

C25 最速低コストな テイクダウンリクエスト送受の 最新動向

2025/7/3 Internet Week ショーケース in 奈良

SPAM, フィッシング、不正アクセス、DDoS, あるいは誹謗中傷、権利を侵害する、違法な、詐欺のコンテンツ。

インターネットはもはや誰もが異常（abuse）を目にする場所です。秩序を保つためには、異常に相応するだけの「止めて！」つまりテイクダウンリクエストを、素早く、大量に、送り、受ける仕組みが必要です。

この必要に対し2024年現在どの程度、実践に耐える技術的な整理がされているか、リクエストを送る側と受ける側それぞれがどのくらいまで試行や整理が進んでいるか、今、どのくらいまでできているか、先進事例と実装法を紹介します。

登壇者紹介・諸注意・プログラム進行のご案内

Internet Week 2024 のC11プログラムからポイントを抜き出してお話します。
IW2024の小高さんのご講演資料は、山下にて代読させていただきます。

小高照正（おだか・てるまさ）

一般社団法人
日本サイバー犯罪対策センター(JC3)所属

- SNSへの投稿拡散ぜひおねがいします！
- ノウハウと事例の情報提供がテーマです。
「必ずうまくいく」完成形ではない点ご了承ください。

山下健一（やました・けんいち）

さくらインターネット株式会社所属
データセンター勤務、仮想化サービスの運用・開発を経て、2016年頃よりabuse窓口の対応に従事

本プログラムは3パート構成です。

1. 標準的なテイクダウンリクエスト送信法の復習（10分）
2. フィッシングサイト撲滅チャレンジカップの結果等について（15分）
3. リクエスト送受自動化の要素技術（30分）

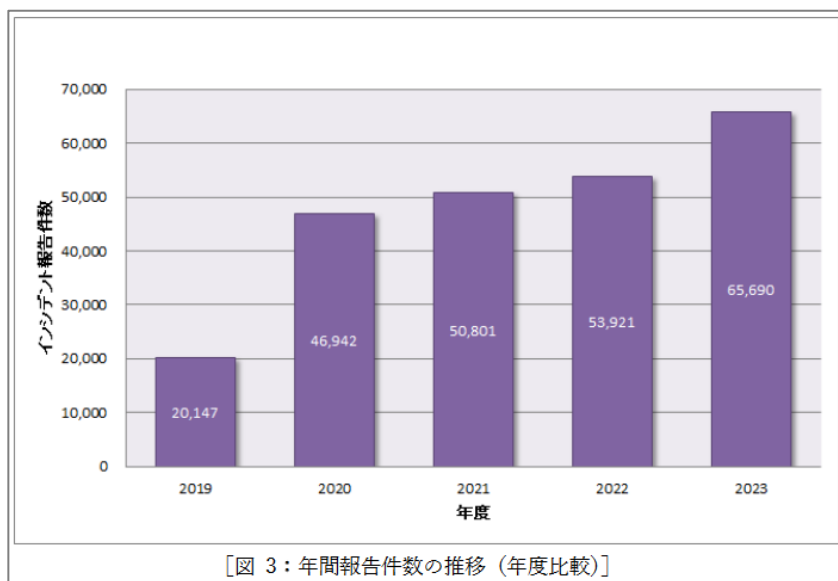
標準的なテイクダウン、削除の リクエスト送信法の復習

2025/7/3 Internet Week ショーケース in 奈良
C25 最速低コストなテイクダウンリクエスト送受の最新動向

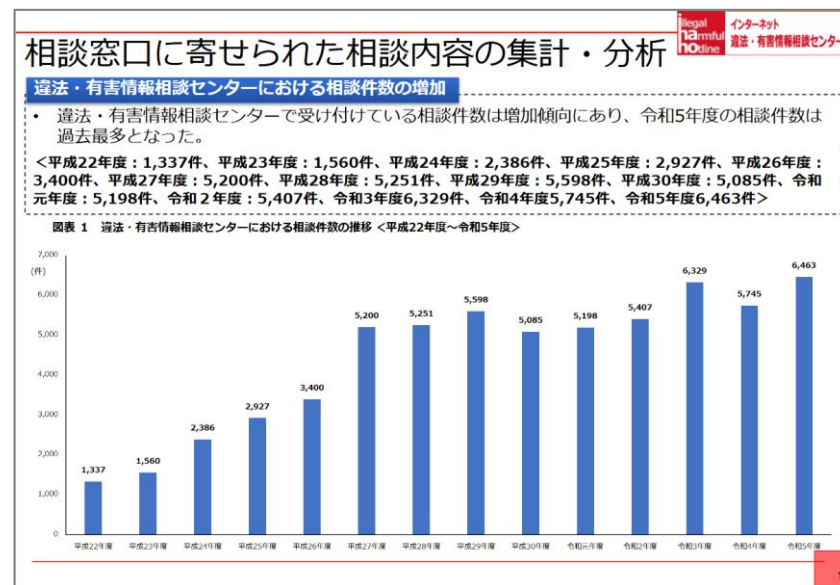
さくらインターネット株式会社 山下健一

インターネットで起こっている問題

JPCERT コーディネーションセンター
「JPCERT/CC インシデント報告対応レポート
2024年1月1日～2024年3月31日」より
<https://www.jpccert.or.jp/ir/report.html>



総務省
「令和5年度インターネット上の違法・有害情報対応
相談業務等請負業務報告書（概要版）」より
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/ihoyugai_02.html



改めて言うまでも無く、数が増加しています。
情報通信研究機構の「NICTER観測レポート」、フィッシング対策協議会の「月次報告書」、定性的情報だと情報処理推進機構の「情報セキュリティ10大脅威」、総じて同じ傾向ではないでしょうか。

インターネットで起きている問題

話を単純化するために

プラットフォーム（SNS, 動画共有, ECモール, デジタル配信サービス, 会員制サービス）を除きますが…

フィッシングサイト

フィッシングメール

EC詐欺サイト

Brute Force Attack

UDP Amp DRDoS

Botnet, C2

改ざんサイト
(SEOスパム・リダイレクター)

改ざんサイト
(Hacked by XXX, 示威声明)

ウェブシェル

マルウェア
ダウンローダー

通信中継
不正送金・クレカ悪用
ランサムウェア含む

違法薬物・大麻・LSD

死体・凄惨な画像

サポート詐欺

自画撮り・セルフィー

リベンジポルノ

CSAM
(1号児童ポルノ)

名指した誹謗中傷

氏名や所属の暴露

過去の写真

過去の逮捕情報

偽ブランド品

マンガ・動画の海賊版

P2Pファイル交換

「こんなものがあるよなあ」と、ささっと振り返ってみました。
(ない方が良くはありますが) 目にしたことありますか？
もしなければ、それは誰かが消してくれているのです。

[Internet Week 2023 O6 Abuse対応の理論と実践 ～abuse対応はじめての1歩～
abuse事象のマインドマップ](#)

「インターネットにおけるabuse」 RFC2142の定義

abuseとは「公共における不適当なふるまい」の連絡先

JPNIC公開文書ライブラリ > 翻訳文書一覧

RFC2142 「一般的なサービス、役割、機能に対するメールボックス名」

<https://www.nic.ad.jp/ja/translation/rfc/2142.html>

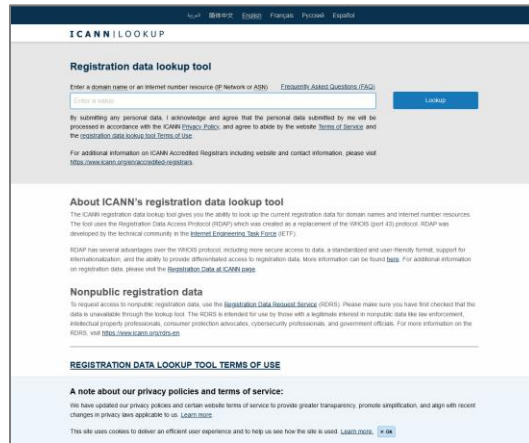
語源から確認するとイメージしやすいです。
IW2023 [06「abuse対応の理論と実践」資料](#)も
ご覧ください。

abuseがあった時、「止めて」は誰に言えば止めてもらえる？

abuseの連絡先窓口はどこにある？

abuse連絡先は、「ドメイン名」「AS番号」「IPアドレス」の
3つのインターネット資源にあります。

abuse連絡先を探す方法



ICANN LOOKUP

<https://lookup.icann.org/>



JPNIC WHOIS Gateway

<https://www.nic.ad.jp/ja/whois/ja-gateway.html>

1. 得ている情報がホスト名 (URL) の場合、host コマンドや dig コマンド等でIPアドレスを解決し、
2. whoisコマンドやwhoisゲートウェイでIPアドレスを検索し、
3. Abuse や、“Abuse Contact” の文言を探します。

なるべくならば

インターネットレジストリのwhoisゲートウェイを使います。

abuse連絡先の調査はコマンドを多用します。Windowsを使用している場合は、WSLを使用してLinuxをインストールすると良いです。

権威のない（レジストリ公式でない）whoisは基本的にはお勧めしません。

でも、使えるものは何でも使うことも正しいです。

whoisは、詳しく話すと沼です。

沼の話はあとでします。

一旦、「abuse連絡先はwhoisで調べることができる」という事にして話を続けます。



Microsoft Learn

WSL を使用して Windows に Linux をインストールする方法

<https://learn.microsoft.com/ja-jp/windows/wsl/install>

問題を連絡する代表的なフォーマット

フィッシングサイトの場合

To whom it may concern,

[簡潔な企業プロフィール].

The website is located at the following address:

<当該フィッシングサイトの URI>

For your information, the fraudulent website appears to be a forgery of this legitimate website:

<正規サイトの URL>

Please take all necessary measures to suspend services of this fraudulent site.

We highly appreciate your cooperation on this matter.

Thank you very much. Sincerely,

--
[担当者、送信者の名前]

[担当者、送信者の所属部署]

[企業名]

[国際電話番号]

[担当者、送信者のメールアドレス]



フィッシング対策協議会
事業者向けフィッシング対策ガイドライン
<https://www.antiphishing.jp/report/guideline/>

+ どんなabuseか識別が容易な件名を付ける
+ サイト・サーバーのIPアドレスを併記する

著作権侵害コンテンツの場合

To “●●●●●●(対象ウェブサイトのURL)”

Notification of Copyright Infringement

On behalf of “●●●●●●(権利者名)”, I notify you of infringement of copyright on “●●●●●●(対象ウェブサイト名)” and request you to remove, or disable access to, the material uploaded on the above web site as follows.

1. Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site:

- “□□□(作品名)”
- “□□□(作品名)”

2. Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material:

—file uploaded on

- URL : http://www.***.com/**** “△△△△(ファイル名)”
- URL : http://www.***.com/**** “△△△△(ファイル名)”

3. The address, telephone number or email address of the complaining party:

- ●●●●●●住所●●●●●●
- ●●●●●●電話番号●●●●●●
- ●●●●●●FAX番号●●●●●●
- ●●●●●●メールアドレス●●●●●●

4. I have a good-faith belief that use of the material on the site is not authorized by the copyright owner.

5. I state that the information in this notification is true and correct, under penalty of perjury, that I am authorized to act on behalf of the copyright owner, and that the information is not false or misleading.

Best regards,

●●●●●● (担当者)



文化庁

初めての「削除要請」ガイドブック、削除要請の参考書式

https://www.bunka.go.jp/seisaku/chosakuken/kaizoku/singai_guide.html

(余談) 文化庁「ぶんかる」のキャラクター「ぶんちゃん」がとてもかわいいです。

JC3小高さん
ご発表パートの代読

フィッシングサイト撲滅チャレンジカップ の結果等について

令和7年7月

一般財団法人 日本サイバー犯罪対策センター (JC3)

法人名

- 一般財団法人 日本サイバー犯罪対策センター（Japan Cybercrime Control Center）
- 平成26年11月13日、業務開始（2014/11/13） 祝10周年！

設立目的

- サイバー空間全体を俯瞰し、産学官それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、サイバー空間の脅威を特定、軽減及び無効化するための活動に貢献する。

事業内容

- サイバー空間の脅威に関する情報の集約・分析
- サイバーに関する研究・人材育成 ■ 国際連携



分野（産業等）横断的な
組織間連携

特定の産業だけでなく分野横断的に連携を行うことで、サイバー空間全体の脅威を俯瞰することを目指す



“Face to Face”の関係の重視

NDA（秘密保持契約）を締結して情報共有を行い、また、直接対面して「信頼関係」を構築することにより、情報を適切に保全（＝情報の提供を促進）



法執行機関（警察）の参画

法執行機関にもその権限を活用してもらい、判明してこなかった脅威の実態解明や無効化・無害化を目指す



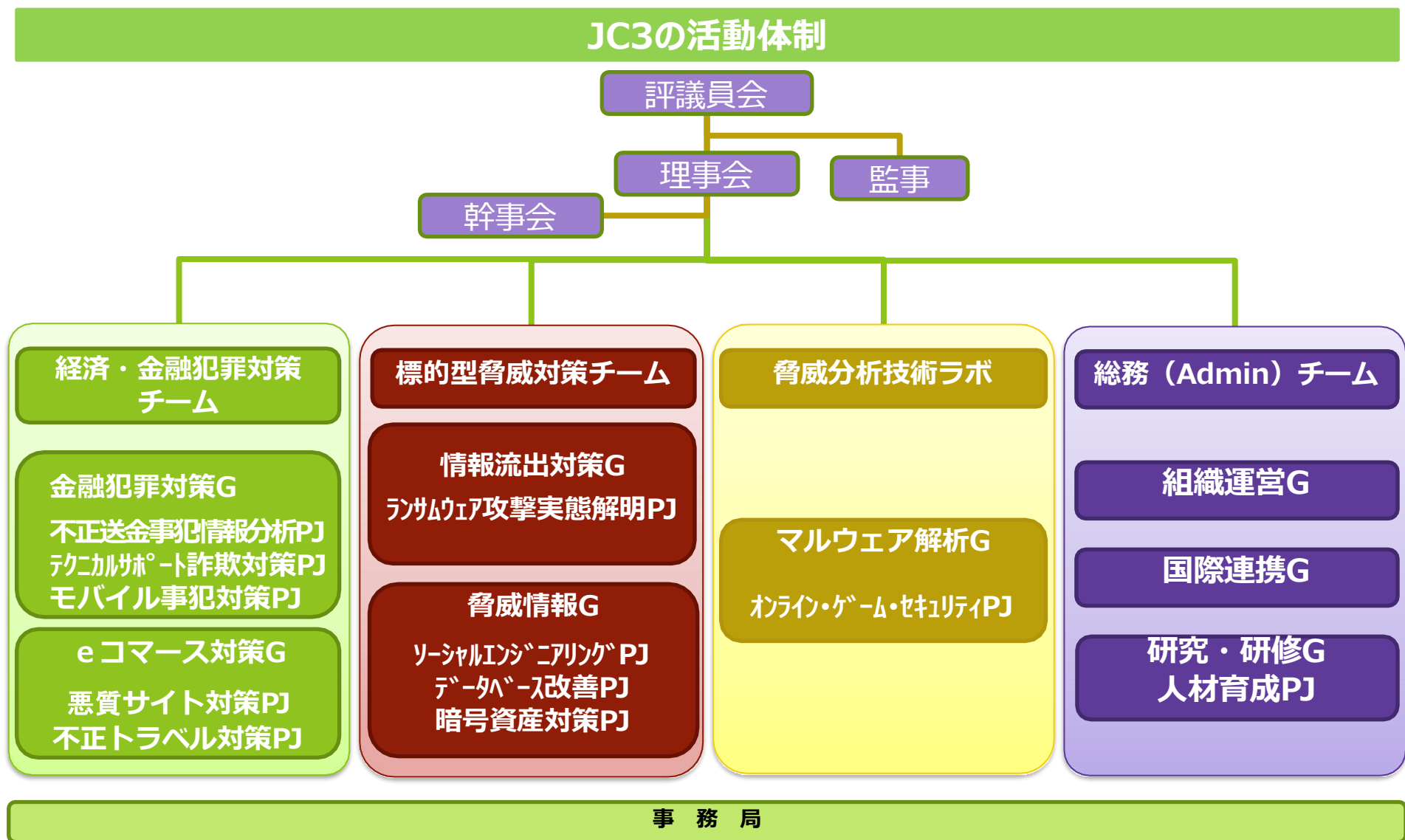
サイバー空間の脅威に関する事象の全貌を把握し、その大本に対処することが可能に

JC3のスキーム



所在地
千代田区神田小川町

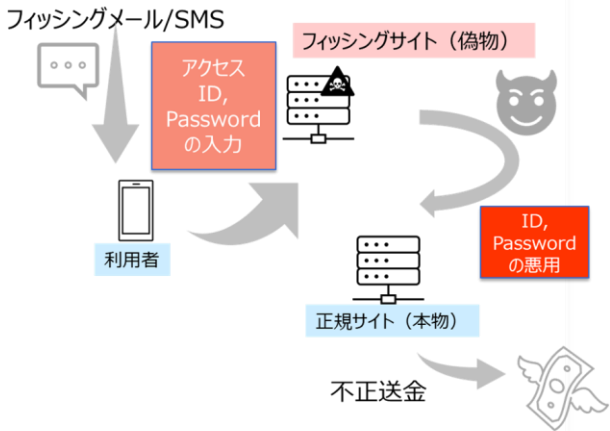




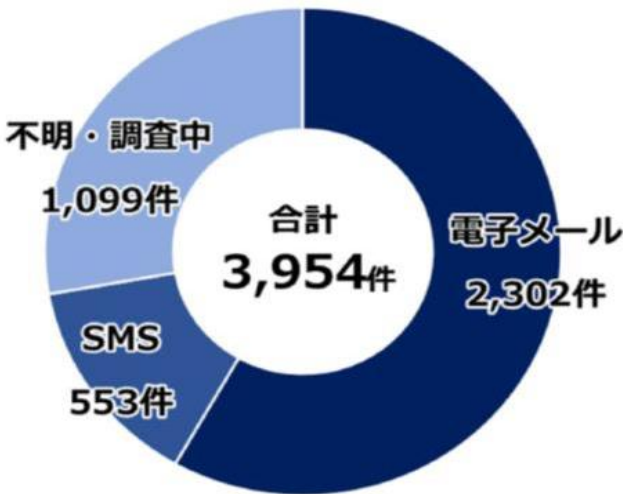
サイバー犯罪の起点となるフィッシングによる被害

貴方の個人情報狙われている！

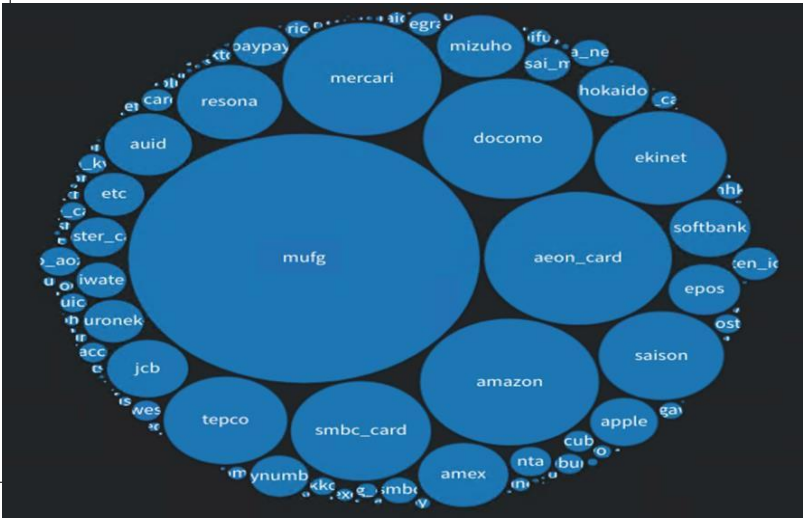
■ フィッシング(Phishing)による情報の窃取



不正送金のためのフィッシングサイトへ誘導する手段の割合



フィッシングサイトのターゲット一覧 (2024年 JC3調べ)



