

RPKIキャッシュサーバの課題と提案

- より信頼できるRPKIを目指して -

2026年7月16日 JANOG58 Meeting 松山
長崎県立大学
後藤 汰珠

自己紹介

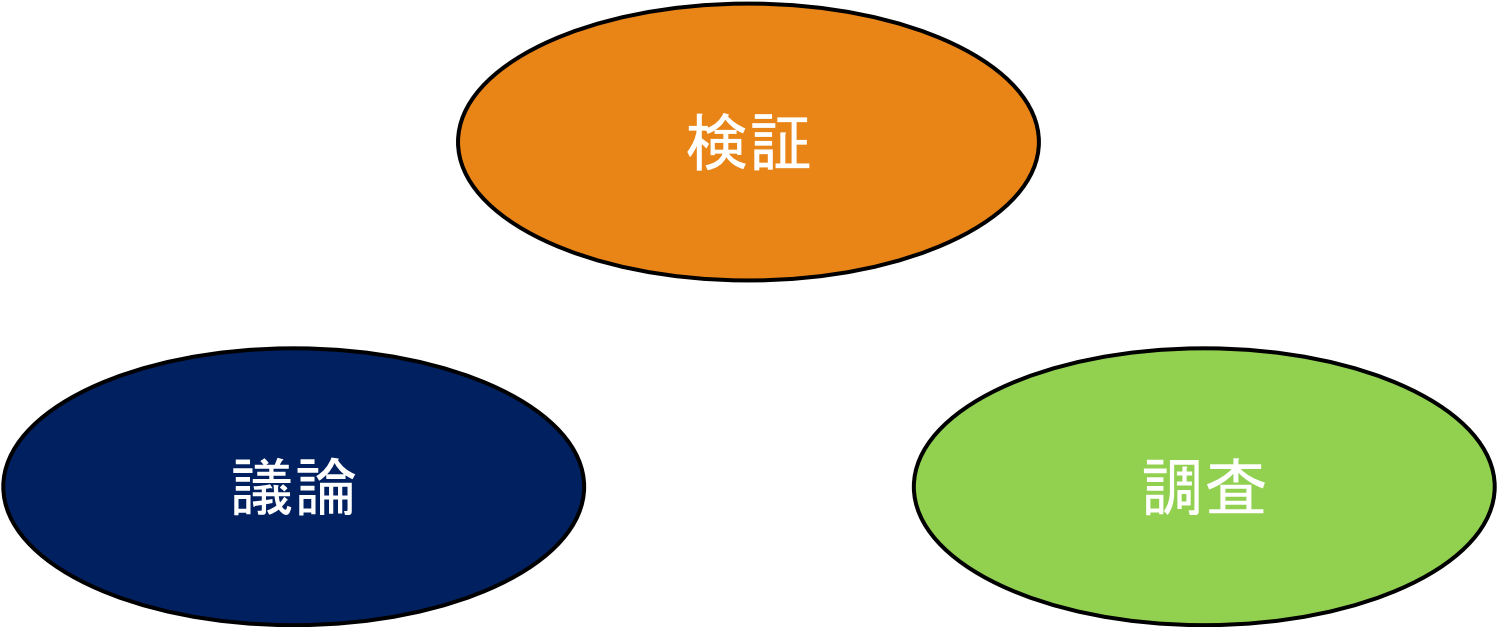
- ・ 所属
 - ・ 長崎県立大学 岡田研究室
- ・ 自己紹介
 - ・ 後藤 汰珠 (Taiju Goto)
 - ・ RPKIキャッシュサーバの仕組みや運用に関する研究を行っており
APNIC60で成果発表経験もあり



JANOG58で計5回目の
参加になります

長崎県立大学とビッグローブの関係

RPKIを含むルーティングセキュリティに関する共同研究を行う関係



検証

議論

調査

不完全なVRPに対する対策の検討

共同研究での議論を通じて以下の対策を実施することとなった

- **不正経路の流入を防止する**
 - 本来ルータに登録すべきでない経路を許可し、INVALID経路の流入を許すことは避けた
- **正常な経路への通信影響を可能な限り減らす**
 - 本来ルータに登録すべき経路を拒否し、顧客へ通信影響を出すことは避けた

