

経済産業省受託調査研究

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報告書

2008年3月

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

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
調査報告書

2008年3月

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

はじめに

JPNIC は我が国における唯一の IP アドレスに関するインターネットレジストリである。本調査研究は、このインターネットレジストリにおいて認証局技術の活用を図ったもので「電子認証フレームワーク」と「IP アドレス認証の展開」という二つのテーマに沿って行われた。

一つ目の電子認証フレームワークは、電子認証技術の各業界における適切な普及を図る為のフレームワークである。電子認証技術の利用や構築のノウハウをドキュメント化する「電子認証プラクティスフォーラム」を実験的に設立し、ML および BoF 等を使ってドキュメント策定活動を行った。二つ目の IP アドレス認証の展開とは、2004 年度までに構築した認証局の技術を応用し発展させる調査研究である。IP アドレスの割り振り情報をインターネット経路制御の安全性向上に役立てるため、「経路情報の登録機構」を設計・開発し、実験運用を行った。

本調査研究は、2005 年度から 3 年間の計画で行われた調査研究の 3 年目である。これまで、電子認証技術の適切な普及と認証局の技術の応用という目標に向かって調査研究が進めてきたが、一方はフォーラムとして、もう一方はシステムとして、形の残るものを世に出すことができた。

本調査研究を通じて作り上げたものが、今後のインターネットコミュニティに役立っていけるよう研究を続けて行きたい。

はじめに

目次

1. 本調査研究の概要と位置づけ	1
1.1. 調査研究の概要	1
1.1.1. 電子認証フレームワークに関する調査研究の概要	2
1.1.2. IP アドレス認証の展開に関する調査研究の概要	3
1.2. 調査研究の背景	3
1.3. 電子認証フレームワークの背景	4
1.4. 2007 年度の位置づけ	5
1.5. IP アドレス認証展開の背景	6
1.6. 2007 年度の位置づけ	7
1.7. 本報告書の内容について	8
2. 電子認証フレームワークに関する調査研究	11
2.1. 概要	11
2.2. 電子認証プラクティスフォーラムの背景	12
2.3. 電子認証プラクティスフォーラムの考え方	14
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	18
2.5. 電子認証プラクティスフォーラムの 3 つの活動	19
2.6. オフライン活動	20
2.6.1. 電子認証プラクティスフォーラム BoF	29
2.7. オフライン活動に関するフィードバック	35

2.8. オンライン活動.....	37
2.9. オンライン活動の考え方	37
2.10. オンライン活動としてのメーリングリスト.....	43
2.10.1. メーリングリストを通じたドキュメント提案.....	45
2.11. ノウハウのドキュメント策定活動	46
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	47
2.13. 本フォーラムを通じて作成されたドキュメント	48
2.14. まとめ.....	73
3. 電子認証技術と技術文書策定に関する国際動向	75
3.1. 調査研究の概要.....	75
3.2. 第 69 回 IETF における PKI 技術の動向.....	75
3.3. 第 69 回 IETF における TAM BoF.....	80
3.4. 第 70 回 IETF における PKIX WG.....	84
3.5. まとめ.....	90
4. IP アドレス認証の展開に関する調査研究.....	93
4.1. 経路情報の登録機構の開発と調査研究.....	94
4.2. 経路情報の登録機構を使った実験の考え方.....	94
4.3. 経路情報の登録機構とは	95
4.4. 経路情報の登録機構を使った IP アドレス関連の業務.....	100
4.5. 許可リストを使った IP アドレス管理業務.....	102
4.6. 経路情報の登録機構の利用実験.....	104

4.6.1. 利用実験の考え方	105
4.6.2. 利用実験の手順.....	105
4.6.3. 利用実験の参加状況	105
4.6.4. 利用実験のフィードバック.....	106
4.7. 経路情報の登録機構の改修.....	107
4.8. 経路情報の登録機構の応用.....	110
4.9. 経路情報の登録機構に関する国際会議での議論.....	112
4.10. 経路情報の登録機構に関する国内会議での議論.....	135
4.11. 経路情報の登録機構と JPNIC 認証局の連携.....	146
4.12. 認証業務規程 (CPS) について.....	150
4.13. まとめ.....	151
5. 経路制御のための電子認証技術に関する国際動向.....	153
5.1. 概要.....	153
5.2. IETF SIDR WG の動向.....	155
5.3. 第 69 回 IETF SIDR (Secure Inter-Domain Routing) WG.....	156
5.4. 第 70 回 IETF SIDR WG.....	160
5.5. リソース証明書に関する RIR の相互運用実験.....	165
5.6. 国際会議 IEPG での発表.....	165
5.7. RIPE NCC における動向.....	167
5.8. 第 54 回 RIPE ミーティング.....	168
5.9. 第 55 回 RIPE ミーティング.....	175
5.10. RIPE Certification Task Force.....	177

5.11. ARIN における動向	182
5.12. 第 20 回 ARIN ミーティング	188
5.13. APNIC における動向	190
5.14. まとめ	192
6. 電子認証フレームワークと IP アドレス認証展開の今後.....	195
6.1. 電子認証フレームワークの今後.....	195
6.2. IP アドレス認証展開の今後	196
6.3. 今後の課題と活動	197
Appendix. 1 経路情報の登録機構のユーザインターフェース	
Appendix. 2 JPIRR 認証局 認証業務規程	
Appendix. 3 JPIRR 認証局 認証業務規程 英語訳	

第 1 章 本調査研究の背景と位置づけ

内容

- 調査研究の位置づけ
- 調査研究の活動と本報告書の内容

1. 本調査研究の概要と位置づけ

本調査研究は、2005 年度から 2007 年度の 3 年計画で実施している調査研究の 3 年目である。また 2005 年度の調査研究に先立ち、本調査研究の背景となった、IP アドレス認証に関する調査研究が行われていた。

本章では、始めに調査研究の概要を示し、次に本調査研究の背景と 3 年計画の中の位置づけについて述べる。

1.1. 調査研究の概要

本調査研究は「電子認証フレームワークに関する調査研究」と「IP アドレス認証の展開に関する調査研究」の二本立てである。各々の調査研究の概要について述べる。

第1章 本調査研究の概要と位置づけ

1.1.1. 電子認証フレームワークに関する調査研究の概要

調査研究の概要を図 1-1 に示す。

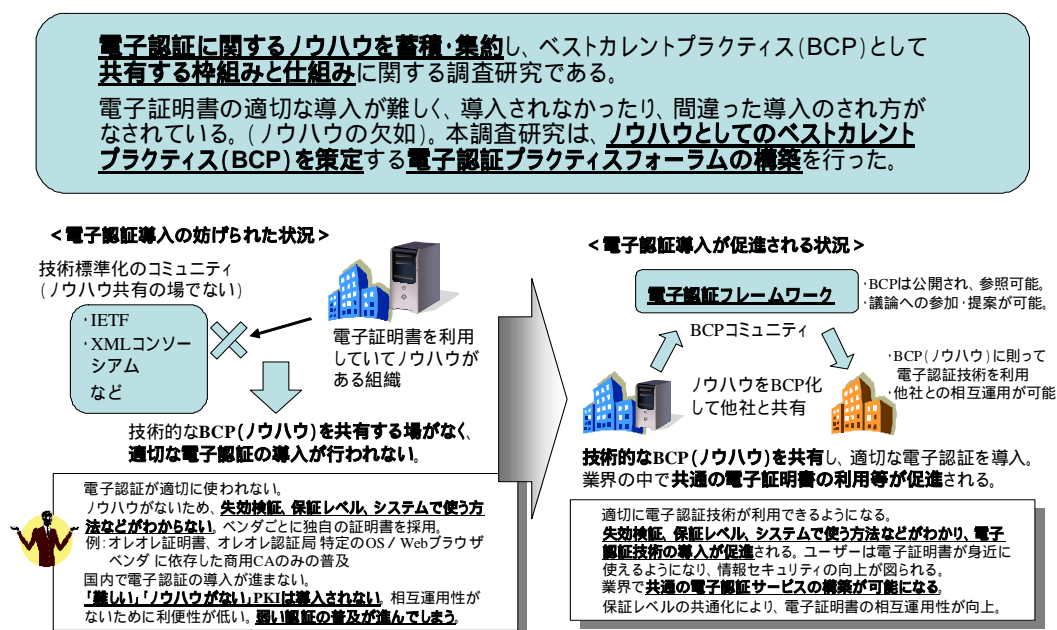


図 1-1 電子認証フレームワークに関する調査研究

電子認証に関するノウハウを蓄積・集約し、ベストカレントプラクティス(BCP)として共有する枠組みと仕組みに関する調査研究である。

電子認証技術は、利用のノウハウが得にくいいため適切に使うことが難しい。例えば失効検証の適切な行い方や保証レベルの設置の仕方、システムで使う方法などのノウハウが考えられる。そのため電子認証技術は「難しい」という印象があり、また相互運用性を確保する使い方がされていないために利便性が低い。

本調査研究では、ノウハウをドキュメント化し、会議を通じて継続的に「ベストカレントプラクティス(BCP)」を策定する電子認証プラクティスフォーラムの構築を行った。

1.1.2. IP アドレス認証の展開に関する調査研究の概要

調査研究の概要を図 1-2 に示す。

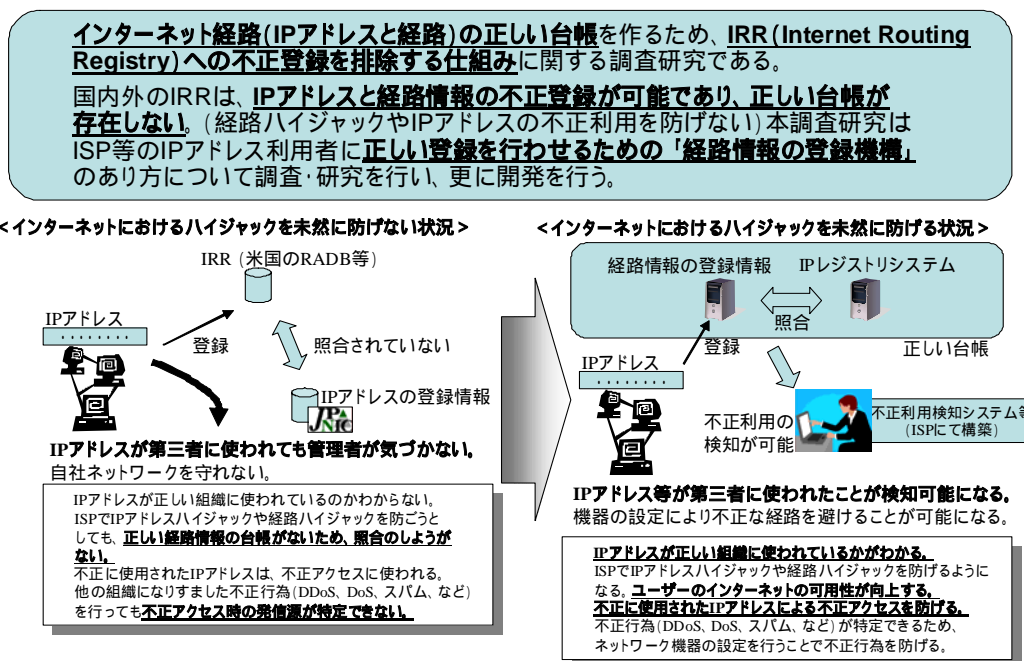


図 1-2 IP アドレス認証の展開に関する調査研究

インターネット経路 (IP アドレスと経路) の正しい台帳を作るため、IRR (Internet Routing Registry) への不正登録を排除する仕組みに関する調査研究である。

IP アドレスの登録情報と経路情報のデータベースが異なり、いわば正しい経路情報の台帳が存在しない。そのため IP アドレスが正しい組織によって使われているのかが本質的にはわからない。なお経路ハイジャックが行われているようなときには、不正アクセスの発信源を特定できない。

本調査研究では、ISP 等の IP アドレス利用者に正しい登録を行わせるための「経路情報の登録機構」のあり方について調査・研究を行い、更に開発を行った。

1.2. 調査研究の背景

2005 年度より以前、当センターでは「IP アドレス認証局」と呼ばれる認証局に関する調査研究を行っていた。これは IP アドレスのレジストリである JPNIC において認証

第1章 本調査研究の概要と位置づけ

局を運用し、インターネットセキュリティの向上に役立てることを目的とした調査研究である。

IP アドレス認証局の調査研究の結果、独自の認証局を構築し、更に IP アドレスに関する登録情報を守るためのユーザ認証用の認証局を構築することとなった。JPNIC 独自の認証局が構築した理由は、IP アドレスやインターネットのアドレッシングに関する「信頼点」として機能する authority を確立し、その認証局を当センターで運用することで登録情報を各種ネットワークサービスに役立てようという考え方に至ったためである。

このような背景から、認証局の構築あたっては、CP (Certificate Policy - 証明書ポリシー) や CPS (Certification Practice Statement - 認証業務規程) の策定や運用のレベル、業務モデルに関する検討を一から行い、同時に IETF PKIX WG などの最新の国際動向の調査を行ってきた。また電子認証技術に関する利用者へのヒアリング等も行ってきた。

2005 年度の本調査研究を開始する段階になると、JPNIC に電子認証に関する知見が得られる人的環境が整ってきたが、すると電子認証技術が持つ課題や、普及のカギが欠けている現状が見えてきた。それが次に述べる電子認証フレームワークと IP アドレス認証の展開の調査研究を行うことになった背景である。本調査研究のテーマが「電子認証フレームワーク」と「IP アドレス認証の展開」の二つになったのには、各々に背景がある。ここで各々の調査研究の背景について述べる。

1.3. 電子認証フレームワークの背景

インターネットを通じて提供されている、様々な個人向けまたは企業向けサービスにおいて、その電子的すなわちオンラインでの認証方法はパスワードが主流である。中には強い電子認証技術を使うような IC カード (Felica とは異なる、耐タンパ性を持った IC カード) を採用しているサービスはあるが、一般のサーバ構築の場面で簡単に利用できるような状況にはなっていない。当センターの認証局および関連サーバを構築した際に改めてわかったことであるが、電子認証技術、特に PKI (Public-Key Infrastructure) の採用に抵抗を感じる開発業者は多い。

しかし、本当に危惧すべきことは、ID/パスワードで十分、もしくはそれしか運用可能な方式がないと考えて採用してしまうという現状である。実際には、パスワードが複数のユーザに共有されていて、漏洩に気づきにくいことになっていたり、パスワードが何年も変更されず、簡単に破られてしまうようなシステムが存在している。本来であれば、一定期間毎にパスワードを変更したり、推測が難しく全ての可能性を試されるような攻撃にも耐えられるように十分に長い文字列を使う必要があったりする。しかしそれではユーザにかかる負担が大きく、実際に行われている事例はほとんど聞いたことがな

い。暗号技術を使った電子認証技術であれば、その必要性は低く、ユーザへの負担は軽いはずである。しかも今日の多くの Web ブラウザには PKI を使った電子認証技術が実装されている。

なぜ、電子認証技術は難しいという印象をぬぐえないのか。本調査研究では、この疑問に答えるためのカギとして、国際会議などで言われているプラクティスと呼ばれる、「実用的なノウハウ」に着目した。プラクティスを蓄積し共有すれば、システム構築を行う者の障壁を下げることができると共に、電子認証の相互運用性を高める効果も期待できる。相互運用性の高い電子認証がインターネットで使われるようになれば、より安全で安心できるネットワークサービスを、一般ユーザに提供しやすくなる。

1.4. 2007 年度の位置づけ

電子認証フレームワークは、各業界に共通して役立つような電子認証に関するフレームワークを意味している。元来、定義のある言葉ではなく、調査研究を通じてあり方を明らかにしてきた。2005 年度の調査の結果から、本調査研究におけるプラクティスの蓄積と共有の為の仕組みを指し、ノウハウを広く共有できるような仕組みをさすこととなった。2005 年度から 2007 年度までの調査研究の実施内容と成果を表 1-1 に示す。

表 1-1 2005 年度から 2007 年度までの実施内容と成果

年度と実施内容	成果
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結果の結果 ・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た結果 ・BCPの策定プロセスの要件
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 ・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 ・議論のためのML、Web等
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 ・レビュー結果

2005 年度は、電子認証フレームワークのための基礎的な調査を行った。各国のプラク

第1章 本調査研究の概要と位置づけ

ティスと呼べるドキュメント（特に電子認証における保証レベルという概念にフォーカスした）について調査を行うと共に、ノウハウをドキュメント（文書）として集約するような社会的な仕組みについて調査を行った。ドキュメントを集約する仕組みとして、IETF や RIR(Regional Internet Registry – 世界に5つある地域インターネットレジストリ)のポリシーミーティングがある。IETF は技術的なプロトコル策定の会議体であり、RIR のミーティングは IP アドレスに関するポリシー文書を策定するための会議であるが、別の見方をすると、参加者のドキュメント化の提案を受け付け、よりよいドキュメントを策定していく社会的な仕組みであると捉えることができる。調査研究ではこれらのドキュメントの策定プロセスに着目し、またルール設計の部分についても意識しながら現地調査を行った。

2006年度は、IETF 等の調査でわかってきたコミュニティの仕組みを構築するため準備の年度であった。まず情報公開や議論の基本的な機能となる、Web サーバやメーリングリストサーバを構築・準備した。またベストプラクティスという、他の種類のドキュメントとの境目が曖昧な話題を扱うことに対する各種の考察を行った。例えば、電子認証技術があるベンダーのシステムに限定されるようなノウハウが公開されると、特定のベンダーの製品の利用を促進するようなことになってしまう。すると電子認証技術自体の発展とは活動主旨が異なってしまう恐れがある。また相互運用性の確保も難しくなることが想像される。2006年度は、これらの検討結果を踏まえたドキュメントの基本的な書式やドキュメント化プロセスの明文化などを行った。

2007年度は、いよいよ実験的に会議体「電子認証プラクティスフォーラム」を運営する段階である。2006年度に構築したシステムに加えて、本フォーラムへの参加に際しての、参加者の同意事項を整備するなどした。本フォーラムの一環としてオンライン活動（Web ページを使ったドキュメント管理やメーリングリストを使ったディスカッション）とオフライン活動（会議）を実施した。更に、そこで策定されたドキュメントとフォーラム活動に対するレビューを行った。この実験的なフォーラムの実施を通じたアウトプットが、本調査研究の成果になると考えられる。

1.5. IP アドレス認証展開の背景

本調査研究の二つ目のテーマである「IP アドレス認証の展開」は、2004年度までのIP アドレス認証に関する調査研究の応用編である。IP アドレス認証とは、IP アドレスなどの登録情報に関する、またはそれを利用した電子認証といった意味であるが、2004年度の段階では登録者の認証の為に各種の仕組みを構築するに留まっていた。これでも登録情報の保護には十分に役立つ仕組みであるが、ユーザ数の拡大やそれに伴う電子認証事業の確立の意味で、ユーザに利便があるような仕組み作りが必要であった。これは電子署名・電子認証技術一般に言われることであるが、既に行われているような業務手続きに対して、安全性を向上させるだけではユーザへの訴求度は低い。利用することで、

それに見合う恩恵を得られるような仕組みが必要である。例えば当センターであれば、IP アドレスの不正な利用を検知できるようになる、インターネットを顧客に安全に提供できるようになる、といった、利用に見合う恩恵が与えられなければならない。本調査研究は、インターネットセキュリティに資するような仕組みの調査研究を行うこととなった。

1.6. 2007 年度の位置づけ

IP アドレス認証の展開は、2004 年度までに構築した ISP 等の IP アドレスの割り振り先の認証を応用し、インターネットセキュリティに資する仕組みを構築する調査研究である。しかしインターネットの運用に関しては、IETF の RFC(Request for Comments) や、国際的なネットワーク運用者のコミュニティにおいて常識になっている文化や理念が存在し、新たに構築した IP アドレスに関連するシステムや業務が簡単に受け入れられるとは考えにくい。一方で、インターネット経路制御の分野では IP アドレスの登録情報を使った不正利用排除のニーズが高まりつつある。2005 年度から 2007 年度までの調査研究の実施内容と成果を表 1-2 に示す。

表 1-2 2005 年度から 2007 年度までの実施内容と成果

年度と実施内容	成果
2005年度 ・IPアドレス認証の展開 ・ISPへのヒアリング ・RIRの状況調査	経路情報の登録機構の要件調査の結果 ・ISP等へのヒアリングを通じて、正しい台帳を作るシステムの要件
2006年度 ・IPアドレス認証の展開 ・経路情報の登録機構設計と実装 ・RIRの登録機構調査	経路情報の登録機構(プロトタイプシステム) ・本機構の設計と実装
2007年度 ・IPアドレス認証の展開 ・ISPとASにおける試験運用 ・RIRの今後の取り組み調査	経路情報の登録機構(プロトタイプシステム) ・実験的にサービス ・フィードバック ・国内・海外でのディスカッションの結果

2005 年度は ISP へのヒアリングや、RIR の状況調査などの基本的な調査を行った。RIR では認証局がすでに構築されており、また IP アドレスに関する登録情報を IRR

第 1 章 本調査研究の概要と位置づけ

(Internet Routing Registry) と連携させる等の仕組みを有している。2005 年度の調査の結果、日本国内において経路情報に関する正しい台帳を持つことの重要性と、その要件が明らかになった。

2006 年度は 2005 年度に明らかになった要件を元に「経路情報の登録機構」の設計と開発を行った。また RIR における IP アドレスのルーティングに対する authorize(認可) の仕組みの詳細について調査を行った。活動の結果、経路情報の登録機構のプロトタイプシステムが完成した。

2007 年度は経路情報の登録機構を実験運用し、実際に ISP の担当者に使ってもらえるようにするための活動を行った。対象となるユーザは ISP の IP アドレスに関する申請業務担当者と、AS の登録情報を管理しているメンテナの登録担当者である。活動の結果、実験サービスを行い、ユーザからのフィードバックを得た。またフィードバックを元に経路情報の登録機構を改修するなどした。

1.7. 本報告書の内容について

本調査研究に関する本報告書でのまとめかたについて述べる。

- **電子認証フレームワークに関する調査研究 (第 2 章)**
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」と呼ばれる会議体を運営し、電子認証技術に関わるノウハウのドキュメント化活動を行った。この活動と活動のレビュー、および活動成果であるドキュメントについて述べる。
- **電子認証技術の動向に関する調査 (第 3 章)**
IETF のミーティングに参加し、電子認証技術の最新動向について調査した。2007 年度は第 69 回 IETF ミーティングと第 70 回 IETF ミーティングに参加した。PKIX WG の動向を中心にまとめる。
- **IP アドレス認証の展開に関する調査研究 (第 4 章)**
調査研究の一環として経路情報の登録機構の実験運用を行った。実際に ISP の担当者に利用してもらいフィードバックを得ると共に、国内および海外の会議でプレゼンテーションを行い、RIR コミュニティの技術的な見地での意見交換を行うなどした。
- **経路制御のための電子認証技術に関する国際動向 (第 5 章)**
経路情報の登録機構は、インターネット経路制御のために役立つ仕組みである。一方、RIR の中には本機構に似た役割を持つ仕組みが適用されていたり、全く別のアプローチであるリソース証明書と呼ばれる電子証明書のシステムが開発されていたりする。そこで IETF や RIR のミーティングに参加し、具体的な

開発動向等について調査を行った。

第 6 章では、電子認証フレームワークと IP アドレス認証の展開の今後の関わり方について整理し、調査研究の方向性を交えてまとめた。

また Appendix として、経路情報の登録機構のユーザインターフェースを解説したものと、JPIRR 認証局の CPS、およびその英語訳を掲載した。

RIR や IETF および IEPG での情報交換のなかで、JPNIC の認証局や本調査研究に対する関心が高いと感じる場面がたびたびあった。そこで英語圏の技術者に対しても JPNIC 認証局に関する情報提供ができるよう、経路情報の登録機構と連携する JPIRR 認証局の CPS の英語訳を作成した。

第 1 章 本調査研究の概要と位置づけ

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

第2章 電子認証フレームワークに関する調査研究

フォーラムの意義に関する高い評価を得ている。このことから、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。

電子認証の適切な普及の課題の分類

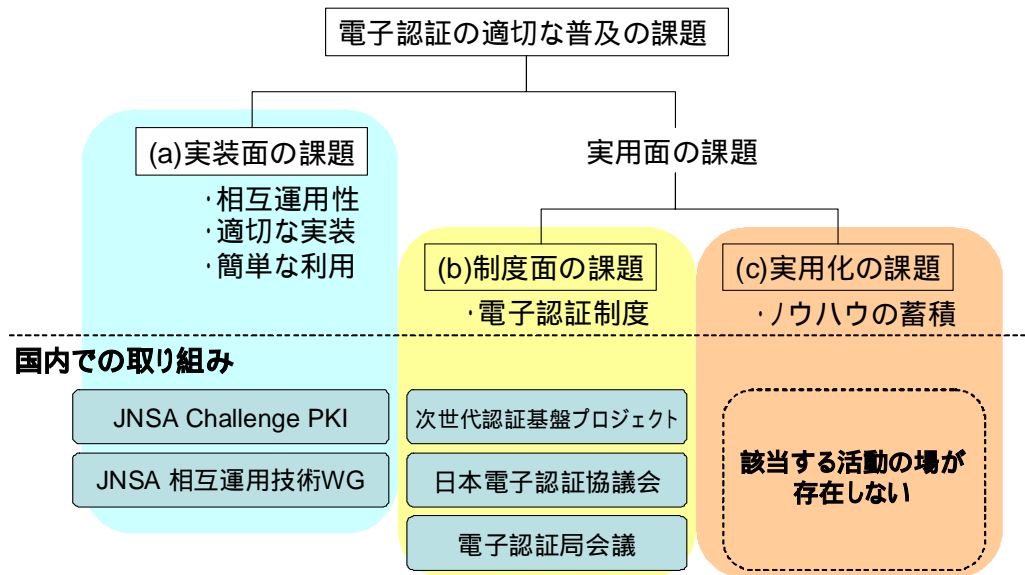


図 2-1 電子認証技術の普及の課題

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。

第2章 電子認証フレームワークに関する調査研究

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。

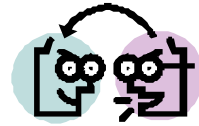
2.3. 電子認証プラクティスフォーラムの考え方

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。

電子認証プラクティスフォーラムの考え方

• 重視する考え方

- ラフコンセンサスを重視
- 現場の現状に基づいた知識
- 議論と成果の公開



- 技術を*標準化*する活動ではない
- 参加者は所属組織を代表するものではない
- 各自の現時点で最善のノウハウを文書化し
共通認識化することに最も重点を置く

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

第2章 電子認証フレームワークに関する調査研究

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）。

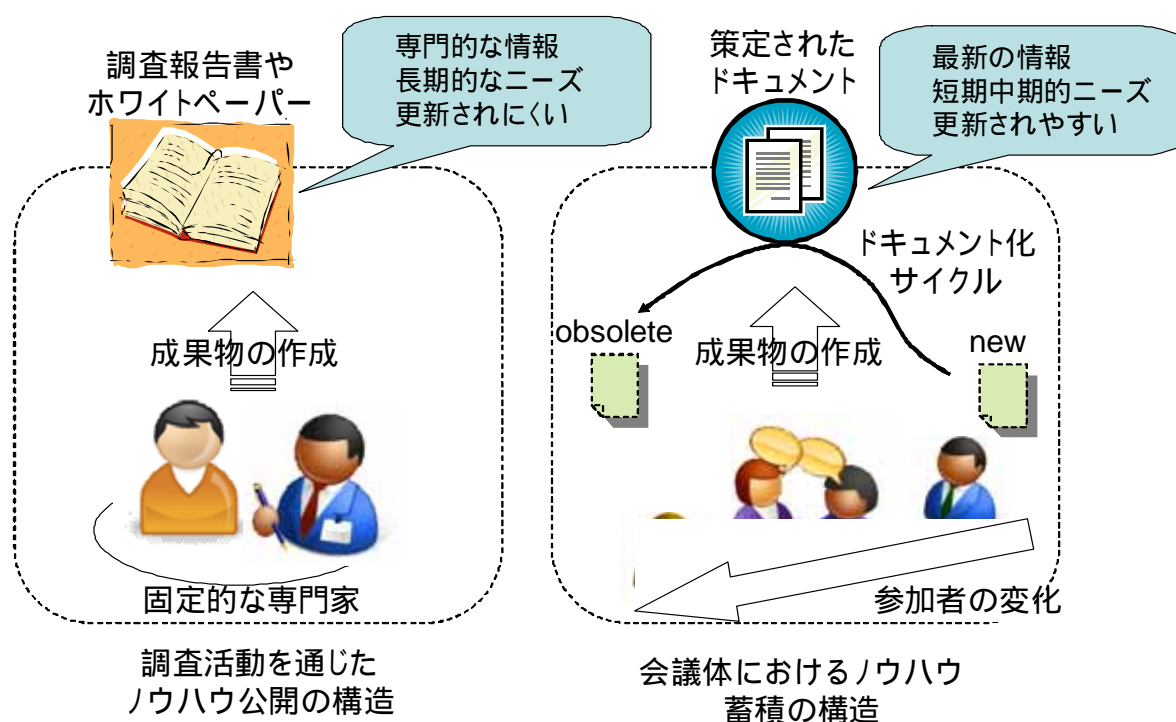


図 2-3 ノウハウのドキュメント化構造の違い

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かれ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 の分けも、技術標準の規模が大きい場合には役に立ちにくい。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。

第2章 電子認証フレームワークに関する調査研究

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 ・必要性和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、技術が未熟なだけでなく、ノウハウが足り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での会議の「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

第2章 電子認証フレームワークに関する調査研究

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、多くの人々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取り、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)

[コーヒープレーク 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。

第2章 電子認証フレームワークに関する調査研究

「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ー管理機関による適切なポリシーマッピングの実現

1. 概要

複数の認証局におけるポリシーマッピングを行う際に起こるポリシー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ー管理機関による運用によって適切なポリシー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ーマッピングを行って電子証明書の相互運用を図る際に、ポリシー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。

(1) ユーザの電子認証に関わるもの

- [bcp-idraft-businesscerts-01] 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)
 - 読者の対象
 - 認証サービスの構築を行う者
 - 概要
 - 一定の確認要件を満たした上で、法人内で発行される電子証明書や担当者の識別子が、会社間のビジネスで有効になる範囲を示す。
 - 三文判の程度の確からしさや事後追跡性、利用性を電子認証技術を使って実現することを目指す。
 - 考えられる効果
 - 認証ドメイン間の認証連携をしやすくする効果が見込まれる。

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。

(2) 機器の電子認証に関わるもの

- [bcp-idraft-iphostcerts-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
 - 読者の対象
 - 認証サービスの構築を行う者
 - 概要
 - IP接続された機器を認証するための電子認証を区分けし、各々の保証レベルを示したもの。ルータ向けに発行された電子証明書やエンドノードに発行された電子証明書で使われる認証基盤のモデルを示す。
 - 機器登録の厳格さを保証レベルとしてレベル分けし、厳しさに応じた用途を規定する。
 - 考えられる効果
 - 将来的に機器等の電子証明書の位置づけを明文化したり、様々な通信における認証の安全性を識別する指標となりうる。

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。

(3) 認証局と表示方法等に関するもの

- [bcp-idraft-certbusinessstype-01] 認証局証明書の区分とその表示方法
 - 読者の対象
 - RP (Relying Party) の開発を行う者
 - 概要
 - 現在、ユーザは予めWebブラウザに組み込まれているかどうかでその信頼度を測らざるを得ない状況がある。認証の区分に応じて信頼度を測れるようなデファクトを作成し、あるべき認証が普及することを目指す。
 - 考えられる効果
 - 例えば、httpsで使われる認証局を"商用"、"政府"、"教育機関"、"医療"といった区分で表し、ユーザが利用している認証局を識別できるようにする。

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。

(4) 認証局の運用に関するもの

- [bcp-idraft-cakeyrollover-01] 認証局のキーロールオーバー手法
 - 読者の対象
 - 認証サービスの構築を行う者
 - 概要
 - ユーザ証明書と同様に、認証局証明書にも有効期限がある。ユーザ向けの証明書の利用上の不具合を避けるには、認証局のキーロールオーバーをスムーズに行う必要がある。既存の認証局等のノウハウを文書化し、チャート等を含むBCPを作成する。
 - 考えられる効果
 - 他の認証局が参照し設計や実施が容易になることを目指す。

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。

その他の例

- パスワード認証方式の*良さそうな*利用方法
 - 桁数 / 変更の頻度 その根拠
 - ユーザ側のポイント
 - サービス提供側のポイント
 - S/MIMEの電子署名の有効性の表示
 - 証明書の有効期限が切れているとき
 - 証明書が失効されているとき
 - 内容が改ざんされているとき！
- これらがあれば仕様を決めるための説明が付きやすい！



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と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
Copyright (C) 1996-2007 Japan Network Information Center. All Rights

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。拳手とその割合など。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-cakeyroll-over-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、

第2章 電子認証フレームワークに関する調査研究

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あるため。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ら	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わないか、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ふ。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

第2章 電子認証フレームワークに関する調査研究

では、WG ごとにチェアがあり、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。

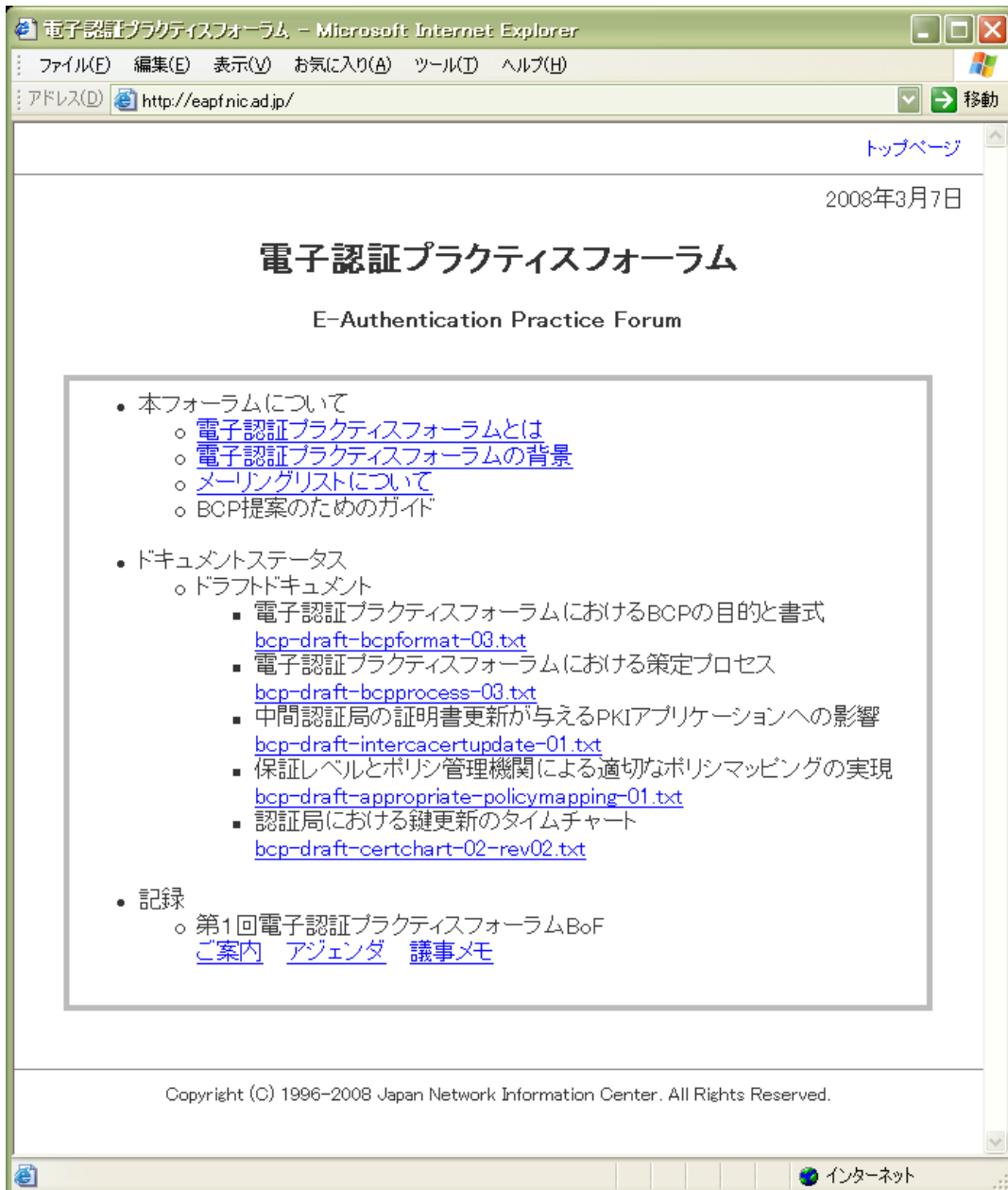


図 2-9 電子認証プラクティスフォーラム トップページ

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によって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。

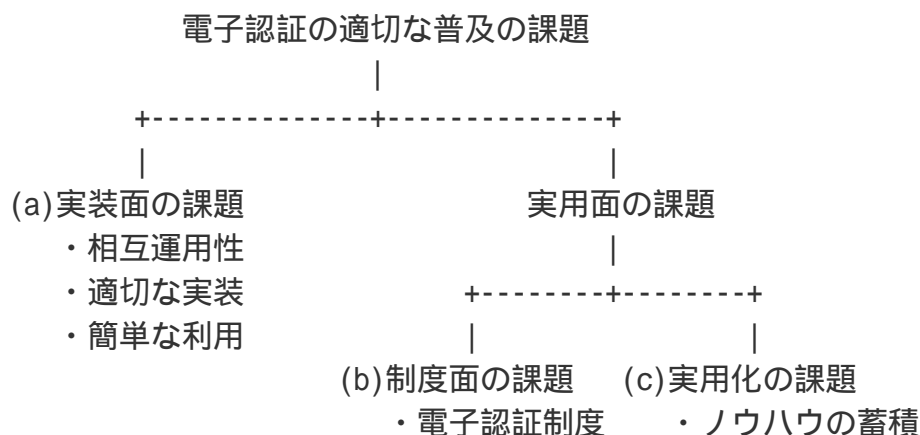


図1 電子認証の適切な普及の課題の分類

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土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 メール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. メールングリストを通じたドキュメント提案

メールングリストは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、メールングリストと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。

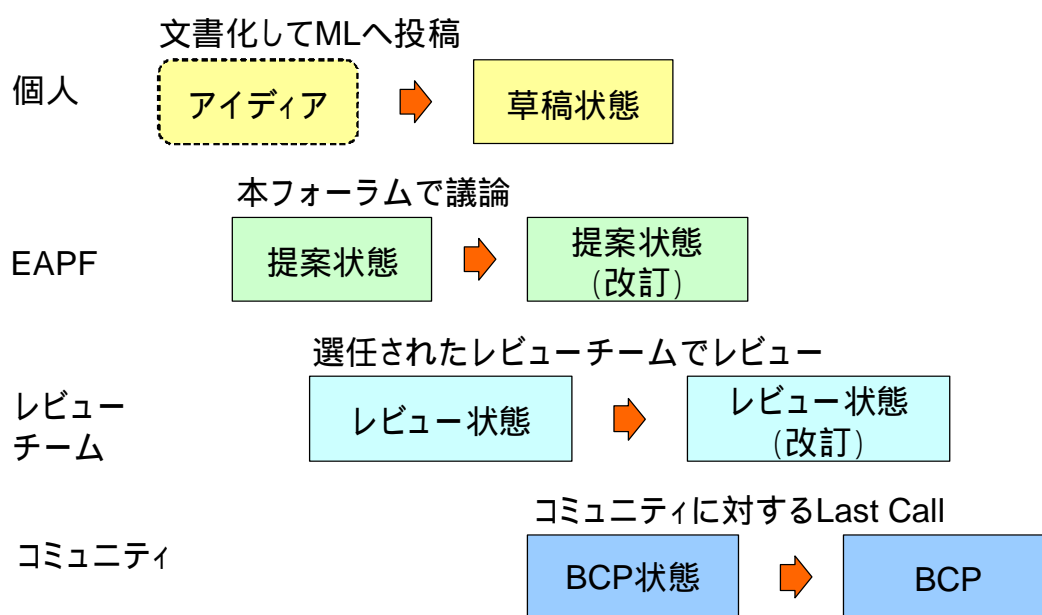


図 2-10 ドキュメント化プロセス

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 を定期的に関開くべき。
- ・フォーラムの認知度向上を図るべき。

第2章 電子認証フレームワークに関する調査研究

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高かったことがわかる。BoF の評価のポイントは、大きく分けて三つ三つあった。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。二つ二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。三つ三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）と二つ二つ目のポイント（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。三つ三つ目（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ー管理機関による適切なポリシーマッピングの実現
[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。

第2章 電子認証フレームワークに関する調査研究

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。

- A. ドラフト(草稿)状態
<draft ステータス>

- B. 提案状態
<proposed ステータス>

- C. レビュー状態
<review ステータス>

- D. BCP 状態
<bcp ステータス>

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でも行うことができる。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、担当レビューが割り当てられる。担当レビューはドキュメントに対するレビューとその対応について責任を持つ。担当レビューは、後述するレビューチームからの立候補とする。担当レビューの責任、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ーと著者が行う。

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

第2章 電子認証フレームワークに関する調査研究

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

第2章 電子認証フレームワークに関する調査研究

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 (IssuerDN) 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
				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)
+	+	する		
			一部の PKI アプリケーションが Apache、Firefox、Thunderbird が新旧の認証局の CRL 正しく解釈できない(*4)	
+	+	しない		
			一部の PKI アプリケーションに Opera が SSL クライアント 認証で不正なパス構築(*5)	
				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)
+	+	する		
				前提条件[発行された End Entity の証明書は有効期限

第2章 電子認証フレームワークに関する調査研究

				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	アプリケーション	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 ケース	コメント
				前提条件[発行された End
認証局証明		する	N/A	Entityの証明書は有効期限
書の有効期				まで使えること]に違反(*1
+限を越えな+	する	-----+	-----+	-----+
いように更				
新		しない	問題なし	
-----+	-----+	-----+	-----+	-----+
				前提条件[発行された End
		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
+直前に更新+	する	-----+	-----+	-----+
				前提条件[発行された End
		しない	N/A	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る、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 のポリス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スマッピングの実現

1. 概要

複数の認証局におけるポリス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ス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、証明書ポリシー(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、ポリシーの伝言ゲーム問題の理解を図ると共に、証明書ポリシー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

異なるポリシーを持つ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ーの伝言ゲーム問題

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ー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ー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ー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ーを、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ー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、ポリシー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。

```

+-----+ CP-X == CP-Y +-----+ CP-Y == CP-Z +-----+
| CA-X |----->| CA-Y |----->| CA-Z |
+-----+ (CRL更新<=24h) +-----+ (CRL更新<=48h) +-----+
    
```

図1 ポリシの伝言ゲーム問題

このように、ポリシー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、ポリシー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ーの伝言ゲーム問題の回避

ポリシーの伝言ゲーム問題を最小に留めるためには、ポリシー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、ポリシー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本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ー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ーを策定した認証局であれば評価することも容易である。

ポリシー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ー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ー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ーは 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ー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ー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、継続的にポリシー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、認証局の持続的な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

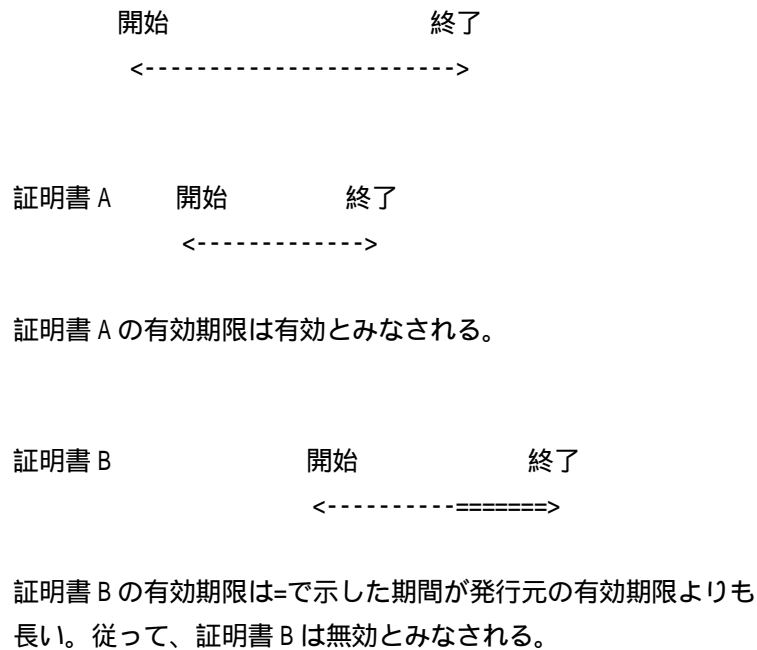


図1 有効とみなされる有効期限と無効とみなされる有効期限の違い

認証局が、図1の証明書Aに示したよ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期間が終わる前に、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。

第2章 電子認証フレームワークに関する調査研究

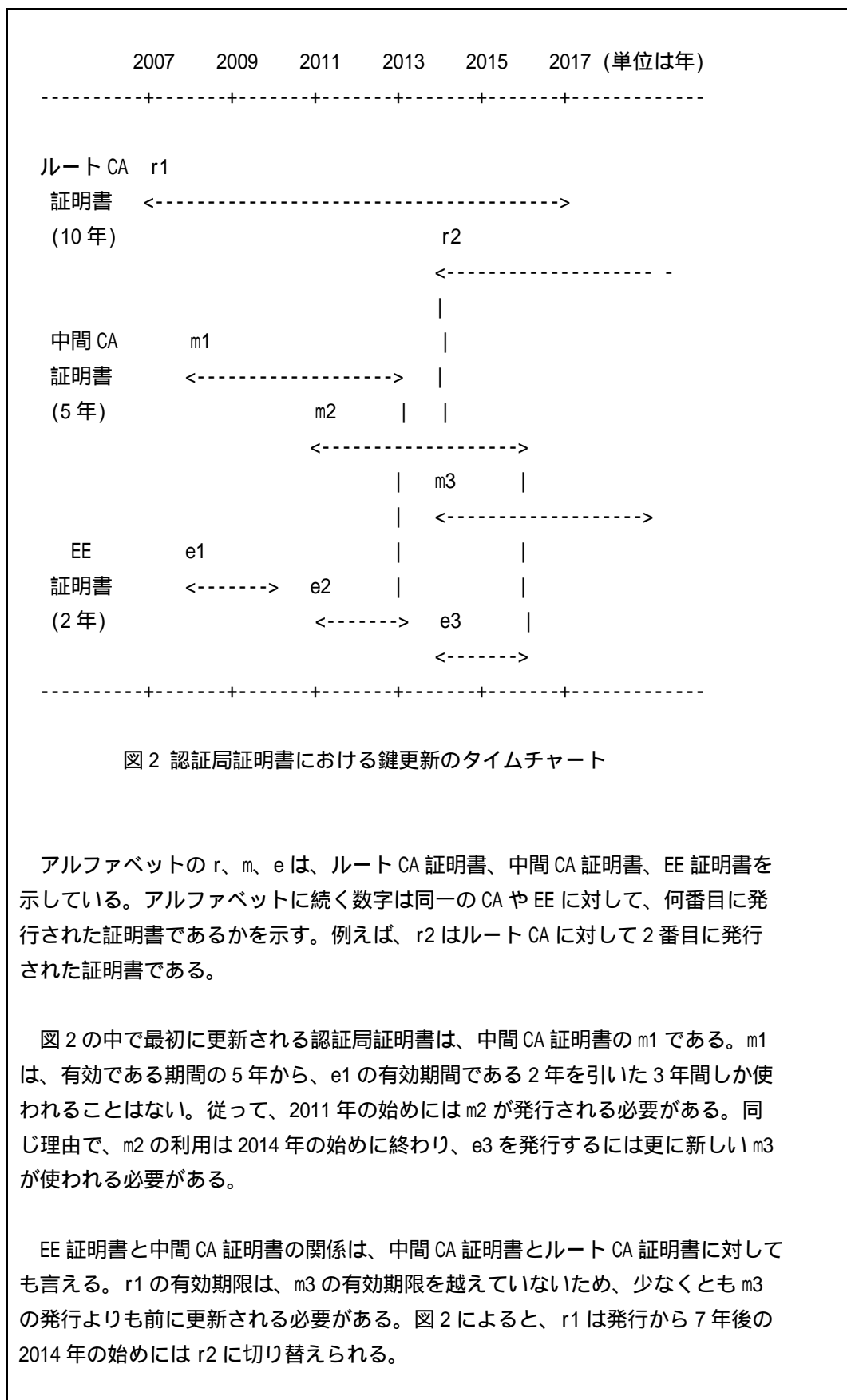


図2 認証局証明書における鍵更新のタイムチャート

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ことを示す。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々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。

第2章 電子認証フレームワークに関する調査研究

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。

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 WG¹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えていないと動向がわかりにくい、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 にとっては会議の時間が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/>

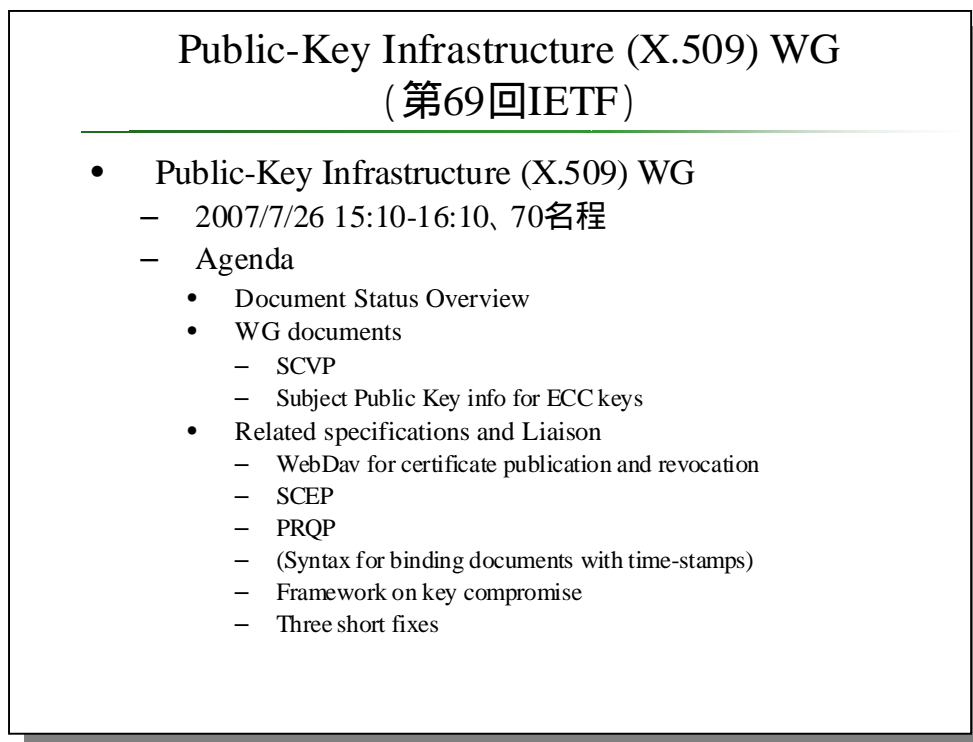


図 3-1 Public-Key Infrastructure (X.509) WG (第69回IETF)

図 3-2 に第 69 回 IETF でのドキュメントステータスを示す。

第69回IETF PKIX WG ドキュメントステータス

- RFC化承認済み(RFC Editorの処理待ち)
 - Lightweight OCSP (Proposed Standard)
 - Service Name SAN(Subject Alt Name)
- IESGレビュー - 中
 - Server-based Certificate Validation Protocol (SCVP)
 - RFC 3280bis
 - CMC (3 documents)
- WG内作業中
 - Draft for ECDSA and DSA with SHA-2 family of hash algorithms
- 期限切れ
 - ECC algorithms
- 個人による投稿
 - Credential Selection Criteria Data Structure

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 RFC5019³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 RFC5055⁴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>

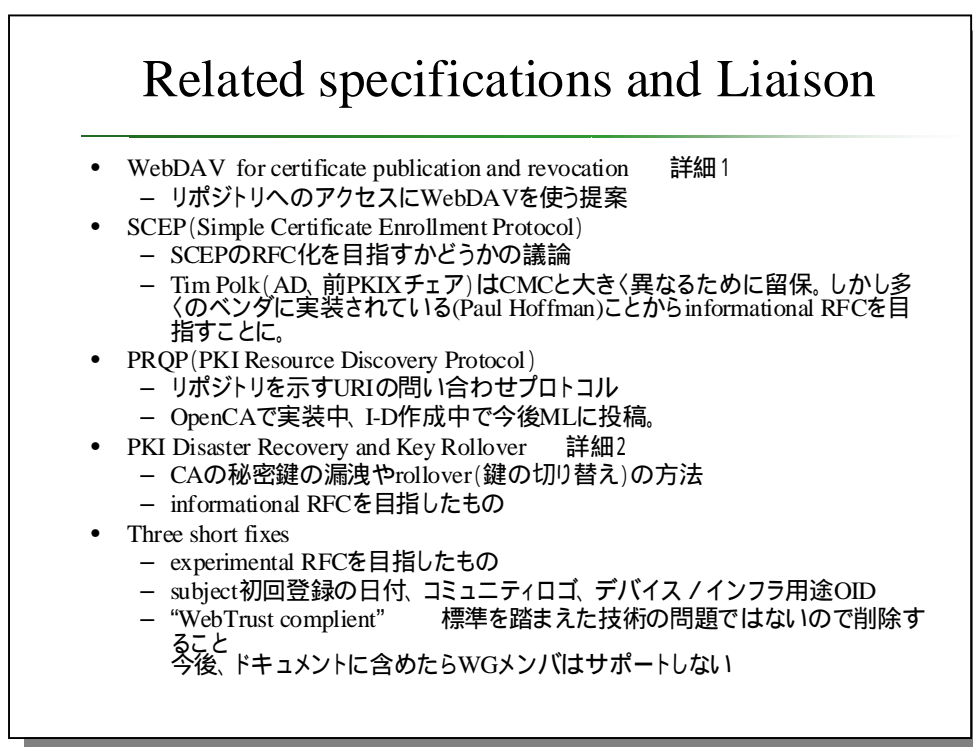
⁴ Server-based Certificate Validation Protocol (SCVP) (RFC 5055)

<http://www.ietf.org/rfc/rfc5055.txt>

第3章 電子認証技術と技術文書策定に関する国際動向

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。



Related specifications and Liaison

- WebDAV for certificate publication and revocation 詳細1
 - リポジトリへのアクセスにWebDAVを使う提案
- SCEP(Simple Certificate Enrollment Protocol)
 - SCEPのRFC化を目指すかどうかの議論
 - Tim Polk(AD, 前PKIXチェア)はCMCと大きく異なるために留保。しかし多くのベンダに実装されている(Paul Hoffman)ことから informational RFCを目指すことに。
- PRQP(PKI Resource Discovery Protocol)
 - リポジトリを示すURIの問い合わせプロトコル
 - OpenCAで実装中、I-D作成中で今後MLに投稿。
- PKI Disaster Recovery and Key Rollover 詳細2
 - CAの秘密鍵の漏洩やrollover(鍵の切り替え)の方法
 - informational RFCを目指したもの
- Three short fixes
 - experimental RFCを目指したもの
 - subject初回登録の日付、コミュニティロゴ、デバイス/インフラ用途OID
 - “WebTrust compliant” 標準を踏まえた技術の問題ではないので削除すること
今後、ドキュメントに含めたらWGメンバはサポートしない

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。

WebDAV for certificate publication and revocation

- リポジトリへのアクセスにWebDAVを使う提案
 - Representational State Transfer (REST) 原理
(情報リソースをURLで識別、キャッシュ可能性情報の提供)
- 利点:ファイアウォールを通りやすい、CRLを検索しやすい、個々の証明書を取り出しやすい、等
- 課題点:DoS攻撃、証明書の情報のプライバシー、プロキシサーバによるキャッシュ
- 例
 - `https://server.dns.name/c=gb/o=University%20of%20Kent/cn=David%20Chadwick/` (証明書)
 - `https://server.dns.name/c=gb/o=University%20of%20Kent/cn=CRLs/` (CRL)

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。

PKI Disaster Recovery and Key Rollover

- 内容
 - 例外的な状況からの復旧方法
 - プライベート鍵の危殆化(漏洩など)や喪失
 - CRLリポジトリに対するDoS
 - 認証局のキーロールオーバー(新しい鍵ペアへの切り替え)の方法
- 検討と記述の対象
 - エンドエンティティ、認証局、Revocation Authority、Attribute Authority、Time-Stamp Authority、CRL Repository
- 今後の進め方
 - individual draftからWG draftへ変更し、PKIX WGページから迎れるようにする。WGでの承認後、活動計画に入れる。

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。

Problem Statement(1 / 2)

- Problem statement
 - draft-wallace-ta-mgmt-problem-statement-01
- 問題点
 - trust anchor storeを管理する標準化された方法が存在しない
 - リモートでの管理は難しい
 - アプリケーションに特化されたものはある
draft-ietf-dnsexp-trustupdate-timers
 - 自己署名証明書があってもtrust anchorの管理手法には直結しない

ここで言われているTrust Anchorとは

- 関連付けられた情報を持つ、信頼された公開鍵
 - rfc3280での意味: 証明書パス検証の為に、公開鍵に関連付けられた発行元、公開鍵アルゴリズム、公開鍵、オプション等
- 証明書のパス検証、署名付きオブジェクトの検証に使われる。署名付きオブジェクト(ファームウェア、タイムスタンプ、OCSPレスポンス、鍵など)

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。

Problem Statement (2 / 2)

- 提案の目的
 - trust anchor storeを管理するプロトコルを提案 (add/remove/query)
 - out-of-bandの信頼メカニズムへの依存を減らすことが目的
- 機能について(1)
 - トランスポートとの独立、アプリケーションによるセッション管理
 - trust anchorを意識させない、または意識しないデバイスなどのサポート
 - trust anchor storeの転送
 - trust anchorの初期登録以外での、out-of-bandによる検証 (fingerprintの確認)を減らす
- 機能について(2)
 - trust anchor storeの内容を示す書式の標準化
 - disaster recoveryのサポート
 - trust anchorのauthority : trust anchor storeの管理に使われる
 - trust anchor managerをtrust anchorとするdelegationの実現

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。

TAM BoFにおけるディスカッション

- BoFの目的 (Tim Polk氏の考え)
 - WGを作るのではなく、problem statementの共有、constituency(関心の度合いを測る or 関心を上げる)こと
- 会場での議論内容
 - プレゼンに関する指摘
 - ユーザの観点とインタラクションが欠けているという指摘
 - trust anchor managerの対象とする範囲が何か
 - 議論のスコープ
 - "ブラウザのtrust anchorをこの議論に含めるかどうか"
 - ブラウザ以外で証明書を使う機器について議論することの重要性が指摘された。APNICのTerry氏からはリソース証明書の話もあった。
 - チャーター作成と今後の活動に関する議論
- 今後の進め方
 - 次回のIETFまでに議論の目的や意味をMLで議論
 - 議論の状況に応じてWG趣意書を作成

