ＩＴ委員会研究資料第３号

認証局のためのWebTrustプログラム
バージョン1.0
2000年8月25日

平成１５年６月９日
日本公認会計士協会

指針についての序文

この文書、AICPA/CICA 認証局のためのWebTrustプログラム バージョン1.0は、公開鍵基盤(PKI)の利用者とプロバイダーを含んだ多様な公開鍵基盤(PKI)実務従事者からの最初の及び継続的なご意見により策定された。公開草案の段階において、AICPA/CICAの電子商取引保証特別委員会は、認証局サービス・プロバイダー、利用者、公共会計団体、国家的会計機構、政府団体を含む多様な国際的機関からの有意義なコメントをたくさん頂戴した。2000年2月に公開草案が公表されて以来、特別委員会のメンバーは、それぞれの頂いたコメントについて検討した。コメントは一般的なものから詳細なものまでにわたっており、有用な指摘を含んでいた。頂いたコメントの大多数は、この文書の若干の変更をもたらしており、いくつかは採用されていないものがあるが、ある場合には、現状の文書の意図する範囲を超えていると見られた。特別委員会は、認証局のためのWebTrustプログラムが、公開鍵基盤技術を進歩させ、認証局のためのWebTrustプログラムの進歩に関心のある当事者とともに検討することを期待する。

序文
この文書での用語「CA」の使用について

この文書は、WebTrust サービスファミリーの一部として開発された **AICPA / CICA 認証局のための WebTrust プログラム**を記述する。

電子商取引の中で、その主なビジネスが認証局の役割を担う会社、あるいは電子商取引ビジネス活動をサポートするために認証局機能を確立した会社が、CA としてあるいは CA 機能を実行するものとして通常言及される。

カナダ（ある特定の他の管轄区域）で、 WebTrust 保証サービスを提供する能力を発揮することを認められる検証責任者を含む公的な会計専門家が、同様に定期的に CA としてあるいは CA であるとして参照された公認会計士の職務を行う。

この文書で混乱を避けるために、会計用語で広く使う用語である「検証責任者」は、WebTrust 保証サービスを行うことを認められる公認会計士又は勅許会計士、あるいはそれと同等な者を識別するために使われている。

用語「CA」は、勅許会計士に言及するこの序文以外には決して使われない。
用語「CA」は、認証局（CA）を意味するか、あるいは認証局機能（CA 機能）に言及するためにのみ使われる。
用語「検証責任者」は、適切に資格を持った、ライセンスを与えられた公認会計士（合衆国）、あるいは（カナダ）勅許会計士を示すために使われる。

訳注：本委員会では、定説のない以下の鍵と証明書ライフサイクルに関する用語の訳を以下のように統一している。

Generation=生成、Renewal/Update＝更新、Rekey=再生成、Escrow=寄託、Distribution=配送、Destruction=破壊、Archival=保存、Revocation=失効、Suspension=一時停止、Issue=発行、Reissue=再発行

目　次

はじめに

この文書は、ライセンスを与えられた WebTrust 検証責任者が、第三者認証の必要性、電子商取引ビジネス活動に関して保証を提供する重要性が増加するにつれて、増加し続ける認証局(CA)によって使用された内部統制の適切性と有効性を評価するためのフレームワークを提供する。電子商取引を保証することに関与する活動の技術的な性質の結果として、この文書ではまた、電子商取引において暗号、TTP 概念とそれらの利用の増加について、公開鍵基盤(PKI)の短い概要を記述する。

機密保持、認証、インテグリティ及び否認防止は、電子商取引の信頼性のために要求される 4 つの最も重要な要素である。これらの要件に対するものとして出現したものが PKI 技術の導入である。PKI は、これらの要件を扱うために、デジタル証明書と非対称の暗号を利用する。

PKI は、それに依拠する他の個人又は当事者の公開鍵が、実際にその個人又は当事者であることを知る当事者（すなわち、それらの証明書あるいは検証された電子署名がそれらの証明書の利用に対して、信頼して行動する証明書の受取人）に手段を提供する。TTP がこの必要性に応じるために設立されたとき、CA 組織あるいは CA が支援を行う。PKI は、数学上関連した公開･秘密鍵ペアを使う。例えば、公衆がアクセスできるリードオンリーのリポジトリにそれを投函することによって、これらの鍵の1つはほとんどの場合公開とされ、他方が秘密に保たれる。公開鍵で暗号化されたメッセージは、このような方法での公開鍵暗号が秘密鍵でのみ復号でき、逆に秘密鍵で署名されたメッセージは公開鍵で検証することができる。この技術は、機密保持、認証、インテグリティ及び否認防止を提供する異なった方法で利用することができる。

安全な電子商取引を確立する上で、暗号は重要な意味を持つ。しかしながら、それは包括的なセキュリティソリューションを提供するために、他の安全なプロトコルと結び付けられなければならない。いくつかの暗号化プロトコルが、独立した TTP（CA）に取引を認証するように電子署名（実際は、電子的証明書）の発行を要求する。CA は、安全な電子商取引においてますます重要な役割を引き受ける。暗号、デジタル証明書の管理及び CA のポリシーと実務での使用のため、既存の国レベルの、国際的な、専門的基準とガイドラインが数多くあるけれども、これらの基準は統一的には適用されてこなかった。

電子商取引を行うことに関して、手段としてのインターネットに対する消費者の信頼を増進し、PKI 技術のアプリケーションに対する消費者の信頼を増進するために、公的な職業会計人は、認証局のための WebTrust 原則と規準を開発し、CA のための一連の原則と規準を推進している。特に、AICPA/CICA によってライセンスを与えられる会計事務所と検証責任者が、特定の認証局によって提供されたサービスがこれらの原則と規準を満たすかどうかを評価して、検証し、保証を提供することができる。認証局のための WebTrust 保証シールを開示することは、検証責任者の無限定報告書の象徴的な表象である。似ているのが消費者対当事者の電子商取引 WebTrust シールであり、そのために同様に認証局によって発行されたデジタル証明書（及び証明書ステータス情報）を利用する者であることを示す（加入者、信頼者）検証報告書を見るために、シールをクリックすることができる。このシールは、検証報告書と他の適切な情報へのリンクと共に CA の Web サイト上に示される。

これは AICPA/CICA 認証局のための WebTrust プログラムの初回のバージョンである。それはユーザー（すなわち、加入者と信頼者）のニーズに取り組み、CA 電子商取引保証のユーザーとプロバイダーにとって、伝達される知識の集合体を提供することによって、利益になるように策定されている。我々は、利用可能な技術とビジネス実務が進展するにつれて、将来の修正がこれらの規準を更新するために要求されることを予想している。読者の意見感想を期待している。それは、これらの原則及びそれをサポートする規準が最新なものになっており、市場のニーズに応えていることを確実なものとするのに不可欠である。AICPA/CICA 認証局のための WebTrust 原則と規準は、米国国家規格協会(ANSI)やインターネット工学特別委員会(IETF)（注 1）によって作成された基準と調和している。

概要

電子商取引とは何か?

電子商取引には、コンピュータ及び電気通信ネットワークを使い、紙の書類を用いず、様々な電子的な商取引に係わる個人及び組織が含まれる。この電気通信ネットワークは、専用回線、公衆回線、あるいは 2 つの組み合わせであ

る。伝統的に、電子商取引の定義は専ら、既に確立された契約上の関係を持っている当事者間に電子取引の主要な手段の電子データ交換（EDI）とされてきた。商取引が同様に売り場において正当なクレジットカード取引、現金自動支払機からのデビットカード取引とキャッシングのかたちで何年間も電子的に行われた。しかしながら、最近は、電子メール及びそれと区別されたブラウザと HTML の開発で、電子商取引の定義は一般に互いに未知の当事者間のインターネット上で行われるビジネスに拡張されてきている。この傾向は、Web の急速な進展と実行可能な伝送メカニズムとしてビジネス情報のため、インターネットを受け入れることに起因している。インターネットのようなインフラに基礎をおく公共ネットワークの使用は、費用の削減を可能とし、大小のビジネスを同じ土俵に乗せた。これにより、すべての規模の当事者にとって、手の届く範囲が広範な消費者にまで拡大することができるようになった。

公開鍵基盤とは何か?

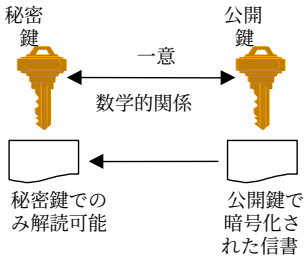
電子商取引の拡大で、 PKI 技術が重要性を増しており、恐らく会社が次の数年に最も重要なセキュリティ投資を行う当事者であろう。PKI は電子商取引の当事者に、デジタル証明書を認証に提供することによって、お互いを識別することができるようにし、電子署名の使用を通して暗号化の使用と認証、データインテグリティと否認防止のための合理的基礎を通して機密保持を提供することによって、信頼できるビジネス通信を可能とする。

PKI は数学上関連した公開･秘密鍵ペアを使う。ほとんどの場合、例えばインターネットでそれを投函することによって、これらの鍵の 1 つが公開にされ、他方が秘密に保たれる。公開鍵暗号ではこのような方法で、公開鍵で暗号化したメッセージは、秘密鍵でのみ復号でき、逆に、秘密鍵で署名されたメッセージは公開鍵で検証できる。この技術はすなわち電子商取引の信頼性のために要求される、4 つの成分を提供する異なった方法（機密保持、認証、インテグリティ、否認防止）に使う。

PKI を使って、加入者（すなわち、その公開鍵がデジタル証明書で当該加入者の身元に暗号化されて対応している最終当事者（あるいは個人））が非対称の暗号化鍵ペア（すなわち、公開鍵と秘密鍵）を持つ。加入者の秘密鍵は秘密にしておかなくてはならないのに対して、通常はデジタル証明書が信頼者に対して、公開鍵が帰属する主体の信憑性を知ることを保証するから、公開鍵は広く利用可能にしてよい。公開鍵暗号を使って、加入者は秘密鍵で署名されたメッセージを送ることができる。署名は、加入者の公開鍵を使ってメッセージの受取人によって妥当性を検査することができる。加入者は、同様に受取人の公開鍵を使ってメッセージを暗号化することができる。メッセージは受取人の秘密鍵でのみ復号することができる。

加入者は、最初に（サービスとして加入者によってあるいは加入者のために生成した）公開/秘密鍵ペアを得る。認証局あるいは CA の代理を務める登録局（RA）にそれらの公開鍵を提出することによって、加入者は、登録プロセスを経る。CA 又は RA が（認証局運用規程に含まれる）CA の確定したビジネス実務のとおりに加入者の身元を確かめて、デジタル証明書を開示する。証明書は、加入者の公開鍵と身元情報を含んでおり、デジタル方式で CA によって署名され、公開鍵に加入者の身元を関連づける。CA は証明書ライフサイクル（登録から失効又は満期を通じての意味）を通じて同様に加入者のデジタル証明書を管理する。ある状況においては、失効もしくは満期を迎えた文書に保存された電子署名が以後も検証可能であるように、満期もしくは失効後であってもデジタル証明書が管理されているということは依然として重要である。

下記の図表は、加入者の秘密鍵と公開鍵の関係及び、信頼者に送られたメッセージを安全に保つために利用される方法を表している。

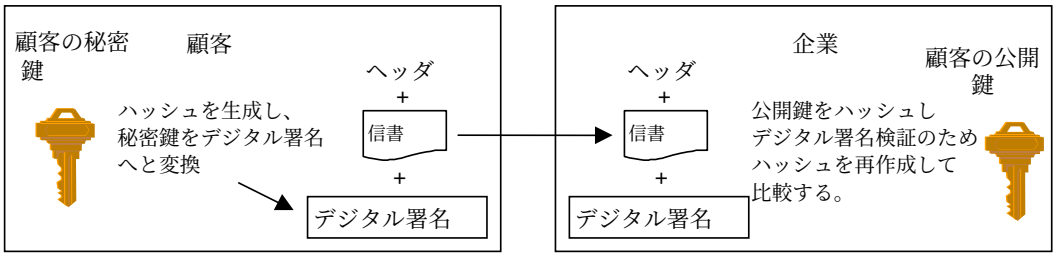


インターネットによってオンラインの当事者に顧客によって提出された取引が当事者の公開鍵で暗号化できて、その当事者によってのみ復号できれば、当事者は高いレベルの機密保持が保証される。機密保持は同様に SSL、S/MIME、SET その他のプロトコルの利用を通して達成することができる。

電子署名とは何か?

電子署名は、認証、インテグリティと否認防止を提供するために使うことができる。一般的にいって、顧客が当事者にデジタル方式で署名されたメッセージを送れば、顧客の秘密鍵は電子署名を生み出すために使われ、顧客の公開鍵は、署名を検証する当事者によって使われることができる。使用された数学的なプロセスは使用された非対称の暗号化アルゴリズムの種類によって幾分異なっている。例えば、プロセスは変更可能な RSA のようなアルゴリズムと電子署名アルゴリズム(DSA)のような非可逆的なアルゴリズム（例えば、暗号化のみならず、電子署名をサポートするのに利用することが既に可能となっているアルゴリズム）のように少し異なっている。

次の例は（RSA のような）変更可能な非対称の暗号化アルゴリズムの電子署名生成と証明書を例示している。顧客が当事者にデジタル方式で署名されたメッセージを送ることを望むとする。顧客は、メッセージを一意に反映するハッシュ（実際には、メッセージの「指紋」）というような方法でのハッシュ電文機能（すなわち、メッセージを固定長データのブロック、ハッシュ電文に換える数学的な機能）を通してメッセージを掲載する。それから顧客は、当該アルゴリズム及びメッセージに添えられる電子署名を作るために顧客の秘密鍵を利用してハッシュ電文を変換する。ヘッダーが同様に当事者の電子メールアドレス、送信者の電子メールアドレスを示しているメッセージとメッセージが送られるときのような他の情報に添付される。メッセージヘッダー、メッセージ自身と電子署名は、それから当事者に送られる。顧客はメッセージそれ自身のオプションとして当事者に公開鍵証明書を送ることができる。これらはすべて、ユーザーにとって透過性のあるプロセスといった方法で、電子メールソフトウェアにより実行される。
下記の図表は、顧客（加入者）が企業に送るメッセージのインテグリティと真正性を保証する加入者の鍵ペアを利用したプロセスを表している。



メッセージが顧客（すなわち、認証）から来たかどうか確認して、メッセージが修正されなかったかどうか確認するために、企業は電子署名の妥当性を検査する。そのために、企業は顧客の公開鍵証明書を得なくてはならない。顧客がメッセージの一部として公開鍵証明書を送らなかったなら、企業は（CA 又は別の CA の代理人あるいは CA と関係しない他の源泉でさえ、に保持されている）オンラインのリポジトリからほとんどの場合、顧客の公開鍵証明書を得る。顧客のデジタル証明書（顧客の公開鍵を含む）が認められた認証局までに署名されたとき、企業は公開鍵と、証明書に表示された顧客との対応が改ざんされていないことを保証する。次に、企業は当初のハッシュを明らかにするために、証明書から公開鍵を抜き出して、電子署名の変換のために当該公開鍵を利用する。企業は、受信したメッセージのハッシュ電文を生成するために同じハッシュ電文機能を通してメッセージを受信する。電子署名を検証するために、企業は、これらの 2 つのハッシュ電文を比較する。それらが一致するなら、電子署名が妥当性を検査され、企業は、メッセージが顧客から来て署名がなされたときから修正されなかったことを知る。ハッシュ電文が一致しないなら、企業は、メッセージが伝送中に修正され、あるいは顧客の秘密鍵で署名されなかったことを知る。結果として、企業は電子署名に依拠することができない。

電子署名は、同様に否認防止の基礎として（すなわち、署名者がメッセージに署名したことを否定することができないこと）を提供するために使うことができる。例えば、1,000 株を購入するオンラインの仲買業顧客がインターネットを通じてデジタル方式で署名された注文は、購入を承認したことを後に否定（すなわち、否認）しようとすることが非常に困難な作業になるであろう。

暗号化鍵ペアと署名鍵ペアの間の相違は何か?

既述のとおり、否認防止の合理的基礎を確立するということは、電子署名（すなわち、署名秘密鍵）を作るために使われた秘密鍵が生成され、安全にユーザーの唯一の統制下に保管されることを要求する。ユーザーがパスワードを忘れるか、喪失するか、壊れるか、あるいは署名公開鍵の鍵を破壊する場合、最小の影響でそれ以降、加入者の使

用のために新しい署名鍵ペアを生成することが認められる。前に署名された文書は、まだユーザーの古い署名証明公開鍵で検証することができる。ユーザーの新しい署名秘密鍵でその後署名された文書は、ユーザーの新しい署名証明公開鍵で検証されなくてはならない。

認証局の署名公開鍵の鍵を安全に保つことには、更なる注意が要求される、それはユーザー証明書に署名するために使われる。CA によって開示されたすべての証明書の信頼性は、CA がその署名秘密鍵を守ることに依存している。上述したように、CA はしばしば安全にそれらの署名秘密鍵のビジネス継続性のために CA のハードウェア障害の結果として、例えば、CA の署名秘密鍵が偶然に破壊（しかし危殆化せずに）される場合、稼働を続けることを可能にする目標を支持する。CA のビジネス継続性目的以外、一般に署名公開鍵のバックアップをとる技術的、あるいはビジネス上の理由はない。

他方、既に見てきたように、暗号化と復号のために使われた鍵ペアが、ユーザーがパスワードを忘れるか、さもなければ復号鍵へのアクセス権を失ったとき、暗号化されたデータを取り戻せることを保証するために安全にバックアップすることはしばしば望ましい。ユーザーがそれを忘れるか、又は容量不足になることに備えてバックアップされた金庫との組み合わせを要求することはそれに似ている。結果として、PKI はほとんどの場合、各ユーザーのために 2 つの鍵ペアを必要とする暗号化と復号のための 1 つの鍵ペアと署名のための 2 番目の鍵ペアと署名証明を有する。

認証局とは何か?

これらの技術により、当事者が安全に電子商取引を行うことができるようにするために、1 つの重要な質問について答えられなくてはならない。どのように我々はデジタル世界で個人の公開鍵が実際にその個人に属することを知るか? 個人についての情報と彼らの公開鍵を含んでいる電子文書であるデジタル証明書がその答えである。この文書はデジタル方式で認証局であると述べられた信頼された組織（CA）によって署名される。基本的な命題は、CA は、個人の身元と彼らの公開鍵の間にリンクを保証することである公開鍵が証明書に含めた保証のレベルを提供するという証明は、本当に証明書で命名された当事者に属する。CA によって公開鍵証明書上に置かれた電子署名は、当事者の公開鍵、証明書の有効期間のような当事者の名前と他の情報の間に暗号を結び付ける。証明書が正当な CA によって開示されたかどうか確認するために、それを信頼者が CA の署名後に証明書が発行されたことを確かめなくてはならない。（後に定義される）多くの共通ルート CA の公開鍵は、標準的な Web ブラウザソフトウェア（例えば、Netscape Navigator あるいは Microsoft Internet Explorer）に前もってロードされる。これは発行されることを確かめる信頼者に証明書が信頼できる CA によって開示されたかどうか確認するために、CA の公開鍵を使った CA の署名を可能とする。

CA の目的は証明書ライフサイクルを管理することである、それは証明書の生成、発行、配送、更新、再生成、失効、一時停止を含む。CA は、しばしば CA のために代理を務める登録局（RA）に加入者の初回の登録を委任する。ある場合には、CA は登録機能を直接的に実行する。証明書失効リスト(CRL)あるいはオンラインの発行ステータスをチェックするメカニズムの保持のように、CA は、同様に証明書ステータス情報を提供することに責任がある。ほとんどの場合、CA は、信頼者がアクセスできる（オンラインのディレクトリのような）リポジトリに開示した証明書及び CRL を投函する。

登録局とは何か?

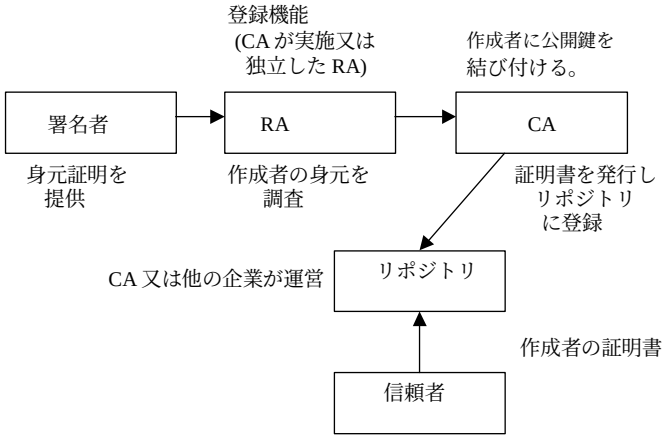
登録局（RA）は、加入者の身元確認と認証に関して責任がある当事者であるが、証明書に署名したり、発行したりはしない。ある場合には、CA は、内部で加入者登録機能を実行する。他の場合、CA は CA と同じ法人の一部であるか、あるいはそうしてはならない（時々支部登録局あるいは LRA であると述べられる）外部登録局に RA の機能を委任する。他の場合には、CA の顧客（例えば、会社）は、CA がそれ自身で RA の機能を実行するか、あるいは代理人を利用すると取り決めることがある。これらの外部登録局は、認証局運用規程と適用される証明書ポリシーで開示され、しばしば文書化された CA のビジネス実務の適切な条項に従うように要求される。認証局のための WebTrust 検証業務において、検証責任者は、どのように CA が RA 機能を処理するか、RA 機能が検証の範囲の中にあるかどうかを考えなくてはならない。例えば、いくつかの銀行に、CA サービスを提供する CA が、それぞれの銀行の中で特に機能的なグループに指名される RA に加入者登録機能を委任する。これらの特定のグループによって実行された機能は、CA のために行われた認証局検証のため、ほとんどの場合 WebTrust の範囲外である。このケースで、経営者の記述書

が CA によって処理されない登録プロセスのそれらの局面を特定するべきであって、それらの局面で CA の内部統制を調査すべきである。

加入者の初回登録プロセスは、CA や発行された証明書の証明書ポリシーによって異なるけれども、おおむね下記のとおりである。加入者は、最初に自身の公開/秘密鍵ペアを生成する。(あるケースでは、CA が加入者の鍵ペアを生成して、加入者に安全にそれを配送するが、これは通常、暗号化された鍵ペアによってのみなされており、署名された鍵ペアによってはなされない) それから加入者は、適用される証明書ポリシーの要件のとおりに身元証明を作り出して、秘密鍵を明らかにしないで公開鍵 (多くの場合、CA によって検証された加入者の電子署名のついた秘密鍵のデータの断片に電子的に署名することによる) に対応している秘密鍵を持つことを明示する。人と公開鍵の間の関係が確かめられたら、CA は証明書を発行する。CA は、真正性と証明書のインテグリティを確立するための手段を提供するためにデジタル方式で、秘密鍵で、開示する各証明書に署名する。

CA は、証明書発行を加入者に通知して、加入者にそれが公開される前に、証明書の内容をレビューする機会を与える。加入者が証明書の正確性を承認すると想定して、加入者は、証明書を公開し、あるいは CA がそれを公開するようにして、それを他のユーザーにとって入手可能であるようにする。リポジトリはオンラインで利用可能な電子証明書データベースである。リポジトリは CA によって維持されてもいいし、第三者がその目的を契約してもよいし、加入者が維持してもいいし、他の当事者が維持してもいい。加入者がリポジトリから他の加入者の証明書と証明書ステータス情報を得てもよい。例えば、加入者の証明書が無効にされたなら、リポジトリは加入者の証明書が無効にされて、信頼されるべきではないことを示す。リポジトリを更新する能力はほとんどの場合 CA によって保たれる。加入者と他の信頼者がリポジトリにリードオンリーのアクセス権を持つ。なぜならば、リポジトリに保存された証明書は、CA によって電子署名されており、何者かがリポジトリに侵入したとしても、それを発見することなくしては、悪意をもって変更され得ないのである。

下記の図表は、加入者、RA と CA 機能の間の関係を表している。



認証局運用規程と証明書ポリシーとは何か?

