第 5 章　電子認証フレームワークの定義と仕組み

内容

- 電子認証に関わるノウハウの蓄積とは
- 電子認証プラクティスフォーラムとは
- フォーラムの設計
- フォーラムの仕組みとコミュニティ構成
- 実現の為のシステムの機能と構築
- 認証局の運用に関する技術的な BCP

5. 電子認証フレームワークの定義と仕組み

RIR における電子認証技術の利用や IETF における電子認証技術の標準化と実用化の現状を鑑みると、電子認証技術は標準化が先行していてインターネットにおける実用化が遅れていると言える。

本調査研究のひとつのテーマである「電子認証フレームワーク」は、この状況を改善し、標準化が進んでいる電子認証技術を適切に普及させる機構、およびコミュニティの形成に関する調査研究である。

2005 年度は、電子認証技術の適切な普及を促進するには電子認証に関するノウハウをドキュメント化し、継続的に更新・公開していく枠組みのあり方について調査した。この調査では国内外の既存のドキュメント策定プロセスについて調査すると共に、電子認証フレームワークに期待されることを列挙した。

2006 年度は、電子認証フレームワークを構築するためのフォーラム「電子認証プラクティスフォーラム」の設立のため、BCP の議論とシステムの整備を行った。このフォーラムは IETF や JPOPM と同様にドキュメント策定プロセスを持ち、一般に公開した文書を元に BCP（ベストカレントプラクティス）の策定を目指す活動である。

ここでは本フレームワークに関する議論の結果、見えてきたフォーラムの構成とフォーラムのシステムについて述べる。今後、本フォーラムの構成自体を継続的に更新していける仕組みとするため、本フォーラムの趣意及び規定を BCP としてまとめていく活動が考えられる。

5.1. 電子認証に関わるノウハウの蓄積とは

IETF や日本国内での PKI 普及の動向から、電子認証技術の普及が遅れている理由は、技術そのものの発展が遅れているためではなく、適切に利用し活用するノウハウが普及していないことに原因として考えられる。

電子認証技術の適切な普及には知見の共有が重要であり、この重要性事態は IETF SAAG（セキュリティエリアの全体会議）でも指摘されていた。しかし IETF の BCP では、概念モデルなどをカバーできない。

しかし日本国内においても、電子認証に関わる運用面での調査研究は行われており、むしろ一定の調査をすれば必要十分なノウハウが得られることが、本調査研究の結果から判明している。

すなわち電子認証に関わるノウハウは、既に公開されているか、認証局の運用を行った後には自明の事実であることが多い。

そこで重要になるのは、これらのドキュメントを継続的に参照可能な仕組みで管理し、新たなノウハウの集約や既存のノウハウの見直しを進められるような仕組み作りが重要であると考えられる。

例えばこれが電子認証技術自体の標準化についてであれば IETF が該当し、IP アドレスポリシーについて JPOPM が、日本国内のインターネットの運用に関するノウハウであれば JANOG が該当すると考えられる。JANOG は JANOG Comment と呼ばれるノウハウのドキュメント化活動を行っており、すでに一般公開が行われている[1]。電子認証技術の運用や利用・活用に関するノウハウについても議論と標準的なドキュメントとしての蓄積があれば、コミュニティ参加者の間で共有できる。IETF や JPOPM、JANOG のすべてに共通する点であるが、コミュニティの参加者は当該分野の専門家ないし業務上の改善に取り組む「提供者」ないし「供給者」の立場が多い。一般ユーザに対するノウハウの提供よりも、このような提供者側でのノウハウの共有によってノウハウが一般ユーザの環境向上に対しても効果を発揮しやすいと考えられる。

5.2. 電子認証プラクティスフォーラムとは

2005 年度および 2006 年度の調査研究の結果から、電子認証プラクティスフォーラムとは、コミュニティにおけるコンセンサスを得ながら、電子認証で必要となるドキュメントを策定し、BCP（Best Current Practice）として普及、改善を図っていく活動になると考えられる。

既存の調査研究などによって明らかになりドキュメントとして公開されているものについては、位置づけを整理した上で本フォーラムの中の位置づけを明らかにする。これによって電子認証の利用に関するノウハウの全体の中で、専門的な調査研究がどのような位置づけにあるのか、ユーザ自身が読む必要があるのかどうか、どのような場面で役立つノウハウであるのか、などがわかるようになる。

なお、本調査研究のテーマである「電子認証フレームワーク」は本フォーラムで初期の段階で策定されるべき BCP の集合であると考えられる。電子認証の用途は、本人性確認手法の違いや保証レベルの違いによって内容が大きく異なる。はじめにこの整理を行うことで、各電子認証技術の位置づけが明らかになるため、逆にその後の BCP がど

[1] JANOG Comment Index
http://www.janog.gr.jp/doc/janog-comment/index.html

の電子認証に適用できるものであるのかの整理が可能になると考えられる。

例えば、以下のような BCP が電子認証フレームワークにあたるドキュメントになると考えられる。

・インターネットで使われる電子認証の保証レベル（分類）
・保証レベルごとの電子認証のユーザインターフェースの違い
・ユーザの組織所属に使われる電子認証のレベル
・商用で使われるユーザアカウントの電子認証のレベル

