WHOIS abuse連絡先正確性向上の検討WG 中間報告（サマリ）

2020年1月24日（金）
WHOIS Abuse連絡先正確性向上の検討WG
主査　鶴巻　悟

はじめに

- 本資料はワーキンググループのおける検討の中間報告のサマリとなります。
  中間報告全文は下記から参照ください。
  https://docs.google.com/presentation/d/1h6bG1knvk3feOG2mmUjz4J081pgN5_Ks_t2DX4ZksgI/edit?usp=sharing

１．中間報告の方向性

中間報告の方向性

- PA割り当て/PI割り当てアドレスに対して、Abuse問い合わせ先項目を追加するべきではないか。

- アドレスの正確性検査は、当初メールアドレス自体の存在確認のみとするのが妥当ではないか。

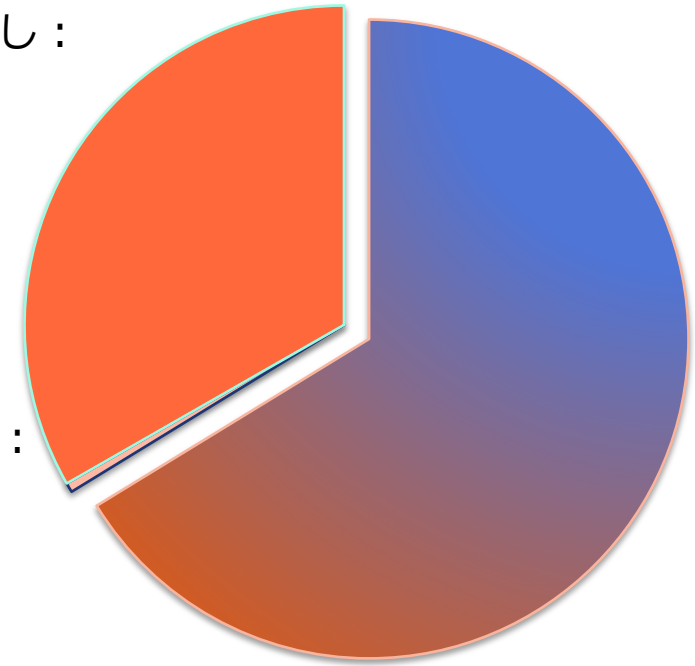
２．PI/PA割り当てアドレスへのAbuse問い合わせ先追加に関する検討すべきポイント

IPv4アドレス数からみた状況

Abuse問い合わせ先項目なし：
約５千万アドレス

Abuse問い合わせ先登録済み：
約１億アドレス
※PA割り当ては内数

Abuse問い合わせ先未登録：
約７２万アドレス



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。

昨今の世界的な状況を鑑みると、Abuse問い合わせ先を追加するべき

検討すべきポイント①　過去に遡及するか

- PIが約５千万個、PAが約１億個がすでに割り当てられている
  - 割り当て済みアドレスまで遡及して登録を必須とすることは現実的に困難。
- 遡及しない場合、追加されるAbuse問い合わせ項目をどうすべきか？
  - →検討すべきポイント②

