第 2 章　電子認証フレームワークに関する調査研究

内容
- 電子認証プラクティスフォーラムとは
- フォーラム活動（BoF、ML）
- ノウハウのドキュメント策定

ほか

2. 電子認証フレームワークに関する調査研究

2.1. 概要

電子認証フレームワークに関する調査研究では、「電子認証プラクティスフォーラム」と呼ばれるフォーラム活動を実験的に行った。本フォーラムは、電子認証に関わるノウハウをドキュメント化し、BCP（Best Current Practice）として公開する会議体である。BCP という言葉は、Business Continuity Plan の略語としてしばしば使われる言葉であるが、本調査研究で動向を追ってきた IETF（Internet Engineering Task Force）では、別の意味で用いられている。

IETF は元来、プロトコル（通信規約）を策定する会議体であるが、”Code then spec”、すなわち動作するプログラムやプロトコルを重視する理念に裏打ちされて、開発や運用の経験を持つ者の意見が尊重される文化がある。そのため IETF には開発ノウハウや運用ノウハウを持った技術者が集っており、それをドキュメント化して残しておく活動が行われてきた。そのドキュメントは BCP（Best Current Practice）と呼ばれている。IETF における BCP は、番号がつけられ、Web を通じて誰もが入手できるようになっている。これは BCP に限った話ではないが、IETF におけるドキュメントは、予め決められた策定プロセスに則って、公開された状態で議論が行われていく。BCP として公開されるまでに多くの人のチェックを受けるため、ドキュメントの品質は高い。

本調査研究は、この IETF における BCP の考え方が電子認証技術に適用できないか、という観点で行われた。PKI（Public-Key Infrastructure）を始めとする電子認証技術は、その技術開発やプロトコル策定は進んでいるものの、それらが適切に利用され、普及しているとはなかなか言えない。電子認証技術における BCP が蓄積されていれば、もっと便利で安全な認証技術が deploy（展開や普及）されているはずだ、というのが 2005 年、第 60 回 IETF のセキュリティエリアの会合で議論されていたことであった。

冒頭で触れた電子認証プラクティスフォーラムは、まさにこの BCP の蓄積を目的とするフォーラムである。メーリングリスト（以下 ML と呼ぶ）でノウハウのドキュメント提案を受け付け、議論し、ある程度レビューされたところで Web ページにその旨を公開する。ノウハウを持っている参加者には、そのノウハウが現行の実用（Practice）において最適であることを確認できる場となる一方、フォーラムに参加する人は共通理解と最新のノウハウを得ることができる。コミュニティ全体としては、参加者が実用上、うまくいきそうな方式を真似ることで、電子認証技術の要である相互運用性の向上を図ることが可能になる。

2007 年度は、本フォーラムのオフラインミーティングである BoF（Birds of a Feather）を開き、また ML にて投稿を受け付けて実際のドキュメント化活動を行った。その結果、ノウハウとしては 3 つのドキュメントが作成された。また BoF の会場で行ったアンケートの結果、参加者に意義が認められ、後述するレビューチームからも本フォ

2. 電子認証フレームワークに関する調査研究

2.1. 概要

電子認証フレームワークに関する調査研究では、「電子認証プラクティスフォーラム」と呼ばれるフォーラム活動を実験的に行った。本フォーラムは、電子認証に関わるノウハウをドキュメント化し、BCP（Best Current Practice）として公開する会議体である。BCP という言葉は、Business Continuity Plan の略語としてしばしば使われる言葉であるが、本調査研究で動向を追ってきた IETF（Internet Engineering Task Force）では、別の意味で用いられている。

IETF は元来、プロトコル（通信規約）を策定する会議体であるが、”Code then spec”、すなわち動作するプログラムやプロトコルを重視する理念に裏打ちされて、開発や運用の経験を持つ者の意見が尊重される文化がある。そのため IETF には開発ノウハウや運用ノウハウを持った技術者が集っており、それをドキュメント化して残しておく活動が行われてきた。そのドキュメントは BCP（Best Current Practice）と呼ばれている。IETF における BCP は、番号がつけられ、Web を通じて誰もが入手できるようになっている。これは BCP に限った話ではないが、IETF におけるドキュメントは、予め決められた策定プロセスに則って、公開された状態で議論が行われていく。BCP として公開されるまでに多くの人のチェックを受けるため、ドキュメントの品質は高い。

本調査研究は、この IETF における BCP の考え方が電子認証技術に適用できないか、という観点で行われた。PKI（Public-Key Infrastructure）を始めとする電子認証技術は、その技術開発やプロトコル策定は進んでいるものの、それらが適切に利用され、普及しているとはなかなか言えない。電子認証技術における BCP が蓄積されていれば、もっと便利で安全な認証技術が deploy（展開や普及）されているはずだ、というのが 2005 年、第 60 回 IETF のセキュリティエリアの会合で議論されていたことであった。

冒頭で触れた電子認証プラクティスフォーラムは、まさにこの BCP の蓄積を目的とするフォーラムである。メーリングリスト（以下 ML と呼ぶ）でノウハウのドキュメント提案を受け付け、議論し、ある程度レビューされたところで Web ページにその旨を公開する。ノウハウを持っている参加者には、そのノウハウが現行の実用（Practice）において最適であることを確認できる場となる一方、フォーラムに参加する人は共通理解と最新のノウハウを得ることができる。コミュニティ全体としては、参加者が実用上、うまくいきそうな方式を真似ることで、電子認証技術の要である相互運用性の向上を図ることが可能になる。

2007 年度は、本フォーラムのオフラインミーティングである BoF（Birds of a Feather）を開き、また ML にて投稿を受け付けて実際のドキュメント化活動を行った。その結果、ノウハウとしては 3 つのドキュメントが作成された。また BoF の会場で行ったアンケートの結果、参加者に意義が認められ、後述するレビューチームからも本フォ

ーラムの意義に関する高い評価を得ている。この事から、調査研究の一定の成果は得られたと考えている。

本章では、はじめに、本調査研究の実践的な活動となった電子認証プラクティスフォーラムについて述べる。このフォーラムとオンラインの活動、オフラインの活動、ドキュメント策定の 3 つの活動について述べる。次に、オンライン活動を支えるシステムはどのように設計されたか、そしてドキュメント策定活動の調査はどのように行われたかについて述べる。最後に今後の課題と展望などについて述べる。

2.2. 電子認証プラクティスフォーラムの背景

電子認証プラクティスフォーラム（以下、本フォーラムと呼ぶ）は、電子認証技術の構築や利用に役立つ概念や知識をドキュメント化し、その共通理解と共有を図る会議体である。このようなフォーラムが必要とされた背景に、電子認証技術が日本国内において本格的に普及していない状況がある。

電子証明書の技術標準に ITU-T の X.509 や IETF の RFC3280 がある。詳しくは第 3 章で述べるが、いずれも技術の標準化が先行しており、実用化は遅れている。いまや多くの Web ブラウザに電子証明書の技術が実装されているが、サーバ認証のみであるなど、一部の機能が使われているに過ぎない。スマートカードの分野では電子証明書の普及が進みつつあるが、相互運用性の面で大きな課題が残っている。つまり一般的な開発者が簡単に実用化できるような状況には至っていない。この状態では、電子認証技術の普及は困難な作業となるはずである。

日本国内における電子認証技術の適切な普及の課題を図 2-1 にまとめる。

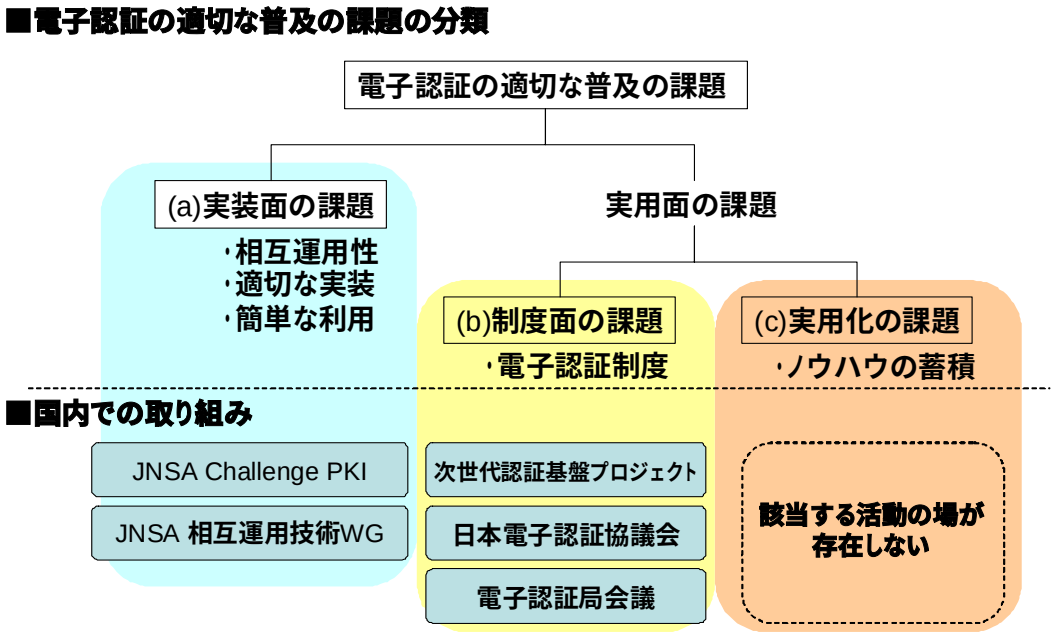

図 2-1　電子認証技術の普及の課題

電子認証技術の適切な普及には、大きく分けて 2 つの課題がある（図 2-1 の上側）。実装面の課題と実用面の課題である。実装面の課題には、相互運用性を確保するための実装を行えるような状況を作ったり、技術標準にあった適切な実装を行えたりするようにするといった課題がある。

(a)実用面の課題は、更に制度面の課題と実用化の課題の 2 つに分かれる。

(a)実装面の課題に対する日本国内の取り組みとしては、日本ネットワークセキュリティ協会（JNSA）の Challenge PKI や相互運用技術 WG の活動が挙げられる。Challenge PKI は、電子証明書の相互運用性に関する試験やテスト環境の開発などが行われた活動である。JNSA の相互運用性技術 WG は、電子署名・認証技術に関わる国内外の動向の調査やセミナー等を行っている。

(b)電子証明書に関わる制度の整備を行う取り組みも日本国内にある。適切な制度の整備が行われなければ、社会的に認められる位置づけになりにくいという観点で、制度面の整備は重要である。まず挙げられるのは経済産業省と日本 PKI フォーラムにおいて行われた次世代認証基盤プロジェクトであろう。このプロジェクトでは電子認証や電子署名の民間での整備に役立つ「保証レベル」の調査などが行われた。この他に士業認証局を含む認証局運営者の会議体である、電子認証局会議が挙げられる。電子署名法や特定認証業務の認定基準に対して、実務的な観点で議論が行われている。また、EV SSL 証明書の日本国内での認定基準の整備などを行っている日本電子認証協議会の活動も制度面での取り組みであると考えられる。

残るは(c)実用化の課題である。実用化とは、技術そのものの改良や改善も含まれるがそれだけではなく、適切かつ効率的に利用されるようにすることである。科学技術の普及に実用化が不可欠であるのと同じように、電子認証技術にも実用化が不可欠である。しかし日本国内においては、電子認証技術の実用化の活動はほとんど見当たらない。また国際的にも多くはない。

ここでいう実用化とは、ベンダーやシステムインテグレータによる開発のことは意味していない。なぜなら、ある特定の要件を持つシステム開発は、技術の利用であって、技術の発展や普及を目的としたものではないためである。本調査研究は電子認証技術の発展や普及を目的としている。複数のベンダーが情報交換し、技術の適切な利用や運用について情報交換することで初めて技術自体が実用化される。そしてその成果が残っていて、皆に役立つように提供されていることも重要である。実用化の場という意味では、IETF や ITU-T は該当しない。これらは、技術標準の策定が目的であって、技術の利用は目的ではない。IETF における BCP は、技術標準の策定や技術標準の運用に寄与するものであったり、技術標準に対する補助的な位置づけであったりするためである。

2.3. 電子認証プラクティスフォーラムの考え方

電子認証技術の実用化に役立つノウハウはどのようにすると蓄積され、活用されるのか。電子認証プラクティスフォーラムでは、会議体におけるノウハウの蓄積を実現する為に図 2-2 に示すような考え方を導入した。本節では、この考え方、すなわち電子認証プラクティスフォーラムで目指すことについて述べる。

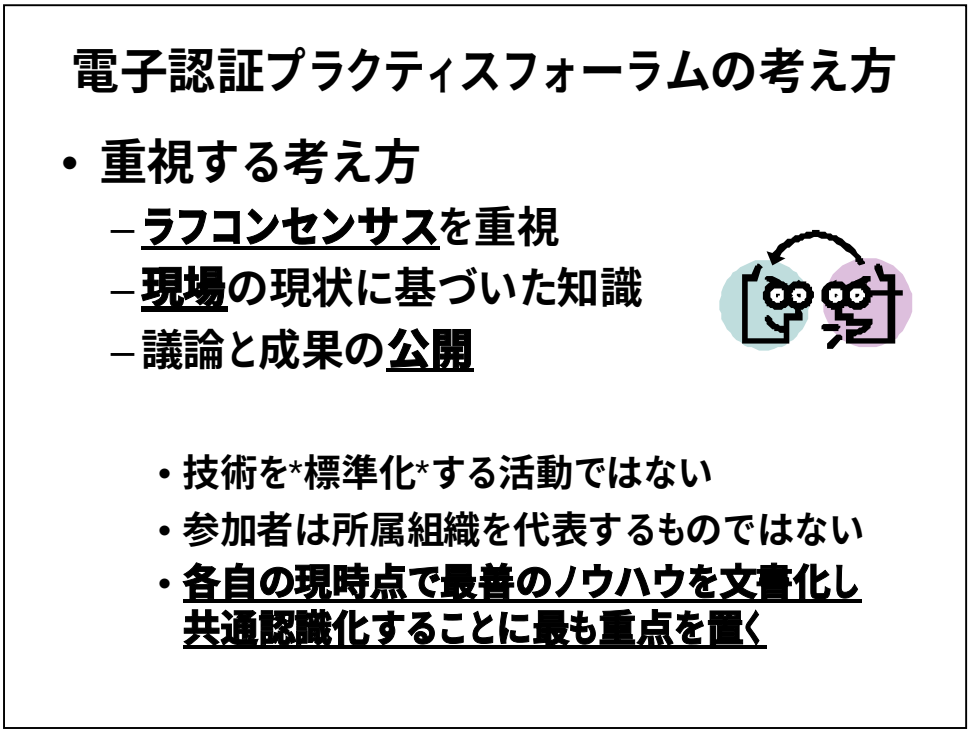

図 2-2　電子認証プラクティスフォーラムの考え方

ノウハウというと、製品やサービスを開発提供する企業において蓄積された企業秘密の情報が類されると考えられる。しかし電子認証技術の発展という意味では、企業秘密では意味がない。企業などで得られたノウハウが共有されて、他の複数の組織によって価値が認められることで、技術に対して意味のあるノウハウだと言える。