これらの BCP が整備されることで、SSL/TLS のサーバ証明書の保証レベルや、商用 Web サイトを利用するための電子証明書などについての共通認識の形成に役立つと考えられる。

本フォーラムで扱う BCP には、電子認証技術の運用に役立つ技術情報なども含まれると考えられる。

5.3. 電子認証プラクティスフォーラムの位置づけ

本節では、具体的なフォーラムの内容を述べる前に、本フォーラムの整理（位置づけ）について述べる。以下の文章は、本フォーラムへの参加を呼びかける際に参加者に位置づけの理解を図るために作成されたものである。

2007/02/16
JPNIC

電子認証プラクティスフォーラムについて

▼はじめに

電子認証はインターネットを使ったサービスにおける安全や安心の基本である。インターネットを使った業務システムを始め、様々なオンラインのサービスでは予め定められた程度にユーザを特定し区別する行為が必要である。そうでなければ、ユーザやシステムが混乱するだけでなく不正行為等の再発を防止することは難しい。

1990 年代以降、インターネットの普及が進む一方インターネットにおける不正行為が数多く露見し、セキュリティ意識を強める必要性が高まりつつある。また電子証明書等のオンラインサービスにおける電子認証技術や IC カード等の認証デバイスの普及に伴い、電子認証技術の厳密かつ適切な利用が図られるようになりつつある。

しかし電子認証技術の普及が促進されるにつれて、これを適切に利用することには多くの課題があることがわかってきた。その課題は実装面と実践面の両方にある。

まず電子認証技術の実装技術は複雑で適切な実装を行うことが難しい。特に相互運用性を確保することは大きな課題である。実践については、更に制度面と実用化面に分かれ、各々に大きな課題がある。制度面では現実社会における電子認証の解釈(制度)の違いによって、公的な認証やビジネスにおける認証において利便性が上がらない問題を起こす。また現実社会において実用的でなければ、安全性向上に寄与しない不適切な利用が起こりうる。

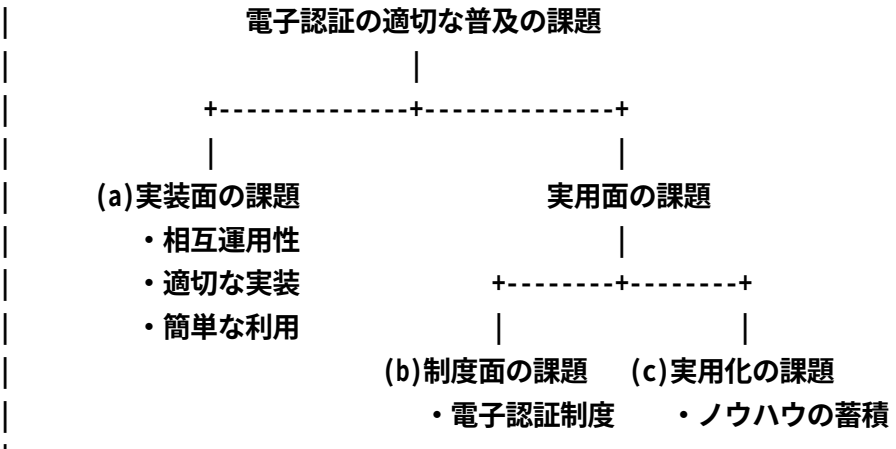

図 1 電子認証の適切な普及の課題の分類

図 1 は電子認証の適切な普及における課題を分類したものである。これらの課題に対して、日本国内ではいくつかの取り組みが行われている。(a) に対する取り組みには JNSA の ChallengePKI および PKI 相互運用性 WG の活動が挙げられる。特に ChallengePKI は電子政府における認証基盤の仕様策定に役立っている。(b)に対する取り組みには士業を中心とする電子認証局会議や日本 PKI フォーラムにおける次世代認証基盤プロジェクトが挙げられる。いずれも Web を使った情報公開が行われており多くの研究者に役立っている。

JPNIC では 2002 年より IP アドレスの管理を行うレジストリにおける認証局について調査研究を行ってきた。その一環として IETF や国内外の PKI の動向について調査を行ってきたが、図 1 の(c)にあたる活動は専門家による必要性が指摘されているにも関わらずほとんど存在しないことがわかってきた。JPNIC では更に 2005 年度から 2006 年度にかけて(c)の活動のあり方について調査研究を行ってきた。

この文書の(c)にあたるものが「電子認証プラクティスフォーラム」であり、(a)および(b)の活動とは補完関係にあると考えられる。この考え方に基づいて、後述する本フォーラムの Web ページに掲載することを想定した趣意を以下に示す。

JPNIC

電子認証プラクティスフォーラムとは

▼電子認証プラクティスフォーラムとは

電子認証プラクティスフォーラムとは、電子認証の適切な普及と発展を図るため、電子認証に関わるノウハウを BCP(Best Current Practice)として策定する活動を行うためのフォーラムである。

