

(提案036-01) JPNICにおけるWHOIS正確性向上のための検証

2019.6.21
JPOPF運営チーム

コンセンサス確認いただきたい事項①

提案の背景①

近年、重要度が増してきている。

	利用目的	利用者
当初 ↓ 近年	ネットワーク障害等への対応	IP指定事業者ネットワーク管理者等
	セキュリティインシデント対応	JPCERT/CCなどのインシデントハンドリングチーム
	一般ユーザからの相談対応、調査	消費者庁迷惑メール対策支援プロジェクト 違法・有害情報相談センター
	犯罪捜査	警察等の法執行機関 (FBIが2年前に来日、 JPOPM31 で問題提起 !!)

RIR	検証項目	検証方法	実施状況	罰則規定
 American Registry for Internet Numbers	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	実施済み	あり (新規申請の制限)
 RIPE NETWORK COORDINATION CENTRE	"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	実施済み	なし
 APNIC	IRT Objectの"email","abuse-mailbox"に登録された連絡先	半年毎にメールを送信し、受信確認を行う	2019/6/30より検査開始	MyAPNICの機能限
 AFRINIC	IRTオブジェクトに登録された連絡先		継続議論	APNICと同等の罰則規定
 lacnic	IRTオブジェクトに登録された連絡先		継続議論	APNICと同等の罰則規定

inetnum Object

← JPNICの「ネットワーク情報」相当

```
inetnum:      192.168.0.0 - 192.168.0.255
netname:      jopof-st Net
~~~~~ 略 ~~~~~
admin-c :     SJxxx-AP
tech-c:       SJxxx-AP
status:       ALLOCATED PORTABLE
~~~~~ 略 ~~~~~
mnt-irt:    IRT-JPOPfST-JP
remarks:      -----
remarks:      To report network abuse, please
remarks:      For troubleshooting, please conta
remarks:      Report invalid contact via www.a
remarks:      -----
~~~~~ 略 ~~~~~
```

IRT Object

```
irt:          IRT-JPOPfST-JP
address:      [住所]
e-mail:       abuse @ jpopf.net
abuse-mailbox: abuse @ jpopf.net
~~~~~ 略 ~~~~~
```

APNICでは、JPNICの「ネットワーク情報」に相当する”inetnum”にAbuse対応組織(Incident Response Team)情報が登録されています。

【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

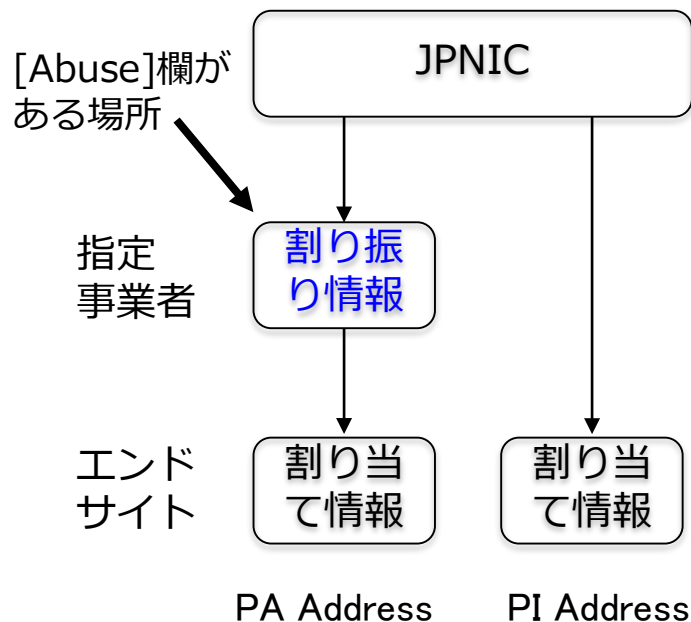
2. 15日間レスポンス無し

→ 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abuse-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。

Abuse の連絡先 ([Abuse]) が記載されている場所は「割り振り情報」のみ。



WHOIS 検索結果	[Abuse] 欄 の有無	[Abuse]対応のための 連絡先の探し方
割り振り情報	有り	検索結果に [Abuse]欄有り。
割り当て情報 (PAアドレス)	無し	割り当て情報における「上位情報」より割り振り情報を検索し、上位組織の[Abuse]欄の連絡先を使う。 又は、[管理者連絡窓口] 又は [技術連絡担当者] を使う。
割り当て情報 (PIアドレス)	無し	[管理者連絡窓口] 又は[技術連絡担当者] を使うしかない。