特定のテーマについて調査結果などがまとめられたホワイトペーパーと呼ばれる文書があるが、こちらは他の組織から参照でき、論文に引用されるなど、「ノウハウの蓄積」に近いものがある。ノウハウには、本書のような調査研究報告書も含まれるかも知れない。また技術解説書の内容にはノウハウは含まれているだろう。まずは、一度ドキュメント化されたノウハウは、一般に公開され、閲覧する立場にとって蓄積されていくことが重要であるといえる。

ここでノウハウの蓄積するための仕組みについて考えてみたい。例えばノウハウをまとめた文書の使われ方を考えると、そのノウハウが置かれる状況はいくつかの段階を持っているといえる。「作成される段階」「共有される段階」「認知されていても利用されない段階」「忘れられる段階」などである。中には「共有される段階」を経ずに「忘れられる段階」になってしまうものがあるかも知れない。ホワイトペーパーや本報告書のようなドキュメントは、一旦「忘れられる段階」を経ると失われた状態になってしまい、例えば関連する新しいノウハウが生み出されて、情報が更新されていくようなことは考えにくい。一方、IETF における RFC はこの更新されるサイクルを持っている。上書きや情報更新によって参照されなくなった古いドキュメントは「obsolete されたもの」とい

う区分を持っており、一方、新しいドキュメントの方には「○○を obsolete した」と書かれる。過去のノウハウは一度ドキュメント化されると失われることはないが、参照されることがなくなるという考え方は重要である。

新しいドキュメント（IETF ではドキュメント化されるのはプロトコルである）は必ずしも古いドキュメントを obsolete する必要はなく、むしろ新しいドキュメントを作成することが奨励される。IETF という会議体の中で参加者の興味や技術動向に応じて次々にドキュメントが作られていく構造がある（図 2-3）。

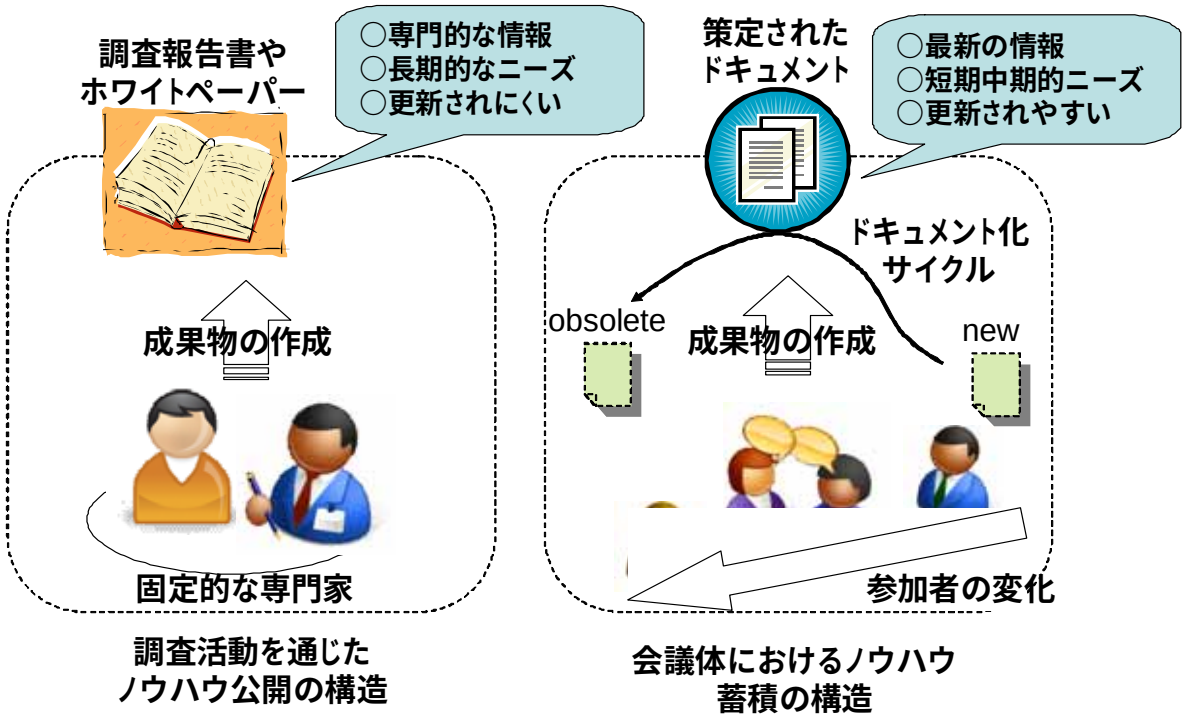

図 2-3　ノウハウのドキュメント化構造の違い

電子認証に関わるノウハウは、その時々のニーズに合わせてノウハウがドキュメント化される状況は望ましい。つまりノウハウを一度ドキュメント化して公開することで活動をやめてしまうのではなく、新たな技術やノウハウの出現を許容し、新たなドキュメントのサイクルを作り出せるような場が必要だと考えられる。それには新たなノウハウはどんどんドキュメント化されていくような、ラフな考え方が不可欠である。IETF では厳密に決議を取るようなことをしない物事の決め方は、ラフコンセンサスと呼ばれ、第一原則の一つとして考えられている。

電子認証技術に関するノウハウは、ラフコンセンサスの考え方で、現代のニーズに即したノウハウを文書化するような活動が適すると考えられる。

本フォーラムにおける考え方の 2 つ目は、「現場の現状に基づいた知識を重視する」ということである。Web ページなどを使って一般公開されているホワイトペーパーの中には、よく練られた論文に近い品質のものがある。優れたドキュメントは、学会等で発表され、普及が図られることで技術の発展に寄与すると考えられる。しかし逆に現場を離れた専門家による文章が多い。きちんとした文書は利用価値が高いと考えるが、一方で現場レベルの情報が少ないことが多い。簡単な設定方法などの情報は、Web ページの個人のページ等で見つけることができるが、現場で実用化に取り組む技術者が求める情報がカバーされにくい。

本フォーラムでドキュメント化されたノウハウの中に、「認証局における鍵更新のタイムチャート」がある。これは認証局において、発行している証明書の有効期限を一定に保つように証明書の発行を行うために、どのようなサイクルで認証局の鍵更新を行っていけばよいかをチャートでまとめたものである。このような情報は、一度認証局を運用してみたものにとっては自明であるが、Web ページ等では公開された情報としてなかなか見つからない。オープンソースソフトウェアを使った認証局の設定方法などは簡単にいくつも見つけられるが、認証局を構築する現場の技術者、または実際に運用を行うものが必要とする情報は、得にくい状況である。

認証局の構築を行うシステムインテグレータが、構築時にノウハウを得られない場合、何らかの課題、例えば継続的な認証局の運用を行うためのシステムの設計には、そのシステムインテグレータによる独自の考え方が盛り込まれる。PKI 製品の中には、失効検証のできないものがあるが、いまや多くの Web ブラウザで失効検証が行われるようになり、PKI の利用が失効検証を当たり前とする情勢になりつつある。これは、個々の製品の実装レベルの違いであると片付けることはできる。しかし PKI における失効検証は新しく現れた技術や方式ではない。開発を行う者が「最低限、備えておくべき機能」という情報を共有していなかったために、同じ PKI を使った製品でも大きな機能の違いが出てしまうのではないだろうか。

それでは、特定の技術標準に準拠するための、ガイダンスのようなドキュメントがあれば実装の差異の問題は解決するのだろうか。仮に、あらゆる実装が技術標準に従うことが可能な状況、つまり技術標準の策定内容が簡単であれば、そのガイドに則って開発を行い、問題解決が図られるかも知れない。しかし、特に電子認証技術にはこの点で大きな問題点がある。IETF の RFC3280 や ITU-T の X.509v3 は、仕様が高度過ぎて多くの実装がカバーしきれていないことである。策定されている内容が多い上に、処理の内容が複雑で、多くのプログラミングを必要としてしまう。（例：横断証明書のパス構築など）

RFC の Request for Comments という意味の通りに捉えれば、実装するものが何かを強制されるものではない。しかし技術標準のどの部分に準拠すべきで、どの部分は準拠しなくていいか、ということは実装者自身が判断するしかなくなってしまう。RFC における MUST、SHOULD、MAY の区分けも、技術標準の規模が大きい場合には役に立ちにくくい。これでは実装の差異が大きくなってしまい、相互運用性が達成されにくくなってしまう。

本フォーラムでは、技術標準よりも現場の現状に基づいた知識を重視するものとした。これは、現場の利用場面は何か、現時点での多くの実装がどうなっているか、といった現場の現状をノウハウの基本とする考え方である。場合によっては、技術標準と異なる仕様が多くの現場で採用されていることも考えられる。技術の標準化の観点では、これは望ましいことではないが、実用化の観点では標準化が功を奏していないと見ることもできる。技術標準を無視して市場の動向にのみ任せることは、相互運用可能な高度な技術の発展の意味では望ましくない。逆に、現場の現状が技術の標準化の場にフィードバックできるような形があればベストである。

これまで述べてきたことを総合すると、本フォーラムが、IETF のプロトコル策定の場や、IP アドレスポリシーの策定の場である OPM（Open Policy Meeting）の考え方に近いと思われたはずである。一方で、電子認証技術の現場と現状に基づくという点、そして日本国内でドキュメント策定を行うことに、トライアル的な要素を感じられたのではないだろうか。本調査研究の 2007 年度の活動は、まさにこのトライアルの部分に取り組んだ。

2.4. 電子認証プラクティスフォーラムのための基礎調査と設計

本調査研究は、開始当初、フォーラム活動を行うような最終的な活動のイメージは明らかにはなっていなかった。2005 年度、2006 年度の調査研究を通じて、電子認証の適切な普及に必要なもの、かつ各分野に横断的に役立つものは何かを探ることが、調査研究の本質的な作業であった。

2005 年度から 2007 年度にかけての 3 年間は、概ね年度ごとに 3 つのステップで進められた

表 1　3 年間の調査研究のステップ

年度と実施項目	活動内容	成果の生かし方
2005年度 ・電子認証フレームワーク ・各国の策定プロセス調査 ・必要性とIETFの状況調査	○電子認証フレームワークにおける策定プロセスに関する調査研究 ・各国のベストプラクティスにあたるドキュメント策定について調査し結果を報告。BCPの策定プロセスの要件をまとめた。	○電子認証技術は、技術が未熟なのではなく、ノウハウが足りていないという現状認識。電子認証技術を利用する敷居を下げ、ノウハウに関する普及・啓発を図る。
2006年度 ・電子認証フレームワーク ・策定プロセス案作成 ・プラクティスドキュメント例作成	○電子認証フレームワークの策定プロセス案とドキュメントの例などの調査 ・策定プロセス案の作成とベストプラクティスドキュメント例の作成。 ・議論のためのML、Web等	○策定プロセス案を通じて、BCPを作成するための書式や、ドキュメント例が得られる。総合運用性のある電子証明書の実現の為に、他社とノウハウを共有するときの書式や手続きが得られる。
2007年度 ・電子認証フレームワーク ・策定プロセスの試験実施 ・体制の評価	○電子認証フレームワークで策定されたBCP ・策定プロセスに則って策定されたBCP	○策定プロセスに参加し、BCPを共有。適切な電子証明書の使い方がわかる。各利用場面において共通のノウハウを作り、相互運用性のある電子証明書の発行が可能となる。電子証明書を通じた安全なやり取りの促進。

2005 年度は、国際動向や類似する活動の動向の基礎調査である。電子認証技術の最新動向は当然の事ながら、国内外でノウハウの蓄積はどのように行われているかを調査した。2006 年度は必要な仕組みの研究を行った。ドキュメントを会議体の中で作成する考え方は 2005 年度の段階であったが、それを国内で実施するために、具体的なシステムの要件等を設計した。

次の節では、2007 年度に行われた本フォーラムの活動について「オフライン活動」「オンライン活動」「ドキュメント策定」の 3 つにわけて報告する

2.5. 電子認証プラクティスフォーラムの 3 つの活動

電子認証プラクティスフォーラムは、電子認証技術に関するノウハウをドキュメント化し共有するという特有の活動を行うフォーラムである。一方、活動の様式は、2006 年度までの調査研究の結果から、BoF と呼ばれるラフな雰囲気の会議の「オフライン活動」、メーリングリストと Web を利用した「オンライン活動」と、そして IETF や IP アドレスに関する OPM で行われている「ドキュメント策定」の仕組みを採用した。

オフライン活動は、議論の方向性やコンセンサスの確認のために行われる。本フォーラムにおける BoF は、IETF と同様で、関心を持つものが集まる場のようなラフな会議の場を指す。ここではノウハウの紹介やドキュメント化プロセスの一環としてのコンセンサスの確認が行われる。BoF の他にはレビューチームの会合がある。レビューチーム

は、ドキュメントが最終的に BCP（Best Current Practice）になる前に、専門的かつ様々な観点でレビューを行うチームである。チームは、認証業務や法制度、電子認証技術に詳しい方などで構成した。またこのチームでは本フォーラムの活動レビューも行った。

オンライン活動は、多くの人が本フォーラムで蓄積されたドキュメントを参照することを可能にする。単に本フォーラムに参加していないものにドキュメントが参照されるだけでも、本フォーラムの意義がある。むしろ策定されたドキュメントが普及することで、技術の相互運用性やノウハウが得られる場を増やすという意味でプラスとなる。本フォーラムにおいてドキュメント化に取り組むものにとっては、IETF におけるプロトコル策定と同じように、著者および著者の属する組織が相当の技術力を持つということが、広く認知される機会となる。

ドキュメント策定とは、予め定めたプロセスに則って参加者のラフコンセンサスをとり、本フォーラムがそのプロセスを経たドキュメントの価値を認めるまでの一連の活動である。これにより、様々な人が参加して提案され、策定されたドキュメントの最終的なクオリティが維持されると共に、フォーラム参加者全体が注目しているノウハウを自然とキャッチアップしていくことを目指している。

本調査研究は、はじめに Web ページとメーリングリストを開設し、続いて BoF を行った。また 2008 年 2 月以降にレビューチームの会合を行った。次に、各活動の詳細について述べる。

2.6. オフライン活動

電子認証プラクティスフォーラムの BoF は、2007 年 11 月 19 日（月）、InternetWeek2007 というカンファレンスと同じ会場で行われた。

BoF には、約 30 名の参加があった。この BoF では主に本フォーラムの紹介と議論を行ったが、ノウハウの紹介も 2 つ行われた。アジェンダを以下に示す。

2007 年 11 月 16 日(金)

第一回 電子認証プラクティスフォーラム BoF アジェンダ

開催日：2007 年 11 月 19 日(月)

場所：秋葉原コンベンションホール 5F 5A

JPNIC

○オープニング、17:30

○電子認証プラクティスフォーラムの紹介、17:35
(JPNIC 木村 泰司)

[コーヒーブレーク 18:00-18:10]

○電子認証技術のノウハウに関するディスカッション、18:10
- ディスカッションに関する説明と例
  (JPNIC 木村 泰司)
- 認証局証明書の更新が与えるユーザアプリケーションへの影響の調査
  (富士ゼロックス 横田 智文氏)
- PKI におけるマルチドメイン問題
  (セコム IS 研究所 島岡 政基氏)

など

○電子認証ブレインストーム、19:00
- ブレインストーミングに関する説明
  (JPNIC 木村 泰司)

