail.gm
ail.com>
Subject: FIVE POINTS CAPITAL
To: <xxxxxx@shoreview.com>
```



パッシブDNS情報

```
;;  bailiwick: fivepointscapital.org.
;;      count: 1
;; first seen: 2022-03-04 15:11:31 -0000
;;  last seen: 2022-03-04 15:11:31 -0000
fivepointscapital.org. IN MX 1 aspmx.l.google.com.
```

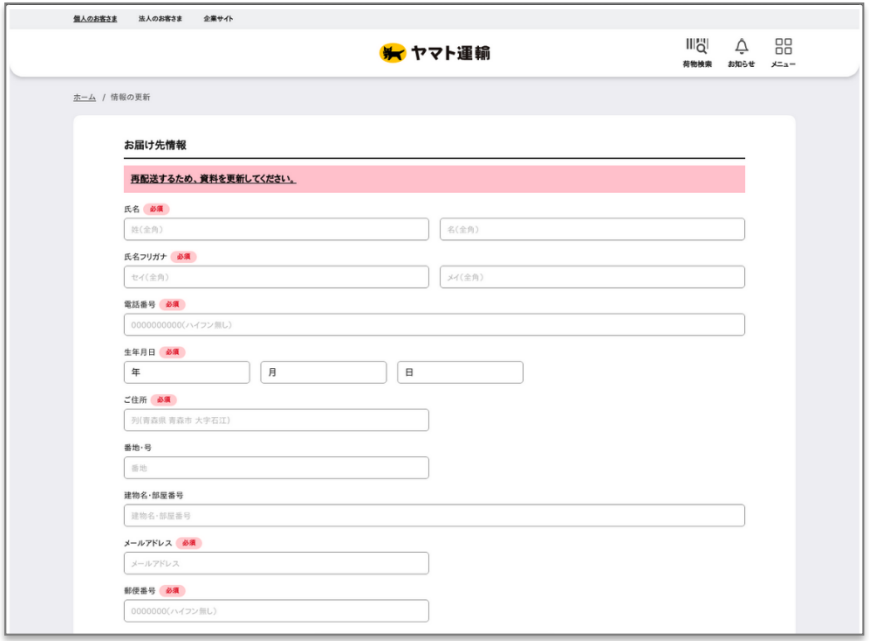
フィッシングメール

- 手法：登録されたドメイン名のなりすまし
  - Header-From なりすまし
  - 正規ドメインになりすました偽装ドメイン

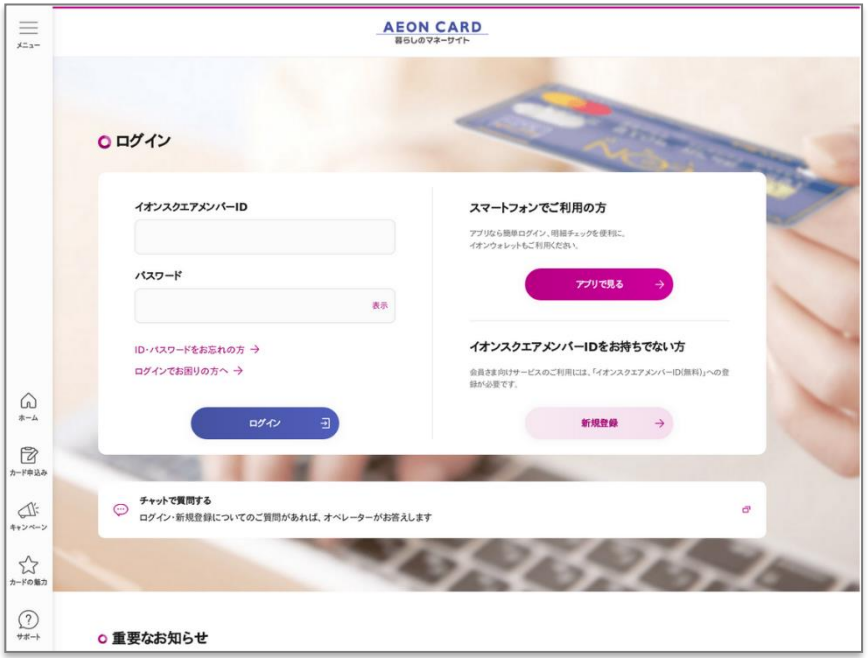
	レジストラー	レジストリ	権威 DNS サーバー運用者	ドメイン名リセラー	再帰リゾルバー運用者	ネットワーク運用者	アプリケーションサービスプロバイダー	ホスティングプロバイダー	脅威インテリジェンスプロバイダー	機器、OS、アプリケーションソフトウェアの開発者	ドメイン登録者	エンドユーザー	法執行機および公安機関	CSIRTs / ISACs	インシデント対応者
検知															
登録されたドメイン名のなりすまし	⊗	✓	⊗	⊗	✓ (DNS 応答の分析を行い RFC 8914 規定の拡張エラーを有効にしている場合)	⊗	✓	✓ (防弾ホスティングでない場合)	✓	⊗	⊗ (DMARC を使用していない場合)	⊗	✓	⊗	✓ (DMARC を使用しているか、pDNS による分析を行っていると想定)
緩和															
登録されたドメイン名のなりすまし	✓ (ドメイン作成時点または存在中に分析を行っている場合)	⊗	⊗	✓ (ドメイン作成時点または存在中に分析を行っている場合)	✓	⊗	⊗	✓ (防弾ホスティングでない場合)	⊗	⊗	✓ (状況に応じて通報するか、UDRP または URS を申し立てる)	⊗	⊗	⊗	⊗ (DMARC を適用していても、なりすましは止められない)
抑止															
