PKIの標準化動向とリソースPKI

JPNIC　セキュリティ事業担当
木村泰司

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

内容

- RFC5280
  - インターネットPKIの標準化動向として、一年ほど前にでたRFC5280を紹介します。

- リソースPKI (RPKI)
  - IPアドレス管理を正しく管理するために、国際的に検討と実装が進められているRPKIを紹介します。

RFC5280

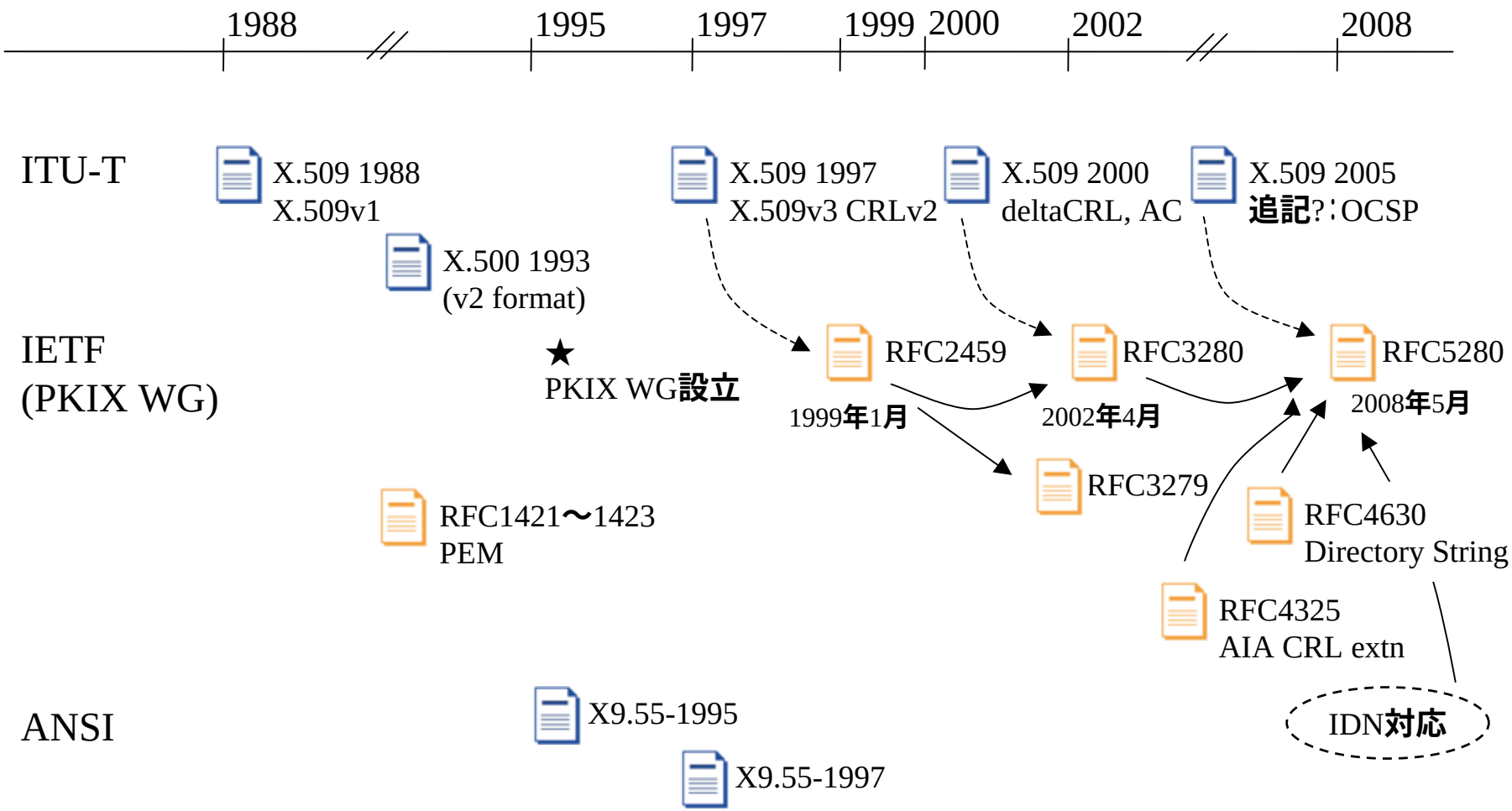
- RFC5280
- RFC3280**との違い**
- **インターネット**PKI**の標準と現実**

RFC5280

RFC5280 (1/4)

- RFC5280とは
  - 「X.509-based PKI」の「X.509証明書とCRL」のプロファイル
  - 2008年5月にpublished

RFC5280 (2/4)


1988
1995
1997
1999
2000
2002
2008
ITU-T
X.509 1988
X.509v1
X.509 1997
X.509v3 CRLv2
X.509 2000
deltaCRL, AC
X.509 2005
追記?：OCSP
X.500 1993
(v2 format)
IETF
(PKIX WG)
★
PKIX WG設立
RFC2459
1999年1月
RFC3280
2002年4月
RFC5280
2008年5月
RFC3279
RFC1421～1423
PEM
RFC4630
Directory String
RFC4325
AIA CRL extn
IDN対応
ANSI
X9.55-1995
X9.55-1997

RFC5280 (3/4) - PKIX WGのRFC

- **基本的**
  - 3279 Algorithm ID
  - 3281 Attribute Certificate
  - 3874 SHA-224
  - 4055 Additional ID for RSA
  - 4158 Path building
  - 4476 AC Policy Extension
  - 4491 GOST
  - **5280 Certificate and CRL Profile**
- **応用的**
  - 3161 Time-Stamp Protocol
  - 3628 Time-Stamping Authority
  - 3709 Logotypes
  - 3739 Qualified Certificate
  - 3779 IP Address and ASN
  - 3820 Proxy Certificate
  - 4334 WLAN
  - 4043 Permanent ID
  - 4059 Warranty Certificate
  - 4683 SIM
  - 4985 Service Name
- **オンライン系**
  - 2585 Operational Protocols
  - 2560 OCSP
  - 5019 Lightweight OCSP
  - 3029 DVCS
  - 3379 DPV/DPD
  - 3494 LDAPv2
  - 4386 Repository Locator Service
  - 4387 Cert store via http
  - 5055 SCVP
- **その他**
  - 2528 Representation of KEA
  - 2875 DH Proof-of-Possession
  - 3647 CP and CPS
  - 4210 CMP
  - 4211 CRMF
  - 4523 LDAP Schema
  - 5272 CMC
  - 5274 CMC: Compliance Requirement
  - 5273 CMC: Transport Protocol

JPNIC

RFC5280の概要 (4/4)

