# WHOIS abuse連絡先正確性向上の検討WG 中間報告

2019年11月27日（水）
WHOIS Abuse連絡先正確性向上の検討WG

# 目次

# 0. はじめに

# はじめに

世界的にWHOISのabuse問い合わせ先情報に対する正確性が問題となっており、APNICではprop-125がコンセンサスとなり2019/6より検査を開始している。

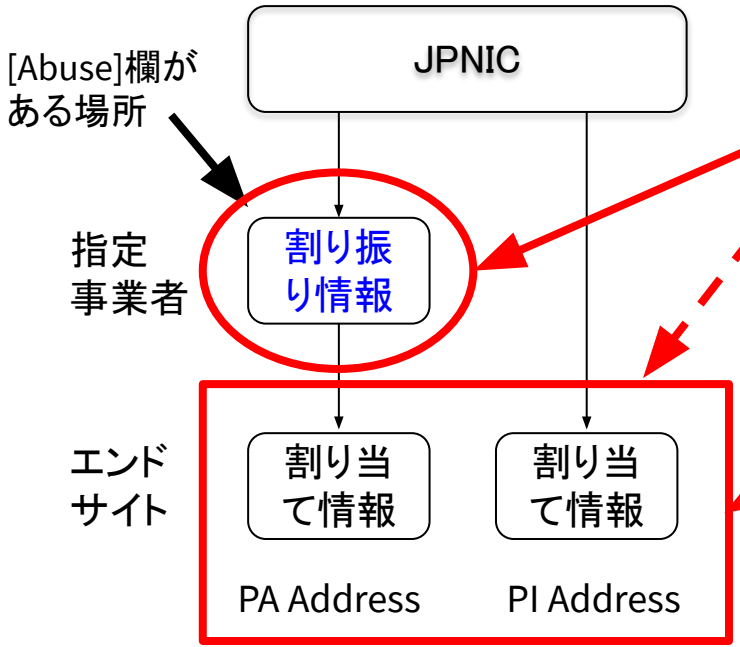
一方JPNICのWHOISでは、abuse問い合わせ先の登録があるのが割り振りアドレスのみで、PI/PA割当されたアドレスには項目自体が存在しない。またアドレス維持料等の支払担当者の連絡先では10%程度メールが不達となっており、abuse問い合わせ先の正確性についても懸念されるところである。

このような状況を受け、JPOPM36において、abuse問い合わせ先の検査手法と、PI/PAアドレスに対するabuse問い合わせ先項目追加の検討をワーキンググループを設置し実施する提案が提出され、コンセンサスとなった。

本書はワーキンググループのおける検討の中間報告をまとめたものである。

# 検討のスコープ

以下の 2つの検討を行う。




検討①
・Abuse連絡先メールを検証する
・WGを作り検証手段を検討する

検討②
・Abuse連絡先情報の追加を 検討する

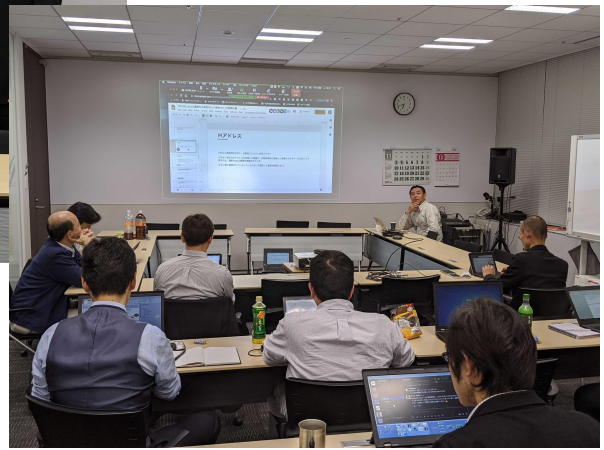
# ワーキンググループ検討メンバ

- 小林努/株式会社インターネットイニシアティブ　　（順不同・敬称略）
- 北口善明/東京工業大学
- 風間勇人/株式会社Geolocation Technology
- 但野正行/株式会社Geolocation Technology
- 外山慎一/ソフトバンク株式会社
- 銭宏皓/ソフトバンク株式会社
- 森川慶彦/株式会社KDDIウェブコミュニケーションズ
- 山下健一/さくらインターネット株式会社
- 吉岡渉/さくらインターネット株式会社
- 小川高扶弥/さくらインターネット株式会社
- 鶴巻悟/JPOPF運営チーム
- 谷崎文義/JPOPF運営チーム
- JPNIC IP事業部（オブザーバ）

