経済産業省委託調査

IP アドレス
認証局のあり方に関する
調査報告書

2003 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

インターネットは､かつてはネットワークの相互接続のための実験ネットワークであった。しかしその実用性と規模拡張性の恩恵により、現在では商業組織・学校・政府組織・任意団体・個人等様々な目的の多様なネットワークサービスがインターネットを用いて運用されるに至っている。企業間の取引や e-Japan 戦略に代表される政府の取り組み、インターネットを利用したソフトウェアの開発など、我々の生活に欠かせないインフラストラクチャ（生活基盤）の側面を持つネットワークになりつつある。

水道、電気、ガスといった既存のインフラストラクチャで共有される「資源」が存在するように、インターネットにはネットワーク資源と呼ばれる資源が存在する。ネットワーク資源とは、IP アドレスや経路情報の交換に使われる AS 番号、ドメイン名といった識別子で、インターネットレジストリによって管理されている。ネットワーク資源の管理は、インターネットの運用だけでなくインターネットを利用する通信サービスにも影響する。例えば、他の組織が登録したネットワーク資源を使って不正な通信サービスが提供された場合、本来、登録されていた組織が不正行為を行ったとみなされる可能性がある。

一方、APNIC や RIPE NCC といったインターネットレジストリでは、登録情報の保護をすでに実施している。ネットワーク資源を利用する組織は、登録内容だけでなく登録情報を書き換える際の認証情報を登録する。そこで使われる認証方式は、電子メールの送信者といった偽造可能な情報をもとにしたものではなく、公開鍵暗号を用いた強い方式である。

他のインターネットレジストリの状況を鑑みても、インターネットレジストリにおける登録情報の保護、延いてはネットワーク資源の不正利用を防止する方策を検討することは急務である。

この報告書では、日本のインターネットレジストリである JPNIC の役割を述べ、登録情報の利用上の脅威について述べる。セキュリティの機能には PKI（Public-Key Infrastructure - 公開鍵基盤）を適用し、安全性が要求される業務の運用要件について述べる。また PKI は登録情報の応用の可能性を広げるため、その可能性についても述べる。

本年度の調査研究は、来年度以降に行う認証業務立ち上げのための基本調査である。来年度以降では、この調査結果を元に認証業務の具体的な要件事項を取り決め、事業を立ち上げるための活動を行う予定である。

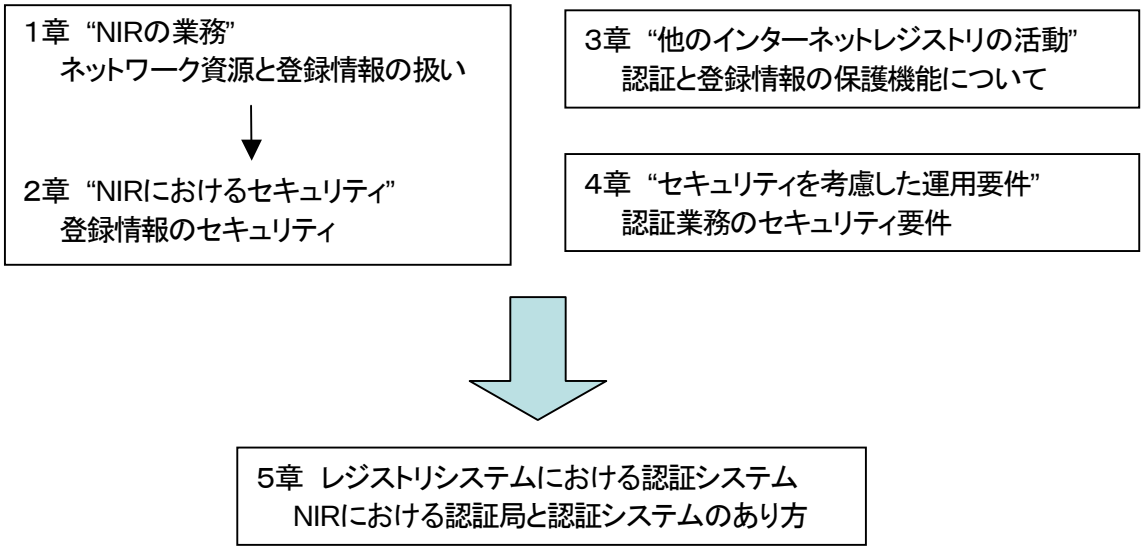
◇

本研究では、日本のインターネットレジストリにおける認証局のあり方について調査を行った。認証局のあり方を考慮するにあたり、以下の調査項目を挙げた。

- NIR におけるネットワーク資源と登録情報の扱い
- 登録情報を扱う際のセキュリティ要件
- 他のインターネットレジストリの認証および登録情報の保護機能
- セキュリティを考慮した運用要件
- レジストリシステムにおける認証システム

これらの項目の調査を通じて、機能的要件とセキュリティ要件の二つの面から、NIR における IP アドレス認証局のあり方を明らかにする。最後に IP アドレス認証局のあり方を元に、得られた知見と今後どのような活動が行われるべきかを述べる。

各章の関係を以下に示す。



第１章および第２章で、NIR の登録情報の扱いとその安全性について述べる。第３章では他のインターネットレジストリにおける認証や登録情報の保護について述べ、第４章では認証業務の運用要件として、認証業務の認定基準を基にした調査結果を述べる。第５章では各章の調査結果を受けて、NIR における認証局と認証システムのあり方についてまとめる。最後の第 6 章にて本報告書の内容をまとめる。

第 1 章　NIR とは

内容

- インターネットレジストリの役割
  - 権限委譲と階層構造
  - IP アドレスの管理
  - NIR の役割
  - 主要なインターネットレジストリ

1. NIR とは

1.1. インターネットレジストリとは

インターネットとは、米国防総省の高等研究計画局（ARPA）が始めた分散型コンピューターネットワークの研究プロジェクトである ARPAnet に起源を発する国際的な相互接続を元にした、世界規模のコンピューターネットワークである。

当初は電子メールを始めとした、文字情報を伝えるアプリケーションの利用が主であり、研究者同士の情報交換のために使われていたが、ウェブの登場以来、画像情報さらには動画情報交換のためにも使われるようになり、高速化と広帯域か進められた現在では、世界規模の情報通信インフラストラクチャとして広範囲の利用が行なわれている。

インターネットの特徴は、全体を統括するコンピュータというものがなく、多くのサーバコンピューターが全体から見ると少しずつの情報を保持、提供し、互いに補完しあうことで巨大なネットワーク構造を維持していることがあげられる。

このような構造を支える様々なプロトコルの基本となるものが IP、インターネットプロトコルである。IP はいくつかの要素から構成される、IP アドレス、ドメイン名、ポート番号、経路制御などであり、これらの情報はリソース、資源と呼ばれている。中でも IP アドレス、ドメイン名、ポート番号、AS 番号（Autonomous System Number - 自律システムの識別番号）のことを総称してアドレス資源と呼ぶ。

アドレス資源はインターネット運用に関する共通の資源であり、ネットワーク全体を通して管理される必要がある。このアドレス資源の管理を任されているのが、インターネットレジストリ（IR：Internet Registry）である。

インターネットレジストリの構成はインターネットの標準規格を定めた RFC で定義されている。この文書によると、インターネットレジストリは階層構造をもって構築されている。

全インターネットを管理する組織として IANA（Internet Assigned Numbers Authority）が存在し、IP アドレス、ドメイン名、AS 番号などについては下部インターネットレジストリに権限委譲されるといった構造により管理体系が構築されている。

この階層には以下の組織が配置されている。

- IANA
- RIR（Regional Internet Registry - 地域インターネットレジストリ）
- NIR（National Internet Registry - 国別インターネットレジストリ）
- LIR（Local Internet Registry - ローカルインターネットレジストリ）
- ISP（Internet Service Provider - インターネットサービスプロバイダ）

上位組織から下部組織に保有するリソース（アドレス資源）の一部が委譲される、これを順々に繰り返す構造になる。

インターネットレジストリの保有するデータベースの維持管理はインターネットの運用にきわめて重要な業務といえる。

本報告書では、インターネットレジストリの管理する各アドレス資源をネットワーク資源とよぶ。ネットワーク資源はインターネット共通の資産であることから、その健全な運用を維持する働きが求められる。

1.1. 権限委譲の一例

ここでは IP アドレスを例にとって、アドレス資源に関する権限委譲の仕組みを概説する。

すべての IP アドレスは IANA の管理下にある。この中からアドレスブロックを各 RIR に割り振る。RIR は割り振られたアドレスブロックを再分割して、またはそのまま NIR に割り振る。NIR は同様の割り振りを LIR に対して行う。LIR から ISP（実態が同じ LIR である場合もある）へ、さらに割り振りが行われ、最終的に ISP がエンドユーザにアドレスの割り当てを行う。

このように、実際の利用者にアドレスを配布することは割り当て（Assignment）と呼ばれ、割り当てを行う事業者等にアドレスを配布することを、割り振り（Allocation）と区別して呼ばれる。アドレスブロックの割り振りを行うということは、そのアドレスブロックの利用（割り当て）権限を委譲することを意味する。

例として官邸オフィシャルサイト www.kantei.go.jp の IP アドレスがどのように割

り当てられているのかを示したものが表 1 である。

表 1　IP アドレス割り当ての例

役割	IP アドレス	名称	所有者（責任者）
RIR	202.0.0.0/8	APNIC-AP	APNIC
NIR	202.232.0.0/15	JPNIC-NET-JP	JPNIC
LIR（ISP）	202.232.190.0/24	SUBA-006-AJ0	IIJ Internet
EU	202.232.190.64/26	KANTEI2	Cabinet Office
HOST	202.232.190.90/32	www.kantei.go.jp	Cabinet Office

表 1 の IP アドレスの / 以降の数値はアドレスブロックの分割位置を示しており、この数値が大きくなるほど、アドレスブロックがより細かく分割されることを意味する。従って表中の下の行ほど、割り振りもしくは割り当てが可能なアドレスブロックが小さくなる。この場合の各ネットワークブロックに存在しうるホスト数は表 2 となる。

表 2　ネットワークブロックあたりのホスト数

所有組織	ネットワークブロック	ブロック中の最大ホスト数
RIR	/8	16581373
NIR	/15	130048
LIR	/24	254
EU	/26	62
HOST	/32	1

1.2. インターネットレジストリの階層構造

図 1 は IP アドレス割り振りに関するインターネットレジストリの関連を示している（RIR にはこの他に LACNIC、ArfiNIC が存在する）。

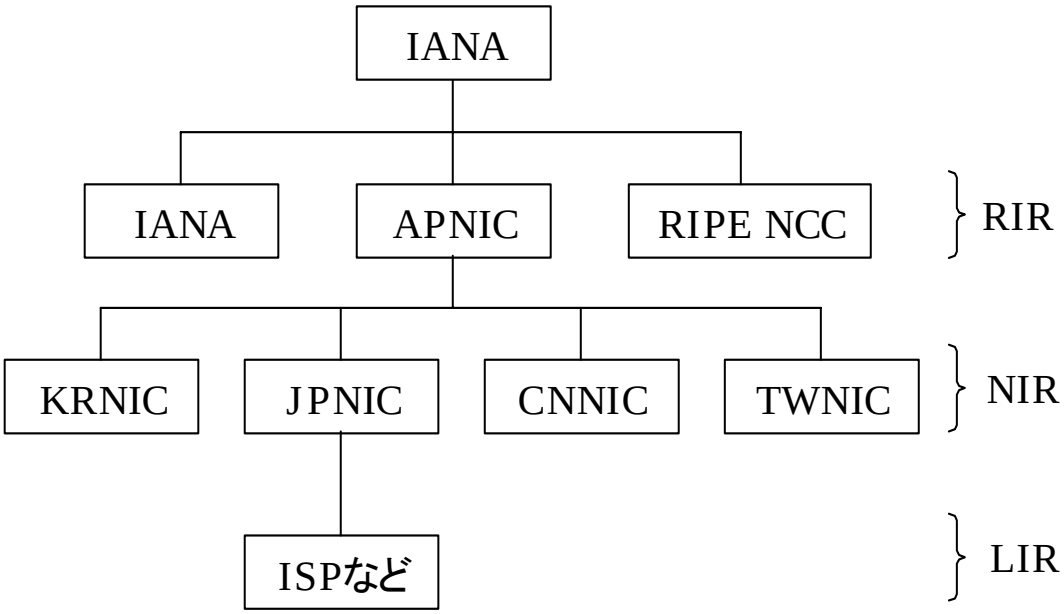


図 1　IP アドレス割り振りに関するインターネットレジストリの関連

図 1 中の各 RIR の正式名称を以下に示す。

- APNIC - Asia Pacific Network Information Centre
- ARIN - American Registry for Internet Numbers
- RIPE NCC - Réseaux　IP　Européens　Network Coordination Centre

1.3. IP アドレスの割り振り/割り当てスキーム

IP アドレスの割り当ては、IANA を頂点とする階層構造によって行われている。IANA からは各 RIR へアドレスブロックが割り当てられ、各 RIR は、割り振りを受けたアドレスブロックをさらに分割して NIR、又は LIR に割り振りを行う。

各 RIR に割り振られたアドレスブロックを表 3 に示す。

表 3　RIR へのアドレスブロックの割り当て

RIR	アドレスブロック
ARIN	残りの全て

RIPE NCC	62.0.0.0/8 164.0.0.0/8 192.16.192.0/24 192.164.0.0/16 193.0.0.0/8 194.0.0.0/8 195.0.0.0/8
APNIC	61.0.0.0/8 169.208.0.0/16 169.208.0.0/16 202.0.0.0/8 203.0.0.0/8 210.0.0.0/8 211.0.0.0/8 212.0.0.0/8 213.0.0.0/8

また、2002 年までの割り振りずみ IP アドレス数を表 4 に示す[1]。

表 4　2002 年時割り振り済み IP アドレス数

RIR	割り振り IPv4 アドレス
ARIN	108,210,000
RIPE NCC	80,866,000
APNIC	80,360,000
LACNIC	3,020,000

アドレス割り振りを規定する文書と発行元を表 5 に示す。

表 5 アドレス割り振り関連文書リスト

規定内容	文書名	発行団体
国際的 IP アドレス割り振り	Internet Registry IP Allocation Guidelines	IETF（RIR 共著）

[1] http://www.potaroo.net/iepg/november2002/rir.pdf より算出

太平洋地域 IP アドレス割り振り	Policies for address space management in the Asia Pacific region	APNIC
日本における IP アドレス割り振り	JPNIC におけるアドレス空間管理ポリシー	JPNIC

1.3.1. 国際的な IP アドレス管理

国際的な IP アドレス管理の枠組みについては“Guidelines for Management of IP Address Space”[2]に初めて、その概要が述べられた。この文書は “IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status”[3] の実現とネットワーク番号空間の割り振りと割り当てに関してのプランを提案するものであり、提案の項目は以下の三つである。

- 分散した地域レジストリの資格
- インターネットレジストリによるネットワーク番号空間の割り振り
- ネットワーク番号の割り当て

地域レジストリについては、「ヨーロッパ、北米、中南米や太平洋地域のインターネットの成長と成熟を考えると、登録機能をこれら各地域に一つの組織に委託することが望ましい。」としている。現在はヨーロッパに RIPE NCC、北米に ARIN、中南米に LACNIC 太平洋地域に APNIC と計画通りに RIR が立ち上がっている。

ネットワーク番号空間については、未割り当て（1992 年当時）クラス C アドレスブロックのうち８つを各地域に割り当てることが示されていたが、現在はそれを上回る数のアドレスブロックが割り当てられている。クラス A、クラス B の割り当てについても方策が示されているが、これも現在の状況は大きく異なり、この文書での懸念が表明されているアドレス空間枯渇問題は深刻になっている。

---

[2] RFC1466, “Guidelines for Management of IP Address Space”, http://www.ietf.org/rfc/rfc1466.txt

[3] RFC1174, “IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status”, http://www.ietf.org/rfc/rfc1174.txt

その後、“Internet Registry IP Allocation Guidelines”[4]により、RFC 1466 が更新された。この文書ではクラス A、B、C アドレスブロックの割り当てに関するインターネットレジストリと RIR の役割について述べられていたが、RFC 2050 では、世界的なアドレス枯渇問題に対応すべく、CIDR（Classless Inter-Domain Routing）の導入など、アドレスの節約を念頭においたアドレス空間の割り振りと割り当てについて述べている。

ISP レベルでは、一次プロバイダから二次プロバイダへ、二次プロバイダから三次プロバイダへと、インターネットレジストリの枠組みを超えてアドレスブロックの割り振りを行う場合があり、このような場合は従来のクラスフルアドレスブロックでは、使われないアドレスが過剰に発生してしまう。このため CIDR を用いて、必要とする最小のアドレスブロックのみを割り振るという政策がとられることになった。

1.3.2. 日本における IP アドレス管理

日本の NIR である JPNIC は APNIC からアドレスブロックの割り振りを受けている。

このポリシーについては "Policies for address space management in the Asia Pacific region" [5]に述べられている。

この文書で述べられているポリシーは APNIC 以下の NIR、LIR に関しても継承して適用されるため、JPNIC においても基本的にこの文書に従っている。

この文書を受けて作成されたものが「JPNIC におけるアドレス空間管理ポリシー」である。ここでは、基本ポリシーが以下のように定義される。

「IANA はアジア太平洋地域への再分配用として APNIC にアドレス空間を割り振り、APNIC は NIR の一つである JPNIC に対し、日本国内のアドレス管理を委任している。そして、JPNIC は日本国内の LIR にアドレス空間割り振り審議を行い、同時にその LIR がエンドユーザに対して割り当てを行う権限の委任も行う。

LIR は JPNIC の指導のもとで、本文書に書かれたポリシーや手続きに従い、自分のメンバーや顧客にアドレス空間を割り当てる。」

---

[4] RFC 2050, “Internet Registry IP Allocation Guidelines”, http://www.ietf.org/rfc/rfc2050.txt

[5] "Policies for address space management in the Asia Pacific region", http://www.apnic.net/docs/add-manage-policy.html

またこの文書では（アドレスブロック）を、以下のように定義されている。

- 割り振り（allocated）

  割り振りアドレス空間とは、インターネットレジストリがさらに他に分配することを目的として、インターネットレジストリに対して分配されるアドレス空間である。

- 割り当て（assigned）

  割り当てアドレス空間とは、ISP やエンドユーザが運用しているインターネットインフラストラクチャ内での特定の利用を目的として、ISP やエンドユーザに対し委譲されたものである。

割り当ては、特定の文書化された目的に沿って行われねばならず、さらに他へ割り当てられるものではない。

JPNIC の割り振りを行っている対象となる LIR は、IP アドレス管理指定事業者（以下、IP 指定事業者）とよばれ、IP アドレス管理業務の委託を受ける。IP 指定事業者はエンドユーザや自組織のネットワークに対して、割り振られたアドレスブロックの中から割り当てを行う。

JPNIC の IP アドレスに関する４つの業務を表 6 に示す。

表 6　JPNIC の IP アドレス業務

業務	概要
審議による効率的な利用の確認	インターネットレジストリは、限られた資源であるアドレス資源を効率的に活用する責務を負っている。JPNIC ではこの責務を果たすために、アドレスの利用に関して、適切な審議を行った上で、割り振りを行っている。
APNIC への追加アドレス申請	RIR から NIR へは必要に応じてアドレスブロックの割り振りを行う。ネットワークの増加または減少を考慮したうえで、割り振り済みアドレスブロックの使用率の変化を予想し、将来的に不足することが考えられる場合には、前もって RIR つまり APNIC に追加のアドレスブロック割り振り

	申請を行う
データベースによる登録情報管理	これは IP アドレスの逆引きと呼ばれる、IP アドレスからホストネームを解決するサービスの提供のことで、JPNIC では、APNIC から管理を委譲された IP アドレスの逆引きネームサーバを関係する組織に協力を受け DNS の運用を行っている。
リストファイルの提供	JPNIC では資源割り当てに関するデータをリストにした 2 種類のファイル提供サービスを行っている。（1）IP アドレスリスト、このリストは同意書に記入の上、郵送で申請を行うことで入手できる。（2）AS 番号リスト、AS 番号とは BGP を利用した経路情報交換を行うために必要である。このファイルは JPNIC より AS 番号の割り当てをうけた組織のリストが載せられている。

以下に、審議による効率的な利用に関する詳細を述べる

- 審議とは

　APNIC は JPNIC や KRNIC などのアドレス管理を確認し、JPNIC は IP 指定事業者のアドレス管理を確認し、IP 指定事業者はユーザのアドレス利用計画を確認する。このように、IP アドレス管理を行うすべてのレジストリは、グローバル IP アドレスを下位ネットワークに割り当てる時、下位ネットワークがどのようにグローバル IP アドレスを使用していくのかを確認する作業を行う。つまり「審議」を行い、有限な資源であるグローバル IP アドレスが有効に使用されるようアドレス管理を行う。

　IP 指定事業者は、自身のインフラに割り当てを行う際、RFC2050、JPNIC ポリシーに基づいた有効利用を確認する必要がある。ユーザネットワークに割り当てを行う際、アサインメントウィンドウサイズ以下、以上に関わらず IP 指定事業者によって RFC2050、JPNIC ポリシーに基づいた有効利用を確認しなくてはならない。

- JPNIC 審議の目的とは

　JPNIC 審議は、IP 指定事業者からの割り振り申請時とアサインメントウィン

ドウサイズ以上の割り当て審議申請時に行う。

IP 指定事業者が RFC2050、JPNIC ポリシーに基づいたアドレス管理業務を習得し、自らで管理業務を遂行できるようになるための手助けをすることが目的である。

- アサインメントウィンドウサイズとは

アサインメントウィンドウとは、IP 指定事業者が JPNIC に割り当て審議申請を行なわずに割り当てができる最大のアドレス空間のことである。一般的に、アサインメンドウィンドウサイズが大きいほど、業務経験が豊富であると考えられる。

JPNIC では審議申請毎に、IP 指定事業者の業務熟達度を確認しており、その業務熟達度により、アサインメントウィンドウサイズの拡大や縮小が決定される。

アサインメントウィンドウサイズの更新は、平均月二回行われ、JPNIC の審議担当者で開かれる会議にて審議の上決定される。ただし、必要に応じて臨時に会議を開催し決定することもある。

1.4. NIR の業務

JPNIC は NIR として、アジア太平洋地域における RIR である APNIC からアドレスブロックの割り振りを受け、日本での IP アドレス管理を行っている。

本節では JPNIC の業務の概要を述べる。

1.4.1. IP アドレスの管理

IP アドレスの管理は割り振り/割り当て、返却プロセスが図 2 に示すように定義されている。

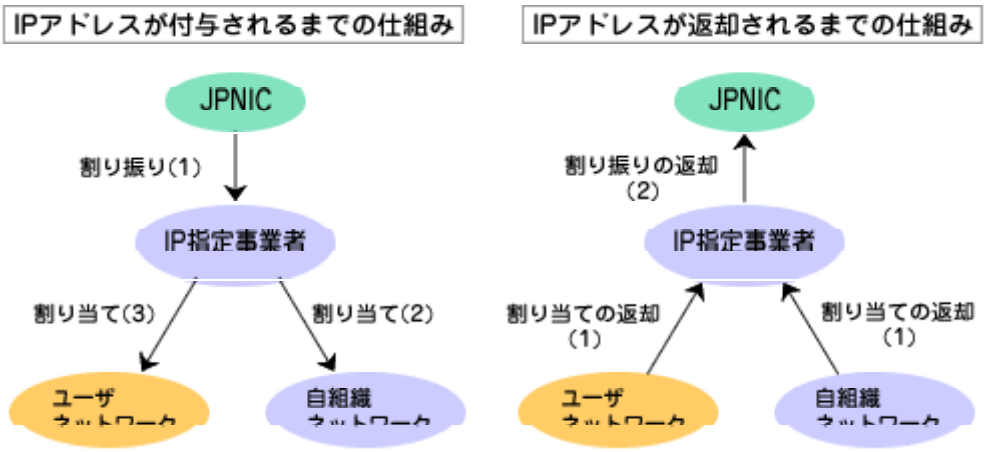


図 2　IP アドレスの割り振りから返却まで

JPNIC では IP アドレスに関する割り振り、返却に加えて以下の業務を行っている。

- 審議による効率的な利用の確認
- APNIC への追加アドレス申請
- データベースによる登録情報管理

IP アドレス管理の詳細については 1.3.2 節にて述べた。

1.4.2. AS 番号の管理

AS（Autonomous System - 自律システム）は、統一された運用ポリシーによって管

理されたネットワークの集まりであり、BGP のような外部経路制御プロトコルによる管理対象となる。通常、規模の大きい ISP のネットワークは、固有の AS を形成する。AS 番号はこの AS に割り当てられた識別番号である。

JPNIC では 2002 年 7 月より AS 番号の正式サービスを開始した。

管理業務として次の二つを行っている

- 登録申請審査
- AS 番号リストデータベースの保守

1.4.3. 登録情報の提供

IP アドレスに関する各種情報提供サービスとして以下の業務を行っている。

- whois データベース

  whois サービスは“NICNAME/WHOIS”[6]で定義されるディレクトリ問い合わせサービスのことで、元々は NIC に登録されたユーザのフルネーム、合衆国郵便アドレス、電話番号、ネットワークメールボックスを広報するものであった。

  JPNIC の whois サービスでは、以下の情報を提供している。

  - IP アドレスに関する情報（ネットワーク情報）
    IP アドレスがどの組織に割り当てられているか

  - AS 番号に関する情報（AS 情報）
    AS 番号がどの組織に割り当てられているか

  - 担当者に関する情報（個人情報）
    技術的な担当者や運用責任者の情報

  - JP ドメイン名に関する情報（ドメイン情報）
    ドメイン名がどの組織に登録されているか

  - ネームサーバホストに関する情報（ホスト情報）
    JP ドメイン名のネームサーバとして登録されているホストの情報

[6] RFC954, “NICNAME/WHOIS”, http://www.ietf.org/rfc/rfc0954.txt

- 逆引き DNS

JPNIC では、APNIC から管理を委譲された IP アドレスの逆引きネームサーバを運用している。JP ドメインのネームサーバの管理は（株）日本レジストリサービスで行っている。

この逆引き用ネームサーバ以下のものが設置されている。

① プライマリーネームサーバ

ns0.nic.ad.jp（JPNIC）

② セカンダリーネームサーバ（公式、whois の検索結果に準じる）

ns0.iij.ad.jp （株式会社インターネットイニシアティブ）
dns0.spin.ad.jp （ジェンズ株式会社）
ns.wide.ad.jp （WIDE Project）
ns-jp.sinet.ad.jp （国立情報学研究所）
ns-jp.nic.ad.jp（JPNIC）

1.4.4. IP アドレス管理指定事業者とは

IP アドレス管理指定事業者は、IP アドレスの割り当て業務およびそれに付随する業務の一部（以下では IP 割り当て管理業務とよぶ）を JPNIC から委託された事業者のことである。JPNIC は、JPNIC に対する要求の多様化に伴い、IP 指定事業者と協同して一般ユーザからの要求にこたえることを目的としている。

割り振り／割り当てを含む IP 割り当て管理業務を行うためには、JPNIC と IP アドレス管理指定事業者契約を締結し、IP 指定事業者になる必要がある。

1.5. 主要なインターネットレジストリ

NIR の業務は、NIR にネットワーク資源の割り振りを行っている RIR の業務に深く関係する。RIR には、北米、欧州、環太平洋、南米、アフリカのそれぞれの地域を担当する５つの組織がある。

以下に各地域インターネットレジストリについて概説する。

1.5.1. ICANN

ICANN は、Internet Corporation for Assigned Names and Numbers の略である。

インターネットにおける番号や名前に関する管理は、インターネットの普及とともに、IP アドレスやインターネットで用いられる論理名（FQDN）の不足、あるいは、各組織の経済的利害関係が発生している。したがって、インターネットにおける番号や名前に関して、国際的な観点から系統的に調整・管理を行うための組織が必要となってきた。当初、以下に述べる IANA の機能を、米国商務省が引き継ぐという提案が行われたが、米国政府という一国の利害を中心とする組織で、グローバルインターネットの名前や番号の問題を処理するのは、健全ではないという意見が、IETF を中心に主張され、ICANN が設立された。1996 年から 1997 年 6 月までの約 2 年間、インターネットのドメイン名の再編成を行う目的で活動した任意団体である IAHC（Internet Ad Hoc Committee） は、このような国際的管理調停組織の先行的な活動であったと言える。

ICANN は、非営利の会社組織であり、現在は米国政府との契約のもと、 IANA が実行している以下の業務の遂行を実現するための組織として存在する。

- IP アドレスの割り当て
- プロトコルパラメータの割り当て
  通信規約で決めるべきデータフォーマットや記述方法など
- ドメインネームシステム（DNS：Domain Name System）の管理
- ルートネームサーバの管理

現在、ICANN は、9 名の At-Large Director（世界の各エリアからの代表者）、9 名のサポート組織（SO; Supporting Organization）からの Directors（3 組織から各 3 名）、President/CEO の合計 19 名の Director により構成されている。 ICANN は、3 つのサポート組織（SO）を持ち、インターネットのポリシーや構造に関する評価検討を行っている。

- アドレスサポート組織（ASO: Address Supporting Organization）
  ASO は、IP アドレス空間の割り当てに関する管理運営に関係する課題を検討している。
- ドメイン名サポート組織 （DNSO: Domain Name Supporting Organization）
  DNSO は、ドメイン名の割り当てに関する管理運営に関係する課題を検討

している。

- プロトコルサポート組織（PSO: Protocol Supporting Organization）
  PSO は、インターネットプロトコルで使用される、プロトコルに関係する番号やパラメータの割り当てに関する管理運営に関係する課題を検討している[7]。

1.5.1.1. InterNIC

インターネット上で利用される IP アドレスやドメイン名などを割り当てる民間の非営利機関。ICANN/IANA の下部組織に当たる。InterNIC は、ヨーロッパを管轄する RIPE NCC、アジア・太平洋地域を管轄する APNIC と協力して管理を行っている。この 3 団体の下に各国 NIC がある（InterNIC は北中南米、アフリカ、その他の地域を統括している）。NIC のない地域では、APNIC などその地域を統括する NIC が業務を代行している。

1.5.1.2. IANA

IANA は、Internet Assigned Numbers Authority の略である。IANA は、米国 南カリフォルニア大学の ISI（University of Southern California, Information Sciences Institute）にあり、インターネットにおける番号 およびパラメータの管理を行っている。IANA の活動は、米国政府の 援助を受け、米国政府との契約に基づいて行われていた。しかし米国政府から独立した運用を行うことが国際的な責任において必要であるため、1999 年から ICANN の援助による IANA の活動が維持されるように変更された。

IANA は、当初、米国 DARPA（Defense Advanced Research Projects Agency） の資金援助をもとに運営を行い、その後 NSF（National Science Foundation）の資金援助を受けながらその運営を行ってきた。IANA の維持運営にあたって は、1998 年に他界した Jon Postel 博士の献身的な貢献に大きく依存していた。 IANA は、インターネットに関する IP アドレス空間の割り当てと管理、ドメイン 名の割り当てと管理、DNS システムの管理運営、TCP/IP プロトコル群で用いられる プロトコルで使用される番号やパラメータの管理を一元管理している。 DNS システムの管理には、世界中に 13 個あるルート DNS サーバシステムの管理運営も含まれている。

IP アドレスとドメイン名の割り当てと管理については、世界を 3 つの領域 に分け、

[7] http://rfc-jp.nic.ad.jp/what_is_ietf/ietf_section2.html

それぞれの領域で、IP アドレスとドメイン名の割り当て管理を行うという運用形態を取っている。欧州は RIPE、アジア太平洋は APNIC、北米およびその他の地域 は ARIN が、それぞれサービスを行っている[8]。

1.5.2. APNIC

アジア・太平洋地域の各国の NIR やインターネットサービスプロバイダに IP アドレスの割り振りを行う機関。ICANN/IANA の下部組織で、アジア・太平洋地域のインターネットレジストリと調整を行う機関でもある。

1.5.3. RIPE NCC

ヨーロッパやその周辺地域における各国の NIR やインターネットサービスプロバイダへの IP アドレスの割り当てを行う機関のことである。ヨーロッパのプロバイダが支払う会費で運営されている。ヨーロッパおよび周辺地域の NIC を統括する機関でもある。

RIPE の目的は欧州 IP ネットワークにまたがったオペレーションを行うために必要な管理業務と技術的な協調を提供することにある。特徴は以下のとおり。

- RIPE は技術情報の交換と、IP ネットワーク上の専門技術推進のためのフォーラムとして機能する。
- RIPE の関わるエリアは欧州である。
- 広域 IP ネットワークをオペレートするすべての組織は参加が奨励される。
- 欧州 IP ネットワークと他の大陸との相互接続を実施し、協調する。
- IP ネットワークに関する参加者のほかの活動に関するフォーカルポイントを提供する。
- RIPE により生成されるすべての文書を公開する。

[8] http://rfc-jp.nic.ad.jp/what_is_ietf/ietf_section2.html

1.5.4. ARIN

アメリカ大陸、サハラ砂漠以南のアフリカ大陸の各地域における IP アドレスの割り当て、管理を行う RIR である。

1980 年代、National Science Foundation 高速ネットワーク、通称 NSFNET は Advanced Research Project Agency 通称 ARPA、現 DARPA の広域ネットワーク、ARPANET に接続された。これが現在のインターネットの基礎と成った。

初期のころ、アドレス割り当て管理タスクは一個人、Jon Postel 氏よって行なわれていた。タスクが大きくなったため IANA が設立され、登録タスクをインターネットレジストリの機能として行うこととなった。

1993 年、インターネットの爆発的な成長にともない、米国政府と NSF は、商業的なインターネットサポートは米国の政府機関から切り離すべきだと決断した。このため、NSF は IP アドレスとドメイン名の登録と割り振りサービスを提供するために NSI（米ネットワークソリューションズ社）との協調の元、InterNIC と呼ばれるプロジェクトを開始した。

後にドメイン名の管理を IP アドレスの管理から切り離すというコンセンサスに至り、IP 登録サービスを独立した非営利企業として行うために 1997 年 10 月、ARIN が設立された。

1.5.5. LACNIC

ラテンアメリカおよびカリブ海沿岸地域を管轄するインターネットアドレスレジストリである。この地域の IP アドレス空間、AS 番号、逆引き、その他のリソースの管理を行うことを目的とている。

目標はラテンアメリカおよびカリビアンインターネットの進展と成長をサポートすると同世に、地域の視点から代表し促進することにある。

行動ガイドラインの一部として、非営利で公正かつ包括的サービスを提供する。LACNIC は民主的かつ非営利の組織で、運営委員はメンバーにより選ばれる。

LACNIC 自体は法的理由からウルグアイに置かれる。

1.5.6. AfriNIC

ICANN が行っていた IP アドレス割り振りを地域レジストリに役割委譲を行ってから、三つの RIR、つまり RIPE、APNIC、ARIN が運営されてきた。2001 年 4 月、ストックホルムで行なわれた会合で ICANN の運営委員は新しい RIR の確立を承認した。

それは、AfriNIC の名称で IP アドレス空間のような乏しいリソースの管理を行うことで、コミュニティ全体に長期の貢献を果たすように提唱されたものである。AfriNIC はアフリカ大陸における IP アドレスの管理をアフリカコミュニティのために行うように提案されたもので、現在は RIPE や ARIN から入手している IP アドレス空間を、将来的には AfriNIC が管理できるように考えられている。

1.6. まとめ

図 3 で示されるインターネットレジストリの階層構造の中に位置し、地域の統括管理を行う RIR の下に配置され、LIR に対するネットワーク資源の割り振りとその情報を保持する役割を持つ。

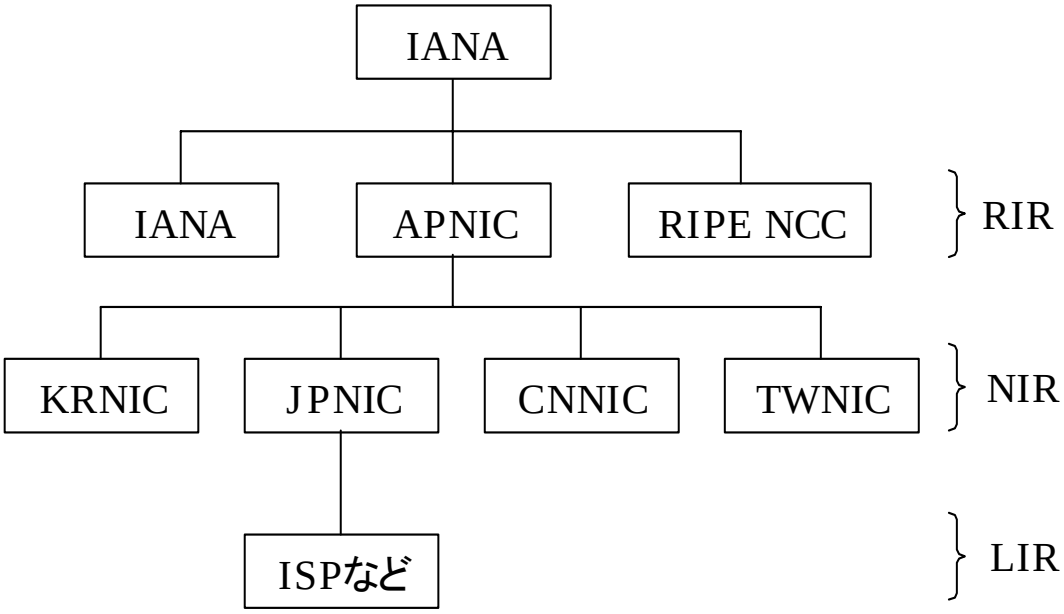


図 3　IP アドレス割り振りに関するインターネットレジストリの関連

その扱うネットワーク資源には、IP アドレス、AS 番号がある。ネットワーク資源に加え、インターネットレジストリが提供するアドレスの逆引き、whois システムは、インターネットの正常な運営に欠かすことの出来ないものである。

また NIR には、ネットワーク資源利用の効率性の維持、LIR および ISP の認定、データベースサービスの提供などの役割がある。

第 2 章　NIR におけるセキュリティ

内容

- 登録情報の利用上の脅威と保護
  - 登録情報
  - ネットワーク資源に対する脅威
  - 脅威の影響と保護
  - 権限委譲と PKI

2. NIR におけるセキュリティ

2.1. 登録情報利用上の脅威

インターネットレジストリに登録されている情報は様々な場面で利用される。これらの情報に対する操作には、情報の登録、参照、編集といったものがある。

これらの操作手段を提供するシステムに安全性を維持する機能がないと、通信路での不正な改ざん、第三者による不正な書き換え、盗聴などが容易に行われてしまう可能性がある。この状況はインターネットの利用の上で問題が起きる可能があるだけでなく、インターネットレジストリの登録管理業務の意義が問われる状況になりかねない。

ここでは、インターネットレジストリが管理している登録情報の種類とそれぞれに想定される脅威について述べる。

2.1.1. インターネットレジストリの登録情報

インターネットレジストリの登録情報は、ネットワークの管理者に連絡を取る際などに利用される。またネットワーク情報の変更の際にその申請者を認証するために使われたり、インシデントレスポンスのためにネットワーク情報の検索に使われたりする。

登録情報は主に whois システムや WWW を利用して閲覧される。インターネットレジストリが管理する登録情報は大きく分けて以下の４つである。

- IP アドレス空間情報
- 逆引きドメイン情報 (in-addr.arpa.)
- AS 情報
- コンタクト(人物)情報

RIPE NCC や APNIC、LACNIC といった RIR では、登録情報の管理の為に、RIPE で開発された Database Management System が利用されている。このシステムは情報をクラスとして定義し、そのインスタンス（実体）をオブジェクトと呼んでいる。クラスとして定義された情報は、インターネットコミュニティで必要とされている情報を網羅していると考えられるため、ここでは情報クラスについて述べる。

表 7　RIPE データベースシステムの情報クラス

カテゴリ	情報クラス名
IP アドレス空間情報	inetnum, inet6num, inet-rtr
AS 番号情報	as-block, as-set, aut-num
コンタクト(人物)情報	person, role, mntner, key-cert, irt

なお、逆引きドメイン情報は DNS を用いて提供されるので、ここでは詳細は述べない。

- IP アドレス空間情報

このカテゴリに含まれる情報クラスは inetnum, inet6num, inet-rtr である。

inetnum オブジェクトは IPv4 アドレス空間の割り当て及び割り振り情報を含む。

実際のデータは次のようになる（以下、データは　whois –h whois.ripe.net 193.0.0.203 のもの）。

```
inetnum:      193.0.0.0 - 193.0.1.255
netname:      RIPE-NCC
descr:        RIPE Network Coordination Centre
descr:        Amsterdam, Netherlands
country:      NL
admin-c:      DDL122-RIPE
tech-c:       OPS4-RIPE
status:       ASSIGNED PI
remarks:      used to be two different /24 inetnum objects
remarks:      until 19990305  (ripe-ncc & ripe-meeting)
mnt-by:       RIPE-NCC-MNT
mnt-lower:    RIPE-NCC-MNT
```

ルータは inet-rtr クラスで特定される。inet-rtr: 属性はルータを表す妥当な DNS 名である。alias 属性が提示されたならば、それはルータのカノニカル DNS 名である。local-as: 属性は、このルータによって所有もしくは操作される AS の AS 番号を特定する。

- AS 番号情報

このカテゴリに分類される情報クラスは as-block, as-set, aut-num がある。

as-block オブジェクトは AS 番号のレンジを委譲するために必要である。このオブジェクトは as-block: 属性によって特定される範囲内の aut-num オブジェクトの生成のための認可に使われる。

aut-num クラスのオブジェクトは、一つかつクリアに定義された外部経路ポリシーを持つ一つかそれ以上のオペレーターにより操作される IP ネットワークのグループを意味する、AS の表現のデータベースである。

このクラスのオブジェクトは経路制御ポリシーを特定するために使われる。aut-num: 属性はこのオブジェクトによってあらわされる AS 番号である。as-name: 属性は AS のシンボリック名である。

- コンタクト(人物)情報

このカテゴリに分類される情報クラスは person, role, mntner, key-cert, irt, がある。

person クラスのオブジェクトは技術または管理コンタクトに関する情報を含む。いったんオブジェクトが生成されると、person: 属性を変更することはできない。

irt オブジェクトは CSIRT の連絡先およびセキュリティ情報を表す。アドレス範囲に対するコンピュータやネットワークのインシデントの扱いに責任がある CSIRT を特定するために inetnum または inet6num オブジェクトから参照される。オブジェクトの名前は “IRT-“ で始めなければならない。

key-cert オブジェクトはサーバに格納される公開鍵のデータベースで、mntner オブジェクトの更新を実施する際の認可に使われる。現在は”OpenPGP Message Format[9]”に準拠した鍵だけがサポートされる。

RIPE データベース中のオブジェクトは mntner オブジェクトを使うことで保護される。このオブジェクトは、生成、削除、修正に必要な認証情報を特定する。このオブジェクトは自動的には生成されず、手動操作によって RIPE データベース管理業務に転送される。

[9] RFC2440, “OpenPGP Message Format”, http://www.ietf.org/rfc/rfc2440.txt

2.1.2. 登録情報に対する脅威

登録情報はインターネットレジストリに保持されるだけでなく、インターネットに関わるユーザや管理者によって参照される。参照情報の利用に関するリスクは表 8 に示すような脅威および原因によって引き起こされる。

表 8　登録情報に関するリスク

リスク	原因となる行為
不正なデータの保持	なりすまされた登録/更新/削除
	登録途中の書き換え
	古いデータの遺棄
不正なデータの提供	提供途中の書き換え
	なりすまされた情報提供
	提供不能行為
データの流出	権限の無い第三者による盗聴
	情報の露出

以下では、表 8 にあげたリスクが、現実のシステムにどのように現れているのか、について述べる。

調査の対象として、APNIC での IP アドレスの登録に存在する脅威、whois サービスによる情報提供に関わる脅威、JPNIC での IP アドレスの登録と更新に存在する脅威の三つをあげる。

2.1.2.1. APNIC での IP アドレスの登録に存在する脅威

APNIC に IP アドレス登録を要求する手順には、認証情報の登録において機密性を欠いているため、パスワードの盗聴による第三者による不正なアクセス権限の入手を始め、様々な脅威、それから生じるリスクが想定される。

この手続きは以下の手順で実施される[10]。

[10] “APNIC guidelines for IPv4 allocation and assignment requests”, http://ftp.apnic.net/apnic/drafts/apnic-draft-v4-guide.txt

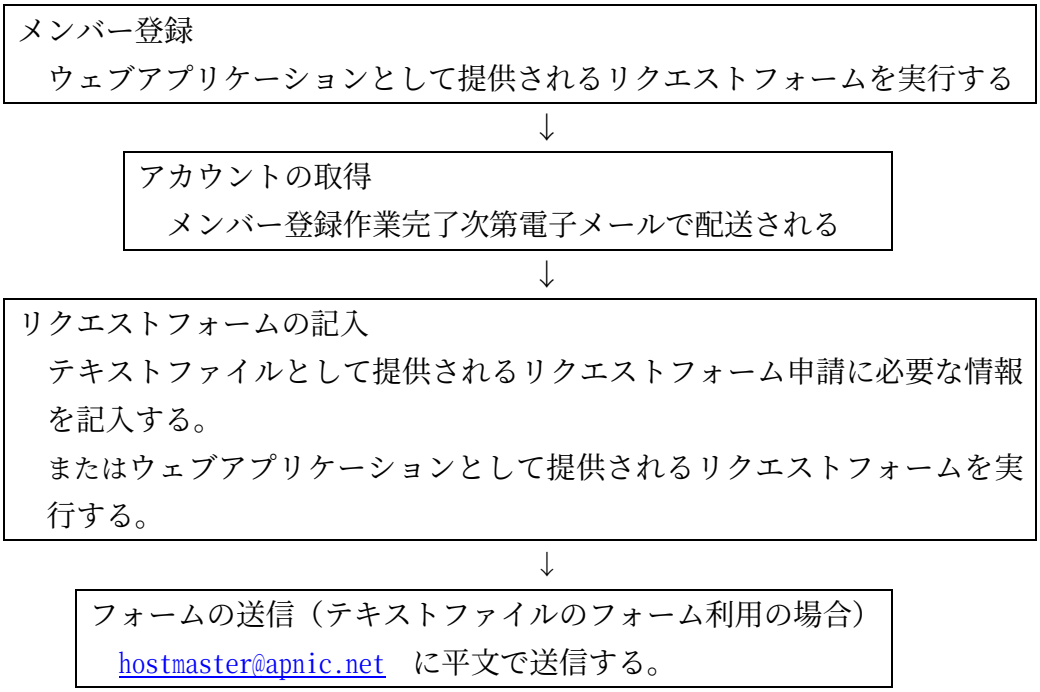


図 4　APNIC における IP アドレス登録プロセス

この手続きのうち、メンバー登録はウェブアプリケーションで行なわれるが、ここでパスワード登録を行うにも関わらず、保護されていないチャンネル経由で通信が行なわれている。

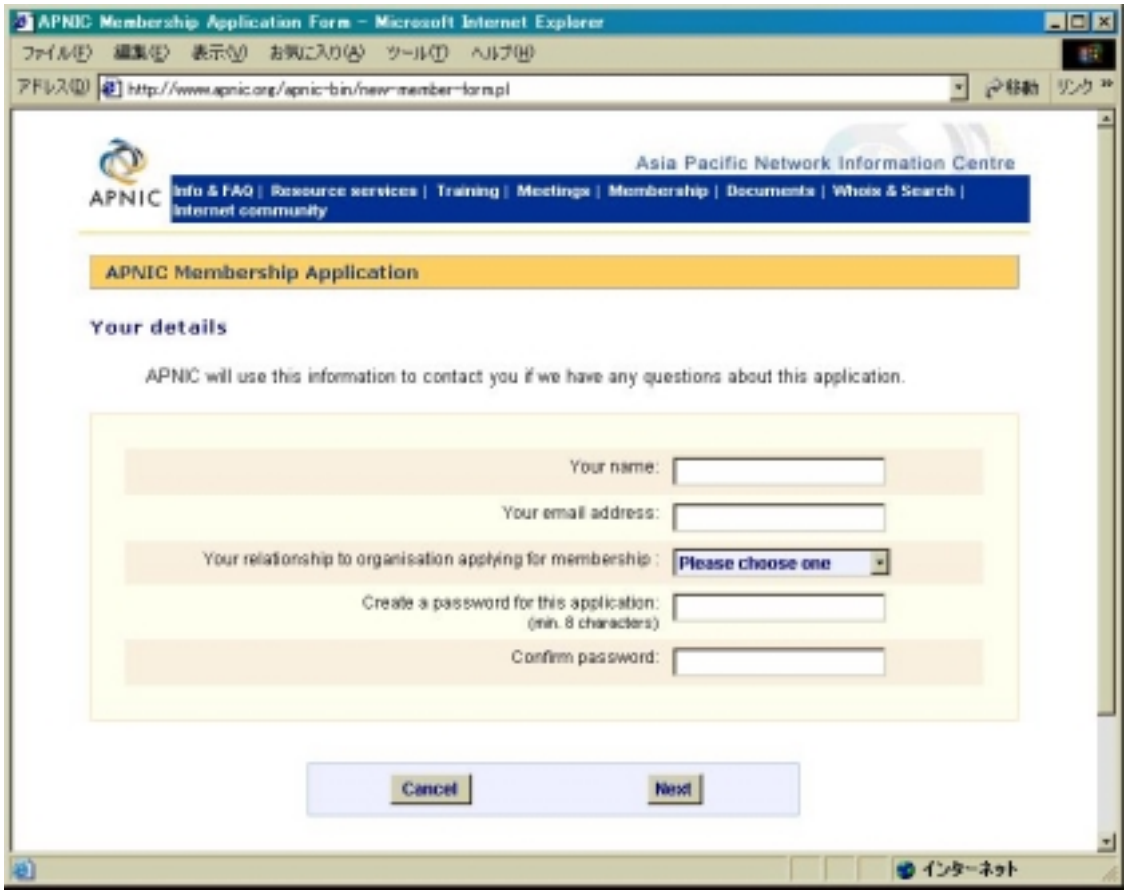


図 5　APNIC のメンバー登録リクエストフォームアプリケーション

APNIC の公開文書である” Policies for IPv4 address space management in the Asia Pacific region[11]”には次の記述があり、機密の保持およびセキュリティに関しての取り組みが行なわれていることがわかる。

セキュリティと機密性 APNIC は会員とその顧客の商業とインフラストラクチャ操作に関連する全ての情報の機密性を保護するためのシステムと業務を維持する。APNIC は全てのスタッフとエージェントの雇用が、そのような情報に関した機密性の明確な条件に基づいて行われることを保証する。 APNIC は APNIC　whois データベースに認可と検証メカニズムを提供する。このメカニズムを適用することは、それぞれのインターネットレジストリとエンドユーザの責任である。

[11] http://www.apnic.net/docs/policy/add-manage-policy.html

ここでは、登録業務に携わる全ての人員が機密性に関して認識を持つこと、システムにはセキュリティに考慮した機能が実装されること、その機能を実行することが宣言されていると考えられる。

しかし、セキュリティはシステムとして完全に機能していなければ意味をなさず、登録時の認証情報の漏えいが、以降のすべての操作における信頼性を損ねる要因となる。

2.1.2.2. whois サービスによる情報提供に関わる脅威

登録情報の利用は whois プロトコルを利用してレジストリデータベースを検索することになる。このプロトコルの仕様は次のようにきわめて単純なものである。

1. サービスホストに TCP ポート 43 で接続する。
2. <CRLF>で終了する一行のコマンド行を送信する。
3. コマンドラインに対応する情報を受け取る。
4. 出力が終わり次第、サーバは終了する。

プロトコル自体には認証、認可、機密性、完全性といったセキュリティ機能の指定はない。このようにセキュリティ機能に乏しいプロトコルを保護するためには、SSL や IPsec などのセキュリティ機能を実装するといったアプローチを取る手法があるが、そのような対策を施した whois サーバを提供しているインターネットレジストリは存在しない。

whois サーバに認証の仕組みがないということは、不正なデータの提供という脅威が存在するということである。この脅威に伴うリスクとして次のシナリオ実現の可能性が発生する。

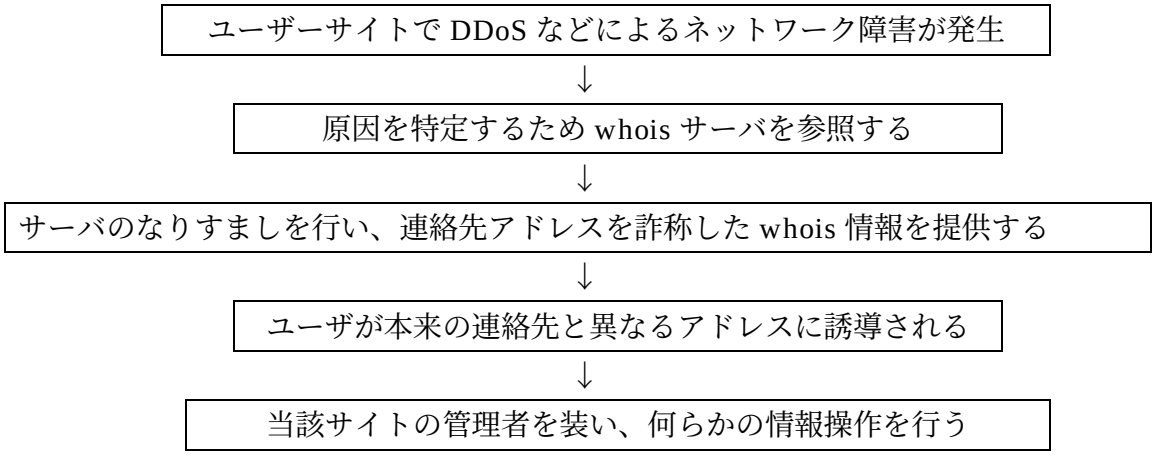


図 6　whois サーバのなりすまし行為

このようにしてなりすまし行為を行い、被害の拡大を図ることが出来る。

また、完全性の保証がないことから、man-in-the-middle 攻撃による情報の不正な書き換えを行うことができる。

また、whois データベース中の情報が現状を反映していないことがあり、情報を参照する価値が無くなっているという問題がある。

このような情報の陳腐化と、その影響は図 7 のように進展していくと考えられる。

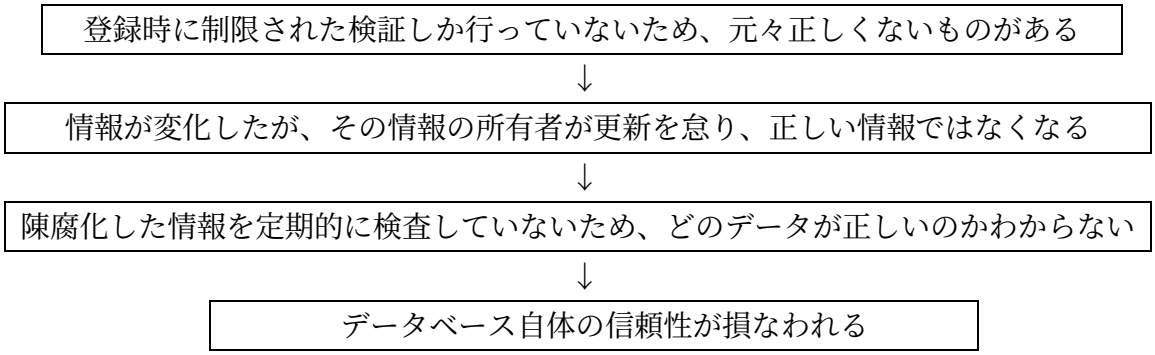
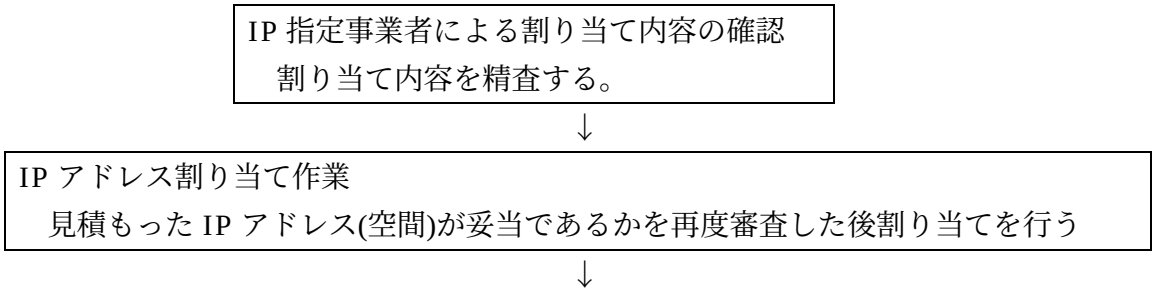


図 7　情報の陳腐化のプロセス

このような状況を放置しておけば、ネットワークの問題解決に使われるべき情報であるにも関わらず、逆に問題を発生させる一因となりかねない。

2.1.2.3. JPNIC での IPv4 アドレスの登録と更新に存在する脅威

JPNIC における IPv4 アドレスの登録手続きは、IP アドレス管理指定事業者(以下では IP 指定事業者とよぶ)からの割り当て報告申請を受け付けることで行われる。この申請手続きについては図 8 のように説明がなされている[12]。



[12] “IP アドレス割り当て報告申請処理について(ユーザネットワーク用)”, http://www.nic.ad.jp/doc/jpnic-00841.html

JPNIC へ割り当て報告申請
　JPNIC へ割り当て申請を行い、JPNIC は申請内容を DB に登録する。

図 8　IP アドレス割り当て報告申請プロセス

アドレス割り当てに関して IP 指定事業者から提出される情報について、JPNIC ではアドレスサイズが規定を超えて大きい場合を除き、特別な審査は行わない。つまり、情報に誤りがあったとしてもデータベースへの登録が行なわれてしまうことになる。

この点について、IP 指定業者が情報確認を行うことを確認するため、割り当て内容の精査について以下の注意が記載されている。

申請者から受け取った内容について記入漏れがないか、記載事項に誤りがないか等について精査してください。申請内容に虚偽がふくまれていないことを確認するのは困難ではありますが、可能な限りこれに努めてください。

登録情報の更新については更なる問題が存在する。ネットワーク資源の割り当てを受けている事業者、または個人による個人情報の変更については、IP 指定事業者を経由することなく、直接 JPNIC に追加・変更申請を行うことになっている。

この手続きは図 9 の手順で行なわれる。

http://www.nic.ad.jp/doc/jpnic-00844.html 中の追加・変更申請フォームの記入
↓
電子メールにより apply@db.nic.ad.jp へと送信
↓
機械的に処理され、データベースに反映される

図 9　登録情報更新プロセス

この手続きには認証手順が含まれないため、第三者が電子メール操作により不正にデータベースの書き換えを行う可能性がある。

この登録と更新に関する問題が、whois サービスで述べたようなデータベースの信頼性を損ね、登録情報の主な利用目的であるネットワーク上の問題解決に悪影響を与える可能性を否定できないと考えられる。

2.1.3. ネットワーク資源に対する脅威

ネットワーク資源は有限であるため、効率的な運用がおこなわれなければインターネットそのものが機能しなくなる危険性をはらんでいる。また、資源の利用に関する規則の遵守は紳士規定に過ぎず、設定ミスばかりでなくとも、意図的に規則を破って不正な情報操作を行うことでネットワークに多大な影響を与える攻撃が存在する。このような事態を引き起こす要因となる脅威には表 9 のものが存在すると考えられる。

表 9　ネットワーク資源に対するリスク

リスク	脅威	原因
ネットワークの飽和	ネットワーク資源の枯渇	不要なネットワーク資源の使用 使用されていないネットワーク資源の申請
通信障害	ネットワーク資源の衝突	割り当てられていないネットワーク資源の使用

以下にこれらの脅威が引き起こすリスクについて記述する。

2.1.3.1. ネットワークの飽和の可能性

インターネットを支える資源のうち、枯渇が問題となっているものの筆頭が IPv4 アドレスである。32 ビット固定長という構造上、最大割り当て数を増やすことができない、RIR へのブロック割り振りの都合上、例えば ARIN に未割り当てアドレスがあったとしても APNIC 管轄の NIR へ割り当てることもできないといった要因から、実際に利用できるアドレス数は理論上のものより少ない。

インターネットが今より小規模であった頃、ある程度の規模を持った企業であれば、クラス B のアドレスブロック（最大で 65534 ホスト）を割り当てられることも珍しくはなかった。現在ではクラス C（最大で 254 ホスト）を割り当てられることも難しい。

このように大きなアドレスブロックを以前に割り当てられた組織に対し、過剰な割り当て分について、自主的に返還することを推進する運動がかつてあった。しかし、割り当てられたアドレスブロックは、将来に備えるといった理由で返還されなかったものもあったと思われる。また割り当てを受けたアドレスブロックが、実際には過多な場合もあると考えられる。

