調整機関から見るドメイン空間で起きていることと対処について考える

一般社団法人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
シニアインシデントコーディネーター
中井 尚子

調整の流れ

受付
- 第三者からの報告
- 当事者からの報告

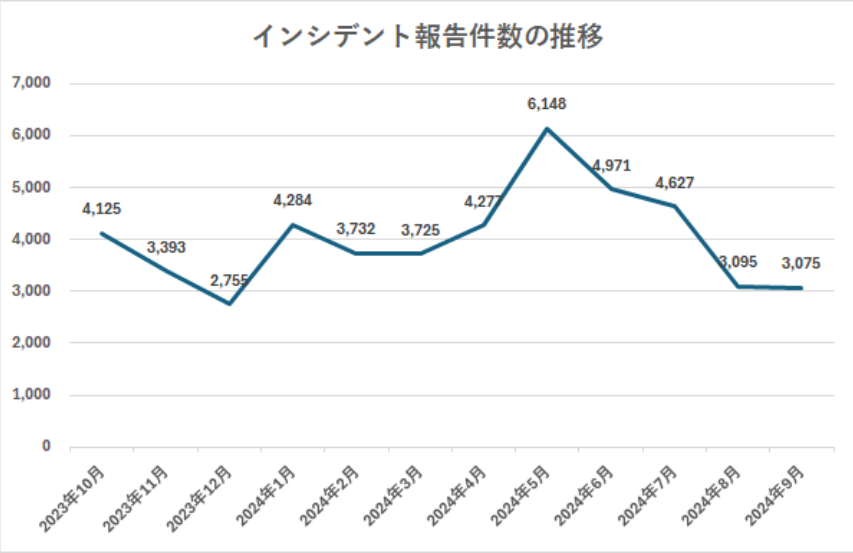
調査
- 改ざんサイト、マルウェアサイトの調査
- 外部関連サイトの調査、情報収集

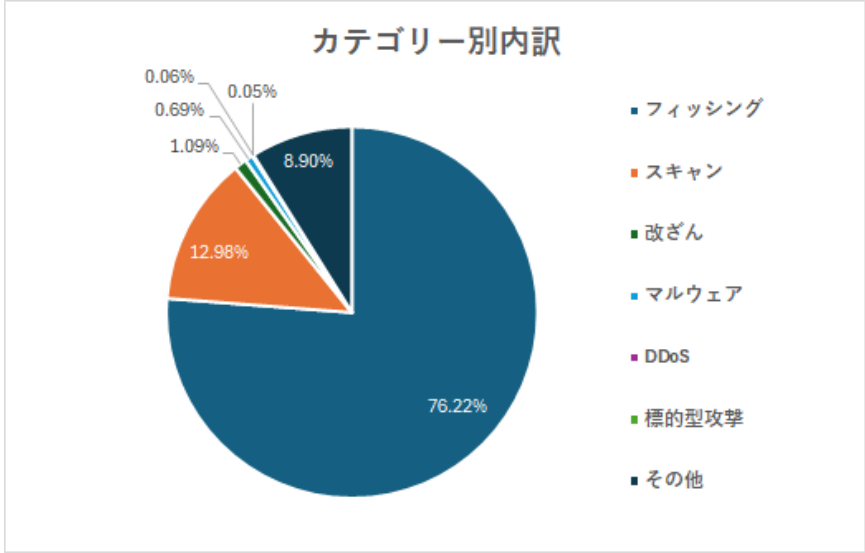
分析
- 証拠の確認(ログ分析、マルウェア分析)
- 状況把握

調整
- 適切な連絡先の特定
- 確認、対処依頼

インシデントの状況

- 2023年10月から2024年9月までのインシデント報告件数の推移とカテゴリー別内訳





インシデントの状況

- インターネット空間で発生するインシデントを調査・調整していくと、多くのケースはドメイン名に関係する

フィッシング

・不正ドメイン名登録
・サブドメイン名不正登録
・DNSレコード改ざん
・DDNSサービス悪用
・など

改ざん・その他

・lame delegation
・subdomain takeover
・ドメイン名ドロップキャッチ
・ドメイン名不正移管
・など

マルウェア

・不正ドメイン名登録
・DNSビーコン
・など

今日のトピック

- 悪意あるドメイン名の登録
- ドメイン名の不正移管
- ドメイン名ドロップキャッチ

悪意あるドメイン名の登録

悪意ある目的で登録されたドメイン名の使われ方

- フィッシング行為
  - フィッシングサイトに使われたドメイン名
    - Kuronekoyamatc[.]cc
    - Biglobes[.]net
    - ucs-card[.]top

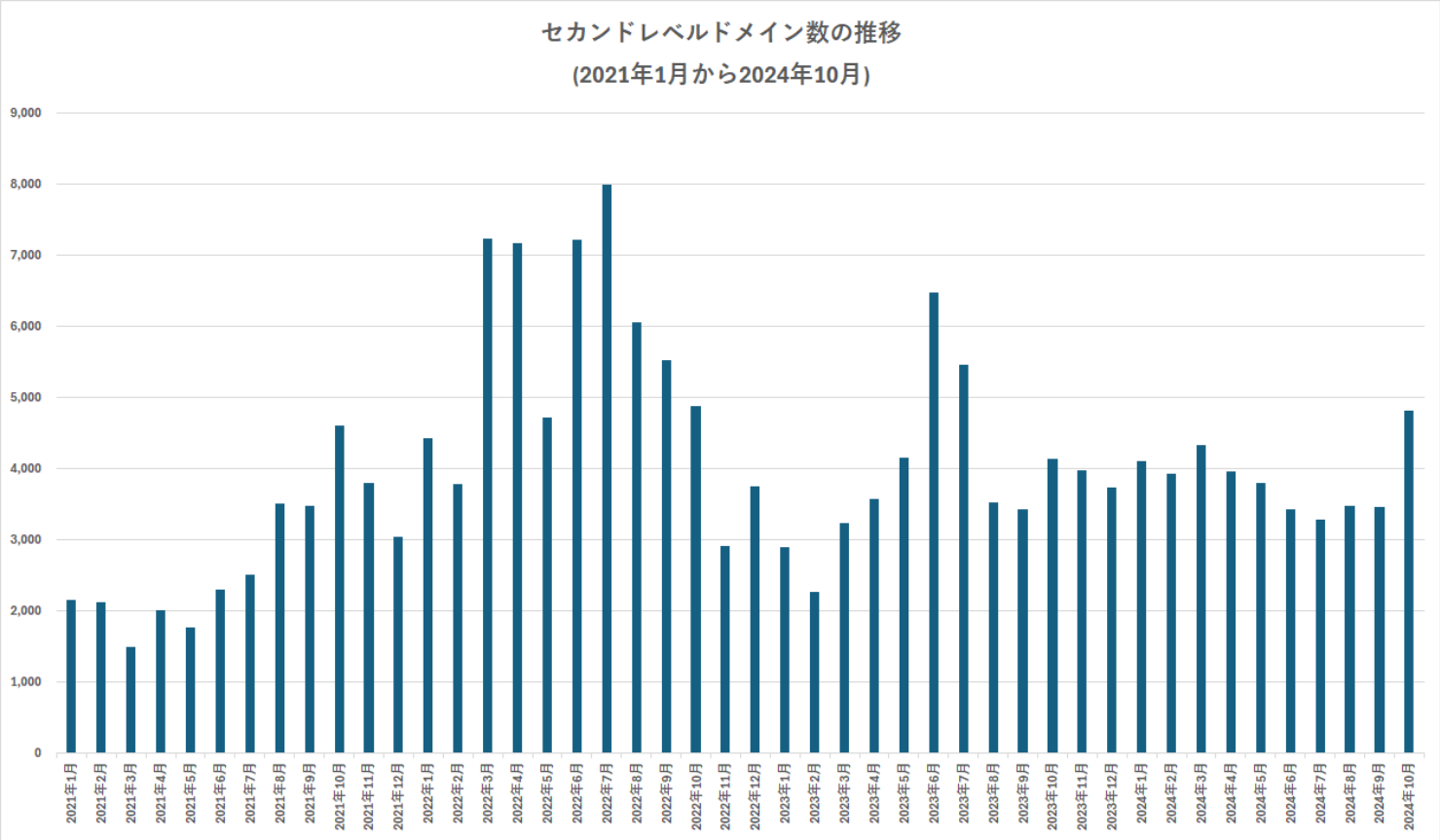
- ドメイン名ハイジャック
  - 不正ネームサーバー用に登録されたドメイン名
    - ns-650.awsdns-017[.]net
    - ns-1985.awsdns-056.co[.]uk

