第 3 章　電子認証技術に関する国際動向

内容

- IETF における PKI 技術の動向
- TAM（Trust Anchor Management）の動向

3. 電子認証技術と技術文書策定に関する国際動向

本章では、電子認証に関する国際動向について述べる。本調査研究では、主に IETF（Internet Engineering Task Force）PKIX WG の現地調査を行った。

3.1. 調査研究の概要

電子認証技術や関連技術の最新動向を調査するため、IETF の PKIX WG[1]を中心に参加し調査を行った。これは 2006 年度の調査結果にもあるように、近年の PKI（Public-Key Infrastructure）に関するプロトコル策定は、IETF PKIX WG で最も活発に行われているためである。2007 年度は、第 69 回 IETF と第 70 回 IETF に参加した。

本章では広範でわかりにくい WG の様子をわかりやすく示すため、一旦スライドにまとめてそれを説明する形とする。PKIX WG の動向は特に中長期的な観点で見ていないと動向がわかりにくいが、これについては 2006 年度の調査研究報告書の第 3 章[2]を参照願いたい。

3.2. 第 69 回 IETF における PKI 技術の動向

第 69 回 IETF における PKIX WG のミーティングは、2007 年 7 月 26 日、5 日目の木曜日に行われた。PKIX WG は電子的な認証基盤の規格である ITU-T の X.509 をインターネットに適用し、新たな規格作りを行っている WG（Working Group - ワーキンググループ）である。アジェンダが多くなりがちな PKIX WG にしては会議の時間が 1 時間と短く、時間が足りずにアジェンダをこなす事ができないミーティングとなった（図 3-1）。

[1] IETF PKIX WG
http://www.ietf.org/html.charters/pkix-charter.html
[2] 2006 年度　電子認証フレームワークのあり方に関する調査報告書
http://www.nic.ad.jp/ja/research/200707-CA/