割り振り、割り当て済み IPv4 アドレスは年々増加する一方であり、このままの状態

が続けば、アドレスが枯渇することは間違いない。この対策として IPv6 への移行が始まって久しいが、緩やかな移行が起こるかどうかは予測できず、アドレスブロックの割り当てが安定して行われるかどうかはわからない。

2.1.3.2. ネットワーク資源の衝突による通信障害の可能性

あるネットワーク、ホストが使用する IP アドレスはインターネット接続前に申請し割り当てを受けていなければならないが、実際には、割り当てを受けていなくても接続することは可能であり、通信を行うことが可能である。

これには経路制御がどこで行われるか、その設定をするのは誰であるか、といった条件が存在するが、RIPE NCC が実施している RRCC（Routing Registry Consistency Check Project）によると、実際に流されている経路情報のうち、相当数のものが未登録であることがわかっている[13]。

インターネットの経路制御は AS を単位として自律的に行われている。そのため悪意を持って流される経路情報がインターネット全体に波及することは十分に考えられる。

The "No Questions Asked" Prefix Return Policy[14]で述べられているように、経路表の膨張に伴うインターネットオペレーション負荷の増大を防ぐためには、アドレスの返却と再割り当てにより、経路表の集約を可能とすることが不可欠である。

2.1.4. ネットワーク資源の脅威の影響

ネットワーク資源に対する浪費の意味での脅威は、いずれの原因でも同等である。しかし「割り当てられていないネットワーク資源の使用」は他の行為とは性質が異なる。割り当てられていないネットワーク資源が悪意のあるユーザに使われた場合に、その影響を抑えることが難しい。たとえば、割り当てられていない AS 番号と IP アドレスがテロ組織によって使用された場合、テロ行為の状況を把握すること、テロ行為を引き起こしているパケットの発信元を特定することが難しくなることが考えられる。これは転送経路を次々に変更することが可能であるためである。

---

[13] “General Routing Registry Consistency Check Report “, http://rrcc.ripe.net/RRCC_general_report.html

[14] The "No Questions Asked" Prefix Return Policy, http://ftp.apnic.net/apnic/docs/no-questions-policy.txt

経路情報を扱う上での一つの問題が swamp address space と呼ばれるものである。これはインターネットレジストリにとって再割り振りが難しい、細かいブロックの集合を意味し、グローバルには IANA が割り振りを行っていた時代に割り振られたクラス C アドレスブロックを指すことがある。

南カリフォルニア大学情報科学研究所の調査プロジェクト、Procedures for Internet and Enterprise Renumbering の 1996 年当時の swamp address に関する報告書[15]によれば、192/8 のクラス C アドレスを持つ、5980 の組織に連絡をとった結果、1850 の回答があり、1448 が配送に失敗した。返答の内訳は以下の通り。

表 10　swamp address の利用に関する調査

	アドレス空間を返却する	しない
アドレスを使っている	189	1351
アドレスを使っていない	135	23

このように実際に使われてしまっているものについて大多数が返却しないと述べているが、さらに重要なことは 20%以上の組織に連絡がとれないことである。つまり、管理者不在の状態で放置されているということである。

これら古い時代に割り振られたアドレスブロックは RIR による割り振りプロセスを経ていないことから、地理的地域性による、経路表の集約といった配慮を欠いている。場合によっては RIR をまたいで割り振られたものがあり、こういったアドレスに関する経路情報は、どこから流されるのか前提条件をもうけることができないため、エッジルータでブロックすることが出来ず、一つのネットワークだけでは正しいものかどうかの検証も難しいため、結果的に経路表に載ることになってしまう。

つまり、現在管理者不在の swamp address を調査し、それらのアドレスに対する経路情報をインターネットに流すことで、インターネットレジストリに登録せずとも、世界中に通信可能なネットワークを設けることが出来るということになる。

前述の RRCC の調査が、実際に登録されていない多数の経路情報が流通していることを示している。インターネットレジストリのポリシーに従ってネットワークを構築し

[15] “PIER - Procedures for Internet and Enterprise Renumbering”, http://www.isi.edu/div7/pier/)

ている組織が、登録をせずにインターネット接続することは考えにくいため、設定間違いによるもの、もしくは確信犯による行為と考えられる。

このようなアドレスを使って不正行為を行うと、実行者を特定するため、および不正行為をブロックするためには、経路上にあるすべてのネットワーク管理者の協力を仰ぐ必要がある。しかし、実行者が複数のアドレスを使い、それらを渡り歩くことで不正行為を継続したとすると、実行者の追跡はほぼ不可能になり、不正行為を遮断することも困難となり、多くのネットワーク接続が不安定な状況になることが考えられる。

図 10 は、攻撃者が不正な経路を作り出すことで、第三者サイトを経由した攻撃を行っている状況を示している。サービス不能攻撃を行うのであれば、被害者サイトがサービス不能に陥ったことを確認した後、経路の公告を停止することで、追跡の手が及ぶ可能性を減らすことができる。

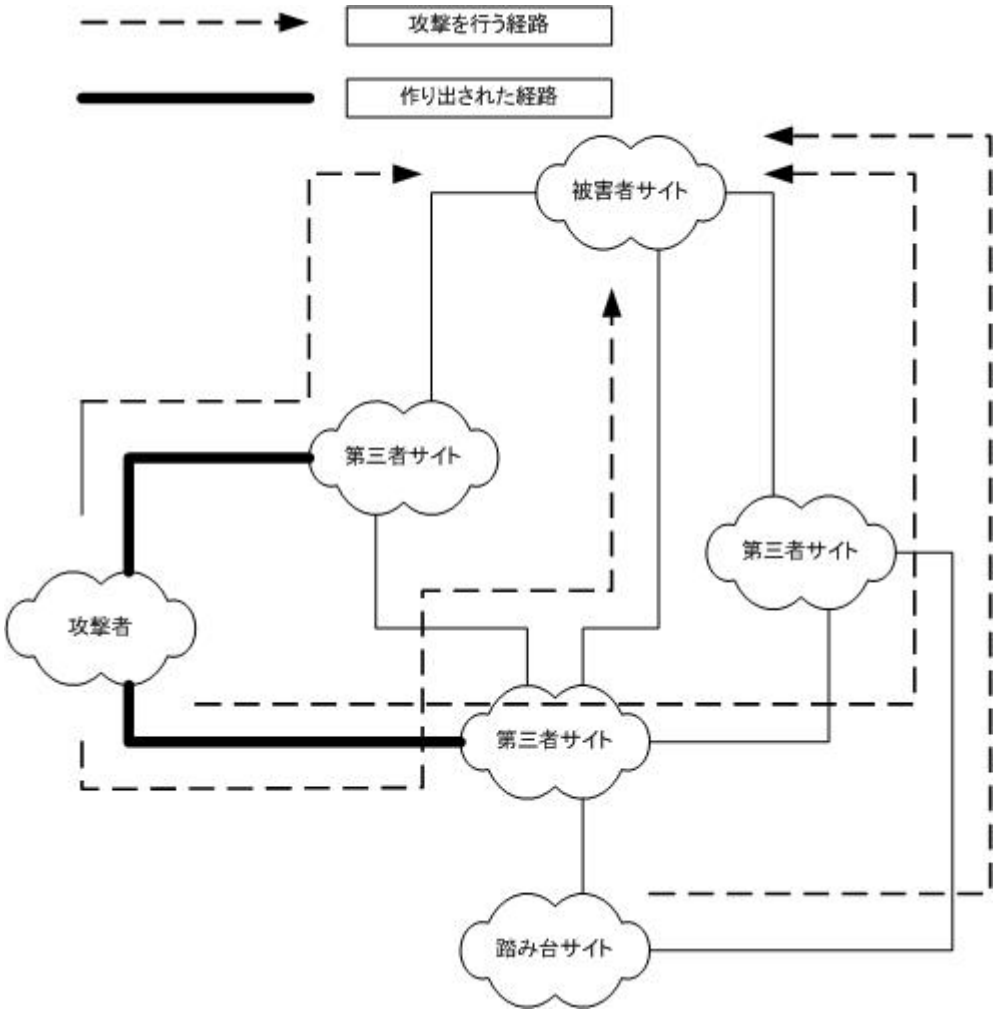


図 10　未登録の経路を利用した攻撃

犯罪組織がネットワーク資源の脅威を利用したこの種の攻撃は実際に発生している。

2003 年 2 月 27 日、RIPE に対する DDoS 攻撃(分散サービス不能攻撃)の影響から、二時間半に渡って、レジストリへのアクセスが不能となった(90%以上のパケットがロスト)。この攻撃は ICMP echo を悪用したもので、DNS、whois、FTP、Web サービスが利用不可能となった。

それぞれのサービスへの攻撃ではなく、大量の ICMP リクエストにより、RIPE の BGP セッションが影響を受け、外部からの通信が正常に行われなくなってしまったのが原因である。

この攻撃は別名 smurf と呼ばれるもので、古典的なものである。攻撃者については

不明とされているが、このような一般によく知られている手法であっても、RIR のネットワークが麻痺状態に陥ったことがわかる。

この事例の場合、RIR ネットワークそのものが孤立した状況に陥ったことで、すべての外部サービスが利用不可能と成った。

BGP ルータのフィルターで攻撃パケットをブロックすることが可能であったなら、サイトがダウンすることも無かったかもしれないが、この件では、攻撃自体検知されたにも関わらず、有効な手立てを打ち出せず、結果的に過剰な負荷によりルータがダウンするという結果となってしまった。

2.2. 登録情報の利用法と脅威の影響

インターネットレジストリの登録情報について想定される利用についてまとめ、これまでに述べた脅威が、その利用にどのような影響を及ぼすのかについて述べる。

2.2.1. 登録情報の利用

ネットワーク情報には IP アドレスのブロックを割り振られた／割り当てられたネットワークの情報のことであり、この情報は JPCERT/CC に代表される CSIRT（Computer Security Incident Response Team) によって、迷惑行為の発信元ネットワークへの連絡先の検索などに使われている。

AS 番号には AS 番号を割り当てられたネットワークの情報が登録されている。間違った経路情報を広告しているネットワークの特定や、ネットワーク管理者による正しい設定内容の検索に使われる。

ドメイン情報にはドメイン名を登録した組織の情報が登録されている。IP アドレスからドメイン名を調べた上で、登録されたドメイン情報が見つかった場合、CSIRT などによる連絡先の検索などに使われる。

組織情報にはデータベースに情報が登録されている組織の情報が登録されている。インシデントレスポンスチームなどによる連絡先の検索などに使われる。

2.2.2. 脅威の影響

登録情報およびレジストリデータベースは、インターネット運営に障害が発生した際のトラブルシューティングに利用されることが多い。つまり危機管理上重要な情報であ

り、インターネットの正常な運営が行われていることを確実なものとするために不可欠の情報といえる。

登録情報に含まれる、連絡先情報が不正な操作により改ざんされ、CSIRT が本来連絡をとるべき管理者に連絡がとれなくなれば、問題の解決に深刻な影響を与えることになる。

2.3. 登録情報/レジストリデータベースの保護

脅威の影響を最小限に抑えるため、情報は不正なアクセスから保護される必要性がある。2.2.2 節で述べた脅威を考慮して、登録情報に求められる性質を挙げる。

- 正確性

  提供する情報が「正しい」こと。正しいというのは提供者が「意図した通り」を意味する

- アクセス管理

  連絡先情報については、パブリックに公開されるべき情報ではあるが、個人情報についてはアクセス制限が要求されることがある

- 安定性

  インシデント解決に利用されることが多いということは、インシデントの発生に左右されることなくサービスが稼働しなくてはならない

- 即時性

  要求された情報が遅延なく提供されること

安定性と即時性についてはレジストリデータベースが配置されるネットワークの保護が必要となる。この保護については、ハードウェア構成に大きく依存するため、本報告書では考察の対象とはしない。

要求される性質のうち、正確性の保証、アクセス管理の実施のため必要な要件を以下に述べる。

・　ユーザ情報

　特定のネットワーク利用組織の登録情報を変更することができるユーザに関する情報のことで、ネットワーク資源の占有や登録情報の不正な書き換えを防ぐため、この情報へのアクセスについては、強力な認証が要求される。

・　認可の実装

　認可とはユーザがある操作を行うことに対する制御を行うことである。たとえば、組織情報のうち、組織名称を変更できるものは管理者のうちでも特定の一人にだけ許可し、組織連絡先電話番号の変更は管理者全員に許可するなどの利用が考えられる。

・　完全性の保証

　情報の経路上での改ざんを防ぐためには電子署名などを用いた完全性の保証を行う必要がある。

・　機密性の確保

　機密性が要求される情報については暗号化を施す必要がある。暗号化された情報は管理者のうち許可されたものおよびデータベース管理者にとって複号可能である必要がある。

・　登録情報の検証

　登録される情報のうち、組織情報、個人情報などは、正しくなければ保証する意味がない。オフラインでの情報の検証が必要となる。

　これらの機能を実現することで、正しい情報の維持が可能となり、また正しく伝えることが可能となる。

2.4. インターネットレジストリにおける権限委譲と PKI

　インターネットレジストリの、ネットワーク資源に関する権限の委譲構造は、権限の認可構造でもある。これは TTP（Trusted Third Party – 信頼できる第三者）を利用する認証基盤である PKI（Public-Key Infrastructure）の Authorization（認

可）構造と近似している。本節ではインターネットレジストリにおける権限委譲と PKI について述べる。また第 55 回 IETF（Internet Engineering Task Force）の PKIX ワーキンググループで議論された PKI の利用事例について述べる。

2.4.1. PKI

本調査研究報告書では「認証局」のあり方に関して述べるため、本節では PKI について概説と共に動向について述べる。

PKI（Public-Key Infrastructure）は公開鍵暗号を利用した認証基盤である。基盤技術であるため、PKI という一つの仕組みを、様々な認証の為に利用できる。

PKI では通信相手が本物であるかどうかの確認（認証）に公開鍵証明書（以下、証明書）を利用する。PKI における証明書は、発行者の名前といった情報が記述されており、身分証明書の役割を果たす。身分証明書を、信頼できる第三者（TTP：Trusted Third Party）に発行してもらうことで、その身分証明書を信頼できるようにするのが PKI の特徴である（図 11）。たとえばここでいう身分証明書が運転免許証であるとすると、信頼できる第三者は公安委員会ということになる。

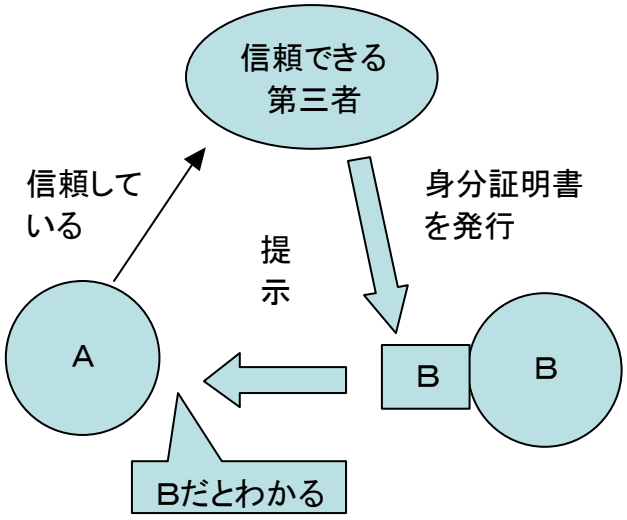


図 11　信頼できる第三者

証明書を利用して相手を認証する際には、証明書が偽造されていないか、その証明書の発行元は信頼がおけるのか、といった確認が行われる。証明書が有効であれば、その証明書の提示を行ったのが正しい相手であることがわかる。そのため初めて通信する相手でも、直接対面することができない通信相手でも認証できる。よって PKI はインタ

ーネットのような通信相手と対面することを前提にできない環境に適している。

以下に PKI の仕組みのうち、X.509 や RFC3280 に基づいた証明書の扱いについて概説する。

2.4.1.1. 証明書の利用

PKI で用いられる証明書は、認証局（CA：Certification Authority）によって発行される。PKI では、この CA が“ 信頼できる第三者 ”にあたる。CA は、いわば身分の証明を行っている機関なので、ユーザに強く信頼されていなければならない。ユーザは、自分が信頼している CA が発行した証明書であれば信じられるということになる。

証明書には身分を証明する内容だけでなく、公開鍵暗号方式で使われる暗号鍵（公開鍵）も含まれている。この暗号鍵は、電子メールの電子署名や Web のサーバやクライアント（ブラウザ）の認証に使うことができる。たとえば電子メールの場合、S/MIME（Secure/Multipurpose Internet Mail Extensions）というプロトコルで、PKI を利用することができる。電子メールでの重要なやりとりでは、送信者は本人に間違いないのか、内容が他人によって書き換えられていないか、といった事が重要になる。PKI を使うと、S/MIME での電子署名が本人のものであるかを確認することができる。また TLS（Transport Layer Security）でも PKI が利用される。Web ブラウザが https（TLS や SSL を使った http）を使って Web サーバと通信を行っているとき、そのことを示す鍵マークが表示される。鍵マークが表示されるまでに、Web サーバと Web ブラウザは証明書の交換を行い相手の証明書を検証するが、この時に PKI が使われる。 PKI は認証情報をアプリケーションとは独立に扱うため、様々なアプリケーションに応用したり、アプリケーションに変更を加えずに PKI の仕組み自体を改良したりできる。

2.4.1.2. 証明書とユーザ

ユーザは CA に証明書を発行してもらい、その証明書をアプリケーションで利用する（図 12）。CA はユーザと同様に証明書を持っており、その証明書に含まれている暗号鍵を使って、発行する証明書に電子署名を施す。ユーザは CA の証明書を参照する事で、検証したい証明書の発行に使われた暗号鍵が、確かにその CA のものであるということを確認できる。

図 13 のように、ユーザはルート CA、もしくはいずれかの CA を信頼し、その CA が発行する証明書は正しいという前提に立って証明書の検証を行う。ユーザが信頼している CA は、そのユーザにとっての“ トラストポイント ”（信頼点）と呼ばれる。トラ

ストポイントはユーザによって異なる。

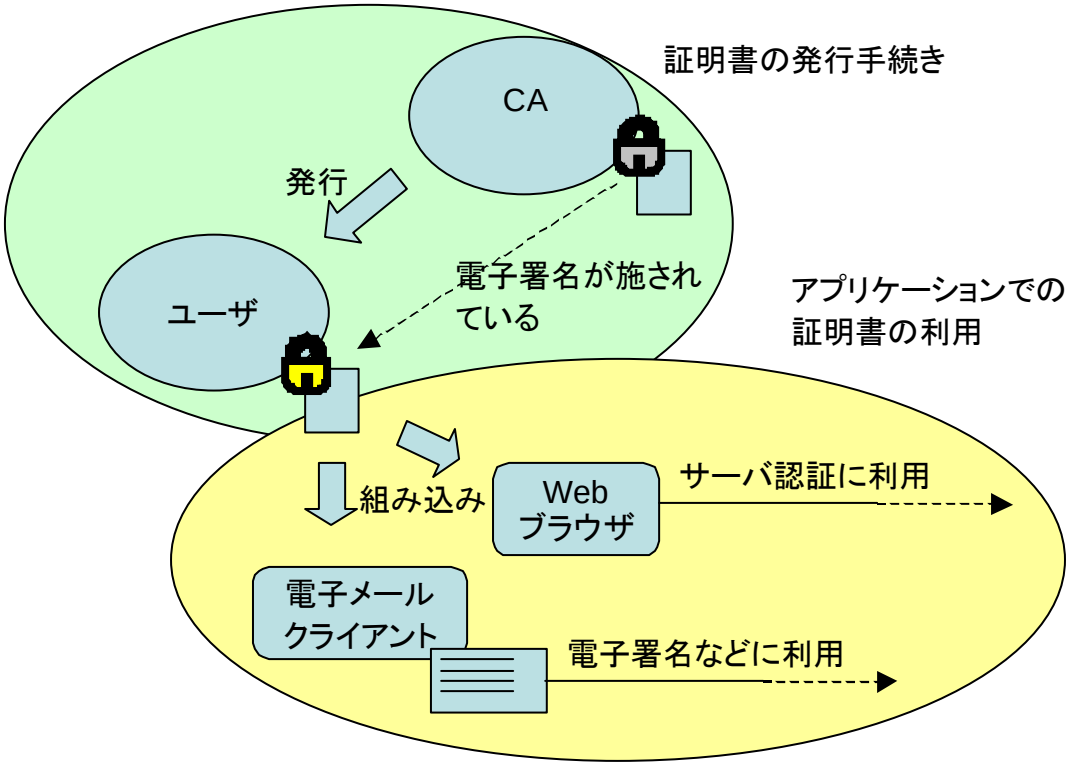


図 12　証明書の発行と利用

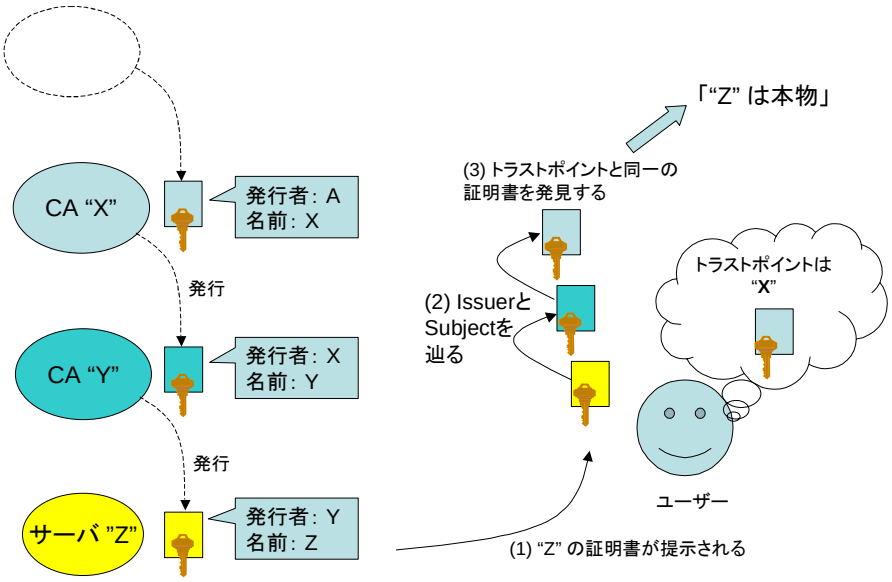


図 13　トラストポイント

2.4.1.3. 証明書の内容

証明書には図 14 のような内容が記述されている。

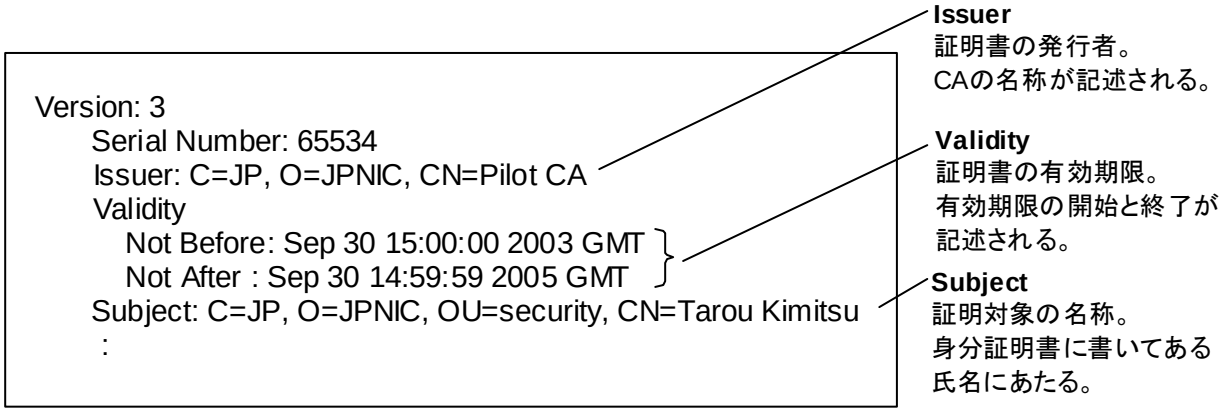


図 14　証明書の例

Subject や Issuer に記述されている名称は、識別名（DN: Distinguished Name）と呼ばれる。表 11 に DN の要素と意味を示す。

要素	意味
C（Country）	国名
O（Organization）	組織名
OU（Organizational Unit）	部門名
CN（Common Name）	一般名

表 11　X.509 形式の証明書で使われる識別名（DN）の要素

この他に、証明書には公開鍵データや CA による署名のデータ、用途などの情報が記述されている。これらのフィールド（項目名と値）は、検証の際に参照される。

2.4.1.4. 証明書の検証

証明書の検証には、二つの側面がある。

一つ目は証明書チェイン（証明書の連鎖）である。証明書チェインとは、検証したい

証明書からトラストポイントもしくはルート CA の証明書までの一連の証明書が連鎖している状態のことである。各々の証明書に電子署名されており、それぞれの電子署名を検証できる公開鍵は、発行者である CA の証明書（以下、CA 証明書）に含まれている。認証したい相手の証明書を検証するには、一連の証明書を次々に検証していく必要がある。

二つ目の側面は、証明内容を受け入れられるかどうかである。証明書には、証明対象の名称や証明書の用途、証明書のポリシー（の識別子）が含まれている。たとえば対象を限定して検証を行いたい場合、Subject の比較を行う。JPNIC という組織に属しているものだけを認証したいとき、Subject に“C=JP, O=JPNIC”が含まれているかどうかを確認する。たとえ証明書の連鎖が成立していても、Subject が想定したものと異なる場合、認証は成立しないことになる。Subject 以外に、受け入れられる用途かどうか、受け入れられるポリシーかどうかといった検査を行う。これらの二つの側面で検査し問題がなければ、認証が成立したことになる。

次に上記で説明した側面をふまえ、証明書の検証手順について説明する。証明書の検証手順には、いくつかの方法が提案されている。ここでは認証対象の証明書から上位の CA に向かって証明書を辿っていく方法を説明する。はじめに認証対象の証明書から上位の CA に向けて証明書のチェインを構築する。この処理はパス構築と呼ばれる。

- Issuer の値（発行者の名称）を元に CA 証明書を入手。
- CA 証明書の Issuer の値を元に、その CA 証明書を発行した CA の証明書を入手。
- CA 証明書入手を繰り返しトラストポイントの CA 証明書に辿り着いたかどうか判断。

次にそれぞれの証明書の証明内容を検査する。

- CA 証明書に含まれている公開鍵で、認証対象の証明書の電子署名を検証。
- 名称、有効期限、鍵の用途が受け入れられるかどうかを検査。
- 証明書が失効していないかを検査。

証明書の失効とは、CA がその証明書の効力が失われたと認識し宣言することである。証明書の失効の理由には、証明内容の変更や暗号鍵（秘密鍵）の紛失などがある。証明書が失効されているかどうかは CA によって発行される CRL（Certificate Revocation List（失効された証明書のリスト））を使って調べることができる。

証明書の検証をネットワークアプリケーションに組み込むと、そのアプリケーションの認証の手順は以下のようになる。

- 認証処理のはじめに証明書を交換。
- 次に相手が提示した証明書を検証。
- CRL の入手などを適宜行い、証明書の最新の状態を確認。
- 証明書が有効である場合、認証できたと判断しアプリケーションのサービスを開始。

このように、証明書の扱いは認証システムとは独立した仕組みであり、認証システムを構築する際には、通信プロトコル等と組み合わせて利用される。

2.4.2. 第 55 回 IETF PKIX ワーキンググループにおける議論

PKI に関する技術動向の一環として、PKI のプロトコル策定活動を行っている IETF（Internet Engineering Task Force）の PKIX（Public-Key Infrastructure (X.509)）ワーキンググループに参加した。米国アトランタで行われたこの会議では、X.509 形式の証明書の検証プロトコルや証明書の値の利用に関する議論が行われた。本節では、利用に関する議論について紹介する。

このセッションでは以下のようなプロトコルに関するドキュメントが紹介され、議論された。

- DPV/DPD（Delegated Path Validation and Delegated Path Discovery Protocol）
- SCVP（Simple Certificate Validation Protocol）

また証明書のフィールド（項目と値）の利用に関して以下のような提案が紹介され、議論された。

- Proxy Certificates
- LDAP Schema
- Attribute Certificate
- Certificate Warranty Extension
- Logotypes in X.509 Certificates

更に、証明書の利用法に関する紹介が行われた。

- SIM（Subject Identification Method）

SIM は、証明書の拡張フィールドに個人を識別する番号を格納する方式である。この方式は、subjectAltName 拡張フィールドに、一方向性関数を利用した値を格納することで、プライバシーの保護と、予め識別子を知っている検証者によるユーザの識別を可能にする。

証明書のフィールドに格納する値は、PKI を使った認証システムの実装によって扱い方が異なる場合がある。特にフィールドに格納された値からユーザを識別する方法については、プロトコルの提案の範囲を外れている。SIM は、一方向性関数の利用等を通じて、格納された値の利用法の開発に積極的に取り組んでいると考えられる。

本調査研究が想定している認証局でも、証明書に格納する値の議論が必要になると考えられる。今後も、SIM のような積極的な取り組みの動向をみていく必要がある。

なおセッションの最後に、日本ネットワークセキュリティ協会による相互運用に関する実験 ChallengePKI 2002 と ChallengePKI 2003 について紹介された。

2.4.3. インターネットレジストリと Authorization（認可）

インターネットレジストリは、上位インターネットレジストリから下位インターネットレジストリに、ネットワーク資源の割り振りに関する権限を委譲する構造を持つ。一方、認証局が発行する証明書には、認証の他にその証明書で示されている属性を証明するという意味がある。属性には、認証局であるかどうか（証明書を発行できるかどうか）、暗号鍵をどのような用途に使うことができるか、といった情報が含まれている。属性として表される値の中に、そのエンティティが利用または割り当てを行うことができるネットワーク資源を表現することができれば、ネットワーク資源の管理に関する権限の委譲を表現することができる（図 15）。

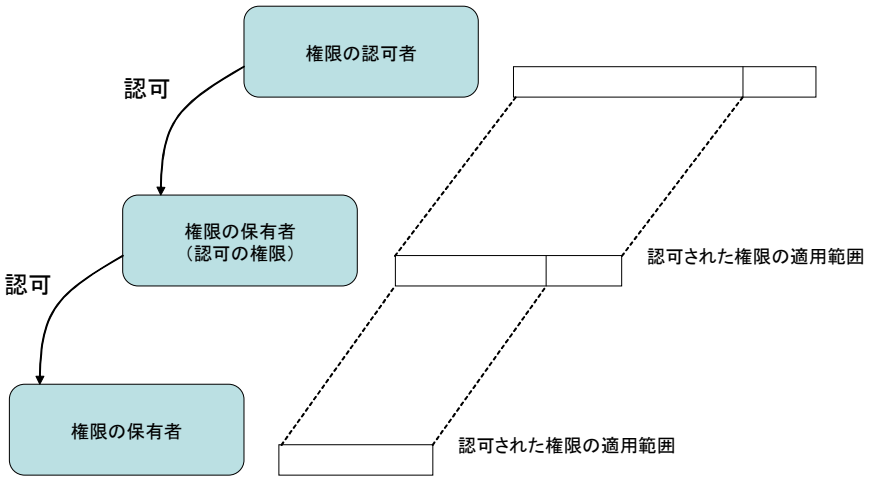


図 15　認可された権限の範囲

しかしこのモデルは、権限の委譲と認可を同等と考えた場合のもので、ネットワーク資源の割り振りに関する権限が「認可」のモデルと一致するかどうかについては議論の余地が大きい。これはネットワーク資源の管理が、合意されたポリシーにもとづいて行われるためで、一義的な「権限の認可」にもとづいていないからである。

またネットワーク資源が証明書で表現されるかどうかについても議論と開発の余地がある。ネットワーク資源の割り振りを検証可能な表現形式で扱ったプロトコルや手法は、日本の NIR や４つの RIR において利用されたことがなく、一般的な概念ではないと考えられる。また PKI の適用に関しては、証明書のフィールドの扱いと、ネットワーク資源の表現方法についての議論が必要である。

2.5. まとめ

インターネットレジストリが提供するサービスおよび保持する情報に関する脅威には次のものなどが存在する。

- 登録情報に関する不正なデータの保持、提供
- ネットワーク資源の浪費、無効化
- データベースサービスへの攻撃

これらが問題となることは、現状の情報提供サービス実装のセキュリティ機能が乏しいことに多くの原因がある。インターネットで広く利用されている SSL（もしくは TLS）は、セッションに機密性と完全性を持たせるプロトコルで、接続先が意図した相手であることを保証するものではない。

また、登録されている情報自体が現状を反映していないという報告が RIR の会合では繰り返されていることなどを考慮すると、登録情報を扱うシステムは次のセキュリティ機能を実装することが急務といえる。

- 正確性
- アクセス管理
- 安定性
- 即時性

データベースの情報を確実なものとし、更新が速やかに行なわれ、安定した情報提供を行い、不正アクセスから保護するということになる。

セキュリティ機能の実装に PKI を使うことが考えられるが、そのためには認証局が重要な検討事項となる。

RIR の試みとしては APNIC の CA パイロットプロジェクトが挙げられる。その詳細については第 3 章で述べる。

第3章 他のインターネットレジストリの活動

内容

- 認証局とデータベース保護に関する活動
  - APNIC
    1. CA Pilot Project
    2. MyAPNIC
  - RIPE NCC
    1. オブジェクトの保護
    2. WebUpdates
  - RIR の whois システム
  - RIPE Database System

3. 他のインターネットレジストリの活動

本章では、データベース保護と PKI に関連する活動について、他の RIR（地域インターネットレジストリ）が取り組んでいるプロジェクトを概説する。

具体的には APNIC における CA（Certification Authority）プロジェクト、RIPE における WebUpdates および LIR Portal プロジェクトとなる。また、ARIN については分散データベースの取り組みとして提供されている RWhois システムを取り上げる。

このうち APNIC と RIPE は SSL を用いたウェブインターフェースを提供している。中でも APNIC の CA プロジェクトの一環として運用されている MyAPNIC では X.509 形式の公開鍵証明書（以下では証明書とよぶ）をサーバだけでなくクライアントにも発行することでサーバ、クライアント間の相互認証を実現している。証明書ベースのクライアント認証を行なうことで、ウェブアプリケーションによく見られるパスワード認証に比べ、遥かに高い信頼性を与えることを可能としている。

今回取り上げた APNIC、ARIN はともに RIPE の開発するデータベースシステムを採用しており、RPSL（Routing Policy Specification Language）を使用している。

本章の終わりに、この RIPE のデータベースシステムについての概要を述べる。

3.1. APNIC

APNIC は Asia Pacific 地域を管轄とする RIR である。APNIC では 1999 年から PKI に対する取り組みを行なっており、パイロット運用を行なっている。

APNIC は管轄地域の IP アドレス割り振り、割り当てに関する権限を持っている。IP アドレスと、それに関する提供情報の価値というものは極めて高いものであり、APNIC の業務と提供情報を正しく維持し、提供することは、インターネット運用上、重要な役割であると考えられる。

- IP アドレス
- AS 番号
- 逆引き情報
- whois 情報

PKI 導入プロジェクトが開始されたのは、APNIC とメンバーのやりとりが非同期の電子メールによるコミュニケーションで行われていることに対する反省が元になっている。

例として、新たに IP アドレスの割り振りを申請する手続きは図 16 のようになっている[16]。

図 16　APNIC における IP アドレス割り振り申請プロセス

この手続きの間、通信経路およびフォームやメールといった情報そのものに特別な保護対策は施されていない。

また、メンバー登録により PIN（Personal Identification Number – 個人識別番号）が発行され、メンバーの認証は、この PIN により行なわれる。つまり、パスワード認証とほぼ同等程度の安全度しか持たない。

メンバーからも、電子メールの認証とプライバシー、およびウェブサイトの認可についての関心が寄せられ、1999 年から 2000 年にかけての第 8 回、第 9 回および第 10 回目の APNIC Open Policy Meeting では、PKI に関する取り組み開始の発表と議論が行なわれた。

より高度なセキュリティを実装するため、1999 年 10 月から 3 ヶ月かけて、PKI の導入による影響の分析、議論のための論点を提供、PKI に関する意識の向上を目的とした Scoping Project が実施された。

さらに Scoping Project の成果を受け、2000 年 4 月から 5 月にかけて Pilot Project

[16] “APNIC IPv4 ISP Request Form”, http://ftp.apnic.net/apnic/docs/isp-address-request

が実施され、PKI を導入する領域の特定、ソフトウェアと手順の開発のスケジュール、リスク分析が行なわれた。

この成果はレポートにまとめられ公開されている。その中で、PKI 導入の試みに関する目的および利点については次のように述べられている。

- APNIC のリソースの不正使用、改ざんを防ぐ。
- ビジネスをより安全に、より良い方向に変えていく。
- これにより中核となるリソースを更に保護できる。
- メンバーとメンバー情報を管理する必要がある。
- APNIC サービスの安全性について改善さらに効率も改善する。

また、ここ数年間に行なわれた PKI および CA 運用に関するプロジェクトは表 12 のようになっている。

表 12　APNIC における PKI および CA 運用に関するプロジェクト

実施時期	プロジェクト
1999 年	Scoping Project 開始
2000 年	Pilot Project 開始
2001 年	MyAPNIC Project 開始

プロジェクトに関する討論の場として、年に二回開催される APNIC Open Policy Meeting では CA に関する BoF が催されている。

表 13 は同ミーティングでの CA プロジェクトに関する発表のリストである。

表 13　APNIC Open Policy Meeting での CA プロジェクトに関する発表

会合	表題
2000 年 APNIC 10 ブリスベーン	APNIC Certification Authority project
2001 年 APNIC 11 クアラルンプール	CA Scoping Project Report
2001 年 APNIC 12 台北	APNIC MyAPNIC project Use of certificates in routing validation

3.1.1. Scoping Project

このプロジェクトはパイロット実装に先立って、必要な要件を定義するために行なわれた。

結論として、メンバーのセキュリティに大きな利点があること、PKI をサポートする標準の育成が重要であることなどがあげられている。

3.1.2. Pilot Project

証明書の利用により、APNIC のメンバーと顧客のために拡張された安全なサービスを提供するために CA を運用する。このサービスの一部として、APNIC はメンバーに証明書を発行することになる。これが Pilot Project である。

このプロジェクトにおいて、APNIC の CA サービスは次の契約条件のもとに提供される：

- CA サーバシステムは安全な環境で維持され、APNIC 内部ネットワークまたはインターネットに接続されることはない。
- APNIC は、プライベート鍵の生成、データの転送、APNIC により運営される他の安全なシステムといった同様の標準に対しての仲介システムを制御する。
- 署名された鍵ペア生成手続きは、アイデンティティの適切な保証を利用する、これはパスポートや他の公式な写真付のアイデンティティ文書のことである。

- APNIC は、鍵の生成、配布、安全な廃棄が行われることを保証する CA サービスプロセスにおいてリーズナブルな対処を行う。

- APNIC は、提案される CA サービスのステータスの変更、鍵ペアの変更について、証明書所有者と連絡を行う。

- APNIC は、APNIC により発行されるデジタル証明書の利用により生じる、信頼の喪失、またはダメージを許容しない。

- APNIC CA により発行されるデジタル証明書の受領者は、証明書の利用により生じるいかなる種類の損害についても、第三者からのクレームに対して、APNIC に補償を行なう。

3.1.3. APNIC の業務に対する PKI の導入

APNIC の業務に PKI を取り入れることについて Pilot Project が行った提案についてまとめる[17]。この提案は 2000 年当時のものである。

この提案では次の処理について述べられている。

- 新規メンバー登録
  - 書面による登録フォームの処理
  - 鍵と証明書要求の生成
  - オンラインでの証明書要求の処理
  - 証明書利用可能および証明書取得手順の通知
  - 新メンバアカウントの初期化
- 安全なオンライン要求の送信
  - APNIC ウェブベースオンラインサービスの強力な認証
  - オンラインサービス要求の完遂
  - SSL を通じた電子署名および転送
  - APNIC によるオンライン要求の検証
  - APNIC によるオンライン要求の処理
- APNIC メンバアカウントの終了
  - アカウントのクリーンアップ、終了
  - (可能であれば)証明書の廃棄

[17] “APNIC PKI pilot project Report”, https://www.apnic.net/ca/ca-scoping.pdf

この報告で提案されている各種手続きについての詳細を以下で述べる。

- 新規メンバー登録（書面による登録フォームの処理）

新規メンバー登録手続きは図 17 のような流れとなる。RA（Registration Authority）は、CA の機能の一つで、証明書の発行要求を受け付けと登録を行う。

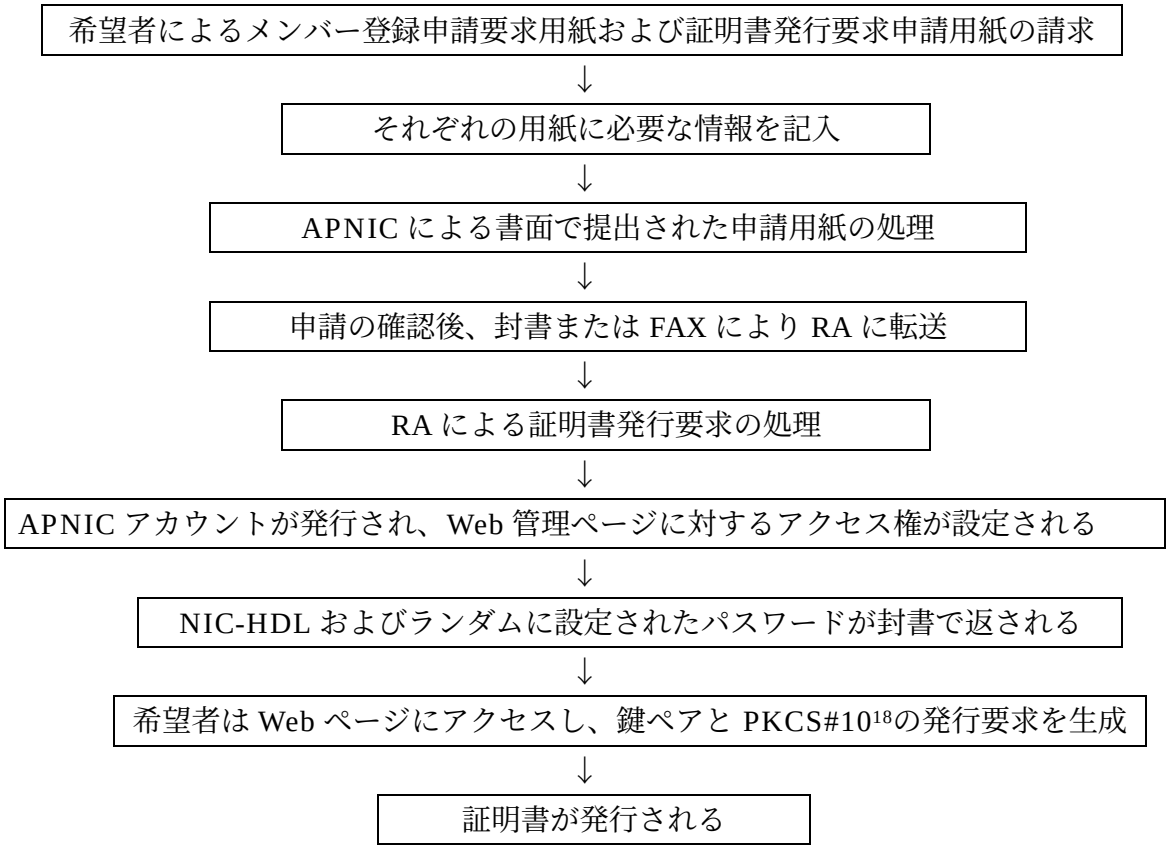
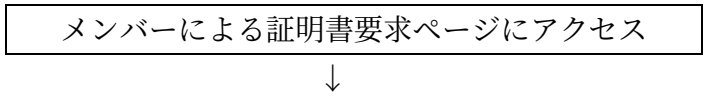


図 17　新規メンバー登録（書面による登録フォームの処理）

ここでは封書を用いてトランザクションが行なわれることになっているが、現在では SSL を用いた Web ケーションによる申請の試みが行なわれている。

- 新規メンバー登録（鍵の生成と証明書要求の処理）

新規メンバー登録手続きのうち、鍵の生成と証明書要求の処理は図 18 のようになる。



[18] PKCS#10, “Certification Request Syntax Standard”, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.ps

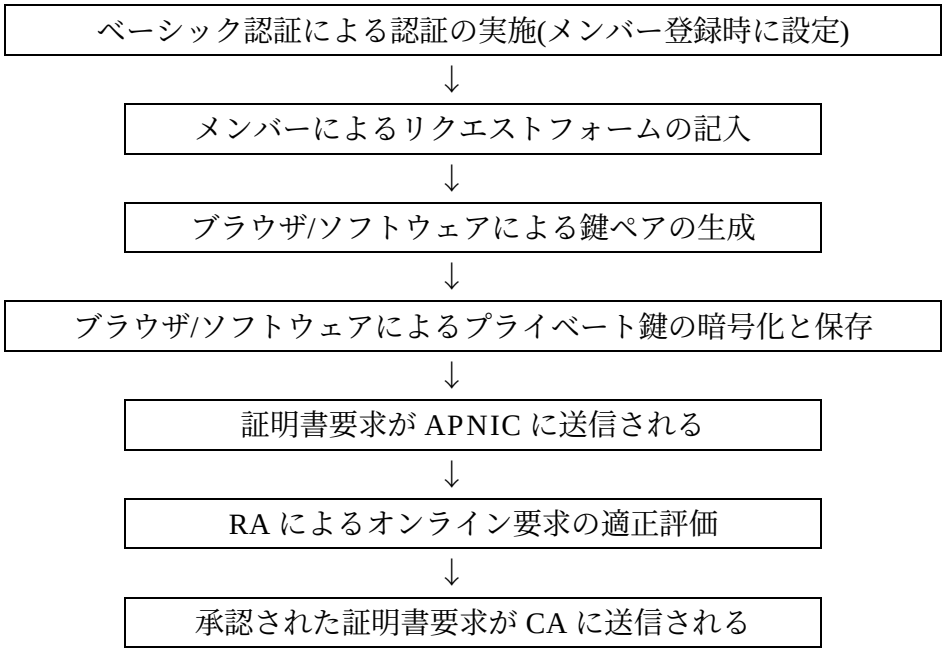


図 18　新規メンバー登録（鍵の生成と証明書要求の処理）

- 新規メンバー登録（新規アカウントの初期化）

新規メンバー登録手続きのうち、新規アカウントの初期化処理は図 19 のようになる。

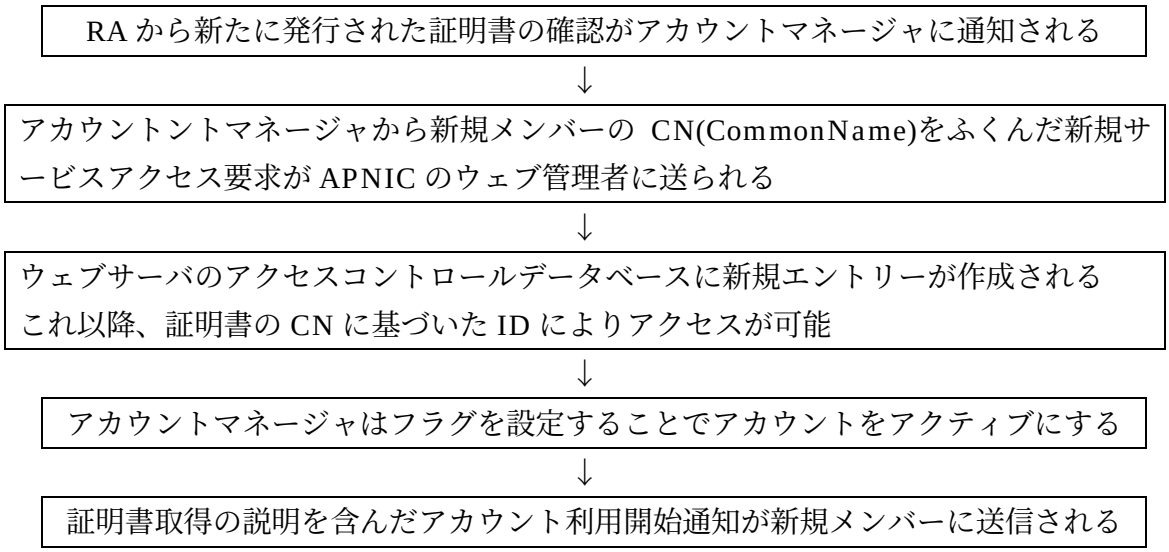


図 19　新規メンバー登録（新規アカウントの初期化）

- 証明書の取得

APNIC CA により生成された証明書は図 20 の手順で取得する。

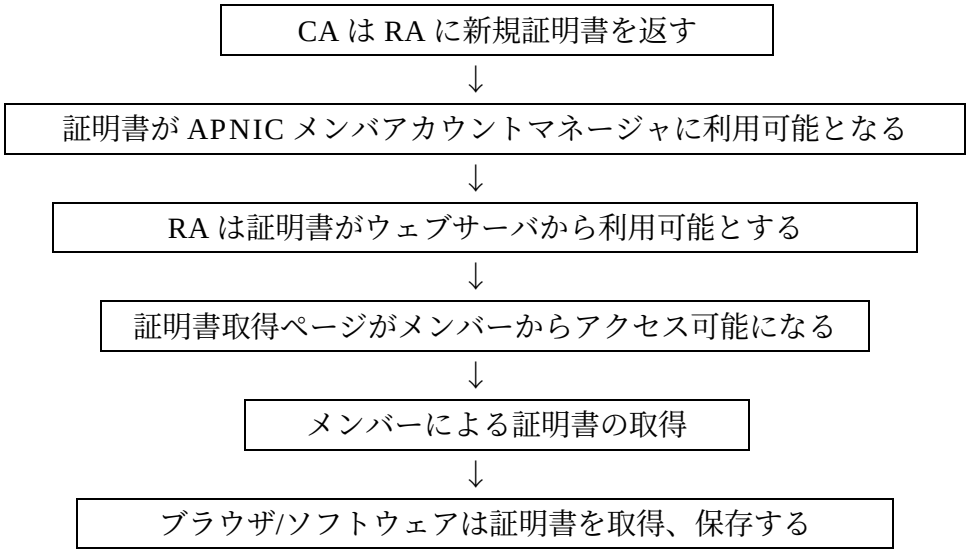
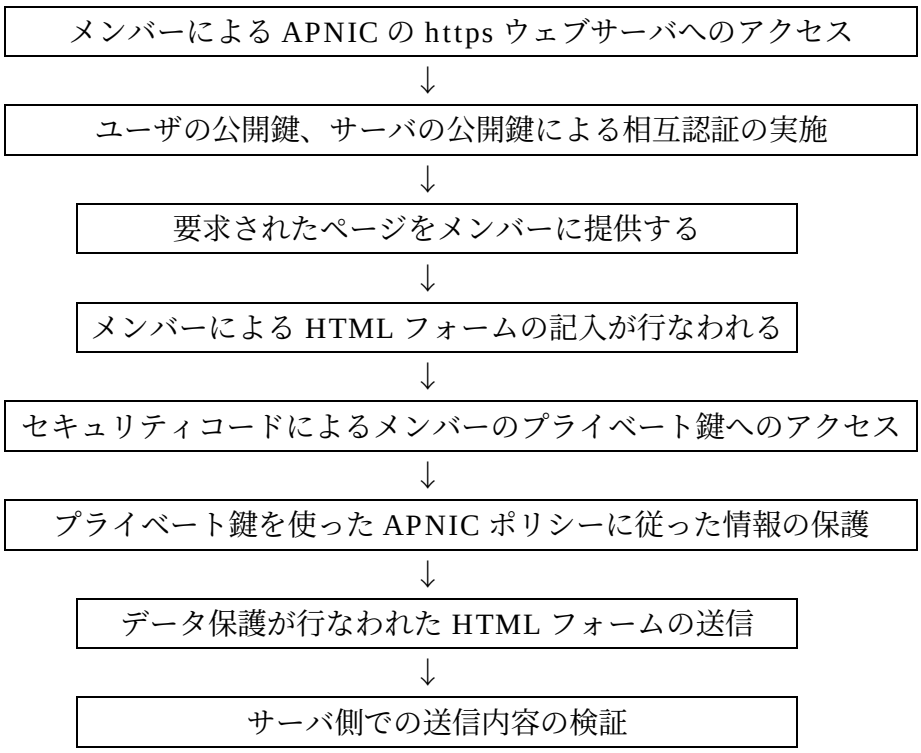


図 20　証明書の取得

この段階でメンバーは APNIC のセキュアオンラインサービスにアクセスするために必要なすべての情報をもつことになる。

- オンラインでのリソース要求

メンバーがプライベート鍵、公開鍵を利用する手順について述べる。



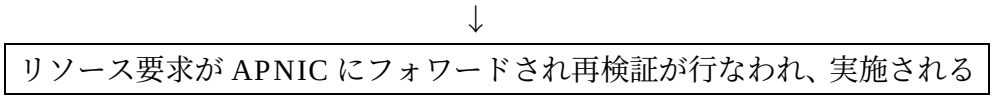


図 21　オンラインでのリソース要求

- オンラインでのリソース要求処理

APNIC の要求処理システムには RT（Request Tracking） システムが実装されている。RT が要求をどのように処理するのかを図 22 に示す。

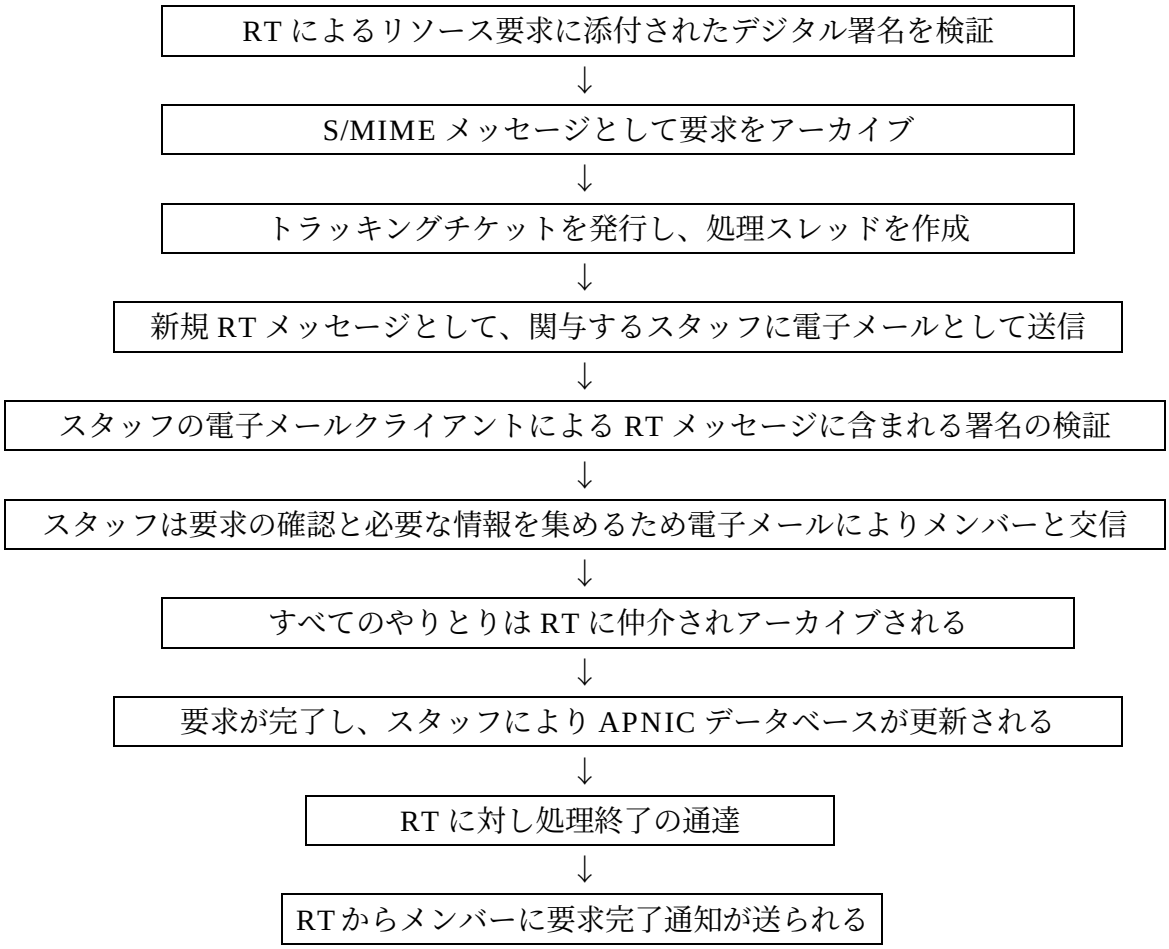
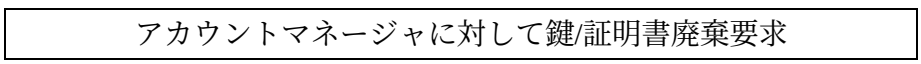


図 22　オンラインでのリソース要求処理

- 証明書廃棄およびアカウントの終了

メンバアカウントの削除および、証明書の廃棄に関する手続きは図 23 のようになっている。



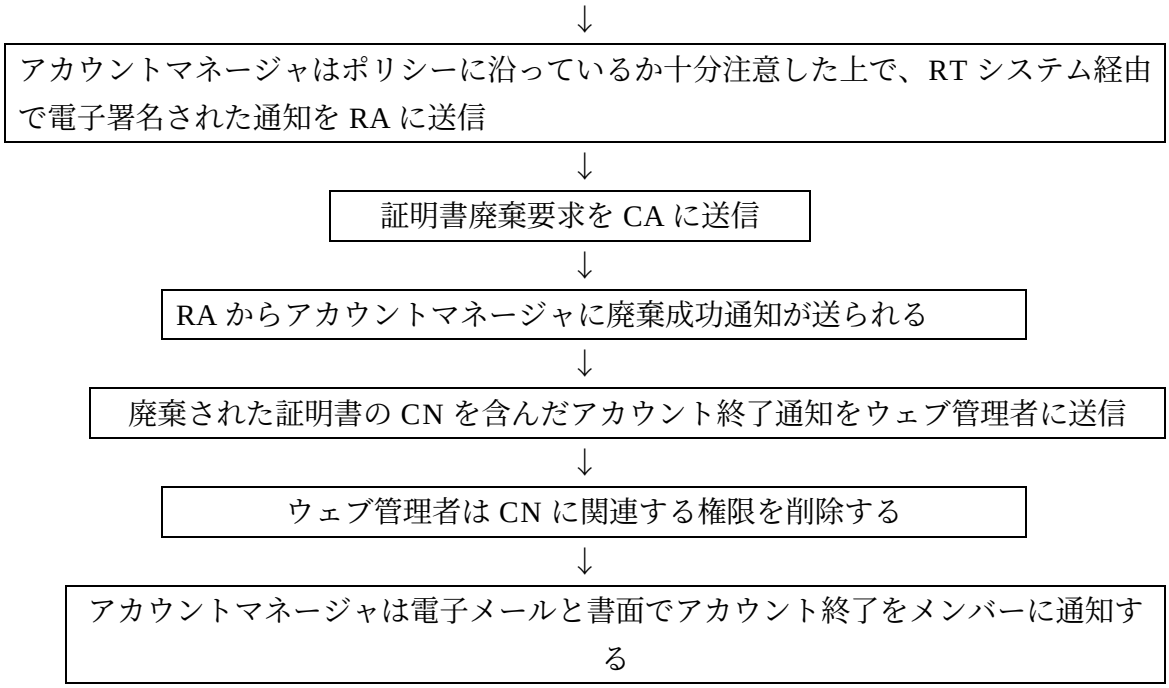


図 23　証明書廃棄およびアカウントの終了

3.1.4. MyAPNIC

MyAPNIC プロジェクトはメンバーに安全なウェブインターフェースを提供し、そのインターフェースを通じた、メンバーの個人情報へのアクセスおよび APNIC サービスの利用を可能とすることを目的としている。このプロジェクトは PKI を利用したもので一連の CA プロジェクトのプロトタイプとして位置付けられている。

プロジェクトの動機となった問題点として次のものがあげられている。

- メンバーが whois 登録情報に関して変更が発生したとしてもデータベースを更新しようとしない。
- 熟練度のギャップが APNIC のホストマスタたちに余計な仕事を作り出している。
- APNIC とメンバー間のセンシティブな情報やりとりがより良い保護機構を要求している。
- 電子メールによるリクエストフォームにはタイプエラーの傾向があり生産性を低下させている。
- メンバシップ価値の向上の試み。

