サイバー攻撃を止めるには？
攻撃の動向&abuse対応依頼入門

2023/7/20
Internet Week ショーケース in 札幌
プログラム C12

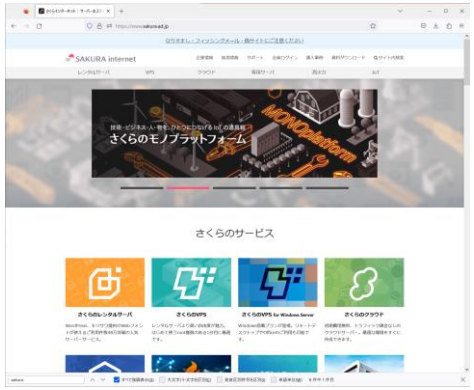
さくらインターネット株式会社 山下健一

私
サイバー攻撃を
受けてる
の権利が
侵害されるて
止めさせたい

目次と自己紹介

1. サイバー攻撃を止めたい！　フィッシングサイトをテイクダウンしたい！
2. 私の権利（例・著作権）が侵害されてる！　被害拡大を止めたい！
3. 「止めて！」どこに言えばよい？　何なら、どう伝えれば、止まる？
4. もしあなたが「止めて！」と「言われる立場の担当者なら」どうする？

「この話をするあなたは誰ですか」「なぜあなたがこの話をするのですか」自己紹介



https://www.sakura.ad.jp/

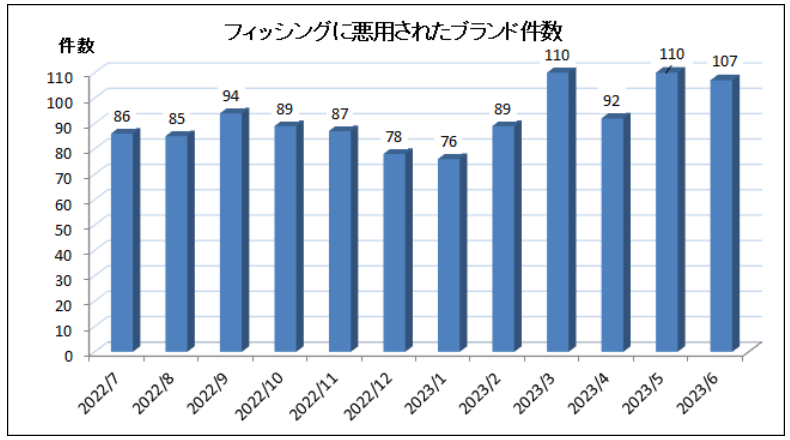
- 私はさくらインターネット株式会社に所属しています。
  弊社はホスティング・クラウド・データセンターサービスを提供する通信事業者です。
- 主に３つのAS番号(7684, 9370, 9371)で、IPv4アドレスを計100万IP程、経路広報しています。
- 私は所属組織のサービスで行われた「サイバー攻撃」「権利侵害」等について「止めて！」と要請を受ける「abuse窓口」の仕事を2016年頃から担当しています。
- 弊社が１年間に取り扱う「abuse案件」は7000件程です。
  これは案件として取り扱い記録した数で、abuse窓口で受信や送信したメールの数ではありません。
- 実務経験をもとに、2023年現時点の実際的な情報をお話します。
  現時点で「ここまでは整理されている」「ここから先は未整理」を示します。

1. **サイバー攻撃を止めたい！**
   フィッシングサイトをテイクダウンしたい！
2. 私の権利（例・著作権）が侵害されてる！
   被害拡大を止めたい！
3. 「止めて！」どこに言えばよい？
   何なら、どう伝えれば、止まる？
4. もしあなたが
   「止めて！」と「言われる窓口の担当者なら」
   どうする？

フィッシング詐欺の「今」

フィッシング対策協議会
「フィッシングレポート 2023」でわかること

- 「フィッシングサイトのURL件数」は
大きく増えている
- 「ブランド名を悪用された企業の件数」も増加
右下の2022グラフでは後半減っているが、
下2023年6月の月次報告では、更に増えている



