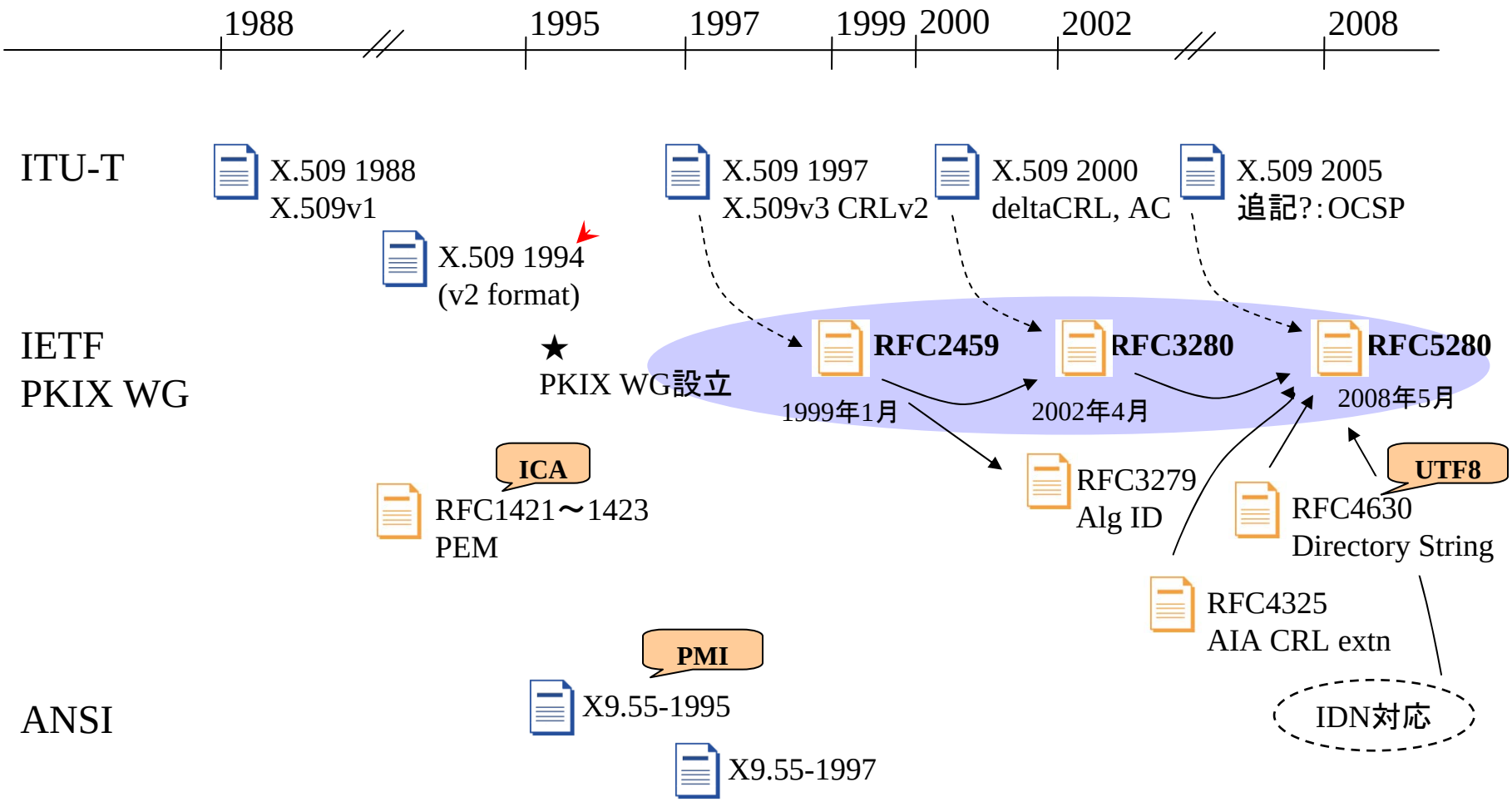
PKIに関わる標準化の歴史と相互運用性

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(JPNIC)
技術部／インターネット推進部　木村泰司

- PKIに関わる標準化の歴史を振り返る
- 相互運用に向けた課題
  - 標準化されたものとの関係は・・？

PKIの標準化の歴史 ー プロトコル



PKI Day 2009木村のプレゼンより

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

2459
↓
3280
↓
5280

- 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

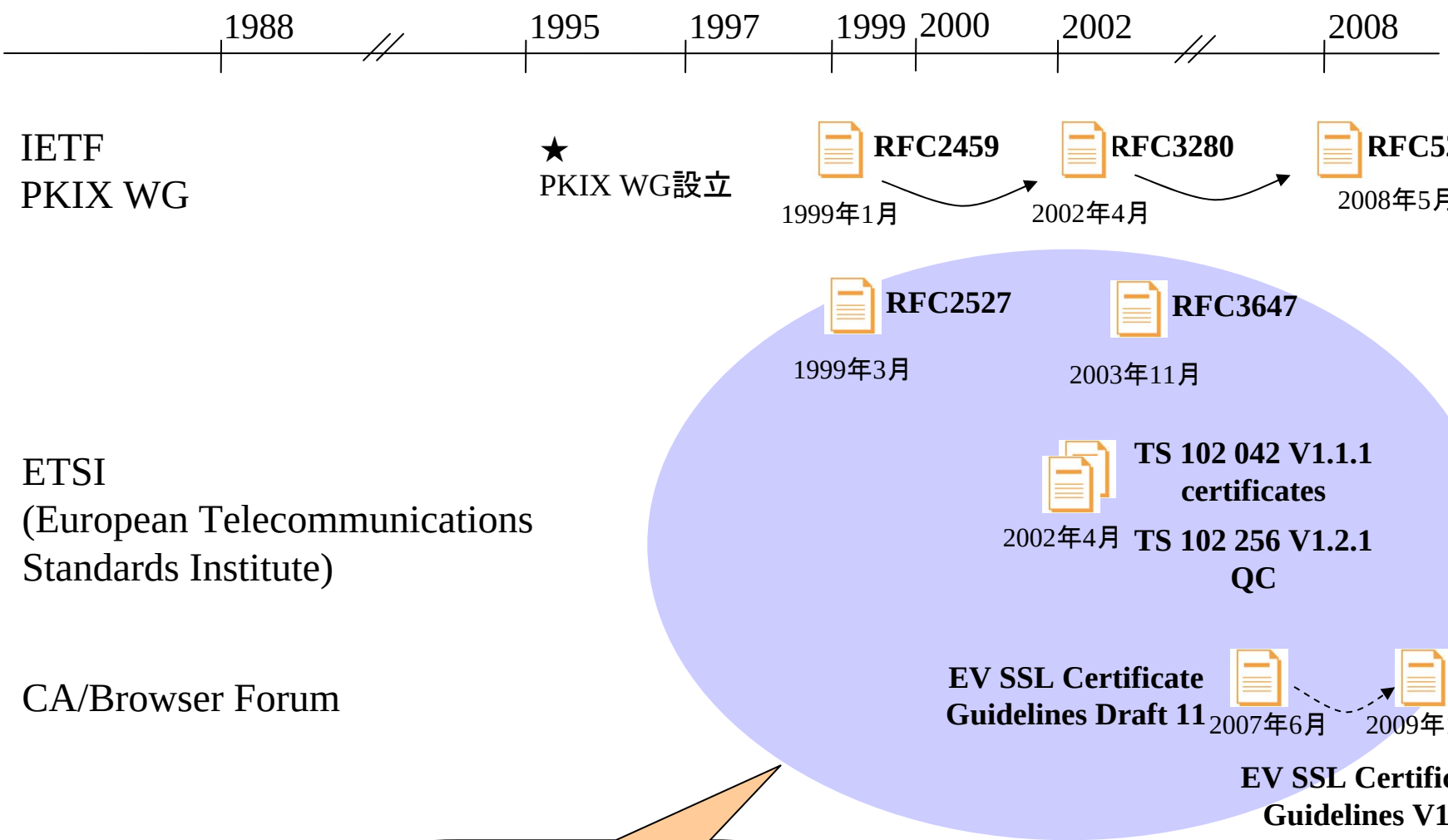
PKI Day 2009木村のプレゼンより

15年前からの変化

内容の変化	種類の変化
– かつては概念の説明に重点が置かれていた（ICA、PMI、AC） – 証明書検証がしっかりしてきた（失効検証）	– オンラインプロトコルが増えた – 応用系が増えた（WLAN、TAM） – 証明書の内容にも入ってきた。（QC、SIM）