認証局運用規程 (CPS) は認証局が発行し、証明書の管理において使用する業務記述書である。証明書ポリシー (CP) は、特定のコミュニティに証明書の適用可能性を、あるいは普通のセキュリティ要件で適用のクラスを示す規則の名前をつけられたセットである。例えば、特定の証明書ポリシーが、商品を売買するために所定の価格限度の中で電子データ交換取引の認証にあるタイプの証明書の適用可能性を示す。

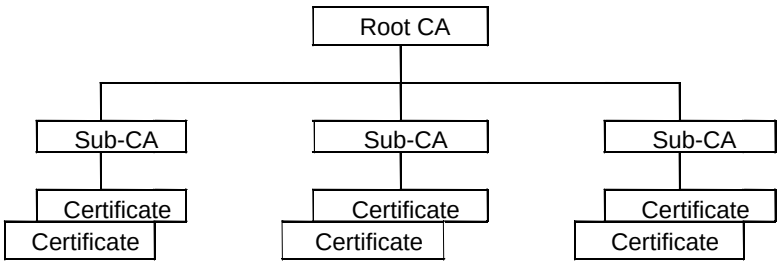
免許付 CA と無免許 CA の間の相違とは何か?

国と他の政府の管轄区域が制定した、あるいは検討中の多くの電子署名法の下では、電子署名法に基づき CA に免許を提供する管轄区域では、ほとんどの場合、免許付 CA によって発行された証明書は、無免許 CA によって発行された証明書より法的に高い認識レベルを有している。多くの管轄区域のために、免許付 CA によって開示された証明書の使用は、それらの管轄区域の電子署名法で特定の認識を用意される。合衆国で、例えば、何人かが、電子

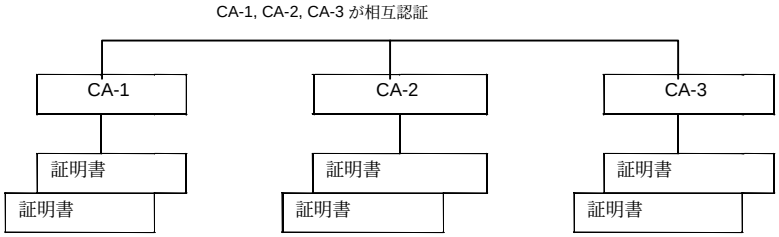
署名法が認証局の検証が免許のための要件として行われることを要求すると述べる。この文書の目的の 1 つは、種々の政府の管轄区域と市場の要件を満たす基準を提供することである。

階層的・相互認証 CA モデルとは何か?

CA は、2 つの基本的なアーキテクチャあるいは 2 つの結合を使ってつながれる (1) 階層的な (2) (共有された信頼) 相互認証である。階層的なモデルで最高水準 (または「ルート」) CA が配置され、従属的な CA は、種々のビジネスユニット、ドメイン、又は利害共同体のために設立される。ルート CA は、従属的な CA を検証し、それは下位 CA 又は直接加入者に順番に証明書を発行する。このようなルート CA は、ほとんどの場合従属的な CA より多くの厳しいセキュリティ要件を有している。攻撃者がルート CA (従属的な CA の証明書を発行、更新、失効させるような滅多にない事象においてのみオンラインで導入される CA) にアクセスすることは難しいけれども、このモデルの欠点はルート CA が 1 ポイントの障害を表すということである。階層的なモデルで、階層でのそれぞれの当事者が業務の最小セットに順応することを保証することによって、ルート CA は、確立された「信頼のコミュニティ意識」を支える。確定したポリシーの遵守が従属的な CA の検証を通して、多くのケースで、登録局で検証される。



相互認証された代替モデルで CA は、「ピア・ツー・ピア」モデル上に築かれる。普通のルート CA を配置するよりむしろ、相互認証のモデルはお互いに知られている CA 間の信頼を共有する。相互認証は 2 つの CA が他の証明書の信頼性を証明するプロセスである。2 つの CA、CA1 と CA2 が相互認証するなら、CA1 が CA2 の公開鍵を含んでいる証明書を作って、デジタル方式で署名する (逆もまた同様である)。したがって、いずれかの CA ドメインのユーザーがそれぞれの CA が他を信頼する、そのためにそれぞれのドメインの加入者がお互いに信頼し合うことができることを保証される。相互認証された CA は、階層的なモデルで障害の 1 ポイントの適用を受けていない。しかしながら、ネットワークは、最も弱い CA と同じぐらい強いだけであり、連続的警戒をしている。相互認証モデルで、信頼の地域コミュニティを設立して、支えるために、信頼のコミュニティのメンバーによって合意されるように、検証がそれぞれの相互認証 CA が業務の最小セットに順応することを保証するために行われる。



結合モデルでは、階層的な構造と相互認証の両方が使用される。例えば、それぞれのコミュニティのメンバーが電子商取引を行うために他によって開示された証明書に依拠することができるように、信頼の 2 つの既存の階層的なコミュニティがお互いに相互証明書を発行することを望む。

CA に関するビジネス問題とは何か?

彼らが政府の免許と規制の適用を受けていないなら、CA は、彼らが証明書を発行する人々の身元を確かめるために異なった基準あるいは手続を使ってもよい。電子署名が、その機能を実行することにおいて、CA が信頼可能であるのと同じぐらい信頼できるだけである。したがって、信頼者がどれぐらいの依存を特定の CA によって発行された証明書によってサポートされる電子署名に置くべきであるか判断するいずれかの方法を必要とする。

CA トポロジー (例えば、階層的、相互認証、あるいは結合モデル) は進展しつつある問題である。いずれのモデルが最も適切であるかは特定のビジネス状況による。公開鍵が保証されていることは重要であるけれども、基準のない

証明書の発行は懸念事項である。例えば、概括的に認められた国際遠距離通信組合電気通信標準化セクタの(ITU-T) X.509 データフォーマット基準(注 2)が使われないなら、加入者と信頼者は、このような証明書を処理することは不可能である。(上に論じられた)相互認証された CA モデルを実行することは同様に非常に難しい。これらの理由により、合衆国及びカナダ政府のような主要な団体が、その内部もしくは外部の活動において X.509 証明書を活用しており、又はその活用を計画している。

認証局のための WebTrust 保証シール

電子取引の数及び種類の急激な増加により Web は、当事者及び消費者の注意を惹きつけてきた。それにもかかわらず、電子商取引は顧客が受容可能なレベルまで電子的にビジネスをするリスクが減少されたとわかるまでに達していないと、多くの人が思っている。顧客は機密保持、認証、インテグリティ、否認防止についての合理的な不安を抱いている。電子商取引の参加者は客観的第三者の保証を必要とする。この保証は独立した、客観性のある検証責任者によって提供され、CA の Web サイト上に安全性を付与された認証局のための WebTrust シールの表示を通して証明されることができる。

認証局のための WebTrust 保証シールは、潜在的な信頼者に資格を持った検証責任者が AICPA/CICA 認証局のための WebTrust の原則と規準に従っているかどうか確認するために CA のビジネス実務と内部統制を評価して、認証局のための WebTrust 原則規準に準拠していることを示すという状態で、無限定意見報告書を開示したことを表象する。付録 A、「検証報告書の開示例」参照。これらの原則と規準は認証局組織あるいは機能の運用の基本的な基準を反映する。

保証専門家としての検証責任者

検証責任者は、財務諸表監査サービスを提供するビジネスに最も公的に認められた人である。これらの専門家は保証事項、財務会計事項に経験を有し、彼らの独立性、誠実性、不偏性、客観性が認識されているので、資格を持った検証責任者によって署名された監査意見が高く評価される。彼らのサービスを提供する場合、検証責任者は、同様に包括的な倫理規則と専門的な規準に従う。しかしながら、財務諸表監査は検証責任者が提供できる多種多様な保証サービスの一部分にすぎない。検証責任者は、同様に指定された規準を内部統制についての保証と準拠に提供する。

そのような計画のために必要とされた業務及び専門的経験、専門知識(電子商取引情報システムセキュリティ、プライバシー、可監査性と内部統制)、専門的特性(独立性、誠実性、不偏性、客観性)は、検証責任者に下記のことを可能にする同一の基本的要素である。それは包括的に、客観的にリスク、内部統制及び電子商取引に関連した企業の開示を評価することである。

認証局のための WebTrust 保証シールの取得と維持

保証プロセス

CA の経営者は下記のように記述する。

経営者がその CA 運用に関して内部統制を評価した。その評価に基づいて、ABC 認証局株式会社(ABC-CA)の経営者の意見では、2000 年○月○日から 2000 年○月○日の期間を通じて、ABC-CA の区域において、下記のように認証局(CA)サービスを提供した。

AICPA/CICA 認証局のための WebTrust 規準に基づき、

- 鍵と証明書ライフサイクル管理のビジネス実務と個人情報保護実務を開示し、開示された実務に従ってサービスを提供した。
- 下記についての合理的な保証を提供するため、有効な内部統制を保持していた。
  - 加入者の情報が(ABC-CA によって実施された登録活動において)適切に認証されていた。
  - 鍵とそれが管理した証明書のインテグリティが確立されて、守られていた。
- 下記についての合理的な保証を提供するため、有効な内部統制を保持していた。
  - 加入者と信頼者情報が、正当な個人に限定されて、CA のビジネス実務の開示において特定されていない使用から保護される。
  - 鍵と証明書ライフサイクル管理運用の継続性は維持された。

— CA システム開発、保有と運用が適切に承認され、CA システムのインテグリティを維持するために行われた。

初回の記述のため、適用される期間は、少なくとも 2 か月又はそれ以上であり、検証責任者により決定される。(確立された CA と CA 機能のために、新しい CA と CA 機能のために、検証責任者がより長い初回の期間がより適切であると信じるのに 2 か月で十分である)。それ以後の記述のため、適用される期間は継続的な記述を提供するため、前の期間の終わりから始めるべきである。(あるケースで、検証責任者は、信頼者のビジネスのニーズあるいは期待という条件のもとでより短い次の期間がより適切であると信じてもよい)

このような記述の基礎を保つために、CA の経営者はリスク評価をして、CA 運用のために適切な内部統制を整備すべきである。認証局のための WebTrust 規準 と内部統制の例示はリスク評価と CA 内部統制の最小限の内容に基礎を提供する。

独立した、客観的で、知識がある検証責任者が AICPA あるいは CICA の専門的基準 (注 3) の下でこれらの記述の検証を実施し、専門な意見を提供し、経営者の記述に信頼性を与える。

サービス監査人報告書と認証局のための WebTrust 検証の比較

検証責任者が第三者サービス・プロバイダーの内部統制 (サービス監査人の契約) について報告するための専門的な基準が現在存在する。これらの契約のための指針は、会計証明基準 (SAS) 70、サービス組織 (AICPA、専門的基準、VOL.1、AU セクション 324) と CICA は、ンドブック保証セクション 5900、「サービス組織における内部統制手続についての意見」の上に AICPA の記述書で万事整っている。認証局のための WebTrust 契約は下記を含む多くの場合サービス検証責任者の契約とは違っている。

目的 - 認証局のための WebTrust は、ビジネスパートナーと既存の、あるいは潜在的顧客を含めて検証責任者のコミュニケーションを通して認証局の活動を利害関係者に報告するために新しいフレームワークを提供する。SAS70 とセクション 5900 (サービス監査人報告書) は、ユーザー検証責任者がサービス組織の顧客の財務諸表について報告するのを補助するために、監査人から監査人へのコミュニケーションのために設計されている。

評価の目標 - 認証局のための WebTrust は特に認証局ビジネス活動の検証のために設計された。サービス監査人報告書は一般サービス組織のために設計された。

契約の種類 - 認証局のための WebTrust は AICPA/CICA 認証局のための WebTrust 原則と規準の遵守について報告することを必要とする。サービス検証報告書は、内部統制の整備と存在について報告するために考案された。それらの有効な内部統制の運用は報告がカバーする一定の時期についてである。

検証基準 - 認証局のための WebTrust は証明業務基準 (合衆国) の記述書に従い、(カナダの) サービス検証報告書は一般に認められた会計監査基準を証明業務基準としている。

活動の範囲 - 認証局のための WebTrust は、特定のエリアの範囲が認証局のための AICPA/CICA WebTrust プログラムによって CA のビジネス実務の開示、サービスインテグリティ (鍵と証明書ライフサイクル管理活動を含めて) と CA 環境の内部統制を含めて定義される必要がある。サービス監査人報告書は財務情報と関係がある内部統制の報告のために設計された。

正式な基準とのつながり - 認証局のための WebTrust は、ANSI X9.79 基準草案 (国際的な標準化のために ISO に提出されるように意図される) から得られた統一基準を提供する。サービス監査人報告書の基礎となっている基準は報告によって対象とされなくてはならない内部統制目的を指定しない。

レビューの期間範囲 - 認証局のための WebTrust は初回の検証の時点から継続的関与を奨励しており、シールを維持するためには継続的関与を必要とする。遵守の後の資格取得が指定された期間 (現在最長 1 年) にわたって最小 2 か月間の期間にわたって、更新検証をすることができる。サービス監査人報告書はサービス組織によって指定された一定の時期を対象とするが、継続的関与を必要としない。

さらには、このアプローチは報告書の WebTrust ファミリーのために使った職業的基準に一貫性を維持する。B2C 電子商取引のための WebTrust 、認証局のための WebTrust プログラム 、WebTrust-ISP と WebTrust 第三者サービス・プロバイダー (TPSP) すべてが CICA セクション 5025 と AICPA AT セクション 100 を報告基準として用いると報告している。

認証局業務と SAS70 とセクション 5900 業務と WebTrust の相違を強調しているテーブルが付録 E、「認証局組織のビジネス活動を包摂する CICA セクション 5900、AICPA SAS70 と AICPA/CICA 認証局のための WebTrust の比較」で、この文書について提供される。

WebTrust シールの取得

WebTrust 保証シールを取得するために、これらのそれぞれと結び付けられた認証局のための WebTrust 原則と規準によって測定されるように、CA はすべての認証局のための WebTrust 原則を満たさなくてはならない。さらには、当事者は⑴ WebTrust サービスを提供する AICPA、CICA、あるいは他の正当な自国の会計士団体の WebTrust ビジネス許可証を持っている検証責任者を関与させなくてはならず、⑵ このような検証責任者から無限定の報告を得なくてはならない。

WebTrust シールの維持

シールが得られたら CA は、提供された Web サイト上にそれを表示し続けて下記を実施することが可能である。

1. 当該 CA の WebTrust 検証責任者が記述の検証の保証を定期的に更新する。当該 CA は、当該検証責任者から継続的に無限定報告書を取得し続けなければならない。そうした更新の間隔は下記の事項によって左右される。

・CA 運用の性格及び複雑性
・CA 運用の大幅な変更の頻度
・ そうした変更が行われたときの、CA のための WebTrust 規準への準拠性を確保するための、当事者の監視及び変更管理の相対的有効性
・検証責任者の専門的判断

例えば、運用を拡張していたり、変更を素早く広範囲に行っていて、機密性の高い伝送・高額の取引に多くの証明書を発行する CA については、相対的に運用が安定していて少ない証明書しか発行しない CA に比較して、更新はより頻繁に行うことが要求される。更新の間隔は 12 か月を超えるべきではなく、この間隔はより短いことが多い。例えば、始動 CA あるいは CA 機能の状態で、初回の検証期間が、次のレビューが、認証局のための WebTrust シールが、その後 12 か月間のレビューサイクルを始めるようになって、与えられるという証明のために 6 か月後に行われるという状態で、3 か月に確立されることはいっそう適切である。継続的関与とシールの維持を提供するために、報告書を更新するための対象期間は、前期間の最終日から始まるか、あるいは初度報告書の期間の初日から始まるべきである。

2. 更新期間に、CA は検証責任者にどんなビジネスポリシー、実務、プロセスの重要な変更でも知らせることを試み、特にこのような変更が認証局、あるいは彼らが適合する方法のために WebTrust の原則と規準を満たし続ける CA の能力に影響を与えるかどうかをコントロールする。このような変更は、ある場合には、シールの除去を検証責任者は、更新検証が実施されるまでシールを除去するか、保証を更新する必要を生じるきっかけとなる。検証責任者は、このような状況の変更に気付いているならば、更新の検証が必要かどうか、更新検証報告書が開示されるまでシールの除去が必要かどうか決定する。

シール管理プロセス

認証局のための WebTrust 保証シールは下記に沿ってシールマネジャーを使って管理される。

・WebTrust 免許保持者となった場合、WebTrust 検証責任者は、登録番号(ID とパスワード)を WebTrust 免許付与機関から取得する。これにより、検証責任者は、認証局に対して WebTrust 保証シールを発行することができる。
・検証責任者が WebTrust 保証シールを発行したとき、検証責任者は、WebTrust セキュアサーバーシステムにアクセスする。登録報酬が支払われたら、検証責任者は、その業務について、2 セットの唯一無二の ID とパスワードを受領する。シールマネジャーは、これらをペアで検証責任者に発行する。一つのセットは、検証責任者に対してセキュアサーバー（下記参照）の読み書きを可能にし、もう一方のセットは、CA に対して、その表示をプレビューすることを可能にする。
・検証責任者が、検証報告書の草案を作成し、経営者の記述書とともにプレビュー用サイトに投函する。
・シールマネジャーが CA に対して、プレビュー用サイトへの適切なリンクによってシールを提供する。提供の通知は検証責任者になされる。

・検証責任者と CA がシールを有効にしようと同意した場合、検証責任者は、シールマネジャーに対して、情報をプレビュー用サイトから有効な WebTrust サイトに転送するように通知し、適切な有効期限を提供する。
・シールは、喪失事由によって除去されない限り、検証責任者によって提供される期間プラス 1 か月の間、有効であり続ける。業務及び他のオープンな項目を完結するのに 1 か月あれば十分である。例えば、もしシールが○○年 6 月 30 日に有効期限が切れる場合は、オープンな項目を完結するのに 30 日を要し、シールマネジャーに新しい文書を投函する。次の検証期間は、○○年 7 月 1 日より始まる。
・検証責任者が、シールが CA の Web サイトから除去されるべきであると決定するなら、彼らは CA に通知して、シールと関連する検証報告書が Web サイトから除去されることを要請する。検証責任者は、また、すべての関連する情報を除去し、このサイトではもはや WebTrust シールは有効ではないとの記述に置き換えさせるためにシールマネジャーに通知する。
・シールマネジャーは、シールが更新される必要のある有効期限の 30 日前に検証責任者に通知する。シールマネジャーは、シール登録報酬が不払いであるか、又は他の適切な事由により、シールを失効させることもできる。

WebTrust シール認証

本物のシールが CA の Web サイト上に表示されたかどうか確かめるため、顧客は下記の事柄を行うことができる。
・シールをクリックして、シールマネジャーによってホストされた WebTrust シールの検証ページに安全な接続によりリンクされる。そのことは、CA の身元を検証し、CA が WebTrust シールを表示させる権利を持っていることを確認させる。また、そのことは適切な原則（例 認証局のための WebTrust 原則）及び他の関連する情報にリンクを提供する。
・シールマネジャーによって保持されている WebTrust シールを受領した企業の一覧を、www.webtrust.org/list.htm においてアクセスする。シールが発行されたとき、当該 CA は一覧に加えられる。当該 CA に対して、その一覧は、WebTrust シールが発行された特定の根拠原則として認証局のための WebTrust 原則を識別させる。

認証局のための WebTrust 原則と規準

次のセクションで明らかにする原則は、エンドユーザー（加入者と信頼者）に、理解できるための認証局のための規準を念頭に信頼者と一緒に開発されており、結果として性質上、実務的で、技術的でないように意図される。

認証局のための WebTrust 原則
CA ビジネス実務の開示

認証局は鍵と証明書ライフサイクル管理のビジネス実務と個人情報保護実務を開示して、開示された実務に従ってサービスを提供する。

認証局は鍵と証明書ライフサイクル管理のビジネス実務と個人情報保護実務を開示しなくてはならない。CA のビジネス実務に関係している情報はすべての加入者、すべての潜在的信頼者にとって入手可能にされるべきであり、ほとんどの場合 Web サイト上に載せられる。このような開示は証明書ポリシー（CP）又は認証局運用規程（CPS）、あるいはユーザー（加入者と信頼者）にとって入手可能な他の示唆に富んだ資料に含まれる。

サービスのインテグリティ

認証局は下記についての合理的な保証を提供するために有効な内部統制を保持する。
・ 加入者の情報が適切に認証されている（ABC-CA によって実施される登録活動として）。
・ 鍵と証明書のインテグリティがそのライフサイクルを通じて確立されている。

有効な鍵管理の内部統制と実務は公開鍵基盤の信頼性に欠かせない。暗号化鍵管理の内部統制と実務がそのライフサイクルを通しての CA 鍵生成、CA 鍵ストレージ、バックアップと回復、CA 公開鍵配送（特に自己署名形式での「ルート」証明書として行われる場合）、（任意の）CA 鍵寄託、CA 鍵使用法、CA 鍵破壊、CA 鍵記録、CA 暗号ハードウェア管理と（任意の）CA によって提供された加入者鍵管理サービスをカバーする。強い鍵ライフサイクル管理内部統制は公開鍵基盤のインテグリティに損害を与えうる鍵危殆化に対してガードするのに極めて重要である。
証明書ライフサイクルは CA によって提供されたサービスの中核である。CA は、発行された CPS と証明書ポリシーでサービスを提供する基準と業務を確立する。証明書ライフサイクルは下記を含む。
・ 登録（すなわち、証明書の個々の加入者を拘束する関係する識別と認証）
・ （任意の）証明書の更新

・ 証明書の再生成
・ 証明書の失効
・ (任意の) 証明書の一時停止
・ 証明書ステータス情報 (証明書失効リストや OCSP を通じて) のタイムリーな発行
・ (任意の) ライフサイクルを通じて秘密鍵を保持することによる IC カードの管理

CA によって発行された証明書に依拠するために、加入者と信頼者の能力を危うくする貧弱な識別・認証コントロールでは、登録プロセスにおける有効な内部統制が不可欠である。有効な失効手続と証明書ステータス情報のタイムリーな発行が同様に重要な要素であり、加入者と信頼者にとっては、CA によって発行された証明書に依拠することができないと知ることは極めて重要である。

CA 環境の内部統制

認証局は下記についての合理的な保証を提供するために有効な内部統制を保持する。
・ 加入者と信頼者情報が適切に本物と証明されて、正当な個人に限定されて、CA のビジネス実務の開示において特定されていない使用から保護される。
・ 鍵と証明書ライフサイクル管理運用の継続性は維持される。
・ CA システム開発、保守と運用が適切に承認されて、CA システムのインテグリティを維持するために行われる。

信頼に値する CA 環境の確立と保持は CA のビジネスプロセスの信頼性に欠くことができない。強い CA 環境の内部統制がなければ、強い鍵と証明書ライフサイクル管理の内部統制の価値は深刻に減少する。CA 環境の内部統制は CPS と CP 管理、セキュリティポリシー管理、セキュリティ管理、資産分類と管理、人員セキュリティ、CA 設備の物理的な環境のセキュリティ、運用管理、システムアクセス管理、システム開発と保守、ビジネス継続性管理、モニタリング、遵守、イベント記録を含む。

認証局のための WebTrust 規準

認証局のための WebTrust 規準に適合することについて、より詳細な指針を提供するため 、認証局のための WebTrust 規準が開発された。これらは規準に対して CA がその適合の自己評価をすることができる基礎を提供して、検証責任者が、CA 業務を検証して評価することにおいて、使うべき一連の首尾一貫した測定規準を提供する。