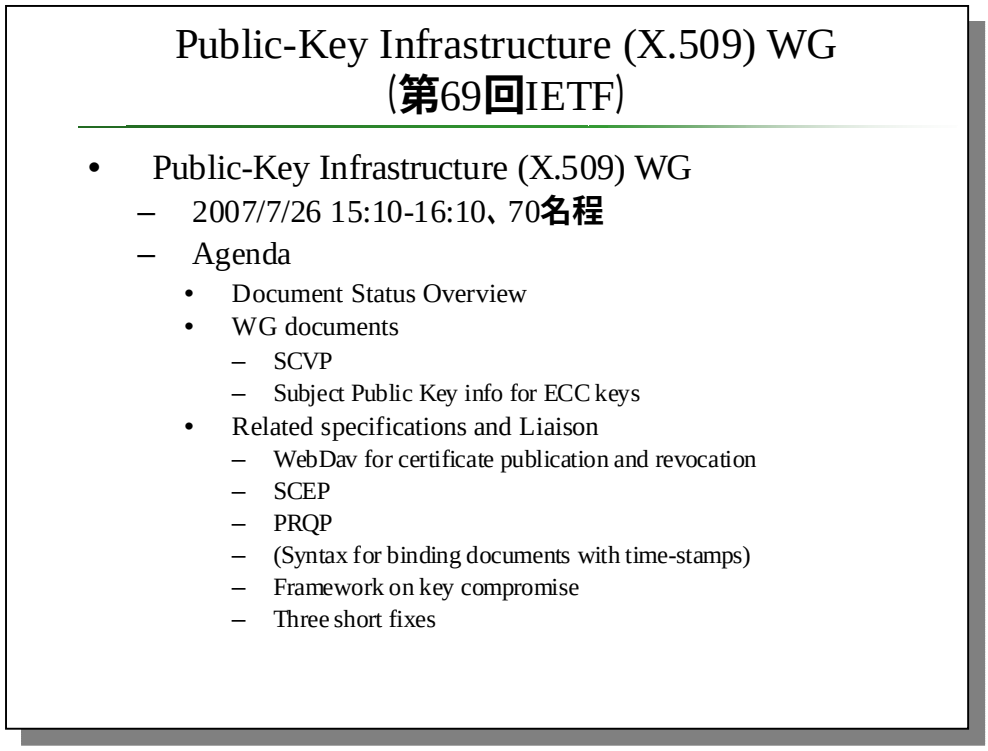

図 3-1　Public-Key Infrastructure (X.509) WG（第 69 回 IETF）

図 3-2 に第 69 回 IETF でのドキュメントステータスを示す。

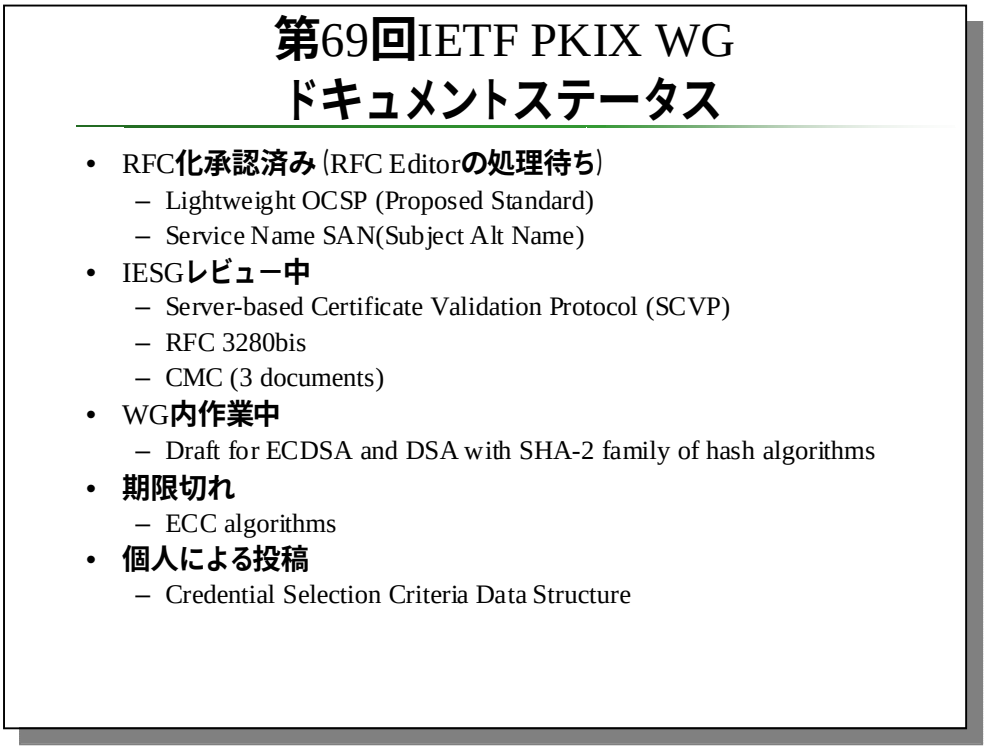

図 3-2　第 69 回 IETF PKIX WG ドキュメントステータス

メッセージの簡略化等を図った Lightweight OCSP と、subjectAltName 拡張フィールドにホスト名やプロトコル名等を入れる仕様の Service Name SAN は、IESG より RFC 化の承認を得た状態となり、第 69 回 IETF の前に RFC Editor の処理待ちとなった。（2008 年 3 月現在、Lightweight OCSP は RFC5019[3]として、Service Name SAN は RFC4985 として公開されている。）

オンラインの証明書検証プロトコルである SCVP(Server-based Certificate Validation Protocol)と、RFC3280 の改良版(RFC3280bis)、それから CMC(Certificate Management over CMS)に関わる 3 つのドキュメントは IESG のレビューを受けている状態であった。（2008 年 3 月現在は、SCVP が RFC5055[4]となった。RFC3280bis と CMC は RFC Editor の処理待ちとなっている。）

RFC3280bis が IESG のレビューに入り、証明書と CRL の処理に関する基本的な仕様が、ある程度固まる時期が来つつあると言える。

[3] The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments (RFC 5019)
http://www.ietf.org/rfc/rfc5019.txt

[4] Server-based Certificate Validation Protocol (SCVP) (RFC 5055)
http://www.ietf.org/rfc/rfc5055.txt

WG ドキュメント（個人としての提案ではなく、WG としてドキュメント化が進められることになっている Internet-Draft）については、SCVP と ECC のための Subject Key Info について議論された。SCVP については、編集上の変更と、http および TLS に関する記述が行われた。ECC のための Subject Key Info については、このときデザインチームによって議論が進められ、後に ML にて報告されることとなっている。2008 年 3 月現在、SCVP は先に述べた通り RFC5055 となっている。ECC については未だに Working Document である。

関連するプロトコルや関連団体のプレゼンテーション（Related specifications and Liaison）について図 3-3 に示す。

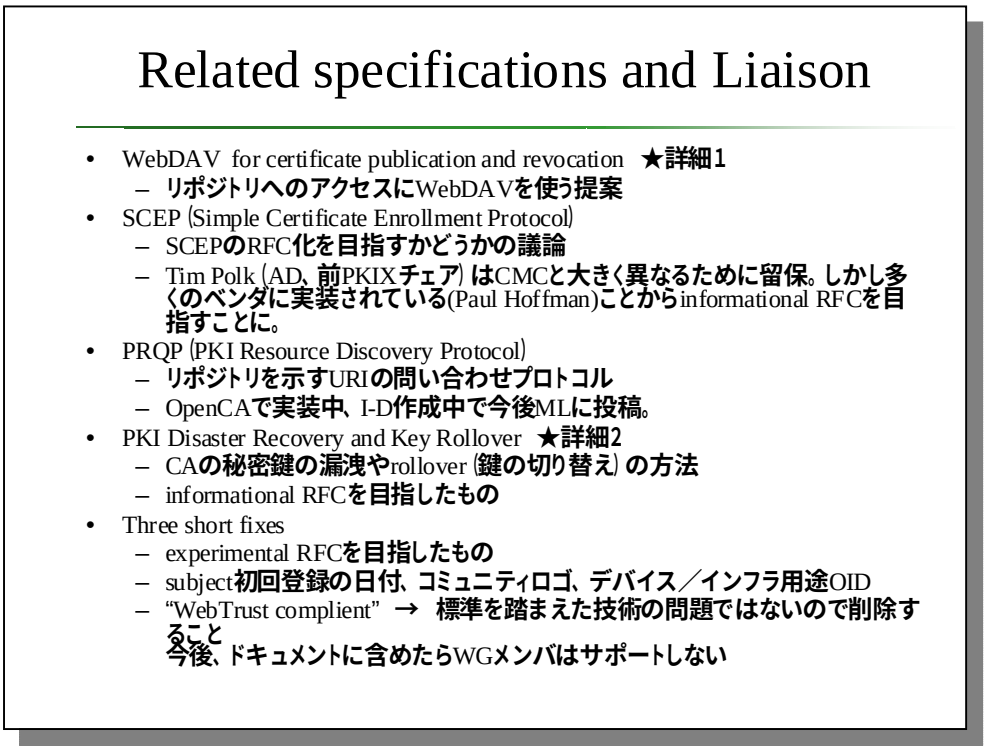

図 3-3　Related specifications and Liaison

PKIX WG ではこの関連するプロトコルや関連団体によるプレゼンテーションが毎回行われている。今回のアジェンダの中では、WebDAV と PKI Disaster Recovery and Key Rollover について報告する。