本フォーラムで解決していくべき課題点をオープンマイクロホンの形式で募集し、その原因や仕組み、あり方などについて議論します。
皆さんが日々心の中に溜めている課題を是非持ち寄ってきて下さい。
以下の 2 つの観点で議論します。

－電子認証の技術に関する課題集めと議論
－本フォーラムに関する課題集めと議論

当日はマイクに向かって簡単に説明して頂いて、会場全体で議論したいと思います。

○クロージング、19:25

以上。

「電子認証プラクティスフォーラムの紹介」では、前節までに述べた、本フォーラムの位置づけや目指すこと、仕組みなどについて紹介を行った。

「電子認証技術のノウハウに関するディスカッション」では、はじめにディスカッションの方法について説明した後、2 つのノウハウの紹介と議論が行われた。以下では、概要を示す。

BCP name: bcp-draft-intercacertupdate-01.txt
Date: 2008/03/04

富士ゼロックス株式会社
横田智文

中間認証局の証明書更新が与える PKI アプリケーションへの影響

1．概要

本ドキュメントは、認証局の電子証明書を更新するにあたって、ユーザへの影響を最小限に押さえつつ、スムーズに更新する条件について、調査結果をまとめたものである。
また本ドキュメントでは、特に中間認証局の証明書更新方法を策定するための情報を提供しているが、認証局証明書更新時の PKI アプリケーションの振る舞いについては、ルート認証局の証明書更新方法を検討する上でも参考になると思われる。

横田氏の発表は、認証局の鍵更新による証明書更新によって、現バージョンのアプリケーションがどのような影響を受けるか、ひいては多くのアプリケーションで問題にならない認証局証明書の更新方法は何か、という調査を行った結果である。このときには調査の経過が発表されたが、最終的にドキュメントにはその結果が盛り込まれた。

BCP name: bcp-draft-appropriate-policymapping-01.txt
Date: 2008/03/05

セコム株式会社
島岡政基

保証レベルとポリシ管理機関による適切なポリシマッピングの実現

1. 概要

複数の認証局におけるポリシマッピングを行う際に起こるポリシの伝言ゲーム問題について述べ、その一つの回避策として保証レベルの導入とポリシ管理機関による運用によって適切なポリシマッピングを実現する方法を紹介する。

島岡氏の発表は、複数の PKI ドメインの間でポリシマッピングを行って電子証明書の相互運用を図る際に、ポリシマッピングを複数経ることで認証のレベルが落ちていく「伝言ゲーム問題」の解決策を示したものである。この解決策は米国の Federal PKI で一部が運用されているという事例の紹介もあった。

木村の発表は、参加者が本フォーラムで扱われるノウハウはどのようなものであるかを理解しやすくするためのものである。そのため、共有すべきノウハウとして考えられるものの例を挙げた。

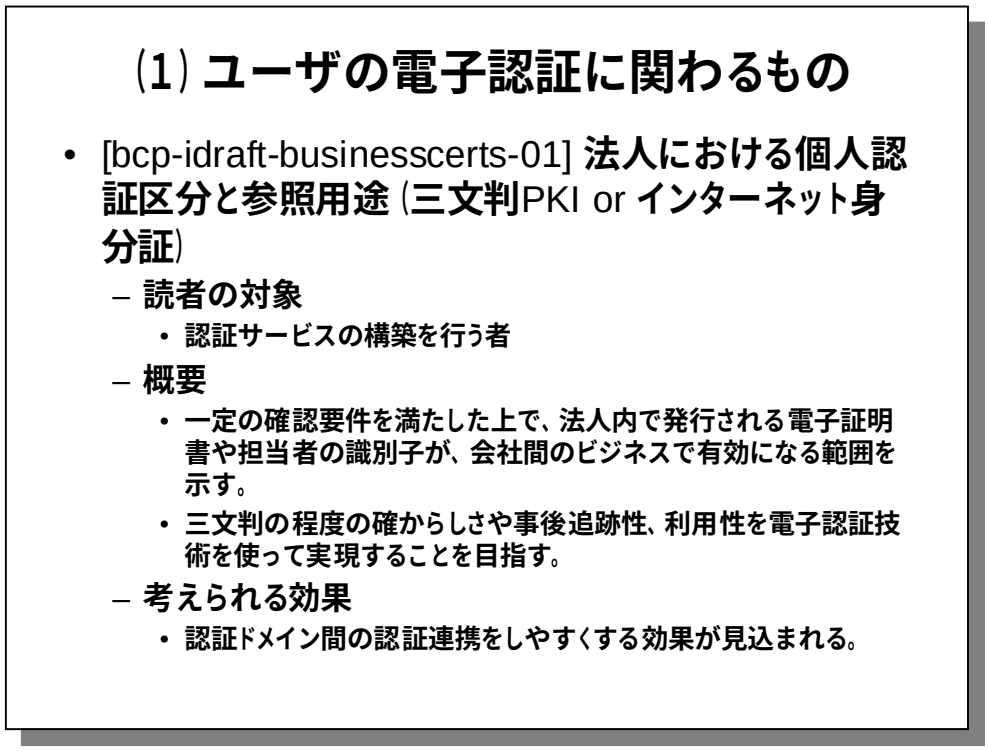

図 2-4　ドキュメント例（1）

「(1) ユーザの電子認証に関わるもの」はインターネットにおいて、ユーザ側に発行された電子証明書の相互運用を図る提案である。例えば社員の証明書を使って、関係他社との取引の中で、簡単な受発注のための担当者印のような位置づけで使えるような電子証明書を提案したものである。これはエントラスト社の故鈴木優一氏が提唱していた「三文判 PKI」の概念に近いものを実現するために考案したものである。

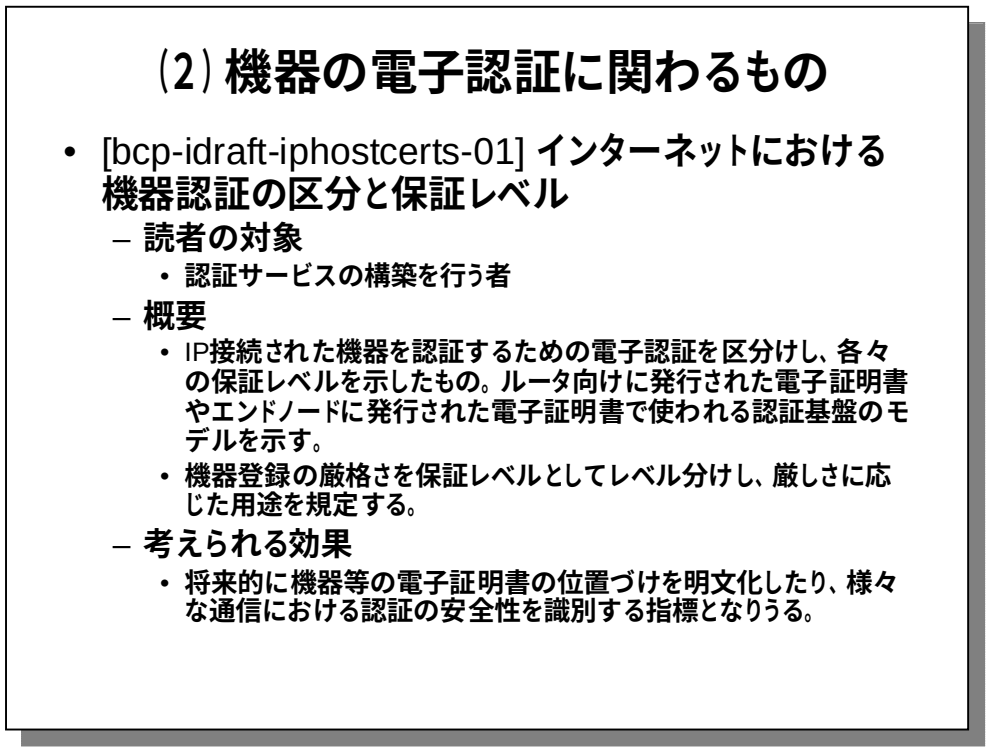

図 2-5 ドキュメント例（2）

「（２）機器の電子認証に関わるもの」は将来的に構築される可能性がある、公共の VPN（Virtual Private Network）またはトンネリングのルータの認証の為、IP アドレスにひもづく電子証明書を提案したものである。この他にルータが検証するリソース証明書の、保証レベルを規定するのにも役立つと考えられる。

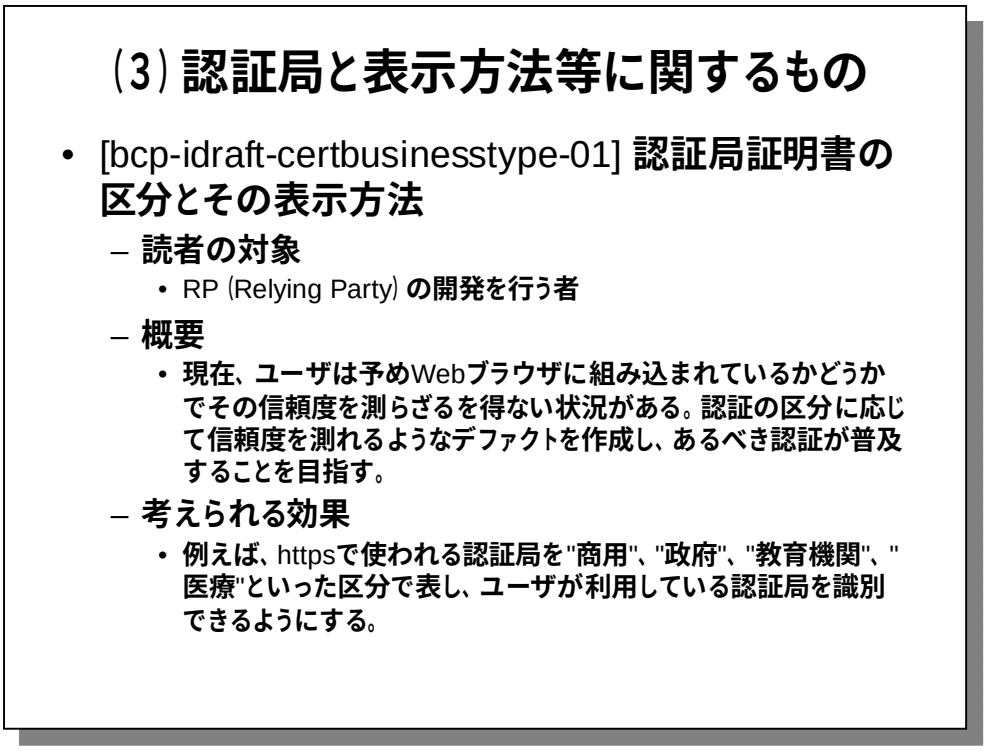

図 2-6　ドキュメント例（3）

「（3）認証局と表示方法等に関するもの」は、証明書検証を行う Web ブラウザなどが、検証を行った証明書の種別に応じて、ユーザにわかりやすく表示を切り替えるアイディアである。例えば政府認証基盤の証明書や、大学法人の証明書（UPKI の電子証明書）、または民間の電子証明書でも帝国データバンクのような企業情報が確認されている電子証明書など、いくつかの区分が考えられる。これらはユーザにとって、高額な電子証明書であるかどうか、という判断基準ではなくアクセスしている先が、どのような存在であるのかをわかりやすくすることを意図したものである。あくまでアイディアであるが、複数の Web ブラウザが本ノウハウに則り、同一の表示を行うと、ユーザの利便性は飛躍的によくなると考えられる。

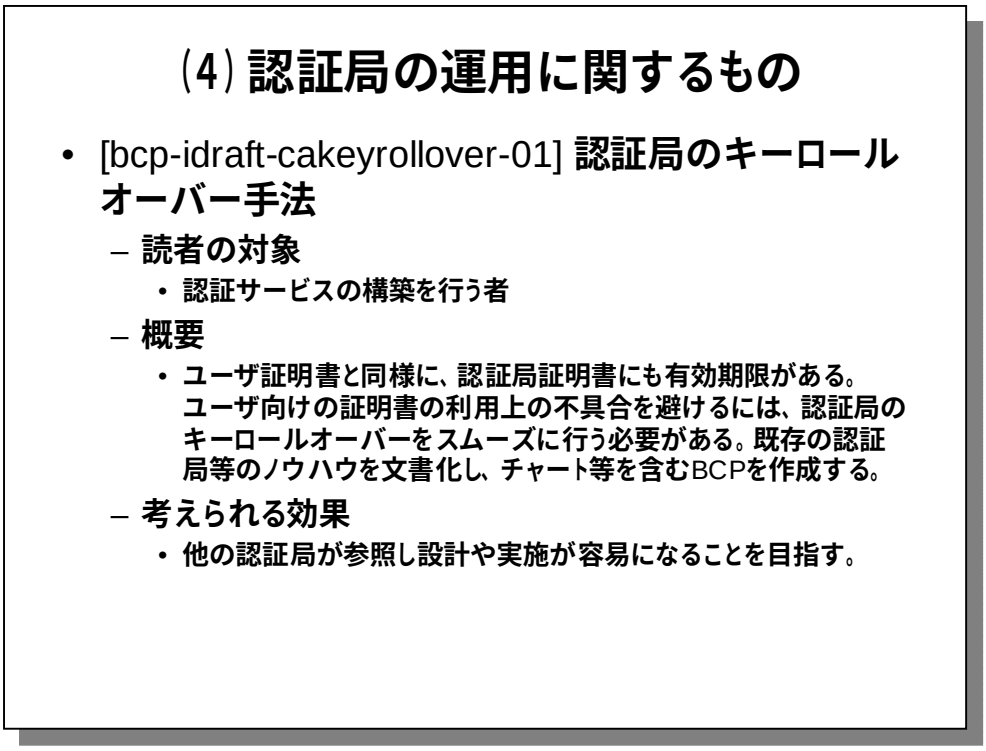

図 2-7　ドキュメント例（4）

認証局の運用を行っていると、認証局証明書の更新のタイミングに合わせてキーロールオーバーを行う必要がある。認証局証明書と、認証局が発行した証明書には有効期限があり、常に発行した証明書の有効期限が、発行元の有効期限に含まれるような発行を行うには、認証局がタイミングよくキーロールオーバーを行っていく必要がある。