# 活動履歴

| | | |
|---|---|---|
| 第1回WG | 2019年8月9日(金) | 目的確認・意識合わせ。ラフスケジュール作成 |
| 第2回WG | 2019年8月28日(水) | 現在のAbuse登録状況、海外での検査状況報告。<br>PI/PAアドレスへAbuse問い合わせ先追加可否について。 |
| 第3回WG | 2019年9月18日(水) | PAアドレスへAbuse問い合わせ先追加可否について。 |
| 第4回WG | 2019年10月9日(水) | PIアドレスへのAbuse問い合わせ先追加可否について。<br>アドレスの検査手法について |
| 第5回WG | 2019年10月30日(水) | Abuse項目が空白の場合の対応について。<br>アドレス検査手法について。 |
| 第6回WG | 2019年11月20日(水) | 中間報告に向けたとりまとめ。 |
| JPOPM37 | 2019年11月27日(水) | 中間報告発表 |


WHOIS abuse
連絡先正確性向上
検討WG
ミーティング



# 1. PI/PAアドレスに対するabuse問い合わせ先情報の追加

# 割り振りアドレスにしかabuseがない理由

2003年　JPNICのIPv4アドレス割り振りルールの変更

　JPNIC独自アドレスプールから割り振り　→　APNICとの共通アドレスプールから割り振り

これと同時にWHOIS登録項目もAPNICの基準に従うことになった。

APNIC WHOISでは当時よりabuseがあったため、それに伴い登録項目を追加した。

この変更はあくまでも「**割り振り**」のみに適応されたので、「**割り当て**」の場合はabuseの登録項目がないまま、現在に至っている。

# 考慮すべき事項

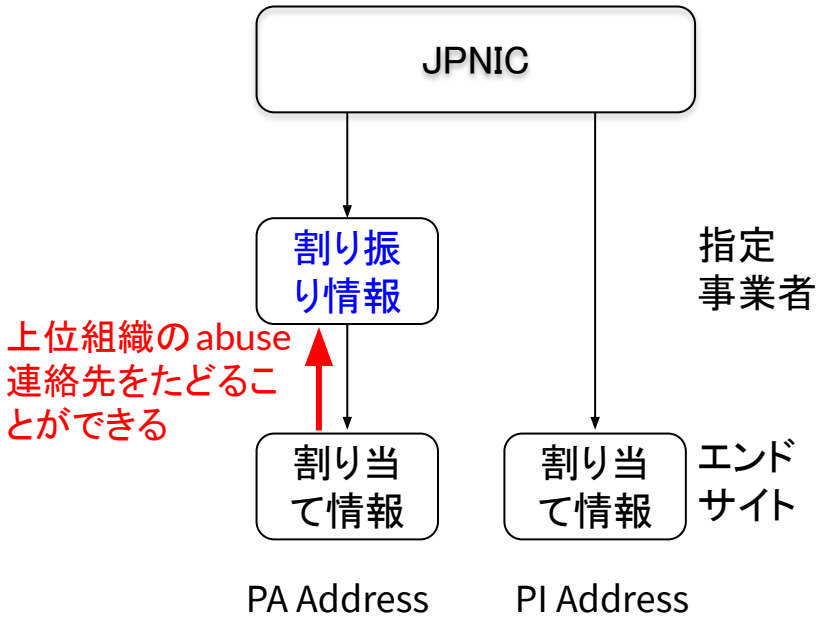
1. 割り当てアドレスに対してabuseを登録するかどうか
    - PIアドレスに対して登録をするか
    - エンドユーザに割り当てられたPAアドレスに対して登録をするか
2. abuseのない既存レコードをどうするか
    - 新ルールの施行までに登録を義務付ける
    - 新ルール施行後、レコード更新時に登録を義務付ける
3. abuseレコードに何を登録するか
    - E-mailアドレス
    - JPNICハンドル/グループハンドル
4. 登録内容の正確性をどう担保するか
    - 何もしない
    - JPNICから確認メールを送信する
    - JPNICから確認メールを送信し、返信を義務付ける
    - その他