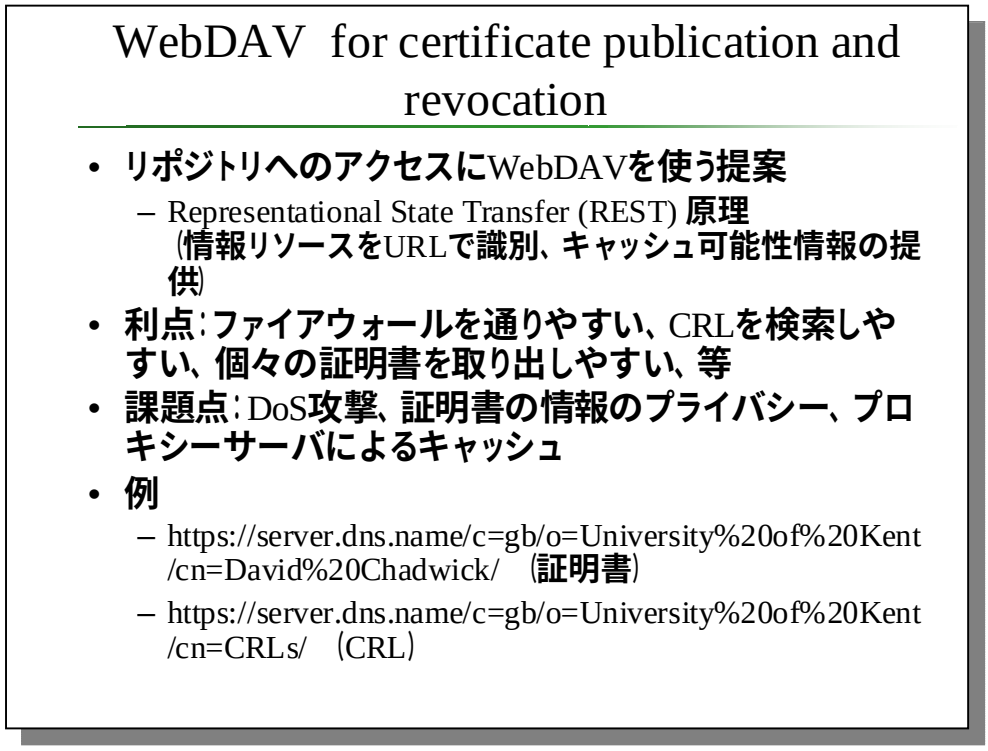

図 3-4　WebDAV for certificate publication and revocation

WebDAV for certificate publication and revocation は、証明書リポジトリへのアクセスに WebDAV を使う提案である。現在、LDAP が多く使われているが、ファイアウォールを運用の判断として通しにくい、個々の証明書を URL のような文字列だけで表記することが難しいといった課題がある。この提案は図の例で示したように、CN（Common Name）を指定した URL を表記でき、この URL に則って WebDAV を使って証明書データを取得できるようにした提案である。当日、このプロトタイプ実装のデモンストレーションが行われた。

PKI Disaster Recovery and Key Rollover は、PKIX WG に寄せられた individual draft ドキュメントである。Disaster Recovery とは災害からの復旧のことで、認証局においてプライベート鍵が漏洩したような状態から通常の運用状態に戻すための、復旧方法などがまとめられたドキュメントである。

図 3-5　PKI Disaster Recovery and Key Rollover

PKI Disaster Recovery and Key Rollover は、実は今回新しく提案されたものではなく 2001 年の 7 月に一度作られたことのあるドキュメントである。今回新たに Joel Kazin 氏によって再編集されたこのドキュメントは、プライベート鍵の危殆化や喪失といった、例外的な状況から正常な運用に復旧する方法が書かれている。主に CPS(Certificate Practice Statement)を記述したり、PKI に関するディザスターリカバリープランを立てる為に役立つ Informational RFC にすることが目指されている。記述されているディザスターリカバリーの対象は、エンドエンティティ、認証局、Revocation Authority、Attribute Authority、タイムスタンプ局(Time-stamp Authority)である。プライベート鍵の危殆化や喪失の他には、CRL のリポジトリに対する DoS(Denial of Services)攻撃や、認証局のキーロールオーバー(鍵の更新)についても言及されている。

3.3. 第 69 回 IETF における TAM BoF

TAM は Trust Anchor Management の略である。TAM BoF は第 69 回 IETF の最終日である 7 月 27 日(金)の午前に行われたにも関わらず、70 名以上の参加者があった。

電子証明書が VPN の機器などで使われるようになるにつれ、証明書検証で使われるトラストアンカー管理の重要性は一層増してきている。TAM BoF は、Web ブラウザや電子証明書の技術を使う VPN 機器などにある、トラストアンカー証明書を格納する領

