「abuse窓口」が見つけられない問題

2023/6/23 JPOPM

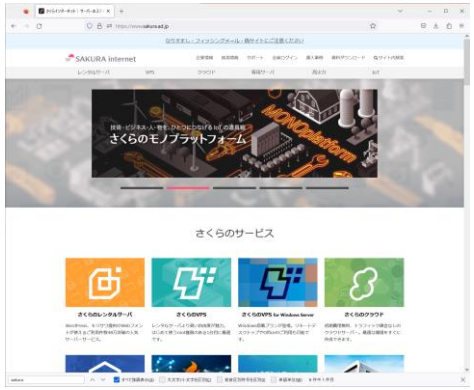
さくらインターネット株式会社 山下健一

この発表のテーマ

発表のテーマ、共有したいこと、議論したいこと

- **「abuse連絡先を登録してほしい、登録を促すどんな方法が考えられる？」**
- 「abuse連絡先を登録することが、何故、どのくらい必要か」
  abuse窓口の仕事の実態と、業務を通じて知っている情報を共有します。

「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。
- 私は所属組織で、この発表のテーマである「abuse連絡先窓口」を、2016年頃から担当しています。
- 弊社のabuse窓口が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。
  「メールの数」はもっと多いです。書面（法令に基づく照会）や電話もあります。

目次・構成

1. 「abuseとは何か」言葉の意味、オンラインabuseに関係するRFC 2142 の確認

2. 番号資源に対し abuse 連絡先窓口の設置を求める資源管理ポリシー、
   APNIC prop-079 とJPOPF p036-01 の確認

3. 実態としてabuse窓口に受ける連絡の紹介、
   実態から推し量る「様々な人に、abuse連絡先が必要とされている様」の説明

4. 外部から見た「日本のabuse連絡先窓口の評価」、
   「日本のabuse連絡先窓口の評価はとても低い」、なぜ低いのか？
   なぜ「日本のabuse連絡先」は見つけてもらえないのか？

5. 「abuse窓口に連絡する」事のトレンドと、abuse窓口を担当して感じる将来展望

6. 「abuse連絡先を設ける」事の大変さ、「abuse連絡先窓口を運用する」大変さ

7. まとめ「なぜ日本のabuse連絡先は見つけてもらえないのか？」課題は何か
   課題解決へのファーストステップ「JPNIC whois に abuse 連絡先を登録して欲しい」
   「JPNIC whois への abuse 連絡先登録を促す良い施策はないものか？」

abuseとは何か・言葉の意味, 語義, RFC 2142 の記述の確認

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」の意味，「公共における不適当なふるまい」とは何か？

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

目次・構成

1. 「abuseとは何か」言葉の意味、オンラインabuseに関係するRFC 2142 の確認

2. 番号資源に対し abuse 連絡先窓口の設置を求める資源管理ポリシー、
   APNIC prop-079 とJPOPF p036-01 の確認

3. 実態としてabuse窓口に受ける連絡の紹介、
   実態から推し量る「様々な人に、abuse連絡先が必要とされている様」の説明

4. 外部から見た「日本のabuse連絡先窓口の評価」、
   「日本のabuse連絡先窓口の評価はとても低い」、なぜ低いのか？
   なぜ「日本のabuse連絡先」は見つけてもらえないのか？

5. 「abuse窓口に連絡する」事のトレンドと、abuse窓口を担当して感じる将来展望

6. 「abuse連絡先を設ける」事の大変さ、「abuse連絡先窓口を運用する」大変さ

7. まとめ「なぜ日本のabuse連絡先は見つけてもらえないのか？」課題は何か
   課題解決へのファーストステップ「JPNIC whois に abuse 連絡先を登録して欲しい」
   「JPNIC whois への abuse 連絡先登録を促す良い施策はないものか？」

「abuse連絡先を登録する」資源管理ポリシー

prop-079: Abuse contact information
https://www.apnic.net/community/policy/proposals/prop-079/

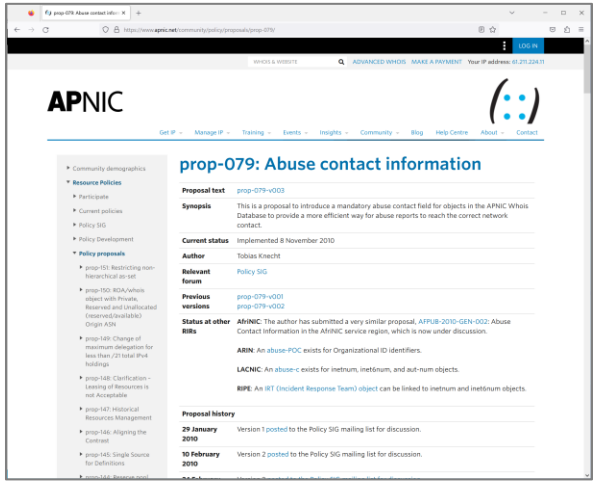
- APNIC Whois データベースにabuse連絡先を設けるポリシーが、8 November 2010 に実装(Implemented)された記録です。

prop-125: Validation of “abuse-mailbox” and other IRT emails
https://www.apnic.net/community/policy/proposals/prop-125

- APNIC Whois データベースに登録されたabuse連絡先が有効に機能していることを確認するポリシーが、09 May 2019 に実装(Implemented)された記録です。
- 説明(Synopsis)に「ネットワーク内で問題が発生していても状況に気づいていない可能性がある LIR に私たち全員が連絡できる必要があります。」とあります。

036-01: JPNICにおけるWHOIS正確性向上の検証
https://www.jpopf.net/p036-01

- APNIC prop-079 と prop-125 を受けつつ、JPNICにおいてもabuse連絡先を設けることを検討し、２０２２年８月２２日、JPNICよりネットワークの不正利用に対応する窓口(Abuse)の登録開始をアナウンスした記録です。
- JPNIC p036-01 で整理できたのは APNIC prop-079 相当までで、「abuse連絡先の検証」には踏み込んでいません。しかし APNIC prop-125 を踏まえると 「abuse連絡先の検証」も、次なる課題になってくる可能性があります。