プロジェクトのシステムは図 24 のように構成される。

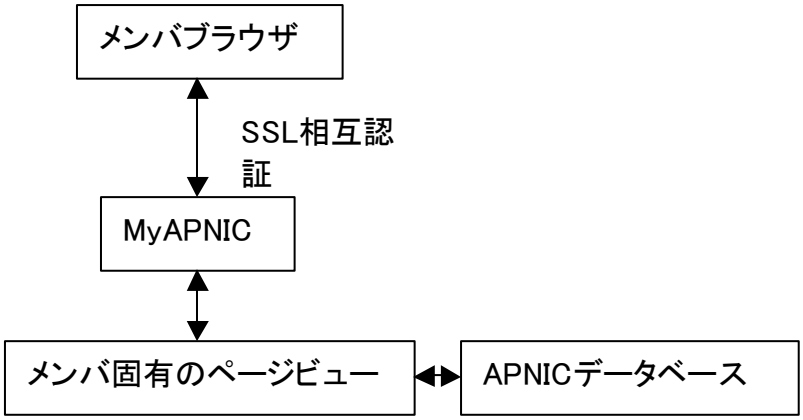


図 24　MyAPNIC の構成

MyAPNIC のコンセプトは次のように表明されている。

- 容易な利用
  - インターネットリソースデータベースの更新を奨励
  - 習熟曲線の短縮
  - シンプル、ユーザは割り当てられた画面だけを見る
  - APNIC がすでに情報を持っていれば予めフォームに入力
- 安全
  - サーバとクライアントの双方が SSL 認証で保護
  - APNIC は trusted CA の役割を果たす
  - 正しいクレデンシャルを持つものだけが情報を見ることが可能(クライアント証明書に束縛)
- 柔軟性
  - メンバーに自身の組織構成に合うユーザベースとオーソリティを設定可能
  - 更なるサービス拡張のプラットフォームを提供

また、機能として次のものが実装される。

- リマインダ
- インターネットリソース管理
- 財政/管理
- 訓練
- セキュリティ

実際のデモ環境では次のものが実装されている[19]。

- 割り当てグラフ

ここではメンバーが割り振られたネットワークごとの割り当て済みアドレスがバーグラフとして表示される。これを参照することで追加割り振り要求を申請する必要があるかどうかを判断することができる。

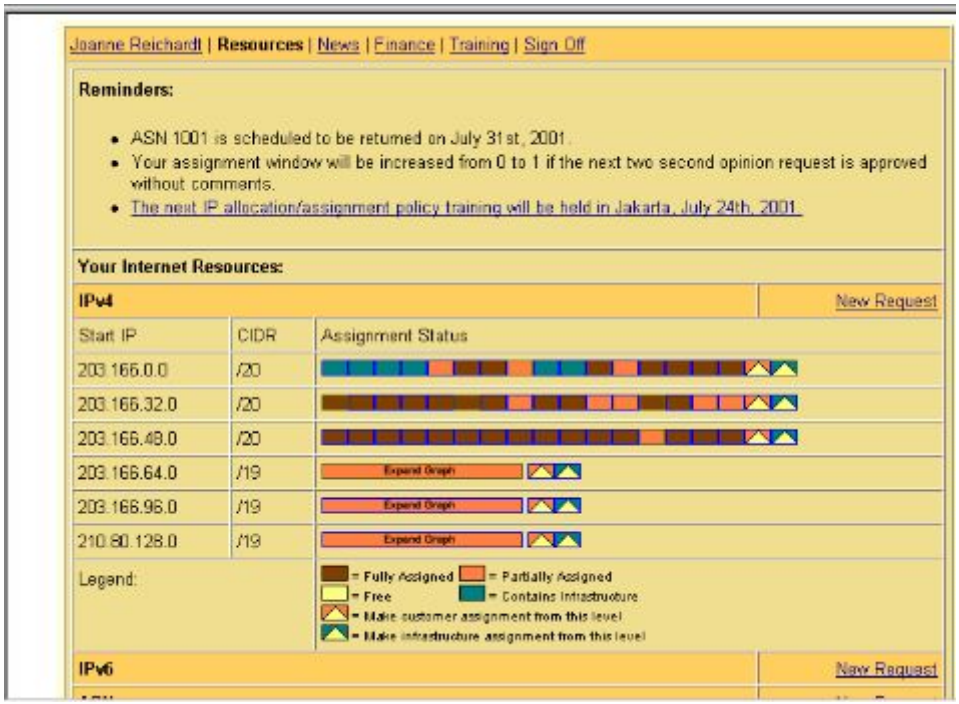


図 25　MyAPNIC 割り当てグラフ

- 割り当て表

ここではメンバーが所有するネットワークごとの割り当て実績に関する情報を表形式で一覧することができる。

[19] http://www.apnic.net/meetings/12/docs/My-APNIC.ppt から抽出

図 26　MyAPNIC 割り当て表

- 割り当て編集

ここでは選択したネットワークに関する情報のうち、ネットワーク名、デバイスの数、サブネットの数、割り当て日時について、オンラインで編集することができる。

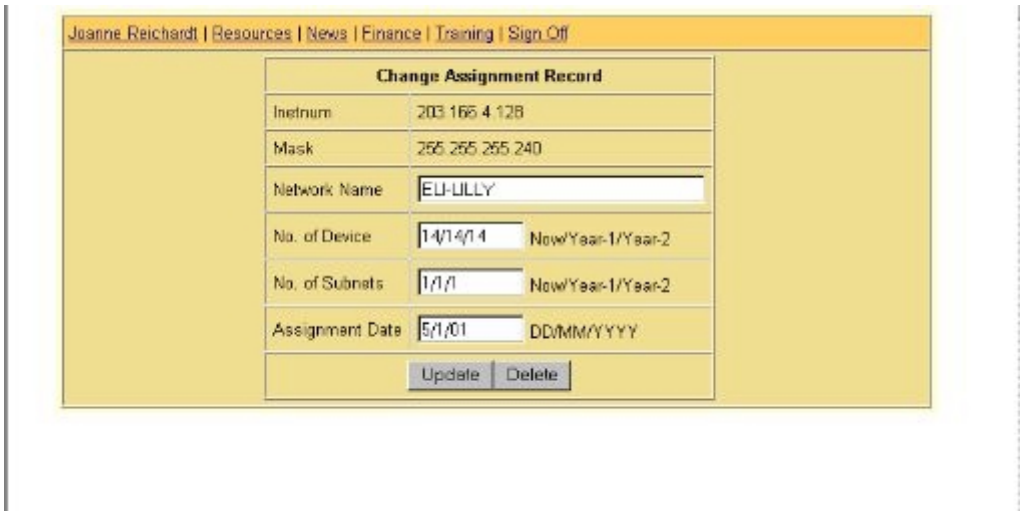


図 27　MyAPNIC 割り当て編集

- 新規割り当て

ここでは所有するネットワーク情報に新規割り当てレコードを登録することができる。その情報は、ネットワークアドレス、ネットワークマスク、ネットワーク名、デバイスの数、サブネットの数、割り当て日時となっている。

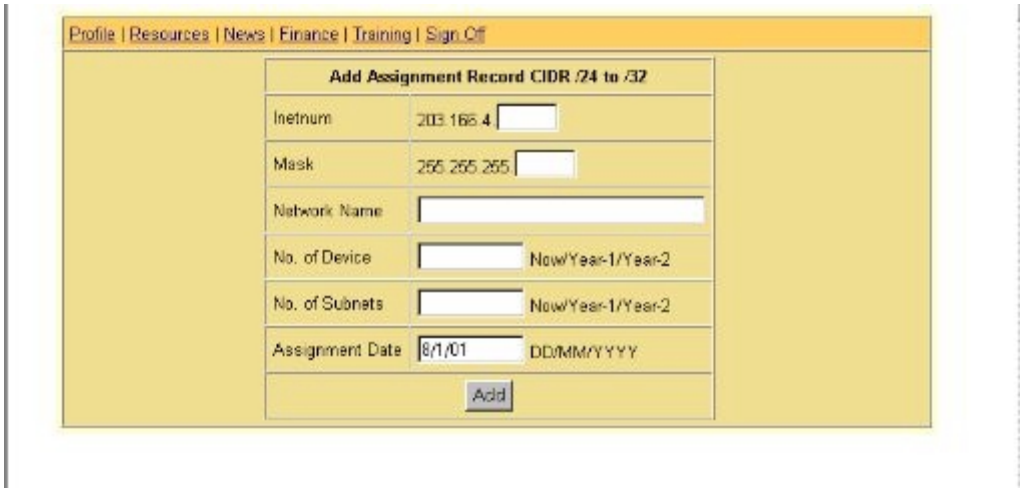


図 28　MyAPNIC 新規割り当て

- プロファイル編集

ここではメンバーのプロファイル情報を編集することができる。その情報は、フルネーム、ポジション、アドレス（都市、州、国、郵便番号）、電話番号、ファックス番号、ホームページ、電子メールアドレスとなっている。

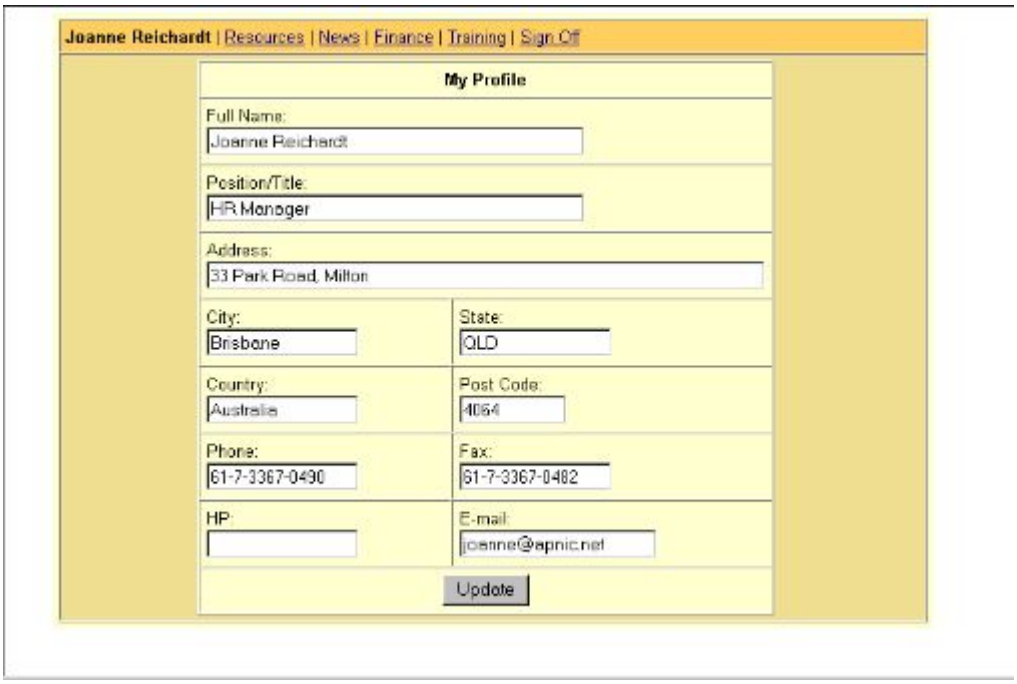


図 29　MyAPNIC プロファイル編集

3.1.5. 今後の展開

APNIC CA プロジェクトの今後の展開に関しては次のような議論が行われている。

- CA 機能の一般化
  - APNIC の証明書を汎用目的で使う
  - 信頼を確保するため APNIC 証明書の強固なポリシー作成と質の高いフレームワークの確立
- 階層的証明
  - APNIC のメンバーが彼ら自身のメンバーや顧客を証明するために、自身の証明書を使う
  - ISP や NIR に利用可能
- 公開鍵証明書
  - アイデンティティの公開鍵にリンクされる証明書（CA が発行）
- 属性証明書
  - アイデンティティの属性にリンクされる証明書（CA または他のオーソリティが発行）
  - 認証のみならず認可情報を提供

（属性証明書は広く採用されてはいない）

3.2. RIPE NCC

RIPE ではデータベースワーキンググループにてセキュリティに関する議論が行なわれている。

1998 年、1999 年とデータベースセキュリティタスクフォースで議論が行なわれていたが、2000 年 2 月の RIPE Meeting 第 35 回以降はワーキンググループに話し合いの場が移された。

2001 年 4 月の同ミーティング第 39 回の会議では PGP でも保護されたオブジェクトが全体の 2%に過ぎないことが報告された。また同じ会議で PGP ライセンスサービスの停止を求める提案がなされた、これは既知の問題のある PGP を使ったライセンスが発行されていること、新しいデータベースが GnuPG を使っていることが理由とされている。

同ミーティング第 42 回の会議では MD5-PW スキームがテストデータベースに導入されたことが報告された。またハッシュパスワードを remarks オブジェクトに埋め込む方式が提案された。

2002 年 9 月の同ミーティング第 43 回では、メインテナの 41%が MD5-PW スキームを利用していることが報告された。この会議では電子メールベースのインタラクションがビギナーには複雑であることから、データベースアクセスにウェブインターフェースを実装することが提案されている。この実装は WebUpdates と呼ばれており、オブジェクトの追加、削除、修正が可能となっている。しかし、パスワード認証のみであること、パスワードがクッキーに保存されることから、この段階ではプロトタイプに過ぎない（このプロトタイプは既に公開されていない）。

3.2.1. オブジェクトの保護

RIPE のデータベースでは、あるオブジェクトが変更されると、そのオブジェクトの所有者であるメインテナに通知されるように設定を行なうことが出来る。また、変更の際に認証を必須とするためにいくつかの認証スキームが設定可能である。この認証スキームを用いるためには以下の手順を実施する。

- mntner オブジェクトに auth:属性を追加
  - NONE、無認証
  - MAIL-FROM、指定した正規表現がメールヘッダの From:に適合することを検

証。容易に成りすましが可能なため推奨されない（すでに使われない）
  - CRYPT-PW、UNIX CRYPT フォーマットによるパスワード検証。パスワードが平文で通信されるため推奨されない
  - MD5-PW、ハッシュパスワード検証。CRYPT-PW よりは良いが強力なものではない。
  - PGPKEY、公開鍵暗号に基づく認証。提供される認証機構中で最も強力
- 認証を要するオブジェクトに mnt-by 属性を追加
- 選択した認証スキームに対するパスワードまたは公開鍵を登録(パスワードの場合は auth: 属性、公開鍵の場合は key-cert: オブジェクトを登録し、auth: 属性には、その ID を登録する)

3.2.2. WebUpdates

現在、WebUpdates は SSL ベースのアプリケーションとして稼動しており、サーバ証明書は米 RSA Security 社によって発行されたものである。このアプリケーションは SSL 経由でも通常の HTTP でもアクセスできる[20]

このインターフェースはサーバ認証のみであり、RIPE 自身での CA 運用もされていない。

RIPE Meeting 第 43 回で WebUpdates の発表が行なわれている。Synchronous Updates and Web Updates in RIPE Database[21]がそれである。

その発表で述べられた現状の更新システムの問題は次のものである。

- 自動化、または管理化の観点から便利なものとはいえない
- 要求の提出と処理に遅れがあり、またどの程度遅れるのかわからない
- ビギナーを悩ませることがある（提出した要求に不備があった場合、エラーメールが送り返され、それに対して再びメールを返して、などしていると効率的でない）
- ほとんどのユーザにとっては電子メールによるインタラクションはなじみの無いものである

そして解決策として次の二つが提案されている。

- 同期した更新の仕組み – syncupdates
- syncupdates に対するウェブインターフェース – WebUpdates

syncupdates が同期するものはいるのは、ユーザが提出した追加、削除、変更要求が

[20] “Web Updates for RIPE Database”, http://www.ripe.net/webupdates/
[21] http://www.ripe.net/ripe/meetings/archive/ripe-43/index.html

直ちに受理されるということであり、実際にデータベースに反映させるのは既存のシステムであるため、処理終了通知は従来どおり電子メールにより送信される。

しかし、インターフェースの時点でデータの不備などは判明するため、以前の電子メールによるやり取りに比べてストレスの少ないものとなることが期待されている。

このシステムの課題としては、ユーザのローカルホスト上にパスワードが格納されるという単純な認証しか行なっていないことから、PGP による認証機構の実装があげられている。

3.2.3. LIR Portal

LIR Portal は、2002 年 9 月からベータテストが開始されたサービスで、LIR による RIPE NCC へのアクセスの増加を受け、ウェブインターフェースを提供することで遅延の減少を目的とするものである。

サポートされる機能には次のものがある。

- LIR コンタクト情報、アドレス情報の閲覧と編集
- 支払い情報の閲覧
- IP および AS リソースの閲覧
- オープンチケット状況の閲覧
- ニュースおよびイベント

このウェブサービスは SSL を通じて提供される。利用するためには、前もって登録を行なう必要がある。

3.2.4. RPSL (Routing Policy Specification Language)

RPSL とは Routing Policy Specification Language [22]で定義されるルーティングポリシー記述言語である。ネットワークオペレータは様々な階層でこの記述を使ってポリシーを定義することができる。

この言語はオブジェクト指向言語として設計されており、オブジェクトがポリシーと管理情報を持つことになる。定義されたオブジェクトは IRR（Internet Routing Registry）に格納される。

---

[22] RFC2280, “Routing Policy Specification Language (RPSL)”, http://www.ietf.org/rfc/rfc2280.txt

表 14 は経路オブジェクトの構造定義を示している。このように RPSL のオブジェクトは（属性、値の概要、値の型）として定義される

表 14　RPSL オブジェクトの例

Attribute	Value	Type
route	<address-prefix>	mandatory, single-valued, class key
origin	<as-number>	mandatory, single-valued, class key
withdrawn	<date>	optional, single-valued
member-of	list of <route-set-names> see Section 5	optional, single-valued
inject	see Section 8	optional, multi-valued
components	see Section 8	optional, single-valued
aggr-bndry	see Section 8	optional, single-valued
aggr-mtd	see Section 8	optional, single-valued
export-comps	see Section 8	optional, single-valued
holes	see Section 8	optional, single-valued

RPSL の目的は、実際にルータで利用される経路情報に加え、管理情報をデータベースとして提供することにある。

3.3. ARIN

ARIN は RPSL によるデータベースを管理しており、その保護の仕組みも RIPE と同様のものである。ARIN には RIPE のデータベースワーキンググループと同様の組織としてデータベース実装ワーキンググループが機能しており、1999 年 4 月の会合でデータベース保護について話されている。

3.3.1. RWhois

RWhois は ARIN により開発されている分散型の whois サービスのことである。従来の whois サーバは中央集権的データベースを持っている。これに対し RWhois では階層的でスケール可能なやり方でデータベースを保持する。RWhois については Referral Whois (RWhois) Protocol V1.5 [23]に詳細が述べられている。

[23] RFC2167, “Referral Whois (RWhois) Protocol V1.5”,

これは一種のディレクトリサービスと位置付けられ、whois のコンセプトを階層的に拡張したものといえる。インターネットをまたいでリソースを発見するための効率的なプロトコルを目指しており、分散データベースである DNS システムを参考にしている。

ある RWhois サーバに対する問い合わせが解決されなかった場合、サーバは、答えを知っているサーバに近いところにあると考えられるサーバへと、クエリを再配送する。これは DNS の再帰問い合わせのメカニズムである。

現状の問題として、分散データベースであるにも関わらず、RWhois サーバを稼動させているインターネットレジストリが少ないため、本来のメリットが生かせないことがあげられる。

しかし、ネットワーク資源の今後の更なる増加を考えると RWhois のような分散データベースの重要性は増すと考えられる。

3.4. RIR の whois システム

ここでは RIR における情報提供サービスである whois システムの外部インターフェースと提供される情報について解説を行なう。システムは ARIN の提供するものと RIPE の提供するものの二つが存在する。APNIC、LACNIC については共に RIPE の開発しているシステムを用いている。

whois サービスは一般に公開されているサービスであるため、提供される情報について知ることは、サービスに必要な保護についての考察を行なう上で重要であると考えられる。

特に組織情報、個人情報には、住所、電話番号といったプライベートな情報が含まれることから、第三者による不正な改ざんから保護すること、また特定の情報についてはビジネス上の観点からアクセス制限を施すことが必要となることも考えられる。

3.4.1. ARIN

ARIN の Whois サービスは ARIN に登録されたリソースのコンタクトおよび登録情報を検索するためのメカニズムを提供する。ARIN のデータベースは IP アドレス、AS 番号、それらのリソースに関連する組織または顧客そして関連するポイントオブコンタ

---

http://www.ietf.org/rfc/rfc2167.txt

クト（POC）を含む。ARIN の Whois はドメイン関連情報、また軍関係の情報を持つことは無い。

実際に www.arin.net 192.149.252.17 のデータを検索すると表 15、表 16、表 17 の出力が得られる。

- Organization Information

表 15　ARIN の whois 出力（組織情報）

OrgName:	American Registry for Internet Numbers
OrgID:	ARIN
Address:	3635 Concorde Parkway, Suite 200
City:	Chantilly
StateProv:	VA
PostalCode:	20151
Country:	US

- Network Address Space Information

表 16　ARIN の whois 出力（ネットワークアドレス空間情報）

NetRange:	192.149.252.0 - 192.149.252.255
CIDR:	192.149.252.0/24
NetName:	ARIN-NET
NetHandle:	NET-192-149-252-0-1
Parent:	NET-192-0-0-0-0
NetType:	Direct Assignment
NameServer:	RS1.ARIN.NET
NameServer:	NS.NETSOL.COM
NameServer:	RIP.PSG.COM
Comment:	
RegDate:	1997-11-05
Updated:	2002-04-05

- Contact Information

表 17　ARIN の whois 出力（コンタクト情報）

```
TechHandle: IP-FIX-ARIN
TechName:   ARIN IP Team
TechPhone:  +1-703-227-0660
TechEmail:  hostmaster@arin.net
OrgTechHandle: IP-FIX-ARIN
OrgTechName:   ARIN IP Team
OrgTechPhone:  +1-703-227-0660
OrgTechEmail:  hostmaster@arin.net
OrgNOCHandle: ARINN-ARIN
OrgNOCName:   ARIN NOC
OrgNOCPhone:  +1-703-227-9840
OrgNOCEmail:  noc@arin.net
```

情報の非公開については “Instructions for Executing ARINs Non-Disclosure Agreement” [24]に詳細が記載されている。ここには ARIN に送信した情報のうち、組織にとってプロプライエタリな情報について非開示契約を ARIN と組織の間に結ぶ際の手続きについて書かれている。

プロプライエタリな情報とは次のようなものと定義され、またそれに限定される。

- ネットワークエンジニアリング計画(次のものを含む、サブネット、ホスト数、サブネット辺りのホスト数)
- ネットワーク配備計画（それぞれのサブネットの主要なマイルストーンを含む）
- 申請者によって作成されたネットワークトポロジー図(一般に公開されたものを含まない)
- 申請者が、無制限な開示、コンペティティブな利用に対抗して保護するこ

[24] “Instructions for Executing ARINs Non-Disclosure Agreement”, http://www.arin.net/library/agreements/nda.pdf

とを希望するその他の情報(この NDA に従って提出されたと互いに合意し、ARIN に提出された際にプロプライエタリであると明確に特定されたもの)

その情報がプロプライエタリであることを明示するために、申請書類ではボールドフェイスで記入されることになっている。

3.4.2. RIPE

RIPE Network Management Database の要素として IP アドレス情報が格納されている。

www.ripe.net 193.0.0.203 を検索すると次の出力が得られる。

```
netnum:        193.0.0.0 - 193.0.1.255
netname:       RIPE-NCC
descr:         RIPE Network Coordination Centre
descr:         Amsterdam, Netherlands
country:       NL
admin-c:       DDL122-RIPE
tech-c:        OPS4-RIPE
status:        ASSIGNED PI
remarks:       used to be two different /24 inetnum objects
remarks:       until 19990305  (ripe-ncc & ripe-meeting)
mnt-by:        RIPE-NCC-MNT
mnt-lower:     RIPE-NCC-MNT
changed:       orange@ripe.net 19960815
changed:       GeertJan.deGroot@ripe.net 19970110
changed:       mir@ripe.net 19970506
changed:       ripe-dbm@ripe.net 19970819
changed:       wilhelm@ripe.net 19990305
changed:       inaddr@ripe.net 19990705
changed:       hostmaster@ripe.net 20010119
changed:       hostmaster@ripe.net 20020410
source:        RIPE
```

3.5. RIPE Database System

RIPE データベースは RPSL を用いている。RPSL はインターネット経路情報レジストリに高度なセキュリティを提供する認可メカニズムを提供する、Routing Policy System Security (RPSS) を実装している。

RIPE ネットワーク管理データベースは IP アドレス空間割り当てと割り振り、経路制御ポリシー、逆引き委譲に関する情報を含むものである。

RIPE データベースの情報はインターネットの公共に提供されるものであるが、著作権は RIPE が所有する。

3.5.1. データベースオブジェクト

RIPE ネットワーク管理データベースは以下のレコードを含む：

- IP アドレス空間の割り当てと割り振り
- ドメイン名 (in-addr.arpa.)
- 経路制御ポリシー情報
- コンタクト情報

データベース中のレコードはオブジェクトと呼ばれる。これには表 18 のものがある。

表 18　データベース中のオブジェクトリスト

Object type (Class name)	短縮形	説明
As-block	Ak	リポジトリに付与された AS 番号の範囲を示す
As-set	As	Aut-num オブジェクトの集合
aut-num	An	データベース中の AS を示す。
domain	Dn	(正引き、逆引き) ドメイン登録
filter-set	Fs	フィルターにマッチする経路の集合
inet6num	i6	IPv6 アドレス空間の割り当て割り振り情報
inetnum	In	IPv4 アドレス空間の割り当て割り振り情報
inet-rtr	Ir	Represents a router in the database.

irt	It	CSIRT のコンタクト、認証情報
key-cert	Kc	メンテナオブジェクトの更新の際に認証に利用される公開鍵証明書
mntner	Mt	メインテナによって保護されるオブジェクトに対する操作（生成、削除、修正）に対して要求される認証情報を特定する
peering-set	Ps	Peering の集合
person	Pn	技術または管理コンタクトの情報
role	Ro	技術または管理コンタクトの情報だが、人間により実行される役割を記述する
route	Rt	インターネットに広報される経路
route-set	Rs	経路の集合
rtr-set	Is	ルータの集合

各オブジェクトには標準テンプレートが用意される。

- as-block

as-block オブジェクトは AS 番号のレンジを委譲するために必要である。このオブジェクトは as-block: 属性によって特定される範囲内の ant-num オブジェクトの生成のための認可に使われる。

```
as-block:       [mandatory]  [single]     [primary/lookup key]
descr:          [optional]   [multiple]   [ ]
remarks:        [optional]   [multiple]   [ ]
tech-c:         [mandatory]  [multiple]   [inverse key]
admin-c:        [mandatory]  [multiple]   [inverse key]
notify:         [optional]   [multiple]   [inverse key]
mnt-lower:      [optional]   [multiple]   [inverse key]
mnt-by:         [mandatory]  [multiple]   [inverse key]
changed:        [mandatory]  [multiple]   [ ]
source:         [mandatory]  [single]     [ ]
```

- inetnum

inetnum オブジェクトは IPv4 アドレス空間の割り当て割り振り情報を含む。

```
inetnum:        [mandatory]  [single]     [primary/lookup key]
```

netname:	[mandatory]	[single]	[lookup key]
descr:	[mandatory]	[multiple]	[ ]
country:	[mandatory]	[multiple]	[ ]
admin-c:	[mandatory]	[multiple]	[inverse key]
tech-c:	[mandatory]	[multiple]	[inverse key]
rev-srv:	[optional]	[multiple]	[inverse key]
status:	[mandatory]	[single]	[ ]
remarks:	[optional]	[multiple]	[ ]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
mnt-lower:	[optional]	[multiple]	[inverse key]
mnt-routes:	[optional]	[multiple]	[inverse key]
mnt-irt:	[optional]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- inet-rtr

ルータは inet-rtr クラスで特定される。inet-rtr: 属性はルータを表す妥当な DNS 名である。alias 属性が提示されたならば、それはルータのカノニカル DNS 名である。local-as: 属性は、このルータによって所有もしくは操作される AS の AS 番号を特定する。

inet-rtr:	[mandatory]	[single]	[primary/lookup key]
descr:	[mandatory]	[multiple]	[ ]
alias:	[optional]	[multiple]	[ ]
local-as:	[mandatory]	[single]	[inverse key]
ifaddr:	[mandatory]	[multiple]	[lookup key]
peer:	[optional]	[multiple]	[ ]
member-of:	[optional]	[multiple]	[inverse key]
remarks:	[optional]	[multiple]	[ ]
admin-c:	[mandatory]	[multiple]	[inverse key]
tech-c:	[mandatory]	[multiple]	[inverse key]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- irt

irt オブジェクトは CSIRT のコンタクトおよびセキュリティ情報を表す。アドレスレンジに対するコンピュータおよびネットワークインシデントのハンドリングに責任ある CSIRT を特定するために inetnum または inet6num オブジェクトから参照される。Irt の名前は “IRT-“ で始めなければならない。

irt:	[mandatory]	[single]	[primary/lookup key]
address:	[mandatory]	[multiple]	[ ]
phone:	[optional]	[multiple]	[ ]
fax-no:	[optional]	[multiple]	[ ]
e-mail:	[mandatory]	[multiple]	[lookup key]
signature:	[mandatory]	[multiple]	[ ]
encryption:	[mandatory]	[multiple]	[ ]
admin-c:	[mandatory]	[multiple]	[inverse key]
tech-c:	[mandatory]	[multiple]	[inverse key]
auth:	[mandatory]	[multiple]	[ ]
remarks:	[optional]	[multiple]	[ ]
irt-nfy:	[optional]	[multiple]	[inverse key]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- key-cert

key-cert オブジェクトはサーバに格納される公開鍵のデータベースで、mntner オブジェクトの更新を実施する際の認可に使われる。現在は”OpenPGP Message Format[25]”に準拠した鍵だけがサポートされる。

key-cert:	[mandatory]	[single]	[primary/lookup key]
method:	[generated]	[single]	[ ]
owner:	[generated]	[multiple]	[ ]
fingerpr:	[generated]	[single]	[ ]
certif:	[mandatory]	[multiple]	[ ]

[25] RFC2440, “OpenPGP Message Format”, http://www.ietf.org/rfc/rfc2440.txt

remarks:	[optional]	[multiple]	[ ]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- mntner

RIPE データベース中のオブジェクトは mntner オブジェクトを使うことで保護される。このオブジェクトは、生成、削除、修正に必要な認証情報を特定する。このオブジェクトは自動的には生成されず、手動操作によって RIPE データベース管理業務に転送される。

mntner:	[mandatory]	[single]	[primary/lookup key]
descr:	[mandatory]	[multiple]	[ ]
admin-c:	[mandatory]	[multiple]	[inverse key]
tech-c:	[optional]	[multiple]	[inverse key]
upd-to:	[mandatory]	[multiple]	[inverse key]
mnt-nfy:	[optional]	[multiple]	[inverse key]
auth:	[mandatory]	[multiple]	[ ]
remarks:	[optional]	[multiple]	[ ]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[mandatory]	[multiple]	[inverse key]
referral-by:	[mandatory]	[single]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

- person

このオブジェクトは技術または管理コンタクトに関する情報を含む。いったんオブジェクトが生成されると、person: 属性を変更することはできない。

person:	[mandatory]	[single]	[lookup key]
address:	[mandatory]	[multiple]	[ ]
phone:	[mandatory]	[multiple]	[ ]
fax-no:	[optional]	[multiple]	[ ]
e-mail:	[optional]	[multiple]	[lookup key]
nic-hdl:	[mandatory]	[single]	[primary/lookup key]

remarks:	[optional]	[multiple]	[ ]
notify:	[optional]	[multiple]	[inverse key]
mnt-by:	[optional]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[ ]
source:	[mandatory]	[single]	[ ]

3.5.2. Queries in the RIPE Database

データベースへの問い合わせは whois プロトコルクライアントを介して行われる。

新しく導入されたメカニズムは、問い合わせの結果を自動的に追跡し、RIPE データベースからのコンタクト情報の取り寄せを制限する機能である。広告などのデータとしての検索を制限するのが目的である。

サーバのレスポンスには一般的な規則がある：

- % サインで始まる出力はレスポンスコードから情報メッセージである。コメントは%サインの後に空白が一つあり、サーバメッセージは%サインのすぐ後に始まる。
- 空行はオブジェクトのデリミタである。
- 二つの空行はサーバレスポンスの終了を意味する。
- レファラルメカニズムを使っている場合、レファラルサーバの出力は修正なしにクライアントに送られる。

3.6. まとめ

RIR のデータベースはいずれも RPSL を用いている。しかし、そのオブジェクトの保護に関しては意見が異なっている。

RIPE NCC では、PGP を使った認証を推奨してはいるものの、PGP になれていないユーザの存在、環境によっては利用上の問題があることなどから、オブジェクトごとに認証に関する選択権を与えていて、必要としないのであれば認証なしで操作できるオブジェクトも多く存在しているという現状となっている。

また、ユーザ管理インターフェースとして WebUpdates を配置しているが、これはサーバ認証を SSL で提供しているのみで、必要でなければ通常の HTTP でもアクセスできるなど、基本的にユーザが必要とするセキュリティを選択して用いればよいという考えに基づいているとものと考えられる。

これに対し、APNIC の CA プロジェクトは証明書の発行を担うことで、PKI の強力な認証機能をユーザに提供するという高い目標を持ったものである。CA の運営に関する課題は多いが、PKI の認証トポロジーと規模拡張性を考えると、今後の応用が期待できる。

ARIN は RWhois の開発を通じて、従来の whois サービスを大きく拡張するスキームを提唱している。DNS に倣った分散データベースサービスである RWhois には、今のところ認証やデータ保護に関する機能が乏しいが、セキュリティ拡張は随時行われていくものと期待される。

いずれの RIR も地域性による制限もあると思われ、データ保護に関するアプローチは異なっているが、保護をどれだけ機能させることができるのかについてはユーザの選択に任されている。

MyAPNIC プロジェクトでは、ユーザの PKI に対する意識の向上を目的の一つに挙げており、ユーザの利便性と安全性に対する検討が行われたことがうかがえる。

第4章 セキュリティを考慮した運用要件

内容

- 認証業務のセキュリティ要件
  - 認定基準／ガイドラインの比較調査
  - 各比較項目についての考察
    1. 各事項について記述
  - 認証局の立ち上げにおける留意事項

※各項目を記述した「基準比較表」を報告書の最後に添付

4. 運用のセキュリティ要件

PKI を利用してネットワーク資源に関する登録情報の証明を行う為には、ネットワーク資源の情報管理システムの他に、認証局が必要となる。従ってインターネットレジストリには、既存のネットワーク資源管理のほかに、認証局の運用と証明書の扱いに関する業務が新たに必要となる。

また官公庁、商用組織、学校法人、任意団体といった様々な組織に対して公平な立場でネットワーク資源を管理するためには、インターネットレジストリにおける認証局が、各組織のセキュリティレベルに比べて十分な確実さをもって運用されなければならない。そのためには、認証局の構築に先立ち、運用の確実さの要件、つまりセキュリティ要件を整理する必要がある。本調査研究では、認証業務の認定基準やガイドラインの調査を通じ、認証業務のセキュリティ要件として比較調査した。本章では NIR における認証局の運用と認証業務の遂行のために挙げられるセキュリティ要件として、この調査について述べる。

4.1. 本章の目的

インターネットにおけるネットワーク資源の管理という観点に適用できる認証業務のガイドライン等は未だ存在していない。しかし認証業務の内容を詳細化するに先立ち、そのセキュリティ要件を明確化する必要がある。そこで既存の認証局に関わるセキュリティ要件を列挙・比較し、各々の項目について検討を行うこととする。この比較検討によって、認証局の構築の際に考慮すべきセキュリティ項目やセキュリティレベルの元になる検討資料ができる。また認証局に認定基準の比較という活動は、未だ一般的には行われていないため、本章は汎用的な認証局のセキュリティ要件の検討資料に十分なりうると考えられる。

4.2. 概要

4.2.1. 概要と構成

認証局に関わるセキュリティ要件として、日本及び米国に存在する認証局の認定基準や運用ガイドラインを取り上げ、CPS（Certification Practice Statement）の記載項目を基準として、セキュリティ要件の分類を整理し、各々の項目について検討事項及び留意事項を記す。はじめに各基準の概要を述べ、次に基準の比較と考察を行う。更に各認定基準の項目について具体的な比較を行う。この具体的な比較については添付資料「基準比較表」として添付した。

CPS の記載事項の列挙には RFC2527[26]を利用した。RFC2527 は CPS の記載項目を整理し、網羅的に列挙したものである。

4.2.2. 対象とする基準

認証業務のセキュリティ基準としては、認証局又は認証業務の認定制度における認定基準及び民間又は公的機関が公表するガイドラインが挙げられる。認定制度における基準として国際的な基準は、ANSI（American National Standards Institute）X9.79 をベースにした WebTrust for CA である。わが国では、電子署名及び認証業務に関する法律（以下では署名法とよぶ）に基づく認証業務の認定基準がある。

強固な認証局の構築を検討するために、比較調査の対象として次の基準を取り上げる。

(1) 認証局運用ガイドライン V1.0（平成 10 年 3 月）

- 電子商取引実証推進協議会（ECOM）*1、認証局検討ワーキンググループ
  *1：現在の組織名称は「電子商取引推進協議会」

(2) 電子署名法

- 電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日法律第 102 号）
- 電子署名及び認証業務に関する法律施行規則（総務省、法務省、経済産業省省令第 2 号、平成 13 年 3 月 27 日）
- 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（総務省、法務省、経済産業省告示第 2 号、平成 13 年 4 月 27 日）
- 特定認証業務調査表 V2.0（2002.11.21 版) の適合例：日本品質保証機構、電子署名・認証調査センター

(3) WebTrust Program for Certification Authorities V1.0（2000 年 8 月 25 日）

- AICPA（American Institute of Certified Public Accounts）／CICA（Chartered Accountants of Canada）

これら以外に認証局のセキュリティ基準を表しているものとして、公表されている CP（Certificate Policy - 証明書ポリシー）又は CPS がある。CP/CPS におけるセキュ

[26] RFC2527, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, http://www.ietf.org/rfc/rfc2527.txt

リティの記述は、当該認証局の証明書発行目的などによってさまざまである。高度なセキュリティを確保して運営されている認証局で参考になる CP/CPS は、金融系の Identrus 及び海外政府系の FBCA（Federal Bridge CA - アメリカ連邦政府のブリッジ認証局）の CP/CPS であるが、ともに WebTrust と同様 ANSI9.79 をベースにしている。

4.2.3. 比較の視点について

3 つの基準はそれぞれ基準の項目分類が異なるため、比較にあたっては共通の項目分類を適用する必要がある。RFC2527 は CP と CPS のフレームワークを提供しており、これらをベースに各基準等の項目を当てはめて比較する。

RFC2527 は認証局に焦点を当てているため、一般的な情報セキュリティの項目よりも鍵管理や証明書管理に重点を置いているが、認証局にかかる基準の比較という点からは、RFC2527 の視点がよいと考える。

各基準において RFC2527 の項目に含まれない基準に関しては、RFC2527 の別項として記述する。

4.3. 調査対象基準の概要

(1) 認証局運用ガイドライン V1.0（ECOM）

> 認証局運用ガイドライン（以下では「ガイドライン」とよぶ）は、公開鍵暗号システムを利用した公開鍵証明書の発行・開示・更新・廃棄などの認証管理サービスを提供する認証局が、その信頼性及び安全性を確立する上で必要な要件を提示することを目的としている。本人確認のための書類及び認証方法についても、その具体的基準を示している。しかし、あくまで認証局（CA）の運用にかかわる範囲の対策基準を規定しており、証明書所有者自身による私有鍵管理等については規定していない。
>
> ガイドラインが読者として想定しているのは、認証局の運営者であり、特に、不特定多数の間で行われる電子商取引や電子決済、電子データ交換、電子メールなどで利用可能な認証書を発行する社会的影響度の大きい認証局に焦点を合わせている。さらにガイドラインでは、より高レベルなセキュリティが要求される認証局（例えば認証局に証明書を発行するような上位認証局）に関して参考的に要件を定めている。本報告書では高レベルなセキュリティ要件に焦点を当て、取り上げている。

(2) 電子署名法　特定認証業務調査表 V2.0(2002.11.21 版)

電子署名や電子認証が本人確認の手段として利用され、ネットワークを通じて取引を行った場合に、その法的な位置付けが明確ではなかったため安心して電子商取引を行うことができないという心配があった。そこで、政府は電子署名や電子認証を行う業務に一定のルールを課して、電子署名を手書きの署名や押印と同様な法的位置付けとする法律､「電子署名及び認証業務に関する法律」を成立させた。署名法の施行により、認証業務のうち一定の基準を満たすものは総務大臣、経済産業大臣及び法務大臣の認定を受けることができる制度が導入された。

認定の基準は、申請に係る業務の用に供する設備が主務省令で定める基準に適合すること、申請に係る業務における利用者の真偽の確認が主務省令で定める方法により行われるものであること、その他申請に係る業務が主務省令で定める基準に適合する方法であることとなっている。「認定」を受けている認証業務については、それが一定基準の信頼性を有していることを国が証明していることになり、署名法 3 条の「電磁的記録の真正な成立の推定」が働きやすくなることが期待される。

署名法で定める特定認証業務の認定事業者が発行する証明書は、個人の印鑑登録証明書に相当する。そのため、認証局における本人確認等については、極めて高いレベルの基準での運用を要求している。国が認定する認証業務であるため、その認定基準（要件）は詳細かつ具体的であり、この点が取り上げた他の基準と大きく異なる点である。

本報告書では、認定の審査において指定調査機関が使用する調査表の適合例を署名法のセキュリティ要件として取り上げた。法律の階層は、法－施行規則－告示（指針）であり、適合例はあくまでも指針を満たす一つの方法なのであるが、適合例は実質的に告示の細則の位置付けにある。

(3) WebTrust Program for Certification Authorities Version1.0（AICPA/CICA）

WebTrust Program for Certification Authorities （以下では WebTrust とよぶ）は､米国公認会計士協会（AICPA）とカナダ公認会計士協会（CICA）によって定められた認定制度であり、電子商取引を行う事業者に対するセキュリティ認定基準として著名である。証明書ポリシー及び認証局実施規定（CP/CPS）等として開示すべき項目及び完全な認証サービスのための対策基準を網羅的かつ詳細に規定しており、認定取得のための実用的なフレームワークを提供している。Microsoft 社では、Web ブラウザへ信頼できる証明書として登録する際に WebTrust の認定を要件としている。

WebTrustでは､本人確認のための手続等の基準は示していないものの、適切な本人確認のために必要な対策基準を、具体例を挙げつつ網羅的かつ詳細に規定している。認証局のあらゆる運用に対応できるよう、認証局による発行申請者の鍵ペア生成・管理、暗号用鍵の扱いについても網羅的に項目を挙げ、各々に対し一定の対策基準を規定している。

4.4. 調査対象基準比較

本節では RFC2527 をビューとした各種基準の比較考察を行う。2.2.1.から 2.2.8 において、［X］、［X.X］のように項番号の右の括弧書きで示した数字は、RFC2527 における章、節、項の番号を示している。2.2.9 は、RFC2527 の項目に含まれない基準について記述した。また、使用する用語は、統一し 3 基準において同意義となるよう記述している。

なお、基準等の詳細については添付資料の基準比較表を参照するものとする。

4.4.1. ［1］はじめに

【RFC2527 記述内容】

当該認証局がどのような認証局であるのか（主体者の記述)、証明書の利用目的、制限事項、利用環境、適用範囲、発行対象、規定集の正式名称と識別子、連絡先など、概要として記載すべき事項に関する要件

【各基準の概要】

3 基準ともに、証明書のポリシー、使用目的、適用範囲、発行対象、制限事項を明確にするよう求めている。署名法においては、加えて、開示すること（指針第 12 条第 1 項第二号）を必要としていることを明記している。WebTrust では CP/CPS のバージョン、有効日付の記述も求めている。

連絡先については、署名法、WebTrust ともに管理組織の連絡先として組織名、責任者、住所、TEL、FAX、メールアドレスの明確化及び開示を求めている。

用語については各種基準ともに特に規定はしていない

【考察】

識別については、規定集（CP/CPS）の名称及び CP のオブジェクト識別子を記述することとなる。これは、証明書拡張の CertificatePolicy 属性において、OID による制御を行う場合等に重要な意味を持つ。

コミュニティと適用性については、認証局が発行する証明書をどのような目的で、どのような組織、人、物に対して流通させるのかという重要な要素を含んでいる。流通させる適用範囲が明確にならないと、本人認証手段、証明書の検証手続等にも影響する。また、適用範囲、使用目的が明らかでないと、証明書に関する事故、訴訟への発展も危惧されるので十分な検討が必要と思われる。

4.4.2. ［2］一般条項

4.4.2.1. ［2.1］義務

［2.1.1］認証局の義務　及び　［2.1.2］登録局の義務

【RFC2527 記述内容】
認証局及び登録局の義務に関する要件。

【各基準の概要】
ガイドラインでは認証局の信頼性と安全性を確保するために必要な運用要件等を明確にし、手順・手続を定めることを求めている。また、利用者、検証者の守るべき義務等について適切な情報の開示又は告知を求めている。

署名法においては、電子署名実施方法及び認証業務の利用に関する重要事項の利用者への説明を義務としている。また、利用者への説明手段を具体的に規定している。さらに、署名法に基づく特有な要件として、虚偽の申し込みに対する法的な罰則があることの説明義務（指針第 8 条第一号）について記述されている。

WebTrust においては、証明書の発行、失効、停止を利用者及び利用者以外へ通知するよう求めている。

【考察】
検証者等の義務を明確にすることは必要であるが、認証事業者と直接契約関係にないため、どのように通知するかが難しい問題である。

［2.1.3］利用者（証明書所有者）の義務

【RFC2527 記述内容】

利用者（証明書所有者）の義務に関する要件。

【各基準の概要】
3 基準ともに、利用者の義務として、正確な虚偽のない情報に基づく申請、自身の私有鍵の保護、情報に変更があった場合の迅速な連絡又は失効申請、鍵が危殆化した場合又はおそれがある場合の迅速な失効申請の義務を CP、CPS、その他書類等へ記述するよう求めている。

ガイドラインは、上記の他に、発行された証明書の記載情報を確認することを利用者の義務に挙げている。

WebTrust では 1.1.1.4.に、ポリシー、CPS に従った証明書の利用が記述されている。

署名法は利用者の義務を直接的に定めていないが、指針第 8 条(2)の認証局による説明義務の中で利用者の義務を記述している。利用者が認証局の指定するアルゴリズムを使用することも利用者の義務としている。

【考察】
利用者が認証局の指定するアルゴリズムを使用することを求めることは必要である。

［2.1.4］検証者の義務

【RFC2527 記述内容】
証明書を受け取りその証明書を信用し利用しようとする検証者の義務に関する要件。

【各基準の概要】
3 基準ともに、証明書の使用目的の確認義務、デジタル署名検証、失効、停止を確認する義務、を挙げている。

ガイドラインでは他に取引の重要性、認証の真正性保証レベルや補償レベル等に応じて、自身の使用目的に適しているかの判断を行うこと、証明書以外の他の確認手段を併用することを記述している。

【考察】
一般的な検証手段の他に、高額な取引に証明書を利用する場合、ガイドラインに記述されているように取引の重要性、補償レベル等によって検証者が判断すること、また他の確認手段の併用を求めることが重要と思われる。

［2.1.5］リポジトリの義務

【RFC2527 記述内容】
証明書と失効情報の適時な公表の義務に関する要件。

【各基準の概要】
ガイドライン及び署名法では、リポジトリの義務としての明確な記述は見当たらないが、3 基準ともに、認証局の義務として、証明書と失効情報を適時に公表することを求めている。

【考察】
RFC の本節にかかる事項は、認証局の役割の一つであるリポジトリの義務として、適切に、証明書及び CRL（Certificate Revocation List – 失効リスト）を掲示する義務がある旨の記述であり、証明書の発行、失効に伴うリポジトリへの公表については、後述の RFC2527 の 2.6 章に記述される。リポジトリの義務として、適時にかつ安定的に、証明書の状態を確認できる機能を提供する必要がある。

4.4.2.2. ［2.2］責任

【RFC2527 記述内容】
各主体（認証局、利用者等）の権利及び限界、認証局、登録局における責任に関する要件。

【各基準の概要】
3 基準ともに、保証、免責を限定する場合、保証、免責の範囲と条件を認証業務規定又は CPS 等に定め、公開することを求めている。

ガイドラインでは、利用者に容易に理解できるように、重要な事項については CPS の開示のみではなく、概要をまとめて開示するなどの工夫も必要と記述されている。

署名法では認証業務規定を電磁的方法により記録し、公開することを求めている。

WebTrust の場合、記述例として、補償額の最高限度、証明書又はトランザクション、クレーム等の 1 件あたりの補償額、補償の優先順位等についてまで記述している。

【考察】
認証業務開始にあたり、証明書の利用目的、対象範囲、取引の重要性、証明書の事故が発生した場合の影響、財務基盤等を十分考慮し、補償、免責の範囲と条件、手続を CP/CPS に明確に定め、公開することが必要と思われる。

4.4.2.3. ［2.3］財務上の責任

【RFC2527 記述内容】
財務的な責任、賠償、各種委託関係に関する要件。

【各基準の概要】
ガイドラインでは、認証局の責に帰する損害への賠償、業務継続に必要な継続的投資を保持する財務基盤を求めている。

署名法では財務的な責任について言及していない。

WebTrust では利用者、検証者等への損害賠償、認証局／登録局と他の委託関係等について記述することを求めている。

【考察】
莫大な損害賠償を求められた場合に備え、企業賠償責任保険への加入などを検討しておくことが必要と思われる。

4.4.2.4. ［2.4］解釈及び執行

【RFC2527 記述内容】
CP/CPS の解釈と執行に関して適用する法律、紛争解決手続、分割、存続、合併及び通知に関する要件。

【各基準の概要】
署名法では、係争が生じた場合に適用される法律、解決手続、管轄裁判所等を CP/CPS 等の認証業務規定に明確に定め、公開することを求めている。

WebTrust においては、適用する法律のほかに、運用の変更時に生ずる CP/CPS の変更時の解釈（分割、解除等）の記述にも及んでいる。

ガイドラインには記述がない。

【考察】
管轄裁判所を記載するだけでなく、仲裁も含めて記述している CP/CPS も見受けられる。仲裁という考え方は日本ではあまりないが、都内にも２つの仲裁機関があり、国際間の紛争になった場合の仲裁も考慮するならば、例えば「仲裁及び裁判地は東京都区内における紛争処理機関を...」というように併記することになる。

4.4.2.5. ［2.5］料金

【RFC2527 記述内容】
証明書に関する料金、払い戻しに関する方針、他のサービス料金等に関する要件。

【各基準の概要】
署名法では必要料金、対象期間、支払い方法、料金返還処理等を認証業務規程に明確に定め、公開することを必要としている。

WebTrust においても署名法と同様な記述を CP/CPS 等へ記述することを必要としている。

ガイドラインでは、記述していない。

【考察】
契約上これらの取り決めは必須事項であるが、CP/CPS には記述せず、別に開示しているケースがほとんどである。

4.4.2.6. ［2.6］情報の公表とリポジトリ

【RFC2527 記述内容】
利用者、検証者に必要な情報（CP/CPS、証明書、CRL 等）を公表するリポジトリに関する要件。

【各基準の概要】
ガイドラインでは、証明書を開示するか否か、開示相手、開示期間について明確に

することとしている。証明書の他に開示すべき情報として、経営情報、技術情報、安全対策実施状況、CPS を挙げている。また、証明書の登録・保管におけるアクセス管理、データ消失に備えたバックアップを求めている。

署名法では、認証局自身の公開鍵にかかる証明書の値の SHA-1 ハッシュ値を記録し、改ざん防止を行うこととしている。また、利用者その他の者が、認証実施の手続、証明書の検証方法、連絡先、提供条件等が適切に定められた認証業務の実施規程等を容易に閲覧できることを求めている。

WebTrust では、認証局情報の公開、公開の頻度、アクセス制御について記述することとしている。

【考察】

リポジトリに公開する対象情報（証明書を開示するか否かも含め）、公開周期を明確にする必要がある。クローズドな証明書の利用においては、証明書を開示すべきか否かについての検討も必要となる。また、OCSP（Online Certificate Status Protocol）等オンラインにて証明書状態の確認を行える機能を提供している場合においては、CRL の開示が不要になることもあり得る。

4.4.2.7. ［2.7］準拠性監査

【RFC2527 記述内容】

認証局の監査に関する要件。

【各基準の概要】

ガイドラインでは、監査人はコンピュータセキュリティに精通した、監査対象から独立した者が行うことを推奨し、複数人による実施を求めている。実施頻度については、基本的に年最低 2 回の監査実施を必要としている。また、監査結果の速やかな開示及び指摘事項への対処、監査結果の安全な、一定期間の保存を求めている。

署名法では、業務の手順等に基づき、適正に業務が運営されていることを確認するための監査に係る基準が業務運用規定に定められ、それに従って定期的な監査が行われること、指摘事項及びセキュリティ対策技術の最新の動向を踏まえ、設備、規程等の見直しを含む対策を講じ、かつその結果を評価することを求めている。

WebTrust では、業務運用のセキュリティポリシや規格への準拠性を定期的にレビューすること、認証局のシステムのセキュリティ基準への準拠性を定期的にチェッ

クすること、業務の中断を最小限にするシステムの監査が計画、承認されることとしている。

【考察】

ガイドラインでは、年最低 2 回の監査を要求しているが、対象となる認証局が、どのレベルの完全性及びそれに伴う保証を行うのかによって、監査周期については判断する必要があると思われる。政府認証基盤内の BCA においても年一回としており、一般的には最低年一回の監査を規定している場合が多いが、認証局が発行する証明書の重要性、影響度、保証レベルによって決定されるものと思われる。

4.4.2.8. ［2.8］秘密保護ポリシー

【RFC2527 記述内容】

情報の保護に関する要件。

【各基準の概要】

ガイドラインでは、機密とすべき情報については、影響度を十分に考慮の上、取り扱いを定め適正な運用及び確認を求めている。また、利用者の個人情報についても、機密範囲・取り扱い方法を定め、適正な運用及び確認を求めている。

署名法では、電子証明書に利用者として記録されている者から、権利又は利益の侵害、又はおそれがあるとの申出があった場合においては、遅滞なく当該電子証明書に係る利用者に関する申込書、真偽確認書類等を開示することとしている。また、認証業務に係る、利用者の個人情報の取り扱いに関する事項を含む、セキュリティに関する事項を明確に定め、公開することとしている。さらに、個人情報の取り扱い及び保護に関して、全ての就業者に役割に応じた教育・訓練計画を行うこと、個人情報の管理・保管場所の整備がなされ、適正な管理が実施されていること等を求めている。

WebTrust では、関連法規に従った、個人情報保護のためのコントロール、機密性のポリシーと手続（情報の分類、情報の開示先、法的要求による開示等）の定義とそれに従った運用を求めている。

【考察】

昨今、個人情報保護法、ISO17799 等の各種基準等により情報の保護が重視されてきており、十分な検討及び個人情報保護方針の開示が必要と思われる。

4.4.2.9. ［2.9］知的財産権

【RFC2527 記述内容】
証明書の所有権、名称の利用、鍵に対する権利等の権利に関する要件。

【各基準の概要】
特段の記述はない。

【考察】
私有鍵、公開鍵、証明書等の電磁的な情報の所有権については法的な見解が明確に定まっておらず、各基準ともに規定していないものと思われる。

4.4.3. ［3］利用者の識別と本人確認

4.4.3.1. ［3.1］新規発行時の利用者の本人確認方法

【RFC2527 記述内容】
新規発行時の審査方法、認証方法、証明書に関する各種規則等に関する要件。

【各基準の概要】
《新規発行時審査・利用者真偽確認・申請意思確認方法》

ガイドラインでは、次の事項を要求しており、オンライン申請、書類送付申請、出頭申請の各申請方式により申請方法と確認情報・書類を例示している。

- 申請情報の真正性の確認として信頼できる機関・組織・人による証明又はそれらの情報と精査することを求め、さらに高い確認方法として複数の情報の利用を推奨している。
- 本人確認において、申請情報の真正性の確認と違う手段（本人への通知）等の利用を求めている。また、より信頼性の高い手段として、本人出頭を推奨している。
- オンライン申請以外の場合は、審査処理を複数人で分担すること。

また、認証申請者からの申請を認証局が受理したことを申請者に対して返答通知するとともに、併せて申請の意思確認を行う必要があるとしている。

署名法では、次のように要求事項を詳細に規定している。

- 申請方法、申請方法別の本人又は代理人の確認資料等本人確認手続、必要資料を明確に業務規定に定め、実施すること
- パスポート、官公庁の発行した免許証等によって利用者又は代理人の真偽を確認する場合は、証明書類が真正なものであることを確認し、かつ、当該証明書等に貼付してある写真と提示者との照合により真偽の確認すること
- 印鑑登録証明書によって利用者又は代理人の真偽を確認する場合は、印鑑登録証明書の真正性を確認すること、かつ、利用申込書に実印が押印され、印鑑登録証明書の印影と一致することを確認すること
- 本人限定受取人郵便又はこれに準ずるものにより、申し込み確認を行うことによって利用者又は代理人の真偽を確認するにあたっては、受取人が本人に限定される書留郵便等による照会書の交付時に行われる真偽の確認を採用する場合は、利用者又は代理人に確かに交付されたことを示す書類を受領すること
- 代理人による利用申込みの委任状には、利用者が代理人に対し委任する利用申込みの内容若しくは代理人による受取りが明確に記されていること
- 代理人による利用申込みの場合、委任状になされた利用者本人の署名を確認するとともに、同文書に押印された利用者の実印の印影と委任状に添付された印鑑登録証明書に証明されている印影の写しが一致することを確認していること
- 利用者の真偽の確認を発行認証局に対して電子証明書を用いて行う場合においては、利用者の電子署名を検証し、当該電子署名に係る有効性を確認している。かつ、新たに発行する電子証明書の有効期間が、規則第５条第１項の各号のいずれかの方法により利用者の真偽の確認が行われ発行された電子証明書の発行日から５年未満に満了することを確認していること
- 利用者の真偽の確認と利用者からの利用者の公開鍵の受領を同時に行わない場合においては、利用者の公開鍵の提出者と利用申込者が一致することを、本人確認後に渡した本人だけに、かつ本人以外には知りえない情報を用いて確認する等により確認をしていること
- 利用者又は代理人の真偽の確認を行うにあたって疑義が生じた場合においては、あらかじめ文書をもって定められた手続に従って、利用者又は代理人の真偽を確認する手続きを行うこと

WebTrust では、審査・真偽確認方法について具体的な基準は示しておらず、CP/CPS 等にその方法を記述することを求めているのみである。

《その他》

署名法では、電子証明書に記録する利用者の公開鍵は、利用者の私有鍵によって行われた電子署名を当該利用者の公開鍵を用いて検証する等の方法により、利用者が公開鍵に対応する私有鍵を保有していることを確認することとしている。

WebTrust では、次の事項を CP/CPS に記述すべき項目として記述している。

- サブジェクトに割り当てられた名前の形式
- 名前が意味を持つ必要があるか否か
- 名前が一意（ユニーク）である必要があるか否か
- 所有者の名前を決定する際の紛争解決手続
- 商標の認識・認証・役割
- 公開鍵に対応する私有鍵の所有を証明する方法

【考察】
利用者真偽確認方法については、利用形態、証明書の利用目的、重要性、保証レベル等を考慮し、必要な要件を定める必要がある。証明書に、より高い完全性、重要性を求める場合においては、ガイドライン又は署名法の基準と同等な要件を定める必要があると思われる。また、公開鍵と対応する私有鍵の保有に関する証明については、PKI を確実ならしめるために必須の要件と考える。なお、FBCA においては保証レベルを 4 段階に分け、それぞれに認証要件を定義している。

FBCA における身元確認：

初期レベル　－　電子メールアドレス

基本レベル　－　データベース、管理者又は申請者による本人を一意に識別できる情報

中位レベル　－　登録局への出頭及び写真付の ID などの身分証明できる書類

高位レベル　－　登録局への出頭及び政府が発行した 2 種類の識別書類（内、一枚は写真付の ID などの身分証明できる書類）

4.4.3.2. ［3.2］通常の更新

【RFC2527 記述内容】

通常の鍵更新における、本人確認、認証手続に関する要件。

【各基準の概要】
3 基準ともに、更新時の本人確認は、新規と同様な手続で行うか又は更新前の私有鍵でデジタル署名を付した要求を受け取り、そのデジタル署名の有効性を検証する方法のいずれでも良いとしているが、各基準によっては、より強い要件を加えている。

署名法では、デジタル署名の有効性の検証をもって本人の真偽確認を行うことを認めているが、5 年に 1 度は新規発行手続と同様の方法で本人の真偽確認を行わなければならないとしている。また、利用者の真偽確認と利用者の公開鍵の受領を同時に行わない場合においては、利用者の公開鍵の提出者と利用申込者が一致することを、本人以外知りえない情報を用いて確認することとしている。

