WHOIS ABUSE連絡先正確性向上の検討
最終報告書

2020年3月25日

WHOIS ABUSE連絡先正確性向上の検討ワーキンググループ

目　次

0. はじめに

世界的にWHOISのAbuse問い合わせ先情報に関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年6月より検査を開始している。

一方JPNICのWHOISでは、Abuse問い合わせ先情報の登録のあるIPアドレスは割り振りアドレスのみで、PI/PAアドレスにはAbuse問合せ先情報を登録する項目自体が存在しない。またJPNICからアドレス維持料等の支払担当者のメール連絡先に連絡した事例では10%程度のメールが不達となっており、同様にして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、2019年6月に開催されたJPOPM36[1]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問い合わせ先情報項目追加の検討を、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。

本書は本ワーキンググループにおける検討の結果をとりまとめたものである。

[1] 提案内容は以下のリンクを参照。http://www.jpopf.net/p036-01/

1. ワーキンググループの体制及び検討のスコープ

1-1 ワーキンググループの体制

JPOPM36におけるコンセンサスを受け、JPOPF運営チームがワーキンググループメンバの公募を実施し、応募者及びJPNIC(オブザーバ)にて検討を実施した。ワーキンググループの体制は以下の通りである。

体制表(氏名五十音順・敬称略)

鶴巻 悟(主査)	JPOPF運営チーム/BBIX株式会社
小川 高扶弥	さくらインターネット株式会社
風間 勇人	株式会社Geolocation Technology
北口 善明	東京工業大学
小林 努	株式会社インターネットイニシアティブ
銭 宏皓	ソフトバンク株式会社
但野 正行	株式会社Geolocation Technology
谷崎 文義	JPOPF運営チーム/西日本電信電話株式会社
外山慎一	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
JPNIC IP事業部・技術部(オブザーバ)	-
豊野 剛(事務局)	JPOPF運営チーム/日本電信電話株式会社

中川 あきら(事務局)	JPOPF運営チーム/日本インターネットエクスチェンジ株式会社(JPIX)

ワーキンググループ開催実績

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。 PI/PAアドレスへの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アドレスへの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。 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。 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。
第7回WG	2019年12月16日(月)	今後の進め方、スケジュール確認。
JANOG45	2020年1月24日(金)	中間報告書サマリ発表。
第8回WG	2020年2月13日(金)	JANOG45発表ののフィードバック。 今後のスケジュール確認。

1-2 検討のスコープ

JPOPM36における提案資料に記載の通り、ワーキンググループの検討のスコープは以下の通りである。

- JPNIC WHOISデータベースに登録されたAbuse問い合わせ先情報の項目に対する正確性検査の実施方法。
- 現在のJPNIC WHOISデータベースではAbuse問合せ先情報の項目が存在しない割り当てアドレス(JPNICから直接エンドサイトに割り当てされたアドレス(PIアドレス)及びIP指定事業者からエンドサイトに割り当てされたアドレス(PAアドレス))に対して、新規にAbuse問い合わせ先情報の項目を追加すべきか。

2. 検討結果

ワーキンググループでは検討の結果、以下にあげる事項について実装することが望ましいと判断した。
なお下記判断の根拠等については3項以降にまとめる。

2-1 PI/PAアドレスに対するABUSE問い合わせ項目の追加について

(1) PIアドレス及びPAアドレスの資源レコードにAbuse問い合わせ先情報の項目を追加する。

(2) 既登録済みの上記資源レコードのAbuse問い合わせ先情報の初期値は空白のままとし、追加申請等の機会にJPNICより登録を促す。

(3) Abuse問い合わせ先情報に登録する内容は、JPNICハンドルまたはグループハンドルとする。

(4) (2),(3)により、IPアドレスに対するWHOISでの検索結果のみではAbuse問い合わせ先メールアドレスが表示されないことから、当該検索結果内に含まれるハンドル情報について現状の検索結果に引き続いて表示されるようにする。

(5) 以上の変更は、割り振りアドレスにも適用する。

2-2 ABUSE問い合わせ先情報の検査について

(1) 検査は該当アドレスに対してメールを送信し、不達等のエラーメールが返ってこないことを確認することで行う。海外レジストリが実施している確認用Webサイトへのリンクを記載する方法は、フィッシングを誘発する可能性があるため実装しない。