フィッシング対策協議会
「2023/06 フィッシング報告状況」2023/7/5 より引用
https://www.antiphishing.jp/report/monthly/202306.html

フィッシングサイトの URL 件数は、2022 年度下半期は 2021 年下半期よりも増加している。(図 1-2)。ブランド名を悪用された企業の件数も、2021 年と比較して増加の傾向にある (図 1-3)。

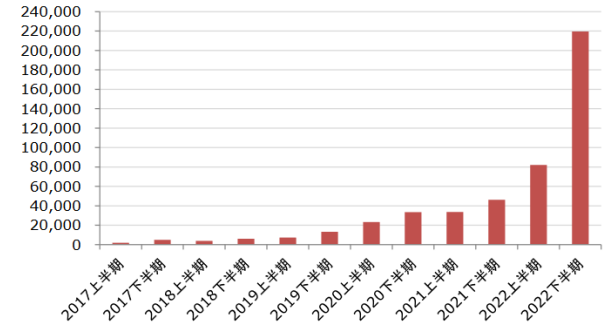


図 1-2　国内のフィッシングサイトの件数 [2]

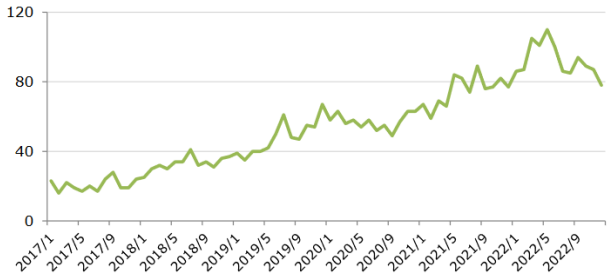
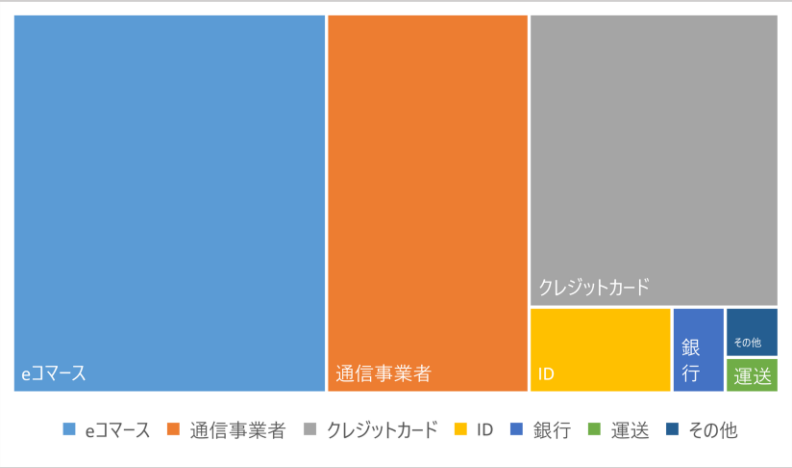


図 1-3　国内のブランド名を悪用された企業の件数 [2]

フィッシング対策協議会
「資料公開: フィッシングレポート 2023 の掲載について」2023/6/1
レポートP2より引用
https://www.antiphishing.jp/report/wg/phishing_report2023.html

フィッシング詐欺の「今」



日本サイバー犯罪対策センター(JC3)
「フィッシングターゲットの変遷」(2022/2/4) より引用
https://www.jc3.or.jp/threats/topics/article-430.html

JC3によれば次の傾向(2022/2/4)

- 銀行を装ったフィッシングサイトの割合は減少
- 通信事業者を装ったフィッシングサイトが急増

フィッシングの目的

- 決済手段搾取 → EC不正購買

通信事業者が急増？

- 決済サービスが狙いか

あるホスティングプロバイダの場合

- メールアカウント搾取 → フィッシングメール送信
- 会員情報搾取 → フィッシングインフラ構築

フィッシング対策協議会
さくらインターネットをかたるフィッシング (2023/01/16)
https://www.antiphishing.jp/news/alert/sakurainternet_20230116.html

