Challenge PKI プロジェクト発 PKI 相互運用の国際標準

セコム株式会社 IS 研究所　島岡 政基

1. Challenge PKI プロジェクト発 PKI 相互運用の国際標準

PKI相互運用技術WGのChallenge PKIプロジェクト（以下、本プロジェクト）[1]では、2001年からPKIの相互運用性確保に向けて様々な取り組みを行ってきた。これらの取り組みから得られた相互運用性確保に関連する知見を国際的にフィードバックするため、IETF（Internet Engineering Task Force）に対して「マルチドメインPKIの相互運用性に関するメモ」（以下、本提案）として提案を行い、2008年7月にRFC 5217 “Memorandum for Multi-Domain PKI Interoperability”[2]として公開された。今回は本プロジェクトがIETFでどのように標準化を進めてきたか、これまでの経緯を振り返りながら説明する。

2. Challenge PKI と IETF との関わり

2001年から活動を始めた本プロジェクトは、PKIの相互運用性確保に必要な様々な知見が、国際的に十分に共有されていないことを懸念してきた。特に、ポリシが異なるPKIドメイン同士が相互運用する場合は、技術仕様上の互換性だけではなく、例えばトラストアンカをどうするか、ドメイン同士で相互接続するのか、あるいはリライングパーティ毎に個々に他のPKIドメインを信頼するべきか、といった運用面での問題も合わせて解決していかなければならない。

本プロジェクトは初めに、こうした問題について2002年7月に横浜で開催された第54回IETF会合で、PKIX WGの有識者を交えて非公式BoF[3]を開催して議論を行った。その結果、こうしたマルチドメインPKIの相互運用性問題については国際的に知見を共有する必要があるという結論に至り、IETFに対して本プロジェクトから提案を行うことになった。

こうした経緯から、本プロジェクトでは、以降のIETF会合に継続的に参加して、1）PKI相互運用の動向について観察、2）標準化提案の進め方について調査・協議、3）標準化にあたっての支持者の獲得、4）実際の標準化提案、を行ってきた。

3. マルチドメイン PKI の相互運用問題

マルチドメインPKIの相互運用における最も重要な問題の一つとして、適切なマルチドメインPKIを設計するためのノウハウが十分に共有されていない、という問題が挙げられる。マルチドメインPKIを実現した例として、米国連邦政府のFederal PKIや、日本の電子政府認証基盤であるGPKIがあり、それぞれのフレームワークの中で相互運用性を確保する情報はある程度整備されているのだが、例えば誰かが大規模なPKIを設計する場合に、マルチドメインPKIで設計すべきかシングルドメインPKIで設計すべきか、またマルチドメインPKIだとしたらどのような信頼モデルを選ぶべきか、といった情報は世界的にもほとんど整備されていなかった。このため、今後出来上がるであろう様々なPKI、特に大規模PKIが十分な相互運用性を確保しないまま構築・運用される可能性が懸念されていた。

[1] http://www.jnsa.org/mpki/
[2] http://www.ietf.org/rfc/rfc5217.txt
[3] Birds of Feather の略。問題提起やブレインストーミングなど目的を厳密に定めない緩やかな会合を指す。

そこで、本提案では相互運用可能なマルチドメインPKIをできるだけ簡単に実現できるようにするために、以下の理解について世界中で共有すべく提案を行った。

表1　本提案の主な章構成

2. Public Key Infrastructure（PKI）Basics	
	PKIドメインの構成要素となる個々のPKIの関係について整理した。 特に信頼関係の観点から、認証局同士の信頼関係と、認証局と利用者（Relying-Party）との間の信頼関係は明確に分けて論述した。
3. PKI Domain	
	PKIドメインの定義と、PKIドメインを確立するための要件、PKIドメインモデル（PKIドメイン同士の信頼関係）について解説した。
4. Trust Models External to PKI Relationships	
	PKI同士の関係に依らない信頼モデルとして、認証局と利用者の信頼関係によって確立されるトラストリストモデルがある。これはPKIドメイン同士の信頼関係とは異なる性質のものであるため、あえて章を分けて記述した。 トラストリストの信頼モデルを分類するとともに、トラストリストによる信頼関係を築く際の考察を行った。

このように、マルチドメインPKIを設計するにあたって必要な知識を正しく共有し、マルチドメインPKIを構成する際の主な選択肢（PKIドメインモデル）を示すことによって、マルチドメインPKIの相互運用性を実現することを目指している。