フィッシング報告件数

引用元：フィッシング対策協議会

過去最多の
年間170万件に！



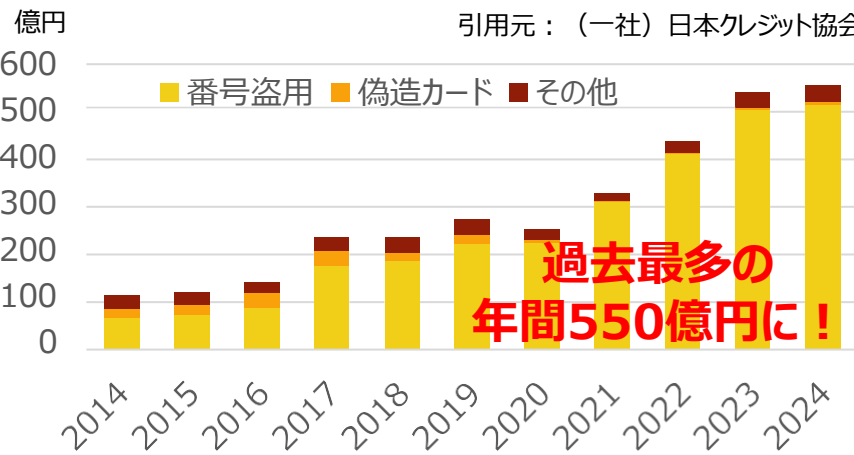
インターネットバンキングに係る不正送金



引用元：令和6年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）ほか

クレジットカード不正利用被害額

引用元：（一社）日本クレジット協会



「国民を詐欺から守るための総合対策」における主な施策 (項目抜粋)

1. 「被害に遭わせない」ための対策

SNS型投資・ロマンス詐欺対策

- 被害発生状況等に応じた効果的な広報・啓発等
- SNS事業者等による実効的な広告審査等の推進
- なりすまし型偽広告の削除等の適正な対応の推進
- 大規模プラットフォーム事業者に対する削除対応の迅速化や運用状況の透明化に係る措置の義務付け等
- 知らない者のアカウントの友だち追加時の実効的な警告表示・同意取得の実施等
- SNSの公式アカウント・マッチングアプリアカウント開設時の本人確認強化
- 新たに開始された金融教育における被害防止に向けた啓発

フィッシング対策

- 送信ドメイン認証技術（DMARC等）への対応促進
- フィッシングサイトの閉鎖促進
- フィッシングサイトの特性を踏まえた先制的な対策

特殊詐欺等対策

- 国際電話の利用休止申請の受付体制の拡充
- SMSの不適正利用対策の推進
- 携帯電話を使用しながらATMを利用する者への注意喚起の推進

2025/4/22 UPDATE!

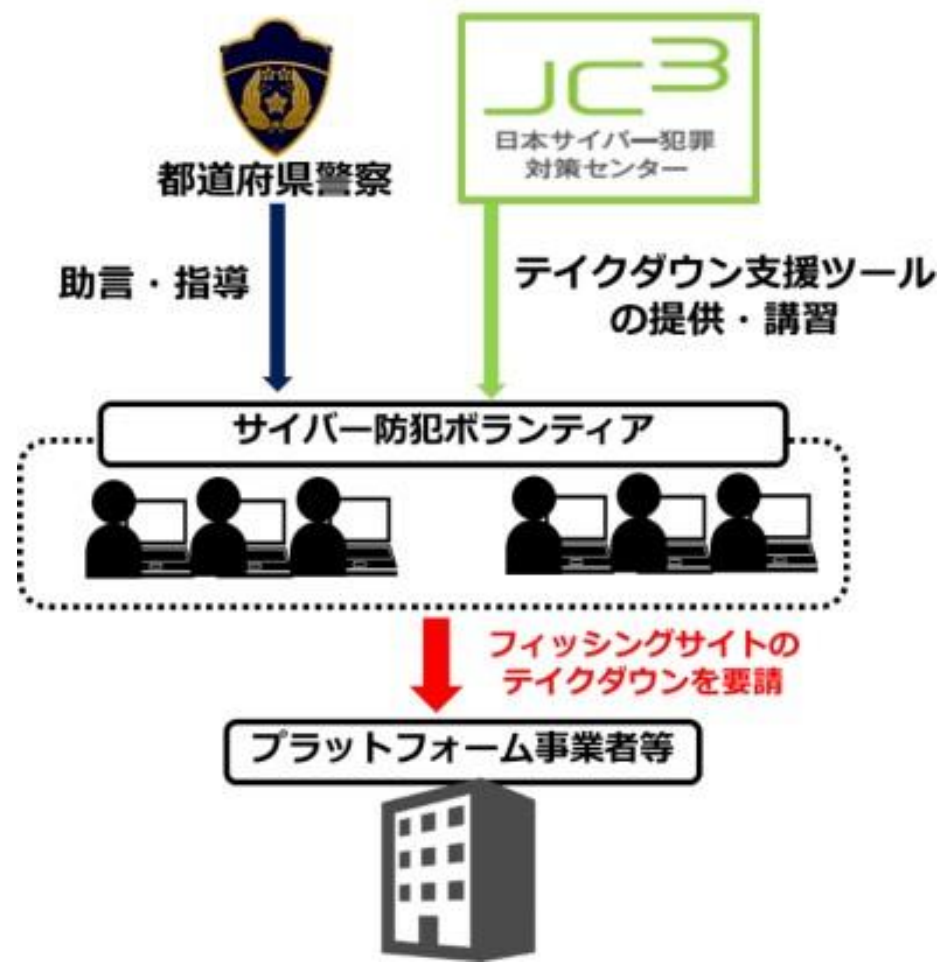
犯罪対策閣僚会議で、「[国民を詐欺から守るための総合対策2.0](#)」が決定されました。
「フィッシングサイトの更なる閉鎖促進」が盛り込まれています！

引用元：警察庁

フィッシング対策への取組紹介（警察庁）

- フィッシングサイトの閲覧防止対策として、各都道府県警察では、サイバー防犯ボランティアの拡大・活性化を図るとともに、**フィッシングサイトのテイクダウンがより効果的に行われるよう各団体へ助言・指導**している。
- 加えて、一般財団法人日本サイバー犯罪対策センター（JC3）では、**専門的な知識を持たない人であってもプラットフォーム事業者等に対してサイトのテイクダウン依頼を行うことができるツールを開発**し、サイバー防犯ボランティア等に提供するとともに、令和6年2月から3月にかけてサイバー防犯ボランティア向けの「**フィッシングサイト撲滅チャレンジカップ**」を実施しており、警察庁はこれを後援している。

【図表 16：サイバー防犯ボランティアへの支援】



引用元：警察庁

テイクダウン支援ツール「プレデター」の改修

■ 漢気仕様



■ かわいい仕様



Predator（プレデター）とは？

「Predator」は、フィッシングサイトをテイクダウンするための支援ツールです。

JC3が運用しているPhishHunter（フィッシングサイト情報収集システム）と連携をしています。

- リストアップされたテイクダウン対象フィッシングサイトを選ぶ
- ↓
- テイクダウンを依頼するドメイン、ホスティング事業者等の決定
- ↓
- abuse通報の作成支援
- ↓
- テイクダウン

テイクダウンのノウハウを共有
作業を一部自動化



Predatorをみんなで使ってフィッシングサイトを撲滅しましょう！

■ 2024年2月13日(火) 14:00～15:00

千代田プラットフォーム(東京都千代田区) + オンライン開催

- ルール説明(採点基準等)
- 特別講演:トレンドマイクロ松ヶ谷新吾氏
- 大幅にアップデートしたプレデターの説明



「第1回フィッシングサイト撲滅チャレンジカップ」

■ 大会概要

- 大会期間：令和6年2月13日～20日（8日間）
- 参加者：125名
 - ・ 都道府県警察 20都道府県警
 - ・ ボランティア団体 27団体参加者

■ 大会結果

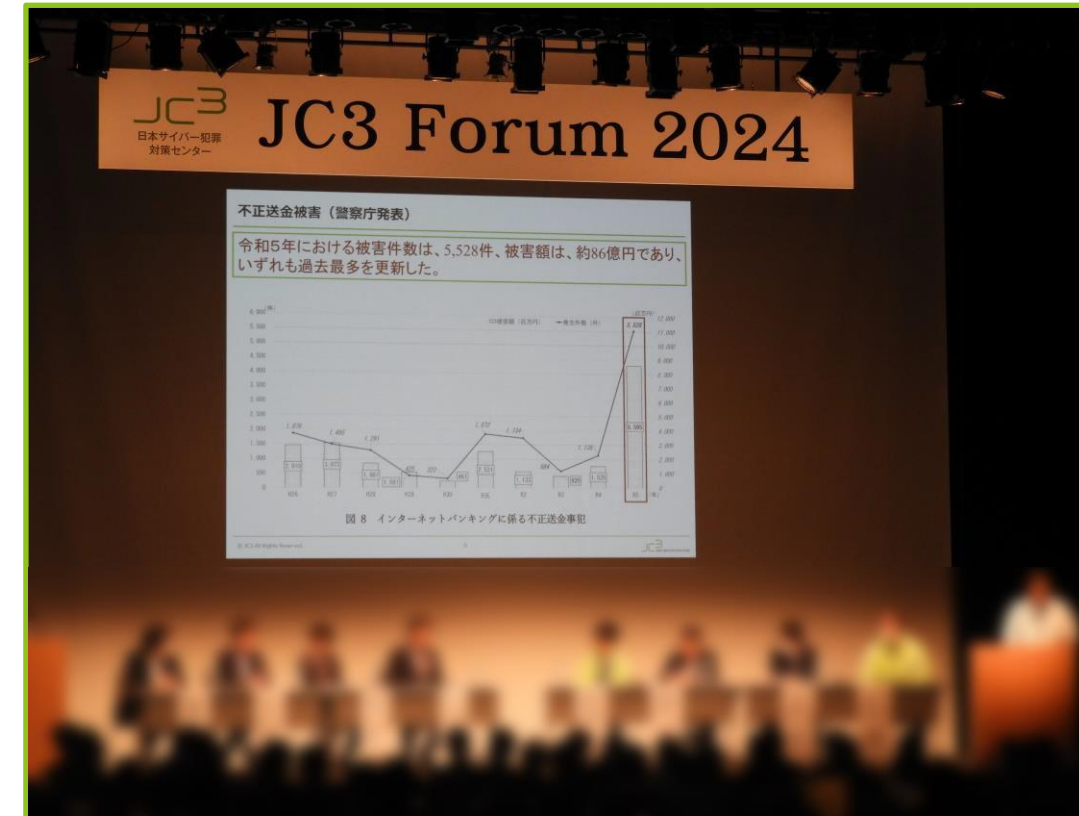
- Abuse報告数：9,319件、テイクダウン数：268件

■ 結果詳細

- ドメイン事業者：Abuse報告数 5,464件、テイクダウン数 264件
- ホスティング事業者：Abuse報告数 3,855件、テイクダウン数 4件
- Google Safe Browsing報告数：2,870件