これは、後に「認証局における鍵更新のタイムチャート」というドキュメントにまとめられることになる。

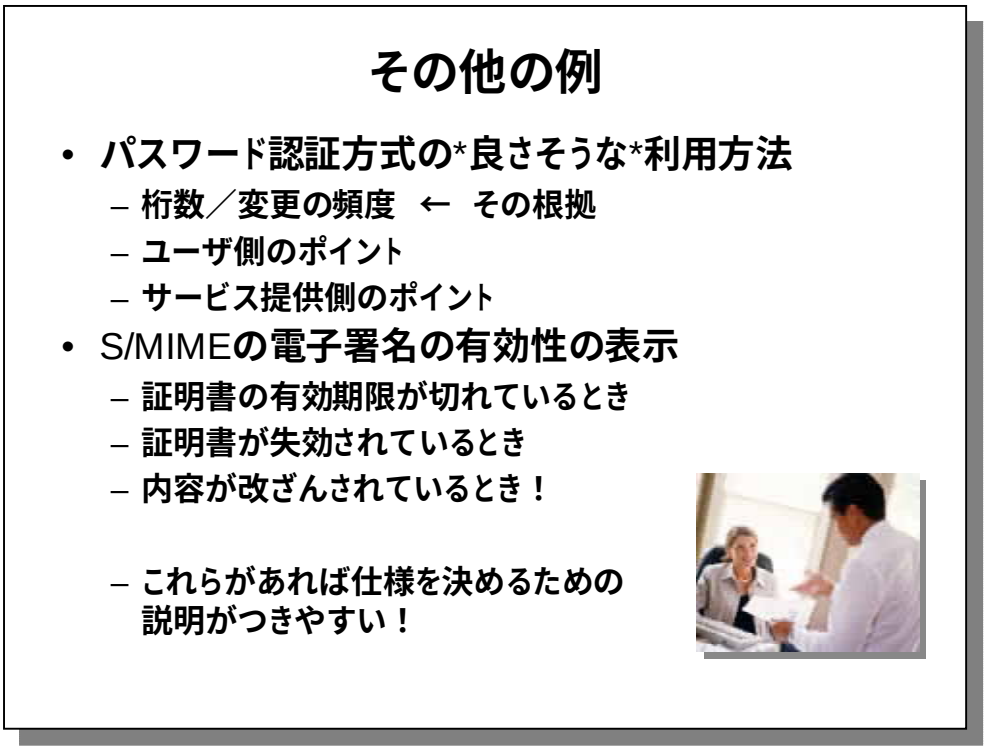

図 2-8　その他のドキュメント例

「パスワード認証方式の良さそうな利用方法」は、パスワード認証方式を適切に利用するためのノウハウである。パスワードはユーザにとって身近で仕組みを理解しやすい認証方式である。しかし推測が簡単なパスワードをユーザがつけてしまうと簡単に破られてしまう。これを防ぐには定期的にユーザにパスワードを変更させたり、一定以上に複雑なパスワードしかつけられないようにしたりする方法があるが、このことで逆にユーザがモニター画面の横に付箋でパスワードを記載してしまうなどの漏洩のリスクが発生しうる。パスワード認証方式は、適切な運用という意味では難しい認証方式である。

IC カードのように、セキュリティを目的としたシステムには、パスワードポリシーと呼ばれる仕組みがある。パスワードをユーザが変更できるかどうかや、つけるパスワードにどのような種類の文字な何文字以上入っている必要があるかの「パスワードの方針」を予め IC カードに組み込んでおき、その方針に反するパスワードの運用方法ができないようにする。このような仕組みによって、認証システム全体の安全性を確保する。

認証システムを設計するものが、このパスワードポリシーの考え方を理解していれば、新たにシステムを構築するときに安全性が著しく低いパスワード認証を行ってしまう恐れを減らすことができる。他にもシングルサインオンシステムを構築する際に、システム間の認証のレベルを合わせることにも役立つと考えられる。

「S/MIME の電子署名の有効性の表示」は、主にメールソフトの表示に関するアイディアである。電子署名付きの電子メールを受け取ったとき、その電子署名の有効性や電

子署名に使われた電子証明書の有効性の表示が、メールソフトによって行われる。しかし電子メールソフトの中には、特定のエラーメッセージをとても重大なインシデントとして提示するものがある。例えば、電子証明書の有効期限が切れていた場合に、単に「有効期限が切れている」と表示して、かつメール本文を表示するのか、「有効期限が切れているので、この電子メールは改ざんの恐れがある」と表示して、メール本文を表示しないのか、といった違いがある。同一のシステムの挙動に対して、メールソフト毎の違いを減らすことは、ユーザの混乱を減らすことに役立つと考えられる。

ユーザに対する情報提示の方法は、メールソフトベンダーの競争や各々の実装方法に任されるべきものである一方、専門家もしくは一般ユーザの観点では、あまりにシステムの間で違いがあるようでは利便性を損ねる要因にしかならない。本フォーラムで様々な観点の意見を集約し、好ましい表示の仕方をまとめることで、ベンダー側の開発の負担も抑えられる可能性がある。

2.6.1. 電子認証プラクティスフォーラム BoF

オフライン活動の一環として行った「電子認証プラクティスフォーラム BoF」について述べる。本フォーラムの BoF の実施にあたっては、議事進行の上で、議論の種類を分別したり、目的の周知を図ったり、また参加意識の向上を図るなどした。以下、BoF の議事メモを掲載する。

2007 年 11 月 21 日(水)

第 1 回電子認証プラクティスフォーラム BoF 議事メモ

JPNIC
木村泰司

▼1.概要

第 1 回電子認証プラクティスフォーラムの BoF は以下の要領で行われた。
本 BoF は経済産業省から JPNIC が受託している調査研究活動の一環である。

日時：2007 年 11 月 19 日(月) 17:30-19:40
場所：秋葉原コンベンションホール 5 階 5A
参加人数：29 名

▼2.著作権表示

Reserved.

▼3.アジェンダ

a.オープニング
b.電子認証プラクティスフォーラムの紹介(JPNIC 木村 泰司)
c.電子認証技術のノウハウに関するディスカッション
c.1.ディスカッションに関する説明と例
(JPNIC 木村 泰司)
c.2.認証局証明書の更新が与えるユーザアプリケーションへの影響の調査
(富士ゼロックス 横田 智文さん)
c.3.PKI におけるマルチドメイン問題
(セコム IS 研究所 島岡 政基さん)
d.電子認証ブレインストーム、19:00
4.1.ブレインストーミングに関する説明 (JPNIC 木村 泰司)
d.クロージング

▼4.ディスカッションの内容

a.オープニング

オープニングでは本 BoF における諸注意やスケジュールなどのアナウンスが行われた。

b.電子認証プラクティスフォーラムの紹介(JPNIC 木村 泰司)

本フォーラムの背景や電子認証技術の普及の課題などの整理のあと、フォーラムの活動目的や扱うトピックの紹介が行われた。

会場からは以下のコメントがあった。

○ドキュメントの有効性を挙げる意味で、知名度を向上させ、ある程度の参加者を確保する必要があると考えられる。
○他の組織にも同様の悩みを持つ方々がいる。アナウンスを広くすることが望ましい。
○ドキュメント化プロセスのルールづくりが重要である。挙手とその割合など。発表者の木村より、プロセス自体をドキュメント化し、文章を通じた明確化を行いたいと回答があった。

○SIG(Special Interest Group)を作らずに個別ドラフトで
BCP 化できるプロセスが欲しい。

c.電子認証技術のノウハウに関するディスカッション

本セッションでは、本フォーラムで扱うと考えられるアイディアについてのディスカッションが行われた。

c.1.ディスカッションに関する説明と例（JPNIC 木村 泰司）

はじめにアイディア例の紹介が行われた。その例を以下に示す。[]内は仮につけられた"ドキュメントファイル名"を示している。このファイル名は現在提案中の「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)に則ってつけられている。

法人における個人認証区分と参照用途
（三文判 PKI or インターネット身分証）
[bcp-idraft-businesscerts-01]

インターネットにおける機器認証の区分と保証レベル
[bcp-idraft-iphostcerts-01]

認証局証明書の区分とその表示方法
[bcp-idraft-certbusinesstype-01]

認証局のキーロールオーバー手法
[bcp-idraft-cakeyrollover-01]

パスワード認証方式の良さそうな利用方法
[ファイル名なし]

S/MIME の電子署名の有効性の表示
[ファイル名なし]

c.2.認証局証明書の更新が与えるユーザアプリケーションへの
影響の調査（富士ゼロックス 横田 智文さん）

資料：「認証局証明書の更新が与えるユーザおよびアプリケーションへの影響」(*2)に沿ってプレゼンテーションが行われた。RFC4210(*3)、RFC3280(*4)で策定されたキーロールオーバーに沿って認証局の鍵更新を行う場合の、

何が行われるか/何が起こるのかの理解と対策を検討するためのノウハウである。

会場では以下のディスカッションが行われた。

○認証局証明書の有効期限が、上位認証局の認証局証明書の有効期限を超えることが現実にある点が確認された。
○中間証明書の認証局証明書の更新についても、リンク証明書を使う手法があるかどうかに関する情報交換
本件について継続して ML で情報交換が行われることとなった。
○技術提案と考えられるネタは、本フォーラムで扱う対象となるか、という質問があった。これに対し、電子認証技術の適切な利用に役立つ内容であれば、本フォーラムで扱う必要があるというコメントが会場からあった。

最後に発表者によるドキュメントを行う方向性の確認が行われた。

c.3.PKI におけるマルチドメイン問題（セコム IS 研究所 島岡 政基さん)

資料：「PKI におけるマルチドメイン問題」(*5)に沿ってプレゼンテーションが行われた。認証局が複数運用されており、相互接続されうる状況について用語と概念を整理したものである。英語では"Memorandum for multi-domain Public Key Infrastructure Interoperability"(*6)としてドキュメント化されている。

会場では以下のコメントが出された。

○概念整理と新たな技術の提案などが含まれているので、少なくともドキュメントは分けられるべきではないか。

d.電子認証ブレインストーム

本セッションでは、電子認証技術の課題点についてオープンマイクロホンの形式で議論が行われた。

d.1.ブレインストーミングに関する説明 (JPNIC 木村 泰司)

ディスカッションに先立ち、各発言の位置づけに関する注意事項が伝えられた。主な事項を以下に挙げる。

○組織を代表するものではない

－なんら義務は発生しない
○宣伝やバッシングはなし
○参考情報である
○実際の経験や考察に基づいていることが望ましい

会場で挙げられた課題点を以下に挙げる。

○JDK 1.5 を使ったパス検証において https で証明書検証をするだけで Warning が出る。

会場からのコメント：
⇒ 中間証明書の取得の問題で、中間証明書を渡す形ならば問題ない。ただし 1.4 ではうまく動作することが確認されていない。

○PKI の IC カードは挙動が遅く入退室システムには遅すぎる。
－普通は Felica ベースのシステムだが、安全性を考えると PKI の IC カードを使うことを考えたい。しかし 5 分も待たされるといわれている。

会場からのコメント：
⇒ IC カードは blackbox のように考えられているケースが多く、ソリューションの情報が普及していない。
⇒ JNSA PKI 相互運用技術 WG の IC カードワークショップにて理解を図りたい。

○暗号アルゴリズム移行問題。暗号の専門家は 2010 年問題と呼ばれる暗号アルゴリズムの転換期に注目している。しかしよりアプリケーションよりの観点での議論も必要とされている。より上のレイヤーでの観点でのノウハウが文書化されることが望ましい。

会場からのコメント：
・鍵長を長いものにしないと、携帯電話など日本だけが遅れてしまう恐れがある。
・証明書の有効期限内で(鍵が)破られることは考えにくい。
一概に 1024bit でダメというのは不適切ではないか。
・社会的にどこまで問題があるかを整理する必要がある。
・技術上どこまでやる必要があるか
・政策としてどこまでやる必要があるか

○今後組み込み型の技術者が、PKI の議論に詳しくなる必要があると

思われる。

続いて、本フォーラムで解決すべき課題や電子認証技術においてあるべきこと等に関するアイディアが会場から出された。

○リポジトリ的活動が必要である。電子認証技術はトータルで議論されることが多いが、担当（技術やビジネスの違い）によって、それはきつい。部品に分けて議論が行われることが望ましい。

○フォーラムの活動として技術の標準化をしないことの必然性がわからない。

○ドキュメント化プロセスのルールづくりが重要だと思われる。挙手によりパーセンテージをみるなど。

○フォーラムプロセスで、SIG にとらわれずに個別ドラフトでも、よいものであれば文書化にもっていけるようなプロセスが欲しい。人数がまだ少なく、SIG をつくったり、SIG のコンセンサスを取るのに労力がいるため。逆にエキスパートチームの負荷が増えることではある。

○本フォーラムの役割として、場の提供ができることが望ましい。
本フォーラムは、PKI エンジニア、アプリケーションユーザなどが、質疑応答を通じて情報交換できるような場になりうる。
文書化はハードルが高いと思う。が、場の提供で情報交換できることにも意味がある。BCP にとらわれずに意見交換の場が使えるとよい。

e.クロージング

クロージングでは発表者および参加者に謝意が示されると共に、BoF の参加人数が発表された。今回の参加者は 29 名であった。

▼Appendix. I

*1 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
bcp-draft-bcpformat-02.txt

*2 認証局証明書の更新が与えるユーザおよびアプリケーションへの影響
http://eapf.nic.ad.jp/bcp-draft-bcpprocess-03.txt

*3 Internet X.509 Public Key Infrastructure

Certificate Management Protocol (CMP)
RFC4210

*4 Internet X.509 Public Key Infrastructure
Certificate and Certificate Revocation List (CRL) Profile
RFC3280

*5 PKI におけるマルチドメイン問題（旧題）
http://eapf.nic.ad.jp/bcp-draft-appropriate-policymapping-01.txt

*6 Memorandum for multi-domain Public Key Infrastructure
Interoperability
draft-shimaoka-multidomain-pki-10

なお、本フォーラムのアンケート結果、およびレビューチームのレビュー結果から本フォーラムの活動が好評であったことから、本調査研究の終了後にも継続することを積極的に検討中である。

2.7. オフライン活動に関するフィードバック

本節では、電子認証プラクティスフォーラム BoF の会場で行ったアンケートの結果について述べる。

アンケートは、本フォーラムのような国内であまり例を見ないフォーラムのオンライン活動に関して、告知方法や参加の動機、参加者における興味の度合い、そして本フォーラムの必要性等について調べるために行った。また自由記述欄にて、電子認証技術に対する課題点・問題点を集めることも行った。

アンケートの結果から、BoF は意義深く、フォーラムへの参加を前向きに検討したいという参加者が多いことがわかった。また参加者の多くはフォーラムへの参加の動機について、電子認証技術に興味があることを最も多く挙げており、電子認証技術に興味がある人が、本フォーラムを意義深いと感じていたと考えられる。

以下に、アンケートの集計結果を示す。

電子認証プラクティスフォーラムBoF　アンケート集計

1 BoFをどのようにして知りましたか。

a	. メーリングリストのアナウンスを見て (ML名:　　)	7	31.8%
b	. JPNICウェブサイトのアナウンスを見て	1	4.5%
c	. 電子認証プラクティスフォーラムのウェブサイトを見て	2	9.1%
d	. その他 (　　)	12	54.5%
e	無回答	0	0.0%
		計22	

2 BoFに参加した主な理由は何ですか。(複数回答可)

a	. 電子認証プラクティスフォーラムの活動に興味があるか	9	23.7%
b	. アジェンダの中に興味をひくものがあったから	0	0.0%
c	. 電子認証技術に興味があるから	14	36.8%
d	. スピーカーに興味があったから	1	2.6%
e	. 電子認証技術に関する業務のため	7	18.4%
f	. 無料だから	4	10.5%
g	. その他 (　　)	1	2.6%
h	無回答	0	0.0%
		計38	

3 BoFに参加して、本フォーラムへの参加に興味を持たれましたか。

a	. ぜひ参加したい	3	13.6%
b	. 今後、前向きに検討したい	14	63.6%
c	. 参加には検討を要する (検討が要される事項:　　)	3	13.6%
d	. その他 (　　)	0	0.0%
e	無回答	2	9.1%
		計22	

4 本フォーラムの必要性についてどう思われますか。

a	. 活動は意義深く必要である	17	77.3%
b	. 活動の意義は薄く不要である	0	0.0%
c	. その他 (　　)	3	13.6%
d	無回答	2	9.1%
		計22	

