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。