検討すべきポイント②　「空白」問題

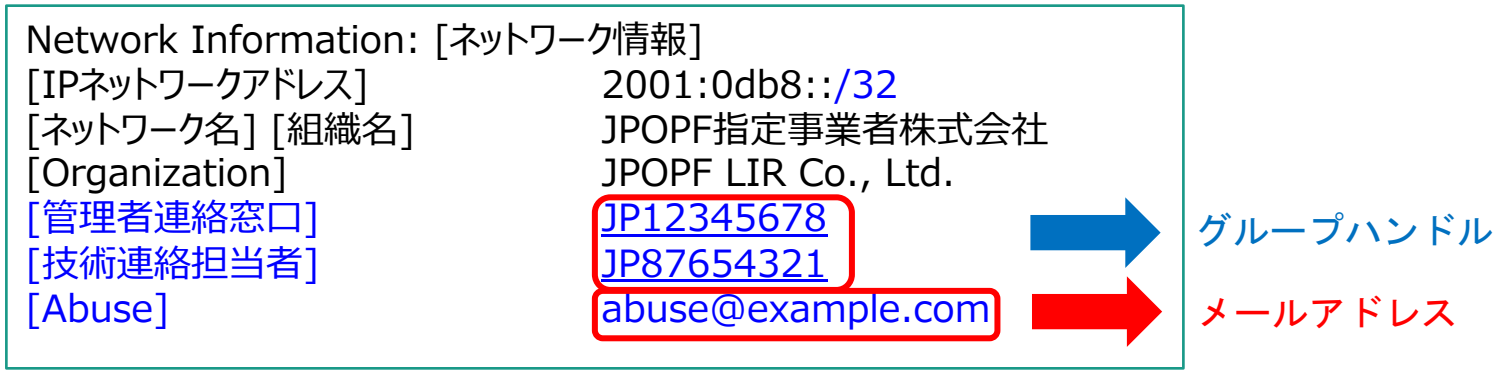
- すでに登録されているアドレス情報にAbuse問い合わせ項目が追加された際に、初期値をどうするか。
  - 空白のままとし、追加割り当て等のタイミングで記入を依頼していく。
  - 「技術連絡担当者」情報をコピーする。
  - （PA割り当てのみ）上位組織のAbuse問い合わせ先をコピーする。

「空白」のabuse問い合わせ先

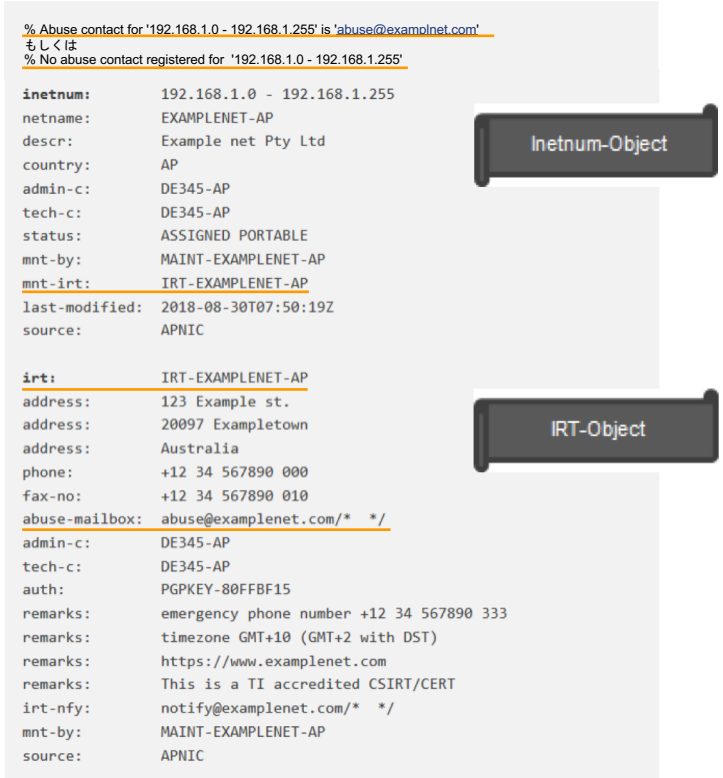
	PIアドレス		PAアドレス	
	Pros.	Cons.	Pros.	Cons.
空白のまま	特別な対応が不要	明示的にabuse対応を行っていないと受け止められかねない	特別な対応が不要	明示的にabuse対応を行っていないと受け止められかねない
技術連絡担当者	現状と変わらないと思われる	本来のabuse問い合わせ先か不明	現状と変わらないと思われる	上位組織の稼働の増加。 本来のabuse問い合わせ先か不明
上位組織のabuse	上位組織なし	上位組織なし	正しいabuse対応が期待できる	実態とそぐわない。 上位組織の負荷増加。