不完全なVRPに対する対策の検討

具体的なデータを用いた「**不完全なVRP**」の定義

検知した「**不完全なVRP**」に対処する仕組み

「不完全なVRP」の定義

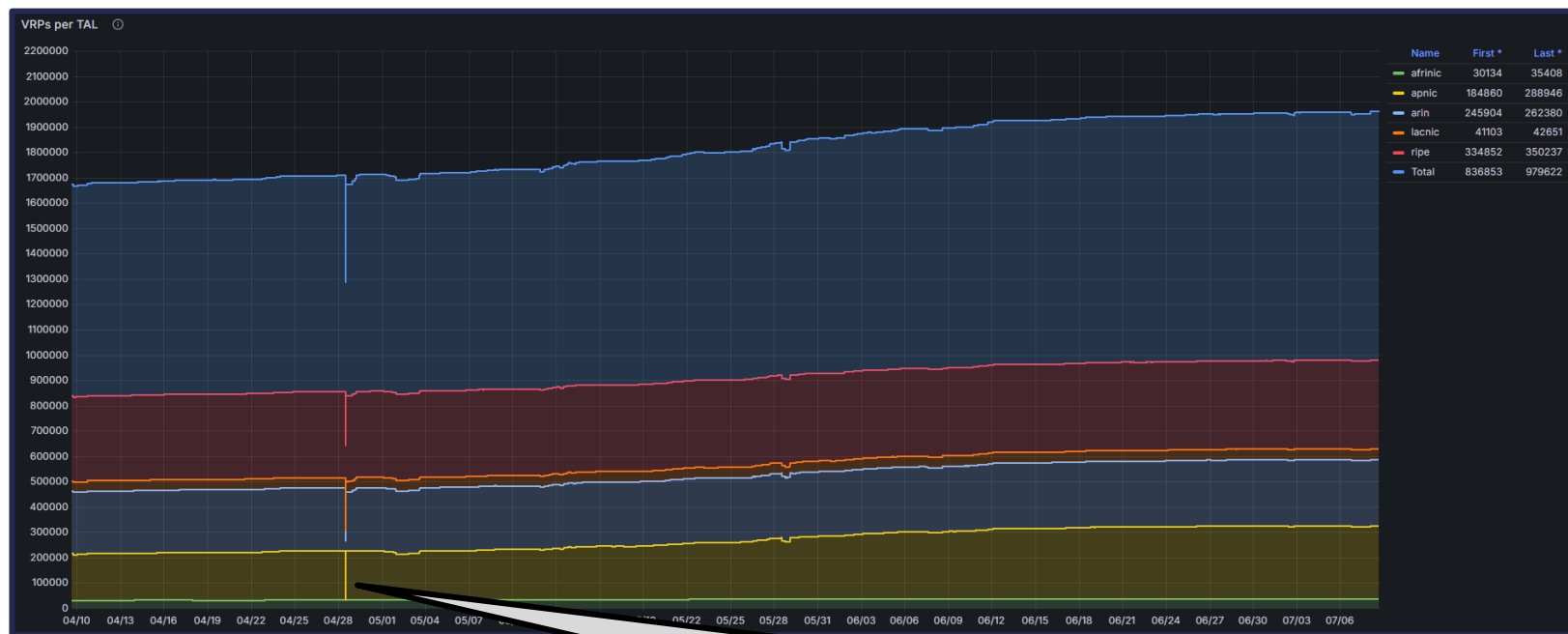
- RPKIキャッシュサーバソフトウェアではROA取得時の情報を観測できるものがある
- これらの情報を蓄積することで「不完全なVRP」の定義を行った

ROAを含めたオブジェクトの取得数やリポジトリごとの同期状況など様々な情報を観測することができる

```
# HELP rpki_client rpki-client information
# TYPE rpki_client gauge
rpki_client_info{nodename="rpki-client",release="9.8"} 1
# HELP rpki_client_job_completion_time end of this run as epoch timestamp
# TYPE rpki_client_job_completion_time gauge
rpki_client_job_completion_time 1783494547.159510645
# HELP rpki_client_repository total number of repositories
# TYPE rpki_client_repository gauge
rpki_client_repository{type="rsync",state="syncd"} 2
rpki_client_repository{type="rsync",state="failed"} 7
rpki_client_repository{type="http",state="syncd"} 5
rpki_client_repository{type="http",state="failed"} 0
rpki_client_repository{type="rrdp",state="syncd"} 102
rpki_client_repository{type="rrdp",state="failed"} 9
# HELP rpki_client_objects total number of objects
# TYPE rpki_client_objects gauge
rpki_client_objects{type="cert",state="valid"} 53109
rpki_client_objects{type="cert",state="failed parse"} 19
rpki_client_objects{type="cert",state="non-functional"} 133
rpki_client_objects{type="manifest",state="valid"} 53090
rpki_client_objects{type="manifest",state="failed parse"} 133
rpki_client_objects{type="manifest",state="sequence gap"} 5634
```