目次・構成

1. 「abuseとは何か」言葉の意味、オンラインabuseに関係するRFC 2142 の確認

2. 番号資源に対し abuse 連絡先窓口の設置を求める資源管理ポリシー、
   APNIC prop-079 とJPOPF p036-01 の確認

3. 実態としてabuse窓口に受ける連絡の紹介、
   実態から推し量る「様々な人に、abuse連絡先が必要とされている様」の説明

4. 外部から見た「日本のabuse連絡先窓口の評価」、
   「日本のabuse連絡先窓口の評価はとても低い」、なぜ低いのか？
   なぜ「日本のabuse連絡先」は見つけてもらえないのか？

5. 「abuse窓口に連絡する」事のトレンドと、abuse窓口を担当して感じる将来展望

6. 「abuse連絡先を設ける」事の大変さ、「abuse連絡先窓口を運用する」大変さ

7. まとめ「なぜ日本のabuse連絡先は見つけてもらえないのか？」課題は何か
   課題解決へのファーストステップ「JPNIC whois に abuse 連絡先を登録して欲しい」
   「JPNIC whois への abuse 連絡先登録を促す良い施策はないものか？」

abuse連絡先を公開する必要性（入門・よくあるabuse）

「abuse窓口を設けてその連絡先を公開する」と、どのようなabuse対応要請が届くか、イメージに繋がるように具体例を挙げてみます。まずは入門編です。ここに挙げるabuse対応要請は「すごく多く」または「多くはないにしてもありふれて」来ます。

「ここに挙げるabuse」は、RFC 2142「役割、機能に対するメールボックス名」と関連するabuseに限ります。
つまり「対応要請がメールで来るabuse」です。プロバイダ責任制限法に基づく「発信者情報開示請求」やその訴訟の訴状、法執行機関からの「捜査関係事項照会」等の照会、差押え、これらに限らず「メールでない手段で届く対応要請」は除外します。

「どのようなabuse対応要請が多いか」は、インターネット接続サービス、ホスティング＆IaaS、SaaS、プラットフォーム、提供するサービスが「接続層からコンテンツ層までの高さのどこにあたるか」により偏りがあります。
ホスティング＆IaaSはちょうどこの層の中間にあって、「abuseのデパート！　総合商社！」になる様子です。

不正アクセスを受けた！
(Bruteforce, 辞書攻撃、クレデンシャルハーベスティング等)

麻薬だ！　脱法ドラッグだ！

詐欺のメール(SCAM)が来た！

実名報道された逮捕情報が今もある、
釈放されたのに！　生活再建できない！

不正ログインされた！
不正送金された！　不正購買された！

受け取りを希望しないメール(SPAM)が来た！

昔のグラビア写真が今もあって。今は子供もいるのに

サイトにアクセスするとマルウェアが降って来るよ！

闇金サイトだ、登録貸金業者番号の明示が無い！

通学先、職場、住宅写真を曝されて

変な探索が来た！
(URLスキャン・脆弱性探索等)

インジェクション攻撃が来た！

児童ポルノだ！
(CSAM: Child Sexual Abuse Materials)

子供の情報が流通してるんだ！
いじめだ、止めてよ！

DoS攻撃(DRDoS)が来た！

未承認医療医薬品を売るって言ってる！

私の名前が書きこまれたんです

Web Shellがあるぞ？
バックドア仕込まれてるぞ！

フィッシングサイトがある！

性器が丸見え！　ブランドコピー！

同人創作したマンガが配布されてる！
委託販売してるのに！

C2がある！
(Command & Control, サイバー攻撃指令サーバ)

このECサイトは詐欺！

スーパーコピー！

映画勝手に配りやがって！（英語）

サイトに変なJavaScriptが挿入されてる！

異常なサイトにリダイレクトされる！

商標権侵害だ！

DMCAに基づき要請する！（英語）

名簿がある！　個人情報が暴露して漏洩してる！
アクセス制御されてない！

認証情報が公開されてたんだけど？

著作物を違法に交換(P2P)してるIPアドレスだ！

abuse連絡先を公開する必要性（入門・よくあるabuse）

個人から届くabuse対応の要請は、言語化不明瞭な場合が多い、たとえば「侵害された権利が何か」すらも不明瞭になりがちです。

「それって、外資の他社がサービス提供する著名SNSなんだけど？　なんでウチにいらしたの？」すらも発生します。
URLが示されていない要請もたびたび届く、インターネット資源との紐づきの説明の無い場合も多いです。

プロバイダはabuse窓口に受けた対応要請を、契約者に転送する必要がある（直接対応できないので、契約者に取次ぐ必要がある）が、個人情報の取り扱いや転送の同意の意思が判らないので、必ず折り返し確認が発生します。めちゃくちゃに手間。

そこでプロバイダは RFC 2142 に従って abuse@ メールボックスを設けることに併せて、ウェブフォームも設けています。
abuse@ メールボックスに受けた要請が不明瞭な場合、ウェブフォームに誘導します。

ここが、実は外せない重要なポイント。

まず第一に RFC 2142 に準拠します。つまり、abuse連絡先のメールボックスが abuse の主たる窓口です。
ウェブフォームはウェブ検索で見つけられるように配慮し見つけやすくするが、「オーソリティーがあるのは abuse連絡先メールボックスだ」ということ。

聞くところの情報では、ある短文投稿型SNSの場合も、abuse連絡先に投稿についての相談を送るとウェブフォームに誘導する返答が来そうです。つまりそのSNS事業者もabuse窓口のメールを「ちゃんと確認している」とわかります。