- 標的型メールに添付された .rdp
  - RDP接続先として準備されたドメイン名
    - us-west-1-amazon.ua-energy[.]cloud
    - aws-s3[.]cloud
    - zero-trust[.]solutions

Amazon：Amazon identified internet domains abused by APT29

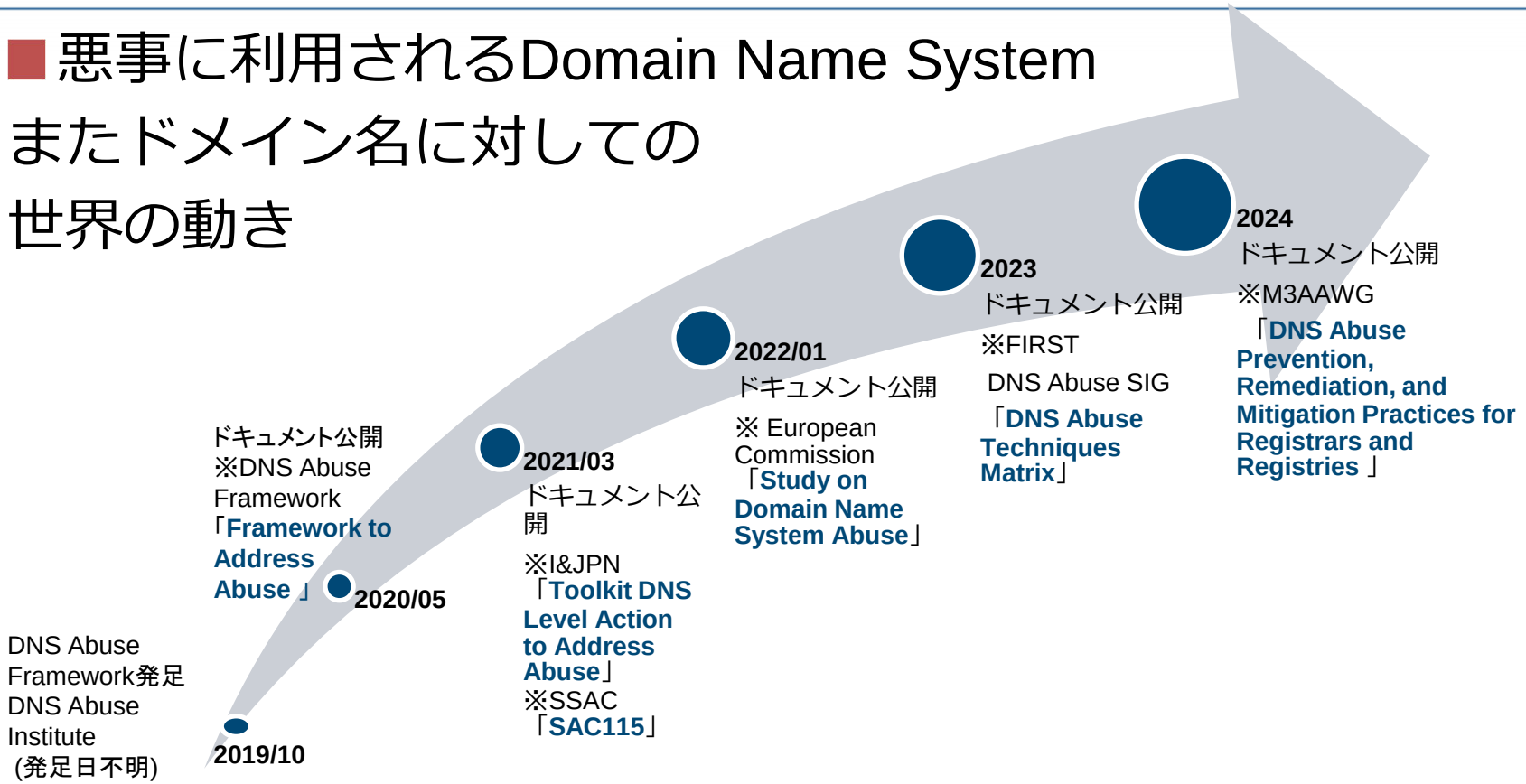
Microsoft ：Microsoft Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files

フィッシングサイトに使われたセカンドレベルドメイン名数の推移



世界の動向

■悪事に利用されるDomain Name System またドメイン名に対しての 世界の動き



ICANN Advisory: Compliance With DNS Abuse Obligations

Background

The ICANN organization contracts with registries to operate gTLDs through an RA. The RA specifies the responsibilities of the registry operator, which include maintaining the authoritative database of all registered domain names in the gTLD and publishing the DNS zone for the gTLD.

ICANN also enters into an RAA with each registrar, which allows the registrar to offer domain name registration services in gTLDs. The RAA outlines the responsibilities of the registrar, such as verifying registrant (or Registered Name Holder) information and maintaining accurate records. The roles and obligations of registrars and registries are distinct and are reflected in their respective agreements, the RAA and the RA.