(2) 複数の「ネットワーク情報」のAbuse問合せ先情報に同一のJPNICハンドルまたはグループハンドルが登録されていた場合は、1つのJPNICハンドルまたはグループハンドルにつき1通のみメールを送信し、メール本文内に管理するネットワーク情報一覧を記載する。

(3) メール本文には検査用メールであること、返信等の対応は不要である旨を記載する。

(4) 検査を実施していく中で、検査精度等に疑義が生じた場合はその都度検査方法等を見直すことが望ましい。

3. 国内外における現在の状況

3-1 JPNICが管理するIPv4アドレスの割り振り/割り当て状況

JPNICより割り振られたIPv4アドレスは約1億アドレスが存在し、内、Abuse問い合わせ先情報の項目にメールアドレスの登録のあるものは99%以上となっている。

またPIアドレスは、約5000万アドレスが割り当て済みとなる。

PAアドレスは、その性質上自社インフラに割り当てられるものと、顧客へ割り当てられるものがある。前者は割り振り情報に登録された組織と割り当て先組織とが同一のためAbuse問い合わせ先の登録が容易であるが、後者は異なる組織となるためAbuse問い合わせ先を一律に登録することは相応でないと考えられる。自社割り当て(インフラ割り当て)と顧客割り当て(ユーザ割り当て)の比率は不明であるが、割り振りアドレスのうち相当数のアドレスが顧客割り当てとなっていることが想定される。

上記をまとめると、

割り振り/割り当てアドレスのうち、Abuse問い合わせ先情報の登録がないものは、

- 割り振られたアドレスの内、Abuse問い合わせ先情報の登録がないもの
- PIアドレス
- PAアドレスのうち、顧客に割り当てられたもの

であり、その総数はJPNICで管理するIPアドレス全体の三分の一以上、少なくとも半数以上存在することが予想される。

3-2 海外レジストリにおける状況

JPNICの上位組織であるAPNICを含め、海外レジストリでは先行してAbuse問い合わせ先情報の検査が実施されている。以下にその状況をまとめる。

3-2-1 APNIC

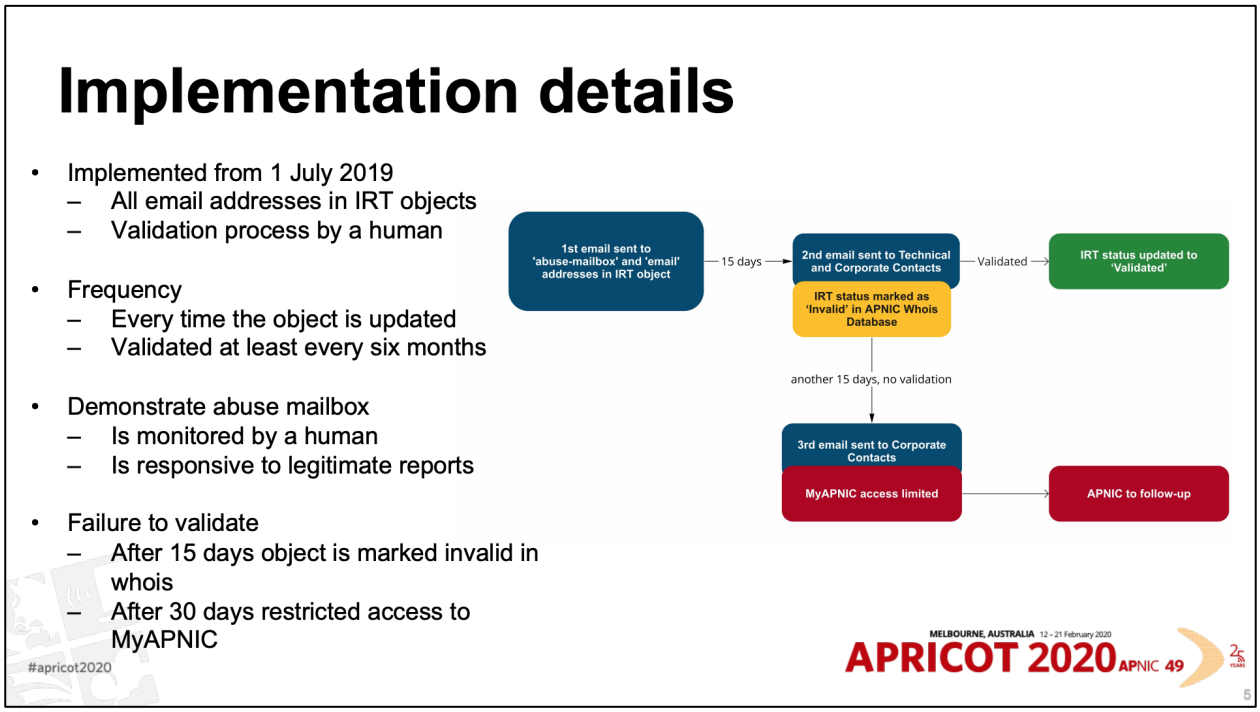
IRT Object[2]内の"email"および"abuse-mailbox"に登録されたメールアドレスを対象に検査を実施するポリシー(prop-125)が2018年に制定され、2019年6月より検査が開始された。