アンケートの結果から、電子認証技術に興味のあるもしくは業務を担当している方が多く参加し、参加者の半分以上が本フォーラムの活動が必要であるという認識を持ったことがわかる。

なお、後述するレビューチームで、BoF の参加者数は 30 名ほどが丁度良いという意見が挙がっていた。これはあまり大きくなると発言しにくくなってしまうのではないか、という懸念があり、逆にあまりに少ないと、専門家の会議になってしまい一般ユーザの観点が抜けてしまうという懸念に基づいている。

2.8. オンライン活動

本フォーラムにおけるオンライン活動は、参加者の目的意識を保つ場である。ここでいうオンライン活動とは Web ページとメーリングリストである。本フォーラムのオンライン活動は 2007 年 10 月～2008 年 3 月にかけて行われた。Web ページは 2007 年 10 月に開設され、メーリングリストは 2007 年 11 月に開設された。その結果、このメーリングリストに 5 つのドキュメントの提案が投げられた。メーリングリストでの議論は活発とはいえなかったが、レビュー結果から BoF との連携が課題であることがわかってきた。

メーリングリストやドキュメントの投稿の時期が遅く、活動期間が短くなってしまったことがあり、メーリングリストがあまり活発に見えてこなかった。BoF との連携を含めて検討していきたい。

2.9. オンライン活動の考え方

会議体のような活動を行うとき、漫然と Web ページとメーリングリストが設置されることがある。Web ページの目的が漫然とした「情報公開」になってしまうと、主催者側に積極的に公開するコンテンツがない限り、Web ページの意義が薄れやすい。またメーリングリストは単なる「情報交換」や「議論」、または会議後の「継続議論」のための場であると、こちらも同様に意義が薄れやすくなってしまう。どちらも「活発な情報更新」や「活発なメールのやり取り」自体が目的ではないが、参加者が「どのようなときに閲覧すべき Web であるのか」「どのようなときに注視し、必要があれば議論に参加すべきメーリングリストなのか」がわかることが肝要だと思われる。

本フォーラムにおいては、各々に欠かせない役割を持たせた。Web ページは、「ドキュメントのステータス確認」と「アーカイブ」、メーリングリストは、「ドキュメントステータスを管理するための告知」と「ドキュメントの議論の場」である。Web ページは、ドキュメントがどのステータスにあるのか（ステータスについては別の節で詳述する）を確認するためと、過去のドキュメントを閲覧するためにある。アナウンス文も掲載することがあるが、こちらはメールなどでアナウンスされた内容を確認するためと捉えることができ、「アーカイブ」の役割に含まれると言える。参加者は常に Web ページを閲覧する必要はなく（主催者はこれを望みがちであるが、そのようなことはないと考えるのが妥当であろう）、例えばドキュメントを提案しようとするときや、または議論になっているドキュメントを閲覧するときに閲覧すればよい。メーリングリストはドキュメントの投稿を受け付ける場であるが、基本的にそれは告知の役割に近い。例えば、一週間後にドキュメントステータスが変わるので、それまでにコメントせよという通知が流れるとする。するとそのときから一週間、メーリングリストはドキュメントステータスに関わる議論の場となる。

IETF や OPM のメーリングリストは、これに近いコントロールを持っている。IETF

では、WG ごとにチェアがおり、メーリングリストと WG のミーティングの進行を担っている。WG の主旨に合わない発言は退けられ、趣意書（チャーター）にあった議論の進行が守られる。

電子認証プラクティスフォーラムにおけるメーリングリストは、最初の段階ということもあり、一つのみ作成した。提案されたドキュメントや、類似する話題に応じて WG または SIG（Special Interest Group）を複数設け、議論の場をわけることも考えられたが、「最初はシンプルに、かつラフに」という考えで一つとした。今後は、これらのメーリングリストにおけるコントロールや、議題に応じたメーリングリストの配置を検討する必要があると思われる。

以下に、本フォーラムの Web ページを以下に示す。

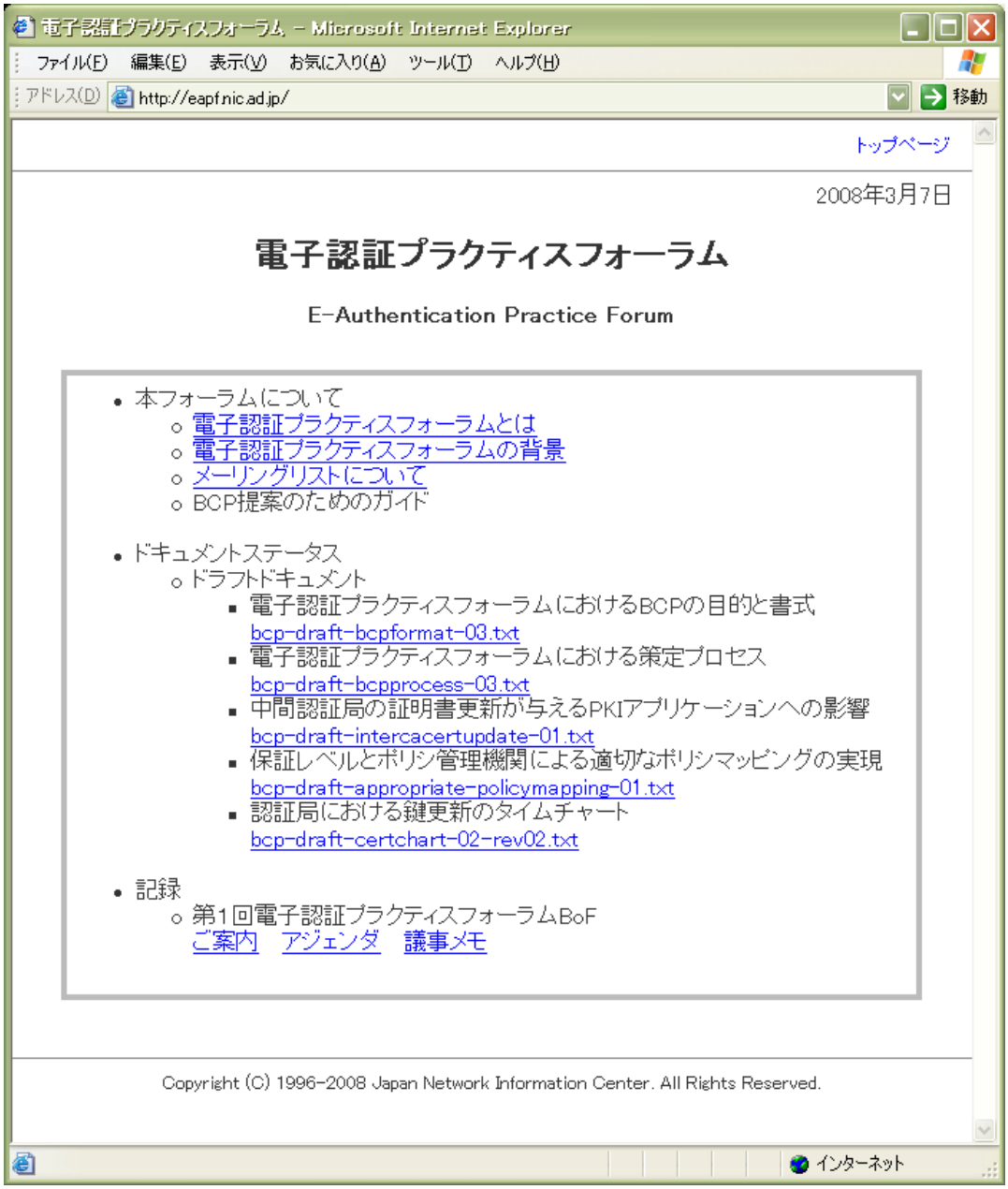

図 2-9　電子認証プラクティスフォーラム トップページ

トップページでは、主に 3 つのコンテンツを提供している。本フォーラム自体に関する情報提供、ドキュメントステータス、記録（アーカイブ）である。トップページではこれらのコンテンツを含めて、わかりやすいように一覧表示した。

本フォーラムの考え方などを明文化し残しておくために用意した Web ページの内容を示す（長文であるため内容のみを載せた）。また活動概要を示しており、例えば参加者が参加にあたって、自社の業務の一環として参加しやすくなることを意図している。

電子認証プラクティスフォーラムとは

EAPF(E-Authentication Practice Forum：電子認証プラクティスフォーラム)は電子認証技術の構築や利用に役立つ概念や知識(ノウハウ)をドキュメント化し、その共通理解と共有を図るフォーラムです。メーリングリストとオフラインミーティングを通じて活動し、技術的知識のドキュメント化を行います。

PKI の技術は、基本的な技術仕様が固まりつつあり、普及段階にあります。しかしその複雑さから、利便性・規模拡張性等の利点が生かされず、適切な普及が図りにくい状況があります。PKI の技術が使われていて安全性の向上が図られているにも関わらず、実態としては利便性が悪く、かつ安全性が向上していないシステムが存在しています。PKI の他にも電子認証技術が適切に利用されていない場面があります。

本フォーラムは、電子認証技術に関して現時点で最良だと思われる考え方(Best Current Practice)を、参加者のコンセンサスに基づいてドキュメント化し、電子認証技術を利用しているもの、または新たに構築しようとするもの等が、共通の理解を得る状況を作ることで電子認証技術が適切に普及することを目指します。

本フォーラムの活動は、経済産業省から JPNIC が受託した調査研究事業(*1)の一環として行っています。

(*1)「平成19年度電子認証フレームワークとIPアドレス認証の展開に関する調査研究に関する委託契約」

本フォーラムは以下の考え方に基づいて活動を行います。

- ラフコンセンサスを重視
- 現場の現状に基づいた知識
- 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オフラインミーティングを通じて行います。

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ません。活動の成果物は BCP と呼ばれるドキュメントです。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ありません。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ありません。

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ます。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ます。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ます。

他のページでも同様であるが、上部に Web サイトのどのページを閲覧しているかを示す表示を行った。また全体的にシンプルなデザインとした。

背景についても「電子認証プラクティスフォーラムとは」のページと同様の配置を行った。本フォーラムの参加者や参加を検討するものが、本フォーラムの位置づけを理解しやすくするために用意した。

電子認証プラクティスフォーラムの背景

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す。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す。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くなります。

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ります。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ります。

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ました。その課題は実装面と実践面の両方にあります。

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困難です。特に相互運用性を確保することは大きな課題です。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ります。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します。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えます。

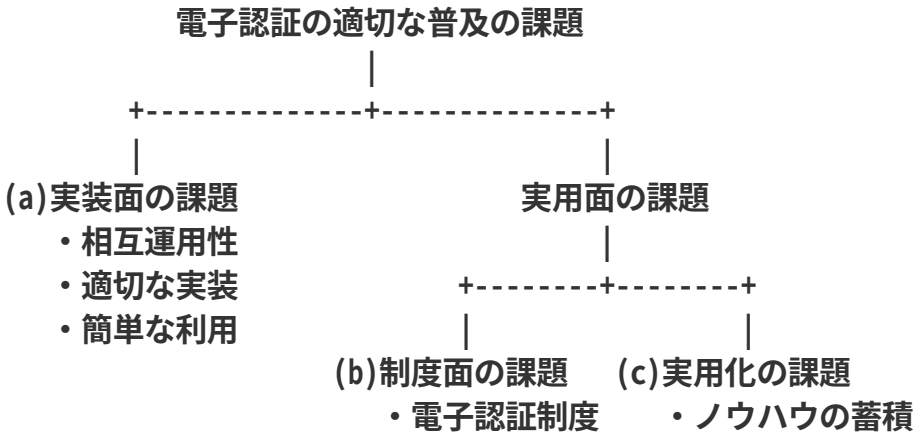

図 1 電子認証の適切な普及の課題の分類

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す。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ます。(a) に対する取り組みには JNSA の ChallengePKI および PKI 相互運用性 WG の活動が挙げられます。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ます。(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ます。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ます。

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ました。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ましたが、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ました。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ました。

本フォーラムでは、メーリングリストに関する情報を「メーリングリストについて」という最初に見えるページと、「メーリングリスト参加同意事項」の二階層目とに分けた。これは、同意事項は確認済である閲覧者が、手続きに必要な情報のみを閲覧する、すなわち最初のページのみを閲覧するだけでよい場合と、参加同意事項を確認する場合のどちらの場合においても、Web ブラウザで進んだり戻ったりをしなくてよいことを考えた。

本フォーラムのアナウンスは、JPNIC のアナウンス用のページを利用した。

2.10. オンライン活動としてのメーリングリスト

本フォーラムにおけるメーリングリストの設置にあたり、一つのメーリングリストであっても検討を要する事項が数多く存在した。例えば、参加者による誹謗中傷行為は、どのように防ぎ、そしてそれによる被害の責任の所在はどこにあるのか、といったことである。メーリングリストに誹謗中傷となるメールが投稿されたとき、更にそれが他の Web ページに掲載されたとき、メーリングリスト主催者はそれに対する責任を負わなければならないだろうか。これらの疑問に対する解は、容易に導き出すことが難しいため、通例や問題対処の方法があるかといった観点が必要になる。

本フォーラムでは、これらの問題を解決しやすくするために、メーリングリストに加入する前に同意する必要がある事項を明示することとした。これにより、例えばメーリングリストにおいて誹謗中傷などの迷惑行為があったときに、強制的に脱退させるなどの措置を行うことが正当化されるはずである。幸いなことにこういった事態は起こっていないが、IETF では逆に議論が活発すぎて参加者が議論を追いきれない、といった弊害があり、チェアが対処を行っているようである。本フォーラムでも、前項の「メーリングリストにおけるコントロール」とあわせて、体制を考えていきたい。以下に、本フォーラムのメーリングリスト参加にあたっての同意事項を示す。

メーリングリスト参加同意事項

- 第１条　（目的）

  本規約は、電子認証プラクティスフォーラムメーリングリスト（以下「EAPF メーリングリスト」という）の利用者に対し、その利用目的に沿った利用の推進を図るために、利用に当たって遵守すべき事項を示すことを目的とする。

- 第２条　（登録資格）

  EAPF メーリングリストへの登録は、希望者のみとする。また、EAPF メーリングリストへ登録した時点で本規約に同意したものとする。

- 第３条　（登録資格の取消）

  EAPF メーリングリストの運営にあたる JPNIC は、本規約を遵守しない利用者に対して、注意、警告を行った上で登録資格の取消を行うことができる。

- 第４条　（利用範囲）

EAPF メーリングリストを利用できる者は、EAPF メーリングリストの登録者に限定する。投稿の内容は広く一般に公開される。

- 第５条　（運営への協力等）

  EAPF メーリングリストの登録者は、EAPF メーリングリストの利用に当たり、本規約を遵守するとともに、配信先アドレスの変更があり次第通知する、配信メールがフィルタリングによる排除を受けないように設定する、などにより EAPF メーリングリストの円滑な運営に協力することとする。

- 第６条　（運営の中断）

  JPNIC は、運営の中断等に関して事前に通知する努力を行うが、予告なく運営の中断を行うことができる。

- 第７条　（禁止事項）

  EAPF メーリングリストの利用に当たっては、以下の行為を禁止する。

  - 公序良俗、法令に違反する行為。
  - 登録者や第三者の著作権を侵害する行為。
  - 登録者や第三者の財産、プライバシーを侵害する行為。
  - 登録者や第三者に不利益を与える行為。
  - 登録者や第三者を誹謗中傷する行為。
  - 宣伝および商行為とみなされる行為。