逆にウェブフォームが見つかりにくい場合、阿鼻叫喚しか書かれていないメールがabuse連絡先に届いて聞き取りに苦労したり、電話や、突然の訪問をいただいたりします。

これらはウェブフォームに誘導する

- 実名報道された逮捕情報が今もある、釈放されたのに！　生活再建できない！
- 昔のグラビア写真が今もあって。今は子供もいるのに
- 通学先、職場、住宅写真を曝されて
- 子供の情報が流通してるんだ！いじめだ、止めてよ！
- 私の名前が書きこまれたんです
- 同人創作したマンガが配布されてる！委託販売してるのに！

abuse連絡先を設ける必要性（発展・珍しいabuse）

「abuse窓口にはこんなのも来る」発展形も挙げてみます。
毎日、あんまりにもabuse-abuseしすぎて脳みそバーンなもので、ごく最近の数か月に abuse@sakura.ad.jp で受信し印象に残ったもののみです。年単位では他にもいろいろあると思うのですが、どんどん忘れないと続かない仕事なので…

EU域内の警察から照会が来た

- EU域内の国から契約者情報の Disclosure Request が来た
- 日本はEUの法域ではないので、答える義務（権限）が無い
- 「『日・EU刑事共助協定』を参照し、日本の警察に捜査共助を要請して」と返答した

米国連邦裁判所を騙る詐欺が来た

- 米国連邦裁判所を名乗るメールが来た、ヘッダーを読むとおかしい、Government Imposter Scams と判断した
- 件名 “Court Order”，HTMLメール本文内の画像（何かの命令書？）が異常なURLにリンクしている
- abuse窓口は裁判とも関わりがある、如何にも「abuse窓口の人に開かせる」ことを狙うメールであるように見えた

OpenBugBounty から脆弱性情報が来た

- OpenBugBount https://www.openbugbounty.org/ から「このサイトに脆弱性が！」と情報提供が来た
- RFC 9116 (ウェブサイトの特定の場所にセキュリティに関する連絡先情報を記述する)が十分に普及していないから、上位プロバイダのabuse窓口に来るのだろうか？
- 提供を受けた情報を契約者に通知した

他組織に宛てるabuseがいっぱい来た

- 他組織に宛てるべきabuseが、宛先の誤りでいっぱい来た
- AS番号単位でabuseの宛先を設定し自動送信している様子
- 「それ、うちじゃないから」と指摘し宛先変更を求めた

- これらを見ると、「abuse窓口は、ハンドリングも窓口として提供する機能のひとつである」とわかります。断ったり、「うちじゃないよ」と返答することが重要です。返答が無いと、要請する人はフラストレーションを高めることになりそう、いや、なるはずです。
- EUからの照会では、「外国ではabuse窓口がこんな風に使われているんだ」と感心しました。

目次・構成（ここまでは準備運動です、既におなか一杯かもしれませんが）

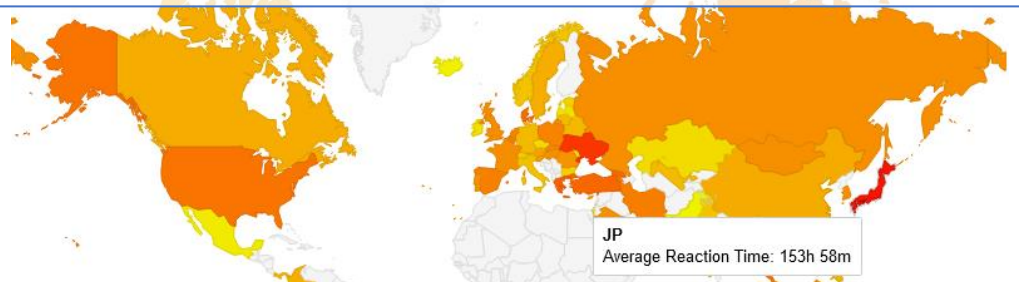
1. 「abuseとは何か」言葉の意味、オンラインabuseに関係するRFC 2142 の確認
2. 番号資源に対し abuse 連絡先窓口の設置を求める資源管理ポリシー、
   APNIC prop-079 とJPOPF p036-01 の確認
3. 実態としてabuse窓口に受ける連絡の紹介、
   実態から推し量る「様々な人に、abuse連絡先が必要とされている様」の説明
4. 外部から見た「日本のabuse連絡先窓口の評価」、
   「日本のabuse連絡先窓口の評価はとても低い」、なぜ低いのか？
   なぜ「日本のabuse連絡先」は見つけてもらえないのか？

本日の主菜

5. 「abuse窓口に連絡する」事のトレンドと、abuse窓口を担当して感じる将来展望
6. 「abuse連絡先を設ける」事の大変さ、「abuse連絡先窓口を運用する」大変さ
7. まとめ「なぜ日本のabuse連絡先は見つけてもらえないのか？」課題は何か
   課題解決へのファーストステップ「JPNIC whois に abuse 連絡先を登録して欲しい」
   「JPNIC whois への abuse 連絡先登録を促す良い施策はないものか？」

外部から見た「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/

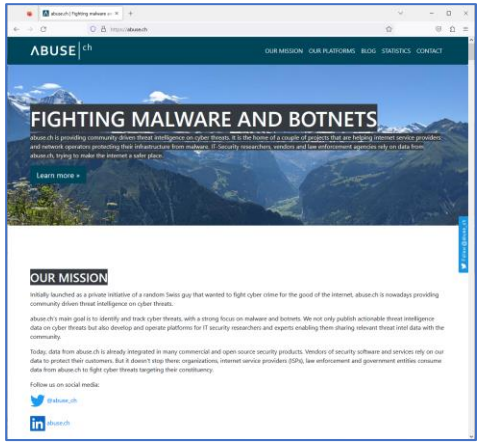


It shows that abuse desks in Ukraine (UA), Japan (JP) and Zimbabwe (ZW) tend to be slower than abuse desks located in e.g. Mexico (MX), Iceland (IS) or Pakistan (PK).