本フォーラムは基本的に考え方に基づいて活動を行う。

・ラフコンセンサスを重視

・議論と成果の一般公開

活動はメーリングリストと一年間に複数回のミーティングを通じて行う。

本フォーラムは、電子認証技術の実用的な利用に役立つノウハウの普及と蓄積を目的としており、技術を標準化することを目的としていない。活動の成果物は BCP と呼ばれるドキュメントである。本ドキュメントは基本的に参照情報であり、強制力を持つものではない。但し本フォーラムの活動内容を規定するものについてはこの限りではない。

本フォーラムの運営は経済産業省からの委託事業の一環として行われる。委託事業に先立ち、PKI(Public-Key Infrastructure)等の電子認証技術には

ノウハウの蓄積と共有が重要であることがわかってきている。本フォーラムは本事業の一環として実験的に運営され、2007 年度の後半に成果と効果の検証が行われる。

▼運営に関する情報

本フォーラムの事務局を JPNIC が行う。

問い合わせ先：

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
（省略）

以上。

5.4. 持続的なフォーラムのための設計

電子認証の技術的な分野においてコミュニティの形成とノウハウの共有が重要である点は前節で述べた通りだが、持続的な活動によってノウハウを蓄積していく仕組みを作るためには、ある程度慎重な設計が必要になる。

これまでにも本調査研究の一環として専門家チームを設立し、技術的な議論やドキュメント策定の活動を行ってきた。しかしいずれもその設立目的を達するか主要な議論を終えてしまうと議論そのものが収束してしまう。持続可能なコミュニティの形成には、IETF でとられているようないくつかの手法を取り入れる必要があると考えられる。

持続的なコミュニティ形成に効果があると考えられる手法（IETF 等の調査より）

- テーマごとの活動をライフサイクルとして捉え、全体のフォーラムは個別のテーマにとらわれずに持続させる意味を持たせる。
- 議論自体を目的とするのではなく、予め想定されるアウトプットを定めてから活動を始め、議論に参加していないものにも活動状況がわかるようにする。
- 趣意はドキュメント化し、実態と離れないようにする。
- 活動自体の見直しを行うことができるよう、活動自体についての文書化を進めておく。

これらの手法を取り入れ、持続的にノウハウの蓄積を行えるようにしたコミュニティが本調査研究で想定するプラクティスフォーラムになると考えられる。電子認証プラクティスフォーラムは、技術の標準化ではなくノウハウを扱うため、話題が多岐に渡る可能性があるため、これらの手法以外にも実施すべき工夫が必要となる可能性はある。

5.5. フォーラムの仕組みとコミュニティ構成

本節では、電子認証プラクティスフォーラムのコミュニティの構成について、これまでの調査研究の一環として行った議論の結果を示す。本節で示す資料は、本報告書作成の為にまとめたものである。

電子認証プラクティスフォーラムにおけるコミュニティとドキュメントの扱いを図 5-1 に示す。

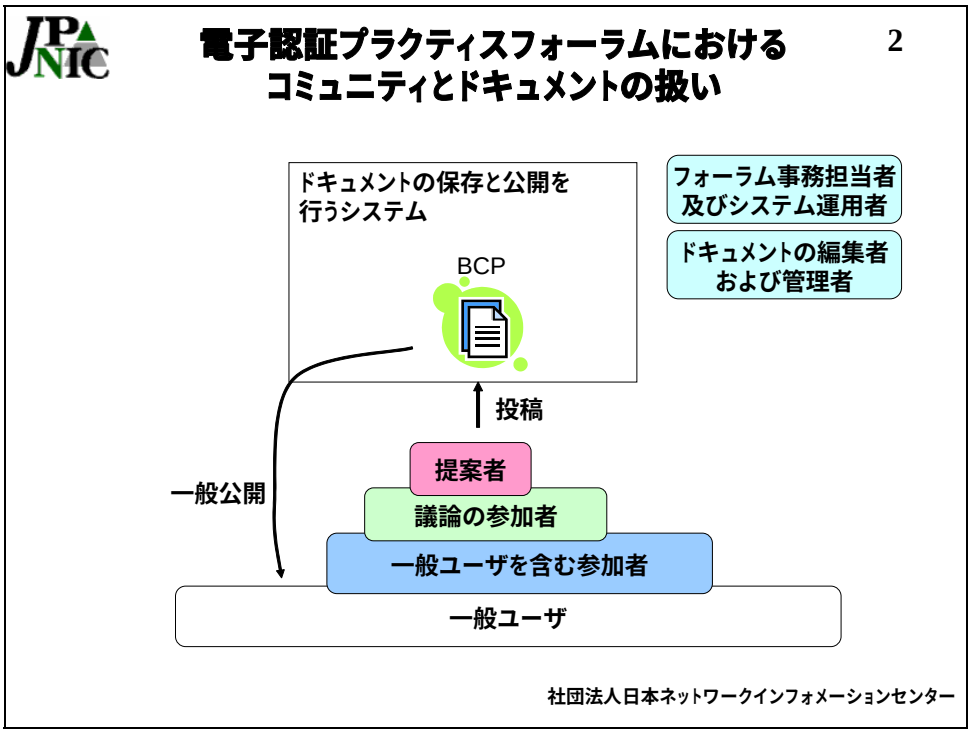

図 5-1　コミュニティとドキュメントの扱い

電子認証フレームワークにおけるコミュニティは、大きく分けて 4 種類のユーザに分けられる。「一般ユーザ」は電子認証の利用の有無に関わらず、Web などを使って本フォーラムが提供するドキュメントを閲覧できるユーザである。「一般ユーザを含む参加

