RPKIとDNSSEC

社団法人日本ネットワークインフォメーションセンター
木村泰司

内容

- RPKIとは
- 何をするための技術なのか
- RPKIとDNSSECの違うところ
- RPKIとDNSSECの似ているところ
- セキュリティ基盤として見たときの論点

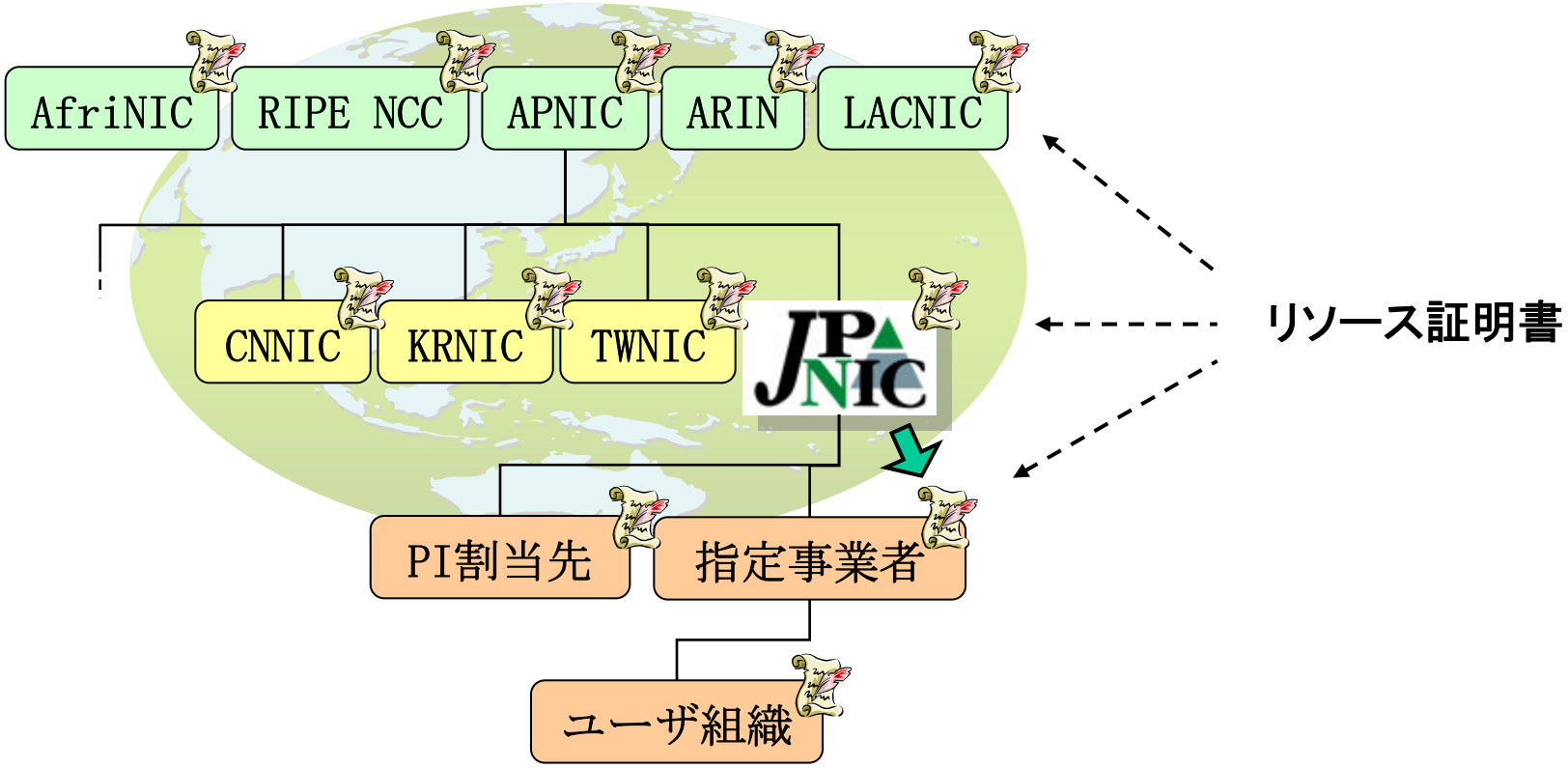
RPKIとは（１ / ４）

Resource PKI (RPKI)