認証局のための WebTrust 規準で提示される 3 つの原則は CA ビジネス実務の開示、鍵と証明書ライフサイクル管理の内部統制を含むサービスのインテグリティと CA 環境の内部統制である。それぞれの原則の中で、CA の経営者がそれを達成したと断言する一連の規準がある。CA によって提供されたサービスの範囲によっては、多くの規準は適用可能でない。CA が関連サービスを提供するかどうかによって、選択肢であると思われる規準は一鍵寄託、証明書更新、証明書一時停止、IC カードの使用と加入者鍵管理サービスの作成である。これらのサービスのいずれかが CA によって提供されるなら、規準は適用可能であって、検証責任者によって検証されなくてはならない。これらのサービスのいずれも CA によって提供されないなら、規準は適用可能でなく、標準的な報告書の修正は不要である。あるケースでは、若干の RA サービスが CA によって実施されず、そのために活動が CA の検証に含められない別の当事者によって実施される。これらの状況で、付録 A、事例 No. 2 に示されるように、標準的な報告 (合衆国のみ) は検証の範囲から特定の RA 活動の除外を指定するために修正されるべきである。これは CA がいずれの RA 活動を統制しないか明示する CA のビジネス実務開示への参照によって達成される。若干の RA 活動が CA によって行われるどんな場合でも、規準の指定した原則 1 及び原則 2 で発表された内部統制の遵守のために検証責任者によって検証されるべきである。(注 4)

認証局のための WebTrust 業務で、検証責任者は、いずれの内部統制規準が適用可能ではないか確認するために CA のビジネスモデルと提供されるサービスを理解しなくてはならない。開示と内部統制規準のそれぞれのために、開示例の詳細な一覧と関連した規準を満たすために CA によって従われる内部統制手続がある。開示例と内部統制の例は規準が所定のビジネス事情で満たされるために必ずしも遵守する必要がなく、選択肢は十分にある。

CA ビジネス実務開示規準は主にインターネット工学特別委員会 (IETF) インターネット X.509 公開鍵基盤証明書ポリシーと証明業務フレームワーク、ANSI X9.79 基準草案の補則 A に取り入れられた RFC 2527 から得られた。CA において導入された内部統制のうち、特定の鍵と証明書ライフサイクル管理及び CA 環境の内部統制の例は、原則 1 に含められた CA のビジネス実務の開示で特に言及することを要求されている内部統制の例のような、CA のビジネス実務によって異なることがある。

認証局のための WebTrust 原則と規準

原則 1:CA ビジネス実務の開示ー認証局は鍵と証明書ライフサイクル管理のビジネス実務と個人情報保護実務を開示して、開示された実務に従ってサービスを提供する。

規準	開示例
1.1 CA ビジネス実務の開示	
認証局は下記を含むビジネス実務を開示する、しかし下記に限定されない。	
一般	
CA が証明書を発行するための CP と CPS の識別。	1 CA は、CPS の日付に従って証明書を発行しました。CA は、次の証明書ポリシー クラス 1 証明書ポリシー、CA のクラス 2 証明書ポリシー、CA のクラス 3 証明書ポリシーと銀行コンソーシアムの証明書ポリシーをサポートする証明書を発行します。
CA によって発行された証明書の PKI と適用可能性の中で当事者のタイプ及び適用可能性の記述を含むコミュニティと適用可能性。	2 CA は、色々な外部の顧客のために証明書サービスを確立、提供します。組織は一つの CA を管理しますが、それはすべての CA の顧客にユーザー証明書を発行します。CA は、開示された証明書ポリシーのとおりに、加入者の身元を確かめる代理人として作用するために顧客によって指名された人員を利用します。加入者にはデジタル証明書サービスのために CA と契約するすべての当事者を含みます。CA によって発行された証明書に依拠するすべての当事者は信頼者として考慮されます。 この CPS（あるいは他の CA のビジネス実務開示）は CA によって発行されたすべての証明書に適用できます。CPS（あるいは他の CA のビジネス実務開示）で記述された業務はユーザーのために CA ドメインの中での証明書発行と証明書失効リスト（CRL）の使用に適用されます。
下記を含む連絡先の詳細と管理規程の作成 ・ 連絡先 ・ ポリシー機関の識別 ・ 番地 ・ CP と CPS のバージョンと有効期限	3 この CPS（あるいは他の CA のビジネス実務開示）は CA の運用マネジャーによって運営され、それぞれの CA の証明書ポリシーは、CA のポリシー機関によって執行されます。連絡情報は下記のとおりです。 CPS の連絡先の詳細は、 CA 運用マネジャー ● 住所 ● 電話番号 ● ファクス番号 ● 電子メールアドレス CA 証明書ポリシーの連絡先の詳細は ポリシー機関 ● 住所 ● 電話番号 ● ファクス番号 ● 電子メールアドレス
責任の配分に関係している適用される規程	4 この CPS、適用される CP を提供したのと同様に特別に除外するのでなければ、あるいは法規制によって、CA の全体の債務はどんな特別な保証書の違反にでもこれの下で CPS を作った、あるいは適用される CP が 1 万ドルの最大の金額（すなわち、賠償限度）を持っている直接の損害に限定されています。賠償限度は開示された CPS、あるいは適用される CP は電子署名の数、取引、あるいはこのような証明書と関係がある苦情にかかわらず同じであるべきです。さらに、賠償限度が超えられる場合、利用可能な賠償限度は最初に、さもなければ裁判所によって命令されないなら、最終の紛争解決を達成する最も初期の苦情に割り当てられるべきです。請求者間の配分方法にかかわらずどんな場合でも賠償限度額に、CA は、それぞれの証明書に対して総計の賠償限度より多くを支払うために引き渡されるべきではありません。
財務的責任、下記を含むこと。 ・信頼者による損害保険 ・信託の関係	5 発行、取得された証明書を適用する場合、又は証明書に加入者、信頼者が依拠する場合は、CA とその人員、組織、当事者、副契約者、提供者、ベンダー、代表者、代理人を、エラー、見落とし、行動、行動の失敗、欠落から生じるあらゆる種類の、加入者が CA に最新、正確、完全な情報を証明書申請の際に提供できなかったり、加入者のエラー、見落とし、失敗、行動、欠落などから生じる証明書の利用によって、あるいはそれに近いことからの賠償、損害、損失、訴訟、支出から補償し、防護し、安全に守ることに同意してください。 CA と RA は、加入者あるいは 信頼者等の代理人でも受託者でも代行者でもありません。

規準	開示例
解釈と施行、下記を含むこと。 ・ 法律 ・ 契約終了、生存、合併と通知 ・ 紛争解決手続	6 法律 法律はすべてのユーザーのために同一の手続と解釈を保証するためにこの CPS（あるいは他の CA ビジネス実務の開示）への強制力と構造を管理すべきです。 契約終了、生存、合併、告知 契約終了あるいは合併がこの CA の範囲、管理あるいは運用に対する変更をもたらします。このような場合、この CPS は同様に修正を必要とします。運用に対する変更が CA の開示された CPS 管理プロセスと調和して起こります。 紛争解決手続 どんな紛争についてもサービスあるいは規程を関与させることはこれによって CPS（あるいは他の CA ビジネス実務の開示）をカバーした場合、苦情元の当事者は紛争に関して最初に CA とすべての他の適切な当事者に通知するべきです。CA は、紛争を解決する適切な人員を関与させます。
料金、下記を含むこと。 ・証明書発行あるいは更新料金 ・証明書アクセス料金 ・失効あるいはステータス情報アクセス料金 ・ ポリシー情報のような他のサービスのための料金 ・返金ポリシー	7 CA は、加入者に CA のサービスの使用に対して料金を請求します。このような料金の最新のスケジュールは URL で CA のリポジトリから利用できます。このような料金は CA のリポジトリでの入力後7日後に変化します。
発行とリポジトリ要件、下記を含むこと。 ・CA 情報の公開 ・公開の頻度 ・アクセスコントロール	8 CA の CPS（あるいは他の CA ビジネス実務の開示）は URL で利用できます。CA の証明書ポリシーは、URL で見いだすことができます。 発行されると、すべての公開鍵証明書と CA によって提供された CRL は CA のディレクトリで公開されます。 すべての加入者と信頼者は、CA のリポジトリにアクセス権を持ちます。
準拠性検証要件、下記を含むこと。 ・当事者の準拠性検証の頻度 ・検証責任者の名前と資格 ・検証によってカバーした課題 ・欠陥の結果としてとられた行動 ・結果の伝達	9 認証局運用に関して CA のビジネス実務の開示の適切性と CA の内部統制の有効性を評価するために会社、独立外部検証責任者によって年次検証が行われます。 年次検証の関与によって次のトピックがカバーされます。 ・CA ビジネス実務の開示 ・サービスのインテグリティ（鍵と証明書ライフサイクル管理の内部統制を含む） ・CA.環境の内部統制 準拠性検証の間に識別された重要な欠陥がとるべき行動の確定をもたらします。この解決は CA の経営者の指図で検証責任者によってなされます。CA は、修正行動が 60 日内にとられるのを見ることに責任があります。CA のインテグリティを危うくするひどい欠陥が万一識別された場合は、CA の経営者は、検証責任者からの指図で、CA の運用の一時停止が正当化されるかどうか考えます。 準拠性検証結果は CA の取締役会、CA の経営者、CA のポリシー機関及びその他の CA の経営者によって適切であるとみなされた当事者に伝達されます。
特定の証明書ポリシーを参照する CA によって発行された証明書の適用可能性のための条件の記述、下記を含むこと。 ・このような使用が特定のアプリケーションに限定されているなら、証明書の明示的に許諾された使途 ・証明書が特別に利用を禁止される場合の証明書利用の制限	10 CA の証明書ポリシーのもとで証明書の発行は○○銀行の消費者インターネット銀行業務アプリケーションに関連した使用に制限されます。CA によって発行された証明書は、他のいかなる目的のためにも使われてはなりません。

規準	開示例
CA 又は RA の義務。 ・証明書を発行すべき加入者への発行通知 ・証明書主体以外の人への証明書の発行通知 ・証明書を失効したり、一時停止とされた加入者への失効通知あるいは一時停止通知 ・証明書を失効したり、一時停止とされた証明書主体以外の人に発行されている証明書の失効通知あるいは一時停止通知	11 CA は、下記のように義務づけられています。 ・ CA リポジトリで公開された修正事項による時宜に応じた修正と同じように、CPS への運用の確認(または CA ビジネス実務の開示) ・適切な証明書ポリシーに基づくタイムリーな証明書発行、公開。 ・ 失効を申請する権利を持った人からの証明書失効申請に基づく CA によって発行された証明書の失効。 ・ 適用される証明書ポリシーと CA の開示されたビジネス実務で述べられた規程に従った定期的な CRL の公開。 ・(1)証明書が生成され(2)加入者がどのように証明書を訂正するかを加入者に電子メールで通知する。 ・ 証明書のクラスによる要求に従って CA が加入者の申請書をうまく検証できない場合、CA は加入者に申請書が却下されたことを通知します。 ・加入者の証明書が失効されたことを加入者に電子メールで通知します。 ・ CA リポジトリで証明書と CRL にアクセスすることで証明書の発行と失効を他の PKI 参加者に通知します。
RA の義務、下記を含むこと。 ・加入者の識別と認証 ・失効及び一時停止の要求の妥当性検査 ・加入者更新や再生成要求の妥当性検査	12 RA (あるいは CA の RA 機能) は下記のように義務づけられています。 ・ 適切な証明書ポリシーのとおりに申請の時に加入者によって提供された、情報の正確さと承認を確かめます。 ・ 証明書を失効する申請の受領に、適切な証明書ポリシーのとおりに CA の妥当性を検査して、安全に失効の申請を送ります。 ・ 更新時、加入者によって提供された情報の正確性と承認を確かめるか、あるいは、適切な証明書ポリシーのとおりに、更新又は再生成します。
リポジトリの義務、下記を含むこと。 ・証明書と CRL のタイムリーな公開	13 CA のリポジトリ機能はタイムリーに証明書と CRL を公開する義務を負っています。
加入者の義務、下記を含むこと。 ・証明書申請の正確な表現 ・加入者の秘密鍵の保護 ・秘密鍵と証明書使用の制限 ・通知上の制限の保護での記述の正確性	14 加入者は、下記のように義務づけられています。 ・ 証明書と身分証明書の情報と認証情報に関して加入者の最も正確で完全な知識と原則を CA に情報提供して、即座にこの情報に対するどんな変更でも CA に通知します。 ・彼らの秘密鍵を危殆化から保護します。 ・ 法律上の目的のために適切な証明書ポリシーとこの CPS (あるいは CA ビジネス実務の開示) のとおりに排他的に証明書を使います。 ・ 加入者が (今まで) 証明書でリストされた公開鍵に対応している彼らの秘密鍵の危殆化があったと信じる理由を持っているなら、即座に CA が証明書を無効にすることを要請します。
信頼者の義務、下記を含むこと。 ・証明書の利用目的 ・電子署名検証責任 ・失効や一時停止のチェック責任 ・適用される義務の限度と保証の周知	15 信頼者は、下記のように義務づけられています。 ・ 証明書のために、適切な証明書ポリシーのとおりに CPS (あるいは CA ビジネス実務の開示) で CA によって開示された証明書に対する依拠を制限します。 ・依拠の時に証明書のステータスを確かめます。 ・ CA によって開示された証明書に対する依存の上に CPS (あるいは他の CA ビジネス実務開示) で記述されるように、責任限界の規程によって拘束されることに同意します。
証明書利用のための適用される依拠あるいは限度額	16 証明書は、CA の証明書ポリシーで開示した 100, 000 ドル下記の取引に関してのみ使われます。
鍵ライフサイクルの管理	
CA 鍵ペア生成、下記を含む。 ・どの鍵サイズが要求されるか。 ・どの鍵生成アルゴリズムが要求されるか。 ・ ハードウェアとソフトウェアのどちらに鍵生成が整備されているか。 ・鍵(例えば、ISO 15782-1/FIPS 140-1/ANSI X9.66 モジュールレベルを要求される)の生成に使うモジュールにどんな基準が要求されるか。 ・鍵を利用する目的は何か。 ・鍵を制限すべき目的は何か。 ・ CA の公開鍵と秘密鍵のそれぞれの使用期限、有効期間はどれだけか。	17 CA の署名鍵ペアは、RSA アルゴリズムの 1024 ビットを使います。 ハードウェアキー生成は、少なくとも FIPS 140-1 レベル 3 に準拠しています。 CA の署名鍵は、証明書と CRL の署名に使います。 CA 署名鍵ペアの有効期間は 5 年です。

規準	開示例
CA 秘密鍵の保護。下記を含むこと。 ・CA の秘密鍵を保管するのに用いるモジュールの基準は何か（例えば、ISO 15782-1/FIPS 140-1/ ANSI X9.66 レベルのモジュールが要求される）。 ・CA の秘密鍵が N 対 M のデュアルコントロールの下で保持されるか。 ・CA の秘密署名鍵が寄託されるか。 ・CA の秘密署名鍵がバックアップをとられるか。 ・CA の署名公開鍵と秘密署名鍵が保管されているか。	18 ハードウェア暗号化モジュールは FIPS 140-1 レベル 3 に保証されています。 CA のルート秘密鍵に物理的、論理的なアクセスの分離があります。2 人の個人がハードウェアモジュールへの物理的なアクセスにデュアルコントロールを提供しています。除去可能な媒体上に他の保護者によって持たれた N 個の秘密の共有の M が秘密鍵の論理名起動のために要求されます。 CA の秘密署名鍵は、FIPS 140-1 レベル 3 を証明されたハードウェアでのみバックアップを取られ、デュアルコントロールでの保管を強制されています。 外部の第三者による CA 秘密鍵の寄託は実行されません。 CA の秘密署名鍵と期限が切れた（無効にされた）CA 公開鍵証明書は保存されます。
CA が加入者の鍵管理や提供されたサービスの記述を提供しているかどうか。	19 CA は、下記を含む加入者鍵管理サービスを提供します。 ・加入者鍵生成 ・加入者鍵ストレージ、バックアップ、復旧 ・加入者鍵保管 ・加入者鍵破壊
CA の公開鍵が加入者と信頼者に安全に提供される方法の記述を含む、CA 公開鍵の配送。	20 CA と加入者のクライアントソフトウェアの間で秘密を共有している認証コードで暗号化されたセッションを使っている加入者に自分で署名された証明書で CA は、公開鍵を配送します。信憑性とインテグリティ保護は認証コードから鍵によって得られた MAC 鍵に基づいています。
CA のユーザーへの新しい公開鍵の提供に利用される手続の記述を含む、鍵の交換。	21 CA のルート署名秘密鍵は、2 年の有効期間を持っており、対応する公開鍵証明書は 4 年の有効期間を持っています。秘密鍵の有効期間の終わりに、新しい CA 署名鍵ペアが生成され、すべてはその後証明書を開示し、CRL は新しい秘密署名鍵で契約されます。対応する新しい CA 公開鍵証明書は、加入者と信頼者に安全に提供されます。
加入者の鍵ペア生成（CA が加入者鍵ペア生成サービスを提供する場合）。下記を含むこと。 ・加入者の鍵ペアがどのように加入者に対して安全に提供されるか。 ・どのくらいの鍵サイズが要求されるか。 ・どのような鍵生成アルゴリズムが要求されるか。 ・鍵生成がハードウェアあるいはソフトウェアで行われるか。 ・鍵生成に用いられるモジュールにどんな基準が要求されるか（例えば ISO 15782-1/FIPS 140-1/ANSI X9.66 レベルのモジュールが要求される）。 ・鍵を利用する目的は何か。 ・ 鍵を制限する目的は何か。	22 加入者のために、CA は暗号化の鍵ペアと対応する暗号化公開鍵証明書を作ります。 加入者のために、暗号化の鍵ペアは、CA と加入者のクライアントソフトウェアの間に暗号化されたセッションによってユーザーに安全に提供されます。 加入者暗号化の鍵ペアは、RSA アルゴリズムを使う 1024 ビットです。 加入者暗号化の鍵ペアを生成する CA のプロセスは CA システムソフトウェアを使って、FIPS 140-1 レベル 1 に従うよう意図されます。
加入者の秘密鍵の保護（CA が加入者鍵管理サービスを提供する場合）。下記を含むこと。 ・加入者の秘密鍵がバックアップを取られるか。 ・加入者の秘密鍵が保存されるか。 ・どのような状況下で加入者の秘密鍵が破壊されうるか。 ・加入者の秘密鍵が CA によって寄託されるか。	23 CA によって生成された加入者の暗号化公開鍵が CA データベースでバックアップをとられます。CA データベースが暗号化され、そのインテグリティはマスターキーによって守られます。加入者の署名秘密鍵が加入者によって生成されて、CA によっても知られ、あるいは保管されません。 すべてのユーザーのための、すべての復号秘密鍵の完全な履歴を含む暗号化の鍵ペアヒストリーは CA データベースで暗号化されて保管されます。 CA によって保管された加入者暗号化公開鍵の鍵は破壊されません。 加入者秘密鍵の寄託が CA によって実行されません。
証明書ライフサイクルの管理	
証明書一時停止がサポートされるか。	24 CA は、証明書の一時停止をサポートしません。

規準	開示例
当事者の登録や証明書発行における、加入者の身元確認と認証、証明書申請の検証への CA の要求の記述を含む、初期登録。 ・ 多様な名義フォーム変換のための証明対象とルールに指定された名前の種類 ・名前は意味を持つべきかどうか。 ・名前は唯一無二であるべきかどうか。 ・ 名前をめぐる苦情、紛争をどのように解決するか。 ・商標の認識、認証及び役割 ・ 登録される相手の公開鍵に対する秘密鍵の所有をどのように証明するか。 ・ 加入者の公開鍵が CA にどのように安全に提供されるか。 ・組織身元確認への認証要求テーマ ・個人身元確認の認証 ・要求される証明書申請データ ・ CA が証明書申請に対してどのように加入者の権限を検証するか。 ・ CA が加入者の証明書申請を含んで、どのように情報の正確性を検証するか。 ・ CA が証明書申請のエラーや欠落をチェックするか。	25 CA は、命名フォームで識別された X.500 を利用した単一の命名階層を確立しました。 例外なく、証明対象の名前は意味を持たなくてはなりません。一般に、(それによって) 加入者は、CA に一般に知られている名前を使うべきです。CA は、加入者通称での偽名の使用をサポートしません。 CA の PKI でのすべての主語はネーミング階層で明瞭に識別されます。 「鈴木一郎」のような識別名に重複があるとき、加入者にとって受け入れられるミドルネーム、あるいは他の修飾を、名前を唯一無二にするために使います。 CA は、閉じられた PKI の中で証明書を発行します。商標と関連した命名の問題はこの領域の中で発行される証明書には一般に適用されません。 証明書ポリシーで定義されるように、秘密鍵の所有はチェック値を提供することによって、証明書申請者によって証明されます。 組織的な身元が証明書ポリシーに基づいて重要であると思われるなら、組織の身元は証明書ポリシーによって承認された方法を使って確かめられます。 個人の識別認証のための要件は証明書ポリシーに証明書によって定義されます。 証明書発行申請書を提出することにおいて、少なくとも次の情報は CA 加入者の公開鍵を提出しなくてはならず、加入者の識別名と他の情報が CA の証明書発行申請書フォームに要求されます。 証明書ポリシーによって要求される場合、CA は、加入者の機関が、組織の人事課あるいは労組の組合員課の問い合わせを通して加入者が特定の組織あるいは労組の従業員であるかどうか調査することによって、証明書申請を確かめます。 CA は、第三者データベースに対して妥当性検査をし、加入者の証明書申請上の情報の正確さを確かめます。 CA は、証明書申請のエラーや欠落をチェックします。
CA の手続を含む、外部登録局が使う登録の要件。 ・外部登録局の身元検証 ・外部登録局の承認 ・RA が責任を持つものとされる、証明書発行申請、証明書更新と証明書再生成プロセスを安全に保つための外部登録局への要求事項 ・外部登録局から受け取った証明書申請入力の認証を CA がどのように検証するか。	26 CA は、CA の職員のために、二つの識別フォームにより物理的に証明することを外部の RA に要求します。 CA は、成功した身元確認と外部 RA 登録と証明書申請フォームを認証し、承認した上で外部の RA を承認します。 外部の RA は、身元確認と加入者の認証に関して責任があって、証明書申請、CA への安全な証明書申請に署名することに対して、使われた彼らの秘密署名鍵を安全に保って、安全に集められた加入者情報を保管しなくてはなりません。 RA の電子署名の妥当性を検査することによって、CA は外部の RA から受け取られた証明書申請の承認を確かめます。
証明書更新。下記のための CA の手続記述を含む。 ・更新の必要 ・身元確認と認証 ・更新申請の証明	27 証明書更新プロセスは新しい証明書の申込に類似しています。しかしながら、加入者は変更された情報を提供する必要があるだけです。
ルーチンな再生成。身元確認と認証と再生成申請検証手続の記述を含む。	28 証明書の再生成に適用される証明書ポリシーによって必要とされないなら、初回の登録のための認証要件を繰り返す必要はありません。加入者が初回の登録のための要件を定義された身元確認と認証プロセスで再生成ごとに 2 度以上、認証を繰り返すことは制限されています。
失効、期限切れ後の再生成。証明書が失効された後の身元確認と認証と再生成申請検証手続の記述を含む。	29 問題となっている証明書が無効にされた後、身分証明書と初回の登録のための認証要件が繰り返されるなら、再生成可能となります。
下記に関する要件の記述を含む、証明書発行。 ・証明書の発行 ・そうした発行該当者への通知	30 証明書は、加入者が認証局の承認を受け、申請書が受理された加入者に発行されます。証明書フォーマット、有効期間、拡張フィールドと鍵使用法拡張フィールド要件が CA の公表した証明書プロファイルのとおりに指定されます。