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。

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

- **Public-Key Infrastructure (X.509) WG**
 - 2007/12/3 13:05-15:05、50名程
 - Agenda
 - WG Status and Direction
 - PKIX WG Specifications
 - Certificate and Certificate Revocation List Profile (3280bis)
 - Certificate Management Messages over CMS
 - Subject public key info resolution for ECC
 - OCSP Algorithm agility
 - Related specifications and Liaison Presentations
 - Liaison statements received from ITU-T SG17
 - Trust Anchor Management Protocol (TAMP)
 - Updating ASN.1 modules to 1998 syntax
 - Credential selection - Mainly a PKI problem (時間がなく中止)
 - Resource Discovery Protocol

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。

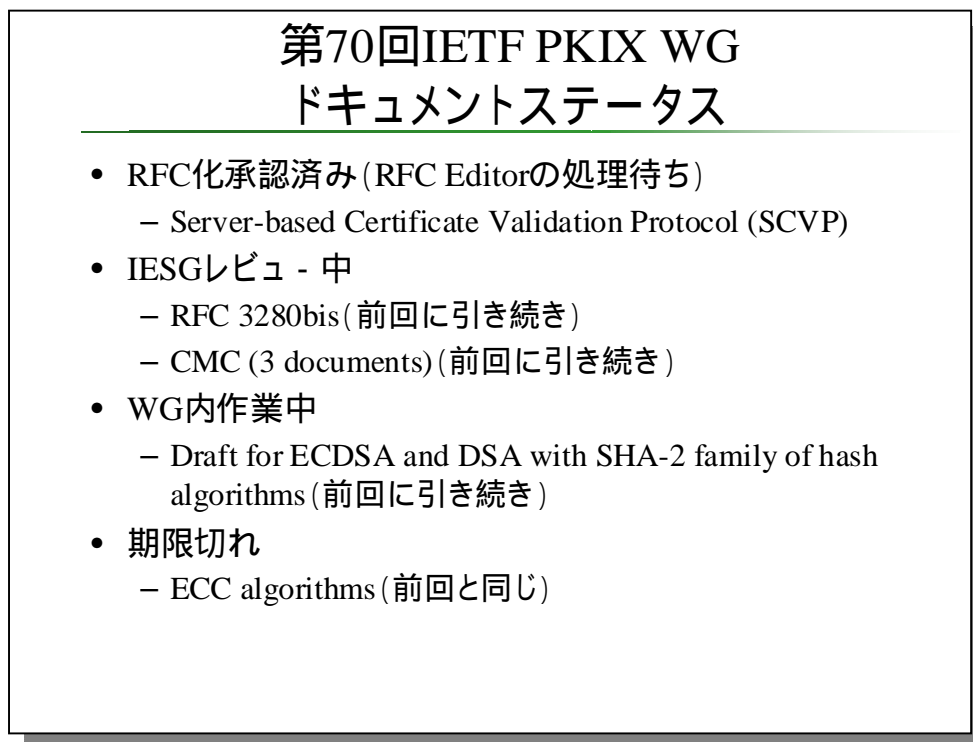


図 3-10 第70回 IETF PKIX WG ドキュメントステータス

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)。

PKIX WGにおける議論(1 / 4)

- Subject public key info resolution for ECC
 - デザインチーム・ジェネレーション2にてECC (Elliptic Curve Cryptography – 楕円暗号)の証明書での扱いについて議論中。第二レポートを12月に。
 - 方法の選択{RFC4055 / X9.62-2005} RFC4055に基づく方式にした。

- OCSP Algorithm agility
 - draft-hallambaker-ocspagility-00.txt
 - 方式の提案:
 - オプションとして署名アルゴリズムを選べるようにする、もしくはクライアントにサポートするアルゴリズムを伝える
 - MLで議論を継続

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、RFC4055⁵の方式か X9.62-2005⁶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>

PKIX WGにおける議論(2 / 4)

- Related Specifications and Liaison Presentations
 - Liaison statements received from ITU-T SG17
 - ITU-TにPKIX WGがコメントを求められた
 - streetAddressに upper boundを設けないこと。unbound文字列を設ける必要があり、多くのプロトコルが影響を受ける。
 - bufferoverflowの危険性を挙げるため、何もしないことを提案。
 - CAの名前が重複することを避ける仕組みをどうするか。
 - “no responsible and no mechanism” という主旨で答えることを提案。

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。

PKIX WGにおける議論(3 / 4)

- Trust Anchor Management Protocol (TAMP)
 - 前回 (IETF-69) TAM BoFでWG設立が諦められた TAMの仕組みを、ProtocolとしてPKIX WGの Working Itemに入れることを提案。
 - MLにて議論継続
- Updating ASN.1 modules to 1988 syntax
 - 多くのASN.1モジュールは1988年版ASN.1に則っている。新版の書式に変えていくことを提案。
 - 1998年版、2002年版 ASN.1は"ANY"(多くのモジュールで使われている)を許容していないが、コンパイラが自動的にチェックすることが可能。
 - 現行のモジュールに変更はない。
 - 議論:LTANSのTobias氏が、der/ber問題を指摘

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。

PKIX WGにおける議論(4 / 4)

- Credential selection - Mainly a PKI problem
 - <http://www.ietf.org/internet-drafts/draft-santesson-credsel-01.txt>
 - 時間がないため中止

- Resource Discovery Protocol
 - 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
 - MLで議論し、strow pollが出される

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

第4章 IPアドレス認証の展開に関する 調査研究

内容

- 経路情報の登録機構のポイントとディスカッション
- 経路情報の登録機構の実験と改修
- 経路情報の登録機構の応用

ほか

4. IP アドレス認証の展開に関する調査研究

平成 14 年度から平成 16 年度にかけて、「IP アドレス認証局」と呼ばれる認証局に関する調査研究を行った¹。「IP アドレス認証」という言葉は、この時に作られた言葉である。

JPNIC は日本国内で唯一、IP アドレスの登録管理業務を行うための組織「インターネットレジストリ」である。IP アドレスはインターネットにおけるホストの識別子であることから、認証技術と組み合わせることで様々なセキュアネットワークサービスが考えられる。IP アドレス認証の調査研究が開始した当時は、その様々なセキュアネットワークサービスのあり方を考える調査研究活動を行った。この中で軸として考えられていたのは、JPNIC において信頼点となる認証局、ルート認証局を立ち上げることである。この認証局の立ち上げについては、2002 年度から 2004 年度にかけて調査研究が行われた。

しかし、認証局を運用するということは、事業の方向性について検討を要するほどに影響のあることであった。認証局は「電子証明書」を発行する機関であるが、その電子証明書で「証明される」内容は、予め証明に足る情報であることが確認されていなければならない。証明に足らない情報を証明しても、単に情報伝達に電子証明書という仕組みを作るだけになってしまい、その仕組み作りが目的化しかねない。そこで、JPNIC という IP アドレスを管理する組織が、どのような情報の証明を行い、それがどのように使われていくべきかを考える必要がある。

ところで、先に述べた IP アドレスにはホストの識別子の他に、もう一つの役割がある。経路制御（ルーティング）の識別子である。ここではインターネットルーティングの詳細は述べないが、IP アドレスの登録管理業務は必然的にルーティングにも影響してしまう。例えば、あるネットワーク利用組織から IP アドレスの返却があるとき、そのネットワーク利用組織は、インターネットにおける経路情報を失わなければ、IP アドレスを使わない状態になったとは言えない。逆に、インターネットにおける経路情報さえあれば、IP アドレスの割り振りを受けていなくても IP ネットワークの到達性を得ることが技術的に可能である。

本調査研究の結果、「IP アドレス認証」は JPNIC における登録情報を不正な書き換えから守り、そして登録情報を正常なインターネットルーティングに役立てるような仕組みになった。JPNIC 認証局は、IP アドレスの割り振りを受け、その IP アドレスに関する情報を JPNIC に登録するユーザの認証と、JPNIC における IRR (JPIRR) に、経路情報を登録するユーザの認証と認可を実現するための電子証明書を発行することとなった。

2007 年度は、経路情報を登録するユーザの認証と認可を実現する「経路情報の登録機

¹ JPNIC 認証局 受託研究の報告書
<http://www.nic.ad.jp/ja/research/ca/>

第4章 IP アドレス認証の展開に関する調査研究

構」の実験運用を開始し、国内外における発表と議論を重ねることとなった。実験システムである為、JPNIC において全面的な導入を図るなどの利用者増は望めなかったが、利用者からのフィードバックを得ることができた。また他の地域（アメリカやヨーロッパ、アジア太平洋地域など）のレジストリの取り組みを現地調査し、比較検討することで、インターネットレジストリにおける経路制御への関与が、どういう意味を持つかがわかった。

本章では、IP アドレス認証の展開に関する調査研究の一環として行った経路情報の登録機構の開発と、国内外でこれについて発表と議論を行ってきた結果について述べる。

4.1. 経路情報の登録機構の開発と調査研究

IP アドレス認証の展開に関する調査研究では、「経路情報の登録機構」を開発し、国内外での発表および議論と、実験運用を行った。経路情報の登録機構は、JPIRR(JPNIC で運用されている Internet Routing Registry) の登録情報の正当性を維持するシステムである。

2008 年 3 月の段階でエンドユーザとしての利用実験に参加したのは 4 社で(この他に利用可能なユーザは 6 社以上) あった。

また APNIC や IEPG などの国際会議で発表や、JANOG 等での発表を通じて、本機構で向上する IRR の信頼性や課題点に関する議論を行うことができた。重要性の高い課題点については改修を行い対策を取った。

4.2. 経路情報の登録機構を使った実験の考え方

経路情報の登録機構を使った実験は、いくつかの段階に分けて行われるものとした。

実験の考え方

- 第一段階 (参加者による実施)
 - 許可リストを利用してIRRのオブジェクトを管理できることを確認する
 - 実験用IRR利用
 - 不正なrouteオブジェクトの登録ができないことを確認
 - 「正しい」routeオブジェクトを試験的に蓄積
- 第二段階 (主にJPNICによる実施)
 - JPIRRに登録されたオブジェクトとの比較、分析
 - 実験用IRRとJPIRRの両方を利用
 - 不適切なオブジェクト(JPIRR)または不適切な認可(経路情報の登録認可機構)を分析、対策手順を検討
- 第三段階
 - JPIRRへの適用
 - JPIRRを利用
 - 適切なrouteオブジェクトを蓄積
- 第四段階
 - JPIRRを用いた経路ハイジャックの検知 など

図 4-1 実験の考え方

第一段階の実験は、登録者による利用実験である。本機構は IP アドレス管理業務を行っているものに利用されることが実験である。業務の中にうまく組み込むことが可能かどうかの検証を行う。それに先立って割り振られた IP アドレスが、他の組織によって経路情報として不正に登録されることを避けられることが理解される必要がある。

第二段階の実験は、データ分析である。本機構によって正当性の担保されたデータが蓄積されると、既存の IRR における不適切なオブジェクトが判別できるようになる。その原因や対策を検討する。

第三段階と第四段階は、実際に JPIRR に本機構を提供し、ルーティング業務において利用する実験である。

4.3. 経路情報の登録機構とは

経路情報の登録機構(以下、本機構と呼ぶ)は、インターネットにおける経路制御の安全性向上のため、JPIRR で提供される経路に関する情報(route オブジェクト)の正当性の向上と維持を図るシステムである。本機構を使うことで、自組織以外のネットワークによる route オブジェクトの不正登録(設定ミスを含む)を防ぎやすくなる。JPIRR における登録情報を使ったインターネット上の不正な経路情報を、より正確に検知できるようになり、経路ハイジャックの予防等に役立つと考えられる。

第4章 IP アドレス認証の展開に関する調査研究

本機構の三つのポイントを以下に示す。

- ポイント1 - 割り振られた IP アドレスが経路広告で使われる組織の指定
- ポイント2 - JPIRR のオブジェクト登録者に対するユーザ認証の強化
- ポイント3 - 認可登録に基づいた JPIRR への route オブジェクトの登録制限

これらの仕組みを実現するため、本機構は JPNIC で運用されている JPNIC 認証局、IP レジストリシステム、JPIRR の三つと連携する。本機構がどのようにこれらのシステムと連携動作するかを図 4-2 に示す。

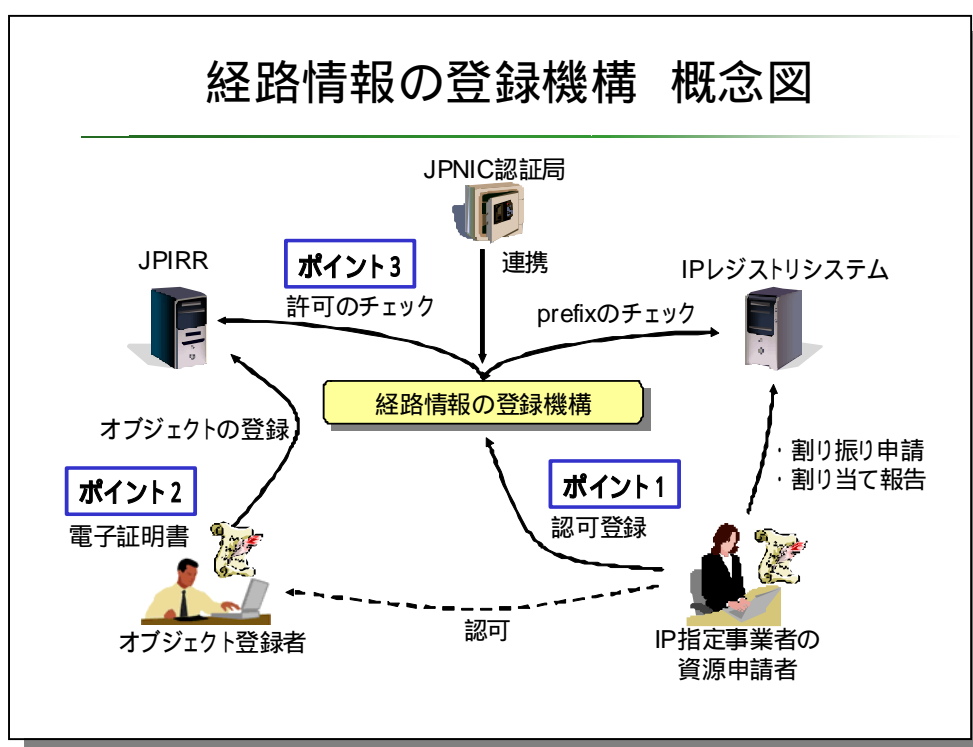


図 4-2 経路情報の登録機構 概念図

IP レジストリシステムは、IP アドレス管理指定事業者（以下、IP 指定事業者）による IP アドレスの割り振り申請や割り当て報告などのために使われているシステムである。「Web 申請システム」と呼ばれる申請用のシステムは、IP レジストリシステムによって提供されている。一方、JPIRR は AS 番号が割り振られている個人またはネッ

トワーク運用組織のオブジェクトの登録のために使われている。

本機構は、IP 指定事業者に割り振られている IP アドレスに関する情報を IP レジストリシステムから取得し、JPIRR に登録される route オブジェクトの IP アドレスが正当なものであるかどうかをチェックする。ここでいう正当性は、IP アドレスが IP 指定事業者に割り振られているか、ということに加え、割り振り先の IP 指定事業者から、JPIRR のオブジェクト登録者であるメンテナーに対して、その登録が認可されているかどうか、という意味である。この正当性の確認のため、本機構は許可リストと呼ばれるデータベースを持ち、IP 指定事業者に対して認可登録の Web インターフェースを提供する。

以下、各々の仕組みについて説明する。

ポイント 1

一つ目は、IP アドレスを割り振られた IP 指定事業者がその IP アドレスの利用をネットワーク運用組織に認可するための、「許可リスト」と呼ばれるデータベースである。

本機構は、IP 指定事業者が認可登録を行うデータベース「許可リスト」を提供する。許可リストは、IP アドレスがどのメンテナーに利用されるかを示すリストで、どのメンテナーがどの IP アドレスを含む route オブジェクトの登録ができるか、という情報を持つ。許可リストで認可登録のできる IP アドレスは、その認可を行おうとしている IP 指定事業者に割り振られた IP アドレスのみである。さらに認可登録の追加項目として、AS 番号を指定することもできる。これによりインターネットにおいて特定の AS から経路広告が行われるような認可登録ができる（図 4-3）。

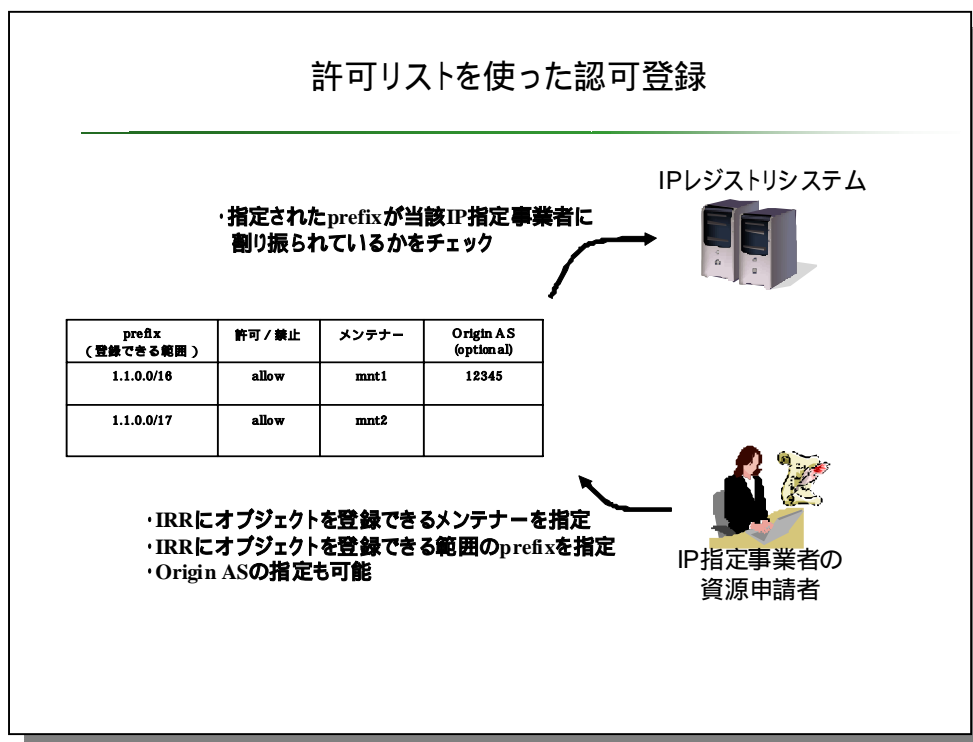


図 4-3 許可リストを使った認可登録

ポイント 2

二つ目は JPIRR におけるオブジェクト登録者に対するユーザ認証に、電子証明書を使う点である。

本機構では、JPIRR における情報登録者を、「メンテナー管理者」と「オブジェクト登録者」という二種類のユーザとして認識する。メンテナー管理者は JPIRR のメンテナーオブジェクトで admin-c や tech-c として登録されているユーザで、次に述べるオブジェクト登録者の電子証明書を管理できる。オブジェクト登録者は、JPIRR に route オブジェクト等の登録ができるユーザである。どのユーザも本機構から発行されたユーザ向けの電子証明書(クライアント証明書)を使ってアクセスする。本機構が提供するクライアント証明書を使うことで、これまでの認証方式であるパスワードや PGP に比べ、ユーザの管理を適切に行いやすくなる。本機構が持つ電子証明書の管理機能は、悪意のある第三者による成りすまし行為が起こった場合に、証明書を即時に失効させるなどの事後の対策を取りやすくしている(図 4-4)。

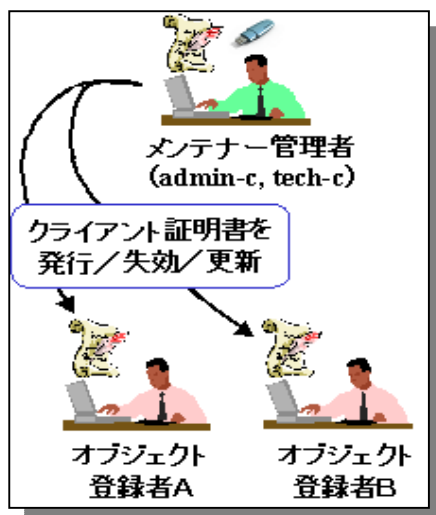


図 4-4 ユーザの違いと役割

メンテナー管理者は JPIRR のメンテナーオブジェクトを管理できるユーザで、メンテナーオブジェクトの内容を編集できる。またオブジェクト登録者のクライアント証明書を発行/失効/更新を行うことができる。オブジェクト登録者のクライアント証明書は認証トークンに入っており、この認証トークンを使って、これらの管理業務を行う(図 4-5)。

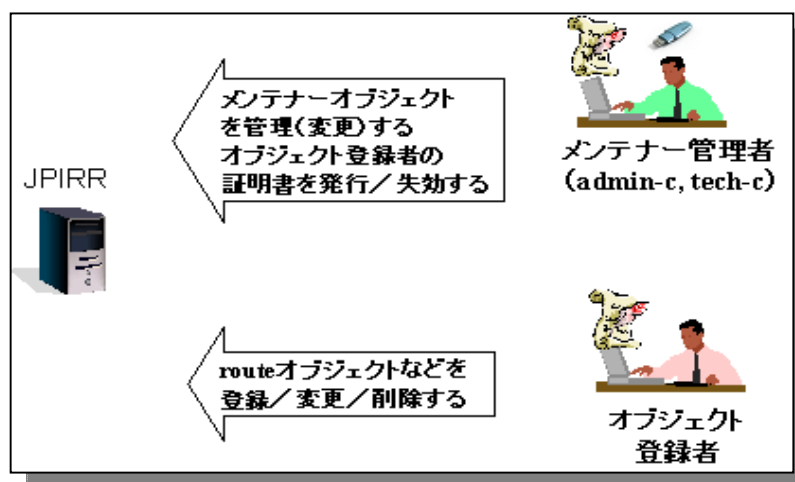


図 4-5 ユーザ毎の登録業務の違い

ポイント3

三つ目は、許可リストを使った、JPIRR でのアクセス制御である。許可されたメンテナーだけが、特定の IP アドレスを含む route オブジェクトを JPIRR に登録できるようになることである。

第4章 IP アドレス認証の展開に関する調査研究

本機構は JPIRR に route オブジェクトが登録される際、申請データの内容を許可リストに基づいて検査し、JPIRR に登録するか登録を拒否するかの制御を行う。IP 指定事業者によってメンテナーが指定されていない IP アドレスなどが、JPIRR に登録されることを防ぐ(図 4-6)。

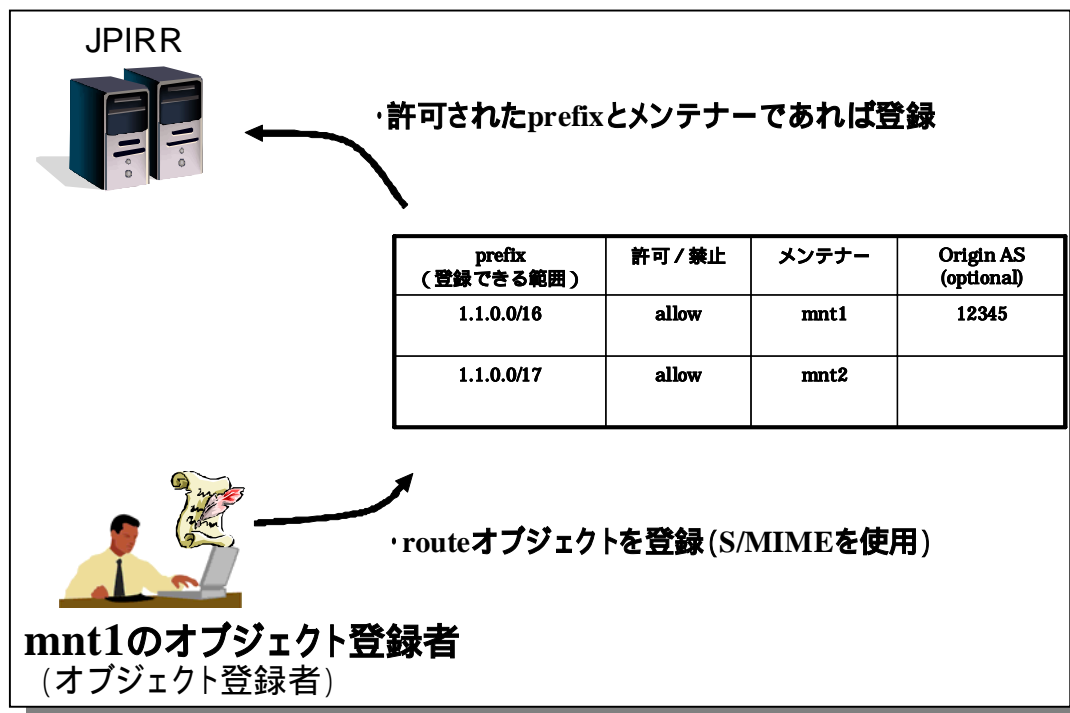


図 4-6 route オブジェクトに対するチェック

本機構を通じて route オブジェクトの正当性を維持することで、JPIRR に不正な route オブジェクトが登録されることを防ぐことが可能になる。この仕組みが適切に運用されれば、JPIRR が、経路ハイジャックの検知等に一層役立つと考えられる。

4.4. 経路情報の登録機構を使った IP アドレス関連の業務

経路情報の登録機構は、いわば IP アドレスの管理とインターネットルーティングの業務を連携させるシステムである。IP アドレスの管理という観点では、インターネットに接続するネットワークの管理業務において、IP アドレスに関わる業務は大きく分けて 3 つある(図 4-7)。

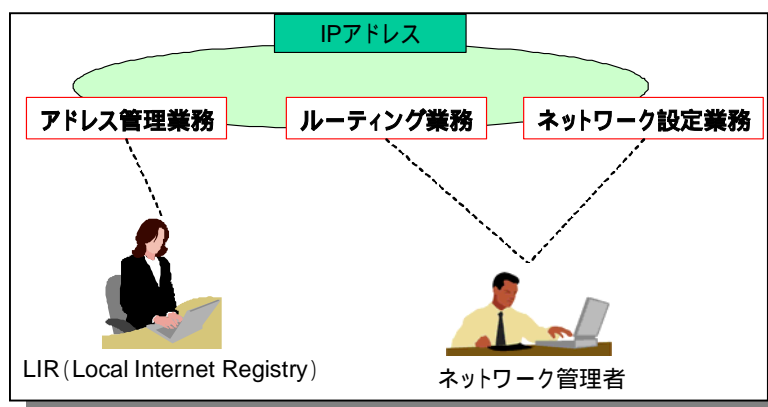


図 4-7 IP アドレスに関連する 3 つの業務

一つ目は IP アドレスの割り振りを受けそのアドレスを管理する業務(アドレス管理業務)である。LIR(主に IP 指定事業者)がその役割を担っている。二つ目は割り当てられた IP アドレスからインターネットルーティングのためのネットワークの設計を行う業務(ルーティング業務)である。これはネットワーク管理者が行っている。三つ目は到達性が確保された IP アドレスをネットワーク機器に設定し、ユーザの接続性を確保する業務(ネットワーク設定業務)である。ネットワーク設定業務もネットワーク管理者によって行われる。ここでネットワーク設定業務を二つに分けた理由は、ルーティング業務とネットワーク設定業務を行う会社や部署が異なるケースが多いためである。

本機構は、このうちアドレス管理業務とルーティング業務を結びつける役割を持っている。ネットワーク設計業務とルーティング業務は、IP アドレスの観点では密接に連携しており、ルーティングの設定が行われていない IP アドレスをネットワーク設定業務で使うことは、インターネットの接続性という観点では直接的には意味がない。

一方、アドレス管理業務とルーティング業務では、特に今日のように ISP の業務細分化が進んでいると、IP アドレスに関する業務の関連性が失われがちである。例えば、ある ISP が IP アドレスの割り振りを受け、ISP 事業で使う際、ルーティング業務を行っている ISP 事業者はそのアドレスの経路広告を委託することがある。この場合、一見割り振られた IP アドレスとインターネットルーティングが一貫性を持っているように見えるが、実はそうではない。他の ISP が IP アドレスの打ち間違いなどを起こしても、IP アドレスの割り振りを受けている事業者にはそのことがわからない。つまり IP アドレスの割り振り先と、ルーティング業務を行う事業者が一方向かつ疎な関係にあると言える。

アドレス管理業務を行っているものとルーティング業務を行っているものが、IP アドレスの利用において密な関係を持つにはどのようにすればよいのか。本調査研究では、許可リストと呼ばれる、ルーティングで IP アドレスを用いる組織を指定する仕組みを提供することにした。こうすることで、割り振りを受けている組織が、意図しない他の組

第4章 IP アドレス認証の展開に関する調査研究

織によって IP アドレスを利用されてしまったときに、それがわかるようになる。そして許可リストに則った経路の情報は、IRR に格納されるものとした。

ルーティング業務では、不適切な IP アドレスの利用、すなわち不適切なルーティングの情報は、経路フィルターと呼ばれる仕組みを使って防がれている。経路フィルターとは、予め不適切とわかっている IP アドレスの経路情報がルータに伝わってきたときに、それをフィルター（遮断）し、ルータの経路制御処理が適切に行われないようにする仕組みである。経路フィルターは特定の Web ページで公開されている、BOGON リストと呼ばれる「経路広告には不適切な IP アドレスのリスト」を使って実施されたり、IRR を使って実施されたりしている。すなわち、ルーティング業務においては、BOGON リストや IRR が、経路情報の正しさを示す指標として考えられている。

4.5. 許可リストを使った IP アドレス管理業務

許可リストを使った IP アドレス管理業務は、割り振り申請や割り当て報告を行った IP アドレスを許可リストに登録するという手順で行われる。許可リストは、IP アドレスが登録されるリストであり、次の節で述べる IRR への登録業務の中で使われる。

図 4-8 は、JPNIC で実験的に運用されている IP アドレス認証局と、経路情報の登録機構を使った、IP アドレス管理業務の手順を示したものである。

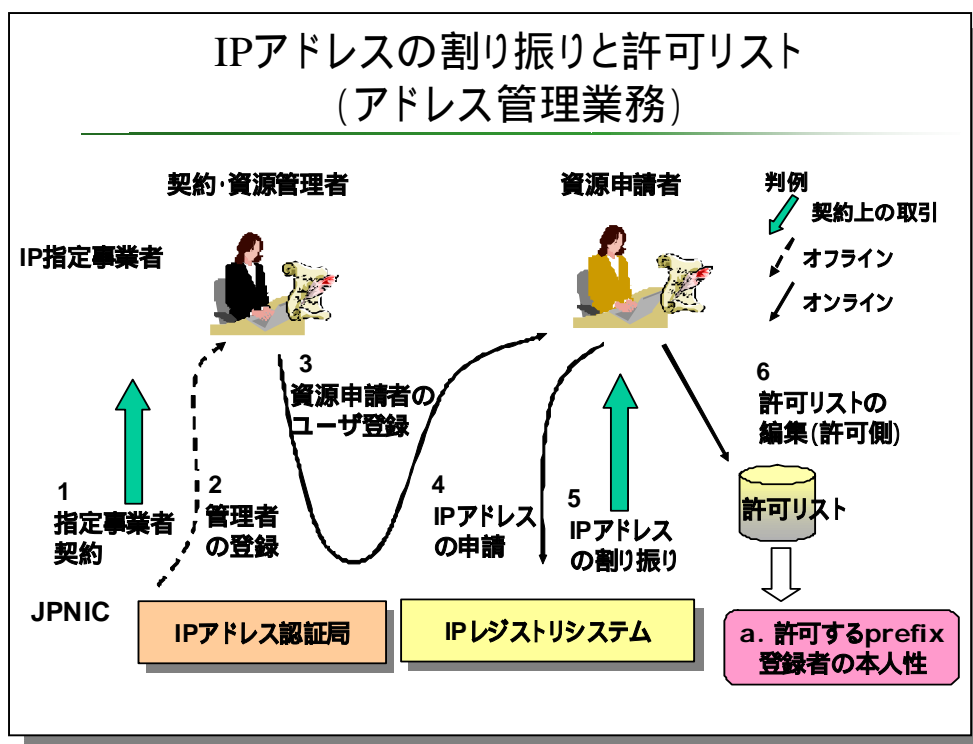


図 4-8 IP アドレスの割り振りと許可リスト

図 4-8 中の矢印は、業務が実施される順番である。はじめにレジストリから IP アドレスの割り振りを受け、IP アドレス管理業務を行うための「指定事業者契約」を結ぶ。これは一度行われてしまえば、その後の IP アドレスの各種申請において逐一行われるものではない。JPNIC 認証局 (IP アドレス認証局) は、この段階で IP 指定事業者の「契約・資源管理者」に電子証明書を発行する (1、2)。契約・資源管理者は、IP 指定事業者の契約情報や資源管理情報を登録・変更・削除できるユーザである。実際の IP アドレスに関する各種申請は「資源申請者」によって行われる。資源申請者は、契約・資源管理者によってユーザ登録される (3)。IP アドレスの申請は資源申請者が担当して実施される (4、5)。最後に割り振られた IP アドレスについて許可リストに登録する (6)。

許可リストへの登録の段階で重要なのは二点である。一つ目は prefix が資源申請者の属する IP 指定事業者に割り振り済みであり、二つ目は登録を行った資源申請者の本人性が確認されていることである。一点目は、許可リストへ登録される段階で、割り振り / 割り当て情報を持つ IP レジストリシステムと照合することで確認される。二点目は、IP アドレス認証局の電子証明書を使って本人性が担保される。

許可リストに登録された prefix は JPIRR への登録の段階で使われる。

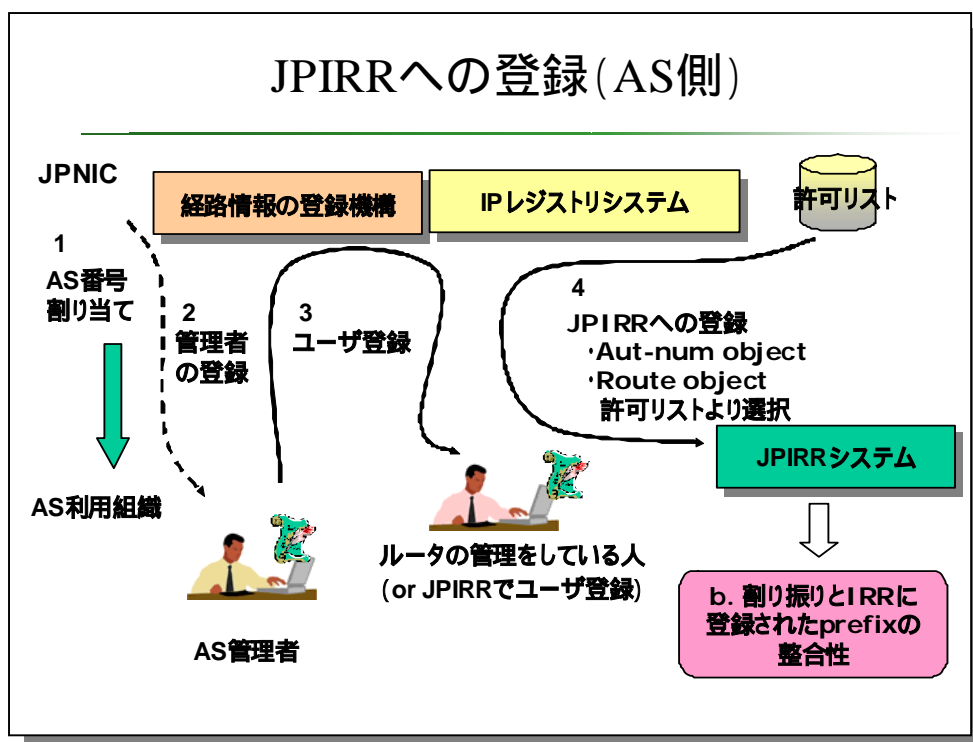


図 4-9 JPIRR への登録 (AS 側)

インターネットにおける BGP を用いたルーティング業務には、AS 番号が必要である。予め AS 番号の割り当てを受けておく必要がある (1)。経路情報の登録機構は、AS 番号の割り当て先の管理者「AS 管理者」に電子証明書を発行する。AS 管理者は資源申請者と同様に、JPIRR に登録業務を行うユーザに電子証明書を発行する (2、3)。このような仕組みは、JPIRR に情報登録を行うユーザが、業務管理を行う AS 管理者とは地理的に離れているケースがあり、またルーティング業務が会社のある場所と離れたデータセンターで行われることなどを考慮して設計された。最後に、JPIRR に情報登録を行う際、許可リストを使って登録データの確認が行われ、問題がなければ JPIRR システムに登録される (4)。ここでいう確認は、route オブジェクトと呼ばれる登録データに含まれる、AS 番号と prefix である。この AS 番号と prefix が、前節で述べた登録内容と齟齬がある場合、経路情報の登録機構は JPIRR への登録を行わせないようにする。これにより、IP アドレスの割り振り先が、その IP アドレスがインターネットルーティングの中でどのように使われるかを指定 / 制限することができる。具体的には意図しない AS から自組織に割り振られた prefix がインターネットで経路広告されたとき、JPIRR の登録情報と比較することで、それが不適切な経路情報であることがわかる。

4.6. 経路情報の登録機構の利用実験

本節では 2007 年度に行った経路情報の登録機構の利用実験について述べる。

4.6.1. 利用実験の考え方

2007 年度に行った利用実験は、図 4-1 に示した四つの段階を想定して行った。第一段階は、許可リストを利用して IRR のオブジェクトを管理できることを確認することである。これは LIR が、割り振られた IP アドレスのルーティングの上での制御ができるようになる、という概念を実際の操作を通じて体験してもらうという実験である。同時に 2006 年度に開発した本システムに関して利用上の不具合があれば挙げてもらうことも行った。

4.6.2. 利用実験の手順

第一段階の利用実験については、Web ページにて手順書を公開した²。この手順書で示した手順を以下に示す。

- 1、LIR の IP アドレス関連の申請担当者は、自組織に割り振られた IP アドレスを確認する。(資源申請者の操作)
- 2、許可リストを操作し、割り振られた IP アドレスを特定のメンテナーに許可する登録を行う。(資源申請者の操作)
- 3、ルーティング業務を行っておりメンテナーの管理を行っているものは、IRR にオブジェクトを登録する担当者「オブジェクト登録者」の証明書を発行する。(IRR のメンテナー管理者の操作)
- 4、オブジェクト登録者は、許可リストの範囲に入っている IP アドレスと入っていない IP アドレスを、各々 route オブジェクトに登録する。(IRR のメンテナー管理者の操作)

最後に許可リストの設定を通じて、IRR への route オブジェクトの登録に関する制御を意図通りに行われたことを確認する。確認の結果は、手順書の最後にあるチェックシートに記録する。

4.6.3. 利用実験の参加状況

利用実験には IP 指定事業者である 4 社が参加した。この 4 社は、資源申請者の証明書だけでなく、IRR のメンテナー管理者のトークンを取得した。利用者からのフィードバックは、主に電子メールを通じて得られた。

² 経路情報の登録認可機構 実験手順書

<http://www.nic.ad.jp/ja/research/ca/routerreg-outline/routerreg-testing-guide-05.pdf>

4.6.4. 利用実験のフィードバック

利用者からは、意図通りの操作ができたことを示す報告があったが、経路情報の登録機構のインターフェースに関する意見はほとんどあがらなかった。

メンテナ管理者のトークンを利用するための技術的な問い合わせがほとんどであった。その中の代表的なものを以下に示す。

利用者からの問い合わせ

「USB トークンを指したままオブジェクト登録者の証明書を取得すると、Web ブラウザではなく USB トークンの方にその証明書がインストールされてしまう。これは技術的な仕様であるか？」

「USB トークンのドライバのインストールはできたが、トークンを使うことができなかった。(以下、利用環境に関する問い合わせなど)」

その他に画面を見せるなどして複数の事業者と情報交換を行った。それらの事業者からは、以下のようなフィードバックがあった。

「許可リストの編集画面で、割り振り済みの IP アドレスを指定する必要があるが、自社は割り振り済み IP アドレスが多く、すべてを常時把握しているわけではない。割り振り済みの IP アドレスを表示するような補助機能が欲しい。」

「メンテナの管理者は、IRR における admin-c であるが、tech-c であることもある。tech-c として登録されている利用者もメンテナ管理者になれるようにして欲しい。」

「許可リストにある IP アドレスの検索機能を充実させて欲しい。検索の際に more specific や less specific といった指定ができるようにして欲しい。」

利用者からの USB トークンに関する問い合わせについては、個別に環境を聞いて対応策を調整するなどした。また上記のフィードバックのうち、経路情報の登録機構の改修が必要なものについては、一旦すべての要件をまとめ、2007 年度中に改修するものとした。

4.7. 経路情報の登録機構の改修

2007年度の調査研究では、経路情報の登録機構の改良を行った。前節までに述べた経路情報の登録機構を使った業務の見直しを行ったが、基本的な業務フローは変更の必要がないことがわかった。一方で、許可リストを操作する画面がIPレジストリシステムのWeb申請システムとは別であることから、利便性が損なわれている状況であった。

2007年度の経路情報の登録機構の改良点を以下にまとめる。

2007年度 経路情報の登録機構の改良点

1. 本機構における割り振り済みアドレス空間の一覧表示

IP指定事業者は割り振られたIPアドレスの空間を把握しながら、本機構を操作する必要があるが、現行のシステムはその情報が表示されない。該当IP指定事業者に割り振られたIPアドレスを表示するように改善する。

2. Windows Vista 対応

Windows Vista では電子証明書に関わるデフォルト機能の仕様に変更があり、本機構で提供している証明書発行機能が利用できない。Windows Vista は普及しつつあるOSであるため、これに対応する。

3. ミドルウェアのアップデート

本機構のプログラムが利用するミドルウェアの不具合を避けるため、アップデートを行う。

4. 証明書発行用アクセスキーのメール通知機能

本機構は、証明書発行の処理を行った後、画面に表示されるアクセスキーの全体を証明書発行対象者に伝達する必要があり、業務が行いにくい。アクセスキーがメールで送られるように改善する。

5. 画面フローの改善および多国言語対応によるユーザビリティの向上

表示される画面の数を減らすと共に、Web ページ表示機能を改善し、ユーザビリティ向上を図る。また本機構は英語圏の技術者にも動向が注目されていることから、英語等での表示ができるようにし、わかりやすさの向上を図る。

6. 許可リスト検索機能の改善

許可リストの検索の項目および表示を変更し、ユーザビリティ向上を図る。

7. 本機構経由で登録されたオブジェクトの識別

本機構を経由して登録されたオブジェクトを識別する仕組みについて、概要設計を行う。

8. 割り振り済みアドレス空間のリアルタイム反映

本機構の許可リストに、割り振り済みアドレス空間をリアルタイムで反映する仕組みについて、概要設計を行

第 4 章 IP アドレス認証の展開に関する調査研究

う。

9. ユーザの利用状況確認 Web インターフェース

ユーザの利用状況を確認する Web インターフェースの仕組みについて、概要設計を行う。

1 の「本機構における割り振り済みアドレス空間の一覧表示」は、経路情報の登録機構の資源申請者がアクセスする Web ページの改良である。許可リストには自組織に割り振り済みの IP アドレスを登録しなければならないが、ユーザは許可リストの編集画面で割り振り済みアドレスを確認することができない。この点の指摘に対してシステムの改良を行う為、経路情報の登録機構が IP レジストリシステムから割り振り済みの IP アドレスの情報を取得し、一画面で割り振り済みアドレスと許可リストを確認しながら、編集ができるように改良した。

2 の「Windows Vista 対応」は、新しい OS である Windows Vista への対応である。Windows Vista に付属する Internet Explorer バージョン 7 では、ユーザ側の鍵生成機能の仕様に変更があることが、2007 年度の後半に判明した。Windows Vista の普及状況を踏まえて今回の改良では、Windows Vista 以前の OS と Windows Vista の両方の Internet Explorer に対応することとした。これは Web サーバ側で通知を受けた、Web ブラウザのバージョン情報に基づいて表示する Web ページを切り替えるだけでよい。しかし Windows Vista は、これまでに使われていた Xenroll から ActiveX の Cenroll が使われるようになり、Cenroll では以前のバージョンで鍵生成を行うことができないことがわかった。

3 の「ミドルウェアのアップデート」は Web サーバのソフトウェアを含むバージョンアップである。各種ソフトウェアのバージョンアップはセキュリティパッチの適用などを踏まえると定期的に行われるべきものである。今回のバージョンアップでは、IP レジストリシステムとの連携上の問題が起こらないかどうかの調査を並行して進めながら行った。

4 の「証明書発行用アクセスキーのメール通知機能」は資源申請者の証明書発行インターフェースにならった改良である。経路情報の登録機構は JPIRR に情報登録を行うユーザ、オブジェクト登録者の証明書発行の際に、電子メールで「アクセスキー」を通知する機能がない。資源申請者の証明書の場合、契約・資源管理者が証明書発行操作を行うと、資源申請者に対して証明書取得用の URL とアクセスキーの一部がメールで送られる。アクセスキーの残りは契約・資源管理者の画面に表示され、その部分をオフライ

ンで資源申請者に伝えることとなっている。オフラインで伝えることで、契約・資源管理者は資源申請者の本人性確認を行うことができ、本人性確認が行われていない電子証明書発行を防ぐことが可能になる。

5 の「画面フローの改善および多国言語対応によるユーザビリティの向上」は証明書の発行の際に表示される確認画面を減らすと共に、Web ページを英語表記することである。確認画面については、様々な内部処理を経るためにユーザには冗長と思われる Web ページの表示が行われていた。そこでユーザの観点で類似する確認画面を省き、利便性の向上を図った。

また Web ページに表示されるメッセージを英語でも表示できるようにした。これは、国際会議などでデモンストレーションを行ったり、画面を見せて説明を行ったりする際に、日本語の表示だけでは操作の意図が理解されなかったためである。IRR を使うようなルーティング業務は、日本人だけで行われているわけではなく、英語を母国語としていて日本の IRR に登録を行うユーザも想定される。今回の改修では RIR で議論されている IP アドレスの authorize 関連のディスカッションで使われていた用語を用いた。

6 の「許可リスト検索機能の改善」は許可リストの操作上の改良である。許可リストは IP アドレスの列挙である為、編集の際に目的とするエントリを探しにくい。特にルーティングで用いられている IP アドレスの指定方法が利用できなければ、IP アドレス管理業務に携わっているユーザには使いにくい。この検索機能の改良は、大手 ISP のルーティング業務を行っている業務担当者に指摘を受けたものである。具体的には、less specific となる IP アドレスと more specific となる IP アドレスを検索できるようにした。less specific と more specific はルーティング業務の中ではよく使われる概念である。なお less specific では、検索結果に入力した IP アドレスが含まれず、実際には less specific or equal (等しいかより少ない指定) という検索条件とした。more specific についても同様である。

7 の「本機構経由で登録されたオブジェクトの識別」は本機構を使って登録された登録情報 (route オブジェクト) が、JPIRR の中で他の route オブジェクトとは区別される仕組みの概要設計である。本機構を使って登録された route オブジェクトは、割り振りが確認されているなど、他の route オブジェクトとは位置づけが異なる。JPIRR を検索したものが本機構を通じて登録されたものとそうでないものを区別することで、例えば経路ハイジャックの判断の際に役立てることができる。巧妙な経路ハイジャックは、IRR に登録された情報から詐称し、あたかも正しい経路であるかのような状況を作ることができると考えられることから、この機能は重要である。しかし 7 の仕組みを実現するには IRR の書式確認機能に改良を加えたり、IRR の登録情報が伝播していくミラー先の IRR の機能確認を行っていったりする必要がある。これにはより長期的な取り組みが

第4章 IP アドレス認証の展開に関する調査研究

必要である為、今回は概要設計に留まった。

8の「割り振り済みアドレス空間のリアルタイム反映」は本機構のリアルタイム処理に関する機能向上である。2006年度に作られた本機構はIRRに対する情報登録の申請メールを逐次処理することができない。しかしIRRにオブジェクトを登録するものは、whois コマンドを使って逐次登録されたことを確認しながら業務を行っていることから逐次処理ができることは本機構の課題であった。ISPのルーティング業務担当者によって指摘された。しかし、逐次処理には大量の申請を処理できるような性能の設計が必要であるが、プロトタイプシステムではこれを避ける性能を確保することが難しいため、今回は概要設計に留まった。

9の「ユーザの利用状況確認 Web インターフェース」もルーティング業務の担当者より指摘された機能である。(なおIPアドレス認証局(認証)でも同様に機能が要望として上がっている)ルーティング業務の中で、JPIRRへの登録業務を誰が行ったのかを確認する業務がある。現在は申請に使われた電子メールを申請者側で確認することで業務の確認が行われていたが、オブジェクト登録者の管理がWebページを使って行われるようになることから、過去にどのユーザによって申請が行われたかについて、Webページで確認できるようにしてほしいという要望である。この機能改善についても、業務フローなどの検討を要するため、概要設計を行った。

4.8. 経路情報の登録機構の応用

経路情報の登録機構は、IRRにおける登録情報の正当性を保つために、独立して機能するシステムである。しかし本機構の仕様を検討する段階で、いくつかの応用が可能であることがわかった。本機構によって正当性が担保された情報を使って、インターネットにおけるIPアドレスの情報を照合し、不適切なIPアドレスの利用がないかどうかを確認するという応用である。ここでは、実現性が高く一部調整に入っている応用を二つ挙げる。

一つは、国内ISPにおける、経路ハイジャックの検知や予防である(図4-10)。

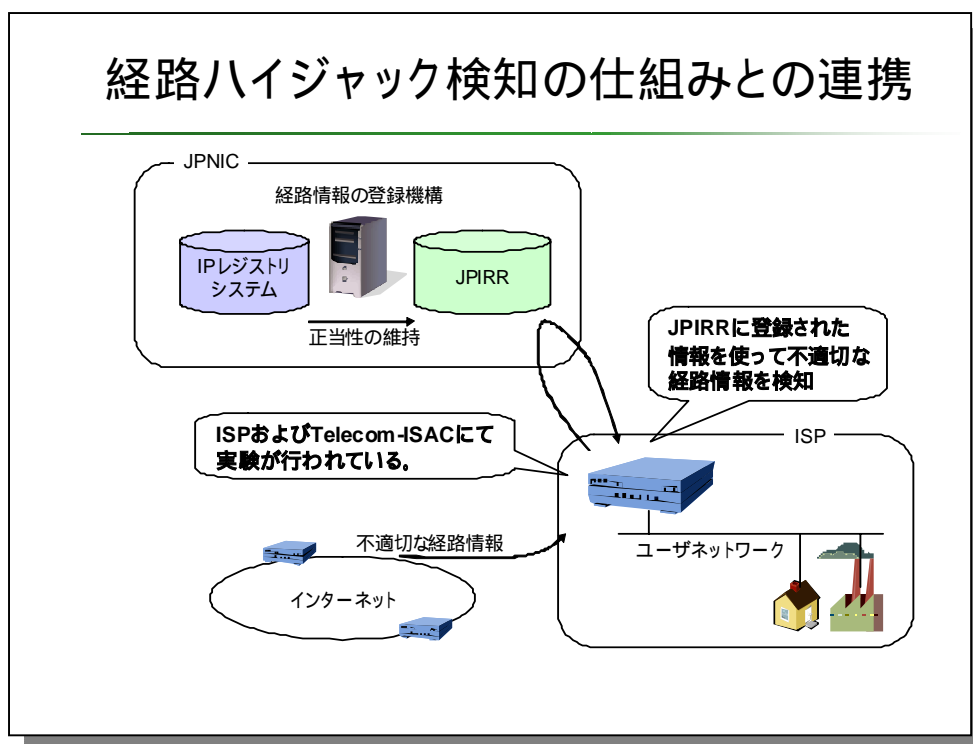


図 4-10 経路ハイジャック検知の仕組みとの連携

経路ハイジャックとはインターネットで交換されている経路情報に不適切な IP アドレスや AS 番号の情報を流すことである。これによって、特定の通信ホストへの成りすましや、盗聴、特定のネットワークに対する利用不能攻撃が可能になる。経路情報の登録機構によって登録された route オブジェクトは、本来使用されるべき、すなわち正しい IP アドレスと AS 番号の組み合わせの情報を IRR で一般に提供できるため、不適切な IP アドレスや AS 番号の利用を検知することが可能である。

もう一つの応用は、リソース証明書³の発行管理システムである。RFC3779 で提案されているリソース証明書は、LIR を含む IP アドレス割り振り先組織において専用の認証局システムが運用されることを想定している。しかしルーティング業務を行っている ISP にとって、認証局の運用業務は本来業務ではなく付帯業務である。しかし認証局の運用は継続性等を踏まえるとルーティング業務と同等かそれ以上の業務負荷を要し、容易に普及することは考えにくい。そこで考えられるのが、IP レジストリシステムもしくは IRR と一体化したリソース証明書管理インターフェースである (図 4-11)。

³ リソース証明書 - IP アドレスや AS 番号の使用権を示す電子証明書。RFC3779 にプロファイル等が定められており、APNIC、ARIN、RIPE NCC で開発が進められている。

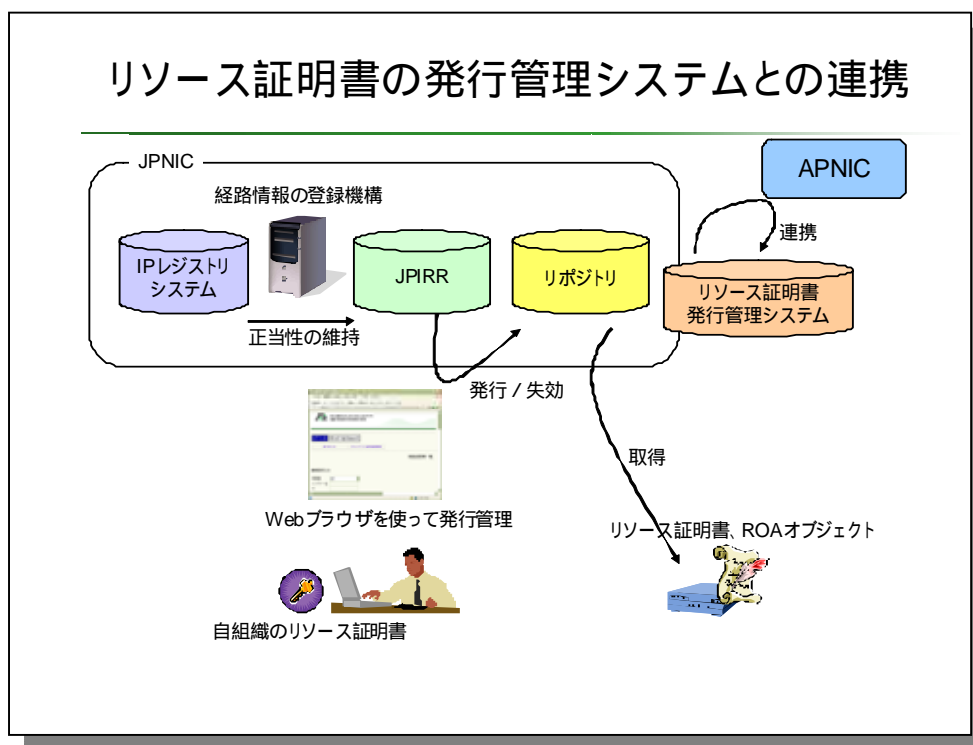


図 4-11 リソース証明書の発行管理システムとの連携

リソース証明書に関する業務の中で管理負荷が比較的高いのは、割り振られた IP アドレスに対するリソース証明書の発行業務や ROA オブジェクト⁴の発行、そしてリポジトリ運用業務であると考えられる。これらは、高い可用性が要されるか高い確実性が要される業務である。図 4-11 で示したシステムはこれらの負荷の高い業務の共通部分を集中化すると共に、リソース証明書システムの共通化を図っている。ISP は自組織のためのリソース証明書と私有鍵、およびリソース証明書発行管理システムにアクセスする Web ブラウザ等のみを持っていればよい。これにより、ルーティング業務に対する付帯業務の負荷を下げ、リソース証明書を扱うための業務負荷を下げる事が可能であると考えられる。

今後、これらの応用について ISP および APNIC との調整を継続していきたい。

4.9. 経路情報の登録機構に関する国際会議での議論

経路情報の登録機構は、IP アドレス管理業務とルーティング業務を結びつける機構である。この根本的な概念は、本調査研究において独自に発想したものではない。ヨーロッパ地域におけるインターネットレジストリの RIPE NCC では、登録情報において

⁴ Route Origination Authorization オブジェクト - IP アドレスがある AS によって経路広告されることを認可したことを示す、構造を持ったデータ。電子署名がついており、その検証にはリソース証明書が使われる。

mnt-route と呼ばれる記入欄を設けることで、同様の概念を実現している。また ARIN では、2006 年度から IP アドレスの割り振り・割り当ての申請書式に OriginatingASList という記入欄を設けることで、IP アドレス管理業務を行う組織が、ルーティング業務を行っている AS の番号を指定できる。これは本機構や RIPE NCC のルーティング業務を行うものを記載するよりも運用の柔軟性は欠けるが、経路ハイジャックのような不適切な IP アドレスの利用を検知できるような、正しいデータを維持するという意味で、同様の概念を実現していると言える。

このように RIR (Regional Internet Registry) では、IP アドレス管理業務とルーティング業務を結びつける機構が利用されている。一方、IETF では、SIDR WG のようにルーティングセキュリティの向上のために、IP アドレスの管理情報とルーティングの情報を電子証明書で結びつける仕組みの Protokol 策定が行われている。

そこで、本調査研究では、経路情報の登録機構について RIR や IETF の参加者が一同に集う会合で発表し、RIR および IETF において有意性などの確認を行った。RIR や IETF の参加者が一同に集う会合に、IEPG (Internet Engineering and Planning Group) がある。IEPG は IETF ミーティングの前日に毎回行われる会議で、IETF の参加者の中でインターネットの運用に興味のある技術者や運用者が参加している (図 4-12)。

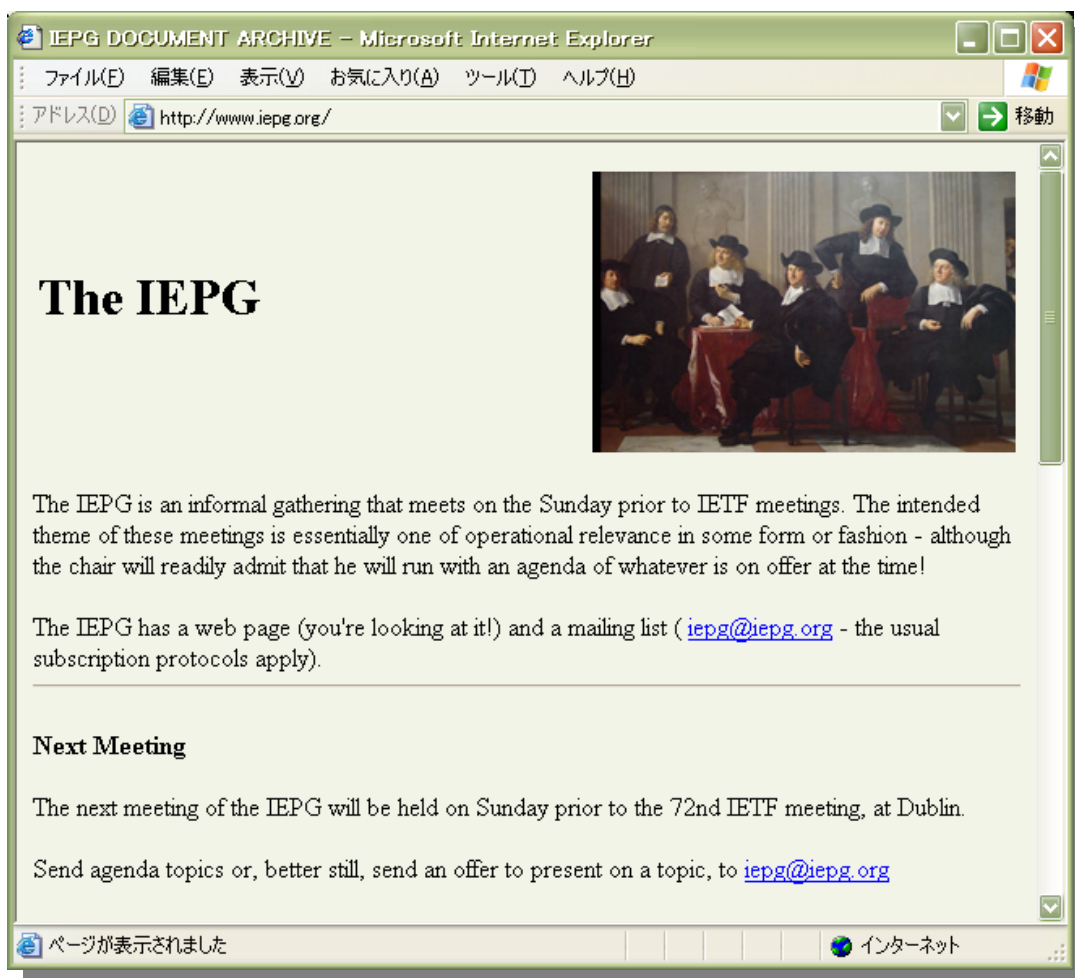


図 4-12 IEPG Web ページ <http://www.iepg.org/>

本節では、2007年12月2日、カナダのバンクーバーで行われた IEPG ミーティングにて行った、経路情報の登録機構に関するプレゼンテーションの内容と行われた議論について述べる。

RIR と IETF のセキュアルーティングにおける議論の中では、IP アドレス管理業務の中でルーティングへの IP アドレスの利用は、IP アドレスの利用認可 (authorization) という概念で捉えられている。経路情報の登録機構はこの利用認可を実現しているため、プレゼンテーションでは JPIRR における authorization の仕組みというタイトルとした (図 4-13)。

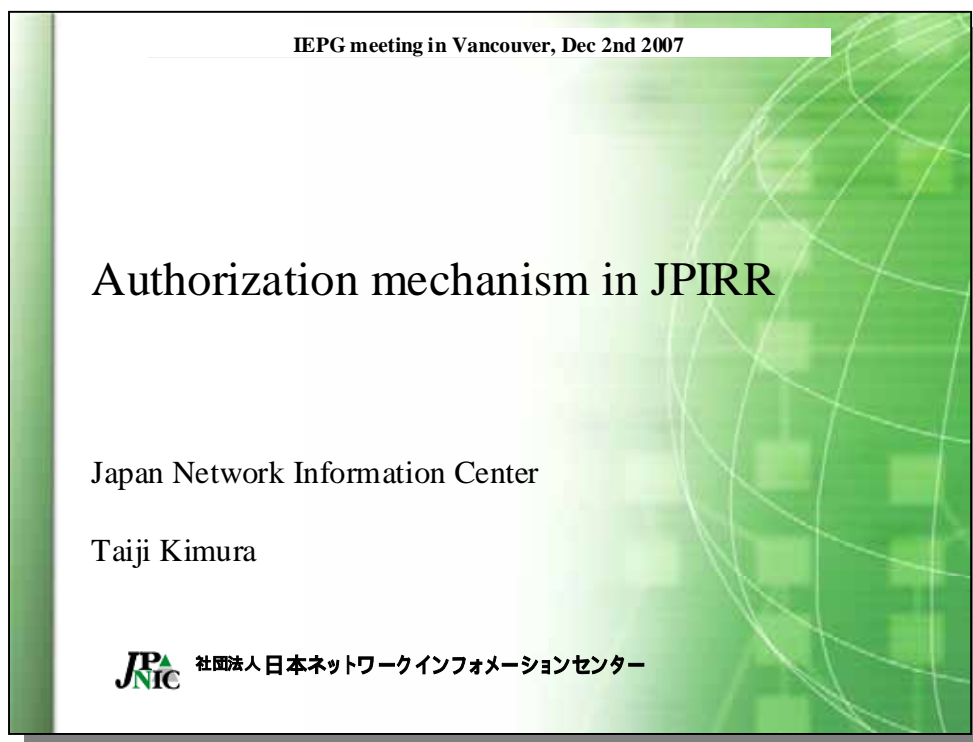


図 4-13 第 70 回 IETF の IEPG ミーティングで行ったプレゼンテーション

経路情報の登録機構に関する説明の前に、本機構の位置づけに関する説明を行った(図 4-13)。経路情報の登録機構は、JPIRR における実験的な実装であり、まだリリースされていないことや、本機構が「許可リスト」によって IP アドレスの利用認可を実現していることなど、概要を説明した。また論点がわかりやすくなるよう、本機構がルーティングセキュリティに効果を持つか、という疑問文を残しておいた。

One topic about Internet Routing Registry

- An trial implementation of authorization mechanism for JPIRR
 - Will be released for LIRs in Japan this month
 - Has LIR's authorization list
 - Maintained by LIRs who have allocated prefixes from JPNIC
 - Allow/Deny mntners in JPIRR to put prefixes in route objects
 - AS numbers can be specified by LIRs.
- Does this works well for routing security?