域をモデル化して「トラストアンカーストア」と呼び、トラストアンカーの取り扱いが標準化されていない状況を改善する目的で開かれた。

はじめに、トラストアンカーに関する課題点をまとめた Carl Wallace 氏から、課題点と解決策のあり方に関するプレゼンテーションが行われた。

目標

－トラストアンカーストアを管理するプロトコルを標準化する

（トラストアンカー証明書の追加／削除／検索）

－out-of-band の信頼メカニズムへの依存を減らす

機能要件

－トランスポート(伝送路)との独立

－トラストアンカーをユーザが意識しない、または意識させない

デバイスなどをサポート

など

図 3-6 と図 3-7 に、TAM の必要性の議論の中で problem statement をまとめたものを示す。

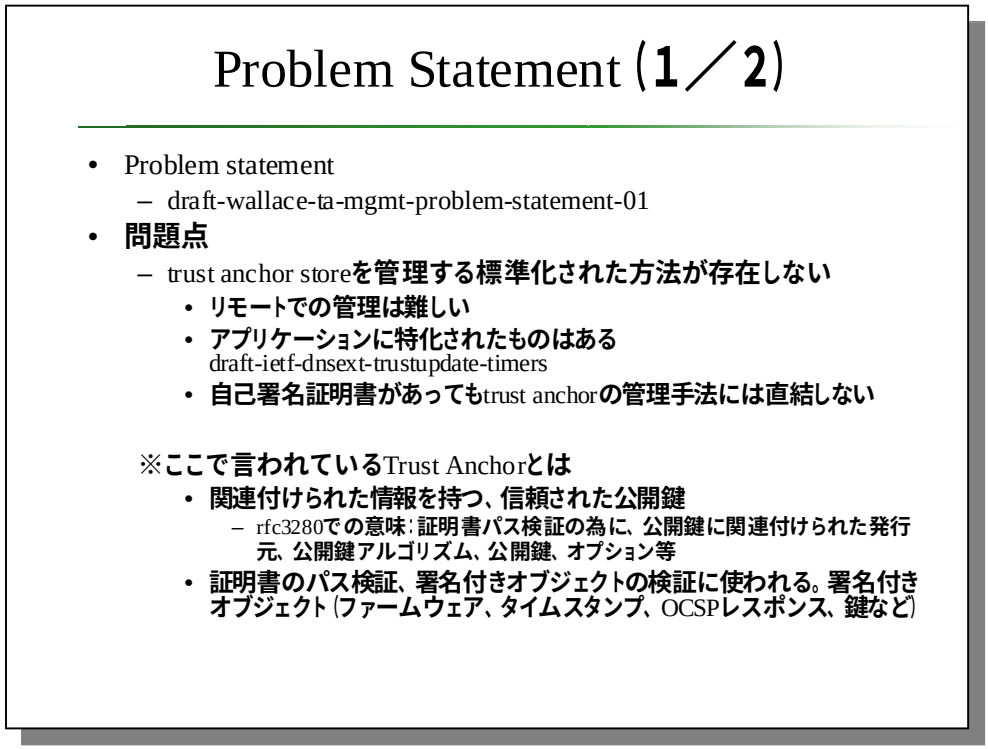

図 3-6　Problem Statement（1／2）

「trust anchor store」は、Web ブラウザや IPsec 機器に実装されている、トラストアンカーの証明書を格納するデータベースである。ユーザの信頼点（トラストアンカー）を管理してわかりやすくユーザに表示する必要があるが、標準化された技術はなく、各々のソフトウェアによって独自の実装が行われているのが現状である。

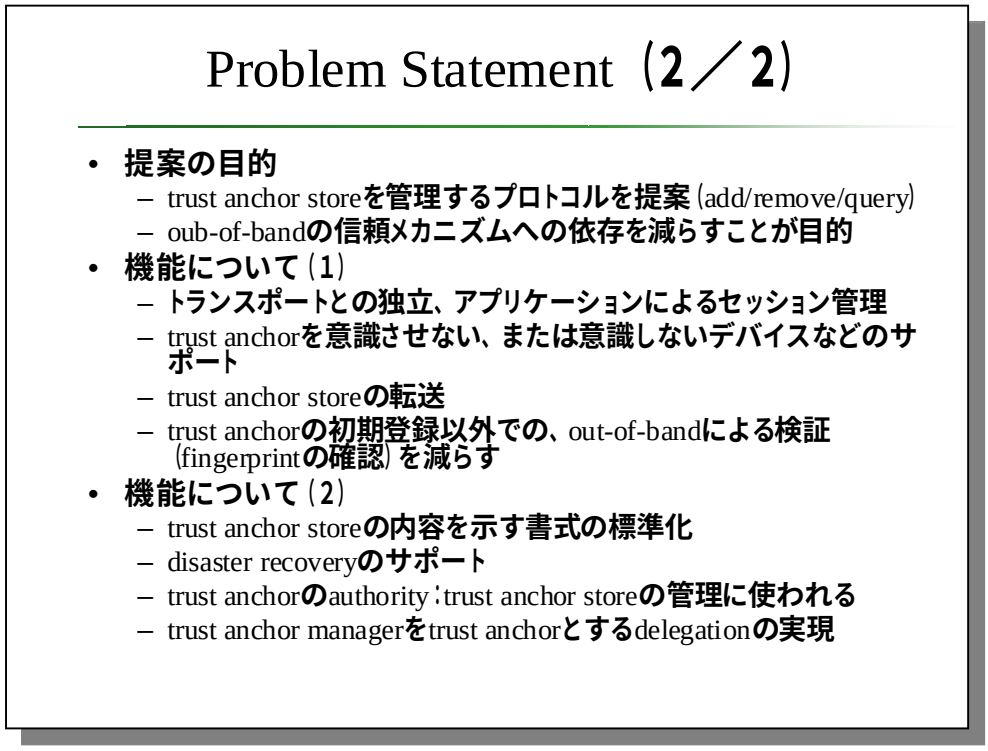

図 3-7　Problem Statement （2／2）

提案の目的は trust anchor store を管理するプロトコルを提案することと、fingerprint を電話などのオフラインの手法（out-of-band の手法）への依存を減らすことである。図に示した内容は、すでにドキュメント案に入っているが、全体の必要性に関してはまだ BoF の参加者に浸透していない様子であった。