「不完全なVRP」の定義

①VRP総数が通常の観測値から大きくかけ離れたとき



一時的に観測できた「不完全なVRP」

期間 90日
初日ROA数 836853個
最終日ROA数 979622個

増加率 約17%
増加率から導かれる予測値を
大きくかけ離れた値になった時
「不完全なVRP」の可能性はある

「大きくかけ離れた」は
最小二乗法で予測される値から
差分10%の値を閾値とした

「不完全なVRP」の定義

②特定ASのROA情報の取得に失敗している時

- 自身のASにとって重要なAS(トラフィック量・SLAがある相手)の経路が破棄されてしまった場合、トランジットに通信が流れることで普段よりコストがかかる場合や、信用問題に発展する可能性がある

③特定リポジトリとの接続状態に異常があるとき

- 証明書ツリーの上流にあるリポジトリとの接続状態に異常がある時、下位リポジトリの持つROAを含むオブジェクト全てが参照できなくなり、注視していない多くの組織への通信ができなくなる可能性がある

不完全なVRPに対応する仕組みの検討

議論を通じて以下の要件が必要であると検討を行った

- 検知

- 「不完全なVRP」の定義を用いて対象を検知する仕組みが必要

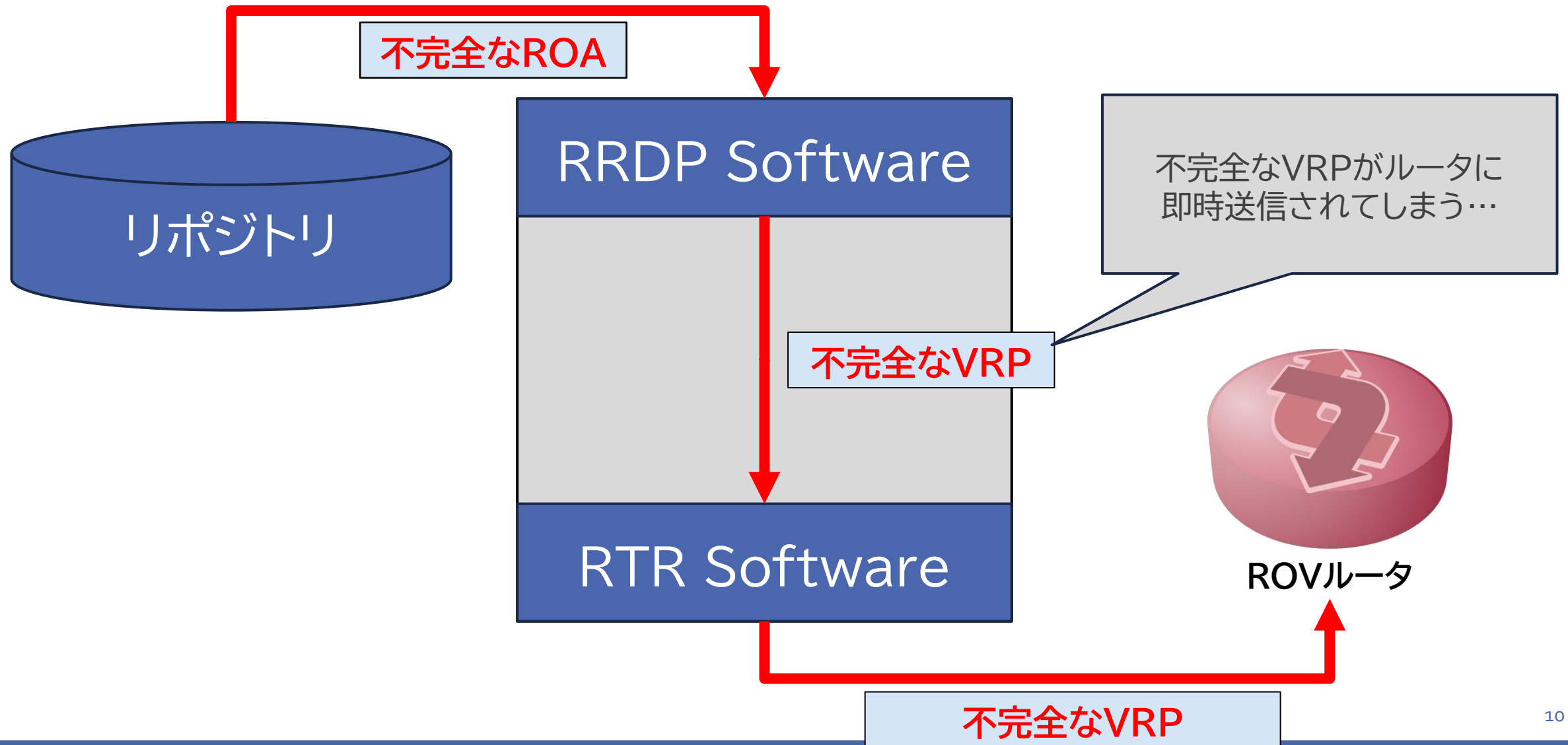
- 防御

- ROVを停止させずに継続させることで
セキュリティを担保しつつ正常な通信環境を提供させる