図 4-14 One topic about Internet Routing Registry

本機構に関する説明のはじめに、本機構が適用される JPIRR と本機構の必要性について述べた(図 4-14)。これは、RIR や IETF では、IRR というと米国 Merit 社の RADB で有名であり、JPIRR の紹介が必要な為である(図 4-15)。

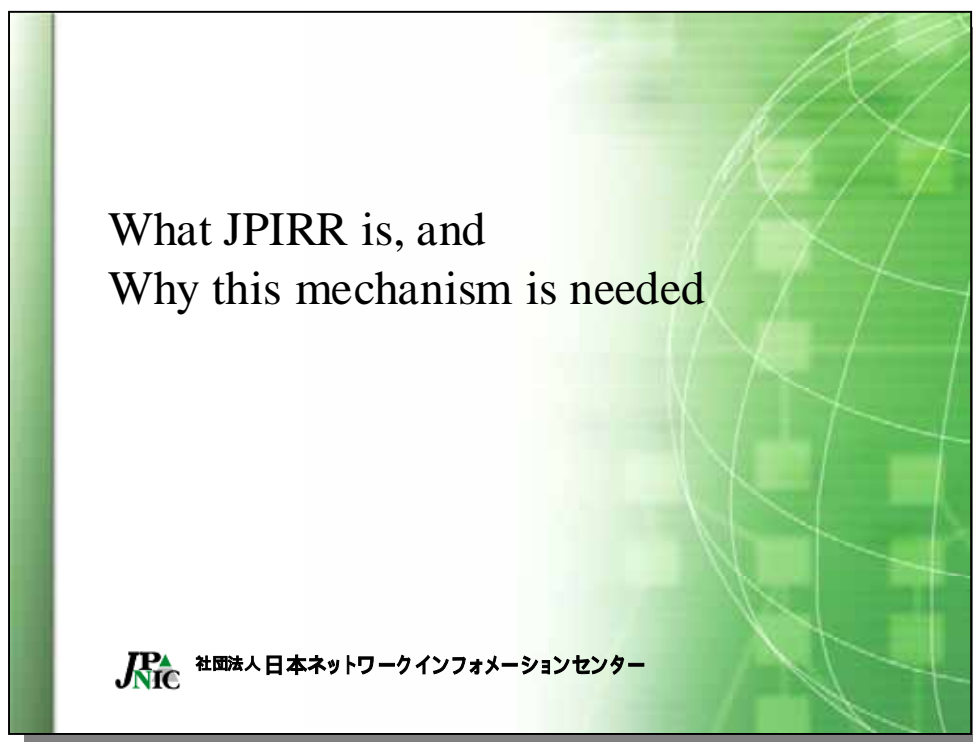


図 4-15 What JPIRR is, and Why this mechanism is needed

JPIRR に関する説明では、そのデータベースの規模と IP レジストリシステムとの連携状況について述べた。JPIRR はメンテナ数が 122 (2007 年 12 月現在) で RADB の約 20 分の一の数の管理者情報が登録されている。一方、経路に関する登録情報は RADB の 10 分の一以上あり、一件辺りの管理者情報に対する経路の情報は、RADB よりも多く登録されていることになる (図 4-16)。

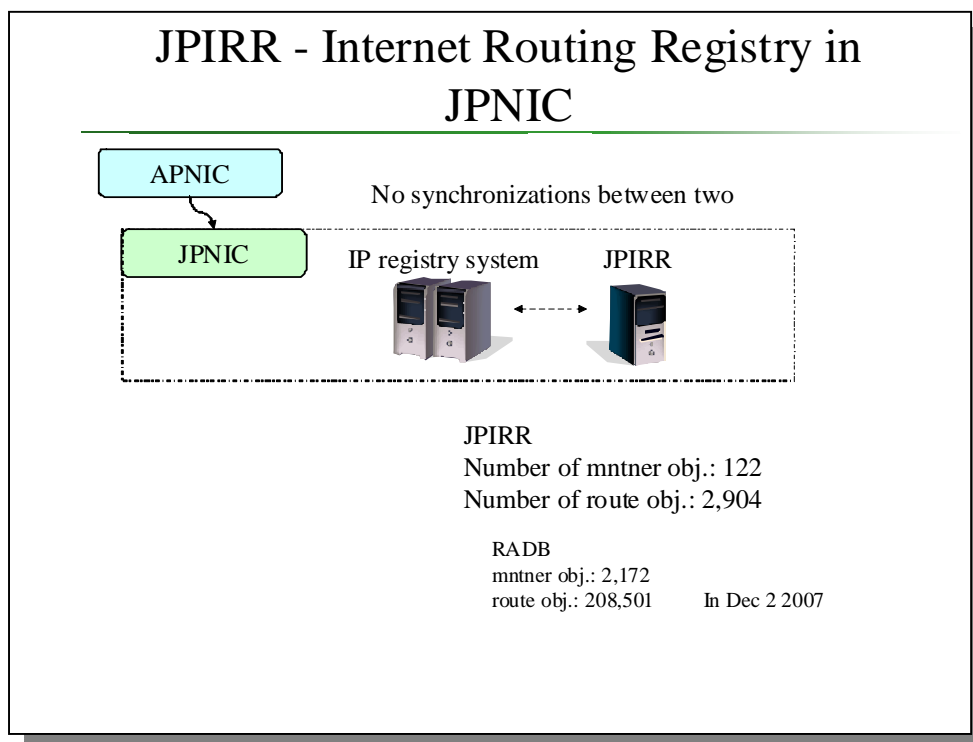


図 4-16 JPIRR - Internet Routing Registry in JPNIC

JPIRR は、JPNIC の IP レジストリシステムとは独立したシステムである(図 4-16)。RIPE NCC の IRR は RIPE NCC における IP レジストリシステムと一体であり、IP アドレスの割り振り / 割り当て情報と、経路の情報は連動している。ARIN や APNIC の IRR は各々の IP レジストリシステムとは分離しており、むしろ分離している方が主流であるといえる。Merit 社の RADB は当然の事ながら IP レジストリシステムと連動していない。

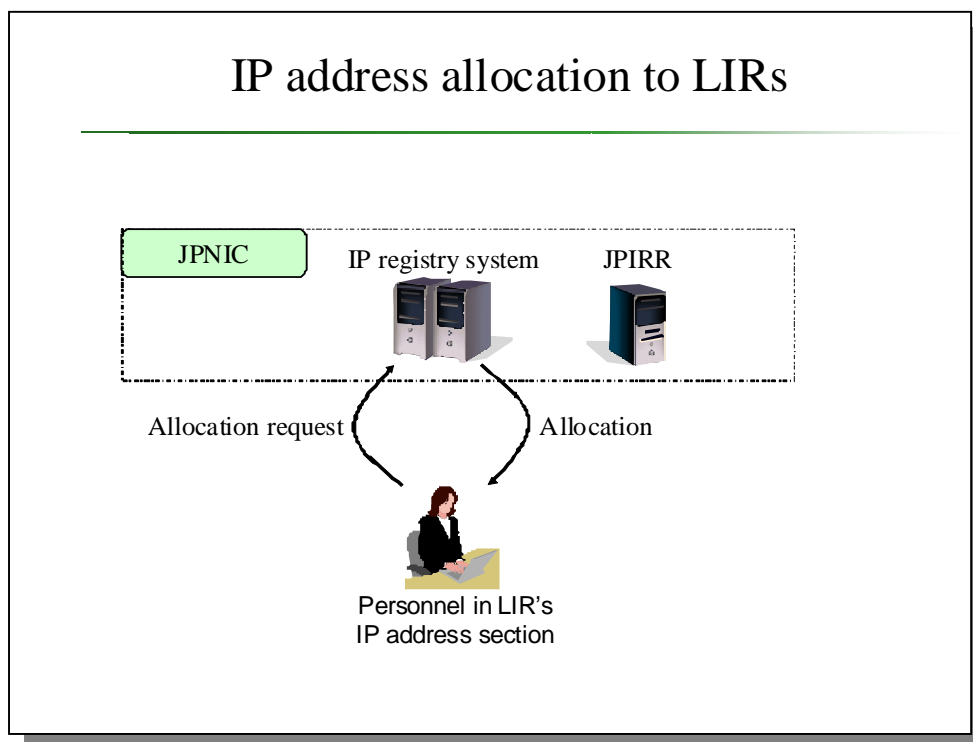


図 4-17 IP address allocation to LIRs

JPIRRの説明の後、JPNICにおけるIPアドレスの割り振り業務について述べた(図4-17)。日本国内のIP指定事業者は、国際的にはLIRと捉えることができるため、簡単のためLIRへの割り振り業務、という説明とした。JPNICからIPアドレスの割り振りを受けても、JPIRRに自動的に登録は行われない。

一方、JPIRRではIPレジストリシステムと独立した登録業務が行われている(図4-18)。JPIRRに登録業務を行うのはISPでルーティング業務を行っているもので、JPIRRにおけるユーザの登録情報もIPレジストリシステムのユーザとは異なっている。

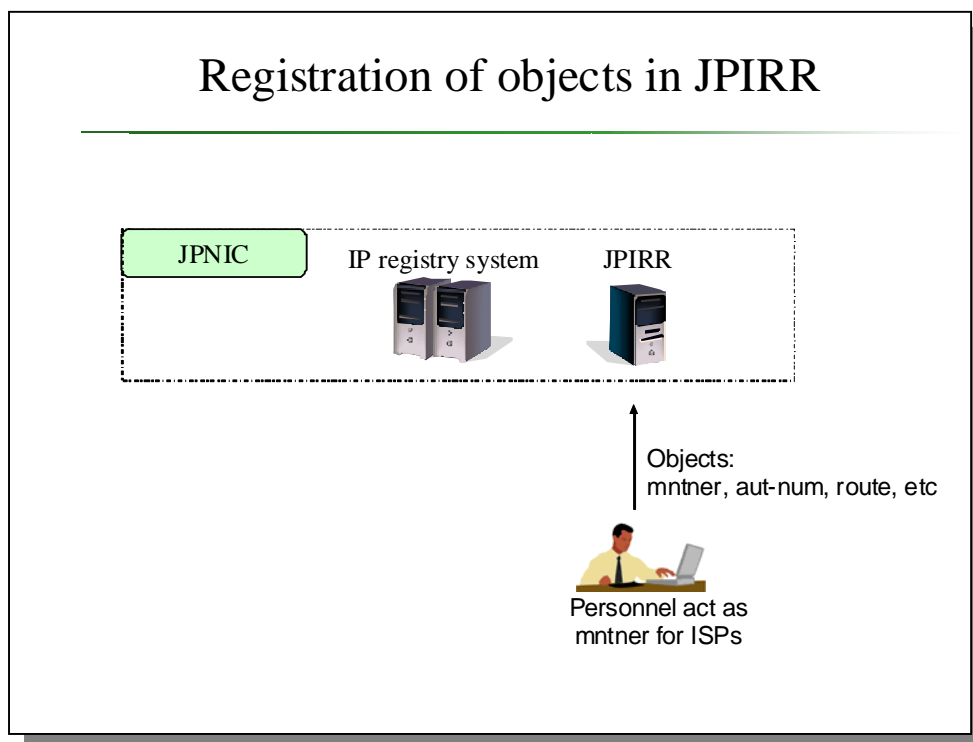


図 4-18 Registration of objects in JPIRR

JPNIC や他の RIR における IRR は、IP レジストリシステムと独立したシステムであるが、ここで二つの疑問を提示した（図 4-19）。

Why this mechanism is needed

- There are no relationship between IP address allocated to LIRs and prefixes in route objects in JPIRR.

Two big questions:

- Does anyone can put any prefixes in route objects? - - Yes he/she can.
- Is there any correctness of prefix-based filtering for BGP routers along with JPIRR? - - Well, yes if all mntner does correctly.
- How should we handle it?
 - At least, LIRs are need to be aware of use of prefixes in global routing operations.

図 4-19 Why this mechanism is needed

一つは「IRR にはあらゆる IP アドレスの登録が可能か？」ということである。現行の IRR では、割り振りが行われていない IP アドレスであっても IRR に登録することが可能である。もう一つは、「BGP ルータで JPIRR の登録情報に従って prefix フィルター（IP アドレスベースのフィルタリング方式）を利用した場合に、それは正しいと言えるか？」ということである。これに対しては「もしもすべての登録者が正しい情報を登録していれば」という逆説的な答えをあえて提示した。つまり、IRR の登録情報を利用して正しい prefix フィルターを利用することが難しいのである。

更に LIR における prefix の利用が、グローバルなルーティング業務で重要な位置づけにあることを述べた。後述する、本機構の狙いの一つに LIR における prefix の正しい利用に関する注意喚起があることに繋げている。

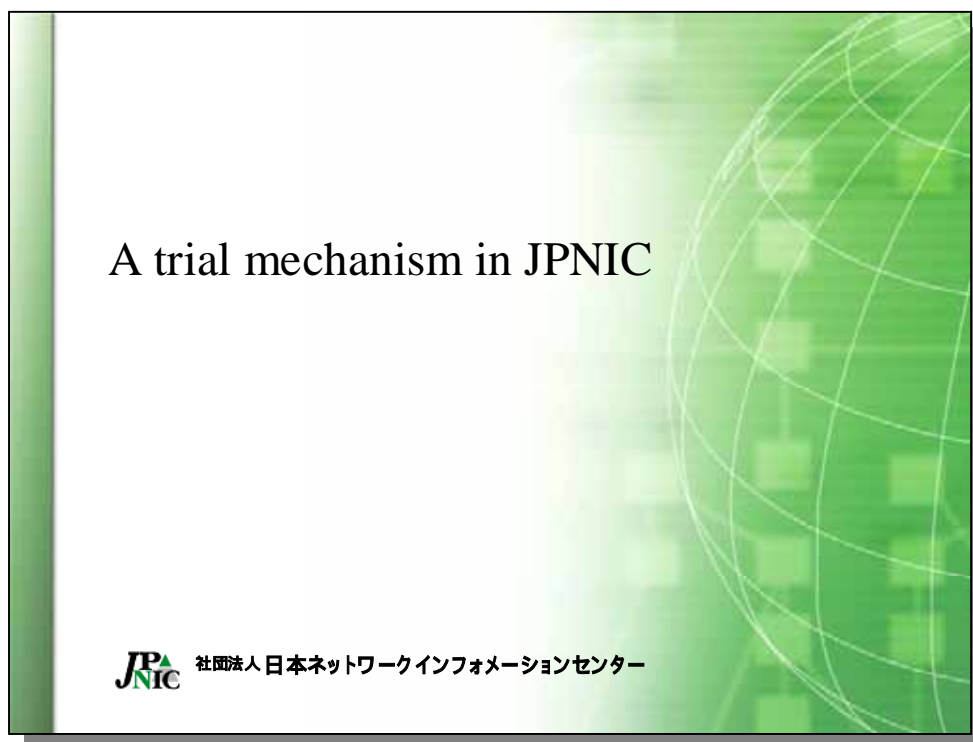


図 4-20 A trial mechanism in JPNIC

本機構の開発は、経済産業省からの受託事業の一環であるため、あくまでトライアルであるという位置づけとした(図 4-20)。JPNIC では IP アドレスの割り振り / 割り当て業務と IRR の運用の両方を行っているため、このトライアルは JPNIC ならではのものであると言える。

はじめに、利用認可の基本概念を説明する。経路情報の登録機構は、LIR に割り振られていない IP アドレスを含む route オブジェクトが JPIRR に登録されることを防ぐシステムである。同時に、IP レジストリシステムと JPIRR における登録業務はこれまでと大きく変わらないように工夫されている。

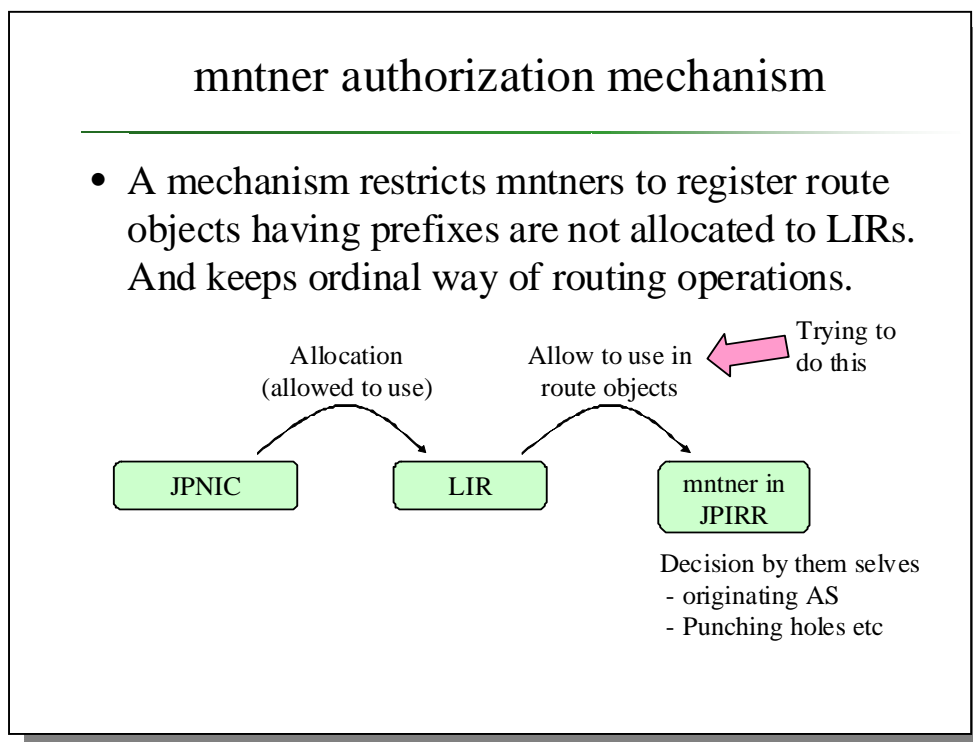


図 4-21 mntner authorization mechanism

図 4-21 は、IP アドレスに対する LIR の概念的な業務内容を示したものである。JPNIC（上位のインターネットレジストリ）は LIR に対して割り振りを行うが、これは IP アドレス利用を認めていることでもある。これと似た形で、LIR は JPIRR におけるメンテナーに対して、IP アドレスのルーティングにおける利用を認可する。JPIRR におけるメンテナーはルーティング業務を行っているもの識別子を持たせて顕在化させるための方法である。ルーティング業務を行うもの、すなわちメンテナーはどの AS を広告元としてルーティング業務を行うか、またどの IP アドレス空間を経路広告せずに下位のネットワークに使わせるか、等のルーティング業務上の判断を行う。

経路情報の登録機構は、LIR が JPIRR におけるメンテナーに対して、route オブジェクトを登録することを認可する、という業務を実現する。

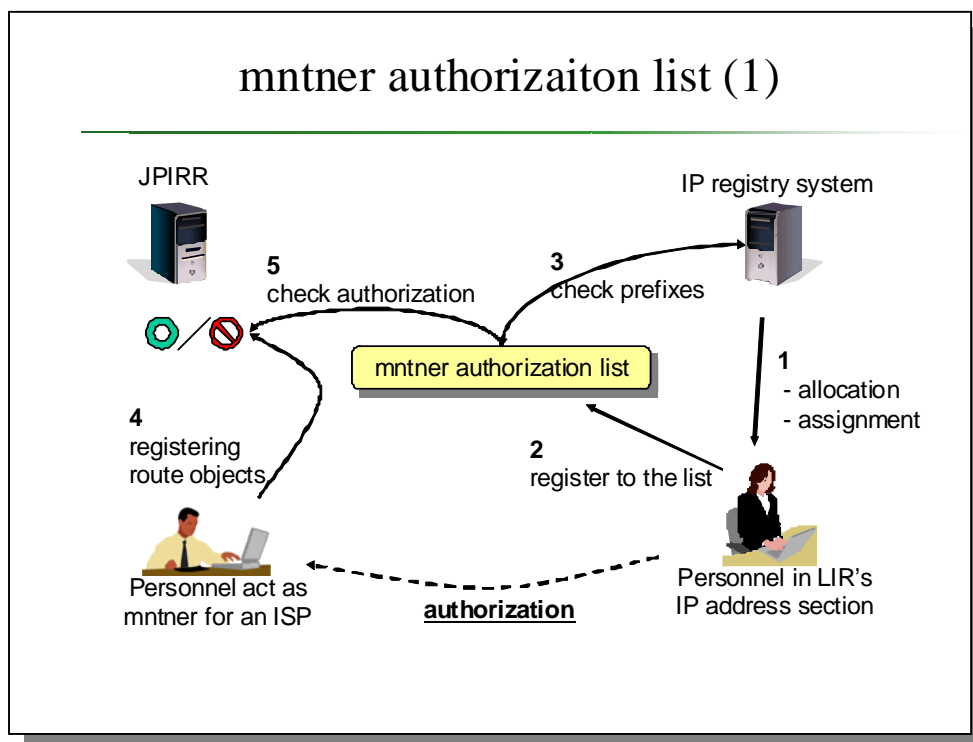


図 4-22 mntner authorization list (1)

経路情報の登録機構における IP アドレスの利用認可登録は、LIR の IP アドレス申請担当者によって行われる。図 4-22 は LIR に IP アドレスを割り振られてから、利用認可の確認された route オブジェクトが登録されるまでの業務流れを示したものである。

はじめに LIR に IP アドレスの割り振り / 割り当てが行われる (1)。これは LIR の IP アドレスの申請業務担当者によって、IP レジストリシステムを通じて行われる。次に、IP アドレスの申請業務担当者は割り振られたアドレスを許可リスト (mntner authorization list) に登録する (2)。この時、登録された IP アドレスがその LIR に割り振り済みであるかどうか確認される (3)。IP アドレスの申請業務担当者はこの操作を必要数だけ行い、自組織に割り振られた IP アドレスを可能であればすべて、特定の mntner に対して利用認可を行う。

JPIRR にオブジェクトを登録するオブジェクト登録者 (Personal act as mntner for an ISP) は、通常の IRR へのオブジェクト登録の書式を使ってオブジェクト登録を行う (4)。この時、登録されようとしている route オブジェクトの検査が行われ、IP アドレスの利用認可がされているかどうか確認される (5)。

mntner authorization list (2)

Prefix (inclusive)	allow / deny	mntner	Origin AS (optional)
1.1.0.0/16	allow	MAINT-JPNIC	12345
1.1.0.0/17	deny	MAINT-AS2515	

図 4-23 mntner authorization list (2)

図 4-23 は、許可リストの内容を説明したものである。ここでは多様な IP アドレスの管理方法に対応できることを説明するため、詳細に説明を行った。

許可リスト (mntner authorization list) は、基本的に 4 つの値を持つ表である。最初は prefix で、IP アドレスの範囲である。二番目の allow/deny は、その IP アドレスに対する認めないし認めないことを示す値である。三番目の mntner は IP アドレスの利用を認可する対象のメンテナー名である。図では、MAINT-JPNIC や MAINT-AS2515 は 1.1.0.0/16 の範囲にある route オブジェクトを登録できる。四番目の Origin AS は登録される route オブジェクトの Origin AS の欄に記入される AS 番号の制限である。図の場合には、1.1.0.0/16 は Origin AS を 12345 に指定した route オブジェクトしか登録することができない。Origin AS の指定は Optional (追加事項) であり指定を行わなくてもよい。

許可リストは、次に述べるような使い方ができる。ある IP 指定事業者が、自社の ISP 事業でのみ IP アドレスを使う場合、自社に割り振られたすべての IP アドレスを自社のメンテナーに許可すればよい。自社に複数の AS 番号が割り当てられており、ルーティング業務の中で随時変更できるようにしておくには、Origin AS の欄には何も記入しないでおく。また IRR への登録業務を自社のメンテナー以外で行う場合には、mntner の欄にそのメンテナー名を併記しておく。これにより、自社に割り振られた IP アドレスが、他の AS によって経路広告されたとき、IRR の登録情報と差異が生じる。すべての割り振り済み IP アドレスを登録しておけば、自社に割り振られた IP アドレスが一部でも他

第4章 IP アドレス認証の展開に関する調査研究

の AS に使われたときに、IRR と比較して異常を発見できる。

自社に割り振られた IP アドレスのルーティング業務を他社に委託する場合には、その他社のメンテナー名を mntner 欄に記入するだけでよい。そのルーティング業務を行う他社は、自社の AS 番号を用いてルーティング業務を行うことができ、また AS 番号が変わる場合やマルチプル Origin (複数の Origin AS の同一 prefix の経路情報) を広告することも可能である。

mntner authorization list (3)

ID	Org	Org Name	Prefix	Mntner Name	AS Number
13	9999	ROUTERS2TEST	100.0.0.0/24	MAINT-ROUTERS2	
19	9999	ROUTERS2TEST	100.0.10.0/24	MAINT-ROUTERS2	AS999, AS25
18	9999	ROUTERS2TEST	100.0.10.0/22	MAINT-ROUTERS2	AS2
23	9999	ROUTERS2TEST	100.0.32.0/18	MAINT-ROUTERS2	AS00001, AS0001, AS3791
14	9999	ROUTERS2TEST	100.0.22.0/18	MAINT-ROUTERS2	
27	9999	ROUTERS2TEST	200.210.99.0/22	MAINT-ROUTERS2	AS37911, AS25
29	9999	ROUTERS2TEST	200.210.99.0/24	MAINT-ROUTERS2	
28	30999	ROUTERS2TEST	200.0.40.0/22	MAINT-ROUTERS2	AS37911, AS25
24	30999	ROUTERS2TEST	200.0/32	MAINT-ROUTERS2	AS99999, AS9999, AS3791
11	30045	JPIRR	2030.0/22	MAINT-ROUTERS2	AS64512, AS00001

図 4-24 mntner authorization list (3)

図 4-24 は、経路情報の登録機構で許可リストを表示した画面である。許可リストは Web インターフェースで編集することができる。ソートや編集、削除などを行うことができる。

なお、テストのために入力された IP アドレスを表示している。メンテナー名もテスト用のものであり、実際には JPIRR に登録されたメンテナー名が表示される。

図 4-25 と図 4-26 はシステムがどのように動作するかを説明したものである。

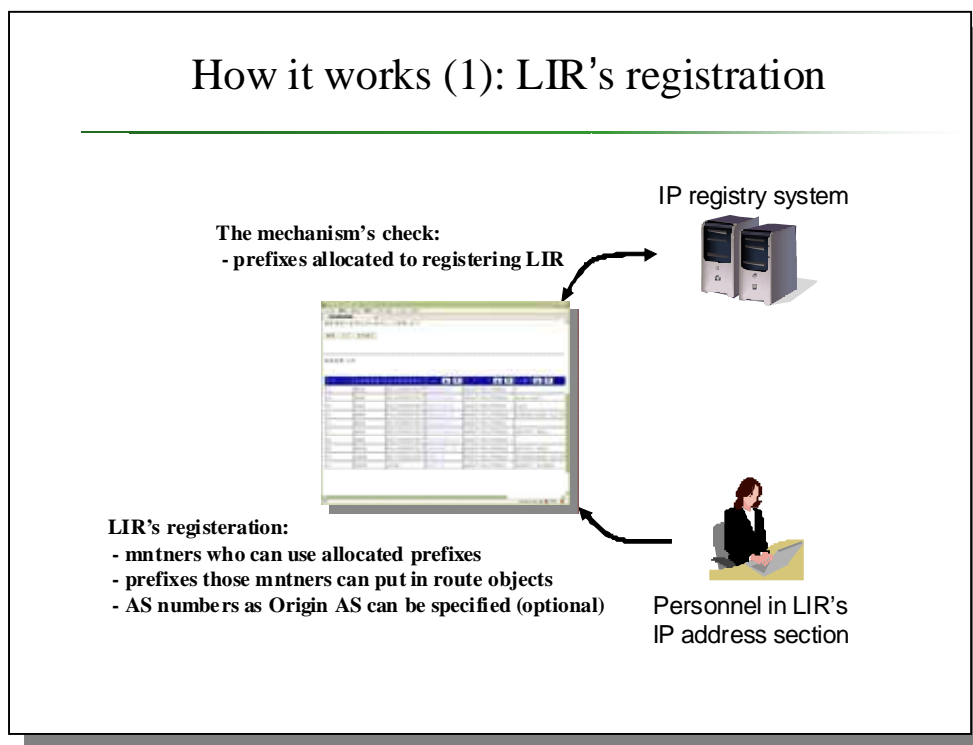


図 4-25 How it works (1): LIR's registration

はじめはLIRによる許可リストへの登録がどのように行われるかを説明した図である。LIRのIPアドレスの申請業務担当者は、自社の認証用の電子証明書を用いて経路情報の登録機構にアクセスする。自社の認証用の電子証明書は、IPアドレス認証局（認証）（サービス名：資源管理認証局）から発行されたクライアント証明書である。

LIRの担当者は、はじめにIPアドレスの利用者であるメンテナー名を登録する。そのメンテナー名はJPIRRにrouteオブジェクトを登録できるメンテナーである。更に必要があればAS番号の指定を行う。経路情報の登録機構がクライアント認証に用いる認証用の電子証明書は、IPレジストリシステムのものと同様であるため、IPレジストリシステムが許可リストに登録を行おうとしているユーザがどのLIRのユーザであるかを認識することができる。許可リストへの登録の差異に、そのLIRに割り振られたIPアドレスが登録されるかどうかの確認を行う（図4-25）。

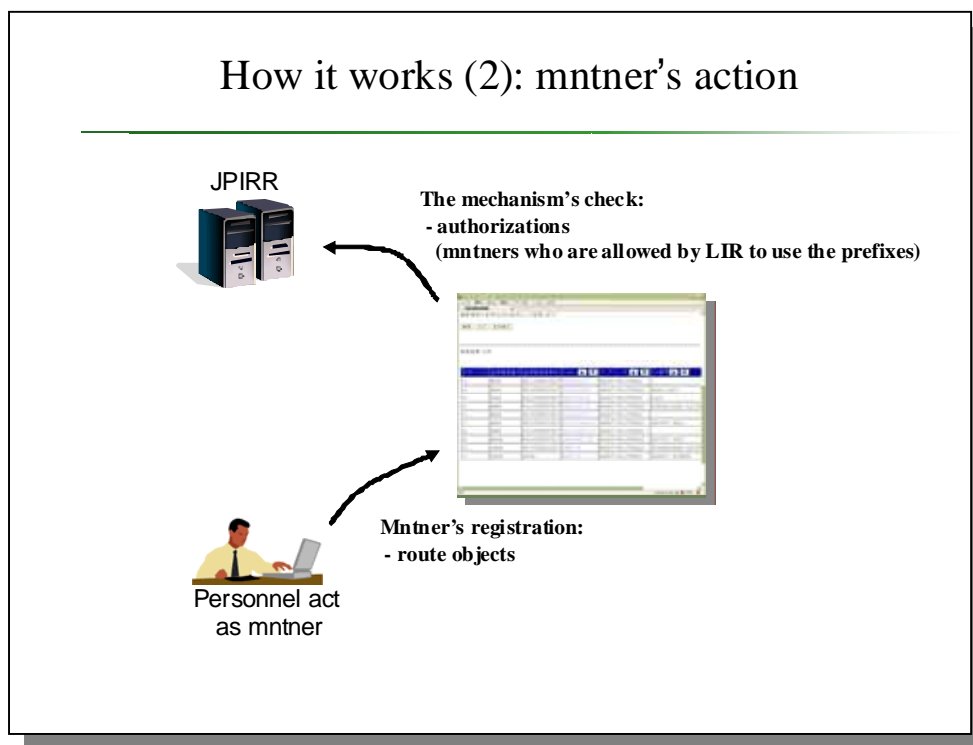


図 4-26 How it works (2): mntner's action

図 4-26 に示したスライドはメンテナによる route オブジェクトの登録について説明している。メンテナの権限で route オブジェクトを登録する際、経路情報の登録機構は route オブジェクトに含まれる IP アドレスが許可リストに載っているものであるかどうかの確認を行う。更に登録しようとしているユーザ（メンテナの権限を使おうとしているユーザ）が、認可の対象になっているかどうかを確認する。

Expected results

- All new registered route objects will have allocated prefixes. And they are registered by appropriate mntners.

This situation can keep:

- Avoiding
 - Use of un-allocated prefixes in route objects
 - Miss-matches from registry's allocations
- Providing
 - Selecting originating AS by mntners according to operational reasons
 - Nothing new if LIR and mntner are the same

図 4-27 Expected results

このスライドは、以上の手続きを踏まれて登録されることでどのような効果が期待できるかを説明したものである。以上の業務手続きにより、JPIRR に登録されるすべての route オブジェクトは、割り振り済みで、かつ利用認可されたメンテナーによって登録されることが担保されるようになる。

このことで、まず route オブジェクトに少なくとも割り振られていない IP アドレスが入ることがなくなる。またインターネットレジストリによる割り振りとなる IP アドレスも入ることがなくなる。

また業務上の自由度を二つの意味で確保している。一つ目はメンテナーによって Origin AS を選択できることである。ルーティング業務においては、ネットワークの構成に自由度を持たせたり、障害時にネットワークの構成を変更できることは重要である。またもし LIR とメンテナーが同一の担当者や担当部署である場合、これまでの業務とほとんど変わらない。すなわち経路情報の登録機構を使うことで業務負荷が大きく変わることはない。

Operator's expect on use of JPIRR in Japan

- irrzebra
 - Checks BGP updates with IRR
 - Shows flags as “checked” when displaying routing table
- Keiro-bugyo
 - (Keiro is 'route')
 - (Bugyo is organized decision makers for local society in Samurai era)
 - Checks received BGP updates with local configurations
 - (Local configurations are checked by using IRR)
 - Notify if a miss-use is detected by e-mail

They will have more accuracy of 'checks' if the authorization mechanism works well.

図 4-28 Operator's expect on use of JPIRR in Japan

このスライドは、経路情報の登録機構の応用に関する日本国内での動向を簡単に紹介したものである。JPIRR は irrzebra⁵や経路奉行⁶と呼ばれる ISP によって開発されたシステムによっても利用されている。irrzebra は BGP の Update メッセージに含まれる prefix に対して IRR を使った検査ができるルーティングデーモンである。ルーティングテーブルに検査の結果を表示することができ、ルーティング業務を行うものは、異常を発見しやすい。

経路奉行は irrzebra と同様に BGP の Update メッセージの検査を行うシステムである。経路奉行は一度に大量の検査が行えるように、一旦ローカルの設定ファイルに IRR の事前調査事項を保存しておく仕組みを持っている。また経路奉行は、検査の結果を電子メールで通知する機能を持っている。

これらの仕組みと IRR および経路情報の登録機構が連携することで、実際のルーティング業務において IP アドレスの利用認可がなされていない IP アドレスを検知できる。

⁵ irrzebra は「インターネット中枢機能のセキュリティ強化に関する研究開発」(委託研究)に掲載されている。

http://www2.nict.go.jp/q/q265/s802/seika/h18/seika/81/81_ntt-com.pdf

⁶ 経路奉行は「Telecom-ISAC Japan の 最近の取組について」に詳しく述べられている。

<http://www.ipa.go.jp/security/event/2006/infra-sem/pdf/Telecom-ISAC.pdf>

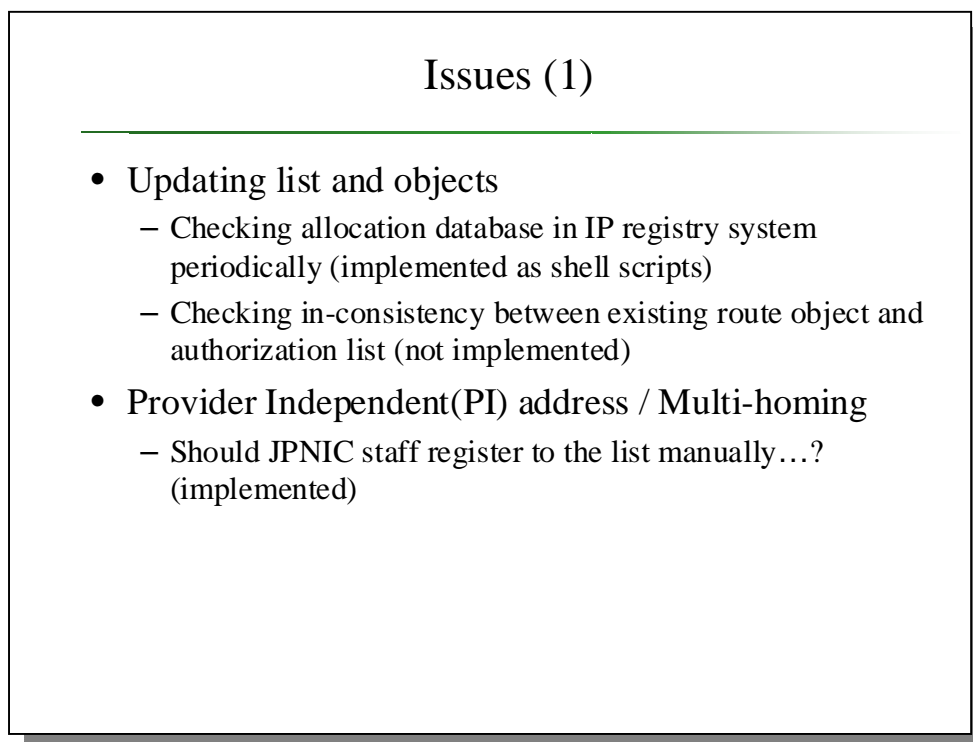


図 4-29 Issues (1)

Issues は、経路情報の登録機構に関する論点を整理したスライドである（図 4-29）。

RIR に同様の仕組みが導入されていることがわかっているため、それらの運用の中で問題点となっていることを中心にまとめた。

経路情報の登録機構の許可リストは、長期間運用されていると古いデータが残る可能性がある。RIPE NCC では割り振り情報と齟齬が生じた状態の、古いデータが残ってしまう問題が起こっている。経路情報の登録機構では、IP レジストリシステムと許可リストを定期的に比較し、齟齬が生じている場合には登録者に通知する機能を実装した。一方で、許可リストと IRR に登録済みの route オブジェクトの比較については、いまのところ行っていない。許可リストは IRR の登録と IP レジストリシステムの割り振り / 割り当てとの間に許可リストというクッションを設けることで、IP アドレスの返却等によって、即座に IRR の登録情報が異常だと検知されるような状況を避けている。しかし逆に許可リストが正しい情報を保持しているか（IP レジストリシステムのデータベースとの比較）、現状とあっているか（IRR の登録情報との比較）を行う必要がある。

PI アドレスとマルチホームに関しては、現在のところ JPNIC の職員が許可リストに登録するものとしている。これは一部の業務上の理由による。PI アドレスの割り当て先は、JPNIC の IP 指定事業者でないケースがあり、また割り当て先組織の本人性確認手順が IP 指定事業者とは異なる。IP 指定事業者に対する電子証明書の発行は実験的に開始しているが、PI アドレスの割り当て先組織には、まだ電子証明書を発行できていない

状況である。

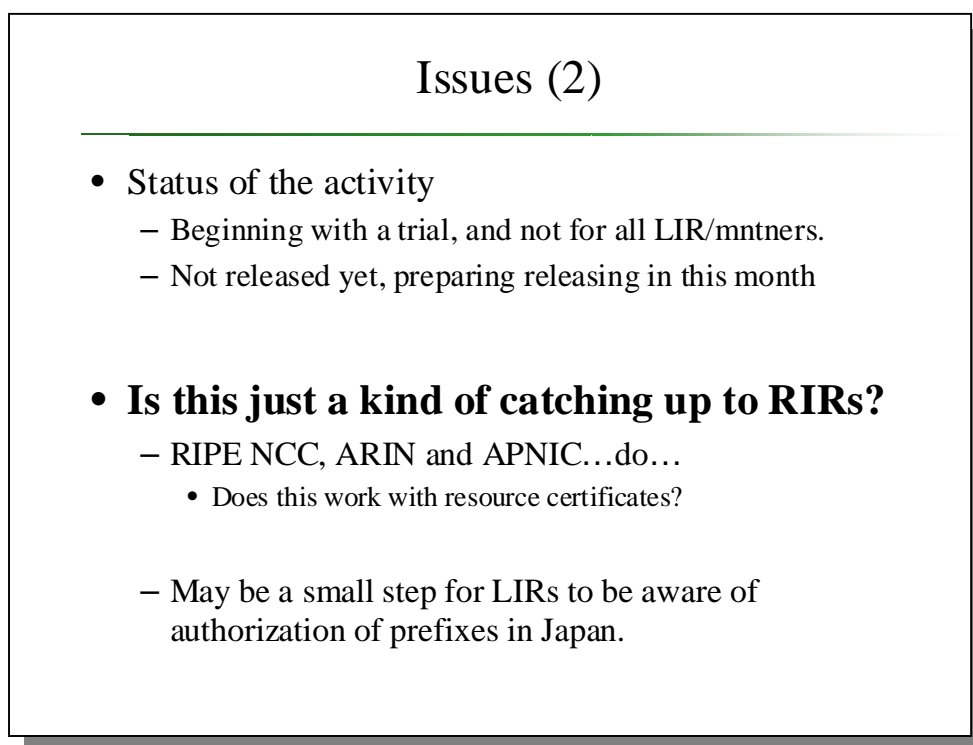


図 4-30 Issues (2)

前述の運用上の論点だけではなく、実験としての論点もある。経路情報の登録機構は、実験を開始したばかりであり、まだすべての LIR やメンテナーが利用できるわけではない。

本機構は RIR (RIPE NCC と ARIN) に対してキャッチアップする位置づけのシステムであると言う事もできる。また主に APNIC で取り組まれているリソース証明書との親和性を検討することも課題である。もしリソース証明書が日本を含むアジア太平洋地域で利用されるようになると、この prefix の利用認可の概念は必ず必要になるものである。

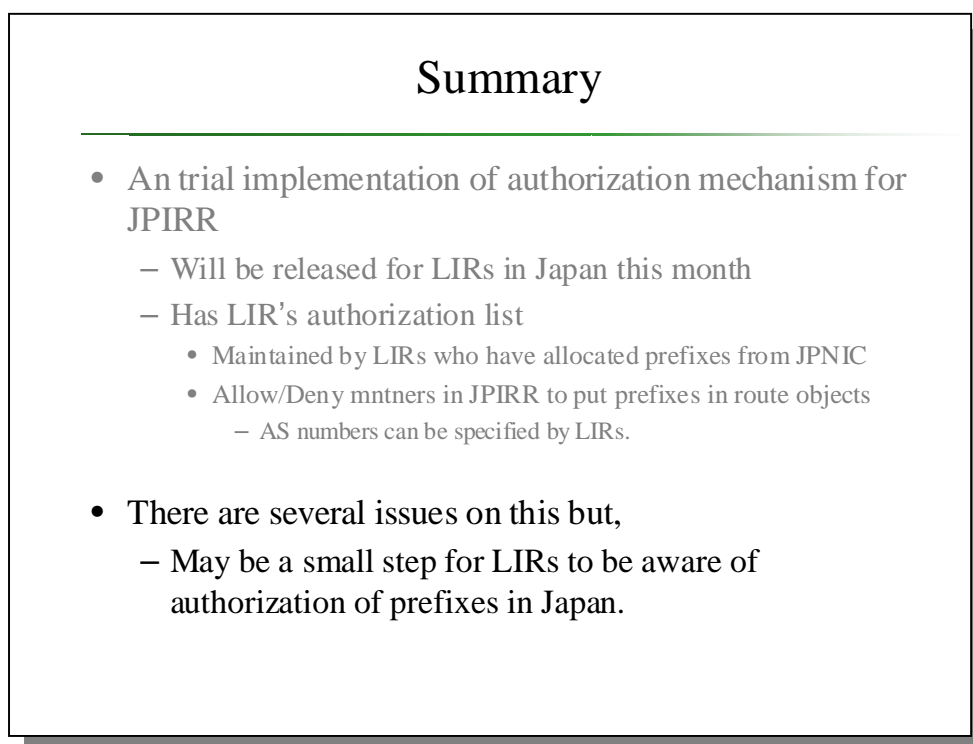


図 4-31 Summary

最後に、プレゼンテーションのサマリを行った（図 4-31）。

経路情報の登録機構が実験的な運用であることは先に述べた通りであるが、この実験によって prefix の安全な利用に関する認識が高まることが重要であると述べた。

以上が IEPG ミーティングにおけるプレゼンテーションである。この後、15 分以上、本件に関する意見交換が行われた。

IEPGミーティング会場でのディスカッション

- コメント
 - 活動をencourage
 - George Michaelson氏(APNIC), Shane Kerr氏(ISC,元RIPE NCC), Andrew de la Have氏(RIPE NCC)
 - 許可リストの状態に関して
 - 「要件」と「チェック機構」が必要であるというコメント(後者は既に開発済み)
 - リソース証明書との関係
 - 本機構とリソース証明書の仕組みは親和性がある(George Michaelson氏)
- 議論
 - その他にRIRと比べた、本機構の位置づけについて議論された。
 - RIPE NCCにおけるRPSS:登録情報の安全性確保手法、等

図 4-32 IEPG ミーティング会場でのディスカッション

図 4-32 は、IEPG ミーティングで行われた意見交換をまとめたものである。まず、この活動を高く評価する意見が多数挙げられた。その後の意見交換の中では大きく分けて二つの点について議論が行われた。

一つは、許可リストの「正しい」状態を保つことに関する議論である。まず「正しい」という状態の要件の定義が必要ではないか、という意見が挙げられた。これは例えば LIR による登録が常にルーティング業務に合ったものであるかどうか分からないという点である。またプレゼンテーション中でも述べた、チェック機構が必要であるという意見である。チェック機構は一部実装されているものではあるが、RIPE NCC のように IRR と IP レジストリシステムが同一であれば、チェック機構はよりシンプルなものになると考えられる。RIPE 地域の発言者は、許可リストによって二重のチェックが必要になっているのでは、という疑問が投げられた。許可リストは確かに二重のチェックを要するものであるが、各々のチェック内容と間違っている場合の通知先が異なる。また同一のシステムの場合、チェック後に IRR の route オブジェクトを消してしまい、ルーティングに障害を起こしてしまいかねない。許可リストのようにクッションを設けるべきか、同一のデータベースで管理されるべきであるかは、実験運用を行ってみてどのような問題が起こるのかを観察することで初めて解決が図られると考えられる。

他に、本機構とリソース証明書の親和性については、APNIC のリソース証明書の開発担当者から発言があった。それは、本機構はリソース証明書と親和性があるというシンプルな発言であった。

これらの議論の他に、RIPE NCC におけるセキュリティの仕組みと比較して本機構がどのような仕組みであるのかを確認したいといった意見交換が行われた。

4.10. 経路情報の登録機構に関する国内会議での議論

経路情報の登録機構に関する国内での議論は、主に JANOG (Japan Network Operator's Group) ミーティングで行った。本節では、第 21 回 JANOG において「IRR を使ったセキュアなインタードメイン・ルーティングを考える会」という時間に行った議論について述べる。

経路制御の問題解決とIRR

- 経路の問題と解決策
 - Inter-Domainの経路制御で、問題解決に人的ネットワークに頼らなくていい部分があるはず...というか、IPv4アドレスプールが枯渇する時期に、いまのままで大丈夫？
- 例えば経路ハイジャックを防ぐとして
 - その情報源は？
- IRRにちゃんとrouteオブジェクトがたまれば大丈夫？
 - routeオブジェクトの割り振り情報との違い
 - IRRには割り振り/割り当てに関わらず、任意のアドレスprefixが入ったrouteオブジェクトを登録できる。
 - 全く関係のない他のISPが経路広告すべきprefix
 - 未割り振りのprefix など

図 4-33 経路制御の問題解決と IRR

これまで、経路制御における問題解決の多くは、人的ネットワークに頼っており、また経路情報の正当性の確認はオペレーターの地道な作業で行われている。しかし IPv4 アドレスの割り振りプールの枯渇時期に入り、他の ISP が経路広告して使うはずの IP アドレスが勝手に使われてしまう事態が今後起こりやすくなり、問題解決をある程度自動化する必要があると考えられる。

経路情報の登録機構は、IRR における登録上の問題を機械的に解決とも言える。既存の IRR には任意の prefix が入った route オブジェクトを登録できるため、他の ISP が経路広告すべき prefix を登録したり、未割り振りの prefix を登録できる。IRR はルー

タにおける経路情報の正しさの確認のために利用されているため、IRR に誤った情報が登録されているとその確認が行えなくなる。経路情報の登録機構は、他の ISP が経路広告すべき prefix を登録できないようにしたり、未割り振りの prefix を登録できないようにできる。

「経路情報の登録認可機構」

- 経路情報の登録認可機構について
 - 割り振られているアドレスなのかってことならば...
 - JPNICがJPIRRをやってるなら確認すればいいのでは？
 - 一括で確認して一定期間したら削除するのではなく、登録するときに「そのアドレス間違ってます」という方がよい
 - 作ってみました。
 - routeオブジェクトを登録する前にチェックします。チェック済みのrouteオブジェクトだけが登録されます。
 - 利用実験をやっています。
 - 詳しくはWebページをご覧ください。
 - <http://www.nic.ad.jp/ja/research/ca/routereg-outline.html>
 - トップページ JPNIC 認証局 経路情報の登録認可機構とは

図 4-34 「経路情報の登録認可機構」(JANOG21)

図 4-34 は経路情報の登録機構を紹介したスライドである。サービス名が「経路情報の登録認可機構」であるため、スライドでは経路情報の登録機構と表記している。経路情報の登録機構は、JPIRR に登録されている情報を一括して検査するようなバッチ形システムではなく、ユーザが登録する段階で、その登録内容のチェックを行うシステムである。これは一定期間後に削除する形では、オペレーターにとって突然経路制御に障害が起こるような事態を引き起こしかねないからである。

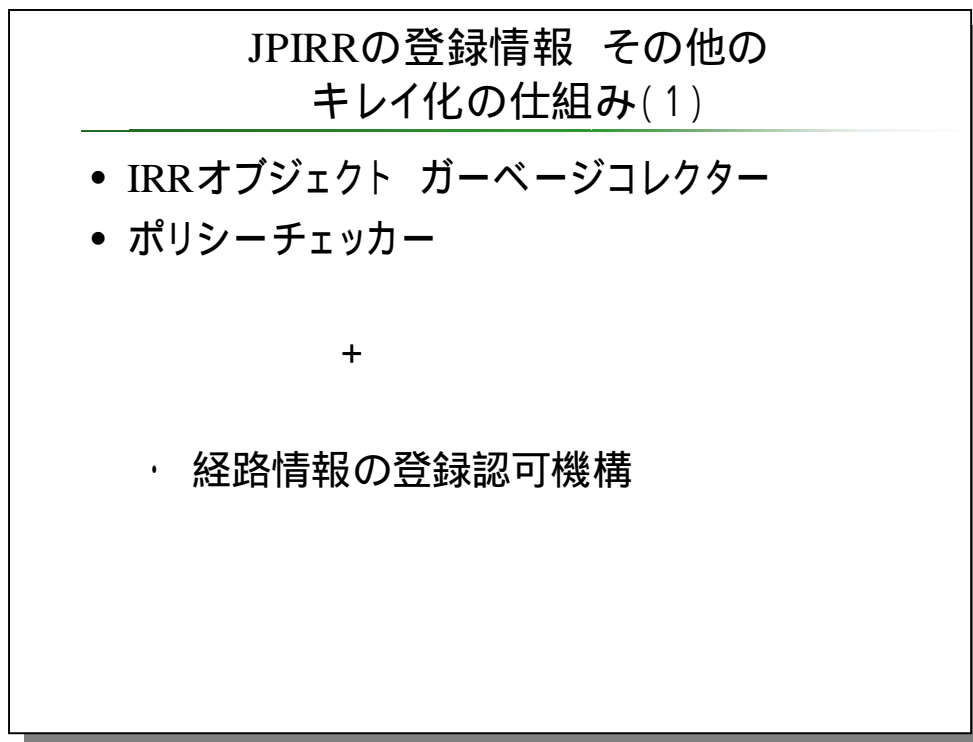


図 4-35 JPIRR の登録情報 その他のキレイ化の仕組み(1)

JPIRR には登録情報の正当性を保つための機能がこれまでに二つ実装されている。一つは「ガーベージコレクター」でもう一つは「ポリシーチェッカー」である。経路情報の登録機構は、この二つに加えて同時に使うことのできる仕組みである。

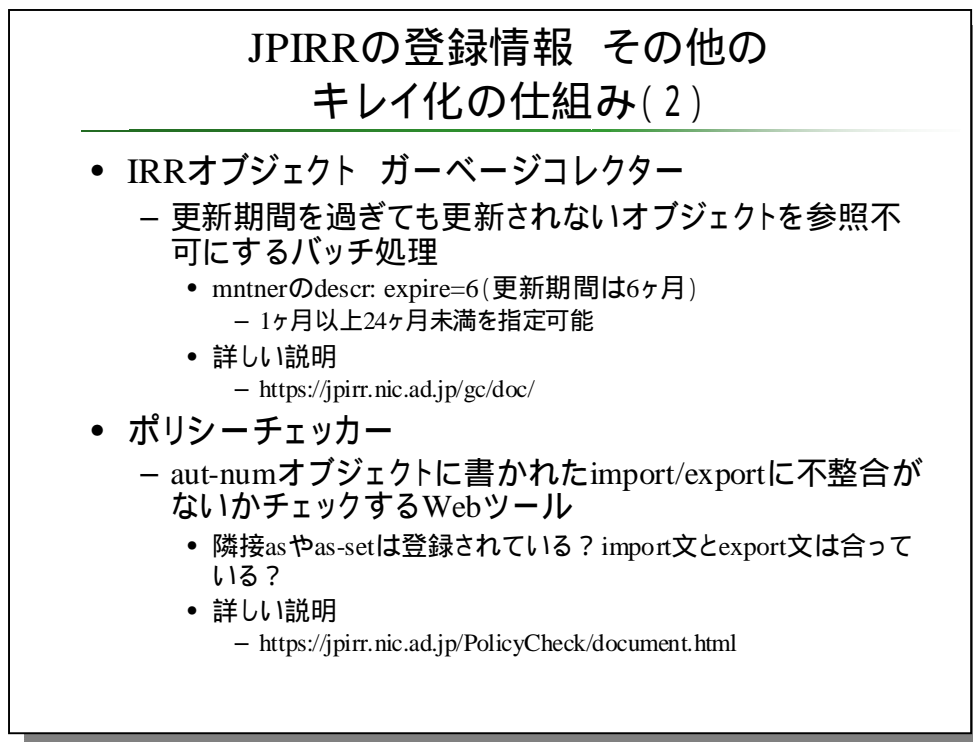


図 4-36 JPIRR の登録情報 その他のキレイ化の仕組み(2)