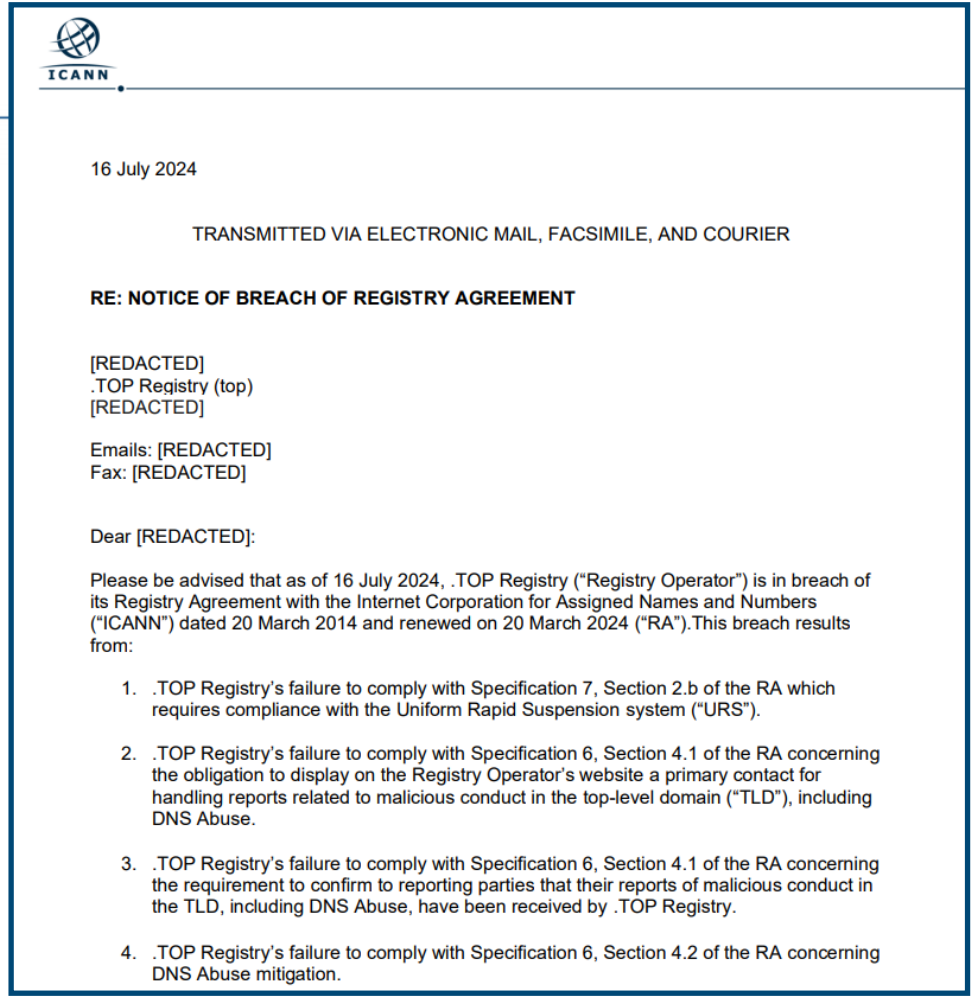
ICANN has the authority to enforce rules related to domain name registration services and domain names as outlined in the RAA and the RA. This Advisory focuses on domain names (or Registered Names) in gTLDs that are used as vehicles or mechanisms for DNS Abuse. The requirements of the DNS Abuse Amendments in the RAA and RA are based on the actions that registrars and registry operators, respectively, can take to minimize the scope and intensity of the harm and victimization caused by DNS Abuse. These requirements also consider that registrars and registry operators represent only a portion of the DNS ecosystem, which is composed of many actors[1]. Depending on the specific circumstances of an instance of DNS Abuse, the most appropriate actor to detect, assess, verify, and stop the abusive activity may vary, and sometimes may be an actor other than a registrar or registry operator.

DNS Abuse

For the purposes of the RAA, the RA, and this Advisory, *DNS Abuse* means malware, botnets, phishing, pharming, and spam (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse) as these terms are defined in Section 2.1 of the Security and Stability Advisory Committee Report on an Interoperable Approach to Addressing Abuse Handling in the DNS (SAC 115[2]):

.top レジストリへの勧告

- 2024年7月 ICANNより .top レジストリに勧告がなされた



ICANN

16 July 2024

TRANSMITTED VIA ELECTRONIC MAIL, FACSIMILE, AND COURIER

RE: NOTICE OF BREACH OF REGISTRY AGREEMENT

[REDACTED]
.TOP Registry (top)
[REDACTED]

Emails: [REDACTED]
Fax: [REDACTED]

Dear [REDACTED]:

Please be advised that as of 16 July 2024, .TOP Registry ("Registry Operator") is in breach of its Registry Agreement with the Internet Corporation for Assigned Names and Numbers ("ICANN") dated 20 March 2014 and renewed on 20 March 2024 ("RA").This breach results from:

1. .TOP Registry's failure to comply with Specification 7, Section 2.b of the RA which requires compliance with the Uniform Rapid Suspension system ("URS").
2. .TOP Registry's failure to comply with Specification 6, Section 4.1 of the RA concerning the obligation to display on the Registry Operator's website a primary contact for handling reports related to malicious conduct in the top-level domain ("TLD"), including DNS Abuse.
3. .TOP Registry's failure to comply with Specification 6, Section 4.1 of the RA concerning the requirement to confirm to reporting parties that their reports of malicious conduct in the TLD, including DNS Abuse, have been received by .TOP Registry.
4. .TOP Registry's failure to comply with Specification 6, Section 4.2 of the RA concerning DNS Abuse mitigation.