4. IETF の標準化プロセス

IETFにおける標準化活動の多くは、IESG（Internet Engineering Steering Group）の下に設置された8つのArea（部会）と、各Areaの下の約120のWG[4]によって進められており、その標準化プロセスは図1のように定められている。各フェーズの左に示す期間は、各フェーズに要する期間の目安としてIESGが定めたもの[5]であり、実際にはこの他に各フェーズでの改訂作業期間や再レビューの期間などを考慮する必要がある。

提案者は、最初に提案内容をI-D（Internet-Draft）としてIETFに投稿し、標準化したい旨を適切なWGまたはAD（Area Director）に表明（Publication Request）する。この提案内容が、IETFのいずれかのWGの活動内容に合致する場合には、WG Draftとして当該WGの中で提案活動を進める。WG Draftは、WGレビューを受けて最終的にWG提案としての合意を得た（WG Last Call[6]を通過した）後、AD Evaluationのステップに進むことになる。

一方、いずれのWGの活動内容にも合致しない場合は、AD-Sponsored Draft（旧Individual Draft）つまりAD後援のもとでの個人提案として提案活動を進めていくことになる。Sponsoring ADは、提案内容に関連する有識者にExpert Reviewを依頼し、その結果を受けてAD Evaluationのステップに進むことになる。

その後IETF Last Call[7]を経て、IESG Evaluation（全ADによるレビューと投票）で承認されれば、あとはRFC-Editorによる編集上の校正と著者による最終確認（AUTH48[8]）を経て正式にRFCとして公開されることになる。なお、これらの標準化プロセスは、I-D Tracker[9]と呼ばれるWebサービスによって進捗管理されており、誰でも状況を確認することができる。

---

4 http://www.ietf.org/html.charters/wg-dir.html

5 http://www3.tools.ietf.org/group/iesg/trac/wiki/PublishPath

6 ○○ Last Call とは、○○における最終的なコメント受付期間を指す。ただし Last Call 期間中のコメント内容によっては期間を延長したり、コメントを受けて改訂した後に改めて再度 Last Call を行う場合もある。

7 基本的には WG Draft の場合は 2 週間、AD-Sponsored Draft の場合は 4 週間が Last Call 期間となる。

8 もともとは「著者による最終確認を 48 時間で済ませる」が語源だが、昨今ではしばしば延長されているのが実情である。

9 https://datatracker.ietf.org/idtracker/

表 2　IETFの8つのArea

Abbrev.	Area
APP	Application Area
INT	Internet Area
OPS	Operations & Management Area
RAI	Real-Time Applications & Infrastructure Area
RTG	Routing Area
SEC	Security Area
TSV	Transport Area
GEN	General Area