者」は本フォーラムに参加しつつも議論への参加や提案を行わず、策定されたドキュメントの閲覧や議論の動向を追っているユーザである。「議論の参加者」は特定のドキュメントについての議論に参加し、ドキュメントを BCP 化することに協力しているユーザである。ここでは特に WG 等への参加を意味しているわけではなく、アクティブな「議論の参加者」ということを意味している。「提案者」はあるドキュメントを BCP 化することを提案したユーザである。提案者は、本フォーラムに投稿された文書が BCP 化されること、および「議論の参加者」や「一般ユーザを含む参加者」に情報公開されることを承知しており、本フォーラムを実現するシステムはその機能を提供する。BCP や議論の途中にあるドキュメントは、一般公開され一般ユーザでも閲覧できる。

本フォーラムを実現するために、参加者や一般ユーザ以外に「フォーラム事務担当者」や「システム運用者」、「ドキュメントの編集者」や「ドキュメントの管理者」が必要である。

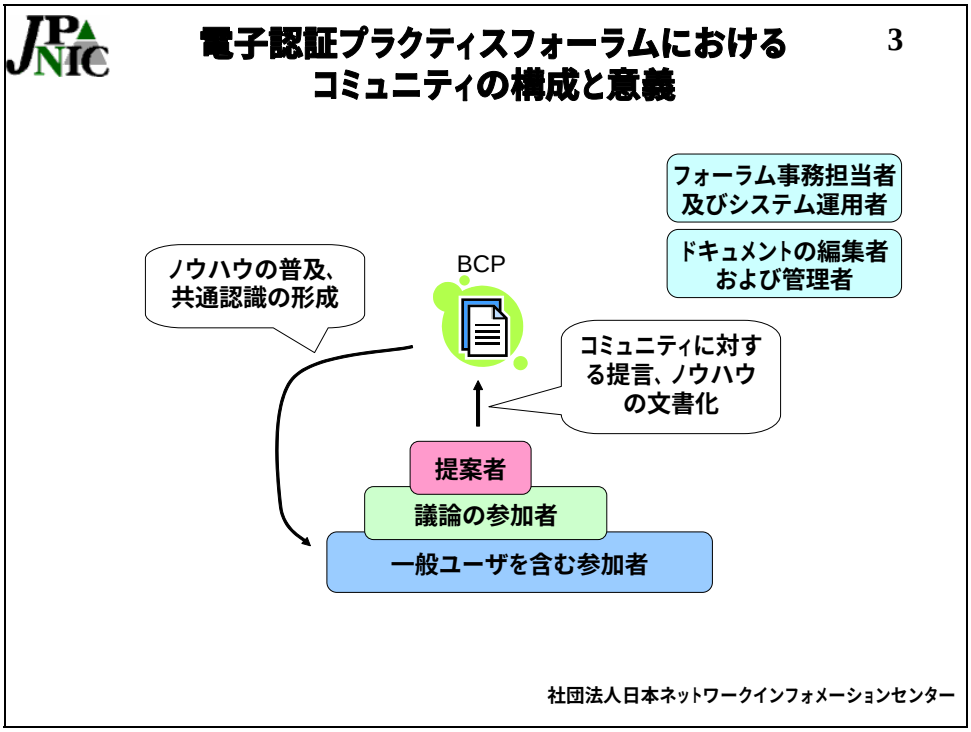

図 5-2　コミュニティの構成と意義

図 5-2 は本フォーラムのコミュニティに対する BCP の意義を示したものである。本フォーラムは提案者や参加者に対する活動に対する見返りは想定していない。従って、ドキュメントの提案者には BCP 化することのモティベーションを維持させ、また一般ユーザを含む参加者には策定された BCP を閲覧し、場合によっては議論に参加するモティベーションを維持させる必要がある。

本フォーラムにおける提案者のモティベーションとして考えられるものは、一般ユー

ザを含む参加者を含むコミュニティに対する提言と、公益性に配慮したノウハウの文書化である。コミュニティに対する提言は、技術情報の整理や分野に応じた利用技術の推奨を通じて共通認識の形成に資すると考えられる。従って技術分野における製品開発やサービス開発に役立つと考えられる。しかし特定の製品やサービスの促進を図ったものは、コミュニティの合意や後に述べる専門家によるレビュを通じて排除される可能性が高い。公益性に配慮したノウハウの文書化は、技術の適切な普及、例えばタイムスタンプビジネスの普及を図るといった観点で行われる提案になると考えられる。