「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。」

このblogを書いた abuse.ch って、誰なの？　どんな組織なの？

「Abuse.ch の主な目標は、マルウェアとボットネットに重点を置いて、サイバー脅威を特定して追跡することです。当社は、サイバー脅威に関する実用的な脅威インテリジェンス データを公開するだけでなく、IT セキュリティ研究者や専門家が関連する脅威インテリジェンス データをコミュニティと共有できるようにするプラットフォームを開発および運用しています。」（サイトトップページの案内の一部を翻訳）



https://abuse.ch/

「日本は遅い」評価は相当だろうか？

abuse.ch がblogに挙げた6カ国の Average Reaction Time の具体的な値は？
その値は相当なのか、例えば各国の人口やGDPと比較した場合に、何かわかるだろうか？

国	Average Reaction Time (2018)	人口(2021)	GDP(2021, USD)	1人あたりGDP (2021, USD)
Ukraine (UA)	130h 06m	43,792,855	200.1B	4,835.6
Japan (JP)	**153h 53m**	**125,681,593**	**4,940.9B**	**39,312.7**
Zimbabwe (ZW)	167h 00m	15,993,524	28.4B	1,773.9
Mexico (MX)	07h 25m	126,705,138	1,272.8B	10,045.7
Iceland (IS)	02h 56m	372,520	25.6B	68,727.6
Pakistan (PK)	02h 04m	231,402,117	348.3B	1,505.0

人口/GDP/１人当たりGDPの値は世界銀行より https://data.worldbank.org/?locations=UA-JP-ZW-MX-IS-PK

メキシコはともかく他の４カ国は経済規模が違いすぎる、それに対応が早い国は政府や法執行機関による統制が厳しい自由度の指数の低い国かもしれない、経済規模が大きく自由度の指数も高いG7の場合はどうだろうか？

国	Average Reaction Time (2018)	人口(2021)	GDP(2021, USD)	1人あたりGDP (2021, USD)
Itary (IT)	35h 48m	59,109,668	2.11T	35,657.5
Germany (DE)	40h 51m	83,196,078	4.26T	51,203.6
Canada (CA)	49h 33m	38,246,108	1.99T	51,987.9
France (FR)	70h 00m	67,749,632	2.96T	43,659.0
United Kingdom (GB)	70h 54m	67,326,569	3.13T	46,510.3
United States (US)	88h 06m	331,893,745	23.32T	70,248.6
Japan (JP)	**153h 53m**	**125,681,593**	**4,94T**	**39,312.7**

人口/GDP/１人当たりGDPの値は世界銀行より https://data.worldbank.org/?locations=IT-DE-CA-FR-GB-US-JP

うわっ…私のabuse対応、遅すぎ…？

abuse.ch が blog に挙げた 6 カ国、G7, 何れと比較しても「日本は遅い」。
なら、「こんなにかかった」と主張する時間の根拠は何だろう？　「いつ」「どこのabuse窓口に」テイクダウンを要請し、「そしていつ」テイクダウンを確認したかのエビデンスはあるだろうか？

この点にも abuse.ch は配慮しており、例えば次のURL等で「abuseに当たる異常(malware, botnet)の情報提供を受けた日時」「プロバイダのabuse連絡先に連絡した日時とその宛先」「現在 online か offline か」を公開している。

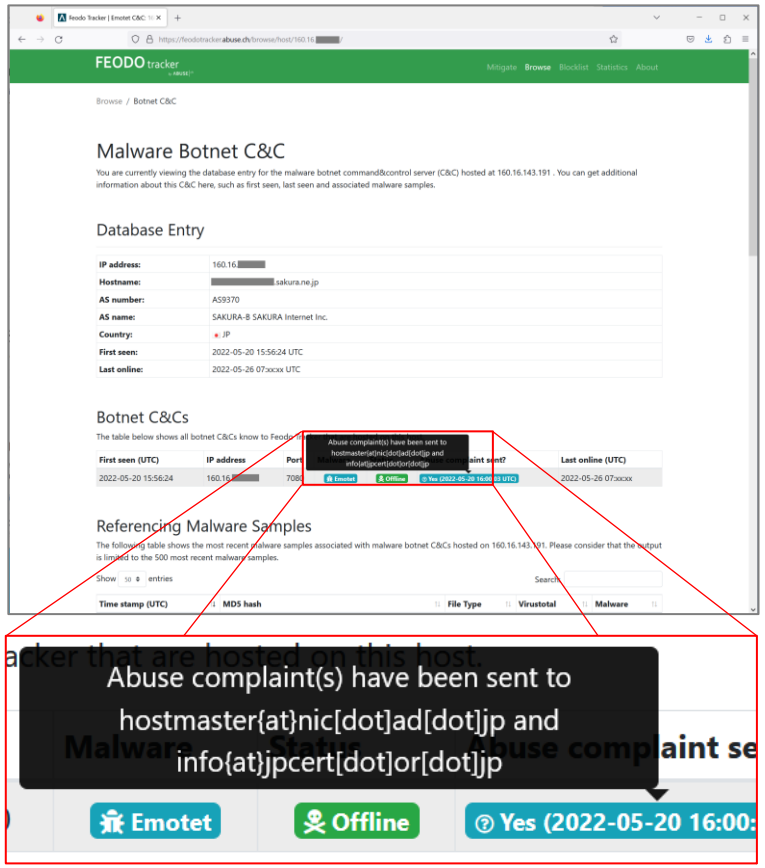
- https://urlhaus.abuse.ch/browse/
- https://feodotracker.abuse.ch/browse/

更にabuse.chは先のblogでプロバイダのabuse連絡先が見つからない問題を指摘するとともに、代替の選択肢として、プロバイダ側から情報取得することもできるようにAS番号単位のRSSフィードも提供している。