ガーベージコレクターは更新期間を過ぎても更新されないオブジェクトを参照不可にする機能である。mntner オブジェクトに予め更新期限を記述しておく、事前・事後の通知のあと最終的に参照できないようにする。このことで、オブジェクトが最新に保たれるようにするバッチ形のツールである。

ポリシーチェッカーは JPIRR に登録される情報の中で、import 文や export 文で不整合が生じていないかどうかを確認することができるツールである。ユーザは Web インターフェイスを使ってポリシーの確認を行うことができる。

経路情報の登録認可機構のチェック

- チェックのタイミング
 - routeオブジェクトを登録しようとするとき
- チェック内容
 - routeオブジェクトに書かれているIPアドレスが、割り振り先によって「routeオブジェクトとして登録してよいよ」と言われているかどうか
 - 「許可リスト」に載っているかどうか

図 4-37 経路情報の登録機構のチェック

経路情報の登録機構は route オブジェクトの登録に関するチェックを行う。このチェックは一定期間毎のバッチ的な処理ではなく、ルーティング業務を行うものが JPIRR にオブジェクトを登録する電子メールを送ったときに行う。

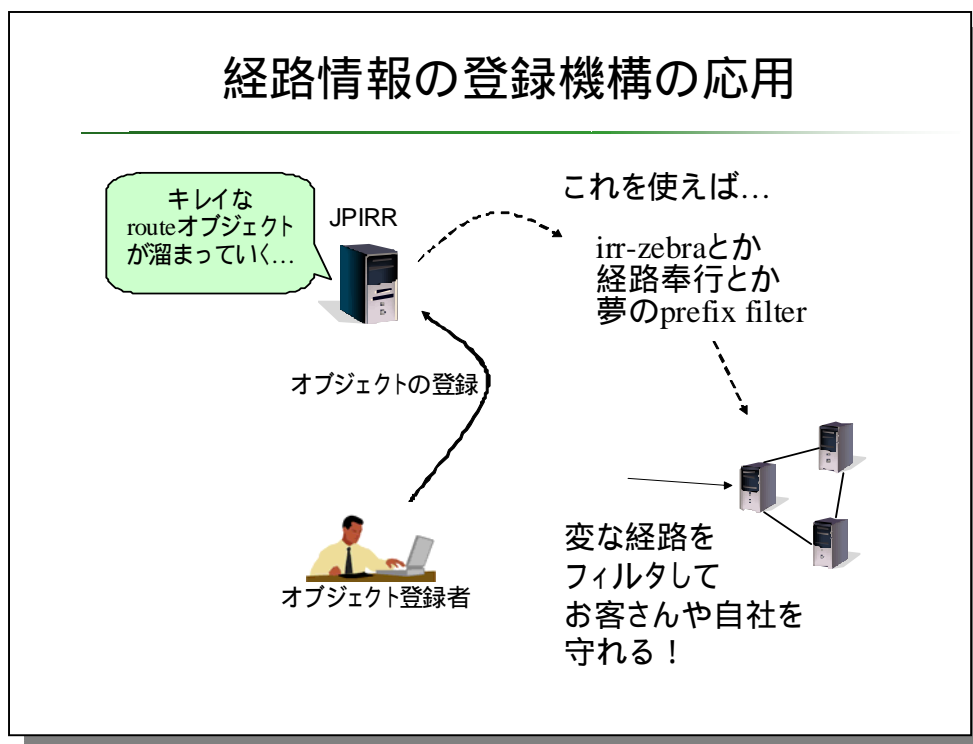


図 4-38 経路情報の登録機構の応用

JANOG では、自組織のネットワークを不正な経路制御から守る、という観点で議論を行った。irrzebra や経路奉行を用いると、不正な経路制御のメッセージを検知することができ、隣接する AS に対する経路制御も正しい状態を保つことができる。図では顧客や自社のネットワークを守ると記述しているが、実際には隣接する AS 同士が不正な経路情報のフィルターを行うことで、経路ハイジャックの影響を広域的に防ぐことができると考えられる。

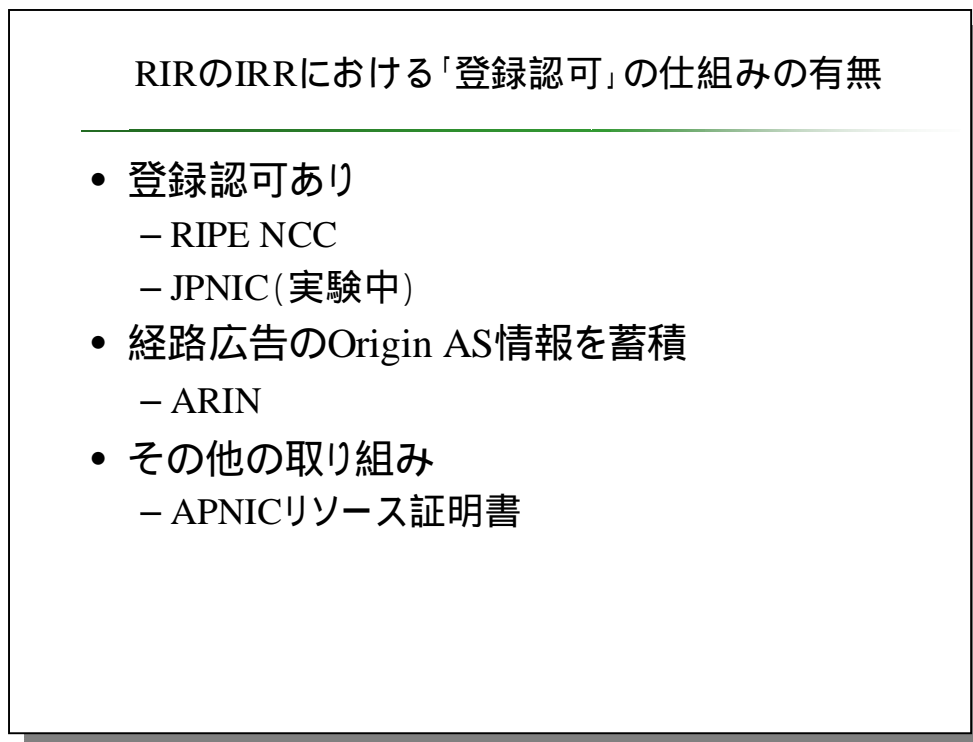


図 4-39 RIR の IRR における「登録認可」の仕組みの有無

JANOG21 では、RIR での取り組みと JPNIC の取り組みをまとめて紹介した（図 4-39）。

IP アドレスの利用認可の登録（図では登録認可）は、RIPE NCC と JPNIC で実施中である。ARIN では Origin AS の情報を蓄積できる申請テンプレート（書式）を 2006 年度より使っている。その他に APNIC のリソース証明書の取り組みがある。



図 4-40 RIPE NCC における割り振り / 割り当て情報と AS 番号を
マッチングする機構

RIPE NCC は mnt-lower と mnt-route を使った登録認可を実現している。mnt-lower は IP アドレスの割り振りが行われているケースで有効であり、mnt-route はルーティング業務を他社に委託している場合に有効である。

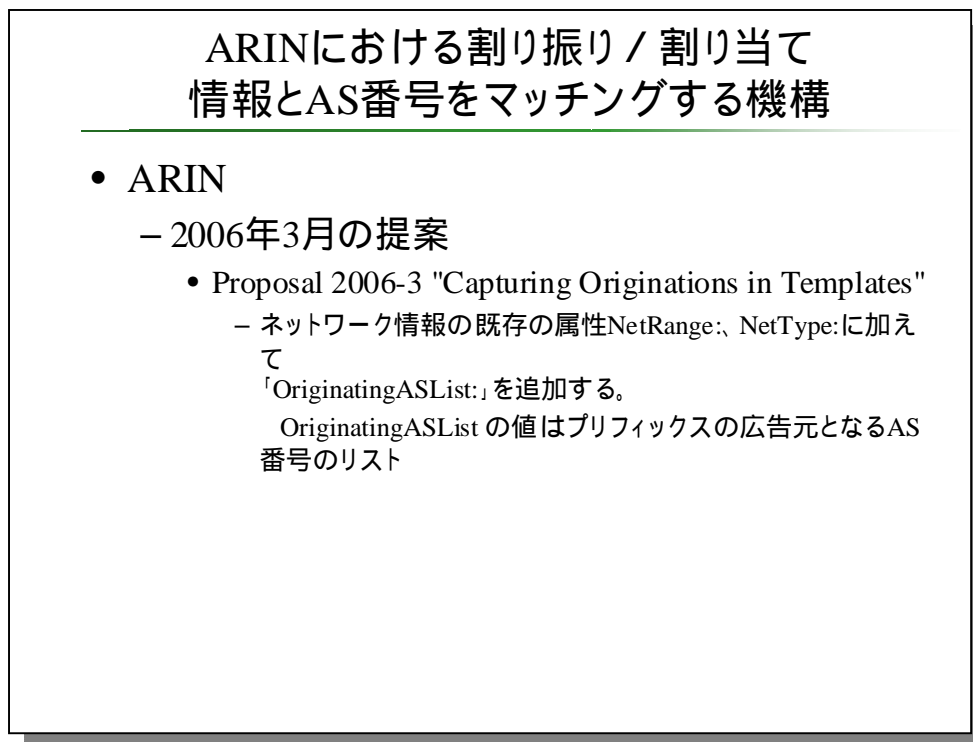


図 4-41 ARIN における割り振り / 割り当て情報と AS 番号を
マッチングする機構

ARIN では、Proposal 2006-03 と呼ばれるポリシー提案で、Origin AS の情報を収集するテンプレートの採用が提案された。すでにこの提案は実装済みであり、ARIN XX での報告によると実際に Origin AS の情報が集まりつつある。

APNIC では、IP アドレスの認可登録の業務の観点よりも、新しい IP アドレスの使用権を示す電子証明書、リソース証明書の開発と標準化に力が入れている。

経路情報の登録機構の利用実験は、Web ページやメーリングリストでのアナウンスに加えて、JANOG でもアナウンスを行った。

実験利用に必要なもの

- JPIRRにオブジェクトを登録する方(オブジェクト登録者)
 - メンテナー名
 - JPIRRにメンテナーを登録している必要があります。
 - S/MIME対応メールソフト
 - Thunderbirdなど
 - USBトークン
 - JPNICより無償でお貸しています。

- IPアドレスの割り振りを受けている方(IP指定事業者)
 - 資源管理証明書(クライアント証明書)
 - 認証強化実験に参加している必要があります。
 - 業務上、IPアドレスに対して経路広告されるメンテナー名を把握しておく必要があります。

図 4-42 利用実験に必要なもの

実験利用には、JPIRR へのメンテナーの登録と、S/MIME 対応のメールソフト、登録機構を使うための USB トークンが必要である。USB トークンは申し込み後に JPNIC から発送しているため、実質的には JPIRR へのメンテナーの登録が必要になる(図 4-42)。

また IP 指定事業者が、認証用の電子証明書を取得している必要がある。

会場でのディスカッション(1)

- 経路ハイジャック(オペミス含む)の対処法
 - ハイジャックされた経路にたいしてmore specificな経路を流す。
 - 経路広告元のASに連絡する。ASに連絡が取れなければ、その国のコミュニティとか上流ISPとかに連絡してみる。
 - オペミスも多い。経路ハイジャック7件。
- 経路情報の登録認可機構に関する意見
 - IRRではオブジェクトがミラーリングされているので、複数のIRRにオブジェクトを登録する必要はないと思う。割り振り元のレジストリにあるIRR (RIPE NCC)には登録しているが、登録された信頼性の高いデータを他のIRRでも見えるようにしたほうが良いのではないか。ASのネットワークのオペレーターがIRRを引いてわかるようなVisibilityが大事。
- IRRを使っているかの挙手結果
 - RADB:10名ほど
 - JPIRR:10名よりは少ない
- IRRの利用に関する意見
 - RADBはインターネット全体に広く知らしめるため
 - JPIRR信頼性の高いデータを蓄積するため、という理由で両方に登録している。

図 4-43 会場でのディスカッション(1)

はじめに、経路ハイジャックが起こったときの対処法について議論が行われた(図4-43)。対処法は経路情報の受け手となる自ASにおける対処法と、経路ハイジャックの発信元と考えられるASに近いネットワークにおける対処法の二つが挙げられた。ハイジャックされた経路に対して、more specificな経路を流すと、各ルータの経路表でハイジャック経路よりもその経路情報が優先されるため、本来のネットワークの接続性を維持できる、実効性の高い方法であるが、ネットワークオペレーターの中にはspecificな経路情報をフィルターしてしまうケースがあり、どの程度の範囲で、どの程度の有効性があるかは定かではない。経路広告元のASに連絡する方法は、より根本的な解決策である。経路の広告元がハイジャックをやめれば被害も止められる。しかし悪質な経路ハイジャックであったり、連絡のつかないようなASであったりすると効力はない。経路ハイジャックの中にはオペレーションミスによるものが多いという意見があげられたが、この後の議論の中で、故意によるものを実際にやられたという情報も寄せられた。

経路情報の登録機構については、IEPGミーティングで出た意見ほど前向きな意見は得られなかった。というのも、JPIRRを利用している理由が、信頼性の高いデータの蓄積という、必須であるとは言えない理由であった。RADb⁷に登録する方がJPIRRよりも実効的であるといったニュアンスが感じられた。特にIRR、特にRADbに対する信頼の置き方がIEPGミーティングでの反応とは異なるようである。

⁷ RADb
<http://www.radb.net/>

会場でのディスカッション(2)

- IRRのメンテナーやAS番号を意識したIPアドレスの管理に関する意見(登録認可機構がワークするか)
 - IPアドレス担当者とIRR担当者は二ホップ以上離れているし、担当者が代わったりするので、人を把握することは難しいと思う。
メンテナー名が必要で、人を覚える必要はない。
 - IPアドレス管理指定事業者とAS番号割り当て先組織は現状バインドしていない。
 - IPアドレスを持っているところがASと経路広告をしているところを渡り歩いているのを見ている。
 - IPアドレス管理指定事業者の担当者にはこの仕組みは複雑すぎて説明してもわからないのではないか。
 - 証明書の仕組みが入るとさらに複雑になるのではないか
いまはPAアドレスという最小限のセットでやっているの
で、要望などを挙げて欲しい。

図 4-44 会場でのディスカッション(2)

次に、経路情報の登録機構が実際に使えるものかどうか、という観点の意見交換を行った(図 4-44)。

挙げた意見は、IP アドレス担当者と IRR 担当者の関係がなくなっているのが難しいという意見を始め、IP アドレスの管理業務を行っているものと AS 番号の管理を行っているものが互いを知らずに業務を行っているという意見が多かった。

これは経路情報の登録機構を使った業務が難しいという意見であると同時に、経路ハイジャックに対して、そして IRR に登録していた route オブジェクトが間違っていたような状況に対して、人的ネットワークを通じた連絡以上の対策が、検討・開発されていないように受け取れた。

今後、ルーティング業務において悪意のあるオペレーターの存在を考える必要があるとすると、RIPE NCC や ARIN、そして APNIC で導入されつつあるような IP アドレスの利用認可の概念を日本国内で普及/啓発していく必要があると考えられる。

4.11. 経路情報の登録機構と JPNIC 認証局の連携

経路情報の登録機構は、これまでに述べた IP アドレスの利用認可という役割の他に、

IRR におけるユーザ認証で使える電子証明書を提供するという役割もある。経路情報の登録機構は内部に認証局機能を持っており、ユーザ管理機能の一環として電子証明書の発行や失効ができる。この認証局機能は 2002 年度以降に構築が行われてきた JPNIC 認証局と連携して行われている。

これは、JPNIC の IP アドレス管理業務における信頼構造に則って各種の業務が行われるような、信頼構造を作る意味を持っている。ユーザ認証に対する信頼性や、登録される情報に対する信頼性は、外部の利用者にとって、広義の JPNIC コミュニティに対する信頼に依存している。JPNIC は業務の信頼性構築の為に、認証基盤を構築し、この基盤に則って業務を行う者に適切な義務を課すことで、業務の信頼性向上が図ることが可能となる。

本節では、JPNIC 認証局が IP アドレス管理業務の中で、経路情報の登録機構とどのように連携しているかについて述べる。

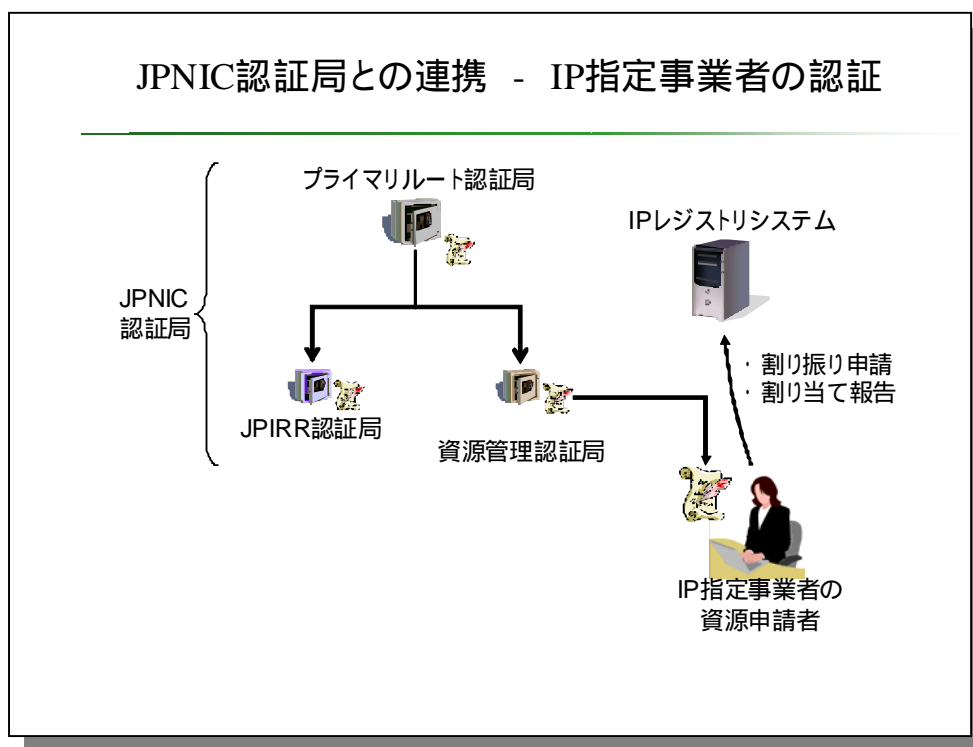


図 4-45 JPNIC 認証局との連携 - IP 指定事業者の認証

まず、許可リストの確認の基盤となる情報は、IP レジストリシステムに登録された IP アドレスの割り振り情報である。従って、IP アドレスの割り振り情報の信頼性確保が重要である。そのために登録者の認証を行い、かつ適切な割り振り業務を行うことが必要になる。

IP レジストリシステムに割り振り申請や割り当て報告を行うのは、IP 指定事業者の資源申請者である。JPNIC 認証局は資源管理認証局を使って資源申請者の電子証明書を発行している。資源申請者の認証は、JPNIC 認証局の信頼点であるプライマリルート認証局を信用することで、オンラインでの認証が可能になる。

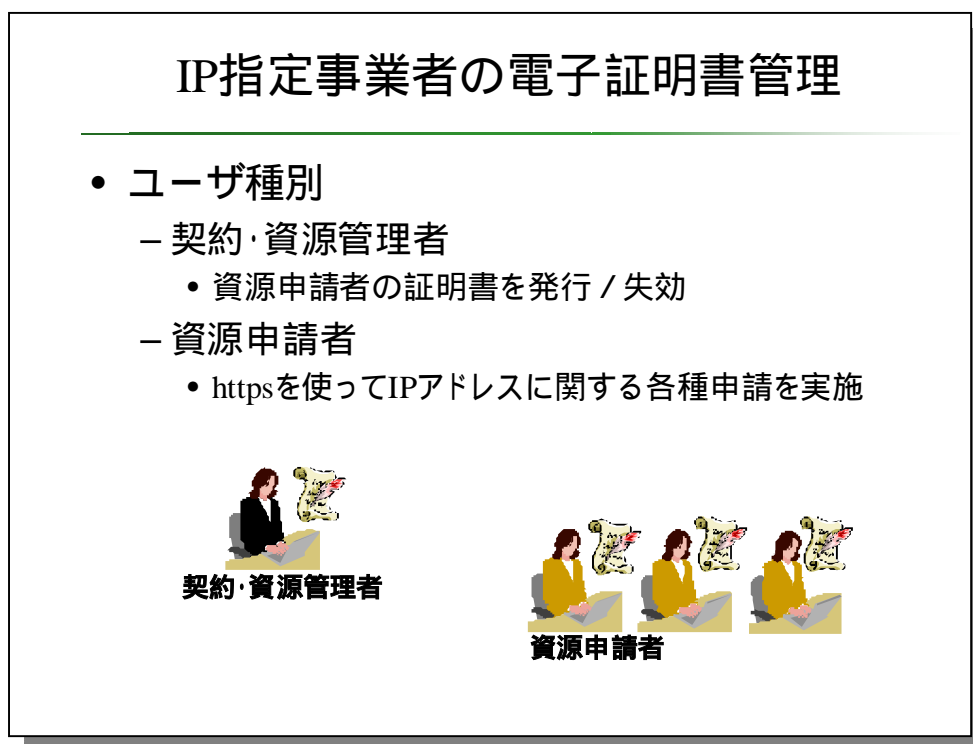


図 4-46 IP 指定事業者の電子証明書管理

資源申請者の証明書は、各 IP 指定事業者に設けられた「契約・資源管理者」によって管理される。これは、資源申請を行う者の本人性確認は、IP 指定事業者内で行われているためである。また JPNIC の申請業務に必要なクレデンシャル（認証に使われるデータ）も同様に IP 指定事業者内の業務管理者によって行われている。資源管理認証局（IP アドレス認証局（認証））は、契約・資源管理者に証明書管理の Web インターフェースを提供している。その Web インターフェースでは、資源申請者の本人性確認を行ってから証明書の発行が行われる。

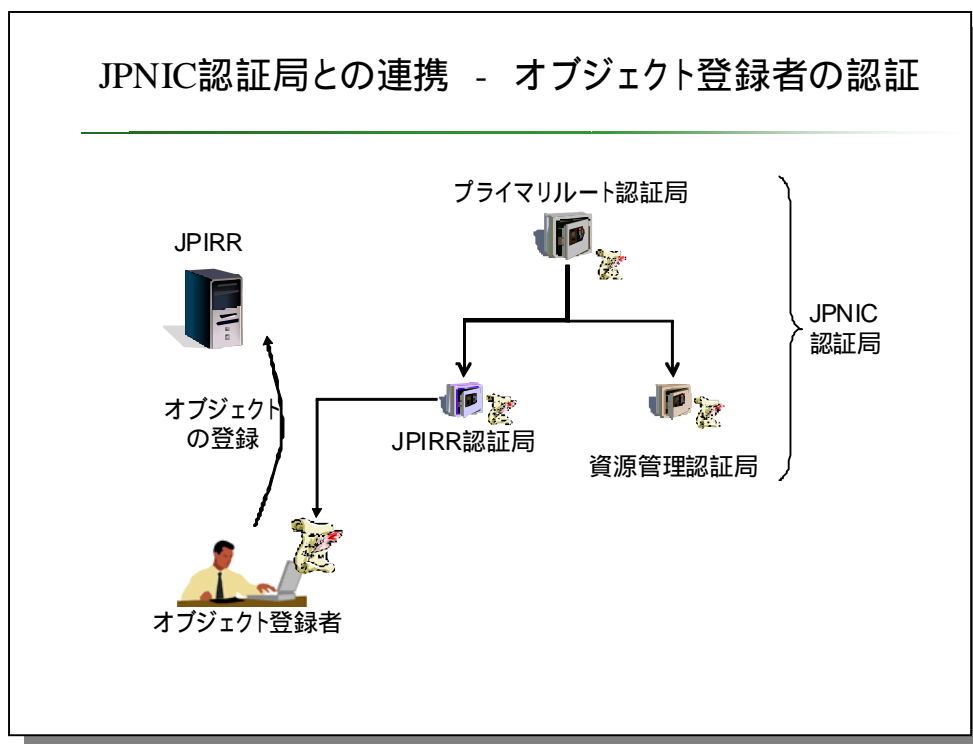


図 4-47 JPNIC 認証局との連携 - オブジェクト登録者の認証

JPIRR における登録者の認証も IP 指定事業者と同様である。JPIRR にオブジェクトを登録するもの「オブジェクト登録者」は、JPIRR 認証局（経路情報の登録機構の一部）の認証業務に則って証明書の発行を受ける。この電子証明書もプライマリルート認証局を信用することでオンラインでの検証が可能になる。

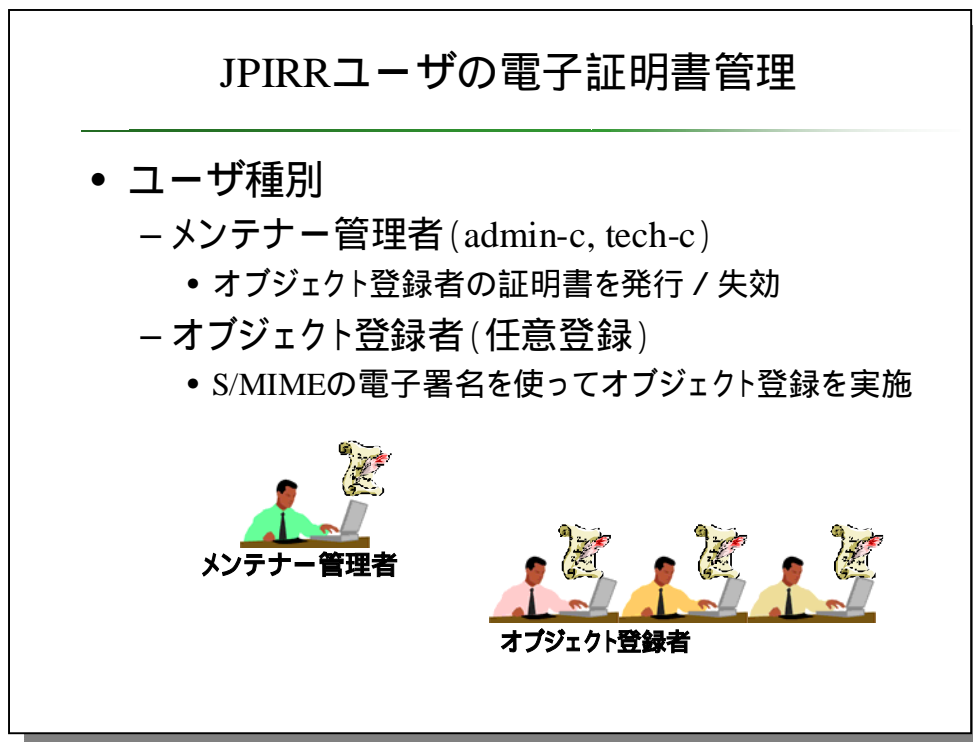


図 4-48 JPIRR ユーザの電子証明書管理

JPIRR のオブジェクト登録者の証明書は、各メンテナーで設けられた「メンテナー管理者」によって行われる。これは IP 指定事業者の場合と同じように、JPIRR にオブジェクト登録を行うユーザの本人性確認は、メンテナーの管理を行っている者によって行われているためである。JPIRR の登録業務に必要なクレデンシャル、パスワードや PGP の鍵の登録なども同様にメンテナーの管理者によって行われている。JPIRR 認証局は、メンテナー管理者に証明書管理の Web インターフェースを提供している。その Web インターフェースでは、オブジェクト登録者の本人性確認を行ってから証明書の発行が行われる。

4.12. 認証業務規程 (CPS) について

JPNIC 認証局の運用にあたり、CPS を策定し、更に業務フローを規定して認証業務を行っている。業務フローは詳細である為ここでは割愛するが、2007 年度にも CPS の見直しを行ったので、紹介する。

認証局は、先に述べた認証基盤を構成する要であり、この運用のレベルによって認証基盤の信頼性が変わる。JPNIC 認証局はプライベートな PKI ドメインを構築しており、業務に合ったレベルの運用を行っている。

レジストリにおける認証局の運用は、RIR コミュニティでも注目されつつあり、IETF

で CPS を閲覧したいという要望があった。IETF の SIDR WG では、リソース証明書のためのレジストリの CPS テンプレートがドキュメント化されており、今後 JPNIC 認証局の CPS との調整も必要になると考えられる。そこで JPIRR 認証局とプライマリルート認証局の CPS の英語訳を作成した。JPIRR 認証局の認証業務規程とその英語訳を Appendix として載せた。

4.13. まとめ

本調査研究のもう一つの柱である「IP アドレス認証の展開」については、JPNIC における認証局を応用した経路情報の登録機構に関する調査研究を行った。経路情報の登録機構は、インターネット経路制御においてルーティング業務担当者に使われている IRR の登録情報を正しく保つ仕組みである。

本調査研究では、本機構の実験運用を行い、フィードバックを通じて明らかになった課題点に対応するための改修を行った。また本機構に関するプレゼンテーションを海外では IEPG で行い、国内では JANOG で行った。そこでのディスカッションの結果、IEPG では高い評価を受ける一方、国内では仕組みが難しそうだという声があがるなどした。

2007 年度、実験運用を開始したわけだが、本機構を本格的に IP アドレス管理業務に組み込むには更に利用者を増やし、利用実験を行う必要があると思われる。今後も実験を継続し、インターネット経路制御に資するような仕組みの確立を目指したい。

第4章 IP アドレス認証の展開に関する調査研究

第 5 章 経路制御のための電子認証技術に 関する国際動向

内容

- IETF SIDR WG の動向
- リソース証明書の動向
- RIR の認証技術に関する動向

5. 経路制御のための電子認証技術に関する国際動向

本調査研究では、経路制御のための電子認証技術の国際動向を調査するため、国際会議に参加して情報共有を行った。参加した会議は、IETF ミーティング、RIPE ミーティング、ARIN ミーティング、APNIC ミーティングである。

本節では経路制御に関連する電子認証技術の国際動向について述べる。国際動向は、わかりやすさのため、一旦スライドにまとめ、それを解説する形で述べる。

5.1. 概要

インターネットにおける経路制御は、国際的なネットワークを通じて行われている。インターネットにおける代表的な経路制御プロトコルは、BGP4 (Border Gateway Protocol) である。インターネットのようなインタードメインの経路制御では、BGP4 のような経路制御プロトコルを使って相互に経路情報を交換している。

インターネットにおける経路制御の安全性を考える場合、国際的に普及されている安全性向上の考え方を取り入れることは肝要である。インターネットは国際的なネットワークであるため、例えば日本だけがセキュアの高い経路制御の仕組みを取り入れることは、相互運用性の観点で難しい。

本調査研究では、国際的な経路制御の電子認証技術について調査を行うため、IETF と RIR のミーティングに参加した。IETF では、2003 年頃より新しいセキュアな経路制御プロトコルの策定が始まっているためである。また RIR では、各 RIR の取り組みに違いはあるものの、各々がセキュアな経路制御に資する仕組みを検討し実装しつつある。

本節では、本調査研究のメインテーマである IRR と電子認証技術に関連する、IETF および RIR (RIPE NCC、ARIN、APNIC) における動向について述べる。

今年度の調査の結果、RIPE NCC は ARIN や APNIC のリソース証明書の開発に参加しつつも、Certification Task Force や CertProto といった委員会活動を通じて、業務面の検討を進めていることがわかった。また ARIN と APNIC は XML ベースのプロトコルを用いた、リソース証明書のプロトタイプシステムの開発を行った。APNIC では 2008 年 3 月に LIR 向けのポータルサイトである MyAPNIC にリソース証明書の機能を実装した。APNIC におけるリソース証明書は、経路制御の安全性向上よりも先に、IP アドレスの使用権を示す署名付データとして捉えられている。

IETF SIDR WG では、APNIC と ARIN のプロトタイプで採用されているような XML ベースのプロトコルの策定とは方向性が異なり、ルータにおけるリソース証明書の検証に話題が絞られてきた。

第 5 章 経路制御のための電子認証技術に関する国際動向

RIPE NCC とは、大手 ISP のメンバーとオフィスを訪問し、IRR の技術的な信頼性向上策について情報交換を行った。RIPE NCC でも IRR の運用上の信頼性向上は取り組み課題となっており、相互の技術交流が可能であることを確認した。

このように、IP アドレスの管理の信頼性向上と IRR の運用上の信頼性向上を図る活動は、IETF および RIR において進みつつあると言える。本調査研究の一環として開発を行った経路情報の登録機構は、IRR とリソース証明書への発展を考慮したシステムである。国際的な動向に合わせて、JPIRR のユーザに経路制御の安全性向上策に必要な仕組みを提供できるようにして行きたい。

5.2. IETF SIDR WG の動向

IETF SIDR (Secure Inter-Domain Routing) WG は、新しいセキュアなインターネットの経路制御アーキテクチャを策定することを目的とした WG¹である。

2007 年度は、リソース証明書を用いたセキュアな経路制御の方式の検討が行われた。リソース証明書がルータにおいて機能する全体像としたときの、2007 年度の SIDR WG の状況を以下に示す。

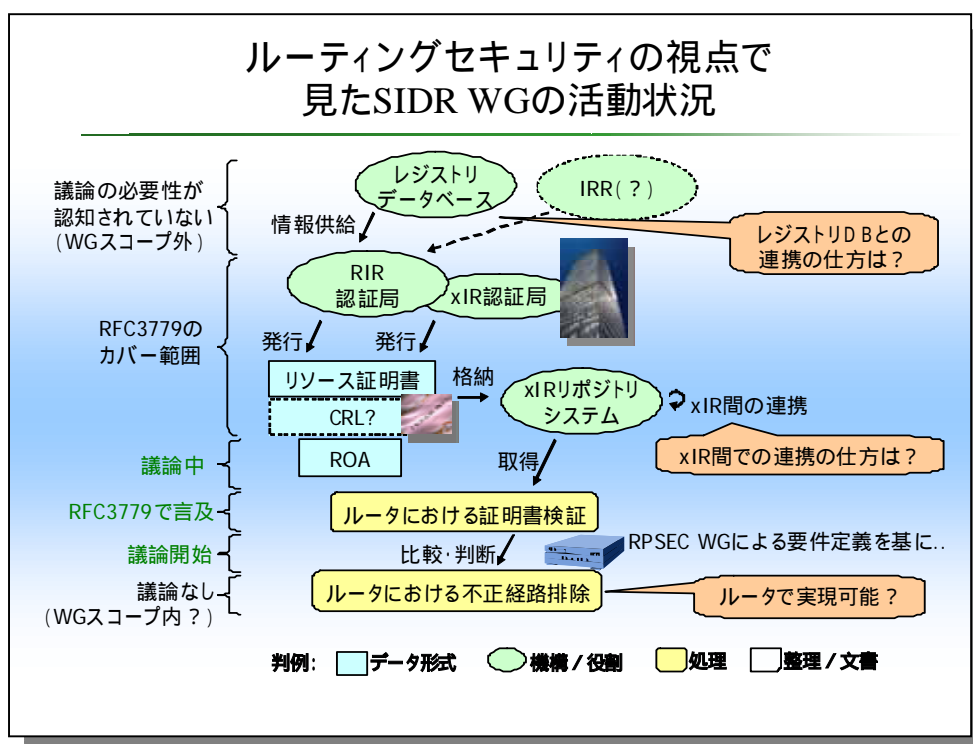


図 5-1 ルーティングセキュリティの視点で見た SIDR WG の活動状況

図 5-1 は、レジストリデータベースに基づいて発行されたリソース証明書が、ルータに取り込まれて検証され、インターネットにおける経路制御がセキュアに行われるまでの情報と処理の流れを示したものである。SIDR WG では、RFC3779²という書式に則った議論が行われているが、2007 年度は、主に ROA (Route Origination Authorization) のデータオブジェクトの要件に関する議論や、リソース証明書の検証方式に関する議論が行われた。

¹ Secure Inter-Domain Routing (sidr)
<http://www.ietf.org/html.charters/sidr-charter.html>
² X.509 Extensions for IP Addresses and AS Identifiers
<http://www.ietf.org/rfc/rfc3779.txt>

第5章 経路制御のための電子認証技術に関する国際動向

しかし、今の段階では大きな三つの課題があると考えられる。これまでの進捗状況から、これらがすぐに解決されるとは考えにくい。ここでは今後の方向性として各々について述べる。

一つ目は、レジストリデータベースとの連携方法である。リソース証明書はレジストリの割り振りや割り当てと同じ内容を持つ電子証明書である。従って、証明書発行システムはIPレジストリシステムと連携している必要がある。ARINやAPNICでは、一部の連携の為に検討が始まっているが、それは技術的な連携方法に留まっている。例えば返却時の処理や、発行の時間的な粒度については、今後議論し、決定していく必要がある。

二つ目は、インターネットレジストリ間の連携方法である。IPアドレスの割り振り先で証明書発行が起こると、その証明書データを提供するリポジトリに発行された証明書が格納される必要がある。そのためインターネットレジストリ間、例えばAPNICとJPNICの間で発行された電子証明書を交換する仕組みが必要になる。APNICとARINで開発されているプロトタイプシステムではXMLベースのプロトコルが使われることになっている。(実装状況は明らかになっていないが、相互運用が実験できる状態にはまだなっていない)

三つ目はルータにおけるリソース証明書の検証である。ルータにおけるリソース証明書の検証については議論が行われているが、有効性が確認された証明書を使って実際の経路制御のどのようなコントロールを行うかは定かになっていない。証明書の有効性が確認できなくなったときに、急にルータがそのprefixを経路表から削除してしまうと、電子証明書に依存しすぎ、管理業務が高くなりすぎてしまう恐れがある。

次に、2007年度に行われた各回のIETF SIDR WGの状況について述べる。

5.3. 第69回 IETF SIDR (Secure Inter-Domain Routing) WG

SIDR WGは5日目の朝、9時から10時45分まで行われた。SIDR WGは、インターネットにおけるドメイン間(AS間)の経路制御をセキュアに行う仕組みを検討しているWGである。今回のWGでは、主にドキュメントの更新に関する議論が行われた。

第69回IETFにおけるSIDR WGの概要

- Secure Inter-Domain Routing WG
 - 7/26 9:00-10:45、100名程
 - Agenda
 - Action Item Update – Sandy Murphy
 - Architecture update – Steve Kent
 - CP/CPS update – Steve Kent
 - Resource Certificates update – Geoff Huston
 - ROA update – Matt Lepinski
 - Private AS space – Sandy Murphy
 - ドキュメントステータス
 - すべて(6つ)Internet-Draftの状態

図 5-2 第 69 回 IETF における SIDR WG の概要

現在、SIDR WG で行われている議論は大きく分けて三つある。一つ目は RFC3779 を使ってセキュアなルーティングを実現するアーキテクチャをドキュメント化するための議論である。二つ目はリソース証明書を発行する認証局の CP(Certificate Policies)と CPS に関する議論で、Stephen Kent 氏を中心に議論が進められている。三つ目は ROA(Route Origination Authorization)の書式と取り扱いに関する議論である。

SIDR のアーキテクチャについては、継続して行われている議論がいくつもある。

SIDR WGにおけるAction Itemと議論
～アーキテクチャドキュメント～

- アーキテクチャドキュメント
 - 経路集約が可能な複数のリソース証明書を発行することのドキュメント上の扱いを明確化する 議論を継続
 - リソース証明書のURIとして“rync”と記述されていることをどう扱うか(needs volunteers) 議論を継続
 - ryncだけが選択肢ではない
 - アプリケーションADによるとURIとして登録は可能
 - Informational RFCにすべきかStandards Trackにすべきかの判断 今回は議論なし
 - 4バイトAS番号に関する技術の追加 済み

図 5-3 SIDR WG における Action Item と議論
～アーキテクチャドキュメント～

まず、経路集約が可能な隣接する IP アドレスのリソース証明書をどのように扱うかという議論がある。単一の ISP に対してレジストリが複数の IP アドレスブロックを割り当てている場合、ISP は集約(route aggregation)された経路を広告することが考えられます。しかしリソース証明書は割り振りブロックを含んだ形で発行されるので、広告される経路情報とリソース証明書が一對一で対応しない。すると集約されたプリフィックスの正しさを検証できないことになってしまう。この件については会場ではあまり議論されず、ML で継続して議論が行われることになった。

他に、リソース証明書と CRL を示す URL で rync をプロトコルとして使うことが提案されているが、書式上認められるか、という議論も進行中で、今は作業を担当する人を探している段階である。WG のマイルストーンによるとアーキテクチャは 2007 年 3 月には RFC 化が目指される予定であるが、大幅に遅れてしまっているようである。なお 4 バイト AS 番号については既に対応済みである。

An Infrastructure to Support Secure Internet Routing

draft-ietf-sidr-arch-01.txt

この他に、リソース PKI のための CPS と ROA に含まれる prefix の比較ルールなどについて議論が行われた。

SIDR WGにおけるAction Itemと議論 ～ その他の議論 ～

- CPSのドラフト
 - Internet-Draftの期限(6ヶ月)内でfixさせる種類のドキュメントではないという懸念の解消、位置づけの明確化 議論を継続
- ROA prefixの比較ルール
 - ROAに含まれるprefixとNLRIの比較はどういうルールで行うか 仕様上は記述しないことにする
- その他
 - RIPE DBと他のRIRのDBの構造の違いに関するコメントに対する回答 議論なし(SIDR WGのスコープ外?)

ROA - Route Origination Authorization
リソース証明書を使って作られる署名付きデータオブジェクト。ASとprefixが入っており、「ASからprefixが経路広告することが認可 authorizeされている」ことを証明。

NLRI - Network Layer Reachability Information
BGP Updateメッセージに含まれる「到達可能なアドレス」の情報。
補足: BGPメッセージの種類 {OPEN, UPDATE, NOTIFICATION, KEEPALIVE, ROUTE-REFRESH}
補足: BGP Updateに含まれる情報: パス属性、NLRI、Withdrawn Routes

図 5-4 SIDR WG における Action Item と議論
～ その他の議論 ～

CPS については、本ドキュメントの策定の時間的な制約に関する議論が行われた。提案者である Stephen Kent 氏によると、本ドキュメントは、リソース証明書を発行する認証局が構築され始める頃には必ず必要になるが、Internet-Draft の有効期限は 6 ヶ月であり、この期限内で有意義な議論が進めることができるか、という疑問が Stephen Kent 氏自身にもあるそうである。議論の結果、今後、ドキュメントの位置づけを明確化することが課題になった。

ROA については、ROA に含まれる prefix と検証の対象である BGP Update に含まれる NLRI との比較ルールについて議論が行われた。前回の SIDR WG では、ROA に内包される prefix が NLRI に含まれるのであればよい、という方向になっていたが、前述の経路集約の問題があり、ROA として比較ルールを定めることは難しいことがわかってきた。ひとまず ROA のドキュメントでは比較ルールを記述しないことになった。

A Profile for Route Origin Authorizations (ROAs)

第 5 章 経路制御のための電子認証技術に関する国際動向

draft-ietf-sidr-res-certs-08.txt

最後に、"Private AS space"というタイトルでチェアの Sandra Murphy 氏よりプレゼンテーションがあった。これは AS 内のプライベートな経路制御のためにユニークローカルアドレス(RFC4193)を使う場合、リソース証明書をどこが発行すればよいのか、という疑問の投げかけである。これはリソース証明書のトラストアンカー(trust anchor - 信頼点)の議論に密接に関係するため、トラストアンカーとして何を想定すべきか、という議論に発展した。IANA をトラストアンカーとして想定すると、RIR への追加割り振りがあった場合にユーザ環境のトラストアンカー証明書を入れ替える必要がなく、手続きは簡単である。また、本来、トラストアンカーは RP(Relying Party - 証明書検証者)によって選ばれることが望ましくもある。しかし現在の IANA にはトラストアンカー認証局を提供する役割がなく、RIR の認証局で対応せざるを得ないのが現状である。

5.4. 第 70 回 IETF SIDR WG

SIDR WG は第一日目の 2007 年 12 月 3 日(月)15 時 25 分から行われた。

第70回IETFにおけるSIDR WGの概要

- Secure Inter-Domain Routing WG
 - 12/3 15:25-17:20、90名程
 - Agenda
 - Administrivia – Sandy Murphy
 - Updates on Draft
 - CP/CPS update – Steve Kent
 - Route Originations - Matt Lepinski
 - Resource Certificates – Geoff Huston
 - New topics
 - Manifests - Steve Kent
 - Rescerts Provisioning - Geoff Huston

図 5-5 第 70 回 IETF における SIDR WG の概要

SIDR WG では既存のドラフトドキュメントの更新に関する議論が三つ、新しいトピックに関する議論が二つあった。既存のドラフトドキュメントの更新に関する議論があった。

SIDR WGにおけるAction Itemと議論(1 / 3)

- Architecture
 - draft-ietf-sidr-arch-02.txt
- Route Originations
 - prefixに対する経路広告元の正当性
 - Draft-ietf-sidr-roa-format-01.txt
- 議論
 - CPとCPSのドキュメント
 - 関係するレジストリの立場の人はコメントを要請(チェア)
 - プライベートアドレスのPath Validation
 - IANAがTrust Anchorでなくてもよいが記述は行う。
 - 複数の証明書パスで単一のprefixの処理
 - 広告されるprefixとROAのprefixが異なる場合にどうするかの問題
 - 今後、選択肢を含むproposalを明確にして検討

図 5-6 SIDR WG における Action Item と議論 (1 / 3)

CP/CPS update

特に内容が update されたわけではないが、インターネットレジストリなどの関係する組織の人はコメントをするように要請があった。

Architecture と Route Originations

リソース証明書のツリーの末端に位置づけられる、ROA(Route Origination Authorizations)に関する議論である。

今回はプライベートアドレスを含む ROA の扱いについて議論された。プライベートアドレスについて、IANA をトラストアンカーとするリソース証明書を発行する必要がないのではないか、各機器がトラストアンカーを定められるような証明書ツリーを構築できるようにすべきでは、という議論である。結局、IANA をトラストアンカーにしなくてもよいが、ドキュメントではIANAについて言及することになった。

複数の証明書パスで単一の prefix の処理

経路広告される prefix と ROA に含まれる prefix が異なる場合に、ルータはどのように処理すべきか、という議論である。例えば、複数の prefix について経路集約を行う場

合、インターネットレジストリの構造に合わせて発行されたリソース証明書と prefix が一致しないことが考えられる。正しく発行されたリソース証明書が実際の正しい経路広告をうまく扱えなければならない。

会場では更に、更に複数のインターネットレジストリ、例えば歴史的 PI の経路集約をどう扱うかといった議論になった。今後、方式の選択肢の提示を含め、提案内容を固めてから議論が進められることになった。

リソース証明書に含まれる prefix の処理

現行のリソース証明書の仕様では、上位 CA が階層ごとに IP アドレスと AS 番号を内包していく構造になっている必要がある。従って、リソース証明書を検証する段階で、両方の包含関係が必ず両立する必要がある。

SIDR WGにおけるAction Itemと議論(2 / 3)

- Certificates
 - draft-ietf-sidr-res-certs-09.txt
 - リソース証明書の要件(RFC3779よりも詳細)
- 議論
 - Geoff Huston氏の新たな提案
 - 上位CAが階層ごとにIPアドレスとAS番号を内包していく構造だと割り振り/割り当ては、両方の包含関係が必ず両立する必要がある。これを避けたい。
 - より上位のCAが、リソースを包含していればよいことにする提案。
 - 意見
 - Trust Anchorを選ぶのはRelying Partyだが、これを定めるとパスを想定してしまうことになってしまう。
 - パス検証を上位CAから下位に向かって行う結果と末端から上位に向かって行う方法で結果が同じであるべき。

図 5-7 SIDR WG における Action Item と議論 (2 / 3)

この仕様を緩め、より上位(すなわち上位の上位など)の CA のリソース証明書が、リソースを包含していればよいことにする提案が、APNIC の Geoff Huston 氏によって行われた。会場ではパス検証の結果が、ツリーの上から行う場合と下から行う場合とで変わってしまうのは良くない、などの議論が行われたが、ML で継続議論される模様である。

SIDR WGにおけるAction Itemと議論(3 / 3)

- New topic
 - Manifests
 - <http://www.potaroo.net/drafts/draft-ietf-sidr-rpki-manifests-00.txt>
 - リポジトリに入っているオブジェクト一覧に署名をしたもの。オブジェクトの削除を知らせるため。
 - CAとEEの両方が発行しうる。発行されたManifestは発行者のリポジトリに入る。
 - Manifestsに関する議論
 - Warningの種類が増えすぎないか
 - George Michaelson氏のシミュレーションでは、リソース証明書は数千になる。利用性の確保ができるのかわからない。WG ItemとするかどうかはMLにて議論中。12/24までに反応。
 - Rescerts Provisioning
 - <http://www.potaroo.net/drafts/draft-ietf-sidr-rescerts-provisioning-00.txt>
 - レジストリとISPの間の証明書管理のやり取りのプロトコル WG Itemとなった。

図 5-8 SIDR WG における Action Item と議論 (3 / 3)

新しいトピックとしては、以下の二つがあった。各々について、WG の working item として採用するかどうかの問いかけ、WG チェアから行われたが、いずれも ML で意見収集を行うことになった。

Manifest とはリポジトリに入っているオブジェクト一覧に署名をしたもので、CRL より早く、証明書検証者に対してオブジェクトの削除を知らせることを目的としたデータである。

会場では、証明書検証に関わる Warning(警告)すべき状態が増えすぎないか、リソース証明書の数は多いために CRL を含めて、利用可能性について検証する必要がある、といった意見が出された。WG の working item とするかどうかについては、12 月 24 日までに ML で意見収集を行い決定していくことになった。

リソース証明書を発行するインターネットレジストリと証明書申請者の間で、証明書管理(発行や失効など)のために使われるプロトコルの提案である。これについては会場では議論は多くなく、WG の working item となった。

SIDR WG は、リソース証明書のルータにおける仕様に関して、これまでにあまり多くの議論がされてきていなかった。今回は、経路集約を踏まえたルータの挙動について議論されており、徐々にではあるが、実用化に向けた動きが見えてきた。しかし Manifest

などの、新しい処理を要するプロトコルが追加され、リソース証明書を扱うプログラムの全体像にたどり着くには、まだ時間がかかりそうである。

5.5. リソース証明書に関する RIR の相互運用実験

第 70 回 IETF では、APNIC、RIPE NCC、ARIN で、リソース証明書の相互運用実験が行われた。結果的に、APNIC と ARIN が開発を行っているプロトタイプシステムの動作検証が行われるに留まった。

リソース証明書に関するRIRの相互運用 実験について

- 実験内容
 - ARINとISC、APNICを中心として開発しているリソース証明書の発行管理システムの動作検証
 - リソース証明書の発行と失効、CRLの発行、マニフェストの発行。
 - リソース証明書の発行・管理システムは、ARINを中心に行っている検討資料の通り、SQLデータベースとXMLベースのトランザクション
- 概要
 - 実験期間
 - IETF期間中、特に時間を区切らずに実施(オンラインを含む)
 - 参加者
 - ISC、APNIC、APNIC、BBN、RIPE NCC、ARIN、IJJ
- 実験結果
 - リソース証明書の発行と失効、CRLの発行、マニフェストの発行は問題なく動作
 - CRLの発行に、一部のシリアル番号が入っていない問題等(原因不明)
- きっかけ
 - 以前より情報交換をしていたRandy Bush氏がJPNICにこられ、RIRのリソース証明書関連の活動にJPNICも参加するように話をもちかけられた。

図 5-9 リソース証明書に関する RIR の相互運用実験について

CRL の発行に、一部問題があったものの、リソース証明書の発行および失効の操作については問題なく行うことができたという報告があった。

5.6. 国際会議 IEPG での発表

第 70 回 IETF の前日に行われた IEPG ミーティングで、経路情報の登録機構に関するプレゼンテーションを行った。

第70回IETF前のIEPG Meeting

- 4-byte ASes and the view from the 2-Byte AS BGP World, Geoff Huston, APNIC
 - 4バイトAS番号と2バイトAS番号が混ざったとき、BGPの経路制御はどうか？
- BGP Damping, Geoff Huston, APNIC
 - BGPの限界と言われている性能要素を確認するため、BGPパケットを収集・分析
- Authorization Mechanisms in Internet Routing Registries, Kimura Taiji, JPNIC
 - 経路情報の登録認可機構を紹介
- "Unusual nature" of j.gltld.biz, Edward Lewis, Neustar
 - IPv6のみで運用しているgTLDサーバにまつわる話
- Mapping fun, Roy Arends, Nominet UK
 - DNSのOpen resolverをグラフィカルなIPアドレス空間の中で描画。特定のprefixをズームアップするなどのデモ

図 5-10 第70回 IETF 前の IEPG Meeting

今回の IEPG ミーティングでは、4 バイト AS や BGP の経路情報の解析など、インターネットメインルーティングに関する発表が APNIC の Geoff Huston 氏によって行われた。経路情報の登録機構に関する発表は、その話題に引き続いて行われた。

IEPGミーティングにおける経路情報の登録 認可機構のプレゼンについて

- 発表内容
 - 経路情報の登録機構の目的 / 仕組み / 論点 など
- 会場での議論
 - コメント
 - 活動をencourage
 - APNIC, ISC, RIPE NCC
 - 許可リストの状態に関して
 - 「要件」と「チェック機構」が必要であるというコメント(後者は既に開発済み)
 - リソース証明書との関係
 - 本機構とリソース証明書の仕組みは親和性がある(APNIC)
 - 議論
 - RIRと比べた、本機構の位置づけについて議論した。
 - (単なるキャッチアップではないか、という問いかけに対して)

図 5-11 IEPG ミーティングにおける経路情報の登録
認可機構のプレゼンについて

IEPG ミーティングにおけるプレゼンテーションの結果、まず複数の参加者より本機構を使った実験に関する encourage するという意見を頂いた。この意見は、ISC(Internet Systems Consortium)、APNIC、RIPE NCC からの参加者から頂いた。プレゼンテーションについては、特に許可リストの正当性についてディスカッションが行われた。

5.7. RIPE NCC における動向

RIPE NCC における経路制御のセキュリティに関する動向調査のため、第 54 回 RIPE ミーティング及び第 55 回 RIPE ミーティングに参加した。

RIPE NCC では、mnt-route、mnt-lower といった IP アドレスの利用認可の機構が既に運用されており、IP アドレスの利用認可という意味では先進的な IP レジストリシステムを有している。またリソース証明書の開発プロジェクトにも参画しており、LIR を交えた検討を行っている。2007 年度は、特にリソース証明書の業務面での影響に着目し、二つのチームを作成して調査を行った。

一つは Certification Task Force (CA-TF) である。CA-TF は、RIPE 地域の LIR からリソース証明書に興味のある参加者を募り、RIPE 地域におけるリソース証明書の影

第 5 章 経路制御のための電子認証技術に関する国際動向

響や意義について検討を行うチームである。CA-TF は、2008 年 1 月にホワイトペーパーを作成した。ホワイトペーパーでは、リソース証明書の提供方法と、リソース証明書を使ったルーティング、IP アドレスの再割り振りの方法などについて、基本的な情報がまとめられている。

もう一つは CertProto である。CertProto は CA-TF をサポートし、RIPE NCC 内でリソース証明書を扱う業務の実現性を検討する目的で作られた。実際にリソース証明書を発行するプロトタイプ業務システムが作られ、RIPE NCC の各セクションのスタッフによって既存の業務との変更点や課題点が RIPE NCC 内部でまとめられた。今後、CertDeploy というチームが作られ、RIPE NCC 内でリソース証明書を扱うためのポリシー調整、料金などに関する検討が進められる。

次節以降では、各 RIPE ミーティングでの議論の詳細について述べる。

5.8. 第 54 回 RIPE ミーティング

第 54 回 RIPE ミーティングは、2007 年 5 月 7 日～5 月 11 日、エストニアのタリンで開催された。

第54回RIPEミーティング

- ミーティング概要
 - 2007年5月7日(月)～5月11日(金)
 - 参加登録者数(参加者リストより集計)
 - 304名
 - 41ヶ国



図 5-12 第54回 RIPE ミーティング

今回の RIPE ミーティングは、規模は 300 名ほどと大きくないものの、参加国数は 40 カ国と多かった。RIPE 地域には多くの国が含まれていることから、毎回参加国数は多いようである。

リソース証明書に関しては、まず CA-TF の活動紹介が行われた。

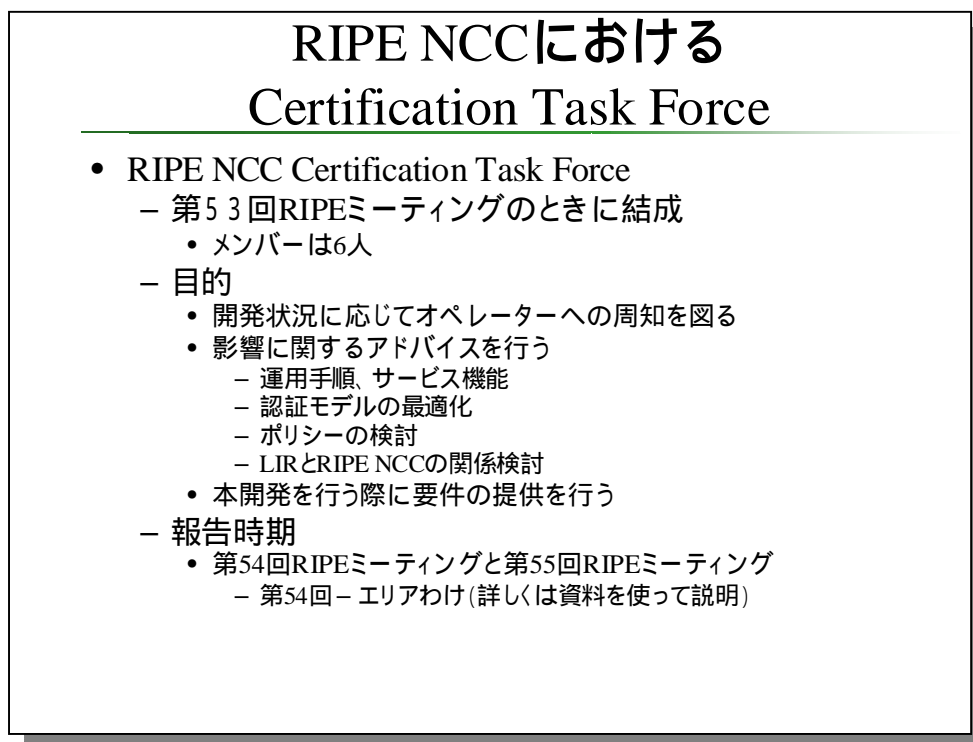


図 5-13 RIPE NCC における Certification Task Force

Certification Task Force は、第 53 回 RIPE ミーティングのときに結成されたもので、LIR 中の希望者によって構成されている。RIPE 地域の ISP のオペレーターにリソース証明書に関する周知を図ったり、RIPE NCC に対して、リソース証明書の影響などに関するアドバイスを行ったりするとされている。

第 54 回 RIPE ミーティングでは、CA-TF の 1 回目となる報告が行われた。発表によると、下記五つのエリアにわけて調査と議論が行われている。

CA-TF で活動中の五つの調査・検討エリア：

ビジネスエリア (ポリシーを含む)