	タイトル (英語)	頁数	内容
1	Introduction	2	章立て、RFC3280との違い
2	Requirements and Assumptions	2	証明書とは何か、どう使われるものか
3	Overview of Approach	8	CAの役割と証明書の有効性
4	Certificate and Certificate Extensions Profile	38	証明書のデータ構造
5	CRL and CRL Extensions Profile	17	証明書失効リストのデータ構造
6	Certification Path Validation	24	証明書の検証処理
7	Processing Rules for Internationalized Names [New]	5	名称欄の国際化対応の処理
8	Security Considerations	1	PKIのセキュリティに関する留意事項
9	IANA Considerations	1	OIDの管理

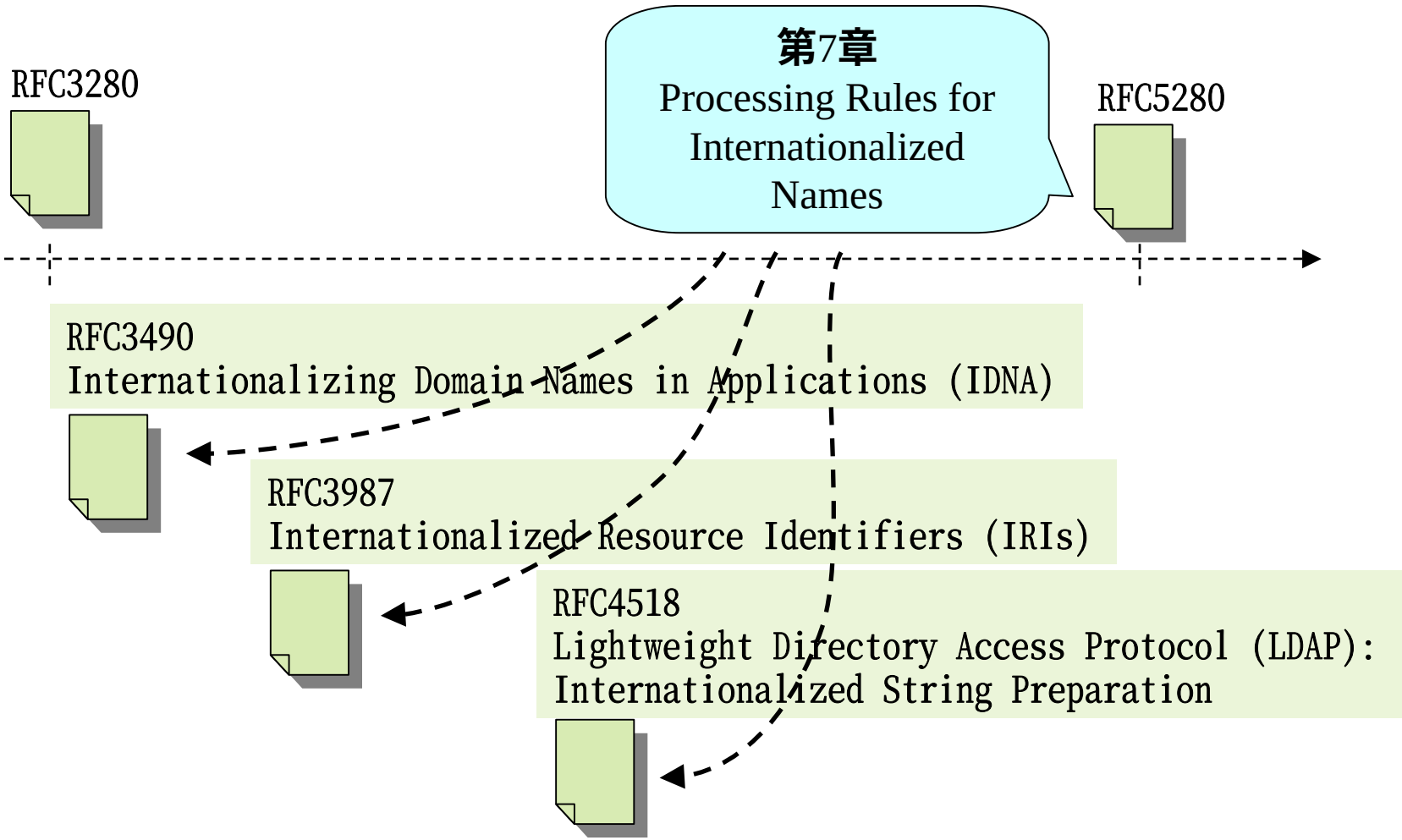
RFC3280との違い

RFC3280との違い

- IDN（国際化ドメイン名）対応（7章）
  - RFC3490 Internationalizing Domain Names in Applications (IDNA)
  - RFC3987 Internationalized Resource Identifiers (IRIs)
  - RFC4518 Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
- Issuer/Subjectのエンコーディングルール（4.1.2.4節, 4.1.2.6節）
  - 「2003年12月31日にUTF8Stringへ移行」を削除
  - 「name rollover」などの記述も削除
- privateKeyUsagePeriodの記述を削除（4.2.1.4節）
- ポリシーマッピングをcriticalに（4.2.1.5節）
- ポリシー制約拡張をcriticalに（4.2.1.11節）
- CRL拡張のauthority Info. accessを追加（5.2.7節） RFC4325
- 認識されないCRL拡張などの扱いを追加（5.2節, 5.3節）
- holdInstructionCode CRLエントリー拡張を削除（5.3.2節）
- CPのcriticalityをRPに返さないようになった（6章）
- security considerationの改良（8章）

LDAP string preparation（RFC4518）に則った変換ルール
＋
格納と比較

IDNへの対応 (1/2)


RFC3280
第7章
Processing Rules for Internationalized Names
RFC5280
RFC3490
Internationalizing Domain Names in Applications (IDNA)
RFC3987
Internationalized Resource Identifiers (IRIs)
RFC4518
Lightweight Directory Access Protocol (LDAP):
Internationalized String Preparation

IDNへの対応 (2/2)

		RFC3280	RFC5280
1	DN(Distinguished Name)	teletexString, printableString, universalString, BMPString, UTF8String (2003年12月31日以降はUTF8String形式のみ) 比較はバイナリ比較	UTF8String, printableString (teletexString, BMPString, universalStringはCAで使用中の場合は使用可) 比較はRFC4518にのっとる。
2	拡張フィールド subjectAltNameや issuerAltNameなど	IA5String (ASCII)	IA5String (RFC3490のASCII変換方法にのっとる)
3	issuerやsubjectに含まれるIDN 及びメールアドレス		RFC3490のToASCII変換が行われ、大文字小文字を区別せずに比較する。(メールアドレスのローカル部は区別)
4	IRI (Internationalized Resource Identifiers) (UnicodeのURI)		RFC3987のASCII変換が行われ、subjectAltNameにIA5Stringで入っている場合、%XXなどを戻して比較する。

UTF8に関する日本勢の活躍

- PKI における UTF8String 問題に関する調査
  - 情報処理振興協議会（IPA）、日本ネットワークセキュリティ協会（JNSA）
  - 報告書
    - Part 1：UTF8String 問題の解説と提言
    - Part 2：PKI 利用製品の UTF8String 項目実装の現状
    - Part 3：東アジア圏における公開鍵証明書の状況
    - Part 4：IETF における標準化動向
    - Part 5：UTF8String 問題を検証するためのテストケース
    - Part 6：公開鍵証明書発行に関する移行ガイド
- 国際化対応I-D（International Strings in Certificate）の著者 Paul Hoffman氏との調整（IETF-61, 2004/11）