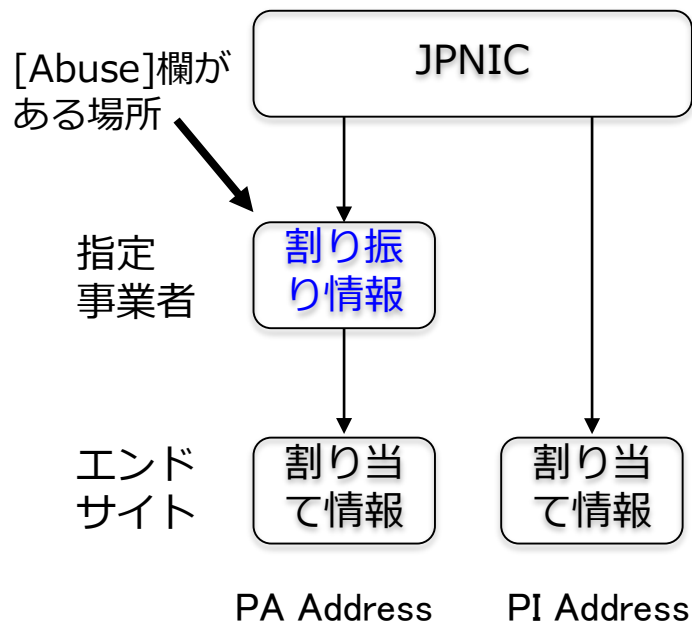
提案内容①

- JPNICにおいても、Abuse問い合わせ先に対する正確性を確認ための検査を実施する。
 - 検査対象は、IP指定事業者へ割り振られたアドレスのネットワーク情報内の[Abuse]に登録されたメールアドレスとする
- 検査の具体的な手法や頻度等を検討するためのワーキンググループを設置する。
 - ワーキンググループでの議論の結果を、JPOPF運営チームよりJPNICへ実装勧告する

コンセンサス確認いただきたい事項②

提案の背景②

Abuse の連絡先 ([Abuse])が記載されている場所は「割り振り情報」のみ。



WHOIS 検索結果	[Abuse] 欄 の有無	[Abuse]対応のための 連絡先の探し方
割り振り情報	有り	検索結果に [Abuse]欄有り。
割り当て情報 (PAアドレス)	無し	割り当て情報における「上位情報」より割り振り情報を検索し、上位組織の[Abuse]欄の連絡先を使う。 又は、[管理者連絡窓口] 又は [技術連絡担当者] を使う。
割り当て情報 (PIアドレス)	無し	[管理者連絡窓口] 又は[技術連絡担当者] を使うしかない。

- APNICでIRT Objectが実装されたことを受け、JPOPM18でJPNICでの実装可否を議論
 - IRT Object自体の実装はコンセンサスに至らず。
 - 代わりにIP指定事業者向けの新規の割り振りアドレスに対してのみ[Abuse]が必須項目となった。
- IP指定事業者に割り振られた全アドレス情報に登録されていない
 - [Abuse]が追加される以前のアドレス情報には未記入のケースもあり。

提案内容②

- PI割り当てされたアドレスやAS番号の管理組織に対する Abuse問い合わせ先の明確化を図るため、APNICにおける IRT Objectに相当する登録情報の実装可否を、ワーキンググループにて検討を行う。

JPNICにおけるWHOIS正確性維持のための 検討ワーキンググループ 設立趣意書(案)

■ワーキンググループ(以下 WG)設立の背景

社会的なWHOISの利用形態の多様化特に法執行機関の利用などに伴い、WHOIS登録情報の正確性の向上・維持管理が求められている。

APNICにおいてもprop-125がコンセンサスとなり、WHOIS登録情報のうち、Incident Response Team (IRT) オブジェクトについて定期的な連絡先の存在確認と到達検証が行われることとなった。

NIRにおいて本提案内容は"reccomended"とされており、JPコミュニティにおいてもAbuse問い合わせ先の正確性向上・維持管理に関する提案[036-01]が議論された。