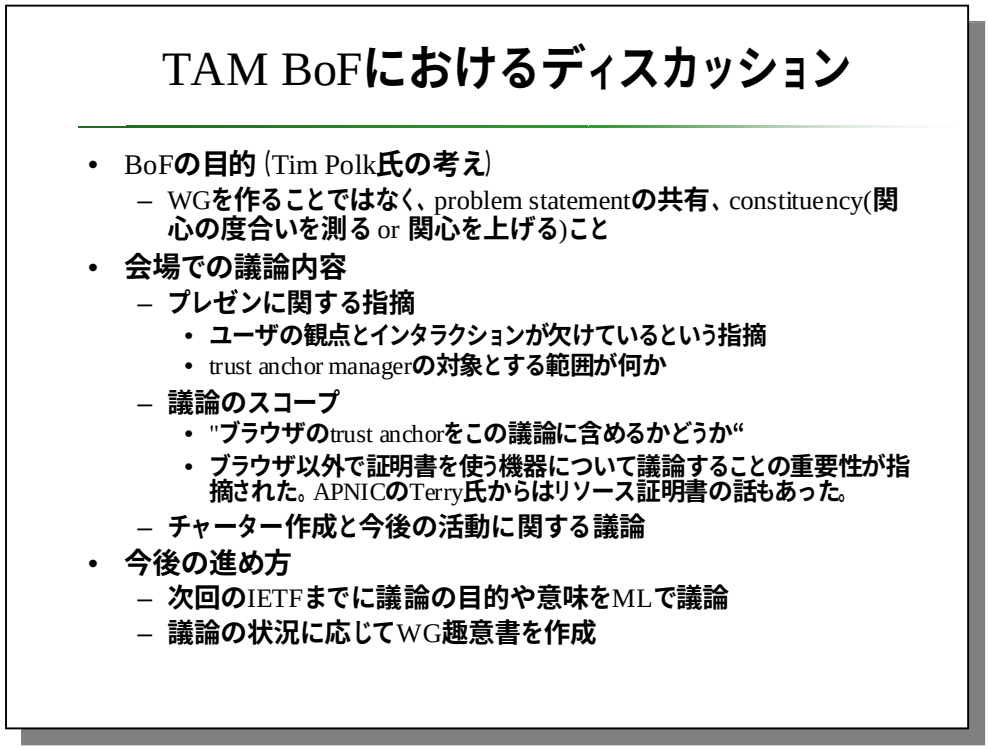

図 3-8　TAM BoF におけるディスカッション

TAM BoF のアレンジを行った Tim Polk 氏からの説明によると、この BoF は WG を作るための準備というよりは、Trust Anchor Management について IETF 参加者の関心を挙げることということであった。

今後はチャーターを作成し、必要があれば WG 化の活動を行うということであったが、後に PKIX WG のドキュメントの一つとして取り上げられることとなる。

3.4. 第 70 回 IETF における PKIX WG

第 70 回 IETF はカナダのモントリオールで行われた。PKIX WG は 2007 年 12 月 3 日の初日に行われた。今回のミーティングも議論が予定以上に延び、1 件のアジェンダを取り消すことになった。

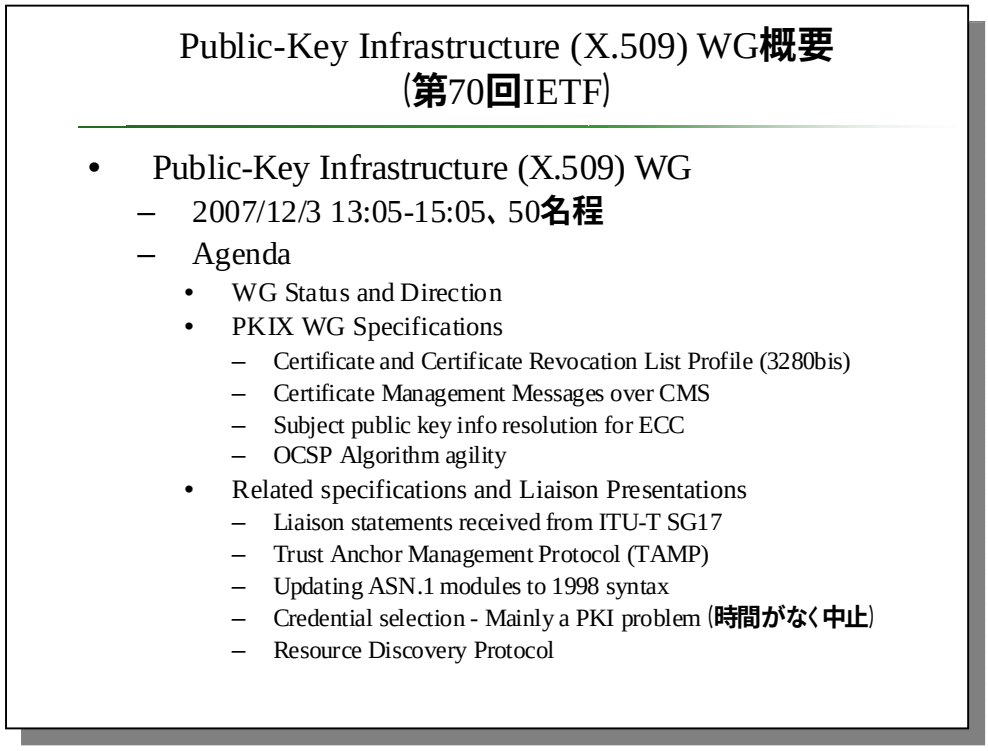

図 3-9　Public-Key Infrastructure (X.509) WG 概要（第 70 回 IETF）

今回も、アジェンダが多く、各内容について時間に追われるように議論をこなしていく会合となった。大きな論点でなければメーリングリストにて継続といった様子である。チェアである Stefan Santesson 氏による Credential selection の議論については時間の節約の為に取り下げとなった。