- http://www.ipa.go.jp/security/pki/utf8string/utf8string.html

ポリシーマッピング拡張

- ポリシーマッピング拡張の扱い

証明書に入れるなら必ずcritical。
（X.509 2000で「criticalでないとCAの決めごとを正しく解釈できない」）

		ポリシーマッピング拡張（Mapping）	
		存在しない	critical
証明書ポリシー拡張（CP）	non-critical	CPを無視できる	（Mappingを無視できない）
	critical	CPを無視できない	両方を無視できない

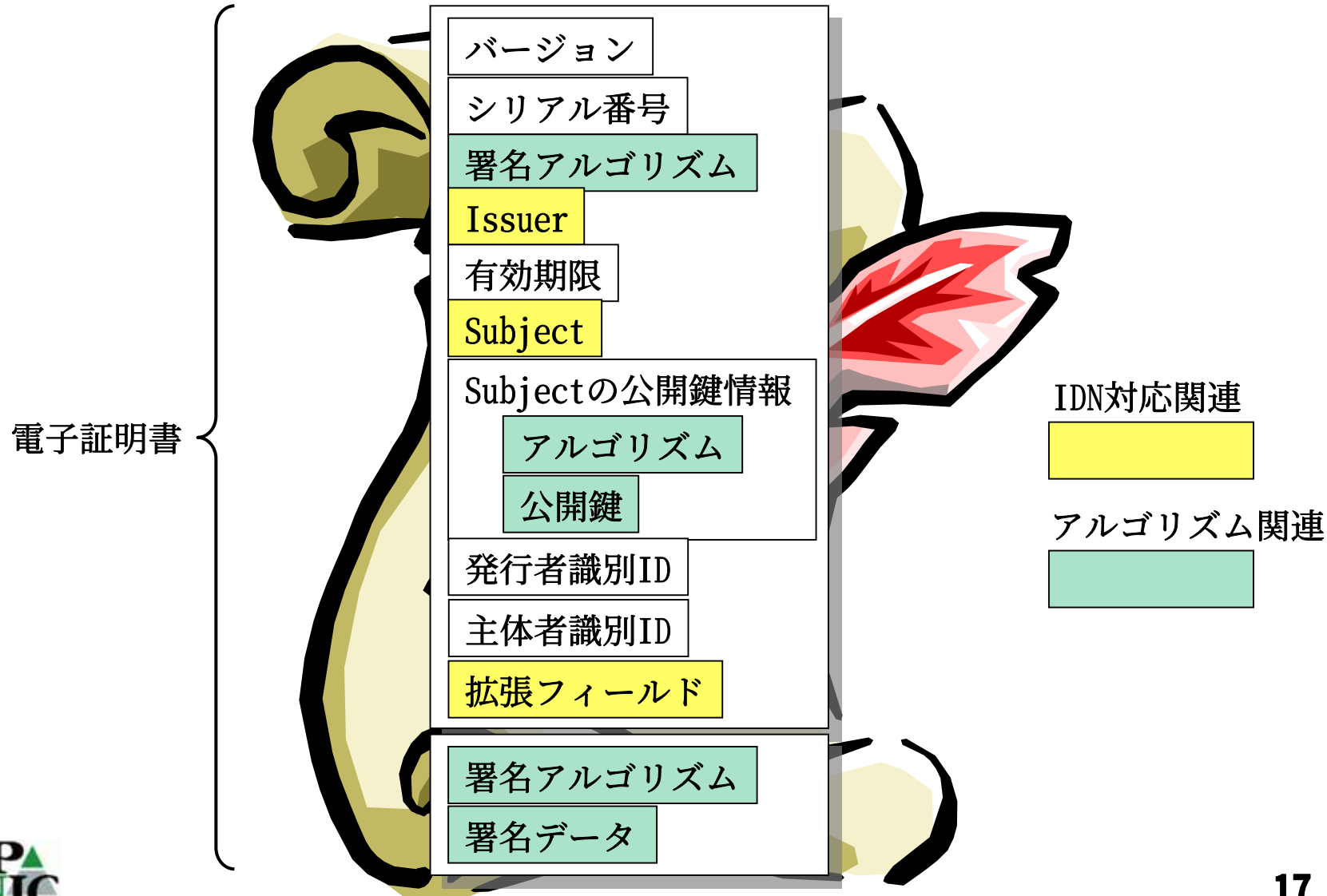
補足：証明書ポリシー

- **証明書ポリシー** (Certificate Policies) – CA,EE
  - critical / non-critical
  - **証明書ポリシー**OID　**例**：2 5 2 9 35 0
- **ポリシーマッピング** (Policy Mappings) - CA
  - **入れるなら**critical
  - **ペア**：issuerDomainPolicy / subjectDomainPolicy
- **ポリシー制約拡張** (Policy Constraints) - CA
  - **証明書パス中の証明書に対して、特定のポリシー**ID**のみを許可でしたり、ポリシーマッピングを禁止したりする証明書拡張**
    - requireExplicitPolicy　**ポリシーを無視できる段数**
    - inhibitPolicyMapping　**マップできる段数**

RFC5280関連情報

X.509証明書で使うことができるアルゴリズム総覧

X.509証明書


電子証明書
バージョン
シリアル番号
署名アルゴリズム
Issuer
有効期限
Subject
Subjectの公開鍵情報
アルゴリズム
公開鍵
発行者識別ID
主体者識別ID
拡張フィールド
署名アルゴリズム
署名データ
IDN対応関連
アルゴリズム関連

X.509証明書で使うことができる（証明書用）署名アルゴリズム

証明書用の署名アルゴリズム	RFCと章	署名形式
Rivest-Shamir-Adelman (RSA)	rfc3279 2.2.1	md2WithRSAEncryption md5WithRSAEncryption sha-1WithRSAEncryption
	rfc4055 5 (PKCS#1 Version 1.5)	sha224WithRSAEncryption sha256WithRSAEncryption sha384WithRSAEncryption sha512WithRSAEncryption
Digital Signature Algorithm (DSA)	rfc3279 2.2.2	id-dsa-with-sha1
Elliptic Curve Digital Signature Algorithm (ECDSA)	rfc3279 2.2.3	ecdsa-with-SHA1
RSA Probabilistic Signature Scheme (RSASSA-PSS)	rfc4055 3.1	RSASSA-PSS-params (SHA-1使用)
GOST R 34.10-94	rfc4491 2.2.1	id-GostR3411-94-with-GostR3410-94
GOST R 34.10-2001	rfc4491 2.2.2	id-GostR3411-94-with-GostR3410-2001