[2] JPNICにおけるJPNICハンドル/グループハンドルに相当するAbuse問い合わせ情報を記載するためのオブジェクト。

検査では、対象メールアドレスに宛てて登録情報の確認・変更用のURLが記載されたメールを送信する。このURLのページはMyAPNIC[3]内に存在するため、メールを受信した者はMyAPNICのアカウントを使用してログイン後、確認・変更を行うこととなる。

送信後15日間反応がない場合、admin-cおよびtech-c[4]宛に同様のメールを送信するとともに、IRT Object内の”email”および”abuse-mailbox”に”Invalid”が追記される。

さらに15日間反応がない場合、MyAPNICの機能が制限され、APNICスタッフによる確認が実施される。



APNICにおける検査プロセス

3-2-2 ARIN

Abuse Contactの正確性を検証するポリシー(ARIN-2017-3)[5]が2018年に制定され、年に1回検証が実施されている。Abuse問い合わせ先にメールを送信することで検証を実施しており、反応が無い場合にARINスタッフによる検討が行われた後、ARIN Online[6]での機能制限がかかると共に、WHOISの検索結果で当該Abuse Contactが”Invalid”である旨が表示されるようになる。

---

[3] JPNICにおけるWeb申請システムに相当するオンライン申請システム。

[4] それぞれ、JPNICにおける管理者連絡窓口、技術連絡担当者に相当。

[5] https://www.arin.net/vault/policy/proposals/2017_3.html

[6] JPNICのWeb申請システムに相当するオンライン申請システム。

また、再割り当て等の申請時に、正確な問い合わせ先情報が登録されていない場合には申請が差し戻されるポリシー提案(ARIN-2017-12)[7]が承認され、現在実装待ちとなっている。

ARIN-2017-3における検査プロセス

3-2-3 RIPE NCC

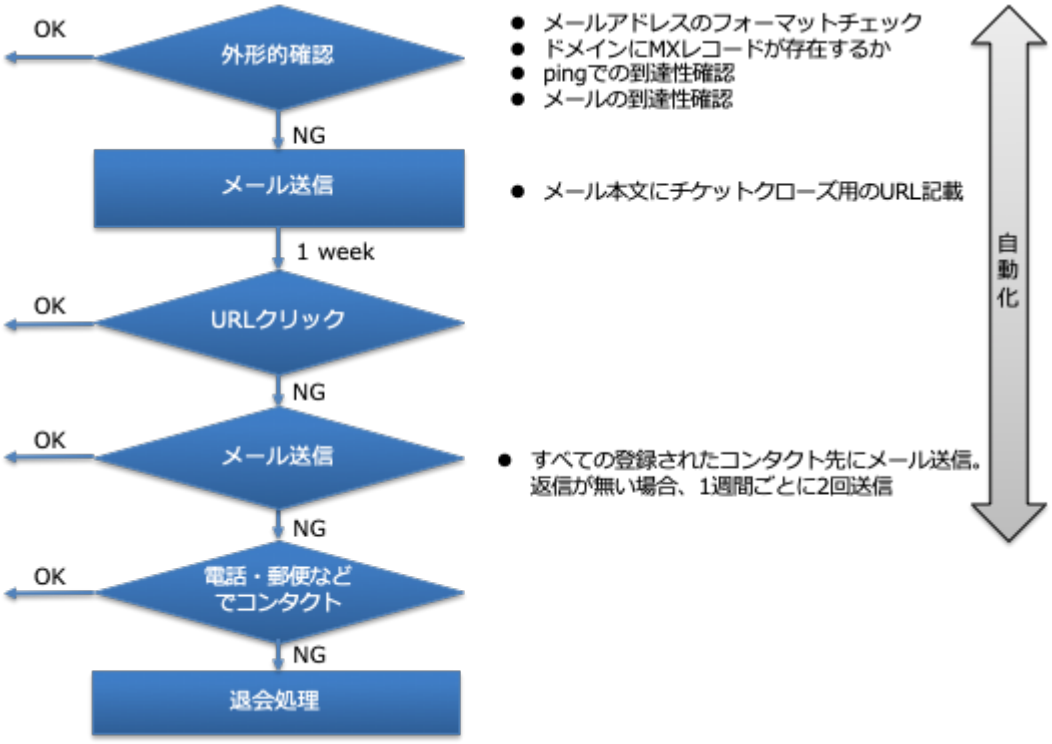
2018年に最低年1回、Abuse問い合わせ先に対する検査を実施することを定めたポリシー(RIPE-705)[8]が制定された。その検査手法は、まず初めにAbuse問い合わせ先メールアドレスのフォーマットや到達性などの外形的確認を行い、異常が認められたメールアドレスに対してメールを送信し、メール受信者がメール本文内のURLを開いたことの確認を以って正確性を確認するというものである。