WebTrust では、主に次の事項を手続項目として記述している。

- 利用者の証明書鍵更新要求には、利用者の識別名、証明書番号、有効期間を含めること
- 証明書更新要求にデジタル署名すること
- 認証局や登録局はエンティティの身元と証明書更新の正当性を検証すること
- 認証局や登録局は証明書更新要求の署名を検証すること
- 認証局や登録局は更新される証明書の存在と正当性を検証すること　等

【考察】
WebTrust では詳細な手続項目を定めており、その項目は確実な認証局の運用として必要な項目であると考えられる。

4.4.3.3. ［3.3］失効後の更新－鍵が危殆化していない場合

【RFC2527 記述内容】
証明書が失効した後の鍵更新のための識別と本人認証の手続に関する要件。

【各基準の概要】
ガイドラインでは、証明書の新規発行と同様の処理を必要としている。

署名法では、この項に対応する特段の記述はないが、新規と同様な手続が必要とな

る。

WebTrust では、新規の証明書発行と同様な登録手続を必要としている。

【考察】
新規発行時と同様な手続を行うものと考える。

4.4.3.4. ［3.4］証明書の失効申請

【RFC2527 記述内容】
失効要求のための識別と本人認証の手続に関する要件。

【各基準の概要】
ガイドラインでは、私有鍵の消失、重要情報の変更の場合は、新規発行と同等の本人確認を必要としている。

署名法では、利用者からの失効要求、真偽確認、失効処理等が明確に認証業務規程及び事務取扱要領に規定され、実施されていることとしている。（調査表-項番 3801）

WebTrust では、認証局は、認証局の規定要件に従って、本人確認と証明書失効要求を認証し、検証することとしている。

【考察】
基準として、詳細な記述はなされていない。利用者の私有鍵の紛失、盗難等により失効申請が必要となった場合の失効申請が、当該私有鍵に基づく署名付き失効要求にて行われうるかについての議論もあるが、私有鍵を保有しているべき利用者以外が失効申請を行ったとしても、それ自体が、私有鍵の危殆化であり、証明書は失効されるべきものと考える。

4.4.4. ［4］運用上の要件

様々な運用要件に関して、認証局、登録局及び利用者に負わされる要件を規定。

4.4.4.1. ［4.1］証明書の申請

【RFC2527 記述内容】
利用者の登録と証明書発行のための申請に関する要件。

【各基準の概要】

ガイドラインでは、本項に係る特段の規定はない。情報の登録として、後から利用できるように登録しておく必要、予め失効などの事故に対する情報など（例えば、失効申請代行者など）を登録させることが望ましいとしている。

署名法では、次のように要求事項を詳細に規定している。

- 申請手続、確認方法、必要資料等が認証業務規程及び事務取扱要領に明確に規定され実施されること。
- 申込みの方式について指定すること、申込方式において利用者および代理人の真偽を確認するために使用する資料の種類を指定すること。
- 指定した方式以外の方式によりなされた電子証明書の交付申込みの受理に関する取り扱い手続について定めること　等。

なお、真偽確認書類については、本書 2.2.3.1［3.1］新規発行時の利用者の本人確認方法、に述べられているとおりである。

WebTrust では、本項に係る特段の指定は行っていない。認証局、登録局のなすべき項目として次の項目を挙げている。

- 認証局は、エンティティに対し規定の要件に従った適切な CSR（Certificate Signing Request - 証明書要求データ）を登録局又は認証局に送信するよう要求する。
- 登録局は、規定要件に従ってエンティティの本人確認手続を行う。
- 登録局は、規定の要件に従って証明書要求の正当性の確認を行う。
- 登録局は、規定の要件に従ってエンティティの CSR に含まれている情報の正確性を検証する。
- 認証局は、登録局からの送信内容の真正性を検証する。
- 認証局は、同一公開鍵を発見した場合、CSR の拒絶とオリジナルの証明書の失効を行う。

また、外部登録局を使用する場合の必要事項が記述されている。

【考察】

署名法にあるように、代理人申請を認める場合は代理人申請の手続を用意しておく必要がある。

4.4.4.2. ［4.2］証明書の発行

【RFC2527 記述内容】
証明書の発行と発行申請者への通知に関する要件。

【各基準の概要】
ガイドラインでは、不正な生成が行われないようにする手続を定める、特にオフラインで生成する場合には審査処理を分離するとともに、権限を有する者以外はアクセスできないシステムが必要としている。また、証明書送付にあたっては、セキュアな手段を講じることが必要であるとしている。さらに、証明書を送付する際、受取りの確認ができる手段を利用することを推奨している。

署名法では、認証業務に係る手順、従事する者の責任、権限等を明確に定め、実施することを必要としている。

また、認証局において利用者の私有鍵を生成する場合、次の事項を要求している。

- 複数の者による私有鍵の作成及び管理その他当該私有鍵の漏えいを防止するために必要な措置が講じられていること。
- 当該利用者の私有鍵及び関連情報が残らないように完全に廃棄若しくは消去されること。
- 生成された利用者の私有鍵は、安全な方法で利用者本人に渡され、利用者から自署又は電子署名が付された受領書を受け取ること。
- 私有鍵及びその格納媒体等の活性化に使用するＰＩＮ等の秘密情報の生成、転送、出力等は、権限のある操作者によって行われ、アクセス権限管理、内部牽制等により盗聴、改変防止等の措置が施されていること。

WebTrust では、認証局はエンティティからの要求を受け付けた後に証明書を発行する、認証局は登録局にいつ利用者に証明書を発行するか知らせる、証明書が発行されるとき、オンライン申請等と異なる手段による通知を要求者に行う等が記述されているが、発行に関する詳細要件は規定していない。

【考察】
認証局が利用者の鍵ペアを生成し証明書を発行する場合においては、安全かつ、私有鍵をその利用者のみが保持していることを保証できる手続を明確に定める必要がある。私有鍵の保持が、その利用者のみであるという保証がなされない場合、署

名の否認等につながるからである。

4.4.4.3. ［4.3］証明書の受理

【RFC2527 記述内容】
発行された証明書の受容と証明書の公表に関する要件。

【各基準の概要】
ガイドラインでは、証明書を送付する際、受取りの確認ができる手段を利用することを推奨している。

署名法では、認証局において利用者の鍵ペア、証明書を生成した場合、受領書の受取を必要としている。

WebTrust では、該当する記述はない。

【考察】
特記なし。

4.4.4.4. ［4.4］証明書の停止と失効

【RFC2527 記述内容】
証明書の停止、失効に関する運用要件。

【各基準の概要】
3 基準ともに、次の事項を要求している。

- 失効要求の申請者の本人確認を行うこと。
- 利用者に失効審査結果、又は失効処理が行われたことを通知すること。
- 検証者が失効に関する情報を容易に確認できること。
- CRL を週次、日次などというように、定期的に発行すること。

ガイドラインでは、他に次の事項を要求している。

- 証明書の誤りや不正使用の検知、本人による失効申請が困難な事由の発生、あるいは証明書の不正発行などの場合は、登録局や認証局あるいは事前に登録されている機関などが本人に代わって失効申請できるようになっていること
- オンライン申請以外の場合は、審査処理を複数人で分担して行うこと

- 失効した証明書の当初の有効期限経過後も一定の期間 CRL 及び関連データを保存すること。
- 災害等に備え CRL のバックアップをとること。

署名法では、他に次の事項を要求している。

- 失効申込み、真偽確認、失効処理等が明確に認証業務規程及び事務取扱要領に規定され、実施され、電子証明書失効情報の確認方法及び期間に関する事項については認証業務規程として電磁的方法により記録され公開されていること。
- 認証事業者自身の起因によるものを含む電子証明書の失効事由、失効申込書又は失効の申込みデータの記載内容、電磁的に記録する失効に関する情報を明確に定めること。

WebTrust では、他に次の事項を要求している。

- 証明書の有効期限までは失効又は停止された証明書は CRL に記載されること
- その他オンラインによる証明書ステータス確認手段の有無、利用法を記述すること

【考察】

証明書状態の確認をしようとする者は、CRL の有効期間の間隔で確認を行う場合が多いと思われる。CRL の発行周期の前に証明書が失効された場合、CRL の確認を行っていないことになり、有効な証明書状態確認が行えないことになる。OCSP の利用や、取引都度に CRL を確認する等が実施できる場合を除くと、CRL の発行間隔は短いほど、安全性が高い（検証者にとって）と思われる。FBCA においては、証明書の保証レベルにより、CRL の発行間隔を、不要、1 週間に 1 度、毎日、12 時間に一度というように 4 段階に分類している。保証レベル、証明書の利用形態、失効情報の提供メカニズム等により検討すべきものと思われる。

4.4.4.5. ［4.5］セキュリティ監査の手続

【RFC2527 記述内容】

セキュアな環境を維持するために実装されるイベントロギングと監査システムに関する要件。

【各基準の概要】

3 基準ともに、監査情報として必要な情報を定義し、その情報の記録を行うことを要求している。また、その記録に対するアクセス制御を必要としている。

ガイドラインでは、他に、必要に応じ適正な期間内に提供可能な状態で保管しておくことを必要とし、適正な間隔でバックアップを取り、遠隔地保管することを推奨している。

署名法では、他に、特定の操作者による操作の履歴のみを表示することができる機能を必要としている。

WebTrust では、全てのイベントジャーナルの記録項目を定義しており、さらに、重大なセキュリティイベント、暗号化装置ライフサイクル管理、鍵ライフサイクル管理及び証明書ライフサイクル管理に関連するイベントについては記録必要イベントの種類を定義しており、その内容の記録をすることを求めている。また、証明書申請時情報の記録必要な種類を定義しており、その記録についても記録を必要としている。さらに、保管されているジャーナルの完全性確認、保存ジャーナルの別地への保管等を多岐にわたり要件として定義している。

【考察】

監査のための情報については重要な要素であり、認証局の運用についての完全性を保証する上でも、保証レベルに見合った情報種類、内容、監査周期を検討する必要があると思われる。FBCA においては 50 数種類の監査イベントを定義し、保証レベルによって 4 段階の区分けを行っている。また、検査頻度においても、保証レベル別に検査周期を決定している。

4.4.4.6. ［4.6］記録の保管

【RFC2527 記述内容】

一般的な記録のアーカイブ化（若しくはレコード保持）の方針に関する要件。

【各基準の概要】

ガイドラインでは、発行した証明書については有効期限が切れた後も、不正なアクセスがなされないような対策を講じて、一定の期間証明書を保存する必要があり、失効した証明書の当初の有効期限経過後も、一定の期間失効リスト及び関連するデータを保存しなければならないとしている。

署名法では、認証業務において保存する帳簿書類の保存期間、保存方法等管理、運用事項を明確に定め、認証業務規程として電磁的方法により記録され公開されていることとしている。

WebTrust では、CRL は認証局の規定要件に従ってアーカイブすること、リムーバブルメディアは組織から持ち出す時に、以前の内容を消去すること、持ち出しには承認を必要とし、監査記録としてすべての持ち出しを記録し保存すること、メディアは、メーカーの仕様に従った安全な環境に保管すること、必要でなくなったメディアは、安全に処分することとしている。

【考察】

保管する情報の種類、重要性、リスク評価を行い、保管期間、保管場所、アクセス制御等の検討が必要となる。また、保管に限定されないが、情報に記録される時間に差異があった場合、情報の整合性がそこなわれるので、認証局のコンピュータシステムの時計は、正確に記録するため時刻の同期化を行う必要があると思われる。さらに、厳格な時間管理が必要となる場合、4.5.4.3 節で述べる TSA（Time Stamp Authority - タイムスタンプ局）の利用も推奨される。

4.4.4.7. ［4.7］鍵の再発行

【RFC2527 記述内容】

認証局の新しい公開鍵を 認証局 のユーザに提供する手続に関する要件。

【各基準の概要】

3 基準ともに記述はない。

【考察】

この項に関しては、認証システム及び利用ユーザのアプリケーションに依存するものと思われる。システムによっては、認証局の鍵の更新を意識せずに利用することも可能である。システム的な対応がない場合は、新規発行時における認証局の公開鍵の提供と同様な手続になると思われる。

4.4.4.8. ［4.8］危殆化と業務の継続性の保証

【RFC2527 記述内容】

危殆化や災害が起きた場合における通知と復旧の手続に関する要件。

【各基準の概要】

3 基準ともに、私有鍵の危殆化又はそのおそれ、災害等の事態に対しての事業継続計画、危機管理計画や私有鍵の危殆化時の失効方法、連絡方法等を事前に定めておくことを要求している。

また、ガイドラインでは、危殆化していないかを確認するため、証明書の利用状況についてサンプリングなどの方法でモニタリングを行うことを推奨している。

署名法では、対応策及び回復手順に従った教育・訓練の定期的な実施、検証者への失効情報の開示が、認証業務規程にて定める時間を超えて停止し、かつ検証者が停止を知る方法が無かった場合の、速やかな主務大臣への通報を定めることとしている。

WebTrust では、事業継続計画の定期的レビュー及びテスト、バックアップ装置及びバックアップデータの遠隔地保管等を実施することとしている。

【考察】

証明書の重要性、補償レベル等に応じて事業継続計画を策定し、バックアップ機器、バックアップデータの遠隔地保管等を考慮する必要があると思われる。なお、長期障害時等の主務大臣への通報は認定認証業務に特有の要件である。

4.4.4.9. ［4.9］認証局の終了

【RFC2527 記述内容】

認証局又は登録局の終了と終了の通知のための手続に関する要件。

【各基準の概要】

ガイドラインでは、業務を終了する場合には、そのスケジュールと手続を決め、その内容を利用者等直接その影響を受けるものに通知する必要があるとしている。

署名法では、発行済み電子証明書の失効処理方法、利用者への連絡方法、連絡時期等を認証業務規程として電磁的方法により記録し公開することとしている。利用者へ通知は 60 日前までに行う必要がある。また、主務大臣への届出も必要となる。

WebTrust では、認証局の PMA（Policy Management Authority - 認証局のポリシーに関する意思決定機関）のみが認証局の終了を決定できるものとし、終了時は発行したすべての証明書を失効させ、証明書の発行を停止することとしている。ま

た、サービス終了 1 か月以上前に利用者に通知すること、認証局の記録はアーカイブされ、管理者に譲渡されること等を要求している。

【考察】
業務の終了に関しては、周到な準備と相応の期間が必要であることを認識しておくべきである。

4.4.5. ［5］建物・関連設備、運用、要員のセキュリティ管理

4.4.5.1. ［5.1］建物及び関連設備管理

［5.1.1］施設の位置と建物構造

【RFC2527 記述内容】
認証局を設置する施設の位置と建物構造に関する要件。

【各基準の概要】
ガイドラインでは、建物は火災、電磁界、水害、落雷、空気汚染による被害を受けるおそれの少ない場所に設け、建物は耐火構造、耐震構造とすることを求めている。認証システム設置室は、他の業務システムと隔離することを求めている。

署名法では、建築物を地震による被害のおそれの少ない地域に建築することがやむを得ずできない場合は不同沈下防止措置を講じることとし、具体的な工法を挙げている。建築の耐火構造に関しては、準耐火建築物の基準に適合していることでもよいとしている。

また、署名法、WebTrust ともに、侵入対策として、上階スラブから床スラブまで隙間のない壁の設置を求めている。

認証局の所在の掲示に関しては、署名法がその掲示がされてはいけない場所を具体的に規定している。

【考察】
署名法の場合、認証設備を認証業務用設備と登録端末用設備に分けてとらえており、認証業務用設備のセキュリティ要件をより高度にしている点は注意が必要である。

［5.1.2］入退管理

【RFC2527 記述内容】
認証局施設における入退管理に関する要件。

【各基準の概要】
各基準ともに、入退管理の徹底を求めている。具体的には、すべての窓・扉に対する防犯措置、入退出記録（人、時刻）の採取とレビュー、管理規定の整備、入退出者に対する資格審査などである。識別証の着用は、ガイドラインと WebTrust で求められている。

認証システム設置室の入室時は、生体認証が求められている。複数人による生体認証を要件としているのは署名法だけである。ガイドライン、WebTrust もオペレーションのデュアルコントロール（複数人操作）は求めているが、入室操作自体の複数人操作までは求めていない。

その他、室が無人となる場合の監視や設備保守などのために第三者が入室する場合の権限者同行などを求めている。

署名法では、上記の事項に対して、さらに詳細な要件が定められている。入室者と同数の複数人の退室操作により退室が可能になること、入室に不必要に時間を要した又は試行回数が規定回数を超えた場合には警報を発すること、死角ができないよう遠隔監視カメラを配置すること、死角が存在する場合には死角内で作業が行われないよう教育等の対策を講じること、遠隔監視装置で認証設備室への入退者及び在室者を常時監視することなどである。

【考察】
ガイドラインは「入退室」と一括りにとらえているが、署名法のように入室時の要件と退室時の要件は分けられるべきである。また、生体認証がどの室の要件とされているかについては、[5.1.1]で述べたように CA サーバが置かれる室と登録用端末設備等が置かれる室とのセキュリティ要件を明確に分けている署名法が参考になる。

［5.1.3］電源及び空調設備

【RFC2527 記述内容】
認証局における電源及び空調設備に関する要件。

【各基準の概要】
各基準ともに電源の安定供給のための対策を求めている。具体的には、ガイドラインや署名法で CVCF、UPS、蓄電池などを求めている。ガイドラインでは、電源設備の避雷措置、電源及び空調設備の防災措置・防犯措置を求めている。署名法では、遠隔監視装置及び映像記録装置と明記して UPS 等の設置を求めている。WebTrust では電源を遮断や破損から保護することを求めている。

【考察】
特記なし。

［5.1.4］水害及び地震対策

【RFC2527 記述内容】
認証局施設における水害及び地震対策に関する要件。

【各基準の概要】
署名法では、水害対策として認証設備室を建築物の 2 階以上に設置するか、1 階以下の場合には水害に対する対策を講じること、認証設備室の直上階の床板にアスファルトやウレタン系防水塗料を塗布する等の防水施工を講じるか、漏水センサを設置することを要求している。また、認証室内には水使用設備を設置しないこと、空調機には漏水センサを設置すること、漏水監視は常時行うことを求めている。地震対策としては、認証設備室内の認証業務用設備に対して転倒防止金具、免震構造を持つ床等の措置を講じて移動・転倒を防止すること、認証業務の構成備品・ラック・什器に、移動・落下・転倒防止等の耐震措置を講じること、フリーアクセスフロアに補強措置を講ずること等が要求されている。

【考察】
特記なし。

［5.1.5］防火設備

【RFC2527 記述内容】
認証局施設において設置すべき防火設備に関する要件。

【各基準の概要】
ガイドラインでは、特に規定していない。

署名法では、認証設備室に自動火災報知器及び消火設備を設置すること、認証設備室は建築基準法に規定する防火区画であることを要求している。

WebTrust では、詳しく規定はしていない。

【考察】
総じて、防火設備としては署名法で要求されている対策を講じることで十分であると思われる。

［5.1.6］記録媒体の保存

【RFC2527 記述内容】
バックアップ、アーカイブ等の各種記憶媒体の保存に関する要件。

【各基準の概要】
ガイドラインでは、特に規定していない。

署名法では、各記録は、施錠可能な自動火災報知器及び消火装置を備えた室で、直射日光に当たらないよう保存することを求めている。原本で保存する場合には、判読不可能とならない環境を備え、専用のファイルに閉じこむことが要求されている。電磁的記録で保存する場合には、適切なケースへの収納、磁気媒体の場合には磁気的影響がない場所に保管すること、媒体の内容を表示できるような環境を維持すること、媒体に合わせて適宜記録し直すことが要求されている。

WebTrust では、重要な情報は厳重に管理することを要求している。

【考察】
総じて、記憶媒体は、電子媒体、紙媒体とも、火災等の災害対策を講じた施錠可能な専用の室にて保管することが必要と思われる。特に、電子媒体の保存は、メディアに応じた特別な要件に注意して保存・管理することが必要となる。

［5.1.7］廃棄物の処理

【RFC2527 記述内容】
不要となった記憶媒体（ハードディスク）、機材等の廃棄に関する要件。

【各基準の概要】
ガイドライン及び署名法では、情報管理の一環としては触れているが、廃棄物の処理としては特に規定されていない。

WebTrust では、記憶媒体を含むすべての機材は、廃棄する前に機密情報がないか確認し、あった場合は物理的に破壊するか上書きすることを要求している。

【考察】
記憶媒体、機材等を廃棄する場合には、機密情報の漏えいに注意する必要がある。そのため、廃棄の手順を適切に定め、WebTrust に示されているように物理的な破壊や上書きするといった対策を講じることが必要となる。廃棄を業者等に依頼する場合には、運用手順や、契約内容に注意する必要がある。

［5.1.8］オフサイト・バックアップ

【RFC2527 記述内容】
オフサイトへのバックアップに関する要件。

【各基準の概要】
3 基準とも、特に規定はしていない。

【考察】
3 基準とも規定はしていないが、災害復旧の際に用いるバックアップや重要なサービスのデータ、その他重要な情報等は、必要に応じて遠隔地へ保管することが望ましいと思われる。

4.4.5.2. ［5.2］手続管理

［5.2.1］信頼される役割

【RFC2527 記述内容】
認証業務上の各役割に関する要件。

【各基準の概要】
ガイドラインでは、情報セキュリティ技術やシステム監査等の専門家を配置すること、専門的な知識やスキルを要する要員を確保することを要求している。またガイドラインでは、認証局が長期的に安全性、信頼性を確保する上で、認証局自体、特

定の企業や組織から影響を受けない公平な立場を保持できることも求めている。

署名法では、認証業務就業者の指揮命令系統、責任及び権限を文書に明確に定め、それに従って業務を実施するよう要求している。

WebTrust では、ポリシー文書に職務の分離を含めるよう要求している。

【考察】
認証業務における職務分掌については、各担当者の責任及び権限を文書として明確に定め、それに従って業務を実施することが求められる。また、要員には専門的な知識やスキルのある者を配置すること、情報セキュリティ技術やシステム監査の専門家を配置することが望ましいと思われる。

［5.2.2］必要とされる人数

【RFC2527 記述内容】
各業務において、業務を遂行するのに必要な人員数に関する要件。

【各基準の概要】
ガイドラインでは、特に規定していない。

署名法では、認証業務の遂行上必要な知識・経験とそれらを有している技術者の必要数を規定し、認証業務に配置するよう求めている。また、認証設備室への立入りは複数名で行うよう求めている。

WebTrust では、特定の認証業務で要求される人数をポリシー文書に含めることを規定している。

【考察】
認証業務において、重要操作については、複数名によるコントロールを導入するのが通例である。そのような操作においては、必要人数を規定し、配置することが必要であると思われる。

［5.2.3］役割ごとの識別と本人認証

【RFC2527 記述内容】

役割ごとの識別と本人認証に関する要件。

【各基準の概要】
ガイドラインでは、特に規定していない。

署名法では、認証業務用設備に対するアクセス権限は操作者単位に設定すること、アクセスの際にはパスワード、電子署名、生体認証等により操作者を確認することが求められている。

WebTrust では、ポリシー文書に各ユーザの識別と認証を含めることを要求している。

【考察】
認証設備に対するアクセス権のセキュリティ基準を文書化することは必須要件である。認証業務用設備へのアクセスを管理するための認証方式としては、特に注意を要するシステムには生体認証を導入し、その他のシステムには、必要に応じパスワードや電子署名による認証を導入すべきであると思われる。

4.4.5.3. ［5.3］要員のセキュリティ統制

［5.3.1］認証局における人事上のセキュリティ管理

【RFC2527 記述内容】
認証局において信頼される役割を担当する要員に要求される経歴チェック、身分証明手続等に関する要件。

【各基準の概要】
ガイドラインでは、人材の採用時には、適切な人物審査を行うことを要求している。
署名法では、特に規定していない。

WebTrust では、認証局の業務へ要員を配置時に身元確認を行うよう求めている。また、従業員は機密保持契約に署名することを求めている。

【考察】
特筆すべき要件は規定されていないが、人員の採用に関しては認証局業務に限ったものではなく、組織自体の基準に従って人物審査を行い、採用することになると思われる。また、従業員には、秘密保持契約に署名させることが望ましいと思われる。

［5.3.2］背景調査

【RFC2527 記述内容】
警備員を含む他の要員のための経歴チェックと身分証明手続に関する要件。

【各基準の概要】
ガイドライン及び署名法では、特に規定していない。

WebTrust では、外部委託等の第三者への素性調査や採用手続を明確に定めるよう要求している。

【考察】
警備員、清掃員やその他外部委託要員等の第三者を採用する際の手続を明確に定める必要があるが、現実には契約に守秘義務等を含めることで対応することになると思われる。

［5.3.3］トレーニング要求

【RFC2527 記述内容】
トレーニング要件と、各役割のためのトレーニング手続に関する要件。

【各基準の概要】
ガイドラインでは、特に規定していない。

署名法では、就業者に応じた教育・訓練計画を策定し、それにそって教育・訓練を実施するよう求めている。

WebTrust では、セキュリティポリシにセキュリティ教育の要求を含め、要員、第三者等すべての者に適切な教育を受けさせるよう要求している。

【考察】
特に教育内容に関する要件はないが、業務ごとの教育計画を策定し、それに従って教育を実施することが必要であると思われる。教育は、認証業務に直接的に従事する要員に限らず実施することが望ましい。

［5.3.4］再トレーニング期間と手続

【RFC2527 記述内容】
各役割についての、再トレーニング期間と再トレーニング手続に関する要件。

【各基準の概要】
ガイドライン及び署名法では、特に再教育としては規定してなく、教育要件の中に包含される。

WebTrust では、認証局のポリシーと手続で各役割における再教育期間と再教育手続について規定し、適切に実施するよう要求している。

【考察】
再教育に関しては、［5.3.3］のトレーニング要求と同様の要件が求められると思われる。

［5.3.5］ジョブローテーションの頻度と順序

【RFC2527 記述内容】
様々な役割の間でのジョブローテーションの頻度と順序に関する要件。

【各基準の概要】
ガイドライン及び署名法では特に規定していない。

WebTrust では、要員が退職、解任する時は適切で迅速な対応をするよう規定している。

【考察】
特筆すべき要件は規定されていない。認証業務要員が退職、解任される等でジョブローテーションが発生する際には、その者の権限を即座に抹消し、代わりの要員を配置する等セキュリティが損なわれないようにする対応が必要になると思われる。

［5.3.6］認可されていない行為に対する制裁

【RFC2527 記述内容】
認可されていない行為、認可されていない認証局の使用、認可されていないシステムの使用についての、要員に対する制裁に関する要件。

【各基準の概要】
ガイドライン及び署名法では特に規定していない。

WebTrust では、セキュリティポリシ及び手続に、許可のない操作、認証局の利用、システムの利用に対する制裁を規定し、それに違反した従業員を懲罰プロセスに従い制裁することを要求している。

【考察】
WebTrust に規定されているように、許可されない操作、システムへのアクセス、認証局の不正利用についての罰則手続を文書化し、それに従って違反した従業員を制裁することになると思われる。しかし、実際には、組織における全社的な罰則規定での制裁を適用することが大半であると思われる。

［5.3.7］契約要員に関する要件

【RFC2527 記述内容】
要員の委託契約に関する要件。

【各基準の概要】
ガイドラインでは、特に規定していない。

署名法では、委託契約内容において委託業務の内容、委託者の指示の遵守及び責任分担、保証等について明確にすること、受託者からの定期的な報告を受けること等により業務を管理することが要求されている。

WebTrust では、第三者の認証局施設やシステムへのアクセスは、契約に基づいて管理することが要求されている。契約内容には、外部委託契約、損害賠償契約、監査及び監視を含めるよう要求している。

【考察】
契約要員との契約内容には、業務内容、責任範囲、損害賠償契約等を含めることが必要である。また、契約要員の監査及び監視のため、委託業務に関する定期的な報告を求める等の管理を行うことが望ましいと思われる。

［5.3.8］担当者に提供されるべき文書

【RFC2527 記述内容】
担当者に提供されるべき文書に関する要件。

【各基準の概要】
ガイドラインでは、場所へのアクセス、機器類へのアクセス、情報へのアクセスに関する事務取扱要領等を規定するよう要求している。

署名法では直接的には規定していないが、業務手順を明確に定め実施すること（規則第 6 条第 15 号）に含まれると解釈できる。

WebTrust では、情報セキュリティポリシ文書をすべての従業員に公開、通知するよう要求している。

【考察】
情報セキュリティポリシをすべての従業員に公開することが必要である。さらに、情報セキュリティポリシの実施手順を定め、前述の教育も含め、実効性を高めていく必要がある。

4.4.6. ［6］技術的なセキュリティ管理

4.4.6.1. ［6.1］鍵ペア生成と実装

［6.1.1］鍵ペアの生成の主体

【RFC2527 記述内容】
各主体の鍵の生成について、鍵生成の主体、鍵の受け渡し、鍵のサイズ、公開鍵パラメータ、鍵の使用制限等に関する要件。

【各基準の概要】
ガイドラインでは、認証局の鍵生成として、複数人の下での鍵生成、信頼できる暗号鍵生成システムの利用を必要とし、暗号化モジュールの使用を推奨している。利用者の鍵管理については利用者の義務として、信頼できるソフトウェアやハードウェア等を利用して生成することとしている。

署名法では、認証局の私有鍵の生成及び管理は、認証設備室内で複数の者によって暗号装置を用いて行われることとしている。また、次の事項についても要求している。

- 認証局において利用者の私有鍵を生成する場合、複数の者による私有鍵の作成及び管理その他当該私有鍵の漏えい防止措置
- 当該利用者の私有鍵及び関連情報の完全廃棄若しくは消去
- 生成された利用者の私有鍵の利用者本人への安全な方法での送付
- 利用者から自署又は電子署名が付された受領書の受領
- 私有鍵及びその格納媒体等の活性化に使われる秘密情報の生成、転送、出力等のアクセス権限管理
- 内部牽制等による盗聴、改変防止等の措置　等

WebTrust では、権限の与えられた作業者によるデュアルコントロールの下で、ISO 15782-1/FIPS 140-1/ANSI X9.66 が要求するレベルを満たす安全な暗号化装置で生成、保管することが求められている。また、認証局が利用者の鍵生成を行う場合、承認された作業者による実施、利用者のみにしか私有鍵が開示されない管理等が記述されている。

【考察】

認証局のドメインにおいて、その信頼の要となる認証局の私有鍵においては、厳密な生成及びその完全性を維持しつづける管理が必要となる。3 基準ともに権限のある複数人による生成、信頼のできる暗号化装置の使用を必要としている。高レベル信頼の認証局において、FIPS 140 レベル 3 認定又は相当の HSM（HardwareSecurityModule）の使用が必要になると思われる。日本の府省認証局などの調達仕様では、認証局の HSM に FIPS140 レベル 3 相当以上といった要求を行っている。

なお、WebTrust にて記述されている FIPS 140-１とは、米国 Federal　Information Standard　Publication の暗号化システム、暗号化装置等の規格であり、現時点では、FIPS 140-2 という新しい規格にて製品認定を行っている。

また、認証局が利用者の鍵ペアを生成する場合においては、利用者による署名の否認の可能性等もあり、手順等の決定において十分な検討が必要と思われる。

［6.1.2］所有者への私有鍵の送付方法

【RFC2527 記述内容】

どのように私有鍵をセキュアに提供するのかに関する要件。

【各基準の概要】
ガイドラインでは、認証局が利用者の鍵を生成することについての記述がない。

署名法では、私有鍵を安全かつ確実に利用者に渡すことができる方法により送付し、かつ、私有鍵及びその複製を直ちに消去することとしている。また、安全な方法で利用者本人に渡され、利用者から自署又は電子署名が付された受領書を受け取ることとしている。

WebTrust では、認証局の規定要件に従い、申請者の鍵ペアを安全に配付する、すでに送付した利用者の私有鍵のコピーを保持しないこととしている。

【考察】
署名に用いる私有鍵の場合、その私有鍵を利用者のみが所持していることを保証できるコントロールが必要であり、手続等詳細に定める必要がある。

［6.1.3］認証局への利用者の公開鍵の送付方法

【RFC2527 記述内容】
利用者の公開鍵の認証局への送付に関する要件。

【各基準の概要】
ガイドラインでは、公開鍵の送付としての記述は見当たらないが、申請情報に私有鍵でデジタル署名させるか、あるいはチャレンジデータにデジタル署名させて認証局に送付させる方法等にて行うとしており、申請情報に公開鍵は含まれている。

署名法では、電子証明書に記録する公開鍵は、私有鍵によって行われた電子署名の公開鍵を用いた検証等の方法により、利用者が公開鍵に対応する私有鍵を保有していることを確認するとしている。

WebTrust では、要求しているエンティティに、署名付きメッセージによって公開鍵を送付することを要求する。また、登録要求に含まれる公開鍵に対応する私有鍵によって、登録要求にデジタル署名することを要求している。

【考察】
証明書を要求している者が公開鍵に対応する私有鍵を保持していることの証明のためには、署名付きの要求メッセージを認証局に送ることが必要と考える。一般的

には、認証システムがそのような機能を提供するものと思われる。

［6.1.4］利用者への認証局公開鍵の配布

【RFC2527 記述内容】
認証局の公開鍵の利用者への配布に関する要件。

【各基準の概要】
ガイドラインでは、認証局の証明書は広く一般に開示若しくは公開する必要があるとしている。

署名法では、認証局の私有鍵に対応した公開鍵に係る電子証明書の値を SHA-1 で変換した値が記録され、業務開始時には改ざん防止措置を施して公開されていることとしている。

WebTrust では、初期配布プロセスにおける、認証局の公開鍵の改ざんを検出できるようなメカニズムを提供することを要求している。また、再配布の方法の例示を行っている。

【考察】
認証システム、エンドエンティティの使用するアプリケーション等の利用環境についての検討が必要となる。ただし、クローズドな利用環境の場合、オンラインのみでなくオフラインによる受け渡し等も可能である。

［6.1.5］鍵のサイズ

【RFC2527 記述内容】
鍵のサイズに関する要件。

【各基準の概要】
ガイドラインでは、アルゴリズム、鍵長の指定はしていない。

署名法では、主務省令に定める基準としており、現状では RSA 方式、又は RSA‐PSS 方式であって、モジュラスとなる合成数が 1024 ビット以上のもの、ECDSA 方式であって、楕円曲線の定義体及び位数が 160 ビット以上のもの、 DSA 方式であって、モジュラスとなる素数が 1024 ビットのもの、主務大臣が認めたものとし

ている。

WebTrust では、認証局の規定要件に従うとしている。ただし、暗号化モジュールの基準のところで、鍵の生成には、ANSI X9 や ISO 規格で規定されているような鍵生成アルゴリズムを用いることとしている。

【考察】
現状、一般的には認証局の鍵の暗号アルゴリズム、鍵長は署名法に記述されているアルゴリズムが使用されることが多いと思われる。

［6.1.6］公開鍵パラメータの生成主体

【RFC2527 記述内容】
公開鍵生成のための暗号化モジュールにおけるパラメータに関する要件。

【各基準の概要】
ガイドラインでは、記述はない。

署名法では、暗号化モジュール及び鍵長について記述している。

WebTrust では、鍵の生成は、ANSI X9 や ISO 規格で規定されている、乱数発生器か擬似乱数発生器を使用すること、ANSI X9 や ISO 規格で規定されている素数発生器を使用することとしている。

【考察】
一般的には、パラメータの生成主体は、認証システム内の暗号化モジュール又は HSM と考えられる。

［6.1.7］パラメータ品質の検査方法

【RFC2527 記述内容】
公開鍵のパラメータの品質チェックにに関する要件。

【各基準の概要】
3 基準ともに、特段の記述はしていない。

【考察】
暗号アルゴリズムに設定するパラメータの値によっては、暗号解読の危険性が増すため、パラメータ品質の確認を行う必要がある。ただし、一般的には HSM 等暗号化モジュールを使用する場合が主であり、その HSM 等暗号化モジュールがどのような認定、例えば FIPS140-1 のような規格、に合致しているかの確認を行うこととなる。

［6.1.8］ハードウェア又はソフトウェアによる鍵ペア生成

【RFC2527 記述内容】
鍵生成はハードウェア又はソフトウェアで生成されるかに関する要件。

【各基準の概要】
［6.1.1］鍵ペア生成の主体にて記述

［6.1.9］鍵の使用目的

【RFC2527 記述内容】
鍵の使用目的、制限に関する要件。

【各基準の概要】
ガイドラインでは、検証者の義務として、証明書の使用目的を確認することとあることと、証明書プロファイル中の KeyUsage に格納される値の、各ビットについて記述している。

署名法では、認証局の私有鍵の用途は認証業務の発行する電子証明書への電子署名のみに使用されるとしている。その他、認証業務上で必要になる認証局私有鍵で署名して良いケースを挙げ、それ以外の用途への署名を禁じている。

WebTrust では、認証局の鍵は、意図した目的のためだけに使用されることを保証するコントロールを求めている。

【考察】
認証局の鍵の使用目的については、CP に記述されている目的以外に使用されるべきでないことは当然であるが、認証局の発行する証明書については、3 基準ともに X509　Version3 証明書拡張の KeyUsage について基準として何を記述すべきかの

記述はない。現在、否認防止の署名に利用する場合、NonRepudiation ビットのみとすべきであると言われるようになってきているが、その証明書を利用しようとすると、一般的なメーラー等でサポートしていない場合があり、利用できないことがある。KeyUsage については、どのような利用を意図しているのか、またどのような利用環境で使用するのかによって注意が必要である。

4.4.6.2. ［6.2］私有鍵の保護

［6.2.1］暗号化モジュールに関する標準

【RFC2527 記述内容】
暗号化モジュールに要求される標準に関する要件。

【各基準の概要】
ガイドラインでは、不正顕示（Tamper evident）機能、不正防護（Tamper resistant）機能、不正対抗（Tamper responsive）機能を求めている。さらに、複数人管理を要求するメカニズム、私有鍵情報を複数要素に知識分散を備えていることを必要としている。

署名法では、次の事項を要求している。

- 認証局の私有鍵の漏えいを防止するために必要な機能を有する専用の電子計算機を使用すること。
- 暗号化、署名等、通常の暗号化機能を実施するための機能を有すること。
- 暗号装置自体の初期化、署名符号などの重要パラメータの投入等、暗号装置を管理するための機能を有すること。
- それぞれに権限の有無が特定されること。
- 安全な擬似乱数生成アルゴリズムを使用すること。

WebTrust では、認証局の署名用の私有鍵は、認証局の規定要件に従い、ISO 15782-1/FIPS 140-1/ANSI X9.66 を満たす安全な暗号化装置に保管するとしている。また、鍵の生成は、ANSI X9 や ISO 規格で規定されている、乱数発生器か擬似乱数発生器、素数発生器、鍵生成アルゴリズムを使用することとしている。

【考察】
署名法では海外の基準を例示できないので、詳細な記述がされているが、概ね認証

局の私有鍵は FIPS 140-1 にて規定される暗号化モジュールの使用が必要と思われる。FIPS 140-1 におけるレベルについては、証明書の保証レベル、私有鍵の管理レベル等複合的に勘案し決定されるものと思われる。私有鍵の安全性、対外的なアピールについても考慮するとなると、FIPS 140-1　レベル 3 の認定を受けた HSM の使用を推奨する。また、利用者の暗号化モジュールについても、FIPS 140-1　レベル１以上の規格に準拠していることが望ましい。

［6.2.2］複数人による私有鍵の管理

【RFC2527 記述内容】
私有鍵のデュアルコントロールに関する要件。

【各基準の概要】
認証局の鍵は、3 基準ともに、権限のある複数人による管理を必要としている。

【考察】
特記なし。

［6.2.3］私有鍵のエスクロー

【RFC2527 記述内容】
私有鍵の寄託に関する要件。

【各基準の概要】
ガイドライン、署名法では、寄託に関する記述はない。

WebTrust では、認証局の私有鍵の管理を第三者に委託する場合、責務と賠償責任を含めた契約を結ぶこととしており、また認証局に寄託された利用者の私有鍵は、リスクアセスメントや認証局の規定要件に基づいた暗号化アルゴリズム･鍵長を用いて暗号化したものを保管するとしている。

【考察】
一般的には､認証局の私有鍵は認証局自身で厳重に管理されるものと考える｡また､利用者の私有鍵についても、認証局で保持しないことが必要と考える。WebTrust に記述されている、認証局による利用者の私有鍵のエスクローは、署名用の鍵についてではなく、暗号用の鍵ペアについての記述と思われる。

［6.2.4］私有鍵のバックアップ

【RFC2527 記述内容】
私有鍵のバックアップに関する要件。

【各基準の概要】
3 基準ともに、認証局の私有鍵のバックアップは使用中の鍵の保管レベルと同等以上のセキュリティで保管が必要であり、ガイドライン、WebTrust ではバックアップは遠隔地に保管することを推奨している。

【考察】
認証局の私有鍵が損壊した場合、その私有鍵で署名した証明書の全てに影響が及ぶため、バックアップがなされ、厳重に管理される必要がある。また、地震等広域災害に備え、遠隔地にバックアップを保管することが望ましい。

［6.2.5］私有鍵のアーカイブ

【RFC2527 記述内容】
私有鍵のアーカイブの有無、アーカイブ形態等に関する要件。

【各基準の概要】
ガイドラインでは、有効期間が終了した私有鍵や共通鍵は、保存期間を定めて、複数人管理や知識分散による保存（archiving）を行う必要があるとしている。また、認証局の公開鍵は有効期間後も可用性を確保することが必要であり、改ざんされないように保存する必要があるとしている。

署名法では、アーカイブとしての記述はない。

WebTrust では、現在使用している鍵と同等かそれ以上のセキュリティコントロール、アーカイブ期間が終了した時には、物理的に安全なサイトにおいてデュアルコントロールを用いて破壊、アーカイブされた鍵は本番環境に戻して使用しない等記述されている。

【考察】
認証局が HSM 等の暗号化モジュールを使用している場合、認証局の私有鍵は HSM 以外には存在せず、HSM の管理が重要となる。

［6.2.6］暗号化モジュールへの私有鍵の格納

【RFC2527 記述内容】
暗号化モジュールへの私有鍵の格納に関する要件。

【各基準の概要】
3 基準ともに、［6.1.1］鍵ペア生成の主体、［6.2.1］暗号化モジュールに関する標準、［6.2.2.］複数人による私有鍵の管理で述べられているように、認証局自身の私有鍵は、権限のある複数人の者によって、安全な暗号化モジュールを使用して、生成、格納することとしている。

【考察】
特記なし。

［6.2.7］私有鍵の活性化方法

【RFC2527 記述内容】
私有鍵を活性化できる者及びコントロールに関する要件。

【各基準の概要】
ガイドラインでは、認証局の私有鍵を利用可能状態にする操作又は利用停止状態にする操作は、複数人管理のもとで行う必要があるとしている。また、より高いセキュリティを確保するため、暗号化モジュールを含むシステムを必要の都度スタンドアロンで運用することが望ましいとしている。

署名法では、認証局の私有鍵の状態変更は認証設備室内で実施され、複数人により行われかつその内の１名だけの操作では状態変更がなされないこととしている。

WebTrust では、認証局の私有鍵の活性化は、複数人コントロールにて行うこととしている。

【考察】
特記なし。

［6.2.8］私有鍵の非活性化方法

【RFC2527 記述内容】
私有鍵を非活性化できる者及びコントロールに関する要件。

【各基準の概要】
［6.2.7］私有鍵の活性化方法と同様。

【考察】
特記なし。

［6.2.9］私有鍵の破棄方法

【RFC2527 記述内容】
私有鍵を廃棄することができる主体者、廃棄方法に関する要件。

【各基準の概要】
3 基準ともに、認証局の私有鍵の使用終了時には、物理的破壊、完全な初期化等の手段により、複数人によって、認証局の私有鍵（バックアップ、アーカイブも含め）の廃棄が行われ元の状態に戻せないことを確認することとしている。

【考察】
使用する HSM 等に応じた方法で、私有鍵の完全な廃棄が必要となる。

4.4.6.3. ［6.3］鍵ペア管理に関するその他の面

［6.3.1］公開鍵の保存

【RFC2527 記述内容】
公開鍵の保存の要否、セキュリティに関する要件。

【各基準の概要】
ガイドラインでは、認証局の公開鍵は有効期間後も可用性を確保することが必要であり、改ざんされないように保存する必要があるとしている。

署名法、WebTrust ともに、公開鍵の開示のための保管は記述しているが、保存に関する要件は示していない。

【考察】

認証局のシステム、鍵更新の仕組みに応じて、検討される必要があると思われる。一般的には、認証局の鍵は、更新されたとしても、新しい公開鍵と古い公開鍵がリンクされ、リポジトリ上に残っているため、検証者による署名検証の可用性は確保される。

［6.3.2］私有鍵と公開鍵の有効期間

【RFC2527 記述内容】
私有鍵と公開鍵の有効期間に関する要件。

【各基準の概要】
ガイドラインでは、有効期間を設け定期的に更新する必要があるが、鍵の有効期間の設定は認証局のポリシーによるものとしている。

署名法では、発行する電子証明書の有効期間は 5 年を超えないこととしている。

WebTrust では、認証局の規定要件に従い定期的に鍵更新するとしているが、期間の限定はない。

【考察】
一般的には、期間の短いほうが、より安全性が高いと言われているが、使用する鍵の生成アルゴリズム等によって決定され、また、暗号解読技術の進展等を踏まえた変更が必要になると思われる。

4.4.6.4. ［6.4］活性化用データ

【RFC2527 記述内容】
暗号化モジュールの起動時に要求される活性化用データの保護方法に関する要件。

【各基準の概要】
ガイドラインでは、活性化用データに関する記述はない。

署名法では、認証局の私有鍵の活性化用データについては触れていない。利用者の私有鍵の活性化に使用するＰＩＮ等の秘密情報の生成、転送、出力等は、権限のある操作者によって行われ、アクセス権限管理、内部牽制等により盗聴、改変防止等の措置が施されていることとしている。

WebTrust では、認証局の私有鍵の活性化データについての記述はないが、活性化は複数人コントロールとしている。

【考察】
特記なし。

4.4.6.5. ［6.5］コンピュータのセキュリティ管理

【RFC2527 記述内容】
コンピュータのセキュリティ管理に関する要件。

【各基準の概要】
ガイドラインでは、不正アクセス対策を講じ、システムの異常状態、不正運用等を早期に発見するためのモニタリングを必要とし、停止を防止するために重要システムの二重化を推奨している。

署名法では、認証業務用設備へのアクセス管理がパスワードを用いてなされる場合は、適切なパスワードの設定、定期変更を要求している。また、システム管理者のアカウントについては、パスワードに特殊文字を含む等のより厳格な管理を要求している。

WebTrust では、使用前のテスト、リポジトリ又は他の公開メカニズムの性能のモニタリング及び完全性の維持管理、悪意のあるソフトウェアの防止及び検出等記述している。

【考察】
認証局特有な鍵管理等の他に、情報セキュリティ全般に係るコンピュータのセキュリティ管理が重要と思われる。

4.4.6.6. ［6.6］ライフサイクルのセキュリティ管理

【RFC2527 記述内容】
システムの開発管理、セキュリティ管理に関する要件。

【各基準の概要】
ガイドラインでは、次の事項を要求している。

- 開発担当者に求められる開発経験、能力等を明らかにし、適切な人材を開発にあてること。
- 品質記録を残すこと。
- 不正プログラムの混入防止のため、セキュリティ機能について第三者によるソースプログラムのレビュー等を実施すること。
- ソフトウェア開発環境の部屋は入退出管理を必要とすること。

また、ドキュメントやプログラムは管理責任者あるいは管理責任者が許可した者だけがアクセスできる環境下で保管されること及び導入システムに関しては、常にセキュリティ上の欠陥等の情報収集に留意し、必要な措置を遅滞なく行うことが望ましいとしている。

署名法では、認証業務用設備に対するセキュリティ基準が文書として規定され、それにかなった設備が設置されていることとしている。

WebTrust では、次に事項を要求している。

- 開発及びテスト装置（環境）は本番環境から分離すること。
- 処理能力及び記憶容量を十分に確保するため、利用状況を監視し将来に必要な処理能力や容量を予測すること。
- ウイルス、不正ソフトウェア、不正侵入者に対する検知や保護を実施すること。
- 新しいシステムの導入前にシステムテストにより評価すること。
- 外部委託の厳格な管理　等。

【考察】

2.2.6.5［6.5］同様な検討の他、開発環境についての管理も求められている。

4.4.6.7. ［6.7］ネットワークのセキュリティ管理

【RFC2527 記述内容】

ファイアウォールを含むネットワークセキュリティに関する要件。

【各基準の概要】

ガイドラインでは、次の事項を要求している。

- ファイアウォールの設置や重要なシステムのネットワークからの分離等の対

策を講じておくこと。
- ファイアウォールのシステム、機器についても防犯・防災対策を講じておくこと。

署名法では、次の事項を要求している。

- 不正なアクセス等を防御するためのファイアウォール及び不正なアクセス等を検知するシステムを備えること。
- 通信機器の要件として、利用しないプロトコルによる通信を遮断すること。
- 通信機器の要件として、特定発信元及び特定着信先の指定並びに指定先以外の通信を遮断すること。
- 通信機器の要件として、利用しないネットワークサービスへの通信を遮断すること。
- 通信の記録が可能であること。

WebTrust では、次の事項を要求している。

- 第三者から保護するため、ファイアウォール等を導入すること。
- アクセス制御ポリシーに従いユーザが使用できるサービス（HTTP、FTP 等）を制限すること。
- ルーティングを管理すること、ユーザ端末からサービスコンピュータへの通信路を管理すること。
- リモートユーザによるアクセスは認証を行うこと。
- 診断ポートの管理をすること　等。

【考察】

外部からのアクセス管理のみではなく、内部からのアクセスについても記録を残す、認証を行う等の十分な管理が行える必要がある。

4.4.6.8. ［6.8］暗号化モジュールの技術管理

【RFC2527 記述内容】

暗号化モジュールの設計、製造、配達やアルゴリズムへの準拠性等の技術的管理に関する要件。

【各基準の概要】

ガイドラインでは、記述はない。

署名法では、認証局の私有鍵の漏えいを防止するために必要な機能を有する専用の電子計算機であり、暗号化、署名等、通常の暗号化機能を実施するための機能、暗号装置自体の初期化、署名符号などの重要パラメータの投入等、暗号装置を管理するための機能を有し、それぞれに権限の有無が特定されることとしている。また、安全な擬似乱数生成アルゴリズムを用いこと等が記述されている。

WebTrust では、暗号化装置のライフサイクル管理という観点で記述されている。暗号化装置のメーカーからの受取時のコントロール、保管に関するセキュリティ要件、使用する前のテストの必要性等。

【考察】
前述の［6.1.1］と同様に、ISO 15782-1/FIPS 140-1/ANSI X9.66 等の基準に基づいて、暗号化モジュールを決定する必要がある。また、製品の選定のみではなく、納品時の検収、検収後の保管管理、使用前のテスト等、納品から本番使用までの間の管理が重要と思われる。

4.4.7. ［7］証明書と失効リストのプロファイル

4.4.7.1. ［7.1］証明書のプロファイル

【RFC2527 記述内容】
証明書の様式、拡張領域を含め様式の各領域の使い方などに関する要件。

【各基準の概要】
署名法では、電子証明書の様式及び記載する基準、記述に使用する言語を明確にし、発行者名、発行番号、有効期間、利用者氏名、利用者署名検証符号及び当該検証符号に係るアルゴリズム識別子を電子証明書に記載するよう求めている。

WebTrust は、証明書のフォーマットを ISO9545 / X.509 に従って生成するよう求めている。

ガイドラインは、特に規定していない。

【考察】

電子証明書のプロファイルはアプリケーションにおいて各フィールドの値を解釈する上で重要である。特に、拡張領域の使用は重要である。署名法の認定審査では、詳細なプロファイルを CP/CPS に記述することが求められる。

4.4.7.2. ［7.2］証明書失効リストのプロファイル

【RFC2527 記述内容】
CRL の様式、拡張領域を含め様式の各領域の使い方などに関する要件。

【各基準の概要】
署名法では、電磁的に記録する失効に関する情報（CRL のこと）を明確に定めることを要求している。

WebTrust では、CRL に通し番号を含めるよう求めている。

ガイドラインは、特に規定していない。

【考察】
署名法の電磁的に記録する失効に関する情報を明確に定めるとは、実質的に CRL のプロファイルの詳細記述を要求している。

なお、証明書の有効性確認に OCSP（Online Certificate Status Protocol）[27]を用いる場合は、OCSP のバージョン情報や拡張領域について記述することになる。

4.4.8. ［8］仕様の管理

【RFC2527 記述内容】
CP/CPS の改訂にかかる手続、改訂内容の公表などに関する要件。

【各基準の概要】
CP/CPS の改訂に関する手続が明確に定められていること及び利用者、検証者へ公表することを要件としている。

署名法の場合は、これらを CP/CPS に定め、かつ電磁的方法により記録し公開することを要求している。

---

[27] RFC2560, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol”, http://www.ietf.org/rfc/rfc2560.txt

WebTrust では、特に、承認機関として権限と責任を有する組織（PMA：Policy Management Authority）の設置を強く求めている。

ガイドラインは、特に規定していない。

【考察】

承認を含む改訂手続を明確にすることは必須要件であるが、実際問題として、重要な問題と軽微な問題とでは手続が異なってしかるべきである。これを分けて記述している CP/CPS もある。

また、発行（公表）日と発効日を分け、公表後、利用者からの意見を受け付ける期間を設定している CP/CPS の例もある。

4.4.9. ［9］その他の要件

本項では、WebTrust の要求事項の内、RFC2527 の 1 から 8 章に分類していない事項を記述している。

【基準の概要】

WebTrust においては、オプション項目として、証明書を IC カードに発行する際の認証局の管理要件を記述している。また、認証局特有なマネジメント以外に全社的な情報セキュリティ、資産管理、法律等への準拠等、全社的なセキュリティマネジメント関する事項を記述している。

IC カードの発行に関する記述としては、IC カード発行機能又はシステムに対する共通データや要求データの扱い、管理主体等が詳細に記述されている。

また、全社的なセキュリティマネジメントとしては、次のような事項を記述している。

- 経営者によるセキュリティポリシの決定及びその周知
- セキュリティポリシの定義項目（目的、適用範囲、重要性、配布方法、教育、事故に対する報告、責任体制等）
- セキュリティポリシの維持責任、レビュープロセス
- 情報セキュリティ委員会等による明確な管理
- 資産の保護

– 新規導入の情報設備の認可プロセス
– 認証局資産の在庫の維持
– 情報保護のコントロール
– 情報分類の定義

【考察】

IC カードに関する要件は、認証局以外がカード発行する場合のコントロールと思われるが、証明書の申請者である利用者自身が生成を行わない場合、私有鍵情報の秘匿性が重要となり、詳細に検討すべき項目と思われる。

認証局の私有鍵管理等の特有な管理要件は、全社的なセキュリティマネジメントがベースにあって成り立つものであり、後述の 3 章においても記述しているが、強固な認証局を構築する場合、高度なセキュリティを維持、管理できるように全社的な情報セキュリティマネジメントを確立すべきと考える。

4.5. 認証局の立ち上げにおける留意事項

4.5.1. 情報セキュリティ全般

強固な認証局の構築を検討する際、認証局特有の業務運用に関する基準については 3 つの基準が参考になるが、全般的な情報セキュリティについても組織体全般に適用が検討されるべきである。WebTrust で一部全般的な情報セキュリティ基準について触れているが、情報セキュリティ基準として検討すべき項目を総括的に見ておく必要がある。

現状では JIS X5080-2002（情報技術－情報セキュリティマネジメントの実践のための規範）がもっとも参考になるといえる。JIS X5080-2002 は、ISO/IEC17799：2000（Information technology－Code of practice for information security management）がベースである。タイトルが示しているように、特定の個別対策ではなく、情報セキュリティマネジメントシステムの確立という視点で管理策が示されている。

以下、JIS X5080-2002 の大分類項目ごとに、管理目的とポイントを記述する。

(1) セキュリティ基本方針

情報セキュリティのための経営陣の指針及び支持を規定するために、情報セキュリティポリシの策定及びリスクアセスメントに基づく見直しなどの必要性を挙げている。

(2) 組織のセキュリティ

情報セキュリティを管理するために、情報セキュリティの承認機関、調整機能の組織化、各部署が持つセキュリティ上の役割の明確化、外部委託の為のセキュリティ要求事項の取り決め、といった必要性を挙げている。

(3) 資産の分類及び管理

重要な情報資産を保護するために、情報の分類、情報の保護レベル、管理責任の明確化などの必要性を挙げている。

(4) 人的セキュリティ

人にかかわるセキュリティ上のリスクを軽減するために、社員等に対する機密保持誓約、教育・訓練、セキュリティ事故に対する報告体制の確立などの必要性を挙げている。

(5) 物理的及び環境的セキュリティ

業務施設や業務情報を不正アクセス、災害等から保護するために、建物・室等の物理的な保護策、入退管理、装置のセキュリティ対策、職場環境の整備などの必要性を挙げている。

(6) 通信及び運用管理

故意又は過失によるセキュリティ上のリスクを軽減するために、運用管理、システム管理、ネットワーク管理、障害管理などの必要性を挙げている。

(7) アクセス制御

情報へのアクセスを制御するために、アクセス権の管理、ネットワークのアクセス制御、アプリケーションへのアクセス制御、モバイルコンピューティングや遠隔作業に関する取り決めなどの必要性を挙げている。

(8) システムの開発及び保守

情報システムに適切なセキュリティ機能を組み込むために、開発するシステムに要求されるセキュリティ要件の明確化、暗号使用に関する方針、開発プロセスの信頼性確保などの必要性を挙げている。

(9) 事業継続管理

重大な障害や災害発生によって中断した業務を速やかに復旧するために、事業継続の考え方、影響分析、継続計画の準備とその有効性確認（テスト）などの必要性を挙げている。

(10) 適合性

コンプライアンスを確実にするために、法的要求事項への的確な対応、準拠性監査などの必要性を挙げている。

4.5.2. 認証局の保証について

4.5.2.1. 保証レベル

証明書は証明書の使途によって要求される信頼性が異なり、認証局に要求されるセキュリティ要件も異なってくる（ECOM ガイドラインの付録 A 認証局のレベリング）。このような考え方で保証レベルを分け、CP/CPS の中で保証レベル別に要件を記述している例がある。FBCA CP、DOD（米、国防総省）CP では、次の項目について保証レベルによる要件を分けて記述している。項目の後の数字は RFC2527 の項番を示す。

- 名前の形式（3.1）
- 本人確認（3.1）
- 鍵更新（3.2）
- 失効申請を受けてから処理するまでに要する時間（4.4）
- CRL の更新周期（4.4）
- 採取すべきログの種類（イベント）（4.5）
- ログの検査周期（4.5）
- 長期保存すべきログの種類（イベント）と保管期間（4.6）
- 暗号化モジュールの仕様（6.1）
- 証明書の有効期間（6.3）

これらの項目は一般的に強固な認証局を構築しようとするときに、高度なセキュリティが確保できるような要件として定義すべきものといえる。

4.5.2.2. 認証局の責任

電子商取引等に関する準則（経済産業省：平成 14 年 7 月）の中に、なりすましを生じた場合の認証機関の責任に関する記述がある。本人確認が不十分な場合について、該当部分を引用し（枠表記、以下同じ）、説明を加える。

第１オンライン取引

１．契約手法に関する問題

（３）なりすましを生じた場合の認証機関の責任

【論点】

電子署名の認証機関による本人確認が不十分なため、なりすましが生じた場合、認証機関は証明書を信頼して損害を受けた者に対してどのような責任を負うか。

（例）　本人確認が不十分なまま、電子署名の認証機関が名義人（本人）になりすました第三者に電子証明書を発行した。証明書を受け取った取引の相手方が第三者を本人と信じたものの、本人との間で取引の効果が認められない結果、損害を受けた場合、認証機関はどのような責任を負うか。

【考え方】

＜Ｉ＞ 本人確認が不十分な場合

i) 原則：不法行為責任

電子署名の認証機関が十分な本人確認をせずに電子証明書を発行し、その後それが利用され、証明書を受け取った相手方がこれを信じたものの、なりすまされた本人（電子署名の名義人）への効果帰属が認められなかったために損害を受けた場合に、認証機関は証明書の受取人に対し、不法行為責任を負う。この場合、受取人側が認証機関の過失（本人確認が不十分であること）について立証責任を負う。