# PIアドレス(1)

PIアドレス(Provider Independent Address/プロバイダ非依存アドレス)

議論整理:

- IPアドレス数ベースでPI:PA≒1:2
  - 議論から除外するには数が多すぎる。
- PA情報にabuse窓口があり、PI情報に無いのは本質的におかしい。
- 最新abuse情報の登録は行うべき。
- JPNICと直接契約があり、比較的コンタクトが取りやすい。
- 朔及して登録させることは非現実的。
  - JPNICから呼びかけ出来るが効果は不明。
  - 大半は一度だけIPアドレスを取得した組織で、初期取得時に登録した情報のままのケースが多いと予想される。



# PIアドレス(2)

PIアドレスにAbuse問い合わせ情報を追加する場合の課題:

- 割り当て済PIアドレスの abuse 情報の追加について
  大半は一度だけIPアドレスを取得した組織で、初期取得時に登録した情報のままのケースが多いと予想される。
  - 更新が行われるまで、同割り当て IPアドレスの技術連絡担当者の内容をコピー。
  - 対応をPAアドレスと統一するか？（後述）

# PAアドレス(1)

Abuse問い合わせの現状:

- Abuseの問い合わせはそれなりにある
- ただし、割り振りブロックのwhois DBに登録されている[abuse]フィールドを参照して問い合わせてきているのかは不明
    - Traceroute などの途中経路上の ISPや、Webサイトの情報等でコンタクトしてきている場合も。
    - 弁護士などの場合は、代表電話番号などに直電も。

割り当てIPアドレスにもAbuse問い合わせ情報を追加する場合の課題:

- ユーザ割り当ての場合、すでに割り当て済みのIPアドレスに対しても登録必須となる場合、既存顧客数百(多い指定事業者だと1,000件以上)の顧客に追加を依頼するのは非現実的
    - 事業者の業務量、お客様へ Abuse問い合わせ情報の内容説明などを考えると。。。
- 事業者によっては、事業者の問い合わせ先を代理で登録して、事業者内の顧客情報等を用いてお客様へ転送できるような登録方法でも良いのでは？
    - 割り振りブロックの [abuse]への問い合わせや、tracerouteの途中経路上の ISPに問い合わせがくる現状と同じ

# PAアドレス(2)

割り当てIPアドレスにもAbuse問い合わせ情報を追加する場合の課題:

- 現状のWeb UIだけだと、更新のために人手が必要。Abuse情報登録を期に、追加更新用APIを実装してもらいたい
  - 現状、whois DBは、割り当て組織が JPNIC whois DBを直接編集することはできず、指定事業者が専用 Web UI経由で入力する必要があるため。
- Abuse情報の更新を簡便にするため、割り当て情報毎の[abuse]フィールではなく、ハンドルで登録できるようにしてほしい
  - [管理者連絡窓口 /Administrative contact] や [技術連絡担当者 /Technical contact] と同じ内容にするときにハンドルだと登録が簡単。また、更新もハンドルの内容更新で対応できる。
  - また、インフラ割り当てでも一斉に更新できる。
- Abuse 情報についてのみ問い合わせ先の有効性確認が行われるようになると、お客様からの問い合わせも増加するかも

# PAアドレス(3)

割り当てIPアドレスにもAbuse問い合わせ情報を追加する場合の課題:

- 割り当て済IPアドレスのabuse情報の追加について
  既存の割り当て先のwhois DB情報を更新するまでには相当な時間がかかると想定される
  - 追加/更新が行われるまで、abuseフィールドをどのように取り扱うべきか
    i. 空白(情報なし)
    ii. 同割り当てIPアドレスの技術連絡担当者の内容をコピー
    iii. 上位組織(割り振り事業者)の abuse問い合わせ先をコピー

  どの対応も一長一短がある。対応を統一するか、指定事業者毎に選択できるようにするか、も課題。

WGメンバーとしては、PAアドレスの各割り当て先の情報にも個々の abuseフィールドを導入することはやむを得ないと考えるも、課題に対してどう対応するべきかは、まだ検討・議論中です。

# 「空白」のabuse問い合わせ先　まとめ

| | PIアドレス | | PAアドレス | |
|---|---|---|---|---|
| | Pros. | Cons. | Pros. | Cons. |
| 空白のまま | 特別な対応が不要 | 明示的にabuse対応を行っていないと受け止められかねない | 特別な対応が不要 | 明示的にabuse対応を行っていないと受け止められかねない |
| 技術担当者 | 現状と変わらないと思われる | 本来のabuse問い合わせ先か不明 | 現状と変わらないと思われる | 上位組織の稼働の増加。<br>本来のabuse問い合わせ先か不明 |
| 上位組織のabuse | 上位組織なし | 上位組織なし | 正しいabuse対応が期待できる | 実態とそぐわない。<br>上位組織の稼働の増加。 |

# 追加される項目の登録内容について

- **登録されたabuse情報はWhois上でどのように表示するべきか**
  - メールアドレスを直接記載している他の項目と統一し、ハンドルとすべきではないか
  - ハンドルとすれば、登録アドレスの変更が容易になる（登録prefix単位での変更が不要）
  - ハンドル情報の内容を再度取得する手間が掛かり、可読性も低い
  - スクリプトを作成し機械的通報を行っている場合も多く、サイバーセキュリティ的観点から は機械的に取得･操作しやすい形式を採用するのが望ましい

**ハンドル表示とした場合、WHOISの表示結果にメールアドレスが直接表示されないため、可読性や一覧性を損なわないような構成にする必要がある。**

# WHOISの表示について

IPアドレス情報を検索した際、割り振りアドレスはabuse欄があり容易に問い合わせ先を確認できるがPI/PAではハンドルのみが表示されることになり、一覧性を欠くことになる

また既存の登録レコードに関しては、実装当初abuse欄が空白となるため、特に海外から日本はabuse対応に消極的といった誤解を招きかねない

以上のことからWHOISの検索結果の表示について以下のような変更を行うことが望ましい

- **空白の際には、代替問い合わせ先への導線となる情報(上位組織情報等) を表示させる**
- **検索時に紐づくハンドルの内容も同時に表示させる(APNICのIRT objectのようなイメージ)**

# APNICにおけるWHOISの表示例

```
% Abuse contact for '192.168.1.0 - 192.168.1.255' is 'abuse@examplnet.com'
もしくは
% No abuse contact registered for  '192.168.1.0 - 192.168.1.255'

inetnum:        192.168.1.0 - 192.168.1.255
netname:        EXAMPLENET-AP
descr:          Example net Pty Ltd
country:        AP
admin-c:        DE345-AP
tech-c:         DE345-AP
status:         ASSIGNED PORTABLE
mnt-by:         MAINT-EXAMPLENET-AP
mnt-irt:        IRT-EXAMPLENET-AP
last-modified:  2018-08-30T07:50:19Z
source:         APNIC

irt:            IRT-EXAMPLENET-AP
address:        123 Example st.
address:        20097 Exampletown
address:        Australia
phone:          +12 34 567890 000
fax-no:         +12 34 567890 010
abuse-mailbox:  abuse@examplenet.com/*  */
admin-c:        DE345-AP
tech-c:         DE345-AP
auth:           PGPKEY-80FFBF15
remarks:        emergency phone number +12 34 567890 333
remarks:        timezone GMT+10 (GMT+2 with DST)
remarks:        https://www.examplenet.com
remarks:        This is a TI accredited CSIRT/CERT
irt-nfy:        notify@examplenet.com/*  */
mnt-by:         MAINT-EXAMPLENET-AP
source:         APNIC
```