SHA-2は
draft段階

X.509証明書で使うことができるSubjectの公開鍵暗号アルゴリズム

公開鍵暗号アルゴリズム	RFCと章	keyUsage	
Rivest-Shamir-Adelman (RSA)	rfc3279 2.3.1	EE: digitalSignature nonRepudiation keyEncipherment dataEncipherment	CA or CRL issuer: digitalSignature nonRepudiation keyEncipherment dataEncipherment keyCertSign cRLSign
Elliptic Curve Digital Signature Algorithm (ECDSA) Elliptic Curve Diffie-Hellman (ECDH)	rfc3279 2.3.5	EE: digitalSignature nonRepudiation keyAgreement encipherOnly or deciphyerOnly	CA or CRL Issuer: digitalSignature nonRepudiation keyAgreement or keyCertSign cRLSign

X.509証明書で使うことができるSubjectの公開鍵暗号アルゴリズム

公開鍵暗号アルゴリズム	RFCと章	keyUsage
Diffie-Hellman (DH)	rfc3279 2.3.3	keyAgreement encipherOnly or decipherOnly
Key Encryption Algorithm (KEA)	rfc3279 2.3.4	keyAgreement encipherOnly or decipherOnly

X.509証明書で使うことができるSubjectの鍵確立用のアルゴリズム

鍵確立用のアルゴリズム	RFCと章	ハッシュアルゴリズム
RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) [PKCS#1 v2.1]	rfc4055 4	SHA-1 (default) (MUST) SHA-224 (MAY) SHA-256 (MAY) SHA-384 (MAY) SHA-512 (MAY)
GOST R 34.10-94	rfc4491 2.2.1	GOST R 34.11-94
GOST R 34.10-2001	rfc4491 2.2.2	GOST R 34.11-94
Elliptic Curve Diffie-Hellman (ECDH)	rfc3279 2.2.3 rfc5480 2.1.2	SHA-1
Elliptic Curve Menezes-Qu-Vanstone (ECMQV)	rfc5480 2.1.2	SHA-1(?)

X.509証明書で使える ハッシュアルゴリズム

ハッシュアルゴリズム	RFCと章	ビット数
MD2 [rfc1319]	rfc3279 2.2.1	128
MD5 [rfc1321]	rfc3279 2.2.2	128
SHA-1 [FIPS180-1] [rfc3174]	rfc3279 3.1.3	160
SHA-224 [PKCS#1 ver1.5]	rfc4055 5	224
SHA-256 [PKCS#1 ver1.5]	rfc4055 5	256
SHA-384 [PKCS#1 ver1.5]	rfc4055 5	384
SHA-512 [PKCS#1 ver1.5]	rfc4055 5	512
GOST R 34.11-94 [GOSTR341194]	rfc4911 2.2.1	256

インターネットPKIの標準化と現実

標準化と現実

	インターネットPKIの標準	インターネットPKIの現実
証明内容と見え方	証明書ポリシーはOID ポリシーマッピング	EV SSL / 組織認証 / ドメイン認証
証明書の表示	主に識別子の議論 有効性表示の議論はなし	ブラウザ依存
証明書 (失効) 検証	OCSP, DVCS, DPV/DPD, SCVP	CRL?
アルゴリズム	徐々に対応してきた	利用環境や認証局の対応

「code then spec.」
動くものをつくろう

やりたいことを思い出そう
- Webの信頼性
- 文書の信頼性
- コードの信頼性

元々は・・・

ここまでのまとめ

- RFC5280
  - RFC3280**との違い**
  - **証明書で使えるアルゴリズム**

リソースPKIの動向

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

リソースPKI

- リソースPKIの背景
- リソース証明書とは
- 国際動向（IETF SIDR WGとRIR）

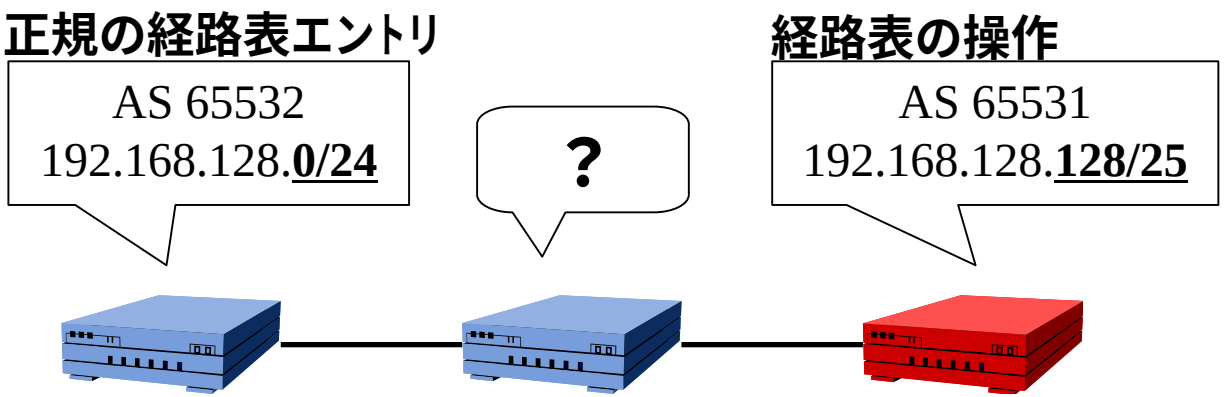
リソースPKIの背景

インターネットルーティングにおけるセキュリティと
アドレス資源の不正利用

JPNIC 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

リソースPKIの背景 (1)

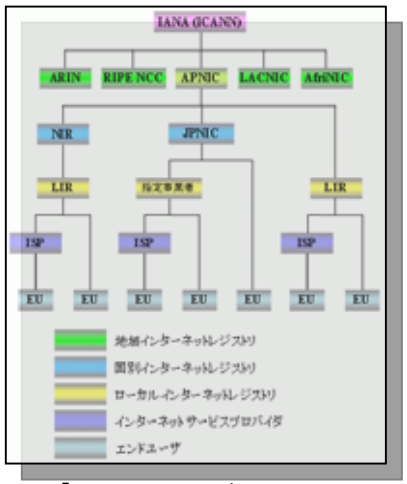
- インターネットルーティング (経路制御) におけるセキュリティ
  - **経路ハイジャック**
    - BGPでのIPアドレスやAS番号の不正利用
      (広義には、不正なASパスも含む)



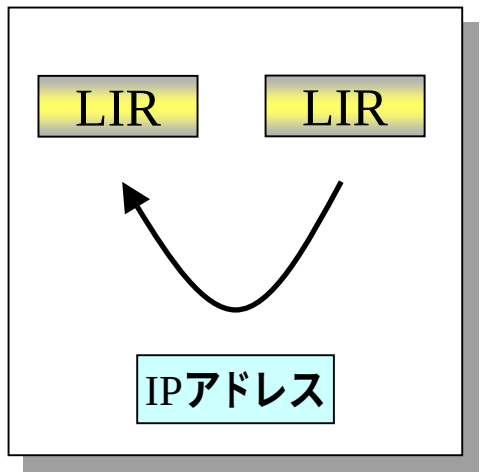
経路情報の発信元が正しいかどうかを検証することが必要

リソースPKIの背景 (2)