規準	開示例
・証明書フォーマット要件 ・有効期間の要件 ・拡張フィールド要件（どのような拡張フィールドが推奨されるか、及びどのように周知するか）	
証明書の受入れ。発行された証明書と証明書の公開効果の受入れに関する要求の記述を含む。	31 証明書を生成したら、加入者によって回収されるまで、それは安全な遠隔リポジトリに保持されます。安全な遠隔リポジトリからの証明書の回収においては、証明書ステータスが更新され、正当に受け入れられていることを反映されます。
証明書の配送。提供する証明書失効リストを信頼者にとって入手可能であるようにすることに対して、CA の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）の記述を含む。	32 単一のリポジトリがすべての加入者、信頼者によって運営されます。CA によって発行されたすべての証明書と CRL は、リポジトリにおいて公開されるべきです。この CA のリポジトリは X.500 ディレクトリシステムによって提供されます。ディレクトリにアクセスするために使われたプロトコルは簡易ディレクトリ・アクセス・プロトコル（LDAP）バージョン 2 です。
証明書の失効。下記を含むこと。 ・証明書が失効される状況 ・失効申請に要求される身元確認と認証手続 ・証明書失効申請の初期認証、検証手続 ・ 加入者への証明書失効申請の利用可能期間 ・ 公開鍵の危殆化の結果としての失効の際の条項検証(失効の第三者対抗として) ・下記の、安全で承認された失効を実現するための速い意思疎通の手段を提供する手続 ・(1) 1 つ以上の当事者には 1 つ以上の証明書 ・(2) 証明書を生成する CA によって利用され、発行される単独の公開鍵、秘密鍵ペアの全証明書のセット ・(3) 公開鍵、秘密鍵ペアが利用されたかにかかわらず、CA によって発行された全証明書 ・ 加入者の証明書が失効されたことについて、加入者に通知する手続 ・ 外部登録局が、失効申請を処理した加入者の証明書の失効に対して通知するか。 ・加入者の証明書ステータス情報が証明書失効によって更新されるのは、どのように、いつか。	33 証明書は、証明書に格納された公開鍵に関連して、秘密鍵のコントロールの疑わしい、もしくは本当の危殆化を含む、いくつかの理由により失効されることがあります。公開鍵を作動できなくするハードウェア又はソフトウェアの障害又は加入者がこの CPS と関連する CP の義務づけに適合できない障害です。失効のための他の事情が特定の CP で明記され、顧客又は従業員ステータスの変更あるいは従業員の特定の役割の変更のような、CA と加入者の関係の変更に関連しています。 失効は、加入者、RA、あるいは CA によって求められます。証明書を無効にする登録局人員による要請には十分な RA システムアクセス権を必要とします。彼ら自身の証明書を無効にする加入者による要請は下記の 1 つを必要とします。 ・ 加入者は、パスフレーズの呈示を初回の申請の時点で作成する。 ・ 証明書ポリシーで提供されている他の手段 ・ 個人的な写真 ID カードを持っている RA への加入者の出頭 ・ RA の加入者の、デジタル方式で署名されたメッセージ 加入者は、CA にオンラインで、電子メールあるいは電話で証明書失効を求めることができます。申請がオンラインでされ、最終当事者が正しいチャレンジフェーズを提供する場合、証明書はすぐに無効にされます。このような申請の有効性が確かめられた後、電子メールあるいは電話によってされた証明書失効の申請が CA によって日次で処理されます。電話と電子メール失効申請のための承認手続が証明書ポリシーで定義されます。検証された証明書失効申請は受領後 24 時間以上処理されません。証明書ポリシーは、失効申請の処理のためにより短い時間を定義します。 鍵危殆化以外の理由の失効申請は失効を必要としている事象から最長 48 時間内でされなくてはなりません。秘密鍵危殆化が疑われるか既知の場合、失効申請は身元確認後にすぐにされるべきです。 CA の証明書失効プロセスは 1 つ以上の対象者の 1 つ以上の証明書の確かな、認証された失効をサポートして、毎日の CRL の発行を通して（あるいは必要な、いっそう頻繁な CRL である場合）このような失効の速い意思疎通の手段を提供します。CA のシステムとプロセスは一つの CA 秘密署名鍵あるいは異なった CA 秘密署名鍵で署名された CA によって開示された証明書のグループを署名された CA によって開示されたすべての証明書のセットを無効にする能力に提供します。 加入者の証明書の失効において、加入者は電子メールによって通知されます。 失効申請が外部の RA によって処理されたとき、外部登録局は加入者の証明書の失効を同様に通知されます。 加入者の証明書の失効を、新たに無効にされた証明書は開示される次の CRL で記録します。

規準	開示例
証明書の一時停止。下記を含むこと。 ・証明書を一時停止する状況 ・失効申請に要求される身元確認と認証の手続 ・証明書一時停止申請の初期認証、検証に用いられる手続 ・一時停止はいつまで続くか。 ・証明書一時停止を延期すべき状況 ・証明書一時停止を延期申請する認証規準 ・秘密鍵危殆化の結果としての一時停止の際の条項検証(他の一時停止理由に反対して) ・下記の、安全で承認された一時停止を実現するための速い意思疎通を提供する手続 (1) 1つ以上の対象者には1つ以上の証明書(2)CAによって証明書を生成した単独の公開鍵、秘密鍵ペアに基づいたCAにより発行されたすべての証明書のセット(3)公開鍵、秘密鍵ペアが利用されたかにかかわらず、CAによって発行されたすべての証明書 ・ 加入者の証明書が一時停止されたことを加入者に通知する手続 ・ 一時停止申請入力が外部登録局によって出され、処理された加入者の証明書の一時停止について外部登録局が通知を受ける手続 ・ 加入者の証明書ステータス情報が、いつどのように証明書一時停止で更新されるか。	34 CAは、証明書一時停止をサポートしません。
証明書ステータス情報の規定。下記を含む。 ・ どのようなメカニズムが使用されているか(CRL、OCSPその他)。 ・CRLメカニズムが使用されている場合、発行の頻度 ・信頼者のCRLへのチェック要求 ・オンライン失効、ステータスチェックの可用性 ・ オンライン失効、ステータスチェックの信頼者の実施要求事項 ・失効広告の、他のフォームの利用可能性 ・ 失効広告の、他のフォームの信頼者による利用可能性 ・ 秘密鍵の危殆化の結果としての、失効と一時停止の上記条項の検証(失効や一時停止の他の理由と反対して) ・ CRL や他の証明書ステータス情報を保管、保持していることへのCAの要求事項 ・ すべての証明書のコピーが発行されるか(すべての期限切れや失効、一時停止済み証明書を含む)保持期限の保持や開示 ・ オンラインステータスメカニズム(例えば、OCSP)が利用されている場合、証明書ステータス申請内容の要求事項 ・ オンラインステータスメカニズム(例えば、OCSP)が利用されている場合、明確な回答メッセージデータの要求事項 ・ 明確な反応メッセージに電子署名するのにどんな鍵が利用されるか。 ・ 証明書ステータス申請に対して返信があった場合、CAはエラーメッセージに署名するかどうか。	35 CAは、午後11時59分に、1日1回CRLを発行します。さらには、CAの人員が(すなわち、重大な秘密鍵危殆化のイベント)それを必要であるとみなす場合、あるいは証明書ポリシーによって規定されるように、CAは仮のCRLを発行します。 証明書ポリシーで述べられるように、CRLの調査はすべての 信頼者のために要求されます。 加入者は、電子メール、郵便、あるいは電話によって証明書の失効を通知されます。CP は失効広告の他のフォームを定義します。 CAはおおむね10年以上、すべての証明書とCAによって提供されたCRLを保管し、保持しています。 CAは、OCSPを利用してオンライン証明書チェックをもサポートしています。 CAは、下記のデータを含むOCSP申請を要求します。 ・プロトコルのバージョン ・サービス申請 ・対象となる証明書の識別子 ・OCSPレスポンダにより処理されるかもしれない任意の拡張 下記を含む明確なOSCP反応メッセージ ・回答構文のバージョン ・レスポンダの名前 ・申請における各証明書への回答(対象となる証明書の識別子、証明書ステータス数値、回答検証間隔、任意の拡張を含む) ・任意の拡張 ・署名アルゴリズムOID ・回答のハッシュを通じて計算された署名 すべての明確な回答メッセージは、疑問符のついている証明書を発行したCAに帰属する鍵により電子的に署名されている。 CA が証明書ステータス申請の返信としてエラーメッセージを受け取った場合、エラーメッセージには電子署名しない。

規準	開示例
証明書プロファイル。下記を含むこと。 ・サポートされるバージョン番号 ・証明書拡張の周知とその重要性 ・オブジェクト識別子の暗号化アルゴリズム ・CA、RA、加入者名のために使う名前のフォーム（つまりネーミング階層は、証明書テーマが唯一無二に識別されることができることに用いられる） ・利用される名前制約、名前フォーム ・構文と意味を定義するポリシー ・暗号アルゴリズム目的識別子 ・適用される証明書ポリシー目的識別子 ・ポリシー限定拡張の利用	36　X.509 証明書フォームの下記のフィールドは CA の PKI で利用される。 ・ V3 にバージョンをセット ・シリアル番号―CA ドメインの各証明書の唯一無二な値 ・署名アルゴリズム識別子―証明書に署名するため CA が利用するアルゴリズム ・発行者―証明書発行者識別子 ・正当性―有効期間の有効性スタート日付と終わり日付が定義される。 ・対象者―証明書主題の識別名の発行者身元確認 ・公開鍵情報―アルゴリズム識別子（すなわち、SHA -1 と RSA）と公開鍵 ・発行者に唯一無二な識別子 ・対象者に唯一無二な識別子 ・拡張
CRL プロファイル。下記を含むこと。 ・CRL のためにサポートされるバージョン番号 ・CRL と CRL 入力拡張の周知とその重要性	37　X.509 CRL フォームの下記のフィールドは CA によって利用されます。 ・バージョン―V2 ・ 署名 ―CRL に署名するのに使うアルゴリズムを識別 ・ 発行者―CRL を発行する CA の識別 ・ 今回の更新―CRL 発行日時 ・ 次回の更新―次に予期される CRL 発行日時 ・ 失効された証明書―失効された証明書情報のリスト CA は、代わりにオンラインの証明書ステータスと失効の調査サービスをサポートします。
IC カード管理ライフサイクル。下記を含むこと。 ・IC カードが CA(又は RA)によって出されるか。 ・ サポートされる場合、CA の IC カード管理ライフサイクルプロセス、IC カード配送プロセスの記述	38　CA は、加入者に IC カードを出しません。加入者は、自身の裁量において、鍵生成と記憶装置の目的のために IC カードとリーダーを購入できます。
CA 環境の内部統制	
CPS と CP の管理。 ・ CPS と CP 変更管理手続 ・公開と通知ポリシー ・CPS と CP 承認手続	39　この CPS への修正は加入者、証明書信頼者、CA によって提供された CRL を利用する当事者への影響を最小にすべきであると CA のポリシー機関がみなすことができます。このような修正は CPS のユーザーにこの CPS のバージョン数を変えないで通知なしでできます。CA のポリシー機関によってこの CPS のユーザーに重要な影響を与えると思われる CPS への修正のみならず、CPS はこれによってサポートされるポリシーがこの CPS のためにユーザーとバージョン数の変更と証明書への修正を 45 日で通知できます。 重要な修正の 45 日前にこの CPS に、CA のポリシー機関は CA の Web サイト上に来たる変更の通知を提供します。 この CPS とどんな次の変更でも CA のポリシー機関によって承認されます。
CA の終結。CA が CA 又は RA の、保管機関の身元確認を含む終了通知と終了手続の CA 手続の記述を含む。	40　CA は、CA の役員会によって終結させることができます。CA が終結する場合、CA の下で開示されたすべての証明書は無効にされ、CA は、証明書を開示することをやめます。CA は、CA のサービスを利用しているすべてのビジネス単位への 1 か月間以上程度の通知を提供します。終結後、CA の記録は保存されて、特定の保管機関に転送されます。

規準	開示例
機密保持。下記を含むこと。 ・ 情報の機密性を維持するための適用される法規要件 ・機密に保たれる情報の種類。 ・ 機密でないと考えられる情報の種類 ・証明書失効と一時停止に関する情報開示 ・司法機関への発行 ・民間の発見の一部としての公開 ・ 所有者の申請に基づく開示 ・ 他の情報公開状況	41 CAによってパブリックドメイン情報であると考えられない機密にしておかれるはずである情報 機密情報は、下記を含む。 ・加入者の秘密署名鍵は機密であって、CA又はRAに提供されません。 ・セキュリティパラメータと監査証跡のような、CAの運用と制御に特殊な情報がCAによって秘密に保たれ、法律によって必要とされない場合、CA組織外に公表されません。 ・ 加入者についての情報がCA又はRAによって、証明書で公開されるCRL、証明書ポリシー、あるいは機密であると思われるCPSを除いて、証明書ポリシーによって要求されるか、あるいはさもなければ法律によって要求される以外に、CA以外に公表されるべきでありません。 ・一般に、開示がCA経営者により必要とみなされない場合、年度の検証の結果は機密にしておかれます。 機密でない情報は、下記を含む。 ・証明書とCAによって提供されたCRLに含まれた情報は機密として取り扱いません。 ・このCAによってサポートされる証明書ポリシーでの情報は機密として取り扱いません。 ・CPS（あるいはCAビジネス実務開示）で開示されたCAの情報は機密として取り扱いません。 ・CAが証明書を無効にするとき、失効理由が無効にされた証明書のCRL項目に含められます。すべての他の加入者と信頼者が共有することができる失効理由コードは機密として取り扱いません。しかしながら、失効に関する他のどのような詳細も通常明らかにされません。 CAは、司法機関職員に情報を公開するために法律上の要件に従います。 CAは、所有者の申請により別の当事者にこのような情報の所有者に関する情報を明らかにできます。
知的財産権	42　公開鍵証明書と CA によって提供された CRL は CA の財産です。CPS と関連した証明書ポリシーは、CA の財産です。
物理的セキュリティコントロール。下記を含む。 ・ サイトの場所と建設 ・ 電源と空調 ・ CA 設備へのアクセス制限、認証統制を含む、物理的なアクセスコントロール ・ 水害 ・ 火災の予防、防止 ・ メディア記憶装置 ・ 廃棄物の処分 ・ 遠隔地のバックアップ	43　すべての重大な CA 運用は機微なハードウェアあるいはソフトウェアへアクセスする少なくとも 4 階層のセキュリティの物理的に安全な設備で行われます。CA の正当な従業員だけがそれらにアクセスすることができるように、このようなシステムは物理的に組織の他のシステムから分離されます。 CA システムへの物理的なアクセスは厳密に制御されています。正当なビジネス上の理由を持っている信頼できる個人だけがこのようなアクセスを用意されます。アクセスコントロールシステムは常に機能しており、アクセスのために入室カードとバイオメトリクスを利用します。 すべての CA システムは適当な営業上の環境を提供する業界標準の電源と空調システムを持っています。 すべての CA システムは漏水の影響を最小にするための合理的な回避メカニズムを持っています。 すべての CA システムは業界標準の火災防止と保護メカニズムを持っています。 CA 第三者プロセッサにおいてのメディアストレージは CA ハードウェアと比べて同じ程度の保護の適用を受けています。CA の内部統制の下のメディアストレージは会社の標準的なメディア記憶装置要件の適用を受けています。 廃棄物が組織の標準的な廃棄物処分要件のとおりに処分されます。暗号装置は物理的に破壊されるか、あるいは処分の前に製造業者の指針に従って初期化します。 遠隔地のバックアップが、付保している第三者記憶装置設備によって物理的に確かな方法で保管されます。
ビジネス継続性管理の内部統制。下記を含む。 ・ CA が重大なビジネスプロセスの中断あるいは障害の後に適度にタイムリーな方法で CA のビジネス運用を保持しているか、あるいは復元するビジネス継続性計画を持っているか。 ・ CA のビジネス継続性計画が許容できるシステム一時停止と復旧時間を定義し定義された時間を開示しているか。 ・ CA の主要サイトの設備復旧見込 ・ 不可欠なビジネス情報とソフトウェアのバックアップコピーをどのように取るか。	44 重大なビジネスプロセスの中断あるいは障害の後に適度にタイムリーな方法で CA は、CA のビジネス運用を復元するためのビジネス継続計画を有します。CA のビジネス継続計画は主要な自然災害あるいは CA の秘密鍵危殆化の場合、24 時間を受容できるシステム一時停止時間と定義します。 不可欠なビジネス情報と CA システムソフトウェアのコピーが毎日行われます。 CA は、CA の主要なサイトからおよそ 50 マイル（80km）に位置している復旧サイトを保持しています。
イベント記録、下記を含む。 ・ CA がイベント記録データを保存する頻度 ・ CA がイベント記録データをレビューする頻度	45 CA についてシステムバックアップ手続を予定した、監査証跡ファイルが少なくとも毎日、媒体にバックアップをとられます。監査証跡ファイルが週単位でシステム管理者によって保存されます。

規準	開示例
	イベント記録が CA 経営者によって少なくとも週単位でレビューされます。

原則 2:サービスのインテグリティ 認証局は下記についての合理的な保証を提供するために有効な内部統制を保持する。

- 加入者の情報が適切に認証されている（ABC-CA によって実施される登録活動として）
- 鍵と証明書のインテグリティがそのライフサイクルを通じて確立されている。

規準	内部統制の例 (ANSI X9.79 草案に詳しく書かれている内部統制手続に基づく)
2.1 鍵ライフサイクル管理の内部統制	
2.1.1 CA 鍵の生成 CA の鍵が工業規格のとおりに生成されるという合理的な保証を提供する内部統制を保持している。	1 CA 鍵の生成が、（原則 1、項目 17 参照）CA のビジネス実務で開示されるように、適切な ISO 15782-1 / FIPS 140-1 / ANSI X9.66 レベル要件を満たしている安全な暗号化装置で行われる。
	2 CA による CA 鍵生成が適切に正当な人員によってデュアルコントロールを必要とする。
	3 CA が使う鍵ペアは、それが生成した装置からそれが使う装置へ直接導入される同じ暗号化方策でそれ自身の鍵ペアを生成する。
	4 ANSI X9 あるいは ISO 基準で指定されるように、鍵の生成には乱数ジェネレーター（RNG）、あるいは擬似乱数ジェネレーター（PRNG）を使う。
	5 ANSI X9 あるいは ISO 基準で指定されるように、鍵の生成には素数ジェネレーターを使う。
	6 CA のビジネス実務（原則 1、項目 17）で開示されるように、鍵の生成には ANSI X9 あるいは ISO 基準で指定されるように、鍵生成アルゴリズムを使う。
	7 CA のビジネス実務（原則 1、項目 17）で開示されるように、鍵の生成により鍵の大きさが決まる。
	8 鍵の生成のために使われたハードウェア/ソフトウェアのインテグリティとハードウェアとソフトウェアへのインタフェースは使用前に検証される。
2.1.2 CA 鍵のストレージ、バックアップと復旧 CA の秘密鍵が秘密に保たれ、それらのインテグリティを持続するという合理的な保証を提供する内部統制を保持している。	1 CA のビジネス実務（原則 1 項目 17）で開示されるように、CA の秘密署名鍵は、適切な ISO 15782-1 / FIPS 140-1/ANSI X9.66 レベル要件を満たして安全な暗号装置で保管される。
	2 CA の秘密鍵が安全な暗号化モジュールから生成され、オフラインの処理あるいはバックアップと復旧の目的のためのストレージを保証されない場合、CA の秘密鍵は生成され、同じ暗号化モジュールの中で使われ、暗号化モジュールの外では決して生成されない。
	3 CA の秘密鍵が安全な暗号化モジュールから生成され、オフラインの処理あるいはバックアップと復旧の目的のためのストレージを保証される場合、秘密鍵は、下記のどれも含めて安全な鍵管理で生成される。 A. デュアルコントロールを使っている暗号文として B. デュアルコントロールを使い、知識/所有権を区分した暗号化鍵フラグメントで C. 別のデュアルコントロールを使っている鍵伝送装置のような安全な暗号化モジュールで
	4 CA の秘密鍵は、バックアップをとられて、保管され、物理的に安全に保たれた環境でデュアルコントロールを使って回収される。
	5 CA の秘密鍵のバックアップコピーは現在使用中の鍵と同等以上のセキュリティコントロールの適用を受けている。
	6 CA の秘密鍵のバックアップと復旧は正当な人員によってだけ行われる。
2.1.3 CA 公開鍵の配送 CA の公開鍵と関連づけられたパラメータは、インテグリティと信憑性が初回と、次の配送の間に維持されるという合理的な保証を提供する内部統制を保持している。	1 初回の配送プロセスの間に CA の公開鍵の修正を検出する（例えば、自分で署名された証明書を使う）ことに対して、CA はメカニズムを提供する。
	2 CA のビジネス実務（原則 1、項目 20）で開示されるように、CA の公開鍵のための初回の配送メカニズムは制御されている。
	3 次の CA のビジネス実務（原則 1、項目 20）の 1 つで開示したように、CA 公開鍵が初めに次の方法の 1 つを使って配られる。 A.機械可読メディア（例えば、IC カード） B.当事者の暗号化モジュールに埋め込まれる。 C.他の安全な方策
	4 CA の公開鍵は、CA のビジネス実務（原則 1、項目 21）で開示されたように、定期的に変更（再生成）される。
	5 CA のビジネス実務（原則 1、項目 21）で開示されるように、CA の公開鍵の次の配送メカニズムは制御されている。
	6 当事者が既に CA の公開鍵の認証されたコピーを持っている場合、CA のビジネス実務（原則 1、項目 21）で開示したように新しい CA 公開鍵が次の方法の一つを使って配送される。 A.CA からの直接電子送信 B.遠隔キャッシュあるいはディレクトリ C.暗号化モジュールにロード D.方法のいずれも初回の配送のために使う
2.1.4 （任意の）CA 鍵の寄託 寄託された CA 秘密署名鍵が機密に保たれるという合理的な保証を提供する内部統制を保持している。	1 第三者が CA の秘密鍵寄託証書サービスを提供する場合、当事者の間に責任と救済を概説している契約が存在する。
	2 CA の秘密署名鍵が寄託証書で持たれる場合、CA 秘密署名鍵の寄託されたコピーが現在使用中の鍵としてセキュリティコントロールの同じであるか、あるいはより大きいレベルの適用を受けている。
2.1.5 CA 鍵の使用法 CA の鍵がそれらの意図する場所で	1 CA の秘密署名鍵の起動は複数要員コントロール（すなわち、N 対 M）を使って行われる。
	2 リスク評価に基づいて必要である場合、CA の秘密署名鍵の起動は複数要因の認証（例えば、IC カードとパスワード、生体認証とパスワード）を使って行われる。