現在問い合わせ先メールアドレスの正確性を高め、受信者がAbuse対応を実施する適切な人員であることを確認することを目的とした修正提案(2019-04)[9]が議論されている。

[7] https://www.arin.net/participate/policy/drafts/2017_12/

[8] https://www.ripe.net/publications/docs/ripe-705

[9] https://www.ripe.net/participate/policies/proposals/2019-04



RIPE-705における検査プロセス

3-2-4 APNIC配下のNIR

2019年9月に開催されたAPNIC48 NIR SIGにおいて、CNNICより3-2-1で記載したAPNIC prop-125に相当する機能の実装を2019年末までに実施することが報告された。[10]

また同NIR SIGにおいて、IDNICではAPNICからの通知を元にAbuse問い合わせ先の確認をメンバに対して実施していることが報告された。[11]

[10] https://conference.apnic.net/48/assets/files/APIC778/CNNIC-update.pdf

[11] https://conference.apnic.net/48/assets/files/APIC778/idnic-apjii-update.pdf

4. PI / PAアドレスに対するABUSE問い合わせ情報の追加について

4-1 PIアドレス

前項3-1に記載の通り、PIアドレスは、JPNIC管理のIPアドレス全体の三分の一を占める。

PIアドレスはJPNICから直接割り当てられることから、PAアドレスと異なり上位組織が存在しないため、WHOISの検索結果からは管理者連絡窓口、技術連絡担当者しか連絡先情報を確認することができない。

しかしこれらの問い合わせ先は必ずしもAbuse問い合わせ先であるとは限らないため、明示的にAbuse問い合わせ先情報を追加することが妥当と考えられる。

4-2 PAアドレス

PAアドレスをWHOISで検索すると、PIアドレスと同様に管理者連絡窓口、技術連絡担当者が表示されることに加え、割り当て元である上位組織の情報も表示される。この上位組織の情報を再度検索することによって、上位組織のAbuse問い合わせ先情報を参照することが可能である。しかし、下位組織のAbuse問い合わせを上位組織で受けた実例はそれほど多くないことをワーキンググループ内の議論でも確認しており、実態としては管理者連絡窓口、技術連絡担当者へ問い合わせされる事例が多数を占めていると予想される。

したがって、PIアドレスと同様に、問い合わせ先を明確化する意味でもAbuse問い合わせ先情報の項目を追加することが妥当と考えられる。

4-3 考慮すべき点

既存の登録済みIPアドレスレコードは数十万件に上ることが予想され、Abuse問い合わせ先情報の項目を新規追加した際に、特にIP指定事業者から割り当てられたPAアドレスについて、その全件のAbuse問い合わせ先情報の登録を既登録の割り当て元事業者に依頼、徹底させることは現実的に困難である。

したがって既存の登録済みIPアドレスについては、新規に設けるAbuse問い合わせ先情報の項目の初期値を決め予め登録する方法が考えられる。

初期値については、何も情報を入力せずに空白のままとする、該当組織の技術連絡担当者の情報を複写する、割り当て元上位組織のAbuse問い合わせ先情報を複写する（PAアドレスの場合のみ）といった方法が考えられる。

