ROA登録チートシート

2022年9月28日

長崎県立大学 岡田 雅之

一般の方のお悩み

- ROAを登録するときの準備はどうすれば‥
- 事前の確認は何をすればいい？
- 登録後はどんな運用をすればいいのか？
- 実際にROA登録を行う際の確認事項をまとめた

ROA登録チートシートのようなもの

ROA登録チートシート

https://docs.google.com/document/d/199B4EDYnu2iSkRDE6pz7LksMKieAnuLgf00yzQq7RgE/edit?usp=sharing

1. 登録以前の状態確認

1. 登録以前の定常状態の確認
    a. 自組織からPing/Traceroute等応答のある外部IPアドレスを複数確保
    b. 問題発生時の対応をスムーズにするため各種情報を確認・更新
        i. IPアドレスレジストリのWHOIS等データベース
        ii. IRR
        iii. PeeringDB
        iv. IX等の連絡先
    c. 外部Looking Glassで自IPアドレスを確認可能なサイトを複数確保
        i. https://www.bgp4.as/
        ii. 経路奉行
        iii. RIPE stat
        iv. Route Views
    d. RPKIに関するポータルサイトでの状況確認
        i. https://console.rpki-client.org/
        ii. https://rpki.cloudflare.com/?view=validator
        iii. https://rpki-validator.ripe.net/ui/
        iv. https://irrexplorer.nlnog.net/
        v. http://roa2.nic.ad.jp:8080/
    e. 登録前のトラフィック(In/Outを確認)

2. 登録対象Prefixの選定

- 可能であれば、空いているアドレススペース
  - 枯渇してるので難しい・・・
- 影響範囲の少ないPrefix
  - /24などのPrefix長の長いもの
- トラフィックが少ないIPアドレスブロック
- ROA登録後、数分で世界中のRPKI-RTRへ
  - 普及率の高い(=routinator3000)RPKI-RTRのデフォルトの差分更新間隔は300秒/5分
  - あやまるとほぼ即時に影響発生

3．ROA登録

a. 必ず**複数人**で登録を実施
b. JPNICの資源管理カードの有効期限が3か月以上あることを確認
c. IPv4とIPv6で資源管理者証明書が異なるので注意
d. JPNICの申請システムでは、ブラウザの”**戻る**”・”**ススム**”は絶対に使ってはいけない
e. JPNICの申請システムでは、複数資源管理証明書の使い分けが難しいので、その場合は、シークレットウィンドウ的なものを使うと回避可能
f. JPNICの資源管理カードを認識し、資源申請者の電子証明書を発行なPCが複数あることを確認
g. JPNICのROA Webへ複数の資源申請者アカウントでログイン可能であることを確認
h. JPNICのROA Webへ複数のPCから資源申請者ログイン可能であることを確認
i. 資源申請者証明書の有効期限が3か月以上あることを確認（期限は発行から25か月）

4. ROA登録後の確認/5. 運用

4. ROA登録後の確認
    a. "1. 登録以前の定常状態の確認"にて確認したサイトにてPing/Traceroute の応答に変化が無い、許容される程度の変化であることを確認
    b. "1. 登録以前の定常状態の確認"にて確認したサイトにて登録したROAが閲覧できることを確認
    c. 登録後のトラフィックに変化が許容範囲であることを確認

5. 定常的なROAの監視と運用への対応
    a. ROAと経路情報の乖離の防止
        i. BGP設定変更時の運用に、ROA確認を追加
    b. レジストリのリポジトリを監視
        i. 発行されたROAのSIA(Webで言うURIのようなもの)を確認して定期的にRsyncでチェックする(やりすぎ？)
        # test-roa -p rpki-repository.nic.ad.jp/ap/A91A73810000/20183/ZhMrUfbcMMYT95MS2_yp80Ekc_8.roa | openssl x509 -text
        ただし、現状のrpki-clientはOpenBSD7.4でしか動かない
        (https://console.rpki-client.org/ で確認するのが吉)
        ii. 自前でキャッシュを運用し、定期的に自組織のROAを確認

5. 定常的な運用確認