- IPv4アドレスの在庫枯渇期におけるセキュリティ
  - **アドレス資源の不正利用**
    - IPアドレスやAS番号の不正な利用や、利用権利の主張など



インターネットレジストリシステム
⇒ whois？



IPアドレスの移転

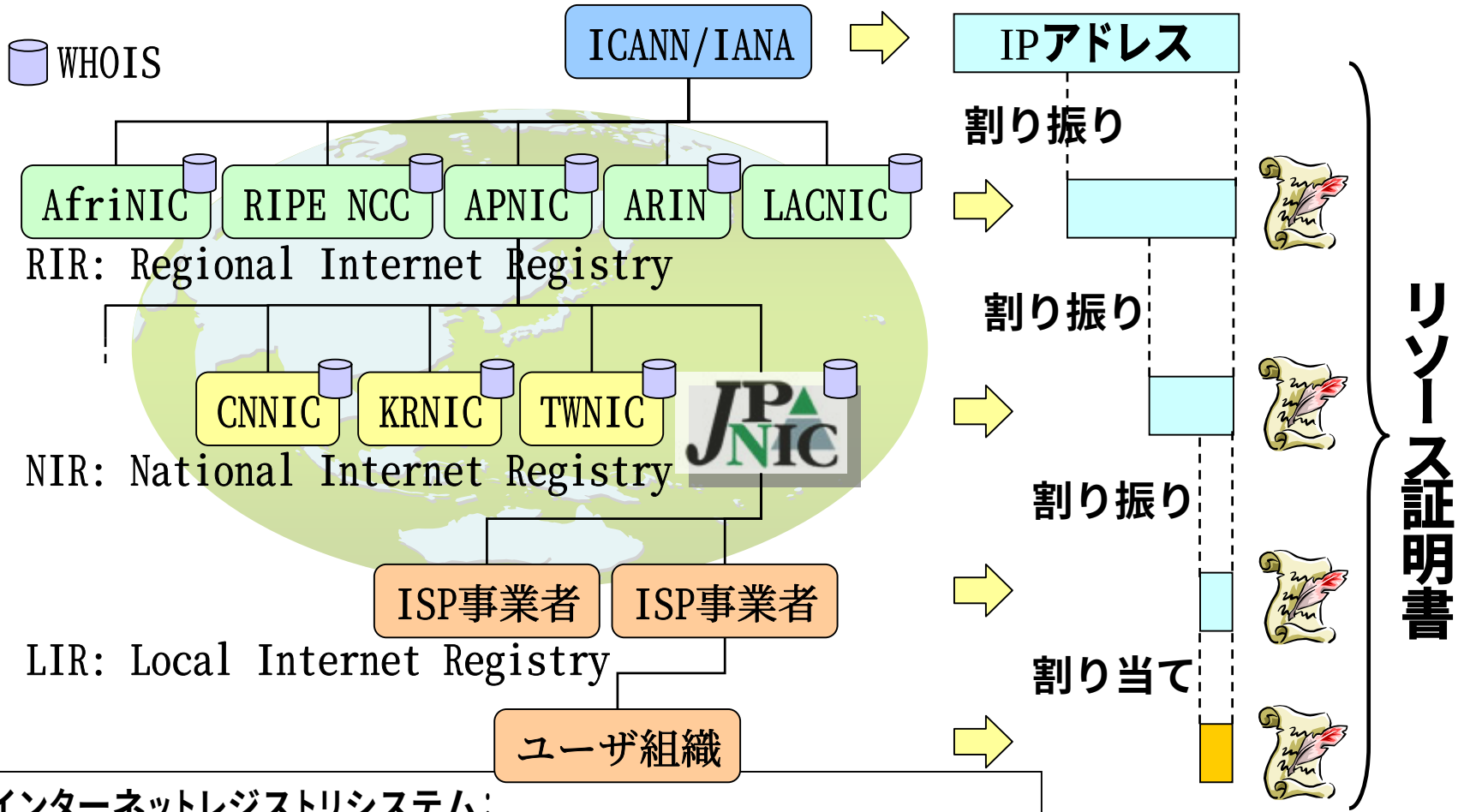
IPアドレスの利用権利を示すデータが必要

リソース証明書とは

IPアドレスとAS番号の利用権を示す電子証明書

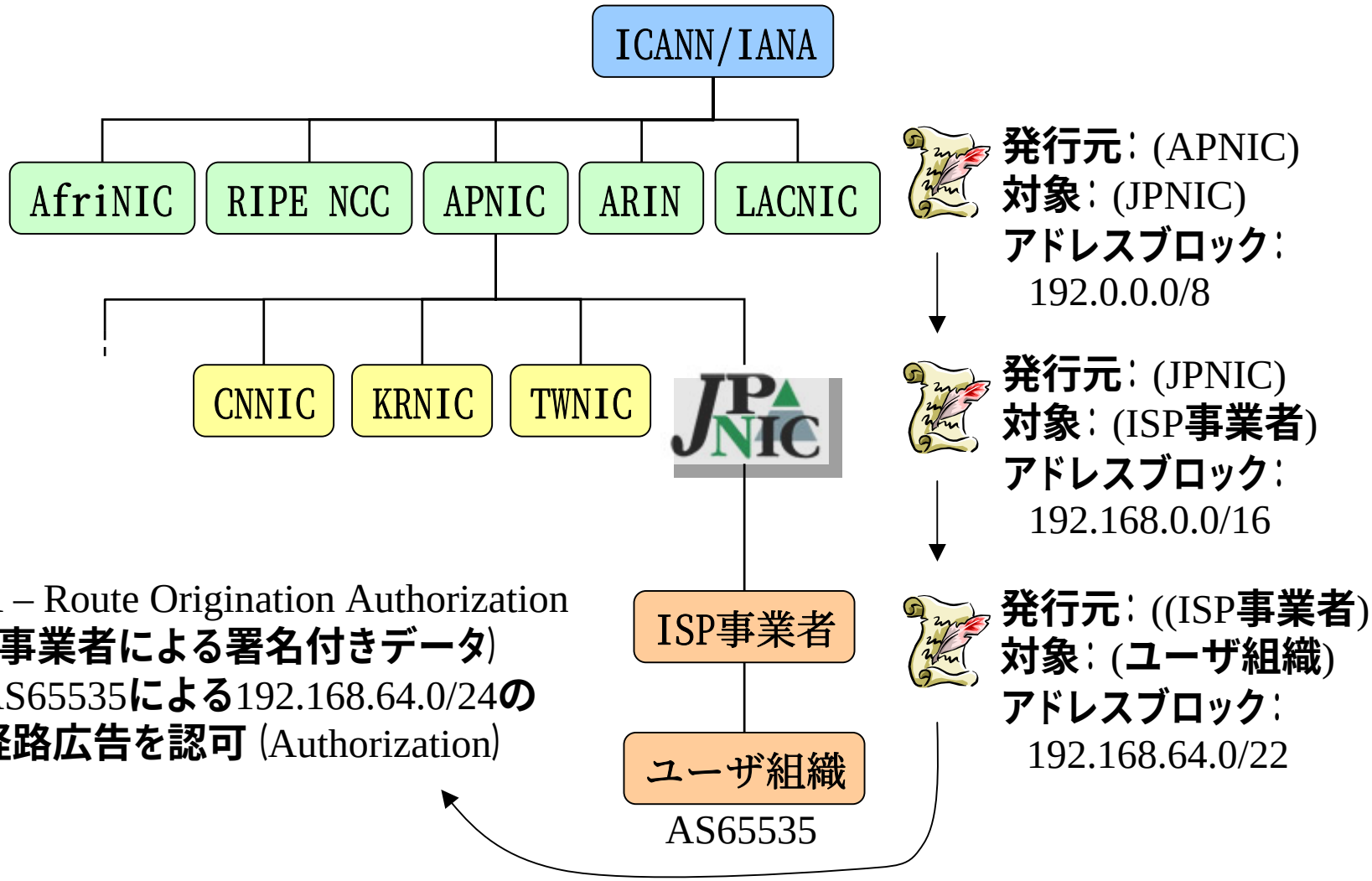
JPNIC 社団法人 日本ネットワークインフォメーションセンター

インターネットレジストリとリソース証明書



インターネットレジストリシステム:
IPアドレスの一意性を保証し経路制御の適応性を向上させる仕組み

ツリー構造


ICANN/IANA
AfriNIC
RIPE NCC
APNIC
ARIN
LACNIC
CNNIC
KRNIC
TWNIC
JPNIC
ISP事業者
ユーザ組織
AS65535
発行元：(APNIC)
対象：(JPNIC)
アドレスブロック：
192.0.0.0/8
発行元：(JPNIC)
対象：(ISP事業者)
アドレスブロック：
192.168.0.0/16
発行元：((ISP事業者)
対象：(ユーザ組織)
アドレスブロック：
192.168.64.0/22
ROA – Route Origination Authorization
(ISP事業者による署名付きデータ)
・AS65535による192.168.64.0/24の
経路広告を認可 (Authorization)

リソース証明書のプロファイル

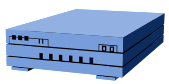
発行元：(RIPE NCC)
対象：(JPNIC)
アドレスブロック：
10.0.56.0/21

Version: 3
Serial: 3fc2
Issuer: CN=0NzrOpdx0k5_wB44AhMeNzEc0Mk