- 第８条　（禁止事項への対応措置）

  禁止事項に該当すると判断される場合、JPNIC は該当者に対して一時的に投稿の差し止め、メーリングリストからの登録抹消といった措置を行えることとする。同様に差別、中傷、その他公序良俗に反すると判断する場合は、該当する投稿を予告なく削除するなどの措置を行えることとする。

- 第９条　（免責事項）

  利用者または第三者に発生した損害について JPNIC は責任を負わないものとする。

- 第１０条　（著作権）

  投稿された内容の著作権は、JPNIC が保持するものとする。投稿するメールに、他の文献や文書等からの引用や改変、要約等を含める場合は、著作権法上認められている原著作者の諸権利を尊重しなければならない。

- 第１１条　（個人情報保護方針）

  EAPF メーリングリストを運営するために必要な個人情報は JPNIC 個人情報保護方針 に沿って利用される。

- 第１２条　（投稿メールの仕様）

  投稿はテキストフォーマットのメールに限定する。ファイルの添付されたメール、HTML フォーマットのメール、リッチテキストフォーマットのメール、開封通知オプションの設定されたメール等の投稿は禁止する。

- 第１３条　（規約改定）

  JPNIC は本規約の改定の必要が生じた場合、登録者に通知の上、規約を改定することができる。

JPNIC の個人情報保護方針が存在したため、本フォーラムがこれに沿うと定めることができたが、フォーラムを独立した会議体によって主催した場合、これらの策定と実施可能な体制作りが必要になる。

2.10.1. メーリングリストを通じたドキュメント提案

メーリングリストは 2007 年 11 月に開設された。2008 年 3 月までの運用の結果、本フォーラム自体の活動を提案するドキュメント 2 つと、ノウハウのドキュメント 3 つが提案された。

ドキュメントに関する議論は、BoF が行われた後とノウハウのドキュメントが提案される際に行われていた。レビューチームのコメントでもあったが、メーリングリストと BoF とが連携する形が見えていることが必要であると考えられる。

2.11. ノウハウのドキュメント策定活動

本フォーラムにおける「ドキュメント策定」は、最も主要な柱である。本フォーラムでは、電子認証に関わるノウハウを「ドキュメント提案」し、メーリングリスト参加者とレビューチームのチェックを受けた後に、BCP（Best Current Practice）と呼ばれるドキュメントになる。この一連の活動がドキュメント策定である。

2007 年度の活動の結果、2 つが最終レビューの対象となる「レビュードキュメント」の段階となり、4 つが本フォーラムにおける議論の対象とする「提案ドキュメント」の段階となった。

最初に議論されたドキュメントは、本フォーラムにおけるドキュメントの書式に関するドキュメントと、ドキュメント策定プロセスを提案したものである。これらは本フォーラムにおける活動自体を規定するものであるが、これらも議論を通じてブラッシュアップし、必要に応じて更新していけるようなサイクルを可能にするために、あえてドキュメント化プロセスを経ることとした。以下に、本フォーラムの策定プロセスを示す。

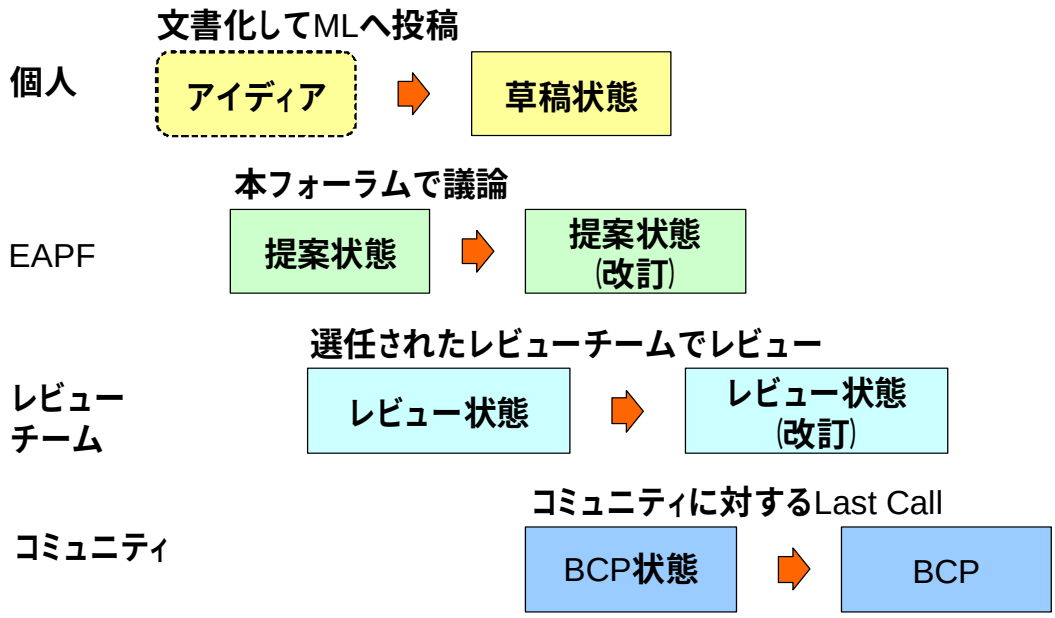

図 2-10　ドキュメント化プロセス

2.12. オンライン活動およびオフライン活動に関するフィードバック

本フォーラムとオフライン活動である BoF は実験的な活動である。日本国内において、電子認証技術のノウハウに関して扱う会議を行うという観点と、BoF というドキュメント策定の場を作る意味での会議という点で、BoF はまさに「実験的な」活動であるった。

そこで本調査研究の一環として、「電子認証プラクティスフォーラム　レビュー専門家チーム」を作成し、専門的な観点で、オフライン活動と後述するオフライン活動のレビューを行った。なお、レビュー専門家チームは本フォーラムにおけるレビューチームを兼ねてている。レビューチームとはおり、本フォーラムの中で提案されたドキュメントのレビューを行うグループである。ドキュメントレビューについては詳細を次の項で述べる。

レビュー専門家チームによるレビュー結果を以下に示す。

レビュー専門家チーム　レビュー結果

▼A. ドキュメントレビュー

ドキュメントレビューの結果、ドキュメント数は以下となった。

・レビュードキュメント　1

・提案ドキュメント　4（うち 1 つは条件付き）

▼B. フォーラム活動のレビュー

フォーラム活動を振り返って評価と課題点をまとめた。

主な評価：

・活動趣意や BoF の評価がとても高い。

・時間的に厳しかったため、ML が不活発であった。

主な課題点：

・BoF と連携して ML を活発化を図るべき。

・BoF を定期的に開くべき。

・フォーラムの認知度向上を図るべき。

上記のレビュー結果から、専門家チームの BoF に対する評価はとても高かったことがわかかるった。BoF の評価のポイントは、大きく分けて三つ 3 つあった。一つ目は BoF の対象者で、電子認証技術に関するノウハウをドキュメント化する、という対象者が興味を持ちやすい主旨で参加を募ることができたという点である。二つ 2 つ目はモデレーション（進行）である。この BoF のように新たな形式の会議では、参加者が発言を行いにくく、会議の目的を達成しにくいと考えられる。そこで議論の目的を伝えながら行うなど進行を工夫する必要がある。三つ 3 つ目は主催組織の位置づけである。電子認証技術に関して専門的な活動を行っている組織は少なくない。その中で、本フォーラムが意図しているベンダーに対する中立性のイメージを持たれる組織において主催されることがポイントとなる。

一つ目（オフライン活動の対象者）と二つ 2 つ目のポイント（モデレーション）は、IETF と RIR（Regional Internet Registry）の IP アドレスポリシーに関する議論のアジェンダ作りと進行方法を参考に作成した。これらは調査研究の一環として参加した国際会議において、電子認証技術の動向だけでなく議事進行や会場の配置などについて調査した成果である。三つ 3 つ目（主催組織）については、特に意識したものではないが、歴史的に JPNIC がインターネットに関する技術的・学術的な活動を行うイメージを持たれていることが伺われた。主催組織については、電子認証局会議のような会議体を主催としたり、IETF のように会議体自体が主催したりする形式も考えられる。

レビュー専門家チームのレビューの中で、特筆すべき議論もあった。日本国内における「議論」とは何かという議論、である。米国では、議論にはいくつかの形があることが認知されていることが多い。一方、日本では後述するような「議論の仕方」に関する情報は日常的には得にくい。例えば、論点の整理の為の議論（例：clarify）や、論点や論旨の正しさを確認するための議論（例：ディベート）はあまり日常的に意識されていないのではないだろうか。会議の際に論争すること自体が避けられたり、意見が発言者の人格と同一視されたりすることがある。その結果、議論の目的を失い、各発言者の言いたいことが発言されるだけの会議になっていることがある。言いたいことを出し合うことを目的とした会議はもちろんあって当然であるが、会議に設定しうる目的はこれだけではない。議論の結果なんらかの結論を出す、周知徹底が図られたことを確認する、参加者に異議がないことを確認する、といった成果を出すことも重要である。

2.13. 本フォーラムを通じて作成されたドキュメント

本節では、本フォーラムでディスカッションが行われ、作成されたドキュメントを紹介する。

はじめに 2007 年度に提案されたドキュメントの一覧を以下に示す。

- 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
  bcp-draft-bcpformat-03.txt、 JPNIC　木村泰司
- 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
  bcp-draft-bcpprocess-03.txt、 JPNIC　木村泰司
- 中間認証局の証明書更新が与える PKI アプリケーションへの影響
  bcp-draft-intercacertupdate-01.txt、 富士ゼロックス　横田智文
- 保証レベルとポリシ管理機関による適切なポリシマッピングの実現
  bcp-draft-appropriate-policymapping-01.txt、 セコム IS 研究所　島岡政基
- 認証局における鍵更新のタイムチャート
  bcp-draft-certchart-02-rev02.txt、 JPNIC　木村泰司

本フォーラムの BCP の目的と書式を提案したドキュメントを以下に示す。

BCP name: bcp-draft-bcpformat-03.txt
Date: 2008/02/06

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
木村泰司

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)の目的と書式を定めたものである。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。

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を通じて得られた知識や、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る。また特定の製品やサービスに限定されない情報に限る。

4. BCP の経緯や想定される状況

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 の書式がドキュメントによって別々になってしまい、作成や理解の妨げになる恐れがある。また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-" に続いて本フォーラムにおけるステータス、内容を示す一語、改訂番号をつなげたもの。

例：bcp-draft-bcpname-01.txt

状態については bcp-draft-bcpprocess 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。

・内容
BCP の内容を記述する。サブタイトルは内容に応じてつける。

・備考
レビューを行うものへの依頼または指示事項として、レビューをする際の観点を挙げるなど、補足事項を記述する。

・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. 備考

特になし。

7. 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
木村泰司
ca-query AT nic.ad.jp

以上。

本フォーラムにおける策定プロセスを提案したドキュメントを以下に示す。

BCP name: bcp-draft-bcpprocess-03.txt
Date: 2008/02/06

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
木村泰司

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について述べる。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 ページで公開される。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。

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、ノウハウが蓄積されない恐れがある。

5. 策定プロセス

本節では、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について述べる。全体の流れを図 1 に示す。

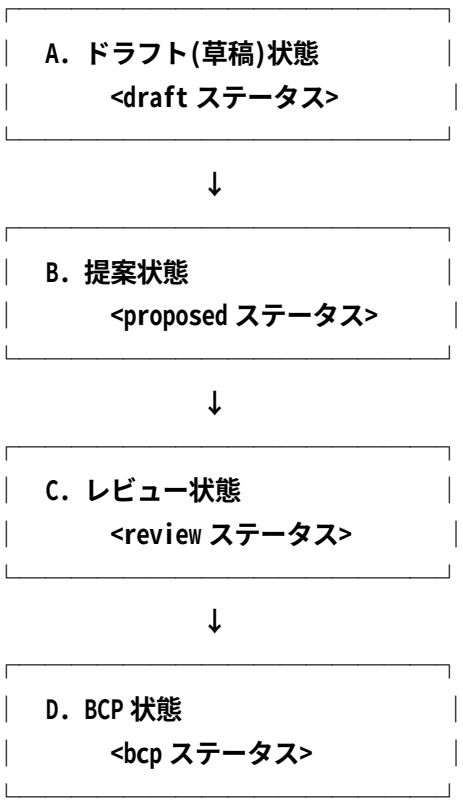

図 1 策定プロセス

5.1. ドラフト(草稿)状態

ドラフト状態の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、電子認証プラクティスフォーラムの参加者であれば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、参加者は内容確認のための議論を行う。

事前に定められた日付までに、オフラインミーティングか ML でコンセンサス

が確認された場合、次に述べる提案状態となる。

5.2. 提案状態

提案状態のドキュメントは、本フォーラムで議論と BCP 作成の対象となることについて参加者のコンセンサスが得られたドキュメントである。基本的にメーリングリストに投稿され、参加者は改善のための議論を行う。

ドキュメントには、担当レビュアが割り当てられる。担当レビュアはドキュメントに対するレビュとその対応について責任を持つ。担当レビュアは、後述するレビューチームからの立候補とする。担当レビュアの責任、すなわち対応が要される期間は、予め定められた期限に限られる。

事前に定められた日付までに、オフラインミーティングか ML でコンセンサスが確認された場合、次に述べるレビュー状態となる。

5.3. レビュー状態

レビュー状態のドキュメントは、レビューチームによってレビューが行われる状態にあるドキュメントである。レビューチームは、予め定められた期間にレビューを行い、その結果はフォーラムの ML に投稿される。

レビューチームのメンバーは、事前に本フォーラムの事務局によって選任される。

レビューチームによってレビュー結果への対応が終わったことが判断された場合、事務局により最終コメント期間の通知が行われる。最終コメント期間のコメント対応は担当レビュアと著者が行う。

5.4. BCP 状態

BCP 状態のドキュメントは、前述のプロセスを経た後、事務局によって整形が行われたドキュメントである。Web ページにて公開される。

BCP 状態のドキュメントは基本的に変更されない。修正が必要な場合は、ドキュメントを廃止して新たなドキュメントとして提案される必要がある。ただし軽微な修正についてはこの限りではない。修正事項は、事務局によって管理

されレビューチームによって実施が判断される。

5.5. 廃止状態

廃止状態のドキュメントは公開されないドキュメントである。レビューチームの判断により、廃止状態にすることがある。

また事務局の判断により、廃止状態であるか否かに関わらず、ドキュメントの公開が止められることがある。事務局の判断で非公開になった場合、ドキュメントは廃止状態にはならない。

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
木村泰司
ca-query AT nic.ad.jp

以上。

次に示すドキュメントは、暗号アルゴリズムの変更などに伴って認証局の鍵更新を行う場合の、Web ブラウザ等の対応状況を調査した結果である。

BCP name: bcp-draft-intercacertupdate-01.txt
Date: 2008/03/04

富士ゼロックス株式会社
横田智文

中間認証局の証明書更新が与える PKI アプリケーションへの影響

1. 概要

本ドキュメントは、認証局の電子証明書を更新するにあたって、ユーザへの影響を最小限に押さえつつ、スムーズに更新する条件について、調査結果をまとめたものである。
また本ドキュメントでは、特に中間認証局の証明書更新方法を策定するための情報を提供しているが、認証局証明書更新時の PKI アプリケーションの振る舞い