規準	内部統制の例 (ANSI X9.79 草案に詳しく書かれている内部統制手続に基づく)
それらの意図する機能のためにだけ使うという合理的な保証を提供する内部統制を保持している。	3 CA は、暗号化期間の終わりあるいは秘密鍵の危殆化が知られるか、あるいは疑われるときに鍵ペアを使うことを終える。
2.1.6 CA 鍵の破壊 CA の鍵が鍵ペアライフサイクルの終わりに完全に破壊されるという合理的な保証を提供する内部統制を保持している。	1 CA のビジネス実務 (原則 1、項目 17) で開示されるように、CA の公開鍵を破壊する認証と CA の秘密鍵が破壊される方法 (例えば、トークン解除、トークン破壊、あるいは鍵の上書き) は限定されている。
	2 CA の秘密鍵のすべてのコピーと断片は鍵ペアライフサイクルの終わりに破壊される。
	3 安全な暗号装置がアクセス可能で、永久にサービスから除去されることを知られているなら、今までにそうであったことがあるか、あるいは潜在的にどんな暗号化目的のためにでも使うことができる装置の中で保管されたすべての CA 公開鍵の鍵は破壊される。
	4 CA の暗号装置がサービスから永久に除去される場合、暗号目的で利用されてきた当該装置に含まれるいかなる鍵も、当該装置から消去される。
	5 CA の暗号装置の箱が耐タンパー性を意図しており、当該装置がサービスから永久に除去される場合、箱は破壊される。
2.1.7 CA 鍵の保管 保存された CA の鍵が機密に保たれ、決して実運用に戻されないという合理的な保証を提供する内部統制を保持している。	1 保存された CA の鍵は、現在使用中の鍵と同等以上のセキュリティコントロールの適用を受けている。
	2 すべての保存された CA の鍵は、物理的に安全なサイトでデュアルコントロールを使って保管期間の終わりに破壊される。
	3 保存された鍵は、決して実運用に戻されない。
	4 保存された鍵が技術的に許される最も短い期間で復旧される。
	5 保存された鍵が定期的に保管期間の終わりにそれらが適切に破壊されることを保証すると確かめられる。
2.1.8 CA の暗号化ハードウェアライフサイクルの管理 CA の暗号化ハードウェアに対して、適切に権限を付与された要員だけがアクセスするという合理的な保証を提供する内部統制を保持している。	このセクションの目的としては、CA の暗号化ハードウェアは、CA の秘密署名鍵を含む装置を指す。
	1 ポリシーと手続が、暗号化ハードウェアが タンパー証明パッケージを使っている書留郵便によって製造業者から送られることを要求する。
	2 暗号化ハードウェアの受領の際に製造業者から、正当な CA の人員が、シールが手つかずであるかどうか確認するためにタンパー証明パッケージの点検をする。
	3 タンパーを回避するため、CA の暗号化ハードウェアは次の特徴を持って、正当な人員に、アクセスが限定されているという状態で、安全な場所に保管されなくてはならない。 A. 各装置の資産管理プロセスと生成、到着、状態、出発、あて先を管理する手続 B. アクセス制御プロセスと物理的なアクセスを制限する手続が人員の承認手続 C. 設備と装置記憶装置メカニズム (例えば、金庫) へのすべてのアクセス成功あるいは失敗がイベントジャーナルに記録される。 D. 障害プロセスとイベント記録と異常なイベント、セキュリティ違反と調査、報告するための手続 E. 内部統制の有効性を確かめるための検証プロセスと手続
	4 暗号化ハードウェアが耐タンパーパッケージでしまっておかれる。
	5 暗号化ハードウェアの取扱いは 2 人あるいはそれ以上の信頼できる従業員の立会の下で行われる。
	6 暗号化ハードウェアの設置は 2 人あるいはそれ以上の信頼できる従業員の立会の下で行われる。
	7 実運用からの暗号化ハードウェアの除去は 2 人あるいはそれ以上の信頼できる従業員の立会の下で行われる。
	8 暗号化ハードウェアがサービスを提供されるか、新しいハードウェア、ファームウェア、あるいはソフトウェアで修繕されるプロセスは 2 人あるいはそれ以上の信頼できる従業員の立会の下で行われる。
	9 サービス・修理区域は資産管理と正当な人員に限定されたアクセスを持っている安全な区域である。
	10 暗号化ハードウェアが分解されて、永久に使用から除去されるプロセスは 2 人あるいはそれ以上の信頼できる従業員の立会の下で行われる。
CA の暗号化ハードウェアが正確に作動しているという合理的な保証を提供する内部統制を保持している。	11 製造業者からの CA 暗号化ハードウェアの受領に際しては、検収テストとファームウェアの設定検証が行われる。
	12 保守ないし修理された CA 暗号化ハードウェアの受領に際しては、検収テストとファームウェアの設定検証が行われる。
	13 秘密鍵のストレージと復旧とこれらの装置へのインタフェースのために使われた装置が使用前にインテグリティについて検証される。
	14 CA の暗号化ハードウェアの正しい処理が定期的に確かめられる。
	15 診断のサポートが 2 人あるいはそれ以上の信頼できる従業員の立会の下 CA 暗号化ハードウェアをトラブルシューティングにより提供される。
2.1.9 (任意の) CA によって提供された加入者鍵管理サービス CA によって生成された加入者の鍵が工業規格のとおりに生成されるという合理的な保証を提供する内部統制を保持している。	このセクションの目的としては、加入者には外部登録局が含まれる。
	1 CA (又は RA) によって行われた加入者鍵の生成が、 CA のビジネス実務 (原則 1、項目 17) で開示されるように、適切な ISO 15782-1 / FIPS 140-1 / ANSI X9.66 レベル要件を満たしている安全な暗号化装置で行われる。
	2 ANSI X9 あるいは ISO 基準で指定されるように、CA (又は RA)によって行われた加入者鍵の生成は乱数ジェネレーター (RNG)、あるいは擬似乱数ジェネレーター (PRNG) を使う。
	3 ANSI X9 あるいは ISO 基準で指定されるように、CA (又は RA) によって行われた加入者鍵の生成は素数ジェネレーターを使う。
	4 CA (又は RA) のビジネス実務 (原則 1、項目 17) で開示されるように、加入者鍵生成が ANSI X9 あるいは ISO 基準で指定されるように、CA の使用によって鍵生成アルゴリズムを実行した。
	5 CA (又は RA) のビジネス実務 (原則 1、項目 17) で開示されるように、CA によって行われた加入者鍵の生成により鍵の大きさが決まる。
	6 CA (又は RA) のビジネス実務 (原則 1、項目 17) で開示されるように、CA によって行われた加入者鍵の生成が正当な人員によって行われる。

規準	内部統制の例 (ANSI X9.79 草案に詳しく書かれている内部統制手続に基づく)
	7 加入者鍵の生成が CA (又は RA)によって行われるとき、CA のビジネス実務 (原則 1、項目 18) で開示されるように、CA (又は RA)は安全に (秘密に) 加入者のために CA (又は RA)によって生み出される鍵ペアを与える。
認証局は CA によって保管された加入者公開鍵が機密に保たれ、それらのインテグリティを維持するという合理的な保証を提供する内部統制を保持している。	8 CA によって保管された加入者秘密鍵が暗号化アルゴリズムを使っている暗号化されたフォームとリスク評価と CA のビジネス要件に基づいた鍵長で保管される。
	9 CA が加入者のために鍵ペアを生成するなら、CA は、その加入者の秘密鍵が鍵の所有者以外の当事者に明らかにされないことを保証する。
	10 CA が公開 /秘密電子署名鍵ペアを生成する場合、CA は、電子署名公開鍵のコピーも保持せず、その鍵は加入者に配送される。
	11 CA が加入者鍵のストレージを提供するなら、バックアップと復旧と加入者秘密鍵のバックアップと復旧が正当な人員によってのみ行われる。
	12 CA が加入者鍵のストレージ、バックアップと復旧を提供する場合、加入者の秘密鍵のインテグリティがそのライフサイクルを通じて維持されることを保証するための内部統制が存在する。
認証局は CA によって保管された加入者の鍵が鍵ペアライフサイクルの終わりに完全に破壊される合理的な保証を提供する内部統制を保持している。	13 CA が加入者鍵のストレージを提供する場合、CA のビジネス実務 (原則 1、項目 22) で開示されるように、加入者の秘密鍵を破壊する認証と (例 、鍵の上書きのために) 加入者の秘密鍵を破壊する手段は限定されている。
	14 CA が加入者鍵のストレージを提供する場合、加入者の秘密鍵のすべてのコピーと断片は鍵ペアライフサイクルの終わりに破壊される。
CA によって保存された加入者の鍵が機密に保たれるという合理的な保証を提供する内部統制を保持している。	15 CA によって保存された加入者秘密鍵が暗号化アルゴリズムを使っている暗号化されたフォームとリスク評価と CA のビジネス要件に基づいた鍵長に保管される。
	16 CA が加入者の鍵保管を提供する場合、すべての保存された加入者の鍵は、保管期間の終わりに破壊される。
CA によって寄託された加入者の鍵が機密に保たれるという合理的な保証を提供する内部統制を保持している。	17 CA によって寄託された加入者秘密鍵が暗号化アルゴリズムを使っている暗号化されたフォームとリスク評価と CA のビジネス要件に基づいた鍵長で保管される。
2.2 証明書ライフサイクルの内部統制	
2.2.1 加入者の登録	注: 申請する当事者は、RA や CA から証明書を申請する加入者、CA から証明書を申請する RA、ルート CA や上位 CA から証明書を申請する下位 CA のどれかである。
加入者が適切に識別されて、認証されるという合理的な保証を提供する内部統制を保持している。	1 CA は、必要とする外部の RA は、CA のビジネス実務 (原則 1、項目 25) で開示されるように、証明書を求めている当事者の身元を検証するか、あるいは確かめる。
	2 CA は、証明書を求めている当事者が CA のビジネス実務 (原則 1、項目 25) で開示されるように作成して、RA (あるいは CA) に適切な証明書申請データ (登録の申請) を提出しなくてはならないことを要求する。
	3 CA は、必要とする外部の RA は、CA のビジネス実務 (原則 1、項目 25) で開示されるように、証明書を求めている当事者の権限を検証するか、あるいは要求する。
	4 CA は、必要とする外部の RA は、中に含まれる情報の正確さを確かめる、CA のビジネス実務 (原則 1、項目 25) で開示されるように、当事者の証明書の申請を検証するか、あるいは求める。
	5 外部登録局を使う場合、CA のビジネス実務 (原則 1、項目 26) で開示されるように、CA は外部登録局の身元を検証する。
	6 外部登録局を使う場合、CA のビジネス実務 (原則 1、項目 26) で開示されるように、CA は外部登録局を承認する。
加入者証明書の申請が正確で、承認され、完全であるという合理的な保証を提供する内部統制を保持している。	7 CA は、証明書を求めている当事者が CA のビジネス実務 (原則 1、項目 25) で開示されるように作成をして、CA あるいは外部の RA に適切な証明書申請データを提出することを要求する。
	8 CA は、必要とする証明のために当事者が CA への署名されたメッセージでその公開鍵を提出することを要請する。CA は、それを必要とする当事者がデジタル方式で秘密鍵を使って登録の申請に署名することを要請して、それは登録の申請で含まれる公開鍵に関連している。 A. 証明書申請プロセスでエラーの検出を可能とする。 B. 公開鍵が登録されることに関して、対の秘密鍵が所有されていると証明する。
	9 公開鍵を中に含んでいた CA 使用を検証する当事者の証明書の申請を求める証明書申請提出書類上に当事者の署名を求める。
	10 外部の RA を使う場合、CA は、RA が提出するその外部ルーチンを必要とする RA によって署名されたメッセージ (証明書の申請) で CA に当事者の証明書申請データを求める。
	11 外部の RA を使う場合、CA のビジネス実務 (原則 1、項目 26) で開示されるように、CA は、RA が (そのために) それ (RA) が責任をもつ証明書申請プロセスのその部分を安全に保つことを要求する。
	12 外部の RA を使う場合、CA は、外部の RA がイベント記録で彼らの行動を記録することを要求する。
	13 外部の RA を使う場合、CA のビジネス実務 (原則 1、項目 26) で開示されるように、CA は、RA によって提出書類の信憑性を確かめる。
	14 外部の RA を使う場合、CA は、証明書の申請に RA の署名を検証する。
	15 CA のビジネス実務 (原則 1、項目 25) で開示されるように、CA 又は RA がエラーあるいは欠落の証明書の申請をチェックする。
	16 CA は、唯一無二であることを確かめるため、CA のドメインの中で当事者の識別名を求める。
	17 CA は、証明書の申請を受け入れるため身元が検証された当事者を求める。

規準	内部統制の例 (ANSI X9.79 草案に詳しく書かれている内部統制手続に基づく)
	18 CA が複製された公開鍵を検出したとき、証明書の申請は拒絶され、オリジナルの証明書は無効にされる。
2.2.2 (任意の) 証明書の更新 証明書更新の申請が正確で、承認されており、完全であるという合理的な保証を提供する内部統制を保持している。	1 加入者の証明書更新の申請は少なくとも加入者の識別名、証明書 (あるいは証明書を識別する他の情報) のシリアルナンバーと CA 又は RA が更新すべき証明書を識別することを可能にする求められた有効期間を含む。
	2 CA は、それを必要とするそこで含まれる公開鍵に関連している秘密鍵を使って当事者がデジタル方式で証明書更新の申請に署名することを要請する当事者の既存の公開鍵証明書を求める。
	3 CA 又は RA が身元を確かめる証明書更新データを処理する当事者を求め、更新される証明書を識別する。
	4 CA 又は RA が証明書更新の申請に署名を有効にする。
	5 CA 又は RA が証明書の存在と有効性が更新されると確かめる。
	6 CA 又は RA が、CA のビジネス実務 (原則 1、項目 28) で開示されるように、申請が、有効期間の延長を含めて要件を満たすことを確かめる。
	7 外部の RA を使う場合、CA は RA が提出する RA によって署名されたメッセージ (証明書更新の申請) で CA に当事者の証明書申請データを求める。
	8 外部の RA を使う場合、RA は (そのために)、CA のビジネス実務 (原則 1、項目 26) で開示されるように、それ (RA) が責任をとる証明書更新プロセスのその部分を安全に保つ。
	9 外部の RA を使う場合、CA は外部の RA がイベント記録で彼らの行動を記録することを要求する。
	10 外部の RA を使う場合、CA は RA によって提出書類の信憑性を確かめる。
	11 外部の RA を使う場合、CA は証明書更新の申請に RA の署名を検証する。
	12 CA 又は RA がエラーあるいは欠落の証明書更新の申請をチェックする。
	13 CA のビジネス実務 (原則 1、項目 27) で開示されるように、CA 又は RA が満期の前に更新の必要な彼らの証明書を加入者に通知する。
	14 更新された証明書の証明書生成と発行の前に、CA 又は RA が下記を検証する。 A. 証明書更新データ提出書類上の署名 B. 証明書更新の存在と有効性 C. CA のビジネス実務 (原則 1、項目 27) で開示されるように、申請が、有効期間の延長を含めて要件を満たすこと。
2.2.3 証明書の再生成 認証局は証明書の再生成申請が正確で、承認されており、完全であることの合理的な保証を提供する内部統制を保持している。	1 加入者の証明書再生成の申請は CA 又は RA が再生成すべき証明書を識別することを可能にするために少なくとも加入者の識別名、証明書のシリアルナンバーと求められた有効期間を含む。
	2 CA は、必要とするそこで含まれる公開鍵に関連している秘密鍵を使って当事者がデジタル方式で証明書再生成の申請に署名することを要請する当事者の既存の公開鍵証明書を求める。
	3 CA 又は RA が身元を確かめるべき証明書再生成の申請を処理する当事者を求め再生成される証明書を識別する。
	4 CA 又は RA が証明書再生成の申請に署名を有効にする。
	5 CA 又は RA が再生成するために証明書の期限と有効性を確かめる。
	6 CA 又は RA が、CA のビジネス実務 (原則 1、項目 28) で開示されるように、証明書再生成の申請が要件を満たすことを確かめる。
	7 外部の RA を使う場合、CA は RA が提出する当事者の証明書が RA によって署名されたメッセージで CA に申請を再生成することを要請する。
	8 外部の RA を使う場合、CA はそれ (RA) が (そのために) プロセスとして責任をとる証明書の一部を RA が CA のビジネス実務 (原則 1、項目 26) を開示されたように安全に再生成することを要求する。
	9 外部の RA を使う場合、CA は外部の RA がイベント記録で彼らの行動を記録することを要求する。
	10 外部の RA を使う場合、CA は RA によって提出書類の信憑性を確かめる。
	11 外部の RA を使う場合、CA は証明書再生成の申請に RA の署名を検証する。
	12 CA 又は RA がエラーあるいは欠落の証明書再生成の申請をチェックする。
	13 CA 又は RA が満期の前に必要な彼らの証明書に再生成が必要であることを加入者に通知する。
	14 生成され再生成された証明書の発行の前に、CA 又は RA が下記を検証する。 A. 証明書再生成データ提出書類上の署名 B. 再生成される証明書の存在と有効性 C. 開示された CA のビジネス実務 (原則 1、項目 28) に適合するように、有効期間の延長を含む申請であること。
証明書申請、再生成、証明書失効あるいは満期が正確で、承認されており、完全であるという合理的な保証を提供するために内部統制を保持している。	15 加入者の既存の証明書の失効あるいは満期の後に、加入者は、CA のビジネス実務 (原則 1、項目 29) で開示されるように、(§2.2.1、加入者の登録指定)、新しい再生成された証明書を得るために CA の加入者登録手続に従うように要求される。
2.2.4 証明書の発行 認証局は新しい、更新された、再生成証明書が生成されて、CA の開示されたビジネス実務のとおりに発行されるという合理的な保証を提供する内部統制を保持している。	1 CA のビジネス実務 (原則 1、項目 30) で開示されるように、CA は、適切な証明書フォーマットを使って証明書を生成する。
	2 CA のビジネス実務 (原則 1、項目 30) で開示されるように、CA は、ISO 9594/X.509 のとおりに証明書を生成する。
	3 CA のビジネス実務 (原則 1、項目 30) で開示されるように、有効期間が ISO 9594/X.509 のとおりにつけられる。
	4 CA のビジネス実務 (原則 1、項目 30) で開示されるように、延長領域が ISO 9594/X.509 のとおりに設定される。
	5 CA のビジネス実務 (原則 1、項目 30) で開示されるように、鍵使用延長領域が ISO 9594/X.509 のとおりに設定される。
	6 CA は、CA の秘密署名鍵に当事者の証明書を求める。

規準	内部統制の例 (ANSI X9.79 草案に詳しく書かれている内部統制手続に基づく)
	7 証明書が受け入れられた後、CA は証明書の発行を CA のビジネス実務 (原則 1、項目 31) で開示されるように、当事者に求める。
	8 RA を使う場合、CA は RA が証明書の申請を提出した加入者に証明書が開示される RA に通知する。
	9 証明書更新のために、CA が、§2.2.2 の証明書更新を指定したように、証明書更新の申請を承認した場合に限り、CA は有効期間と CA 署名によってだけ前の証明書とは違う証明書の新しい例を生み出して、それに署名する。
	10 再生成された証明書のために、CA は新しい証明書を生成して、それに署名する、CA が証明書を承認したなら、§2.2.3 の証明書が再生成されたことを明示したように、申請を再生成する。
	11 CA は、外部からの通知を開示し、証明書の開示を当事者に求める。
2.2.5 証明書の配送 CA の開示したビジネス実務に従って、完全で正確な証明書が発行され、加入者・信頼者が入手可能であるという合理的な保証を提供する機関が内部統制を保持している。	1 CA のビジネス実務 (原則 1、項目 32) で開示されるように、CA は CA によって開示された証明書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) を使っている信頼者にとって入手可能であるようにする。
	2 証明書発行の際に、CA のビジネス実務 (原則 1、項目 32) で開示されるように、CA はリポジトリあるいは代わりの配送メカニズムに証明書をポストする。
	3 正当な CA の人員だけが CA のリポジトリあるいは代わりの配送メカニズムを執行できる。
	4 CA のリポジトリあるいは代わりの配送メカニズムの性能はモニターされて、管理される。
	5 リポジトリあるいは代わりの配送メカニズムのインテグリティは維持される。
2.2.6 証明書の失効 認証局は、証明書が承認、検証された失効申請に基づいて無効にされるという合理的な保証を提供する内部統制を保持している。	1 CA のビジネス実務 (原則 1、項目 33) で開示されるように、CA は下記の確かな、承認された失効を容易にするために速い意思疎通の手段を提供する。 A. 1 つ以上の当事者には 1 つ以上の証明書 B. 証明書を生成するのに使う単一の公開/秘密鍵ペアに基づき CA によって証明書がすべて発行される。 C. すべての証明書が、公開/秘密鍵ペアにかかわらず、CA によって開示される
	2 CA は、検証するか、あるいは必要とする、CA のビジネス実務 (原則 1、項目 33) で開示されるように、外部の RA は、証明書の失効を求めて当事者の身元と権限を確かめる。
	3 外部の RA が失効の申請を受け入れる場合、CA は、CA のビジネス実務 (原則 1、項目 33) で開示されるように、RA が認めた方法で CA に証明書失効の申請を提出することを要求する。
	4 外部の RA が CA に失効の申請を受諾して転送し、CA がそうするための失効の本物と証明された受取りの通知を提供するなら、CA のビジネス実務 (原則 1、項目 33) で開示されるように、RA に求める。
	5 CA のビジネス実務 (原則 1、項目 33) で開示されるように、CA は証明書失効の際に証明書失効リスト (CRL) を更新する。
	6 すべての証明書失効の申請とそれらの結果は CA によってイベント記録で記録される。
	7 CA のビジネス実務 (原則 1、項目 33) で開示されるように、CA 又は RA がその証明書が無効にされた当事者に失効の本物と証明された受取りの通知を提供する。
	8 証明書更新がサポートされるところで、証明書が無効にされるとき、証明書のすべての正当なインスタンスは同様に無効にされる。
2.2.7 (任意の) 証明書の一時停止 証明書が承認、検証された証明書一時停止申請に基づいて一時停止されることの合理的な保証を提供する機関が内部統制を保持している。	1 CA のビジネス実務 (原則 1、項目 34) で、CA が提供することを開示したように、速い意思疎通の手段が下記の確かな、承認された一時停止を容易にするために備わっている。 A. 1 つ以上の当事者には 1 つ以上の証明書 B. 証明書を生成するのに使う単一の公開/秘密鍵ペアに基づき CA により証明書がすべて発行される。 C. すべての証明書が、公開/秘密鍵ペアにかかわらず、CA によって開示される。
	2 CA は、検証するか、あるいは必要とする、CA のビジネス実務 (原則 1、項目 34) で開示されるように、外部の RA は、証明書の一時停止を求めて当事者の身元と権限を確かめる。
	3 外部の RA が一時停止の申請を受け入れる場合、CA のビジネス実務 (原則 1、項目 34) で開示されるように、RA は、認証された方法で CA に証明書一時停止の申請を提出する。
	4 CA のビジネス実務 (原則 1、項目 34) で開示されるように、CA 又は RA が証明書一時停止の場合、最終当事者に通知する。
	5 証明書一時停止申請が CA のビジネス実務 (原則 1、項目 34) で開示されるように処理されて、検証される。
	6 CA のビジネス実務 (原則 1、項目 34) で開示されるように、CA は証明書一時停止の際に証明書失効リスト (CRL) その他の証明書ステータスメカニズムを更新する。
	7 CA のビジネス実務 (原則 1、項目 34) で開示されるように、証明書が許容時間だけ一時停止される。
	8 証明書一時停止が公表されると、一時停止は次の 3 つの方法の 1 つで処理される A. 一時停止された証明書の入力が、ユーザーに待機期間になされた取引を拒絶させて、それ以上の行動がない CRL 上に残留する。 B. 一時停止された証明書への CRL 入力は同じ証明書での失効入力によって取って代わられる。 C. 一時停止された証明書は明示的に公表され、入力は CRL から削除される。
	9 証明書一時停止 (待機) 項目が基礎をなしている証明書の満期あるいは一時停止であることはどちらの満期までも CRL の上に残留する。
	10 CA は、CA のビジネス実務 (原則 1、項目 34) で開示されるように、証明書一時停止を撤回するために、証明書失効リスト(CRL)及び他の証明書ステータスメカニズムを更新する。
	11 CA は、検証するか、あるいは必要とする外部の RA は、証明書の一時停止が撤回されることを要請して当事者の身元と権限を確かめる。
	12 証明書一時停止と証明書一時停止を撤回することはイベント記録で記録される。
2.2.8 証明書ステータス情報の処	1 CA のビジネス実務 (原則 1、項目 35) で開示されるように、証明書ステータス情報は、すべての関係当事者にとって利用可能である。