Not Before: 2008**年**10**月**30**日** 15:52:32
Bot After: 2009**年**7**月**1**日** 9:00:00
Subject: CN=0a8f65ba-d8e2-4759-b73c-8913ffc731f2
Subject Key Identifier: 22d85f282bdf913326cf29d2149a26d82ac37fe4
Authority Key Identifier: d0dceb3a9771d24e7fc01e3802131e37311cd0c9
Authority Info Access: CA Issuers:
URI: rsync://certtest.ripe.net/certrepo/4e/2df8f5-18be-4542
-b991-d2dde6d19ebb/1/0NzrOpdx0k5_wB44AhMeNzEc0Mk.cer
Subject Info Access: caRepository -
URI: URI:rsync://certtest.ripe.net/certrepo/16/135b01-8cde-4286
-aa68-5d517f5e2c1b/1/IthfKCvfkTMmzynSFJom2CrDf-Q.roa
CRL Distribution Points:
URI:rsync://certtest.ripe.net/certrepo/16/135b01-8cde-4286-aa68
-5d517f5e2c1b/1/0NzrOpdx0k5_wB44AhMeNzEc0Mk.crl
Certificate Policies: critical 1.3.6.1.5.5.7.14.2
sbgp-ipAddrBlock: IPv4: 10.0.56.0/21

利用法(1) セキュアルーティング

インターネット

Secure BGPなど



ルータ

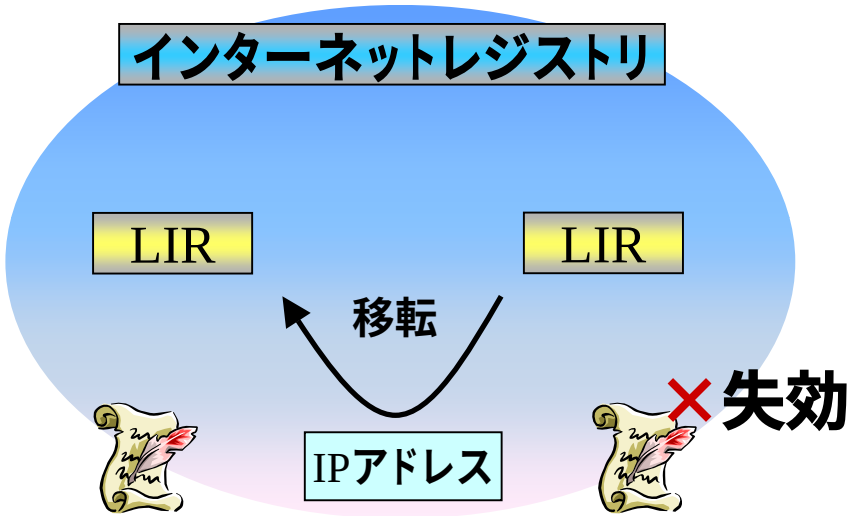
経路情報
Origin AS: AS65532
Prefix: 192.168.128.0/24