- https://urlhaus.abuse.ch/feeds/asn/9370/

AS9370の場合 abuse.ch は 「abuse{at}nic[dot]ad[dot]jp と info{at}jpcert[dot]or[dot]jp にabuse対応要請を送った」と言います。しかしAS9370が運用しているabuse連絡先は abuse@sakura.ad.jp です。「**日本の遅さ」は連絡の行き違いが原因**と受け止めます。

では**なぜ、連絡に行き違いが生じるのでしょうか。**



https://feodotracker.abuse.ch/

abuse連絡先を調べてみる（APNIC whois の場合）

```
$ whois 160.16.0.0

Found a referral to whois.apnic.net.

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '160.16.0.0 - 160.16.255.255'

% Abuse contact for '160.16.0.0 - 160.16.255.255' is 'hostmaster@nic.ad.jp'

inetnum:        160.16.0.0 - 160.16.255.255
netname:        SAKURA
descr:          SAKURA Internet Inc.
descr:          Tokyo Tatemono Umeda Building 11F,1-12-12,Umeda,Kita-ku,Osaka 530-0001 Japan
country:        JP
admin-c:        JNIC1-AP
tech-c:         JNIC1-AP
status:         ALLOCATED PORTABLE
remarks:        Email address for spam or abuse complaints : abuse@sakura.ad.jp
mnt-irt:        IRT-JPNIC-JP
mnt-by:         MAINT-JPNIC
mnt-lower:      MAINT-JPNIC
last-modified:  2021-10-15T02:53:12Z
```

「なぜ、abuse連絡の行き違いが発生するのか」調べてみます。

左は、JPNICから、さくらインターネットに割振りされているIPアドレスを、whoisサーバを指定せずwhoisコマンドで照会した例で、APNIC whois が表示されています。
160.16.0.0 を照会して、160.16.0.0/16 の情報が得られています。160.16.0.0/16 はプロバイダ集成可能アドレス（PAアドレス: Provider Aggregatable Address）です。

“Abuse contact for <SNIP> is ‘hostmaster@nic.ad.jp’” とあるので、素直に読めば、これがabuse連絡先だと解釈して自然です。

しかし、実際にこのIPアドレスを割振られた組織が運営しているabuse連絡先は abuse@sakura.ad.jp です。
これは下の remarks に表示されますが、「分かっている読み手」でないと、 remarks にはたどり着けなさそうです。

abuse連絡先を調べてみる（JPNIC whois の場合）

```
$ whois -h whois.nic.ad.jp 160.16.0.0

Network Information:
a. [Network Number]              160.16.0.0/24
b. [Network Name]                SAKURA-NET
g. [Organization]                SAKURA Internet Inc.
m. [Administrative Contact]      KT749JP
n. [Technical Contact]           JP00072233
o. [Abuse]
p. [Nameserver]                  ns1.dns.ne.jp
p. [Nameserver]                  ns2.dns.ne.jp
[Assigned Date]                  2014/08/27
[Return Date]
[Last Update]                    2014/08/27 05:47:03(JST)

Less Specific Info.
----------
SAKURA Internet Inc.
                        [Allocation]                        160.16.0.0/16
```

こちらは同じIPアドレスを JPNIC whois に照会した例です。
160.16.0.0 を照会して、160.16.0.0/24 の情報が得られています。160.16.0.0/24 は、160.16.0.0/16 の「PA割振り」アドレスから、使用するために「割当て」たIPアドレス（PA割当てアドレス）です。

o.[Abuse] は空欄です。
そして下に上位であるPA割振りIPアドレスブロックが表示されます。

この空欄の‘[abuse]’欄は、「『PA割当てアドレス』の『abuse連絡先』」です。

JPNIC地域に割り振られたPAアドレスの割当てアドレスと、PIアドレス(Provider Independent Address)、そしてAS番号にabuse連絡先が設けられたのは 2022年のことです。
2023年現在、これらの連絡先欄は空欄が多いと思われます。
（弊社も登録を頑張っている途中です）

abuse連絡先を調べてみる（JPNIC whois の場合）

```
$ whois -h whois.nic.ad.jp 160.16.0.0/16

Network Information:
[Network Number]                160.16.0.0/16
[Network Name]
[Organization]                  SAKURA Internet Inc.
[Administrative Contact]        KT749JP
[Technical Contact]             JP00072233
[Abuse]                         abuse@sakura.ad.jp
[Allocated Date]                2013/01/07
[Last Update]                   2022/06/08 10:30:26(JST)

Less Specific Info.
----------
No match!!
```

こちらはPA割振りアドレスである160.16.0.0/16 を JPNIC Whois に照会した例です。
こちらではabuse連絡先abuse@sakura.ad.jp が正しく得られます。

このように「PA割振りアドレスには正しいabuse連絡先が登録されて」いますが、「abuse連絡先を探す人が、この情報にまでたどり着けるか」は疑問です。

実務でも、whoisコマンドや、 JPNIC WHOIS Gateway(https://www.nic.ad.jp/ja/whois/ja-gateway.html)の印刷物を弁護士から受け取った例は思い当たりません。受け取るのはいつも「APNIC whois の結果が表示されている、APNICでもないどこかのウェブサイト」の印刷物です。
たぶん弁護士はレジストリなんて知らないし、whoisの事もよくわかっていません。whoisの調べ方が司法試験に出るとも思われません。
「詳しく知らなくても何とかなる仕組み」が必要です。