規準	内部統制の例 (ANSI X9.79 草案に詳しく書かれている内部統制手続に基づく)
理 完全な、正確な証明書失効リストが生成されて、タイムリーに開示されるという合理的な保証を提供する内部統制を保持している。	2 CA のビジネス実務 (原則 1、項目 35) で開示されるように、CA は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) を使って 信頼者にとって入手可能な CA によって提供されたそれぞれの証明書失効リスト (CRL) を作る。
	3 CA は、デジタル方式で当事者が CRL のインテグリティと発行の日付を検証できるように公開するそれぞれの CRL に署名する。
	4 たとえ変更が最後の証明書の発行から起こらなかったとしても、CA は、 CA のビジネス実務 (原則 1、項目 35) で開示されるように一定間隔で CRL を提供する。
	5 最小限において、無効にされた証明書を識別している CRL 項目が証明書の有効期間の終わりまで CRL の上に残留する。
	6 証明書一時停止がサポートされる場合、そのオリジナルの行動日付と有効期限を持っている証明書サスペンション (待機) 項目が証明書の標準的な満期まで CRL の上に残留する。
	7 CA ビジネス実務 (原則 1、項目 35) で開示されるように、CRL は保存される。
	8 CA は、当該 CA によって公開されたそれぞれの CRL (例えば、1、2、3) に単調な増加する連続数を含む。
	9 CRL は CA によって開示されたすべての無効にされた期限切れでない証明書の項目を含んでいる。
	10 CA のビジネス実務 (原則 1、項目 35) で開示されるように、古い CRL が適切な一定の時期の間維持される。
	11 証明書が、期限が切れて、無効にされるか、あるいは一時停止されるかにかかわらず、CA のビジネス実務 (原則 1、項目 35) で開示されるように、証明書のコピーが適切な一定の時期の間維持される。
	12 CA のビジネス実務 (原則 1、項目 35) で開示されるように、オンライン証明書ステータスメカニズム (例えば、OCSP) が利用されている場合、CA はすべての必要なデータの入った証明書ステータス調査結果 (例えば、OCSP リクエスト) を要求する。
	13 証明書ステータスリクエスト (例えば、OCSP リクエスト) を信頼者から入手するに際しては、CA は下記の場合に、信頼者に対して、はっきりとした回答を行う。 A.リクエストメッセージがよく整理されている。 B.レスポンダが要求したサービスを提供するために構築されている。 C. CA のビジネス実務 (原則 1、項目 35) で開示されるように、リクエストがレスポンダによって必要とされている情報を含んでいる。
	14 CA のビジネス実務 (原則 1、項目 35) で開示されるように、すべてのはっきりとした回答メッセージにはデジタル的に署名がなされている。
	15 CA のビジネス実務 (原則 1、項目 35) で開示されるように、はっきりとした回答メッセージには、すべての必要なデータが含まれている。
	16 三つの条件 (項目 13 に指定) のどれかが満たされていない場合、CA は CA のビジネス実務 (原則 1、項目 35) で開示されるように、署名済又は未署名のエラーメッセージを作成する。
2.2.9 (任意の) IC カードライフサイクルの管理 IC カードの作成が安全に CA (又は RA)によってコントロールされるという合理的な保証を提供する内部統制を保持している。	注:このセクションの目的としては、IC カード (例 スマートカード) には加入者の秘密鍵及び証明書を入れた装置が含まれる。
	1 CA (又は RA)は、カード発行者として、IC カード個人割当 (共通データファイル (CDF) データとその関連した暗号化鍵のローディング) をチェックする。
	2 IC カード、カード発行者とカード所有者を識別する共通のデータが IC カード共通データファイル (CDF) でカード発行者によって保管される。共通データファイル (CDF) 起動が安全に制御されたプロセスを使って、カード発行者として、CA (又は RA)によって行われる。
	3 CDF 起動の後に、IC カードは CDF がステータスを活性化したことを示す。
	4 IC カード個人割当と CDF 起動が CA (又は RA)によってログファイルに書かれる。
IC カードアプリケーションデータファイルの (ADF) 作成が安全に CA (又は RA)によってチェックされるという合理的な保証を提供する内部統制を保持している。	5 IC カードに保管された特定のアプリケーション提供元データはアプリケーションデータファイル (ADF) に位置している。アプリケーションデータファイル (ADF) 配置 (集積回路でのメモリエリアの配置) は CA によって、カード発行者として安全に制御されている。
	6 CA は、アプリケーション提供元として、ADF 個人割当 (ADF 関連の鍵とデータのローディング) をチェックする。
	7 CA は、カード発行者として、安全に制御されたプロセスを使って ADF 起動 (カード所有者による使用のための ADF の作成) をチェックする。
	8 CDF が同様に起動あるいは再起動した状態にあるとき、ADF が始動できるだけである。
	9 ADF 起動の後に、IC カードは ADF がステータスを活性化したことを示す。
	10 CA は、ADF のアロケーション、個人割当と起動をログファイルに採取する。
IC カードの使用が IC カード発行の前に CA (又は RA)によって可能にされるという合理的な保証を提供する内部統制を保持している。	11 カードが個人割当されない限り、IC カードが出されない。
	12 CDF が起動あるいは再起動した状態にないなら、IC カードが使用できない。
認証局は IC カードが CA (又は RA) によって安全に保管され配送されるという合理的な保証を提供する内部統制を保持している。	13 IC カードが配送の前に安全に保管される。
	14 IC カードの受領、起動と配送がイベント記録で記録される。IC カードとそれらのステータスの台帳が維持される。
	15 CA のビジネス実務 (原則 1、項目 38) で開示されるように、IC カードが安全に配送される。
IC カードの非活性化と再活性化が安全に CA (又は RA)によってチェックされるという合理的な保証を提供する内部統制を保持している。	16 アプリケーションデータファイル (ADF) 停止が、アプリケーション提供元として、CA によってだけ行われることができる。
	17 共通データファイル (CDF) 停止が、カード発行者として、CA によってだけ行われることができる。
	18 CDF の再起動が CA の内部統制の下で、カード発行者として行われる。
	19 ADF の再起動が CA の内部統制の下で、アプリケーション提供元として行われる。

規準	内部統制の例 (ANSI X9.79 草案に詳しく書かれている内部統制手続に基づく)
	20 ADF 停止、CDF 停止、CDF 再起動、ADF 再起動が記録される。
認証局は CA に返した IC カードの使用が安全に終えられる合理的な保証を提供する内部統制を保持している。	21 CA は、アプリケーション提供元として、ADF 終了をチェックする。
	22 共通データファイル (CDF) 終了が、カード発行者として、CA によってチェックされる。

原則 3:CA 環境の内部統制 認証局は下記についての合理的な保証を提供するために有効な内部統制を保持する。
・ 加入者と信頼者情報が適切に本物と証明されて、正当な個人に限定されて、CA のビジネス実務の開示において特定されていない使用から保護される。
・鍵と証明書ライフサイクル管理運用の継続性は維持される。
・CA システム開発、保守と運用が適切に承認されて、CA システムのインテグリティを維持するために行われる。

規準	内部統制の例 (ANSI X9.79 草案に詳しく書かれている内部統制手続に基づく)
3.1 認証局運用規程と証明書ポリシーの管理	
認証局は、CA の CPS、CP 管理の内部統制が効果的であるという合理的な保証を提供する内部統制を保持している。	1 CA 組織は CA の認証局運用規程 (CPS) を指定して、承認するための最終の権限と責任をもつ管理グループを持っている。
	2 証明書ポリシーを指定して、承認するための責任と最終の権限がポリシー管理機関にある。
	3 ポリシー管理機関 (あるいは同等のグループ) はビジネスリスクを評価して、セキュリティ要件と操作上の手続が下記のために適用される証明書ポリシーあるいは認証局運用規程に含められると決定するために評価を行う。 A. 鍵ライフサイクル管理の内部統制 B. 証明書ライフサイクル管理の内部統制 C. CA 環境の内部統制
	4 CA の CPS は承認され、定義されたレビュープロセスのとおりに、CPS を保持しているための責任を含めて修正される。
	5 CA は、すべての適切な加入者と信頼者にその公共の認証局運用規程 (CPS) を利用可能にする。
	6 CA の CPS への修正が加入者と信頼者にとって入手可能であるようにする。
	7 証明書ポリシーが承認され、定義されたレビュープロセスのとおりに、証明書ポリシーを保持するための責任を含めて修正される。
	8 定義されたレビュープロセスが、証明書ポリシーが CA の CPS によってサポートされることを保証するために存在する。
	9 CA は、すべての適切な加入者と信頼者に CA によってサポートされる証明書ポリシーを利用可能にする。
	10 CA によってサポートされる証明書ポリシーへの修正を加入者と信頼者にとって入手可能にする。
3.2 セキュリティ管理	
経営者の指示と情報セキュリティに対するサポートが提供されるという合理的な保証を提供する内部統制を保持している。	1 情報セキュリティポリシー文書 (セキュリティポリシー) が適切な管理者によって承認されすべての従業員に発表され、伝達される。
	2 セキュリティポリシーは、それを可能にしているメカニズムとして情報共有のために情報セキュリティの定義、その全体的な目的と範囲とセキュリティの重要性を含んでいる。
	3 セキュリティポリシーは、情報セキュリティのゴールと原則をサポートして、経営理念の記述書を含んでいる。
	4 セキュリティポリシーは、下記を含めてセキュリティポリシー、組織への特定の重要性を持っている原則、基準と遵守要件の説明を含んでいる。 A. 法、契約の要件の遵守 B. セキュリティ教育要件 C. ウィルスと他の悪意があるソフトウェアの予防検出 D. ビジネス継続管理 E. セキュリティポリシー違反の結果
	5 セキュリティポリシーは、情報セキュリティ管理に対する一般的な、特定のセキュリティ事件の責任、報告を含む定義を含んでいる。
	6 セキュリティポリシーは、ポリシーをサポートする文書への参照を含んでいる。
	7 セキュリティポリシーを保持している、責任と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。
情報セキュリティが組織の中で適切に管理されるという合理的な保証を提供する内部統制を保持している。	8 経営陣上層部あるいはレベルが高い管理情報セキュリティ委員会が明確な指示とセキュリティ指導に対する目に見える管理サポートがあることを保証する。
	9 管理グループあるいはセキュリティ委員会が情報セキュリティ対策の導入を調整するために存在する。
	10 個別の資産保護のための特定のセキュリティプロセスを実行するための責任が明らかに定義される。
	11 新しい情報処理設備の管理認証プロセスが存在して、とられる。
第三者による CA 設備、システムと情報資産へのアクセスのセキュリティを維持するという合理的な保証を提供する内部統制を保持している。	12 常駐委託業者と取引パートナーあるいはジョイント・ベンチャーを含む第三者によって CA 設備とシステムに物理的、論理的なアクセスをコントロールするために従われる手続が存在する。
	13 CA のために CA 設備とシステムに第三者アクセスを可能とするビジネスの必要がある場合、リスク評価がセキュリティ目標と特定の内部統制要件を確認するために行われる。
	14 CA 設備とシステムに第三者アクセスに関する取り決めはすべての必要なセキュリティ要件を含んでいる正式の契約に基づいている。

他の組織あるいは当事者に委託された CA に対する責任が作用するとき、情報のセキュリティが保持されるという合理的な保証を提供する内部統制を保持している。	15 CA がすべての管理と内部統制あるいはその情報システム、ネットワーク、あるいはデスクトップ環境を委託する場合、CA のセキュリティ要件は当事者の間に承認された契約で扱われる。
	16 認証局サービス・プロバイダーは認証局の役割と機能の一部を委譲することを選択でき、認証局サービス・プロバイダーは実施される特定の機能及び認証局運用規程（すなわち、CPS）の作成と保持の完遂に最終的に責任がある。
3.3 資産の分類と管理	
CA の資産と情報が保護の適切なレベルを受けるという合理的な保証を提供する内部統制を保持している。	1 所有者がすべての主要な CA 資産のために識別されて、適切な内部統制の保持に対する責任を割り当てられる。
	2 重要な CA 資産の台帳が保持される。
	3 CA は、情報分類を実行し、あるいは情報を共有するか制限するかといったビジネス影響度と必要性を考慮する情報のための関連する保護統制を採用している。
	4 情報にラベルをはることと取扱いが CA の情報分類体系のとおりに行われることを保証するために手続が定義される。
3.4 人員のセキュリティ	
認証局は人員と雇用の実務が、CA の運用の信頼性を強化し、支援するための合理的な保証を提供する内部統制を保持している。	1 セキュリティ役割と責任が、組織のセキュリティポリシーで指定されるのと同様に、職務記述で文書化される。
	2 常勤職員の身元調査が採用時に行われる。CA のポリシーと手続は管理人のスタッフを含めて経歴調査と信頼できる役割を満たしている人員と他の人員、雑用係を含めて要求される。
	3 従業員が彼らの初回の条件の部分と雇用の条件として機密保持（非公開）合意に署名する。
	4 契約社員の管理は下記を含む。 A. 契約社員の採用条件 B. 契約社員の行為による損害賠償金を含む契約要件 C. 契約社員の監査とモニタリング
	5 組織のすべての従業員、適切である場合は、第三者ユーザーが、組織的なポリシーと手続で適切なトレーニングを受ける。CA のポリシーと手続は下記を指定する。 A. トレーニング要件とそれぞれの役割のためのトレーニング手続 B. 再教育期間とそれぞれの役割のための再教育手続
	6 定期的なレビューが鍵管理と関係がある証明書の管理と関係がある活動に関係している人員の継続的な信頼性を確かめるために行われる。
	7 正式の規律上のプロセスが存在して、組織的なセキュリティポリシーと手続に違反した従業員のためにとられる。CA のポリシーと手続は無許可の行動、権限の無許可の使用とシステムの無許可の使用のために人員に対して制裁を指定する。
	8 従業員が、内部統制とセキュリティがこのような事象によって害されないように、退職するとき、適切な、タイムリーな行動がとられる。
3.5 物理的、環境的セキュリティ	
CA 設備への物理的なアクセスが適切に正当な個人に制限され、CA 設備が環境のリスクから保護されるという合理的な保証を提供する内部統制を保持している。	1 物理的な保護がビジネス家屋と CA 設備の周りに明らかに定義されたセキュリティ境界線（すなわち、物理的な障壁）の作成を通して達成される。
	2 建物の境界線あるいは CA 設備を含む区域が物理的に健全（すなわち、そこに侵入が容易に起こりうる境界線での弱点がない）である。
	3 有人の受信エリアあるいは物理的なアクセスをコントロールする他の手段が建物へのアクセスを制限するか、あるいは正当な人員のみにハウジング CA の運用を設置するために備わっている。
	4 無許可の侵入と環境の汚染を妨げるために、CA のビジネス実務（原則 1、項目 43）で開示されるように、適切な物理的な障壁が（例えば、二重床や吊り天井でも本当の床から本当の天井まで）備わっている。
	5 CA 設備の周りのセキュリティ境界線の上のすべての防火扉は警備されていて、隙間なく閉まる。
	6 侵入者検出システムが CA 設備と CA 設備それ自身を収容している建物のすべての外部の入口をカバーするために据え付けられて、規則的に検証される。
	7 無人のとき、CA 設備は警備されている。
	8 CA 設備は物理的に錠を掛けられて、無人のとき、定期的にチェックされる。
	9 安全な CA 設備での監督されていない仕事は共に安全の理由及び悪意がある活動の機会を妨げるために許されない。
	10 すべての人員は目に見える身元確認を身につけるように要求されて、目に見える身元確認を身につけていない人には誰にでも強く糾問しなければならない。
	11 CA のビジネス実務（原則 1、項目 43）で開示されるように、CA 設備へのアクセスは認証コントロールの使用を通してだけ正当な人々に制御されていて、限定されている。
	12 CA 設備に入って、去るすべての人員は記録される（すなわち、安全に維持されたアクセスのすべての監査証跡）。
	13 CA 設備への来訪者が監督され、彼らの入退日時は記録される。
	14 要求された場合のみ、第三者支持サービス人員が CA 設備を安全に保つために限定されたアクセスを認められこのようなアクセスは承認されて、モニターされる。
	15 CA 設備へのアクセス権が規則的にレビューされて、更新される。
認証局は資産の危殆化とビジネス活動の中断が妨げられる損失、損害に用意するという合理的保証を提供する内部統制を保持している。	16 環境の脅威とリスクと無許可のアクセスの機会のリスクを軽減するように装置が維持され、あるいは保護される。
	17 装置が停電と他の電気の異常から保護される。
	18 データを運び、CA サービスのサポートする電力・通信ケーブルが傍受あるいは損害から保護される。
	19 装置がその継続的な有効性とインテグリティを保証するために製造業者の指令あるいは他の文書化された手続のとおりに保持される。

	20 記憶装置媒体（すなわち、固定されているハードディスク）を含んでいる装置のすべての項目はそれらが処分あるいは再利用の前に機密性が高いデータを含んでいるかどうか決定するためにチェックされる。機密性が高い情報を含んでいる記憶装置が物理的に破壊されるか、あるいは処分・再利用の前に安全に上書きされる。
情報と情報処理設備の危殆化あるいは盗みが妨げられるという合理的な保証を提供する内部統制を保持している。	21 必要とされないとき、CA 設備が立ち退かれるとき、機微あるいは重要なビジネス情報がロックされる。
	22 パーソナル・コンピュータとワークステーション上にログオンしている状態にしておかれなくて、使用中でないとき、キーロック、パスワード、あるいは他の内部統制によって保護される。
	23 装置、情報と組織に帰属しているソフトウェアが認証なしで施設外に持っていけない。
3.6 運用管理	
CA 情報処理設備の正しい、セキュリティが高い運用が保証されるという合理的な保証を提供する内部統制を保持しているという。	1 CA の運用手続が文書化されて、保持される。
	2 正式の管理責任と手続が CA 装置、ソフトウェアと運用手続に対するすべての変更を統制するために存在する。
	3 無許可の修正あるいは情報の誤用、サービスの機会を減らすために職務の範囲と義務が分離される。
	4 開発とテスト設備が運用設備から分離される。
	5 外部の設備管理サービスを使う前に、リスクが識別され、適切な内部統制が委託先と合意され、契約に取り入れられる。
CA システム障害のリスクが最小にされるという合理的な保証を提供する内部統制を保持している。	6 容量需要がモニターされ、将来の容量要件の予測が適切な処理能力と記憶装置が利用可能であることを保証する。
	7 新しい情報システム、更新、新バージョンのシステムの検収基準が確立されており、適合テストが検収前に実行される。
CA システムと情報のインテグリティをウィルスと悪意があるソフトウェアから保護するという合理的な保証を提供する内部統制を保持している。	8 ウィルスと悪意があるソフトウェアから保護するための検出と防止のコントロールと適切なユーザーへの周知手続が整備される。
報告と対応手続の利用を通じてセキュリティ事件と障害による損害を最小にするという合理的な保証を提供する内部統制を保持している。	9 正式の報告手続、事件報告を受けたときに取るべき行動を列挙する事件対応手続が共に存在し、遵守される。
	10 CA のユーザーがセキュリティのシステム又はサービスでの弱点あるいはそれへの脅威を観察するか、あるいは推測するように要求される。
	11 ソフトウェア障害を報告することに対して手続が存在し、準拠されている。
	12 障害が報告され、調整行動がとられることを保証する手続が存在して、準拠される。
	13 事件と障害の種類、規模、コストは数量化されて、モニターされる。
	14 事件管理責任と手続がセキュリティ事件に対する速い、有効な、正式な対応を保証するために存在して、準拠される。
媒体を盗難や無許可のアクセスによる損害から守るために媒体が安全に処理されるという合理的な保証を提供する内部統制を保持している。	15 リムーバブルなコンピュータ媒体の管理のための手続が下記を必要とする。 A. もはや必要でない場合、組織から除去されるどんな再利用可能な媒体の前の内容も消去される。 B. 認証が組織から取り除かれたすべての媒体のために要求される監査証跡を維持するためのすべての除去の記録が保持される。 C. すべての媒体は、製造業者の仕様書のとおりに、安全な環境にしまっておかれる。
	16 もはや必要とされない場合、媒体が安全に処分される。
	17 情報の取扱と保管のための手続が存在して、このような情報を無許可の開示あるいは誤用から守るために準拠される。
	18 システムドキュメンテーションが無許可のアクセスから保護される。
3.7 システムアクセス管理	
CA システムのアクセス権が適切に正当な個人に制限されるという合理的な保証を提供する内部統制を保持している。	**ユーザーアクセス管理**
	1 アクセス制御の要件がビジネス任務のそれぞれのユーザー分類のために定義され、アクセス制御ポリシーとして文書化される。少なくとも下記を含む。 A. 役割とそれに対応するアクセス許可 B. 各ユーザーの身元確認と認証プロセス C. 職務分離 D. 多くの人々が特定の CA 運用（すなわち、M 対 N 規則）を行うように要求される。
	2 正式のユーザー登録と CA 情報システムとサービスにアクセスを与えるための登録解除手続が準拠される。
	3 アロケーションと特権の使用は限定されていて、制御されている。
	4 パスワードのアロケーションは正式の管理プロセスを通して制御されている。
	5 ユーザーのアクセス権は一定間隔でレビューされる。
	6 ユーザーがセレクションとパスワードの使用で定義されたポリシーと手続に従うように要求される。
	7 ユーザーが離席中の適切な保護を持っていることを保証するように要求される。
	ネットワークアクセスコントロール
	8 ユーザーが特に使う権限を与えられたサービスにだけ直接のアクセスを用意される。
	9 ユーザー端末からコンピュータサービスへの経路は制御されている。
	10 認められる場合、遠隔ユーザーによるアクセスは認証の適用を受けている。
	11 離れたコンピュータシステムへの接続が認証される。
	12 診断のポートへのアクセスは安全に制御されている。
	13 内部統制（例えば、ファイアウォール）は CA の内部のネットワークドメインを第三者によってアクセス可能な外部のネットワークドメインから守るために備わっている。

	14 内部統制が CA のアクセスコントロールポリシーのとおりにユーザーにとって入手可能なサービス（例えば、HTTP、FTP）を制限するために備わっている。
	15 ルーティング制御がコンピュータ接続と情報の流れが組織のビジネスアプリケーションのアクセスコントロールポリシーを破らないことを保証するために備わっている。
	16 組織によって使われたすべてのネットワークサービスのセキュリティ機能は CA によって文書化される。
	オペレーティング・システムアクセスコントロール
	17 自動的な端末識別が特定の場所にポータブルな装置に接続を認証するために使われる。
	18 CA のシステムへのアクセスは安全なログオンプロセスを使用している。
	19 活動が、責任がある個人に追跡されることができるように、すべてのユーザーは彼らの個人的な、使用のために唯一無二な識別子（ユーザーID）を持っている。
	20 パスワード管理システムがパスワード品質を保証する有効な、対話型設備を提供するために備わっている。
	21 システムユーティリティープログラムの用途が限定されて、厳格にコントロールされる。
	22 リスク評価に基づいて要求される場合、威圧警告が強要の目標であるユーザーに提供される。
	23 定義された不活動時間の後にアクティブでない端末が無許可の人々によってアクセスされることを妨げるため、CA システムはタイムアウトをサポートする。
	24 接続時の制限が、リスクが高いアプリケーションに追加のセキュリティを提供するために使われる。
	アプリケーションアクセスコントロール
	25 情報へのアプリケーションシステム機能はアクセスコントロールポリシーのとおりに限定されている。
	26 機密度の高いシステムは専用の（分離された）コンピューティング環境を必要とする。
3.8 システム開発と保守	
CA システム開発と保守活動が CA システムのインテグリティを維持するために適切に承認されるという合理的な保証を提供する内部統制を保持している。	1 新しいシステムあるいは既存のシステムへの改良のためのビジネス要件が内部統制の要件を指定する。
	2 変更管理手続が存在し、使用可能なシステム上にソフトウェアの導入のために従われる。
	3 変更管理手続が存在し、予定されたソフトウェアリリースと修正のために従われる。
	4 変更管理手続が存在し、緊急ソフトウェア修理のために従われる。
	5 検証データは保護されていて、制御されている。
	6 厳密な制御がソースライブラリをプログラムするためにアクセスの上に維持される。
	7 変更の導入は厳密に情報システムの障害のリスクを最小にするための正式の変更管理手続の使用によってコントロールされる。
	8 アプリケーションシステムがレビューされて、オペレーティング・システム変更が起こるとき、検証される。
	9 ソフトウェアパッケージへの修正は抑止され、重要な変更は厳しく制限されている。
	10 ソフトウェアの購入、使用と修正は可能なコバートチャネルとトロイのコードから保護するためにコントロールされて、チェックされる。
	11 内部統制は外注に出されたソフトウェア開発を保証するために備わっている。
3.9 ビジネス継続性の管理	
認証局は災害が生じたとき運用の継続性の合理的な保証を提供するために内部統制を保持している。	1 CA は、ビジネス継続計画を開発し維持するための、管理されたプロセスを持っている。
	2 CA は、適切なリスク評価に基づいてビジネス継続計画戦略を持っている。
	3 CA は、CA のビジネス実務（原則 1、項目 44）で開示されるように重要なビジネスプロセスの中断、障害に対しタイムリーに運用を保持し、復旧するためのビジネス継続計画を持っている。
	4 CA は、ビジネス継続計画が下記を扱うことを必要とするビジネス継続計画のフレームワークを有している。 A. 計画を作動させるための条件 B. 緊急時手続 C. フォールバック手続 D. 再開手続 E. 保守スケジュール F. 周知と教育要件 G. 個人の責任
	5 ビジネス継続計画が最新で、効果的であることを保証するために規則的に検証される。
	6 ビジネス継続計画が規則的に維持され、継続的有効性を保証するためにレビューされ、更新される。
	7 ビジネス継続計画が CA のビジネス実務（原則 1、項目 44）で開示されたとおり、障害の間に受容できるシステム停止時間、復旧と障害の間の平均時間を定義する。
	8 CA のビジネス継続計画はこれらの構成要素の 1 つあるいは更に多くの障害の場合、ハードウェア、ソフトウェアと鍵を含めて、CA システムのすべての重要な構成要素の災害復旧プロセスを組み込んでいる。
	9 CA は、計算リソース、ソフトウェア、又はデータが崩壊するか、あるいは崩壊が疑われる場合、復旧手続の利用で対処する。
	10 CA のビジネス継続計画は、自然、あるいは他の災害後一定の時期の間にその設備を安全に保つことに対して、安全な環境がオリジナルのサイトあるいは遠いホットサイトにおいて同様に再確立される前に手続を組み込んでいる。
	11 CA のビジネス実務（原則 1、項目 44）で開示されるように、不可欠なビジネス情報とソフトウェアのバックアップコピーが定期的にとられる。これらのコピーのセキュリティ要件はバックアップをとられた情報のために内部統制と調和している。
	12 CA のビジネス実務（原則 1、項目 44）で開示されるように、フォールバック装置とバックアップメディアがメインサイトにおける災害からの損害を避けるために安全な距離において設置される。