IPアドレスやAS番号といった
アドレス資源のこと

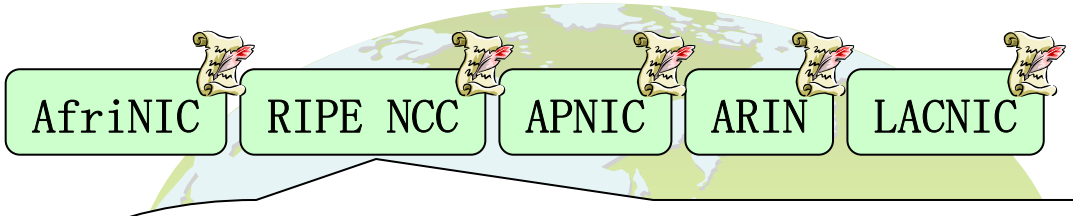
Public-Key Infrastructure
公開鍵基盤のこと

RPKIとは（２／４）



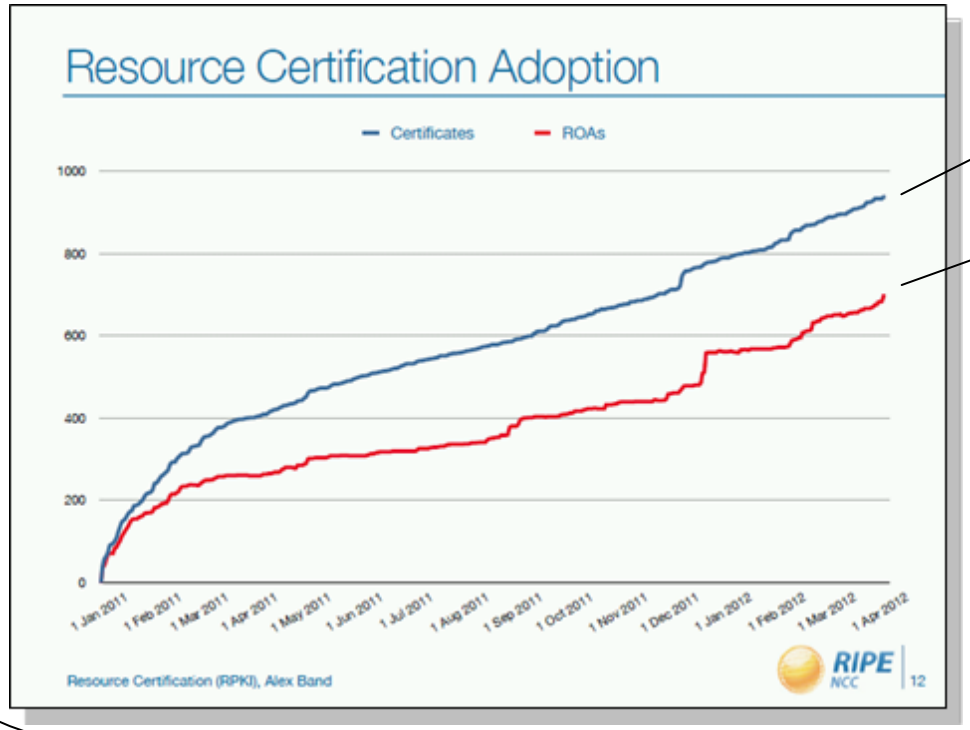
RPKI　＝　アドレス資源が割り振られていることの証明をするための公開鍵基盤　（この証明書はリソース証明書と呼ばれる）