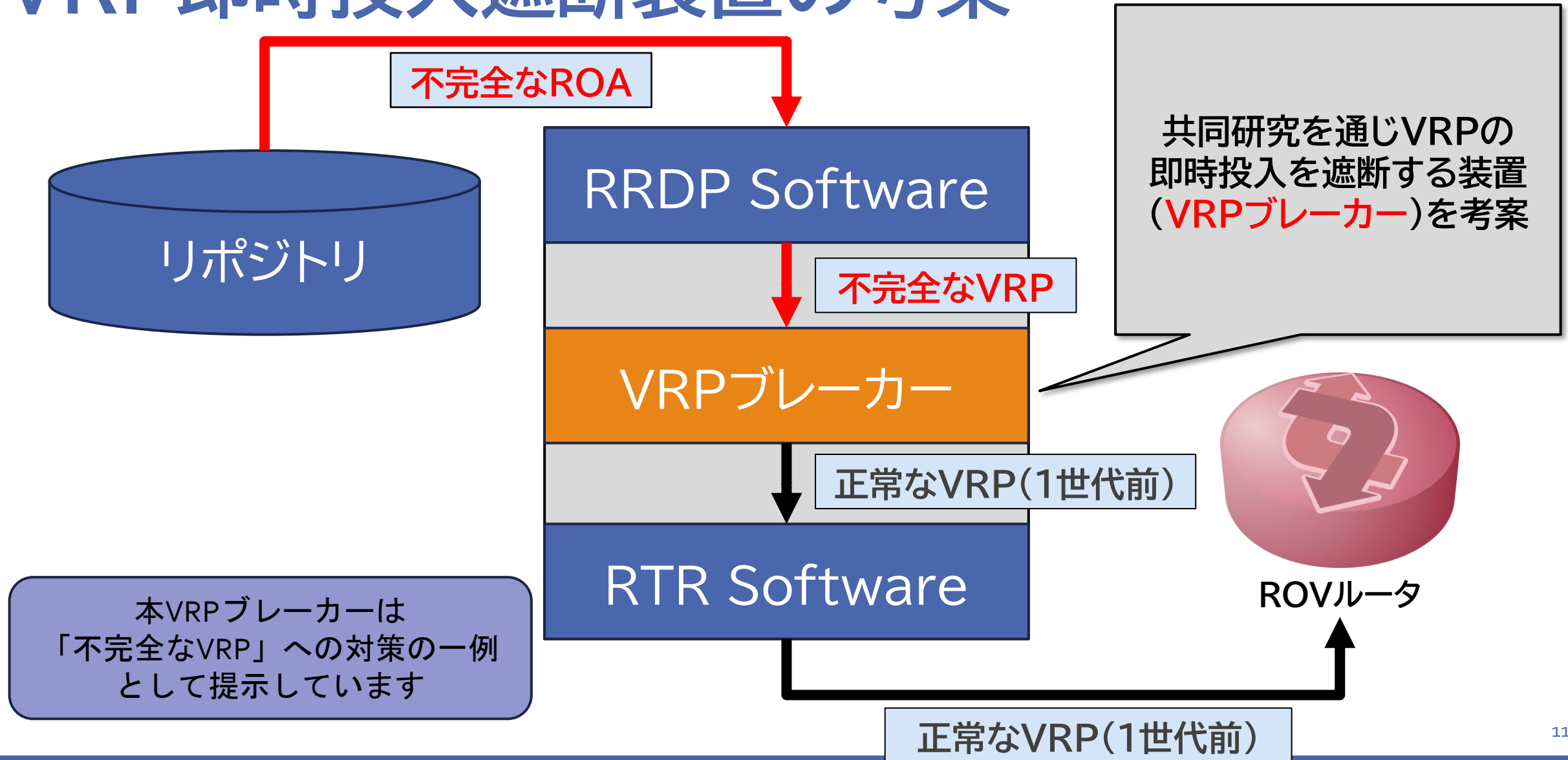
運用・保守

- 継続的な運用・保守の観点から既存のソフトウェアのソースコードは書き換えない

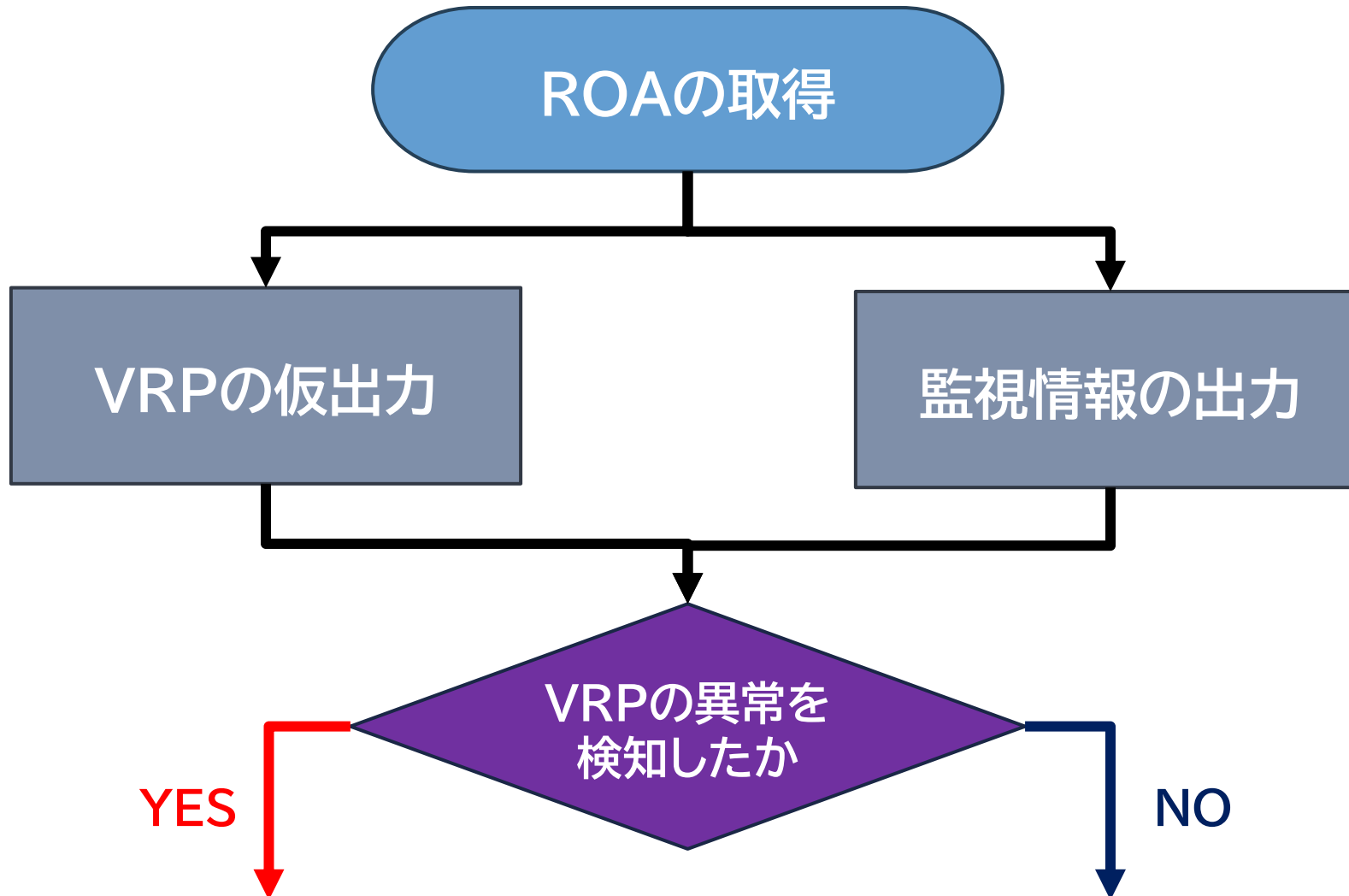
通常のRPKIキャッシュサーバの動作



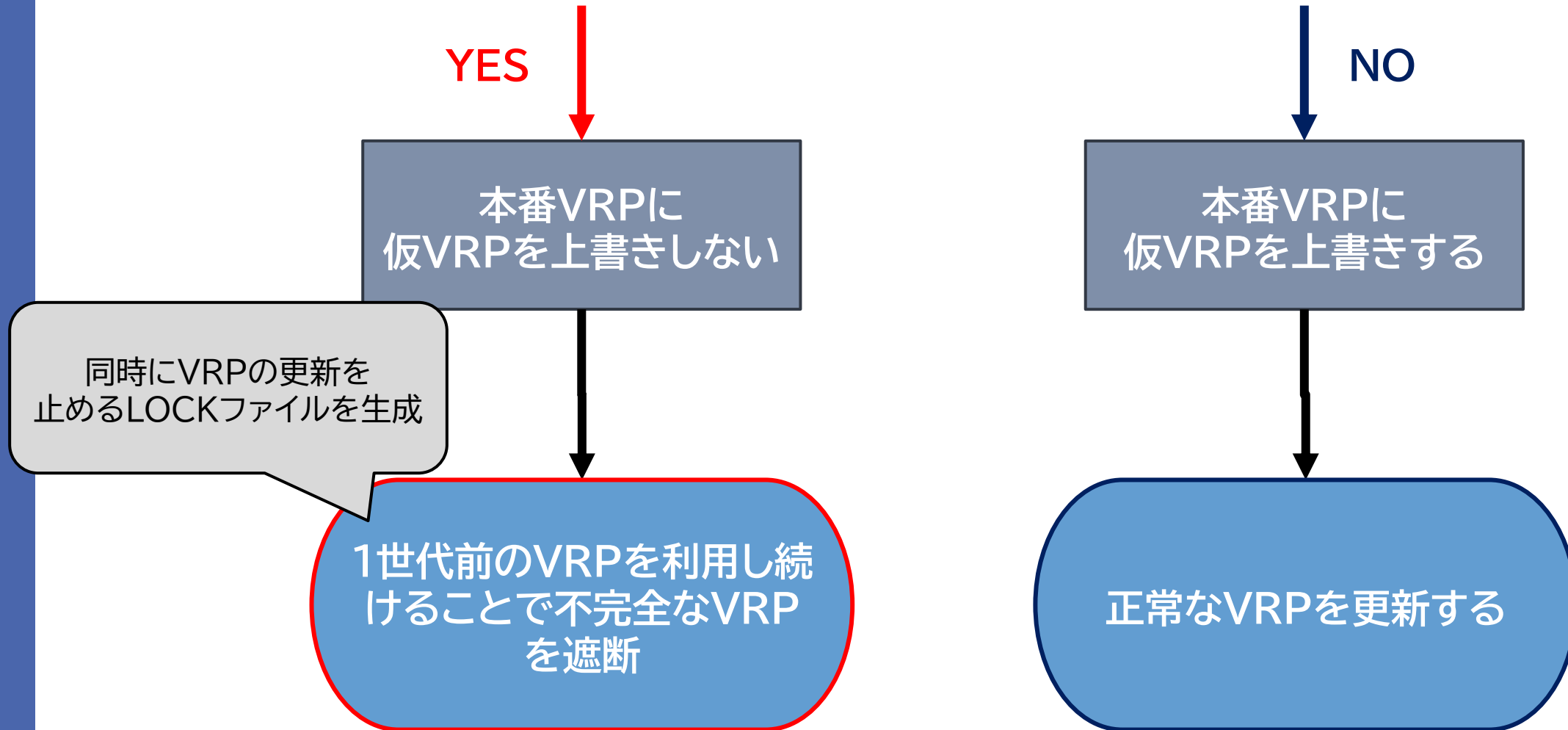
VRP即時投入遮断装置の考案



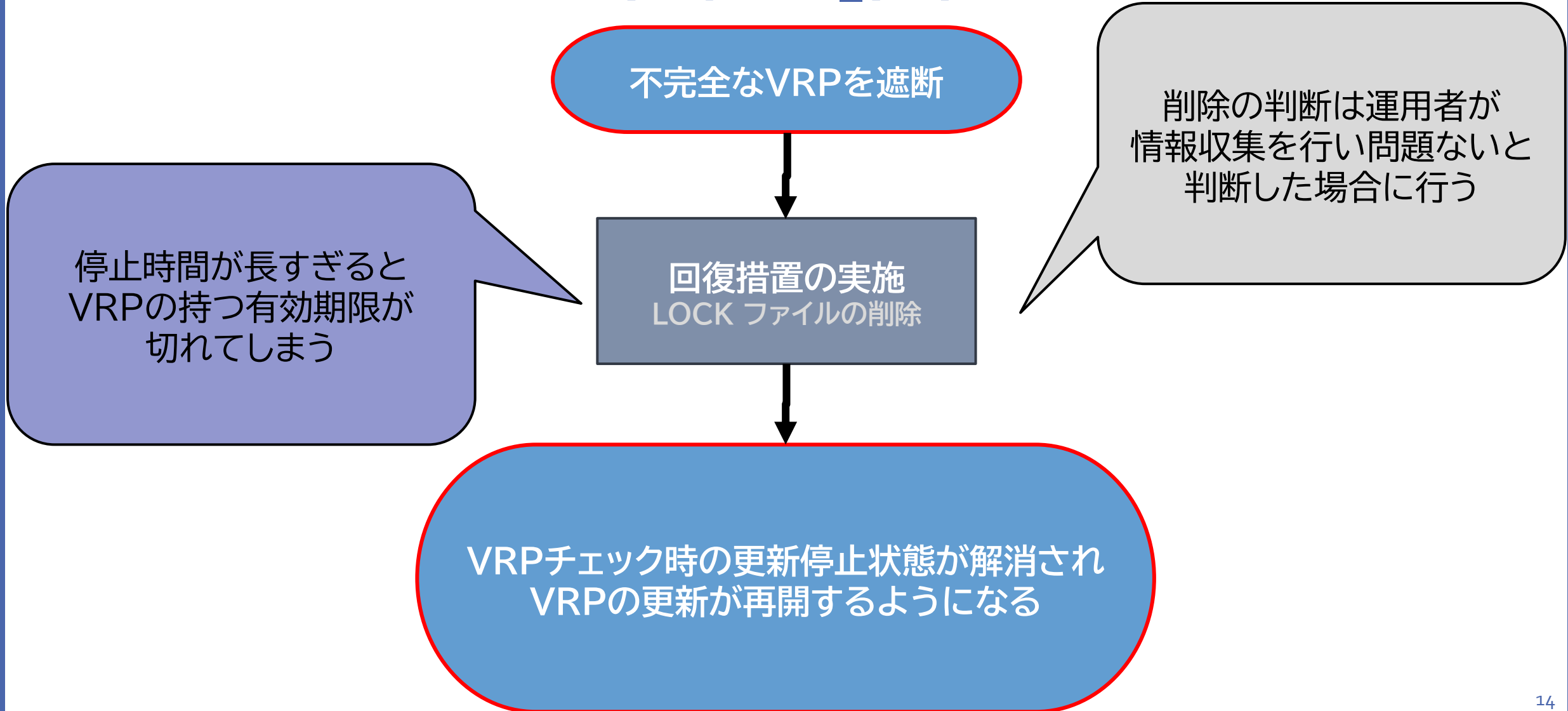
VRPブレーカーの仕組み_検知



VRPブレーカーの仕組み_遮断



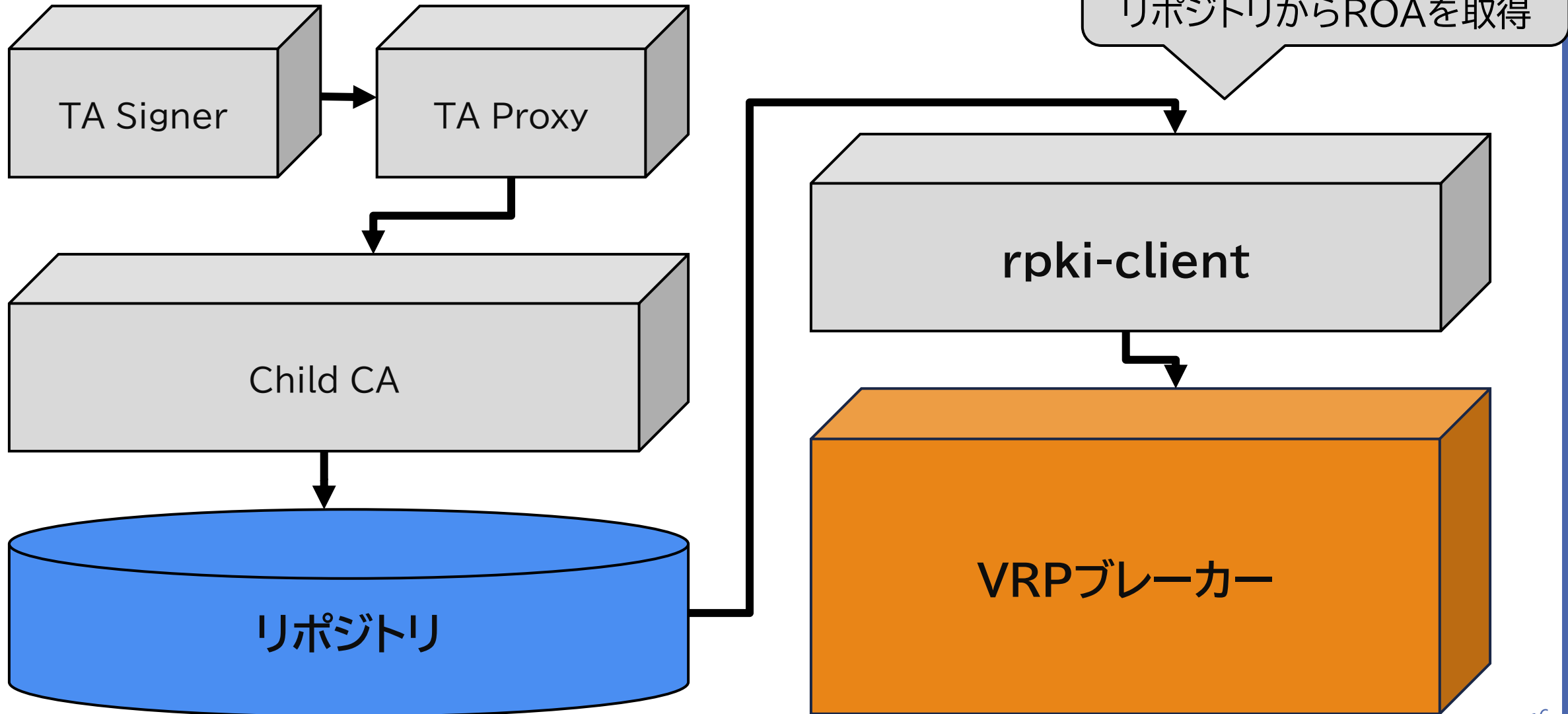