■ チャレンジカップ表彰式



■ パネルディスカッション

「第2回フィッシングサイト撲滅チャレンジカップ」

■ 目的と概要

ボランティアがJC3とその関係企業、関係機関と一丸となって、短期間で一斉に大量のフィッシングサイトをテイクダウンさせる「フィッシングサイト撲滅チャレンジカップ」を開催

■ abuse報告・フィッシングサイトのテイクダウン数を点数化して競技を実施

■ 団体戦

3人1チームとし、成績優秀団体と取組状況に応じた個人表彰を実施

■ 大会日程

- 開会式：7月22日（月）（オンライン開催）
- 開催期間：7月22日～29日
- 閉会式（表彰式）：8月8日（木）

埼玉県警イベント「SCSCサマーキャンプ2024」と共催



**第2回
フィッシングサイト撲滅
チャレンジカップ**

【開会式】
7/22（月） 11:00～（online）

【開催期間】
7/22（月）～ 7/29（月）
12:00 18:00

【閉会式・表彰式】
8/8（木） 13:30～
（さいたま市大宮区 ソニックスシティビル）
※ 埼玉県警察による啓発イベントを同時開催

【主催】 一般財団法人日本サイバー犯罪対策センター
【後援】 サイバーセキュリティ戦略本部 経済産業省 警察庁
フィッシング対策協議会
特定非営利活動法人日本ネットワークセキュリティ協会
【協力企業】 トレンドマイクロ株式会社
【協賛企業】 株式会社ラック Gftd Japan株式会社 日本電気株式会社
日本マイクロソフト株式会社 LINEヤフー株式会社

「第2回フィッシングサイト撲滅チャレンジカップ」大会結果

■大会概要

- ・開催期間：8日間
7月22日（月）から29日（月）

■参加者

- ・参加者数：359名（前回125名）
- ・都道府県警察：
31都道府県（前回20県）
- ・企業参加（Gftd Works様）
- ・ボランティア団体：
46団体（前回27団体）
- ・チーム数：133チーム

■大会結果

- ・Abuse報告数：12,072件（前回 9,319件）
- ・テイクダウン数：2,201件（前回 268件）

■結果詳細

- ・ドメイン事業者
 - ・Abuse報告数：9,837件（前回 5,464件）
 - ・テイクダウン数：2,004件（前回 264件）
- ・ホスティング事業者
 - ・Abuse報告数：2,235件（前回 3,855件）
 - ・テイクダウン数：197件（前回 4件）

どの程度、フィッシングサイトを撲滅できたか

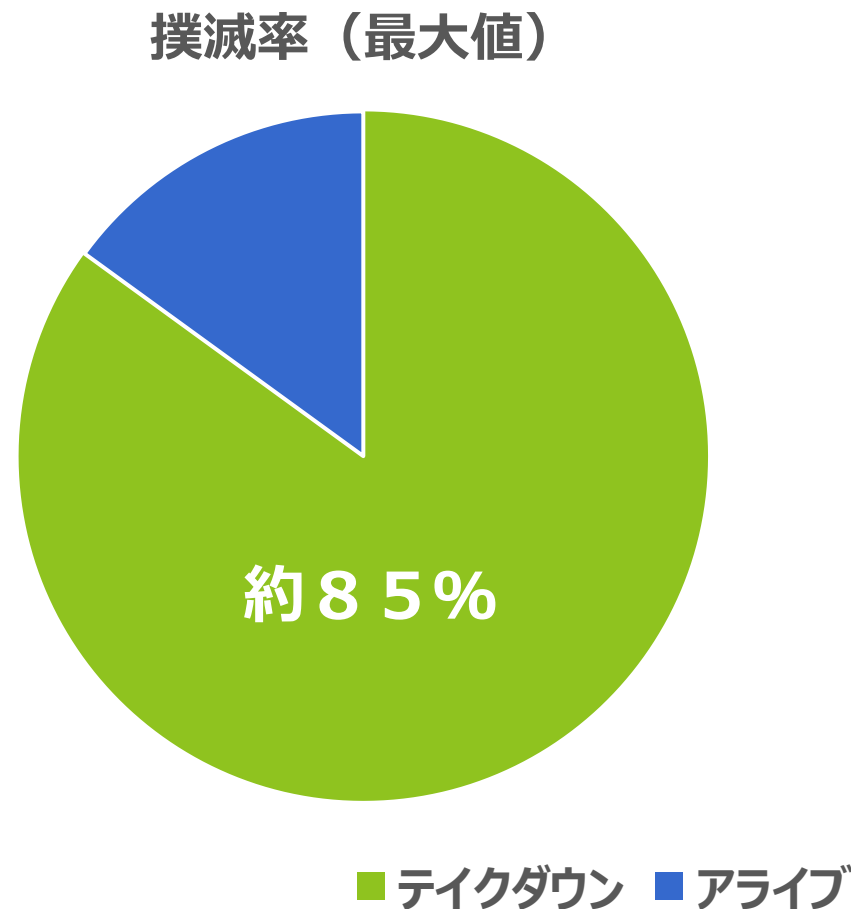
■ テイクダウン率 : **84.6%**

■ 全テイクダウン : **1642件**

- ドメイン重複除く
- ホスティング+レジストラ

■ フィッシング稼働状況 : **1939件**

- 全体 : 3769 Domains
- duckdns : 1835 Domains
- サブドメインを含んだ数
- 7/22-7/29 18:00まで



参加したいと思った方

- フィッシングサイト撲滅運動に参加したい！と思った方は、
まずは、都道府県警察の担当者へ連絡してください！
- みなさんができる範囲で、サイバー防犯活動をしましょう！



身近に潜むサイバー犯罪を予防するために

- サイバー犯罪者は、互いの専門性を共有する独自のエコシステムを**既に完成させています**
- サイバー犯罪者は、今後も我々に対して、様々な違法な手段、方法で攻撃し続けてきます
現代において、サイバー空間と無縁な方はいません！
- 「子供からお年寄りまで」 狙われる際、被害者の**年齢**は関係ありません！
- 「知識や技術がある人、ない人も」 犯罪手口は**多種多様**です！
- 「都会でも地方でも」 サイバー空間に**場所**の制限はありません！
- 「家庭においても仕事中でも」 あなた方の**心の隙間**を突いてきます！
- サイバー犯罪者に対し、一個人、一企業、一組織が**単独で対抗・防御することは、ほぼ無理な時代です**

- ◆ 情報とリソースを持った信頼できる組織の存在
公的機関：自治体、勤務先、学校、警察 etc.
各事業者：サイバーセキュリティ事業者、システム提供事業者、通信事業者等
これらの組織が国民の期待に応える能力を備え、積極的な働きかけをすることが必要
- ◆ リテラシーの強化に向けた取り組み
どのような脅威があるのか、どうしたら自分を守れるか等について、自分自身で問題意識を
リテラシー強化の要素として、社会教育、学校教育の中で提供できる環境づくり
社会全体で、サイバー犯罪を起こさせない環境を整備

テイクダウン、削除の リクエスト送受の実態と 自動化の要素技術

2025/7/3 Internet Week ショーケース in 奈良
C25 最速低コストなテイクダウンリクエスト送受の最新動向

さくらインターネット株式会社 山下健一

連絡すれば止まるのか・実態は…

止めるのは簡単ではありません！

1. 正しい連絡先に連絡できたかわからない、連絡先が無い
1回の操作で連絡先を見つけることができる単純明快かつ
世界共通の方法が無い
2. 要請が受け取られ、正しく理解されたのかわからない
「連絡したい事柄」に合わせたベストプラクティスの
フォーマットは整理されていない
3. いつ止まるのかわからない、
連絡した後どのくらい待つことが普通なのかわからない
いつまで待っても止まらない、連絡先abuse窓口の稼働の問題

正しいabuse連絡先・誰に「止めて」と言うべきか

「名前資源（ドメイン名）」の管理者、
「番号資源（IPアドレス、AS番号）」の管理者

インターネット資源管理者に言う！
……どの資源の？

最適なabuse連絡先はどこか・誰に言うべきか

• IPアドレスの「割当て先」

①基本はココ

でも「割振り」「割当て」…って
一般的に知られているとは到底言えないよね？

• IPアドレスの「割振り先」

②番目はここのはずなんだけど…

• 経路を広報する「AS番号」

AS(ASN), BGP, ネットワークオペレーター

②番目はここが良い、と思う

AS番号？ BGPオペレーターでない人にはほとんど知られていない
IPアドレスからASNを調べられるのは
RIPE/NCC のwhoisだけ…

• ドメイン名の「レジストラ」

ドメイン名そのものを
止めてほしい場合…

• ドメイン名の「レジストリ」

例外だが有効な時もある

• ドメイン名の「権威DNS管理者」

ドメイン名がハイジャックされている時とか…
ドメイン名のリセラーとDNSホスティング事業者が一致していて、不正に登録された異常なドメイン名の停止に成功する場合もあり得る