RPKIとは（3 / 4）



すべてのRIRで
提供中（実験含む）

RIPE NCCの場合



900以上

700前後

第64回RIPEミーティングに
おける発表（2012年4月17日）

RPKIとは（４ / ４）

- インターネット経路制御における応用
  - ROA（Route Origination Authorization）を使った BGPメッセージの検証と経路表への反映

```
rpki-rtr>show ip bgp rpki table
1565 BGP sovc network entries using 137720 bytes of memory
1678 BGP sovc record entries using 33560 bytes of memory

Network          Maxlen  Origin-AS  Source  Neighbor
24.232.0.0/16      32      10318      0      193.0.19.44/8282
27.50.32.0/24      24      38186      0      193.0.19.44/8282
27.50.32.0/21      21      6939       0     193.0.19.44/8282
27.50.34.0/24      24      38478      0      193.0.19.44/8282
:
```

イメージ

```
rpki> show validation statistics
Total RV records: 2167
Total Replication RV records: 2167
  Prefix entries: 2019
  Origin-AS entries: 2167
Memory utilization: 442765 bytes
Policy origin-validation requests: 144362365
  Valid: 604484
  Invalid: 557774
  Unknown: 143200107
BGP import policy reevaluation notifications: 33639
  inet.0, 33639
  inet6.0, 0
```

イメージ

何をするための技術なのか（1/2）

- RPKI
  - IPアドレスが正しいものかどうかを確かめられる
    - レジストリによって正しく割り振られたものか
    - エンドサイトに正しく割り当てられたものか
  - 不正なインターネット経路制御の影響を小さくする

何をするための技術なのか（２ / ２）

- DNSSEC
  - リソースレコードが正しいことを確かめられる
  - リソースレコードが書き換えられたときに見つけられる
  - リソースレコードを使ってデータを伝える（!?）
    - DANEやROVER

RPKIとDNSSECの違うところ

	RPKI	DNSSEC
グローバルなトラストアンカーは何か	RIRかIANA	ルートゾーン
運用としてすること	割り振りに応じた証明書発行 ルーター内の不正経路情報の扱い	ゾーン情報の登録に応じた署名 キャッシュサーバにおける署名検証と応答
運用の関係者	レジストリ（アドレス）、ASのオペレーター	レジストリ（ドメイン名）、レジストラ、ゾーン管理者
“普及”の母数	AS数(*1) 40,907 Prefix数(*1) 408,679 BGPルーター数	ドメイン名登録数(*2) 約2億2,500万件 ＃ゾーン署名(*3) 9,556 キャッシュサーバ数

*1 CIDR Report http://www.cidr-report.org/as2.0/ 2012年4月17日時点
*2 ドメイン名業界概要報告 http://www.verisigninc.com/assets/domain-name-brief-march2012-ja.pdf
*3 http://scoreboard.verisignlabs.com/

RPKIとDNSSECの似ているところ

- 鍵管理が必要なところ
  - 秘密鍵のセキュリティ／鍵更新
- 有効性の扱い方がまだわかっていないところ
  - 検証できなかった場合、使えなくなってもいいか／有効であれば全て信じてもいいか
- デプロイメントの仕方
  - レジストリで導入されつつある

セキュリティ基盤として見たときの論点

セキュリティ基盤として見たときの論点1

- 目指しているものと効用
  - DNSのセキュリティが確保されることでアプリケーションにどのような安全がもたらす事ができるのか
    - Webのセキュリティに対するDNSの正しさ
  - ゾーン管理者はどの程度ゾーンの正しさを担保できるのか
    - DANEを使ったSSL証明書の正しさ／信頼の置き所

セキュリティ基盤として見たときの論点2

- 手段と目的
  - DNSという名前解決の手段にセキュリティを確保することで、何がどのようによくなるのか
    - キャッシュポイズニングの被害を低減？
  - 仕組みを維持するために必要な労力に見合うセキュリティ・メリットが得られるのか

おわり