VRPブレーカーの仕組み_再開



VRPブレーカーの動作検証

- 自前のローカルリポジトリを利用
 - 検証中に任意のタイミングでROAの追加や削除を行うため
- 検証内容
 - ROA総数を閾値としてVRPブレーカーを作動させる
 - 特定ROAの存在有無を閾値としてVRPブレーカーを作動させる

VRPブレーカーの動作検証環境



VRPブレーカーの動作検証結果

- ROA総数を閾値とした動作確認

- ROA総数が閾値以下となるようにリポジトリの公開するROA数を減らし、VRPブレーカーの動作を確認
- どこかのリポジトリがダウンしたり、パケットロスなどでROAの取得量が低下した場合にVRPブレーカーが作動することを確認できた

- 特定ROAの存在有無を基準とした動作確認

- 特定ROAをリポジトリから削除し、VRPブレーカーの動作を確認
- 自身のASと密接なASのROAに問題があった場合に早急に察知、対処できるような状態であることが確認できた

VRPブレーカーで守られるインシデント例

- LACNICリポジトリのソフトウェアバグによるROA消失(2024年1月)
 - 署名用ソフトウェアのバグにより全ROAがリポジトリから一時的に消失してしまった
 - **ROA総数を閾値としたブレーカーで守られた事例**
 - <https://packetvis.com/blog/rpki-trust-anchor-malfunctions/>
- Orange EspañaへのRPKI悪用攻撃(2024年1月)
 - 攻撃者がRIPEアカウントを乗っ取り不正なASを広告元とするROAを作成したことで正規経路のRPKIが無効に
 - **特定ROA存在有無の確認により異常を察知できた事例**
 - <https://www.kentik.com/blog/digging-into-the-orange-espana-hack/>

今後の展望

- 不完全なROVとなりうる状態を継続的に調査・観測
 - VRPブレーカーに限らずより信頼性の高いROVを行う方法を模索する
- 「不完全なVRP」問題の存在を多くの場で周知
- インターネットを模擬した環境での継続的な動作検証