検討すべきポイント③　email or ハンドル

- 現在Abuse問い合わせ先情報のみメールアドレスとなっているが、他の情報との整合性をあわせる意味でもハンドルとすべきではないか。
- ただし、ハンドルにした場合一覧性が失われるため、WHOISの結果表示の際に記載されたハンドルの内容も表示されることが望ましい。



APNICにおけるWHOISの表示例



- 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

３．メールアドレスの正確性検査について

海外の手法における懸念点（再掲）

【APNICでの検証プロセス】

1. 半年に1度の検証 !!
   APNICよりIRT Objectに登録された“e-mail” 及び “abuse-mailbox”宛に各2通のメールが送信されます。
   1通目は検証用のURL
   2通目には検証用のパスコード
2. 15日間レスポンス無し
   → MyAPNICに警告が表示
3. 30日間レスポンス無し
   → ・MyAPNICの機能が制限
   (IRT Objectに abuseが応答がない旨の記載) 且つ
   ・親レコード(IPアドレスの登録情報)にabuse-c Objectが追加
   (このabuce-c 宛に問い合わせが届いた際には、APNICからリソースホルダーに対して手動で検証の要求が行われます。

海外の手法における懸念点 （再掲）

【APNICでの検証プロセス】

1. 半年に1度の検証 !!
   APNICよりIRT Objectに登録された“e-mail” 及び “abuse-mailbox”宛に各2通のメールが送信されます。
   1通目は検証用のURL
   2通目には検証用のパスコード
2. 15日間レスポンス無し
   → MyAPNICに警告が表示
3. 30日間レスポンス無し
   → ・MyAPNICの機能が制限
   (IRT Objectに abuseが応答がない旨の記載) 且つ
   ・親レコード(IPアドレスの登録情報)にabuse-c Objectが追加
   (このabuce-c 宛に問い合わせが届いた際には、APNICからリソースホルダーに対して手動で検証の要求が行われます。

複数NWを管理している人に大量のメールが送付されない？

懸念点 （再掲）

検証を騙ったspamメールが飛んでこない？
反応する ＝ Abuse対応しているといえる？

APNICよりIRT [illegible] e-mail” 及び “abuse-mailbox”宛に各2通の
メールが送信さ[illegible]。
1通目は検証用のURL
2通目には検証用のパスコード

2. 15日間レスポンス無し
→ MyAPNICに警告が表示
3. 30日間レスポンス無し
→ ・MyAPNICの機能が制限
(IRT Objectに abuseが応答がない旨の記載) 且つ
・親レコード(IPアドレスの登録情報)にabuse-c Objectが追加
(このabuce-c 宛に問い合わせが届いた際には、APNICからリソースホルダーに対して手動で検証の要求が行われます。

複数NWを管理している人に大量のメールが送付されない？

懸念点 （再掲）

検証を騙ったspamメールが飛んでこない？
反応する ＝ Abuse対応しているといえる？

APNICよりIRT [illegible]された e-mail” 及び “abuse-mailbox”宛に各2通の
メールが送信さ[illegible]。
1通目は検証用のURL
2通目には検証用のパスコード

2. 15日間レスポンス無し
→ MyAPNICに警告が表示

3. 30日間レスポンス無し
→ ・MyAPNICの機能が制限
(IRT Obje[illegible]seが応答がない旨の記載) 且つ
[illegible]にabuse-c Objectが追加
[illegible]届いた際には、APNICからリソースホルダーに対し
[illegible]。