何故、abuse連絡先はこうも探しにくいのか

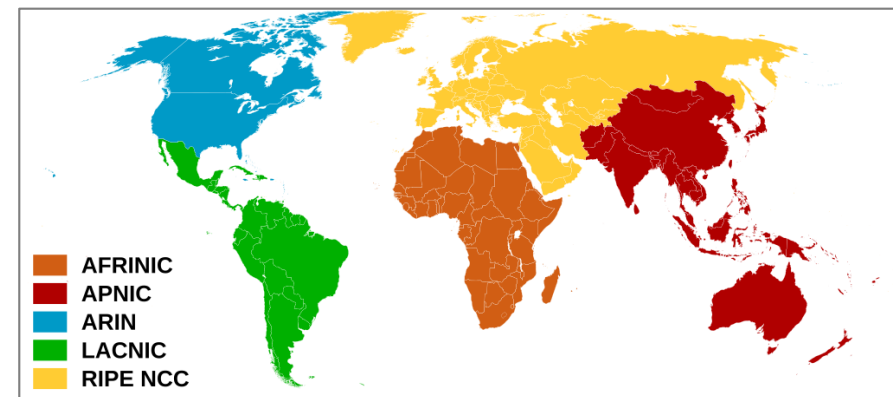
abuse連絡先の探しづらさは、IPアドレスやAS番号の分配の仕組み、ドメイン名の種類やドメイン名登録の仕組み、「インターネット資源管理の仕組み」に由来します。

ICANN, IANA, インターネットレジストリ, RIR, NIR, LIR, ASN, レジストラ, レジストラント, gTLDドメイン, ccTLDドメイン, whois, RDAP, 一気に用語が出てきて、めまいがします。

インターネット資源管理の構造は、素人目にはかなりわかりづらいです。

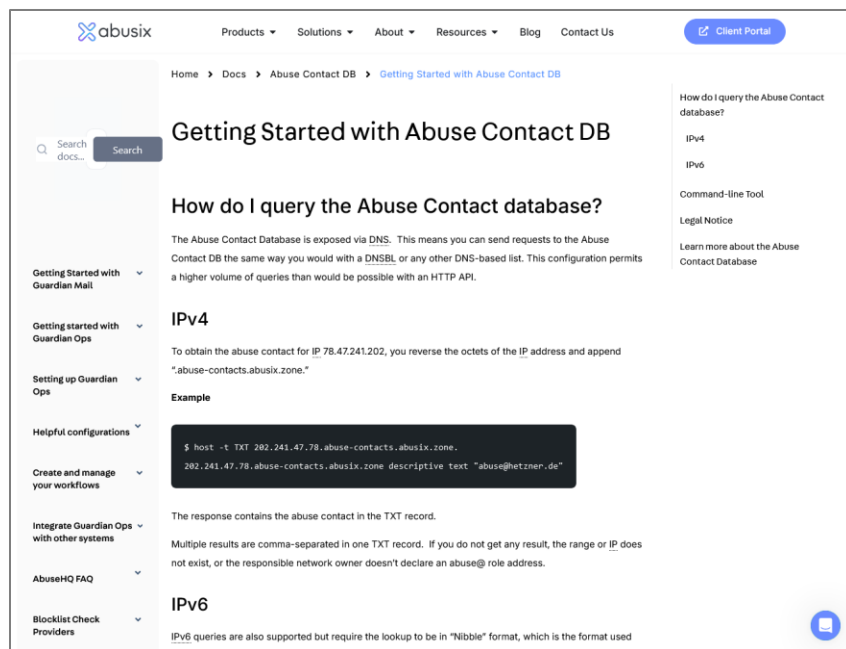
インターネット上でabuseに遭遇し、abuse窓口に連絡したいと考えるのは、言うまでもない事です。ネットワークエンジニアだけではありません。

abuseに遭遇した人に、「資源管理の仕組みを勉強して」と求めるのは無理があります。既に被害に遭っていて、直ちに止めてほしいのだから。abuse連絡先に対するユニバーサルアクセス（非エンジニアを含む）が必要です。



Wikipedia「[地域インターネットレジストリ](#)」

インターネット資源管理の用語や仕組みを知りたい人は、Internet Week Basic オンデマンド「[インターネットの番号資源管理教室 ～ IPアドレス・AS番号の管理について ～](#)」がお勧めです。



「abuse連絡先がわからない」問題へのアプローチ

Abuse Contact DB で abuse連絡先を解決する

abusix.com

Getting Started with Abuse Contact DB

<https://abusix.com/docs/abuse-contact-db/getting-started-abuse-contact-db/>

Getting Started with Abuse Contact DB

Abusix GmbH の Abuse Contact DB を使用して、www.apnic.net のabuse連絡先を調べる

```
$ host www.apnic.net
www.apnic.net is an alias for www.apnic.net.cdn.cloudflare.net.
www.apnic.net.cdn.cloudflare.net has address 104.18.235.68
www.apnic.net.cdn.cloudflare.net has address 104.18.236.68
www.apnic.net.cdn.cloudflare.net has IPv6 address 2606:4700::6812:eb44
www.apnic.net.cdn.cloudflare.net has IPv6 address 2606:4700::6812:ec44

$ dig -t txt 68.235.18.104.abuse-contacts.abusix.zone. +short
"abuse@cloudflare.com"
```

コマンドラインツールが便利、v4アドレスはもちろんv6アドレスを調べる場合に格別便利

```
$ pip install querycontacts
$ querycontacts 2606:4700::6812:eb44
abuse@cloudflare.com
```

Abuse Contact DB が優れる点

単に、abuse連絡先のメールアドレスだけを返してくれる

- RIR(AfriNIC, APNIC, ARIN, LACNIC, RIPE/NCC)それぞれのwhois応答フォーマットの違いを調べて、メールアドレスだけを抜き出す処理が不要になる
- whoisの応答の中から、IPアドレスの割振り・割当てを読み解いて、「どこに連絡すればいいんだ」を考える必要もない

DNSで動作するので、とにかく速い、レートリミットも無い

- whoisは、手で一つ一つ調べる用途であれば、なんら問題ない
プログラムを用いて全自動でwhoisの登録情報を照会しようとするするとTCP通信で速いとは言いきく、そしてレートリミットがあり、自動化された照会には「いつ応答しなくなるか」知れない
- RDAPも同様
- Abuse Contact DB はアカウント登録不要で無料で使うことができ、そしてレートリミットが無い
([ContactDB is a free service, so you don't need to subscribe or create an account to use it!](#))

Abuse Contact DB は whois, RDAP と比べ、圧倒的に
abuse連絡先の解決自動化、abuse宛て連絡送信の自動化に向きます。

Abuse Contact DB を使うには？

Abuse Contact DB の使い方・導入方法

- 使い方は Getting Started with Abuse Contact DB を読む
<https://abusix.com/docs/abuse-contact-db/getting-started-abuse-contact-db/>
- 諸注意が Abuse Contact DB FAQ にあるので読む
<https://abusix.com/docs/abuse-contact-db/abuse-contact-db-faq/>
特に Do I need to provide attribution to the Abuse Contact DB when I use the service? に注意

Abuse Contact DB が回答するabuse連絡先メールアドレスは確かと言えるの？

- Abusix GmbH は、**RIRのwhoisデータベースからメールアドレスを収集している**と説明しています。
<https://abusix.com/docs/abuse-contact-db/abuse-contact-db-overview/>
- Abusix GmbH は、abuse連絡先メールアドレスが有効か検証していると説明しています。
<https://abusix.com/docs/abuse-contact-db/validate-abuse-role-addresses/>

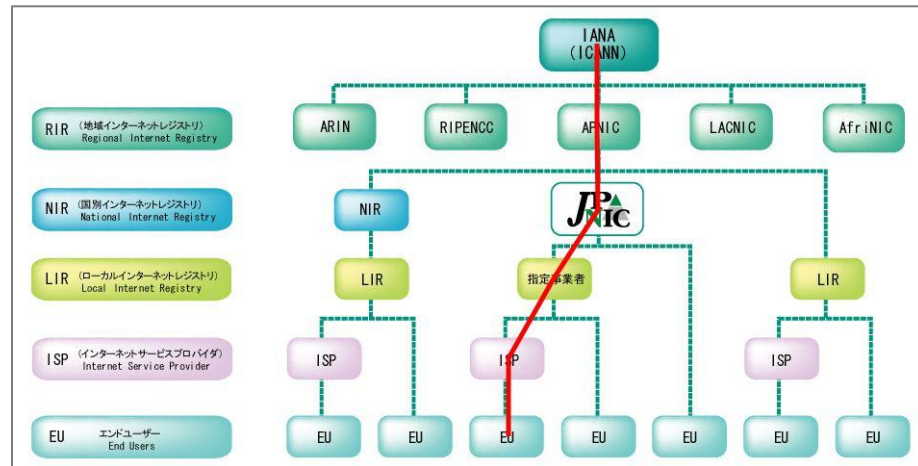
発表者は abusix GmbH の関係者ですか？

Internet Week はベンダーニュートラルのイベントでは？

- Abuse Contact DB は whois, RDAP の問題を、一部とはいえ解決してくれるソリューションです。
- ベンダー依存？ 黒い猫でも白い猫でも鼠を捕るのが良い猫ではないでしょうか。

Abuse Contact DB が解決しない問題

Abuse Contact DB は日本のIPアドレス等、
NIRのwhoisに登録されたabuse連絡先は解決してくれません。



JPNICブログ

「JPNICのような組織（NIR）は他の国にもあるの??」

<https://blog.nic.ad.jp/2022/7172/>

Abusix GmbH は「RIRのwhoisデータベースからメールアドレスを収集している」と言っています。
つまり Abuse Contact DB はNIR, 国別インターネットレジストリのwhoisに登録された連絡先は解決してくれません。

「JPNIC whois を参照してよ」と主張したいですが、JPNIC whois にabuse連絡先は（ほとんど・大半が）登録されていません。
abuse連絡先の登録欄の設置自体、2022年7月、近年のことです。現時点で日本のabuse連絡先は「どこにもない」「見つけれない」に等しいです。

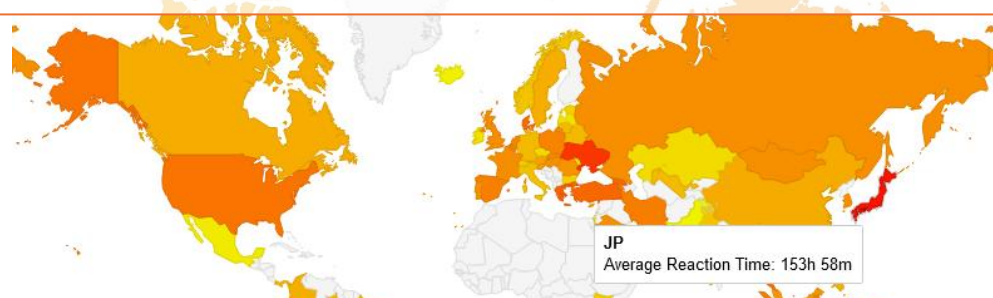
あなたが資源管理者なら – 「abuse連絡先」登録のお願い

(JPNIC) IPアドレス管理業務に関するJPNIC文書施行のお知らせ
～移転手続きにおける申請書の統一およびネットワークの不正利用に対応する窓口(Abuse)の登録開始～

<https://www.nic.ad.jp/ja/topics/2022/20220822-02.html>

外国から見た「日本のabuse連絡先窓口の評価」

abuse.ch “Measuring Reaction Time of Abuse Desks” (2018/10/1)
<https://abuse.ch/blog/measuring-reaction-time-of-abuse-desks/>



It shows that abuse desks in Ukraine (UA), Japan (JP) and Zimbabwe (ZW) tend to be slower than abuse desks located in e.g. Mexico (MX), Iceland (IS) or Pakistan (PK).