ちょっと確認、「フィッシング」って何だろう？

フィッシングは「なりすまし詐欺」のひとつ

ブランドに
なりすます詐欺サイト

- オンラインバンキング詐欺
- カードブランド詐欺
- Apple, Google, Microsoft…
- 配達詐欺
- テクニカルサポート詐欺
- アンケート詐欺
- 行政機関を騙る詐欺

ブランドに
関係しない詐欺サイト

- ワンクリック詐欺
- 当選詐欺
- 悪質EC詐欺

「EC詐欺」の内の一部、「特定商取引法に基づく表記」が異常なECサイト等

- ブランドになりすます詐欺が「フィッシング」！
  だから、「なりすまされたブランド」があり、「ブランドのユーザーが被害を受ける」
- 所属組織のブランド・サービスが騙られた場合への、備えはありますか？
  「その時」に、ユーザー様を守るために何をしたらよいか、ご存じですか？

フィシングのターゲットブランドにされてしまったら

フィッシング対策協議会が公開する
「フィッシング対策ガイドライン」を参照
https://www.antiphishing.jp/report/guideline/

「フィッシング被害が発生してしまった」際の初動

- 「とにかく被害を減らす」「ユーザーを保護する」観点では、P29～P33 を参照して対応すると良いです。
- まず素早くガイドライン「4.5.2.URL フィルターへ登録」！
  - 「どこで登録できるか」はご存じですか？
  - 平常時に、一度はガイドラインに目を通しておく、予め、たとえば “Report a Phishing Page” (Google Safe Browsing), “Report an unsafe site” (Microsoft Security Intelligence) 等のウェブサイトを確認しておくと良いです。

そして、フィッシングサイトのテイクダウン（停止）へ！
自分自身でフィッシングサイトのあるISPに「止めて！」と連絡する方法と、JPCERT/CC に停止要請の中継を依頼する方法がある

JPCERT/CC インシデントの報告(Webフォーム)
https://form.jpcert.or.jp/

フィッシングサイトのテイクダウン要請の具体例

- フィッシング対策ガイドラインより要請文例抜粋
  必要カ所を埋めて、プロバイダにメールを送る
- 送り先プロバイダの特定法、
  送り先メールアドレスの特定法は、後述

ところでガイドラインの文例は、要請を受ける側の経験者としては、
とても丁寧な文の印象を受けます。
受ける要請は、文例と比べ「素っ気ない」シンプルな文が多いです。
例は、汎用性のあるよい文例だと感じます。

追加の考え方

- （たとえばSSHに）Bruteforce攻撃を受けたら？
- （たとえばサイトに）インジェクション攻撃を受けたら？

→ログ（不正アクセスの証跡）に置き換えて連絡する

更に追加の考え方

- 成功する不正アクセスを受けたら…？
- クレジットカードを悪用するアクセスを受けたら…？

To whom it may concern,

[簡潔な企業プロファイル].

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「フィッシング対策ガイドライン」
P42より抜粋
https://www.antiphishing.jp/report/guideline/

1. サイバー攻撃を止めたい！
   フィッシングサイトをテイクダウンしたい！
2. **私の権利（例・著作権）が侵害されてる！**
   被害拡大を止めたい！
3. 「止めて！」どこに言えばよい？
   何なら、どう伝えれば、止まる？
4. もしあなたが
   「止めて！」と「言われる窓口の担当者なら」
   どうする？