第 70 回 IETF の PKIX WG におけるドキュメントステータスを図 3-10 に示す。

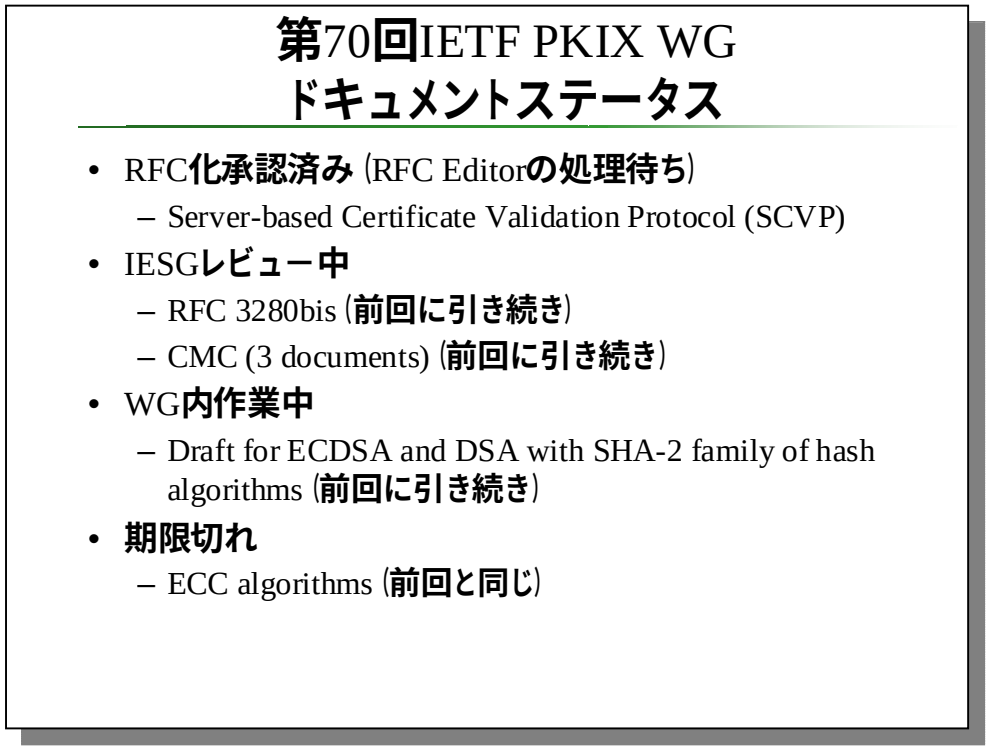

図 3-10　第 70 回 IETF PKIX WG ドキュメントステータス

Server-based Certificate Validation Protocol (SCVP)は、この時に RFC Editor の処理待ちの状態となっている。RFC3280bis、CMC に関わる三つのドキュメントに関しては IESG レビュー中の状態である。

2008 年 3 月現在は、SCVP が RFC5055 となっている。RFC3280bis と CMC は RFC Editor の処理待ちになっている。

次に PKIX WG における議論について述べる（図 3-10）。

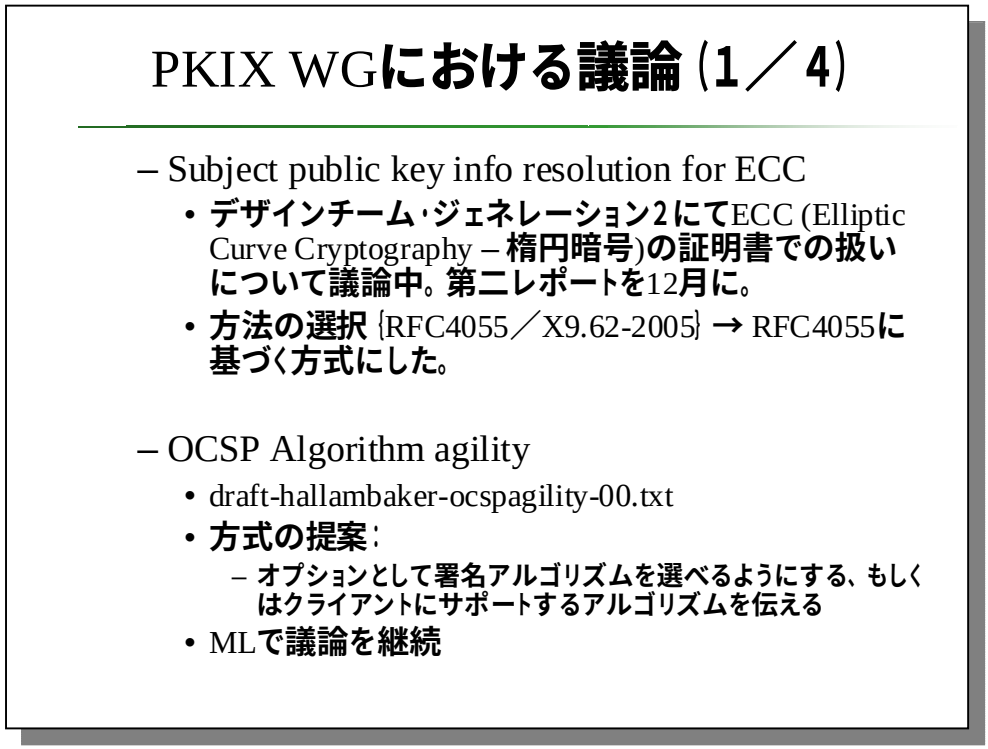

図 3-11　PKIX WG における議論（1／4）

PKIX WG では楕円暗号の ECC の証明書に関する扱いについて検討を行っている。検討はデザインチーム・ジェネレーション 2 と呼ばれる有志のグループで行われている。グループの現在の検討は方針に関するもので、RFC4055[5]の方式か X9.62-2005[6]の方式かを検討している状況であった。検討の結果、RFC4055 の方式を採用するとの事であった。

OCSP Algorithm agility は、OCSP（Open Certificate Status Protocol）でハッシュアルゴリズムを選択可能にするための提案である。ドキュメントは、OCSP のための要件や考察をまとめたもので具体的な書式を提案しているわけではない。

関連するプロトコルや関係組織からのプレゼンテーションが行われる時間には、ITU-T から PKIX WG にコメントが求められた件についてディスカッションが行われた。