「ウクライナ、日本、ジンバブエのabuseデスクは、メキシコ、アイスランド、パキスタンなどにあるabuseデスクよりも時間がかかる傾向があることを示しています。」

「日本のabuse対応は遅い」評価は、諸外国の人々は「RIRのwhois情報までしか見てくれない」「JPNICのwhois情報を見てくれない」為に発生しています。
そして日本のabuse対応は、先進7か国・G7の中でも格段に遅いと評価されています（2023/6/23 JPOPM44「『Abuse窓口』が見つけれられない問題」, [資料](#)・[youtube動画](#)）。

サイバー攻撃・セキュリティインシデントの連絡をくれるのは圧倒的に外国の事業者です。
サイバーセキュリティ向上のためにも、**abuse連絡先を登録し参照可能にする必要**があります。

abuse連絡先はウェブフォームか、メールアドレスか



abuse連絡ウェブフォームの例
<https://abuse.sakura.ad.jp/>

abuse連絡先はメールアドレスが正！（キリッ

- 実際のところ、「ウェブフォームの方が対応はされやすい」しかし、正しい（権威がある）連絡先はメールアドレス
- メールアドレスのabuse連絡先はRFC2142で標準化されている

ウェブフォームの問題は何か

- ウェブフォームのURLは標準化されていない
- ウェブフォームの設計は標準化されていない
- ウェブフォームへの入力は自動化に向かない

どこにあるか
いちいち探せと？

独自の入力項目！
独自のページ遷移！

「ウェブフォームが使いにくい」？ ウェブフォームとはそういうもの

- 「サイトのAレコードが複数ある時に、複数のIPアドレスを入力できない」
- 「侵害された権利を複数主張したい、複数の権利を選択できない」
- 「ログを貼り付けたいが、入力できる文字数が少なすぎる」
- 「要請したい対象が多数ある、フォームからの入力が必要な手間、全ての連絡を一度で済ませたい」
- 「画像等の証拠として提示したいファイルが添付できない」

メールで
連絡しましょう

abuse連絡を受け付けるウェブフォームは何故あるか

ウェブフォームが
ない

- 電話をいただくことになる、聞き取りが大変
「メールで連絡してください」押し問答する
- 話がこじれる、ハラスメントを受ける
プロバイダはあなたのための相談員ではない



ウェブフォームが
ある

- 受け取った連絡の中にURLが無い！ IPアドレスが無い！
「ご意見」、そして何を言っているかわからない連絡が来る！
- 誰でも知ってる巨大SNS宛ての削除請求が何故か弊社に来る！



作りこまれた
ウェブフォームが
ある

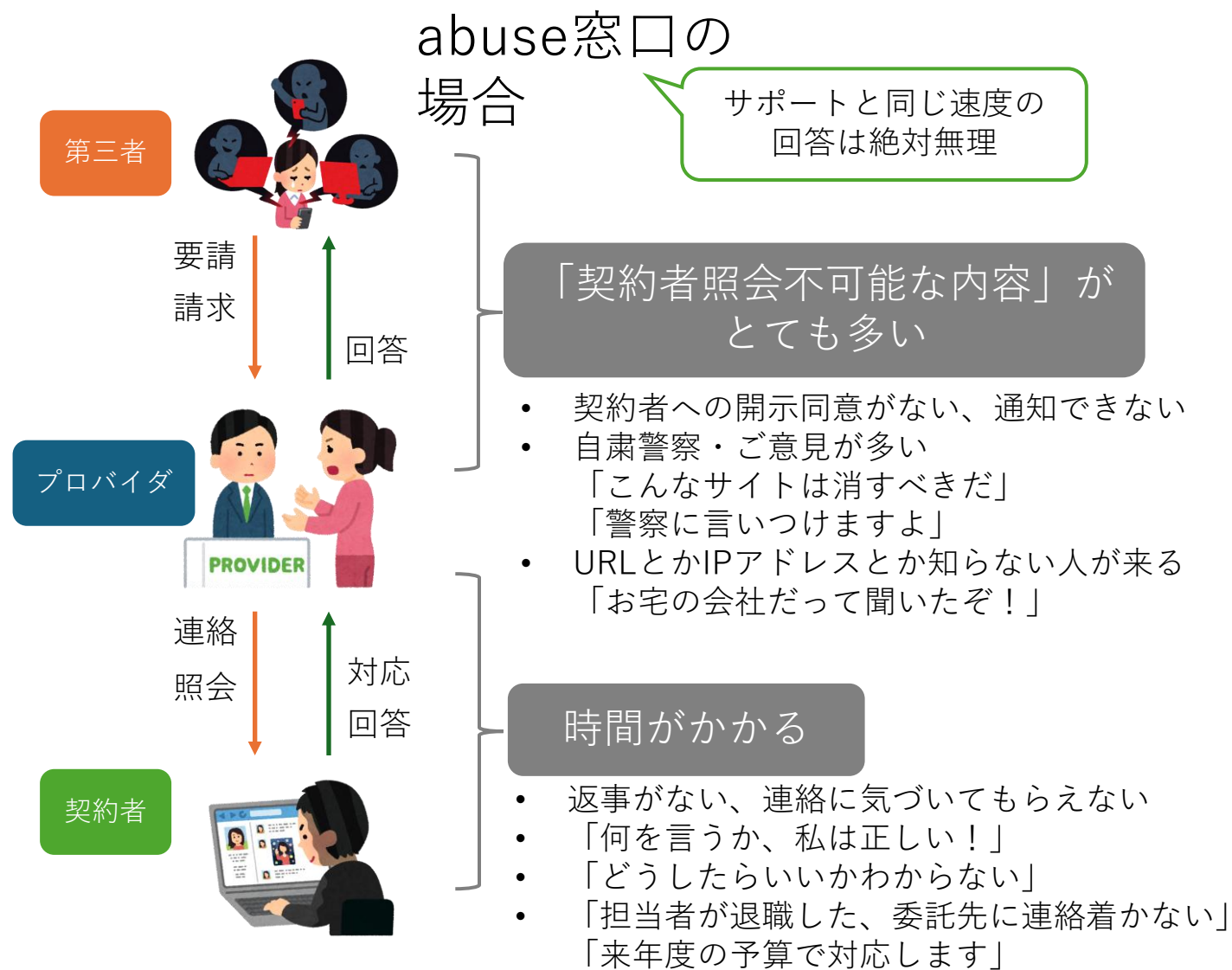
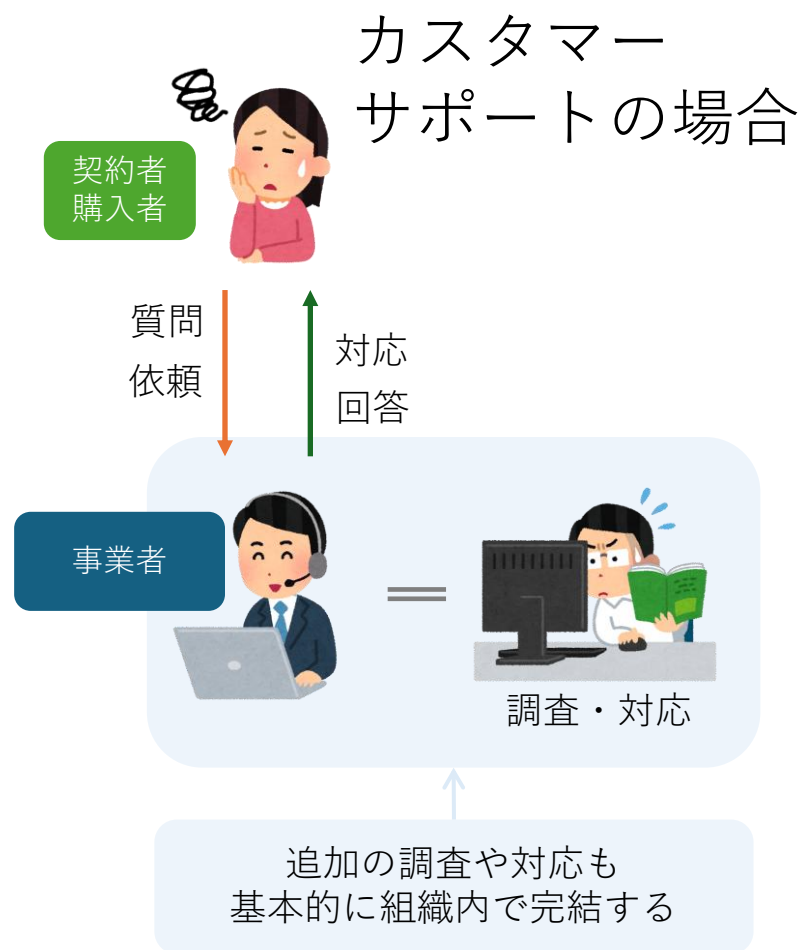
- フォームは、沢山受けたどうにもならない連絡への回答の結晶
- プロバイダそれぞれ「**この情報が必須、この同意が必須**」を示す
- それでもフォームをハックして対応不可能な連絡をしてくる人は居る



プロバイダが必要とする情報を適切に伝えれば、ウェブフォームからの連絡は必須ではありません。
メールの連絡に対応しないプロバイダは、インターネット標準への配慮に疑問があると言えます。