問題は何か

1. abuse 連絡先は、「公共における不適当なふるまい」に直面した多様な人々に必要とされている。
2. abuse.ch の場合、「hostmaster{at}nic[dot]ad[dot]jp に連絡した」と言っていた。
   彼らがこの連絡先をどこで得たか、おそらくAPNICと推測するものの、正確にはわからない。
3. APNIC whois は、JPNIC地域のIPアドレス（割振りと割当ての両方を含む）のabuse連絡先は「hostmaster@nic.ad.jp である」と返す。しかし**JPNICはabuseをハンドリングする組織ではない。**
4. IPアドレスのabuse連絡先は JPNIC whois で調べても空欄である。
   「PAアドレスに限れば、特にPA割振りアドレスを指定して調べることで」abuse連絡先は得られるが、abuse連絡先を必要とするすべての人にこの方法を求めることは現実的でない。
5. JPNIC地域に割当てられた番号資源（IPアドレスとAS番号）の正しいabuse連絡先は、JPNIC, APNIC, どこのレジストリにも登録されていない。どこにもないのだから、whoisであれ、RDAPであれ、どのような照会方法を用いても正しいabuse連絡先は得られない。
6. **どこにも正しい連絡先は登録されていないから、「正しい連絡先はこっちだ」と指摘も誘導も事も出来ない。**

- 導線を考えると、APNIC whois にJPNIC地域のabuse連絡先を表示させられると良いです。
  けれども「APNIC whois で表示させたいabuse連絡先」が既に登録されているレジストリがあるかと言うと、どこにもありません。
- 「JPNIC whois を調べれば正しいabuse連絡先が得られる」わけでもないので、「JPNIC whois で調べて欲しい」と要望する事もできません。

abuse連絡先を解決するその他のソリューション

abuse 連絡先を得ることのできる、こんなソリューションもあります。

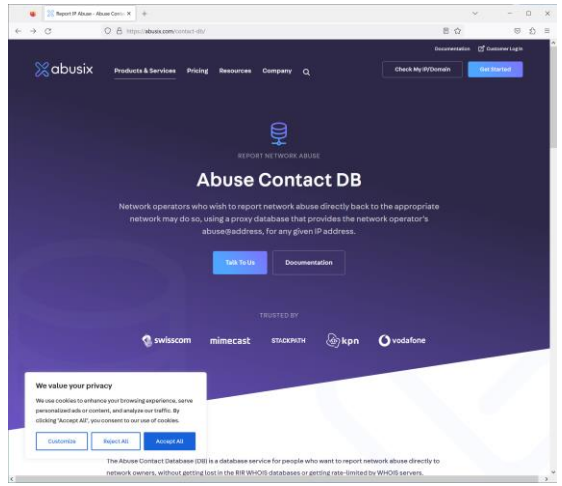
```
$ host -t TXT 1.0.16.160.abuse-contacts.abusix.zone.
1.0.16.160.abuse-contacts.abusix.zone descriptive text "hostmaster@nic.ad.jp"
```

```
$ pip install querycontacts
$ querycontacts 160.16.0.1
hostmaster@nic.ad.jp
```

それぞれabuse連絡先が abuse@sakura.ad.jp であるIPアドレス 160.16.0.1 について、abuse連絡先を照会した例です。**何れも abuse@sakura.ad.jp ではない連絡先を返します。**

このソリューションはドイツ Abusix GmbH が運営しています。彼らは「RIR(ARIN, RIPE, LACNIC, APNIC, AFRINIC)に登録されているabuse連絡先を返す、フェイルオーバーとして技術連絡先を返す場合もある」と説明しています。

このソリューションが返すのは単に「abuse連絡先のみ」です。abuse宛てに連絡するプログラムを作りたい時、このソリューションを使えば「whoisやRDAPの結果からabuse連絡先を抜き出す」処理が省けて便利です。
またこのソリューションはDNSを用いて作られているので、とても高速に動作することも長所です。



https://abusix.com/contact-db/

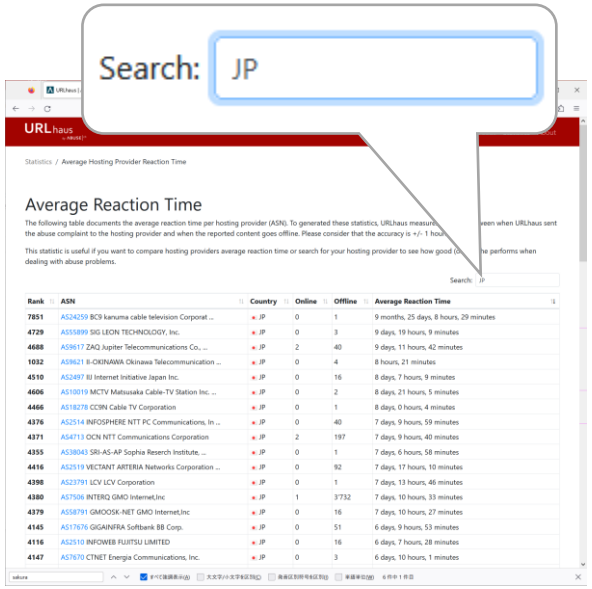
abuse連絡先は「本当に様々な場面で必要とされているのだろう」とわかります。

でも、「私の組織」にabuse連絡先が必要？

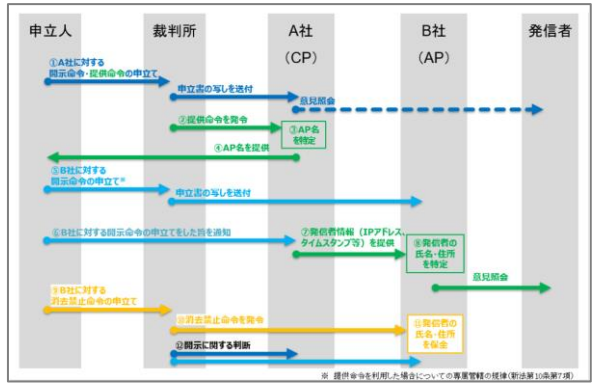
「でも、私の組織にabuse連絡先が必要ですか、abuse連絡先はホスティングや、クラウドサービスに必要とされているのではないですか」という疑問もあると思います。
これに違う材料を挙げてみます。