登録されたドメイン名のなりすまし	✓ (eSLD のみ。ドメイン生成時に分析を行う)	⊗	✓ (偽装ドメインがサービス対象となり解決が行われるのを防止する)	✓ (eSLD のみ。ドメイン生成時に分析を行う)	⊗	⊗	⊗	✓ (防弾ホスティングでない場合)	⊗	✓	該当なし (登録者が脅威アクターそのもの)	⊗	✓	✓ (情報を共有し関心を高める)	⊗

フィッシングサイト

https://kuronekohelp.com/information



https://japan-japan-aeon.shop/index.php



フィッシングサイト

■ 手法：(実効的)セカンド レベルドメインの 悪意ある登録

	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
検知															
(実効的)セカンドレベルドメインの悪意ある登録	✓ (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)	✓	✓ (登録された文字列による)	✓	✓ (pDNS 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)	✗	✓ (レジストラーに連絡し、レジストリへのエスカレーションを要請)	✗	✗ (登録の検知はできない)
緩和															
(実効的)セカンドレベルドメインの悪意ある登録	✓ (ステータスを onHold に更新する、またはネームサーバーを変更する)	✓	✗	✓ (ステータスを onHold に更新する、またはネームサーバーを変更する)	✓	✗	✗	✗	✗	✗	該当なし (登録者が脅威アクターそのもの)	✗	✓ (レジストラー/レジストリへの通知、(法執行機関による)ドメインの押収)	✗	✗ (登録それ自体には対処できない)
抑止															
(実効的)セカンドレベルドメインの悪意ある登録	✓ (eSLD のみ。ドメイン作成時に分析を行う)	✓	✗	✓ (eSLD のみ。ドメイン作成時に分析を行う)	✗	✗	✗	✗	✗	✓	該当なし (登録者が脅威アクターそのもの)	✗	✓ (レジストラーに通知し、レジストリへのエスカレーションを要請)	✓ (関連するステークホルダーに連絡する)	✗

フィッシング活動の準備

- DNSを改ざんしフィッシング活動開始前の環境の準備

- TXT レコードのSPF認証情報の改ざん ➡ フィッシングメール送信の準備