「十分な本人確認をせずに」とは、CPS に規定された本人確認手続に違反したという意味である。

ii) 例外：契約責任

認証機関と受取人との間に通常は契約関係がないので、認証機関は原則として契約上の責任を負うことはない。

しかし、例えば第三者が証明書を受け取る場合に、認証機関から認証業務規程（CPS ）が示され、受取人が CPS を承認する旨応答する場合などの中には、契約関係の成立を認めることができる場合もあり得る。契約関係が認められた場合、認証機関は CPS を遵守する義務があり、CPS で定めた本人確認手続に違反したときは、債務不履行責任を負う。この場合、認証機関側が自己の無過失について立証責任を負う。

「受取人が CPS を承認する旨応答する場合などの中には、契約関係の成立を認めることができる場合もあり得る」とある。これは、検証者（受取人）が受け取った証明書から発行元の CP/CPS を参照しにいったときに、承認する旨の確認ボタンを押すような場合のことである。このようなアクションで契約関係が成立するためには検証者を特定する情報が必要になるが、そのような仕組みをもった認証局の例を見たことはない。

この前提が現実的であるか、疑問が多い。

4.5.3. 認証局の監査

4.5.3.1. セキュアな認証局であることの保証

認証局の運用の信頼性を一般ユーザに示す端的な方法は、認定制度の活用である。直接的には認証業務の認定取得であるが、認証業務の認定取得以外にも ISMS や BS7799 の認定制度がある。また、ISO/IEC15408 や FIPS の認定製品を使用することも保証を表す一つの手段といえる。

認定取得以外に認証局の運用の信頼性を一般ユーザに示すためには、CP/CPS においてその方針を示すことに加え、実際の運用が CP/CPS に準拠して行われていることを客観的に示すことが必要である。このための一つの手段が監査結果の公表である。

(1) 監査人

RFC2527 において、監査の頻度、監査人の要件、監査項目など、認証局の準拠性監査に関する要件が記載されている。しかしながら、認証局の準拠性監査は法定監査である会計監査とは異なり任意監査なので、監査人の要件を満たす公的な資格があるわけではない。したがって、信頼できる監査結果を得るための一つの方法は、認証局監査の実績がある監査機関を選定することである。また、監査機関の選定の際に、認証業務や PKI に関する知識の有無をヒアリングなどによって確認することも有効である。

(2) 公表

客観的な信頼を示すためには、監査結果の公表が必要であるが、誰に、どこまでを開示するかということを検討しておく必要がある。

証明書の利用が閉じた環境であれば利用者＝検証者であるが、オープンな環境では、利用者（証明書発行対象者）ではない検証者も存在する。認証局と直接の契約関係にあるのは利用者であるが、検証者も認証局が発行した証明書を信頼して利用する以上、検証者に対しても監査結果を公表することが望まれる。したがって、信頼を示す対象は利用者と検証者であることが望ましいと考える。

監査結果報告は、通常、総合的な所見を記述した監査報告書と検証結果の詳細を記述した検証報告書（この名称はさまざまであるが）に分けられる。公表する報告書は、総合的な所見を記述した監査報告書のみとすべきである。検証報告書は、セキュリティ上開示すべきでない詳細情報が含まれている場合があるため、基本的に開示対象とすべきではない。

4.5.3.2. 認証業務の監査 ― 経済産業省の情報セキュリティ監査研究会中間報告書

2002 年 9 月に経済産業省、商務情報政策局長の諮問機関として「情報セキュリティ監査研究会」が設置され、民間の有識者を中心に検討が行われてきた。その中間まとめが本年 1 月 29 日に公表され、パブリックコメントを募集した。その結果を反映し、最終報告書が 3 月一杯にまとめられる予定である。

この報告書の内容は、経済産業省の施策として取り込まれる予定になっている。具体的には、情報セキュリティ管理基準や情報セキュリティ監査基準の公表（告示）や情報セキュリティ監査企業台帳登録制度などであると考えられる。

これらの施策の実施は認証業務に対して直接的なインパクトを与えるものではないが、組織に求められる情報セキュリティ及びその保証としての監査制度のあり方など、動向を把握しておく必要がある。以下、中間報告書の一部分について、そのポイントと考察を記述する。

(1) 情報セキュリティ監査の対象

情報セキュリティ監査の対象はシステムではなく情報資産であり、情報資産に対するマネジメント（情報資産に対するリスクマネジメントが効果的であるか）を監査するという視点である。

これは、経済産業省がシステム監査との違いで強調している点である。認証業務を行う組織についても、組織全体としての情報セキュリティマネジメントは必要であると考える。

(2) 多種多様な組織体の多種多様なニーズに応じた監査制度

組織体が監査に求めるニーズを、監査人から情報セキュリティ対策不備の指摘を得て改善することを意図した「助言型監査」と監査人から情報セキュリティ対策の有効性に関する「お墨付き」を得ることを意図した「保証型監査」に分けている。

特に保証型監査の場合、監査を行う上での判断尺度（Criteria）が明示されていることが必要であり、それを情報セキュリティ管理基準としてまとめている。情報セキュリティ管理基準は ISO/IEC17799 をベースとして、監査の立場からコントロール項目を基礎に細分化している。

しかし、各組織が情報セキュリティの信頼性をユーザに保証するためにどのような監査を行えばよいか、どの程度の監査を行えばよいかといった基準までは示されていない。

保証型監査を定着させることは一朝一夕には難しく、まだまだ議論の余

地があると思われる。しかしながら、被監査組織にとって保証を得るための監査という要求は強くなるであろうことから、経済産業省がどのような施策を講じていくかを注意しておく必要はある。

(3)監査人の独立性

保証型監査において監査人の独立性は必須要件である。監査人の独立性に関しては、特に電子政府の情報セキュリティ監査を行う主体に対しては厳格な基準を設けている。

信頼の置ける監査という意味では、独立性だけでなく監査人の資質にかかわる部分が大きい。独立性の問題だけを厳格に意識する必要はなく、一般的に外部の第三者機関であれば十分と考える。

(4)情報セキュリティ監査企業台帳の創設

監査人を選定する目安として、任意登録制（毎年登録）の企業台帳（個人事業者を含む）の創設を掲げている。これは、同時に情報セキュリティ監査を行う主体の質の問題も含んでおり、現存する資格制度は今回の制度と完全に親和性をもつものではないため、人材の資格制度のあり方を検討する必要があるとしている。

この制度ができた場合、企業台帳の利用は監査機関を選定する上で参考になるかもしれない。しかし、監査機関の選定に当たっては、提案書の検討などから適切な監査委託先であることを被監査組織側が評価できることが重要になる。

4.5.4. 証明書のプロファイルと証明書の扱いに関する要件

4.5.4.1. 証明書プロファイル（Key Usage）

証明書のプロファイルに関しては、証明書の使用目的に依存するため各基準ともその内容までは規定していない。しかしながら、否認防止を目的とした場合、証明書プロファイルの Key Usage の Non-Repudiation が該当するが、4.5.4.2 節の項で述べているように、Non-Repudiation にビットを立てたときは他のビットを立ててはいけないということに注意が必要である。

4.5.4.2. Qualified Certificates

QC（Qualified Certificate）は、EU Directive に基づいて検討されている否認防止をサポートする証明書である。これに対応し、かつ特定の法的要件に依存しないように

QC のプロファイルを規定したものが RFC3039[28]として公表されている。以下、QC プロファイルとして記述すべき領域とその内容の概要を示す。

(1) 証明書の基本領域

- 発行者名（Issuer）

  次の属性を使って名前をユニークに定める。domainComponent、countryName 、 stateOrProvinceName 、 organizationName 、localityName、serialNumber、他の属性を追加することも可能であるが、発行機関の識別にそれらの属性を必須項目とすべきではない。

- 主体者名（Subject）

  次の属性を使って名前をユニークに定める。countryName、commonName、surname、givenName、pseudonym、serialNumber、organizationName、organizationalUnitName、stateOrProvinceName、localityName、postalAddress、このうち少なくとも commonName、givenName、pseudonym のどれかを含めなければならない（pseudonym でもよいとしている)。

  また、他の属性が存在してもよいが、発行者ドメイン内でほかの主体者名から該当主体者名を識別するための必須項目にしてはならない。

(2) 証明書拡張領域

- 主体者ディレクトリ属性（Subject Directory Attributes）

  この拡張は主体者の属性を次のものから選択して記述できる。ノンクリティカルである。title、dateOfBirth、placeOfBirth、gender、countryOfCitizenship、countryOfResidence

- 証明書ポリシー（Certificate Policies）

  証明書ポリシーは、少なくとも 1 つの証明書ポリシーOID を含めなければならない。これは認証局の CPS を反映したものでなければならない。この拡張はクリティカルとして良い。

- 鍵使用目的（Key Usage）

  この拡張は必ず含めなければならない。もしこの拡張に nonRepudiation ビットを立てた場合は他の鍵使用目的を指定してはいけない。この拡張はクリティカルとして良い。

---

[28] RFC3039, “Internet X.509 Public Key Infrastructure Qualified Certificates Profile”, http://www.ietf.org/rfc/rfc3039.txt

- バイオ情報

  この拡張は QC としての独自拡張で、バイオ情報を指定できる。バイオメトリクスの情報は、バイオメトリクスのハッシュ値の形で格納される。この拡張の目的は生体情報による認証方法を提供することであり、格納されたハッシュ値に対応する生体情報そのものは拡張に格納されない。ノンクリティカルである。

- QC 宣言（Qualified Certificate Statements）

  ある特定の法制度に従った証明書を QC として発行するという発行者の宣言は、この拡張へ適合する典型的な宣言である。ここには法で規定された指定宣言や認証局の義務や制限も書くことができる。各宣言は OID で指定できるものでなければならない。この拡張はクリティカルでもノンクリティカルでも良いが、クリティカルとした場合は、この QC 宣言拡張のすべてがクリティカルであるとされる。

4.5.4.3. TSA のセキュリティ要件

電子署名を検証するためには、署名者のデジタル署名の適用が署名者の証明書の有効期間中に行われたことを証明しなければならない。時刻を証明する方法として、あるデータが特定時刻以前に存在していたことを証明できるタイムスタンプを使用する方法がある。

タイムスタンプは電子署名の重要な要素であり、RFC3161 にも規定されている。ここでは、ETSI TS 102 023 V1.1.1「タイムスタンプ局のポリシー要件」をもとに、TSA に求められる要件について記述する。

(1) 実施及び開示規定

- TSA 実施規定

  認証局における CP/CPS にあたるような規定として、TSA においては TSA 実施規定を策定する。TSA 実施規定には、セキュリティ管理と運営手順、組織の義務等を記述する。

- TSA 開示規定

  TSA はすべての利用者と検証者に対してタイムスタンプサービスの使用に関する条件を開示する必要がある。契約情報・義務等、認証局でも開示が求められるものの他に、TSA 独自に求められる項目として次のものがある。

- タイムスタンプポリシ
- タイムスタンプが付与されるデータを表現するために使用されているハッシュアルゴリズム
- タイムスタンプトークンに署名するために使用される署名の予想寿命（使用されるハッシュアルゴリズム、使用される署名アルゴリズム及び私有鍵の長さに依存）
- タイムスタンプトークン内の時刻の UTC（協定世界時刻）に対する精度

• 鍵管理サイクル

TSA においても、認証局と同レベルの厳格な鍵の運用管理が求められる。署名鍵の生成や私有鍵を保管する暗号化モジュールについては、次のレベルが求められる。

- FIPS140-1 レベル 3 以上に定める要件を満足するモジュール
- CEN Workshop Agreement14167-2 に定める要件を満足するモジュール
- ISO15408 の EAL4 以上又は同等のセキュリティ基準が保証された信頼あるシステム

TSA 公開鍵の配布、TSA 鍵の再発行、TSA 鍵のライフサイクルの終了、暗号化モジュールのライフサイクル管理における運用管理においては、認証局と同レベルの厳格な運用管理体制が必要となる。

• タイムスタンピング

– タイムスタンプトークン

TSA は、タイムスタンプトークンがセキュアに発行され、正しい時刻を含むことを保証するものである。タイムスタンプトークンには、次の要件が求められる。

- タイムスタンプトークンは、タイムスタンプポリシの識別子を含むものとする。
- 各タイムスタンプトークンには、一意の識別子が与えられるものとする。
- TSA がタイムスタンプトークンにおいて使用する時刻値は、UTC（k）の研究所によって配信される実際の時刻値の少なくとも 1 つに基づくものとする。UTC（k）とは、UTC との誤差 100ns（ナノ秒）内で実現されている時間スケールのこと。
- タイムスタンプトークンに含まれる時刻は、このポリシーに定める精度内又はタイムスタンプトークンそのものに精度が定められている場合にはその精度内で UTC と同期するものとする。
- タイムスタンププロバイダの時計が定められた精度外にあるとわかった

場合、タイムスタンプトークンは発行されない。

- タイムスタンプトークンには、要求者の指示に従ってタイムスタンプを付与されたデータの表現（ハッシュ値等）を含むものとする。
- タイムスタンプトークンは、生成された専用の鍵を使用して署名が行われるものとする。
- 発行を行う TSA の名前は、タイムスタンプトークンに指定されるものとする。これには次の識別が含まれる。
  - ・該当する場合には、TSA が設置されている国の識別子
  - ・TSA の識別子
  - ・タイムスタンプを発行するユニットの識別子

- UTC との時計の同期

  TSA は、時計が定められた範囲内で UTC と同期していることを保証する。したがって、次の要件に注意する必要がある。

  - TSA の時計の調時を行い、時計が宣言された精度を維持するようにする。
  - TSA の時計は、その目盛を越えるような変化をもたらすおそれのある脅威から保護される。

- TSA の管理及び運営

  TSA における資産管理、人員のセキュリティ、物理的環境的セキュリティ、運用管理のセキュリティ、システムアクセス管理、システムの導入とメンテナンス、TSA サービスの危殆化時の対応、TSA の業務終了、法的要件の遵守、運営に関する情報の記録等、TSA の管理運営にかかわる事項については、基本的には認証局と同レベルの管理運用が求められる。TSA において独自に求められる要件を次に挙げる。

  – 人員のセキュリティ

    認証局に要求される事項に加え、TSA の人員には次のことが求められる。

    - タイムスタンプ技術、デジタル署名技術、TSA の時計の調時又は UTC との同期のメカニズムに関する知識を有する要員を採用すること。

  – タイムスタンプサービスの運営に関する情報の記録

    認証局の要件に加え、次にあげる時計の同期に関連する事項を記録する必要がある。

    - TSA の時計の UTC への同期に関連したすべてのイベントに関するレコードのログが記録されるものとする。この中には、タイムスタンプで使用される時計の通常の調時又は同期に関する情報を含むものとする。
    - 非同期の検出に関連したすべてのイベントに関するレコードのログが記録されるものとする。

4.6. まとめ

本章では、ネットワーク資源の管理を考慮した認証業務のセキュリティ要件を求めるために行った、認証業務の認定基準やガイドラインの比較調査について述べた。ガイドラインや認定基準といったものが国内外で整備されつつあるなかで、この比較調査の結果は認証局構築の際に参照することができる、詳細な基本資料となる。

比較調査の対象とした認証局運用ガイドライン、WebTrust Program for CA、特定認証業務調査表の３基準は、適用分野と対象環境の違いからくる分類の違いがあった。しかし運用上の要件等、共通して考察されていることがあり、認証業務の方針策定の際に重点的に検討する内容を抽出できることがわかった。

また本章では、比較を行うだけに留まらずに、ネットワーク資源の管理を踏まえて、確実な運用を要する認証局と認証業務に向けた考察を述べた。

第5章 レジストリシステムにおける認証システム

内容

- レジストリシステムにおける認証機能
  - レジストリシステムの構成
  - 情報モデルとセキュリティモデル
  - PKI を用いた認証機能
  - レジストリデータベースの応用

5. レジストリシステムにおける認証システム

ネットワーク資源の割り振り及び割り当ての情報は、インターネットレジストリの「レジストリシステム」とよばれるシステムで管理される。レジストリシステムは、ネットワーク資源だけでなくインターネットレジストリがネットワーク利用者の登録情報も管理している。インターネットにおける正しい資源利用の信頼性を向上させるためには、レジストリシステムにおける登録情報（レジストリデータ）の確実な扱いが必要になる。

本章では、レジストリシステムにおけるレジストリデータの確実な取り扱いのために、既存のレジストリシステムにどのような機能を持たせるべきかについて述べる。レジストリデータの信頼性はレジストリシステムの認証機能と、インターネットのような分散環境で信頼性を検証する機能の二つで実現される。従って本章ではレジストリシステムだけでなく、信頼性を検証するユーザ環境についても述べる。更にこれらの機能を利用することで実現可能な応用方法について述べる。

5.1. NIR におけるレジストリシステム

NIR は国別のインターネットレジストリであるため、ネットワーク資源の割り振り及び割り当ては当該国に存在するネットワーク利用組織を対象にして行われる。日本の NIR である JPNIC は、ネットワーク資源を割り振った組織の情報を日本における存在証明書類に基づいて確認する。この登録情報はネットワーク資源の管理のために使用される。またネットワーク利用組織の情報は運用上に必要となる相互の連絡などに使われるため、一部が公開される。

JPNIC における、レジストリシステムとそれに関わる組織の概要を図 30 に示す。

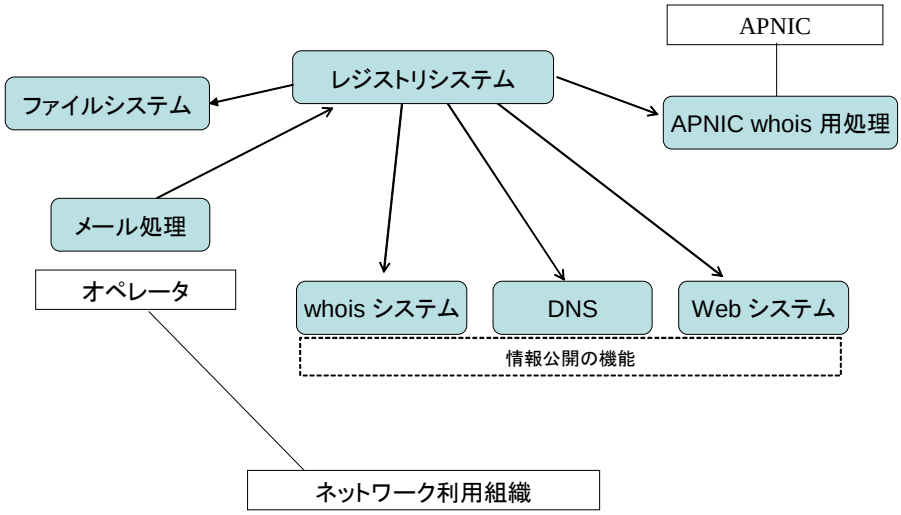


図 30　レジストリシステムに関わる組織とシステム

JPNIC はネットワーク資源の割り当て及び割り振りと同時に、ネットワーク利用組織をレジストリデータベースに登録する。登録情報は、ネットワーク利用組織から電子メールを通じて送られ、オペレーターが対応する。レジストリシステムに入力された登録情報の一部は whois システムなど情報公開の機能をを使って公開され、ネットワークの運用やネットワーク利用組織の相互の連絡等に用いられる。

5.2. レジストリシステムの構成

JPNIC で管理されるネットワーク資源は IP アドレスと AS 番号である。AS 番号は「IRR（Internet Routing Registry)」とよばれるシステムでも管理されているが、これはネットワークの運用の為の情報共有が主な目的であり、ネットワーク資源の管理が目的ではない。

本研究ではネットワーク資源、特に IP アドレスの割り当ての確実性に注目するため、IP レジストリシステムに注目する。IP レジストリシステムの概要を図 31 に示す。

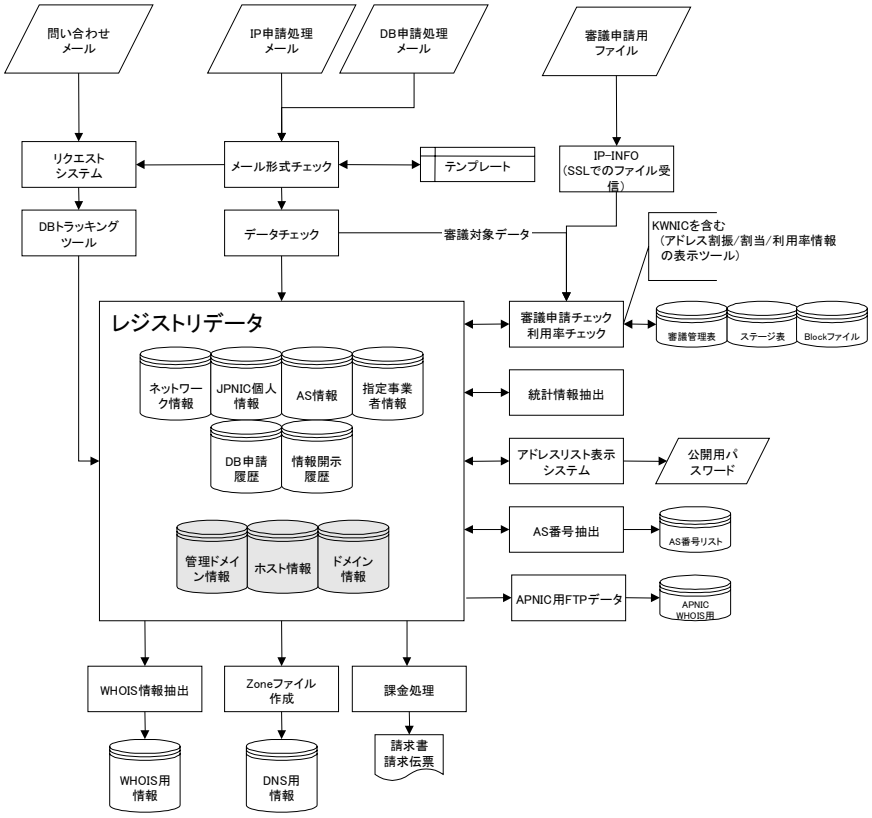


図 31　IP レジストリステム概要図

IP レジストリシステムの主要な処理は中央の四角で囲われたレジストリデータの扱いである。多くの RIR では、whois システムが、レジストリシステムとは別のシステムに位置付けられているが、ここでは後に述べるメッセージ認証機能を考慮するためレジストリシステムの情報公開機能に位置付ける。

IP アドレスの割り振りを受ける LIR（ネットワークサービスプロバイダー等）は電子メールを利用して IP アドレスのアドレスブロックの操作（新規割り振り、サイズの変更）を申請する。レジストリシステムはこのメールを処理し、ホストマスターの審議結果に基づいて情報登録等を行う。登録情報が格納されるデータベースは「レジストリデータベース」とよばれる。

5.3. whois システム

whois システムは登録情報のうち、ネットワーク組織のネットワーク管理者が相互に連絡を取り合うための情報を公開するシステムである（図 32）。1.4.3 節ではこの機能

を「登録情報の提供」として述べた。

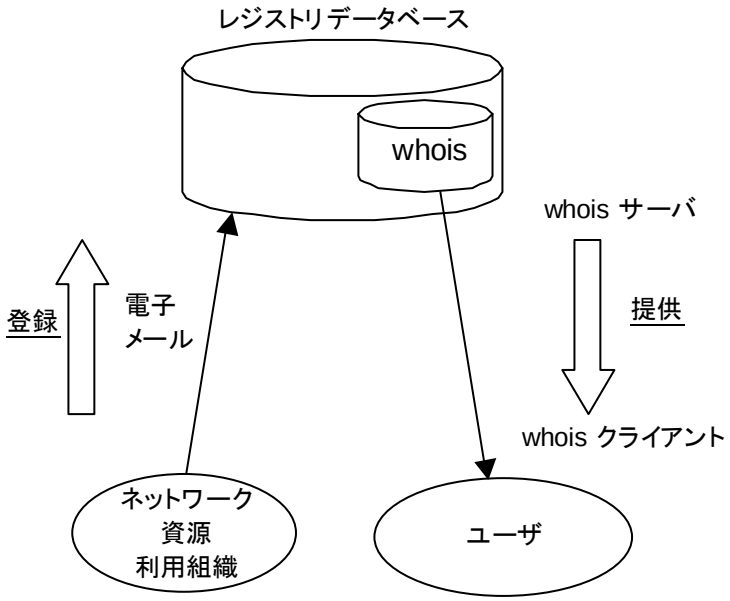


図 32　whois システム

ネットワーク資源を利用する組織が、情報を登録し、その情報を whois システムが提供することで、ネットワーク利用組織の相互連絡の手段を提供している。whois システムは、サーバ-クライアント方式で通信を行うシステムで、ユーザはサーバに格納された情報を検索し、閲覧する。whois システムの構成を図 33 に示す。

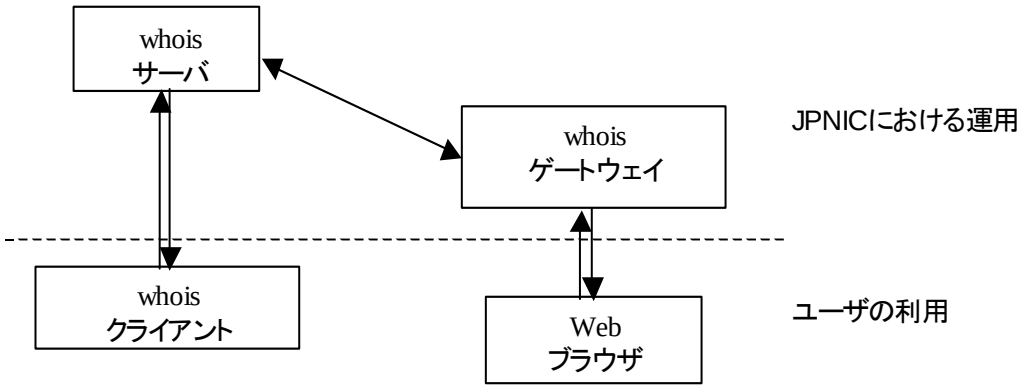


図 33　whois システムの構成

whois システムは、JPNIC における whois サーバとユーザが利用する whois クライアントで構成される。whois サーバは whois ゲートウェイを通じて利用することもできる。

whois システムは、扱われるデータがテキストのみであり、また GUI(Graphical User Interface）の開発環境が現在ほど一般的になっていない時代に開発されたため、多くのクライアントプログラムは CUI（Character User Interface）である。しかし JPNIC では WWW（World Wide Web）インターフェースを提供しており、ユーザは Web ブラウザを使って whois のデータを検索することができる(図 34)。なおこのような Web インターフェースは他の多くのインターネットレジストリでも提供されている。

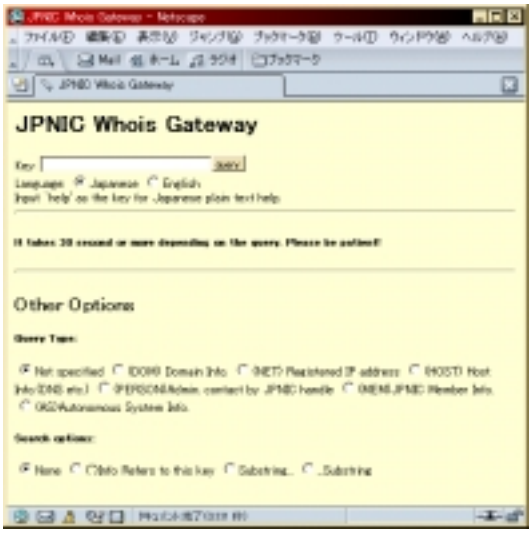


図 34　whois の Web インターフェース

whois の Web インターフェースは、通信プロトコルに HTTP を利用しており、ユーザが検索した結果のデータを転送するプロトコルは、既存の whois クライアントを利用した場合と異なる。https とよばれる TLS を利用した HTTP は、多くの Web ブラウザで利用可能であるため、Web インターフェースの場合には https を利用する構成にすることが可能である。転送プロトコルが異なると安全な通信のための設計に影響がある。

whois システムで扱われる情報は、項目名と値の組み合わせがテキスト形式で表現される。項目名の組み合わせは、データの分類ごとに定義されており、情報を新規に登録する場合、その分類に必要な項目に対応する値を入力する必要がある。

JPNIC の whois システムで扱われる登録情報の分類はレコードの種類の違いとして扱われる。それぞれのレコードのために定義された項目を表 19 に示す。

表 19　whois データのレコードと項目名

レコード名	レコードに含まれる項目名
ネットワーク情報	IPネットワークアドレス、ネットワーク名、組織名、運用責任者、技術連絡担当者、 ネームサーバ、割当年月日、返却年月日、通知アドレス、最終更新
AS情報	AS番号、AS名、組織名、運用責任者、技術連絡担当者、技術連絡担当者 AS-IN、AS-OUT、割当年月日、返却年月日、通知アドレス、最終更新
個人情報	ホスト名、IPアドレス、技術連絡担当者、通知アドレス、最終更新
ホスト情報	JPNICハンドル、氏名、電子メイル、NICハンドル、組織名、 郵便番号、住所、部署、肩書、電話番号、FAX番号、通知アドレス

表 19 で示した項目はすべて whois システムを使って公開されるものである。「ネットワーク情報」は、IP アドレスのブロックが割り振り又は割り当てられている組織の情報を含んでいる。「AS 情報」は AS 番号がその組織に割り当てられていることを示している。「運用責任者」や「技術連絡担当者」は、これらの情報の書き換えを行うことができるユーザを示していると同時に、ネットワーク利用組織の間で連絡を取る際に利用される。「個人情報」は、「運用責任者」や「技術連絡担当者」に含まれる人物情報のレコードである。「個人情報」に変更があった場合でも、「ネットワーク情報」等を変更せずに「個人情報」のみを変更するだけでよい。「ホスト情報」は DNS サーバの情報を登録するために存在する。各ネットワーク利用組織の DNS サーバは必ず「ホスト情報」として登録されなければならない。DNS における名前解決のための権限の委譲は「ホスト情報」に登録されたホストに対して行われる。

JPNIC における DNS は、主に IP アドレスからホスト名を検索する”逆引き”の利用を想定している。これは JPNIC が IP アドレスを割り振る NIR であり、その割り振られた IP アドレスに基づいて DNS が利用されるためである。

このように、whois システムはネットワーク資源の割り振り及び割り当ての情報そのものを提供しており、ネットワーク利用組織の管理者はその前提の上に運用管理を行う。

5.4. レジストリシステムにおける認証機能

レジストリデータの登録や公開を行うレジストリシステムに、セキュリティ機能を持たせるためには、レジストリデータの信頼性を定義し、また運用上の信頼性の度合いを表す尺度が必要となる。定義内容を満たす手法を実現し、その手法の確実性の度合いを増すことで、レジストリデータの信頼性が向上する。

信頼性の度合いは、レジストリシステムの運用上のセキュリティ要件を、どの程度満たしているかによって測られる。従って運用業務の内容と運用結果が明らかにならなければわからない。信頼性を考慮した運用業務の内容は、セキュリティ要件を予め決めることで決定される。本研究では運用業務の内容を決定する作業を、調査研究の後に行うものに位置付けており、信頼性の度合いについてはここでは言及しない。なお、セキュリティを考慮した運用要件を求める方法と基本調査については４章で述べた。

この節では、レジストリシステムにおけるセキュリティモデルと情報モデルについて述べた上で、認証機能のあり方について述べる。

5.4.1. 情報通信のセキュリティモデル

情報のやり取りが行なわれるエンティティの間のセキュリティは、大きく分けて「トランスポートセキュリティ」と「オブジェクトセキュリティ」の二つのセキュリティモデルに沿って考察される（図 35）。

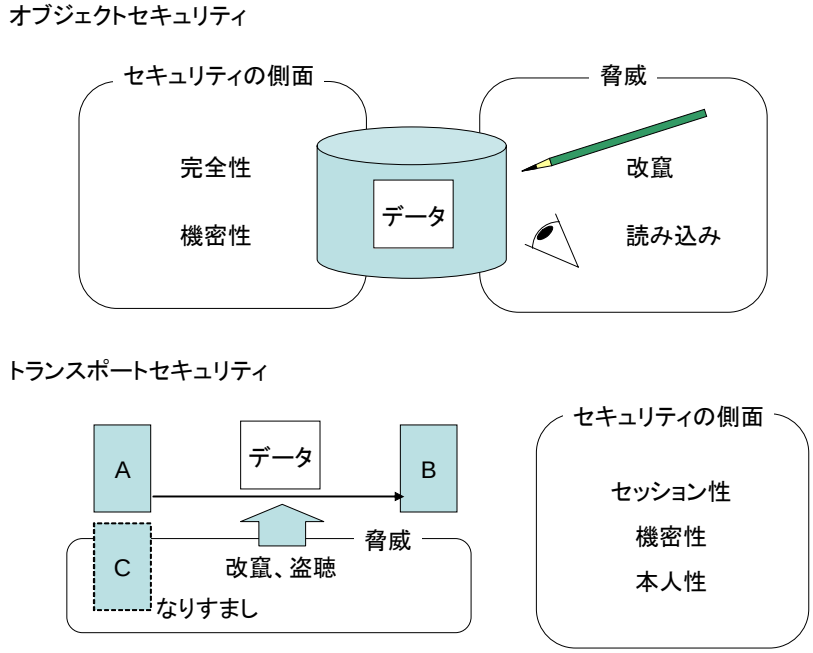


図 35　二つのセキュリティモデル

オブジェクトセキュリティとは、情報の機密性、完全性など、データの状態に注目したモデルである。このモデルでは機密性や完全性を保証する暗号強度などが問題となる。

トランスポートセキュリティとは、二つのエンティティの間でやり取りされる情報をいかに保護するかに注目したモデルである。このモデルでは通信相手の認証、通信相手の特定、メッセージの完全性などが問題となる。

情報は、対象とする情報モデルに応じて適切に適用されなければならない。例えば電子メールのセキュリティプロトコルを考案する際に、トランスポートセキュリティのモデルは適さない。これは保護対象が電子メールのメッセージであるため、個々の通信を保護するモデルでは、次々に転送される電子メールの仕組みにそぐわないからである。

5.4.2. レジストリシステムの情報モデル

レジストリシステムにおける保護対象は、レジストリデータである。レジストリデータには個人情報や組織情報など機密性を要求される情報が含まれていると同時に、whois システムを用いてユーザに開示される情報が含まれている（図 36）。

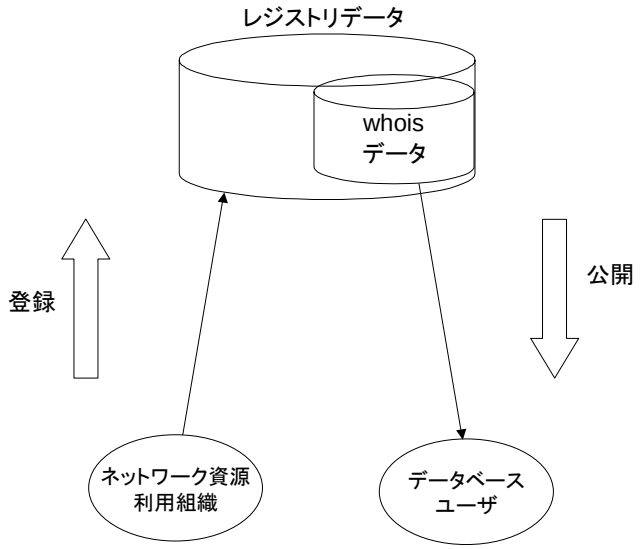


図 36　レジストリデータの情報モデル

１章及び２章で述べたように、レジストリシステムで管理される情報は、委譲された権限の範囲の情報である。この情報は、ネットワークを通じてやり取りされるかどうかに関わらず保護されなければならない。従ってオブジェクトセキュリティのモデルを適用するべきである。

しかしインターネットを通じて使われる通信プロトコルのうちオブジェクトセキュリティを適用としたものは少ない。例えば https や SSH といったプロトコルは、通信相手の認証や、やり取りされるデータの機密性を実現するためのもので、トランスポートセキュリティのモデルが適用されている。whois システムのように即時操作性を提供するサービスを使ってレジストリデータの情報公開機能を実現するには、レジストリシステムにトランスポートセキュリティのモデルを適用し、サービスシステムを設計する必要がある。

5.4.3. レジストリデータのオブジェクトセキュリティ

レジストリシステムで保護すべきデータは、レジストリデータであり、オブジェクトセキュリティのモデルを適用すべきであることは既に述べた。そのデータはインターネットを使った転送および書き換えの際にも保護されていなければならない。ここでいう保護とは、メッセージの機密性と完全性である。

5.4.3.1. メッセージの機密性

レジストリデータには、whois システムを用いて公開されている情報の他にネットワーク利用組織の電話番号など公開されない情報が含まれている。そのため非公開の情報を、インターネットを使って転送したり書き換えたりする必要がある場合に、メッセージの機密性を保持する必要がある。

JPNIC の現行の IP レジストリシステムと管理業務では、レジストリデータの登録及び書き換えのメッセージは電子メールを使ってやりとりされる。このときにデータの機密性は維持されていない。ただし、現行の whois システムでは機密性を要するデータは特定のユーザにしか提供しておらず、提供時の機密性の保持に関する問題を回避している。

5.4.3.2. メッセージの内容証明

委譲された権限とネットワーク資源を示すレジストリデータの内容は、電子的手段を用いて正しさが証明されていなければならない。証明されていない場合、その権限とネットワーク資源の保有を主張する第三者に対して、その真偽を示すことができない。また、登録されたネットワーク利用組織同士がレジストリデータの内容を相互に確認できなければ、自律的な問題解決を行うことはできない。

従って whois システムを使って提供されるデータや、レジストリデータの新規登録及び変更の結果は、その内容が証明されていなければならない。またその内容の証明を、whois システムの利用者が検証できる環境が必要である。

証明書を用いて内容証明を行うには、その保証レベルを予め定義しておくべきである。保証レベルについては 4.5.2.1 節で述べた。

5.4.4. レジストリシステムにおけるトランスポートセキュリティ

レジストリデータの操作（新規作成及び変更、削除）におけるトランスポートセキュリティは、手続きを行うものの本人性と権限の確からしさ、セッションの一貫性の三つの要素によって成り立つ。この三つの要素は、セキュリティプロトコルを設計する際の留意事項のうち、トランスポートセキュリティのモデルに当てはまるものである。これらの要素が IP レジストリシステムにどう関係するかを表 20 に示す。

表 20　IP レジストリシステムにおけるセキュリティ要素

	主体 （本人性の条件）	権限 （権限の確認方法）	セッションの一貫性
アドレス ブロック	LIR	割り振りを受けたアドレスブロックの再割り当て	やり取り中の 電子メール送信者の同一性
	ネットワーク利用組織	割り当てを受けたアドレスブロックの利用	
AS 番号	個人情報が登録された 申請者	対向とpeerを確立する	やり取り中の 電子メール送信者の同一性
個人情報 （登録情報として）	個人情報の申請者	登録申請と 登録情報の変更	やり取り中の 電子メール送信者の同一性

5.4.4.1. 本人性

IP レジストリシステムの申請者による操作要求は電子メールを通じて送られる。申請者の判別は MAIL-FROM とよばれるメールフォーマット[29]のヘッダー”From:”行の文字列を利用する。しかしこの文字列は第三者によって書き換えることが容易であり、あたかも申請者自身から送信された電子メールであるかのようにメッセージを偽造することが可能である。S/MIME といったメッセージ保護の機能を利用すれば、電子メールを利用してもなりすましを防ぐ方法を実現できる。例えば保護範囲の中に本人を示す値を含めておくことによって第三者による偽造を検出し、要求の受け入れを拒否することができる。しかし現行の IP レジストリシステムと、これを使った現行の業務では S/MIME を利用することはできない。RIPE NCC などで利用されている PGP についても、現在は利用することができない。

5.4.4.2. 権限の確からしさ

権限の確からしさはアクセス制御とよばれる処理で確認される。アクセス制御は、検査対象にその権限があるかどうかを判断し、権限があればその行使を許可し、権限がなければアクセスを拒否する処理である。アクセス制御は、アクセス制御規則とよばれる規則に従って実施される。

IP レジストリシステムにおけるアクセス制御は、レジストリデータを書き換えられ

[29] RFC822, “Standard for The Format of ARPA Internet Text Messages”, http://www.ietf.org/rfc/rfc822.txt

るかどうかの判断に用いられる。アクセス制御には、表 21 に示すエンティティと権限の確認方法が適用される。

表 21　アクセス制御の為のエンティティと権限の確認方法

	情報を更新するエンティティ	権限の確認方法
ネットワーク情報	LIRとネットワーク利用組織 （運用責任者及び技術連絡担当者）	MAIL-FROMとLIR情報の比較
AS情報	自律システム （運用責任者及び技術連絡担当者）	MAIL-FROMとAS情報の比較
個人情報	登録者	MAIL-FROMと個人情報の比較
ホスト情報	ホストの管理者 （運用責任者及び技術連絡担当者）	MAIL-FROMとホスト情報の比較

なお、JPNIC におけるレジストリデータの為のアクセス制御は業務の中で実施され、レジストリシステムの処理には含まれていない。

現行のアクセス制御は、先に述べた本人性に基づいて行なわれている。すなわち MAIL-FROM を用いた方法で本人性を確認し、その権限を確認した上で書き換え許可の判断を行なっている。アクセス制御の処理は本人性に依存するため、例え権限の確からしさを業務手続の中で確認したとしてもそれが本来あるべき権限であったかどうかはわからない。

5.4.4.3. セッションの一貫性

セッションの一貫性とは、セッションとよばれる一つの目的を持った通信のまとまりにおいて、やりとりされるメッセージの目的が終始一貫しているという性質である。偽造したメッセージが挿入されたり、通信相手がすりかわったりすることで、メッセージの一貫性が損なわれる。whois システムにおけるにおけるメッセージの一貫性について図 37 に示す。

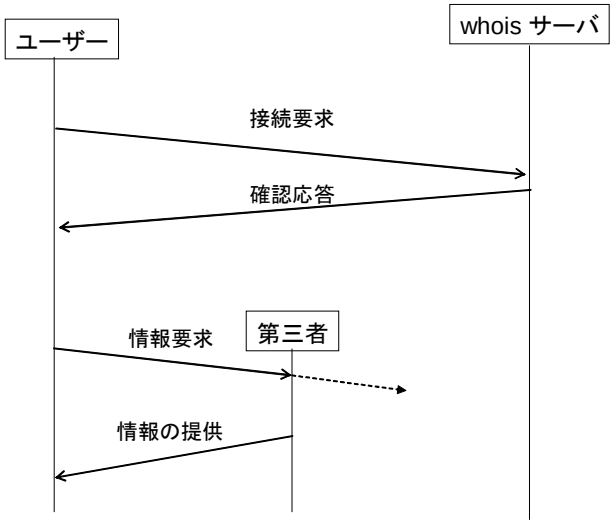


図 37　whois におけるセッションの一貫性

メッセージの一貫性は、予め定義され、保護されたセッション識別子を使用することで保持することができる。セッション識別子とは、セッションごとに別々の識別子を決め、その識別子を含まないあるメッセージがセッション中のものかどうかを確認するためのものである。セッション識別子が偽造されるとメッセージの一貫性が損なわれるため、偽造された場合に、通信相手がそれを検知できる仕組みが必要になる。

現行の IP レジストリシステムでは、ユーザと IP レジストリシステム及びオペレーターは、電子メールを使ってメッセージをやり取りしている。また電子メールの本文にセッション識別子は含まれていない。whois システムは TCP を使っているため、そのセッション管理機能を利用することができる。しかし TCP のセッション識別子は保護されておらず、通信経路上で書き換えることが可能である。TLS のセッション管理機能を用いると安全なセッション管理が実施できるが、whois のクライアントやサーバプログラムで TLS を利用している実装は、これまでには見つかっていない。

従ってレジストリデータは、登録及び変更のセッション中や提供セッション中に偽造することが可能である。どちらのセッションにおいても一貫性が保持される仕組みが必要である。

5.5. PKI を用いた認証機能

レジストリシステムの認証機能に、公開鍵暗号を使った強い認証機能を適用するには、

その認証機能をどの場面で利用するのかが検討課題になる。PKI を用いた認証機能は、この節では 5.4 節で述べた情報モデルとセキュリティモデルに基づき、レジストリシステムに適用するための、PKI を用いた認証機能について述べる。

5.5.1. レジストリデータのメッセージ認証

5.4.3 節で述べたように、レジストリデータは本来オブジェクトセキュリティのモデルを適用すべきである。このモデルの適用し、情報の完全性を検証する環境を実現することで、whois のユーザはレジストリデータの完全性を確認することができる。また転送プロトコルに依存せずに、様々なネットワークサービスで情報提供及び入手を行うことが可能になる。

レジストリデータの完全性は、メッセージ認証機能の付加によって実現することができる。メッセージ認証機能には、データエントリーへの電子署名と、その電子署名を検証する環境の二つが必要になる。

データエントリーへの電子署名は、IP レジストリシステムの処理の中で行われる。電子署名が行なわれたデータエントリーは既存のデータエントリーの扱いと同様にデータベースに格納されることで既存の whois システムを使った情報公開を継続することができる。この構成にすることで、ユーザはこれまで通り Web ブラウザを用いて閲覧することができる（図 38）。

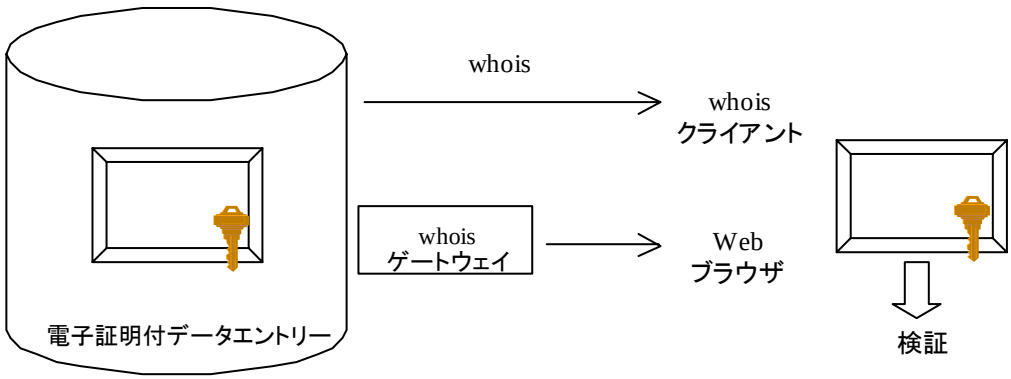


図 38　レジストリデータのメッセージ認証

しかし既存の Web ブラウザや whois クライアントには、電子署名が付加されたデータエントリーの正当性を確認することはできない。これはこれらのクライアントプログ

ラムには、テキスト文字列に対する電子署名の検証機能が実装されていないためである。

メッセージ認証機能をレジストリシステムに適用するには、電子署名が付加されたデータエントリーの転送と、テキストデータへの電子署名を検証できるユーザの環境が必要になる。電子署名はオブジェクトセキュリティのモデルを適用したシステムであり、転送プロトコルを選択する必要はない。しかしユーザの利便性を考慮すると、電子署名が施されたデータオブジェクトを受信し、証明書を用いて検証することができるプログラムが必要となる。この環境を実現するには、既存のクライアントプログラムに変更を行うか、新たなクライアントプログラムの開発が必要となる。

5.5.1.1. メッセージ認証のメッセージフォーマット

多くの RIR では、レジストリデータ（whois データ）の表現言語に RPSL を利用している。RPSL には RPSS（Routing Policy System Security[30]）とよばれる認証と認可を実現するための仕組みがある。しかし RPSL には暗号技術を利用したデータ完全性の保護機能がない。従ってそのままでは分散環境におけるデータの保護と検証のために利用することはできない。今後、RPSL に電子署名の機能を付加するか、構造化された言語にデータを変換して提供する手法が開発される可能性がある。

PKI を利用した、メッセージ認証を実現する既存のメッセージフォーマットには S/MIME や PKCS#7 が存在する。S/MIME は IETF smime WG で提案されたメッセージフォーマットで、任意のデータに電子署名や暗号化を施すことができる。PKCS#7 は S/MIME バージョン 3 より早い 1993 年に RSA Data Security 社によって提案されたメッセージフォーマットで、内容は S/MIME のエンベロープ（電子封筒）とほぼ同じである。

S/MIME や PKCS#7 を用いる場合、任意のデータに対するエンベロープ（電子封筒）を適用することになり、各々のデータの構造が無視される。whois システムでは、しばしば連鎖した検索のようなデータの構造を利用した処理を行うため、構造化されていないデータの扱いは適さない。レジストリデータの構造に対するエンベロープの適用方法について、新たなプロトコルを策定するか、代替手段を用いたメッセージ認証機能を実現する必要がある。

[30] RFC2725, “Routing Policy System Security”, http://www.ietf.org/rfc/rfc2725.txt

5.5.1.2. 実装の際の留意事項

IETF の provreg ワーキンググループでは、whois に代わるプロトコル epp（extensible provisioning protocol）の策定が行われている。レジストリシステムの情報公開機能とユーザ環境の実装の際には、このような新しいプロトコルへの対応等に留意する必要がある。また W3C（World Wide Web Consortium）では XML Signature とよばれる、構造化された拡張可能言語 XML に電子署名を付加するプロトコルが提案されている。今後、構造化されたテキスト表現に対する電子署名を実現するプロトコルが利用される可能性がある。

5.5.2. レジストリシステムにおける認証システム

第三章で述べたように、他のインターネットレジストリでは Web インターフェースによるレジストリデータの書き換え等のサービスが提供されている。APNIC の MyAPNIC のように、クライアントに対しても強い認証が実施され始めている。NIR は LIR によって登録されている情報を公開するため、LIR による情報登録や更新といった機能を実現する必要がある。

5.5.2.1. 相互認証

ユーザにレジストリデータの登録や更新のサービスを提供する場合、ユーザのなりましやサーバのなりすまし、通信経路でのデータの改ざんや破棄といった脅威が存在する。これを防ぐには、暗号技術を利用したセキュリティプロトコルを利用する必要がある。

ユーザ及びサーバのなりすましを防ぐには、相互認証を行うことができるプロトコルを利用する必要がある。相互認証とは、ユーザがサーバを認証すると同時にサーバがユーザを認証する仕組みである。PKI を用いて相互認証を実現するには、予め信頼する認証局の証明書を入手しておき、認証対象が提示した証明書を検証する必要がある。

サーバがユーザを認証するには、サーバ（サーバ管理者）が信頼する認証局が、ユーザの証明書を発行しておく必要がある。またユーザは、その証明書をクライアントソフトウェアに組み込んでおき、サーバにアクセスした際にそれを利用できなければならない。

サーバによるユーザ認証を実施するには、LIR の登録情報を更新する必要があるユーザが、証明書を利用できる環境が必要である。また鍵ペアと証明書の扱いに関して第４章 4.4.6 節の事項、すなわち鍵の安全性と用途に関して留意する必要がある。

ユーザがサーバを認証するには、ユーザが信頼する認証局がサーバの証明書を発行している必要がある。そのためには少なくともレジストリデータを編集する必要があるユーザの全員が信頼する認証局が存在し、その証明書がユーザの環境になければならない。

5.5.2.2. ユーザーインターフェースとプロトコル

インターネットを通じてレジストリデータの登録や更新の機能を実現するには、5.4.1 節で述べたトランスポートセキュリティのモデルを適用するか、ユーザの申請内容をオブジェクトセキュリティのモデルで保護するという、二つの方法が考えられる。APNIC の MyAPNIC や RIPE NCC の LIR Portal といった Web インターフェースを使った登録や更新の機能が実装されている状況は、LIR による手続きの簡便化の要求が存在することを意味している。これは、ユーザの申請内容を保護する方法は、そのデータ（電子メール）のやり取りに時間がかかり、また申請書類の書式に間違いがある場合などに再送の必要があるなど、やりとりに必要となるオーバーヘッドが大きい。一方、Web インターフェースでは書式に間違いがある場合に、すぐにエラーをユーザに知らせることができ、また再申請の際に一度入力された情報を入力フォームに表示しておくことで、ユーザに再入力を要求する必要がない。

HTTP を使ったシステムを構築する場合、トランスポートセキュリティのモデルを適用した https か、HTTP にて転送される MIME オブジェクトにオブジェクトセキュリティのモデルを適用したプロトコルを利用する方法が挙げられる。しかし後者の形式のプロトコルは未だ実装されておらず、S/MIME オブジェクトを HTTP で転送するといった手法は一般的ではない。前者の https を使う方法は、多くの Web ブラウザに PKI を利用する機能が実装されていることから、より実用的である。

https の利用の際には、5.4.4.3 節で述べた一貫性の保証が重要課題となる。これは一つの目的に対して複数の TCP コネクション及び TLS コネクションを利用する必要があるためである。この問題に対して、多くの Web ページでは cookie を用いてアプリケーションのためのセッション管理機能を実現している。しかしユーザ環境に保存された cookie のデータの扱いを誤ると、NIR が管理していない Web サーバにそのデータが転送される可能性がある。この問題は CSS（Cross-Site Scripting）問題の一つである。セッションの管理機能については、慎重に設計される必要がある。

またユーザ環境に組み込まれている認証局の証明書が、NIR の認証局だけであることは想定しにくい。このことは多くの認証局ベンダが発行している証明書が、ユーザ環境では有効であると表示される状況を作り出す。従ってある NIR と同名のサーバ証明書が、いずれかの認証局によって発行された場合、ユーザはその証明書を提示したサー

バを誤って認証してしまう。ユーザの証明書に対する誤認を防ぐ仕組みが必要である。

5.5.3. 分散環境でレジストリデータを検証する環境

インターネットレジストリにおける登録を、分散環境（インターネットのようなネットワーク環境）で検証する環境について述べる。

5.5.3.1. インターネットレジストリの証明書

1 章で述べたように、CIDR ブロックの割り振りは ICANN、RIR、NIR、LIR のどのレベルでも行われる。あるネットワーク資源の割り振りを示す証明書を検証しようとした場合、その証明書を発行した認証局の証明書が正当であり有効であることを確認できなければならない。インターネットレジストリ全体のネットワーク資源の管理構造に PKI を利用する場合、いずれのインターネットレジストリの認証局が発行した証明書であっても、ある信頼点に基づいて検証できなければならない。すなわち信頼のチェインがインターネットレジストリの認証局の間で一貫性を持っている必要がある。

この報告書では NIR における認証局のあり方について注目しているが、インターネットにおけるネットワーク資源の確認方法に PKI を利用する場面を考えると、他のインターネットレジストリにおける認証局との連携の仕方について検討する必要がある。他の認証局との連携の際には、第 4 章で述べた保証レベルを検討しなおすなど新たな課題がある。

5.5.3.2. 検証環境における証明書

whois システムのユーザが、レジストリデータの証明内容を電子的に検証するには、ユーザ環境に、電子署名を検証するための証明書が必要となる。第２章で述べたように NIR の提供するレジストリデータの内容は、NIR によって証明される。従って NIR の認証局の証明書がユーザ環境に組み込まれている必要がある。またユーザの信頼する認証局の証明書を使って、NIR の認証局が発行した証明書の正当性を確認できる状況が必要である。そのためには、NIR の認証局の証明書を予め whois のユーザに配布しておくか、ユーザが信頼している認証局によって NIR の認証局の証明書を発行しておくという二つの方法が考えられる。

第１章で述べた NIR の権限の構造を、証明書のツリー構造になぞらえると、ICANN によってルート認証局が運用され、RIR に証明書を発行する構造が考えられる。この場合、RIR は更に NIR に証明書を発行することになる。しかし第３章で述べた調査結果から、インターネットレジストリ間で証明書を発行している例はない。また JPNIC は

IP アドレスの割り振り対象を確認する際に、APNIC の審査基準を用いるだけでなく、日本国における存在証明を利用している。この方法はインターネットレジストリに共通したものではなく、JPNIC のポリシーによるものである。従って JPNIC が、あるエンティティに発行した証明書は、JPNIC の認証局を信頼していなければ正しさを検証することができない。これはユーザにとって JPNIC の認証局が信頼点である必要がある。

5.6. 認証機能を持つレジストリシステム

PKI を用いた認証機能をレジストリシステムに組み込むと、メッセージ認証、ユーザ認証を行った上でのレジストリデータの書き換えなどが実施できるようになる。本節では、前節の認証機能をレジストリシステムに組み込んだ場合のシステムの概要を示す。

5.6.1. whois におけるクライアント認証とメッセージ認証

PKI と whois を組み合わせた使ったユーザ認証に基づくレジストリデータの変更とメッセージ認証の概念図を図 39 に示す。

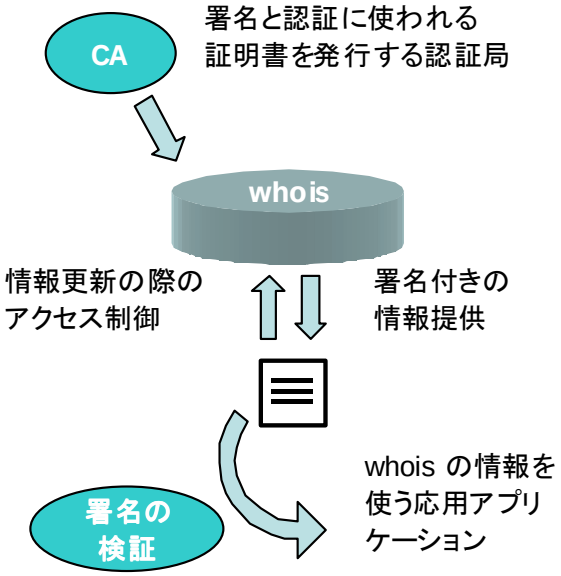


図 39　whois における認証

中央の白い四角が登録情報で、この情報が whois に登録される際に認証とアクセス制御が行われる。また whois は登録された情報の出所を確認できる手段をもって提供し、ユーザは登録情報が確かに JPNIC の whois によって提供されていることを確認することができる。この方法には、オブジェクトセキュリティのモデルを適用し、レジス

トリデータに電子署名を付加する方法と、トランスポートセキュリティのモデルを適用し、ユーザがサーバ認証を行った上で、情報を確認する方法の二つが考えられる。図 39 では前者の電子署名を示している。5.5.1.2 節で述べたように、情報の提供方法を実装する際に、利用する転送プロトコルと表現プロトコルを検討する必要がある。https クライアントとなる様々な Web ブラウザが実装されている状況を考えると、はじめに https を利用した相互認証を段階的に実現し、同時にメッセージ認証を行う環境を整えておくといった手順が考えられる。

whois を利用して、レジストリデータ書き換えの為のクライアント（ユーザ）認証と whois で公開される情報のメッセージ認証機能を提供する仕組みの構成図を図 40 に示す。

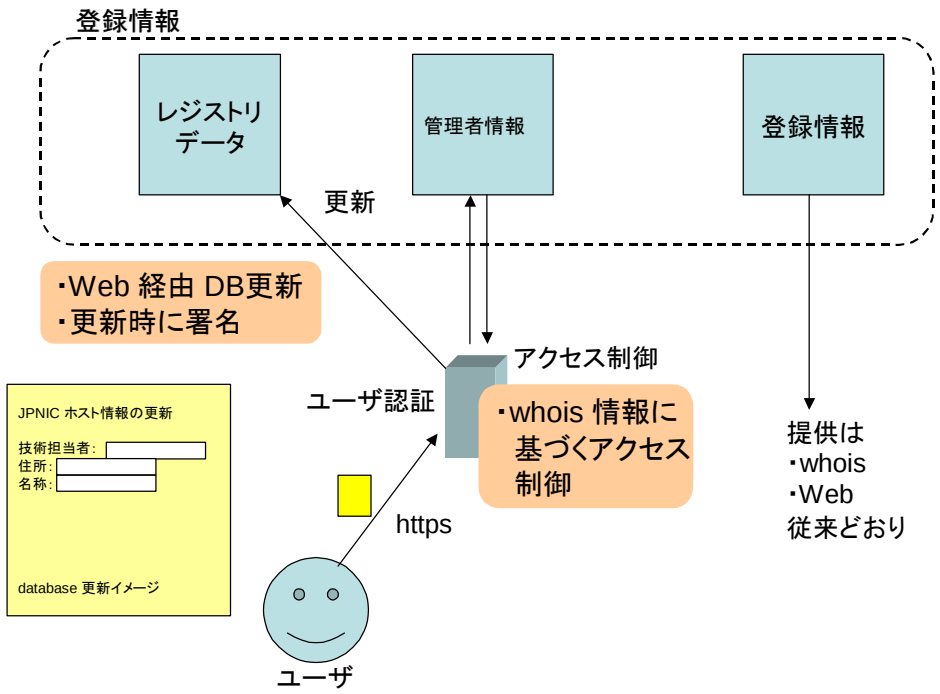


図 40 whois におけるユーザ認証とメッセージ認証

レジストリデータを書き換えようとするユーザは、ユーザ認証を受け、更に書き換える情報に対応してアクセス制御が行われる。特定のレジストリデータの書き換え権限が認められたユーザは、書き換えを実施し、レジストリデータを更新する。なおこの動作はユーザの操作だけで完結するものと、オペレーターの承認といった操作を要するものが存在する。またユーザ認証に https のクライアント認証のみを使うだけでなく、