「権利を侵害する情報」の概観

個人の場合（一部のみ）

- 名誉棄損
- 誹謗中傷
- 個人情報の暴露拡散
- 肖像（写真）の未承諾使用

事業（財産）の場合（一部のみ）

- 著作物の拡散・海賊版
- 商標権の侵害・ブランドコピー
- サイバースクワッティング

「権利を侵害する情報があった時」のアプローチ

1. 被害の拡大を止めたい！ → 削除要請
2. 被害の回復（損害賠償）を求めたい！ → 開示請求

開示請求は大変。。。**詳しい**弁護士に相談したほうが現実的と思う。

削除要請は、「権利の侵害を受けた当事者」から「侵害された権利を適切に伝える」ことで、削除に繋がる可能性がある。

「削除を要請したい！」

話を単純化するために、いったん、著作権に絞ります。

文化庁「初めての『削除要請』ガイドブック」がすばらしい！

文化庁　初めての「削除要請」ガイドブック
https://www.bunka.go.jp/seisaku/chosakuken/kaizoku/singai_guide.html

すばらしい理由

- 新しい（重要！！　2022年3月作成・新品ぱりぱり）
- クリエイター・中小企業も想定したと思われる「わかりやすさ」
- 削除要請の参考書式（英語含む！）が付属！
  「代表的な削除要請窓口」紹介も付属！
- 関連文書（「著作権侵害（海賊版）対策ハンドブック」他）も充実！

「初めての『削除要請』ガイドブック」は、他に比べる物ないほどにわかりやすい、すばらしい

著作権関係は、以前より「プロバイダ責任制限法 関連情報Webサイト」に「著作権関係様式」がある。
こちらは「プロバイダが日本の事業者である場合」にしか、役に立たない。

「初めての『削除要請』ガイドブック」は、英語で「消して」と伝える実践的方法を示してくれており、すばらしい。発表者が窓口で受けているメールの形式と概ね同じで、プロバイダ側も違和感なく受けることができる。

侵害された権利が商標権の場合も、この派生形で削除要請できそう。

「止めて欲しいこと」は「他にもある！」

止めて欲しいと思った時、要請したり、相談したり、情報提供できる窓口がある。

「止めて欲しい」情報・コンテンツ	要請先・情報提供窓口
これはEC詐欺サイトじゃないの？	SIA 悪質ECサイトホットライン https://www.saferinternet.or.jp/akushitsu_ec_form/
違法ポルノだ！　児童ポルノだ！	インターネットホットラインセンター https://www.internethotline.jp/
これは未承認医薬品では？	厚生労働省 あやしいヤクブツ連絡ネット https://www.yakubutsu.mhlw.go.jp/
被害をうけてる、何が頼めるか判らない、 相談先もわからない！　助けて欲しい！	違法・有害情報相談センター https://ihaho.jp/
私に対する誹謗中傷を消してほしい！	SIA 誹謗中傷ホットライン https://www.saferinternet.or.jp/bullying/
迷惑メールだ！	迷惑メール相談センター http://www.dekyo.or.jp/soudan/contents/ihan/

他、「止めたい」以外の「被害回復を求めたい時」、発信者情報の開示を求めたい時の説明は、本講演では省きます。

1. サイバー攻撃を止めたい！
   フィッシングサイトをテイクダウンしたい！
2. 私の権利（例・著作権）が侵害されてる！
   被害拡大を止めたい！
3. **「止めて！」どこに言えばよい？**
   何なら、どう伝えれば、止まる？
4. もしあなたが
   「止めて！」と「言われる窓口の担当者なら」
   どうする？

「アビューズ」窓口を、探してください。”abuse” と書きます。

辞書的な意味

乱用する・悪用する・裏切る・虐待する・酷使する・粗末に扱う

abuse = ab + use (cf. ab-normal, ab-struct, ab-sent)