認証と業務上の関連性(エンドユーザや PI アドレスの割り当て先)、ERX や RIR 間におけるアドレス資源の移転に関する事項を扱う。

サービスエリア

公開用の証明書データベースとしての証明書リポジトリやリソース証明書の検証サービスに関する事項を扱う。

テクニカルエリア

証明書リポジトリのアーキテクチャや性能の影響に関する事項を扱う。

RIR エリア

信頼点 (trust anchors) や導入プランに関する事項を扱う。

アプリケーションエリア

ルーティングにおける IP アドレスの認可 (authorization) や RPSL との互換性、準備の自動化などに関する事項を扱う。

今回は評価の結果や内容については報告されておらず、第 55 回 RIPE ミーティングで結果報告のドキュメントが公開されることになっている。結果として、2008 年 1 月にホワイトペーパーが出され、更に RIPE NCC における適用に関する議論も行われた。

また今回、CertProto チームについても紹介された。CertProto プロジェクトは、リソース証明書のシステム評価を行う RIPE NCC 内部のプロジェクトで、CA-TF と同じ 3 日目の NCC Services WG において、RIPE NCC の Henk Uijterwaal 氏によって活動内容が紹介された。CertProto プロジェクトは 2007 年 1 月頃に始められたもので、CA-TF の活動促進と RIPE NCC 内部でのリソース証明書についての理解を深めることを目的としている。

第54回RIPEミーティングにおける CertProtoチームの紹介

- CertProto
 - RIPE NCCの関係部署からメンバーを集め、様々な観点でリソース証明書システムの理解を図るプロジェクト
 - Certification Task Forceを補助する役割もある
 - 活動期間: 2007年1月～2007年6月(計画)
 - 活動内容
 - 最低限のプロトタイプシステムを導入
 - 業務手順を検討
 - 課題を列挙、要件事項をまとめ

図 5-14 第 54 回 RIPE ミーティングにおける CertProto チームの紹介

活動の一環として、プロトタイプシステムの構築や、業務プロセスの仮構築が行われている。プロジェクトメンバーは、RIPE NCC の各部から選ばれたスタッフで構成されている。

CertProto プロジェクトの注目すべきところは、本番用のシステム開発を行う前に試験利用のためのシステムを開発し、このシステムを使うことでスタッフがリソース証明書の業務プロセスを理解する工程が入っている点である。これによって、RIPE NCC でリソース証明書のサービスを行う場合に、業務を変更するための課題やシナリオを具体化しやすくなると考えられる。これまでの APNIC や ARIN の活動状況をみる限り、このような活動は RIPE NCC でしか行われていない。

RIPE ミーティングでは、IPv4 アドレスの枯渇の問題や IPv6 関連の話題もあった。

IPv4 アドレス枯渇関連の話題

- 2007-03: IPv4 Countdown
 - コンセンサスには至らなかった。
 - 適切なアクションは必要とされた。
- IPv4 lifetime
 - APNIC Geoff Huston 氏による IPv4 アドレスの枯渇時期のアップデートに関するプレゼンテーション

図 5-15 IPv4 アドレス枯渇関連の話題

IPv4 アドレスの枯渇については、JPNIC を中心として提案された IPv4 Countdown ポリシーである。これは IANA から RIR への最後のブロックの割り振り方に関するポリシーである。コンセンサスには至らなかったが、このポリシーで取り組もうとしている割り振りの課題について、適切なアクションを取ることが必要であるという認識を広める結果になった。

また APNIC の Geoff Huston 氏より「IPv4 lifetime (IPv4 アドレスの寿命)」と題してプレゼンテーションが行われた。IPv4 アドレスの枯渇時期の予測にあたって、より現状に近くなるような式を当てはめた結果、枯渇時期が前倒しになったというプレゼンテーションである。いずれにしても予測される時期は 2011 年頃である。

IPv6 については三つほどのプレゼンテーションがあった。

IPv6関連の話題

- The Cost of Not Deploying IPv6, Jordi Palet
 - IPv6非対応のコスト
 - 教育、ネットワーク対応、デュアルスタックの運用
- IPv6 deployment in reality, Juan Pedro Cerezo
 - IPv6利用中のサーバの国別の数や増加率
 - 著名なサーバのIPv6対応状況
- IPv6 Routing Update
 - IPv6経路エントリ数の動向
 - 6Boneの収束、/24の増加傾向など

図 5-16 IPv6 関連の話題

「The Cost of Not Deploying IPv6」は、IPv6 を利用しない場合には、IPv4 のみのネットワークを維持し続けるよりもコストがかかる、というプレゼンテーションである。発表者の Jordi Palet 氏は、IPv6 の普及の為にこのようなプレゼンテーションを各 RIR で行っており、またチュートリアルにも力を入れている人物である。

「IPv6 deployment in reality」は、IPv6 の利用状況を簡単な統計データを元に紹介したものである。増加傾向はあるものの、国に依存する様子が伺われた。またインターネットレジストリや著名な検索エンジンの Web サーバで、IPv6 が使われていないような意外な事実も紹介された。

「IPv6 Routing Update」は、IPv6 の経路表の統計データなどについて述べたものである。6bone のプロジェクトが終わったことの影響が経路表から見て取れたり、/24 の経路情報の増加傾向がわかるような説明が行われた。

その他に、インターネットに関わるいくつかの話題についてもプレゼンテーションが行われた。

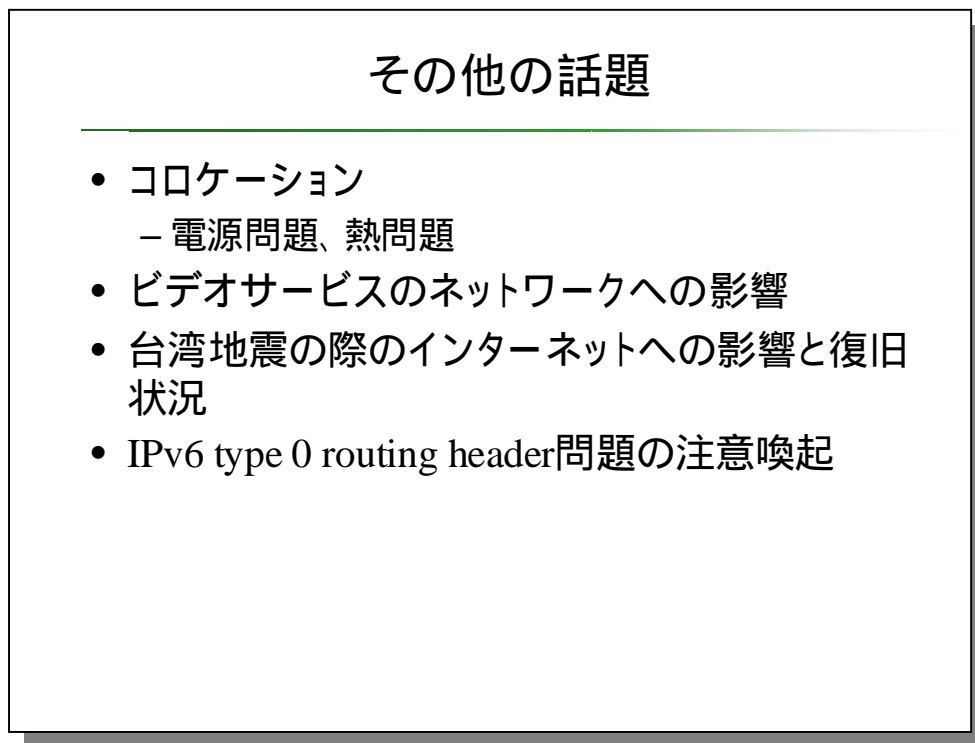


図 5-17 その他の話題

RIPE ミーティングの参加者には LIR が多く、従ってサーバ設備を持つ ISP であることも多い。最初の「コロケーション」では米国にある巨大なデータセンターにおいて取り組まれている電源問題や熱問題について紹介された。

RIPE 地域では、各種ビデオストリーミングサービスのサービス形態が日本とは大きく異なっている。ヨーロッパ地域全体という視点では、日本のように ISP に共通のネットワーク基盤が存在するわけではないので、各 ISP がネットワーク帯域等を考慮したコンテンツデリバリーネットワークを検討し、構築する必要がある。ネットワーク帯域とユーザ数を考慮して、いくつかのコスト対収容可能顧客数のモデルが示されていた。コンテンツ提供側との接続をよくすると維持費がかかるが、より高品質なビデオサービスを提供できることになり、顧客獲得に繋がりやすい。

この他に、他に台湾でおきた地震の影響でインターネット経路制御が変化した様子を統計データを元に示したプレゼンテーションなどが行われた。

5.9. 第 55 回 RIPE ミーティング

第 55 回 RIPE ミーティングは、2007 年 10 月 22 日～10 月 26 日、オランダのアムステルダムで行われた。会場は RIPE NCC のオフィスに歩いて行ける距離にある

Krasnapolsky ホテルである。

第55回RIPEミーティング

- ミーティング概要

- 2007年10月22日(月) ~ 10月26日(金)

- 参加登録者数

- 375名

- 40ヶ国



図 5-18 第55回 RIPE ミーティング

第55回 RIPE ミーティングでは、リソース証明書の動向の調査などと共に、IRRの信頼性向上に関する研究を行っている NTT コミュニケーションズ社と RIPE NCC を訪問し情報交換を行った。

RIPE NCCのデータベースグループとの 情報交換

- 概要
 - IRR サーバの信頼性向上に関する技術的な情報交換を、2007年10月23日、RIPE NCCのオフィスにて行った。
 - 参加者
 - RIPE NCC側: データベースグループ、Jos氏、Agoston氏、Luis氏
 - 日本側: NTTコミュニケーションズ社 吉田氏、白崎氏、JPNIC 木村
 - ディスカッションの内容
 - NTTコミュニケーションズ社とJPNICにおける取り組み
 - RIPE NCCにおける取り組み
 - JPNICを含めた今後の協力関係に関する議論

図 5-19 RIPE NCC のデータベースグループとの情報交換

本調査研究の経路情報の登録機構を使って登録情報の正当性の維持を図ると共に、NTT コミュニケーションズ社が開発中の IRR サーバシステムを用いると運用の冗長性を確保するというアイデアがある。

ディスカッションの結果、RIPE NCC でも IRR システムの信頼性向上を課題としており、可能であれば技術的に協力関係を築きたいという意向であることがわかった。

5.10. RIPE Certification Task Force

第 55 回 RIPE ミーティングの初日に、RIPE Certification Task Force に関するミーティングが行われた。このミーティングはインフォーマルに行われたが、議事についての情報は RIPE ミーティング期間中に得ることができた。以下、概要を示す。

RIPE Certification Task Force ミーティング (1)

- アジェンダ
 - APNICの活動状況の報告
 - ARINの開発状況の報告
 - RIPE NCCの活動状況の報告

図 5-20 RIPE Certification Task Force ミーティング (1)

今回のミーティングは、リソース証明書について活動を行っている各 RIR の活動状況を報告することが主な議題であった。はじめに APNIC が活動状況を報告し、その次には ARIN が、最後に RIPE NCC が活動報告を行った。

APNIC の報告の概要を以下に示す。

RIPE Certification Task Forceミーティング(2)

- APNICの活動状況
 - APNIC内部で開発を実施している。
 - APNICを発行者とする証明書発行コードを実装した。
- APNICの今後の予定
 - 今後、AP地域での理解を深め、普及を図る為に、APNICスタッフの教育強化を予定している。
- 関連状況など
 - NIRとはディスカッションを行っている。

図 5-21 RIPE Certification Task Force ミーティング(2)

APNIC は APNIC 内部でプログラム開発を行っており、リソース証明書に関する中心的なシステムである証明書エンジンの開発が終わっている。ただし、AP 地域においてリソース証明書の理解は進んでおらず、普及の目処が立っていない。APNIC の LIR 向けのポータルサイト「MyAPNIC」では 2008 年 3 月に実装される予定になっている。

APNIC では、普及の目処が立っていない原因を AP 地域の NIR の理解不足である為だと考えており、普及を図る為の APNIC スタッフ向けの教育コースを検討している。

APNIC、ARIN、RIPE NCC の中では NIR があるのは APNIC だけであり、リソース証明書の NIR の認証局の構築には、NIR の協力が不可欠となる。しかし次の ARIN の報告にもあるように、RIR 自身が NIR のリソース証明書機能を持つ方法も考えられる。

RIPE Certification Task Force ミーティング (3)

- ARINの活動状況
 - ARIN地域ではまだ注目を浴びてはいない。
 - 開発はAPNICと共同で行っている。
 - 証明書発行エンジンとRIR-LIR間プロトコルを実装した。相互運用実験を予定している。
 - LIR向けのポータルサイトとの関係を検討している。
- 関連状況など
 - ARIN地域にはNIRはないが、3000近いLIRに加えてsub-allocationがある。

図 5-22 RIPE Certification Task Force ミーティング (3)

ARIN では、APNIC と共同でリソース証明書の開発を進めている。証明書エンジンをはじめ、認証局システムが行う 3 種類の通信プロトコルの実装を進めている。一つは認証局とレジストリシステムであり、もう一つは RIR-LIR 間のプロトコルである。三つ目は、証明書の公開機能（証明書リポジトリにあたる）であるが、この開発は未着手である。

RIPE Certification Task Forceミーティング(4)

- RIPE NCCの活動状況
 - 技術開発よりもIPアドレスポリシーへの影響に注目して活動している。
 - システム開発の終了を2008年4月～5月に予定している。
 - IRRと連携したシステムを検討している。

図 5-23 RIPE Certification Task Force ミーティング(4)

RIPE NCCでは、ARINやAPNICのようにプログラム開発よりも、リソース証明書のIPアドレスポリシーへの影響について注目した活動を行っている。Certification Task ForceではIPアドレスポリシーやRIPE NCCでのIPアドレスに関するビジネスへの影響を調査することになっており、活動中である。すでに業務検討のためのプロトタイプシステムは開発済みであるが、今後業務で利用可能なシステムの開発を予定している。この開発は2008年度の初頭に完成するとされている。なおRIPE NCCではリソース証明書システムとIRRの連携を含めてシステムを検討しているとの事であった。

RIPE Certification Task Force ミーティング (5)

- ディスカッション
 - RIR間の情報共有と互いのアウトプットを共有することが重要である。
 - LIRの理解を得るためには、技術面だけでなくサービス面での検討が重要であり、APNICではAPNIC内で連携を進めている。
 - RIPE NCCではCertification Task Forceが活動している。

図 5-24 RIPE Certification Task Force ミーティング (5)

RIPE Certification Task Force ミーティングでは、問題点と今後の課題についてもディスカッションが行われた (図 5-24)。

問題点は普及に向けた LIR の理解が得にくいことである。これは主に APNIC が指摘している。ミーティングでは、APNIC や ARIN が、RIPE NCC の開発や実験に対するより多くの協力を行うように求めている側面があるように思われたが、RIPE NCC としては、ビジネス面および IP アドレスポリシーへの影響など、必要不可欠な検討を行っているという回答であり、RIR 同士の連携が、今後の課題であるという確認が行われた。

「RIPE Certification Task Force ミーティング」であったが、ARIN や APNIC が主に発言し、RIPE との協力関係を模索するようなミーティングとなった。

5.11. ARIN における動向

ARIN における電子認証とリソース証明書の動向を調査するため、第 19 回 ARIN ミーティングと第 20 回 ARIN ミーティングに参加した。本節では、ARIN ミーティングを通じてわかってきた ARIN における取り組みについて述べる。

第19回ARINミーティング

- ARIN XIX
 - 2007年4月22日(日)～4月25日(水)
 - 参加登録者数
 - 144名
 - うちアメリカからは62名、カナダ3名、カリブ海と北大西洋地域から3名、他RIR関係者など
 - ARIN XIII 163名(前回)

図 5-25 第19回 ARIN ミーティング

ARIN ミーティングは、RIPE NCC のミーティングに比べると参加人数は少なく、併設されることの多い NANOG (North American Network Operator's Group)³のミーティングよりも少ない(図 5-25)。ARIN 地域では、アメリカの LIR が多いため、参加者の多くはアメリカの人である。また各 RIR からの参加者は多い。

³ The North American Network Operators' Group
<http://www.nanog.org/>

全体概要

- Sunday
 - Workshop “Practical Guide to IPv6”
 - First-Timer Luncheon
 - Introduction to the Internet Resource Policy Evaluation Process
 - Open Policy Hour
- Public Policy Meeting Day-1
- Public Policy Meeting Day-2
- Member Meeting

図 5-26 全体概要

第 19 回 ARIN ミーティングは、プエルトリコのサンファンで行われた（図 5-26）。ARIN ミーティングは初日の日曜日にチュートリアルやワークショップが行われ、二日目から三日目に IP アドレスポリシーに関する議論が行われた。最終日は ARIN の Member Meeting（JPNIC でいうところの総会）である。

IP アドレスポリシーの中で、ARIN における電子認証に関連するポリシー提案があった。電子認証に関連するポリシー提案は三つあった。三つのポリシー提案は、ARIN におけるポリシー文書である NRPM（ARIN Number Resource Policy Manual）に電子認証に関する章を設けることに各々が関連しており、いわば電子認証方式に関する包括的な提案である。

ARINにおける認証方式の動向(1/3)

- 2007-1: Reinstatement of PGP Authentication Method
 - InterNIC時代には使えていたPGPを復活させる提案。
 - ARINにおける認証方式は"mail-from"と"X.509"のみ
 - mail-from – 昔からなりすまし攻撃をされやすい
 - X509 – S/MIMEをサポートしたメールクライアントが必要
 - » コミュニティの中にはPKIを嫌うものもいる
 - 2007-2、2007-3と共に、NRPMに第12章を設け、"mail-from"、"PGP"、"X.509"の3つが使えることを明記

図 5-27 ARIN における認証方式の動向 (1 / 3)

一つ目は、歴史的に古い IP アドレスの割り振り先組織に対する電子認証の方式に、PGP を使った方式を加える提案である(図 5-27)。ARIN では mail-from と X.509(PKI の電子証明書を使う方式) が使われることになっているが、すでにユーザがなじんでいる PGP を使えるようにするポリシー提案である。

ARINにおける認証方式の動向(2 / 3)

- 2007-2: Documentation of the Mail-From Authentication Method
 - 2007-1、2007-3と共に、NRPMに第12章を設け、“mail-from”、“PGP”、“X.509”の3つが使えることを明記
 - 但し、推奨しない
 - #RIPE NCCではメンテナオブジェクトにおけるmail-fromを廃止済み
 - 2002年8月22日
 - <http://www.ripe.net/db/news/mailfrom.html>

図 5-28 ARIN における認証方式の動向 (2 / 3)

二つ目は、新たに設ける第12章で mail-from についても方式の一つとして明文化するという提案である(図 5-28)。ただし、この方式は推奨しないことを明記することとなっている。

ARINにおける認証方式の動向(3 / 3)

- Policy Proposal 2007-3: Documentation of the X.509 Authentication Method
 - 2007-1、2007-2と共に、NRPMに第12章を設け、“mail-from”、“PGP”、“X.509”の3つが使えることを明記
 - POC(Point of Contacts)には“crypt-auth”と表示
 - 電子署名付きの申請メールで認証(POCに対応する申請担当者であることの認証)が受け付けられる。
 - X.509に移行後はmail-fromは使用不可になる(併用や逆戻りは基本的にできない)

図 5-29 ARIN における認証方式の動向 (3 / 3)

三つ目は、X.509形式の電子証明書を用いた認証方式である。ARINではすでにS/MIMEの電子署名を用いた申請業務を開始している(図5-29)。電子証明書の発行対象は、ARINにおけるLIRの連絡先情報であるPOC(Point of Contact)に対応する申請業務担当者とされている。また一旦電子証明書を用いた方式に移行すると、基本的にmail-fromの方式に戻ることはできない。

リソース証明書については、プログラム開発の動向を中心に発表があった(図5-30)。

ARINにおけるリソース証明書の動向

- デザインチーム
 - Prague(IETF-68) (3/18-3/27) にて会合
 - ARINのレジストリシステムとResource PKIシステムのやり取りを図式化、一部lispを使って役割を定義(作業は現在も継続中)
 - NANOG40(6/3-6/6) にて専門家(Steven Bellovin氏とRuss Housley氏)のセキュリティレビューを受けた。
- 開発チーム
 - ISC等の複数組織から参加者

図 5-30 ARIN におけるリソース証明書の動向

プログラム開発は、ISC や APNIC と共同のチームで行われている。開発の際には、デザインチーム(概要設計を行う専門家グループ)が作られ、概要設計の段階で、セキュリティレビューを受けたとの報告があった。本格的な開発はこのあとに行うとされていたが、2007年7月下旬に行われた第69回 IETF で相互運用試験が予定されていることから、詳細設計と開発が同時に行われていることが伺われる。

5.12. 第 20 回 ARIN ミーティング

第 20 回 ARIN ミーティングは、アメリカ合衆国のアルバカーキで行われた。第 20 回 ARIN ミーティングに先立ち、第 41 回 NANOG ミーティングが行われた。NANOG は北米地域のネットワークオペレーターの会合で、ネットワークオペレーションに関わる技術的な議論が行われる。参加者は ARIN ミーティングよりも NANOG の方が多い傾向がある。

第20回ARINミーティング

- ARIN XX
 - 2007年10月17日(水)～10月19日(金)
 - 参加登録者数
 - 203名
 - うちアメリカからは162名、カナダ10名、カリブ海と北大西洋地域から1名、他RIR関係者など
 - (前回)ARIN XIX 144名(プエルトリコ)
- 第41回NANOG(併催)
 - 2007年10月14日(日)～10月16日(火)
 - 参加登録者数
 - 452名

図 5-31 第20回 ARIN ミーティング

ARIN のメンバーミーティングで取り上げられた、電子認証に関わる話題を示す。

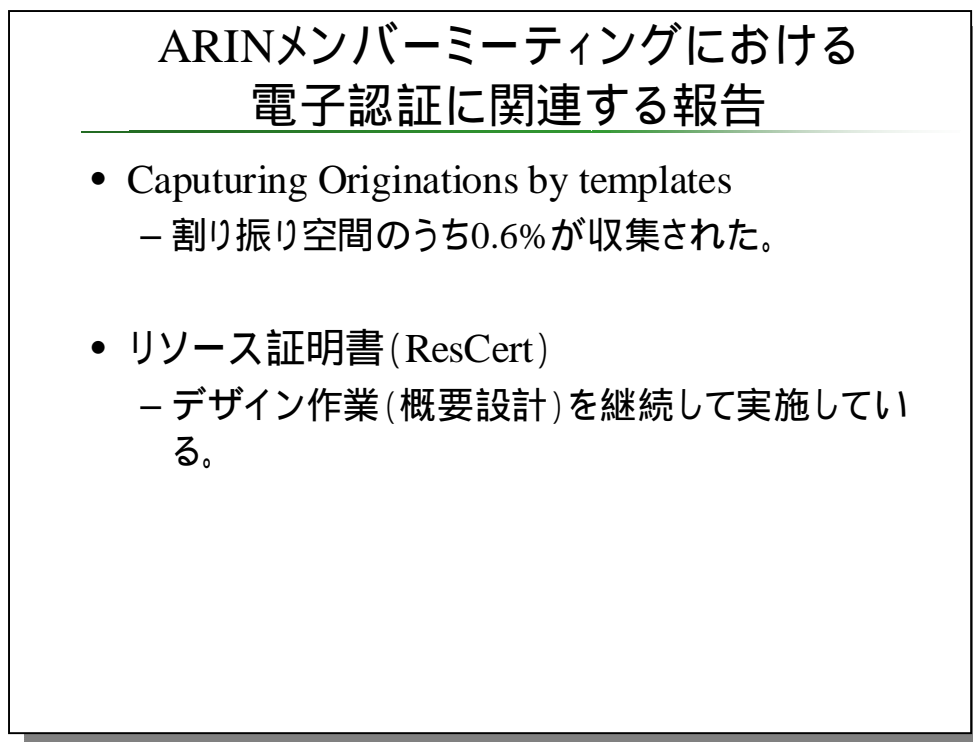


図 5-32 ARIN メンバーミーティングにおける電子認証に関連する報告

ARIN の技術部門から報告によると、Proposal 2006-3 で提案された割り振り / 割り当てテンプレートを使った Origin AS の情報は、割り振り / 割り当て情報のうち 0.6% が収集されたとのことである (図 5-32)。発表者は、これはペースが遅いという考えを持っていたようだが、提案が採用されて一年程で、ARIN の割り振り / 割り当て情報の中の 0.6% という数字は決して少なくはない。

リソース証明書については、情報が少ないながら、ARIN としても公にして活動を始めた。前回の第 69 回 IETF での様子から、このときは既にプロトタイプシステムができており、動作試験ができているが、メンバーサービスとしてはまだ実装途中であると言える。

5.13. APNIC における動向

APNIC における電子認証とリソース証明書の動向について調査するため、第 24 回 APNIC ミーティングに参加した。

第 24 回 APNIC ミーティングは、インドのニューデリーで行われた。この APNIC ミーティングでは、NIR hostmaster workshop (NIR の IP アドレス申請業務担当者向けのワークショップ) として、リソース証明書に関するディスカッションが行われた。

APNIC では、2006 年度の初め頃からリソース証明書の開発に取り組んでいる。今回のワークショップは、リソース証明書のサービス化に先立って、リソース証明書の提供方法に関する意見を NIR から集めるという趣旨であった。

AP 地域には NIR が多く存在しているため、リソース証明書を提供する形態が、他の RIR よりも複雑になる。少なくとも、二種類の方式が考えられる。一つは APNIC が集中的に証明書を管理する方式で、もう一つは各 NIR が証明書の管理を行う方式である。リソース証明書の技術には、他に利用可能性等の課題があるが、こちらについてはアジェンダになく、議論されなかった。

今回の Workshop でわかってきたことは、まず APNIC ではリソース証明書の 2007 年度末のサービス化を、変更する余地のない計画だと考えている点である。IPv4 アドレスプールの枯渇期において、IP アドレスの不正利用対策としては、リソース証明書が唯一の手段であるように捉えられているようで、サービス開始を急ぎたい様子である。ただし、APNIC におけるリソース証明書の提供には次に述べるような利用可能性等に関する課題がある。

サービス化に先立って存在する利用可能性の課題

APNIC 側が考えるリソース証明書の用途は二つあるとされている。一つは IP アドレスの割り振りを通じた正当な利用権利を示すデータである。もう一つは IETF SIDR WG で議論されている、セキュアなドメイン間ルーティングである。

リソースに対する電子証明書がいくら発行されても、それが本来の目的を達せなければ意味がない。ここでいう本来の目的とは、リソースの不正利用を排除したり、レジストリの登録情報に基づいてルーティングの安全性向上が図れるか、といったことである。つまり、サービス化の前に、以下に挙げる課題をクリアしている必要があると言える。

サービス化に先立つ、リソース証明書の利用可能性の課題

- a. リソースの不正利用があったときに、それを回避する / 拒否する

手法を確立すること

- b. IETF SIDR WG で提案されているように、S-BGP 等で利用し、ルー

ティングの安全性への利用ができること

前述の通り、今回のワークショップではこれらの課題に関する議論はできず、単に APNIC がサービス化する意思を NIR に伝える場になっていた。

第5章 経路制御のための電子認証技術に関する国際動向

リソース証明書に関する NIR の動向

ワークショップの終了後、ワークショップに参加していた NIR の各担当者の方々がほぼ全員残る形で、リソース証明書に関する情報交換が行われた。KRNIC や TWNIC は、そもそもリソース証明書に関する技術的な情報が足りていない状況があり、懸念点がわからない様子であった。

今回のワークショップについては、以下のような意見が挙げられた。

KRNIC や TWNIC の意見

a. リソース証明書の技術的な必要性が理解できていない。

費用がかかる大きなプロジェクトだがその理由付けが少なすぎる。

b. 実験的な利用開始はよいが、サービス化は改めて検討が必要。

- ルーティングの安全性向上は LIR に求められていることではある。

- 投資の検討は必要だと考えられる。

今回の Workshop は、APNIC からの情報伝達に近いものがあったが、今後アジア太平洋地域での適切な普及を図るには、まず NIR の理解を図ることから始める必要があると考えられる。

これは、RIPE NCC における Certification Task Force ミーティングにおける発言にあった APNIC の認識と近いものがあるが、技術面に傾倒しており、AP 地域での普及にはコストとベネフィットを踏まえた、LIR へ提供することの妥当性の議論が必要であると考えられる。

5.14. まとめ

RIR と主に IETF SIDR WG では、リソース証明書を使った経路制御の安全性向上策について議論が行われている。

リソース証明書については、APNIC が中心的に推進しており、開発は APNIC と ARIN が主に行っている。RIPE NCC は開発に参加しつつも、IP アドレスに関するポリシーの関連の仕方など、総合的な捉え方をしている。2007 年度末には APNIC にて実装がリリースされることから、ARIN 地域や RIPE 地域に比べて AP 地域におけるリソース証明書の提供は早い。一方で、APNIC では技術開発に力が入れられており、LIR へのサービスとしてのリソース証明書、すなわちビジネス面の検討はまだ進んでいない状況である。

ARIN および RIPE NCC では、LIR の認証に関する取り組みが行われている。両 RIR

共に電子証明書を使った LIR の認証は採用済であり、認証方式の明文化や mail-from などの弱い認証方式（認証を行っていないとも言える）の削除の動きがある。

IETF SIDR WG では、ルータにおけるリソース証明書の検証にまで議論が進みつつあるが、インターネット経路情報に対してどのようにフィルタ等を適用すべきかについて、いまだ議論が進んでいない状況である。

本章で述べた RIR および IETF における電子認証に関わる動向調査は、ほとんどすべてについて現地調査を通じて行った。これにより、ここでは報告しきれないほどの情報を逐次得ることができ、また関係者と直接ディスカッションができる基盤ができた。

第 5 章 経路制御のための電子認証技術に関する国際動向

第6章 電子認証フレームワークと IP アドレス認証の今後

内容

- IP アドレス認証と電子認証フレームワーク
- 今後のレジストリセキュリティ

6. 電子認証フレームワークとIPアドレス認証展開の今後

2006年度の調査報告書の第6章で、本調査研究の将来像について述べた。2007年度でもその将来像は大きく変わらないが、ここではより近い将来について述べたい。

まず電子認証フレームワークの今後について述べ、次にIPアドレス認証の展開の今後について述べたい。

6.1. 電子認証フレームワークの今後

電子認証フレームワークの調査研究の一環として立ち上げた、電子認証プラクティスフォーラムは、今後、まず、各分野に共通の電子認証リスクの回避に役立つようなノウハウの集約が図られると考えられる(図6-1)。

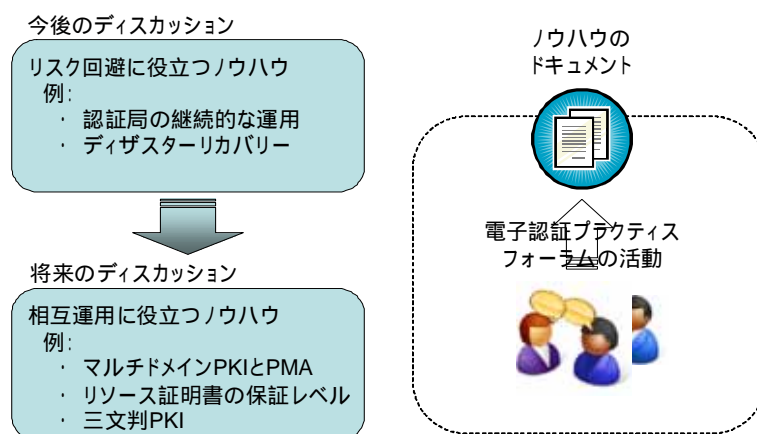


図 6-1 今後のディスカッションの傾向

これは現代、暗号アルゴリズムの変更可能性に関する議論や電子署名法をめぐる議論など、日本国内の認証局のビジネス環境に変化が起きているためである。その中で、富士ゼロックスの横田氏が行ったようなPKIアプリケーションの挙動の違いに関する調査結果と、例えば問題が起こりにくいキーロールオーバーの方法に関する情報が貴重である。

更にその先には、相互運用に役立つノウハウの提案やディスカッションが行われると考えられる。これはセコム株式会社の島岡氏やJPNICの木村がアイデアとして提案したもので、複数のPKIドメインを超えるような電子証明書の利用のために役立つようなノウハウである。

6.2. IPアドレス認証展開の今後

IPアドレス認証展開に関する調査研究の一環で開発した経路情報の登録機構は、今後、実験を継続し、IRR (Internet Routing Registry) の登録者増を図ると共に本機構の利用者増を図る。

本機構の今後は、すでに第4章で述べたISPとの連携である(図6-2)。国内ISPにおける正常な経路制御のために、JPIRRに蓄積された経路の情報が利用されることを示している。JPIRRは「正しい経路台帳」の役割を果たす。

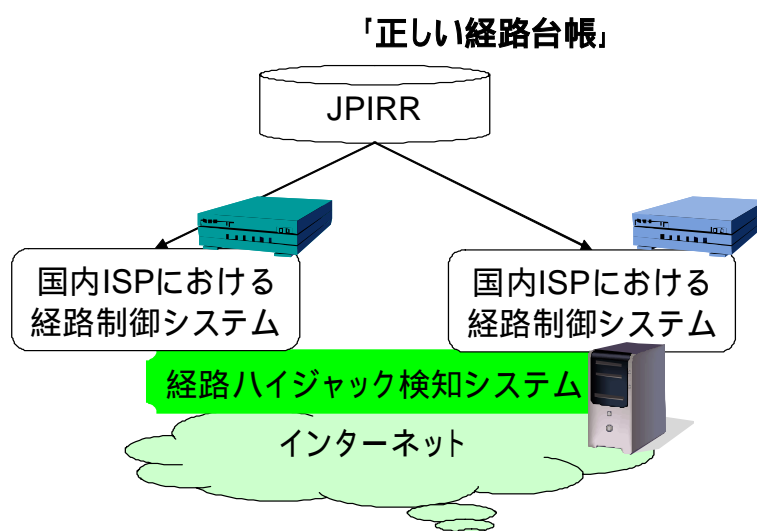


図 6-2 経路情報の登録機構の今後

IPv4アドレスの枯渇に伴い、自組織のIPv4アドレスが無断で使われてしまう問題が起きる可能性が高まると考えられる。これを避けるためには不正な経路情報を検知し回避することが重要である。今後、本機構の利用によって蓄積された正しい経路台帳を有効に活用し、広範囲のネットワークで役立つような普及を図ることが重要であり、また課題でもある。

もう一つ、将来像として考えられることはリソース証明書の発行である。第5章のRIPE NCCのCA-TFの調査の際に、APNICの技術者がNIRの動向としてprovisioningに関する活動を行っていると紹介していた。この指摘が経路情報の登録機構に関する調査研究を指しているかどうか定かではないが、本機構がリソース証明書の発行インターフェースの一部として利用できる。

リソース証明書を発行する段階になると、電子認証プラクティスフォーラムにおける活動との連携が必要になる。リソース証明書の相互運用には、各レジストリやLIRによって発行される証明書の相互運用性が必須である。電子証明書の相互運用性は、プロフ

ファイルとしての相互運用性よりも、保証レベルとしての相互運用性の方が問題になりやすい。電子認証プラクティスフォーラムにて、相互運用が可能なリソース証明書を発行するための認証業務やCPをドキュメント化し、リソース証明書を検証するシステム開発者がそれを参照するような状況になることが望ましい。

6.3. 今後の課題と活動

前節で述べた今後の活動のためには、二つの調査研究で取り組んできたフォーラムおよびシステムの利用実験について、以下の課題があると考えられる。

- 電子認証プラクティスフォーラムの継続と発展
2007年度はドキュメント策定のプロセスを実験的に行ったが、今後は実際のノウハウを蓄積するための活動として継続する必要がある。そのために認知度を上げることや、コンテンツの充実、ノウハウの活用などを図る必要があると考えられる。
- 経路情報の登録機構の利用者の増加と普及
経路情報の登録機構は、一部の希望者によって使われているだけでは効果が薄い。日本国内のIPアドレスの安全性を高めるという意味では、多くのISPに利用され、またできればIPアドレス管理業務の一環として組み入れられる必要があると思われる。

今後これらの活動に取り組み、より適切な電子認証技術の利用と普及、およびインターネットセキュリティの向上を図りたい。

第6章 電子認証フレームワークとIPアドレス認証の展開の今後

Appendix 1

経路情報の登録機構における
電子証明書と許可リストのインターフェース

A.1. 経路情報の登録機構のユーザインターフェース

Appendix. 1 では、経路情報の登録機構のユーザインターフェースを簡単に紹介する。経路情報の登録機構は 2006 年に開発されてから、2007 年度のフィードバックを受けて改修された。改修後のものについて述べる。

本機構は、大きく分けると証明書管理と許可リストの二つのユーザインターフェースを提供する。証明書管理は、IRR のメンテナ管理者がオブジェクト登録者の証明書を発行するための機能である。メンテナ管理者は複数のオブジェクト登録者を登録でき、各々に対して S/MIME 用の証明書を発行できる。またこの機能は、JPNIC からメンテナ管理者に対して証明書を発行する際にも使われる。

許可リストは IP アドレスの割り振り先組織の担当者が編集できる表である。IP アドレスの割り振り先組織は、予め「資源管理証明書」と呼ばれる https の認証用証明書が発行されている。この証明書は IP アドレスに関する申請を行う「Web 申請システム」にアクセスするために使われている。つまり IP アドレスの割り振り先組織の担当者は、一つの証明書で IP アドレスに関する申請と、許可リストの編集を行うことができる。

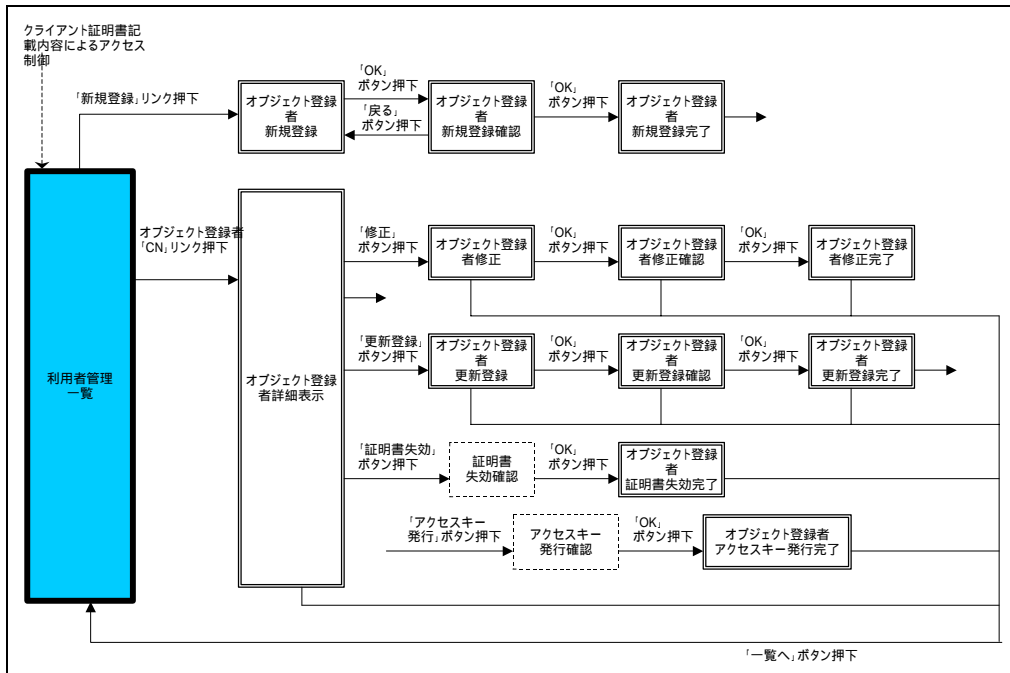
A.1.1. クライアント証明書管理者用インターフェース

このインターフェースは、メンテナ管理者のためのユーザインターフェースである。メンテナ管理者はオブジェクト登録者の新規登録、アクセスキーの発行、失効などの機能を提供する。

A.1.1.1. 利用者管理一覧

利用者管理一覧画面を示す。

Appendix. 1 経路情報の登録機構のユーザインターフェース



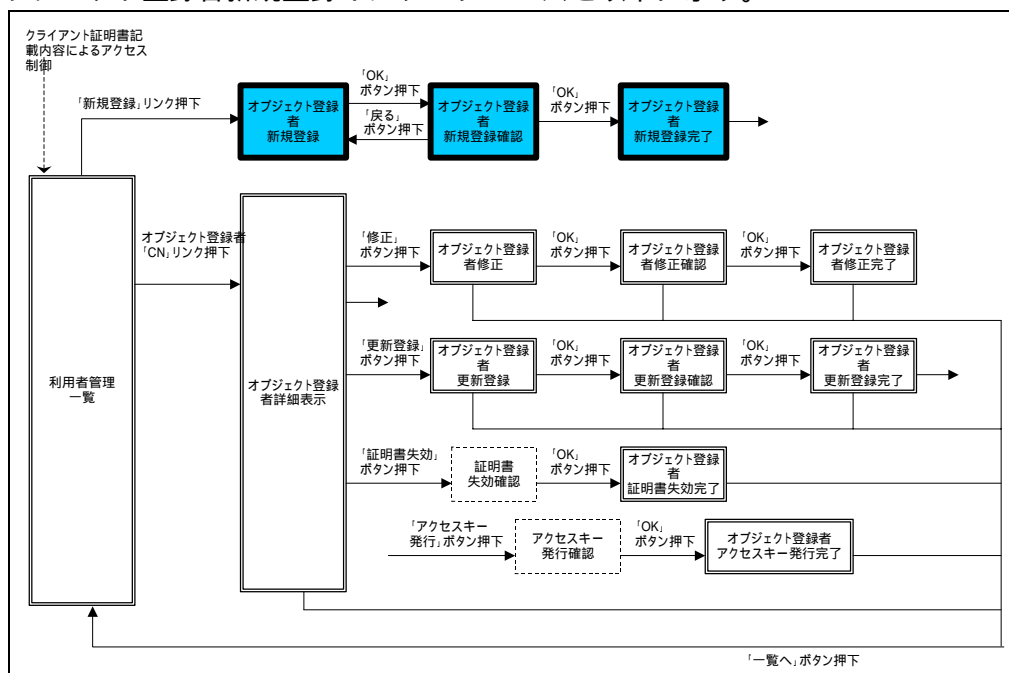
ログイン時のトップページとして利用者管理一覧画面が表示される。

cn	E-mailアドレス	状態	更新状況	notBefore	notAfter
IRR-OR test1 01	test1@nicad.jp	発行済	更新済	2007/10/19 12:00:00	2008/11/17 11:59:59
IRR-OR test2 01	test2@nicad.jp	発行済	更新済	2007/10/19 12:00:00	2008/11/17 11:59:59
IRR-OR test3 01	test3@nicad.jp	未発行	更新済		

証明書の管理対象メンテナ名に該当する利用者の情報を取得し表示する。
「cn」リンクをクリックすると「オブジェクト登録者情報詳細」に遷移する。

A.1.1.2. 利用者新規登録

オブジェクト登録者新規登録インターフェースを以下に示す。



利用者一覧画面からオブジェクト登録者新規登録画面に遷移する。



オブジェクト登録者新規登録画面を表示し、利用者情報を入力する。
「OK」ボタンをクリックすると「オブジェクト登録者新規登録確認」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

The screenshot shows the JPNIC (Japan Network Information Center) user interface. At the top left is the JPNIC logo and the text "日本ネットワークインフォメーションセンター Japan Network Information Center". Below the header, there are two input fields: "ログインID" (Login ID) with the value "IRR-MA JPPIRR Operation Team three 01" and "管理対象メンテナ" (Managed Maintainer) with the value "MAINT-ROUTEREG2". A button labeled "クライアント証明書管理" (Client Certificate Management) is visible. The main content area displays the message "オブジェクト登録者新規登録完了" (New Object Registrant Registration Completed) and "オブジェクト登録者情報を登録しました。" (Object registrant information has been registered). Below this message is a button labeled "アクセスキー発行" (Issue Access Key). At the bottom of the page, there is a footer with links for "お問い合わせ" (Contact Us), "著作権/リンク" (Copyright/Link), "JPNIC個人情報保護方針" (JPNIC Personal Information Protection Policy), and "Q&A", along with the copyright notice "Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved."

オブジェクト登録者新規登録の確認画面である。

「登録」ボタンをクリックすると「オブジェクト登録者新規登録完了」に遷移する。

The screenshot shows the JPNIC user interface. At the top left is the JPNIC logo and the text "日本ネットワークインフォメーションセンター Japan Network Information Center". Below the header, there are two input fields: "ログインID" (Login ID) with the value "IRR-MA JPPIRR Operation Team three 01" and "管理対象メンテナ" (Managed Maintainer) with the value "MAINT-ROUTEREG2". A button labeled "クライアント証明書管理" (Client Certificate Management) is visible. The main content area displays the message "オブジェクト登録者新規登録確認" (New Object Registrant Registration Confirmation). Below this message are three input fields: "cn" with the value "IRR-OR test3 01", "利用者名" (User Name) with the value "test3", and "E-mailアドレス" (E-mail Address) with the value "test3@nic.ad.jp". Below these fields is the question "上記内容で登録します。よろしいですか?" (I will register with the above information. Is it all right?). Below the question are two buttons: "OK" and "戻る" (Back). At the bottom of the page, there is a footer with links for "お問い合わせ" (Contact Us), "著作権/リンク" (Copyright/Link), "JPNIC個人情報保護方針" (JPNIC Personal Information Protection Policy), and "Q&A", along with the copyright notice "Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved."

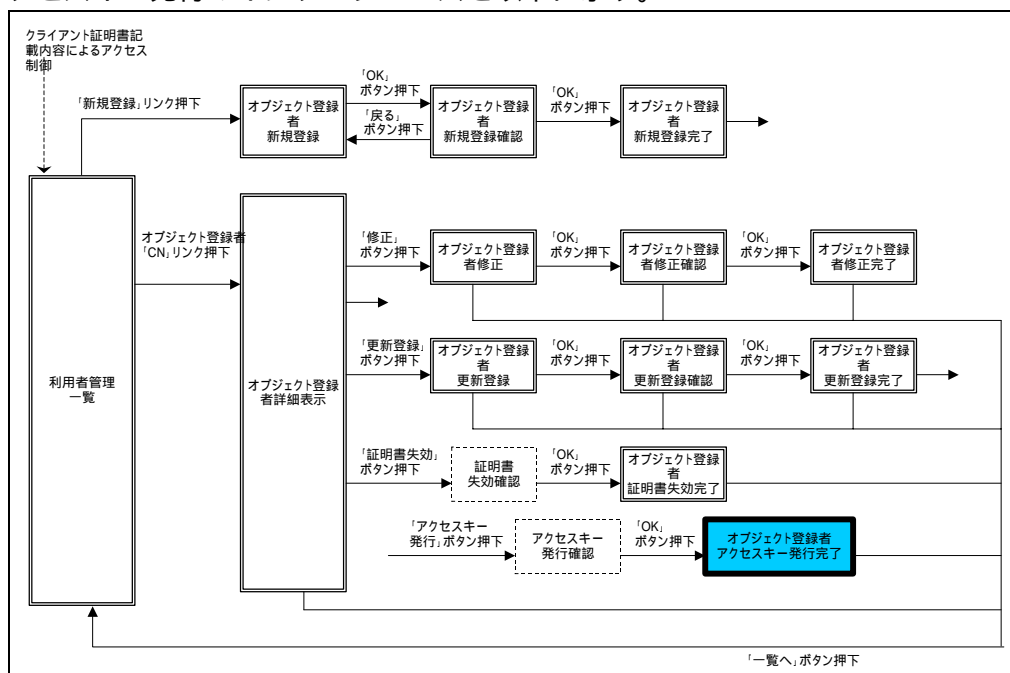
オブジェクト登録者新規登録の完了を知らせる。

「アクセスキー発行」ボタンをクリックすると「オブジェクト登録者アクセスキー発行完了」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

A.1.1.3. アクセスキー発行完了

アクセスキー発行のインターフェースを以下に示す。



オブジェクト登録者詳細表示画面、オブジェクト登録者更新登録完了画面からアクセスキー発行完了画面に遷移する。

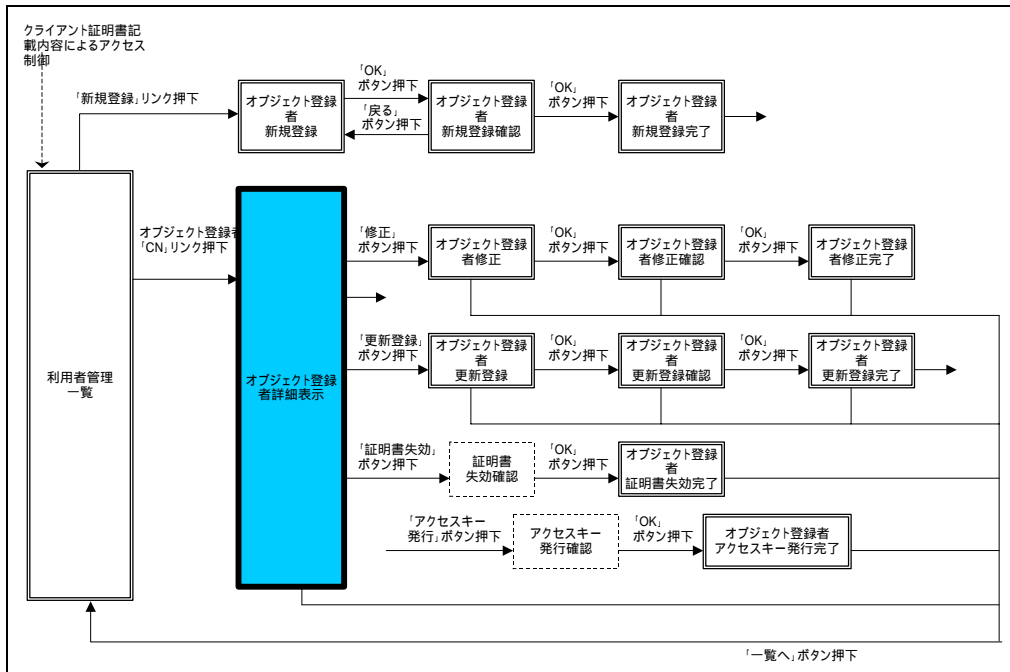


オブジェクト登録者アクセスキー発行の完了を知らせる。
「一覧へ」ボタンをクリックすると「利用者管理一覧」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

A.1.1.4. オブジェクト登録者情報詳細

オブジェクト登録者情報詳細インターフェースを以下に示す。



利用者管理一覧画面からオブジェクト登録者情報詳細画面に遷移する。

利用者管理一覧より取得した利用者の情報を表示し、状態、更新状況により使用でき

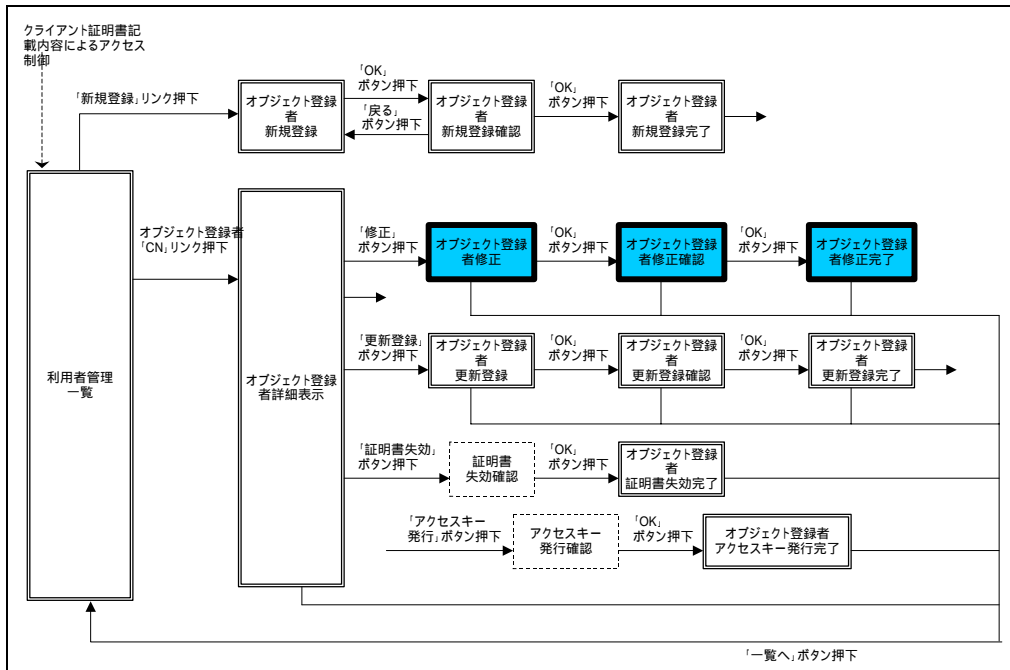
Appendix. 1 経路情報の登録機構のユーザインターフェース

るボタンを設定する。「修正」ボタンをクリックすると「オブジェクト登録者修正」に遷移する。「アクセスキー発行」ボタンをクリックすると「オブジェクト登録者アクセスキー発行完了」に遷移する。「更新登録」ボタンをクリックすると「オブジェクト登録者更新登録」に遷移する。「証明書失効」ボタンをクリックすると「オブジェクト登録者証明書失効完了」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

A.1.1.5. オブジェクト登録者修正

オブジェクト登録者修正インターフェースを以下に示す。



オブジェクト登録者情報詳細画面からオブジェクト登録者修正画面に遷移する。

オブジェクト登録者修正画面を表示し、利用者情報を入力する。

「OK」ボタンをクリックすると「オブジェクト登録者修正確認」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

The screenshot shows the JPNIC (Japan Network Information Center) user interface. At the top left is the JPNIC logo and the text "日本ネットワークインフォメーションセンター Japan Network Information Center". Below the logo is a navigation bar with a button labeled "クライアント証明書管理". The main content area is titled "オブジェクト登録者修正確認". It contains a form with three rows of input fields: "CN" with the value "IRR-OR test1 01", "利用者名" with the value "test1", and "E-mailアドレス" with the value "tost1@nic.od.jp". Below the form is the text "上記内容で登録します。よろしいですか？" and three buttons: "OK", "戻る", and "一覧へ". At the bottom of the page, there is a footer with links for "お問い合わせ", "著作権/リンク", "JPNIC個人情報保護方針", and "Q&A", along with the copyright notice "Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved."

オブジェクト登録者修正の確認画面を表示する。

「OK」ボタンをクリックすると「オブジェクト登録者修正完了」に遷移する。

The screenshot shows the JPNIC user interface after the registration confirmation. The layout is similar to the previous screenshot, but the main content area is titled "オブジェクト登録者修正完了". Below the title is the text "オブジェクト登録者情報を修正しました。" and a single button labeled "一覧へ". The footer and navigation bar are identical to the previous screenshot.

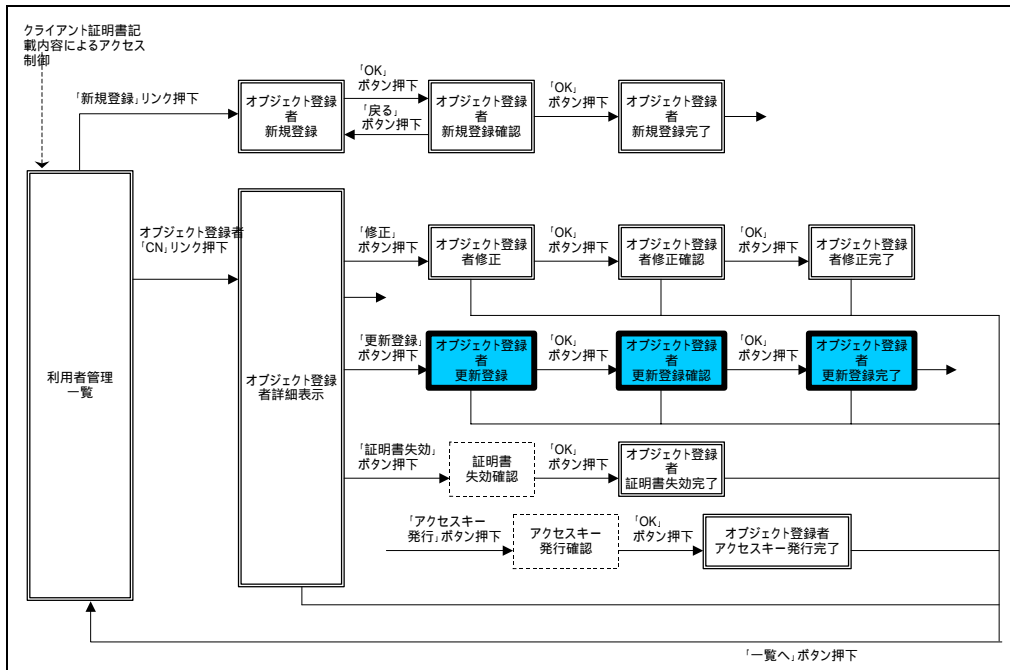
オブジェクト登録者修正の完了を知らせる。

「一覧へ」ボタンをクリックすると「利用者管理一覧」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

A.1.1.6. オブジェクト登録者更新登録

オブジェクト登録者更新登録方法を以下に示す。



オブジェクト登録者詳細表示画面からオブジェクト登録者更新登録画面に遷移する。



日本ネットワークインフォメーションセンター
Japan Network Information Center

ログインID

IRR-MA JPIRR Operation Team three 01

管理対象メンテナンス

MAINT-ROUTEREG2

[クライアント証明書管理](#)

オブジェクト登録者更新登録

cn	IRR-OR test1 01
利用者名	test1
E-mailアドレス(*) (半角英数字, 記号)	test1@nic.ad.jp

(*)は必須入力

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A |

Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved.

更新対象利用者の情報をもとにオブジェクト登録者の利用者情報を新たに作成する。「OK」ボタンをクリックすると「オブジェクト登録者更新登録確認」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

The screenshot shows the JPNIC (Japan Network Information Center) user interface. At the top left is the JPNIC logo and name. Below it, there are two input fields: 'ログインID' (Login ID) with the value 'IRR-MA JPPIR Operation Team three 01' and '管理対象メンテナンス' (Maintenance target) with the value 'MAINT-ROUTEREG2'. A button labeled 'クライアント証明書管理' (Client certificate management) is visible. The main content area is titled 'オブジェクト登録者更新登録確認' (Object registrant update registration confirmation). It contains a table with the following information:

cn	IRR-OR test1 01
利用者名	test1
E-mailアドレス	test1@nic.ad.jp

Below the table, the text reads: '上記内容で更新登録します。よろしいですか?' (I will update the registration with the above information. Is it all right?). There are three buttons: 'OK', '戻る' (Back), and '一覧へ' (Go to list).

At the bottom of the page, there are links for 'お問い合わせ' (Contact), '著作権/リンク' (Copyright/Link), 'JPNIC個人情報保護方針' (JPNIC Personal Information Protection Policy), and 'Q&A'. The footer text is 'Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved.'

オブジェクト登録者更新登録の確認画面を表示する。
「登録」ボタンをクリックすると「オブジェクト登録者更新登録完了」に遷移する。

The screenshot shows the JPNIC user interface after the registration process is complete. The top part is identical to the previous screenshot, showing the login ID and maintenance target. The main content area is titled 'オブジェクト登録者更新登録完了' (Object registrant update registration completed). Below the title, the text reads: 'オブジェクト登録者情報を更新登録しました。' (Object registrant information has been updated and registered). There is a single button labeled '一覧へ' (Go to list).