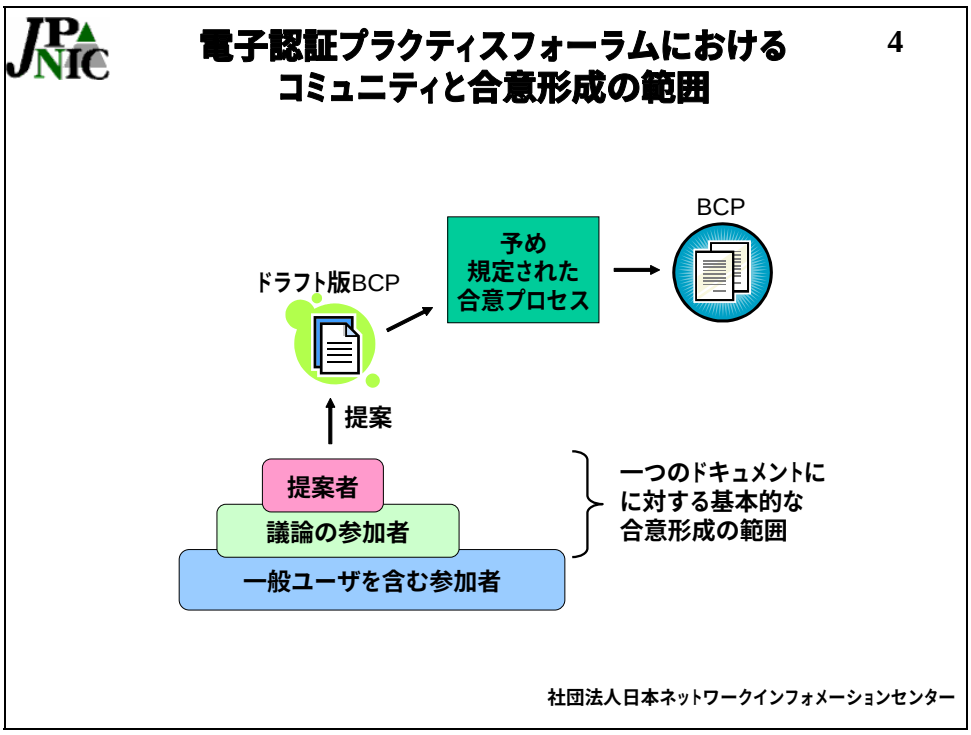

図 5-3　コミュニティと合意形成の範囲

図 5-1 で示したように、本フォーラムで策定されるドキュメントは参加者以外の一般ユーザにも公開されるが、BCP 化のプロセスの中では合意形成の範囲が設けられることが望ましい（図 5-3）。これは各ドキュメントには一定程度の専門性があると考えられ、本質的には、議論に参加していない、またはコミュニティに参加していない（参加者ではない）一般ユーザを合意形成の範囲に含めてしまうと議論が発散し、BCP 化を図ることが難しいと考えられる。従って現在の想定では提案者及び議論の参加者までの範囲とし、なおかつ合意プロセスは予め規定されドキュメント化されている必要がある。あるドキュメントの BCP 化に反対するものは議論に参加し、合意形成プロセスに含まれるようにする。また合意プロセスに反対するものは、合意プロセスを定めた BCP（事前に策定する必要がある）の「議論の参加者」として新たな BCP の形成に参加する必要があるものとする。

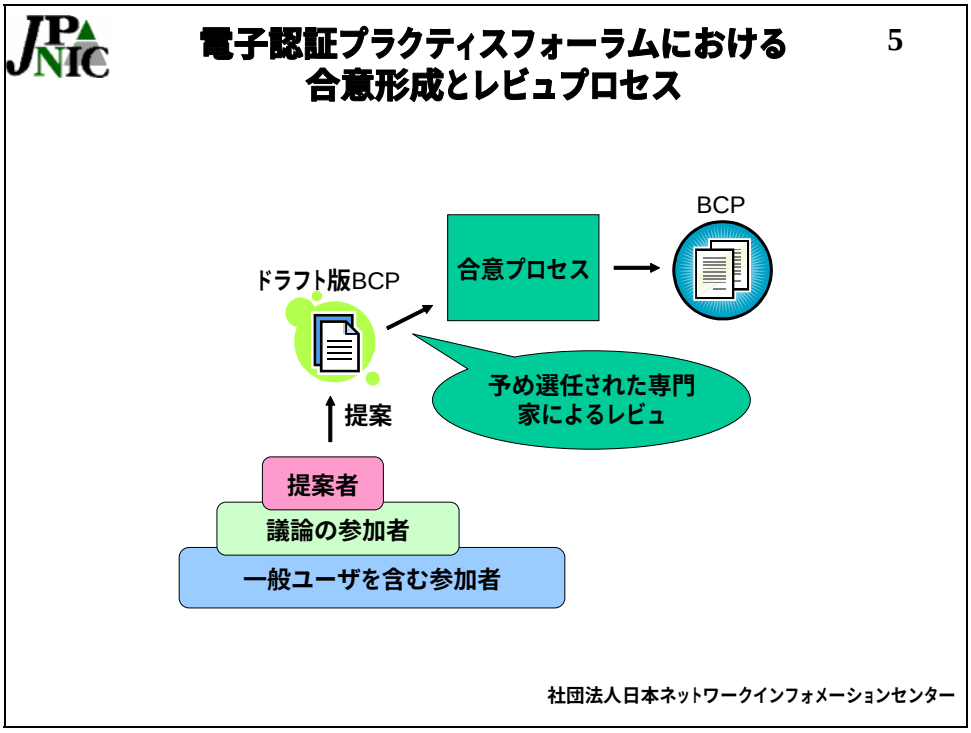

図 5-4　合意形成とレビュプロセス

本フォーラムでは、ドキュメント策定の基本原則は参加者によるコンセンサスに基づく合意プロセスであると考えられるが、専門的な技術に対するドキュメントの論旨を大きく外れないように修正する役割が必要になると考えられる。