認証局は CA の秘密署名鍵の危殆化の場合、運用の継続性の合理的な保証を提供するために内部統制を保持している。	13 CA のビジネス継続計画が災害による秘密署名鍵の危殆化あるいは疑われる危殆化を扱う。
	14 CA の秘密鍵の危殆化あるいは危殆化が疑われる場合、災害復旧手続が CA の秘密鍵で署名されたすべての証明書の失効と再発行を含む。
	15 CA の秘密鍵が危殆化され、CA の公開鍵が無効にされる場合、用いられる復旧手続は下記を含む。 A. 安全な環境がどのように再確立されるか。 B. CA の古い公開鍵を失効する方法 C. CA の新しい公開鍵がユーザーに提供される方法 D. 対象者が再証明される方法
	16 CA の鍵がルート公開鍵に取って代わらなければならない場合、手続は下記の確かな、認証された失効のために備わっている。 A. CA によって開示されたすべての証明書のセット B. 危殆化した秘密鍵に基礎づけた従属的な CA 秘密鍵と対応する証明書 C. 下位 CA の秘密鍵及び対応する証明書
	17 鍵危殆化の CA のビジネス継続計画はシステムソフトウェアとハードウェア、対称、非対称の鍵で既発行の署名、暗号化したデータについて誰に通知されるか、何の行動がとられるか、を取り扱う。
CA のサービス中止の結果として生ずる加入者への信頼者の混乱の可能性が最小化されるという合理的な保証を提供する内部統制を保持している。	18 CA は、影響を受けた当事者への終了及び通知のために、CA のビジネス実務（原則 1、項目 40）で開示されるように、保管者に適切な保管された CA 記録を転送することに対して手続を保持している。
3.10 モニタリングと遵守	
CA が法律上の要件に従うという合理的な保証を提供する内部統制を保持している。	1 すべての適切な法令、規則、契約の要件は明示的に定義されて、それぞれの情報システムのために文書化される。
	2 CA のビジネス実務（原則 1、項目 42）で開示されるように、適切な手続が知的財産権に関して、専有のソフトウェアプロダクトの使用で資料の使用上の法律上の制約の遵守を保証するために実行される。
	3 組織の重要な記録が喪失、破壊と偽造から保護される。
	4 内部統制が適切な法律のとおりに個人情報を守るために適用される。
	5 経営者が情報処理設備の使用を承認し、内部統制がこのような設備の誤用を妨げるために用いられる。
	6 内部統制は暗号化コントロールへのアクセスあるいはそれの使用をコントロールするために国家の協定、法律、規則、あるいは他の手段の遵守を保証するために備わっている。
	7 CA のビジネス実務（原則 1、項目 41）で開示されるように、CA の機密保持ポリシーと手続は下記を扱う。 A. CA 又は RA によって機密にしておかれなくてはならない情報の種類 B. 機密として取り扱われる情報の種類 C. 誰が証明書の失効と一時停止の理由を知らせる権利を与えられているか D. 司法機関職員への情報の開示のポリシー E. 情報が裁判証拠となりうること F. CA 又は RA が所有者の申請により情報を開示する条件 G. 機密情報を開示する他の一定の状況
CA のセキュリティポリシーと手続の遵守が保証されるという合理的な保証を提供する内部統制を保持している。	8 マネジャーは、責任区域の中のセキュリティ手続が正確に実行されることを保証することに責任がある。
	9 CA の運用はセキュリティポリシーと基準の遵守を保証する通常のレビューの適用を受けている。
	10 CA システムが定期的にセキュリティ導入基準の準拠性についてチェックされる。
システム監査プロセスの有効性が最大にされ、システム監査プロセスからの妨害を最小化されるという合理的な保証を提供する内部統制を保持している。	11 ビジネスプロセス混乱のリスクを最小にするような運用システムの監査が計画され、承認される。
	12 システム監査ツールへのアクセスは可能な誤用あるいは危殆化を妨げるために保護される。
無許可の CA のシステム使用が検出されるという合理的な保証を提供する内部統制を保持している。	13 CA システムの使用をモニターするための手続が確立され、モニタリング活動の結果は規則的にレビューされる。
3.11 イベント記録	
重要な CA 環境で、重要な管理と証明書管理イベントが正確に、完全にログファイルに採取されるという合理的な保証を提供する内部統制を保持している。	1 CA が自動作成（電子）、あるいは適切な場合は手動のイベント記録を作る。
	2 すべての記録項目は次の要素を含む。 A. 入力の日時 B. （自動記録の）入力のシリアル、シーケンス番号 C. 入力の種類 D. 入力の発生源（例えば、端末、ポート、場所、顧客） E. 入力した当事者の身元

	3 CA は、下記の鍵ライフサイクル管理関連事象を記録する。 A. CA(及び該当あれば、加入者)鍵の生成 B. 手動暗号化鍵の導入と結果(操作者の身元とともに) C. CA(及び該当あれば、加入者)鍵のバックアップ D. CA(及び該当あれば、加入者)鍵のストレージ E. CA(及び該当あれば、加入者)鍵の復旧 F. CA(及び該当あれば、加入者)鍵の寄託活動(任意) G. CA 鍵の利用 H. CA(及び該当あれば、加入者)鍵の保管 I. サービスからの鍵化対物の除去 J. CA(及び該当あれば、加入者)鍵の破壊 K. 鍵管理運用を承認する当事者の身元 L. 鍵化体物(鍵構成要素や媒体や携帯装置に保存された鍵など)を取り扱う当事者の身元 M. 鍵及び鍵を保有する装置、媒体の管理 N. 秘密鍵の危殆化
	4 イベント記録で記録されるイベントは暗号鍵入力資料に関して次の情報を含む。 A. 証明書申請に対する受領(新規申請、更新申請、再生成申請を含む) B. 証明書公開鍵の提出 C. 対象者の提携関係の変化 D. 証明書の生成 E. CA 公開鍵の配送 F. 証明書の失効申請 G. 証明書の一時停止申請(もし該当あれば) H. CRL の生成と発行 I. 証明書の期限切れに対する措置
	5 CA は、次の暗号化装置ライフサイクル管理関連のイベントを記録する。 A. 装置の受領 B. 記憶装置からの装置の据え付け、除去 C. 装置の利用 D. 装置の除去 E. サービスと修繕のための装置の特定 F. 装置の除却
	6 CA は、(あるいはそれを必要とする RA は)次の証明書申請情報を記録する。 A. 申込者から出された本人確認書類の種類 B. 該当あれば、本人確認書類の(例えば、申込者の運転免許証番号)唯一無二な識別データ、番号、組み合わせ C. 申請書、本人確認書類のコピーの保管場所 D. 申請を受け入れる当事者の身元 E. 該当あれば、本人確認書類を検証する方法 F. 該当あれば、受け取った CA や提出した RA の名前
	7 CA は、下記のセキュリティ上の機微な事項を記録する。 A. イベント記録を含む、読み書きされたセキュリティ上の機微なファイルもしくは記録 B. セキュリティ上の機微なデータの削除 C. セキュリティプロファイルの変更 D. 成功及び失敗(認証の複数の失敗を含む)の識別認証メカニズムの使用 E. システムクラッシュ、ハードウェア障害及びその他の異常 F. コンピュータ運用者、システム管理者、システムセキュリティ統括者により取られた措置 G. 当事者の提携関係の変化 H. 暗号化、認証プロセスもしくは手続の回避決定 I. CA システムもしくは何らかの構成要素へのアクセス権
	8 イベント記録はどんな秘密鍵の共通テキスト値も記録しない。
	9 CA コンピュータシステム時計が正確な記録のために同期をとられる。
現在の、保存されたイベント記録の機密保持とインテグリティが維持されるという合理的な保証を提供する内部統制を保持している。	10 現在の、保存されたイベント記録が無許可の改ざんあるいは破壊を妨げる方式で保持される。
	11 現在の、保存された自動化されたイベント記録が改ざんあるいはすり替えから保護される。
	12 イベント記録に署名することに対して、使われた秘密鍵は、他のいかなる目的のためにも使われない。
イベント記録がビジネス実務に開示したように完全に秘密に保存されるという合理的な保証を提供する内部統制を保持している。	13 CA のビジネス実務(原則 1、項目 45)で開示されるように、CA は定期的にイベント記録データを保存する。
	14 リスク評価が保存されたイベント記録の保存のための時間の適切な長さを決定するために実施される。
	15 CA は、前もって決定された期間に安全な遠隔地の場所において保存されたイベント記録を保持している。
イベント記録が定期的に正当な権限者によってレビューされるという合	16 現在の、保存されたイベント記録が正当なビジネスあるいはセキュリティ目的のために正当な権限者によってのみ検索される。
	17 CA のビジネス実務(原則 1、項目 45)で開示されるように、イベント記録が定期的にレビューされる。

理的な保証を提供する内部統制を保持している。	18 現在の、保存されたイベント記録のレビューはイベント記録のインテグリティの妥当性検査と例外的、無許可、あるいは怪しい活動の識別とフォローアップを含む。

付録 A ー 検証報告書の開示例

この付録は認証局のための WebTrust 業務のために 6 つの報告例を提示する。1-3 は米国公認会計士協会（AICPA）証明基準に従って作成されている。

米国証明基準の下で、検証報告書の最初の段落は検証責任者がビジネス実務の開示についての経営者の記述書の検証を、認証局のための WebTrust 原則規準に従って有効な内部統制を保持したと述べる。検証責任者は、(1)経営者の記述書あるいは（2）対象事項について、直接意見を述べてもよい。両方の種類の検証報告書の例が提供されている。

合衆国での使用（すべての規準が適用可能である例）のための事例 No. 1

独立した公認会計士の検証報告書

ABC 認証局株式会社
代表取締役社長 殿

当監査法人は 2000 年○月○日から 2000 年○月○日の間の、ABC 認証局株式会社（以下、ABC-CA）が認証局(CA)サービスを提供する場所で、ABC-CA の経営者による記述書を検証した。
AICPA/CICA 認証局のための WebTrust 規準に基づいて、
・ 鍵と証明書ライフサイクル管理ビジネスと個人情報保護実務が開示されており、提供された同サービスは開示された実務に従って提供されていた。
・ 下記についての合理的な保証を提供する有効な内部統制を保持していた。
ー 加入者情報が（ABC-CA の実施した登録活動において）適切に認証されていた。
ー 鍵と証明書のインテグリティは、そのライフサイクルを通じて管理が確立され、保護されていた。
・ 下記についての合理的な保証を提供する有効な内部統制を保持していた。
ー 加入者と信頼者の情報が適切に認証され、正当な個人に制限され、CA のビジネス実務の開示において特定されていない利用から保護されていた。
ー 鍵と証明書のライフサイクル管理運用の継続性が維持されていた。
ー CA のシステム開発、保守と運用が適切に承認されて、AICPA /CICA 認証局のための WebTrust 規準に従って CA システムのインテグリティを維持するために行われた。
ABC-CA の経営者はその記述書に関して責任がある。当監査法人の責任は当監査法人の検証に基づいて経営者の記述書に関する意見を表明することである。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に従って行われた。それには下記が含まれる。(1)ABC-CA の鍵と証明書ライフサイクル管理ビジネスと個人情報保護実務、鍵と証明書のインテグリティ管理、加入者と信頼者の情報の許可と個人情報保護、鍵と証明書ライフサイクル管理運用の継続性、システムインテグリティの開発、保守、運用に関して理解すること。(2) 開示された鍵と証明書ライフサイクル管理ビジネス実務と個人情報保護実務に従って、選択した検証対象取引をテストすること。(3)内部統制の運用状況の有効性についてテストし、評価すること。(4)状況に応じて必要と認めた他の手続を実施すること。当監査法人は当監査法人の検証が当監査法人の意見に合理的な基礎を提供すると信じる。

当監査法人の意見では、2000 年○月○日から 2000 年 ○月○ 日の間に、ABC-CA 経営者の記述書は、最初の段落にあるように、AICPA/ CICA 認証局のための WebTrust 規準に基づいて、すべての重要な事項について適正に表示している。

内部統制の固有の限界のために、エラーあるいは不正が起こっても、検出されないかもしれない。さらに、当監査法人の発見事項に基づいたどんな結論の予測でも、将来の時期には（1）システムあるいは内部統制に対する変更、（2）

処理要件の変更、(3) 時間の経過によって必要となる、あるいは (4) ポリシーや手続への準拠性の程度の悪化、により当該結論の正当性が変更されるリスクに晒されている。

認証局のための WebTrust 保証シールは ABC-CA の Web サイト上にこの報告の内容の象徴的な陳述を形成するが、それはこの報告書を更新するか、あるいは追加の保証を提供するように意図されてもいないし、そう解釈されるべきでもない。

ABC-CA における特定の内部統制の相対的な有効性と重要性及び、加入者と信頼者の内部統制リスクの評価に与える影響は、彼らの内部統制への相互作用に依存しており、その他の要因は個別の加入者と信頼者の場所において示される。当監査法人は個別の加入者と信頼者の場所における内部統制の有効性を評価するための手続を実施していない。

この報告書は認証局のための WebTrust 規準で対象とした範囲を越えた ABC-CA のサービスの品質についての表現を含んでおらず、また、いかなる顧客の意図する目的のための ABC-CA のサービスの適合性についても同様である

[監査法人名]
公認会計士
[住所]
[日付]

合衆国での使用 (外部の RA を利用していたり、CA が IC カードや加入者の鍵管理サービスを利用しており、鍵寄託、証明書更新、証明書一時停止をサポートしていない場合) のための事例 NO. 2

独立した公認会計士の検証報告書

ABC 認証局株式会社
代表取締役社長 殿

当監査法人は 2000 年○月○日から 2000 年○月○日の間の、ABC 認証局株式会社 (以下、ABC-CA) が認証局(CA)サービスを提供する場所で、ABC-CA の経営者による記述書を検証した。
・ 鍵と証明書ライフサイクル管理ビジネスと個人情報保護実務が開示されており、提供された同サービスは開示された実務に従って提供されている。
AICPA/CICA 認証局のための WebTrust 規準に基づいて、
・ 鍵と証明書ライフサイクル管理ビジネスと個人情報保護実務が開示されており、提供された同サービスは開示された実務に従って提供されていた。
・ 下記についての合理的な保証を提供する有効な内部統制を保持していた。
― 加入者情報が (ABC-CA の実施した登録活動において) 適切に認証されていた。
― 鍵と証明書のインテグリティは、そのライフサイクルを通じて管理が確立され、保護されていた。
・ 下記についての合理的な保証を提供する有効な内部統制を保持していた。
― 加入者と信頼者の情報が適切に認証され、正当な個人に制限され、CA のビジネス実務の開示において特定されていない利用から保護されていた。
― 鍵と証明書のライフサイクル管理運用の継続性が維持されていた。
ABC-CA の経営者はその記述書に関して責任がある。当監査法人の責任は当監査法人の検証に基づいて経営者の記述書に関する意見を表明することである。

ABC-CA は、ABC-CA のビジネス実務の開示において開示されたように、特定の加入者の登録活動のために、外部の RA を利用している。当監査法人の検証は、外部の RA の内部統制に拡張されることを意図していない。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に従って行われた。それには下記が含まれる。(1)ABC-CA の鍵と証明書ライフサイクル管理ビジネスと個人情報保護実務、鍵と証明書のインテグリティ管理、加入者と信頼者の情報の許可と個人情報保護、鍵と証明書ライフサイクル管理運用の継続性、システムインテグリテ

ィの開発、保守、運用に関して理解すること。(2) 開示された鍵と証明書ライフサイクル管理ビジネス実務と個人情報保護実務に従って、選択した検証対象取引をテストすること。(3)内部統制の運用状況の有効性についてテストし、評価すること。(4)状況に応じて必要と認めた他の手続を実施すること。当監査法人は当監査法人の検証が当監査法人の意見に合理的な基礎を提供すると信じる。

当監査法人の意見では、2000 年○月○日から 2000 年 ○月○ 日の間に、ABC-CA 経営者の記述書は、最初の段落にあるように、AICPA/ CICA 認証局のための WebTrust 規準に基づいて、すべての重要な事項について、適正に表示している。

内部統制の固有の限界のために、エラーあるいは不正が起こっても、検出されないかもしれない。さらに、当監査法人の発見事項に基づいたどんな結論の予測でも、将来の時期には (1) システムあるいは内部統制に対する変更、(2) 処理要件の変更、(3) 時間の経過によって必要となる、あるいは (4) ポリシーや手続への準拠性の程度の悪化、により当該結論の正当性が変更されるリスクに晒されている。

認証局のための WebTrust 保証シールは ABC-CA の Web サイト上にこの報告の内容の象徴的な陳述を形成するが、それはこの報告書を更新するか、あるいは追加の保証を提供するように意図されてもいないし、そう解釈されるべきでもない。

ABC-CA における特定の内部統制の相対的な有効性と重要性及び、加入者と信頼者の内部統制リスクの評価に与える影響は、彼らの内部統制への相互作用に依存しており、その他の要因は外部の RA と個別の加入者と信頼者の場所において示される。当監査法人は外部の RA と個別の加入者と信頼者の場所における内部統制の有効性を評価するための手続を実施していない。

この報告書は認証局のための WebTrust 規準で対象とした範囲を越えた ABC-CA のサービスの品質についての表現を含んでおらず、また、いかなる顧客の意図する目的のための ABC-CA のサービスの適合性についても同様である

[監査法人名]
公認会計士
[住所]
[日付]

合衆国での使用 (すべての規準が適用可能である例) のための事例 NO. 3

独立した公認会計士の検証報告書 (直接報告書)

ABC 認証局株式会社
代表取締役社長 殿

当監査法人は 2000 年○月○日から 2000 年○月○日の間に、AICPA/CICA 認証局のための WebTrust 原則と規準に基づいて、鍵と証明書ライフサイクル管理ビジネスと個人情報保護実務の Web サイトへの開示、鍵と証明書のインテグリティ、加入者及び信頼者の認証及びプライバシー、鍵と証明書ライフサイクルの運用の継続性、システムインテグリティの開発と保守と運用に関する内部統制の有効性、に関する、ABC 認証局株式会社 (以下、ABC-CA) が認証局(CA)サービスを提供する場所で、ABC-CA の経営者による記述書を検証した。

ABC-CA の経営者はそれらの開示と内部統制に関して責任がある。当監査法人の責任は当監査法人の検証に基づいて経営者の記述書に関する意見を表明することである。

当監査法人の検証は、米国公認会計士協会によって確立された証明基準に従って行われた。それには下記が含まれる。(1)ABC-CA の鍵と証明書ライフサイクル管理ビジネスと個人情報保護実務、鍵と証明書のインテグリティ管理、加入者と信頼者の情報の許可と個人情報保護、鍵と証明書ライフサイクル管理運用の継続性、システムインテグリティの開発、保守、運用に関して理解すること。(2) 開示された鍵と証明書ライフサイクル管理ビジネス実務と個人情報

保護実務に従って、選択した検証対象取引をテストすること。(3)内部統制の運用状況の有効性についてテストし、評価すること。(4)状況に応じて必要と認めた他の手続を実施すること。当監査法人は当監査法人の検証が当監査法人の意見に合理的な基礎を提供すると信じる。

当監査法人の意見では、2000 年○月○日から 2000 年 ○月○ 日の間に、ABC-CA は、AICPA/ CICA 認証局のための WebTrust 規準に基づいて、下記の事柄を実施している。

・鍵と証明書ライフサイクル管理ビジネスと個人情報保護実務を開示し、開示された実務に準拠してサービスを提供した。
・加入者の情報が(ABC-CA によって実施される登録活動のために)適切に認証されており、彼らが管理する鍵と証明書のインテグリティが確立されており、そのライフサイクルを通じて保護されているという合理的な保証を提供する内部統制を保持した。
・加入者と信頼者の情報が承認された個人に制限されており、CA のビジネス実務の開示に特定された目的以外の利用から保護されており、鍵と証明書ライフサイクル管理の運用の継続性が保持されており、CA システムの開発・運用・保守が適切に承認されており、CA システムのインテグリティが保持されているという合理的な保証を提供する内部統制を保持した。

内部統制の固有の限界のために、エラーあるいは不正が起こっても、検出されないかもしれない。さらに、当監査法人の発見事項に基づいたどんな結論の予測でも、将来の時期には (1) システムあるいは内部統制に対する変更、(2) 処理要件の変更、(3) 時間の経過によって必要となる、あるいは (4) ポリシーや手続への準拠性の程度の悪化、により当該結論の正当性が変更されるリスクに晒されている。

認証局のための WebTrust 保証シールは ABC-CA の Web サイト上にこの報告の内容の象徴的な陳述を形成するが、それはこの報告書を更新するか、あるいは追加の保証を提供するように意図されてもいないし、そう解釈されるべきでもない。

ABC-CA における特定の内部統制の相対的な有効性と重要性及び、加入者と信頼者の内部統制リスクの評価に与える影響は、彼らの内部統制への相互作用に依存しており、その他の要因は個別の加入者と信頼者の場所において示される。当監査法人は個別の加入者と信頼者の場所における内部統制の有効性を評価するための手続を実施していない。

この報告書は認証局のための WebTrust 規準で対象とした範囲を越えた ABC-CA のサービスの品質についての表現を含んでおらず、また、いかなる顧客の意図する目的のための ABC-CA のサービスの適合性についても同様である

[監査法人名]
公認会計士
[住所]
[日付]

付録 B ー 経営者の記述の開示例

合衆国 (すべての規準が適用可能である例) での使用のための事例 NO. 1

2000 年○月○日から 2000 年○月○日の間のビジネス実務の開示と認証局運用上の内部統制に関する経営者の記述書

[日付]

ABC 認証局株式会社は ABC-CA として知られている認証局 (CA) として事業を行う。ABC-CA が、ルート CA (もしくは DEF 認証局株式会社の従属 CA) として、次の認証局サービスを提供する。

・加入者鍵の管理サービス
・加入者の登録

・証明書の更新
・証明書の再生成
・証明書の発行
・〔オンラインのリポジトリを使う〕証明書の配送
・証明書の失効
・証明書の一時停止
・〔オンラインのリポジトリを使う〕証明書ステータス情報の処理
・IC カードのライフサイクル管理

ABC-CA の経営者は、CA のビジネス実務の開示、サービスのインテグリティ（鍵と証明書ライフサイクル管理内部統制を含む）、CA 環境の内部統制を含む CA の運用に関して有効な内部統制を確立し、保持することに対して責任がある。これらの内部統制はモニタリングメカニズムを含んでおり、識別された欠陥を修正するための行動がとられる。

人間の誤謬、内部統制の迂回、無視を含む内部統制の固有の限界がある。したがって、有効な内部統制といえども ABC-CA の認証局運用に関して合理的な保証しか提供できない。さらに状況の変化により、内部統制の有効性は長い時間にわたって変化する。