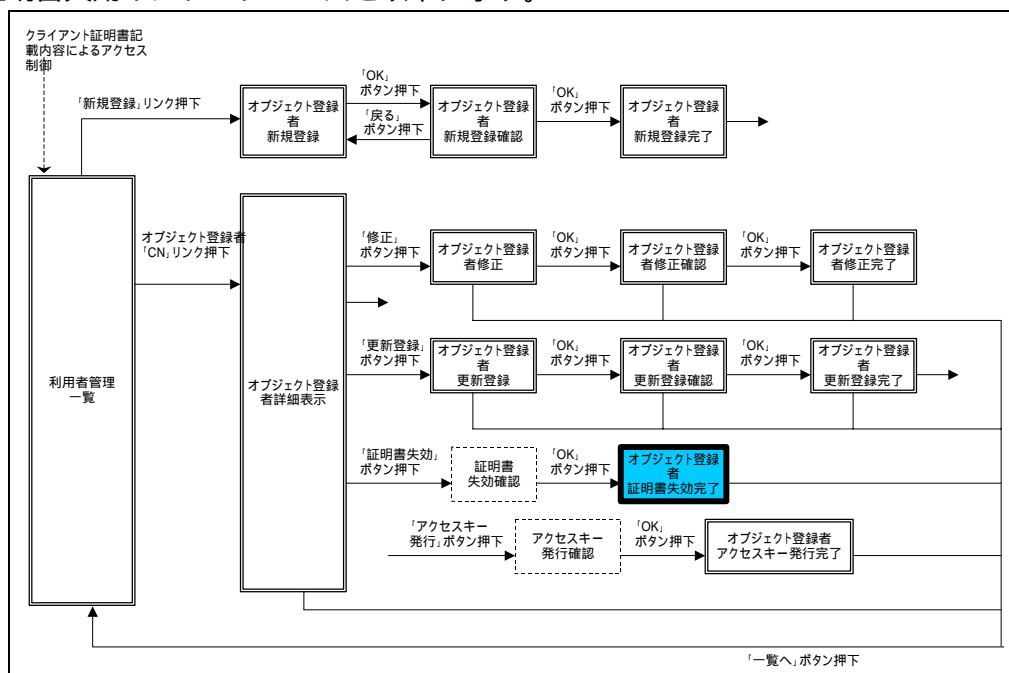
At the bottom of the page, there are links for 'お問い合わせ' (Contact), '著作権/リンク' (Copyright/Link), 'JPNIC個人情報保護方針' (JPNIC Personal Information Protection Policy), and 'Q&A'. The footer text is 'Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved.'

オブジェクト登録者更新登録の完了を知らせる。
「アクセスキー発行」をクリックすると「アクセスキー発行完了」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

A.1.1.7. 証明書失効

証明書失効インターフェースを以下に示す。



オブジェクト登録者詳細表示画面から証明書失効完了画面に遷移する。



証明書失効の完了を知らせる。

「一覧へ」をクリックすると「利用者管理一覧」に遷移する。

A.1.1.8. エラー表示

エラー表示画面について述べる。



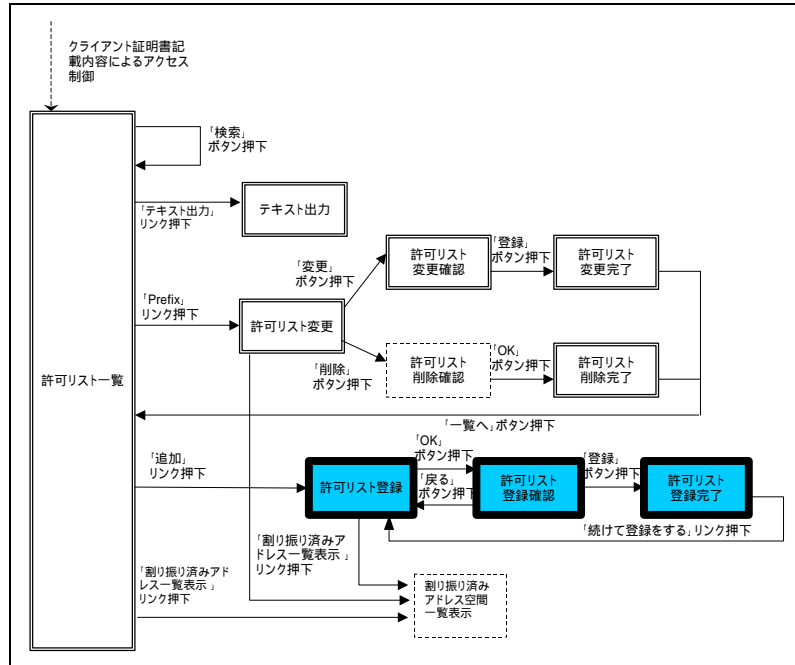
Web ページへのアクセス時に起こるエラーは様々である。HTTP で使われているエラーコードの中には現在ほとんど起きることがないものもある。ほとんどのエラーに対して、一般ユーザが対応できるのは URL の指定を見直すことだけである。そこで、本機構では各々のエラー一般の表示を行うのではなく、共通の Web ページを用意した。ただし、エラーコードのみを表示する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

A.1.2. 資源管理者用インターフェース

A.1.2.1. 許可リスト登録

許可リスト登録方法を以下に示す。



許可リスト一覧画面から許可リスト登録画面に遷移する。

ログインID: LIR 11M 0000275 user_00
 許可リスト
 割り振り済みアドレス一覧

開始アドレス	終了アドレス
202.210.58.0	202.210.59.255
202.210.58.0	202.210.59.255

許可リスト登録

Prefix(*) (v4[172.168.0.0/16], v6[2001::/32])	<input type="text"/>
モニター名(*) (半角英数字、記号)	<input type="text"/>
AS番号 (半角英数字、記号 カンマ区切りで複数入力可)	<input type="text"/>
allow/deny(*)	allow

(*)は必須入力

OK クリア

許可リスト情報を入力する。自身が管理する Prefix のみ設定が可能である。自身の管

Appendix. 1 経路情報の登録機構のユーザインターフェース

理外のものについてはエラーとし、登録できない。その検証のため、資源管理 CA クライアント証明書のプロファイルに対応する資源管理番号により割り振り済みか否かのチェックを行う。また、JPNIC 担当者の許可リスト登録時と同様に、Prefix について以下の入力チェックを行う。

同一のメンテナー名かつ同一の許可・禁止区分で、登録済み許可リストと範囲が重なるPrefixがある場合、エラーとし登録不可とする。同一のメンテナー名で、「禁止」の登録済み許可リストの範囲に含まれるか、または等しいPrefix がある「許可」を新規登録しようとした場合、エラーとし登録不可とする。同一のメンテナー名で、「許可」の登録済み許可リストの範囲を含むか、または等しいPrefix がある「禁止」を新規登録しようとした場合、エラーとし登録不可とする。

メンテナー名については、入力されたメンテナー名がJPIRRのメンテナーオブジェクトとして存在するかどうかを確認する。

AS 番号については、1つの許可リストにつき最大100件まで登録可能とする。

「登録」ボタンをクリックすると「許可リスト確認」に遷移する。

The screenshot shows the JPNIC (Japan Network Information Center) user interface. At the top, there is a header with the JPNIC logo and the text "日本ネットワークインフォメーションセンター Japan Network Information Center". Below the header, there is a login field labeled "ログインID" with the value "LIR-HM 0000275 user_03". A button labeled "許可リスト" is visible. The main content area is titled "許可リスト登録確認" (Permission List Registration Confirmation). It contains a table with the following information:

Prefix	202.210.58.0/24
メンテナー名	MAINT-ROUTEREG2
AS番号	AS37911
allow/deny	deny

Below the table, there is a question: "上記の内容で登録してよろしいですか?" (Is it okay to register with the above information?). There are two buttons: "登録" (Register) and "戻る" (Back). At the bottom of the page, there is a footer with the text: "お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | ©&N | Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved."

許可リスト登録の確認画面を表示する。

「登録」ボタンをクリックすると「許可リスト完了」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

日本ネットワークインフォメーションセンター
Japan Network Information Center

ログインID: LIR-HM 0000275 user_03

許可リスト

許可リスト登録完了

許可リストID	57
Prefix	2002.210.58.0/24
マネージャ名	MAINT-ROUTEREG2
AS番号	AS37811
allow/deny	deny

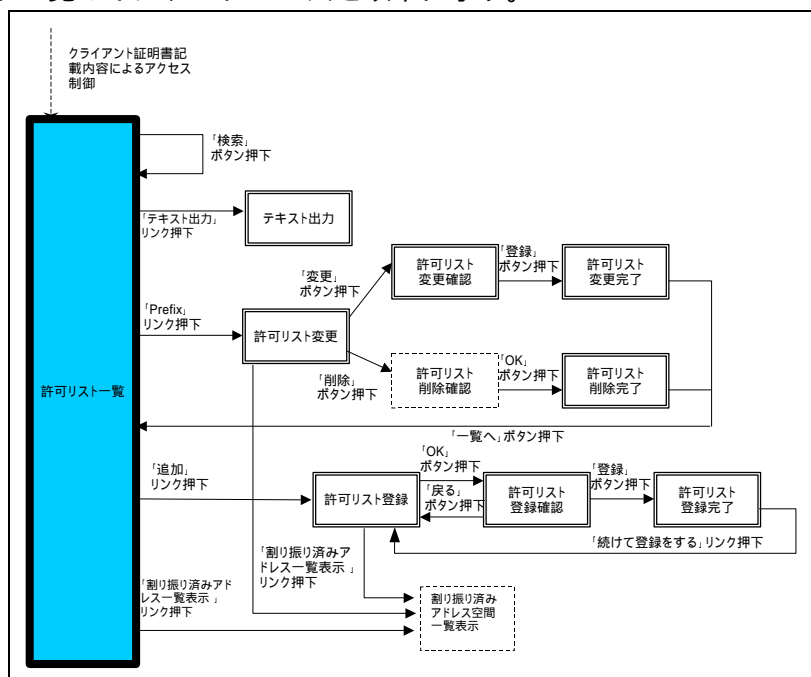
上記の内容で登録完了しました
[続けて登録をする](#)

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | O&A |
Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved.

許可リスト登録の完了を知らせる。登録された許可リストの内容を表示する。「続けて登録する」をクリックすると「許可リスト登録」に遷移する。


A.1.2.2. 許可リスト一覧

許可リスト一覧のインターフェースを以下に示す。



ログイン時のトップページとして許可リスト一覧画面が表示される。

Appendix. 1 経路情報の登録機構のユーザインターフェース


日本ネットワークインフォメーションセンター
Japan Network Information Center

ログインID LIR-HM 0000275 user_03

許可リスト

割り振り済みアドレス一覧

開始アドレス	終了アドレス
202.210.58.0	202.210.58.255
202.210.58.0	202.210.58.255

許可リスト一覧

検索条件入力

許可リストID	<input type="text"/>	IPバージョン	<input type="text" value="全て"/>	<div style="border: 1px solid gray; padding: 5px; width: fit-content; margin: auto;">お知らせ Information</div>
メンテナー名	<input type="text"/>	AS番号	<input type="text"/>	
allow/deny	<input type="text" value="全て"/>	登録者種別	<input type="text" value="全て"/>	
Prefix (<input checked="" type="radio"/> equal or less specific <input type="radio"/> equal or more specific) <input type="text"/>				









検索項目の条件はAND条件として検索します。

検索
クリア
全件表示

追加

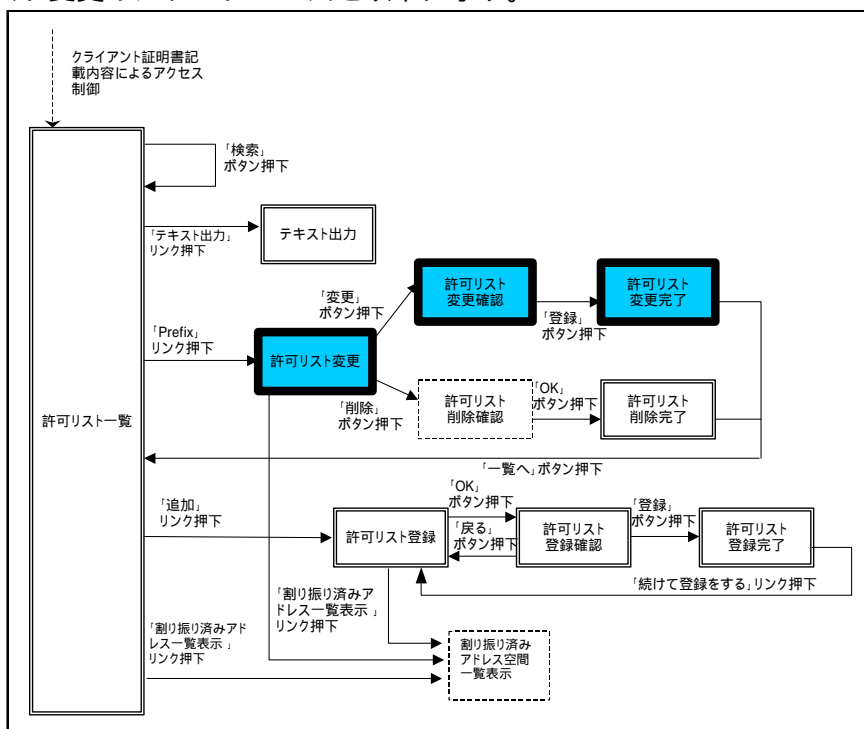
検索結果 7件 テキスト出力

許可リストID ▲ ▼	Prefix ▲ ▼	メンテナー名 ▲ ▼	AS番号 ▲ ▼	allow/deny	登録者種別
57	202.210.58.0/24	MAINT-ROUTEREG2	AS37911	deny	
33	100.0.32.0/19	MAINT-ROUTEREG2	AS37911, AS00001.00001	allow	jnic
31	202.210.58.0/23	MAINT-ROUTEREG2	AS37911	allow	
30	202.210.58.0/23	MAINT-ROUTEREG2	AS37911	allow	
19	100.0.10.0/24	MAINT-ROUTEREG2	AS9.9, AS2.5	allow	
18	100.0.10.0/32	MAINT-ROUTEREG	AS2.2	allow	
14	100.0.32.0/19	MAINT-ROUTEREG		allow	jnic

「許可リスト検索」、「許可リスト一覧」で入力された検索条件に該当する許可リストの情報を取得し表示する。「検索」ボタンまたは「全件表示」ボタンをクリックすると「許可リスト一覧」に遷移する。「許可リスト ID」の横の  をクリックすると検索結果を許可リスト ID の昇順で表示する。「許可リスト ID」の横の  をクリックすると検索結果を許可リスト ID の降順で表示する。「Prefix」の横の  をクリックすると検索結果をPrefix の昇順で表示する。「Prefix」の横の  をクリックすると検索結果をPrefix の降順で表示する。「メンテナー名」の横の  をクリックすると検索結果をメンテナー名の昇順で表示する。「メンテナー名」の横の  をクリックすると検索結果をメンテナー名の降順で表示する。「AS 番号」の横の  をクリックすると検索結果をAS 番号の昇順で表示する。「AS 番号」の横の  をクリックすると検索結果をAS 番号の降順で表示する。「Prefix」をクリックすると「許可リスト変更」に遷移する。

A.1.2.3. 許可リスト変更

許可リスト変更インターフェースを以下に示す。



許可リスト一覧画面から許可リスト変更画面に遷移する。

JPNIC 日本ネットワークインフォメーションセンター
 Japan Network Information Center

ログインID: LIR-HM 0000275 user_03

許可リスト

割り振り済みアドレス一覧

開始アドレス	終了アドレス
202.210.56.0	202.210.59.255
202.210.56.0	202.210.59.255

許可リスト変更

許可リストID	57
Prefix(*) (v4[172.168.0.0/16], v6[2001::/32])	202.210.58.0/24
ルーター名(*) (半角英数字, 記号)	MAINT-ROUTER02
AS番号 (半角英数字, 記号 カンマ区切りで複数入力可)	AS37911
allow/deny(*)	deny

(*)は必須入力

[変更] [クリア] [削除]

[一覧へ]

Appendix. 1 経路情報の登録機構のユーザインターフェース

許可リスト情報を変更する。任意のPrefix に対して許可リストを登録することができる。Prefixとメンテナ名については「許可リスト登録」と同じ入力チェックを行う。「変更」ボタンをクリックすると「許可リスト変更確認」に遷移する。「削除」ボタンをクリックすると「許可リスト削除完了」に遷移する。

許可リストID	57
Prefix	202.210.58.0/24
メンテナ名	MAINT-ROUTEREG2
AS番号	AS37911, AS25
allow/deny	deny

上記の内容で登録してよろしいですか？

許可リスト変更の確認画面を表示する。

「登録」ボタンをクリックすると「許可リスト変更完了」に遷移する。

許可リストID	57
Prefix	202.210.58.0/24
メンテナ名	MAINT-ROUTEREG2
AS番号	AS37911, AS25
allow/deny	deny

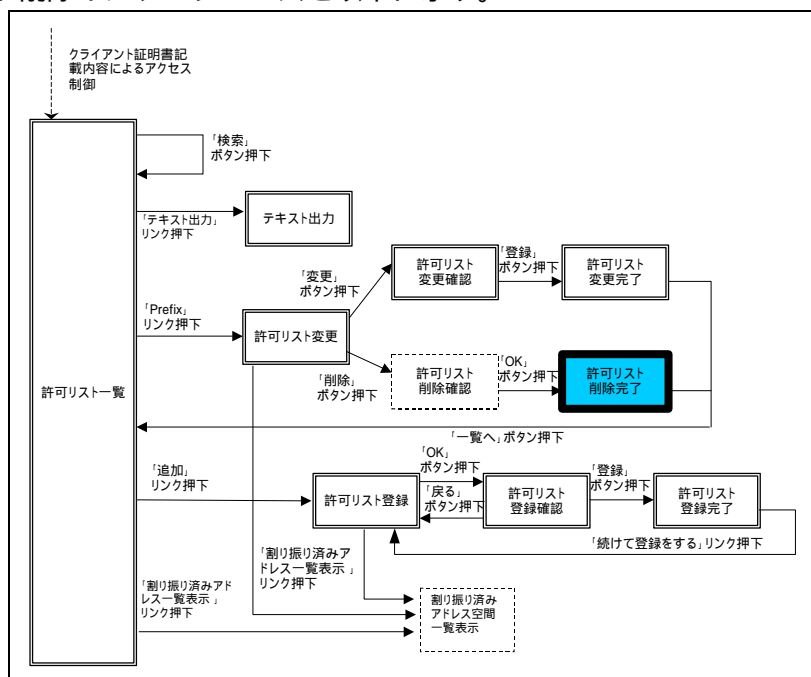
上記の内容で登録完了しました

許可リスト変更の完了を知らせる。変更された許可リストの内容を表示する。

「一覧へ」ボタンをクリックすると「許可リスト一覧」に遷移する。

A.1.2.4. 許可リスト削除

許可リスト削除インターフェースを以下に示す。



許可リスト変更画面から許可リスト削除完了画面に遷移する。

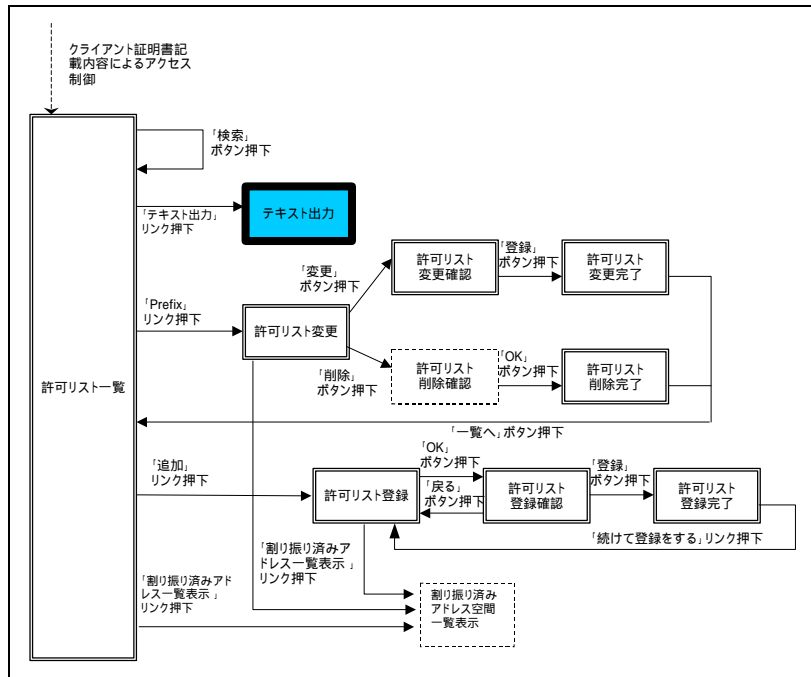


許可リスト削除の完了を知らせる。削除された許可リストの内容を表示する。「一覧へ」ボタンをクリックすると「許可リスト一覧」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

A.1.2.5. 許可リストテキスト表示

許可リストテキスト表示画面を以下に示す。



許可リスト一覧画面から許可リストテキスト表示画面に遷移する。

```

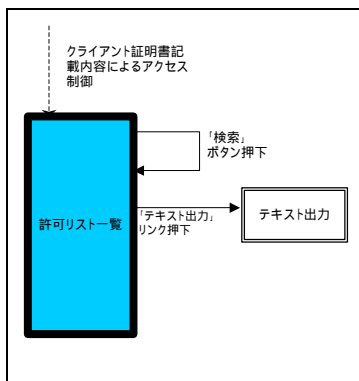
33 100.0.32.0/19 MAINT-ROUTERS "AS37911, AS00001.00001" allow "jpnic"
31 202.210.58.0/23 MAINT-ROUTERS "AS37911" allow ""
30 202.210.56.0/23 MAINT-ROUTERS "AS37911" allow ""
19 100.0.100.0/24 MAINT-ROUTERS "AS9.9, AS2.5" allow ""
18 100.0.100.0/32 MAINT-ROUTERS "AS2.2" allow ""
14 100.0.32.0/19 MAINT-ROUTERS "" allow "jpnic"
    
```

「許可リスト一覧」に表示されている許可リストの情報を取得し表示する。テキスト表示は、ルーティング業務を行う者がテキスト処理を行うために利用できるように実装した。

A.1.3. オブジェクト登録者用インターフェース

A.1.3.1. 許可リスト一覧

許可リスト一覧画面を以下に示す。



ログイン時のトップページとして許可リスト一覧画面が表示される。

許可リストID	資源管理者略称	Prefix	AS番号	allow/deny	登録者種別
34	ROUTEREGTEST	5000-/32	AS99999.99999, AS37911	allow	jpnict
33	ROUTEREGTEST	100.032.0/19	AS37911, AS00001.00001	allow	jpnict
32	ROUTEREGTEST	2001.0c40-/32	AS37911	allow	
31	ROUTEREGTEST	202.210.58.0/23	AS37911	allow	
30	ROUTEREGTEST	202.210.56.0/23	AS37911	allow	
19	ROUTEREGTEST	100.0.100/24	AS8.9, AS2.5	allow	

「許可リスト一覧」で入力された検索条件と利用者の管理対照メンテナに該当する許可リストの情報を取得し表示する。

「検索」または「全件表示」をクリックすると「許可リスト一覧」に遷移する。「許

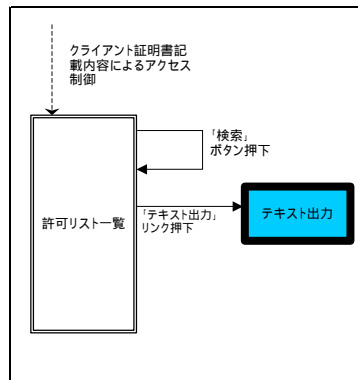
Appendix. 1 経路情報の登録機構のユーザインターフェース

可リストID」の横の をクリックすると検索結果を許可リストIDの昇順で表示する。

「許可リストID」の横の をクリックすると検索結果を許可リストIDの降順で表示する。「Prefix」の横の をクリックすると検索結果をPrefixの昇順で表示する。「Prefix」の横の をクリックすると検索結果をPrefixの降順で表示する。「AS番号」の横の をクリックすると検索結果をAS番号の昇順で表示する。「AS番号」の横の をクリックすると検索結果をAS番号の降順で表示する。

A.1.3.2. 許可リストテキスト表示

許可リストテキスト表示画面を以下に示す。



許可リスト一覧画面から許可リストテキスト表示画面に遷移する。

```
34 ROUTEREGTEST 5000-/32 ~AS99999.99999, AS37911~ allow ~jpnrc~  
33 ROUTEREGTEST 100.0.32.0/19 ~AS37911, AS00001.00001~ allow ~jpnrc~  
32 ROUTEREGTEST 2001.0c40-/32 ~AS37911~ allow ~~~~  
31 ROUTEREGTEST 202.210.58.0/23 ~AS37911~ allow ~~~~  
30 ROUTEREGTEST 202.210.56.0/23 ~AS37911~ allow ~~~~  
19 ROUTEREGTEST 100.0.10.0/24 ~AS9.9, AS2.5~ allow ~~~~
```

「許可リスト一覧」に表示されている許可リストの情報を取得し表示する。

Appendix. 1 経路情報の登録機構のユーザインターフェース

A.1.3.3. 証明書の取得

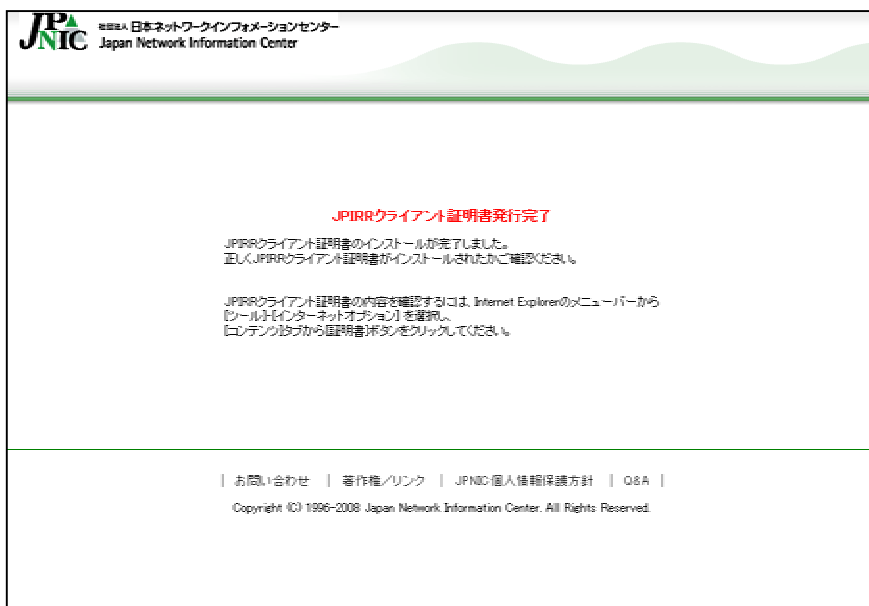
証明書の取得画面について述べる。

The screenshot displays the JPNIC (Japan Network Information Center) website interface for certificate acquisition. At the top, the JPNIC logo and name are visible. The main content area contains the following elements:

- Instructional text: "JPNICクライアント証明書取得用のアクセスキーを入力し、「証明書発行」ボタンを押してください。" and "「証明書発行」ボタンを押すと、次のような警告ダイアログが表示されます。"
- Two warning dialog boxes with yellow triangles and exclamation marks:
 - The first dialog asks: "この Web サイトはユーザーの代わりに新しい証明書を要求しています。ユーザーの代わりに証明書を要求できるのは、信頼された Web サイトだけに制限する必要があります。証明書を要求しますか?" with "はい(Y)" and "いいえ(N)" buttons.
 - The second dialog asks: "この Web サイトは 1 つ以上の証明書をこのコンピュータに追加しています。信頼していない Web サイトがユーザーの証明書を要求できる可能性があります。この Web サイトは、信頼されていない Web サイトからインストールされ、まだ信頼されていない可能性があります。このコンピュータ上でも実行され、ユーザーのカーソルでアクセスする可能性があります。このプログラムで証明書を追加しますか? この Web サイトを信頼している場合は、「はい」をクリックします。信頼していない場合は、「いいえ」をクリックします。" with "はい(Y)" and "いいえ(N)" buttons.
- Red text instruction: "これらのダイアログでは必ず、「はい」を選択してください。" and "いいえ」を選択した場合、正解に JPNICクライアント証明書がインストールされませんのでご注意ください。" and "いいえ」を選択してしまった場合は再度 JPNICクライアント証明書発行処理をやり直してください。"
- An "アクセスキー" (Access Key) input field with a button to the right.
- A "証明書発行" (Certificate Issuance) button.
- Footer: "お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | O&A | Copyright (C) 1996-2008 Japan Network Information Center. All Rights Reserved."

オブジェクト登録者用証明書の取得を行う。
アクセスキーを入力し「証明書発行」ボタンをクリックすることで、認証を行い「証明書発行完了」に遷移する。

Appendix. 1 経路情報の登録機構のユーザインターフェース



オブジェクト登録者用証明書の発行が完了したことを表示する。確認にはWebブラウザの証明書管理画面を参照する。(図ではInternet Explorerの例を示しているが、Mozilla Firefoxでも同じような操作である。)

Appendix 2

JPIRR 認証局 認証業務規程

第 1 版

JPIRR 認証局
認証業務規程
(Certification Practice Statement)

Verion 1.0

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

目次

1. はじめに.....	1
1.1. 概要.....	1
1.2. 文書の名前と識別.....	1
1.3. PKI の関係者.....	3
1.4. 証明書の使用方法.....	6
1.5. ポリシ管理.....	7
1.6. 定義と略語.....	8
2. 公開とリポジトリの責任.....	10
2.1. リポジトリ.....	10
2.2. 証明情報の公開.....	10
2.3. 公開の時期又は頻度.....	10
2.4. リポジトリへのアクセス管理.....	11
3. 識別及び認証.....	12
3.1. 名前決定.....	12
3.2. 初回の本人性確認.....	13
3.3. 鍵更新申請時の本人性確認と認証.....	15
3.4. 失効申請時の本人性確認と認証.....	15
4. 証明書のライフサイクルに対する運用上の要件.....	16
4.1. 証明書申請.....	16
4.2. 証明書申請手続.....	18
4.3. 証明書発行.....	20
4.4. 証明書の受領確認.....	21
4.5. 鍵ペアと証明書の用途.....	22
4.6. 証明書の更新.....	23
4.7. 証明書の鍵更新.....	24
4.8. 証明書の変更.....	25
4.9. 証明書の失効と一時停止.....	26
4.10. 証明書のステータス確認サービス.....	30
4.11. 登録の終了.....	30
4.12. キーエスクローと鍵回復.....	30
5. 設備上、運営上、運用上の管理.....	31
5.1. 物理的管理.....	31
5.2. 手続的管理.....	33
5.3. 人事的管理.....	34
5.4. 監査ログの手続.....	36
5.5. 記録の保管.....	38
5.6. 鍵の切替.....	40
5.7. 危殆化及び災害からの復旧.....	41
5.8. 認証局又は登録局の終了.....	41
6. 技術的セキュリティ管理.....	43
6.1. 鍵ペアの生成及びインストール.....	43
6.2. 私有鍵の保護及び暗号モジュール技術の管理.....	45
6.3. その他の鍵ペア管理.....	47
6.4. 活性化データ.....	48

6.5. コンピュータのセキュリティ管理.....	48
6.6. ライフサイクルの技術上の管理.....	49
6.7. ネットワークセキュリティ管理.....	49
6.8. タイムスタンプ.....	49
7. 証明書と、証明書失効リスト及びOCSPのプロファイル.....	50
7.1. 証明書のプロファイル.....	50
7.2. 証明書失効リストのプロファイル.....	55
7.3. OCSP プロファイル.....	57
8. 準拠性監査とその他の評価.....	58
8.1. 評価の頻度又は評価が行われる場合.....	58
8.2. 評価人の身元又は資格.....	58
8.3. 評価人と評価されるエンティティとの関係.....	58
8.4. 評価で扱われる事項.....	58
8.5. 不備の結果としてとられる処置.....	58
8.6. 評価結果の情報交換.....	58
9. 他の業務上の問題及び法的問題.....	60
9.1. 料金.....	60
9.2. 財務的責任.....	60
9.3. 情報の秘密性.....	60
9.4. 個人情報のプライバシー保護.....	62
9.5. 知的財産権.....	63
9.6. 表明保証.....	64
9.7. 保証の制限.....	65
9.8. 責任の制限.....	65
9.9. 補償.....	66
9.10. 有効期間と終了.....	67
9.11. 関係者間の個別通知と連絡.....	67
9.12. 改訂.....	67
9.13. 紛争解決手続.....	68
9.14. 準拠法.....	68
9.15. 適用法の遵守.....	68
9.16. 雑則.....	68
9.17. その他の条項.....	69

1. はじめに

1.1. 概要

本 JPIRR 認証局 認証業務規程（以下、CPS という）は、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（以下、JPNIC という）にて運用されている経路情報データベース（IRR（Internet Routing Registry の略））の各種管理業務における電子的な認証手続きを提供する JPIRR 認証局（以下、本認証局という）の認証業務運用規則を定める。

本認証局は、本 CPS に基づき、各種申請処理業務を行う者等に証明書を発行する等の認証サービスを提供する。本認証局は実験としての位置づけで運用される。

本 CPS の構成は、IETF PKIX WG において標準化されている RFC3647「証明書ポリシーと認証実践の枠組み（Certificate Policy and Certification Practices Statement Framework）」に準拠している。

本認証局は、CP（証明書ポリシー）及び CPS（認証実施規程）をそれぞれ独立したものとして定めず、本 CPS として証明書ポリシー及び運用規程を定めるものとする。

JPNIC は、認証業務の提供にあたり、自らのポリシー、証明書所有者及び証明書検証者の義務等を、本 CPS、証明書所有者同意書によって包括的に定める。なお、本 CPS と証明書所有者同意書の内容に齟齬がある場合は、証明書所有者同意書が優先して適用されるものとする。

本 CPS は、証明書所有者及び証明書検証者がいつでも閲覧できるように JPNIC の Web ページ上（<http://jpnica.nic.ad.jp/>）に公開する。

(1)CPS

CPS は、証明書の目的、適用範囲、証明書プロファイル、本人認証方法及び証明書所有者の鍵管理並びに認証業務に関わる一般的な規定を記述した文書である。本 CPS は、必要に応じて証明書所有者同意書を参照する。

(2)証明書所有者同意書

証明書所有者同意書は、認証サービスの内容や証明書所有者の義務等、証明書所有者と JPNIC 間における、認証サービス利用上の諸規則を記述した文書である。

1.2. 文書の名前と識別

本 CPS の正式名称は「JPNIC 認証局 認証業務規程」という。

JPNIC 及び本認証局に関連するオブジェクト識別子を表 1-1 に示す。

表 1-1 JPNIC 及び JPNIC 認証局に関連するオブジェクト識別子

オブジェクト	オブジェクト識別子
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	1.2.392.200175
JPIRR 認証局 認証業務規程 (CPS)	1.2.392.200175.1.2.2
EE 証明書ポリシー	1.2.392.200175.1.2.2

1.3. PKI の関係者

1.3.1. 認証局、登録局、所有者及び検証者

本認証局が発行する証明書の流通するコミュニティの PKI 関係者には、表 1-2 に示す登場者が含まれる。

表 1-2 コミュニティに関する登場者と役割

登場者	略称	役割、説明
サーバ		本認証業務に用いる JPNIC のサーバ
資源申請者		許可リストの登録業務を行う者
オブジェクト登録者		JPIRR へオブジェクト登録業務を行う者
オブジェクト登録者証明書		オブジェクト登録者に対して発行される証明書
メンテナ管理者		オブジェクト登録者の任命及び解任、委任等を行う者
メンテナ管理者証明書		本認証局の認証業務に必要な運用用証明書の一つ。オブジェクト登録者への証明書発行時のメンテナ管理者の認証に必要な証明書であり、その取扱いについては運用規則に則って厳格に管理・運用されるものとする。
JPNIC 職員向け証明書		本認証局の認証業務に必要な運用用証明書の一つ。IP レジストリシステムにおけるメンテナ管理者の識別子の管理等の業務を行う JPNIC の職員に対して発行される証明書
エンドエンティティ	EE	証明書の発行対象である、オブジェクト登録者、メンテナ管理者、JPNIC 職員の総称
エンドエンティティ証明書	EE 証明書	EE に発行される証明書の総称
証明書申請者	申請者	証明書を申請中の者
証明書所有者	所有者	証明書発行申請を行い、自ら鍵を生成し、認証局により証明書を発行される主体をあらわす。本 CPS では、EE 証明書を所有している者又はサーバの管理者となる。
証明書検証者	検証者	証明書を受け取る者で、その証明書をを用いて検証することにより、その証明書及び/又はデジタル署名に依拠して行動する者

登場者	略称	役割、説明
JPNIC 発行局	JPNIC IA	JPNIC ルート認証局内の発行局及び JPNIC 資源管理認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC 資源管理認証局で発行業務をつかさどる組織。RA より依頼された証明書の発行を行う。 認証局 (CA) の内、証明書の発行、失効等の証明書管理機能を表す場合に使用。
JPNIC 登録局	JPNIC RA	証明書発行の証明書申請者の本人を確認し、主として登録業務・失効業務をつかさどる組織。証明書の所有者の本人確認と認証に責任を持っている。
担当理事		JPNIC セキュリティ事業の担当理事。JPNIC 認証局の運営方針の決定等を行う。
認証局管理者	CAO	認証局サーバ、ディレクトリサーバ等認証局システムの運用管理をする者。
登録局管理者	RAO	登録局 (RA) を管理し運営する者。証明書発行、失効の登録作業を行う。
リポジトリ		認証局が署名した証明書及び CRL 等を格納し公表するデータベース。
JPNIC ルート認証局		JPNIC が運営を行う認証局全体のルート認証局。JPNIC における認証階層経路の最上位に位置し、自己署名し、かつ配下にある下位認証局 (資源管理認証局) の証明書に電子署名を行う。
JPIRR 認証局		JPNIC が運営を行う IRR 管理業務に関連する証明書の発行を行う認証局。JPIRR 認証局証明書は、JPNIC ルート認証局により電子署名される。
JPNIC 認証局		JPNIC が運営を行う認証局の総称。
ローカル RA		証明書を発行する組織とは異なる組織若しくは団体であり、RA 業務において、本人の確認・審査、証明書発行申請処理及び証明書失効申請処理を行う組織。JPNIC 認証局の場合、IP アドレス管理指定事業者がローカル RA となる。

登場者	略称	役割、説明
ローカル RA 責任者		IP アドレス管理指定事業者の中における、ローカル RA 業務の責任者。メンテナー管理者の任命・解任を行う。
メンテナー管理者		オブジェクト登録者のメンバ管理と認証及びオブジェクト登録者証明書の発行申請操作を行う。

1.3.2. その他の関係者

規定しない。

1.4. 証明書の使用方式

1.4.1. 適切な証明書の使用

本 CPS に基づき発行される証明書は、JPNIC の行う経路情報管理業務における各種の申請及び連絡等を目的として、経路情報の登録認可機構がユーザ及びメッセージを検証する為に使われるものとする。

1.4.2. 禁止される証明書の使用

本 CPS に基づき発行される証明書は、JPNIC における各種申請処理業務等に利用することを意図するものである。また JPNIC は、オブジェクト登録者相互間での証明書の使用を制限するものではないが、本使用に対してなんら責任を負うものではない。

1.4.3. 証明書の相互運用性

JPNIC 認証局は、他の認証局と相互認証を行うことがあるものとする。

1.5. ポリシ管理

1.5.1. 文書を管理する組織及び連絡担当者

本 CPS を管理する組織及び問い合わせ先を次に定める。

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

受付時間：月～金（年未年始 / 祝祭日は除く） 10:00～18:00

電子メールアドレス：(ca-query@nic.ad.jp)

1.5.2. CPS のポリシ適合性を決定する者

本 CPS が、本認証局の運営方針として適切か否かの判断は、JPNIC の担当理事が行う。

1.5.3. CPS 承認手続

本 CPS の改定は、担当理事により承認を受けた後に公表されるものとする。

1.6. 定義と略語

本 CPS にて使用される用語は、表 1-3 に示すとおりである。

表 1-3 用語

用語	略称	説明
電子証明書	証明書	ある公開鍵を、記載されたものが保有することを証明する電子的文書。認証局が電子署名を施すことで、その正当性が保証される。本 CPS では、特に断らない限りオブジェクト登録者証明書、サーバ証明書及び運用用証明書を総称して「証明書」と呼ぶ。
認証局	CA	証明書の発行・更新・失効、認証局等私有鍵の生成・保護及び証明書申請者の登録を行う機関。本 CPS 内で、単に認証局という場合は証明書の発行業務及び登録業務を含む。
RFC 3647 (Request For Comments 3647)		認証局 や PKI のための CPS の執筆者を支援するフレームワーク。
オブジェクト識別子 (Object Identifier)	OID	世界で一意となる値を登録機関 (ISO、ITU) に登録した識別子。PKI で使うアルゴリズム、証明書内に格納する名前 (subject) のタイプ (Country 名等の属性) 等は、オブジェクト識別子として登録されているものが使用される。
X.509		ITU-T が定めた証明書及び証明書失効リストのフォーマット。X.509 v3 では、任意の情報を保有するための拡張領域が追加された。
公開鍵		公開鍵暗号方式において用いられる鍵ペアの一方。私有鍵に対応する、公開されている鍵。
私有鍵		公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、本人のみが保有する鍵。
証明書発行要求 (Certificate Signing Request)	CSR	証明書を発行する際のもととなるデータファイル。CSR には証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して証明書を発行する。

用語	略称	説明
CRL (Certificate Revocation List)		証明書の有効期間中に、認証局私有鍵の危殆化等の事由により失効された EE 証明書及び運用用証明書の失効リスト。
PIN (Personal Identification Number)		個人を識別するための情報。

2. 公開とリポジトリの責任

2.1. リポジトリ

本認証局は、リポジトリを一日 24 時間、一週 7 日間利用できるように維持管理に努める。リポジトリには証明書リポジトリと情報公開用リポジトリがある。システムの保守等において、一時的に停止を行う必要がある場合は、証明書所有者、証明書検証者及び関係者に対して、事前に通知若しくは Web ページで公表するものとする。ただし、災害、事故、障害発生時等やむを得ない事態が発生した場合はこの限りではない。

2.2. 証明情報の公開

次の情報を情報公開用リポジトリ上に公開する。

- CPS

また次の情報を証明書リポジトリ上に公開する。

- EE 証明書
- CRL

ただし EE 証明書と CRL は検証者のみに公開する。

なお、CPS 及び認証局に関する重要情報は、次に示す URI の Web ページにおいても公開される。

<http://jpnica.nic.ad.jp/>

2.3. 公開の時期又は頻度

本認証局が公開する情報について、公開の時期及び頻度は次のとおりである。

- CPS については改定の都度に公表される。
- 自己署名証明書、リンク証明書、下位認証局証明書については、発行及び更新の都度公表される。
- CRL については、発行の都度公表される。発行の頻度は本 CPS「4.9.7.

証明書失効リストの発行頻度」で規定される。

- 認証局に関する重要情報若しくはその他の情報は、必要に応じて適宜更新が行われる。
- EE 証明書については、発行及び更新の都度公表される。

2.4. リポジトリへのアクセス管理

本認証局は公開情報に関して、読み取り専用の制御以外に特段のアクセスコントロールは行わない。認証に使われる EE 証明書の証明書検証者は JPNIC であるとする。従って基本的に証明書リポジトリは JPNIC に向けて提供される。

3. 識別及び認証

3.1. 名前決定

3.1.1. 名前の種類

証明書発行者の名前と発行対象の名前は、X.500 シリーズ定義の識別名の規定に従って設定する。

3.1.2. 名前が意味を持つことの必要性

証明書に記載される名前は、個人名、組織名、役割名、および機器名をあらわすものである必要がある。

3.1.3. 所有者の匿名性

証明書には、個人、組織、役割、および機器が特定できる名前であれば、実名を使用する必要はない。

3.1.4. 種々の名前形式を解釈するための規則

様々な名前の形式を解釈するルールは、X.500 シリーズ定義の識別名の規定に従う。

3.1.5. 名前の一意性

証明書に記載される名前は、本認証局が同一ポリシーのもとで発行する全ての EE に対して一意とする。同一 EE に対する証明書の更新が行われた場合、更新前の証明書と名前が重複する場合がある。

3.1.6. 商標の認識、認証及び役割

規定しない。

3.2. 初回の本人性確認

3.2.1. 私有鍵の所持を証明する方法

本認証局は、PKCS#10 (Public-Key Cryptography Standards #10) に従った電子署名のされた証明書発行要求の利用、その他本認証局が認めた方法を通じて、オブジェクト登録者証明書の申請者が私有鍵を所有していることを確認する。

サーバ証明書に関しては、本認証局は、予め規定された方法により証明書申請者が私有鍵を所有していることを確認する。

3.2.2. 組織の認証

本認証局は、ローカル RA に対して組織若しくは団体の認証を行う。ローカル RA としての認証を受けようとする組織若しくは団体は IP 指定事業者でなければならない。

サーバ証明書に関しては、本認証局は、証明書の発行対象となるサーバを運用・管理する組織若しくは団体が、JPNIC 又は JPNIC が認める組織若しくは団体であることを確認する。

3.2.3. 個人の認証

JPNIC は、メンテナナー管理者証明書の申請者の発行登録を行う際に、所定の手続きに従って申請者の認証を行うこととする。

メンテナナー管理者は、オブジェクト登録者証明書の申請者の発行登録を行う際に、所定の手続きに従って申請者の認証を責任を持って行うこととする。

JPNIC は、JPNIC 職員向け証明書の申請者の発行登録を行う際に、所定の手続きに従って申請者の認証を行うこととする。

サーバ証明書に関しては、本認証局は、証明書の発行を申請する者が、JPNIC 又は JPNIC が認める組織若しくは団体より証明書の発行の許可を受けている者であることを確認する。

3.2.4. 確認しない所有者の情報

規定しない。

3.2.5. 権限の正当性確認

本認証局は、メンテナナー管理者からオブジェクト登録者証明書の申請登録を受け付けるにあたって、当該メンテナナー管理者の正当性を確認する。

3.2.6. 相互運用の基準

規定しない。

3.3. 鍵更新申請時の本人性確認と認証

3.3.1. 通常の鍵更新の本人性確認と認証

本 CPS「3.2.初回の本人性確認」に定める手順と同様とする。

3.3.2. 証明書失効後の鍵更新の本人性確認と認証

本 CPS「3.2.初回の本人性確認」に定める手順と同様とする。

3.4. 失効申請時の本人性確認と認証

JPNIC は、メンテナ管理者証明書に対する失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。

メンテナ管理者は、原則としてオブジェクト登録者証明書に対する失効申請者の本人確認を行い、本認証局の定めた方式により、本認証局に失効登録を行うものとする。

JPNIC は、JPNIC 職員向け証明書に対する失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。

サーバ証明書に関しては、本認証局は、証明書の失効を申請する者が、JPNIC 又は JPNIC が認める組織若しくは団体より証明書の発行の許可を受けている者であることを、予め規定された方法により確認する。

4. 証明書のライフサイクルに対する運用上の要件

4.1. 証明書申請

4.1.1. 証明書申請を提出することができる者

メンテナ－管理者証明書の申請を行うことができる者は、以下の(1)～(4)のいずれかに該当する者とする。

- (1)IP アドレス管理指定事業者
- (2)特殊用途用プロバイダ非依存アドレスの割り当てを受けた組織
- (3)JPNIC から AS 番号の割り当てを受けた組織または個人
- (4)JPNIC から歴史的経緯を持つプロバイダ非依存アドレスの割り当てを受けた組織または個人

オブジェクト登録者証明書の申請を行うことができる者は、認証されたメンテナ－管理者とする。

JPNIC 職員向け証明書の申請を行うことができるものは、JPNIC に所属する者とする。

サーバ証明書の申請を行うことができる者は、JPNIC の職員若しくは JPNIC が指定した者とする。

4.1.2. 登録手続及び責任

メンテナ－管理者証明書の申請者は、JPNIC により事前に周知された方法に従い、JPNIC に対して証明書の発行申請を行う。メンテナ－管理者は申請書の記載によって役割を確認される。

オブジェクト登録者証明書の申請者は、メンテナ－管理者により事前に周知された方法に従い、メンテナ－管理者に対して証明書の発行申請を行う。また、証明書申請者は、本認証局より鍵ペア生成及び証明書発行に必要な 2 種類の情報が通知されたならば、鍵ペアを生成し、本認証局へ PKCS#10 等の証明書発行要求のデータ形式に従った電子署名のされた証明書発行要求をセキュアなオンライン通信を介して送付する。証明書発行要求の電子署名は検証される。

サーバ証明書の申請者は、本認証局に対して予め規定された方法により証明書の発行申請を行う。

JPNIC 職員向け証明書の申請者は、本認証局に対して予め規定された方法により証明書の発行申請を行う。

証明書申請者は証明書を申請するにあたって、次の責任を負うものとする。

- 本 CPS、その他本認証局により開示された文書の内容の承諾
- 証明書申請内容の正確な提示

4.2. 証明書申請手続

4.2.1. 本人性確認と認証機能の実行

メンテナ－管理者証明書の申請者の本人性確認は JPNIC の登録局管理者が行う。

オブジェクト登録者証明書の申請者の本人性確認はメンテナ－管理者が行う。メンテナ－管理者は、本 CPS「1.1.1.個人の認証」に基づき、オブジェクト登録者証明書の申請者の本人確認を実施する。メンテナ－管理者は、オブジェクト登録者証明書の申請者の本人確認に関して責任を負うものとする。

JPNIC 職員向け証明書の申請者の本人性確認は、本認証局が予め規定された方法により行う。

サーバ証明書の申請者の本人性確認は、本認証局が予め規定された方法により行う。

4.2.2. 証明書申請の承認又は却下

メンテナ－管理者はオブジェクト登録者証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は、本認証局に対し証明書の申請登録を行う。メンテナ－管理者は申請の審査に関して責任を負うものとする。

JPNIC の登録局管理者はメンテナ－管理者証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は本認証局に対し証明書の申請登録を行う。JPNIC の登録局管理者は申請の審査に関して責任を負うものとする。

なお、本認証局は、オブジェクト登録者証明書の申請登録を行うメンテナ－管理者の本人性確認を行った後、証明書の発行手続を開始する。

JPNIC 職員向け証明書に関しては、本認証局が申請の諾否を決定する。

サーバ証明書に関しては、本認証局が申請の諾否を決定する。

4.2.3. 証明書申請の処理時間

メンテナ－管理者は、オブジェクト登録者証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。

JPNIC の登録局管理者はメンテナ－管理者証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。

本認証局は、メンテナ－管理者又は JPNIC の登録局管理者からの発行申請登録を受理した場合、速やかに証明書の発行を行う。

JPNIC 職員向け証明書に関しては、本認証局は、本 CPS「4.1.1.証明書申請を提出することができる者」にて規定した者より発行申請を受理した場合、速やかに証明書の発行を行う。

サーバ証明書に関しては、本認証局は、本 CPS「4.1.1.証明書申請を提出することができる者」にて規定した者より発行申請を受理した場合、速やかに証明書の発行を行う。

4.3. 証明書発行

4.3.1. 証明書の発行過程における認証局の行為

本認証局は、メンテナー管理者からのオブジェクト登録者証明書の発行申請登録を受け付けるにあたって、予め定められた方法によりメンテナー管理者の権限確認を行う。またメンテナー管理者証明書の発行申請登録を受け付けるにあたって、予め定められた方法によりメンテナー管理者の権限確認を行う。本認証局は、申請登録の真正性を確認した後、オブジェクト登録者証明書の申請者に対し、本 CPS「4.3.2.認証局の所有者に対する証明書発行通知」に定められた方法で証明書の発行が許可されたことを通知する。

本認証局は、オブジェクト登録者証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、セキュアなオンライン通信を介してオブジェクト登録者証明書の申請者に対し証明書を発行する。

本認証局は、メンテナー管理者証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、オフラインの手段を介してメンテナー管理者証明書の申請者に対し証明書を発行する。

JPNIC 職員向け証明書に関しては、本認証局は、申請者の本人性確認を行った後、予め規定された方法により証明書の発行を行う。

サーバ証明書に関しては、本認証局は、申請者の本人性確認を行った後、予め規定された方法により証明書の発行を行う。

4.3.2. 認証局の所有者に対する証明書発行通知

メンテナー管理者証明書はオフラインの手段により申請者に対し発行通知を行う。

本認証局は、証明書発行に必要な情報を生成し、メンテナー管理者経由でオブジェクト登録者証明書の申請者へ通知する。

JPNIC 職員向け証明書に関しては、本認証局は、予め規定された方法により申請者に対し発行通知を行う。

サーバ証明書に関しては、本認証局は、予め規定された方法により申請者に対し発行通知を行う。

4.4. 証明書の受領確認

4.4.1. 証明書の受領確認の行為

メンテナ－管理者証明書に関してはオフラインの手段を使い受領する。証明書に不具合がある場合は JPNIC へ連絡を行う。配達後一週間後までに連絡がない場合は受領したとみなす。

本認証局は、到達確認のできる方法でメンテナ－管理者の証明書を配達する。オブジェクト登録者証明書の申請者による証明書のダウンロードし、確認した上で受領するものとする。証明書に不具合がある場合はメンテナ－管理者を通じて JPNIC へ連絡を行う。ダウンロード後一週間後までに不具合の連絡がない場合は受領したとみなす。

JPNIC 職員向け証明書に関しては、本認証局は予め規定されたオフラインの手段を使う方法により証明書の受領を確認する。

サーバ証明書に関しては、本認証局は予め規定された方法により証明書の受領を確認する。

なお、証明書の申請者は、証明書ファイルが自身の環境で利用可能であること、証明書の記載内容が正しいことを確認しなければならない。

4.4.2. 認証局による証明書の公開

本認証局は、本 CPS「2.2.証明情報の公開」に規定する証明書をリポジトリにて公開する。

4.4.3. 他のエンティティに対する認証局の証明書発行通知

本認証局は、他のエンティティに対して証明書の発行通知を行わない。

4.5. 鍵ペアと証明書 の用途

4.5.1. 所有者の私有鍵及び証明書 の使用

本 CPS に基づき発行される証明書は、JPNIC と IP アドレス管理指定事業者間での申請等業務に利用することを意図するものである。

証明書所有者は、私有鍵及び証明書の使用に関して、次の責任を負うものとする。

- 証明書の記載内容の受領時確認と誤記内容の申告
- 私有鍵の盗難・漏えい・紛失・他者による不正利用等を防ぐことへの十分な注意と管理
- 鍵の危殆化又はその可能性がある場合の速やかな失効申請
- 使用目的の確認及び、その目的内での使用
- 私有鍵の秘匿管理や私有鍵と公開鍵の対応管理

4.5.2. 検証者の公開鍵及び証明書 の使用

証明書検証者は、証明書を信頼するにあたって、次の責任を負う。

- 証明書を信頼する時点で、本 CPS の理解と承諾
- 証明書の使用目的と自己の使用目的が合致していることの承諾
- 証明書に行われた電子署名の検証と発行者の確認
- 証明書の有効期間や記載項目の確認
- CRL に基づいて、証明書が失効していないことの確認
- 証明書パス上の全証明書の改ざん、有効期間、失効、使用目的の確認

4.6. 証明書を更新

本認証局では、鍵ペアの更新を伴わない証明書の更新は行わない。証明書を更新する場合は、新たな鍵ペアを生成することとし、本 CPS「4.7.証明書の鍵更新」に定める手続とする。

4.6.1. 証明書更新が行われる場合

規定しない。

4.6.2. 証明書の更新を申請することができる者

規定しない。

4.6.3. 証明書の更新申請の処理

規定しない。

4.6.4. 所有者に対する新しい証明書の通知

規定しない。

4.6.5. 更新された証明書の受領確認の行為

規定しない。

4.6.6. 認証局による更新された証明書の公開

規定しない。

4.6.7. 他のエンティティに対する通知

規定しない。

4.7. 証明書のカ更新

4.7.1. 証明書の更新の場合

証明書の更新は、次の場合に行われるものとする。

- 証明書の有効期間が終了する場合
- 鍵の危険化を理由に証明書が失効された場合

4.7.2. 新しい公開鍵の証明申請を行うことができる者

本 CPS「4.1.1.証明申請を提出することができる者」と同様とする。

4.7.3. 証明書の更新申請の処理

本 CPS「4.2.証明申請手続」及び「4.3.証明発行」に定める手続と同様とする。

4.7.4. 所有者に対する新しい証明書の通知

本 CPS「4.3.2.認証局の所有者に対する証明発行通知」と同様とする。

4.7.5. 更新された証明書の受領確認の行為

本 CPS「4.4.1 証明書の受領確認の行為」と同様とする。

4.7.6. 認証局による更新済みの証明書の公開

本 CPS「4.4.2.認証局による証明書の公開」と同様とする。

4.7.7. 他のエンティティに対する通知

本 CPS「4.4.3.他のエンティティに対する認証局の証明発行通知」と同様とする。

4.8. 証明書の変更

4.8.1. 証明書の変更の場合

証明書の変更は、次の場合に行われるものとする。

- 証明書に含まれる公開鍵以外の情報に変更が生じた場合

4.8.2. 証明書の変更を申請することができる者

本 CPS 「4.7.2.新しい公開鍵の証明申請を行うことができる者」と同様とする。

4.8.3. 変更申請の処理

本 CPS 「4.7.3.証明書の鍵更新申請の処理」と同様とする。

4.8.4. 所有者に対する新しい証明書の通知

本 CPS 「4.7.4.所有者に対する新しい証明書の通知」と同様とする。

4.8.5. 変更された証明書の受領確認の行為

本 CPS 「4.7.5.鍵更新された証明書の受領確認の行為」と同様とする。

4.8.6. 認証局による変更された証明書の公開

本 CPS 「4.7.6.認証局による鍵更新済みの証明書の公開」と同様とする。

4.8.7. 他のエンティティに対する認証局の証明書発行通知

本 CPS 「4.7.7.他のエンティティに対する通知」と同様とする。

4.9. 証明書の失効と一時停止

4.9.1. 証明書失効の場合

オブジェクト登録者証明書の証明書所有者は、メンテナ管理者に証明書の失効申請を行わなければならない。

メンテナ管理者証明書の証明書所有者は、JPNIC に証明書の失効申請を行わなければならない。

本認証局は次の項目に該当すると認めた場合、いずれの証明書の失効処理を行うことができる。

- 本認証局を廃止する場合
- 認証局私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書記載事項が事実と異なる場合
- 証明書所有者の私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書の不正使用、若しくはそのおそれがある場合
- 証明書所有者あるいはローカル RA が、本 CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合
- JPNIC 認証局と IP アドレス管理指定事業者との間の契約が解除された場合
- その他本認証局が失効の必要があると判断した場合

サーバ証明書の証明書所有者は次の項目に該当する場合に本認証局に対し失効申請を行わなければならない。

- サーバの使用を停止する場合
- サーバの私有鍵が危殆化した（又はそのおそれがある）場合
-

また、本認証局は、証明書所有者からの失効申請のほか本認証局は、証明書所有者からの失効申請の他に、次の項目に該当すると認めた場合、サーバ証明書の失効処理を行うことができる。