図 1　IETFの標準化プロセス

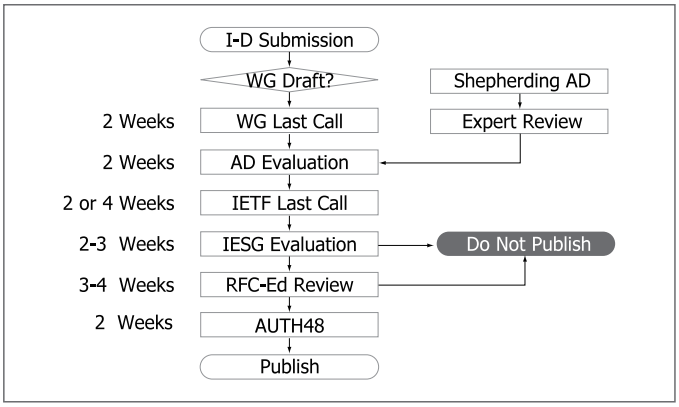
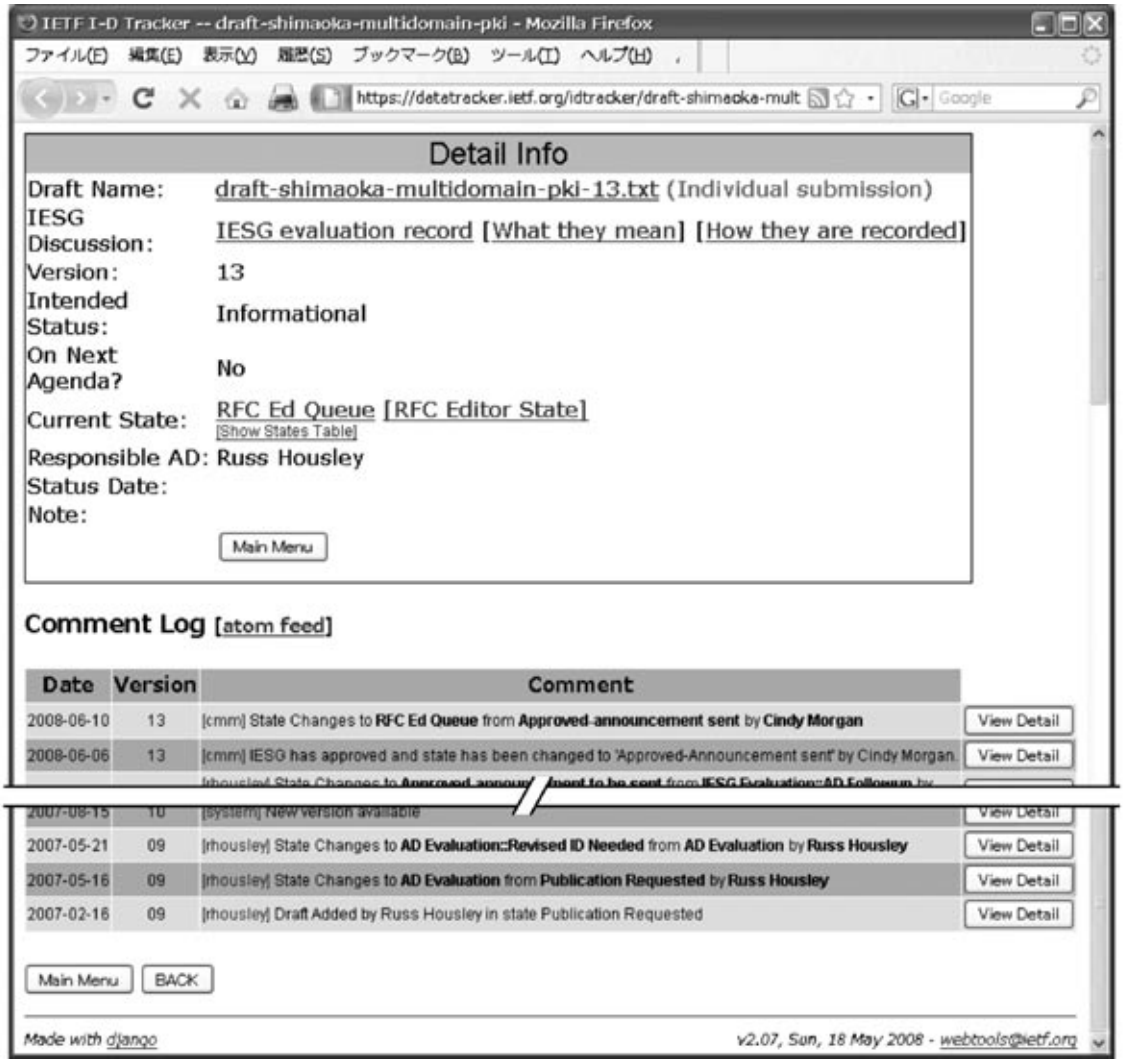


図 2　I-D Trackerによる進捗管理



5. NIST とのコラボレーション

PKIや暗号技術の分野において、米NIST（National Institute of Standards and Technology）/CSD（Computer Security Division）[10]は非常に大きな影響力を発揮してきた。NISTは、暗号鍵管理装置のセキュリティ要件を定めたFIPS140-2をはじめとする様々な米連邦政府の暗号製品調達基準の策定や、SHA-1やRSA1024bitの暗号アルゴリズムの移行指針を示したSP800-57をはじめとするSP800シリーズ文書の公開を行うとともに、実運用が行われている数少ないマルチドメインPKI環境である米Federal PKIの設計・構築に早くから携わっている。こうした経験や実績から、NISTはIETFにおいてもPKIX WGやS/MIME WGでの標準仕様策定で中心的役割を担っており、NISTのマルチドメインPKIに関する実績はIETFに限らず世界的にも広く認知されている。