図 5-4 は合意プロセスに入る前に「予め選任された専門家によるレビュ」が入っており、ドキュメントの洗練や技術の方向性に対する助言などができるような仕組みを示している。なお、IETF では参加者による合意プロセスの後に IESG（各エリアのエリアディレクター）によるレビュが行われることになっており、複数の専門家によるレビュが入る仕組みとなっている。本フォーラムでこれを実施するには、専門家のチームを予め作成しておき、更に本フォーラム全体の活動のレビュができるようなメンバーを選定しておく必要がある。

5.6. 電子認証プラクティスフォーラムの趣意と基本的な BCP

本節では、2006 年度の調査研究の一環で議論され、また可能な範囲で文書化した本フォーラムの趣意と基本的な BCP について述べる。本フォーラムは、フォーラム自身のルールを BCP として扱い、適宜再検討や更新を可能にする必要があると考えられている。基本的な規定を高頻度で変更することはコミュニティの活動を阻害する可能性があ

るが、ルールに関する BCP の提案者や専門家によるレビュが、その頻度を適切なものにすると考える。

本フォーラムにおける BCP の目的と書式を規定するドキュメント（BCP 案）を以下に示す。

```
BCP name: bcp-bcpformat-2007-01-draft.txt
Date: 2006/02/18
                                                              JPNIC

          電子認証プラクティスフォーラムにおける BCP の目的と書式


1. 概要

  電子認証プラクティスフォーラムで策定される BCP(Best Current Practice)の
目的と書式についてまとめたものである。本ドキュメントは本フォーラムの活動
を規定するものであるため、一部に強制力がある。


2. BCP の対象

  電子認証プラクティスフォーラムにおける BCP の読者および作成者


3. BCP の目的

  電子認証フレームワークにおける BCP は、電子認証技術の適切な普及を図ること
を目的として、ノウハウをドキュメント化したものである。

  ここでいうノウハウとは、BCP の提案者による十分な議論か既存の実用化を通じ
て得られた知識を指す。ドキュメント化の対象は一般公開が可能であるものに限り、
特定の製品やサービスに限定されない情報に限る。


4. BCP の経緯が想定される状況

  電子認証フレームワークにおける BCP を作成する場合や、BCP を理解するために
```

役立つ。

　本ドキュメントがなければ、BCP の書式がまちまちになって作成や理解の妨げになるだけでなく、ノウハウが蓄積されない恐れがある。

5．BCP の項目と書式

5.1．項目

BCP は以下の項目を含まなければならない。

・ヘッダー

－BCP name
BCP の名前を示す。"bcp-"に続いて作成または公開された年と改定番号をつなげたもの。最後に本フォーラムにおける状態をつなげたものとする。

例：bcp-bcpname-2007-01-draft
2007 年の 1 番目に公開されたもので、

状態については bcp-bcpprocess-2007-01-draft.txt を参照。

－Date
公開された日付を示す。

－著者の所属と氏名
著者の所属と氏名。所属組織の記入は任意である。

・タイトル

タイトルは全角で 12 文字～48 文字とする。

・概要

BCP 全体概要を示す。6 行以内で記述する。

・BCP の対象

BCP の対象読者を示す。「BCP の経緯や想定される状況」と合わせて閲覧者がドキュメントを読むべきかどうかを判断するのに役立つように記述する。

・BCP の目的

BCP によって当該ノウハウをまとめることの目的を示す。

・BCP の経緯や想定される状況

BCP としてまとめるべき知識が得られた経緯や、その知識が役立つと思われる状況を記述する。

・連絡先

BCP の改善のために使われる連絡先を記述する。所在地、所属、連絡先、担当または氏名などで、メールアドレスは必ず記述する必要がある。個人のアドレスである必要はない。メールアドレスの '@' は ' AT 'に置き換えること。

5.2. 記述の書式

BCP の書式はテキストファイルとする。図は基本的に罫線を利用しテキストで記述する。

書式の統一化は、事務局にて行う。公開に先立って著者の確認は行われる。

6. 連絡先

・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
（省略）

以上。

5.7. フォーラムのドキュメント策定プロセス

2006 年度の調査研究の段階での策定プロセスを定めた BCP を以下に示す。今後、コ

ミュニティの作成後、これらのプロセスをレビュし、参加者からのフィードバックを得て策定していく必要がある。

```
BCP name: bcp-bcpprocess-2007-02-draft.txt
Date: 2006/02/18
                                                              JPNIC

            電子認証プラクティスフォーラムにおける策定プロセス


1. 概要

   電子認証プラクティスフォーラムにおけるドキュメントの策定プロセスを
まとめる。全てのドキュメントは、ラフコンセンサスに基づいて参加者に
よる BCP としての認定が行われる。BCP として認定されたドキュメントは Web
ページにその旨が記載され公開される。本ドキュメントは本フォーラムの
活動を規定するものであるため、一部に強制力がある。


2. BCP の対象

   電子認証プラクティスフォーラムにおける BCP の読者および作成者


3. BCP の目的

   本 BCP は、電子認証プラクティスフォーラムにおける BCP 策定のプロセスを
明確化することを目的とする。


4. BCP の経緯が想定される状況

   電子認証フレームワークにおける BCP を作成する場合や、BCP を理解するために
役立つ。本ドキュメントがなければ、BCP の意味が不明瞭になりノウハウが蓄積
されない恐れがある。


5. 策定プロセス
```