■WG設立の目的

上記背景を受け、本WGはJPNINCにおけるAbuse問い合わせ先の正確性向上を図るために必要となる検査の手法、検査対象等の検討を実施することを目的とする。

■ WGにおける検討事項

具体的に実現可能なAbuse問い合わせ先の本WGで取り扱わなければならない事項は以下の通りである。

- IPアドレス管理指定事業者の管理管轄である、IPアドレス、及びAS番号のWHOISにおける[Abuse]問い合わせ先の正確性の向上・維持管理手法

実現に当たって考慮すべき点は以下の通りである。

- IPアドレス管理指定事業者が現実的かつ時間軸・コスト的に適正な範囲において実現可能な確認・対応の業務プロセス・ワークフローの検討と提案。
- JPNICが現実的かつ時間軸・コスト的に適正な範囲において実現可能な確認・対応の業務プロセス・ワークフローの検討と提案。
- なお、APNIC prop-125やAPNICでの実装方法を参考とし、複数回の確認を含め、また事後の修正・リカバリ等の手段も検討範囲に含まれることが望ましい。

また、ポリシー提案及びOPMでの合意に基づき求められた場合、以下についても検討項目とする。

- PIアドレスホルダに対する[Abuse]相当の問い合わせ先の正確性の向上・維持管理手法

■WGのゴール

本WGは検討及びJPOPFに対するWHOIS正確性向上のための施策案の報告を最終的な成果とする。
なお、実際の実装・実現方法についてはJPNICに一任することとする。

■前提と制約

現在JPNICのWHOIS登録情報にはAPNICにおけるIRTオブジェクトが存在しないため、APNIC Prop-125と全く同様の対象の検査を実施した場合、その検査対象や効果がAPNICと同等とならない可能性があることに留意する必要がある。

またIP指定事業者の登録オブジェクトの[Abuse]項目は、それが追加される以前のオブジェクトに対する登録が任意となっているため、[Abuse]項目の検査を実施しても全IP指定事業者の登録オブジェクトが検査されない点についてもあわせて留意する必要がある。

■体制

- ・ 公募による立候補制で有志メンバで構成する。
- ・ メンバ互選により主査及び副査を設置する。
- ・ メンバ多数になった場合、意見集約及び効率向上を目的とし公正な抽選法により最大20名以内とする。また分科会制により作業分担を行う。
- ・ なお、JPOPF運営チームは複数名が事務局参加することとする。(メンバとしての参加と重複しても良い)
- ・ なお、JPNICは複数名がオブザーバメンバとして参加することとする。なおオブザーバ意見はJPNIC正式回答と見做さない。

■想定されるリスク

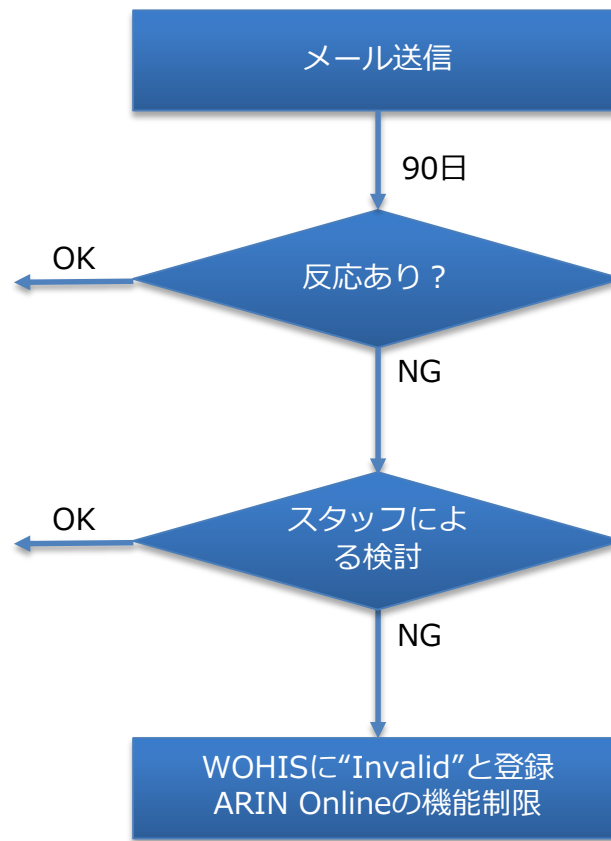
- ・ IPアドレス管理指定事業者の管理負担の過剰な増大
- ・ IPアドレス管理指定事業者の下位組織の管理負担の過剰な増大
- ・ JPNICのIPアドレス指定事業者対応の過剰な増大
- ・ JPNICのWHOIS管理・運用負担の過剰な増大
- ・ PIアドレス管理者の管理負担の過剰な増大
- ・ JPNICのPIアドレス管理対応の過剰な増大
- ・ 世界動向に対して本件自体の実装と実現の遅れ