繰り返しですが、「ウェブフォームから連絡したほうが早く対応される」傾向はあります。

いつになったら返事をもらえる？ サポートとabuseの違い



abuse窓口の中の人はどうな仕事をしている？



192.0.2.10 から
203.0.113.10 から
192.0.2.10 から
192.0.2.10 から
198.51.100.10 から
不正アクセスが！

spam



192.0.2.1 から
203.0.113.1 から
192.0.2.1 から
192.0.2.1 から
198.51.100.1 から
スパムメールが！



example.net にある
私の写真を消して
example.edu にある
私の名前を消して



203.0.113.20 が
P2Pでファイル交換し
著作権侵害している
発信者情報の
任意開示を求める



警察官巡回中

example.org は
闇金サイトなので
消して



203.0.113.10 の
契約者情報を照会したい
example.jp の
データを差し押さえたい



example[.]jp に
example[.]jp に
example[.]com に
example[.]jp に
example[.]jp に
フィッシングサイトが！

罵られたり

From: noreply@
自動送信メールだったり

高圧的だったり

残虐・不愉快な画像

来客！

紙！

期日！



何の要請か「速く」「正確に」識別するスキルが必要
同じ事象に対する要請はグループ化もする
そして優先順位をつける、トリージする

識別スキルの不足、
順位付け誤りが
起きるとどうなる？



example.net の
発信者情報の開示が
申立てられたよ

abuse窓口の中は、どんな働き方をするどんな人たちが

abuse窓口の中は「野戦病院」「ダメコン」

- “[damage control wet training](#)” なんて検索すると、「これウチの職場イメージにぴったりだ！」がいっぱい出てくる
 - 和気あいあいとした楽しい職場です！
- “I am sorry to hear how busy your role is - sadly many anti-abuse desk workers would have a similar story” と言われた
 - “similer story” がとても悲しい

発表者の所属組織とは無関係に、一般化して考えるのですが

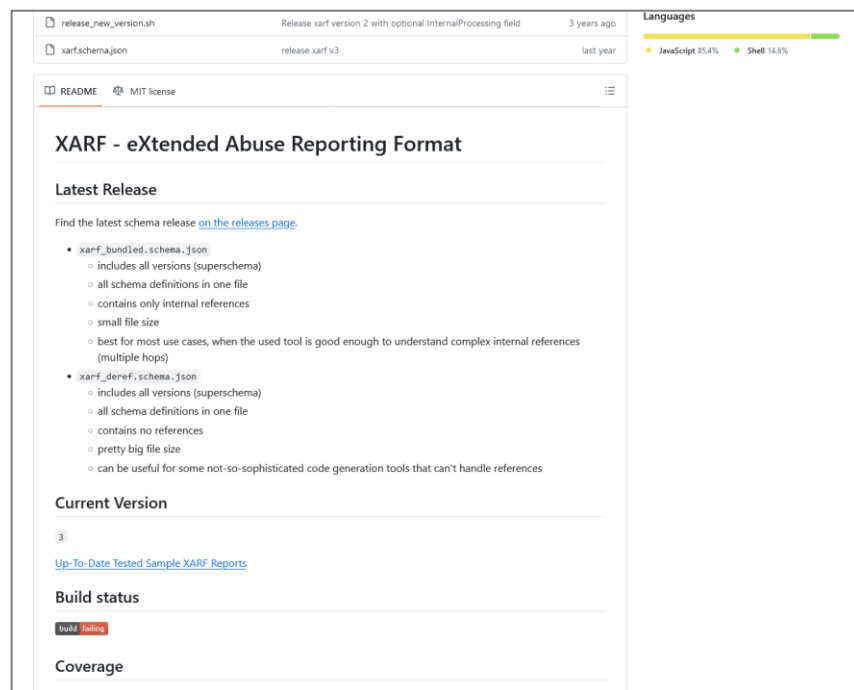
abuse窓口の中の仕事は“Shit Jobs” に当たる

- 「社会から必要とされるが感謝はされない」特徴がある、存在自体認知されていないかもしれない
デイヴィッド・グレーバーの著作「[ブルシット・ジョブ](#)」[ブルシット・ジョブ](#) [クソどうでもいい仕事の理論](#)」で分類すると、これは明らかに「クソどうでもいい仕事」ではない、「クソ仕事」ということになる
- 「世の中が本当に必要としている仕事」の給与はたいてい安く、発言力も低い
 - 様々な仕事を想像する、abuse窓口の仕事は何と似ていてそれらとはどのように違うか…医療、福祉、衛生、介護、保育、物流
- 連絡を受け取って対応してくれる人は、セキュリティエンジニアや弁護士ではないと考えた方が良い

窓口の中の忙しい人に間違わせない伝え方が必要だけれど、それではどう伝えればよいのか。



U.S. Navy, it is in the public domain in the United States.

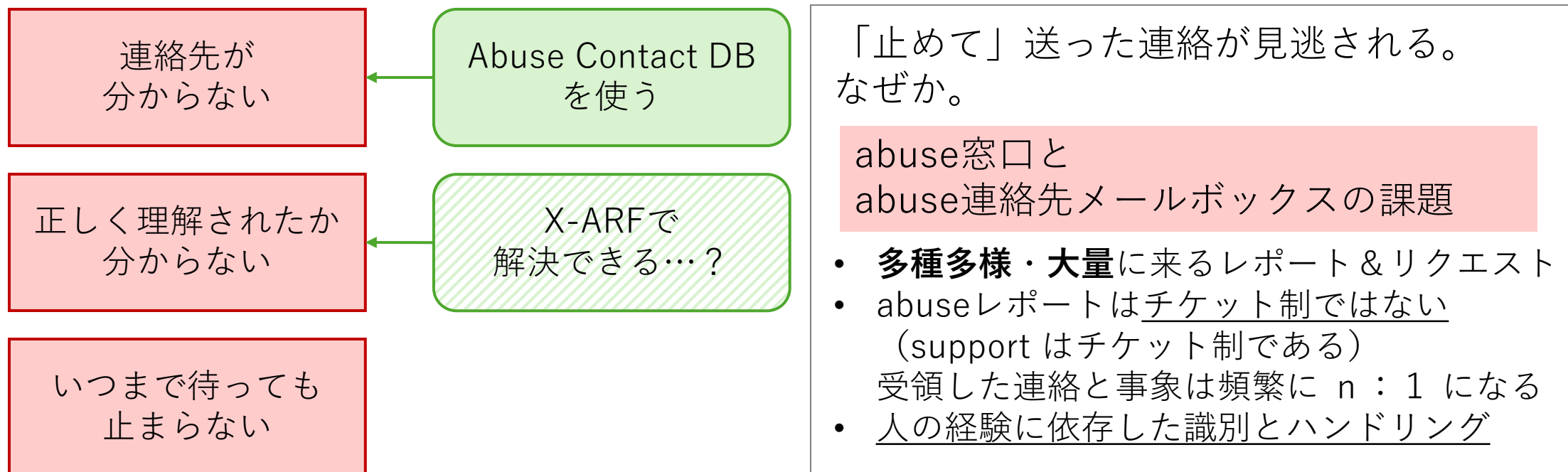


GitHub abusix / xarf
<https://github.com/abusix/xarf>

「正しく伝えられたかわからない」問題へのアプローチ

X-ARFを使用して
ハンドリングが容易な
abuseレポートを送る

振り返り・次につづく課題の再確認・X-ARFの紹介



- 窓口の体制はabuse窓口専門の場合、サポート兼業の場合、いずれもある
サポート出身、エンジニア出身、法務・バックオフィス出身、バックグラウンドも様々
- 課題になるのは識別とハンドリング、担当によりブレが大きい（担当ガチャ）
- X-ARF は **eXtended Abuse Reporting Format** の略、「えっくすあーふ」と読む
起こり得るabuseをJSONスキーマ化（類型化）している、abuse窓口に宛てるメールにJSON形式で添付する

X-ARFの使い方 <https://github.com/abusix/xarf> を読む！

- メールヘッダーで
Content-Type: multipart/report; report-type=feedback-report; を指定する
- 人間が読む（abuse窓口の人に読んでもらう）部分、機械に解析させる部分、XARF JSONレポートの3パート構成
- XARFのスキーマは次のURL
<https://github.com/abusix/xarf/tree/master/samples/positive/3>

サイバー攻撃関連

- botnet
- ddos
- exploit
- loginattack
- malware
- openservice
- phishing
- portscan
- potentially_compromised
- spam
- webcrawler

侵害情報関連

- childabuse
- copyright
- harassment_image
- harassment_url
- trademark

X-ARF online Validator が
blocklist.de にあるので活用すると
良いです。
<https://www.blocklist.de/de/xarf-validator.html>

```
{
  "Version": "3",
  "ReporterInfo": {
    "ReporterOrg": "ExampleOrg",
    "ReporterOrgDomain": "example.com",
    "ReporterOrgEmail": "reports@example.com",
    "ReporterContactEmail": "contact@example.com",
    "ReporterContactName": "Mr. Example",
    "ReporterContactPhone": "+ 01 000 1234567"
  },
  "Disclosure": true,
  "Report": {
    "ReportClass": "Content",
    "ReportType": "Phishing",
    "Date": "2018-02-05T14:17:10Z",
    "SourceIp": "192.0.2.55",
    "SourcePort": 80,
    "SourceUrl": "http://phish.example.org/index.html",
    "Ongoing": true,
    "Samples": [
      {
        "ContentType": "text/html",
        "Base64Encoded": false,
        "Description": "Just a test sample",
        "Payload": "<html>Phishy</html>"
      }
    ]
  }
}
```

phishing content の場合のスキーマ
https://github.com/abusix/xarf/blob/master/samples/positive/3/phishing_sample.json

Abuse Contact DB と X-ARF を手早く試す方法

HIDSの fail2ban に

- Abuse Contact DB で abuse連絡先を解決し、
- X-ARF 形式でabuse窓口にレポートする

アクションがあります！ **完全自動です！**

右例は、次の環境の場合です。

AlmaLinux release 9.3 (Shamrock Pampas Cat)

fail2ban-1.0.2-12.el9.noarch

Postfix 等のMTAを動かせば、sshd宛てに Brute force Attack 等が来た時、ただこれだけでabuseレポートが自動送信されます。冗談でなくこれだけでabuseレポートが送信されてしまう（＝**プロバイダのabuseデスクがテイクダウンに動く**）ので、*jail* の条件は慎重に決める必要があります。