RFC 2142 の記述

4.　ネットワーク運用に関連するメールボックス名

運用に関するアドレスは、その組織のインターネットサービスに対する難点を経験した顧客やプロバイダなどが連絡を取り合うことを想定している。

メールボックス	分野	取り扱い
ABUSE	**顧客関連**	**公共における不適当なふるまい**
NOC	ネットワーク管理	ネットワーク・インフラストラクチャ
SECURITY	ネットワーク セキュリティ	セキュリティに関する報告 または問い合わせ

https://www.nic.ad.jp/ja/translation/rfc/2142.html
https://www.ietf.org/rfc/rfc2142.txt

abuse窓口は、どこにあるか、ちょっと余談

インターネット通信は、TCP/IPプロトコルというデファクトスタンダードと、「インターネット資源」が管理されることで、成り立っています。

そして「インターネット資源」に、「abuse窓口（『公共における不適当なふるまい』の連絡先）」があります。

「インターネット資源」は**すごく大切**な基礎知識、
でも「正確に説明しようとすると長い話」になります。省きます。

持ち帰ってもらいたい「ふたつのポイント」＋whois！

次の二つにabuse窓口がある、もしも困ったことがあった時には、ここに、頼もう。

- 名前資源（ドメイン名！）
- 番号資源（IPアドレス！）

ウェブ検索エンジン等で「whois」を調べる（大いに端折っています、不正確です）。

説明は「とりあえずは使える」けど「正しくないし、正確でもない」方法です。

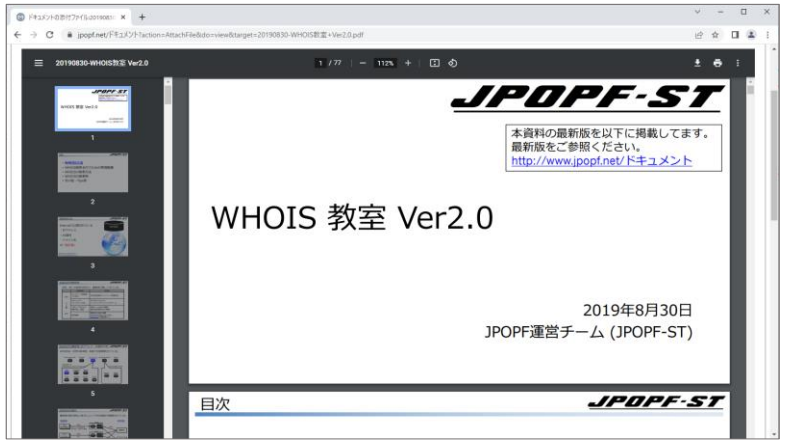
ただ「とりあえずウェブ検索する」ことで、それなりに情報は得られます。

丁寧に進める必要がある場合は、専門知識のある方を頼ってください。

「インターネット資源」とabuse連絡先

もう少し詳しく・もう少し正確に

- 「インターネット資源（ドメイン名、IPアドレス, AS番号）」の「abuse連絡先(abuse, abuse-c, IRT-Object)」に対応依頼できる
- インターネット資源は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」、whoisはJPOPF運営チーム「WHOIS 教室」ドキュメントが有益なのでおススメ！



JPOPF運営チーム 「WHOIS教室」
https://www.jpopf.net/ドキュメント

実務的な、abuse連絡先の探し方

1. ウェブ検索で、”whois” + “abuse” 等のキーワードを検索
2. プロバイダ名を特定し、更にウェブ検索
3. プロバイダのウェブフォームを探す
4. ウェブフォームから連絡
5. ウェブフォームが無ければ、whoisで調べた「abuse連絡先のメールアドレス」に宛ててメールで連絡