＋

ROA

ROAとリソース証明書の検証を行い、経路情報の発信元(Origination)が正しいことを確認する

利用法 (2) アドレス資源の利用権利

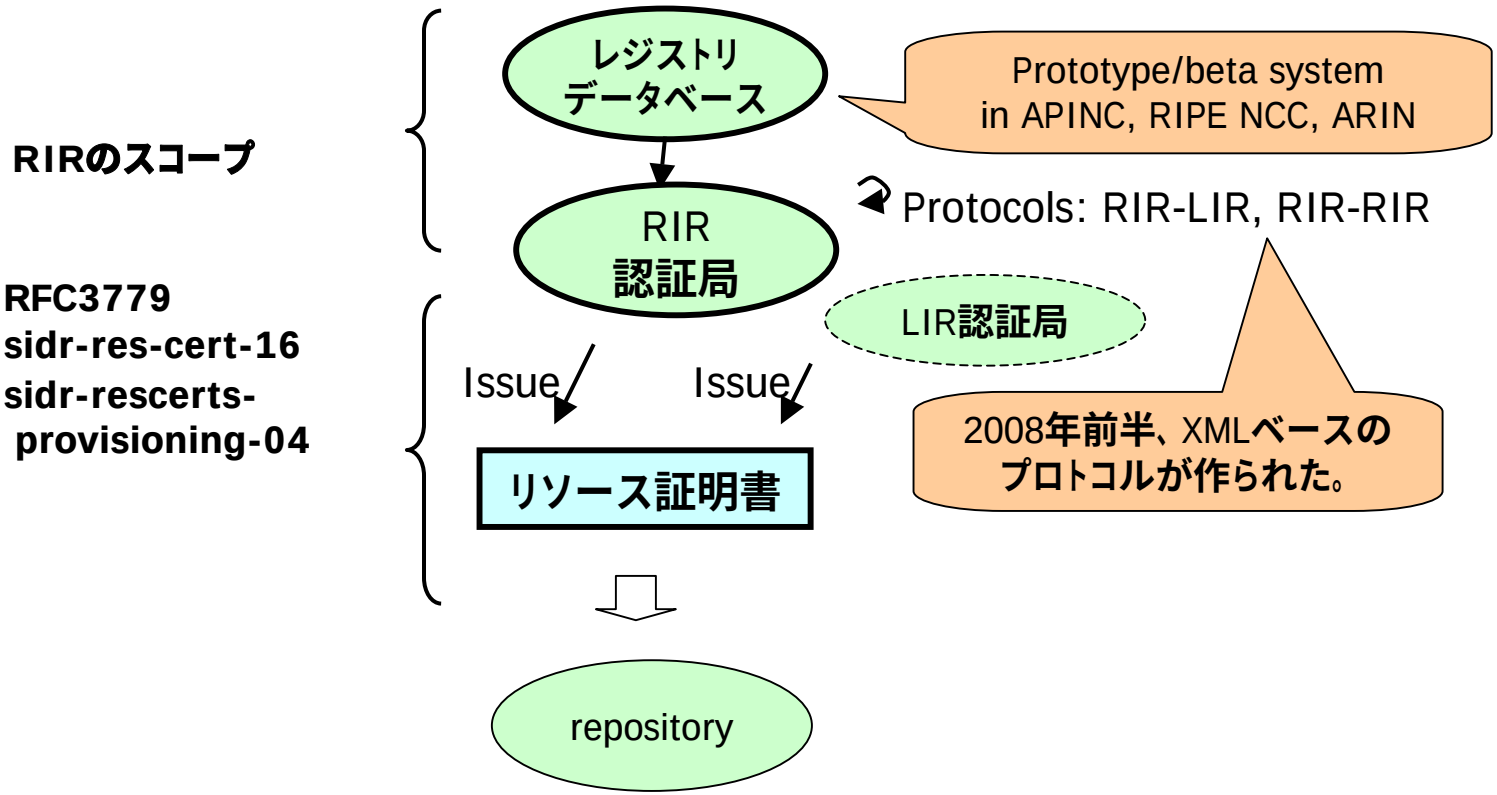


一意なIPアドレスの利用権利を確認できる

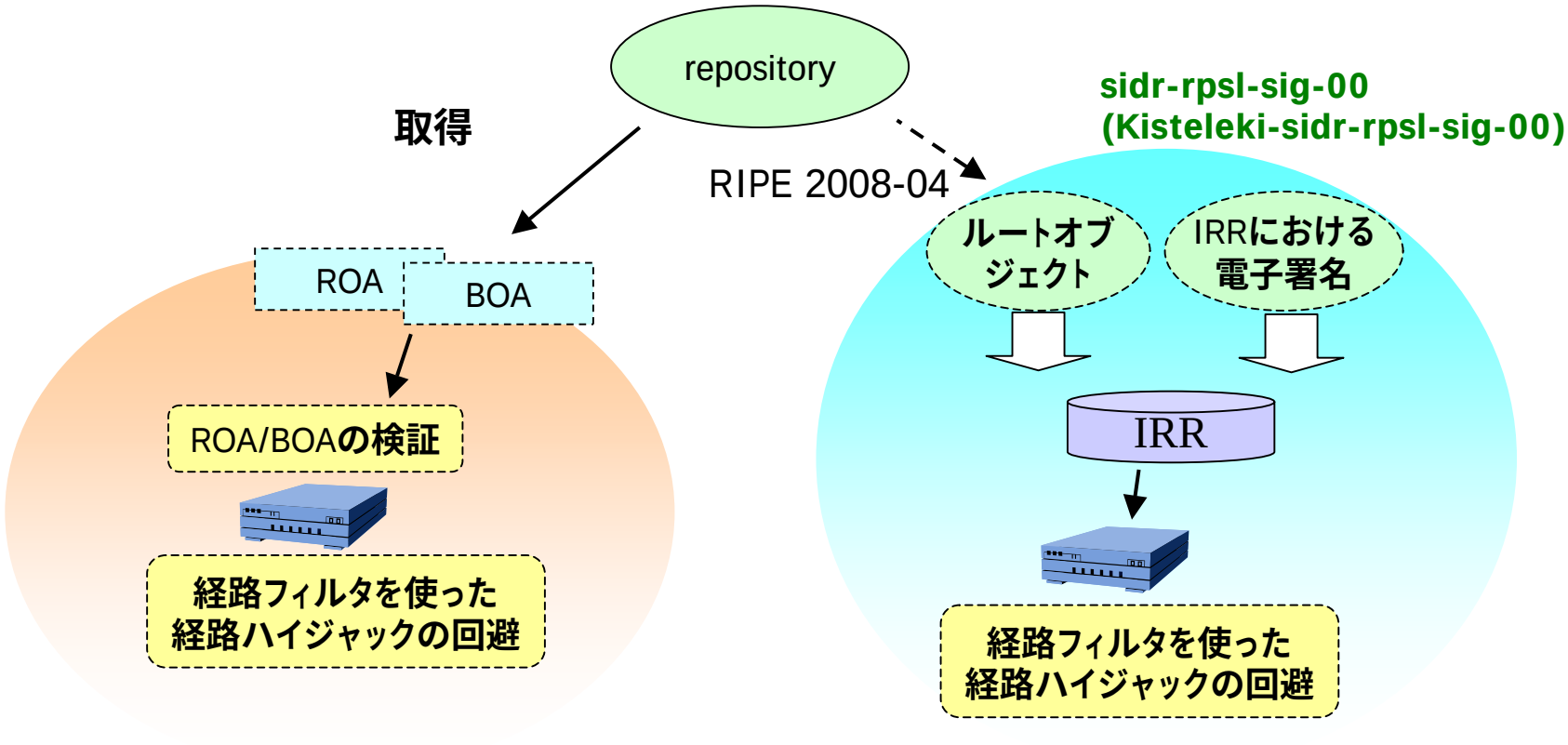
RPKI関連のドキュメント

- PKIX (Public-Key Infrastructure – X.509) WG
  - RFC3779
    - X.509 Extensions for IP Addresses and AS Identifiers
      - Jun 2004, C. Lynn, S. Kent, K. Seo
- SIDR (Secure Inter-Domain Routing) WG
  - An Infrastructure to Support Secure Internet Routing
    - draft-ietf-sidr-arch-06
  - A Profile for X.509 PKIX Resource Certificates
    - draft-ietf-sidr-res-certs-16
  - Certificate Policy (CP) for the Resource PKI (RPKI)
    - draft-ietf-sidr-cp-05
  - A Protocol for Provisioning Resource Certificates
    - draft-ietf-sidr-rescerts-provisioning-04