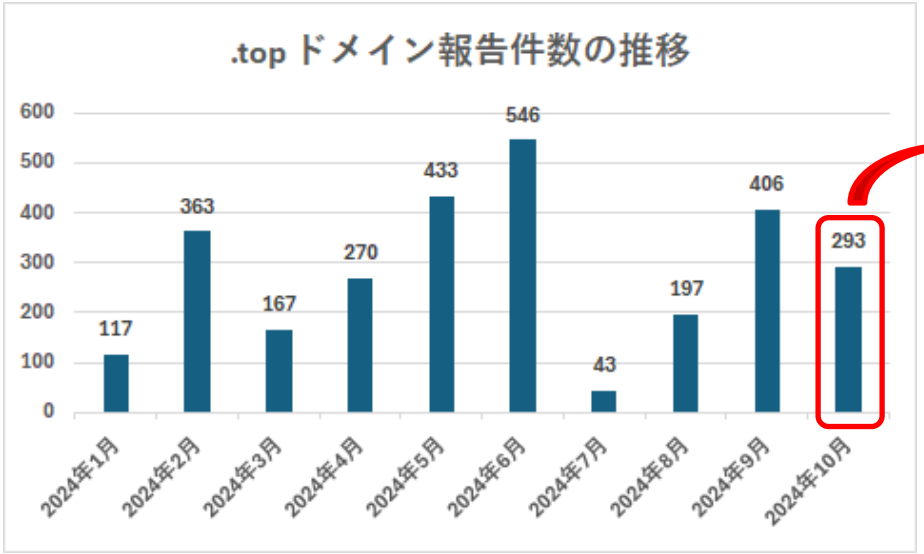
.top レジストリの対応の変化

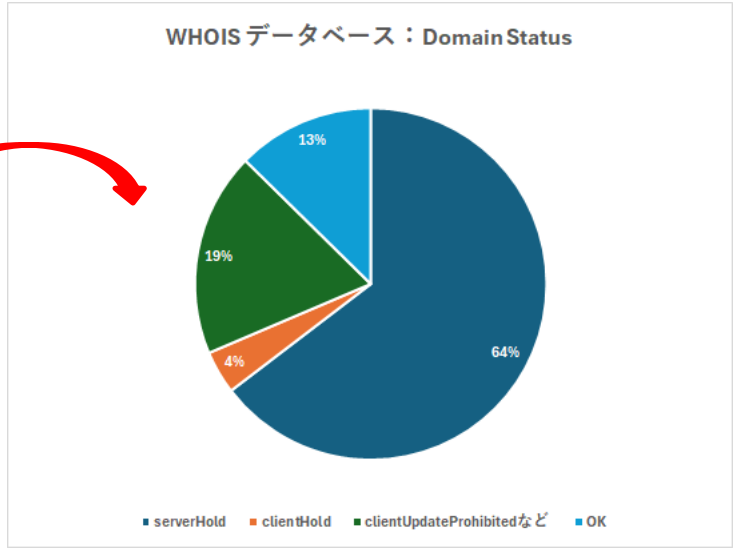
- 2024年9月以降、.top レジストリによる悪意あるドメイン名への対処がされ、ドメイン名無効化が迅速に行われている

対象ドメイン名	報告日	対処日（レジストリから応答のあった日）	WHOIS データベース Domain Status
ddhhgvu.top	9月26日	9月26日	Domain Status: serverHold
tiktokfr.top	10月1日	10月3日	Domain Status: serverHold
sc.efqwd21e.top	10月3日	10月8日	Domain Status: serverHold

.top レジストリの対応の変化

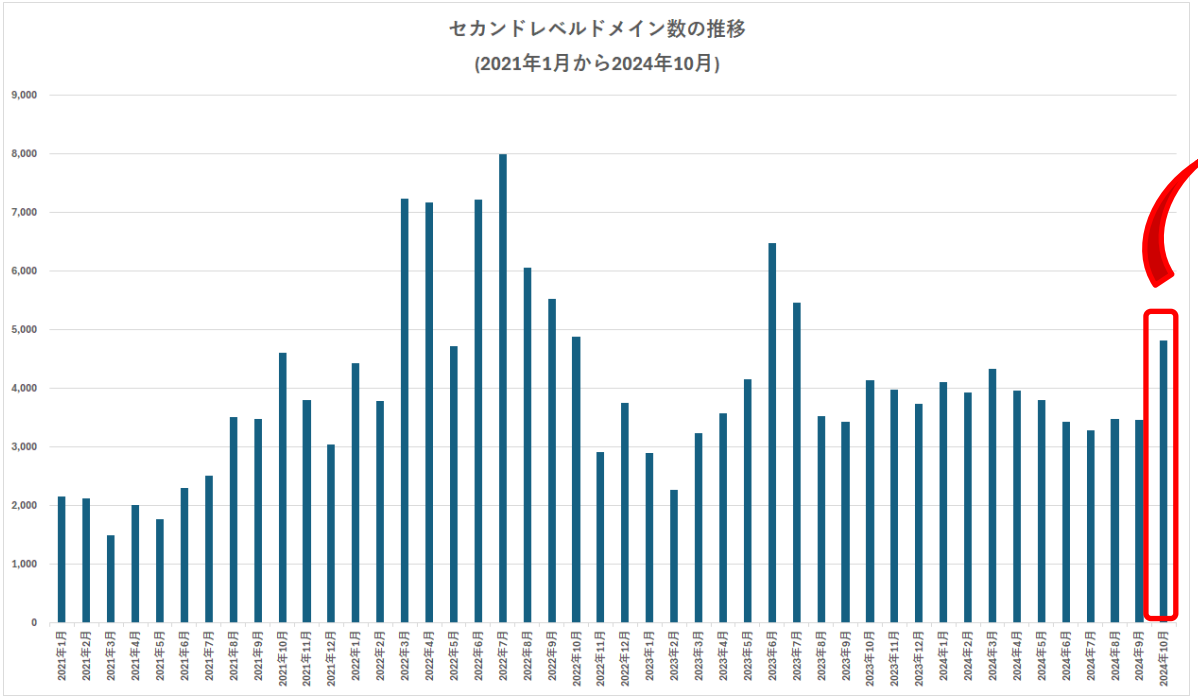
- ICANNより勧告を受けた後の .top の変化
  - 7月以降増加傾向にあったが、10月に観測された .top のDomain Status の状態結果から、87% 無効化またはNXDOMAIN状態を確認（ 11月16日時点のWHOIS結果）

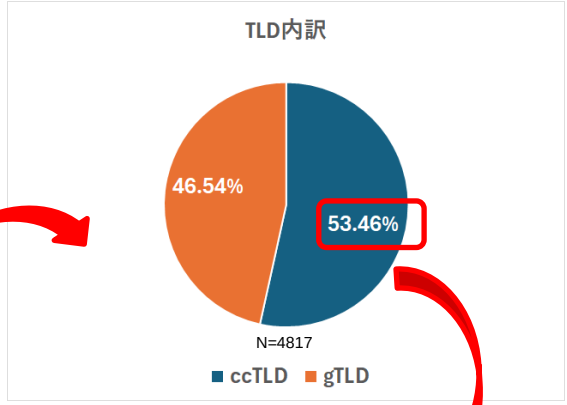


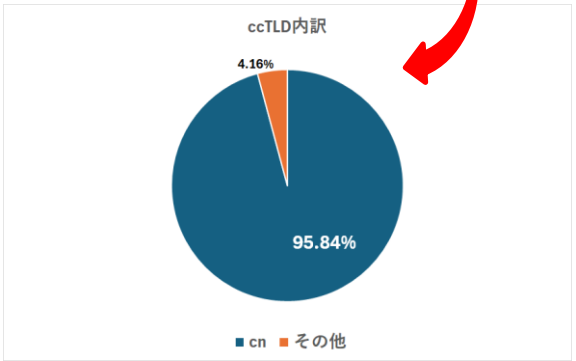


改めてセカンドレベルドメイン名の状況確認

- ICANNによる活発な活動の成果が見られない観測状況を改めて確認
  - gTLDよりccTLDが多いという結果で.cn が大半を占める







悪意あるドメイン名登録に対して

悪意あるドメイン名の登録を抑制することは難しいが、調査結果から、ドメイン名の悪事が確認され次第、各レジストリ、レジストラーにてドメイン名の無効化など対処されている。