については、ルート認証局の証明書更新方法を検討する上でも参考になると思われる。

ユーザ(End Entity)証明書に対する前提条件を定め、その条件を満たすような更新方法と、関連するパラメーターについて概説する。

2. BCP の対象

ユーザ証明書を発行している認証局を運用している者や、認証局の運用の設計を行う者。

3. BCP の目的

認証局を持続的に運用するための、ノウハウもしくは持続的運用に向けた検討材料を提供することを目的とする。

4. BCP の経緯や想定される状況

認証局を持続的運用は、多くの認証局において必ず求められることであり、またその方法論は特定の認証局に限られたものではない。しかしこれまでに、そういったノウハウが一般に流通していることはなく、各認証局が独自に解決を図る必要があった。

本ドキュメントは、現在の実装状況を調査した結果を踏まえ、筆者の想定において、最も適すると思われる条件を定め、検討を進めた結果である。しかし本ドキュメントで述べる End Entity 証明書に対する前提条件などは、すべての認証局に共通するものではない。

5. 中間認証局の証明書更新が与える PKI アプリケーションへの影響

ここでは、想定される認証局の証明書更新方法を実施した際の PKI アプリケーションの挙動を明らかにし、実際に運用している認証局の証明書更新方法を決定するために必要な情報を提供する。

5.1. 想定した認証局の証明書更新方法

ここでは、想定した認証局の証明書更新方法について述べる。
本節の想定した認証局の証明書更新方法は、「認証局の証明書更新に関するパラメータ」の組み合わせにより決定されているため、実際に運用されている認証局に適用できない認証局の証明書更新方法が含まれている可能性がある。
認証局の証明書更新方法によっては、認証局の CP/CPS に違反しないように留意する必要がある。

認証局の証明書更新に関するパラメータとして、下記の 4 つを想定した。
a.証明書更新時期
－認証局が発行する証明書の有効期限が、認証局証明書の有効期限を越えないように事前に更新
－認証局証明書の有効期限直前に更新
(End Entity 証明書の有効期限は、認証局証明書の有効期限を越えることになる)

b.認証局名称(IsserDN)変更
－する
－しない

c.認証局私有鍵変更
－する
－しない

d.旧認証局証明書破棄
－する
－しない

パラメータの組み合わせより全 16 種類の認証局の証明書更新方法が存在するが、実際には意味のない組み合わせ(「認証局名称変更あり」の時の「認証局私有鍵変更」)が存在するため、全部で 12 種類の認証局の証明書更新方法となる。

5.2. 調査結果

ここでは、中間認証局の証明書更新方法の調査結果について述べる。
「5.3. 前提条件」で述べる前提条件を満たし、かつ調査対象の PKI アプリケーション(詳細は「5.5. 調査対象 PKI アプリケーション」を参照)の動作に影響がない、中間認証局証明書の更新方法は、1 つしか存在しなかった。

・中間認証局証明書更新方法
－証明書更新時期

→認証局が発行する証明書の有効期限が、認証局証明書の有効期限を越えない

－認証局名称(IsserDN)変更
→する

－認証局私有鍵変更
→する

－旧認証局証明書破棄
→しない

中間認証局の証明書更新方法の調査結果を表 1、表 2 にまとめる。

表 1 調査結果（認証局名称を変更しない場合）

証明書更新時期	認証局私有鍵変更	旧認証局証明書破棄	PKI アプリケーション	コメント
認証局証明書の有効期限を越えないように更新	する	する	N／A	前提条件[発行された End Entity の証明書は有効期限まで使えること]に違反(*1)
		しない	一部の PKI アプリケーションが NG	Apache、Firefox、Thunder bird が新旧の認証局の CRL を正しく解釈できない(*4)
	しない	する	N／A	認証局の私有鍵変更が行われていないため、理論上問題なしが、事実上無理(*2)
		しない	一部の PKI アプリケーションが NG	旧認証局証明書有効期間後に Opera が SSL クライアント認証で不正なパス構築(*5)
認証局証明書の有効期限を越えないように更新	する	する	N／A	前提条件[発行された End Entity の証明書は有効期限まで使えること]に違反(*1)
		しない	N／A	前提条件[発行された End Entity の証明書は有効期限

				まで使えること]に違反(*3|
直前に更新				
				認証局の私有鍵変更が行わ|
		する	N／A	れていないため、理論上問|
				題なしが、事実上無理(*2)|
	しない			
			一部の PKI	旧認証局証明書有効期限後|
		しない	アプリケー	に Opera が SSL クライアント|
			ションが NG	認証で不正なパス構築(*5)|

表 2 調査結果（認証局名称を変更する場合）

証明書更新時期	認証局私有鍵変更	旧認証局証明書破棄	PKI アプリケーション	コメント
				前提条件[発行された End
認証局証明書の有効期限を越えないように更新	する	する	N／A	Entity の証明書は有効期限まで使えること]に違反(*1
		しない	問題なし	
		する	N／A	前提条件[発行された End Entity の証明書は有効期限まで使えること]に違反(*1
直前に更新	する			
		しない	N／A	前提条件[発行された End Entity の証明書は有効期限まで使えること]に違反(*3

*1：旧認証局証明書を破棄すると、旧認証局から発行されたすべての証明書が失効と判定され、ユーザは証明書を利用することができない。
これは「5.3. 前提条件」の「発行された End Entity の証明書は有効期限まで使えること」に違反する。

*2：認証局の私有鍵変更が行われていないため、理論上問題ない。しかし旧認証局の証明書破棄が行われるまでに、すべてのユーザに新認証局の証明書

を配付する必要があり、これは事実上無理だと考えられる。
よって結果として*1 と同じ現象になり、前提条件に違反する。

*3：旧認証局証明書の有効期限を越える有効期限を持つ End Entity の証明書は、旧認証局証明書の有効期限切れと共に無効な証明書となる。
これは「5.3. 前提条件」の「発行された End Entity の証明書は有効期限まで使えること」に違反する。

*4：Apache、Firefox(Thunderbird)が新旧の認証局から発行された CRL を正しく解釈できない。

*5：移行期間中(新旧の認証局が共に有効)の動作に問題なし。ただし旧認証局証明書有効期限後に Opera が、SSL クライアント認証で有効期限切れの旧認証局証明書を使ってパス構築を行い、サーバに送信していた。

5.3. 前提条件

ここでは、中間認証局の証明書更新の前提条件について述べる。
実際に運用している認証局においては、認証局の証明書更新によって、ユーザ(End Entity)に影響が少ないことが好ましい。つまり旧(現)認証局から新認証局への移行がスムーズに行われることが望まれる。

よって End Entity 証明書の前提条件は、下記のように定義する。
・End Entity 証明書への前提条件
－発行される End Entity の証明書の有効期間に変更がないこと
(例えば End Entity の証明書は 3 年の有効期間を持つとなっている場合、認証局は常に 3 年の有効期間を持った証明書を発行すること。つまり認証局の証明書有効期限等に応じて、End Entity 証明書の有効期間を調整しないこと)

－発行された End Entity の証明書は有効期限まで使えること
(例えば End Entity の証明書は 3 年の有効期間を持つとなっている場合、認証局の証明書有効期限、もしくは認証局の証明書更新によって、3 年未満の有効期間とならないこと)

また本調査で利用した証明書には、鍵識別子(Authority Key Identifier、Subject Key Identifier)を記載するものとした。

証明書に鍵識別子が記載されていない場合の PKI アプリケーションの動作は、本調査結果と異なるため注意すること。
鍵識別子が記載されていない場合の調査結果は、本ドキュメントでは述べない。

5.4. PKI アプリケーションの確認項目

ここでは、中間認証局の証明書更新を行った後に、PKI アプリケーションの挙動について確認した項目について述べる。

・PKI アプリケーションの確認項目
－旧認証局から発行された証明書を検証できること(パス検証、失効確認)
－旧認証局から発行された CRL を検証できること
－新認証局から発行された証明書を検証できること
－新認証局から発行された CRL を検証できること
－旧認証局証明書の有効期限を越えた有効期限を持つ End Entity 証明書が発行されている場合、旧認証局の証明書有効期限後にその End Entity 証明書を検証できること

証明書検証においては、認証局証明書のパス構築と CRL を使った失効確認を行った。

5.5. 調査対象 PKI アプリケーション

ここでは、調査を行った PKI アプリケーションについて述べる。
調査する PKI 機能としては、S/MIME 署名検証、SSL サーバ認証、SSL クライアント認証の 3 つとし、調査対象の PKI アプリケーションは、これらの PKI 機能を利用する上で広く使われていると思われるアプリケーションを選定した。

・調査対象 PKI アプリケーション
－S/MIME 署名検証
Outlook Express (6.00.2600.0000) [Windows XP SP なし]
Thunderbird (2.0.0.5 [20070716])

－SSL サーバ認証
Internet Explorer (6.00.2600.0000) [Windows XP SP なし]
Firefox (2.0.0.5)
Opera (9.22)

－SSL クライアント認証
Apache (2.2.4)

5.6. 考察

前提条件を満たし、かつ調査対象の PKI アプリケーションの動作に影響がない中間認証局証明書の更新は、認証局名称の変更すれば問題ないことがわかった。しかしながらこれは PKI アプリケーションとしては別認証局という扱いになっていると考えられる。

今回の調査で正常に動作しなかった PKI アプリケーションも、今後認証局の証明書更新という事象について考慮される可能性は十分に考えられる。

6．備考

特記事項なし。

7．連絡先

（eapf 事務局：ca-query AT nic.ad.jp）

以上。

次に示すドキュメントは、PKI のポリシマッピングを複数の PKI ドメインにおいて行ったときに起こる「伝言ゲーム問題」の対策の為、保証レベルを導入し、PMA（Policy Management Authority）を設ける方法を提案したドキュメントである。

BCP name: bcp-draft-appropriate-policymapping-01.txt
Date: 2008/03/05

セコム株式会社
島岡政基

保証レベルとポリシ管理機関による適切なポリシマッピングの実現

1．概要

複数の認証局におけるポリシマッピングを行う際に起こるポリシの伝言ゲーム問題について述べ、その一つの回避策として保証レベルの導入とポリシ管理機関による運用によって適切なポリシマッピングを実現する方法を紹介する。

2．BCP の対象

認証局において、証明書ポリシ(CP)を設計するもの。

3．BCP の目的

複数のポリシマッピングによって起こる、ポリシの伝言ゲーム問題の理解を図ると共に、証明書ポリシを設計するものがその問題の対策を講じられるようにすることを目的とする。

4．BCP の経緯や想定される状況

異なるポリシを持つ 2 つの認証局が適切な信頼関係にあることを表現する手法として、横断認証におけるポリシマッピングがある[1]。しかし 3 つ以上の認証局の間でポリシマッピングを行うと適切な信頼関係を表現できなくなる可能性がある。
本ドキュメントは、ポリシマッピングを検討する際に、この問題を避けるために役立つ。

5．PKI ドメイン間のポリシマッピングと保証レベル

5.1．ポリシマッピングにおけるポリシの伝言ゲーム問題

ポリシマッピングは 2 つの異なるオブジェクト識別子を持つ証明書ポリシが実質的に同等であることを示すものだが、一般に証明書ポリシの内容は多岐にわたっており、異なる認証局同士の証明書ポリシが完全に一致することはまずないと言ってよい。このため、現実のポリシマッピングは、信頼する対象となる認証局の証明書ポリシを、何らかの評価要件にもとづいて評価することで実現している。
このような評価要件は一般に評価項目と評価基準によって構成されるべきだが、標準化されたものはなく、あくまで当該認証局間での合意に従う、というのが実情である。このため、ポリシマッピングにおける評価要件は認証局間によって様々であり、その結果、一つの認証パスの中で複数のポリシマッピングを経た場合に、意図した通りのポリシマッピングが実現できない場合がある。これをポリシマッピングにおけるポリシの伝言ゲーム問題と呼ぶ。

例えば、図 1 において認証局 X は、失効リストの更新頻度が 24 時間以内であることを条件として認証局 Y を信頼しており、一方認証局 Y は失効リストの更新頻度が

48 時間以内であることを条件に認証局 Z を信頼していたとする。この時、ポリシマッピングだけを見る限り認証局 X は認証局 Z を信頼していることになるが、それは本来認証局 X が求めていた失効リストの更新頻度は 24 時間以内という評価基準から逸脱したものになる。

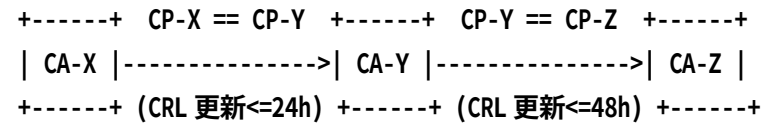

図 1 ポリシの伝言ゲーム問題

このように、ポリシマッピングにおける評価項目・評価基準が認証局毎に様々であることが、ポリシの伝言ゲーム問題につながっている。

5.2. 保証レベルによるポリシの伝言ゲーム問題の回避

ポリシの伝言ゲーム問題を最小に留めるためには、ポリシマッピングに用いる評価項目と評価基準を、横断認証する可能性のある認証局間で共有することが望ましい。しかし、これまでは認証局毎に多様であった評価項目や評価基準を広い範囲で共有することは難しかった。
これに対して米 Federal PKI では「証明書が何を保証するのか」という観点から、ポリシマッピングにおける評価項目と 4 段階の評価基準(Rudimentary, Basic, Medium, High)を定めた[2]。この米 Federal PKI のアプローチは、4 段階の評価基準になぞらえて「保証レベルの導入」と呼ばれる。

米連邦政府によると、保証とは
- ・証明書が発行された人の身元を確認するプロセスに対する信頼度
- ・証明書を使う人が、証明書を発行された当人であることに対する信頼度

の 2 点によって定義されており[3][4]、具体的には以下の評価項目について、各保証レベルでどのような要件を満たすべきか、が定義されている[2]。

- 命名要件
- 本人身元確認要件
- 鍵ペア管理要件
- 失効要件
- 認証局システム運用・監査要件

これらの評価項目は RFC 3647 の定める証明書ポリシの記載項目と関連づけられているため、RFC 3647 にもとづいた証明書ポリシを策定した認証局であれば評価することも容易である。

ポリシの伝言ゲーム問題を回避するには、このように様々な認証局に公正な評価項目と、多様な証明書ポリシに対応できる複数段階の評価基準を策定すべきであり、米 Federal PKI による保証レベルは、その一つの実現解として参考にする価値があると思われる。

5.3. 運用機関としての PMA の設置

評価項目・評価基準を定めた後には、実際に評価対象となる各認証局の証明書ポリシに対して評価を実施する機関が必要となる。このような機関としては、各認証局と利害関係を持たない中立的第三者機関として PMA(Policy Management Authority)[3]の設立が望ましい。
評価を実施した後も、各認証局の証明書ポリシは PDCA サイクルに従い必要に応じて改訂が行われる可能性があるため、PMA は改訂されたポリシに対して適切な頻度で再評価を実施する必要がある。
また、PMA 自身も同様に PDCA サイクルに従い評価項目・評価基準を見直し、必要に応じて改訂していくことが望ましい。

例えば米 Federal PKI では、連邦政府 CIO 審議会管轄の省庁間組織として Federal PKI Policy Authority(FPKI PA)が設置されている。
FPKI PA では、評価基準となる 4 段階の保証レベルを実装した CP for Federal Bridge CA(FBCA CP)[2]を策定し、これにもとづいて FBCA と横断認証する各認証局の証明書ポリシの評価を実施している。また継続的に FBCA CP の改訂も行っている。

このように、評価項目・評価基準策定後も PMA を設立・運用していくことによって、継続的にポリシの伝言ゲーム問題を回避することができると考えられる。

6. 考察

米連邦 Federal PKI のようにトップダウン型で PKI が整備されたケースでは、各認証局の合意が得られやすいと考えられる。逆に、ボトムアップ型で構築されていく場合には、どこまでの認証局に合意を求めるか(対象とする認証局の範囲)、評価項目・評価基準の策定や PMA の運用は具体的に誰が行うのか、といった課題を解決する必要があると考えられる。

7. 参考文献

7.1. この文書が準拠する文献

[1] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

7.2. この文書が参考とする文献

[2] Federal Public Key Infrastructure Policy Authority, "X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 2.7", http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf, September 2007.