Windows には
whoisコマンドが無い…

「最も正しい方法」ではない
比較的成功する「現実的な方法」

フォームがあれば、フォームから連絡する
「フォームがある」ことには理由がある

abuse窓口への頼み方、abuse窓口に頼めること

abuse窓口への伝え方・摘示

大まかには右４点を伝える

「人」がabuse窓口の中に居る、
理解を得やすい＆受け容れられやすい伝え方が**良**

1. abuse行為の概要
2. エビデンス
   （URL・ログ・侵害情報の摘示、正確に！）
3. abuse行為に当たると判断した理由、
   あるいは行為により侵害された権利
4. 求める対応

abuse窓口に依頼できない事柄

- abuse窓口にファストパスは無い・優先順位はabuse窓口の中のポリシーに依る
- 「迷惑だ」「不快だ」主観はダメ
  - プロバイダの「サービス利用契約約款」に違反していれば、対応してもらえる
- 「違法だ」違法性を判断する権限は、ふつう、個人・私人には無い
  - 専門機関に情報提供して、専門機関に任せる
- abuse窓口はサポートセンターや「ご意見窓口」ではない
  迷う場合はabuse窓口ではなく専門家（詳しい弁護士・公的相談員・技術者）や公的機関（警察）に相談を

1. サイバー攻撃を止めたい！
   フィッシングサイトをテイクダウンしたい！
2. 私の権利（例・著作権）が侵害されてる！
   被害拡大を止めたい！
3. 「止めて！」どこに言えばよい？
   何なら、どう伝えれば、止まる？
4. **もしあなたが**
   「止めて！」と「言われる窓口の担当者なら」
   どうする？

abuseの仕事「何がabuseで、何がabuseでないか」

RFCは「公共における不適当なふるまい(Inappropriate public behaviour)」を具体的に指定しません。
「社会はどのように考えているか」代わる情報を探す必要があります。

- Wikipedia 「嫌がらせ」 https://ja.wikipedia.org/wiki/嫌がらせ
- Wikipedia ”Harassment” https://en.wikipedia.org/wiki/Wikipedia:Harassment
- Wikipedia “Cyberbullying” https://en.wikipedia.org/wiki/Cyberbullying
- PEN America “Defining Online Abuse: A Glossary of Terms” https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

出てくるキーワード

- ネットいじめ
- サイバーストーキング
- フェイク
- DoS攻撃
- ハッキング
- スパミング
- 個人情報暴露
- ヘイトスピーチ
- リベンジポルノ
- なりすまし
- フィッシング

情報を探していくと、（正しいかどうかはわからないが）次の様子が見て取れます。

- 広義に「嫌がらせ」があり、abuseはその中でも悪質性の高い行為を指す言葉である
- abuseが起こる場は様々あって、オンラインはその一つである

abuse窓口の担当者の仕事

もし、あなたがabuse窓口の担当なら

- 「abuseの意味」を確認しよう！
  「何がabuseで何がabuseで無いか」判らないと混乱する
- Inbound abuse と Outbound abuse は違う
  - Inbound abuse　は「他社のabuse対策担当の仕事」
    そして「自組織のセキュリティ担当の仕事」
    または「自組織の法務（知財）担当の仕事」
  - Outbound abuse 対策が「私の仕事」

LACNIC 27 “Abuse Desk Training”
https://www.lacnic.net/innovaportal/file/2675/1/abuse-desk-training.pdf

abuse窓口の仕事

対応！　対策！　ハンドリング！

- 対応と対策はちがう、対応しながら対策（総量を減らしたり、自動化したり）する
- abuse窓口には変な要請や宛先違いの要請がいっぱいくる、ハンドリングする
- 数値化（どのくらいのコストがかかっている？　レポート化できる？）
- 必要な知識はどこで得られる？　コミュニティ活動で担当者同士情報交換をしよう！

「abuse窓口の仕事」の難しさ

よくある、答えの得にくい悩み

- 上司・会社・周囲の理解は、どうしたら得られますか？
- あまりにも人手が足りません！
- 必要とはされるけれど、誰からも感謝してもらえません…

新たにabuse窓口の担当になる方に向けて、担当者として言えることがあるとすれば、「メンタルに気を付けて、ヘルスケアをしてね」です。時に「強くストレスのかかるabuse」の対応もあります。

それから、「このような仕事によっても支えられていることを、社会はまだ知らない」ので、可能な場合は、認知を得る活動をしましょう。

おわりに・もし、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