Inetnum-Object

IRT-Object

- まず最初にabuse情報の有無が表示される
- Inetnum-Object内には紐づくIRT-Object名を表示
- abuse情報はIRT-Object内のabuse-mailbox項目に表示されるがInetnum-Objectの情報とセットで表示される為、直感的可読性は高い

# 2. メールアドレスの正確性検査について

# 海外における取り組み状況

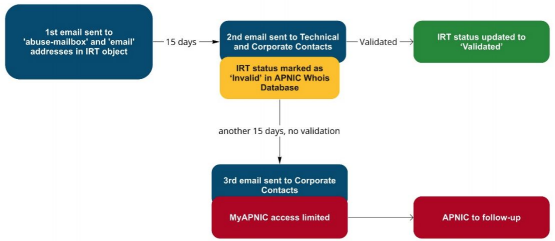
| RIR | 検証項目 | 検証方法 | 罰則規定 | 実施状況 |
|---|---|---|---|---|
| ARIN | PoCの連絡先情報 | 年1回メールを送信し、60日以内に受信確認・情報の更新を行う | あり<br>(新規申請の制限) | 実施済み |
| RIPE NCC | “abuse-mailbox”に登録された連絡先情報 | 最低年1回メールを送信し、受信確認を行う | なし | 2019/1開始 |
| APNIC | IRTオブジェクトに登録された連絡先 | 内容の更新もしくは6ヶ月ごとにメールを送信し受信確認を行う | ポリシー提案では新規申請を制限 | 2019/6開始 |
| AFRINIC | IRTオブジェクトに登録された連絡先 | | | 継続議論中 |
| lacnic | IRTオブジェクトに登録された連絡先 | | | 継続議論中 |

CNNIC(中国)やIDNIC(インドネシア)でも、同様の取り組みを準備もしくは実施中。

# APNICにおける検査実施手法

**prop-125: Validation of “abuse-mailbox” and other IRT emails**

- Implemented from 30 June 2019
  - All email addresses in IRT objects
  - Validation process by a human
- Frequency
  - Every time the object is updated
  - Validated at least every six months
- Demonstrate abuse mailbox
  - Is monitored by a human
  - Is responsive to legitimate reports
- Failure to validate
  - After 15 days object is marked invalid in whois
  - After 30 days limited access to MyAPNIC






- IRT-Object内の”abuse-mailbox”,”abuse”宛にメールを送信
  - メール内に検証用URLが記載
  - URLをクリックするとMyAPNICの認証となり、認証通過後ボタン押下で検証完了
- 15日以内に反応しない場合、WHOISの検索結果に”Invalid”と表示される
- 30日以内に反応しない場合、MyAPNICの機能制限

https://conference.apnic.net/48/assets/files/APIC778/implementation-update.pdf

# 海外の手法における懸念点

## 検査手法

- 到達確認メールに記載した検証用URLをクリックすることにより確認を行う(APNIC　RIPE)
  【懸念点】abuse連絡先確認を装ったフィッシングメールが発生する可能性がある。

- 到達確認メールへのメール返信
  【懸念点】どのIPアドレスに対する返信なのか、どのハンドルに対する返信なのかを判断する必要がある。

## 確認がとれない場合の罰則

- 管理画面の機能制限(My APNIC　ARIN Online)

  【懸念点】Webシステムの利用制限などの罰則規定は、特にPI/PAフォルダーに対しては無意味。

# 確認手法

- 複数の割り当てネットワークに同一の連絡先が設定されている場合は、送信するメールは1通。

- Abuse連絡先に対してメールでの到達確認のみを行う。
  到達とはUSER UNKNOWN等のエラー応答がないものであり、Abuse連絡先からの返信は求めない。応答がない=到達したものと考える。