電子認証プラクティスフォーラムにおける策定プロセスを図１にまとめる。

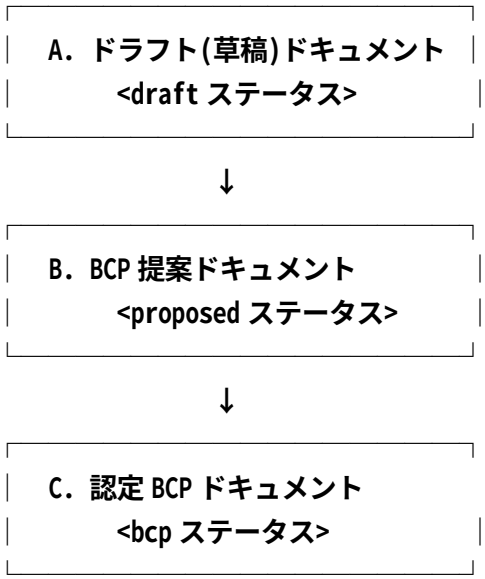

図１ 策定プロセス

・ステータスの移動

「ドラフトドキュメント」は草稿段階のドキュメントである。このドキュメントの作成は誰もが行うことができる。基本的にメーリングリストに投稿される。

以下の２点は今後記述されるべきと考えられている項目である。

・ドラフトドキュメントの提案者

・ドキュメントの有効期限

6. 連絡先

・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
（省略）

以上。

5.8. フォーラムの為のシステム提供

本フォーラムはコミュニティにおけるドキュメントの共有と一般ユーザへの公開、そして参加者や一般ユーザに策定状況をまとめた情報の提供の機能が必要となる。これまでの検討の結果以下のサービスを提供することが必要になると考えられる。

○メーリングリスト（ML）

コミュニティへの参加者が議論を行うためのメーリングリストである。またコンセンサスを得るためや、策定プロセスの進行に関する各種連絡などにも使われることが想定される。

一般ユーザがコミュニティに自由に入れる状況を作るためには、このメーリングリストは一般ユーザ自身が操作して加入できるような仕組みである必要がある。一方、スパムメールの流入を防ぐため、メンバーのみが投稿できる制限や、参加者のメールアドレスからスパムメールが送られたときの対処などが必要になると考えられる。

○メーリングリストアーカイブ

ドキュメント策定プロセスの中で過去の議論を参照したり、適切な議論が行われたことを証拠としてメーリングリストでの議論はアーカイブしたりされ、次の項で述べるWeb ページで提供されることが想定される。

○Web ページ

Web ページでは参加者へのドキュメント（BCP）の提供の他にドキュメントの策定状況がわかるような「ステータスページ」が必要になる。この他に本フォーラムにおいてオフラインでのミーティングが行われる場合には、資料や議事録がおかれることが考えられる。