S/MIME などオブジェクトセキュリティのモデルを適用した方法も考えられる。その場合には、ユーザが記述する申請形式の差異を吸収する仕組みが必要と考えられる。

登録されたレジストリデータは従来と同じ方法すなわち whois および Web を使って公開される。この提供方法を変更しないとすると、クライアントソフトウェアの変更は必要ない。ただし、メッセージ認証機能を実現するには、クライアントソフトウェアの検証機能の開発が必要になる。

また ARIN で利用されている RWhois のように、一元化された whois のインターフェースに対応するためには、登録情報の提供機能に付加的なソフトウェアの開発が必要となる。

5.7. レジストリデータベースの応用

5.5 節で述べた、レジストリデータのメッセージ認証機能を実現すると、ネットワーク資源の割り振り／割り当ての情報の正当性を示すことができる。この機能は、同時に登録されたネットワーク利用組織と特定の識別子（IP アドレス）の関係を結びつける根拠となる。この性質を応用すると、様々なネットワーク資源に関する証明を行うことができる。本節では、内容が証明されたレジストリデータベースの応用について述べ、更に応用例を紹介する。

5.7.1. IP アドレスに基づく実在性の証明

NIR によるネットワーク資源の割り振り／割り当てといった情報の登録は、登録されたネットワーク利用組織に対する権限の委譲を示すものが存在する。第１章で述べたようにアサインメントウィンドウ等がその例である。一方この情報は、あるアサインメントウィンドウが実際にどの組織に割り振られているのかを示す情報でもある。つまり特定の IP アドレスの範囲に対して、そこに含まれる IP アドレスを割り当てる権限を持つ組織が存在するのか、またあるとするとその組織はどのような組織であるのか、という情報を示す。JPNIC によるアサインメントウィンドウの割り振り対象は、登記簿謄本等書類の検査に基づいて実在性が確認されている。従って IP アドレスを元にして、その IP アドレスを利用する組織や、割り振る権限を持つ組織を特定することができる。

ネットワーク利用組織が利用することができるネットワーク資源には、IP アドレスの他に AS 番号、ホスト（登録されたもの）、ドメイン名といったものがある。これらの登録情報についても、アサインメントウィンドウの情報と同様に関連する組織の情報を確認することができれば、ネットワーク資源に関するレジストリデータを利用した確

実なネットワークを構築することができる。例えば、IP アドレスの割り当てが証明されている組織とのみ経路交換の peer を確立する経路交換や VPN の構築などが挙げられる。更に、レジストリデータを認証基盤として応用し開発を進めると、公衆交換電話網のゲートウェイを認証した上で接続する安全な IP 電話、予め登録されたメーカーに作られたインターネット家電の認証等、様々な分野への適用が考えられる。また登録情報の重要性を民間組織であるかネットワーク管理組織かといったレベル分けをすることで、利便性と運用の安全性のバランスを取り、分野に応じた安全な認証基盤の構築を視野に入れることができる。

5.7.2. 応用例

本節では、内容が証明されるレジストリデータを応用し、各分野で開発を進めることで考えられる応用の可能性を示す。これらの応用例は、本調査報告書で示す認証局が実現した上に、各種サービスのための開発が進んだ際に実現する可能性があるもので、必ずしも NIR における認証局がこれらを目標として運用されるわけではない。

5.7.2.1. ゲートウェイの証明書

インターネットに接続したネットワーク組織では、インターネットを通じて接続を受け付けるためゲートウェイを構築することがある。ユーザは重要なサービスを利用するためにゲートウェイを利用する際には、そのゲートウェイを認証し、接続を試みる。

既存の多くのゲートウェイの認証対象はアプリケーションゲートウェイであり、正当性が確認されるべき主体はサービス提供者であった。しかし、IPsec を使った通信サービスの提供や IP 電話で利用される公衆交換網ゲートウェイなど、認証対象の主体がネットワーク資源を持つ主体と同一である、もしくはネットワーク資源の利用権限をもつ主体である考えられる状況が存在する。ネットワークサービスを提供する主体が、然るべきネットワーク資源を持つことをユーザが確認できれば、ゲートウェイに対して、より確実な認証を行うことができる（図 41）。

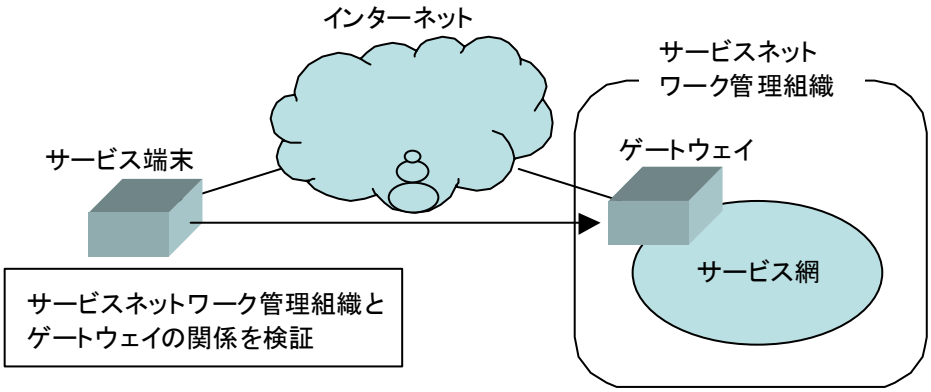


図 41　ゲートウェイの認証

5.7.2.2. 認証局の証明書

インターネットを利用する通信サービスで PKI を利用していると、新たな認証局をトラストポイント（信頼点）に加える場面が存在する。また認証局が発行する失効情報をいち早く入手しなければならない場面がある。

原理的な PKI の利用方法に従うと、認証局の信憑性を確認する手段として、インターネットを利用しない方法が順当である。しかしオフラインの方法では情報が古かったり入手方法自体が不明であったりする。これまでは、ユーザのトラストポイントの扱いについては基本操作に留めておき、トラストポイントの追加の方法を実現したソフトウェアはほとんど見られなかった。そのためユーザはデフォルトで組み込まれている認証局をトラストポイントに設定せざるを得ず、認証のたびに証明書ツリーを確認しない限り、認証対象の妥当性や認証局の保証内容などを無視して PKI を利用することになる。

ある証明書の正当性を確認する手段には、証明書ツリーを利用して検証する方法の他に、トラストポイントの追加手順を利用する方法がある。すなわち信頼する認証局の情報を入手し、その認証局が発行している証明書の fingerprint などの情報と、別の方法で入手した証明書が同一であるかどうかを確認する方法である。

レジストリシステムの情報公開機能で認証局の fingerprint を扱うことができれば、上で述べた「別の方法」の一つを提供できる可能性があると考えられる。または証明書リポジトリとして機能し、ネットワーク利用組織と認証局の相互の利用を促進する役割が考えられる。

5.7.2.3. ネットワーク利用組織をまたぐ認証

PKI を使った証明書の検証環境には、証明書のトポロジーに従った認証の範囲が存在する。この範囲は PKI ドメインと呼ばれる。異なる PKI ドメインと相互に認証を行うためには、相互認証証明書を発行することで証明書のトポロジーを確証するか、トラストポイントを追加する必要がある。

相互認証証明書の発行先の信頼性や、新たなトラストポイントの信頼性を確認する際に、証明書に関する情報を含むレジストリデータを利用することで、信頼のレベルを測ることができる可能性がある。NIR は組織の実在性の確認とネットワーク資源に関する審議を行っているため、特定のネットワーク資源と、特定の認証局の組み合わせが申請された通りであることを証明することができる。ユーザはその組み合わせの証明に基づき、異なるネットワークに属するエンティティの認証に応用することが考えられる。

5.8. まとめ

本章では、NIR における認証局を構築する際に、ネットワーク資源を管理するレジストリステムに、どのような認証システムを適用することができるかについて述べた。その際に、IP レジストリシステムの情報モデルとセキュリティモデルを元に、モデルとしてのセキュリティ要件について述べた。

レジストリシステムにおける認証システムは、データベースの保護の為のユーザ認証と、データエントリーの内容を証明するためのメッセージ認証の機能を持つ必要がある。これらの機能を実現するために、ユーザ環境と規模拡張性を考慮して PKI を適用する場合の、ユーザ環境や認証システムの要件について述べた。

またネットワーク資源の割り当てや割り振りといった内容が証明される機能を、認証基盤として応用することについて述べた。更にその応用例を紹介した。

第6章 まとめ

内容

- 本報告書のまとめ
  - NIR における認証局の運用
  - 他のインターネットレジストリの活動
  - NIR の役割とセキュリティ要件
  - レジストリシステムと whois システムのセキュリティ
  - 登録情報の認証基盤の応用
  - インターネットレジストリの今後

6. まとめ

IP アドレスはインターネットにおけるネットワーク資源の一つである。インターネットの運用と、インターネットを利用した通信の信頼性の向上には、ネットワーク資源の確実な管理が必要である。この調査研究では、日本のネットワーク資源を管理する役割を担っている NIR（National Internet Registry – 国別インターネットレジストリ）における認証局のあり方に関して調査を行った。

6.1. NIR における認証局の運用

NIR は階層構造の組織関係を持つインターネットレジストリの中で、一つの国内の組織を対象としたネットワーク資源の管理を行う組織である。ネットワーク資源の管理は、経路情報の集約やアドレス資源の節約、予め登録された ISP（Internet Service Provider）へのアドレスブロックの割り振りなど、インターネットの運用上重要な役割を果たしている。アドレスブロックや AS 番号といったネットワーク資源の不正利用は、インターネットを使った大規模な不正行為を追跡不能にするなど影響が大きい。従って NIR の業務は、安全で確実に行われなければならない。

NIR における登録と割り振りの情報は、レジストリシステムとよばれるシステムで管理されている。レジストリシステムに登録された情報の一部は、ネットワーク利用組織同士が自律的な問題解決を行うことを可能にするために公開されている。従って NIR における資源管理の確実性を向上させるためには、レジストリシステムにおける登録情報の保護が必要となる。ネットワーク資源の管理権限を委譲していくインターネットレジストリの階層構造は、信頼できる第三者を見立てる認証方式を適用しやすい。そこで PKI を利用した認証システムをレジストリシステムに適用することが考えられる。

6.2. 他のインターネットレジストリの活動

APNIC や RIPE NCC といった他のインターネットレジストリでは、既にレジストリデータを保護する活動に取り組んでいる。APNIC や RIPE NCC では、登録情報の中に認証に関する情報を含め、書き換えを行うユーザの認証方法が明示されている。この一連の認証方式の中には、PKI を利用した方法は含まれていないものの、公開鍵暗号を利用した強い認証を使っているものが含まれている。更に、APNIC では CA Pilot Project の一環として認証局を構築し、X.509 形式の公開鍵証明書の利用を開始している。また RIPE NCC では、商用認証局ベンダーの証明書を使用した TLS を活用しており、PKI を利用した強い認証と利便性の両立を図っている。

6.3. NIR の役割とセキュリティ要件

NIR は国別のインターネットレジストリであり、ネットワーク資源の割り当て先に関する分類を持たない。つまり NIR が割り振ったネットワーク資源はインターネットに接続する政府、民間組織、任意団体などの様々な組織で使われる。そのため、NIR の運用はネットワーク資源の効率的な利用に貢献するだけでなく、信頼性の高い業務が行われる必要がある。特に NIR における認証業務は、各種セキュリティ要件を考慮した上に行われなければならない。

PKI を利用する認証業務は、認証局の運用を中心として行われる。本調査研究では認証局と認証業務の運用に関する、国内外の認定基準やガイドラインを調査した。具体的には、電子商取引実証推進協議会の認証局運用ガイドライン、電子署名法と施行規則および業務調査表、AICPA/CICA の WebTrust for CA の 3 基準を比較し、考察を行った。この調査を通じて、本人認証や設備、証明書の管理等、確実な認証業務の運用要件として検討されるべき項目が明確になった。また各項目についての考察を通じて、セキュリティ要件を定める為のいくつかの指針が得られた。またこの調査結果は、一般的な認証局の構築の際に参照できる詳細な基本資料になると考えられる。

6.4. レジストリシステムと whois システムのセキュリティ

インターネットレジストリにおいてネットワーク資源の管理に使われるレジストリシステムは、ユーザによる情報更新や、登録情報の一部を公開する機能を提供している。ネットワーク資源管理の確実性を向上するには、管理業務とこれらの情報サービスを提供するシステムに保護機能が必要である。

レジストリシステムに格納される情報は、データエントリー毎に、そのエントリーを書き換えることができる対象が決まっている。この条件をアクセス制御規則として定義し、強い認証が行われた上でアクセス制御の処理が実施されることで、登録情報の確実性が向上する。また whois システムが提供する情報の正当性をユーザが検証できるようにすることで、ネットワーク利用組織間の自律的な問題解決の際に、なりすましなどの安全性の問題に対策を取ることができる。

レジストリシステムと whois システムのセキュリティを、セキュリティモデルと情報モデルに基づいて検討した結果、登録情報は、本来オブジェクトセキュリティのモデルで保護機能を設計すべきであることがわかる。ただし、ユーザの利便性や PKI を利用することができるソフトウェアの実装状況を考えると、通信中のデータを保護するトランスポートセキュリティのモデルを適用する場合が考えられる。ユーザ向けのサービ

スの違いと、whois システムに適用できるプロトコル策定状況を鑑みて、今後更に検討が行われ、そして設計が行われる必要がある。

6.5. 登録情報の認証基盤の応用

ネットワーク資源の利用が確実な登録情報に基づいて行われると、その情報を用いた各種ネットワークプロトコルの、より安全な利用方法が考えられる。例えば、ある組織と、その組織がネットワークサービスの一環として提供しているゲートウェイの IP アドレスの組み合わせが正しいことを確認できる機能が考えられる。IP アドレスはインターネットの運用に直接的に関係する識別子であるため、インターネットレジストリにおける確実な管理と組み合わせることで、ネットワーク利用組織の実在性、サービスを提供するホストの IP アドレスについて、その組織の所属性を確認できる認証基盤ができる可能性がある。また識別子の組織の所属性を登録情報で証明することで、認証局の為の証明書リポジトリや証明書の確認手段を提供することも考えられる。

6.6. インターネットレジストリの今後

この調査研究を通じて、インターネットレジストリの役割が、インターネットの運用だけでなく、その安全性にも影響することが明らかになった。今後、ネットワーク資源管理の確実性が向上することで、今後インターネットの利用法の中に確実なやり取りを必要とする、クリティカルなサービスが含まれていくと考えられる。インターネットレジストリは、運用の保全と共に、ユーザ環境における利便性と安全性に関する知識を蓄積していくことが必要になると考えられる。

第 6 章　まとめ

添付資料

基準比較表

<基準比較表について>

- この資料は、認証業務の基準／ガイドラインについて、具体的に比較した項目を表にまとめたものである。比較の概要と考察については第 4 章にて述べた。
  - ガイドラインについては認証局の運用、環境等における高レベルの要件を含めて記述している。
  - 署名法については、電子署名及び認証業務に関する施行規則及び指定調査機関による特定認証業務調査表 V2.0 の適合例にて記述している。なお、4 桁の数字が付されているものは調査表の適合例の番号である。
  - WebTrust for CA は、3 セクションに分かれている。
    - セクション 1：CP/CPS 等への認証ビジネスにおける開示必要項目、及び例示
    - セクション 2：認証局の完全性を維持するためのコントロール
    - セクション 3：認証局の環境的なコントロール
  - セクション 1 は CP/CPS に記述すべき項目の記述であり、認証局構築にあたっての基準と言う観点では記述されていないので、基本的には比較対象項目からははずしている。ただし、一部、署名法、ガイドラインの記述に対応して必要と思われるものは記述している。
  - 基準比較表において、ガイドライン、署名法の用語は、原文のままを使用している。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
	1. はじめに			
1	1.1. 概要 仕様化についての一般的な紹介。 · 規程の適用範囲 · 依拠する文書 · 参照する文書			
2	1.2. 識別 規定集のオブジェクト識別子を含む、すべての適用可能な名前、若しくは他の識別子等			1.1.1 識別 認証局が証明書を発行するCPとCPSの識別。
3	1.3. コミュニティと適応性 証明書が流通するコミュニティと適用範囲 1.3.1. 認証局 (Certification Authority) 1.3.2. 登録局 (Registration Authority) 1.3.3. エンドエンティティ (End Entity) 1.3.4. 適用範囲 適合するアプリケーション、制限されるアプリケーション､使用禁止されるアプリケーションの記述も含む		(指針第１２条第１項第二号) 証明の目的、対象又は利用範囲について制限を設ける場合においては、その制限に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3903 (3) 証明の目的、対象及び制限に関する事項 ① 認証業務によって電子証明書を発行する相手 ② 認証業務で発行する電子証明書が使用できる目的、使用に当たっての制限及びそれらの関連事項等 ③ 電子証明書に記載されている利用者の属性の確認方法は認定の対象外であること	1.1.2 コミュニティと適用性 PKIにおけるエンティティのタイプと証明書の適用可能性についての記述。
4	1.4. 連絡先の詳細 認証ポリシ、若しくはCPSの登録、維持管理、解釈に責任を負う者への連絡先 ・組織の名前 ・住所 ・連絡先の担当者の名前 ・電子メールアドレス ・電話番号 ・FAX 番号		(指針第１２条第１項第一号) 認証事業者の名称及び連絡先（住所、電話番号、ファクシミリ番号及びメールアドレス） 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3902 (2) 認証事業者の名称及び連絡先（住所、電話番号、ファクシミリ番号、電子メールアドレス）等 ① 認証事業者の名称及び住所（郵便番号、都道府県名、ビル名、階等を含む） ② 連絡担当窓口の名称 ③ 電話番号（事業者番号、市外局番号を含む）及び受付時間 ④ファクシミリ番号（事業者番号、市外局番号を含む） ⑤ 電子メールアドレス	1.1.3 連絡先と管理組織 管理組織名、責任者、住所、TEL、FAX、メールアドレス。CP/CPSのバージョン、有効日付。
5	1.5. 用語集			

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
	2. 一般条項			
6	2.1. 義務 各主体において、その主体の他の主体に対する義務に関する、すべての適用可能な規制。 2.1.1. 認証局の義務 2.1.2. 登録局の義務 ・ 発行された証明書のサブジェクト（対象）である登録者への証明書の発行、失効、停止の通知 ・ 証明書のサブジェクト以外への証明書の発行、失効、停止の通知	2.1 義務 2.1.1 認証局の義務 （１） 認証局自身の信頼性と安全性の確保 本ガイドラインで述べられるマネージメント要件、運用要件、システム・設備要件に適うポリシーを明確化し、それを実行するために必要な具体的手順・手続きを定めて、適切な運用を継続する義務がある。 （２） 登録局やレポジトリの信頼性と安全性の確保 認証局が外部の登録局やレポジトリ等と連携する場合には、認証局はそれらの外部機関に認証局の定めたポリシーを遵守させ、信頼性と安全性の一貫性を保持する義務がある。 （３） 加入者及び信頼者に対する適切な情報提供 認証局は、次に述べるような加入者及び信頼者の義務について周知させる義務がある。また、その履行に必要な各種情報を適切なタイミングで提供する義務もある。	(第６条第一号) 利用申込者に対し、書類の交付その他の適切な方法により、電子署名の実施の方法及び認証業務の利用に関する重要な事項について説明を行うこと。 (指針第８条）： 規則第六条第一号に規定する利用申込者に対して説明を行うべき事項とは、次の各号に掲げる事項を内容として含むものとする。 (指針第８条第一号) 認定認証業務においては、虚偽の利用の申込みをして、利用者について不実の証明をさせた者は、法第四十一条の規定により罰せられること。 (指針第８条第二号) 電子署名は自署や押印に相当する法的効果が認められ得るものであるため、利用者署名符号については、十分な注意をもって管理する必要があること。 (指針第８条第三号) 利用者署名符号が危殆化（盗難、漏えい等により他人によって使用され得る状態になることをいう。以下同じ。）し、又は危殆化したおそれがある場合、電子証明書に記録されている事項に変更が生じた場合又は電子証明書の利用を中止する場合においては、遅滞なく電子証明書の失効の請求を行わなければならないこと。 (指針第８条第四号) 認定認証業務に係る電子証明書を使用する場合における電子署名のためのアルゴリズムは、認証事業者が指定したものを使用する必要があること。 3113 (3) 利用者への説明は以下のいずれかの方法により行われている。 ① 書類の交付(郵送、手交、電子メール) ② 対面による説明 ③ その他①、②と同等な方法 (規則第６条第八号) 電子証明書に利用者の役職名その他の利用者の属性（利用者の氏名、住所及び生年月日を除く。）を記録する場合においては、利用者その他の者が当該属性についての証明を認定認証業務に係るものであると誤認することを防止するための適切な措置を講じていること。 3601 (1) 電子証明書に利用者の肩書き等の属性を記録する場合は、以下を明確に認証業務規程及び事務取扱要領に規定している。 3602 (2) 属性についての証明は本認定制度における認定の対象外である旨の注記もしくはその情報へのリンク先の表示を電子証明書に行っている。	1.1.11 認証局と登録局の義務 ・発行される証明書の対象である申請者に対する証明書発行の通知 ・証明書の対象以外の者への証明書発行の通知 ・証明書の失効及び停止している利用者への証明書失効や停止の通知 ・証明書の対象以外の者への証明書失効や停止の通知 1.1.12 登録局の義務 ・申請者からの情報の真正性の検証 ・証明書失効要求の真正性を検証 ・証明書更新や鍵更新時の利用者から送信された情報の真正性の検証 2.2.3.13 認証局又は登録局は、証明書の有効期限が切れる前に利用者に通知する。 3.6.1 認証局運用の手続は文書化され、維持管理される。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
7	2.1.3.　利用者の義務 ・証明書アプリケーションにおける表現の正確性 ・主体の私有鍵の防護 ・私有鍵と証明書使用についての制限 ・私有鍵改ざんについての通知	2.1.2 証明書加入者の義務 （１）　正確な情報の提示 加入者は、認証申請などに際して、正確な情報を認証局に提示する義務がある。 （２）　証明書発行の確認 加入者は、認証局による証明書発行に際して、証明書の記載情報を確認する義務がある。 （３）　私有鍵の保護 加入者は、公開鍵／私有鍵ペアの生成において、信頼できるソフトウェアやハードウェア等を利用して安全な方法で生成するとともに、私有鍵は他人に知られないように管理する義務がある。 （４）　迅速な失効手続き 加入者は、私有鍵が危瀕した場合や証明書記載の情報に変更が生じた場合等、迅速に失効手続きを行う義務がある。	(指針第８条) 規則第六条第一号に規定する利用申込者に対して説明を行うべき事項とは、次の各号に掲げる事項を内容として含むものとする。 3111 (1) 以下の(2)の事項を満足する規定が、認証業務規程及び事務取扱要領等に明確に規定され、実施されている。 3112 (2) 以下の各項目について、利用者に理解しやすく、かつ具体的に記述され利用者に説明されている。 ① 当該業務は、主務大臣から認定されたものであり、虚偽の申込みをして、不実の証明をさせた場合には、罰せられること。 ② 電子署名は、自署や押印に相当する法的効果が認められ得るものであり、充分な注意をもって利用者署名符号の管理を行い、秘匿性を維持すること。 ③ 利用者署名符号が危殆化（盗難、漏えい等によりその機密性を失うこと。以下同じ。）した場合、若しくは危殆化したおそれがある場合、電子証明書の記載内容に変更が生じた場合及び電子証明書の利用を中止する場合においては、遅滞なく証明の失効請求を行うこと。 ④ 当該電子証明書に係る電子署名アルゴリズムは、当該認証事業者が指定するものを用いること。	1.1.14 利用者の義務 ・身元確認情報その他の利用者情報に変更があった場合の迅速な連絡 ・私有鍵の保護 ・ポリシやCPSに従った適切な証明書の利用 ・利用者の私有鍵が危殆化した場合の迅速な連絡
8	2.1.4.　検証者の義務 · 証明書が使用される目的確認 · デジタル署名検証の義務 · 失効と停止をチェックする義務 · 適用可能な依存可能性の限度と権利の承諾	2.1.3 証明書信頼者の義務 （１）　証明書の適格性のチェック 信頼者は、受け取った証明書が目的に適したものであるかどうかを判断する義務がある。例えば、取引の金額的な限度は、認証の真正性保証レベルや補償レベル等に応じて決める義務がある。 （２）　証明書の確認 受け取った証明書の有効期限、利用目的、署名の正当性を確認する義務がある。 （３）　失効のチェック 受け取った証明書が失効していないことを確認する義務がある。 （４）　証明書以外の情報の利用 取引の重要性に応じて、証明書だけに依存するのではなく他の手段も併用する必要があることを認識しておく義務がある。		1.1.15 検証者の義務 ・証明書の使用目的を確認する ・証明書ステータスの検証 ・責任の限界を確認し、同意する

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
9	2.1.5. リポジトリの義務 · 証明書と失効情報の適時な公表	3.2.9 認証局の公開鍵の管理 （２）認証局の証明書は広く一般に開示もしくは公開する必要がある。 3.3.4 証明書の開示 ①登録・保管された証明書の開示もしくは非開示等についてポリシーで明らかにする事 ②開示もしくは公開する場合には、下記について明確にする事 ・開示先：誰に開示するかを明確にする事 ・開示方法：開示サービス時間帯と併せアクセス方法、開示情報フォーマット等も明確にする事 ・開示期間：加入者への証明書発行後その有効期限内は開示する事		1.1.13 リポジトリの義務 適切な時に、証明書とCRLを発行する。
10	2.2. 責任 2.2.1 認証局の責任 各主体のタイプごとの依存可能性の分担に関するすべての適用可能な規定。 · 権利と、権利についての限度 · 補償される被害の種類（例、非直接的、特別、因果的、偶発的、可罰、整理による被害、過失、詐欺）と適用除外者 · 証明書ごと、若しくはトランザクションごとの損害（賠償）限度 · 他の例外事項（例、天災、他の主体の責任）	2.2 責務 責任と補償の内容を定め利用者に周知する事 （１） 認証局は、認証局が果たすべき義務及び証明書を取得または利用しようとする者が果たすべき義務を定めておく必要があるとともに、双方の義務を前提とする認証局の責任と保証に関するポリシーを定め、開示する必要がある。 （２） またポリシーを開示するに際し、利用者が認証局の信頼度を評価でき、さらに利用者の履行すべき義務および認証局の履行すべき義務について利用者が容易に理解できるように、CPSを開示するだけでなく、重要な事項については概要をまとめて開示する工夫が必要である。	(指針第１２条第１項第三号) 認定事業者が負担する保証又は責任の範囲について制限を設ける場合においては、その制限に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3904 (4) 保証、免責について限定を設ける場合にはその範囲 ① 認証業務による保証及び免責について制限を設ける場合は、保証、免責の範囲と条件	3.2.16 認証局サービス・プロバイダは、認証局の役割及びそれぞれのファンクションの一部分を委託することがある。 認証局 サービス・プロバイダは、CPSに定義されている、認証の役目において最終的な責任がある。
11	2.3. 財務上の責任（取引に関わる法律上の責任） 財務的な責任に関する、すべての適用可能な規定。 2.3.1 依存する主体による 認証局、又は、登録局の賠償 2.3.2 様々な主体との間の受託関係（又は、その不存在） 2.3.3 管理的手続（例、課金、監査）	2.4 財務基盤 以下の財務基盤を保持し運営する事 ①認証局の責に帰される損害への賠償 ②認証局の諸機能遂行に係る継続的な投資		1.1.5 賠償責任 ・検証者に対する補償 ・委託関係

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
12	2.4.　解釈及び執行 認証ポリシ CPS の解釈と執行に関する若しくは すべての適用可能な規定 2.4.1　適用される法律 2.4.2　分割、存続、合併及び通知 2.4.3　紛争解決の手続		(指針第１２条第１項第十一号) 認証事業者との間で係争が生じた場合に適用される法令及び解決のための手続に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3912 (12) 認証事業者と関係者の間で係争が生じた場合に適用される法令及び解決のための手続きに関する事項 ① 認証業務に関して、認証事業者と関係者間で係争が生じた場合に適用される法令（原則日本国内法等） ② 係争解決のための手続き、係争を取り扱う管轄裁判所等	3.2.4-a 下記を含み、セキュリティポリシはセキュリティポリシの解釈、方針、標準、及び、組織への特別な重要性の承諾要求を含む a.法律及び契約上の要求への準拠 3.10.1 すべての法令、規定、契約要求を厳格に定義し、それぞれの情報システムにおいて文書化する。 3.10.2 情報システムの権利やソフトウェア製品の使用において、法に準拠していることを保障するため、適切な手続を実行する。 3.10.6 暗号システムの利用は国家的合意、法律、規則等に準拠しコントロールされる。
13	2.5.　料金 発行料、アクセス料金等に関する事項。		(指針第１２条第１項第八号) 認証業務の利用に係る料金に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3909 (9) 料金に関する事項 ① 利用者が認証業務を利用するに当たって必要となる料金と証明対象となる期間、支払方法、料金返還処理等	1.1.7 手数料 ・発行、再発行料金 ・執行また証明書状態確認アクセス料金 ・他のサービス料金 ・払い戻しポリシ

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
14	2.6.　情報の公表とリポジトリ 情報の公表に対する責任について規定。 ・証明書、証明書の最新のステータスに関する情報を公表する義務 ・公表の頻度 ・認証ポリシ、CPS、証明書、証明書ステータス、CRL を含む公表された情報オブジェクトに対するアクセスコントロール ・認証局 若しくは他の独立主体によって運用されているリポジトリの利用に関する要件	3.3.4 証明書の開示 （１）　認証局は登録・保管された証明書の開示もしくは非開示等についてポリシーで明らかにする必要がある。開示もしくは公開する場合は、以下の様に開示先・開示方法・開示期間などについても明確にする必要がある。 ・開示先：誰に開示するかを、明確に定める必要がある。 ・開示方法：開示の方法としては、開示サービスの時間帯等と併せて、アクセス方法、開示情報フォーマット等も明確にする必要がある。 ・開示期間：証明書の開示期間は加入者への証明書発行後、その証明書の有効期限内は開示する必要がある。 3.3.3 証明書の登録・保管 （１）認証局は作成した証明書の登録・保管において、不正アクセスを防止するためにアクセス管理を行なう必要がある。 （２）登録・保管された証明書は、災害もしくは消失等に備えてバックアップをとっておくことが望ましい。	（指針第１０条第ニ号） 発行者署名検証符号に係る電子証明書の値をＳＨＡ－１で変換した値によって認定認証業務を特定すること。 3513 (3)当該発行者署名符号に対応した発行者署名検証符号に係る電子証明書の値をSHA-1で変換した値が記録され、業務開始時には改ざん防止措置を施して公開されている。 (指針第１１条) 規則第六条第九号に規定する必要な情報は、次の各号に掲げる事項を含むことを要するものとする。 3711 (1)以下の事項について、その内容、手続等が、認証業務規程及び事務処理要領等に明確に規定され、それに従って署名検証者への開示が実施されている。 3712 (2)署名検証者に関する(3)の事項を記述している場所が、電子証明書にリンク先を表示する等の方法によって署名検証者が理解し易くなっている。 3713 (3)以下の各項について署名検証者に理解しやすくかつ具体的に記述され(2)で指定された場所に存在する。 ① 署名検証者は、信頼すべきかを判断する電子証明書について、電子証明書の目的など使用範囲及び制限（利用者に通知した利用条件を含む。）を確認すること。 ② 署名検証者は、発行者署名検証符号を確実に入手し、電子署名が行われた情報を検証すること。 ③ 署名検証者は、適切な手段を用い、電子証明書が失効されていないかどうかについて確認すること。	1.1.8　公表とリポジトリの義務 ・認証局情報の公開 ・公開の頻度 ・アクセス制御 2.2.5.1 認証局の規定に従ってディレクトリ等のリポジトリにて、発行された証明書を検証者に利用可能とする。 2.2.5.2 証明書の発行において、認証局は開示された認証局の要件に従ってリポジトリその他の配布メカニズムによって証明書を配布する。 2.2.5.3 権限のある認証局作業者だけが、認証局のリポジトリやその他の配布メカニズムを管理する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
14		2.5 情報開示 以下の情報を開示する事 2.5.1 経営情報 （１）　利用者が認証局の経営に対する健全性を確認できるように、財務状況を含めた経営情報の開示あるいは公開が必要である。例えば、認証局が法人の場合は、主要株主、役員、財務諸表 2.5.2 技術情報 （１）　利用者が認証局の技術に対する安全性や信頼性を判断できるように、開示あるいは公開できる範囲での技術情報の開示あるいは公開が必要である。例えば、暗号アルゴリズム、暗号通信プロトコル等の技術情報を開示あるいは公開する必要がある。 2.5.3 安全対策実施状況 （１）　認証局の業務運営が安全に実施されているか利用者が確認できるように、業務運営（内部不正防止対策、権限の分散、教育など）に対する定期的な監査実施結果などを開示あるいは公開する必要がある。 2.5.4 認証実施規定（CPS） （１）　利用者が認証局を信頼性・安全性・経済性等の面から評価できるように、認証実施規定（ＣＰＳ）を開示あるいは公開することが必要である。	(規則第６条第十三号) 認証事業者の連絡先、業務の提供条件その他の認証業務の実施に関する規程を適切に定め、当該規程を電磁的方法により記録し、利用者その他の者からの求めに応じ自動的に送信する方法その他の方法により、利用者その他の者が当該規程を容易に閲覧することができるようにすること。 (指針第１２条) 規則第六条第十三号に規定する認証業務の実施に関する規程は、次の各号に掲げる事項に関する規定を含むことを要するものとする。 (指針第１２条第１項第一号) 認証事業者の名称及び連絡先（住所、電話番号、ファクシミリ番号及びメールアドレス） (指針第１２条第１項第二号) 証明の目的、対象又は利用範囲について制限を設ける場合においては、その制限に関する事項 (指針第１２条第１項第三号) 認定事業者が負担する保証又は責任の範囲について制限を設ける場合においては、その制限に関する事項 (指針第１２条第１項第四号) 利用申込みの方法及び利用者の真偽の確認の方法に関する事項 (指針第１２条第１項第五号) 電子証明書の失効の請求に関する事項 (指針第１２条第１項第六号) 電子証明書の失効に関する情報の確認の方法及び確認することができる期間に関する事項 (指針第１２条第１項第七号) 認証業務に係るセキュリティに関する事項（利用者に係る個人情報の取扱いに関する事項を含む。） (指針第１２条第１項第八号) 認証業務の利用に係る料金に関する事項 (指針第１２条第１項第九号) 帳簿書類の保存に関する事項 (指針第１２条第１項第十号) 業務の廃止に関する事項 (指針第１２条第１項第十一号) 認証事業者との間で係争が生じた場合に適用される法令及び解決のための手続に関する事項 (指針第１２条第１項第十二号) 当該規程の改訂に関する事項及び利用者その他の者に対する通知方法に関する事項	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
15	2.7.　準拠性監査 準拠性監査に関する規定 2.7.1.　各主体に対する準拠性監査の頻度 2.7.2.　監査者の身元・資格／認定にかかる事項 2.7.3.　監査者と被監査部門の関係 2.7.4.　監査テーマ 2.7.5.　監査指摘事項への対応 2.7.5.　監査結果の通知、開示等	3.6.4 監査人の選定 （1）監査人は、コンピュータ・セキュリィティに関する専門的知識を有するもので、監査対象から独立かつ客観的立場の者を選定することが望ましい。 （2）監査人は複数人を選定する事 3.6.5 監査の頻度 監査は下記事態発生の場合を除き、年最低２度行なう事 ・システム資源の異常な負荷増大、処理件数の異常増加、通常とは異なる時間帯や場所からアクセスが発生した場合 ・ＣＰＳ等に重要な変更が生じた場合 ・利用者間のトラブルが多発した場合 ・その他監査が必要と判断される場合 3.6.6 監査結果の開示と対処 （１）　監査実施後は、監査結果を速やかに開示するものとし、監査の結果として欠陥が指摘された場合には、以下の対処を行う必要がある。 ・欠陥が修正されるまでの対処（例えば、運用の停止、利用者に対する十分なアナウンス等） ・欠陥への対処 3.6.7 監査後の監査情報及び監査結果の保存 （１）　監査情報及び監査結果の保存は、監査後の保存期間を予め定め、不正なアクセスによる情報の変更・改竄・削除等が無いよう適切かつ合理的な安全対策を講ずる必要がある。	(規則第６条第十五号) 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 (第６条第十五号ニ) ニ　業務の監査に関する事項 3C31 (1) 以下の(2)～(3)を含む事項について規定が定められ、手順等を含め認証業務規程及び事務取扱要領に規定されている。 3C32 (2) 認証業務に係わる監査基準（規則第６条第十三号に規定する規程及び同号イの規定により定められる業務の手順等に基づき、適正に業務が運営されていることを確認するための監査に係る基準）が定められ、それに従って定期的な監査が行われる。 3C33 (3) 監査報告書での指摘事項及びセキュリティ対策技術の最新の動向を踏まえ、設備、規程等の見直しを含む対策を講じかつその結果の評価を行う。	1.1.9 準拠性監査 ・準拠性監査の周期 ・監査人と非監査部門の関係 ・監査の対象 ・結果が不十分であった場合の対処 ・結果の通知 3.10.8 管理者は、職務範囲においてセキュリティ手続が適切に実行されていることを保証する責任がある。 3.10.9 認証局のオペレーションは、セキュリティポリシや規格に準拠しているかを定期的にレビューする。 3.10.10 認証局のシステムが、セキュリティ基準に準拠しているか定期的にチェックする。 3.10.11 ビジネスプロセスの中断を最小にするよう、オペレーションシステムの監査が計画、承認される。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
16	2.8.　秘密保護ポリシ 個人情報等秘密情報の取扱に関する規定。 2.8.1.　秘密扱いとする情報 2.8.2.　秘密扱いとしない情報 2.8.3.　証明書失効及び停止情報の開示 2.8.4.　法的執行機関への情報開示 2.8.5.　民法上の要求にともなう開示 2.8.6.　利用者の要求に基づく情報開示 2.8.7.　その他の理由に基づく情報開示	3.5.1 加入者秘密情報の定義 加入者秘密情報とは、証明書あるいは失効リストに記載される情報以外の加入者に関する情報であり、加入者のプライバシーに係る情報および利用履歴等を含む。例えば証明書の発行・更新・失効のために加入者から提示された氏名、生年月日、パスワードその他の記述又は加入者に付された番号、記号その他の符号（当該情報のみでは識別できないが、他の情報と容易に照合する事ができ、それにより当該個人を識別できるもの）が含まれる。 2.6 機密保持 2.6.1 セキュリティ維持に関わる機密情報を保持する事 （１）　運用者の特定、運用体制、マシン室のレイアウト、監査情報、設備・システムセキュリティ等の機密にすべき情報については、その影響度を十分考慮した取り扱い方法を定め、それに従った運用が適正に行われているか適時確認することが必要である 2.6.2 加入者関連情報を保護する事 （１）　加入者に関わる情報が目的外に利用されたり、不正に漏洩されたりすることがないように、機密範囲とその取り扱い方法を定め、それに従った運用が適正に行われているか適時確認することが必要である。加入者に関わる情報には、加入者が証明書申請時に提供するプライバシー情報だけでなく、認証局がその運用によって知り得た情報（例えば、どのような利用者から証明書の有効確認の問合せがあったかという情報やその頻度）なども含まれる。	(規則第６条第十四号) 電子証明書に利用者として記録されている者から、権利又は利益を侵害され、又は侵害されるおそれがあるとの申出があった場合においては、その求めに応じ、遅滞なく当該電子証明書に係る利用者に関する第十二条第一項第一号ロ及びハに掲げる書類を当該申出を行った者に開示すること。(第６条第十四号) 3B01 (1) 電子証明書の名義人から権利又は利益を侵害され、又は、侵害されるおそれがあるとの申し出があった場合、当該電子証明書利用申込書類及び利用者の真偽を確認するための資料、電子証明書記載データ等を開示することに関する規定が明確に認証業務規程及び事務取扱要領等に規定され、実施されている。 3B02 (2) 情報開示の条件として、開示を請求した者が当該電子証明書の名義人であることの確認方法及び開示範囲、手順等について明確に、認証業務規程及び事務取扱要領等に規定され、実施されている。 (指針第１２条第１項第七号) 認証業務に係るセキュリティに関する事項（利用者に係る個人情報の取扱いに関する事項を含む。） 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3908 (8) セキュリティに関する事項 ① 採用しているセキュリティ基準、技術標準等に関する事項 ②個人情報の取扱いに関する事項	3.10.4 関連法規に従うよう、個人情報保護のためのコントロールを導入する。 3.10.5 情報処理設備の使用を認可し、設備の誤用を妨げるため管理する。 3.10.7 開示された認証局の要件に従い、機密性のポリシと手続は以下のことを記述する。 a．認証局か登録局によって機密に保たれなければならない情報の種類 b．機密であることを考慮しなくともよい情報の種類 c．証明書の失効と停止において通知を受ける者は誰か d．法執行機関への情報の提供に関するポリシ e．一般的に明らかになった情報の提供 f．認証局や登録局が、所有者の要求に応じて情報を提供する条件 g．その他、機密情報を公開しなければならない状況

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
16		3.5.2 加入者秘密情報へのアクセス権限 （１）　加入者秘密情報へのアクセスは、機密保持の為に、権限を有する者だけが行なえる様にする必要がある。 3.5.3 加入者秘密情報の保管 （１）　加入者秘密情報は、不正に改竄・消去・漏洩等がなされないように安全に保管する仕組み、および必要に応じて取り出せる仕組みを持つことが必要である。 （２）　加入者秘密情報は、災害等により消失することのないように必要に応じてバックアップをとることが望ましい。 3.5.4 加入者秘密情報の開示 （１）　認証局は、加入者秘密情報を開示してはならない。ただし、以下の場合はその限りではない。 ・加入者本人または本人の代理人から自己の登録情報に関して開示要求があった場合。ただし、認証局はあらかじめ本人であることを確認する要領を定める必要があり、その要領に従って本人確認を実施した後、開示するものとする。 ・法令の定めにより、回答が義務づけられているもの。また、法令の範囲内で本人の同意を得た場合。 3.5.5 加入者秘密情報の保存 （１）　証明書の有効期限が切れた後も、認証局は一定の期間加入者秘密情報を保存する必要がある。 （２）加入者秘密情報は、不正なアクセスによる情報の改竄・消去・漏洩等が無いよう適切な手段を講じて保存する必要がある。	(規則第６条第十五号) 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 (第６条第十五号へ) へ　利用者の真偽の確認に際して知り得た情報の目的外使用の禁止及び第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置 3C51 (1) 電子証明書交付申込時に利用者より提出される個人情報について、電子証明書に記載する等、認証業務の用に供する以外は使用しない等の取扱いを明確にした個人情報取扱及び保護に関して、認証業務規程、事務取扱要領等に規定され、実施されている。 3C52 (2) 電子証明書交付申込時に、個人情報の取り扱い方法、電子証明書への記載範囲について利用者に明示し、利用者の承認を受けている。 3C53 (3) 個人情報の取扱及び保護に関して、全ての就業者を対象とした、役割に応じた教育・訓練計画が策定され、教育・訓練等が同計画に沿って実施されている。 3C54 (4) 個人情報の管理・保管場所の整備がなされ、適正な管理が実施されている。	
17	2.9.　知的財産権 証明書の所有権、CP／CPSの仕様、 名前、鍵に対する権利等の規定。			

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
	3.　利用者の識別と本人確認			
18	3.1.　新規発行時での利用者の本人確認方法 証明書主体（サブジェクト）の登録、若しくは証明書発行における識別と本人認証の手続に関する規定。 3.1.1.　サブジェクトに割り当てられた名前の形式 3.1.2.　名前が意味を持つ必要があるか否か 3.1.3.　様々な名前の形態を変換するルール 3.1.4.　名前が一意である必要があるか否か 3.1.5.　所有者の名前を決定する際の紛争解決手続 3.1.6.　商標の認識・認証・役割 3.1.7.　公開鍵に対応する私有鍵の所有を証明する方法 3.1.8.　サブジェクト（ 認証局、登録局、末端主体）の組織（法人）としての識別のための認証要件 ・要求される識別証の数 ・認証局、若しくは登録局が、提供された識別証の認定方法 ・出頭の必要性 ・組織の一員として個人が認証されるのか 3.1.9.　個人の認証要件	3.1.1 証明書新規発行時の審査 3.1.1.1 本人確認と情報の真正性確認 （１）　申請された情報の真正性確認のために、信頼できる機関・組織・人による証明あるいは確認済みの情報と一致していることを照査する必要がある。より高い真正性確認のために、複数の情報源の情報を利用するのが望ましい。 （２）　申請者の本人確認のために、真正性確認とは異なる手段を用いることが必要である。例えば、審査結果等の通知に際して、申請者に通知が確実に届くような手段（例えば郵便など）を利用する必要がある。より高い信頼性を確保するためには、本人出頭が望ましい。 （３）　オンライン申請以外の場合は、証明書の不正発行を防止するために、審査処理を複数人で分担して行なう必要がある。 ●オンライン申請 申請者が認証局に対してオンライン形態で認証書申請を行う方式である。 例えば、カード会員等個人の認証に適した申請方法である。認証局所定の申請フォームを画面上に呼び出し、入力フィールド（申請必要項目）に以下のような情報を複数入力させて認証局に送信する。 ・生年月日 ・自宅住所 ・自宅電話番号 ・クレジットカード番号／預金口座番号 ・暗証番号（ＰＩＮ） ・母親旧姓（米国の例） 等々、及びその組合わせが考えられる。本人確認は、これらの情報を信頼できる機関（クレジットカード会社、銀行等）の保有する情報、あるいは自局が保有する情報との突き合わせ、及び審査結果等を簡易書留などで申請者に郵送することによって行なわれる。	(規則第６条第五号) 電子証明書には、次の事項が記録されていること。 (第６条第五号ニ) ニ　当該電子証明書に係る利用者署名検証符号及び当該利用者署名検証符号に係るアルゴリズムの識別子 3413 (3) 規則第６条第五号ニに規定する電子証明書に記録する利用者署名検証符号は、利用者署名符号によって行われた電子署名を当該利用者署名検証符号を用いて検証する等の方法により、利用者が当該利用者署名検証符号に対応する利用者署名符号を保有していることを確認する。 (規則第５条第1項第一号）出入国管理及び難民認定法（昭和二十六年政令第三百十九号）第二条第五号に規定する旅券、別表に掲げる官公庁が発行した免許証、許可証若しくは資格証明書等、外国人登録法第五条に規定する外国人登録証明書又は官公庁（独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第十五号の規定の適用を受けるものをいう。）を含む。）がその職員に対して発行した身分を証明するに足りる文書で当該職員の写真をはり付けたもののうちいずれか一以上の提示を求める方法 2201 (1) 規則第５条第１項第一号の方法によって利用者または代理人の真偽を確認するにあたっては、提示された官公庁が発行した証明書等について少なくとも記載内容、形式、有効期限等が真正なものであることを確認している。かつ、当該証明書等に貼付してある写真と提示者との照合により真偽の確認を行っている。	1.1.25 初期登録 認証局の、申請者（利用者）の申請者の本人確認、認証要件と申請者登録時又は証明書発行時の証明書リクエストの検証。 ・サブジェクトに割り当てられた名前の形式 ・名前が意味を持つ必要があるか否か ・名前が一意である必要があるか否か ・所有者の名前を決定する際の紛争解決手続 ・商標の認識・認証・役割 ・公開鍵に対応する私有鍵の所有を証明する方法 ・証明書発行の為の申請者の公開鍵をどのように安全に認証局に送付するか ・組織員における認証要件 ・要求データの要件 ・証明書要求をどのように検証するのか ・証明書要求に含まれる情報の正確さをどのように検証するのか ・証明書要求のエラー又は欠落をチェックするか否か

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
18		●書類送付申請 認証局所定の申請書式に必要事項を記載させるとともに、申請者が本人であることを証明する以下のような書類を送付させる。 ・印鑑登録証明書（法人・個人） ・戸籍謄本（個人） ・商業登記簿謄本（法人） 等々、およびその組み合わせが考えられる。本人確認は、証明書等の記載事項及び捺印の確認をもって行われる。 ●出頭申請 申請者本人が出頭しての対面による申請受付のことである。認証局所定の申請書式に必要事項を記載させるとともに、以下のような書類を提示させる。 ・運転免許証 ・パスポート ・健康保険証 等々、およびその組み合わせが考えられる。本人確認は、証明書等の写真および記載事項の確認をもって行なわれる。 3.1.1.2 申請の受理と意思確認 （１）　認証申請者からの申請を認証局が受理したことを申請者に対して返答通知するとともに、併せて申請の意思確認を行う必要がある。なお、意思確認は、結果通知による事後的確認であっても構わない。 3.1.1.3 唯一性確認 （１）　被認証者名について、少なくとも当該証明書を発行する認証局配下では重複がなくユニークであることを確認する必要がある。 （２）　申請者の公開鍵について、少なくとも当該証明書を発行する認証局配下では重複していないことを確認するのが望ましい。 （３）　証明書に記載される公開鍵に対応する正当な私有鍵を申請者が所持していることを確認するのが望ましい。 例えば、申請情報に私有鍵でデジタル署名させるか、あるいはチャレンジデータにデジタル署名させて認証局に送付させる方法等によって行なう。 3.1.1.4 審査情報の登録 （１）　申請情報及び審査情報は、後から利用できるように登録しておく必要がある。 （２）　申請時に、予め失効などの事故に対する情報など（例えば、失効申請代行者など）を登録させることが望ましい。	(規則第５条第1項第二号) 利用の申込書に押印した印鑑に係る印鑑登録証明書（利用申込者が国外に居住する場合においては、これに準ずるもの）の提出を求める方法 2202 (2) 規則第５条第１項第号二号の方法によって利用者または代理人の真偽を確認するにあたっては、印鑑登録証明書について少なくとも記載内容、形式、有効期限等が真正なものであることを確認している。 かつ、利用申込書に利用者又は代理人の実印が押印され、利用者又は代理人の真偽の確認資料としてその押印に係る印鑑登録証明書が添付されている場合は、利用申込書に押印された実印の印影と利用申込書に添付された印鑑登録証明書に証明されている印影の写しが一致することを確認している。 (規則第５条第1項第三号) 郵便規則（昭和二十二年逓信省令第三十四号）第百二十条の三十の十に規定する本人限定受取郵便又はこれに準ずるものにより、申込みの事実の有無を照会する文書を送付し、これに対する返信を受領する方法 2203 (3) 規則第5条第１項第三号の方法によって利用者または代理人の真偽を確認するにあたっては、受取人が本人に限定される書留郵便等による照会書の交付時に行われる真偽の確認を採用する場合は、利用者又は代理人に確かに交付されたことを示す書類を受領している。 2204 (4) 代理人による利用申込み、及び規則第5条第1項第三号に規定する申込みの事項の有無を照会する文書の代理人による受取りの場合において提出を求める委任状には、利用者が代理人に対し委任する利用申込みの内容もしくは代理人による受取りが明確に記されている。 2205 (5) 代理人による利用申込み、及び規則第５条第１項第三号に規定する申込みの事項の有無を照会する文書の代理人による受取りの場合、委任状になされた利用者本人の署名を確認するとともに、同文書に押印された利用者の実印の印影と委任状に添付された印鑑登録証明書に証明されている印影の写しが一致することを確認している。	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
18		3.1.1.5 審査結果の通知 （１）　審査結果は、通知あるいは問合せに対する回答等によって、申請者に通知する必要がある。	(規則第５条第2項) 前項の規定にかかわらず、利用者が現に有している電子証明書の発行者に対し、新たな電子証明書の利用の申込みをする場合において、当該電子証明書の有効期間が、同項に規定する方法により当該利用者の真偽の確認を行って発行された電子証明書の発行日から起算して五年を超えない日までに満了するものであるときは、当該利用者が現に有している電子証明書に係る電子署名により当該利用者の真偽を確認することができる。 2206 (6) 利用者の真偽の確認を規則第５条第２項の規定により行う場合においては、利用の申込みに係る情報に講じられた利用者の電子署名を検証し、当該電子署名に係る電子証明書について、失効に関する情報が記録されていないこと等有効性を確認している。かつ、新たに発行する電子証明書の有効期間が、規則第５条第１項の各号のいずれかの方法により利用者の真偽の確認が行われ発行された電子証明書の発行日から５年未満に満了することを確認している。 2207 (7) 利用者の真偽の確認と利用者からの利用者署名検証符号の受領を同時に行わない場合においては、利用者署名検証符号の提出者と真偽の確認を行った利用申込者が一致することを、本人確認後に渡した本人だけに、かつ本人以外には知りえない情報を用いて確認する等により確認をしている。 2208 (8) 利用者または代理人の真偽の確認を行うにあたって疑義が生じた場合においては、あらかじめ文書をもって定められた手続に従って、利用者または代理人の真偽の確認の手続を行う。	
19	3.2.　通常の更新 各主体（ 認証局、登録局、利用者）の通常の鍵更新のための識別と本人認証の手続	3.1.2 証明書定期更新時の審査 （１）　証明書の定期更新申請に対する審査は、新規発行時の場合と同様、本人確認、唯一性確認、意思確認、審査結果通知、登録などの処理が必要である。 （２）　なお、本人確認や意思確認については、新規発行時とは異なる手段を用いて行なうことも可能である。例えば、名前などの重要な情報に変更がない場合には、申請情報に対して更新前の私有鍵でデジタル署名させることで本人確認や意思確認を行うことも可能である。	(規則第６条第四号) 電子証明書の有効期間は、五年を超えないものであること。 3401 (1) 以下の（２）の事項の範囲内において電子証明書の有効期間が、認証業務規程及び事務取扱要領に明確に規定され、実施されている。 3402 (2) 利用者に発行する電子証明書の有効期間は証明の可否判断日から起算して５年未満である。	2.2.3.1 認証局や登録局が証明書の更新時に証明書の確認を行えるよう、利用者の証明書鍵更新要求には、利用者の識別名、証明書番号、有効期間を含める。 2.2.3.2 認証局はエンティティに、公開鍵証明書の公開鍵に対応する私有鍵を使用して証明書更新要求にデジタル署名することを要求する。 2.2.3.3 認証局や登録局は、エンティティの身元と証明書更新の正当性を検証する。 2.2.3.4 認証局や登録局は、証明書更新要求の署名を検証する。 2.2.3.5 認証局や登録局は、更新される証明書の存在と正当性を検証する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
19				2.2.3.6 認証局や登録局は、認証局の規定に従った証明書更新要求であるかを検証する。 2.2.3.7 外部登録局を使用する場合、認証局は外部登録局に、登録局が署名したエンティティからの証明書更新要求を認証局に送信するように要求する。 2.2.3.8 外部登録局を使用する場合、開示された認証局の要件に従って、認証局は登録局に証明書更新のプロセスにおける責任を持ち、安全を保つよう要求する。 2.2.3.9 外部登録局を利用する場合、認証局は外部登録局に、イベントジャーナルへ登録局の作業を記録するよう要求する。 2.2.3.10 外部登録局を利用する場合、認証局は登録局から送信された内容の真正性を検証する。 2.2.3.11 外部登録局を利用する場合、認証局は登録局からの証明書更新要求の登録局の署名を検証する。 2.2.3.12 認証局や登録局は、証明書更新要求のエラー、欠落のチェックを実施する。 2.2.3.13 認証局や登録局は、更新が必要となる証明書の有効期限前に、利用者に通知する。(2.1.1にもあり) 2.2.3.14 証明書更新の生成及び発行の前に、認証局や登録局は下記の検証を行う。 a．証明書更新データ要求の署名の検証 b．更新対象の証明書の存在と検証の確認 c．証明書有効期間を含み、証明書が認証局の規定の要求を満たすか 2.2.2.1（Certificate Renewal -Optional） 申請者の証明書更新要求は、申請者の識別子、証明書のシリアルナンバー、有効期間が含まれる。 2.2.2.2（Certificate Renewal -Optional） 認証局はエンティティに、エンティティの公開鍵証明書にある公開鍵に対応する私有鍵で証明書更新要求に署名するように要求する。 2.2.2.3（Certificate Renewal -Optional） 認証局や登録局は、エンティティの身元確認と証明書更新を確認するため、証明書更新データを処理する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
19				2.2.2.4 (Certificate Renewal -Optional) 認証局や登録局は、証明書更新要求の署名を検証する。 2.2.2.5 (Certificate Renewal -Optional) 認証局や登録局は、証明書の存在と正当性を検証する。 2.2.2.6 (Certificate Renewal -Optional) 認証局や登録局は、（有効期間の延長を含む）要求が開示された認証局の要件を満たしているか検証する。 2.2.2.7 (Certificate Renewal -Optional) 外部登録局を使用する場合、認証局は外部登録局に登録局によって署名されたエンティティの証明書要求データを送信するよう要求する。 2.2.2.8 (Certificate Renewal -Optional) 外部登録局を使用した時、登録局は責任のある証明書更新プロセスを安全に保つ。 2.2.2.9 (Certificate Renewal -Optional) 外部登録局を使用する場合、認証局は外部登録局に処理をイベントジャーナルに記録するように要求する。 2.2.2.10 (Certificate Renewal -Optional) 外部登録局を使用する場合、認証局は登録局からの通信の真正性を検証する。 2.2.2.11 (Certificate Renewal -Optional) 外部の登録局を使用する場合、認証局は証明書更新要求の登録局の署名を検証する。 2.2.2.12 (Certificate Renewal -Optional) 認証局や登録局は、証明書更新要求にエラーや誤りがないかチェックする。 2.2.2.13 (Certificate Renewal -Optional) 認証局や登録局は、証明書の更新が必要になる期限が終了する前に、利用者に通知する。 2.2.2.14 (Certificate Renewal -Optional) 更新された証明書を発行する前に、認証局や登録局は以下のことを検証する。 a．証明書更新データの署名 b．更新された証明書存在と正当性 c．要求（有効期間の延長を含む）が開示された認証局の要件を満たしているか