複数NWを管理している人に大量のメールが送付されない？

制限されても気が付かないのでは･･･

検討すべきポイント④　確認手法

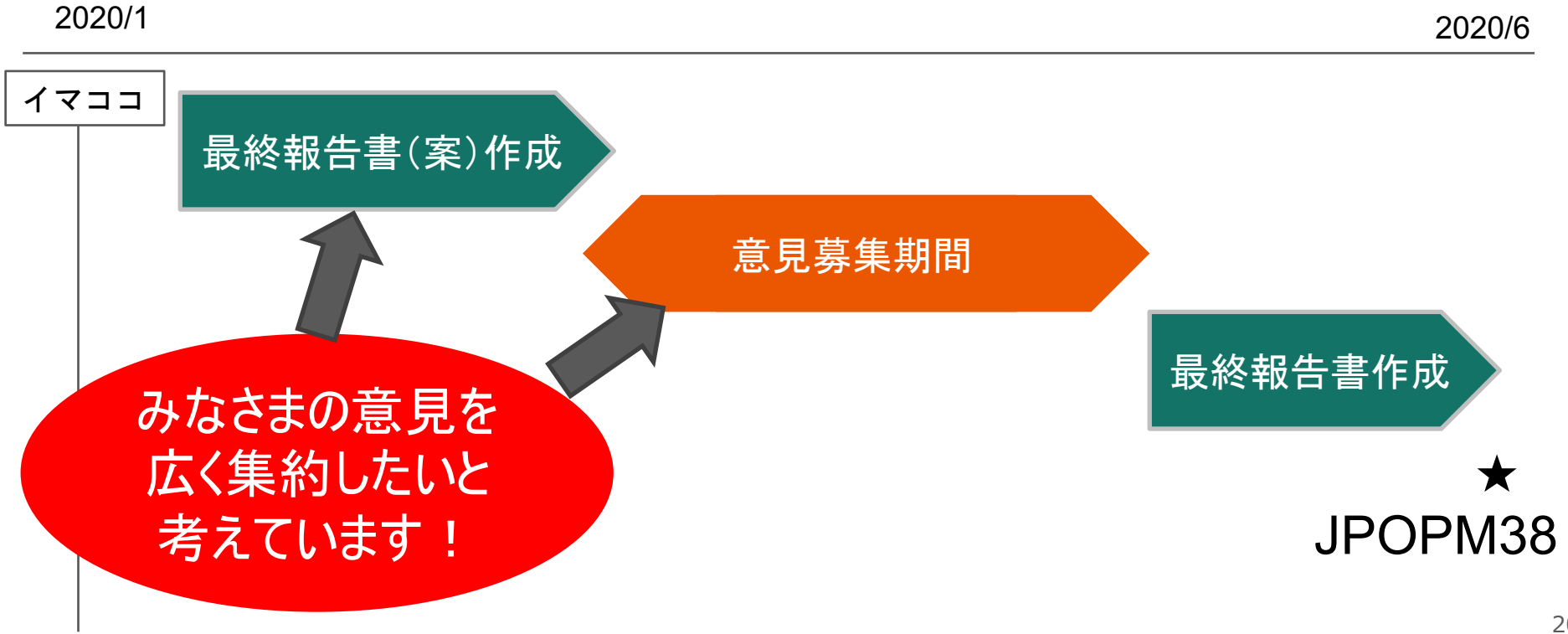
- 複数の割り当てネットワークに同一の連絡先が設定されている場合は、送信するメールは1通。

- 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。

４．ディスカッション

今後のWGの進め方（予定）



議論したいポイント①

「中間報告書の方向性」についての意見・コメントを是非お願いします！

中間報告の方向性

- PA割り当て/PI割り当てアドレスに対して、Abuse問い合わせ先項目を追加するべきではないか。

- アドレスの正確性検査は、当初メールアドレス自体の存在確認のみとするのが妥当ではないか。

議論したいポイント②

「検討すべきポイント」としてあげた4点について、是非みなさまのご意見をお聞かせください！

① Abuse問い合わせ先は、既存登録済みの情報まで遡及すべきか？

② 訴求しない場合、空白となる問い合わせ先情報をどうすべきか？

③ 登録情報はemailとハンドルのどちらが好ましいか？

④ メールアドレスの検証は、アドレスの存在確認のみで妥当か？