課題

・ICANNと契約のない ccTLDによって発生する悪意あるドメイン名の登録

対応策

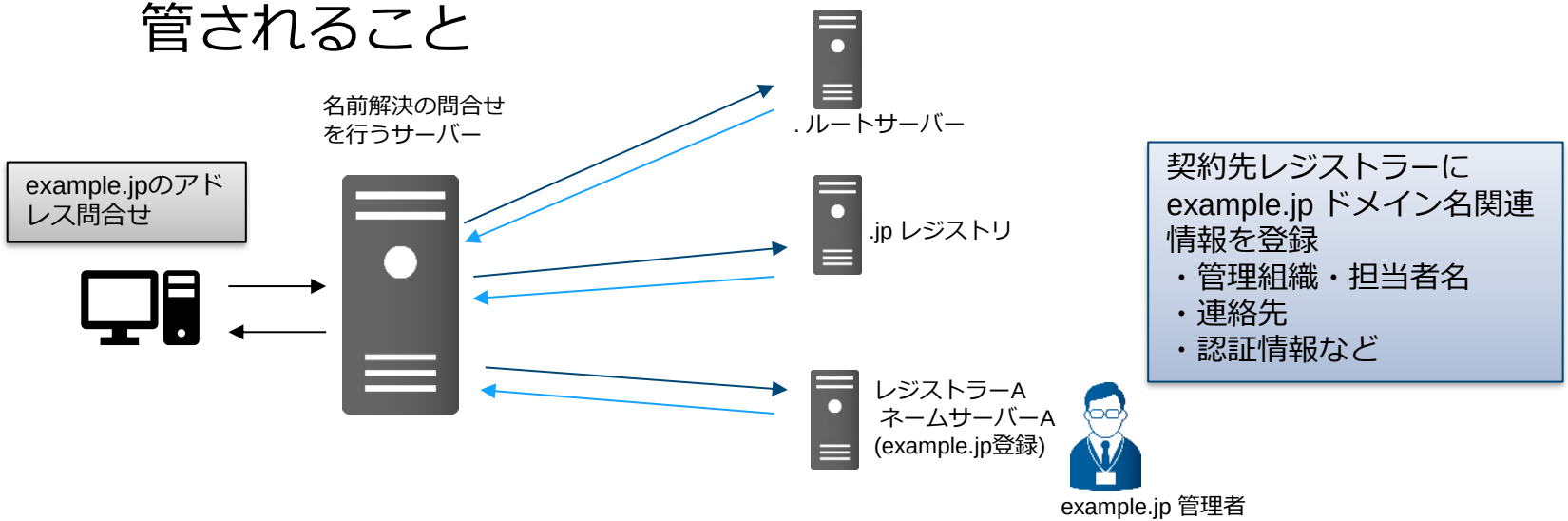
・情報を適切に届け状況改善に活かす
  - ICANNコミュニティやAPTLDコミュニティなど適切な場所への働きかけ

・有効なサービスを活用しレポートを提出
  - Submitting a Complaint to ICANN Contractual Compliance
  - JPCERT/CC へ報告 インシデント対応依頼

ドメイン名の不正移管

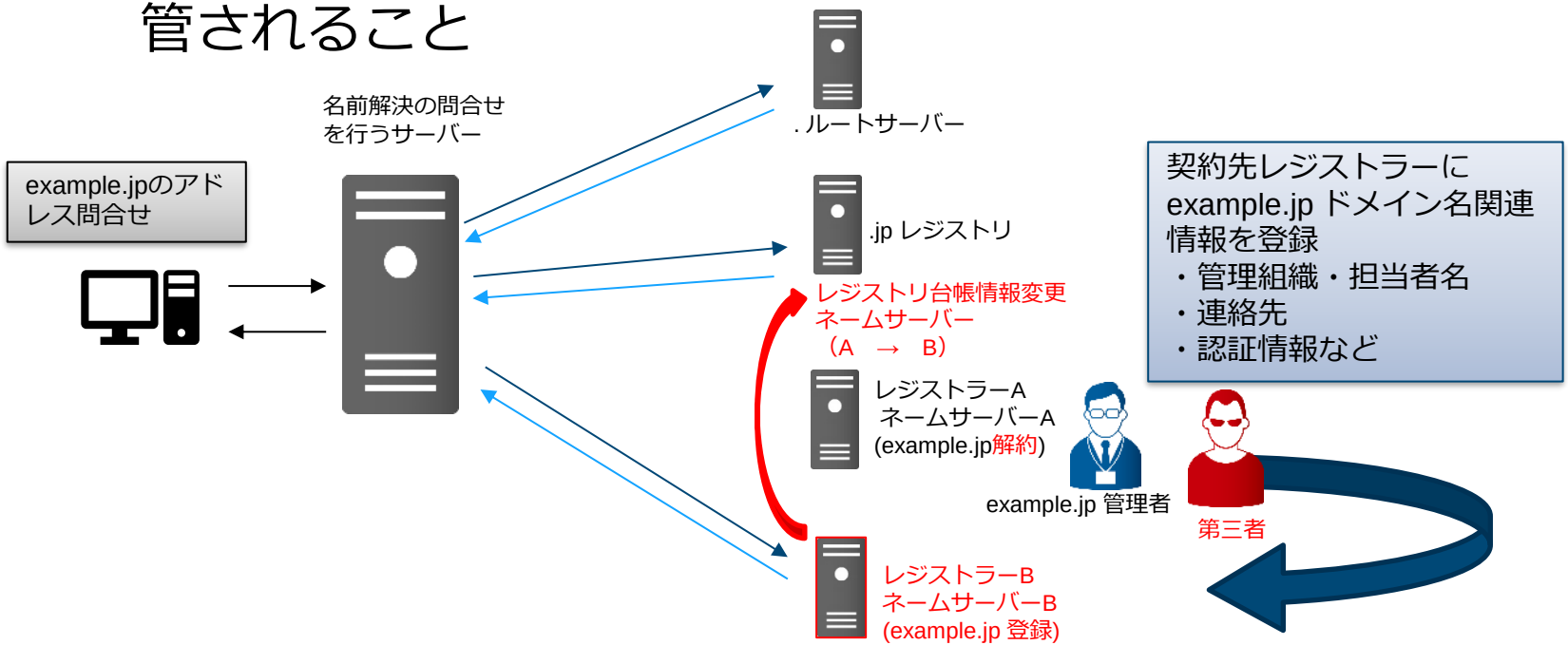
ドメイン名の不正移管

- ドメイン名の不正移管とは
  - ドメイン名が不正に第三者によって別のレジストラーに移管されること



ドメイン名の不正移管

- ドメイン名の不正移管とは
  - ドメイン名が不正に第三者によって別のレジストラーに移管されること



WHOISデータベース上での変化

- 不正移管されたドメイン名の WHOISデータベース上で更新される情報

Domain Name: [redacted]
Registry Domain ID: 2581251559_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2023-08-18T14:34:43Z
Creation Date: 2020-12-28T12:55:56Z
Registry Expiry Date: 2028-12-28T12:55:56Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: BRISTOL.NS.CLOUDFLARE.COM
Name Server: KAI.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-09-08T08:28:28Z <<<