[3] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[4] U.S. Office of Management and Budget, "E-Authentication Guidance for Federal Agencies", Memorandum M-04-04, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf, 16 December 2003.

8. 備考

特記事項なし。

9. 連絡先

（eapf 事務局：ca-query AT nic.ad.jp）

以上。

次のドキュメントは、ユーザに発行される証明書の有効期限を一定に保ちつつ、認証局が鍵更新を行って継続的に運用を行っていくためのチャートを示したものである。

BCP name: bcp-draft-certchart-02.txt
Date: 2008/03/06

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
木村泰司

認証局における鍵更新のタイムチャート

1. 概要

認証局の持続的な運用のための情報として、認証局における鍵更新のタイムチャートを示す。

本ドキュメントは、PKI の技術仕様を元にした考察の結果である。

2. BCP の対象

認証局の設計・構築・運用を行うもの。

3. BCP の目的

認証局を持続的に運用するために発生する、中長期的な鍵更新のタイムチャートを示し、読者の環境において、認証局の持続的運用に支障が起きないような鍵更新を事前にスケジュールできるような状況作りを目指す。

4. BCP の経緯や想定される状況

PKI における電子証明書(以下、証明書と呼ぶ)には有効期限がある。PKI アプリケーション(証明書の検証を行うプログラム)の中には、ある証明書の有効期限が、その発行元の証明書の有効期限に含まれていることを想定しているものがある。

このような PKI アプリケーションにおける、有効とみなされる有効期限を持つ証明書と、無効とみなされる有効期限を持つ証明書の違いを図 1 に示す。

■発行元の証明書の有効期限

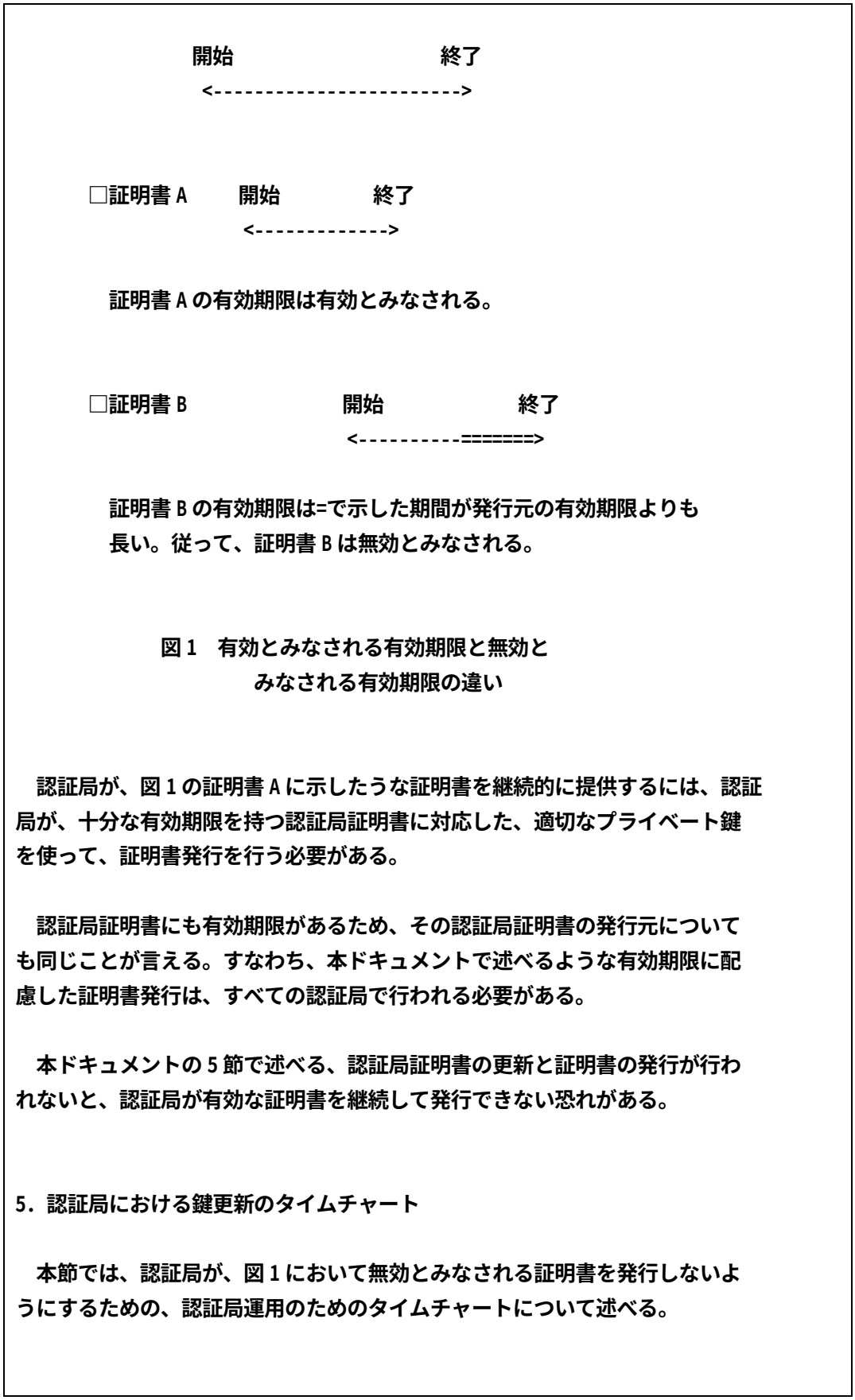

図 1　有効とみなされる有効期限と無効と
みなされる有効期限の違い

認証局が、図 1 の証明書 A に示したうな証明書を継続的に提供するには、認証局が、十分な有効期限を持つ認証局証明書に対応した、適切なプライベート鍵を使って、証明書発行を行う必要がある。

認証局証明書にも有効期限があるため、その認証局証明書の発行元についても同じことが言える。すなわち、本ドキュメントで述べるような有効期限に配慮した証明書発行は、すべての認証局で行われる必要がある。

本ドキュメントの 5 節で述べる、認証局証明書の更新と証明書の発行が行われないと、認証局が有効な証明書を継続して発行できない恐れがある。

5．認証局における鍵更新のタイムチャート

本節では、認証局が、図 1 において無効とみなされる証明書を発行しないようにするための、認証局運用のためのタイムチャートについて述べる。

5.1. タイムチャートからわかること

5.2 節で示すタイムチャートから、わかることを以下にまとめた。

A. CA 証明書の更新のタイミング

CA 証明書の更新のタイミングは、下位の認証局を含むすべての証明書の有効期間の影響を受ける。例えば、新たに、有効な期間が 1 年長い EE(エンドエンティティ)証明書が発行されるようになると、2 つ上位の CA 証明書は以前よりも 2 年以上早く証明書更新を行う必要が出てくる可能性がある。

ルート CA が、EE 証明書や下位認証局証明書の有効期間の変動の影響を受けないためには、予め 5.2 節で示すようなタイムチャートを考慮し、そのタイムチャートに変更を要するような有効期限を持つ証明書を下位認証局に発行させないよう、制限する必要がある。

B. 認証局プライベート鍵の利用可能期間

認証局証明書が鍵更新を伴って更新される場合、プライベート鍵は認証局証明書の有効期限の満了まで使われることはない。

旧認証局証明書の有効期限

開始　　終了
<----------->

発行した証明書の有効期限

開始　　終了
<----------->

旧認証局プライベート鍵の利用可能期間

開始　　終了
<----------->

⇒ 旧認証局のプライベート鍵の利用機関が終わる前に、新認証局のプライベート鍵を使い始める必要がある。

例えば、認証局証明書の有効期限が 10 年であり、発行した証明書の有効期限が 2 年であれば、開始後 8 年以内に鍵更新を行う必要がある。

なお再発行の際に鍵更新を行うことを考えると、更に事前にキーセレモニー等の準備を開始する必要がある。

5.2. 認証局証明書における鍵更新のタイムチャート

認証局における鍵更新のタイムチャートを図 2 に示す。図 2 では、ルート CA 証明書と中間 CA 証明書、EE 証明書の各々が、各々の有効期限が切れる前に新しい証明書に切り替わる様子を示している。切り替わりに要される証明書更新は、前倒しして実施することが可能であるが、ここでは最も遅いケース、すなわち証明書の有効期限が切れるまで使われるケースを示す。

図 2 のルート CA は 2007 年の始めに発行され、10 年間の有効期限を持っている。中間 CA 証明書は 2008 年の始めに発行され、5 年間の有効期限を持っている。EE 証明書は 2 年間の有効期限を持っている。

なお、本節でいう認証局証明書の利用とは、正確には証明書に対応したプライベート鍵を証明書を発行するための利用を意味している。証明書の更新が行われた後でも、旧証明書は使われなくなるわけではない。例えば、更新の直前に発行された証明書を検証するには、旧証明書が必要である。

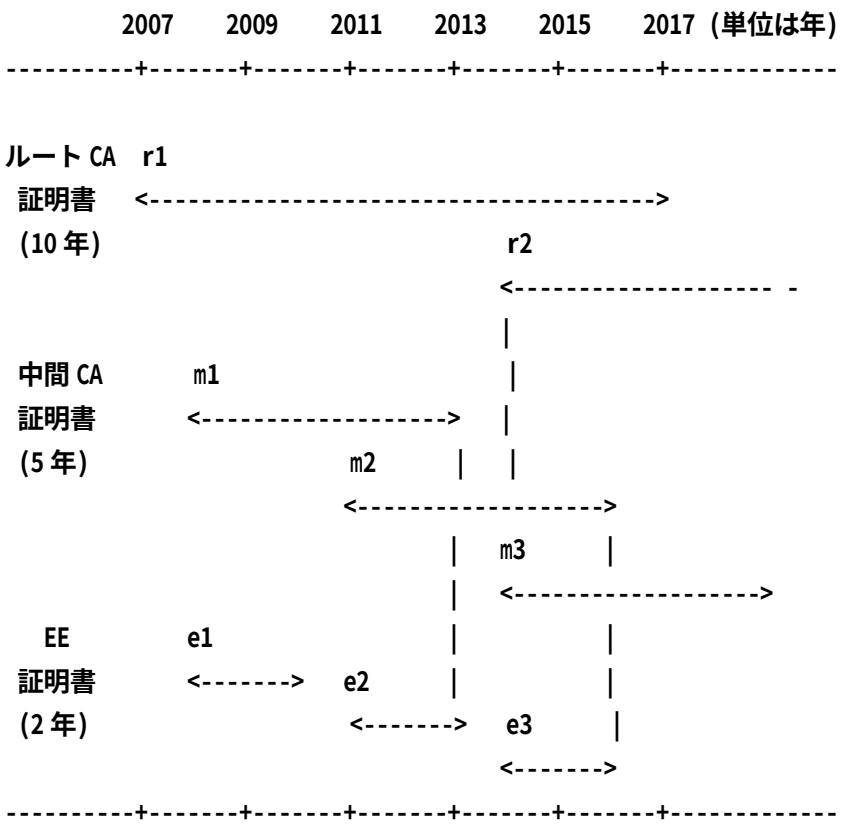

図 2 認証局証明書における鍵更新のタイムチャート

アルファベットの r、m、e は、ルート CA 証明書、中間 CA 証明書、EE 証明書を示している。アルファベットに続く数字は同一の CA や EE に対して、何番目に発行された証明書であるかを示す。例えば、r2 はルート CA に対して 2 番目に発行された証明書である。

図 2 の中で最初に更新される認証局証明書は、中間 CA 証明書の m1 である。m1 は、有効である期間の 5 年から、e1 の有効期間である 2 年を引いた 3 年間しか使われることはない。従って、2011 年の始めには m2 が発行される必要がある。同じ理由で、m2 の利用は 2014 年の始めに終わり、e3 を発行するには更に新しい m3 が使われる必要がある。

EE 証明書と中間 CA 証明書の関係は、中間 CA 証明書とルート CA 証明書に対しても言える。r1 の有効期限は、m3 の有効期限を越えていないため、少なくとも m3 の発行よりも前に更新される必要がある。図 2 によると、r1 は発行から 7 年後の 2014 年の始めには r2 に切り替えられる。

以上の事から、ルート CA 証明書の更新のタイミングは、EE 証明書の有効期限や中間 CA 証明書の有効期限の影響を受けることがわかる。例えば、3 年間の有効期間を持つ EE 証明書を新たに発行することになると、m2 や m3 の発行は更に 1 年早く行われる必要がある。すると r2 は図 2 で示されているよりも 2 年早く発行される必要が出てくる。

6. 備考

特筆すべき事項として、認証局証明書における暗号アルゴリズムの切り替えについて補足する。

認証局証明書における暗号アルゴリズムの切り替えは、本ドキュメントで述べた証明書更新を必要とする。証明書更新後、旧証明書は発行した証明書の有効期限が切れる前までは、旧証明書の並行運用が必要である。ここでいう並行運用とは、CRL の発行、証明書リポジトリの提供を含む。

7. 連絡先

（eapf 事務局：ca-query AT nic.ad.jp）

以上。

2.14. まとめ

本章では、調査研究の一つの柱である電子認証フレームワークについて述べた。この調査研究では 2005 年度に基礎調査を、2006 年度にシステムや制度面の調整を、2007 年度には「電子認証プラクティスフォーラム」と呼ばれる会議体を構築した。

電子認証プラクティスフォーラムは電子認証技術の普及や発展に役立つノウハウを集約しドキュメント化する活動である。その活動は IETF や RIR におけるドキュメント策定プロセスに習い、ラフコンセンサスであり現場の情報を多くの人が得られるように設計を行った。

2007 年度に電子認証プラクティスフォーラムの活動を実験的に行った結果、BoF と呼ばれる会議の参加者の評価は高かった。またメーリングリストを通じて 3 つのノウハウのドキュメント化が行われた。フォーラム活動のためのドキュメントを含めると 5 つのドキュメントが作成されたことになる。

本フォーラムのドキュメントと活動をレビューする専門家チームによると、本フォーラムの評価は高かった。現在、ドキュメントに対するコメントに対して、提案者による対応作業が行われている。

今後、BoF と連動することでメーリングリストの活性化を図り、また参加者から出ていた情報共有の場としても機能できるような場になることを目指したい。