1. abuse.ch は、彼らが連絡した事のあるabuseデスクについて、彼らが計測した平均対応時間を公開しています。
   ”Average Reaction Time” のページで確認してみてください。
2. 発表者自身の業務でも、abuse連絡先を探して、対象は日本のIPアドレスであるにもかかわらず見つけられなかった体験が幾度となくあります。
   弊社を騙るフィッシングメール送信を止めたいと考えた時、不正アクセス元が暴露したIoT機器であると発見した時などでした。
3. 発信者情報開示命令事件では、発信者情報の提供命令を受けたコンテンツプロバイダは、発信者情報を有するアクセスプロバイダに対し、IPアドレスとタイムスタンプを提供することとされています。
   この時に、「具体的に、どこで探して得たどの宛先に提供するか」は、誰も、たぶん、よく分っていません。

上は発表者でも思い当たった材料であって、「abuse窓口が必要とされる程度」は、「将来、今は知らないabuseも起こりうる」以上、想像できません。
abuseは「公共における不適当なふるまい」と緩やかに定義されており、内容は時代とともに変わり得ます。abuse窓口に「いつ、誰が、何が起こって、連絡したいと考える得るか」は、資源管理者（IPアドレスを管理する人、 ASを運用する人）では判断できません。



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



別冊「発信者情報開示命令事件」に関する対応手引き
https://www.isplaw.jp/

目次・構成

1. 「abuseとは何か」言葉の意味、オンラインabuseに関係するRFC 2142 の確認

2. 番号資源に対し abuse 連絡先窓口の設置を求める資源管理ポリシー、
   APNIC prop-079 とJPOPF p036-01 の確認

3. 実態としてabuse窓口に受ける連絡の紹介、
   実態から推し量る「様々な人に、abuse連絡先が必要とされている様」の説明

4. 外部から見た「日本のabuse連絡先窓口の評価」、
   「日本のabuse連絡先窓口の評価はとても低い」、なぜ低いのか？
   なぜ「日本のabuse連絡先」は見つけてもらえないのか？

5. 「abuse窓口に連絡する」事のトレンドと、abuse窓口を担当して感じる将来展望

6. 「abuse連絡先を設ける」事の大変さ、「abuse連絡先窓口を運用する」大変さ

7. まとめ「なぜ日本のabuse連絡先は見つけてもらえないのか？」課題は何か
   課題解決へのファーストステップ「JPNIC whois に abuse 連絡先を登録して欲しい」
   「JPNIC whois への abuse 連絡先登録を促す良い施策はないものか？」

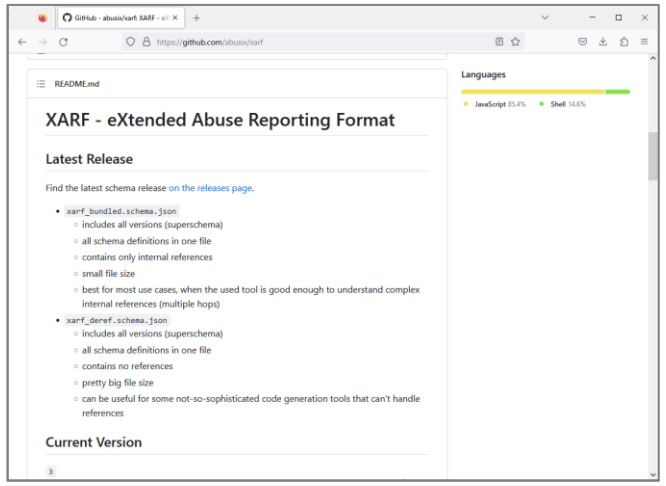
abuse窓口の将来展望（abuse窓口の担当者として感じている展望）

「abuse窓口に連絡する」事のトレンド

「abuse窓口に連絡すること」は自動化がトレンドです。

初期の自動化の試みは、RFC 6449 “Complaint Feedback Loop Operational Recommendations” (November 2011) から伺えますが、直近は X-ARF (eXtended Abuse Reporting Format) の開発が盛んな様子です。
Abuse Reporting に積極的な事業者、たとえば Netcraft や SpamCop が採用しており、またレポートを受ける側の事業者でも、たとえば DigitalOcean が「X-ARF形式のレポートを受け付ける」と言っています。
INHOPE（児童ポルノに対策する国際団体）も、「内部で X-ARF を使っている」と意見交換の場で話していました。

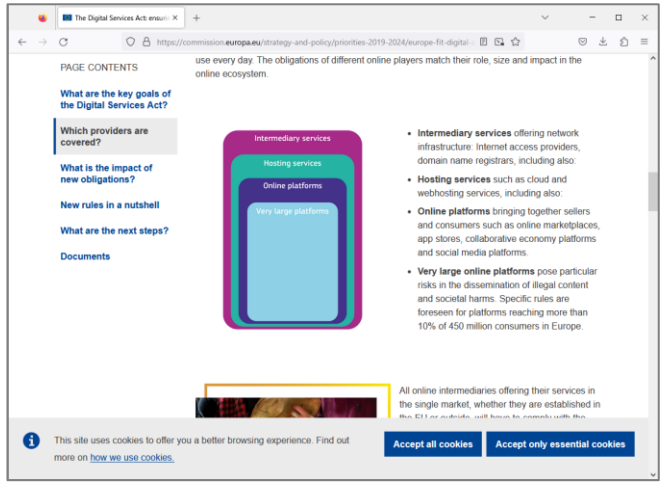
「abuseのひとつひとつにwhoisを引き、手でメールをタイプし、abuse窓口に連絡する」は人的資源の無駄です。馬鹿げていると私も思います。