ドメイン名ドロップキャッチとの違い

ドメイン名のドロップキャッチ

・ドメイン名の契約更新をせず契約期限切れとなったドメイン名
・利用期間が終了し手放したドメイン名

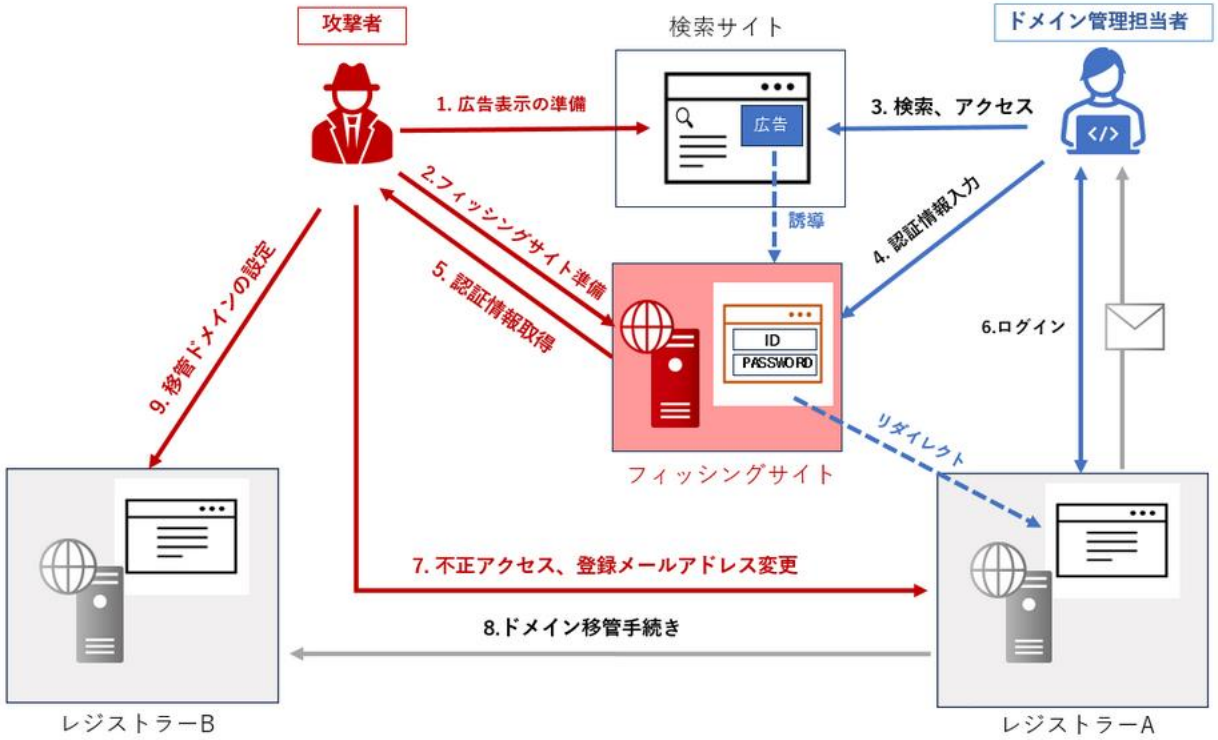
第三者にて、手放されたドメイン名が正当な方法で取得し運用される
→ドロップ後キャッチされたドメイン名