そこで本プロジェクトがIETFでの提案を円滑に進めるにあたっては、NISTの支援を得ることが重要であると考え、キーパーソンとして当時PKIX WG co-chairを務めていたTim Polk氏（NIST）と、横浜のIETF会合以降も継続して提案の進め方について協議を重ねてきた。また、本プロジェクトを立ち上げ当初から支持いただいている宮川寧夫氏（IPAセキュリティセンター）の仲介により、Polk氏の同僚でありFederal PKIの設計にも携わってきたNelson Hastings氏（NIST）を、2004年9月から共著者として迎え入れることができた。更に2006年1月には、Hastings氏の紹介により、やはりFederal PKIやDoD PKIの設計に携わってきたRebecca Nielsen女史（Booz Allen Hamilton社）が共著者として名乗り出てくれたため、最終的には筆者を含めた3名で提案文書の執筆を進めることになった。

6. IETF における標準化

前述の第54回IETF会合での非公式BoFの結果を受けて、著者は本プロジェクトが持つ知見をまとめた内容をI-D初版として2003年7月にIETFへ投稿し、翌8月のオーストリア・ウィーンで開催された第57回IETF会合では、PKIX WGにて本提案の内容について発表を行った。当時PKIX WG co-chairのPolk氏は、当初このI-DをWG Draftとすることで合意してくれていたが、PKIX WGは当時WG Draftを非常に多く抱えており、WG Draft削減の見直しを図るようIESGに求められていたこと、またWGメンバから本提案が技術仕様の策定ではなく運用要件に主眼をおいたものであるというコメントを受けた経緯もあり、WG DraftではなくIndividual Draft（後にAD-Sponsored Draft）として提案を進めることになった。

その後、PKI相互運用技術WG内部でもレビューと改訂を重ねながら、2004年9月にHastings氏、2006年1月にはNielsen女史を共著者に加えたこともあり、2007年2月に、共著者らが従事してきたFederal PKIやDoD（米国防総省）PKIの知見を包括した大幅改訂を完了させた。

この間、並行してIETF会合ではPolk氏をはじめ、もう一人のPKIX WG co-chairであるStephen Kent氏（BBN社）や、当時のSecurity ADでありPKIX WGだけでも16本ものRFC文書を執筆したRuss Housley氏（Vigil Security社）、PKIX WGに限らずIETFの様々なAreaで幅広く活躍しているPaul Hoffman氏（VPN Consortium）らと標準化の進め方についても継続的に協議を進めてきた。実はこの頃のIETFはまだIndividual Draftの標準化プロセスにおいてAD Sponsoringの考え方が不明瞭だったため、筆者も具体的なアクションがわからずに迷走気味だった。偶然にも本I-Dの大幅改訂を終えた2007年春に、Individual Draftの標準化プロセスを明瞭にする2本の文書[11, 12]が発行された。これに伴い筆者は直ちに、Housley氏にSponsoring ADとなっ

[10] http://csrc.nist.gov/
[11] RFC 4858 “Document Shepherding from Working Group Last Call to Publication”
[12] IETF Operational Notes: “Guidance on Area Director Sponsoring of Documents”、http://www.ietf.org/IESG/content/ions/ion-ad-sponsoring.html

てもらうことを依頼し、これまでの経緯からすぐに快諾してもらうことができた。

その後は、Housley氏自身と氏が指名したPolk氏によるExpert Reviewを受け、IETF Last Call、IESG Evaluation、RFC Editor Reviewと順調に進んだわけだが、実はHousley氏にSponsoring ADを依頼した直後に、Security ADだったHousley氏がIETF Chairに昇任、Expert Reviewをする予定だったPolk氏もまたSecurity ADに昇任するという、筆者らにとってはまさにサプライズ人事があった。このため、本提案は光栄にもIETF Chair Sponsored（?）Draftとして、またSecurity ADによるExpert Reviewを伴って標準化を進めていくことができた。AD Sponsored Draftとなってから極めて順調にプロセスが進んだ背景には、こうしたIETFにおけるキーパーソンのポジションの変化が一つの要因としてあったようにも思える。また、PKIX WGの中心として活躍してきたHousley氏、Polk氏がIETFの中でステップアップしたという事実は、IETFの今後の流れがPKI技術をはじめとするセキュリティ技術へと少しずつ潮目が変わり始める兆しなのではないだろうか。