■ WGのマイルストーンとスケジュール

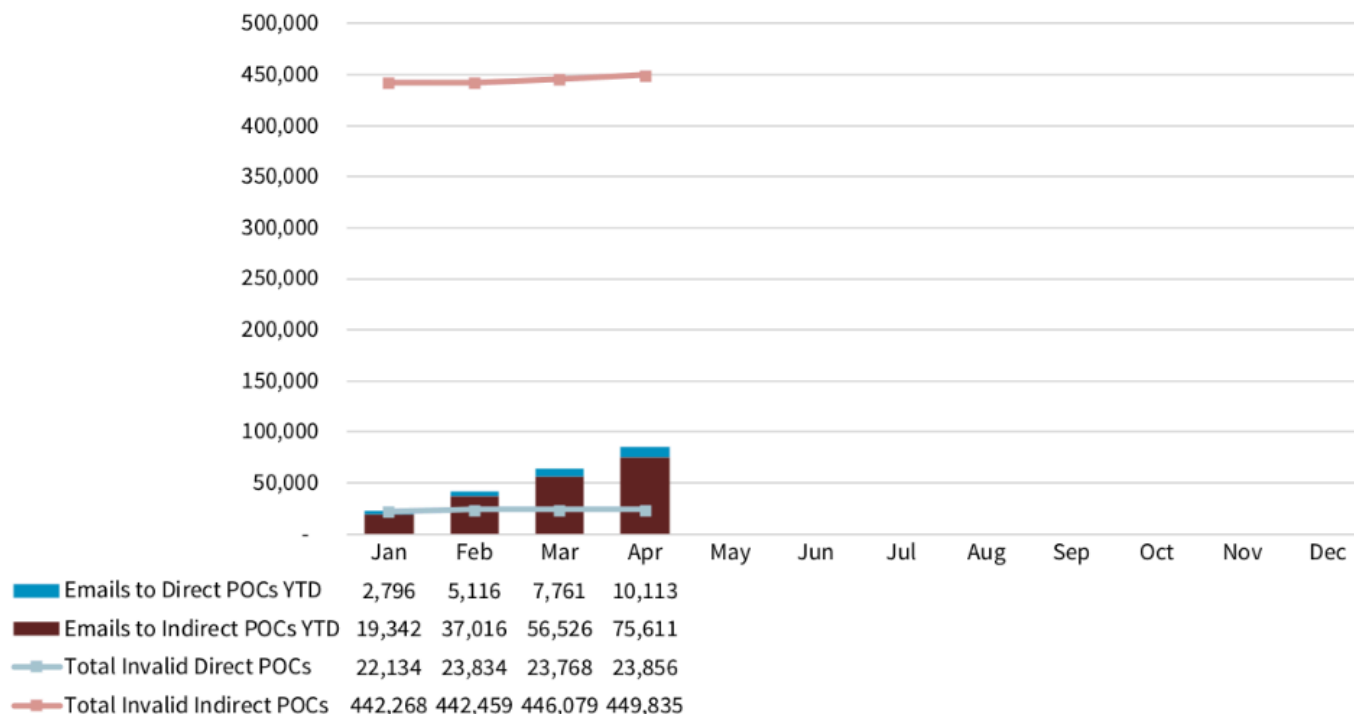
- 2019年7月まで WGメンバーの公募。
- 2019年7月～9月 一次案検討、JPNICによる課題抽出。
- 2019年10月～11月 二次案検討、JPOPM37にて中間報告を開催。
- 2019年11月～2020年2月 報告書とりまとめ。
- 2020年3月以降 WGからJPOPFに対して報告書を提出。