以下それぞれのメリット、デメリットを表にまとめる。

	メリット	デメリット
空白のまま	特別な対応が不要。	Abuse対応を行っていないと受け止められかねない。
技術連絡担当者	現状と変わらないと予想される。	本変更を説明する為の稼働が上位組織に発生する。 技術連絡担当者が本来のAbuse問い合わせ先かどうか不明。
上位組織のAbuse （PAアドレスのみ）	正しいAbuse対応が期待できる	本来対応すべき組織外への問い合わせとなる。 上位組織の稼働の増加。

次に登録される内容について、現在割り振りアドレスに登録される”Abuse”はメールアドレスとなっており、管理者連絡窓口や技術連絡担当者に登録されているJPNICハンドル/グループハンドルと異なっている。

これはWHOISを検索した際ひと目で問い合わせ先メールアドレスを参照できるメリットがある一方で、メールアドレスを変更したい場合、すべての登録済みレコードの”Abuse”の内容を変更しなければいけないなどのデメリットも存在する。

4-4 実装するべきと考えられる内容

以上のことから、実装すべきと考えられる内容は以下の通りである。

- PIアドレス、PAアドレスともにAbuse問い合わせ先項目を追加することが妥当と考えられる。

- 既存の登録済みIPアドレスまで遡及して登録を必須とすることは困難であることから、初期値は空白とし、新規登録の際に記載を必須とする。

- 登録する内容は、運用性を考慮し、メールアドレスではなくJPNICハンドル/グループハンドルとする。

- この場合、WHOIS検索結果の一覧性が失われること、Abuse問い合わせ先をあえて空白のままとしていると曲解されることを避けるため、WHOISの検索結果表示に情報を追加する。
  具体的には、
  - APNIC WHOISの検索結果表示のように、検索したレコードに登録されているハンドル情報を、元の検索結果に追加して表示する
  - Abuse問い合わせ先が空白の場合、技術連絡担当者宛に連絡することを促すような記載を追加する

5. 問い合わせ先の検査手法について

5-1 海外における検査手法の問題点、検討すべき事項

3-2-1記載の通り、APNICではメール記載のリンクをクリックし、登録情報の確認用Webサイトに飛ばす仕様となっているが、この仕組みはフィッシングサイトへの誘導を目的としたspamに悪用される懸念がある。実際に、2020年2月開催のAPNIC49での実施報告[12]によると、ある政府機関より、フィッシングが疑われるリンクはクリックができない、というコメントが寄せられたことが報告されている。

また、PAアドレスにおいて上位組織のAbuse問い合わせ先が登録されているケースが見られ、この場合複数のIPアドレスに対して同一のメールアドレスが登録されている可能性がある。この場合、IPアドレス情報に記載されたAbuse問い合わせ毎に確認メールを送信すると、特定のメールアドレス宛に大量の確認メールが送付されることとなり、対応が困難になることが予想される。

APNICでは罰則規定が設けられているが、日本の多くの組織が1回のみのアドレス取得であるケースがほとんどであり、例えばAPNICと類似のJPNIC Web申請システムの機能制限を行ったとしても効果は限定的と想定される。

さらに根本的な問題として、どこまで検査すべきか、何を目的とするか、という問題がある。

APNICではポリシーの策定時に自動応答などを排除する仕組みが必要、という提案者からの指摘があり現在のような手作業を介在する実装となっているが、メールのフォーマットや送信元アドレスが特定できれば自動応答などの処理は可能であり、応答があることがイコール正確なAbuse対応問い合わせ先であることを必ずしも保証するものではない。

5-2 実装すべき検査手法について

以上から、検査手法について次のような実装が妥当と考えれられる。

- メールアドレスの検査は初めての試みであることを考慮し、最初の段階ではメールアドレスの到達性のみを確認する手法とすべきである、具体的には確認メールを送信しUSER UNKNOWN等のエラーで不達とならなければ、そのメールアドレスは有効であると判断する。

- 複数のIPアドレスに登録されたメールアドレスであっても、確認メールは1通のみ送信する。

[12] https://2020.apricot.net/assets/files/APAE432/prop-125-implementation-update.pdf p.14参照。

- 確認メールの内容には、以下が含まれていることが望ましい。
    - 確認メールであること
    - 送付したメールアドレスが登録されている全IPアドレス
    - 返信等の反応は不要であること

- エラー等で不達となったメールアドレスに対しては、登録されたIPアドレスに紐づく管理者連絡窓口、技術連絡担当者などを通じて修正を促す。