≠

ドメイン名の不正移管

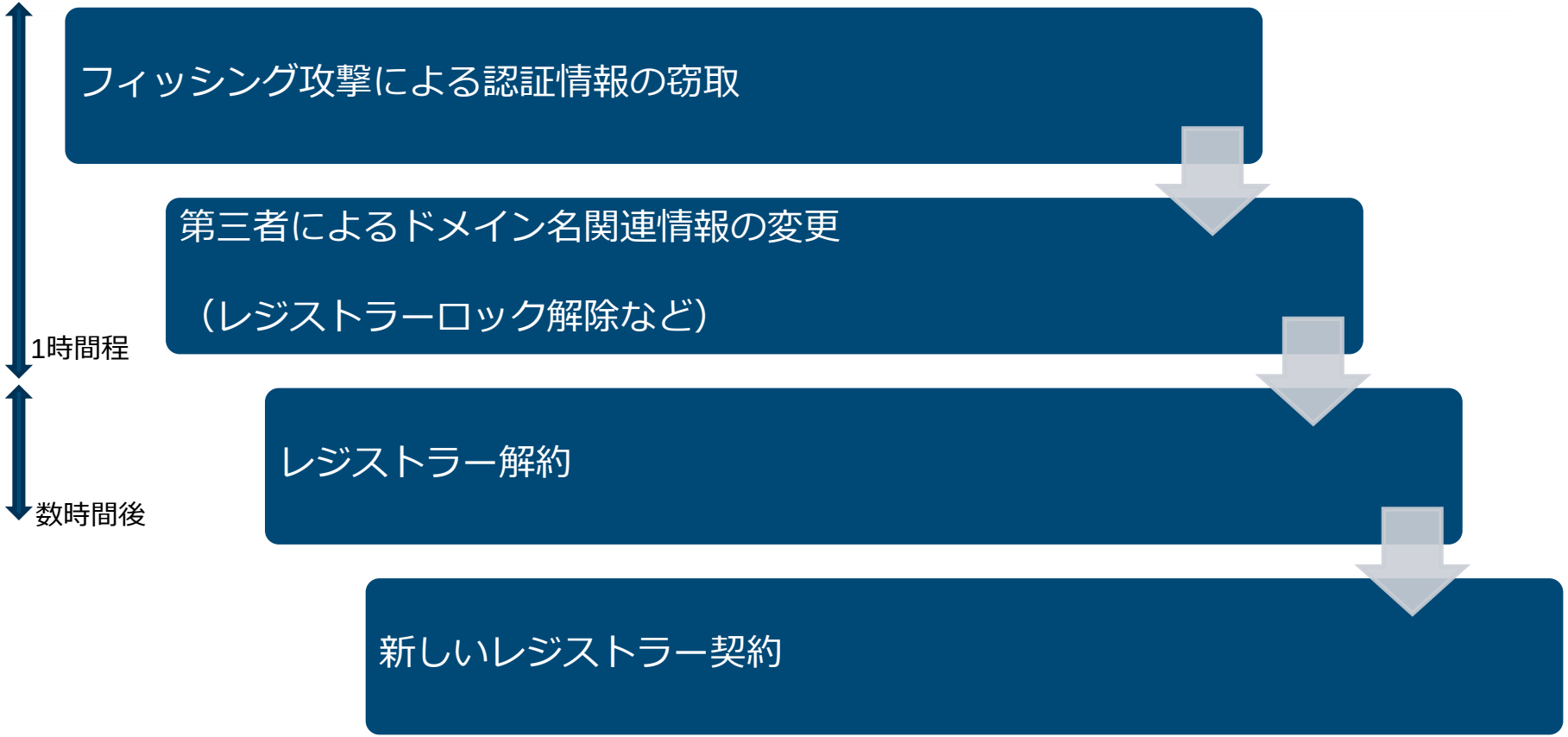
使用期間中のドメイン名が不正に第三者によって別のレジストラーに移管されること

実際の事例



JPCERT/CC Eyes：フィッシングサイト経由の認証情報窃取とドメイン名ハイジャック事件

ドメイン名の不正移管までの流れ



ドメイン名不正移管：未然防止策

レジストラーロック

- レジストラー事業者から提供されるサービス
- ドメイン名情報の不正変更を阻止するサービス
- ドメイン名管理者がレジストラーのサービスを利用

レジストリロック

- レジストリ事業者から提供されるサービス
- ネームサーバー情報変更などに制限を設け不正変更を阻止するサービス
- レジストリごとにサービス形態が異なる

  JPRS：**レジストリロックサービス**

  VERISIGN：**Registry Lock Service**

ドメイン名不正移管：事後対応

Registrar Transfer Dispute Resolution Policy（TDRP)

In any dispute relating to Inter-Registrar domain name transfers, Registrars are encouraged to first of all attempt to resolve the problem among the Registrars involved in the dispute. In cases where this is unsuccessful and where a registrar elects to file a dispute, the following procedures apply. It is very important for Registrars to familiarize themselves with the Transfer Dispute Resolution Policy (TDRP) as described in this document before filing a dispute. Transfer dispute resolution fees can be substantial. It is critical that Registrars fully understand the fees that must be paid, which party is responsible for paying those fees and when and how those fees must be paid.

This version of the TDRP and corresponding procedures will apply to all Complaints filed on or after 1 December 2016.

ドメイン名の不正移管など意図しない移管が発生した際、当該移管に関与するレジストラ―間で問題解決を試みる、それでも解決出来ない場合に、レジストラーが紛争申し立て（TDRP）を行うことができる。

ドメイン名不正移管に対して

ドメイン名を登録運用している事業者やドメイン名管理担当者は、ドメイン名は狙われるということを認識し、当該ドメイン名のインターネット空間での価値を理解する事が重要。その価値に基づいて防御策を講じる必要がある。

防御
・事業者が提供する防御策の利用
（レジストラーロック、レジストリロックなど）

もしもの時に備えて
・事業者が提供するセキュリティ対策を把握する
  - レジストラーロック、レジストリロック適用方法や変更発生時の対応内容など
  - 事業者のTDRPなど利用者保護への対応

・ドメイン名の価値を考慮し、適切な保障を提供するサービスプロバイダーを選択する

ドメイン名ドロップキャッチ

ドメイン名のドロップキャッチとは

ドメイン名のドロップキャッチ

・ドメイン名の契約更新をせず契約期限切れとなったドメイン名
・利用期間が終了し手放したドメイン名

第三者にて、手放されたドメイン名が正当な方法で取得し運用される
→ドロップ後キャッチされたドメイン名

JPCERT/CC に報告されるドメイン名ドロップキャッチ

- JPCERT/CCに相談・報告されるドメイン名のドロップキャッチ事案に対して
  - 不正と判断が出来ないため、関与する事業者への連絡を控える
  - 参考情報として、ドメイン名紛争処理をご案内

JPNIC

ドメイン名紛争処理方針(DRP)

JPRS

JPドメイン名紛争処理方針

海外事例： dotmobiregistry.net

- WHOISサーバーに利用されていたドメイン名のドロップキャッチ事案
  - 対象ドメイン名：dotmobiregistry.net
  - WHOIS サーバー名：whois. dotmobiregistry.net

古いWHOISサーバー情報を利用したままのレジストラーや、WHOIS機能搭載しているWebサイトからの .mobiクエリーを確認（例えば：VirusTotal, GoDaddy)

➡ ハイジャック防止のため、**Shadowserver** にて当該ドメイン名をShinkholeし管理

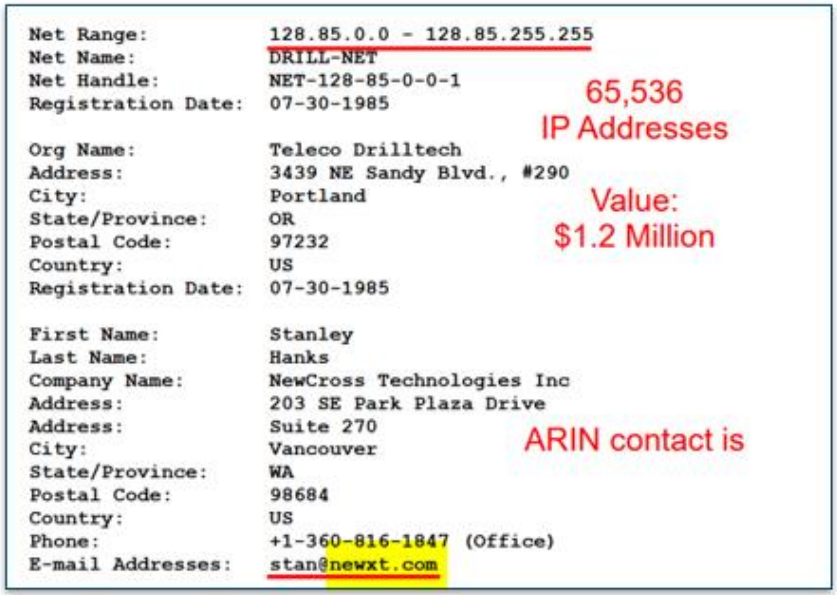
watchTowr Labs: We Spent $20 To Achieve RCE And Accidentally Became The Admins Of .MOBI