https://github.com/abusix/xarf

担当して感じる将来展望

EU Digital Service Act は ISP, ドメインレジストラ、ホスティングから大規模プラットフォーマーまで、「連絡窓口を設けよ、透明性レポートを公開せよ」と求めています。
日本も総務省のプラットフォームサービス研究会にDSAを研究する資料や議論がありました。「abuse窓口等を設け、窓口を適切に運用し、対応についてレポートを公開する」事は、社会のあたりまえになって行くのでしょう。



https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

目次・構成

1. 「abuseとは何か」言葉の意味、オンラインabuseに関係するRFC 2142 の確認

2. 番号資源に対し abuse 連絡先窓口の設置を求める資源管理ポリシー、
   APNIC prop-079 とJPOPF p036-01 の確認

3. 実態としてabuse窓口に受ける連絡の紹介、
   実態から推し量る「様々な人に、abuse連絡先が必要とされている様」の説明

4. 外部から見た「日本のabuse連絡先窓口の評価」、
   「日本のabuse連絡先窓口の評価はとても低い」、なぜ低いのか？
   なぜ「日本のabuse連絡先」は見つけてもらえないのか？

5. 「abuse窓口に連絡する」事のトレンドと、abuse窓口を担当して感じる将来展望

6. 「abuse連絡先を設ける」事の大変さ、「abuse連絡先窓口を運用する」大変さ

7. まとめ「なぜ日本のabuse連絡先は見つけてもらえないのか？」課題は何か
   課題解決へのファーストステップ「JPNIC whois に abuse 連絡先を登録して欲しい」
   「JPNIC whois への abuse 連絡先登録を促す良い施策はないものか？」

abuse連絡先登録すんの、すんげー大変

「あなたの言う事は分かるよ、でも、そうは言っても、PIアドレス、PA割当てアドレス、すべてにabuse連絡先を登録するなんて、めちゃくちゃ大変、とても現実的とは思えないんだけど？」

はい、そうだろうと思います。
私は所属組織のLIR機能担当者ではありませんが、「とてつもなく大変だろう」とは想像しています。

- ISP, アクセス回線はIPアドレスがとにかく多い！（ヘイシャーのIPv4アドレスはたった１００万個）
- 小さなブロックに分割した割当ても、とにかく多い！
- 組織の合併や事業譲渡など、組織の歴史を反映した複雑なブロックになってる
- 予め、機械的に、容易に変更することを想定して作られたシステムではない
- etc...

AS番号はともかく、PI/PA割当てアドレスにabuse連絡先を登録するのは、それはそれは大変なのだろうと思います。
その上で「社会がabuse窓口を必要としている様」や、ここまでに説明した情報、２０年、５０年先の未来を想像して、考えてみて、と願います。

abuse窓口の担当者になると、すんげー大変

これは何しろ私自身が担当者なので、知っています。めちゃくちゃ大変です。
abuse窓口にはabuseしか来ません。とにかく罵られ、「必要とされるのに感謝はされない」です。
売上げを生まないので、組織的な支援が得られるかも、わかりません。

「どのくらい大変か」伝えるエピソードを二つ紹介します。

- RBL(Realtime Blackhole List, DNSBL)事業者の人とやり取りをした時、
  「返事遅れてごめん、僕は Anti-Abuse Desk の担当なんだ」と言った所、
  “I am sorry to hear how busy your role is - *sadly many anti-abuse desk workers would have a similar story*” と言われました。
  - RBL事業者は「SPAM止めろ！」と、様々な組織のabuse窓口担当者とコミュニケーションする機会を持つはずです。
    それだけに、この言葉には重みがあります。
- abuse窓口の同僚は「ここは野戦病院なんで」と言っていました。

新たにabuse窓口の担当になる方に向けて、担当者として言う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」「無理だと感じてしまったら、壊れる前に辞めよう」です。

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。

（本日、お話する機会をいたこと、JPOPF-ST, JPNIC, ご参加の皆様に感謝申し上げます）

目次・構成

1. 「abuseとは何か」言葉の意味、オンラインabuseに関係するRFC 2142 の確認
2. 番号資源に対し abuse 連絡先窓口の設置を求める資源管理ポリシー、
   APNIC prop-079 とJPOPF p036-01 の確認
3. 実態としてabuse窓口に受ける連絡の紹介、
   実態から推し量る「様々な人に、abuse連絡先が必要とされている様」の説明
4. 外部から見た「日本のabuse連絡先窓口の評価」、
   「日本のabuse連絡先窓口の評価はとても低い」、なぜ低いのか？
   なぜ「日本のabuse連絡先」は見つけてもらえないのか？
5. 「abuse窓口に連絡する」事のトレンドと、abuse窓口を担当して感じる将来展望
6. 「abuse連絡先を設ける」事の大変さ、「abuse連絡先窓口を運用する」大変さ
7. まとめ「なぜ日本のabuse連絡先は見つけてもらえないのか？」課題は何か
   課題解決へのファーストステップ「JPNIC whois に abuse 連絡先を登録して欲しい」
   「JPNIC whois への abuse 連絡先登録を促す良い施策はないものか？」

まとめ

- なぜabuse窓口を見つけてもらえないのか、正確な理由はわからない
- しかしそもそもJPNIC地域のLIRのabuse連絡先情報は、JPNICにも、APNICにも、どこにも整理されていない
- 条件考えずに理想を言えば、APNIC whois で番号資源を調べることで、JPNIC地域のLIRのabuse連絡先が得られると良い
  - JPNIC whoisに連絡先があれば、APNIC whois で表示するために連携（複写する・転写する・参照させる）する事も検討出来ないか
  - たとえ理想まで辿りつけなくても「JPNIC whois を見て」とは言えるようになる
- 問題提起しようにも、「JPNIC地域のLIRのabuse連絡先はどこにも無いじゃないか」と言われてしまってはぐうの音も出ない
- JPNIC whois でabuse連絡先が表示されるように登録して欲しい
  まず JPNIC へのabuse連絡先登録率を上げないと話が始まらない