アクションを定義しているファイルは
/etc/fail2ban/action.d/xarf-login-attack.conf です。

送信するメールの本文、X-ARF のJSONを記述する部分があり、参考になります。

```
# cat /etc/fail2ban/jail.local
```

```
[DEFAULT]
```

```
bantime.increment = true
```

```
ignoreself = true
```

```
bantime = 1d
```

```
findtime = 40m
```

```
maxretry = 10
```

```
backend = auto
```

```
usedns = warn
```

```
logencoding = auto
```

```
[sshd]
```

```
enabled = true
```

```
action = %(action_xarf)s
```

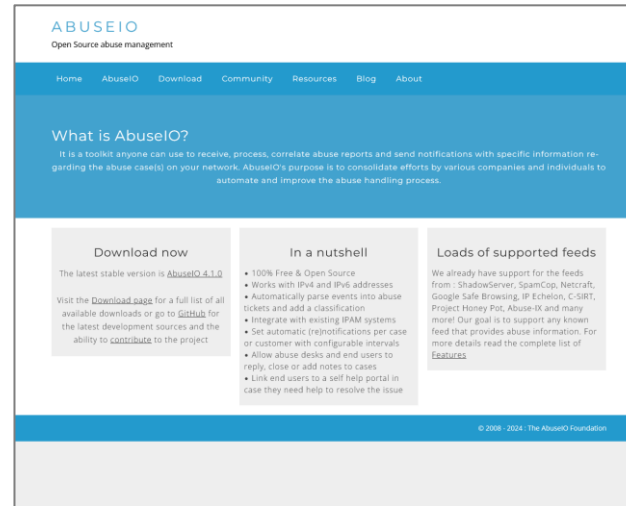
action = %(action_xarf)s を書くだけ

（注）例です。ban条件が緩いかも。。。

X-ARF形式のレポートとabuseメールボックスの自動化

abuseメールボックスの問題点

- チケット形式ではない
- abuse事象の識別が複雑
- 顧客を特定しなければならない
- 返信不要な自動送信されたレポートと返信必要な人が手で送ってきたレポートを識別しなければならない
- 一部に継続的かつ大量に送られてくる特定のレポート形式がある



AbuseIO
Open Source Abuse Management
<https://abuse.io/>



Abusix GmbH
Abuse Management
<https://abusix.com/network-abuse-management-solution/>

- 問題点の解決には、一般的な Mail User Agent や CRM とは違うソリューションが必要
- 実装例は [AbuseIO](https://abuse.io/)（機能は限定的・デモ有り）、[Abacus](https://abusix.com/network-abuse-management-solution/), [Abuse Management](https://abusix.com/network-abuse-management-solution/)（旧 AbuseHQ）, 2024現在の選択肢はX-ARFをパースできる Abuse Management 一択、でも [AbuseIO](https://abuse.io/) のデモを試すことでも「こういう問題を解決したい」思想は読み取れる

「たくさんレポートしたい人」はX-ARFを使用し、「X-ARFを解析できるabuseメールボックスに受け取らせる」事を狙うと、素早い対応やX-ARF普及に資するでしょう。

でも X-ARF って使われているの？ 初めて聞くけど

- 積極的にX-ARFを使用してレポートしてくる団体は少ないです。たぶん、10団体あるかないか。ところが「とにかく大量にレポートする」団体も限られていて、「とにかく大量にレポートする団体（クジラと言っている）」はX-ARFを導入済みです。
そのためにabuse窓口で受け取るレポートにX-ARFが使用されている割合は高いです。特にフィッシング、不正アクセス。
- 「X-ARFで受け取る」と公言しているabuse窓口も少ないです。たぶん、10団体あるかないか。ただし、欧米の一部大手は導入済みです。たとえば [Digital Ocean](#).
他、[Swisscom](#), [Mimecast](#), [Stackpath](#), [KPN](#), [Vodafone](#) が導入しているようです。
- X-ARFはスキーマが定義されているので、複数組織間でabuseの情報を交換する用途にも採用できます。
CSAM（児童に対する性的虐待の様相）対抗活動にあたる団体の中の人が、「捜査機関とX-ARFでデータ交換している」と話していました。

2024年現在、X-ARFが実用されている範囲はおそらく限定的です。

でも「とにかく大量にabuseレポートを送る人」「大量のabuseレポートを受け取る大手プロバイダ」「abuseレポートを大量流通させたい人」たちは使っている、スケーラビリティが示された、採用が進んでいるソリューションと言えるのではないのでしょうか。

X-ARFとabuseレポートハンドリングの将来展望

- X-ARFのスキーマは偏っているとは感じる、現状では。
 - サイバー攻撃の種類が充実している一方、権利侵害、法令違反情報、法執行に関するスキーマは不足している印象
 - 日本法の権利の体系に十分に即していない印象
 - X-ARFを解析できるメールボックスシステムは日本に無い。
 - Abusix Abuse Management はSaaS型。
日本のプロバイダは個人情報の域外移転規制が関係して使用できないと思われる
- それでも **自動化は正義**
 - 重要な点「現在、**日本にはカウンタープランが無い**」、
選択肢は、カウンタープランを出すか開発参加する（使ってみる）かどちらか

「上手く行くようになった未来」には、「Predator はJC3によるARS実装(Abuse Reporting System)のひとつ」とか「AbuseIO は OSS の AMS実装(Abuse Management System)のひとつ」のように、「この種のソフトウェアジャンルの名前」が生まれるように思います。

対応しないabuse窓口にはどうする

- 最も多い間違った方法
「abuse窓口の担当者をののしる」
- 次に多い間違った方法「SNSで非難する」

気持ちはわかります。

支援欠乏した野戦病院スタッフを
罵倒しても改善は見込めません。

データ・エビデンス・統計が重要
統計情報を公開するのです。

- 最も優れた例は、abuse.ch の URLhaus です。
- abuse.ch のレポートは ICANN の [Domain Abuse Activity Reporting \(DAAR\)](#) のデータソースの一つにもなっています。
- abuse.ch のレポートは精緻で理想的と言って良く、abuse.ch がabuse窓口に連絡した組織内の記録を直接参照して生成されているようです。

URLhaus					
From ABUSE® © URLHAUS					
14	AS209363 sco-webage-20190220	- None	0	1	9 minutes
15	AS268490 A.I.P._INTERNET	BR	0	1	9 minutes

The following table shows the top 15 hosting providers with the **slowest** abuse desks. To generate these statistics, URLhaus measures the time between when URLhaus sent the abuse complaint to the hosting provider and when the reported content goes offline. Please consider that the accuracy is +/- 1 hour.

Rank	ASN	Country	Online	Offline	Average Reaction Time
1	AS8245 VIDEOBROADCAST-AS	AT	0	1	5 years, 6 months, 6 days, 17 hours, 2 minutes
2	AS23520 COLUMBUS-NETWORKS	US	0	1	4 years, 6 months, 14 days, 16 hours, 19 minutes
3	AS6 BULL-HN	US	0	1	4 years, 2 months, 23 days, 19 hours, 10 minutes
4	AS10099 UNICOM-Global	HK	0	11	3 years, 9 months, 6 days, 10 hours, 11 minutes
5	AS197838 CHEELOO-AS	PL	0	1	3 years, 8 months, 1 days, 17 hours, 58 minutes
6	AS199391 XGlobe-199391	IL	0	3	3 years, 6 months, 25 days, 19 hours, 21 minutes
7	AS57043 HOSTKEY-AS	RU	0	1	3 years, 5 months, 20 days, 12 hours, 33 minutes
8	AS263057 Connect_Network	BR	0	1	3 years, 5 months, 14 days, 4 hours, 29 minutes
9	AS24164 UBBNET-AS-TW	TW	2	1	3 years, 1 months, 15 days, 18 hours, 40 minutes
10	AS30782 TOYA-KRAKOW-AS	PL	0	1	3 years, 1 months, 4 days, 20 hours, 34 minutes
11	AS37024 Yoprov	ZW	0	1	2 years, 9 months, 27 days, 23 hours, 58 minutes
12	AS60822 WISP1	IT	0	1	2 years, 9 months, 15 days, 2 hours, 6 minutes
13	AS9811 DRCSCNET	CN	2	2	2 years, 9 months, 5 days, 8 hours, 32 minutes
14	AS10292 CWJ-1	US	0	1	2 years, 7 months, 25 days, 16 hours, 36 minutes
15	AS57803 TELESERVIS-AS	RU	0	2	2 years, 7 months, 22 days, 1 hours, 44 minutes

The full list of average reaction time over all hosting providers (ASNs) can be found here:

- [Average Reaction Time \(for all hosting providers\)](#)

If you are a hosting provider, network owner or national CERT, you can subscribe to the URLhaus feed for your ASN or country here:

- [URLhaus Feeds](#)

© abuse.ch 2024

URLhaus Statistics

<https://urlhaus.abuse.ch/statistics/>

URLhaus Average Hosting Provider Reaction Time

<https://urlhaus.abuse.ch/statistics/reactiontime/>

おわりに・まとめ

2024年現時点で必要とされているのは、確実さより圧倒的に量であり、量を実現する**手軽さ**と**速さ**ではないか

- 結果止まらなかったとしても、何の連絡もなしに、止まることはあり得ない
- 結果止まらなかったとしても、何も連絡しなかったならば、なぜ止まらないかの分析情報も得られない
- とにかくabuse連絡（停止・テイクダウンリクエスト、削除・リムーバルリクエスト）しましょう

「正しいやり方」は予め用意されているわけではない、
正しいやり方は、「リクエストする人」「対応する人」
両方でつくりあげるもの

- abuse宛ての連絡(abuse reporting)のスタンダードやベストコンプラクティスは未だ無い
abuse連絡先がwhoisに登録されていることを確実にする道も長い、abuse対応にルーズなプロバイダも多い
- とにかくabuse連絡しましょう

インターネットはずっと続く…続くからこそ必要になる取り組みがある

ご清聴ありがとうございました。