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
20	3.3.　失効後の更新－鍵が危殆化していない場合 証明書が失効した後に、各主体（ 認証局、登録局、証明書所有者）の鍵更新のための識別と本人認証の手続	3.1.4 失効後の証明書再発行時の審査 （１）　公開鍵や重要情報の変更が伴う失効の場合、失効後の証明書の再発行は、証明書の新規発行と同様の処理が必要である。 （２）　本人以外の失効申請に基づく失効の場合、失効後の証明書の再発行は、証明書の新規発行と同様の処理が必要である。		2.2.3.15 証明書が失効又は有効期限切れの場合、新規の証明書発行と同様な登録手続を必要とする。
21	3.4.　証明書の失効申請 各主体（ 認証局、登録局、利用者）による失効要求のための識別と本人認証の手続	3.1.3 証明書失効時の審査 3.1.3.1 申請者確認 （１）　申請者の本人確認は、私有鍵の危瀕時などの場合には迅速に行なう必要がある。 例えば、私有鍵の危瀕時などの場合には、申請情報にデジタル署名を付したもので受け付けるなど（この場合は、私有鍵を不正に入手した者、あるいは正当な保持者による失効申請は実効性がある）。 （２）　私有鍵の消失、重要情報の変更の場合は、新規発行と同等の本人確認が必要である。 （３）　証明書の誤りや不正使用の検知、本人による失効申請が困難な事由の発生、あるいは証明書の不正発行などの場合は、登録局や認証局あるいは事前に登録されている機関などが本人に代わって失効申請できるようになっていることが必要である。 （４）　オンライン申請以外の場合は、証明書の不正な失効を防止するために、審査処理を複数人で分担して行なう必要がある。		2.2.6.2 認証局は、開示された認証局の要件に従って、外部登録局が本人確認と証明書失効要求の認証をするよう要求し、検証する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
	4. 運用上の要件			
	様々な運用要件に関して、認証局、登録局、若しくは証明書所有者に負わされる要件を規定。			
22	4.1. 証明書の申請 利用者の登録と、証明書発行のための申請に関する要件の規定。	3.1.1.4 審査情報の登録 （１） 申請情報及び審査情報は、後から利用できるように登録しておく必要がある。 （２） 申請時に、予め失効などの事故に対する情報など（例えば、失効申請代行者など）を登録させることが望ましい。	(規則第５条第1項) 法第六条第一項第二号の主務省令で定める方法は、認証業務の利用の申込みをする者（以下「利用申込者」という。）に対し、住民票の写し、戸籍の謄本若しくは抄本（現住所の記載がある証明書の提示又は提出を求める場合に限る。）、外国人登録法（昭和二十七年法律第百二十五号）第四条の三に規定する登録原票記載事項証明書又はこれらに準ずるものの提出を求め、かつ、当該利用申込者について、次の各号に掲げる方法のうちいずれか一以上のものにより行うものとする。ただし、認証業務の利用の申込み又は第三号に規定する申込みの事実の有無を照会する文書の受取りを代理人が行うことを認めた認証業務を実施する場合においては、当該代理人に対し、その権限を証する利用申込者本人の署名及び押印（押印した印鑑に係る印鑑登録証明書が添付されている場合に限る。）がある委任状（利用申込者本人が国外に居住する場合においては、これに準ずるもの）の提出を求め、かつ、当該代理人について、次の各号に掲げる方法のうちいずれか一以上のものにより、真偽の確認を行うものとする。 2101 (1) 以下の（２）～（５）について、手続き、確認方法、必要資料等が、認証業務規程及び事務取扱要領に明確に規定され、実施されている。 2102 (2) 自己の業務において例えば、対面による申込み、郵送による申込み、オンラインによる申込み等の、採用する方式について指定する。 2103 (3) 指定した申込方式において利用者及び代理人の真偽の確認のために使用する資料の種類を指定する。 2104 (4) 指定した方式以外の方式によりなされた電子証明書の交付申込みの受理に関する取扱い手続きについて定めている。 2105 (5) 規則第6条第二号で規程されている利用申込書(利用申込みデータ)を受領（受信）後、住民票の写し、戸籍の謄本若しくは抄本（現住所の記載がある証明書の提示又は提出を求める場合に限る。）、外国人登録法（昭和二十七年法律第百二十五号）第四条の三に規定する登録原票記載事項証明書を求める。	2.2.1.1 認証局は、外部登録局が開示された認証局の要件に従ってエンティティの本人確認手続を行うように要求し、検証する。 2.2.1.2 認証局は、証明書を要求しているエンティティに、認証局の規定の要件に従った適切な証明書要求データ（登録要求）を登録局又は認証局に送信するよう、要求する。 2.2.1.3 認証局は、外部登録局が認証局の規定の要件に従って証明書要求の正当性の確認を行っていることを要求し、検証する。 2.2.1.4 認証局は、外部登録局が認証局の規定の要件に従ってエンティティの証明書要求に含まれている情報の正確性を検証するよう要求し、検証する。 2.2.1.5 外部の登録機関を使用する場合、認証局は開示された認証局の要件に従って登録機関の身元を検証する。 2.2.1.6 外部の登録機関を使用する場合、認証局は、開示された認証局の要件に従って外部登録機関を認可する。 2.2.1.7 認証局は、開示された認証局の要件に従って（証明書を要求する）エンティティが認証局や外部登録局に適切な認証要求データを送信するよう要求する。 2.2.1.8 認証局は要求しているエンティティに、署名付メッセージによって公開鍵を送付することを要求する。 認証局は、登録要求に含まれる公開鍵に対応する私有鍵によって、登録要求にデジタル署名することを要求する。 a．認証アプリケーションプロセスにおいてエラーを検知するため。 b．登録された公開鍵に対応する私有鍵を持っていることを証明するため。 2.2.1.9 認証局は、エンティティの証明書要求を確認するため、証明書要求に含まれている公開鍵を使用する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
22			(指針第９条) 規則第六条第二号の利用申込書その他の書面又は利用の申込みに係る情報は、次の各号に掲げる事項の記載又は記録を含むことを要するものとする。 （指針第９条第一号） 利用申込者の氏名、住所、生年月日 (指針第９条第二号) 利用の申込みをする電子証明書の用途 (指針第９条第三号) 利用申込者の氏名のローマ字表記 (指針第９条第四号) 利用申込者の自筆署名又は利用者の真偽の確認の方法として印鑑登録証明書を用いる場合においては、当該証明書に係る印鑑による押印（利用の申込みに係る情報の送信の場合を除く。） (指針第９条第五号) 代理人が申込みをする場合においては、前各号に掲げる事項に加え、代理人の氏名及び自筆署名又は印鑑登録証明書に係る印鑑による押印（代理人の真偽の確認の方法として印鑑登録証明書を用いる場合に限る。）並びに代理人による申込みの理由 3211 (1)認証業務において採用する申込方式に応じた利用申込書であること及び以下の(２)、（３）の事項について明確に認証業務規程及び事務取扱要領に規定され、利用申込が行われている。 3212 (2)利用申込書に指針第9条第一号から第四号までの記載事項がある。オンライン申込みの場合は指針第9条第四号に代えて有効な電子署名が付されている。 3213 (3)代理人による申込みの場合においては、利用申込書には指針第9条第一号から第四号に加えて、指針第9条第五号に定める代理記載事項がある。 (指針第１２条第１項第四号) 利用申込みの方法及び利用者の真偽の確認の方法に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3905 (5) 利用申込み及び利用者の真偽の確認に関する事項 ① 電子証明書交付申込みの方法、交付申込みに必要となる提出書類、利用者の真偽の確認の方法、真偽の確認に使用する資料等	2.2.1.10 外部登録局を使用する場合、認証局は登録局によって署名されたメッセージ（証明書リクエスト）により、EEの証明書リクエストデータを認証局に送付することを要求する。 2.2.1.11 外部の登録局を使用する場合、開示された認証局の要件に従うよう、認証局は登録局に認証アプリケーションプロセスの一部を保証するよう要求する。 2.2.1.13 外部登録局を使用する場合、認証局は開示された認証局の要件に従って登録局からの送信内容の真正性を検証する。 2.2.1.14 外部登録局を使用する場合、証明書要求の登録局の署名を検証する。 2.2.1.15 認証局又は登録局は、開示された認証局の要件に従い、証明書要求のエラー、欠落をチェックする。 2.2.1.16 認証局は、認証局ドメイン内のエンティティの識別名が一意であることを確認する。 2.2.1.17 認証局は、身元確認がなされたエンティティからの証明書要求を受け付ける。 2.2.1.18 同一公開鍵を発見した場合、認証局は証明書要求の拒絶とオリジナルの証明書の失効を行う。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
23	4.2. 証明書の発行 証明書の発行と、発行の申請者への通知に関する要件の規定。	3.3.1 証明書作成 （１） 証明書作成にあたっては、不正な生成が行なわれないようにする手続きを定める必要がある。特にオフラインで生成する場合には審査処理を分離するとともに、権限を有する者以外はアクセスできないシステムが必要である。 3.3.2 証明書の送付 （１） 証明書送付にあたっては、セキュアな手段を講じることが必要である。 （２） 証明書を送付する際、受取りの確認ができる手段を選択することが望ましい。		2.2.4.6 認証局は認証局の署名用私有鍵を用いて、エンティティの証明書に署名する。 2.2.4.7 開示された認証局の要件に従い、認証局はエンティティからの要求を受け付けた後に証明書を発行する。 2.2.4.8 登録局を利用する場合、認証局は登録局にいつ利用者に証明書を発行するか知らせる。 2.2.4.9 （鍵更新をともなわない証明書更新）更新要求を認めた場合、証明書の有効期間と認証局の署名のみを変更した証明書を生成し署名する。 2.2.4.10 証明書の更新は、認証局が証明書更新要求を受け付けていた場合のみ新しい証明書を生成し署名をする。 2.2.4.11 証明書が発行されるとき、認証局は要求者に、申請とは異なった方法で通知を行う。
24	4.3. 証明書の受理 発行された証明書の受容と、それによって生ずる証明書の公表に関する要件を規定。			

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
25	4.4.　証明書の停止と失効 証明書の停止、失効に関する運用要件の規定。 4.4.1.　証明書が失効される理由 4.4.2.　証明書の失効要求の主体者 4.4.3.　証明書失効要求の手続 4.4.4.　失効要求の有効期間 4.4.5.　証明書が停止理由 4.4.6.　証明書の停止要求の主体者 4.4.7.　証明書の停止要求の手続 4.4.8.　停止が継続する期間 4.4.9.　証明書失効リスト（CRL）の発行頻度 4.4.10. 検証者における CRLをチェックする要件 4.4.11. オンラインの失効／ステータスチェックの利用可能性 4.4.12. 検証者におけるオンラインの失効／ステータスチェックを行う要件 4.4.13. 利用可能な他の形態の失効情報 4.4.14. 検証者における他の形態の失効情報をチェック要件 4.4.15. 鍵の危殆化に関する特別な要件	3.1.3.2 失効情報の登録 （1）　失効リスト生成などのために使用した申請情報及び審査情報は後から利用出来る様に登録する必要がある。 3.1.3.3 失効審査結果の通知 （1）　失効審査結果は、通知あるいは問合せに対する回答等によって、申請者に通知する必要がある。 3.4.1 失効リストの生成 （1）　失効リストの生成および認証局による署名は、証明書発行の場合と同等のセキュリテイ管理が必要である。 （2）　失効リストの発行は１週間毎、１日毎などというように定期的に行う必要がある。当該期間中に失効がない場合でも、ないことを知らせるために失効リストを発行する必要がある。どのような周期で行うかは、利用者に明確に示しておく必要がある。 3.4.2 失効リストの保管 （1）失効リストは、不正アクセスによる改竄、消去、漏洩等が行われない様に保管する必要がある。 （2）失効リストは災害もしくは消失等に備えバックアップを取っておく事が望ましい。 （3）失効した証明書が膨大になる場合の対応として、失効リストを分散配置したり、高度な失効管理が行える機関にその一部ないし全ての機能を行わせることも可能である。 3.4.3 失効リストの開示 (1) 失効した証明書もしくは証明書の最新ステータスは、失効リスト等によって正当な利用者が問合せ出来る様にする必要がある。 (2) 失効した証明書の当初の有効期限経過後も一定の期間失効リスト及び関連データを保存する事	(規則第６条第十号) 電子証明書の有効期間内において、利用者から電子証明書の失効の請求があったとき又は電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該電子証明書の失効の年月日その他の失効に関する情報を電磁的方法（電子的方法、磁気的方法その他の人の知覚によっては認識することができない方法をいう。以下同じ。）により記録すること。 3801 (1) 以下の事項を含む失効に係る当該利用者からの失効申込み、真偽確認、失効処理等が明確に認証業務規程及び事務取扱要領に規定され、実施されている。 3802 (2) 認証事業者自身の起因によるものを含む電子証明書の失効事由を明確に定める。 3803 (3) 失効申込書または失効の申込みデータの記載内容を明確に定める。 (規則第６条第十一号) 電子証明書の有効期間内において、署名検証者からの求めに応じ自動的に送信する方法その他の方法により、署名検証者が前号の失効に関する情報を容易に確認することができるようにすること。 3811 (1) 以下の事項について明確に認証業務規程及び事務取扱要領に規定され、遅滞なく実施されている。 ① 電子証明書に記載されている当該証明書の有効期間（開始日～終了日）の間、署名検証者が電子証明書の失効有無を確認する方法、失効情報の更新サイクル等 ② 電子証明書の有効期間が終了した場合の署名検証者からの問い合わせへの対応方法 3812 (2) 署名検証者が電子証明書の失効有無を確認する方法は、以下のいずれかの手段によって行われている。 ① 失効された電子証明書を記載した電子証明書失効リストの開示 ② オンラインによる電子証明書状態確認プロトコルによる電子証明書の失効状態の確認 ③ その他、上記①、②と同等の機能を有する手段	2.2.6.1 認証局の規定に従い、以下にたいして、認証局によって発行された証明書において認証局は迅速な安全かつ認可された失効方法を提供 a．一つ又は複数の証明書 b．認証局が使用している公開/私有鍵ペアによって生成された全ての証明書 c．公開/私有鍵ペアの使用にかかわらず、認証局が発行した全ての証明書 2.2.6.3 外部登録局が失効要求を受け付けた場合、開示された認証局の要件に従って、認証局は外部登録局に承認された方法で証明書失効要求を送付するよう要求する。 2.2.6.4 外部の登録局が失効要求を受け付け認証局に送信した場合、開示された認証局の要件に従って、認証局は登録局へ要求された失効の承認を提供する。 2.2.6.5 認証局又は登録局は、開示された認証局の要件にしたがって、証明書が失効されたエンティティへ失効したことを通知する。 2.2.6.7 認証局又は登録局は、開示された認証局の要件に従って、証明書が失効されたエンティティへ失効したことを通知する。 2.2.6.8 証明書が失効された場合、すべての更新された証明書も失効される。 2.2.7.1 開示された認証局の要件に従い、認証局は安全で認可された迅速な停止通知の方法を提供する。 a．1つ又は複数の証明書 b．認証局が使用している公開/私有鍵ペアによって生成された全ての証明書 c．公開/私有鍵ペアの使用にかかわらず、認証局が発行した全ての証明書 2.2.7.2 認証局は、開示された認証局の要件に従って、外部登録局が本人確認と証明書停止要求の認証をするよう要求、検証する。 2.2.7.3 外部登録局が停止要求を受け付けた場合、開示された認証局の要件に従って登録局は認証局に、承認された方法で証明書停止要求を送付するよう要求する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
25			(規則第６条第十二号) 第十号の規定により電子証明書の失効に関する情報を記録した場合においては、遅滞なく当該電子証明書の利用者にその旨を通知すること。 3821 (1) 電子証明書の失効に際し、当該電子証明書の利用者への通知及び通知方法を明確に認証業務規程及び事務取扱要領に規定し、実施している。 (指針第１２条第１項第五号) 電子証明書の失効の請求に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3906 (6) 電子証明書の失効請求に関する事項 ① 失効の請求の方式 ② 失効の請求書又は請求情報に記載又は記録すべき事項 ③ 電子証明書の失効事由（認証事業者の行為に起因するものを含む。） ④ 請求者の真偽の確認の方法 (指針第１２条第１項第六号) 電子証明書の失効に関する情報の確認の方法及び確認することができる期間に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3907 (7) 電子証明書失効情報の確認方法及び期間に関する事項 ① 公開される失効に係る情報の内容及び公開の方法、電子証明書失効リストの更新の周期 ②失効に係る電子証明書の利用者への通知方法 ③有効期間の経過後に署名検証者からの当該電子証明書の失効に関する情報について照会を受けた場合の対応方法等	2.2.7.4 認証局若しくは登録局は、開示された認証局の要件に従って証明書の停止をエンドンティティに通知する。 2.2.7.5 証明書停止要求は、認証局の規定要求に従って実施し、承認する。 2.2.7.6 認証局は認証失効リスト（CRL）や証明書停止にかかわる他の証明書ステータスのアップデートを開示された認証局の要件に従い実施する。 2.2.7.7 証明書は、開示された認証局の要件従い、許容された時間だけ停止する。 2.2.7.8 証明書が停止されると、停止は以下の3つの方法の1つで扱われる。 a．停止されている証明書のエントリはCRLに残っており、ホールド期間中はトランザクションの発生が拒絶される b．停止した証明書のCRLエントリは、同じ証明書の失効エントリに取って代わる c．停止証明書が開放されて、CRLからエントリが取り除かれる 2.2.7.9 証明書停止エントリは、古いものであっても、証明書の期限か停止の期限までCRLに残っている。 2.2.7.10 認証局は開示された認証局の要件に従い、証明書失効リスト（CRL）や証明書停止の取消しにかかわる他の証明書ステータスメカニズムのアップデートを行う。 2.2.7.11 認証局は、外部登録局がエンティティの身元確認や証明書停止の取消し要求の確認をするよう要求し、検証する。 2.2.8.1 証明書ステータス情報は、開示された認証局の要件に従い、関連するすべてのエンティティが参照できるようにする。 2.2.8.2 認証局は発行されたCRLを確立されたメカニズム（例えばディレクトリのようなリポジトリ）を用いて検証者が参照できるようにする。 2.2.8.3 認証局は、エンティティがCRLの完全性と発行日を確認できるよう、CRLにデジタル署名をする。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
25				2.2.8.4 認証局は、開示された認証局の要件に従い、最後の発行から何も変更されていなくとも一定の間隔でCRLを発行する。 2.2.8.5 少なくとも、証明書の有効期限までは取り消された証明書はCRLに記載される。 2.2.8.6 証明書の停止がサポートしている場合、証明書の通常の有効期限まで証明書停止はCRLに記載される。 2.2.8.9 CRLには、認証局によって発行された有効期限満了前に失効された証明書のすべてが記録される。 2.2.8.10 古いCRLは、開示された認証局の要件に従って一定期間保管される。 2.2.8.11 証明書は、期限切れ、失効、停止に関らず、開示された認証局の要件に従って、コピーを一定期間保管する。 2.2.8.12 オンライン証明書ステータスメカニズム（例えばOCSP）が使用されている場合、認証局は開示された認証局の要件に従って、証明書ステータス問い合わせ（例えばOCSP要求）にすべての要求されるデータが含まれていることを要求する。 2.2.8.13 下記の場合、検証者からの証明書ステータス要求（例えばOCSP要求）を受け取った場合、認証局は検証者に最終的に返答をする： a．要求メッセージが適切な形式である b．レスポンダーは要求されるサービスを行うためのものであり、かつ c．要求は、レスポンダーによって必要とされる情報が含まれる 2.2.8.14 最終的な応答メッセージは、開示された認証局の要件に従ってデジタル署名される。 2.2.8.15 最終的な応答メッセージは、開示された認証局の要件に従って、すべての要求データが含まれている。 2.2.8.16 （2.2.8.13の）3つの状態のどれにも当てはまらない場合、認証局は署名を付けた（付けていない）エラーメッセージを送信する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
26	4.5.　セキュリティ監査の手続 セキュアな環境を維持するために実装されるイベントロギングと監査システムに関する要件 4.5.1.　記録されるイベントの種類 4.5.2.　監査ログの処理頻度 4.5.3.　監査ログの保存期間 4.5.4.　監査ログの保護 ・誰が監査ログを見ることができるか ・監査ログの改ざんに対する防護措置 ・監査ログの削除に対する防護 4.5.5.　監査ログのバックアップ 4.5.6.　監査ログの収集システム 4.5.7.　イベントを引き起こした人への通知 4.5.8.　セキュリティ対策の見直し	3.6.2　監査情報の定義 監査情報とは、認証局のCPS・技術情報・安全対策実施状況・システムイベントの記録等の監査を行うために必要な情報をいう。例えば、監査情報には以下のような情報が含まれる。 ・認証申請の情報：申請書類、申請受付担当者、本人確認手段など ・認証局の鍵管理履歴：生成、ロード、バックアップ、保管、リカバリー、廃棄など ・機密情報のアクセス履歴：機密データの入出力・削除、セキュリティプロファイルの変更、システムダウンと復旧処理、監査情報のアクセス、設備等の入退室など ・受発信データ：認証局が交信したデータ、発行証明書、失効申請など 3.6.3 監査情報の保管 （１）　監査情報は、そのアクセス権限を明確にし、不正アクセスによる情報の改竄、消去、漏洩等に対して保護し、必要に応じ適正な期間内に提供可能な状態で保管しておく必要がある。 （２）監査情報は適正な間隔でバックアップを取り、隔地保管することが望ましい。	(指針第６条第２項第一号）各動作の要求者名、内容、発生日時、結果等を履歴として記録する機能 1351 (1) 履歴記録に関する以下の(2)、(3)を含む認証業務用設備に対するセキュリティ基準が文書として規定され、それにかなった認証業務用設備が設置されている。 1352 (2) 認証業務用設備単位に記録する操作履歴等が明確に規定され文書化されている。 1353 (3) 上記記録には、以下の項目が含まれている。 ① 各イベントを起こした者の識別 ② 各イベント要求の発行先（例えば、端末IDなど） ③ 各イベントの種類（ファイルのオープン、クローズ、名前変更、属性変更、削除など） ④ 各イベント発生日時 ⑤ 各イベントの成否 (指針第６条第２項第二号） 特定の操作者による操作の履歴のみを表示することができる機能 1361 (1) 以下の(2)を含む認証業務用設備に対するセキュリティ基準が文書として規定され、それにかなった認証業務用設備が設置されている。 1362 (2) 認証機能を提供するアプリケーションが生成する履歴記録に関して、任意の操作者の操作履歴が表示できる。	2.2.1.12 外部登録局を使用する場合、認証局は外部登録局に、イベントジャーナルに行動の記録をするよう要求する。 2.2.6.6 認証局は、すべての証明書失効要求とそれらの結果をイベントジャーナルに記録する。 2.2.7.12 証明書停止と証明書停止の取消しは、イベントジャーナルに記録される。 3.10.12 システム監査ツールへのアクセスは、不正使用や誤用を防ぐように防御する。 3.10.13 認証局システムの使用を監視するための手続を確立し、監視活動の結果を定期的にレビューする。 3.11.1 認証局は、適宜自動（電子的）や手動でイベントジャーナルを取得する。 3.11.2 すべてのジャーナルエントリは、以下の項目を含める。 a．エントリの日付と時間 b．エントリのシリアルか連続番号 c．エントリの種類 d．エントリのソース(例えば、端末、ポート、位置、カスタマ) e．ジャーナルエントリを作成したエンティティの識別子

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
26				3.11.3 認証局は、下記のような鍵ライフサイクル管理に関連するイベントを記録する。 a．認証局（利用者）の鍵生成 b．手動での暗号化鍵のインストールとその結果（オペレータの識別子） c．認証局（利用者）の鍵保管 d．認証局（利用者）の鍵バックアップ e．認証局（利用者）の鍵回復 f．認証局（利用者）の鍵エスクロウ g．認証局の鍵の使用 h．認証局（利用者）の鍵のアーカイブ i．サービスからの鍵の失効 j．認証局（利用者）の鍵配送 k．キー管理操作を認可するエンティティの識別子 l．鍵が格納されている素材（鍵コンポーネントや鍵が格納されている装置・メディア）を使用したエンティティの識別子 m．鍵の管理、装置の管理、鍵の入ったメディアの管理 n．私有鍵の危殆化 3.11.4 認証局は、下記のような証明書ライフサイクル管理に関連するイベントを記録する。 a．証明書要求の受付-初期の証明書要求、更新要求、鍵の再要求を含む b．証明書のための公開鍵の送付 c．エンティティの加入の変更 d．証明書の発行 e．認証局公開鍵の配布 f．証明書失効要求 g．証明書停止要求 h．証明書失効リスト（CRL）の作成と発行 i．証明書の有効期限切れによる操作 3.11.5 認証局は、下記のような暗号化装置ライフサイクル管理に関連するイベントを記録する。 a．装置の受領 b．ストレージからの装置の入力、除去 c．装置の使用 d．装置の撤去 e．サービスや修理のための装置の指定 f．装置の廃棄 3.11.6 認証局（登録局）は、下記のような証明書申請情報を記録する。 a．申請者によって提示された身元確認資料の種類 b．ユニークな識別データ、番号、又はそれらの組合せの記録（例えば運転免許番号） c．アプリケーションと身元確認資料のコピーの保管場所 d．アプリケーションを受け付けたエンティティの識別子 e．身元確認資料を使用する方法 f．受け取った認証局と送信した登録局の名前

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
26				3.11.7 認証局は、下記の重大なセキュリティイベントを記録する。 a．機密ファイルやイベントジャーナルへの、リード・ライトの記録 b．機密データの削除 c．セキュリティプロファイルの変更 d．成功、不成功にかかわらず、認証メカニズムの使用 e．システムクラッシュ、ハードウェア障害、その他の異常 f.コンピュータオペレータ、システム管理者、システムセキュリティ監督者が行った作業 g．エンティティの加入の変更 h．暗号化/認証プロセス、手順の回避の決定 i．認証局システムや他のコンポーネントへのアクセス 3.11.8 イベントジャーナルには、私有鍵の平文を記録しない。 3.11.10 使用している及び自動的にアーカイブされたジャーナルは、認められていない改変や破壊をされないよう保護する。 3.11.11 使用している及び自動的にアーカイブされたジャーナルは、変更や置換えされないよう保護する。 3.11.12 イベントジャーナルに署名するための私有鍵は、他の目的には使用しない。 3.11.13 認証局は定期的にイベントジャーナルデータをアーカイブする。 3.11.14 アーカイブされたイベントジャーナルの適切な保存期間を決定するため、リスクアセスメントを実行する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
26				3.11.15 認証局は、決められた期間、安全な別地の場所へアーカイブされたイベントジャーナルを保存する。 3.11.16 使用している及びアーカイブされたジャーナルは、ビジネス上、セキュリティ上妥当である許可された人員のみ検索できる。 3.11.17 イベントジャーナルは、開示された認証局の要件に従い、定期的にレビューする。 3.11.18 使用している及びアーカイブされたイベントジャーナルは、完全性の確認、検査、例外・無権限・不審な行動のフォローアップのため、レビューを行う。
27	4.6. 記録の保管 一般的な記録のアーカイブ化（若しくはレコード保持）ポリシを記述する。 4.6.1. アーカイブの種類 4.6.2. アーカイブの保存期間 4.6.3. アーカイブの保護 ・ 誰がアーカイブを見ることができるか ・ アーカイブの改ざんに対する防護 ・ アーカイブの削除に対する防護 4.6.4. アーカイブのバックアップ手順 4.6.5. 記録に対するタイムスタンプ要件 4.6.6. アーカイブの収集システム 4.6.7. アーカイブ情報の検証手続	3.3.5 証明書の保存 （１） 発行した証明書の有効期限が切れた後も、改竄、消去、漏洩等の不正なアクセスがなされないような対策を講じて、認証局は一定の期間証明書を保存する必要がある。 3.4.4 失効リストの保存 （１）失効した証明書の当初の有効期限経過後も、認証局は一定の期間失効リストおよび関連するデータを保存しなければならない。	(指針第１２条第１項第九号) 帳簿書類の保存に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3910 (10) 帳簿書類の保存に関する事項 ① 認証業務において保存する帳簿書類の保存期間、保存方法等	2.2.8.7 CRLは開示された認証局の要件に従ってアーカイブする。 3.6.15 リムーバブルメディアは、以下の要件を満たす管理を行う。 a．長期保存の必要がない場合は、組織から持ち出す時に、以前の内容を消去する b．持ち出しに承認を必要とし、監査記録としてすべての持ち出しを記録し保存する。 c．すべてのメディアは、製造メーカの仕様に従った安全な環境に保管する。 3.6.16 必要でなくなったメディアは、安全に処分する。 3.11.9 認証局コンピュータシステムの時計は、正確に記録するため同期化する。
28	4.7. 鍵の再発行 新しい公開鍵を 認証局 のユーザに提供する手続。			

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
29	4.8. 危殆化と業務の継続性の保証 改ざんや災害が起きた場合における通知と復旧の手続に関する要件を記述。			
	4.8.1. コンピューティング資源、ソフトウェア、かつ／又は、データが破壊された、若しくは、破壊されたことが疑われる場合に使用 される復旧手続。これらの手続は、どのようにセキュアな環境は再構築されるか、どの証明書が失効するか、主体の鍵は失効されるのか、どのように新しい主体の公開鍵はユーザに提供されるのか、どのようにサブジェクトは再認証されるのか、を記述します。	3.2.8 鍵の危瀬 （１）認証局は、認証局の私有鍵が内部不正によって漏洩したり、第三者によって私有鍵が解読された場合、さらには災害によって認証局がダメージを受けた場合などの事態に対して、事前に対応策を策定しておく必要がある。 （２）認証局の私有鍵が危瀬した場合、あるいはその可能性がある場合、認証局は速やかに対応する証明書の失効を行う必要がある。	(規則第６条第十五号) 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 (第６条第十五号ト) ト　危機管理に関する事項 3C61 (1) 以下の（２）から（５）に係る規定が、認証業務規程及び事務取扱要領等に規定され、実施される。	2.1.5.3 認証局は、有効期間の終わり又は、私有鍵の危殆化又はそのおそれがある場合には鍵ペアの使用を停止する。 3.9.1 認証局は、事業継続計画を作成、維持していく。 3.9.2 認証局は、リスクアセスメントに基づき、事業継続計画を策定する。
	4.8.2. 主体の公開鍵が失効された場合に使用される復旧手続。 これらの 手続は、どのようにセキュアな環境は再構築されるか、どのよう に新しい主体の公開鍵はユーザに提供されるのか、どのようにサブジェクトは再認証されるのか、を記述します。	（３）認証局の私有鍵が危瀬した場合、その私有鍵で署名した加入者の証明書を失効させ、失効させたことを加入者に通知する必要がある。また、下記の対応を行う必要がある。 ・申請者からの認証要求を見合わせている旨の開示。 ・利用者が認証局の状況確認を行える窓口の設置。		3.9.3 認証局は規定要件に従い、サービスの中断や障害に迅速に対応し、メンテナンスや回復ができるよう事業継続計画を策定する。
	4.8.3. 主体の鍵が改ざんされた場合に使用される復旧手続。 これらの手続は、どのようにセキュアな環境は再構築されるか、どのように新しい主体の公開鍵はユーザに提供されるのか、どのようにサブジェクトは再認証されるのか、を記述します。	（４）認証局の私有鍵の危瀬／災害の事態から復旧する際には下記の対応が必要である。 ・安全な環境に復していることの確認。 ・認証局の鍵と証明書の更新。 ・加入者の証明書の再発行手続き。	3C62 (2) 発行者署名符号の危殆化もしくは危殆化の恐れがある場合の対応策及び回復手順には、以下の項目が含まれている。 ① 当該署名符号を用いて発行した電子証明書の失効 ② 電子証明書利用者への告知、署名検証者への開示及びその方法 ③ 原因及び被害の追求と原因別対応策 ④ 主務大臣への通報	3.9.4 認証局は、以下の点を考慮した事業継続計画のフレームワークを策定する。 a．いかなる事象において計画を実行するか b．非常時の手順 c．フォールバック手順 d．正常操業に復帰するための再開手順 e．計画の見直しスケジュール f．教育啓蒙活動 g．各人の責任
	4.8.4. 天災、若しくは他の災害後、かつ、セキュアな環境が、元のサイト、又は遠隔のホットサイトのいずれかで再構築される前の期間に、認証局が、そのファシリティをセキュアにする手続。 例えば、地震で被害を受けたサイトからの、取り扱いに注意を要する資材の盗難を防護する手続。 天災もしくは災害時における、システム再構築までの資材等の保護要件。	（５）認証局の私有鍵が危瀬していないかを確認するため、証明書の利用状況についてサンプリングなどの方法でモニタリングを行うことが望ましい。 （６）証明書の再発行に当っては、認証局側からの自動再発行はせず、加入者からの再発行要求があった場合にのみ行うのが望ましい。	3C63 (3) 認証業務停止が伴う災害等による障害発生への対応策及び回復手順には、以下の項目が含まれている。 ① 電子証明書利用者への告知、検証者への開示及びその方法 ② 原因及び被害の追求と原因別対応策 3C64 (4) 対応策及び回復手順に従った教育・訓練計画が作成され、就業者の役割に応じた教育・訓練が定期的に実施されている。 3C65 (5) 発行者署名符号の危殆化又はもしくは危殆化のおそれがある場合及び、天災事変等の被災、認証業務用設備の故障等により署名検証者への失効情報の開示が、認証業務規程にて定める時間を超えて停止し、かつ署名検証者が停止を知る方法が無かった場合は、直ちに障害の内容、発生日時、措置状況等確認されている事項を主務大臣に対して通報する。	3.9.5 事業継続計画は、常に最新のものであるか、効果的であるかを確かめるために定期的にテストを行う。 3.9.6 事業継続計画の定期的レビューを行い、常に効果的であるように保つ。 3.9.7 事業継続計画において、開示された認証局の要件に従い、許容される業務停止時間、復旧時間、停止平均時間が定義される。 3.9.8 認証局の事業継続計画には、ハードウェア、ソフトウェア、鍵における復旧プロセスが含まれる。 3.9.9 認証局の事業継続計画は、コンピュータ資源、ソフトウェア、データが改変、又は改変の疑いがある場合の復旧手順を定める。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
29				3.9.10 認証局の事業継続計画は、災害発生前の安全な環境に戻るまでの、ファシリティにおける手続を策定する。 3.9.11 サービス情報や、ソフトウェアのバックアップは開示された認証局の要件に従い、定期的に取得する。それらのコピーのセキュリティ要件は、情報バックアップにおけるコントロールと同様である。 3.9.12 フォールバック装置やバックアップメディアは、開示された認証局の要件に従い、安全な遠隔地へ保管する。 3.9.13 認証局のサービス継続計画に、認証局の署名用私有鍵の危殆化時の対応方針を定める。 3.9.14 認証局私有鍵の危殆化、危殆化のおそれがある場合、災害復旧手順に認証局の私有鍵で署名されたすべての証明書の失効と再発行について定める。 3.9.15 認証局の私有鍵が危殆化した場合、復旧手順に従う。認証局の公開鍵の失効は、以下のことに注意する。 a．どのように安全な環境を再確立するか b．どのように認証局の古い公開鍵を失効させるか c．どのように新しい認証局の公開鍵をユーザに送付するか d．どのように再認証されるか 3.9.16 認証局が認証局ルート私有鍵を変更しなければならない場合、下記に対して、安全で承認された失効の手続をとる。 a．古い認証局ルート公開鍵 b．危殆化した私有鍵に基づき、認証局によって発行されたすべての証明書セット c．すべての下位認証局の私有鍵及び対応する証明書 3.9.17 鍵危殆化時の認証局の事業継続計画には、誰が通知するか、システムソフトウェア、ハードウェア、対称/非対称鍵、生成した署名、暗号化データをどのように使用するか、定めている。 3.9.18 認証局は、認証局終了時、開示された認証局の要件に従って、影響するエンティティへの通知、認証局の記録を管理者へ引き継ぐ手順を整備する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
30	4.9.　認証局の終了 認証局 若しくは 登録局 の終了と終了の通知のための手続に関する要件について記述します。アーカイブ化レコードの対応も含む。	2.7 業務終了 業務終了を加入者等に通知する事 （１）　認証局が何らかの理由により、その業務を終了する場合には、そのスケジュールと手続きを決め、その内容を加入者等直接その影響を受けるものに通知する必要がある。	(指針第１２条第１項第十号) 業務の廃止に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3911 (11) 業務の廃止に関する事項 ① 認証業務を廃止する時の、発行済み電子証明書の失効処理方法、利用者への連絡方法、連絡時期等 (指針第１２条第２項) 前項第十号に掲げる事項には、認定に係る業務を廃止する日（認定の更新を受けない場合においては、認定期間の満了の日。以下同じ。）の六十日前までにその旨を利用者に通知すること（法第十四条第一項の規定により認定を取り消された場合等、やむを得ない場合はこの限りでない。）及び認定に係る業務を廃止する日までに利用者に対して発行した電子証明書について失効の手続を行うことが含まれるものとする。 3A01 (1) 認定認証業務を廃止することとした場合、以下の(2)、(3)を含む利用者への通知、発行済み電子証明書の失効及び廃止後の失効情報の開示等について明確に定め、手段、手順等を含め認証業務規程及び事務取扱要領等に、明記されている。 3A02 (2) 認定の更新を受けない場合等を含め、 認定認証業務を廃止する場合には、60日前までに利用者に通知する。 3A03 (3) 認定認証業務の廃止日迄に、当該認証業務によって発行された全ての電子証明書を失効する。	1.1.40 認証局におけるPMAのみが認証局を終了させることができる。 認証局が終了した場合、発行したすべての証明書を失効させ、証明書の発行を停止する。 認証局はサービス終了1ヶ月以上前に利用者に通知する。 終了時、認証局の記録はアーカイブされ、管理者に譲渡される。 1.1.41 パブリックドメイン情報は機密に保存される。機密情報は以下のものである。 ・利用者の私有鍵 ・オペレーションや認証局の管理がわかる情報、セキュリティ設定や監査査証等（法の要求がない限り） ・認証局や登録局が保持している利用者についての情報（証明書ポリシや法の要求がない限り） ・年次監査の結果（認証局管理者により公表が決定されない限り）

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
	5.　建物・関連設備、運用、要員のセキュリティ管理			
31	5.1.　建物及び関連設備管理 認証局のシステムを関連するファシリティについての物理的な統制を記述。 5.1.1.　施設の位置と建物構造	4.4 設備 4.4.1 設備の種類 ・建物立地場所 建物、コンピュータ室は、火災、電磁界、水害、落雷、空気汚染による被害を受ける恐れの少ない場所に設ける事 ・建物の構造 建物は、耐火構造、耐震構造とする事 4.4.2 認証局特有の要件 （1）認証システム設置室の隔離 証明書や個人の審査情報などを扱う証明書発行システムを設置する室（認証システム設置室）は、最低限間仕切りなどで隔離し、その他の業務システムとは別の室に設置する必要がある。	(指針第６条第１項第四号) 認証業務用設備の所在を示す掲示がされていないこと。 1341 (1) 以下の(2)を含む認証業務用設備に対するセキュリティ基準が、文書として規定され、実施されている。 1342 (2) 認証業務用設備を収容する建築物の外部及び建築物内に認証業務用設備の所在を明示又は暗示する名称が、看板もしくは表示板等によって掲示されていない。 例えば、次のような場所に掲示をしていない。 ・認証業務用設備を収容する建築物の外部 ・認証業務用設備を収容する建築物のエントランスの案内板 ・認証業務用設備を収容する建築物のエレベータの案内板 ・認証設備室の入口 ・受付 ・その他のパンフレット、ホームページ等 (指針第７条第二号) 認証設備室　次に掲げる要件を満たすこと。 (指針第７条第二号ロ) ロ　隔壁により区画されていること。 1531 (1) 認証設備室は、容易に破壊されない構造・強度を持った間仕切り壁又は隔壁により事務室等認証設備室以外の室と区分されている。 1532 (2) 間仕切り壁等の隔壁は、侵入が可能となるような開口部を設けず、上部は上階スラブに、下部は床スラブに、それぞれ固定されている。	3.5.1 物理的保護は、認証局 設備の周辺の明瞭に定義されたセキュリティ区画（ 物理的障壁 ）によって行なわれる。 3.5.2 認証局施設のあるビルディング、又は、区画は、侵入が容易におこらないよう物理的に保護される 3.5.3 認証局施設へのアクセスは有人の入場エリアや他の物理的なアクセスコントロールによって、認可された人間だけがアクセスできるようにコントロールする。 3.5.4 無許可の入場や環境汚染を防ぐため、物理的な障壁は真の床から真の天井部まで設置する（隙間がなく、侵入が発生しないような完全な区画制御）。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
31			(指針第７条第三号) 認証設備室を設置する建築物　次に掲げる要件を満たすこと。 (指針第７条第三号イ) イ　建築されている土地の地盤が地震被害のおそれの少ないものであること。ただし、やむを得ない場合であって、不同沈下を防止する措置を講ずる場合は、この限りでない。 1571 (1) 認証設備室を設置する建築物は、地震による被害の恐れの少ない地域に設置されている。やむを得ない場合には、例えばパイル打設等の軟弱な地盤に対する不同沈下防止措置を講じている。 不同沈下に対する対策工法の基本原理には次のようなものがある。 ・締固め工法　　：サンドコンパクション、バイブロフローテーション ・間隙水圧消散工法：グラベルドレーン ・強制圧密脱水工法：ウエルポイント ・固結工法　　：注入工法（グラウト工法）、深層混合処理工法 ・その他　　：置換工法等 (指針第７条第三号ロ) ロ　地震に対する安全性に係る建築基準法（昭和二十五年法律第二百一号）又はこれに基づく命令若しくは条例の規定に適合する建築物であること。 1581 (1) 認証設備室を設置する建築物は、建築基準法に規定する構造耐力等の基準に適合している。 (指針第７条第三号ハ) ハ　建築基準法に規定する耐火建築物又は準耐火建築物であること。 1591 (1) 認証設備室を設置する建築物は、建築基準法に規定する耐火建築物又は準耐火建築物の基準に適合している。	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
32	5.1.2.　入退管理	4.4 設備 4.4.1 設備の種類 ・建物入退室管理 ①窓、扉には防犯措置を講ずる事 ②入退出記録をとり、管理する事 ③入退出に関する管理規定を整備し、管理責任者を決める事 ④入退出者に関する資格審査を行い、識別証により入退出を管理する事 4.4.2 認証局特有の要件 ・認証システム設置室への入退管理 ①生体認証装置による施錠・解錠を行う事 ②入退出に関する管理規定を整備し、管理責任者を決める事 ③認証システム設置室が無人となる場合、センサなどにより不正侵入を検知し、システム管理者などへ通知する対策を講じることが望ましい	(指針第４条第一号) 認証設備室（規則第四条第一号に規定する認証業務用設備を設置する室をいう。ただし、認証業務用設備のうち、もっぱら電子証明書の利用者を登録するために用いられる設備（以下「登録用端末設備」という。）のみが設置されている室を除く。以下同じ。）　次に掲げる要件を満たすこと。 (指針第４条第一号イ) 入室する二以上の者の身体的特徴の識別（あらかじめ登録された指紋、虹彩その他の個人の身体的特徴の照合を行うことをいう。）によって入室が可能となること。 1111 (1) 以下の(2)、(3)の事項を満足する規定が事務取扱要領等に明確に規定され、実施されている。 1112 (2) 認証設備室への入室には、入室する複数人による生体認証装置（身体的特徴を識別する装置）の操作が必要である。 1113 (3) 認証設備室へ入室する者の入室時に生体認証装置によりあらかじめ登録されている者であることが識別・認証された上での入室が可能となっている。	3.2.11 新しい情報処理設備を導入する際の管理許可プロセスが存在し、かつ実施される。 3.2.12 外部委託者、取引業者等を含む第三者による認証局設備やシステムへの物理的アクセス、論理的アクセスを管理するための手続が存在し、実施される。 3.2.13 第三者による認証局設備やシステムへのアクセスが必要な場合、セキュリティ要件、及び、特定のコントロール要求を決定するためにリスク評価を実施する。 3.5.5 セキュリティ区画のすべての防火ドアは監視され、閉じられている。 3.5.6 認証局施設及び、 認証局施設そのものを収容する建物、区画の全ての外部の入口に侵入者検出システムを設置し、定期的にテストする。
		・認証システム設置室の入退出ログ管理 ①入退出記録をとり、管理する事 ②入退出ログは改竄されないよう対策を講じる事 ③ログの内容は定期的に検査する事 ④定期的に入退出の監査を行なう事 ・設備保守方法 ①保守方法の明文化と設備毎の作業員を特定を行う事 ②設備保守要員には当該セキュリティ権限を有する要員の帯同を行う事	(指針第４条第一号ロ) 入室者の数と同数の者の退室を管理すること。 1121 (1) 以下の(2)(3)の事項を満足する規定が、事務取扱要領等に明確に規定され、実施されている。 1122 (2) 入室者と同数の複数人の退室操作により退室完了状態となり、退室者数が入室者数と同人数であることが確認できる。 1123 (3) 退出完了後、認証設備室内はモーションセンサを働かせるなどで、無人の認証設備室内で何かの動きを検出した場合に警報を発せられる。	3.5.7 認証局施設が無人である場合、監視する。 3.5.8 無人時は、 認証局施設は物理的にロックされ、定期的にチェックされる。 3.5.9 セキュアな認証局施設における管理されていない作業は、安全のためと悪意の行動を防ぐために許可されない。 3.5.10 全ての人員に識別証を着用させる。 3.5.11 認証局施設へのアクセスは、開示された認証局の要件に従った認可のコントロールにより、認可された要員にのみ許される。 3.5.12 認証局施設への要員の入退場は、すべて記録される（すべてのアクセスの監査証跡を記録するため）。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
32			(指針第４条第一号ハ) 入室のための装置の操作に不正常な時間を要した場合においては、警報が発せられること。 1131 (1) 以下の(2)～(3)の事項を満足する規定が、事務取扱要領等に明確に規定され、実施されている。 1132 (2) 入室操作に要する時間（扉が開いている時間を含む）及び試行回数を設定し、登録している。 入室操作に要する時間とは、例えば認証精度（本人拒否率、他人受入率）、生体認証装置の照合スピード及び認証精度を満たすのに必要な照合処理の試行回数（生体認証の不安定性を考慮して、複数回の試行を許可する必要がある）を考慮した時間（すなわち許容できる入室操作時間）を指している。 1133 (3) 入室操作において、(2)で設定し、登録した時間または試行回数を超えた場合は、常時（２４時間）人のいる場所に警報を発する。もしくは、入室操作の実施状況を遠隔監視装置で常時(24時間)モニタリングし、異常な行動が見られた場合にはただちに対応できる体制が整っている。 (指針第４条第一号ニ) 入室者及び退室者並びに在室者を自動的かつ継続的に監視し、及び記録するための遠隔監視装置及び映像記録装置が設置されていること。 1141 (1) 以下の(2)～(7)までの事項を満足する規定が、事務処理要領等に明確に規定され、実施されている。 1142 (2) 認証設備室への入退者及び在室者の撮影に死角ができないような位置に遠隔監視カメラを設置している。やむなく、撮影に死角が存在する場合、その場所に位置しないように、また、その場所に位置する者がいないことをチェックするように認証設備運用要員に対する教育がなされている。 1143 (3) 1週間分以上の映像が記録できる映像記録装置を設置している。	3.5.13 部外者の認証局施設への入場は、入場時間、退場時間が記録され管理される。 3.5.14 サポートサービスを行う第三者要員の認証局施設へのアクセスは、要求があり、かつそのアクセスが認められ監視できる場合のみに制限される。 3.5.15 認証局 施設へのアクセス権利は、定期的に再検討されて、アップデートされる。 3.5.16 装置は、環境上の脅威及び危険、不正アクセスから危険を減少させるように設置、若しくは保護される。 3.5.23 装置、情報、及び、所有するソフトウェアは、許可なしでオフサイトへ持ち出せない。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
32			1144 (4) 遠隔監視装置で認証設備室への入退者及び在室者が常時（24時間）撮影並びにモニタ表示されている。または、侵入検知センサ等と遠隔監視装置を連動させることで、入退者及び在室者が存在する場合だけを自動的かつ継続的に監視及び記録している。 1145 (5) 映像記録装置の記録媒体の交換時におけるブランクが生じないようにしている。やむを得ない場合、記録媒体の交換は、認証設備室への入室者及び在室者が居ないことを確認しながら、速やかに行っている。 1146 (6) 遠隔監視カメラで撮影している映像及び記録された映像は被写体が明確に確認できる。 ※（1147は5.1.3の項に記載） (指針第４条第二号) 登録用端末設備が設置される室であって、認証設備室に該当しないもの　関係者以外が容易に登録用端末設備に触れることができないようにするための施錠等の措置が講じられていること。 1151 (1) 以下の(2)(3)の事項を満足する規定が、認証業務規程及び事務取扱要領等に明確に規定され、実施されている。 1152 (2) 登録用端末設備を設置する室の出入口には錠を取付けてあり、無人の際には施錠されている。 1153 (3) 登録用端末設備を設置する室においては、登録用端末設備が設置されている場所は間仕切りで登録用端末設備以外の区画と区分する等により、関係者以外が容易に登録用端末設備に触れる事ができないような措置を講じている。 (指針第１３条第二号) 設備の保守その他の業務の運営上必要な事情により、やむを得ず、立入りに係る権限を有しない者を認証設備室へ立ち入らせることが必要である場合においては、立入りに係る権限を有する複数の者が同行すること。 3D21 (1) 認証設備室への入室について(2)、(3)の事項が明確に定められ、方法、手続き等が認証業務規程及び事務取扱要領に規定され実施されている。 3D22 (2) 入室権限を有しない者を入室させるケース及びその時における権限を有する複数の者の同行が規定されている。 3D23 (3) 上記(2)とおりに実施されているかが日常チェック、監督されている。	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
33	5.1.3.　電源及び空調設備	4.4 設備 4.4.1 設備の種類 ・電源設備 ①避雷措置、防火、耐火措置等の防災措置及び防犯措置を講ずる事 ②電圧、周波数等の安定した電力を供給できる措置を講じておく事 ③電源系統の２系統化、蓄電池の併用等による停電対策を講じる事 ④災害時等の継続的停電の対策として、自家発電設備を設置する事 ・空調設備 ①防火、耐火、漏水対策等の防災措置及び防犯措置を講ずる事 ②適切な室内空調を安定して提供できる事	(指針第４条第一号) 認証設備室（規則第四条第一号に規定する認証業務用設備を設置する室をいう。ただし、認証業務用設備のうち、もっぱら電子証明書の利用者を登録するために用いられる設備（以下「登録用端末設備」という。）のみが設置されている室を除く。以下同じ。）　次に掲げる要件を満たすこと。 (指針第４条第一号ニ) 入室者及び退室者並びに在室者を自動的かつ継続的に監視し、及び記録するための遠隔監視装置及び映像記録装置が設置されていること。 1141 (1) 以下の(2)～(7)までの事項を満足する規定が、事務処理要領等に明確に規定され、実施されている。 1147 (7) 遠隔監視装置及び映像記録装置には停電時対応のためのUPS等を設置している。 (指針第７条第二号) 認証設備室　次に掲げる要件を満たすこと。 (指針第７条第二号ホ) ホ　室内において使用される電源設備について停電に対する措置が講じられていること。 1561 (1) 認証設備室において使用される認証業務用設備及び入退出管理装置には、UPS（無停電電源装置）又はCVCF（定電圧定周波装置）と蓄電池を設置している。	3.5.17 装置は、停電や他の電気異常から保護される。 3.5.18 認証局 サービスをサポートする電源及びデータを送信する通信ケーブルは、遮断や破損から保護する。 3.5.19 装置は可用性、完全性を確保できるようメーカの指示や文書化された手続に従って維持管理される。
34	5.1.4.　水害及び地震対策		(指針第７条第一号) 認証業務用設備　通常想定される規模の地震による転倒及び構成部品の脱落等を防止するための構成部品の固定その他の耐震措置が講じられていること。 1511 (1) 認証設備室内に設置される認証業務用設備に対しては以下のいずれかの地震による移動・転倒防止対策が講じられている。 ① 認証業務用設備が設置してある室のフロアレスポンスに応じて、認証業務用設備メーカの推奨する設置方式を考慮した移動・転倒防止等の措置が講じられている。 ② 耐震脚、転倒防止金具等で建物構造体に固定されている。 ③ 建築物全体、認証業務用設備が設置してある床等が免震構造を持つ、もしくは、認証業務用設備が免震台により支持されている。この場合、その効力を証明する認定書（原本又はその写し）を所持している。	3.5.16 装置は、環境上の脅威及び危険、不正アクセスから危険を減少させるように設置、若しくは保護される。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
34			1512 (2) ラックは例えば建物構造体への固定等により移動、転倒防止措置が講じられている。 1513 (3) 認証業務用設備の構成部品は、例えば、落下防止金具や耐震バンド等で固定されている。 1514 (4) フリーアクセスフロアは地震で損壊しないよう例えば、アングルやストリンガー等の補強措置が講じられている。 1515 (5) 地震の際に認証業務用設備に被害を与えないよう、認証業務用設備室内の什器・備品等に耐震措置が講じられている (指針第７条第二号) 認証設備室　次に掲げる要件を満たすこと。 (指針第７条第二号イ) イ　水害の防止のための措置が講じられていること。 1521 (1) 認証設備室が設置されている建築物及び認証設備室について水害、火災、地震等の災害への対策を規定した文書が作成されている。 1522 (2) 次の①または②のいずれかを満足している。 ① 認証設備室を建築物の2階以上に設置する。 ② 認証設備室を建築物の1階以下に設置する場合には水害に対して十分な対策を講じる。特に、過去に出水被害がある場合又は海抜ゼロメートル地帯等である場合には、浸水対策を講ずる。 1523 (3) 直上階の床板にアスファルトやウレタン系防水塗料を塗布する等の防水施工を講じている。防水施工が困難な場合は直上階床板下面のはり及び柱の周辺に全面検知型の漏水センサを設置し、室内に防水カバーを常備している。 1524 (4) 認証設備室には流し台、給茶機等の水使用設備は設置しない。 1525 (5) 認証設備室に空気調和機を設置する場合は、空気調和機の周辺に防水提又は水受け皿等を設置し、かつ防水提又は水受け皿等の内側に漏水センサを設置している。 1526 (6) 漏水監視は中央監視盤等により常時行っている。	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
34			(指針第７条第二号ハ) ハ　自動火災報知器及び消火装置が設置されていること。 1541 (1) 認証設備室には、消防法施行令に規定した自動火災報知器及び消火装置を設置し、消防署等の検査を受け、定期点検を実施している。 (指針第７条第二号ニ) ニ　防火区画内に設置されていること。 1551 (1) 認証設備室又は認証設備室を含む区画は建築基準法に規定する防火区画である。 1552 (2) ケーブルが防火区画を貫通する場合は、当該ケーブルが貫通する部分及び貫通する部分から両側1m以内の部分は不燃材料等による延焼防止措置を講じている。 1553 (3) 換気、暖・冷房のダクトが防火区画を貫通する場合は、ダクトの防火区画を貫通する部分又はこれに近接する部分に防火上有効なダンパを設けている。	
35	5.1.5.　防火設備			
36	5.1.6.　記録媒体の保存		(規則第６条第十五号) 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 (第６条第十五号へ) へ　利用者の真偽の確認に際して知り得た情報の目的外使用の禁止及び第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置 3C55 (5) 以下の(6)に関する事項を含む規則第12条第1項各号に揚げる帳簿書類の保護が、認証業務規程及び事務取扱要領等に規定され、それに従って帳簿書類の保護がなされている。 3C56 (6) 各記録は滅失又はき損防止のため、次の要件を満足する。 ① 共通要件 ・各記録は、施錠可能な出入口を持ち、間仕切り又は壁等によって区分された室の中に保存する。 ・各記録が保存される室には、自動火災報知器及び消火装置が備えられている。 ・各記録は直射日光が直接当たらない場所に保存するか、直射日光が当たらないよう、遮蔽措置を講ずる。	3.5.21 機密情報又は重要なビジネス情報は厳重に管理される。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
36			② 原本で保存される資料等における追加要件 ・原本上の記録が判読不能とならない環境を備えている。 ・専用のファイルにとじ込む。 ③ 電磁的記録で保存される記録における追加要件 ・横積等により記録媒体の変形を防ぐため、適切なケースに収容する。 ・特に磁気媒体で保存されている記録は、CRT等磁気的影響がある場所に保存しない。 ・当該記録媒体の内容を表示することが出来るように、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを維持・保存しておくこと。特に、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを更新する場合は、当該記録媒体との互換性を確保すること等により、表示不能を生じさせないこと。 ・媒体の特徴に合わせて適宜記録し直すなどの措置が実施されるようになっている。ただし、その際、保存内容の完全性・機密性を損なわない方法でなされている。	
37	5.1.7. 廃棄物の処理			3.5.20 記録媒体（ハードディスク）を含むすべての機材は、廃棄又は再利用される前に機密情報がないか確認する。機密情報を含む記録媒体は、廃棄又は再利用する前に物理的破壊又は安全に上書きする。
38	5.1.8. オフサイト・バックアップ			
39	5.2. 手続管理 信頼される役割、各役割の義務及び必要人数を記述。	2.3.3 組織体制 認証局の運用に関わる組織の体制としては、以下が必要である。 （1）クリティカルデータに接触可能な部署は他から隔離されている事 （2）事故を未然に防ぐために、部署内での内部牽制が行われる事 （3）部署外からの監査等のチェック機能が働く事 （4）事故発生時に、その発生源が特定できる事		3.7.1 アクセスコントロールにおけるビジネス要件を定義し、以下の項目を含めたポリシ文書を策定する。 a．役割と対応するアクセス許可 b．各ユーザの識別と認証 c．職務の分離 d．特定の認証局業務で要求される人数 3.7.2 認証局の情報システムとサービスのアクセス許可のため、正規のユーザ登録と抹消の手続を規定する。 3.7.3 特権の割り当てと使用は制限され、管理される。 3.7.5 ユーザのアクセス権限を定期的にレビューする。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
40	5.2.1.　信頼される役割	2.3.1 独立性／第三者性 （1）認証局の安全性と信頼性を長期的に確保するためには、特定の企業・機関・組織の短期的／自己戦略的な影響からできるだけ独立しており、また第三者的に公平な立場を保持できることが望まれる。 （2）利用者の利便性を高めるために複数の認証局が相互に接続し合う場合には、異なる認証局相互の利用者の信頼を得るうえでも、できるだけ第三者性を高めることが望ましい。 2.3.2 専門性 （１）　安全性と信頼性の高い運用を持続的に行い、また技術進歩に適切かつ充分に対応していくため、さらにはトラブル等に迅速に対応するためには、情報セキュリティ技術やシステム監査等の専門家を配置しておくことが必要である。 特に、認証サービス自体がまだ揺籃期にある現在、未知や想定外の問題が惹起する可能性が高く、そのような問題に迅速に対応していくためには専門的な知識やスキルを有する要員を確保しておくことが必要である。	(規則第６条第十五号) 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 (第６条第十五号ロ) ロ　業務に従事する者の責任及び権限並びに指揮命令系統 3C11 (1) 認証業務就業者について、指揮命令系統、責任及び権限が、内部牽制を考慮した上で文書に明確に定められ、それに従って業務が実施されている。 3C12 (2) 認証業務における指揮命令系統、責任及び権限について、全ての就業者の役割に応じて教育・訓練計画等が策定され教育・訓練がそれに沿って実施されている。 3C13 (3) 指揮命令系統、責任及び権限に変更がある場合、規程等の変更手順等が明確に定められ、それに従って変更が行われる。また、変更に係る教育・訓練が全ての就業者の役割に応じて実施されている。	
41	5.2.2.　必要とされる人数		(規則第６条第十五号) 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 (第６条第十五号ホ) ホ　業務に係る技術に関し充分な知識及び経験を有する者の配置 3C41 (1) 認証業務の遂行に際して事務取扱要領等で電子署名技術、鍵管理技術、セキュリティ技術等に関する業務遂行上に必要な知識、経験それらを有している技術者の必要数が規定され、認証業務に配置されている。 (指針第１３条第一号) 認証設備室への立入りは、複数の者により行われること。 3D11 (1) 認証設備室への入室について (2)、(3)の事項が明確に定められ、方法、手続き等が認証業務規程及び事務取扱要領に規定され実施されている。 3D12 (2) 認証設備室への入室が許可されている者の指定、登録及び複数人による入室がなされている。 3D13 (3) 上記(2)とおりに実施されているかが日常チェック、監督されている。	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
42	5.2.3.　役割ごとの識別と本人認証		(指針第６条第１項第一号) 認証業務用設備を作動させる権限を操作者ごとに設定することができること。 1311 (1) 以下の(２)を含む認証業務用設備に対するセキュリティ基準が文書として規定され、それにかなった設備が設置されている。 1312 (2) 認証業務用設備に対するアクセス権限は、操作者単位に設定できる。 (指針第６条第１項第二号) 認証業務用設備を作動させるに当たっては、操作者及びその権限の確認を行うことができること（登録用端末設備から認証設備室内に設置されている電子計算機に情報の送信が行われる場合においては、認証設備室内に設置されている電子計算機において登録用端末設備の操作者及びその権限の確認を行うことができるものに限る。）。 1321 (1) 以下の(2)～(4)を含む認証業務用設備に対するセキュリティ基準が、文書として規定され、それにかなった設備が設置されている。 1322 (2) 認証業務用設備へのアクセスには、例えばパスワード等の本人しか知りえない情報による操作者の認証または電子署名による操作者の認証、または生体認証等による操作者確認が行える機能を備え、操作者が特定できる。 1323 (3) 操作者の認証の際には、予め設定されたアクセス権限の確認を行う機能を備えている。 1324 (4) 登録用端末設備においては、接続されている認証業務用設備が上記適合例(2)(3)の機能を備えている。	
43	5.3.　要員のセキュリティ統制 5.3.1.　認証局における人事上のセキュリティ管理 ・要員に要求される経歴チェック ・身分証明手続	2.3.4 人事管理 （1）　認証局の信頼確保のために信頼できる人材が運用にあたる必要がある。そのためには採用において適切な人物審査を行う必要がある。 （2）　実際の運営にあたり、メンタルヘルス・健康管理・適正な処遇等における継続した人事管理を行う必要がある。		3.4.1 組織のセキュリティポリシに従って、指定されたセキュリティ上の役割、及び、責任は、職務記述書において文書化される。 3.4.2 常時スタッフの身元確認は、ジョブの任命時に行なわれる。 認証局のポリシや手続には、信頼されるべき役割を果たす要員だけでなく用務員も含めた他の要員にも要求される、素性調査や採用手続を明確に規定する。 3.4.3 従業員は雇用時に秘密保持契約に署名する。 3.4.6 鍵管理や証明書管理等の役割を担う全ての要員の継続的な信頼性について、定期的に検証する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
44	5.3.2.　背景調査			
45	5.3.3.　トレーニング要求 ・ トレーニング要件 ・ 役割ごとのトレーニング手続		(規則第６条第十五号) 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 (第６条第十五号イ) イ　業務の手順 3C01 (1) 認証業務の手順の細目が明確に、事務取扱要領に規定され、実施されている。 3C02 (2) 全ての就業者の役割に応じた教育・訓練計画が策定され、教育・訓練が計画に沿って実施されている。 3C03 (3) 業務の手順等に変更がある場合、遅滞なく、事務取扱要領の必要な箇所が変更され、その変更に係る教育・訓練が各就業者の役割に応じて実施されている。 3C04 (4) 業務内容、手順等の変更に伴う事務取扱要領の改訂に関する手順等を明確に定めた規定が明確に規定され、実施されている。	3.2.2 セキュリティポリシは、情報セキュリティ、その全体の目的、及び、有効範囲、及び、情報シェアリングのための適用メカニズムとしてのセキュリティの重要性の定義を含む。 3.2.3 セキュリティポリシは、管理目的、目標、情報セキュリティの方針を含める。 3.2.4b セキュリティポリシは下記を含む。 b.セキュリティ教育の要求
46	5.3.4.　再トレーニング期間と手続			3.4.5 組織及び関連する第三者等全ての従業員は、組織の方針、手続により適切な教育を受ける。認証局の方針と手続は、下記を規定する。 a．各役割の教育要求、手続 b．各役割の再教育期間と再教育手続
47	5.3.5.　ジョブローテーションの頻度と順序			3.4.8 コントロール、及び、セキュリティが損なわれないように、従業員が退職、解任する時は、適切で、タイムリーな対応を行う。
48	5.3.6.　認可されていない行為に対する制裁			3.4.7 正式の懲罰プロセスは、組織上のセキュリティポリシや手続に違反した従業員に行なわれる。認証局のポリシ及び手続は、許可のない操作、許可のない認証局の利用、許可のないシステムの利用に対し制裁を規定する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
49	5.3.7.　契約要員に関する要件 ・ 契約要員の監査と監視 ・ 要員と契約する際の他の統制		(規則第６条第十五号) 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。 (第６条第十五号ハ) ハ　業務の一部を他に委託する場合においては、委託を行う業務の範囲及び内容並びに受託者による当該業務の実施の状況を管理する方法その他の当該業務の適切な実施を確保するための方法 3C21 (1) 業務の一部を他の認証事業者に委託して実施する場合、業務委託に係る手順及び以下の（２）～（３）に関する事項が、事務取扱要領等に明確に規定され、実施されている。 業務委託する場合、その範囲は業務の一部に限定される。業務の一部とは、利用者の真偽の確認に係る業務、認証業務の管理・運用に係る業務、帳簿の保存に係る業務等である。 3C22 (2) 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委託者の指示の遵守及び責任分担、保証等について明確にする。 3C23 (3) 委託業務に関して受託者からの定期的な報告を受けること等により、業務が適切に行われていることを管理する。	3.2.14 第三者による認証局設備やシステムへのアクセスを含む協定は、全ての必要なセキュリティ要求を含む正式契約に基づく。 3.2.15 すべての又はいくつかの情報システム、ネットワーク、デスクトップ環境の外部委託管理、コントロールにおける 認証局 のセキュリティ要求は、当事者同士が同意した契約において扱われる。 3.4.4 契約社員のコントロールには以下の項目を含める。 a．外部委託契約 b．損害賠償誓約 c．監査及び監視 3.6.5 外部の設備管理サービスを利用する前に、リスクを明確にし、契約業者とコントロールに関する同意事項を契約に明記する。
50	5.3.8.　担当者に提供されるべき文書	2.3.5 事務取扱要領等の規定 認証局のポリシーを実務として遂行していくためには、作業項目や手続き、さらにはコンテンジェンシープラン等について、具体的作業が正確に行えるようにマニュアル等を整備し、それらが適正に実施されるようマネージメントすることが必要である。特に以下の観点から、ポリシーに準じた厳密な事務取扱要領等を規定しておく必要がある。 （１）セキュリティの対象となる場所へのアクセス ・入退館、入退室管理 ・施錠、鍵の管理 ・監視装置等へのアクセス　　等 （２）セキュリティの対象となる機器類（端末等）へのアクセス ・端末使用権限 ・カード、キー等の保管　　等 （３）セキュリティの対象となる情報へのアクセス ・情報のセキュリティレベル ・アクセス権限付与 ・媒体類の取扱い（持込み、持出しを含む） ・ドキュメント類の管理　　等		3.2.1 経営者側によって決定した情報セキュリティポリシドキュメントはすべての従業員に公開し通知する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
	6. 技術的なセキュリティ管理			
	発行認証局 の暗号鍵とアクティヴェーションデータ（例、PIN、パスワード、若しくは相互保有される共有鍵）を防護するために認証局 によって採用されるセキュリティ手段を規定する。 また、セキュアな鍵生成の機能、ユーザの本人認証、リポジトリ、サブジェクト 認証局、登録局、エンドエンティティについての他の技術的なセキュリティ統制を規定するのにも使用する。			
51	6.1. 鍵ペアの生成と実装 6.1.1. 鍵ペアの生成主体	3.2.1 鍵の生成 （1）鍵ペアや共通鍵の生成は、信頼できる暗号鍵生成システムを利用して行なう必要がある。なお、暗号鍵生成システムの機能は、暗号鍵管理モジュールの内部に実装されていることが望ましい。 （2）鍵ペアや共通鍵の生成は、複数人管理のもとで行う必要がある。なお、複数人管理では、メンバーを異なる組織の権限を有する者から構成することが望ましい。 3.2.2 鍵の保管 （1）暗号鍵生成システムによって生成された鍵は、暗号鍵管理モジュール内に保管する必要がある。 3.2.9 認証局の公開鍵の管理 （1）認証局は生成した鍵ペアの公開鍵に対して、上位認証局が存在する場合にはその上位認証局から証明書を取得するか、存在しない場合には自らの私有鍵で署名した証明書を作成する必要がある。	(規則第６条第三号) 利用者が電子署名を行うために用いる符号（以下「利用者署名符号」という。）を認証事業者が作成する場合においては、当該利用者署名符号を安全かつ確実に利用者に渡すことができる方法により送付し、かつ、当該利用者署名符号及びその複製を直ちに消去すること。 3301 (1) 認証事業者が、利用者署名符号の生成を行う場合は、以下の（2）～（5）を含む利用者署名符号生成と利用者への受け渡しについての基準、方法、手順等が明確に認証業務規程及び事務取扱要領等に規定され、それらに従って利用者署名符号の生成が実施されている。 3302 (2) 利用者署名符号の生成は、認証設備室内又は同等の安全性が確保できる環境で行われる。また、その生成は、複数人で行われる。 3303 (3) 利用者署名符号を符号生成装置から取り出した後、利用者に手渡されるまでに経由した装置、通信回線を構成する装置等にあっても当該利用者署名符号及び関連情報が残らないように完全に廃棄、もしくは消去される。 (指針第１４条第一号) 発行者署名符号の生成及び管理は、認証設備室内で複数の者によって規則第四条第四号に規定する専用の電子計算機を用いて行われること。 3E11 (1) 以下の(2)～(4)までの事項について明確に認証業務規程及び事務取扱要領に規定され、実施されている。 3E12 (2) 発行者署名符号の生成は、複数人によって行われかつその内の１名だけでは生成されない方法によって行われている。 3E13 (3) 発行者署名符号の生成は認証設備室内で行われている。 3E14 (4) 発行者署名符号の生成は暗号装置を用いて行われている。	2.1.1.1 認証局の署名用私有鍵は、開示された認証局の要件に従い、ISO 15782-1/FIPS 140-1/ANSI X9.66が要求するレベルを満たす安全な暗号化装置に保管する。 2.1.1.2 認証局による認証局の鍵生成は、権限の与えられた作業者によるデュアルコントロールで行う。 2.1.1.3 認証局は、使用する暗号化装置にて認証局自身のキーペアを生成する。若しくは、キーペアは、それが使われるであろうデバイスに、キーペアが生成されたデバイスから直接格納される。 2.1.9(利用者の鍵を認証局が生成する場合) 認証機関は、認証局（登録局）が規格に従い適切に申請者の鍵を生成しているかを保証するためのコントロールを導入する。 2.1.9.6(利用者の鍵を認証局が生成する場合) 申請者の鍵生成は、開示された認証局の要件に承認された作業者が行う。 2.1.9.9(利用者の鍵を認証局が生成する場合) 認証局は、利用者のみにしか私有鍵が開示されないことを保証する。 2.1.9.12(利用者の鍵を認証局が生成する場合) 利用者の私有鍵の完全性を保証するため、バックアップや回復のコントロールを導入する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
52	6.1.2.　利用者への私有鍵の送付方法		(規則第６条第三号) 利用者が電子署名を行うために用いる符号（以下「利用者署名符号」という。）を認証事業者が作成する場合においては、当該利用者署名符号を安全かつ確実に利用者に渡すことができる方法により送付し、かつ、当該利用者署名符号及びその複製を直ちに消去すること。 3301 (1) 認証事業者が、利用者署名符号の生成を行う場合は、以下の（２）～（５）を含む利用者署名符号生成と利用者への受け渡しについての基準、方法、手順等が明確に認証業務規程及び事務取扱要領等に規定され、それらに従って利用者署名符号の生成が実施されている。 3304 (4)生成された利用者署名符号は、例えば、手交もしくは電子署名及び暗号化通信等による安全な方法で利用者本人に渡され、利用者から自署又は電子署名が付された受領書を受け取る。	2.1.9.7(利用者の鍵を認証局が生成する場合) 開示された認証局の要件に従い、認証局又は登録局は申請者の鍵ペアを安全に配布する。 2.1.9.10(利用者の鍵を認証局が生成する場合) 認証局は、すでに送付した利用者の私有鍵のコピーを保持しない。
53	6.1.3.　認証局への利用者の公開鍵の送付方法			2.2.1.8 認証局は要求しているエンティティに、署名付メッセージによって公開鍵を送付することを要求する。認証局は、登録要求に含まれる公開鍵に対応する私有鍵によって、登録要求にデジタル署名することを要求する。 a．認証アプリケーションプロセスにおいてエラーを検知するため。 b．登録された公開鍵に対応する私有鍵を持っていることを証明するため。
54	6.1.4.　利用者への認証局公開鍵の配布			2.1.3.1 認証局は、初期配布プロセスにおいて、認証局の公開鍵の改ざんを検出できるようなメカニズムを提供する。(公開鍵を配布する際、改ざんされないような対策を取る) 2.1.3.2 認証局の公開鍵の初期配布メカニズムは、開示された認証局の要件に従いコントロールされる。 2.1.3.3 認証局公開鍵の初期配布は、開示された認証局の要件に従い、下記のいずれかを使用する。 a．読み出し可能メディア（例えばスマートカード） b．暗号化モジュールへの組み込み c．他の安全な方法 2.1.3.5 認証局の公開鍵の再配布メカニズムは、開示された認証局の要件にコントロールされる。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
54				2.1.3.6 エンティティがすでに認証局公開鍵のコピーを認証している場合、新しい認証局公開鍵は開示された認証局の要件に従い、以下のいずれかの方法で配布する。 a．認証局から直接、電子的に送付 b．リモートキャッシュかディレクトリに格納 c．暗号化モジュールへのロード d．初期の配布方法と同様
55	6.1.5.　鍵のサイズ		(規則第６条第六号) 電子証明書には、その発行者を確認するための措置であって第二条の基準に適合するものが講じられていること。 3421 (1) 以下の(2)の事項について利用者電子証明書の発行に使用する電子署名方式及び鍵長を明確に認証業務規程及び事務取扱要領に規定している。 3422 (2) 電子証明書の発行に利用する電子署名方式は、以下のいずれかの方式を用いている。 ① RSA方式（オブジェクト識別子　1 2 840 113549 1 1 5）又はRSA‐PSS方式（オブジェクト識別子1 2 840 113549 1 1 10）であって、モジュラスとなる合成数が1024ビット以上のもの ②ECDSA方式(オブジェクト識別子 1 2 840 10045 4 1)であって、楕円曲線の定義体及び位数が160ビット以上のもの ③ DSA方式(オブジェクト識別子 1 2 840 10040 4 3)であって、モジュラスとなる素数が1024ビットのもの	2.1.1.7 鍵のサイズは、開示された認証局の要件に従う。 2.1.9.8 申請者の私有鍵は、リスクアセスメントや認証局のビジネス要求に基づく暗号化アルゴリズム、鍵長を使用して暗号化する。
56	6.1.6.　公開鍵パラメータの生成主体			2.1.1.4 鍵の生成は、ANSI X9やISO規格で規定されている、乱数発生器(RNG)か擬似乱数発生器(PRNG)を使用する。 2.1.1.5 鍵の生成は、ANSI X9やISO規格で規定されている、素数発生器を使用する。
57	6.1.7.　パラメータ品質の検査方法			
58	6.1.8.　ハードウェア又はソフトウェアによる鍵ペア生成			