[5] Certificate and Certificate Revocation List (CRL) Profile (RFC 4055)
http://www.ietf.org/rfc/rfc4055.txt

[6] ANSI X9.62-2005 Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)
http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.62%3A2005

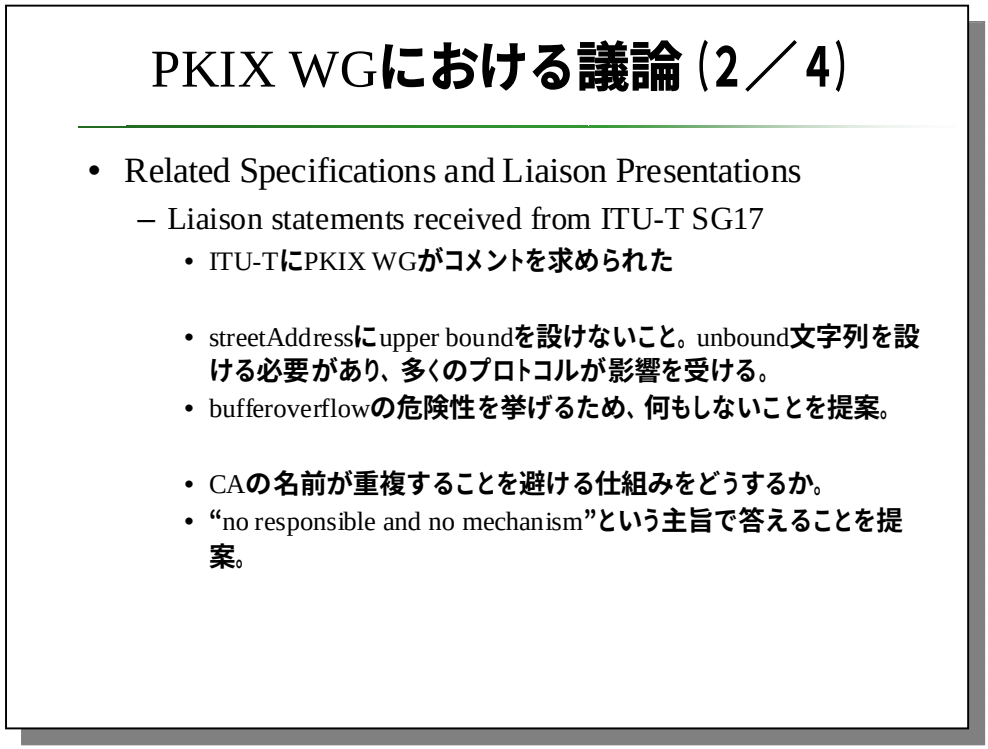

図 3-12　PKIX WG における議論（2／4）

ITU-T からは二点についてコメントを求められていた。一つは証明書の名称として使われている DN（Distinguished Name）の文字数制限についてである。DN の streetAddress や organizationName といった属性には 64 文字や 128 文字といった目安がある。しかしこれを制限とみなしてプログラムにハードコーディングされていることがあり、相互運用性に問題があるとの懸念が示されていた。これに対して PKIX WG としては、上限を設けない実装を多くの人に行わせることで、PKI の処理の部分で bufferoverflow を起こしがちになる危険性があるとし、プロトコルの変更に関してはアクションを取らないことを返答することとなった。

二点目はトラストアンカーとなる CA の名前の重複を避ける仕組み（何らかの機関で登録管理するなど）はあるか、という問い合わせである。これについてもわからない、という返答を返すこととなった。証明書検証を行うプログラムで設定されるトラストアンカーは、その下位認証局が発行する多くの証明書の有効性を左右するため、ユーザが CA を間違えるような状況を避ける必要がある。そこで CA の名称が同一にならないような制度や仕組みを設けることが考えられるが、そのような仕組みに関する情報を頂きたいという問い合わせであった。また PKIX WG がそれを行わないのか、という問い合わせもあったようである。しかし IETF はプロトコルの策定のための会議であるため、PKIX WG としては実施できないと返答することとなった。

前回の第 69 回 IETF で BoF が行われた TAM は、PKIX WG で扱われることとなった。PKIX WG では、これを WG でのプレゼンテーションと ML での議論で決定しているが、そのプレゼンテーションは今回（第 70 回）IETF の PKIX WG で行われた。