7. 標準化から学んだこと

こうしてIETFを通じて得られた様々な人脈や知見、特に一般的なWG Draftという形ではなく完全に個人の提案としてRFCを発信したことから得られた知見は実に貴重なものだが、今後IETFの標準技術に関わる方々に対して、またIETFに限らず国際標準化や世界的な合意形成を目指す方々にも有効と思われるいくつかの情報を述べておきたい。

7-1. RFCを読む全ての人たちへ

まず、標準化活動までは携わらないかもしれないが、IETFの標準技術を勉強したり調査したりする人たちにとって有益な情報を紹介する。

(1) RFC Reading Tools (http://tools.ietf.org/inventory/reading-tools)

本来テキストファイルであるRFCをタグ付き文書で読むことができるツールが提供されており、ページや章節、参考文献などがハイパーリンク化されている他、改訂版や旧版の有無、元のI-Dへのリンクや、各文書との差分表示など、非常に使い勝手がよい。

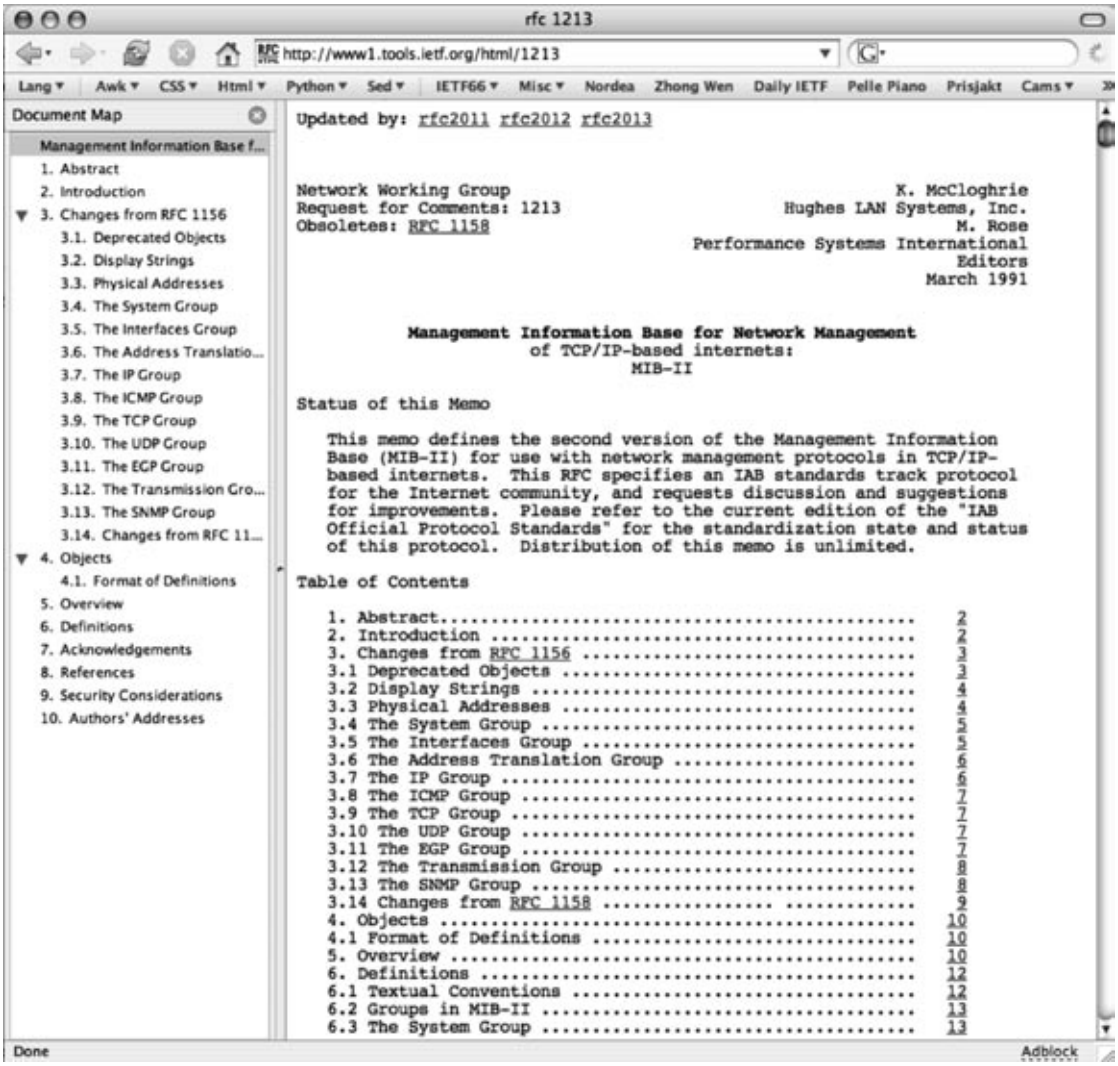
オンラインで利用するWebサービス[13]や、オフラインで利用可能なqRFCviewの他、Firefoxの拡張機能として利用可能なDocument Map[14]も提供されている。