- 本認証局を廃止する場合
- 認証局私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書記載事項が事実と異なる場合
- サーバの私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書の不正使用、若しくはそのおそれがある場合
- 証明書所有者が本 CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合

- その他本認証局が失効の必要があると判断した場合

4.9.2. 証明書失効を申請することができる者

オブジェクト登録者証明書の失効要求ができる者は、次のとおりである。

- 証明書所有者
- 証明書所有者の法律上の正式な代理人
- 証明書所有者が所属する組織のローカル RA 責任者、メンテナー管理者
- 本認証局

サーバ証明書の失効要求ができるものは、次のとおりである。

- 証明書所有者
- 本認証局

4.9.3. 失効申請手続

メンテナー管理者は所定の手続きに従って失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。

JPNIC は所定の手続きに従って失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。

サーバ証明書の所有者は、本認証局に対し予め規定された方法により失効申請を行う。

なお、「4.4.1.証明書が失効される理由」にて列挙する項目に該当すると本認証局が認めた場合には、本認証局が自身の判断により証明書の失効登録を行うことがある。

4.9.4. 失効申請の猶予期間

証明書の失効要求は、失効すべき事象が発生した場合、可能な限り速やかに行われるものとする。

4.9.5. 認証局が失効申請を処理しなければならない期間

本認証局における証明書の失効処理は、失効申請の受領後、5 営業日以内に行われる。

4.9.6. 検証者の失効調査の要求

証明書検証者は、本認証局により発行された証明書を信頼し利用するにあたって、

最新の CRL を参照し当該証明書の失効処理が行われていないことを確認しなければならない。

4.9.7. 証明書失効リストの発行頻度

CRL は証明書失効の有無に関わらず、24 時間以内に更新される。証明書の失効が申請された場合は、失効手続が完了した時点で更新される。

4.9.8. 証明書失効リストの発行最大遅延時間

本認証局は、CRL が生成された後、速やかにリポジトリに公開する。

4.9.9. オンラインでの失効/ステータス確認の適用性

OCSP 等のオンラインの失効又はステータスチェックの機能はサポートしない。

4.9.10. オンラインでの失効/ステータス確認を行うための要件

規定しない。

4.9.11. 利用可能な失効通知の他の形式

規定しない。

4.9.12. 鍵更新の危殆化に対する特別要件

本認証局は、本認証局の私有鍵に危殆化又は危殆化のおそれがある場合は、直ちに全ての証明書の失効処理を行い、CRL に登録し、証明書所有者に対してメール等の手段で本認証局の私有鍵の危殆化等の事実と証明書失効の通知を行う。

4.9.13. 証明書の一時停止の場合

本認証局は、発行した証明書の一時停止を行わない。

4.9.14. 証明書の一部停止を申請することができる者

規定しない。

4.9.15. 証明書の一部停止申請手続き

規定しない。

4.9.16. 一部停止を継続することができる期間

規定しない。

4.10. 証明書のステータス確認サービス

4.10.1. 運用上の特徴

本認証局は、証明書検証者における証明書ステータスの確認手段として、CRL を提供する。CRL へのアクセス要件は、本 CPS「2.4.リポジトリへのアクセス管理」に規定する。また、CRL の発行頻度及び発行最大遅延時間については、本 CPS「4.9.7. 証明書失効リストの発行頻度」及び「4.9.8. 証明書失効リストの発行最大遅延時間」に規定する。

4.10.2. サービスの利用可能性

本 CPS「2.1.リポジトリ」に規定する。

4.10.3. オプションな仕様

規定しない。

4.11. 登録の終了

証明書所有者が本認証局のサービスの利用登録を終了する場合、本認証局は証明書所有者に対して発行した証明書の全てを失効する。

4.12. キーエスクローと鍵回復

本認証局は私有鍵を第三者に対して寄託しない。

4.12.1. キーエスクローと鍵回復ポリシー及び実施

規定しない。

4.12.2. セッションキーのカプセル化と鍵回復ポリシー及び実施

規定しない。

5. 設備上、運営上、運用上の管理

5.1. 物理的管理

5.1.1. 立地場所及び構造

本認証局に係わる重要な設備については、火災、水害、地震、落雷その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。建物の内外には、認証設備室の所在についての表示を行わない。

また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置する。

5.1.2. 物理的アクセス

本認証局は、認証設備室に関して、事前に定められた本人の特定及び入室権限の確認を可能とする入退室管理を行う。本認証局は、入室権限を有しない者の入室を原則として認めない。やむを得ずこれを認める場合は、予め認証局運用管理者の許可を得て、入室権限者同行のうえこの者を入室させることとする。

5.1.3. 電源及び空調

本認証局は、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電及び電圧・周波数の変動に備えた対策を講ずる。また空調設備に関して、各種使用する機器類に悪影響を与えないよう維持管理を行う。

5.1.4. 水害及び地震対策

本認証局の設備を設置する室は防水対策を施し、浸水による被害を最小限に抑える。また、JPNIC 認証局は、地震等による機器及び什器の転倒及び落下を防止する対策を講ずる。

5.1.5. 火災防止及び火災保護対策

本認証局は、設備を防火壁によって区画された防火区画内に設置する。また防火区画内では電源設備や空調設備の防火措置を講じ、火災報知器及び消火設備の設置を行う。

5.1.6. 媒体保管場所

アーカイブデータ、バックアップデータを含む媒体は、適切な入退管理が行われた室内の保管庫に保管される。また複製された重要な媒体は、本認証局の設置場所とは別の適切な入退管理が行われた室内の保管庫に保管される。

5.1.7. 廃棄処理

本認証局は、機密扱いとする情報を含む書類・記録媒体について、情報の初期化・裁断等、事前に定められた方法に従い適切に廃棄処理を行う。

5.1.8. 施設外のバックアップ

規定しない。

5.2. 手続的管理

5.2.1. 信頼される役割

証明書の発行、更新、失効等の重要な業務に携わる者は、本 CPS 上信頼される役割を担う。

5.2.2. 職務ごとに必要とされる人員

認証局設備の保守、JPNIC 認証局機器等の故障時対応等において、認証設備室への入室権限を有しない者が入室する必要がある場合は、必ず入室権限者の立会いを必要とする。

5.2.3. 個々の役割に対する本人性確認と認証

認証局の設備は、操作者及び必要権限を識別する機能を有するものとする。また、認証局設備を操作する権限は、操作者ごとに設定可能であるものとする。

5.2.4. 職務分割が必要となる役割

権限を特定の個人に集中させず複数人に権限を分離することで、単独操作で発生する不正行為等の防止を図る。システム操作、承認行為及び監査に関する権限は分離される。

5.3. 人事的管理

5.3.1. 資格、経験及び身分証明の要件

JPNIC は、職員に認証局の役割を任命する際及びその後定期的に、適切な人物審査を実施のうえ、任命を行う。任命の際には守秘義務契約を結び、情報の適切な管理を行う。また日常業務においては、メンタルヘルス、健康管理及び適正な処遇等による継続した人事管理を行う。

5.3.2. 人員配属に関する規定事項

認証局業務に関わる要員を任命するにあたって、業務の遂行上支障が出ない適切な人員を配置する。配属されるものは機密保持及び内部規定の遵守に対する誓約書を提出する。

5.3.3. 研修要件

運用要員の教育を次のように行う。

- 運用要員が役割に就く前に、認証局の運用に必要な教育を実施する。
- 役割に応じた教育・訓練計画を策定し、計画に沿って定期的に教育・訓練を実施する。
- 業務手順に変更がある場合は遅滞なく事務取扱要領の必要箇所を変更し、その変更に関わる教育・訓練を実施する。

5.3.4. 再研修の頻度及び要件

JPNIC は定期的に本認証局の要員に対して適切な教育を行い、以降必要に応じて再教育を行う。

5.3.5. 仕事のローテーションの頻度及び順序

規定しない。

5.3.6. 認められていない行動に対する処罰

JPNIC は、本認証局の運用要員による認可されていない行為に対し、予め決められた規程に従って処罰する。

5.3.7. 独立した契約者の要件

JPNIC は、委託契約において委託業務の内容を明確にするとともに、受託者に対して JPNIC の指示の遵守、責任分担、保証、違反時の罰則等について明確にし、かつ受託者と守秘義務契約を結ぶ。また委託後は受託者の業務が適切に行われていることを監督し管理する。

5.3.8. 要員へ提供される資料

運用に必要な文書を運用要員に開示し周知する。

5.4. 監査ログの手続

5.4.1. 記録されるイベントの種類

本認証局システム上で起こったイベントは、それが手動、自動であるかにかかわらず、日付、時刻、イベントを発生させた主体、イベント内容等が記録される。

認証局システムにおける誤操作、不正操作の検知及び運用の正当性を証明するために必要な監査ログとして、次の操作について履歴を記録する。

- 認証局の私有鍵の操作に関する記録
- 証明書の発行及び失効等の作業に関する記録
- 失効情報の作成作業に関する記録
- 監査ログの確認に関する記録

また、認証局設備へのアクセスに関する履歴を記録する。

5.4.2. 監査ログを処理する頻度

本認証局は、監査ログ及び関連する記録を定期的に精査する。

5.4.3. 監査ログを保持する期間

監査ログは、最低 2 ヶ月間は認証局サーバ内に保持される。その後、外部記憶媒体に一定期間保管される。また、認証設備室への入退室に関する記録や不正アクセスに関する記録は、次回の監査終了まで保存されるものとする。

5.4.4. 監査ログの保護

本認証局は、JPNIC によって認可された人員のみが監査ログファイルにアクセスすることができるようにするために権限者を定め、許可されていない者が閲覧、修正又は削除をすることから保護する。また定期的に監査ログのバックアップを外部記憶媒体に取得し、適切な入退室管理が行われている室内において、施錠可能な保管庫に保管する。

5.4.5. 監査ログのバックアップ手続

監査ログは、認証局システムのデータベースとともに、事前に定められた手続に従い、外部記憶媒体に定期的にバックアップがとられ、それらの媒体は安全な施設に保管される。

5.4.6. 監査ログの収集システム

監査ログの収集機能は認証局システムの一機能として内在しているものとし、セキュリティに関する重要なイベントを監査ログとして収集する。

5.4.7. イベントを起こしたサブジェクトへの通知

本認証局では、監査ログの収集を、イベントを発生させた人、システム又はアプリケーションに対して通知することなく行う。

5.4.8. 脆弱性評価

認証業務において用いるハードウェア及びソフトウェアは、監査ログ検査等によるシステム面及び運用面におけるセキュリティ上の脆弱性評価に加え、最新の実装可能なセキュリティ・テクノロジーの導入等、セキュリティ対策の向上を図るものとする。

5.5. 記録の保管

5.5.1. アーカイブ記録の種類

本 CPS「5.4.1.記録されるイベントの種類」に規定する監査ログに加えて、本認証局は次の記録を保存する。

【認証局システムに記録されるイベント】

- 本認証局の署名用鍵ペアの生成
- システムからの証明書所有者の追加及び削除
- 証明書の発行・失効を含めた鍵の変更
- 登録局管理者権限の追加、変更及び削除

【紙媒体又は外部記憶媒体として保存するもの】

本認証局は次に掲げる運用関連記録のアーカイブを維持、管理する。

- 本 CPS、証明書所有者同意書及びその変更に関する記録
- 認証業務に従事する者の責任及び権限に関して記載した文書及びその変更に関する記録
- 認証業務の一部を他に委託する場合においては、委託契約に関する書類の原本
- 監査の実施結果に関する記録及び監査報告書

5.5.2. アーカイブ保持期間

本認証局は、認証局システムのデータベースの履歴及び監査ログファイルの履歴を一定期間保存する。紙媒体及び外部記憶媒体の保存期間に関しては本 CPS「5.5.1.アーカイブ記録の種類」に規定する。

5.5.3. アーカイブ保護

アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。本認証局は、アーカイブデータのバックアップを定期的に外部記憶媒体に取得し、JPNIC の管理部門が許可した者以外の者がアクセスできないように制限し、温度、湿度等の環境上の脅威から保護された施設に保管する。

5.5.4. アーカイブのバックアップ手続

本認証局は、認証局システムのデータベースに対して、自動的かつ定期的にサーバ上にバックアップを行う。更に、監査ログも定期的に外部記憶媒体に格納する。

5.5.5. 記録にタイムスタンプを付ける要件

本認証局は、本認証局内で記録される重要情報に対してレコード単位にタイムスタンプを付するものとする。ここでいうタイムスタンプとは暗号技術を用いたものではない。

5.5.6. アーカイブ収集システム

認証局サーバデータベース用の履歴収集システムは、認証局サーバシステムに内在している。監査ログファイル用の履歴収集システムについては、本 CPS「5.4.6.監査ログの収集システム」に規定する。

5.5.7. アーカイブの情報を入手し、検証する手続

アーカイブデータは、厳格に管理された区画からアクセス権限者が入手し、外部記録媒体の可読性確認を定期的に行う。また必要に応じ、アーカイブデータの完全性及び機密性の維持に留意し、新しい媒体へ複製を行うとともに、保管期間の過ぎた古い媒体は破棄する。

5.6. 鍵の切替

本認証局の私有鍵は、その有効期間の残りが EE 証明書の最大有効期間よりも短くなる前に、JPNIC はその鍵による新たな EE 証明書の発行を中止し、新たな認証局鍵ペアを本 CPS「6.1. 鍵ペアの生成及びインストール」に定める方法で生成する。新たな公開鍵は JPNIC ルート認証局から証明書の発行を受け、本 CPS「6.1.4. 検証者に対する認証局の公開鍵の交付」に定めた方法と同様に配布を行う。

5.7. 危殆化及び災害からの復旧

5.7.1. 事故及び危殆化の取扱手続

認証局私有鍵の危殆化又は危殆化のおそれがある場合、及び災害等により認証業務の中断又は停止につながるような問題が発生した場合、本認証局は予め定められた計画及び手順に従い、認証業務の再開に努める。

5.7.2. コンピュータの資源、ソフトウェア及び/又は、データが破損した場合

JPNIC 認証局は、ハードウェア、ソフトウェア又はデータが破壊された場合、事前に定められた復旧計画に従い、バックアップ用のハードウェア、ソフトウェア及びデータにより、速やかに復旧作業に努める。

5.7.3. エンティティの私有鍵が危殆化した場合の手続

認証局私有鍵が危殆化した場合は、予め定められた計画に基づいて認証業務を停止し、次の手続を行う。

- メンテナー管理者証明書、オブジェクト登録者証明書、JPNIC 職員向け証明書の失効手続
- 認証局私有鍵の廃棄及び再生成手続
- メンテナー管理者証明書、オブジェクト登録者、JPNIC 職員向け証明書証明書等の再発行手続

また、証明書所有者の私有鍵が危殆化した場合は、本 CPS「4.9.証明書の失効と一時停止」において定める手続に基づき、証明書の失効手続を行う。

5.7.4. 災害後の事業継続能力

災害等により JPNIC 認証局の設備が被害を受けた場合は、JPNIC は予備機を確保しバックアップデータを用いて運用の再開に努める。

5.8. 認証局又は登録局の終了

JPNIC において本認証局の認証業務の終了が決定した場合は、業務終了の事実、並びに業務終了後の本認証局のバックアップデータ及びアーカイブデータ等の保管組織

及び開示方法を業務終了 14 日前までに証明書所有者及び証明書検証者に告知し、所定の業務終了手続を行う。

6. 技術的セキュリティ管理

6.1. 鍵ペアの生成及びインストール

6.1.1. 鍵ペアの生成

本認証局の鍵ペアの生成は鍵管理者立会いのもと、複数人の CAO によって認証設備室内で行われる。本認証局の鍵ペアの生成は、FIPS140-1 レベル 3 の暗号化モジュールを使用して行われる。

メンテナ管理者証明書及び JPNIC 職員向け証明書の鍵ペアの生成は、FIPS140-2 レベル 3 の暗号化モジュールを使用して行われる。

6.1.2. 所有者に対する私有鍵の交付

メンテナ管理者証明書及び JPNIC 職員向け証明書の鍵ペアの生成は、本認証局において暗号化モジュール内で行われる。生成された鍵ペアは暗号化モジュールを含むハードウェアトークンを使って申請者に交付される。

本認証局はオブジェクト登録者証明書の鍵ペアの作成を行わないため、本項の規定を行わない。

6.1.3. 証明書発行者に対する公開鍵の交付

オブジェクト登録者証明書の公開鍵の本認証局への送付は、暗号化された通信下で、PKCS#10 形式のファイルの本認証局へ送付することで行われる。

6.1.4. 検証者に対する認証局の公開鍵の交付

本認証局の証明書の配布は、次の 2 つの方法のうち EE に応じてどちらかより適切な方法を使用して行う。

- JPNIC 認証局の Web ページにて本認証局の証明書を公開する。本認証局の証明書の公開には暗号機能を持つセキュアなプロトコルを使用し、改ざん防止措置をとる。証明書検証者は同ページより本認証局の証明書をダウンロードして使用することとする。証明書検証者はダウンロードした本認証局の証明書のフィンガープリントとインターネッ

トを使わない方法で公開されているフィンガープリントを比較し、一致していることを確認する。

- オブジェクト登録者にはメンテナ-管理者が本認証局の証明書を渡すものとする。

6.1.5. 鍵サイズ

本認証局は 2048 ビットの RSA 鍵ペアを使用する。EE については、1024 ビット以上の RSA 鍵ペアを使用することを義務とする。

6.1.6. 公開鍵のパラメータの生成及び品質検査

本認証局の鍵ペアを生成するための公開鍵パラメータは、鍵ペア生成に使用される安全性の高い暗号化モジュールを含むソフトウェアに実装された乱数生成モジュール（以下、RNG という）を用いて生成される。

公開鍵パラメータの品質検査については、特に規定しない。

6.1.7. 鍵用途の目的

本認証局の証明書の keyUsage は keyCertSign、cRLSign のビットを使用する。本認証局の私有鍵は EE 証明書及び CRL の発行にのみ使用する。

メンテナ-管理者証明書、オブジェクト登録者証明書、JPNIC 職員向け証明書の keyUsage は digitalSignature、keyEncipherment、dataencipherment のビットを使用する。S/MIME、SSL/TLS のクライアント証明書としてのみ使用するものとする。

6.2. 私有鍵の保護及び暗号モジュール技術の管理

6.2.1. 暗号モジュールの標準及び管理

規定しない。

6.2.2. 私有鍵の複数人管理

本認証局の私有鍵の管理は、複数の CAO に権限を付与することによって行う。2名以上の CAO が揃わなければ本認証局の私有鍵を操作することはできない。

6.2.3. 私有鍵のエスクロー

本 CPS「4.1.2.キーエスクローと鍵回復」に規定する。

6.2.4. 私有鍵のバックアップ

本認証局の私有鍵は、予め定める外部記憶媒体にバックアップされる。バックアップ作成時も鍵管理者の立会いと複数名の CAO を必要とする。

本認証局は、そのバックアップを予め定める保管場所に保管する。

なお、本認証局は、EE の私有鍵のバックアップを行わない。

6.2.5. 私有鍵のアーカイブ

本認証局の私有鍵のアーカイブは行わない。

EE の私有鍵についても同様にアーカイブは行わない。

6.2.6. 私有鍵の暗号モジュールへの又は暗号モジュールからの転送

本認証局の私有鍵は、安全性の高い暗号化モジュールを含むソフトウェアで生成され、他のハードウェア及びソフトウェア等が介入することはない。

6.2.7. 暗号モジュールへの私有鍵の格納

本認証局の私有鍵は、安全性の高い暗号化モジュール内で生成、格納される。

オブジェクト登録者の私有鍵はオブジェクト登録者自身が私有鍵の生成を行い、オブジェクト登録者自身で格納を行う。メンテナ－管理者及び JPNIC 職員向けの秘密鍵は JPNIC において、安全性の高い暗号化モジュール内で生成、格納される。ただし、サーバにおいてはサーバ証明書の管理者が格納を行う。

6.2.8. 私有鍵の活性化方法

本認証局の私有鍵の活性化は、認証設備室内において行われる。

EE の私有鍵に関しては、規定しない。

6.2.9. 私有鍵の非活性化方法

本認証局の私有鍵の非活性化は、認証設備室内において、操作をする者とその監視をする者とに分かれて行われる。

EE の私有鍵に関しては、規定しない。

6.2.10. 私有鍵の破棄方法

本認証局の私有鍵を破棄しなければならない状況の場合は、鍵管理者によって、私有鍵の格納されたハードディスクを完全に初期化又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続によって破棄する。

EE の私有鍵は、EE 自身で確実に破棄するものとする。メンテナ－管理者の秘密鍵は基本的に JPNIC において破棄するものとする。ただし、紛失等の場合はこの限りではない。

6.2.11. 暗号モジュールの評価

規定しない。

6.3. その他の鍵ペア管理

6.3.1. 公開鍵のアーカイブ

本認証局は、本認証局の証明書及び本認証局によって発行される全ての証明書のバックアップを行う。

6.3.2. 証明書の運用上の期間及び鍵ペアの使用期間

本認証局の証明書の有効期間は 10 年、私有鍵の有効期間は 8 年とする。本認証局は私有鍵の有効期限前に鍵ペアの更新を行う。

EE 証明書の有効期間は 2 年とする。私有鍵は復号を行う場合においてのみ、2 年を超える使用を認めるものとする。

6.4. 活性化データ

6.4.1. 活性化データの生成及び設定

本認証局の私有鍵に対するものを含め、本認証局で使用される PIN やパスワードは、英大文字、英小文字、数字を全て含む 8 文字以上の長さのものとする。

6.4.2. 活性化データの保護

本認証局で使用される PIN やパスワードについては、封印されたうえで運用管理者による管理のもと保管される。

6.4.3. 活性化データの他の考慮点

規定しない。

6.5. コンピュータのセキュリティ管理

6.5.1. 特定のコンピュータのセキュリティに関する技術的要件

本認証局のサーバシステムに関わる業務は、原則として複数人の CAO によって行われる。ただし、ハードウェア障害時等に発生する専門的な知識を必要とする作業については、CAO の立会いのもとで保守員によって行うものとする。システムに対して行われた重要な操作については、全てログが残るよう設定する。システムにアクセスするための全てのパスワードについては、適切な管理を行う。本認証局のサーバシステムについては、常時リソース監視を行い、システムの異常や不正運用を検知した場合には、速やかに適切な対策を実施する。

6.5.2. コンピュータセキュリティ評価

本認証局は使用する全てのソフトウェア、ハードウェアに対して事前に運用テストを行い、信頼性の確認を行う。

6.6. ライフサイクルの技術上の管理

6.6.1. システム開発管理

システムの品質及びセキュリティを保つために、開発時における各工程の管理、導入前の評価等を実施する。

6.6.2. セキュリティ運用管理

システムのセキュリティ管理として、入退室管理、教育を含む要員管理、権限管理等の運用管理の実施、不正侵入対策、ウイルス対策等の体系的なセキュリティ対策、セキュリティ対策ソフトウェアの適時更新等を実施する。

6.6.3. ライフサイクルのセキュリティ管理

規定された管理方法により、システムが管理されているかの評価を行う。

本認証局のシステムに対して、セキュリティに関する情報収集を行い、最新の動向を考慮し、適切な評価及び改善を行う。

6.7. ネットワークセキュリティ管理

本認証局の存在するネットワークにはファイアウォールを使用し、ファイアウォール外からのアクセスについては必要最低限のプロトコルに制限する。またアクセス可能なホストも限定する。

6.8. タイムスタンプ

タイムスタンプの使用に関する要件は、本 CPS「5.5.5.記録にタイムスタンプを付ける要件」に規定する。

7. 証明書と、証明書失効リスト及び OCSP のプロファイル

7.1. 証明書のプロファイル

本認証局が発行する証明書は、X.509 証明書フォーマットのバージョン 3 に従う。証明書プロファイルは、表 7-1 のとおりである。

7.1.1. バージョン番号

本認証局が発行する証明書は全て X.509 バージョン 3 証明書フォーマットに従う。

7.1.2. 証明書拡張

本認証局が発行する証明書に使用される拡張領域は表 7-3 のとおりである。

7.1.3. アルゴリズム OID

本認証局が発行する証明書において使用されるアルゴリズム OID は次の 2 つである。

- sha1withRSAEncryption (1.2.840.113549.1.1.5)
- rsaEncryption (1.2.840.113549.1.1.1)

7.1.4. 名前形式

本 CPS 「3.1.1.名前の種類」に従う。

7.1.5. 名前制約

本認証局は、発行する全ての証明書において nameConstraints 拡張を使用しない。

7.1.6. 証明書ポリシー OID

オブジェクト登録者証明書、メンテナー管理者証明書、JPNIC 職員向け証明書のいずれも本 CPS 「1.2.文書の名前と識別」に定める EE 証明書ポリシーの OID を使用する。

7.1.7. ポリシ制約拡張

本認証局は、発行する全ての証明書において policyConstraints 拡張を使用しない。

7.1.8. ポリシ修飾子の記述と意味

オブジェクト登録者証明書、サーバ証明書共にポリシ修飾子の値として本 CPS が公開されている URI を使用する。

7.1.9. critical な証明書 certificatePolicies 拡張の処理

本認証局が発行する証明書に含まれる certificatePolicies 拡張は全て non-critical であり、本項の規定を行わない。

表 7-1 JPIRR 認証局が発行する証明書プロファイル (基本領域)

領域名	設定値	備考
version (バージョン番号)	v3	X.509 証明書バージョン 3 を示す。
serialNumber (シリアル番号)		CA システムにより自動生成
signature (署名アルゴリズム)	SHA1withRSA	
issuer (発行者)	C	JP
	O	Japan Network Information Center
	OU	JPIRR Certification Authority 01
Validity (有効期間)		2年 + 30日
notBefore (開始日)	YYYYMMDDHHMMSS	
notAfter (終了日)	YYYYMMDDHHMMSS	

領域名	設定値	備考
subject (主体者)	【表 7-2 に記載する】	
subjectPublicKeyInfo (主体者公開鍵情報)		
algorithm (アルゴリズム識別子)	1.2.840.113549.1.1.1	RSA 1024bit
subjectPublicKey (主体者公開鍵)		CA システムにより自動生成

JPIRR クライアント証明書を付与される利用者ごとの subject (主体者) 属性に設定される値について、下表に記載する。

表 7-2 JPIRR クライアント証明書の利用者ごとの主体者情報

DN	利用者			
	JPNIC 担当者		JPIRR 証明書 管理者	オブジェクト登録 者
	S/MIME I/F			
C	“ JP ”			
O	“ Japan Network Information Center ”		“ Resource Holder ”	
O			“ ASN Holder ”	
OU	“ Internet Resource Service ”		“ IRR Maintainer Administrator ”	“ IRR Object Registrant ”
OU	“ Secretariat ”		(付与された利用者の 管理対象のメンテ ナー名)	(付与された利用 者の管理対象のメ ンテナ名)
OU	“ IRR Administrator ”			
CN	以下の各項目を 半角スペースで 区切り、併記。 “ IRR-AD ” [64文字以内 の任意の名 称] シーケンス 番号… お	“ JPIRR Secure MIME Gateway ”	以下の各項目を半角 スペースで区切り、併 記。 “ IRR-MA ” メンテナーオブ ジェクトの admin-c 項目 シーケンス番 号… および	以下の各項目を半 角スペースで区切 り、併記。 “ IRR-OR ” メンテナーオブ ジェクトの tech-c 項目 シーケンス番 号… 及び の

DN	利用者			
	JPNIC 担当者		JPIRR 証明書 管理者	オブジェクト登録 者
	S/MIME I/F			
	よび の組合 せで同一の利 用者内で、証 明書発行回数 のシーケン ス。新規発行 時は“01”。		の組合せ(同一の 利用者)で、証明 書発行回数のシー ケンス。新規発行 時は“01”。	組合せ(同一の利 用者)で、証明書 発行回数のシー ケンス。新規発行 時は“01”。

利用者は、subject (主体者) 属性に設定された DN のうち、CN により一意に識別される。また CN 内にシーケンス番号を付加することで、利用者ごとに発行した JPIRR クライアント証明書を一意に特定できる。なお実際に使用する利用者が同一の利用者であっても、JPIRR クライアント証明書に記載された CN 情報のうちシーケンス番号を除く項目に変更があった場合、シーケンス番号は“01”が設定される(新規発行と同様の扱いとなる)。

表 7-3 JPIRR クライアント証明書 詳細プロフィール(拡張領域)

領域名	クリティカル フラグ	設定値	備考
authorityKeyIdentifier (認証局鍵識別子)	Non		JPIRR 認証局証明書の公開鍵のハッシュ値
subjectKeyIdentifier (主体者鍵識別子)	Non		本 JPIRR クライアント証明書の公開鍵のハッシュ値
keyUsage (鍵使用法)	Critical	digitalSignature(デジタル署名の検証) keyEncipherment(鍵の暗号化)	
extendedKeyUsage (拡張鍵使用法)	Non	1.3.6.1.5.5.7.3.2 : SSL/TLS クライアント認証 1.3.6.1.5.5.7.3.4 : 電子メール の保護	
certificatePolicies (証明書ポリシー)	Non	[1]Certificate Policy: Policy Identifier=1.2.392.200175.1.2.	

領域名	クティカ フラグ	設定値	備考
		2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://jpnica.nic.ad.jp/capub/ jprr/jprr-ca_cps.html	
subjectAltName (主体者別名)	Non	[rfc822name]	利用者の電子メール アドレス
basicConstraints (基本制約)	Non		
Subject Type		End Entity	
Path Length Constraints		None	
cRLDistributionPoints (CRL 配付点)	Non	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://jpnica.nic.ad.jp/capub/ jprr/jprr-ca.crl	

7.2. 証明書失効リストのプロファイル

本認証局が発行する CRL は、X.509CRL フォーマットのバージョン 2 に従う。CRL プロファイルは、表 7-4 のとおりである。

7.2.1. バージョン番号

本認証局が発行する CRL は全て X.509 バージョン 2CRL フォーマットに従う。

7.2.2. CRL 及び CRL エントリ拡張

本認証局は次の 2 つの CRL 拡張を使用し、CRL エントリ拡張は使用しない。

7.2.2.1. cRLNumber

本認証局が発行する CRL において一意となる非負の整数を使用する。

7.2.2.2. authorityKeyIdentifier

keyIdentifier の値として本認証局の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

表 7-4 JPIRR 認証局が発行する CRL プロファイル

領域名	設定値	備考
version (バージョン番号)	v2	バージョン 2 を示す。
signature (署名アルゴリズム)	SHA1withRSA	
subject (主体者)	C	JP
	O	Japan Network Information Center
	OU	JPIRR Certification Authority 01

thisUpdate (今回の更新日時)	YYYYMMDDHHMMSS	CRL が発行されたシステム時刻
nextUpdate (次回の更新日時)	YYYYMMDDHHMMSS	thisUpdate より 15 日後の日時
revokedCertificates (失効された JPIRR 証明書のリスト)		
userCertificate (失効した利用者証明書)		失効した証明書の シリアル番号
revocationDate (失効日時)	YYYYMMDDHHMMSS	失効処理が実施された日時

crlExtensions (CRL 拡張領域)			
領域名	クリティカル フラグ	設定値	備考
authorityKeyIdentifier (認証局鍵識別子)	Non		JPIRR 認証局証明書の公開鍵のハッシュ値
cRLNumber	Non		CA システムにより自動生成

7.3. OCSP プロファイル

7.3.1. バージョン情報

使用しない。

7.3.2. OCSP 拡張

使用しない。

8. 準拠性監査とその他の評価

8.1. 評価の頻度又は評価が行われる場合

本認証局は必要に応じて監査を実施する。

8.2. 評価人の身元又は資格

JPNIC は、認証局の準拠性監査を、担当理事が選定する認証業務に精通した監査者により実施する。

8.3. 評価人と評価されるエンティティとの関係

JPNIC は、本認証局の認証業務に関わる要員以外から監査者を選定する。

8.4. 評価で扱われる事項

本認証局の準拠性監査は、認証局の運営が本 CPS 及び関連する規定を遵守して運営されているかを監査するものである。

また、担当理事が必要と認めた場合、担当理事が指定する監査目的による監査を実施する。

なお、JPNIC はローカル RA の監査を行う権利を有する。

8.5. 不備の結果としてとられる処置

本認証局は、監査報告書で指摘された事項に対して、担当理事がその対応を決定する。担当理事は、指摘事項に関して、セキュリティ技術の最新動向も踏まえ、問題が解決されるまでの対応策も含め、その措置を JPNIC 認証局の運営責任者に指示する。講じられた対応策は、担当理事に報告され、評価されるとともに、次の監査において確認される。監査において発見された不備等の指摘事項への対応をしない場合は、担当理事によって予め定められた罰則が課される。

8.6. 評価結果の情報交換

監査結果の報告は監査者から担当理事に対して行われる。本認証局は、法律に基づく開示要求があった場合以外は、監査結果を外部へ開示しない。

なお、監査報告書については、JPNIC 認証局運営責任者が最低 5 年間保管管理するものとする。

9. 他の業務上の問題及び法的問題

9.1. 料金

本認証局が発行する証明書に関わる発行料金、更新料金、利用料金等は、別途定めるものとし、事前に関係者に周知する。

9.2. 財務的責任

規定しない。

9.3. 情報の秘密性

9.3.1. 秘密情報の範囲

本認証局が保持する情報は、本 CPS 「2.2.証明情報の公開」で公表すると定めた情報、本 CPS の一部として明示的に公表された情報、Web ページで公表している情報、証明書の失効理由及び失効に関するその他の詳細情報を除き、秘密扱いとする。

証明書所有者の私有鍵は、その証明書所有者によって秘密扱いとされる情報とする。

9.3.2. 秘密情報の範囲外の情報

本 CPS で公表すると定めた情報、本 CPS の一部として明示的に公表された情報、Web ページ等で公表している情報、証明書の発行者である認証局情報と失効日時を含む CRL は秘密扱いとしない。その他、次の状況におかれた情報は秘密扱いとしない。

- JPNIC の過失によらず知られるようになった情報
- JPNIC 以外の出所から、機密保持の制限なしに JPNIC に知られるようになった情報
- JPNIC によって独自に開発された情報
- 開示対象の情報に関連する人又は組織により承認を得ている情報

9.3.3. 秘密情報を保護する責任

本認証局で取扱う情報に関して、捜査機関、裁判所その他法的権限に基づいて情報を開示するように請求があった場合、JPNIC は法の定めに従って法執行機関へ情報を開示することができる。また、本認証局で取扱う情報に関して、調停、訴訟、仲裁、

その他の法的、裁判上又は行政手続の過程において、裁判所、弁護士、その他の法律上の権限を有する者から任意の開示要求があった場合、当該要求情報に関し開示することができる。更に、本認証局では、メンテナ－管理者から、メンテナ－管理者の管理する証明書所有者に関連する情報について、権利、利益を侵害又は侵害するおそれがあるとの申出を受けた場合、メンテナ－管理者の本人確認及び開示要求の対象情報との関連を確認のうえ、メンテナ－管理者から受領した証明書所有者に関する情報及び証明書記載情報を開示することができる。

JPNIC 認証局は、業務の一部を委託する場合、秘密情報を委託先に開示することがある。ただし、その委託契約においては秘密情報の守秘義務を規定する。

JPNIC 認証局は、前述の場合を除いて秘密情報を開示しない。秘密情報が漏えいした場合、その責任は漏えいした者が負う。

なお、個人情報の保護に関する取扱いは、本 CPS「9.4.個人情報のプライバシー保護」に定める。

9.4. 個人情報のプライバシー保護

9.4.1. プライバシポリシー

本認証局は個人情報保護の重要性を認識し、個人情報を本 CPS「9.3.3.秘密情報を保護する責任」と同様に取扱うことに加え、次のポリシーを遵守する。

- (1) 管理責任者をおき、個人情報の適切な管理を行う。
- (2) 個人情報を収集する場合、収集目的を知らせたうえで、必要な範囲の情報のみを適法かつ公正な手段で収集する。
- (3) 証明書所有者から提出を受けた個人情報は、次の目的にのみ使用する。
 - IP アドレス管理業務の潤滑な運用を行うため
 - 証明書における、認証サービス上の責任を果たすため
 - その他認証業務に関連した目的のため
- (4) 証明書所有者の同意がある場合及び法令に基づく場合を除き、個人情報を業務委託先以外の第三者に開示することはしない。業務委託先に開示する場合は、当該業務委託先に対し本書と同等の条件を義務付けるものとする。
- (5) 個人情報の管理責任者は、適切な安全対策を講じて、個人情報を不正アクセス、紛失、破壊、改ざん及び漏えい等から保護するよう努める。
- (6) 証明書所有者自身の個人情報について開示を求められた場合、第三者への個人情報の漏えいを防止するため、証明書所有者自身であることが JPNIC 認証局において確認できた場合に限り、JPNIC 認証局において保管している証明書所有者の個人情報を本人に開示する。また、証明書所有者の個人情報に誤りや変更がある場合には、証明書所有者からの申出に基づき、合理的な範囲で速やかに、不正確な情報又は古い情報を修正又は削除する。証明書所有者は JPNIC 認証局に開示を求める場合、JPNIC 認証局により定められた方法により申請を行うものとする。
- (7) JPNIC 認証局は、認証業務に従事する職員に対して個人情報保護の教育活動を実施する。
- (8) 証明書所有者の個人情報に関して適用される法令、規範を遵守するとともに、適切な個人情報保護を維持するために、個人情報保護方針を適宜見直し、改善を行う。

9.4.2. プライバシとして扱われる情報

規定しない。

9.4.3. プライバシとはみなされない情報

規定しない。

9.4.4. 個人情報を保護する責任

JPNIC 認証局は、本 CPS「9.4.1.プライバシポリシー」に則って個人情報を保護する責任を負う。

9.4.5. 個人情報の使用に関する個人への通知及び承諾

規定しない。

9.4.6. 司法手続又は行政手続に基づく公開

規定しない。

9.4.7. 他の情報公開の場合

規定しない。

9.5. 知的財産権

別段の合意がなされない限り、知的財産権の扱いは次に従うものとする。

- JPNIC 認証局の発行した証明書、CRL は JPNIC に帰属する財産とする
- 本 CPS は JPNIC に帰属する財産とする
- JPNIC 認証局の私有鍵及び公開鍵は JPNIC に帰属する財産とする
- JPNIC 認証局から貸与されたソフトウェア、ハードウェア、その他文書、情報等は JPNIC に帰属する財産とする

9.6. 表明保証

9.6.1. 発行局の表明保証

JPNIC 発行局は、JPNIC 発行局の業務を遂行するにあたり次の義務を負う。

- JPNIC 発行局の証明書署名鍵のセキュアな生成・管理
- JPNIC 登録局からの申請に基づいた証明書の正確な発行・失効管理
- JPNIC 発行局のシステム稼働の監視・運用
- CRL の発行・公表
- リポジトリの維持管理
- 本 CPS に従った受付時間内の問合せ受付

9.6.2. 登録局の表明保証

JPNIC 登録局は、JPNIC 登録局の業務を遂行するにあたり次の義務を負う。

- 登録端末のセキュアな環境への設置・運用
- 証明書発行・失効申請における JPNIC 発行局への正確な情報伝達
- 証明書失効申請における JPNIC 発行局への運用時間中の速やかな情報伝達

9.6.3. ローカル登録局の表明保証

ローカル RA は、ローカル RA 業務を遂行するにあたり次の義務を負う。

- 証明書所有者と証明書申請者が同一であることの検証
- JPNIC 登録局への正確な申請情報の伝達
- 証明書使用におけるオブジェクト登録者の教育
- 正当な証明書申請者への確実な証明書配布
- 証明書失効の妥当性の確認
- その他、JPNIC との契約に準拠した運用の厳守

9.6.4. 所有者の表明保証

証明書所有者は、証明書所有にあたり次の義務を負う。

- 本 CPS 及び本認証局が提示するその他の文書（証明書所有者同意書）の理解と承諾
- 本 CPS 「4.5.1.所有者の私有鍵及び証明書の使用」に規定する義務

9.6.5. 検証者の表明保証

証明書検証者は、本 CPS「4.5.2.検証者の公開鍵及び証明書の使用」に規定する義務を負う。

9.6.6. 他の関係者の表明保証

規定しない。

9.7. 保証の制限

JPNIC は、本 CPS「9.6.1.発行局の表明保証」かつ「9.6.2.登録局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害、派生的損害に対する責任を負わない。

9.8. 責任の制限

本 CPS「9.6.1.発行局の表明保証」かつ「9.6.2.登録局の表明保証」の内容に関し、次の場合には JPNIC は責任を負わないものとする。

- JPNIC に起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- ローカル RA 又は証明書所有者が自己の義務の履行を怠ったために生じた損害
- ローカル RA 又は証明書所有者の端末のソフトウェアの瑕疵、不具合その他の動作自体によって生じた損害
- JPNIC の責に帰することのできない事由で証明書及び CRL に公開された情報に起因する損害
- JPNIC の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
- 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、認証局業務の停止に起因する一切の損害
- 証明書発行申請における本人認証手続等のローカル RA が行った業務に起因する損害

9.9. 補償

本認証局が発行する証明書を申請、受領、信賴した時点で、証明書所有者及び証明書検証者には、JPNIC に対する損害賠償責任及び保護責任が発生する。当該責任の対象となる事象には、各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行のうち、証明書申請時に証明書申請者が本認証局に最新かつ正確な情報を提供しなかったことに起因するもの又は各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるような証明書所有者及び証明書検証者の行為、怠慢な行為、各種行為、履行遅滞、不履行等が含まれる。

9.10. 有効期間と終了

9.10.1. 有効期間

本 CPS、契約書及び協定等の文書は、正当な承認手続にて発行されてから正当な承認手続にて改訂されるまで有効とする。

9.10.2. 終了

本 CPS、契約書、協定等の文書全部又は一部、若しくは特定の関係者に対して規定されている条項が無効になった場合、その該当部分は終了とする。

9.10.3. 終了の効果と効果継続

本認証局は、本 CPS、契約書、協定等に変更又は終了が発生する場合においても、合意事項に責任を持ち続けることに最善を尽くすものとする。

9.11. 関係者間の個別通知と連絡

規定しない。

9.12. 改訂

9.12.1. 改訂手続

本認証局は、証明書ポリシー及びその保証、義務に著しい影響を与えない範囲での本 CPS 変更の必要性が生じた場合、証明書所有者又は証明書検証者に事前の承諾なしに、随時、本 CPS を変更することができる。なお、改訂の通知から改訂が有効になるまでの期間に改訂に対する異議の申出がない場合は、改訂に対する合意が得られたものとする。改訂に対し合意できない関係者においては、即時に本認証局から発行された証明書の使用を中止するものとする。

9.12.2. 通知方法及び期間

本認証局は、変更された CPS をその改訂が有効になる 10 営業日前までに、変更履歴とともにリポジトリに公開することにより、証明書所有者及び関係者に改訂の通知

を行うものとする。

9.12.3. オブジェクト識別子を変更されなければならない場合

規定しない。

9.13. 紛争解決手続

本認証局が発行する証明書に関わる紛争について、JPNIC に対して、訴訟、仲裁等を含む法的解決手段に訴えようとする場合は、JPNIC に対して事前にその旨を通知するものとする。仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とすることに、全ての当事者は合意するものとする。また、本 CPS、契約書にて定められていない事項やこれらの文書の解釈に関し疑義が生じた場合は、各当事者はその課題を解決するために誠意を持って協議するものとする。

9.14. 準拠法

本認証局、証明書所有者及び証明書検証者の所在地に関わらず、本 CPS の解釈、有効性及び本認証局の証明書発行に関わる紛争については、日本国の法令が適用される。

9.15. 適用法の遵守

本認証局は、国内における各種輸出規制を遵守し、暗号ハードウェア及びソフトウェアを取り扱うものとする。

9.16. 雑則

9.16.1. 完全合意条項

本 CPS、契約書又は協定等における合意事項は、これらが改訂又は終了されない限り他の全ての合意事項より優先される。

9.16.2. 権利譲渡条項

規定しない。

9.16.3. 分離条項

本 CPS、証明書所有者同意書及び本認証局より示す協定等において、その一部の条項が無効であったとしても、当該文書に記述された他の条項は有効に存続するものとする。

9.16.4. 強制執行条項

規定しない。

9.17. その他の条項

規定しない。

Appendix 3
JPIRR 認証局 認証業務規程
第 1 版 英語訳

<Appendix3 について>

- この資料は、JPIRR 認証局証明書の利用規約を英訳したものである。
 - 諸外国の技術者による内容の理解を図るために翻訳されたものである。
正確な内容確認には原文を参照する必要がある。

JPIRR Certification Authority (Certification Practice Statement)

Version 1.0

Japan Network Information Center

CONTENTS

1. Introduction	1
1.1. Overview	1
1.2. Documentation Name and Identification.....	2
1.3. Individuals and Entities related to the PKI	3
1.4. Certificate Usage Methods	6
1.5. Policy Management.....	7
1.6. Definitions and Abbreviations	8
2. Disclosure and Repository Liability.....	10
2.1. Repository	10
2.2. Certification Information Disclosure	10
2.3. Disclosure Timing and Frequency.....	10
2.4. Repository Access Management	11
3. Identification and Authentication.....	12
3.1. Name Determination	12
3.2. Initial Authentication of Individual or Entity	13
3.3. Identification and Authentication of Individual or Entity when Applying for Key Update	15
3.4. Identification and Authentication of Individual or Entity during Certificate Revocation Application.....	15
4. Operational Requirements concerning Certificate Lifecycle.....	16
4.1. Certificate Application	16
4.2. Certificate Application Procedures.....	17
4.3. Certificate Issue	19
4.4. Certificate Receipt Confirmation	20
4.5. Utilization of Key Pairs and Certificates.....	21
4.6. Certificate Updating	22
4.7. Certificate Key Updating.....	23
4.8. Certificate Revision.....	24
4.9. Certificate Revocation and Temporary Suspension.....	25
4.10. Certificate Status Confirmation Service	29
4.11. Registration Completion.....	29
4.12. Key Escrow and Key Recovery	29
5. Facility, Management, and Operational Controls.....	30
5.1. Physical Controls.....	30
5.2. Procedural Controls	32
5.3. Personnel Controls	33
5.4. Audit Log Procedures.....	35
5.5. Record Storage	37
5.6. Key Switching.....	39
5.7. Recovery from Key Compromise and Disasters.....	40

5.8. Termination of Certification Authority or Registration Authority Practices.....	41
6. Technical Security Management.....	42
6.1. Key Pair Generation and Installation.....	42
6.2. Private Key Protection and Cryptographic Module Technical Administration	44
6.3. Other Key Pair Administration	46
6.4. Activated Data.....	47
6.6. Administration of Life Cycle Technology	48
6.7. Network Security Management	48
6.8. Time-stamps	48
7. Profiles of Certificates, Certificate Revocation Lists, and OCSP Profiles	49
7.1. Certificate Profile	49
7.2. Profile of Certificate Revocation List	52
7.3. OCSP Profile.....	54
8. Compliance Audit and Other Assessments	55
8.1. Assessment Frequency and Circumstances requiring Assessment.....	55
8.2. Identity and Qualifications of Assessor	55
8.3. Relationship between the Assessor and the Entity Assessed	55
8.4. Items covered by the Assessment.....	55
8.5. Measures taken in Event of Unsatisfactory Results	55
8.6. Assessment Result Information Exchange	56
9. Problems relating to Other Practices and Legal Problems	57
9.1. Fees	57
9.2. Financial Liability.....	57
9.3. Information Confidentiality.....	57
9.4. Protection of Personal Data Privacy	59
9.5. Intellectual Property Rights	61
9.6. Representation Warranties.....	62
9.7. Limitations of Warranty	63
9.8. Limitations of Liability	64
9.9. Indemnity	65
9.10. Periods of Validity and Termination	65
9.11. Individual Notification and Contact between Related Persons.....	66
9.12. Amendments	66
9.13. Dispute Resolution Procedures	66
9.14. Governing Law.....	67
9.15. Compliance with Applicable Laws	67
9.16. Miscellaneous Regulations	67
9.17. Other Provisions	67

1. Introduction

1.1. Overview

This JPIRR Certification Authority Certification Practice Statement (henceforth known as the CPS) defines the operation regulations of the certification practices of the JPIRR Certification Authority (henceforth known as the Certification Authority) which provides electronic certification procedures in various administrative practices of the routing information database (IRR (abbreviation of Internet Routing Registry)) operated by the Japan Network Information Center (henceforth known as JPNIC).

Based on this CPS, the Certification Authority provides certification services, such as issuing certificates to persons conducting the various application processing practices. The Certification Authority is operated on an experimental basis.

The structure of this CPS conforms to the RFC3647 Certificate Policy and Certification Practices Statement Framework standardized by the IETF PKIX WG.

The Certification Authority does not determine each of the CP (Certificate Policy) and the CPS (Certification Practices Statement) as independent items; rather it stipulates the certificate policy and operations statement as this CPS.

Concerning the provision of the certification practice, JPNIC comprehensively determines its own policies and the obligations of certificate subjects and relying parties in this CPS and the certificate subject agreement. Note that if there is variance between the content of this CPS and the certificate subject agreement, the certificate subject agreement shall be given priority in application.

This CPS is disclosed on the JPNIC Website at <http://jpnica.nic.ad.jp/> in order that it may be viewed at any time by certificate subjects and relying parties.

(1) CPS

The CPS is a document that describes the certificate purpose, applicable range, certificate profile, user authentication method and the certificate subject key administration, together with the general regulations relating to certification practices. This CPS refers whenever necessary to the certificate subject agreement.

(2) Certificate Subject Agreement

The certificate subject agreement is a document that describes the various regulations for use of the certification service between the certificate subject and JPNIC, including details of the certification service and obligations of the certificate subject.

1.2. Documentation Name and Identification

The official name of this CPS is the “JPNIC Certification Authority Certification Practice Statement”.

The object identifiers relating to JPNIC and the Certification Authority are shown in Table 1.1.

Table 1-1. Object Identifiers relating to JPNIC and the JPNIC Resource Service Certification Authority

Object	Object Identifier
Japan Network Information Center	1.2.392.200175
JPIRR Certification Authority Certification Practice Statement	1.2.392.200175.1.2.2
End-entity Certification Policy	1.2.392.200175.1.2.2

1.3. Individuals and Entities related to the PKI

1.3.1. Certification Authority, Registration Authority, Certificate Subjects, and Relying Parties

The community of individuals or entities related to the PKI to whom the Certification Authority distributes certificates includes the participants shown in Table 1-2.

Table 1-2 Participants and Roles relating to the Community

Participant	Abbreviated Name	Role and Explanation
Server		JPNIC server utilized in the certification practices.
Resource Subscriber		Individuals and entities conducting permission list registration practices.
Object Registrant		Individuals and entities conducting object registration practices to JPIRR.
Object Registrant Certificate		Certificate issued to object registrants
Maintainer Administrator		Individuals or entities conducting object registrant appointment, removal, and custody.
Maintainer Administrator Certificate		One of the operations certificates required for the Certification Authority certification practices. It is the certificate required for certification of maintainer administrators when issuing certificates to object registrants. Concerning the handling of this certificate, management and operations are carried out while strictly following the operation regulations.
JPNIC Employee Certificate		One of the operations certificates required for the Certification Authority certification practices. It is the certificate issued for JPNIC employees conducting practices such as the management of maintainer administrator identifiers in the IP registry system.
End-entity	EE	General name for subjects of certificate issuing, such as object registrants, maintainer administrators, and JPNIC employees.
End-entity Certificate	EE Certificate	General name for certificates issued to end-entities.

Participant	Abbreviated Name	Role and Explanation
Certificate Subject	Subject	Signifies individuals or entities that have carried out certificate issue application, generated their own key, and have had certificates issued by the Certification Authority. In this CPS, this means individuals or entities that are EE certificate subjects, or server administrators.
Relying Party	RP	Individuals or entities that receive certificates, and who use these certificates for verification, carrying out their actions based on the certificate and/or a digital signature.
JPNIC Issuing Authority	JPNIC IA	General name for the Issuing Authority inside the JPNIC Root Certification Authority and the Issuing Authority inside the JPNIC Resource Service Certification Authority. It is the organization that administers the certificate issuing practices in the JPNIC Root Certification Authority and the JPNIC Resource Service Certification Authority. It issues certification that has been requested from the RA. It is used inside the Certification Authority (CA) in the situation where the certification administration functions, including certificate issuing and revocation, are to be shown.
JPNIC Registration Authority	JPNIC RA	Organization that confirms that the subscriber for the certificate issue is the correct individual or entity, and mainly administers registration and revocation practices. Takes responsibility for confirming and authenticating the certificate subject.
Trustee in Charge		This is the trustee in charge of JPNIC security operations, who determines the JPNIC Certification Authority operations policy.
CA (Certification Authority) Operator	CAO	Individual or entity that operates and administers the Certification Authority system, including the CA Server and Directory Server.
RA (Registration Authority) Operator	RAO	Individual or entity that manages and operates the Registration Authority (RA). Carries out registration work for certificate issuing and revocation.

Participant	Abbreviated Name	Role and Explanation
Repository		Database where certificates signed by the Certification Authority and CRLs are stored and disclosed.
JPNIC Root Certification Authority		This is the Root Certification Authority of all the Certification Authorities operated by JPNIC. It is positioned at the top of the certification hierarchy route in JPNIC, and carries out self-signing as well as the electronic signing of certificates for subordinate downstream Certification Authorities (Resource Service Certification Authority).
JPIRR Certification Authority		This is the Certification Authority that carries out issuing of certificates relating to IRR administration practices operated by JPNIC. JPIRR Certification Authority certificates are electronically signed by the JPNIC Root Certification Authority.
JPNIC Certification Authorities		General name for the Certification Authorities operated by JPNIC.
Local RA		This is an organization or group different from the organization that issues certificates. In RA practices, the organization carries out identification and judging of the correct individual or entity, certificate issue application processing, and certificate revocation processing. In the case of the JPNIC Certification Authority, the IP Address Management Agents are Local RAs.
Local RA Manager		Manager of Local RA practices in the IP Address Management Agent, who conducts the appointment and removal of maintainer administrators.
Maintainer Administrator		Carries out object registrant member administration and authentication, and object registrant certification issue application operations.

1.3.2. Other Related Individuals or Entities

Not prescribed.

1.4. Certificate Usage Methods

1.4.1. Appropriate Certificate Use

Certificates issued based on this CPS are used by routing information registration approval organizations for verification of users and messages for the purpose of various types of applications and communications in routing information administration practices carried out by JPNIC.

1.4.2. Prohibited Certificate Use

Certificates issued based on this CPS are intended for use in various application processing practices in JPNIC. Although JPNIC does not restrict mutual use of certification between object registrants, it does not accept any liability for use in this way.

1.4.3. Certificate Mutual Operability

The JPNIC Certification Authority may carry out reciprocal certification with another Certification Authority.

1.5. Policy Management

1.5.1. Organization Administering the Documentation, and Contact Details

The organization administering this CPS, and its contact details, are determined as follows:

Japan Network Information Center

Inquiries accepted: Monday to Friday 10:00-18:00 (Excepting year-end, new year and public holidays)

E-mail address: ca-query@nic.ad.jp

1.5.2. Person determining CPS Policy Compatibility

The JPNIC trustee in charge will conduct judgment of whether or not the CPS is compatible with the Certification Authority's operation policy.

1.5.3. CPS Approval Procedures

Revisions to this CPS will be disclosed after approval has been received from the trustee in charge.

1.6. Definitions and Abbreviations

The terms used in this CPS are as shown in Table 1-3.

Table 1-3 Terms Used

Term	Abbreviation	Explanation
Electronic Certificate	Certificate	This is an electronic document which certifies that the content described using a certain public key is held by the sender. The electronic signing of the document by the Certification Authority ensures its correctness. In this CPS, provided there are no special restrictions, the object registrant certificate, server's certificate, and operations certificate are all known under the general name of "certificates".
Certification Authority	CA	This is the organization that carries out certificate issuing, update, and revocation, Certification Authority private key generation and protection, and certificate subscriber registration. In this CPS, in cases where only Certification Authority is mentioned, it includes the certificate issuing practices and the registration practices.
RFC 3647 (Request For Comments 3647)		Support framework for writers of CPS for Certification Authorities and PKI.
Object Identifier	OID	This is an identifier registered in a registration organization (such as ISO or ITU) that will become globally unique. Registered items such as the algorithm used by the PKI, the name stored in the certification (subject), and the type (attributes such as the country name) and other items are used as the object identifier.
X.509		Format of certificates and certificate revocation lists determined by ITU-T. In X.509 v3, extension fields are added for storing optional information.
Public Key		One of the key pairs utilized in the public key encryption method. This is the key that is made public which corresponds to the private key.

Term	Abbreviation	Explanation
Private Key		One of the key pairs utilized in the public key encryption method. This is the key corresponding to the public key which is held only by the individual or entity concerned.
Certificate Signing Request	CSR	This is the data file that forms the basis when issuing a certificate. The CSR includes the public key of the individual or entity requesting the certificate issue, and the certificate is issued with the signature of the issuer to authorize this public key.
Certificate Revocation List CRL		This is the revocation list of EE certificates and operation certificates that have been revoked during the certificate validity period for reasons such as compromise of the Certification Authority private key.
PIN (Personal Identification Number)		Information used for identification of individuals.

2. Disclosure and Repository Liability

2.1. Repository

The Certification Authority strives for maintenance and administration that will allow repository use 24 hours per day, seven days a week. The repository includes a certificate repository and an information disclosure repository. In the situation where it is necessary to suspend the system for system maintenance, notification will be sent to certificate subjects, relying parties and related individuals or entities beforehand, or an announcement will be made on the Website. However, this may not always be possible, such as on the occurrence of unavoidable situations, including natural disasters, incidents, and problems.

2.2. Certification Information Disclosure

The following information is disclosed on the information disclosure repository:

- CPS

Further, the following information is disclosed on the certificate repository.

- EE certificates
- CRL

However, the EE certificates and CRL will only be disclosed to relying parties.

Note that important information relating to the CPS and the Certification Authority is disclosed on the Website with the URI shown below.

<http://jpnica.nic.ad.jp/>

2.3. Disclosure Timing and Frequency

Regarding the information disclosed by the Certification Authority, the disclosure timing and frequency will be as follows:

- For the CPS, disclosure will be made whenever revisions are made.
- For self-signed certificates, linked certificates, and downstream Certification Authority certificates, disclosure will be made whenever issued or updates are made.
- For the CRL, disclosure will be made whenever issued. The frequency of issue will be as stipulated in “4.9.7 Certification Revocation List Issuing Frequency” in this CPS.
- Important information and other information concerning the Certification Authority will be updated as appropriate whenever necessary.
- For EE certificates, disclosure will be made whenever issued or updated.

2.4. Repository Access Management

Concerning the information disclosed by the Certification Authority, with the exception of read-only control, special degrees of access control are not implemented. The relying party for the EE certificates used for verification will be JPNIC. Accordingly, the certificate repository is basically provided to JPNIC.

3. Identification and Authentication

3.1. Name Determination

3.1.1. Types of Names

The certificate issuer name and issue subject name will be configured according to the regulations for the identifying name in the X.500 Series definitions.

3.1.2. Necessity for Names to Incorporate Meanings

It is necessary that names described in the certificate should show the subject individual's name, organization, role name, and equipment name.

3.1.3. Subject Anonymity

In the certificate, as long as the name allows specification of the individual, organization, role, and equipment, it is not necessary to use real names.

3.1.4. Regulations for Interpreting Various Name Formats

The rules for interpreting the various name formats follow the regulations for the identifying name in the X.500 Series definitions.