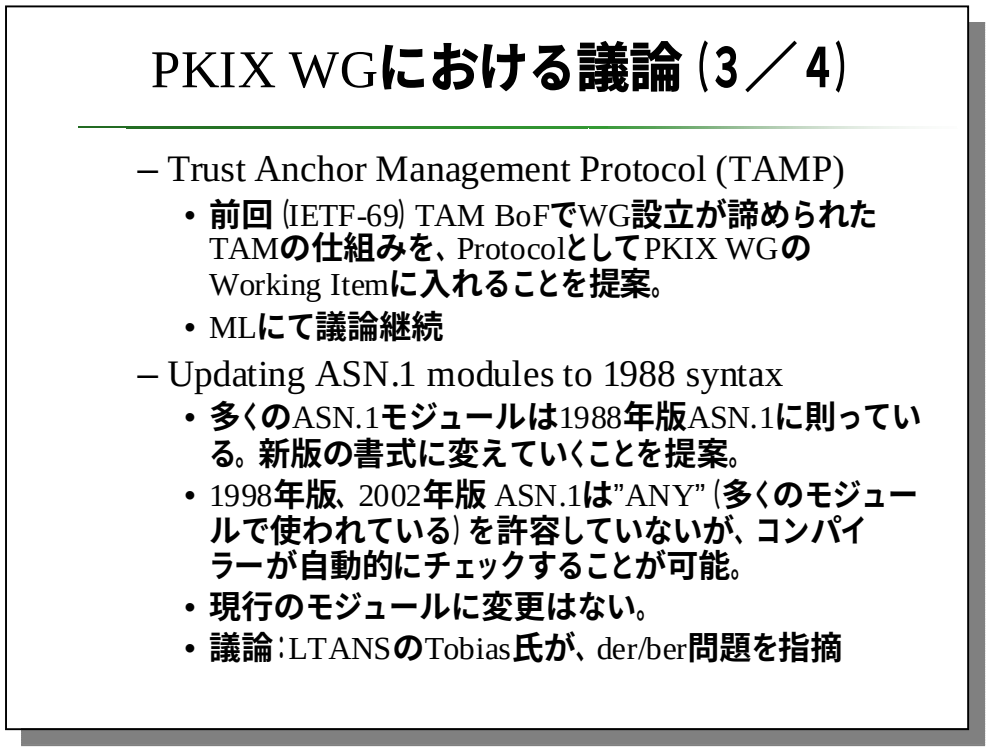

図 3-13　PKIX WG における議論（3／4）

ASN.1 モジュールについては、WG ドキュメントではなく individual ドキュメントであるが、"PKIX WG に関連する活動"として WG に認められた提案である。（2008 年 3 月現在、WG ドキュメントとしてディスカッションが行われている）現行の PKIX WG で使われている ASN.1 記法は 1998 年版の ASN.1 を用いている。これを 2002 年版のものにアップデートする提案である。このドキュメントでは、PKIX WG で策定された RFC の変更点がまとめられている。

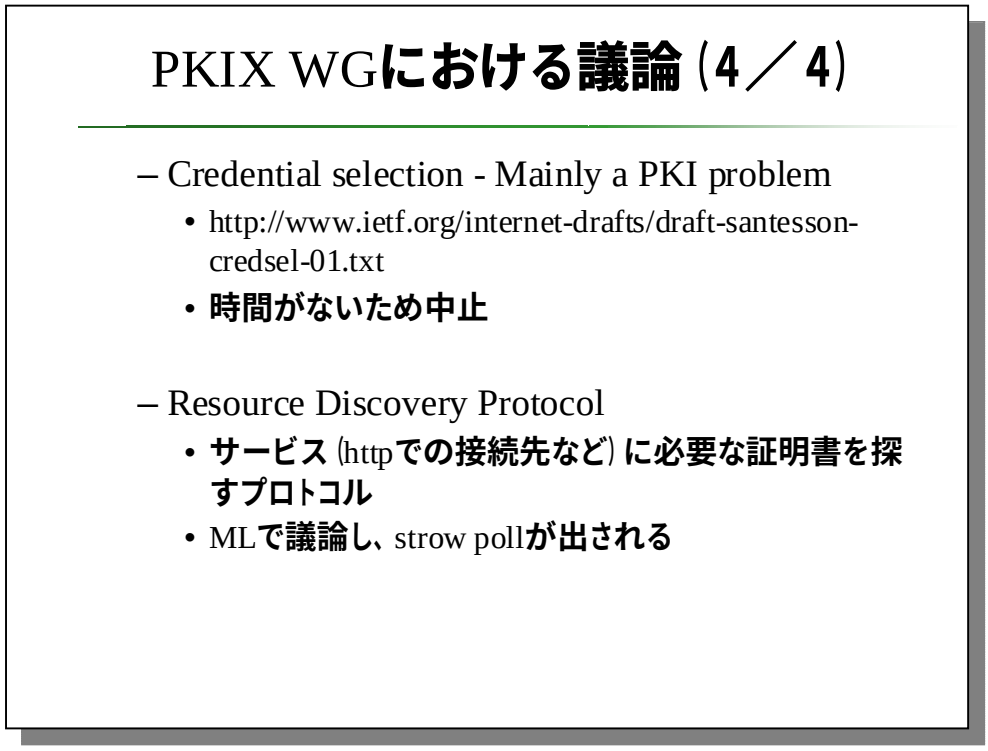

図 3-14　PKIX WG における議論（４／４）

この他に、「Credential selection」と「Resource Discovery Protocol」が予定されていたが、Credential selection は時間が押してきていたために今回は取りやめとなった。

Resource Discovery Protocol はサービス（http での接続先など）に必要な証明書を探すプロトコルである。Internet-Draft がまだないことから、ML で議論を進めた後に、たたき台が出されることとなった。

3.5. まとめ

本章では、電子認証技術の最新動向に関する調査について述べた。本調査研究ではインターネットに関わるプロトコル策定を行っている IETF のミーティングに参加し、インターネットにおける X.509 の適用に取り組んでいる PKIX WG の動向を調査した。また PKI の利用に当たって重要な Trust Anchor Management に関する議論の動向も調査した。

2007 年度の PKIX WG の動向として注目すべきものを 3 つ挙げるとすれば、以下の三つである。

- 電子証明書のプロファイルなどを定めた、基本的なドキュメントである RFC3280 の後継にあたるドキュメントが固まってきた。

- ハッシュアルゴリズムの変更を可能にするための対応が、各プロトコルで必要であり、Russ Housley 氏を中心に提案作業が進められている。
- 私有鍵の漏洩などの事態に対応するためのディスカッションやプロトコルの提案が見られるようになってきた。

しかし、PKIX WG において策定されているプロトコルで、身近に使われているものは一部のものに留まっている。PKI が汎用的な技術であるために、電子証明書を特定の環境で使うために新たなプロトコルの策定が必要になり、その結果 PKIX WG のアジェンダを増やしている。PKI 技術がインターネットで適切に普及するための活動には、新たなプロトコルの策定よりも、既存のプロトコルが現状に適合しているのかといった確認の作業や、実用化が可能かどうかを検証することが重要ではないかと考えられる。

第 3 章　電子認証技術と技術文書策定に関する国際動向