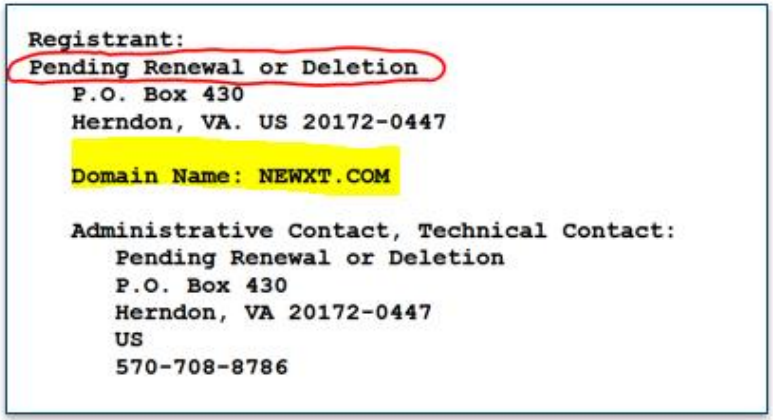
dotmobiregistry.net

```
Domain Name: DOTMOBIREGISTRY.NET
Registry Domain ID: 2906024697_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: http://registrar.amazon.com
Updated Date: 2024-09-10T14:30:28Z
Creation Date: 2024-08-07T01:47:10Z
Registry Expiry Date: 2025-08-07T01:47:10Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: trustandsafety@support.aws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: ok https://icann.org/epp#ok
Name Server: SINKHOLE-00.SHADOWSERVER.ORG
Name Server: SINKHOLE-01.SHADOWSERVER.ORG
Name Server: SINKHOLE-02.SHADOWSERVER.ORG
Name Server: SINKHOLE-03.SHADOWSERVER.ORG
Name Server: SINKHOLE-04.SHADOWSERVER.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-11-17T06:55:31Z <<<
```

海外事例： newxt.com

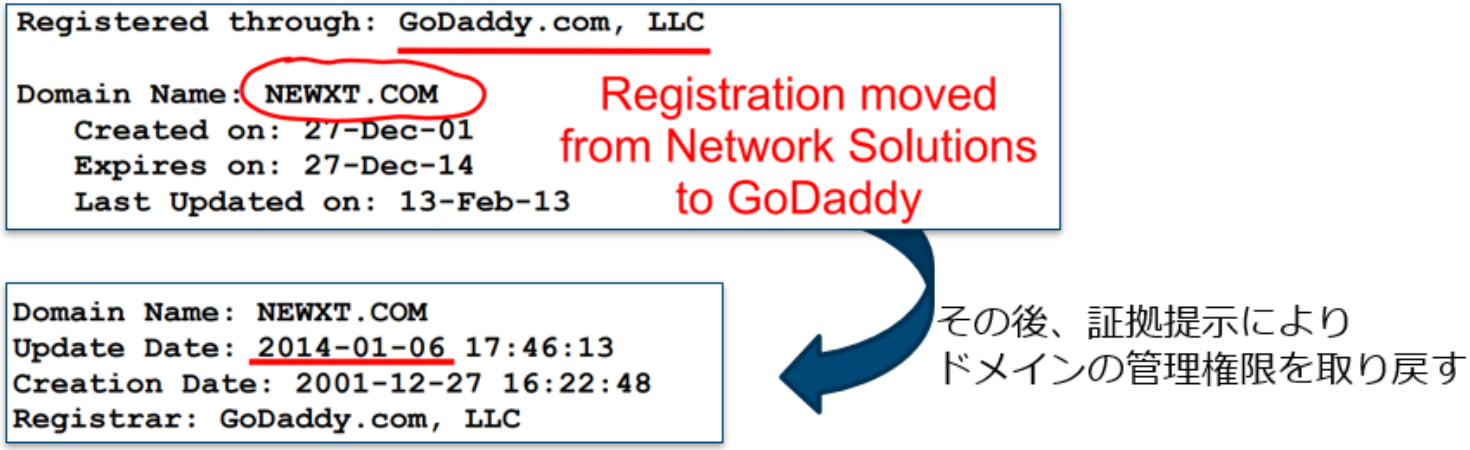
- IP address 128.85.0.0 - 128.85.255.255 の管理者情報として登録されていたEmailアドレスのドメイン名 newxt.com を第三者がオークションで購入し、その後、ARINに対象IPアドレス空間の保有者として接する





Threat InSites Matthew Schneider [Hijacking Hijinks]

その後、GoDaddy に移管

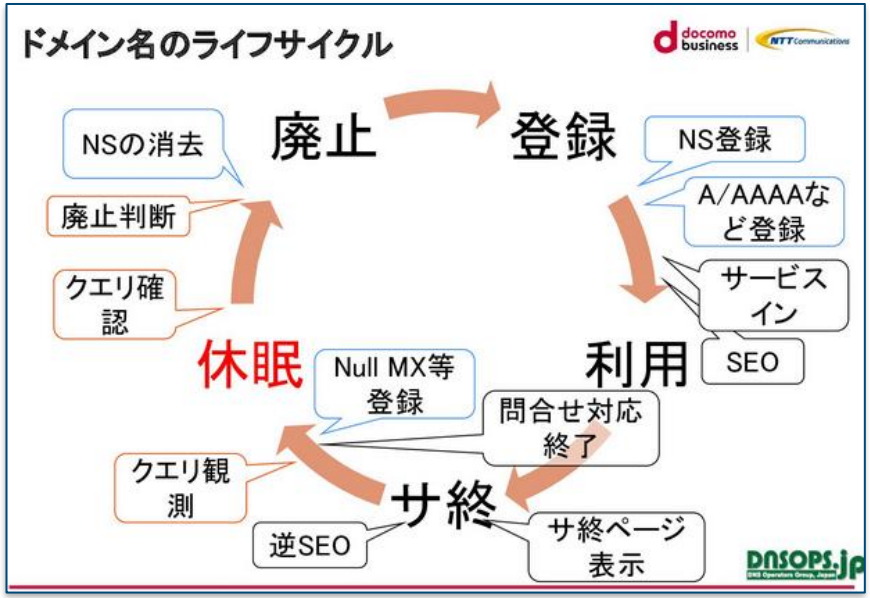


Threat InSites Matthew Schneider [Hijacking Hijinks]

ドメイン名ドロップキャッチに対して

期限切れもしくは手放したドメイン名に関わるインシデントの火消しは、当該ドメイン名の価値があるほどコストや労力を要する。

- 自組織のドメイン名管理体制を再確認し、管理者名簿作成など棚卸しを実施する
  - ドメイン名管理者にて手放して問題のないドメイン名なのか確認
- JPAAWG7th GMでDNSOPS.jpより発表された**ドメイン名ライフサイクル**を参考



ドメイン名の終活について - JPAAWG 7th - - Speaker Deck

さいごに

今日お話した内容

- 悪意あるドメイン名の登録
- ドメイン名の不正移管
- ドメイン名ドロップキャッチ

ドメイン名に関わる事案の状況把握、今後の対策または被害に遭った際の対処の参考としていただけたら幸いです。

ご清聴ありがとうございました