```
;;  bailiwick: *****.jp.
;; first seen: 2022-01-28 20:59:00 -0000
;;  last seen: 2022-01-28 20:59:00 -0000
*****.jp. IN TXT "v=spf1 ip4:133.242.52.116 ~all"
*****.jp. IN TXT "v=spf1 ip4:27.102.118.13/17 ~all"
*****.jp. IN TXT "v=spf1 a mx ptr a: ***** .jp ip4:27.102.118.0/24 ?all"
```

- サブドメインの追加 ➡ フィッシングサイト稼働の準備

```
;;  bailiwick: *****.jp.
;;      count: 93
;; first seen: 2022-01-23 12:38:07 -0000
;;  last seen: 2022-01-29 03:26:55 -0000
xserver-vps. *****.jp. IN A 115.144.69.72
```

フィッシング活動の準備

■手法：ドメイン名の侵害

DNSの不正使用手法に対抗するためのマトリックスの活用方法

その他

- Lame Delegation（レイムデレゲーション）
- 権威DNSサーバーに対する水責め攻撃
- ドメインハイジャックによるキャッシュ汚染

Lame Delegation （レイムデレゲーション）

Lame Delegationとは、delegation（委任）の際に上位ゾーンに登録したDNSサーバが、何らかの理由によりそのドメインのDNSサーバとして正しく動作していない状態

（引用：JPRS「DNSの健全な運用のために～Lame Delegation 編～」(https://jprs.jp/tech/notice/2003-05-20-dnsqc-lame-delegation.html)

```
Domain Information: [ドメイン情報]
[Domain Name]                **********.JP

[登録者名]                   **********株式会社
[Registrant]                 **********

[Name Server]                ns-1926.awsdns-48.co.uk
[Name Server]                ns-309.awsdns-38.com
[Name Server]                ns-1008.awsdns-62.net
[Name Server]                ns-2000.awsdns-58.co.uk
[Signing Key]

[登録年月日]                 2016/11/15
[有効期限]                   2023/11/30
[状態]                       Active
[最終更新]                   2022/12/01 01:05:08 (JST)
```

不一致

```
$ dig @ns-309.awsdns-38.com **********.jp

;; AUTHORITY SECTION:
**********.jp. 172800 IN NS ns-1008.awsdns-62.net.
**********.jp. 172800 IN NS ns-1268.awsdns-30.org.
**********.jp. 172800 IN NS ns-2000.awsdns-58.co.uk.
**********.jp. 172800 IN NS ns-309.awsdns-38.com.
```

```
$ dig @ns-1926.awsdns-48.co.uk **********.jp

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 24815
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available
;; QUESTION SECTION:

; **********.jp. IN A
```

ns-1926.awsdns-48.co.uk は情報をもっていない

Lame Delegation（レイムデレゲーション）

- 手法：Lame Delegation（レイムデレゲーション）
  - ドメイン登録者での対応がメイン

	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
検知															
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）
緩和															
lame delegation（レイムデレゲーション）	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗		✓（ネームサーバーを更新する）	⊗	⊗	⊗	⊗ レジストラーなどに連絡を推奨
抑止															
lame delegation（レイムデレゲーション）	⊗	✓	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓（ドメインポートフォリオを管理するための優れた実践を導入する）	⊗	✓	✓（関連するステークホルダーに連絡する）	⊗

権威DNSサーバーに対する水責め攻撃

- DNS水責め攻撃
  - —Open Resolverを利用し水責め攻撃を実行
  - — 対象は jpcert.or.jp ドメイン権威DNSサーバー

JPCERT/CCドメインが対象となった水責め攻撃の一部
2023-07-08 21:46:53.570989 IP SourceOfAttack.39636 > Open Resolver.53: 19199+ A? amur.jpcert.or.jp. (35)
2023-07-08 21:46:55.153998 IP SourceOfAttack.39636 > Open Resolver.53: 52204+ A? chickadee.jpcert.or.jp. (40)
2023-07-08 21:47:00.651903 IP SourceOfAttack.39636 > Open Resolver.53: 9206+ A? cycle1.jpcert.or.jp. (37)
2023-07-08 21:47:02.548646 IP SourceOfAttack.39636 > Open Resolver.53: 11887+ A? mosaffa.jpcert.or.jp. (38)
2023-07-08 21:47:05.370698 IP SourceOfAttack.39636 > Open Resolver.53: 18118+ A? sokolova-nina.jpcert.or.jp. (44)

権威DNSサーバーに対する水責め攻撃

- 手法：DoS を目的とした DNS サーバーの 不正使用

	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
検知															
DoS を目的とした DNS サーバーの不正使用	⊗	⊗	✓ (攻撃が権威サーバーの応答を利用している場合)	⊗	✓ (攻撃が再帰リゾルバーまたは権威サーバーに対するもので、かつロギング、NetFlow/Zeek 等によるトラフィック分析を行っている場合)	✓ (NetFlow/Zeek 等によるトラフィック分析を行っている場合)	⊗	⊗	⊗	✓	⊗	⊗	✓	⊗	✓
緩和															
DoS を目的とした DNS サーバーの不正使用	⊗	✓	✓	⊗	✓	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓
抑止															
DoS を目的とした DNS サーバーの不正使用	⊗	⊗	✓ (攻撃が権威サーバーの応答を利用している場合)	⊗	✓ (ACL やレート制限などを適用する)	⊗	⊗	⊗	⊗	✓	⊗	✓ (ファームウェアを最新の状態に保ち、適切な設定を行うなど)	✓ (踏み台となっている DNS サーバーを特定するためナショナルレベルの CERT に関与を要請)	✓ (オープンリゾルバーおよび感染した機器について調整を行う)	✓ (感染した機器をクリーンアップする)

ドメインハイジャックによるキャッシュ汚染

- NSサーバー情報の改ざんにより、不正な情報が再帰リゾルバー（キャッシュDNSサーバー）に記録されキャッシュが汚染される状況

正常な状態