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
59	6.1.9.　鍵の使用目的		（指針第１０条） 規則第六条第七号に規定する利用者その他の者が認定認証業務と他の業務を誤認することを防止するための適切な措置には、次の各号に掲げる場合を除き発行者署名符号を当該認証業務以外の業務のために使用しないことが含まれるものとする。 3511 (1) 以下の（２）～（３）までの事項について明確に認証業務規程及び事務取扱要領に規定され、実施されている。 3512 (2) 発行者署名符号の用途は認証業務の発行する電子証明書への電子署名のみに使用される。 上記以外に発行者署名符号を使用する場合は、以下の項目内に限定される。 ① 他の認定をうけた認証業務または認定認証業務と同等の公の認証業務との相互認証の実施 ② 当該認証業務の電子証明書への電子署名（自己署名） ③ 当該発行者署名符号の更新処理のため、新しい当該認証業務の電子証明書への電子署名 ④ 当該発行者署名符号の更新処理のため、古い当該認証業務の電子証明書への電子署名 ⑤ 当該認証業務用設備およびそれを操作する者に対して発行する電子証明書への電子署名 ⑥ 電磁的に記録する失効に関する情報への電子署名 ⑦電子証明書失効情報および当該認証業務に関する情報等を開示する設備に対して発行する電子証明書への電子署名 ※(3)は、2.6に記述	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
60	6.2.　私有鍵の保護 6.2.1.　暗号化モジュールに関する標準 鍵を生成するのに使用されるモジュールに要求される標準。	4.3 暗号化鍵モジュール 4.3.1 暗号鍵管理モジュールのセキュリティ機能 （１）　暗号鍵管理モジュールの使用にあたっては、使用する運用条件等を考慮にいれて、以下のセキュリティ機能の一部あるいは全てを組み合わせた適切な暗号鍵管理モジュールを選択する必要がある。 ・不正顕示（Tamper evident） 不正なアクセスによる暗号鍵等内部データの漏洩、改竄及び不正使用の証拠を残す機能。例としては、暗号鍵管理モジュールへの不正な物理的アクセスにより施錠が解かれた場合にその証拠が残る機能や、物理的な損傷が残り、サービスへの再使用ができなくなる機能等が ある。 ・不正防護（Tamper resistant） 不正なアクセスによる暗号鍵等内部データの漏洩、改竄及び不正使用から防護する機能。例としては、物理的に非常に強固なカバーによる保護、電磁波やＸ線による内部情報の漏洩を防止する措置、アクセス権限の確認機能等がある。 ・不正対抗（Tamper responsive） 不正なアクセスによる暗号鍵等内部データの漏洩、改竄及び不正使用に対し対抗動作を行う 機能。 例としては、不正アクセスを検知した時点で内部データをゼロクリアする機能等がある。		2.1.1.1 認証局署名用私有鍵は、開示された認証局の要件に従い、ISO 15782-1/FIPS 140-1/ANSI X9.66を満たす安全な暗号化装置に保管する。 2.1.1.4 鍵の生成は、ANSI X9やISO規格で規定されている、乱数発生器(RNG)か擬似乱数発生器(PRNG)を使用する。 2.1.1.5 鍵の生成は、ANSI X9やISO規格で規定されている、素数発生器を使用する。 2.1.1.6 鍵の生成には、ANSI X9やISO規格で規定されているような鍵生成アルゴリズムを用いる。 2.1.2 認証局は、認証局の私有鍵の機密性及び完全性を保つように保証を提供する。
		4.3.2 暗号鍵管理モジュール使用システムの機能 （１）　暗号鍵管理モジュールあるいはそれを使用するシステムの操作（例えば、初期化やデータ入出力のための操作、あるいは内部の暗号鍵を利用可能状態または利用停止状態にするための操作など）には、複数人管理を要求するメカニズムを備えている必要がある。 （２）　さらに暗号鍵管理モジュールあるいはそれを使用するシステムは、そこから暗号鍵等の秘密情報を出力する場合に、秘密情報を複数要素に知識分散し、単独の要素だけでは元の情報の１ビットをも知り得ないようにするメカニズムを備えている必要がある。		2.1.9.1(利用者の鍵を認証局が生成する場合) 利用者の鍵生成は、ISO 15782-1/FIPS 140-1/ANSI X9.66 等のレベルを満たす装置で行う。 2.1.9.2(利用者の鍵を認証局が生成する場合) 利用者の鍵生成は、乱数発生器（RNG）や擬似乱数発生器（PRNG）を使用する。 2.1.9.3(利用者の鍵を認証局が生成する場合) 利用者の鍵生成は、ANSI X9やISO規格に適合している素数発生器を使用して行う。 2.1.9.4(利用者の鍵を認証局が生成する場合) 利用者の鍵生成は、ANSI X9やISO規格に適合している鍵生成アルゴリズムを使用して行う。 2.1.9.5(利用者の鍵を認証局が生成する場合) 認証局によってアーカイブされた利用者の私有鍵は、リスクアセスメントや開示された認証局の要件に基づいた暗号化アルゴリズム・鍵長を用いて暗号化したものを保管する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
61	6.2.2.　複数人による私有鍵の管理 複数名統制の方法。	3.2.2 鍵の保管 （２）鍵を知識分散して保管する場合には、知識分散された鍵の情報は各鍵構成要素について、権限を有するものが個別に保管する必要がある。 （３）鍵を暗号鍵管理モジュール内で保管する場合には、複数人の権限を有する者が揃わなければ暗号鍵管理モジュールの持ち出し等ができないよう複数人管理のもとで保管する必要がある。		2.1.1.2 認証局による認証局の鍵生成は、権限の与えられた作業者によるデュアルコントロールで行う。 2.1.2.3 認証局私有鍵が、オフラインプロセスやバックアップ・リカバリーのために安全な暗号化モジュールから取り出され、安全なストレージへ移動する際には、私有鍵は以下に示すような安全な鍵管理方法を用いて取り出す。 a．デュアルコントロールによる暗号化 b．デュアルコントロールや知識/権限の分割による暗号化鍵の断片化 c．デュアルコントロールを使用した鍵配送のような、安全な暗号化モジュールの使用 2.1.2.4 認証局の私有鍵は、物理的に安全な環境において、デュアルコントロールを用いた権限を所有している作業者によって、バックアップ・保管・回復がなされる。 2.1.8.5 認証局の暗号化ハードウェアの使用は、2人以上の信頼できる作業者によって行われる。 2.1.8.6 認証局の暗号化ハードウェアの導入は、2人以上の信頼できる作業者によって行われる。 2.1.8.7 認証局の暗号化ハードウェアの取り外しは、2人以上の信頼できる作業者によって行われる。 2.1.8.8 認証局の暗号化ハードウェアの新しいハードウェア、ファームウェア、ソフトウェアへの保守、修理作業は、2人以上の信頼できる作業者によって行われる。 2.1.8.10 認証局の暗号化ハードウェアを分解、取り除く場合には、2人以上の信頼できる作業者によって行われる。 2.1.8.15 認証局暗号化ハードウェアの故障修理の診断サポートは、2名以上の信頼できる管理者同伴で行う。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
62	6.2.3.　私有鍵のエスクロウ 私有鍵は寄託の有無、奇託機関、奇託する形態（例は、プレーンテキスト、暗号化、分割鍵を含む）、寄託システム上のセキュリティ統制。			2.1.4.1 認証局私有鍵のエスクロウを第三者に委託する場合、責務と賠償責任を含めた契約を結ぶ。 2.1.4.2 認証局がエスクロウされた署名用私有鍵を保持している場合、エスクロウされた署名用私有鍵は現在使用している鍵と同等かそれ以上のセキュリティで管理する。 2.1.9.17(利用者の鍵を認証局が生成する場合) 認証局によってエスクロウされた利用者の私有鍵は、リスクアセスメントや開示された認証局の要件に基づいた暗号化アルゴリズム・鍵長を用いて暗号化したものを保管する。
63	6.2.4.　私有鍵のバックアップ 私有鍵はバックアップの有無、バックアップエージェント、バックアップ形態　（例は、プレーンテキスト、暗号化、分割鍵を含む）　バックアップ　システム上のセキュリティ統制。	3.2.4 鍵のバックアップ （１）私有鍵や共通鍵の偶発的な消失等によって、認証局業務の停止、さらに鍵の更新に伴う対応処理の発生などを避けるために、鍵のバックアップを行う必要がある。バックアップにおけるセキュリティ要件は、保管と同程度以上でなければならない。 （２）バックアップされた鍵は、鍵が保管あるいは利用されている場所から離れた所に保管することが望ましい。 3.2.5 鍵の保存 ①有効期間が終了した私有鍵や共通鍵で、それらが有効期間後も必要になるものは（例えば、鍵暗号化鍵を復号するための私有鍵など）、保存期間を定めて、複数人管理や知識分散による保存（archiving）を行う必要がある。 ③有効期間が終了した私有鍵や共通鍵の内、有効期間後も必要なものは、保存に際し複数人管理や知識分散の基で行なう事	(指針第１４条第二号) バックアップ用の発行者署名符号の複製は、次に掲げるいずれかの方法により行われること。 3E21 (1) 以下の(2)～(4)までの事項について、認証業務規程及び事務取扱要領に明確に規定され、実施されている。 3E22 (2) 発行者署名符号のバックアップは当該認証業務を行う認証設備室内で、複数人によっておこなわれかつそのうちの１名だけでは操作できない方法によっておこなわれている。 3E23 (3) 発行者署名符号のバックアップが暗号装置自体の複製機能を使用して行われる場合は、以下の要件を満たすものである。 ① バックアップされた暗号装置は、認証設備室もしくはそれと同等の安全性を有する場所に保存される。 3E24 (4) 発行者署名符号のバックアップに暗号装置自体の複製機能を使用しない場合は、秘密分散手法が用いられ以下の要件を満たすものである。 ① 分散された符号は、権限を有する人間以外が触れることのできない施錠等によるアクセス制御及び耐火等の防災措置がとられた場所に保管される。 ② 分散された符号は、それぞれが異なる場所に保管される。	2.1.2.5 認証局の署名用私有鍵をバックアップする場合、認証局私有鍵は現在使用してる鍵と同等又はそれ以上のレベルによるセキュリティコントロールを用いる。 2.1.2.6 認証局の署名用私有鍵をバックアップする場合、認証局の私有鍵の回復は、デュアルコントロールを用いた、バックアッププロセスと同様のセキュアな方法を用いて行う。 2.1.9.11(利用者の鍵を認証局が生成する場合) 利用者の鍵のバックアップ・リカバリは、認可された要員により行われる。 2.1.9.15(利用者の鍵を認証局が生成する場合) 認証局によってアーカイブされた利用者の私有鍵は、リスクアセスメントや開示された認証局の要件に基づいた暗号化アルゴリズム・鍵長を用いて暗号化したものを保管する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
64	6.2.5.　私有鍵のアーカイブ 私有鍵のアーカイブの有無、アーカイブエージェントで、アーカイブ形態（例は、プレーンテキスト、暗号化、分割鍵を含みます。）アーカイブシステム上のセキュリティ統制。	3.2.5 鍵の保存 （１）有効期間が終了した私有鍵や共通鍵で、それらが有効期間後も必要になるものは（例えば、鍵暗号化鍵を復号するための私有鍵など）、保存期間を定めて、複数人管理や知識分散による保存（archiving）を行う必要がある。 （２）認証局の公開鍵は有効期間後も可用性を確保することが必要であり、改竄されないように保存する必要がある。		2.1.7.1 アーカイブされた認証局の鍵は、現在使用してる鍵と同等かそれ以上のセキュリティコントロールをすること。 2.1.7.2 アーカイブされたすべての認証局鍵は、アーカイブ期間が終了した時には、物理的に安全なサイトにおいてデュアルコントロールを用いて破壊される。 2.1.7.3 アーカイブされた鍵は本番環境に戻して使用しない。 2.1.7.4 アーカイブされた鍵は、（本番環境以外で使用する場合）技術的な最短時間で回復可能とする。 2.1.7.5 アーカイブされた鍵が、アーカイブ期間が終了した際には確実に破壊されているか、定期的に確認する。
65	6.2.6.　暗号化モジュールへの私有鍵の格納 私有鍵を暗号化モジュールに入れる主体者、格納形態（つまり、プレーンテキスト、暗号化若しくは分割鍵）、私有鍵はモジュール内での格納。			2.1.2.1 認証局の署名用私有鍵は、開示された認証局の要件に従い、ISO 15782-1/FIPS 140-1/ANSI X9.66の要求を満たすレベルの安全な暗号化装置に格納する。 2.1.2.2 認証局の私有鍵において、オフラインプロセスやバックアップ・回復のために暗号化モジュールから取り出し安全なストレージへ移すという作業がない場合、認証局の私有鍵の生成及び使用は暗号化モジュール内でのみ行い、暗号化モジュール外には取り出さない。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
66	6.2.7.　私有鍵の活性化方法 私有鍵をアクティベート（使用）することができる主体者、アクティベート方法、アクティベートの有効期間	3.2.3 鍵の利用 （１）保管されている私有鍵や共通鍵をデジタル署名や復号に利用する際には、暗号鍵管理モジュールに入れて使用することが必要である。 （２）暗号鍵管理モジュールを証明書発行システム等に接続したり、暗号鍵管理モジュール内の鍵を利用可能状態にする操作は、複数人管理のもとで行う必要がある。 （３）暗号鍵管理モジュールが接続されたシステムを停止する場合などにおいて、暗号鍵管理モジュール内の鍵を利用可能状態から利用停止状態に切り替える処理は、複数人管理のもとで操作を行う必要がある。 （４）鍵の利用において、より高いセキュリティを確保するため、暗号鍵管理モジュールを含むシステムを必要の都度スタンドアロンで運用することが望ましい。	(指針第１４条第三号) 発行者署名符号の使用を可能とし、又は不可能とするための認証業務用設備の設定の変更は、認証設備室内で複数の者により行われること。 3E31 (1) 以下の(2)の事項について、認証業務規程及び事務取扱要領に明確に規定され、実施されている。 3E32 (2) 発行者署名符号の状態変更は、以下の条件で行われている。 ① 状態変更は認証設備室内で実施される。 ② 状態変更は、複数人により行われかつその内の１名だけの操作では状態変更がなされない。	2.1.5.1 認証局署名用私有鍵の活性化は、複数人コントロールにて行う。
67	6.2.8.　私有鍵の非活性化方法 私有鍵を無効化の主体者、無効化方法。			
68	6.2.9.　私有鍵の破棄方法 私有鍵を廃棄することができる主体者、廃棄方法。	3.2.6 鍵の破棄 （１）有効期間が終了した認証局のデジタル署名用の私有鍵や、保存期間が終了した鍵などは、その後の不正利用が行われないように廃棄する必要がある。 （２）廃棄は、複数人管理のもとで、秘密情報の一部でも露顕したり残存させたりすることなく行われる必要がある。	(指針第１４条第四号) 発行者署名符号の使用を終了する場合には、複数の者により物理的な破壊又は完全な初期化等の方法により完全に廃棄し、かつ、複製された発行者署名符号についても同時に廃棄すること。 3E41 (1) 以下の(2)～(3)までの事項について、認証業務規程及び事務取扱要領に明確に規定され、実施されている。 3E42 (2) 発行者署名符号（バックアップも含む）の廃棄には、以下のいずれかの方法を用いいずれも複数人によって行われ元の状態に戻せない事を確認する。 ① 物理的破壊 ② 完全な初期化 ③ その他、廃棄対象の発行者署名符号のすべての部分が元の状態に戻せないことが保証できる方法 3E43 (3) バックアップされた発行者署名符号（複製および分散された符号を含む）の廃棄はバックアップ元発行者署名符号の廃棄を含めた一連の作業指示において遅延なく実施される。	2.1.6.1 認証局私有鍵の破壊の権限とどのように破壊するか（例えば、トークンの解体、トークンの破壊、鍵の上書き）は開示された認証局の要件に限定される。 2.1.6.2 認証局署名用私有鍵のすべてのコピー及び断片は、鍵ペアライフサイクルの期限が終了した際に破壊する。 2.1.6.3 安全な暗号化装置がアクセス可能でありサービスから除外されることがわかった場合、装置に格納されているすべての認証局私有鍵は破壊する。 2.1.6.4 認証局の暗号化装置がサービスから取り除かれる場合、装置に格納されているすべての鍵は装置から抹消する。 2.1.6.5 認証局暗号化装置のケースがタンパ特性を持っており、装置がサービスから取り除かれることになった場合、ケースを破壊する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例（指定調査機関）	WebTrust for CA (AICPA/CICA)
68				2.1.9.13(利用者の鍵を認証局が生成する場合) 認証局が利用者の私有鍵を保管している場合、利用者の私有鍵の破壊は、開示された認証局の要件に従い許可された方法により実施すること。（利用者のみが私有鍵を保持していることを保証するコントロールが必要） 2.1.9.14(利用者の鍵を認証局が生成する場合) 鍵ペアの使用（ライフサイクル）終了時、利用者の私有鍵のすべてのコピーや断片を破壊する。 2.1.9.16(利用者の鍵を認証局が生成する場合) アーカイブ期間が終了した場合、アーカイブされていた利用者の鍵すべてを破壊する。
69	6.3.　鍵ペア管理に関するその他の面 6.3.1.　公開鍵の保存 ・公開鍵はアーカイブされるか ・アーカイブ化システム上のセキュリティ統制 6.3.2.　私有鍵と公開鍵の有効期間	3.2.5 鍵の保存 ①有効期間が終了した私有鍵や共通鍵で、それらが有効期間後も必要になるものは（例えば、鍵暗号化鍵を復号するための私有鍵など）、保存期間を定めて、複数人管理や知識分散による保存（archiving）を行う必要がある。 ②認証局の公開鍵は有効期間後も可用性を確保するために改竄されない様に保存する事 ③有効期間が終了した私有鍵や共通鍵の内、有効期間後も必要なものは、保存に際し複数人管理や知識分散の基で行なう事 3.2.7 鍵の定期更新 （１）　認証局の鍵は、あらかじめ有効期間を設け、定期的に更新する必要がある。なお、鍵の有効期間の設定は認証局のポリシーによる。		2.1.3.4 認証局の公開鍵は、開示された認証局の要件に従い、定期的に鍵更新する。
70	6.4.　活性化用データ 暗号化モジュールを動かすのに要求される活性化用データの保護方法。		(規則第６条第三号) 利用者が電子署名を行うために用いる符号（以下「利用者署名符号」という。）を認証事業者が作成する場合においては、当該利用者署名符号を安全かつ確実に利用者に渡すことができる方法により送付し、かつ、当該利用者署名符号及びその複製を直ちに消去すること。 3305 (5)利用者署名符号及びその格納媒体等の活性化に使用するＰＩＮ等の秘密情報の生成、転送、出力等は、権限のある操作者によって行われ、アクセス権限管理、内部牽制等により盗聴、改変防止等の措置が施されている。	2.1.5.2 リスクアセスメントに基づき必要であれば、認証局署名用私有鍵の使用は複数の要素による認証（例えば、スマートカードとパスワード、バイオメトリクスとパスワード）を用いて行う。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
71	6.5.　コンピュータのセキュリティ管理 コンピュータセキュリティ統制を記述する。 6.5.1.　信頼されるコンピューティング基本コンセプト ・アクセス コントロール ・ラベル ・強制アクセスコントロール ・オブジェクト再利用 6.5.2.　コンピュータセキュリティ評価 ・監査 ・識別 ・信頼されたパス ・セキュリティテスト ・ペネトレーション（侵入）テスト ・製品認定	4.2 システムセキュリティ 4.2.1 システム構成 （２）認証情報等の重要な情報を扱うシステム、構成機器については、認証業務の停止を防止するために２重化しておくことが望ましい。 4.2.3 システムの運用 （１）　システムの操作は、不正なアクセスを防止するために権限を有する者が　ＩＤ、パスワード等の個人認証機能を利用する事によってはじめて可能になる様な対策を講じる必要がある。 （２）　システムの異常状態、不正運用等を早期に発見するために、システムの稼動状況をモニタリングし監視する必要がある。	(指針第１３条第三号) システム管理者に係る識別符号については、特に厳重な管理が行われていること。 3D31 (1) 認証業務用設備へのアクセス管理がパスワードを用いてなされる場合は、適切なパスワードの設定、定期変更を含む変更等の方法、手続きが事務取扱要領等に明確に規定され、実施されている。また、パスワードファイル等、電磁的方法によるパスワードの記録は暗号化されており、これらへのアクセスは、権限を有する者のみが可能である等の事項が事務取扱要領等に規定され実施されている。 3D32 (2) システム管理者用アカウントのパスワードは、上記(1)とは区別された特殊文字の混入、変更サイクルの短期化、遠隔操作によるパスワード操作の禁止等、より厳重な管理規定が事務取扱要領等に規定され実施されている。	2.1.1.8 鍵生成に使用するハードウェア/ソフトウェアの保全性と、ハードウェアとソフトウェアのインターフェースは、使用前にテストを行う。 2.2.5.4 認証局のリポジトリ又は他の公開メカニズムの性能はモニタリングされ、管理される。 2.2.5.5 認証局のリポジトリ又は他の公開メカニズムの完全性は維持管理される。 3.2.4c セキュリティポリシには、下記を含める。 c．ウイルス、及び、他の悪意のあるソフトウェアの防止、及び、検出 3.5.22 パーソナルコンピュータやワークステーションは、担当者が離れた場合、キーロック、パスワード、その他のコントロールにて保護される。 3.6.2 認証局 装置、ソフトウェア、オペレーティング手続等のすべての変更をコントロールするために正式な管理責任及び手続を定める。 3.6.3 認可されない改変や情報・サービスの不正使用を防ぐために、責務の義務と範囲を分割する。 3.7.4 パスワードの割当ては、正式な管理プロセスでコントロールする。 3.7.6 ユーザは、パスワードの選択や使用において、ポリシ・手続に規定されたものが許可される。 3.7.7 ユーザは、無人時の装置に対して適切な保護対策を行う。 3.7.17 特定の場所やポータブル装置へ接続する際の認証には、自動端末装置識別機構を使用する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
71				3.7.18 認証局システムへのアクセスには、安全なログオンプロセスを使用する。 3.7.19 個々の責任による作業が追跡できるよう、すべてのユーザに一意な識別子（ユーザID）を付与する。 3.7.20 品質の良いパスワードを保証するため、パスワード管理システムを導入する。 3.7.21 システムユーティリティソフトウェアの使用は制限され、管理される。 3.7.22 リスクアセスメントに基づき、脅迫された時のための警報装置を取り付ける。 3.7.23 許可されないアクセスを防ぐため、認証局システムの端末は一定時間経過した後、タイムアウトする。 3.7.24 リスクの高いアプリケーションは、接続時間を制限する。 3.7.25 情報及びアプリケーションシステム機能へのアクセスは、アクセスポリシに制限される。 3.7.26 機密性の高いシステムは、専用の（孤立した）環境に設置する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
72	6.6.　ライフサイクルのセキュリティ管理 システム開発統制及びセキュリティ管理統制。 6.6.1　システム開発管理 ・開発環境のセキュリティ 6.6.2.　セキュリティ管理統制 ・製品メンテナンスにおける設定管理セキュリティ ・ソフトウェア エンジニアリング統制 ・ソフトウェア開発手法 ・モジュール化、階層化 ・フェイルセーフ設計と実装 6.6.3.　ライフサイクル評価	4.1.1 システムの品質管理 （１）開発担当者に求められる開発経験、能力等を明らかにし、適切な人材を開発に当てることで、品質やセキュリティの低下を防ぐことが必要である。 （２）品質記録（レビューの記録、試験成績書等）を残すことにより、開発時のバグの混入を低下させる必要がある。 （３）設計、製造、試験等の開発工程において、セキュリティポリシーに従ったセキュリティ機能が作り込まれているか、確認しておくことが必要である。 （４）不正プログラムの混入防止 アクセス管理機能その他のセキュリティ機能について開発担当者による意識的な不正プログラムの混入を防ぐ為、開発終了後、該当部分についての第３者によるソースプログラムのレビュー等を実施することが望ましい。 4.1.2 開発環境 4.1.2.1 開発に使用するソフトウェアの管理 （１）ＯＳ、開発ツール等開発に使用するソフトウエアのバージョン／レベルやそれらの品質状況を管理することにより、バグの混入度合いを低下させ、また不正プログラムの混入を防止する必要がある。 （２）認証局の業務システムに使用するソフトウェアを外部から導入する際には、事前に評価を行ないバグや不正プログラムの混入を防止し、運用開始後の障害発生度合いを低下させる必要がある。 4.1.2.2 開発環境へのアクセス管理 （１）開発を行うコンピュータシステムへのアクセスは　ＩＤ、パスワード等の個人認証機能により不正アクセスまたは不正者による不正ロジックの混入等を防止する必要がある。 （２）ソフトウェア開発環境の置かれている部屋は、入退出管理が行われ、管理責任者あるいは管理責任者が許可した者だけが入退出できる環境下にあることが望ましい。 （３）開発終了後のドキュメントやプログラムは、管理責任者あるいは管理責任者が許可した者だけがアクセスできる環境下で保管されることが望ましい。 4.1.2.3 実運用システムの環境設定の管理 認証局業務のシステムを実運用に移行する場合のセキュリティ上重要なシステム環境設定は、誤った設定、不正な設定がされないために、権限を持った特定の者が複数人で作業を行い、相互に確認し合うことが必要である。		3.6.4 開発及びテスト装置（環境）は、稼動装置（本番環境）から分離する。 3.6.6 情報システムの処理能力及び記憶容量を十分に確保するため、利用状況を監視し将来に必要な処理能力や容量を予測すること。 3.6.7 新しい情報システムの導入基準は、アップグレードやニューバージョンへの移行や、導入前にシステムテストを行うことにより評価する。 3.6.8 ウイルス、不正ソフトウェア、不正侵入者に対する検知や保護を実施する。 3.6.9 予期せぬ障害への対処手順と同様、障害発生の報告を受けて行われる行動を規定する正式な報告手順が存在しかつ遵守される。 3.6.10 認証局システムのユーザは、システムやサービスに影響のあるセキュリティ上の弱点の発見に留意し、報告する。 3.6.11 ソフトウェアの誤動作に関する報告の手続が存在し、遵守する。 3.6.12 障害が報告され、正しい対処が行われる手順が存在し、遵守する。 3.6.13 障害や誤動作の種類、規模、コストを定量化し、監視する。 3.6.14 セキュリティ障害に迅速に効果的に対応するための、障害管理の責任の所在と手順が存在し、遵守する。 3.6.17 認可されないアクセスや誤用から情報を保護するため、情報装置と取り扱いに関する手続を定め、遵守する。 3.6.18 システムドキュメントは、許可されないアクセスから保護する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
72		4.2 システムセキュリティ 4.2.1 システム構成 （１）導入ソフトウェア全体のコピーをソフトウェアシステム構成のバックアップとして作成することが必要である。 （２）認証情報等の重要な情報を扱うシステム、構成機器については、認証業務の停止を防止するために２重化しておくことが望ましい。 （３）導入システムに関しては、常にセキュリティ上の欠陥等の情報収集に留意し、必要な措置を遅滞なく行うことが望ましい。		3.8.1 新しいシステムや既存システム拡張のためのビジネス要件は、コントロールに要求される事項を考慮する。 3.8.2 オペレーションシステム上のソフトウェアの変更に関する手順を整備し、遵守する。 3.8.3 ソフトウェアの開放や修正のスケジュールに関する変更手続が定められ遵守される。 3.8.4 緊急事態のソフトウェアフィックスに関する変更管理手続が定められ、遵守される。 3.8.5 テストデータは保護され、管理される。 3.8.6 プログラムソースライブラリへのアクセスは厳格に管理される。 3.8.7 変更の実施は、情報システムの不正侵入のリスクを最小限にするための正式な変更手続に従い、厳格に管理する。 3.8.8 オペレーティングシステムを変更する際は、アプリケーションシステムのレビュー及びテストを実施する。 3.8.9 パッケージソフトウェアの変更は、最小限におさえるよう厳格に管理する。 3.8.10 ソフトウェアの購入、使用、変更は、コバート（秘密の）通信路やトロイの木馬から保護するため管理し、チェックする。 3.8.11 ソフトウェア開発を外部委託する場合、厳格に管理する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
73	6.7.　ネットワークのセキュリティ管理 ファイアウォールを含むネットワークセキュリティに関する統制。	4.2.2 外部ネットワークへの接続 （１）システムを外部のオープンなネットワークに接続する場合は、ファイア・ウォールの設置や重要なシステムの別ネットワーク化等の対策を講じておくことが必要である。 （２）　また、ファイア・ウォールのシステム、機器についても防犯・防災対策を講じておくことが必要である。	(指針第５条第一号) 認証業務用設備が電気通信回線に接続している場合においては、認証業務用設備（登録用端末設備を除く。）に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するためのファイアウォール及び不正なアクセス等を検知するシステムを備えること。 1211 (1) 以下の(2)～(4)を含むセキュリティ基準が文書として規定され、それにかなった設備が導入されている。 1212 (2) 認証業務用設備（登録用端末設備を除く。）が外部のネットワークと接続している場合、その認証業務用設備は、不正アクセス行為を防御するためのファイアウォール機能及びネットワークベースの侵入検知機能を備えた通信機器を有し、それらを介して通信が行われる。 1213 (3) ファイアウォール機能を備えた通信機器は次の要件を満たしている。 ① 利用しないプロトコルによる通信を遮断できる。 ② 特定発信元及び特定着信先を指定し、それ以外の通信を遮断できる。 ③ 利用しないネットワークサービスへの通信を遮断できる。 ④ 処理する通信の記録ができる。 1214 (4) ネットワークベースの侵入検知機能を備えた通信機器は次の要件を満たしている。 ① ネットワーク上を流れるパケットをモニタし、不正な侵入あるいはサービス妨害攻撃が検出できる。 ② 検出の基準となる不正な侵入の兆候（シグネチャ）ファイルを手動で設定ができる、あるいはソフトウェア等のアップデートによって定期的に更新できる機能を有している。 ③ 不正な侵入またはその兆しを発見した時に、管理者へ報告する機能を備えている。	3.7.8 サービスへの直接アクセスは、使用を許可されたユーザのみが行える。 3.7.9 ユーザ端末からサービスコンピュータへの通信路は管理される。 3.7.10 リモートユーザによるアクセスは、認証を行う。 3.7.11 リモートコンピュータへの接続は、認証を行う。 3.7.12 診断ポートへのアクセスは、安全に管理する。 3.7.13 認証局の内部ネットワークドメインを第三者による外部ドメインからのアクセスから保護するため、ファイアウォール等を導入する。 3.7.14 認証局のアクセス制御ポリシに従い、ユーザが使用できるサービス（HTTP、FTP等）を制限する。 3.7.15 コンピュータの接続と情報の流れがアクセス管理ポリシに違反しないよう、ルーティングを管理する。 3.7.16 すべてのネットワークサービスのセキュリティ設定は、文書化する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
73			(指針第５条第二号) 認証業務用設備が二以上の部分から構成される場合においては、一の部分から他の部分への通信に関し、送信をした設備の誤認並びに通信内容の盗聴及び改変を防止する措置 1221 (1) 以下の(2)(3)を含む認証業務用設備に対するセキュリティ基準が、文書として規定され、それにかなった設備が設置されている。 1222 (2) 認証業務用設備が２以上の部分から構成され（例えば、発行業務に用いる設備と登録業務に用いる設備に分かれている場合）、外部ネットワークを経由して接続されている場合、当該設備間の通信は、各設備の認証並びに通信内容の盗聴及び改変を防止する措置が講じられている。 1223 (3) 認証業務用設備が２以上の部分から構成され、同一認証設備室内に設置されている場合、当該設備間の通信は、システムの設定、アクセス管理、内部牽制等の運用上の措置により適合例(2)と同等の措置が行われている。 (指針第６条第１項第三号) 電気通信回線経由の遠隔操作が不可能であるように設定されていること。ただし、電子証明書の発行及び失効の要求その他の電子証明書の管理に必要な登録用端末設備の操作については、この限りでない。 1331 (1) 以下の(2)を含む認証業務用設備に対するセキュリティ基準が、文書として規定され、それにかなった設備が設置されている。 1332 (2) 認証業務用設備は、登録用端末設備からの証明書発行要求や、証明の失効要求等の電子証明書の管理に必要な操作のために利用する以外はネットワーク経由の遠隔操作が不可能であるように設定されている。	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
74	6.8.　暗号化モジュールの技術管理 要件は、U.S. FIPS 140-1 のような標準への参照を通じて表明されます。 ・暗号化モジュール境界の識別 ・入力／出力 ・役割とサービス ・制限状態のマシン ・物理的セキュリティ ・ソフトウェア セキュリティ ・オペレーティングシステム ・アルゴリズム準拠性 ・電磁的互換性及び自己テスト		(規則第４条第四号）認証業務用設備のうち電子証明書の発行者（認証業務の名称により識別されるものである場合においては、その業務を含む。以下同じ。）を確認するための措置であって第二条の基準に適合するものを行うために発行者が用いる符号（以下「発行者署名符号」という。）を作成し又は管理する電子計算機は、当該発行者署名符号の漏えいを防止するために必要な機能を有する専用の電子計算機であること。 1410 (1) 発行者署名符号の生成、管理に使用する暗号装置(規則第4条第四号の専用の電子計算機のことをいう）は、発行者署名符号の漏えい、破損、消失等の事象の発生を可能な限り低い確率に抑えるために以下の機能を備えている。 1411 ① 暗号化されていない状態の暗号符号や認証データ等、保護されていない形式の重要なデータに係る暗号装置への入出力が行われるインタフェースが存在する場合は、そのインタフェースは他のデータの入出力を行うインタフェースとは物理的に独立している。 1412 ② 暗号装置は、以下の機能を有するものであるとともに、暗号装置の操作者ごとに機能ごとの権限の有無が特定されている。 （ｱ）操作者機能：暗号化、署名等、通常の暗号化機能を実施するための機能 （ｲ）管理者機能：暗号装置自体の初期化、署名符号などの重要パラメータの投入等、暗号装置を管理するための機能 1413 ③ 発行者署名符号等のデータの盗難を回避するため、暗号装置は、以下のいずれかの物理的なセキュリティ対策が講じられている。 （ｱ）暗号装置がICチップ単体からなる場合、ICチップが強固で除去困難な材質の不透明なコーティングで覆われている。 （ｲ）暗号装置にカバーが施されている場合、物理的な侵入行為に対し、暗号装置の機能の停止、内部データの無効化等の耐タンパー対策が講じられている。 （ｳ）暗号装置の筐体に排気用スリットもしくは空孔が存在する場合、それらは十分小さく、かつ、検出されずに筐体の中をプローブされることを防止する対策が講じられている。	2.1.8.1 認証局暗号化ハードウェアは、タンパーエビデント容器を使用して販売店から送付されるようポリシ、手続を規定する。 2.1.8.2 販売店から認証局暗号化ハードウェアを受け取った際、権限のある人員がシールが無傷であるか検査する。 2.1.8.3 認証局暗号化ハードウェアは、以下の特性を備えた権限のある人員しか入れない安全な場所に保管する。 a．入庫、状態、出庫、場所を管理するための棚卸のプロセスと手順の策定 b．物理的アクセスが許可された者に限定されるようなプロセス、手順の策定 c．認証局施設とデバイスストレージメカニズムへのアクセスの成功と失敗をすべて、イベントジャーナルに記録する。 d．異常事態、セキュリティ不正、侵入等の障害報告に関するプロセスと手順を策定する e．管理の効果を検証するため、監査のプロセスと手順を策定する。 2.1.8.4 暗号化ハードウェアは、対タンパ性のあるパッケージに保管する。 2.1.8.9 サービスサイト、在庫サイトは、棚卸管理と許可された人員のみにアクセスが制限された安全なサイトである。 2.1.8.11 製造メーカから認証局暗号化ハードウェアを受け取る際は、テスト及びファームウェアの検証を行う。 2.1.8.12 サービス、修理を受けた認証局暗号化ハードウェアを受け取る際は、テスト及びファームウェアの検証を行う。 2.1.8.13 私有鍵を格納、回復する装置と装置のインターフェイスは、完全性を保つため使用する前にテストを行う。 2.1.8.14 認証局暗号化ハードウェアの動作確認を定期的に行う。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
74			1414 ④ 暗号装置に係る発行者署名符号の管理に関し、以下の措置が講じられている。 （ｱ）暗号装置内で発行者署名符号生成を行う場合、安全な擬似乱数生成アルゴリズムを用いるものである。 （ｲ）暗号装置への発行者署名符号の入出力を行う場合には当該入出力は暗号装置に対して直接行われたものであるとともに、以下のいずれかの方式である。 ・発行者署名符号は暗号化された上で入出力される ・発行者署名符号を２つ以上の構成要素に分割して、入出力を行う。この場合、発行者署名符号の各構成要素に対する操作者の認証を行う。発行者署名符号の各構成要素は、暗号装置内で分割、結合される。 （ｳ）発行者署名符号を暗号化されていない状態で暗号装置内に保管する場合は、外部からアクセスできない仕組みとする。 （ｴ）発行者署名符号を破棄する際には、暗号化されていない状態の発行者署名符号その他のセキュリティパラメータを無効化する機能を有する。 1420 (2) 上記(1)にかかわらず、暗号装置を設置する電子計算機のオペレーティングシステム等が以下の機能・要件を満たし、認証業務用設備及び認証設備室全体のセキュリティ対策を講ずることにより同等の安全性が確保できる場合には、これに代えることができる。 1421 ① 暗号装置を駆動するためのソフトウェア類は、実行可能コードのみの形でインストールされている。 1422 ② 暗号ソフトウェア、署名符号その他の重要なセキュリティパラメータ、制御情報、状態情報等は、入出力を監査するための機能を備えるオペレーティングシステムの管理下にある。 1423 ③ 署名符号、認証データその他の重要なセキュリティパラメータ等を不正なアクセス等から保護するための機能を有するオペレーティングシステムが用いられている。 1424 ④ 上記(1)①の物理的に独立したインターフェースに関する事項を満たさない場合、重要なデータの入出力は暗号装置を設置する計算機のオペレーティングシステム等により他のデータと混じることのないよう安全な方法で実施される。	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 (指定調査機関)	WebTrust for CA (AICPA/CICA)
74			1425 ⑤ 上記(1)②のうち、操作者ごとの権限の特定ができない場合、暗号装置を設置する電子計算機のオペレーティングシステム等により操作者の特定が行える。 1426 ⑥ 暗号装置の耐タンパー対策が以下のいずれかの場合、非作動中の装置の安全な保管場所への保管、電子計算機の物理的な攻撃に対する監視機器等でのモニタ及び論理的な攻撃に対する電子計算機のオペレーティングシステム等で保護されている。 (ｱ) ICチップが、不正なアクセス等が試みられたことを検知可能な不透明のコーティングで覆われている。 (ｲ) 暗号装置が不透明な筐体でカバー等が施されており、不正なアクセス等が試みられたことを検知可能な不透明のコーティングで覆われている。 1427 ⑦ 上記(1)④(ｲ)に関し、暗号装置を設置する電子計算機のオペレーティングシステム等により、上記(1)④(ｲ)の方式以外では、入出力できないよう措置されている。	

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
	7. 証明書と失効リストのプロファイル			
	証明書のフォーマットと、CRL が使用されている場合には CRL フォーマットを仕様化。 プロファイル、バージョン、拡張についての情報等。			
75	7.1. 証明書のプロファイル · サポートされるバージョン番号 · 採用されている証明書拡張とその重要性 · 暗号アルゴリズムオブジェクト識別子 · 認証局名、登録局名、末端主体名に使用される名前形態 · 使用される名前制約と、名前制約に使用される名前形態 · 適用可能な認証ポリシオブジェクト識別子 · ポリシ制約拡張の使用 · ポリシ認定子のシンタックスとセマンティックス · クリティカル認証ポリシ拡張についての処理セマンティックス		(規則第６条第五号) 電子証明書には、次の事項が記録されていること。 3411 (1) 以下の(2)が記載される電子証明書について、次のことが明確に定められ、かつ(3)の要件を満たした認証業務規程及び事務取扱要領が規定され、実施されている。 ① 発行に使用する電子証明書の様式及び記載する基準 ② 電子証明書の記述に使用する言語 ③ 電子証明書に記載する(2)の項目を含む項目及びそれらに対応する内容 3412 (2) 利用者に発行する電子証明書は以下の情報が記載されている。 ① 発行者名(複数の認証業務を行っている場合には、業務の種類を含む) ② 発行番号（当該認定対象認証業務を含む認証業務内で唯一であること） ③ 開始日及び終了日により表わされる有効期間（時、分、秒を含む） ④ 利用者の氏名 ⑤ 利用者署名検証符号および当該検証符号に係るアルゴリズム識別子 ※(3)は3.1に記述	2.2.4.1 認証局は、認証局の開示要件に示したように適切な証明書フォーマットを用いて証明書を生成する。 2.2.4.2 認証局は、認証局の開示要件に示したようにISO 9594/X.509に従い証明書を生成する。 2.2.4.3 開示された認証局の要件に示したように、ISO 9594/X.509に従って有効期限を設定する。 2.2.4.4 認証局の開示要件に示したように、ISO 9594/X.509に従って拡張フィールドを設定する。 2.2.4.5 認証局の開示要件に示したように、ISO 9594/X.509に従って鍵利用目的の拡張フィールドを設定する。
76	7.2. 証明書失効リストのプロファイル · CRL についてサポートされるバージョン番号 · CRL と、採用された CRL エントリ拡張と、それらのクリティカル性		(規則第６条第十号) 電子証明書の有効期間内において、利用者から電子証明書の失効の請求があったとき又は電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該電子証明書の失効の年月日その他の失効に関する情報を電磁的方法（電子的方法、磁気的方法その他の人の知覚によっては認識することができない方法をいう。以下同じ。）により記録すること。 3804 (4) 電磁的に記録する失効に関する情報を明確に定める。	2.2.8.8 CRLは規則的に増加する通番を含む。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
	8.　仕様の管理			
77	8.1.　改定手続 8.2.　公表と通知の手続 8.3.　承認の手続		(指針第１２条第１項第十二号) 当該規程の改訂に関する事項及び利用者その他の者に対する通知方法に関する事項 3901 (1) 以下の項目及び内容を含む管理、運用事項が明確に定められ、認証業務規程として電磁的方法により記録され公開されていること。 3913 (13) 本規程の改訂に関する規定及び通知方法に関する事項 ①本規程の改訂に関する手続き等 ②本規程の改訂に関する通知の方法	3.1.1 認証局組織はCPSを明確に策定し、その承認をする最終的な権限及び責任のあるマネジメント組織を設置する。 3.1.2 ポリシ管理組織（PMA）は、証明書ポリシの策定とその承認において、最終の決定権限及び責任をもつ。 3.1.3 PMAはビジネスリスクの評価、セキュリティ要件、鍵ライフサイクル管理、証明書ライフサイクル管理、認証局環境管理のために適用するCP/CPSに含まれる運用上の手続を決定する。 3.1.4 認証局のCPS は、定められたレビュー手順に従って改訂、承認される。 3.1.5 認証局はすべての適切な利用者、検証者に公開されたCPSを利用可能にする。 3.1.6 CPSの改定はすべての適切な利用者、検証者に利用可能とする。 3.1.7 認証局のCPは、定められたレビュー手順に従って改訂、承認される。 3.1.8 定められたレビュー手順は、CPがCPSによってサポートされることを保証する。 3.1.9 認証局はすべての適切な利用者、検証者にCPを参照可能にする。 3.1.10 CPの改定はすべての適切な利用者、検証者に利用可能とする。
	9．その他の要件			

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例（指定調査機関）	WebTrust for CA (AICPA/CICA)
78	9.1.　ICカード（ICC）のライフサイクル管理			2.2.9 2.2.9.1 カードを発行する認証局（登録局）はICCデータ（CDFデータや関連する暗号化鍵）を管理する。 2.2.9.2 ICCを識別する共通データを、カード発行者やカード所有者はICC共通データファイル（CDF）に保管する。認証局（登録局）によるCDFのアクティベーションは、管理された安全なプロセスを使用して行う。 2.2.9.3 CDFのアクティベーション後、ICCはCDFアクティベートステータスを表示する。 2.2.9.4 認証局（登録局）は、ICCパーソナリゼーションとCDFのアクティベーションを記録する。 2.2.9.5 ICCに保存されている申込みデータは、アプリケーションデータファイル（ADF）に記録される。ADFの配置場所（集積回路のメモリーの場所）は、認証局によって安全に管理される。 2.2.9.6 アプリケーション提供者である認証局は、ADFパーソナリゼーションを管理する（ADFの読み出しに関連する鍵とデータ）。 2.2.9.7 カード発行者である認証局は、ADFの開始を管理された安全なプロセスを使用して行う。 2.2.9.8 ADFは、CDFがアクティベートか再アクティベートになった時のみアクティベートされる。 2.2.9.9 ADFのアクティベート後、ICCはADFアクティベートステータスを表示する。 2.2.9.10 認証局はADFの場所、パーソナリゼーション、アクティベーションを記録する。 2.2.9.11 ICCはカードがパーソナリゼーションされない限り発行されない。 2.2.9.12 ICCはCDFがアクティベートか再アクティベート状態になった時のみ使用できる。 2.2.9.13 ICCは配布する前は安全に保管する。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 (指定調査機関)	WebTrust for CA (AICPA/CICA)
78				2.2.9.14 ICCの受取り、アクティベーション、配布は、イベントジャーナルに記録される。 2.2.9.15 ICCは開示された認証局の要件に従って安全に配布される。 2.2.9.16 ADFの非アクティベーションは、アプリケーション提供者である認証局のみが実行できる。 2.2.9.17 CDFの非アクティベーションは、カード発行者である認証局のみが実行できる。 2.2.9.18 CDFの再アクティベーションはカード発行者である認証局の管理下でのみ行える。 2.2.9.19 ADFの再アクティベーションは、アプリケーション提供者である認証局の管理下でのみ行える。 2.2.9.20 ADFの非アクティベーション、CDFの非アクティベーション、ADFの再アクティベーションは記録される。 2.2.9.21 認証局はADFの終了を管理する。 2.2.9.21 CDFの終了は認証局によって管理される。
79	9.2.　セキュリティマネジメント			3.2 3.2.1 経営者側によって決定した情報セキュリティポリシドキュメントはすべての従業員に公開し通知する。 3.2.2 セキュリティポリシは、情報セキュリティ、その全体の目的、及び、有効範囲、及び、情報シェアリングのための適用メカニズムとしてのセキュリティの重要性の定義を含む。 3.2.3 セキュリティポリシは、管理目的、目標、情報セキュリティの方針を含む文書。 3.2.4 下記を含み、セキュリティポリシはセキュリティポリシの解釈、方針、標準、及び、組織への特別な重要性の承諾要求を含む a．法律及び契約上の要求への準拠 b．セキュリティ教育の要求 c．ウイルス、及び、他の悪意のあるソフトウェアの防止、及び、検出。 d．ビジネス継続管理 e．セキュリティポリシ侵害の結果

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 (指定調査機関)	WebTrust for CA (AICPA/CICA)
79				3.2.5 セキュリティポリシは、セキュリティ事故の報告を含み、情報セキュリティ管理に対する一般的な、そして特定の責任の定義を含む。 3.2.6 セキュリティポリシは、方針をサポートするドキュメンテーションの参照を含む。 3.2.7 セキュリティポリシを維持するために責任、及び、レビュー日付を含む定義されたレビュープロセスがある。 3.2.8 上級管理職、又は、高水準の管理情報セキュリティ委員会は、明瞭な指導を保証及び明白な管理を行なう。 3.2.9 管理グループ、又は、セキュリティ委員会は、情報セキュリティ施策のインプリメントを統合する。 3.2.10 個々の資産の保護、特定のセキュリティプロセスを実行することに対する責任は、明瞭に定義される。 3.2.11 新しい情報処理設備のための管理許可プロセスは、存在しかつ実施される。
80	9.3.　資産の分類と管理			3.3 3.3.1 全ての主要な認証局資産に管理者を定め、責任をもって適切なコントロールの維持を行う。 3.3.2 重要な認証局資産の在庫は、維持される。 3.3.3 認証局は、情報共有、情報分散のためのビジネスニーズを考慮した情報の分類と情報保護コントロールを実施する。 3.3.4 手続は、情報が分類していることを保証するために、定義され、そして扱いは認証局の情報分類スキームに従って行われる。

No	RFC2527概要	認証局運用ガイドラインV1.0(ECOM)	「特定認証業務の認定に係る調査表」の適合例 （指定調査機関）	WebTrust for CA (AICPA/CICA)
81	9.4.　監視と準拠			3.1 3.10.1 すべての法令、規定、契約要求を厳格に定義し、それぞれの情報システムにおいて文書化する。 3.10.2 情報システムの権利やソフトウェア製品の使用において、法に準拠していることを保障するため、適切な手続を実行する。 3.10.3 すべての関連法規、規定、契約要件を厳格に定義し、文書化する。