その他、インターネット上に公開されているRFC文書を取得するコマンドラインツール(RFC util)も提供されている。こちらはキーワードや正規表現検索も可能なので、自分に必要なRFCを簡単に確認・取得することができる。

[13] http://tools.ietf.org/html/

[14] 本原稿執筆時点では、残念ながらまだ Firefox 3.0 には対応してなかった。

図3　HTMLized RFCs with Document Map



(2) Unofficial Repository (http://www.potaroo.net/ietf/)

公開されたRFCや最新のI-DはIETFリポジトリからも取得できるが、旧版のI-Dや期限切れI-D[15]はIETFリポジトリから取得することができない。この非公式サイトでは、過去のI-Dの履歴を(ほとんど)全てアーカイブしているだけでなく、前後の版との差分も表示してくれるので、各RFCが議論されてきた経緯や変遷などを調査する場合には非常に便利である。

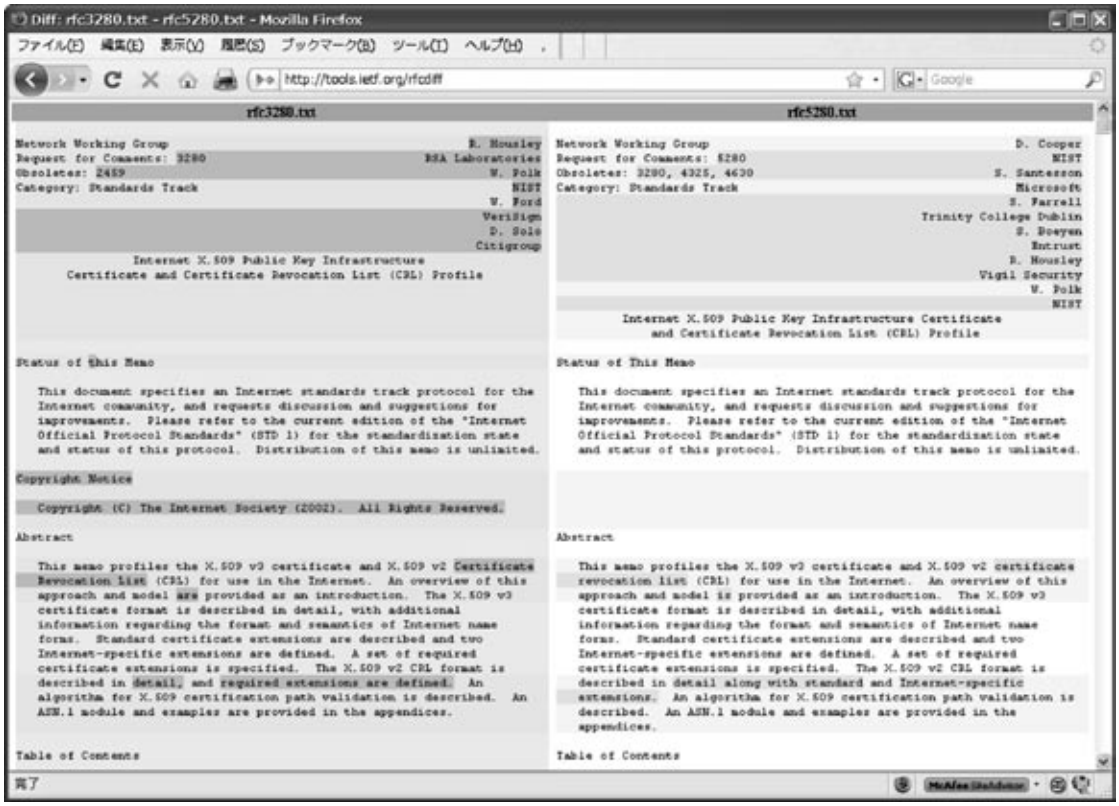
(3) Rfcdiff Tool (http://tools.ietf.org/tools/rfcdiff/)