RPKIアーキテクチャと関連活動 (1/2)



RPKIアーキテクチャと関連活動 (2/2)



課題

- 証明書データの正当性維持
  - 再割り振りやパンチングホールの扱い
  - BOGON prefixの扱い
  - 証明書データの元になるレジストリデータベースの正当性
    など
- アドレス資源の扱い
  - 移管： RIR-RIR間、RIR-NIR間
  - 返却： リソース証明書の失効タイミング
    - ルーティングへの影響

RIRにおける取り組み状況

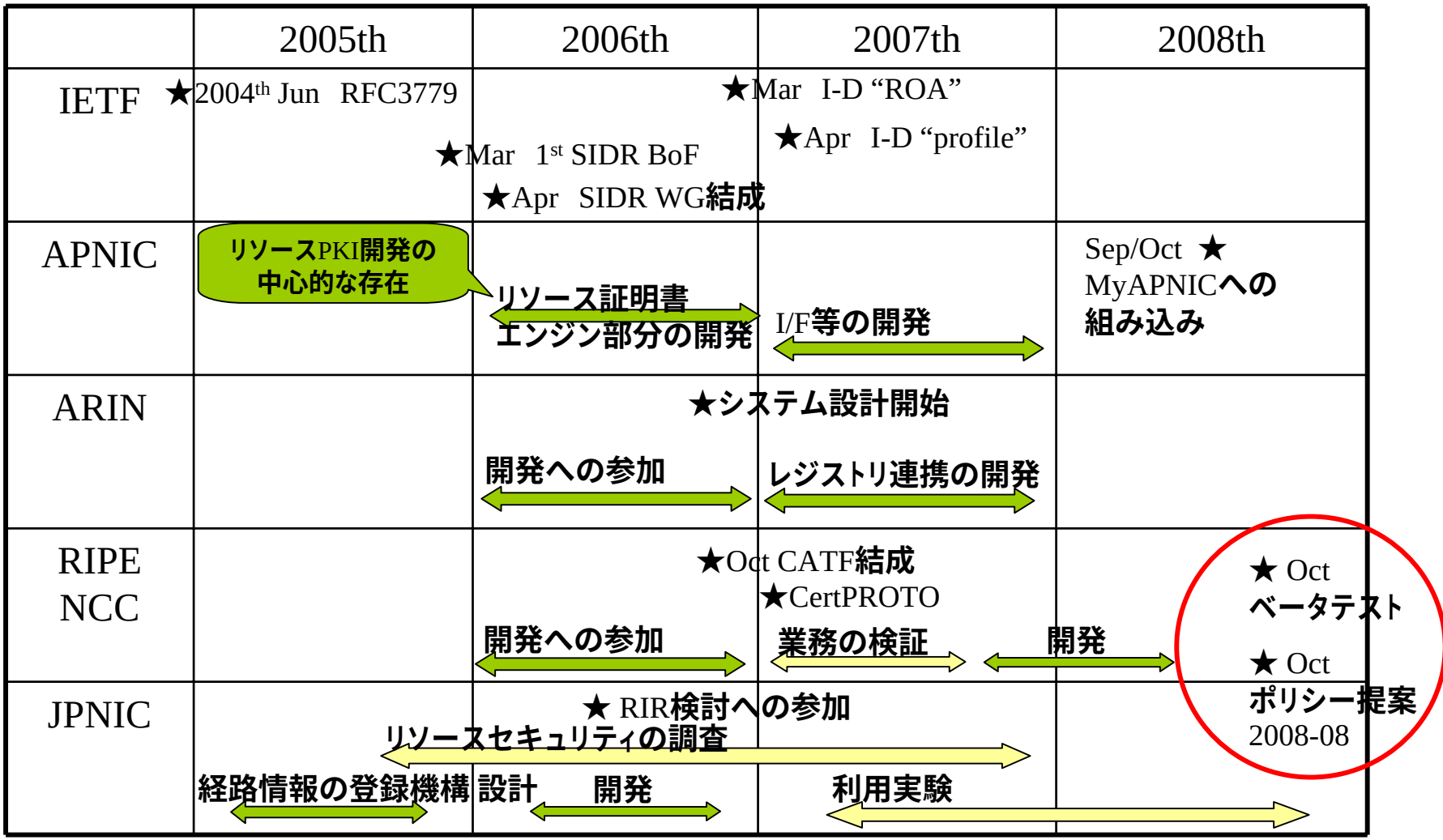
社団法人 日本ネットワークインフォメーションセンター

RIRにおけるリソースCA

	APNIC	ARIN	RIPE NCC	JPNIC
リソースCAの構築	実験運用中	不明	実験運用中	調査継続中
リソース証明書関連の活動	トライアルシステム運用中 (MyAPNIC組み込み済み)	APNICと連携しシステム開発 (ISC)	ベータシステム運用中 (2009年LIRPortal組み込み予定)	(経路情報の登録認可機構)

- 取り組み
  - 認証強化　crypto-pw、mail-from等から“X.509”認証への移行
  - 利用実験　リソース証明書

時系列


2005th
2006th
2007th
2008th
IETF
★2004th Jun RFC3779
★Mar 1st SIDR BoF
★Apr SIDR WG結成
★Mar I-D "ROA"
★Apr I-D "profile"
APNIC
リソースPKI開発の中心的な存在
リソース証明書エンジン部分の開発
I/F等の開発
Sep/Oct ★ MyAPNICへの組み込み
ARIN
★システム設計開始
開発への参加
レジストリ連携の開発
RIPE NCC
★Oct CATF結成
★CertPROTO
開発への参加
業務の検証
開発
★ Oct ベータテスト
★ Oct ポリシー提案 2008-08
JPNIC
★ RIR検討への参加
リソースセキュリティの調査
経路情報の登録機構 設計
開発
利用実験

APNICとRIPE NCCのプロトタイプシステム

- APNIC
  - MyAPNIC v2.0
    - https://myapnic.net/
- RIPE NCC
  - Certtest
    - https://certtest.ripe.net/

まとめ

- リソースPKI
  - アドレス資源の利用権利を示す電子証明書
  - 用途
    - セキュアルーティング
    - IPアドレスの利用権利
  - 取り組み
    - IETF SIDR WG
    - RIR - APNIC、RIPE NCC、ARIN
  - 課題
    - 証明書を利用したアプリケーション仕様
    - リソース証明書に含まれる情報の正しさ

本日の話

- RFC5280
- **インターネットPKIの標準と現実**
- **リソースPKIの動向**

ご清聴、ありがとうございました。