```
whois :*********.com
Domain Name: *********.COM

Name Server: NS-1515.AWSDNS-61.ORG
Name Server: NS-1985.AWSDNS-56.CO.UK
Name Server: NS-405.AWSDNS-50.COM
Name Server: NS-650.AWSDNS-17.NET
```

ハイジャック後

```
;;  bailiwick: *********.com.
;;      count: 1,686
;; first seen: 2020-05-30 15:43:14 -0000
;;  last seen: 2020-06-01 16:04:04 -0000
coincheck.com. IN NS ns-650.awsdns-017.net.
coincheck.com. IN NS ns-1515.awsdns-061.org.
coincheck.com. IN NS ns-1985.awsdns-056.co.uk.
```

NS-650.AWSDNS-17.NET	➡	ns-650.awsdns-017.net
NS-1515.AWSDNS-61.ORG	➡	ns-1515.awsdns-061.org.
NS-1985.AWSDNS-56.CO.UK	➡	ns-1985.awsdns-056.co.uk

ドメインハイジャックによるキャッシュ汚染

手法：DNS キャッシュポイズニング

	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
検知															
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)
緩和															
DNS キャッシュポイズニング	⊗	⊗	✓	⊗	✓ (DNSSEC 署名検証を行う)	✓	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗ (権威サーバー運用者などに連絡を推奨
抑止															
DNS キャッシュポイズニング	⊗	⊗	⊗	⊗	✓ (再帰リゾルバーで DNSSEC 署名検証を有効にする)	⊗	⊗	⊗	⊗	⊗	⊗	⊗	✓	✓ (再帰リゾルバー運用者またはネットワーク運用者に連絡し、キャッシュのクリア/リフレッシュを確認)	⊗ (キャッシュは組織外にあると想定)

本日のプレゼンテーションの内容

1. DNSの不正使用手法に対抗するためのマトリックスとは
2. ドキュメントの構成
3. マトリックスの見かた
4. 活用方法（ケーススタディ）
5. 課題点

課題点

国や地域によってステークホルダーの責任範囲が異なるケースもある

悪意をもった事業者によるサービス提供下においては、本マトリックスの活用は困難

ポリシーに係る事象を対処する際、本マトリックスの活用は困難

対抗処置はアップデートされるため、マトリックスの更新も必要となる

さいごに

- **DNSの不正使用手法に対抗するためのマトリックス**は、インシデント対応者やDNS不正使用を調査されている方向けにまとめたものです。

- セキュリティインシデントを深く調査する中で、DNSに関わるケースがあると思います。その際、**DNSの不正使用手法に対抗するためのマトリックス**が調査や、調整の一助となれば幸いです。

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

インシデント報告

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

インシデントレスポンスグループ

- Email：ir-info@jpcert.or.jp

ご清聴ありがとうございました

参考Webサイト

- JPCERT/CC
  - DNS の不正使用手法に対抗するためのマトリックス
  - Phishing URL dataset from JPCERT/CC
- FIRST DNS Abuse SIG
  - DNS Abuse Technique Matrix
- Framework to Address Abuse
  - DNS Abuse Framework
- ICANN
  - SAC115（SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS）
- INTERNET & JURISDICTION POLICY NETWORK
  - Toolkit DNS Level Action to Address
- EU(European Union)
  - Study on Domain Name System (DNS) abuse
- 米国歳入庁(IRS)
  - IRS reports significant increase in texting scams; warns taxpayers to remain vigilant
- Nominet
  - Dangling DNS is no laughing matter