前述のリポジトリでも使われている、RFC文書形式のテキストファイルの差分を表示するツールが提供され

[15] I-D の有効期間は原則として 6 カ月であり、期限内に更新されないと IETF リポジトリから削除される（厳密には「期限切れとなった」旨のメッセージで上書きされる）。

ている。コマンドラインから利用するものだけでなく、Webサービスとしても提供されているので、わざわざ比較文書をダウンロードしなくても確認できるのは非常にありがたい。差分表示の形式は何種類か定義されており、選択することができる。

図 4　RFCdiff Web Serviceの表示例（Side-by-side diff）



(4) Pre-formatted bibligraphic entries for RFCs　(ftp://ftp.rfc-editor.org/in-notes/rfc-ref.txt)

RFC文書のReferencesに記載されている形式のテキストデータが提供されている。RFC文書を参考文献として記述したい場合に便利である。

7-2. IETFで標準化活動に関わる人たちへ

次に、IETF中心ではあるものの、他の標準化団体も含めて国際標準化や世界的な合意形成を目指す方々に役立つであろう情報を紹介する。

(1) Educational Materials（http://tools.ietf.org/group/edu/）

ここには、IETFで標準化を進める上で有益となる様々な教材が公開されている。これらは主にIETF会合初日のトレーニングセッションで用いられる資料である。

① IETF Structure and Internet Standards Process
（http://www.ietf.org/proceedings/07dec/slides/newcomer-0/70newcomers.ppt）

IETFの組織概要や標準化プロセスの概説と、各組織が標準化においてどのような役割を持つのか、また知的財産権の扱いなどを解説している。

② RFC Editor Tutorial（ftp://ftp.rfc-editor.org/in-notes/rfc-editor/tutorial71.pdf）
RFCの種類や標準化プロセスの紹介、I-Dの書き方などを解説している。I-Dを書き始める人たち、あるいは既に書き始めた人でも是非一度はこれに目を通して欲しい。

③ Introduction to WG Leadership
（http://www.ietf.org/proceedings/07jul/slides/leadership-0.pdf）
WG設立の手順やWG運営に関する解説であり、一般には関係なさそうだが、WG chairがどのような方針に基づいて判断を行うのか、を理解しておくことはWG内での標準化を進める上で有益な情報源になると考えられる。

(2) xml2rfc（http://xml.resource.org/, http://tools.ietf.org/tools/templates/）

以前はI-Dはnroffというマクロ言語で書く必要があったが、最近はXMLベースが主流となってきている[16]。このページでは、XMLファイルからRFCフォーマットのテキストファイルを生成するxml2rfcというツールとその関連情報が公開されている。XMLファイルとすることで、nroffでは自動化できなかった参考文献や図表へのクロスリファレンス、目次などの自動生成もできるようになった。

xml2rfcでは、RFCフォーマット以外にも”ページ制御なしRFCフォーマット”（Wordなどへコピペする時に便利）や、HTML形式での出力もできる。

(3) IESG Additional Materials（http://www.ietf.org/IESG/content/index.html）

これもWG運営同様で、I-Dを最終承認するIESGがどのような方針で判断を行うのか、を理解しておくことは最終承認を円滑に進める上で有益な情報源になると考えられる。
具体的には、以下の情報が参考になると考えられる。

- WG Document Shepherd writeup questions and template
- Document Shepherd template for individual submissions via AD

8. 最後に

本プロジェクトおよび本提案にご理解ご支援をいただいたPKI相互運用技術WGはじめJNSAメンバの皆様に改めて御礼申し上げます。また、長年の上司でもありPKI相互運用技術WGリーダでもある松本泰氏、IETF会合でPolk氏らとの協議をいつもサポートしてくださった富士ゼロックスの稲田龍氏、JPNICの木村泰司氏、JNSA事務局の安田直義氏にも心から感謝の意を表します。

[16] I-D を XML 形式で記述することは RFC 2629 および下記の URL で規定されている。
http://xml.resource.org/authoring/draft-mrose-writing-rfcs.html