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。