(参考) 海外RIRでの実装について

- 2017年にAbuse Contactの検証を年1回行うポリシーを制定(ARIN-2017-3)
 - コンタクトが取れない場合、ARIN Onlineの一部機能（支払いと情報更新）以外へのアクセス停止となる
https://www.arin.net/vault/policy/proposals/2017_3.html
- 再割り当て等の登録情報の変更時に正確性を確認する提案(ARIN-2017-12)がARIN41でコンセンサスとなったが、ACへ差し戻し
 - https://www.arin.net/policy/proposals/2017_12.html



2019 POC Validation Emails Year-To-Date (YTD) and Total Invalid POCs

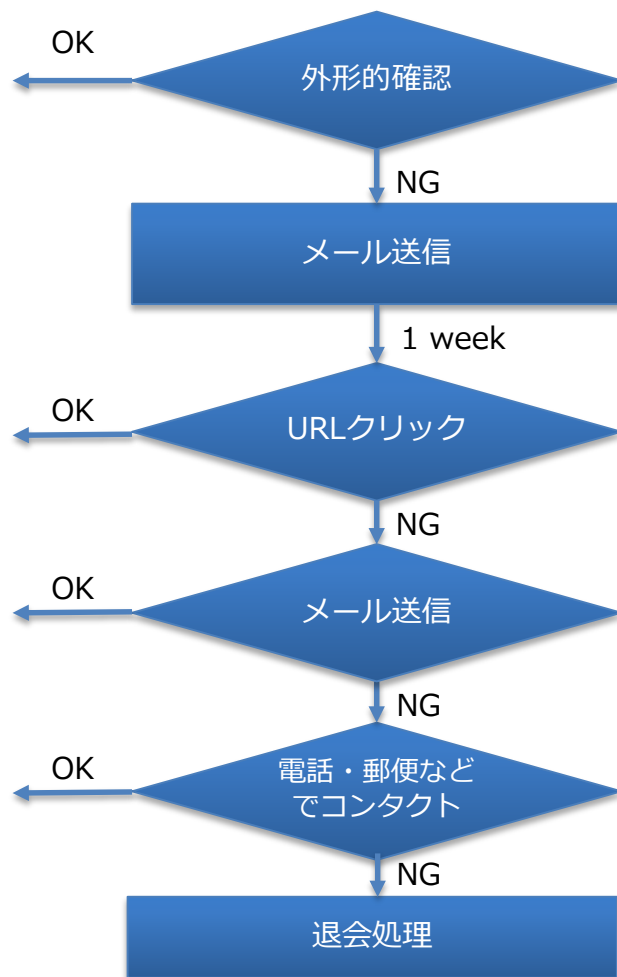


- 2012年にAbuse ContactをWHOISに登録するポリシーを制定(RIPE-563)
 - 登録者に正確な情報を維持するインセンティブが無く、アドレス情報の正確性に懸念が生じる
- 2018年に最低年1回アドレス情報の正確性を検証するとしたポリシーに改定(RIPE-705)
 - 正確でない情報を登録している組織に対しての罰則規定等を盛り込まない前提
- 2019年1月に最初の登録情報の検証を実施

<https://ripe78.ripe.net/presentations/111-Abuse-c-update-RIPE-78.pdf>

実証実験のプロセス：

https://labs.ripe.net/Members/angela_dallara/how-we-will-be-validating-abuse-c



- メールアドレスのフォーマットチェック
- ドメインにMXレコードが存在するか
- pingでの到達性確認
- メールへの到達性確認

- メール本文にチケットクローズ用のURL記載

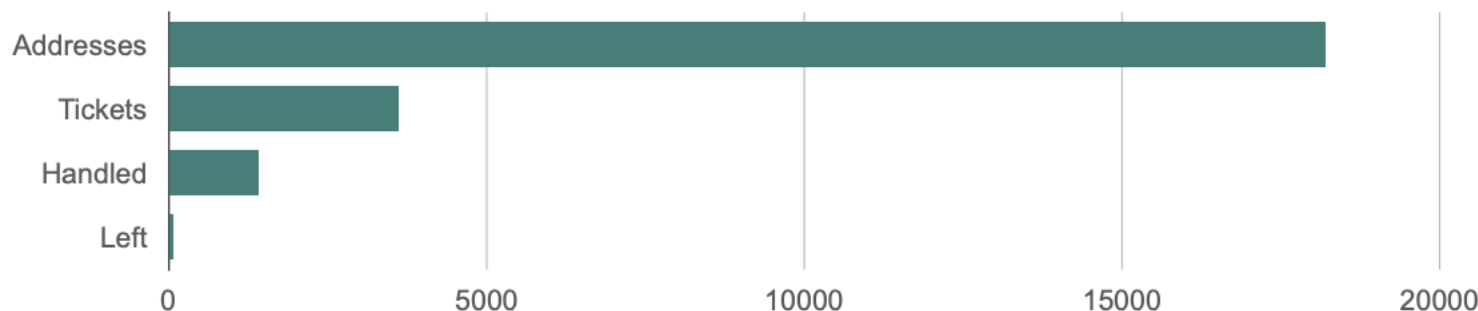
- すべての登録されたコンタクト先にメール送信。
返信が無い場合、1週間ごとに2回送信