- メール文面には到達テストであり返信不要である事の記載を行う。

上記方法で確認を実施し、経年変化を確認する。状況が改善されない等の問題が確認された場合は、別途JPNICにて対応策を検討する（WGの再開と善後策の検討など）

【議論された事項など】

- 該当アドレスをblackhole化している場合はどうなるか。
  →現状では到達したものと判断される。Abuse連絡先は、今回新規で登録される項目の為、意図的にBlackholeに落とすようなアドレスを指定する可能性は低い。

# 到達確認が取れない場合の対応

【本WGにて合意した内容】

- JPNIC が届かなかった組織に個別連絡をとる。
- 確認メールが届かない abuse連絡先には「空白」又は「不正」などの記載を入れる。
- 到達確認がとれなくても罰則を設けない。
- 確認は年に一回。
- 到達確認が取れない場合、リトライは 2週間後。

【議論された事項など】

- Abuse を連絡したい立場としては、その連絡先が生きているか死んでいるかのみを知りたい。
- Abuse窓口で届かない場合は、繰り返し送り、更に別の窓口に届く。返信はしないが仕事を行う事業者も多い。
- PA の割り当て先に罰則を作っても効果が無いのではないか。 → 割り振り組織に任せる。
- PI に対して到達確認がとれない場合は、 JPNIC にて対応する。
- Name サーバーの Lame のようにすることは可能。ただし開発が必要になる。
- 確認メールが届かない abuse連絡先には「空白」又は「不正」とする案もある。
  → これを実施する場合は、規則に明記するなどが必要。

# 3. まとめ

# 実装すべき事項

- PIアドレスのwhoisにabuse連絡先を設ける。登録方法は議論中。

| | | |
|---|---|---|
| 方法 | abuse連絡先新規登録を依頼 | 既存の技術担当者連絡先をコピー |
| 課題 | 十分な周知期間が必要<br>IPアドレスの新規割り当て・変更のない場合、<br>登録情報を更新するきっかけが乏しい | 十分な周知期間が必要<br>技術担当者が法的知識を十分に有すとは限らない<br>日常的にメール確認しているか不明 |

- PA割り当てアドレスのwhoisにabuse連絡先を設ける。登録方法は議論中。

| | | | |
|---|---|---|---|
| 方法 | abuse連絡先新規登録を依頼 | 既存の技術担当者連絡先をコピー | 空白を許容し、上位組織のabuse連絡先を表示 |
| 課題 | 全PAアドレスの登録徹底は非常に困難<br>割り振り元組織の判断に委ねる必要がある | 複写するメールアドレスが現在有効か不明<br>割り振り元組織の判断に委ねる必要がある | 「上位組織のabuse連絡先を表示」するための開発が必要<br>上位組織にabuse対応の負担発生の恐れ |

表示形式について

- abuse連絡先は管理者 /技術担当者連絡先と同じくJPNICハンドル/グループハンドルを使用する
- whois検索時、abuse連絡先ハンドル内容を APNIC whois の IRT-Object 相当に同時に表示させる仕様とする

# JPNICにおける実装について

IPアドレスwhoisに以下の開発が必要、かかる開発難易度を継続調査

- PIアドレスにおいてAbuse連絡先が空白だった場合に、技術担当者への問い合わせを促す等の記述を表示させる機能
- PAアドレスにおいてAbuse連絡先が空白だった場合に、上位組織のabuse連絡先情報を合わせて表示させる機能
- Abuse連絡先の到達確認ができなかった場合に、到達性が無いことを示す機能

Abuse連絡先の確認方法

- Abuse連絡先メールアドレスにメール送信し到達確認のみ行う・人為確認しているか否かは確認しない

以下の場合にスパム学習される可能性があるが、ユニークメールアドレス単位で到達確認すること、数十万・数百万単位で送信するメールではないことから、可能性は低いと考える

- 同一ドメインの異なるアドレスが多数abuse連絡先に登録されている場合
- 異なるドメインのアドレスが多数同一のメールサービス・メールサーバに存在する場合