電子証明書の書式は・・・ほとんど変わってない

PKIの標準化の歴史 － 運用のフレームワーク



相互運用に向けた課題

技術課題

	課題	対策の考え方
デバイス	ユーザ環境として何を利用するか	開発・選択 ICカード、PC（Webブラウザ）、携帯
継続運用	アルゴリズムの世代交代	標準での新たなアルゴリズムへの対応 認証局の運用対応

PKIの標準化がメインフォーカスではない。
（新しいアルゴリズム対応などのメンテナンスは必要）

運用上の課題

	課題	対策の考え方
証明書プロファイル	プロファイルの考え方を合わせる。	個々の保証レベルを考える。（松本キューブ?）
相互運用	登録と発行のレベルを合わせる。	相互運用される範囲全体の認証基盤として考える。

もはやプロトコル標準化とは離れた世界。
（何を認証し、何を識別子として、どんな世界を作るか）

伝えたいこと

- いまのPKI技術の標準化は肝要なところは完了している。そして15年間、肝要なところを使い続けてきた。

- もはや運用上の課題は技術仕様の標準化によって解決するものではない。
  - 認証基盤として運用のレベルを保つフレームワークの普及

- 何を認証し、何を識別子として、どんな世界を作るかが、電子認証を基盤とするための課題である。