自動化

Completed Validation LIR Organisation



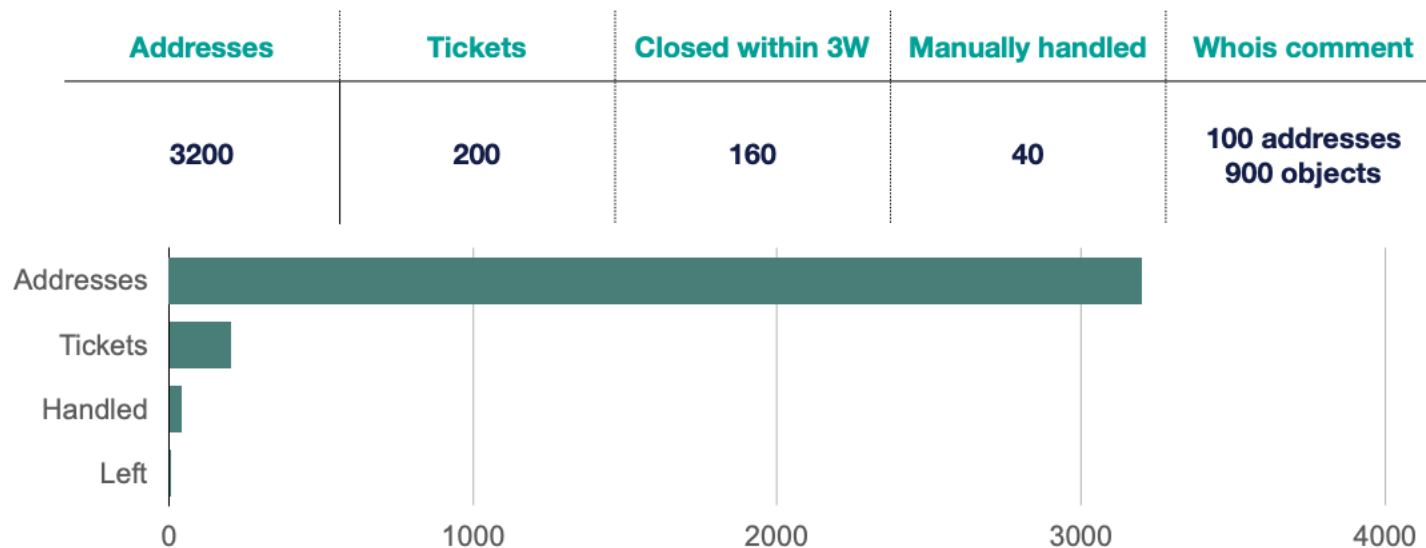
~ 22,500 LIRs



Completed Validation LIR Resources



~ 1,200 LIRs



Comment on LIR and End User resources



Search results

[PERMA](#) [XML](#) [JSON](#)

This is the RIPE Database search service. The objects are in RPSL format.
The RIPE Database is subject to [Terms and Conditions](#).

Responsible organisation: [redacted]
Abuse contact info: abuse@[redacted]
Abuse-mailbox validation failed. Please refer to [ORG-\[redacted\]](#)-RIPE for further information.

inetnum:
netname:
descr:
country:
admin-c:



Update object

RIPEstat [↗](#)

Challenges



- Aiming for minimal disturbance
- Using clear communication
- Non-technical people on the phone
- Unresponsive resource holders
- Detecting new issues in a timely manner
- Accuracy in handling large number of tickets per day