経営者が CA 運用に関して内部統制を評価した。その評価に基づき、ABC 認証局株式会社（ABC-CA）の経営者の意見では、認証局(CA)の場所での運用は、2000 年 ○月○日から 2000 年○月○日の間に、AICPA/CICA 認証局のための WebTrust 規準に基づいて下記の事柄が実施されていた。
・ 鍵と証明書ライフサイクル管理ビジネス実務と個人情報保護実務を開示し、その開示された実務に準拠してサービスを提供した。
・下記についての合理的な保証を提供する内部統制を保持した。
－加入者の情報が（ABC-CA による登録活動のために）適切に認証されていた。
－彼らが管理する鍵と証明書のインテグリティが確立されており、ライフサイクルを通じて保護されていた。
・下記についての合理的な保証を提供する内部統制を保持した。
－ 加入者と信頼者の情報が適切に本物と証明され、正当な個人に限定され、CA のビジネス実務の開示において特定されていない使用から保護された。
－ 鍵と証明書ライフサイクル管理運用の継続性は維持された。
－ CA システム開発、保守、運用が適切に承認され、CA システムインテグリティを維持するために行われた。

CA ビジネス実務の開示
サービスインテグリティ

鍵ライフサイクル管理の内部統制
CA 鍵の生成
CA 鍵のストレージ、バックアップ、復旧
CA 公開鍵の配送
CA 鍵の寄託
CA 鍵の利用
CA 鍵の破壊
CA 鍵の保存
CA 暗号ハードウェアのライフサイクル管理
CA が提供する加入者鍵管理サービス
証明書ライフサイクル管理内部統制
加入者の登録
証明書の更新
証明書の再生成
証明書の発行
証明書の配送
証明書の失効
証明書の一時停止
証明書ステータス情報の処理

ICカードのライフサイクル管理

CA環境の内部統制

認証局運用規程と証明書ポリシー管理
セキュリティ管理
資産分類と管理
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
システムアクセス管理
システム開発と保守
ビジネス継続性管理
監視と準拠性
イベント記録

[氏名]
[職位]

合衆国での使用（外部のRAを利用していたり、CAがICカードや加入者の鍵管理サービスを利用しており、鍵寄託、証明書更新、証明書一時停止をサポートしていない場合）のための事例NO. 2

2000年○月○日から2000年○月○日を通しての期間のそのビジネス実務のその開示とその内部統制についての、認証局運用上の経営者の記述書

[日付]

ABC認証局株式会社はABC-CAとして知られている認証局（CA）として事業を行う。ABC-CAが、ルートCA（もしくはDEF認証局株式会社の従属CA）として、次の認証局サービスを提供する。
・証明書の再生成
・証明書の発行
・［オンラインのリポジトリを使う］証明書の配送
・証明書の失効
・［オンラインのリポジトリを使う］証明書ステータス情報の処理
ABC-CAは、ABC-CAのビジネス実務の開示において開示されたように、特定の加入者の登録活動のために、外部のRAを利用している。

ABC-CAの経営者は、CAのビジネス実務の開示、サービスのインテグリティ（鍵と証明書ライフサイクル管理内部統制を含む）、CA環境の内部統制を含むCAの運用に関して有効な内部統制を確立し、保持することに対して責任がある。これらの内部統制はモニタリングメカニズムを含んでおり、識別された欠陥を修正するための行動がとられる。

人間の誤謬、内部統制の迂回、無視を含む内部統制の固有の限界がある。したがって、有効な内部統制といえどもABC-CAの認証局運用に関して合理的な保証しか提供できない。さらに状況の変化により、内部統制の有効性は長い時間にわたって変化する。

経営者がCA運用に関して内部統制を評価した。その評価に基づき、ABC認証局株式会社（ABC-CA）の経営者の意見では、認証局(CA)の場所での運用は、2000年○月○日から2000年○月○日の間に、AICPA/CICA認証局のためのWebTrust規準に基づいて下記の事柄が実施されていた。
・鍵と証明書ライフサイクル管理ビジネス実務と個人情報保護実務を開示し、その開示された実務に準拠してサービスを提供した。
・下記についての合理的な保証を提供する内部統制を保持した。
－加入者の情報が（ABC-CAによる登録活動のために）適切に認証されていた。
－彼らが管理する鍵と証明書のインテグリティが確立されており、ライフサイクルを通じて保護されていた。
・下記についての合理的な保証を提供する内部統制を保持した。

－ 加入者と信頼者の情報が適切に本物と証明され、正当な個人に限定され、CA のビジネス実務の開示において特定されていない使用から保護された。
－ 鍵と証明書ライフサイクル管理運用の継続性は維持された。
－ CA システム開発、保守、運用が適切に承認され、CA システムインテグリティを維持するために行われた。

CA ビジネス実務の開示
サービスインテグリティ

鍵ライフサイクル管理の内部統制
CA 鍵の生成
CA 鍵のストレージ、バックアップ、復旧
CA 公開鍵の配送
CA 鍵の寄託
CA 鍵の利用
CA 鍵の破壊
CA 鍵の保存
CA 暗号ハードウェアのライフサイクル管理
CA が提供する加入者鍵管理サービス
証明書ライフサイクル管理内部統制
加入者の登録
証明書の再生成
証明書の発行
証明書の配送
証明書の失効
証明書ステータス情報の処理

CA 環境の内部統制

認証局運用規程と証明書ポリシー管理
セキュリティ管理
資産分類と管理
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
システムアクセス管理
システム開発と保守
ビジネス継続性管理
監視と準拠性
イベント記録

［氏名］
［職位］

付録 C － 経営者の確認書の開示例
合衆国（すべての規準が適用可能である例）での使用のための事例 NO. 1

［日付］

X、Y ＆ Z 監査法人
［住所］

○○監査法人 殿

2000 年○月○日から 2000 年○月○日の間に、ABC 認証局株式会社（ABC-CA）のビジネス実務の開示と認証局の運用に関する内部統制に関する当社の記述書についての貴監査法人の検証は、すべての重要な側面に関して当

社の記述書が適正に表示されているかどうかについて意見を表明する目的のためにされており、貴監査法人の意見は、当社の記述書に記載された有効な内部統制のための規準に基づいている。当社は当社の記述書に関して責任がある。貴監査法人の検証、管理に関連して下記の事柄を認めます。

A. CA ビジネス実務の開示、認証局（CA）運用の場所における有効な内部統制を確立して保持する責任、サービスインテグリティ（鍵と証明書ライフサイクル管理内部統制を含む）と CA 環境の内部統制を含めて、当社の責任であることを自覚しております。
B. 2000 年○月○日から 2000 年○月○日の間に当社の記述書に記載された ABC-CA の CA のビジネス実務の開示、サービスインテグリティ（鍵と証明書ライフサイクル管理内部統制を含む）、CA 環境の内部統制について評価を行い、規準の要求する最小要件に適合していると信じております。
C. 当社の記述書の評価について用いられ、表明された規準は、合理的で適切であると信じます。
D. ABC-CA の CA ビジネス実務の開示、サービスインテグリティ（鍵と証明書ライフサイクル管理内部統制を含めて）と CA 環境の内部統制に関連して、規準に従う会社の能力に対して不利な影響を与えることがある内部統制の設計と運用に重要な欠陥がなく、経営者の記述書と調和していることを明らかにしました。
E. 当社の記述書と関係があるすべての重要な情報及び記録を貴監査法人に提供しました。
F. 貴監査法人の検証期間に貴監査法人によって当社にされたすべての質問に回答しました。
G. 重要な欠陥に対して経営者が実施した修正行動を含む、内部統制に著しく影響を与えうる内部統制あるいはその他の要因において 2000 年○月○日以降に起こった、あるいは計画されたいかなる変化についても貴監査法人に開示しました。

ABC-CA の経営者の意見では、認証局(CA)の場所での運用は、2000 年 ○月○日から 2000 年○月○日の間に、AICPA/CICA 認証局のための WebTrust 規準に基づいて下記の事柄が実施されていた。
・ 鍵と証明書ライフサイクル管理ビジネス実務と個人情報保護実務を開示し、その開示された実務に準拠してサービスを提供した。
・下記についての合理的な保証を提供する内部統制を保持した。
－加入者の情報が（ABC-CA による登録活動のために）適切に認証されていた。
－彼らが管理する鍵と証明書のインテグリティが確立されており、ライフサイクルを通じて保護されていた。
・下記についての合理的な保証を提供する内部統制を保持した。
－ 加入者と信頼者の情報が適切に本物と証明され、正当な個人に限定され、CA のビジネス実務の開示において特定されていない使用から保護された。
－ 鍵と証明書ライフサイクル管理運用の継続性は維持された。
－ CA システム開発、保守、運用が適切に承認され、CA システムインテグリティを維持するために行われた。

CA ビジネス実務の開示
サービスインテグリティ

鍵ライフサイクル管理の内部統制
CA 鍵の生成
CA 鍵のストレージ、バックアップ、復旧
CA 公開鍵の配送
CA 鍵の寄託
CA 鍵の利用
CA 鍵の破壊
CA 鍵の保存
CA 暗号ハードウェアのライフサイクル管理
CA が提供した加入者鍵の管理サービス
証明書ライフサイクル管理の内部統制
加入者の登録
証明書の更新
証明書の再生成
証明書の発行
証明書の配送
証明書の失効

証明書の一時停止
証明書ステータス情報の処理
IC カードライフサイクルの管理

CA 環境の内部統制

認証局運用規程と証明書ポリシー管理
セキュリティ管理
資産分類と管理
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
システムアクセス管理
システム開発と保守
ビジネス継続性管理
監視と準拠
イベント記録

以上

[氏名]
[職位]

合衆国での使用（外部の RA を利用していたり、CA が IC カードや加入者の鍵管理サービスを利用しており、鍵寄託、証明書更新、証明書一時停止をサポートしていない場合）のための事例 NO. 2

[日付]

X、Y & Z 監査法人
[住所]

○○監査法人 殿

2000 年○月○日から 2000 年○月○日の間に、ABC 認証局株式会社（ABC-CA）のビジネス実務の開示と認証局の運用に関する内部統制に関する当社の記述書についての貴監査法人の検証は、すべての重要な側面に関して当社の記述書が適正に表示されているかどうかについて意見を表明する目的のためにされており、貴監査法人の意見は、当社の記述書に記載された有効な内部統制のための規準に基づいている。ABC-CA は、ABC-CA のビジネス実務の開示に開示したように、特定の登録活動について、外部の RA を利用している。当社は当社の記述書に関して責任がある。貴監査法人の検証、管理に関連して下記の事柄を認めます。

A. CA ビジネス実務の開示、認証局（CA）運用の場所における有効な内部統制を確立して保持する責任、サービスインテグリティ（鍵と証明書ライフサイクル管理内部統制を含む）と CA 環境の内部統制を含めて、当社の責任であることを自覚しております。
B. 2000 年○月○日から 2000 年○月○日の間に当社の記述書に記載された ABC-CA の CA のビジネス実務の開示、サービスインテグリティ（鍵と証明書ライフサイクル管理内部統制を含む）、CA 環境の内部統制について評価を行い、規準の要求する最小要件に適合していると信じております。
C. 当社の記述書の評価について用いられ、表明された規準は、合理的で適切であると信じます。
D. ABC-CA の CA ビジネス実務の開示、サービスインテグリティ（鍵と証明書ライフサイクル管理内部統制を含めて）と CA 環境の内部統制に関連して、規準に従う会社の能力に対して不利な影響を与えることがある内部統制の設計と運用に重要な欠陥がなく、経営者の記述書と調和していることを明らかにしました。
E. 当社の記述書と関係があるすべての重要な情報及び記録を貴監査法人に提供しました。
F. 貴監査法人の検証期間に貴監査法人によって当社にされたすべての質問に回答しました。

G.　重要な欠陥に対して経営者が実施した修正行動を含む、内部統制に著しく影響を与えうる内部統制あるいはその他の要因において 2000 年○月○日以降に起こった、あるいは計画されたいかなる変化についても貴監査法人に開示しました。

ABC-CA の経営者の意見では、認証局(CA)の場所での運用は、2000 年 ○月○日から 2000 年○月○日の間に、AICPA/CICA 認証局のための WebTrust 規準に基づいて下記の事柄が実施されていた。
・ 鍵と証明書ライフサイクル管理ビジネス実務と個人情報保護実務を開示し、その開示された実務に準拠してサービスを提供した。
・下記についての合理的な保証を提供する内部統制を保持した。
－加入者の情報が（ABC-CA による登録活動のために）適切に認証されていた。
－彼らが管理する鍵と証明書のインテグリティが確立されており、ライフサイクルを通じて保護されていた。
・下記についての合理的な保証を提供する内部統制を保持した。
－ 加入者と信頼者の情報が適切に本物と証明され、正当な個人に限定され、CA のビジネス実務の開示において特定されていない使用から保護された。
－ 鍵と証明書ライフサイクル管理運用の継続性は維持された。
－ CA システム開発、保守、運用が適切に承認され、CA システムインテグリティを維持するために行われた。

CA ビジネス実務の開示
サービスインテグリティ
鍵ライフサイクル管理の内部統制
CA 鍵の生成
CA 鍵のストレージ、バックアップ、復旧
CA 公開鍵の配送
CA 鍵の利用
CA 鍵の破壊
CA 鍵の保存
CA 暗号ハードウェアのライフサイクル管理
証明書ライフサイクル管理の内部統制
加入者の登録
証明書の再生成
証明書の発行
証明書の配送
証明書の失効
証明書ステータス情報の処理
CA 環境の内部統制
認証局運用規程と証明書ポリシー管理
セキュリティ管理
資産分類と管理
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
システムアクセス管理
システム開発と保守
ビジネス継続性管理
監視と準拠
イベント記録

以上

［氏名］
［職位］

付録 D は省略。

付録 E －認証局組織の事業活動を対象とする AICPA SAS70、AICPA / CICA 認証局のための WebTrust の報告書の比較

この文書は、示唆された規制事項の下でのレビューと報告書のフォームと内容を分析して適切な類似点と相違点を示している。認証局のための第三者意見表明に関して、それが認証局の役割を務めている組織の報告義務があるビジネス活動について特に開発されたため、最も適切なアプローチは可能なところならどこでも AICPA/CICA 認証局（CA）信頼アプローチを使うことである。

内容 / アプローチ	AICPA SAS70	AICPA/CICA 認証局のための WebTrust
目的	－ 監査目的のために連携する監査人と監査人のコミュニケーション － 特定のアプリケーション、機能と処理環境を対象とする。 － 現在、実務上広く利用されている。	－ ビジネスパートナー、既存顧客、見込み客を含む利害関係者への検証責任者のコミュニケーション － 下記に記載した法定の適用範囲 － 認証局の意見表明活動の新しい基準
評価の目標	各業務によって定義される。	認証局のビジネス活動が原則と規準で前もって定義されている。
業務の種類	－ 内部統制の運用状況の報告 － 内部統制の運用の有効性の検証と報告。	－ WebTrust 原則と規準の準拠性の報告
検証の基準	一般に認められた会計監査基準	証明業務基準（アメリカ）
適用範囲	適用範囲は任意。 適用範囲は各業務のために定式化されて、報告対象で定義されなくてはならない。	原則と規準によって定義された適用範囲、下記を含む領域 － CA のビジネス実務の開示（加入者と信頼者情報のプライバシーを含む） － サービスのインテグリティ 　－ 鍵ライフサイクル管理の内部統制 　－ 証明書ライフサイクル管理の内部統制 － CA 環境の内部統制
他の基準への関係	特定のレビューの一部として種々の関係が確立される必要がある。 契約に従って、監査人が実質的に適切な内部統制目標を決定する。	原則と規準が国際的な標準化のために ISO に提出されるように意図され、ANSI X9.79 に関連づけた基準となっている。 AICPA / CICA は、業界の認められた基準に関連づけた同一の基準を提供する。
レビューの適用期間	受容できる選択肢 －（内部統制が稼動している）特定日対象 －（クライアントによって決定された）特定期間対象	付与時点からの継続的適用。遵守の後の付与が最小 90 日間の期間にわたって検証されることができる。指定された期間内に更新する。（現在これが 6 か月間であるか、あるいは1年とするかを検討している）

付録 F － 認証局のための WebTrust 業務の検証責任者ポリシーと指針

はじめに

このセクションは、WebTrust 業務を実施する際に検証責任者が従わなければならない実務を列挙した、（WebTrust ビジネスライセンスの付録 A 用語の定義「ポリシー文書」で定義されたような）検証責任者のポリシーを含んでいる。これらのポリシーは、罫線で囲まれている。このセクションはまた、これらのポリシーを導入する際の検証責任者の追加的な指針も含んでいる。この指針は罫線で囲まれていない。

クライアント・業務受嘱

検証責任者は、WebTrust シールが読者を誤らせるように付与されるような業務を受嘱すべきでない。

WebTrust シールは、企業が広範に合理的な開示と内部統制を有しているという評判のいいサイトであると示すものである。したがって、検証責任者は、企業の業務の範囲外の開示が読者を誤らせるものとして知られている場合、業務の範囲に直接には影響しない内部統制の重大な問題点が知られている場合、又は企業が法規制の違反者として知られている場合は、WebTrust 業務の受嘱を避けることになる。

WebTrust シールの付与する WebTrust サービスを提供する手続は高水準の保証（例　監査又は証明レベル）で行われるべきである。

検証責任者は、認証局のための WebTrust 規準を満たさない潜在的領域を識別するための CA の予備的レビューのような WebTrust に関連する様々なサービスを提供できるのだが、WebTrust シールを提供するいかなる業務も、無限定意見報告書の基礎として、高水準の保証（例　監査又は証明レベル）を提供する手続を含んでいる必要がある。

初度対象期間

初度の認証局のための WebTrust 業務についての対象期間は、最低でも 2 か月以上が検証責任者によって決定されねばならない。

初度対象期間を決定するに際しては、検証責任者は、自らの意見の基礎となる十分かつ有効な証拠を得るために必要な期間の長さに留意する。例えば、既存の CA 及び CA 機能については 2 か月でも極めて十分であるが、新規の CA 及び CA 機能については、検証責任者は、より長い初度期間がより適切であると考える。

更新頻度

認証局のための WebTrust シールの更新間隔は、12 か月を超えるべきでなく、この間隔はしばしばより短いと考えられる。

更新間隔を決定するに際しては、検証責任者は、下記の事項に留意する。

- CA 運用の性質と複雑性
- CA の運用の重要な変更の頻度
- 変更があった際の、該当する認証局のための WebTrust 原則と規準への継続的準拠を保証するための、企業のモニタリング及び変更管理内部統制の相対的有効性
- 検証責任者の職業的判断

例えば、始動 CA 又は CA 機能の状況においては、初度検証期間は 3 か月に設定し、認証局のための WebTrust シールが付与された後の次の検証期間は 6 か月として実施して、その後、12 か月のレビューサイクルに移行するのがより適切かもしれない。対象範囲の継続性とシールの取得を実現するには、報告書を更新する対象期間は、前回の期間の終わりからでもよいし、初度報告書の期間の始まりでもよい。

企業が、検証責任者に対して、更新期間の間の業務の範囲を含む、適用される認証局のための WebTrust 規準への充足度に影響を与えうる重要な変更を通知した場合、検証責任者は、下記のいずれかを決定すべきである。

A. 更新検証を実施する必要がある。
B. 更新検証が完了して、検証報告書が発行されるまではシールを除去する必要がある。
C. 変更の性格及び企業のモニタリングや変更管理内部統制によっては、何らの行動もとる必要がない。

経営者の記述書

経営者は、Web サイト上に適切な書面の記述書を提供すべきである（経営者の記述書の事例は、付録 B で記載した）。

経営者の記述書は、通常特定の認証局を対象とし、特定の期間（通常は検証報告書の対象期間と同じ）を対象とし、例えば認証局モデルのような下記の記述を含んでいるべきである。

経営者が CA 運用に関して内部統制を評価した。その評価に基づき、ABC 認証局株式会社（ABC-CA）の経営者の意見では、認証局(CA)の場所での運用は、2000 年 ○月○日から 2000 年○月○日の間に、AICPA/CICA 認証局のための WebTrust 規準に基づいて下記の事柄が実施されていた。

- 鍵と証明書ライフサイクル管理ビジネス実務と個人情報保護実務を開示し、その開示された実務に準拠してサービスを提供した。
- 下記についての合理的な保証を提供する内部統制を保持した。

－加入者の情報が（ABC-CA による登録活動のために）適切に認証されていた。
－彼らが管理する鍵と証明書のインテグリティが確立されており、ライフサイクルを通じて保護されていた。

・下記についての合理的な保証を提供する内部統制を保持した。
― 加入者と信頼者の情報が適切に本物と証明され、正当な個人に限定され、CA のビジネスと関係がない使用から保護された。
― 鍵と証明書ライフサイクル管理運用の継続性は維持された。
― CA システム開発、保守、運用が適切に承認され、CA システムインテグリティを維持するために行われた。

クライアントのポリシーと開示の変更

企業の開示したポリシーの変更は、Web サイト上に開示される必要がある。クライアントが適切に当該変更を開示している場合、当該変更について検証報告書で言及する必要はまったくない。

無限定意見のための十分な規準

無限定意見を得るためには、企業はすべての重要な側面において、報告対象期間及び更新期間の間、業務の範囲を含めて、すべての適用される認証局のための WebTrust 規準に合致すべきである。

後発事象

検証責任者は、検証報告書日までの後発事象の影響について留意すべきである。検証責任者が、対象事項及び検証責任者の結論に重要な影響を及ぼす事象を知るに至った場合、検証責任者は、開示された実務に当該事象が適切に反映されているかどうか、又は当該事象が検証報告書に適切に取り扱われているかどうかについて留意すべきである。

確認書

業務の結論に先立って、そして報告書の発行に先立って、クライアントは検証責任者に確認書を提出する必要がある。(確認書の事例は、付録 C に記載した)。

注 1　ANSI X9F5 電子署名と証明書ポリシーワーキンググループは金融サービス業界のための X9.79 PKI の実務とポリシーフレームワーク(X9.79)基準を開発している。この基準は認証局に対して評価される詳細な認証局の内部統制目標を含む。国際基準化機構(ISO)ワーキンググループが新しい国際規格で国際要件に基づいて X9.79 を標準化するために形成された。さらには、米国弁護士協会の情報セキュリティ委員会(ABA-ISC)は認証局のための法律上の、専門的な要件を扱う PKI 評価ガイドライン(PAG)を開発している。PAG は X9.79 基準草案で詳述されて、認証局のための WebTrust 原則と規準に反映される認証局の内部統制目標に言及する。これらの文書のそれぞれに言及された認証局の内部統制目標は ANSI 、ISO、IETF と他の既存の基準団体において開発された。

注 2　ITU-T 勧告 X.509 (1997 年)は ISO/IEC 9594-8 として同様に ISO によって標準化された。

注 3　これらのサービスは、AICPA の証明業務基準(SSAE)第 1 号、証明基準(AICPA 、職業的基準、VOL. 1、AU セクション 100)の下で合衆国において、あるいは(同様に CICA ハンドブック、セクション 5025 として知られている)証明業務の CICA 基準の下でカナダにおいて行われる。検証責任者が AICPA、CICA、あるいは他の正当な全国会計事務所から、彼らのクライアントに認証局のための WebTrust サービスを提供するための認証局のための WebTrust サービス提供と WebTrust ビジネスライセンスを訓練して、適切な技能と経験を必要とする。検証責任者は、認証局のための WebTrust シールを付与できるように、「検証」レベルで業務を行う必要がある。レビューレベル契約では十分ではない。

注 4 ここで示唆されているように、AICPA/CICA 認証局のための WebTrust プログラムは、AICPA/CICA 電子商取引保証特別委員会が、加入者登録が CA 自身あるいは外部の RA によって実施されている状況を想定した。この認証局のための WebTrust プログラムのバージョンは、そのような登録活動が、CA の外部の当事者によって行われているとして起草された。一部のエンドユーザーの目的のために、このアプローチは当該エンドユーザーの独立した検証のすべての要求事項に対処していないかもしれない。特別委員会は、認証局のための WebTrust プログラムをまとめるに際して、こうした状況についてはよくわかっており、特別委員会は、この基準(バージョン 1.0)の発行と利用が望ましいものであり、第三者登録機能の影響はこのプログラムのバージョンの範囲を超えていると結論づけた。この問題は、認証局のための WebTrust プログラムの今後の改訂において考慮されることになる。