図 5-5 に本フォーラムの実現の為のシステムの機能を示す。

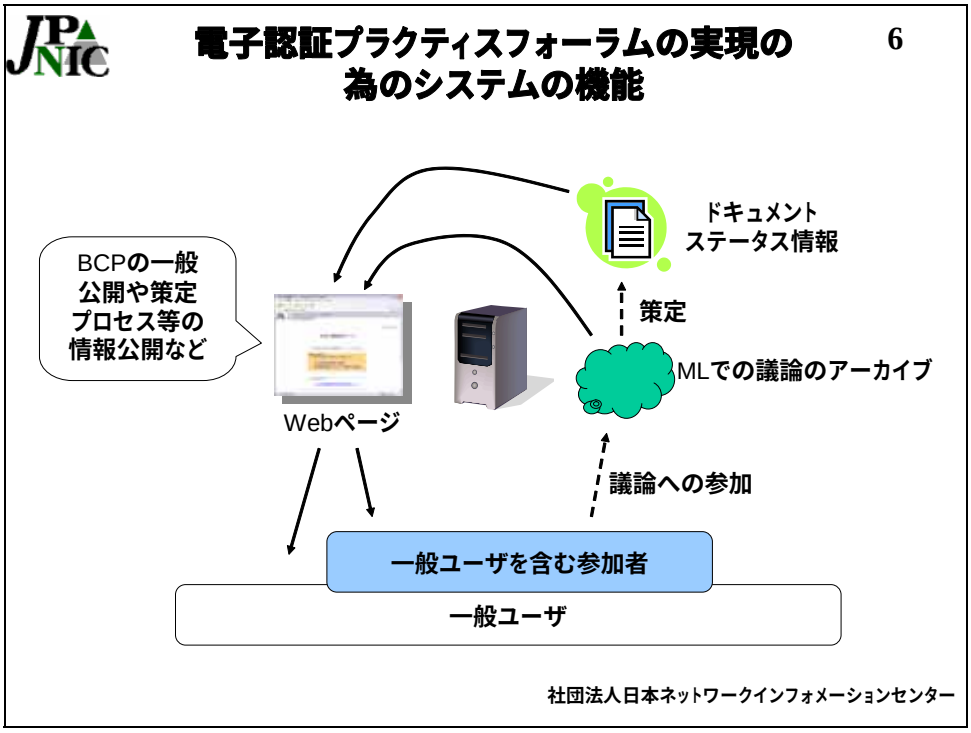

図 5-5　フォーラムの為のシステムの機能

本フォーラムでは議論され、合意プロセスを経たドキュメントは BCP として策定され Web ページで公開される。議論の内容も ML での議論のアーカイブとして公開される。従ってこれらを逐次保存し Web ページの更新を行う仕組みが必要となる。

2006 年度の調査研究では、これらの機能を実現するシステムの構築を行った。Web ページの提供や一般ユーザが参加できるような ML システムの設定も行った。今後、メーリングリストでの議論の内容を Web ページで逐次提供する機能を設置したり、本フォーラムに関する Web のコンテンツの準備などを進めたりする必要がある。

5.9. 議論と策定が必要な BCP

本調査研究では「IP アドレス認証の展開」の一環として「経路情報の登録機構」を構築し、その設計・開発の中で認証局の運用に関するノウハウがいくつか得られている。本フォーラムでは、これらの認証局の運用に役立つノウハウなどの BCP が策定できると考えられる。以下に本フォーラムで策定することが想定できる内容を挙げる。

〇認証局の運用に関する技術的な BCP

- CRL の管理運用
  ネットワークアプリケーションにおける電子認証の為の電子証明書を発行する認証局では、電子証明書の失効情報の提供の仕方に工夫が必要になる。それはアプリケーション上でのユーザアカウントの有効性と電子証明書の有効性を、予め定めた状態に定める必要があるためである。例えば電子証明書は有効であってもログインはできないといった状態を作るには、予め失効情報をアプリケーション側に転送しておき、SSL/TLS のコネクションを張りつつ、アプリケーション上でのエラー表示が必要となる。「経路情報の登録機構」ではこれらの状態のあり方について検討し、設計・開発を行った。

- 認証局証明書のライフサイクル
  認証局証明書は 20 年から 30 年といった長期的な有効期限を持つものであるが、クライアント証明書の有効期限と認証局証明書の有効期限の整合性を合わせるにはいくつかの工夫が必要となる。例えばクライアント証明書の有効期限を 2 年間と定める場合、認証局は認証局証明書の有効期限が切れる 2 年前には新しい認証局証明書を前提としたクライアント証明書の発行を行う必要がある。認証局証明書の更新の際に鍵の更新を行う方針で運用するならば、認証局において実際に一つの鍵を使ってクライアント証明書の発行を行うことができる期間は 18 年である。この点を踏まえてキーセレモニー（鍵生成）を行っていく必要がある。

- クライアント環境に応じた電子認証の保証レベル
  クライアント証明書を使った電子申請や商用の Web サイトにおけるユーザ認証が多く行われているが、相互に利用可能であるかどうかの判断基準は少ない。クライアント証明書の利用環境（IC カードを使用しているか等）や、クライアント証明書の発行状況に応じた電子認証の保証レベルがわかる指標が普及すれば、相互の利用可能性を判断する材料になると考えられる。自然人を対象とした電子証明書である場合には、プライバシー保護の観点からインターネットを介した商取引に向かない場合があるが、社員証と同等の効力を持つクライアント証明書が他社ないし取引先でのネットワーク接続（無線 LAN における認証など）や、三文判としての電子署名としての効力を持たせられるような相互利用の可能性がある。他の認証局が発行した電子証明書の効力をどの程度のレベルであるかにマッピングすることで、同程度のレベルであれば相互の利用が可能になるような概念の普及を図ることが考えられる。

5.10. まとめと今後の課題

本章では、2005 年度より調査研究を行ってきた「電子認証フレームワーク」を策定するフォーラムである「電子認証プラクティスフォーラム」について述べた。本フォーラムは、電子認証に関わるノウハウを BCP としてドキュメント化し、一般ユーザにおける共通認識の形成などを目指したフォーラムである。「電子認証フレームワーク」は本フ

ォーラムで策定される BCP の一部に位置づけられる。電子認証フレームワークは、電子認証における保証レベルや電子認証技術の運用に関わるノウハウを BCP として扱い、複数の業界で共通認識として参照可能な概念を明文化する。

本フォーラムを実現するため、2006 年度はより詳細なフォーラムの機能とシステムの要件を明らかにした。更にそれらの機能を実現するためのサーバ構築等を行った。

今後、本フォーラムを運営するための資料作成や ML の立ち上げなどが課題となる。また今後一部の専門家だけでなく一般の人々の中から興味を持って参加して頂く方法について検討することも課題として挙げられる。