3.1.5. Uniqueness of Names

The names described in the certificates issued based on the same policy by the Certification Authority will be unique for all EEs. In the situation where an update has been carried out on a certificate for the same EE, there may be duplication of the certificate and name prior to updating.

3.1.6. Trademark Recognition, Authentication and Roles

Not specified.

3.2. Initial Authentication of Individual or Entity

3.2.1. Method used to Prove Possession of Private Key

The Certification Authority confirms that the applicant for the object registrant certificate possesses the private key utilizing a certificate signing request (CSR) that has been digitally signed following PKCS#10 (Public-Key Cryptography Standards #10) or another method determined by the Certification Authority.

Concerning the server's certificates, the Certification Authority uses a method stipulated beforehand to confirm that the certificate subscriber possesses the private key.

3.2.2. Authentication of Organization Identity

The Certification Authority conducts authentication of organizations and groups as Local Registration Authorities. Organizations and groups intending to receive authentication as Local RAs must be IP Agents.

Regarding server's certificates, the Certification Authority confirms that the organization or group conducting the operation and maintenance of the server for which the certificate is to be issued is JPNIC or an organization or group approved by JPNIC.

3.2.3. Authentication of Individuals

When conducting issue registration of applicants for maintainer administrator certificates, JPNIC authenticates the applicants following the prescribed procedures.

When conducting issue registration of applicants for object registrant certificates, maintainer administrators take responsibility for carrying out authentication of applicants following the prescribed procedures.

When conducting issue registration of applicants for JPNIC employee certificates, JPNIC will authenticate the applicants following the prescribed procedures.

Concerning the server's certificates, the Certification Authority will confirm that persons requesting the issuing of certificates are persons who have received permission for certificate issue from JPNIC or an organization or group approved by JPNIC.

3.2.4. Unconfirmed Subject Information

Not specified.

3.2.5. Confirmation of Authority Appropriateness

Regarding the receipt of application registrations for object registrant certificates from maintainer administrators, the Certification Authority will confirm the appropriateness of the maintainer administrator concerned.

3.2.6. Mutual Operation Standards

Not stipulated.

3.3. Identification and Authentication of Individual or Entity when Applying for Key Update

3.3.1. Identification and Authentication of Individual or Entity for Normal Key Updating

Same as procedures defined in “3.2 Initial Authentication of Individual or Entity” in this CPS.

3.3.2. Identification and Authentication of Individual or Entity for Key Updating after Certificate Revocation

Same as procedures defined in “3.2 Initial Authentication of Individual or Entity” in this CPS.

3.4. Identification and Authentication of Individual or Entity during Certificate Revocation Application

After conducting identification of an individual or entity as the revocation applicant for maintainer administrator certificates, JPNIC will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

The maintainer administrator will in principle conduct identification of an individual or entity as the revocation applicant for object registrant certificates, and will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

After conducting identification of an individual or entity as the revocation applicant for JPNIC employee certificates, JPNIC will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

Regarding server’s certificates, the Certification Authority will confirm using a method prescribed beforehand that the individual or entity applying for the certificate revocation has received permission to issue certificates from JPNIC or an organization or group approved by JPNIC.

4. Operational Requirements concerning Certificate Lifecycle

4.1. Certificate Application

4.1.1. Individuals or Entities that can Submit Certificate Applications

Individuals or entities that can apply for maintainer administrator certificates will be individuals or entities corresponding to either of the items (1)-(4) below.

- (1) IP Address Management Agents
- (2) Organizations that have been allocated a Provider Independent Address for special applications
- (3) Organizations or individuals who have been allocated an AS number from JPNIC
- (4) Organizations or individuals who have been allocated a Provider Independent Address with historical circumstances by JPNIC

Individuals or entities that can apply for object registrant certificates will be authenticated maintainer administrators.

Individuals who may apply for JPNIC employee certificates will be persons employed by JPNIC.

Individuals who may submit applications for server's certificates will be JPNIC employees or persons specified by JPNIC.

4.1.2. Registration Procedures and Responsibilities

Applicants for maintainer administrator certificates should apply to JPNIC for issue of the certificate according to the method notified beforehand by JPNIC. According to the content of the application, the maintainer administrator will confirm the role.

Applicants for object registrant certificates should submit the certificate issue application to the maintainer administrator using the method notified beforehand by the maintainer administrator. Further, providing that the certificate applicant has been notified by the Certification Authority of the 2 types of information necessary for key pair generation and certificate issue, the key pairs should be generated and the electronically signed certificate signing request should be sent via secure online communications to the Certification Authority following the certificate signing request data format such as PKCS#10. The electronic signature of the certificate signing request will be verified.

Applicants for server's certificates should conduct certificate issue application using the method prescribed beforehand by the Certification Authority.

Applicants for JPNIC employee certificates should carry out certificate issue application using the method prescribed beforehand by the Certification Authority.

Concerning the application for certificates, the certificate applicant will bear the following responsibilities:

- Acceptance of the contents of this CPS and other documentation disclosed by the Certification Authority.
- Correct production of certificate application content.

4.2. Certificate Application Procedures

4.2.1. Individual or Entity Identification and Authentication Function Implementation

Authentication of an individual or entity as an applicant for maintainer administrator certificates is carried out by the JPNIC Registration Authority administrator.

Authentication of an individual or entity as an applicant for object registrant certificates is carried out by the maintainer administrator. The maintainer administrator implements authentication of correct individual or entity as applicants for object registrant certificates based on “1.1.1 Authentication of Individuals” in this CPS. The maintainer administrator takes responsibility relating to the authentication of an individual or entity as an applicant for object registrant certificates.

Authentication of an individual or entity as an applicant for JPNIC employee certificates is carried out according to the method prescribed in advance by the Certification Authority.

Authentication of an individual or entity as an applicant for server’s certificates is carried out according to the method prescribed in advance by the Certification Authority.

4.2.2. Certificate Application Approval and Rejection

Regarding the applications from applicants for object registrant certificates, the maintainer administrator determines whether the certificate application will be accepted or rejected based on judging standards prescribed beforehand. In the case where the application is accepted, certificate application registration will be carried out for the Certification Authority. The maintainer administrator will take responsibility for the application judging.

Regarding the applications from applicants for maintainer administrator certificates, the JPNIC Registration Authority administrator determines whether the certificate application will be accepted or rejected based on judging standards prescribed beforehand. In the case where the application is accepted, certificate application registration will be carried out for the Certification Authority. The JPNIC Registration Authority administrator will take responsibility for the application judging.

Note that after conducting confirmation of the correct individual or entity as the maintainer administrator carrying out application registration of the object registrant certificate, the Certification Authority will begin the certificate issuing procedures.

Regarding JPNIC employee certificates, the Certification Authority will determine whether the application will be accepted or rejected.

Regarding the server's certificates, the Certification Authority will determine whether the application will be accepted or rejected.

4.2.3. Certificate Application Processing Time

In the case where the issue application from applicants for object registrant certificates is accepted, the maintainer administrator will swiftly carry out the certificate issue application registration.

In the case where the issue application from applicants for maintainer administrator certificates is accepted, the JPNIC Registration Authority administrator will swiftly carry out the certificate issue application registration.

In the case where the issue application registration is accepted from the maintainer administrator or the JPNIC Registration Authority administrator, the Certification Authority will swiftly issue the certificate.

Regarding JPNIC employee certificates, in the case where the Certification Authority accepts an issue application from an individual or entity prescribed in "4.1.1 Individuals or Entities that can Submit Certification Applications", it will swiftly carry out issue of the certificate.

Regarding the server's certificates, in the case where the Certification Authority accepts an issue application from an individual or entity prescribed in "4.1.1 Individuals or Entities that can Submit Certification Applications", it will swiftly carry out issue of the certificate.

4.3. Certificate Issue

4.3.1. Certification Authority Actions in the Certificate Issuing Process

Concerning the receipt of the issue application registration for object registrant certificates from the maintainer administrator, the Certification Authority will conduct authority confirmation of the maintainer administrator using the method prescribed beforehand. Further, concerning the receipt of the issue application registration for maintainer administrator certificates, authority confirmation of the maintainer administrator will be carried out according to previously prescribed methods. After confirming the authenticity of the application registration, the Certification Authority will give out notification of permission for issue of the certificate to the applicant for the object registrant certificate using the methods prescribed in “4.3.2 Certificate Issue Notification for Certification Authority Subjects” in this CPS.

The Certification Authority verifies the electronic signature of the certificate signing request sent by the applicant for the object registrant certificate. Then, after confirming the authenticity of the certificate signing request, the certificate is issued to the applicant for the object registrant certificate via secure online communications.

The Certification Authority verifies the electronic signature of the certificate signing request sent by the applicant for the maintainer administrator certificate. Then, after confirming the authenticity of the certificate signing request, the certificate is issued to the applicant for the maintainer administrator certificate via offline means.

Concerning JPNIC employee certificates, after conducting confirmation of correct individual or entity for the applicant, the Certification Authority will issue the certificate using the method prescribed beforehand.

Concerning server’s certificates, after conducting confirmation of the correct individual or entity for the applicant, the Certification Authority will issue the certificate using the method prescribed beforehand.

4.3.2. Certification Issue Notification for Certification Authority Subjects

Issue notification regarding maintainer administrator certificates will be sent to applicants using offline means.

The Certification Authority will generate the information necessary for the certificate issuing, and will notify the applicant for the object registrant certificate via the maintainer administrator.

Regarding JPNIC employee certificates, the Certification Authority conducts issue notification to applicants using methods prescribed beforehand.

Regarding server's certificates, the Certification Authority will conduct issue notification to applicants using the methods prescribed beforehand.

4.4. Certificate Receipt Confirmation

4.4.1. Certificate Receipt Confirmation Actions

Receipt of maintainer administrator certificates will be conducted using offline means. If no contact is received by JPNIC within 1 week of sending the certificate, it will be considered to have been received.

The Certification Authority will deliver maintainer administrator certificates using a method that will allow confirmation of the certificate's arrival. Downloading of the object registrant certificate will be carried out by the applicant for the certificate, and the certificate should be received after confirming the content. In the case where there is a problem with the certificate, contact should be made with JPNIC via the maintainer administrator. If no contact is received by JPNIC within 1 week of sending the certificate, it will be considered to have been received.

Regarding JPNIC employee certificates, the Certification Authority will confirm the receipt of the certificate using a method involving offline means prescribed beforehand.

Regarding server's certificates, the Certification Authority will confirm the receipt of the certificate using the method prescribed beforehand.

Note that the applicant for the certificate must confirm that the certificate file is possible to be used on their computing environment, and that the details described in the certificate are correct.

4.4.2. Disclosure of the Certificate by the Certification Authority

The Certification Authority will disclose the certification using the repository according to "2.2. Certification Information Disclosure" in this CPS.

4.4.3. Certification Issue Notification by Certification Authority to Other Entities

The Certification Authority will not carry out certification issue notification to other entities.

4.5. Utilization of Key Pairs and Certificates

4.5.1. Subject Private Key and Certificate Use

Certificates issued based on this CPS are intended to be used for practices such as applications between JPNIC and IP Address Management Agents.

Certificate subjects will bear the following responsibilities regarding the use of the private key and the certificate:

- Confirmation and reporting of any errors in the content of the certificate on receipt of the certificate.
- Taking of adequate care and administration of the private key to prevent theft, leakage, loss, or inappropriate use by another entity.
- Swift revocation application in situations where there is a danger or possibility of the key becoming compromised.
- Confirmation of the usage purpose and use within this purpose.
- Maintaining the confidentiality of the private key and administering the correspondence of the private key and public key.

4.5.2. Relying Party Public Key and Certificate Use

The certificate relying party bears the following responsibilities concerning the reliability of the certificate:

- Understanding and agreement with this CPS at the point of time that the certificate is trusted.
- Agreement that the certificate usage purpose and the relying party's usage purpose are in accord.
- Verification of the electronic signature used in the certificate and confirmation of the issuing authority.
- Confirmation of the certificate period of validity and the described items.
- Confirmation using the Certificate Revocation List (CRL) that the certificate has not been revoked.
- Confirmation of all certificates on the certificate path regarding falsification, periods of validity, revocation, and usage purpose.

4.6. Certificate Updating

In the Certification Authority, certification updating will not be conducted without revising the key pair. In the case where the certificate is updated, a new key pair will be generated using the procedure defined in “4.7 Certificate Key Updating” in this CPS.

4.6.1. Case where Certificate Updating is to be Conducted

Not stipulated.

4.6.2. Individuals or Entities that can Apply to Update Certificates

Not stipulated.

4.6.3. Certificate Updating Application Processing

Not stipulated.

4.6.4. Notification to Subjects of New Certificates

Not stipulated.

4.6.5. Updated Certificate Receipt Confirmation Actions

Not stipulated.

4.6.6. Disclosure of Certificates Updated by the Certification Authority

Not stipulated.

4.6.7. Notification to Other Entities

Not stipulated.

4.7. Certificate Key Updating

4.7.1. Situations where Certificate Key is Updated

Certificate key updating will be carried out in the following situations:

- Case where the certificate period of validity has expired.
- Case where certificate has been revoked due to the reason of key compromise.

4.7.2. Individuals or Entities that can Apply for New Public Key Certification

Same as “4.4.1. Certificate Receipt Confirmation Actions” in this CPS.

4.7.3. Certificate Key Updating Application Processing

Same as procedures defined in “4.2. Certificate Application Procedures” and “4.3. Certificate Issue” in this CPS.

4.7.4. New Certificate Notification for Subjects

Same as “4.3.2. Certificate Issue Notification for Certification Authority Subjects” in this CPS.

4.7.5. Key Updated Certificate Receipt Confirmation Actions

Same as “4.4.1. Certificate Receipt Confirmation Actions” in this CPS.

4.7.6. Disclosure of Certificate that has had Key Updated by the Certification Authority

Same as “4.4.2. Disclosure of the Certificate by the Certification Authority” in this CPS.

4.7.7. Notification to Other Entities

Same as “4.4.3. Certificate Issue Notification by Certification Authority to Other Entities” in this CPS.

4.8. Certificate Revision

4.8.1. Case where Certificates will be Revised

Certificate revision will be carried out in the following situation:

- Case where information in the certificate other than the public key has been revised.

4.8.2. Individuals and Entities that can Apply for Revisions to Certificates

Same as “4.7.2 Individuals or Entities that can Apply for New Public Key Certification” in this CPS.

4.8.3. Revision Application Processing

Same as “4.7.3. Certificate Key Updating Application Processing” in this CPS.

4.8.4. New Certificate Notification for Subjects

Same as “4.7.4. New Certificate Notification for Subjects” in this CPS.

4.8.5. Receipt Confirmation Actions for Revised Certificates

Same as “4.7.5. Key Updated Certificate Receipt Confirmation Actions” in this CPS.

4.8.6. Disclosure of Revised Certificates by Certification Authority

Same as “4.7.6. Disclosure of Certificate that has had Key Updated by the Certification Authority” in this CPS.

4.8.7. Certificate Issue Notification by Certification Authority to Other Entities

Same as “4.7.7. Notification to Other Entities” in this CPS.

4.9. Certificate Revocation and Temporary Suspension

4.9.1. Circumstances of Certification Revocation

The subject of the object registrant certificate must carry out certificate revocation application to the maintainer administrator.

The subject of the maintainer administrator certificate must carry out certificate revocation application to JPNIC.

In situations where it is determined that the following items apply, the Certification Authority will be able to revoke the various certificates:

- Situation where the Certification Authority is abolished.
- Situation where the Certification Authority private key has been compromised, or there is a danger of compromise.
- Situation where the certificate content items differ from the actual situation.
- Situation where the private key of the certificate subject has been compromised, or there is a danger of compromise.
- Situation of inappropriate use of certification, or the danger of inappropriate use.
- Situation where the certificate subject or the local RA does not implement work according to this CPS or other agreements, regulations and laws.
- Situation where the agreement between the JPNIC Certification Authority and the IP Address Management Agent has been cancelled.
- Other situations in which the Certification Authority has determined that revocation is necessary.

In the situation where the following items apply to the subject of the server's certificate, the revocation application must be carried out through the Certification Authority.

- Situation where the server use is suspended.
- Situation where the server private key has been compromised or there is a danger of compromise.

Further, in the situation where the following items are found to apply, it will be possible for the Certification Authority to carry out server's certificate revocation in addition to cases where the Certification Authority receives a revocation request from the certificate subject.

- Situation where the Certification Authority is abolished.
- Situation where the Certification Authority private key has been compromised or there is a danger of compromise.
- Situation where the certificate content items differ from the actual situation.
- Situation where the server private key has been compromised or there is a danger of compromise.

- Situation where the certificate is used inappropriately or there is a danger of inappropriate use.
- Situation where the certificate subject does not implement work according to this CPS or other agreements, regulations, and laws.
- Other situations in which the Certificate Authority judges that revocation is necessary.

4.9.2. Individuals or Entities that can Apply for Certificate Revocation

Individuals or entities that can request revocation of object registrant certificates are as follows:

- Certificate subject
- Legal representative of the certificate subject
- Local RA manager and maintainer administrator of the organization to which the certificate subject belongs.
- The Certification Authority

Individuals or entities that can request revocation of server's certificates are as follows:

- The certificate subject
- The Certification Authority

4.9.3. Revocation Application Procedures

After confirming the appropriateness of the revocation request according to the specified procedures, the maintainer administrator carries out certificate revocation registration in the Certification Authority.

After confirming the appropriateness of the revocation request according to the specified procedures, JPNIC carries out certificate revocation registration in the Certification Authority.

The server's certificate subject carries out the revocation application for the Certification Authority using the methods that have been previously prescribed.

Note that in the situation where the Certification Authority has determined that the items specified in "4.9.1. Circumstances of Certificate Revocation" are applicable, this Certificate Authority may carry out the certificate revocation registration following its own judgment

4.9.4. Revocation Application Delay Period

In the situation where conditions have occurred that require certification revocation, the revocation will be conducted as swiftly as possible.

4.9.5. Period during which the Certification Authority should carry out Processing of the Revocation Application

The certificate revocation processing will be carried out in the Certification Authority within five working days of receiving the revocation application.

4.9.6. Relying Party Revocation Checking Request

Concerning the reliance and use of the certificate issued by the Certification Authority, the certificate relying party must refer to the latest Certificate Revocation List (CRL) to confirm that the certificate in question has not had revocation processing carried out.

4.9.7. Certificate Revocation List Issuing Frequency

Regardless of whether or not there are certificate revocations, the CRL will be updated within 24 hours. In the situation where certificate revocation has been applied for, the CRL will be updated as soon as the revocation procedures have been completed.

4.9.8. Maximum Grace Period for Issue of Certificate Revocation List

After generating the CRL, the Certification Authority will swiftly disclose it on the repository.

4.9.9. Applicability of Revocation/Status Confirmation Online

Online revocation or status check functions such as OCSP are not supported.

4.9.10. Requirements for Conducting Online Revocation/Status Confirmation

Not stipulated.

4.9.11. Other Formats of Revocation Notification that may be Used

Not stipulated.

4.9.12. Special Conditions regarding Compromise of the Key Update

In the situation where there has been a compromise or danger of compromise of the private key of the Certification Authority, revocation processing of all of the certificates will be immediately conducted. Certificates will be registered in the CRL, and the facts of the compromise of the Certification Authority's private key and the notification of certificate revocation will be sent to certificate subjects using means such as E-mail.

4.9.13. Situation of Certificate Temporary Suspension

The Certification Authority will not temporarily suspend a certificate that has been issued.

4.9.14. Individuals or Entities that can Apply for Temporary Suspension of Certificates

Not stipulated.

4.9.15. Certificate Temporary Suspension Application Procedures

Not stipulated.

4.9.16. Period over which the Temporary Suspension can be Continued

Not stipulated.

4.10. Certificate Status Confirmation Service

4.10.1. Characteristics of Operation

The Certification Authority will provide CRLs as a means for relying parties to confirm certificate status. The conditions for accessing the CRL are specified in “2.4. Repository Access Management” in this CPS. Further, the CRL issue frequency and maximum issue grace period are specified in “4.9.7. Certificate Revocation List Issuing Frequency” and “4.9.8. Maximum Grace Period for Issue of Certificate Revocation List” in this CPS.

4.10.2. Service Usage Possibility

Specified in “2.1 Repository” in this CPS.

4.10.3. Optional Specifications

Not stipulated.

4.11. Registration Completion

In the situation where the certificate subject has completed the Certification Authority service usage registration, the Certification Authority will revoke all of the certification issued to the certificate subject.

4.12. Key Escrow and Key Recovery

The Certification Authority will not deposit its private key with any third party.

4.12.1. Key Escrow and Key Recovery Policy and Implementation

Not stipulated.

4.12.2. Session Key Encapsulation and Key Recovery Policy and Implementation

Not stipulated.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

The important facilities related to the Certification Authority are installed in locations where they will not be easily affected by damage from fire, water exposure, earthquakes, lightning or other natural disasters. The building structure incorporates measures for resistance to earthquakes and fire, and prevents against illegal entry. There is no indication of the location of the certification facilities room inside and outside the building.

Further, the equipment used will be located in a secure place, protected from disasters and improper access.

5.1.2. Physical Access

Concerning the certification facilities room, the Certification Authority conducts room entry-exit management that allows identification of persons who have been cleared for entry beforehand and confirmation of entry clearance. The Certification Authority in principle does not permit entry to the room of persons who do not have entry clearance. In situations where it is necessary for entry to be permitted, clearance will be obtained from the Certification Authority Operation Administrator beforehand, and the person granted entry will be accompanied at all times by a person who has clearance to enter the room.

5.1.3. Electric Power and Air Conditioning

In addition to securing an adequate capacity of electric power supply for operating the equipment, the Certification Authority will also implement measures to prepare against momentary power lapses, power failures, and fluctuations in voltage and frequency. Further, regarding air conditioning equipment, the room temperature will be maintained and administered at levels that will not adversely affect the various equipment being used.

5.1.4. Measures against Water Exposure and Earthquakes

Measures against water exposure will be implemented in the room where the Certification Authority is located in order to keep the level of damage due to water exposure to a minimum. Further, the JPNIC Certification Authority will implement measures to prevent equipment and furniture from toppling over or falling down in the occurrence of an earthquake.

5.1.5. Fire Prevention and Fire Protection Measures

The Certification Authority has located the facilities inside fire prevention blocks that divide the area using fire walls. Further, inside the fire prevention blocks, fire prevention measures are implemented in the power source and air conditioning equipment, and fire detectors and fire-fighting equipment is also installed.

5.1.6. Media Storage Location

The media including archived data and backup data are stored in a storage warehouse inside a room where appropriate entry-exit management is carried out. Further, duplicates of important media will be stored in a storage warehouse that is separate from the Certification Authority's equipment location inside a room where appropriate entry-exit management is carried out.

5.1.7. Disposal Processing

For documentation and recording media including information that requires handling as confidential data, the Certification Authority will conduct appropriate disposal processing following methods prescribed beforehand including information initializing and deletion.

5.1.8. Backup Outside the Facilities

Not stipulated.

5.2. Procedural Controls

5.2.1. Trusted Roles

Persons carrying out key practices such as certificate issue, updating, and revocation undertake trusted roles in this CPS.

5.2.2. Employees Required for Each Operation

In the situation where it is necessary for persons who do not have entry authority to enter the Certification facilities room, such as for the maintenance of the Certification Authority facilities and responses during failures of the JPNIC Certification Authority equipment, the people will at all times be accompanied by a person who is authorized to be in the room.

5.2.3. Identification and Authentication of Individual or Entity for Particular Roles

The Certification Authority equipment includes a function for discriminating between operators and necessary authorization. Further, the authorization for operation of the Certification Authority equipment can be configured for each operator.

5.2.4. Roles Requiring Task Division

By dividing authority among several persons rather than concentrating authority in a particular person, it is intended to prevent the occurrence of improper actions caused by individual operation. The authority will be divided for system operation, approval actions, and auditing.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Identification Requirements

When appointing employees to roles in the Certification Authority, and periodically afterwards, JPNIC will implement appropriate character investigations before making appointments. When making appointments, non-disclosure agreements will be signed, and appropriate information management will be carried out. Further, during daily practices, continuous personnel management will be carried out including mental health and health management and appropriate treatment.

5.3.2. Regulatory Items relating to Personnel Assignments

Concerning the appointment of key persons for the Certification Authority practices, appropriate personnel will be allocated to avoid problems occurring during operation execution. Allocated employees will be required to submit pledges to strictly maintain confidentiality and observe internal regulations.

5.3.3. Training Requirements

For the education of key operational personnel, the following will be carried out:

- Before the key operational personnel take up their roles, necessary education will be implemented regarding the Certification Authority operations.
- Education and training plans will be developed supporting each role, and regular education and training will be implemented following the plans.
- In the situation where changes are made to the practice procedures, the changes to the work handling points will be made without delay, and education and training relating to these changes will be implemented.

5.3.4. Retraining Frequency and Requirements

JPNIC will regularly conduct appropriate education for Certification Authority key employees, and will carry out re-education afterwards if necessary.

5.3.5. Work Rotation Frequency and Order

Not stipulated.

5.3.6. Penalties for Carrying out Unapproved Actions

Concerning unapproved actions carried out by Certification Authority key operational personnel, penalties will be imposed according to the regulations specified beforehand.

5.3.7. Independent Contractor Requirements

JPNIC will clearly explain the details of the commissioned work in the commissioning agreement, clarifying for the contractor the strict observance of JPNIC directions, liability sharing, warranty, and penalties for infringements, and will also enter into a non-disclosure agreement. Further, after commissioning the work, auditing and administration will be carried out to confirm that the practices are being implemented appropriately.

5.3.8. Materials Supplied to Key Employees

Documentation necessary for the operations will be disclosed and notified to the operations key employees.

5.4. Audit Log Procedures

5.4.1. Types of Events Recorded

For events occurring in the Certification Authority system, regardless of whether they occur manually or automatically, the date, time, subject of the event, and the event details will be recorded.

The following records will be recorded as the necessary audit log for detecting Certification Authority mistaken operation and improper operation, and certifying the appropriateness of operations:

- Records relating to the operation of the Certification Authority private key
- Records relating to certificate issue and revocation work
- Records relating to the revocation information production practices
- Records relating to the confirmation of the audit log

Further, the records of accesses to the Certification Authority equipment will be recorded.

5.4.2. Frequency of Processing the Audit Log

The Certification Authority regularly reviews the audit log and the related records.

5.4.3. Period during which the Audit Log is Retained

The audit log will be retained on the server inside the Certification Authority for a minimum of 2 months. After this time, it will be stored for a fixed period on an external recording medium. Records relating to the entry and exit from the certification facilities room, and records concerning improper access will be retained until completion of the next audit.

5.4.4. Audit Log Protection

In order that only authorized JPNIC employees can access the audit log file, the Certification Authority appoints an authorizer to protect the log file from being viewed, edited, or deleted by unauthorized persons. Further, the audit log will be regularly backed-up to external recording media which will be stored in a lockable storage warehouse in a room with appropriate entry and exit administration.

5.4.5. Audit Log Backup Procedure

Following procedures determined beforehand, the audit log together with the Certification Authority system database will be regularly backed-up on external recording media, and the media stored in a safe facility.

5.4.6. Audit Log Collection System

An audit log collection function is incorporated as one of the functions in the Certification Authority system, and important events relating to security are collected as the audit log.

5.4.7. Notification to Subject causing the Event

In the Certification Authority, the audit log collection is carried out without giving notification to the person, system or application that caused the event.

5.4.8. Vulnerability Assessment

The hardware and software used in the certification practices is assessed for security vulnerabilities from the system and operations points of view using audit log inspections, and the latest applicable security technology is introduced to improve security measures.

5.5. Record Storage

5.5.1. Archive Record Types

In addition to the audit log specified in “5.4.1. Types of Recorded Events” in this CPS, the Certification Authority stores the following records:

[Events Recorded in the Certification Authority System]

- Generation of the Certification Authority signature key pair
- Additions and deletions of certificate subjects from the system
- Changes in keys, including certificate issues and revocations
- Additions, changes and deletions of Registration Authority administrator authority

[Events Recorded as Paper Media and External Recording Media]

The Certification Authority maintains and administers an archive relating to the following operations-related records.

- Records relating to this CPS and the certificate subject agreement, and changes made to them.
- Records relating to the responsibilities and authority of persons conducting the certification practices, and changes made to them.
- In the case where part of the certification practices are commissioned to another entity, the original documentation relating to the commissioning agreement.
- Records relating to the audit implementation result, and the audit report.

5.5.2. Archive Storage Period

The Certification Authority will store the Certification Authority system database records and the audit log file records for a fixed period. The storage period for paper media and external recording media are defined in “5.5.1. Archive Record Types” in this CPS.

5.5.3. Archive Protection

Access control is implemented for the archived data, together with measures that allow detection of alterations. The Certification Authority regularly backs up the archived data to external recording media, restricting access only to persons who have received clearance from the JPNIC Administration Division, and storing the media in facilities that are protected from environmental dangers such as temperature and humidity.

5.5.4. Archive Backup Procedures

The Certification Authority implements automatic and regular backups of the Certification Authority system database on the server. Further, the audit log is also regularly stored on external recording media.

5.5.5. Requirements for Attaching Time-stamps to Records

The Certification Authority attaches time-stamps to each record of important information recorded in the Certification Authority. The time-stamps indicated here do not utilize cryptographic technology.

5.5.6. Archive Collection System

A Certification Authority server database record collection system is incorporated in the Certification Authority server system. The audit log file record collection system is defined in "5.4.6. Audit Log Collection System" in this CPS.

5.5.7. Procedures for Obtaining and Verifying Archived Information

For the archived data, a person permitted to access the strictly administered storage section will obtain the data and regularly confirm the readability of the external recording media. Further, when necessary, the data will be copied onto new media and the old media that has exceeded its storage period will be destroyed in consideration of maintaining the completeness and confidentiality of the archived data.

5.6. Key Switching

Before the remaining validity period of the Certification Authority private key becomes less than the maximum validity period of the EE certificates, JPNIC will prevent the issue of new EE certificates using the key. JPNIC will then generate a new Certification Authority key pair using the method specified in “6.1. Key Pair Generation and Installation” in this CPS. The new public key will receive issue of a certificate from the JPNIC Root Certification Authority, and will be distributed in the same way as the method specified in “6.1.4. Delivery of Certification Authority Public Key to Relying Parties” in this CPS.

5.7. Recovery from Key Compromise and Disasters

5.7.1. Handling Procedures for Incidents and Key Compromise

In situations where the Certification Authority private key has been compromised or there is a danger of compromise, or when a disaster has occurred that has led to the interruption or suspension of certification practices, the Certification Authority will strive to restart the certification practices following plans and procedures defined beforehand.

5.7.2. Case where Computer Resources, Software and/or Data has been Corrupted

In a situation where hardware, software or data has been corrupted, the JPNIC Certification Authority will strive to quickly implement recovery work using backup hardware, software and data following recovery plans determined beforehand.

5.7.3. Procedures when Entity Private Key has been Compromised

In a situation where the Certification Authority private key has been compromised, plans defined beforehand will be followed to halt the certification practices and then carry out the following procedures:

- Revocation procedures for maintainer administrator certificates, object registrant certificates, and JPNIC employee certificates.
- Procedures to destroy the Certification Authority private key and generate new keys
- Procedures to re-issue the maintainer administrator certificates, object registrant certificates, and JPNIC employee certificates.

Further, in the situation where a certificate subject's private key has been compromised, certificate revocation procedures will be carried out based on procedures determined beforehand in "4.9. Certificate Revocation and Temporary Suspension" in this CPS.

5.7.4. Business Continuation Capability after Disaster Occurrence

In the situation where the JPNIC Certification Authority facilities receive damage due to a disaster or incident, JPNIC will strive to re-start operations by securing reserve equipment and using backup data.

5.8. Termination of Certification Authority or Registration Authority Practices

In the case where JPNIC has decided to terminate its Certification Authority certification practices, the specified practices termination procedures will be implemented, in which notification will be given to certificate subjects and relying parties 14 days before the termination of practices, explaining that the certification practices of the JPNIC Certification Authority will be terminated. The explanation will also describe the storage organization and disclosure method for the Certification Authority backup data and archive data after the termination of business

6. Technical Security Management

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Generation of Certification Authority key pairs should be carried out by several CAOs in the presence of the key administrator inside the certification facilities room. The generation of Certification Authority key pairs is carried out using FIPS140-1 Level 3 cryptographic modules.

Generation of key pairs for maintainer administrator certificates and JPNIC employee certificates should be carried out using FIPS140-2 Level 3 cryptographic modules.

6.1.2. Delivery of Private Keys to Subjects

Generation of key pairs for maintainer administrator certificates and JPNIC employee certificates is conducted by the Certification Authority inside the cryptographic module. The generated key pair will be delivered to applicants using a hardware token that includes a cryptographic module.

Because the Certification Authority does not carry out generation of key pairs for object registrant certificates, this item is not regulated.

6.1.3. Delivery of Public Keys to Certificate Issuers

The delivery of object registrant certificate public keys to the Certification Authority should be carried out using encrypted communications to send the PKCS#10 format file to the Certification Authority.

6.1.4. Delivery of Certification Authority Public Keys to Relying Parties

Distribution of certificates by the Certification Authority is carried out using the most appropriate of the following two methods according to the EE.

- The Certification Authority certificates are disclosed on the JPNIC Certification Authority Website. In the disclosure of the Certification Authority certificates, a secure protocol with an encryption function is used, and alteration prevention measures are applied. Certificate relying parties download the Certification Authority certificates from the same page for use. The relying parties compare the fingerprint of the downloaded Certification Authority certificates with the fingerprint that has been disclosed using a non-Internet method and confirm that they match.

- For object registrants, the Certification Authority certificates will be handed over by the maintainer administrator.

6.1.5. Key Size

The Certification Authority uses 2048-bit RSA key pairs. EEs are obliged to use RSA key pairs with 1024 bits or more.

6.1.6. Public Key Parameter Generation and Quality Inspection

The public key parameters for generating the Certification Authority key pairs use Random Number Generation (known henceforth as RNG) incorporated in software that includes highly secure cryptographic modules for use in the key pair generation.

For the quality inspection of the public key parameters, there is no particular specification.

6.1.7. Key Application Purpose

The Certification Authority certificate keyUsage uses the keyCertSign and cRLSign bits. The Certification Authority private key is only used for issuing EE certificates and the CRL.

The maintainer administrator certificate, object registrant certificate, and JPNIC employee certificate keyUsage uses the digitalSignature, keyEncipherment, and dataencipherment bits. They are only used for S/MIME and SSL/TLS client certificates.

6.2. Private Key Protection and Cryptographic Module Technical Administration

6.2.1. Cryptographic Module Standards and Administration

Not stipulated.

6.2.2. Multi-person Control of Private Key

The Certification Authority private key administration is carried out by investing authority in a number of CAOs. It will not be possible to operate the Certification Authority private key unless there are two or more CAOs present.

6.2.3. Private Key Escrow

Specified in “4.12. Key Escrow and Key Recovery” in this CPS.

6.2.4. Private Key Backup

The Certification Authority private key will be backed-up on external recording media determined beforehand. During production of the backup, it will also be necessary for the key administrator and several CAOs to be in attendance.

The Certification Authority will store the backup in a storage location determined beforehand.

Note that the Certification Authority will not carry out backing-up of EE private keys.

6.2.5. Private Key Archiving

Archiving of the Certification Authority private key will not be conducted.

Similarly, archiving of EE private keys will not be carried out.

6.2.6. Transferring Into or From the Private Key Cryptographic Module

The Certification Authority private key is generated using software that includes a highly secure cryptographic module, with no intervention from other hardware or software.

6.2.7. Storage of Private Key in the Cryptographic Module

The Certification Authority private key is generated and stored in a highly secure cryptographic module.

For the object registrant private key, the object registrant will carry out generation and storage of the private key themselves. The confidential keys of the maintainer administrator and JPNIC employees will be generated and stored inside highly secure cryptographic modules by JPNIC. However, for the server, the server's certificate administrator will carry out the storage.

6.2.8. Private Key Activation Method

Activation of the Certification Authority private key is carried out inside the certification facilities room.

The EE private key activation is not stipulated.

6.2.9. Private Key Deactivation Method

Deactivation of the Certification Authority private key is carried out inside the certification facilities room, with the work divided between the person conducting the operation and a person supervising.

The EE private key deactivation is not stipulated.

6.2.10. Private Key Destruction Method

In the situation where the Certification Authority private key must be destroyed, the key administrator will completely initialize or physically destroy the hard disk on which the private key was stored. At the same time, the backup private key will also be destroyed using the same procedures.

EE private keys should be completely destroyed by the EE itself. The confidential key of the maintainer administrator will basically be destroyed by JPNIC. However, in situations such as when it has been lost, this may not be carried out.

6.2.11. Cryptographic Module Assessment

Not stipulated

6.3. Other Key Pair Administration

6.3.1. Public Key Archiving

The Certification Authority will back-up the Certification Authority certificates and all the certificates issued by the Certification Authority.

6.3.2. Period of Certificate Operation and Key Pair Usage Period

The period of validity of Certification Authority certificates is 10 years and the validity period of the private key is 8 years. The Certification Authority will update the key pair before the private key validity period ends.

The period of validity of EE certificates is 2 years. Use will be permitted for more than 2 years only in situations where private key decoding is carried out.

6.4. Activated Data

6.4.1. Activated Data Generation and Configuration

Including the Certification Authority private key, the PINs and passwords used in the Certification Authority have lengths of 8 or more capital or small alphanumeric characters.

6.4.2. Activated Data Protection

Regarding the PINs and passwords used in the Certification Authority, after sealing, they are stored under the administration of the operations administrator.

6.4.3. Other Considerations for Activated Data

Not stipulated.

6.5. Computer Security Management

6.5.1. Technical Requirements relating to the Security of Particular Computers

Practices relating to the Certification Authority server system will in principle be conducted by several CAOs. However, work that is necessary to be carried out such as during hardware failures by persons with specialized knowledge will be conducted by maintenance persons in the presence of the CAO. Important operations concerning the system are all configured to be stored in the log. All passwords used for accessing the system will have appropriate administration conducted. Regarding the Certification Authority server system, constant resource monitoring will be carried out, and appropriate measures will be implemented swiftly in the situation where a system abnormality or improper operation is detected.

6.5.2. Computer Security Assessment

All of the software and hardware used by the Certification Authority will have operation testing conducted before use to confirm the reliability.

6.6. Administration of Life Cycle Technology

6.6.1. System Development Administration

In order to maintain the system quality and security, administration of each process during development and assessment before introduction will be implemented.

6.6.2. Security Operations Administration

For the system security management, usage administration including room entry-exit administration, key employee administration including education, and authority administration will be carried out. Security measures such as improper entry measures and virus countermeasures, and the timely updating of security countermeasures software will be implemented.

6.6.3. Life Cycle Security Management

Using the specified administration method, assessment will be carried out regarding whether the system is being managed.

Regarding the Certification Authority system, information collection will be conducted relating to security, and appropriate assessment and improvements will be implemented while referring to the latest trends.

6.7. Network Security Management

A firewall is used for the network in the Certification Authority, and access from outside the firewall is restricted using the necessary minimum protocol. Further, the hosts that can be accessed are also limited.

6.8. Time-stamps

Requirements relating to the use of time-stamps are stipulated in “5.5.5. Requirements for Attaching Time-stamps to Records” in this CPS.

7. Profiles of Certificates, Certificate Revocation Lists, and OCSP Profiles

7.1. Certificate Profile

Certificates issued by the Certification Authority conform to X.509 certificate format v3. The certificate profile is as shown in Table 7-1.

7.1.1. Version No.

All certificates issued by the Certification Authority conform to X.509 v3 certificate format.

7.1.2. Certificate Extensions

The extension fields used in certificates issued by the Certification Authority are as shown in Table 7-3.

7.1.3. Algorithm OID

The algorithm OIDs used in certificates issued by the Certification Authority are the two shown below:

- sha1withRSAEncryption (1.2.840.113549.1.1.5)
- rsaEncryption (1.2.840.113549.1.1.1)

7.1.4. Name Format

Conforms to “3.1.1. Types of Names” in this CPS.

7.1.5. Naming Constraints

The nameConstraints extension is not used in any of the certificates issued by the Certification Authority.

7.1.6. Certificate Policy OID

Object registrant certificates, maintainer administrator certificates, and JPNIC employee certificates each use the EE certificate policy OID defined in “1.2 Documentation Name and Identification” in this CPS.

7.1.7. Policy Constraints Extensions

The policyConstraints extension is not used in any of the certificates issued by the Certification Authority.

7.1.8. Policy Qualifier Description and Meaning

The URI disclosed in this CPS is used both in object registrant certificates and in server's certificates as the policy qualifier value.

7.1.9. Processing of certificatePolicies Extensions for Critical Certificates

The certificatePolicies extensions included in certificates issued by the Certification Authority are all non-critical, and regulations are not carried out for this item.

Table 7.1 Profile of Certificates issued by the JPIRR Certification Authority (Basic Fields)

Field	Setting Value	Remarks	
version	v3	Shows X.509 Certificate Version 3	
serialNumber		Automatic generation by the CA System	
signature	SHA1withRSA		
issuer		Same value as the Subject of the JPNIC Primary Root CA	
	C	JP	
	O	Japan Network Information Center	
	OU	JPIRR Certification Authority 01	
Validity		Two years and 30 days	
notBefore	YYYYMMDDHHMMSS		
notAfter	YYYYMMDDHHMMSS		
subject	[Described in Table 7.2]		
subjectPublicKeyInfo			
	algorithm	1.2.840.113549.1.1.1	RSA 1024bit
	subjectPublicKey		Automatic generation by the CA System

Regarding the values set as the subject attributes for each user conferred by the JPIRR Client Certificate, a description is given in the table below.

Table 7.2 Subject Information for each JPIRR Client Certificate User

DN	User			
	JPNIC Contact		JPIRR Certificate Administrator	Object Registrant
	S/MIME I/F			
C	" JP "			
O	" Japan Network Information Center "		" Resource Holder "	
O			" ASN Holder "	
OU	" Internet Resource Service "		" IRR Maintainer Administrator "	" IRR Object Registrant "
OU	" Secretariat "		(User administration subject maintainer name conferred)	(User administration subject maintainer name conferred)
OU	" IRR Administrator "			
CN	Each of the following items should be written separated by a space character. (1) "IRR-AD" (2) Optional name of up to 64 characters (3) Sequence Number... Sequence number of certificates issued to the same user combination of (1) and (2). For new certificate issues, this will be "01".	" JPIRR Secure MIME Gateway "	Each of the following items should be written separated by a space character. (4) "IRR-MA" (5) Maintainer object admin-c item (6) Sequence Number... Sequence number of certificates issued to the combination of (4) and (5) (same user). For new certificate issues, this will be "01".	Each of the following items should be written separated by a space character. (7) "IRR-OR" (8) Maintainer object tech-c item (9) Sequence Number... Sequence number of certificates issued to the combination of (7) and (8) (same user). For new certificate issues, this will be "01".

Out of the DN set as the subject attributes, the user is solely identified using the CN. Further, by adding the sequence number in the CN, the JPIRR Client certificates issued to each user can be solely specified. Note that even when the user who actually uses the certificate is the same user, if items apart from the sequence number described in the CN information in the JPIRR client certificate are changed, the sequence number will be set to "01". (It will be handled as though the certificate is being newly issued.)

Table 7.3 Detailed Profile of JPIRR Client Certificates (Extension Fields)

Field	Critical Flag	Setting Values	Remarks
authorityKeyIdentifier	Non		Public key hash value of JPIRR Certification Authority certificates
subjectKeyIdentifier	Non		Public key hash value of this JPIRR Client certificate
keyUsage	Critical	digitalSignature (Digital signature verification) keyEncipherment (Key encipherment)	
extendedKeyUsage	Non	1.3.6.1.5.5.7.3.2: SSL/TLS client authorization 1.3.6.1.5.5.7.3.4: E-mail protection	
certificatePolicies	Non	[1]Certificate Policy: Policy Identifier=1.2.392.200175.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://jpnica.nic.ad.jp/capub/jpirr/jpirr-ca_cps.html	
subjectAltName	Non	[rfc822name]	User's E-mail address
basicConstraints	Non		
Subject Type		End Entity	
Path Length Constraints		None	
cRLDistributionPoints	Non	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://jpnica.nic.ad.jp/capub/jpirr/jpirr-ca.crl	

7.2. Profile of Certificate Revocation List

CRLs issued by the Certification Authority comply with X.509 CRL format v2. The CRL profile is as shown in Table 7-4.

7.2.1. Version No.

All CRLs issued by the Certification Authority comply with X.509 v2 CRL format.

7.2.2. CRL and CRL Entry Extensions

The Certification Authority uses the following two CRL extensions, and CRL entry extensions are not used.

7.2.2.1. cRLNumber

CRLs issued by the Certification Authority use a non-negative integer that will become unique.

7.2.2.2. authorityKeyIdentifier

The Certification Authority public key 160-bit SHA-1 hash value is used as the keyIdentifier value. This extension is non-critical.

Table 7.4 CRL Profiles issued by the JPIRR Certification Authority

Field		Setting Values	Remarks
version		v2	Shows Version 2
signature		SHA1withRSA	
subject		C	JP
		O	Japan Network Information Center
		OU	JPIRR Certification Authority 01
thisUpdate		YYYYMMDDHHMMSS	System time that the CRL was issued
nextUpdate		YYYYMMDDHHMMSS	Date and time 15 days following thisUpdate
revokedCertificates			
userCertificate			Serial number of the revoked certificate
revocationDate		YYYYMMDDHHMMSS	Date and time that revocation processing was implemented

crlExtensions			
Field	Critical Flag	Setting Values	Remarks
authorityKeyIdentifier	Non		Public key hash value of JPIRR Certification Authority certificate
cRLNumber	Non		Automatic generation by the CA System

7.3. OCSP Profile

7.3.1. Version Information

Not stipulated

7.3.2. OCSP Extensions

Not stipulated

8. Compliance Audit and Other Assessments

8.1. Assessment Frequency and Circumstances requiring Assessment

The Certification Authority will implement audits whenever required.

8.2. Identity and Qualifications of Assessor

JPNIC will have the Certification Authority compliance audit implemented by an assessor who is knowledgeable of the certification practices selected by the trustee in charge.

8.3. Relationship between the Assessor and the Entity Assessed

JPNIC will select the assessor from among personnel excluding key persons relating to the Certification Authority certification practices.

8.4. Items covered by the Assessment

The Certification Authority compliance audit will assess whether the management of the Certification Authority strictly complies with this CPS and other related stipulations.

Further, in situations where the trustee in charge determines it necessary, audits will be implemented according to audit purposes specified by the trustee in charge.

Note that JPNIC has the authority to conduct audits of local RAs.

8.5. Measures taken in Event of Unsatisfactory Results

For items indicated in the audit report, the Certification Authority trustee in charge will decide the measures. For the specified items, the trustee in charge will give direction including measures for solving the problems to the JPNIC Certification Authority manager responsible, based on the latest trends in security technology. The response measures implemented will be reported to the trustee in charge, and will be assessed and confirmed in the next audit. In the situation where a response is not made to the unsatisfactory items discovered by the assessment, penalties determined beforehand by the trustee in charge will be applied.

8.6. Assessment Result Information Exchange

Reporting of the assessment result will be carried out by the assessor to the trustee in charge. Except in situations where the Certification Authority is legally required to make a disclosure, the assessment results will not be disclosed outside the organization.

Note that the JPNIC Certification Authority manager in charge has a responsibility to store and administer the audit reports for a period of at least 5 years.

9. Problems relating to Other Practices and Legal Problems

9.1. Fees

The issuing fees, updating fees, and usage fees relating to the certificates issued by the Certification Authority will be determined separately and notified beforehand to individuals and entities concerned.

9.2. Financial Liability

Not stipulated

9.3. Information Confidentiality

9.3.1. Scope of Confidential Information

Information retained by the Certification Authority will be treated as confidential information, with the exception of the information determined for disclosure in “2.2. Certification Information Disclosure” in this CPS, information explicitly disclosed as part of the CPS, information disclosed on the Website, reasons for certificate revocation and other detailed information relating to certificate revocation.

The private keys of certificate subjects are information that should be treated as confidential information by the certificate subject.

9.3.2. Information Outside the Scope of Confidential Information

Information determined for disclosure in this CPS, information explicitly disclosed as part of the CPS, information disclosed on the Website, and CRLs including information about the Certification Authority as the certificate issuer and the revocation date are not treated as confidential information. In addition, information satisfying the following conditions will not be treated as confidential information.

- Information that has become known through no negligence on the part of JPNIC.
- Information that has been provided to JPNIC from another source with no confidential restrictions attached.
- Information that has been independently developed by JPNIC.
- Information that has been confirmed by persons or organizations related to the subject of the released information.

9.3.3. Liability for Protecting Confidential Information

Concerning the information handled by the Certification Authority, in the situation where a request is received for information disclosure based on the legal authority of an investigative agency or court, JPNIC can disclose the information to the legal enforcing institution according to law. Further, regarding the information handled by the Certification Authority, in the case where an optional disclosure request is received from a court, lawyer, or other person with legal authority concerning arbitration, litigation, mediation, and other legal, judicial, or administrative processes, JPNIC can disclose the relevant information relating to the request. Additionally, concerning information received from maintainer administrators relating to the certificate subject administered by the maintainer administrator, in the situation where a request is received that violates or has a danger of violating the subject's rights or interests, the Certification Authority will confirm the correct identity of the maintainer administrator and the relationship with the disclosure request subject information. The Certification Authority can then disclose the information received from the maintainer administrator concerning the certification subject and the information described in the certificate.

In the situation where a part of the practices are commissioned, the JPNIC Certification Authority may disclose confidential information to the commissioned entity. However, the commissioning agreement incorporates an obligation to maintain the confidentiality of the information.

With the exceptions of the situations mentioned previously, the JPNIC Certification Authority will not disclose confidential information. In the case where confidential information is leaked, the liability will be borne by the person leaking the information.

Note that handling concerning the protection of personal data is specified in "9.4. Protection of Personal Data Privacy" in this CPS.

9.4. Protection of Personal Data Privacy

9.4.1. Privacy Policy

The Certification Authority recognizes the importance of personal data protection. In addition to handling personal data in the same way as “9.3.3. Liability for Protecting Confidential Information” in this CPS, the following policy is strictly observed.

- (1) An administrator responsible will be appointed to carry out appropriate administration of personal data.
- (2) In the situation where personal data is collected, the purpose for collecting the data will be notified, and collection will be conducted only of information that falls within the necessary scope of purpose using legal and fair means.
- (3) Personal data received through submission by certificate subjects will only be used for the following purposes:
 - To allow smooth operation of IP address administration practices
 - To allow fulfillment of responsibilities regarding certification services for certificates
 - For other purposes relating to certification practices
- (4) With the exception of situations where the agreement of the certificate subject has been received or in cases when legally obligated, personal data will not be disclosed to third parties apart from commissioned practices entities. When disclosing personal data to commissioned practices entities, the commissioned practices entities concerned will be obliged to follow the same conditions as this document.
- (5) The personal data administrator responsible for the personal data will strive to protect the personal data using appropriate security measures to prevent improper access, loss, corruption, alterations, or leaks.
- (6) In situations where requests are received for disclosure of personal data from the certificate subjects themselves, in order to prevent disclosure of personal data to third parties JPNIC will only disclose the certificate subject personal data stored in the JPNIC Certification Authority to the subject themselves after confirming the identity of the subject. Further, in the situation where there is an error or changes in the certificate subject personal data, incorrect data or old information will be swiftly revised or deleted over the logical range based on the notification received from the certificate subject. In a situation where the certificate subject requests disclosure from the JPNIC Certification Authority, the JPNIC Certification Authority will carry out the application following the specified method.

- (7) The JPNIC Certification Authority will implement education activities relating to personal data protection for employees carrying out the certification practices.
- (8) Regarding the personal data of certificate subjects, in addition to strictly observing the applicable laws and regulations, the personal data protection policy will be revised whenever necessary for improvement to maintain appropriate personal data protection.

9.4.2. Information treated as Privacy

Not stipulated

9.4.3. Information not considered as Privacy

Not stipulated

9.4.4. Liability for Protecting Personal Data

JPNIC Certification Authority will bear liability for the protection of personal data according to “9.4.1. Privacy Policy” in this CPS.

9.4.5. Notification and Agreement to Individuals relating to Use of Personal Data

Not stipulated

9.4.6. Disclosure based on Judicial Procedures and Administrative Procedures

Not stipulated

9.4.7. Other Information Disclosure Situations

Not stipulated

9.5. Intellectual Property Rights

Providing there has been no particular agreement made, intellectual property rights will be treated as follows:

- Certificates and CRLs issued by the JPNIC Certification Authority are the property of JPNIC.
- This CPS is the property of JPNIC.
- The JPNIC Certification Authority private key and public key is the property of JPNIC.
- Software, hardware, and other documents and information loaned from the JPNIC Certification Authority are the property of JPNIC.

9.6. Representation Warranties

9.6.1. Issuing Authority Representation Warranty

The JPNIC Issuing Authority will fulfill the following obligations concerning the performance of the JPNIC Issuing Authority practices:

- Secure generation and administration of JPNIC Issuing Authority certificate signing keys
- Correct certificate issue and revocation administration following requests from the JPNIC Registration Authority.
- JPNIC Issuing Authority system operation audit and operation
- CRL issue and disclosure
- Repository maintenance and administration
- Receipt of questions relating to this CPS during the reception opening times.

9.6.2. Registration Authority Representation Warranty

The JPNIC Registration Authority will fulfill the following obligations regarding the performance of the JPNIC Registration Authority practices:

- Installation and operation of a secure environment for registration terminals
- Correct information transfer to the JPNIC Issuing Authority of applications for certificate issuing and revocation.
- Swift information transfer to the JPNIC Issuing Authority during operation times for certificate revocation applications.

9.6.3. Local Registration Authority Representation Warranty

The Local Registration Authority will fulfill the following obligations regarding the performance of the Local Registration Authority practices:

- Verification that the certificate subject and the certificate subscriber are the same.
- Correct application information transfer to the JPNIC Registration Authority.
- Object registrant education for certificate use.
- Precise certificate distribution to the correct certificate subscriber
- Appropriate confirmation of certificate revocation
- Strict observance of other operations conforming with the agreement with JPNIC.

9.6.4. Subject Representation Warranty

The certificate subject will fulfill the following obligations regarding the holding of the certificate:

- Understanding and agreement with this CPS and other documentation (such as certificate subject agreements) shown by the Certification Authority.
- Obligations stipulated in “4.5.1. Subject Private Key and Certificate Use” in this CPS.

9.6.5. Relying Party Representation Warranty

The certificate relying party will fulfill the obligations stipulated in “4.5.2. Relying Party Public Key and Certificate Use” in this CPS.

9.6.6. Other Related Person Representation Warranty

Not stipulated

9.7. Limitations of Warranty

JPNIC will not bear liability for any indirect damages, special damages, accompanying damages and secondary damages relating to the warranty specified in “9.6.1. Issuing Authority Representation Warranty” together with “9.6.2. Registration Authority Representation Warranty” in this CPS.

9.8. Limitations of Liability

Concerning the contents of “9.6.1. Issuing Authority Representation Warranty” together with “9.6.2. Registration Authority Representation Warranty” in this CPS, JPNIC will not bear liability in the following situations:

- All damages occurring due to illegal actions, improper use, or negligence not caused by JPNIC.
- Damages occurring due to negligence of the Local RA or certificate subject in fulfilling their obligations.
- Damages occurring due to Local RA or certificate subject computer terminal software defects, problems, or other actions themselves.
- Damages caused by information disclosed in certificates and CRLs for reasons that can not be attributed to JPNIC.
- All damages caused by conditions where normal communications cannot be carried out for reasons that can not be attributed to JPNIC.
- Damages caused by improvement in hardware or software encryption algorithms that are not possible to be foreseen at the current time.
- All damages caused by suspension of Certification Authority practices due to acts of God, earthquakes, volcanic eruptions, fires, tidal waves, water damage, lightning, wars, riots, terrorism, and other irresistible forces.
- Damage caused by practices carried out by Local RA such as in individual authentication procedures for certificate issue applications.

9.9. Indemnity

At the point of time that the certificate issued by the Certification Authority is applied for, received, and trusted, damage liability and protection liability is created for JPNIC regarding the certificate subject and the relying party. Among the liability phenomena covered will be mistakes, negligent actions, various actions, delays in implementation, and non-fulfillment caused by the certificate subscriber not supplying the latest and correct information to the Certification Authority when applying for the certificate, resulting in various liabilities, loss, damage, and litigation, and any kind of financial burden. In addition, certificate subject and relying party actions, negligent actions, various actions and non-fulfillment resulting in various liabilities, loss, damage, and litigation, and any kind of financial burden will also be covered.

9.10. Periods of Validity and Termination

9.10.1. Periods of Validity

Documents including this CPS, contracts, and agreements are valid from the time they are issued based on appropriate approved procedures until the time they are amended based on appropriate approved procedures.

9.10.2. Termination

In the situation where all or parts of documentation including this CPS, contracts, and other agreements become invalid, or if specified conditions make the documents invalid for particular related persons, the parts concerned will be terminated.

9.10.3. Effect of Termination and Effect Continuation

Even in the situation where changes or terminations occur in this CPS, contracts, or agreements, the Certification Authority will endeavor to continue taking responsibility for the agreed items.

9.11. Individual Notification and Contact between Related Persons

Not stipulated

9.12. Amendments

9.12.1. Amendment Procedure

In the situation where it becomes necessary to amend this CPS over an extent that will not radically influence the certificate policy, warranties and obligations, the Certification Authority may amend this CPS whenever necessary without giving prior notice to certificate subjects and relying parties. Note that in the situation where no objections are received during the period between the amendment notification and the amendment becoming valid, this will be taken to signify agreement with the amendment. Related persons who do not agree with the amendment should immediately stop using the certificates issued by the Certification Authority.

9.12.2. Notification Method and Period

The Certification Authority will give notification of the amendment to certificate subjects and related persons by disclosing the amended CPS together with the amendment history on the repository more than 10 working days before the amendment is due to become valid.

9.12.3. Situation where Object Identifier must be Changed

Not stipulated

9.13. Dispute Resolution Procedures

For disputes arising relating to certificates issued by the Certification Authority, in the situation where legal means such as litigation or arbitration are to be used to solve the dispute this fact should be notified to JPNIC beforehand. All parties concerned agree that the arbitration and court location will be within the Tokyo metropolitan wards under the exclusive jurisdiction of a dispute handling institution. Further, regarding the situation where questions arise about items not determined in this CPS or in agreements, or about the interpretation of the documentation, all parties will resolve the issues through sincere discussions.

9.14. Governing Law

Regardless of the location of the Certification Authority, certificate subject, or relying party, Japanese laws will apply regarding the interpretation of this CPS, the validity, and disputes relating to the issue of certificates by the Certification Authority.

9.15. Compliance with Applicable Laws

The Certification Authority will strictly observe the various export restrictions, and will handle cryptographic hardware and software.

9.16. Miscellaneous Regulations

9.16.1. Entire Agreement

The agreed items in this CPS, contracts and agreements will have priority over all other agreed items until amended or terminated.

9.16.2. Transfer of Rights

Not stipulated

9.16.3. Severability

In this CPS, certificate subject agreements, and agreements provided by the Certification Authority, even if one part of the provisions is invalid, the other provisions described in the document concerned will continue to remain valid.

9.16.4. Enforcement

Not stipulated

9.17. Other Provisions

Not stipulated