金融分野におけるPKI：技術的課題と研究・標準化動向

宇根正志（うねまさし）

要　旨

PKI（public key infrastructure）は、認証機関が発行する公開鍵証明書を用いて、公開鍵暗号の鍵ペアとその持ち主を結び付けるとともに、鍵ペアの適切な管理を保証する仕組みである。金融分野におけるPKIの利用は、認証サービスの専業会社が発行した公開鍵証明書を、インターネット・バンキングにおける本人確認手段として活用することから始まった。

最近では、金融機関自身が認証機関となると同時に、業界内にルート認証機関を設ける高度な形態のPKIを構築し、企業間電子商取引等における電子認証のインフラとして活用しようとする動きが拡大している。また、証明書ポリシー（CP）・認証実施規程（CPS）の作成指針として、米国国内標準ANS X9.79-1が策定されるなど、金融機関が認証機関として情報セキュリティ対策を検討する際に活用できる制度的枠組みや各種標準等が整備されつつある。

しかし、現時点では、金融機関が参画して構築を進めているPKIにおいては、情報セキュリティ対策に関する情報が必ずしも十分には公表されておらず、認証機関の信頼性等を外部から評価することが困難な状況にあるように思われる。金融機関が認証機関としてPKIの運営に参画していくに当たっては、適切な情報セキュリティ対策を講じたうえで、利用者の信頼を向上させるために情報セキュリティ対策の開示等を行っていくことが重要であると考えられる。

本稿では、まずPKI関連技術の研究・標準化動向を紹介したうえで、金融機関が参画する主なPKIの構造や情報セキュリティ対策の概要について紹介する。次に、今後、金融機関が認証機関としてPKIの運営に参画していくうえでの課題を説明し、考えられる対応策について説明する。

キーワード：PKI、公開鍵暗号、証明書ポリシー、情報セキュリティ、デジタル署名、電子認証、認証機関、認証実施規程

本稿は、2002年2月28日に日本銀行で開催された「第4回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている内容および意見は筆者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

宇根正志　日本銀行金融研究所研究第2課（E-mail: masashi.une@boj.or.jp）

１．はじめに

インターネット等オープンなネットワークの急速な拡大や情報通信技術の進展等によって、インターネット・バンキングや企業間電子商取引等、ネットワークを活用したさまざまなサービスが提供されている。こうした直接取引相手を確認できない環境においてデータのやり取りを安全に行う手段として、暗号技術をはじめとする情報セキュリティ技術が活用されている。特に、データ送信者の本人確認や交信されるデータの一貫性確認の手段として公開鍵暗号技術によるデジタル署名を利用するケースが増えてきている。

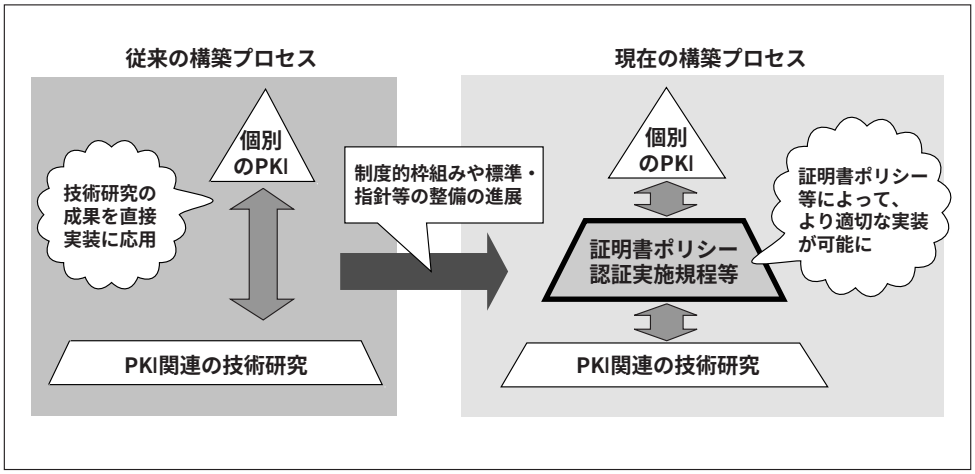
公開鍵暗号技術を適切に利用するためには、公開鍵・秘密鍵ペアの持ち主を特定し、鍵ペアが適切に管理されていることを保証する仕組みが必要となるが、このような機構としてPKI（public key infrastructure）が金融分野をはじめとする幅広い分野において利用されている。2001年4月には「電子署名及び認証業務に関する法律」（以下、電子署名法という）が施行されたことによって、一定の条件のもとでデジタル署名が手書き署名や押印と同等の法的効果をもつようになったため、電子的なデータ交信を安心して行うための機構としてPKIへの注目度が一層高まっている。

金融分野におけるPKIの利用は、各金融機関がインターネット・バンキングやオンライン証券取引等のサービスを提供する際に、認証サービスの専業会社が発行した公開鍵証明書を利用してサービス利用者の本人確認を実施するということから始まった。これに対し、最近では、金融機関自らが認証機関となり、企業間電子商取引や金融機関間情報通信等における電子認証の実現を目指して業界内にルート認証機関を設ける高度な形態のPKIを構築する動きがみられる。代表的なものとして、全国銀行協会（全銀協）、アイデントラス（Identrus）、スイフト（SWIFT）がそれぞれルート認証機関となるPKIが挙げられる。

同時に、金融機関が認証機関として情報セキュリティ対策を検討する際に利用できる制度的枠組みや各種標準等の整備も進みつつある。特に、米国において金融分野向けの証明書ポリシー・認証実施規程の作成指針ANS X9.79-1が2001年に策定されたことが注目される。証明書ポリシーは、「どのような環境の下で公開鍵証明書をどのような目的で利用するか」という認証業務の基本方針を指し、認証実施規程は、証明書ポリシーの規定を実現するための具体的な施策（運用・管理方法や情報セキュリティ対策等）を指す。認証業務を行う金融機関は、ANS X9.79-1等を参考にすることで従来に比べて容易かつ適切に証明書ポリシーや認証実施規程を作成し、それらに基づいてより有効な情報セキュリティ対策が実施可能となったと考えられる（図1参照）。

しかし、認証機関を運営する際には、個人認証技術、公開鍵暗号技術、ネットワーク・セキュリティ技術等、金融機関が従来利用してきたセキュリティ技術とは異なる技術を活用することが必要である。また、金融機関が参画して構築を進めているPKIにおいては、情報セキュリティ対策に関する情報が必ずしも十分には

図1　PKIの構築プロセスを巡る環境変化



公開されていないように思われる。今後、金融機関が認証機関としてPKIの運営に参画するに際して、認証業務に必要な情報セキュリティ対策を適切に講じたうえで、これを利用者に効果的に示していくことが最も重要な課題であると考えられる。そのためには、①PKIのシステム構築時に情報セキュリティ技術を適切に選択して証明書ポリシー・認証実施規程を作成し、セキュリティを損なわない範囲でそれらの内容を開示する、②PKIのサービス開始後に認証業務が適正に運用・管理されていることを第三者によるセキュリティ監査によって確認し、その結果を開示する、といった措置を講じることが考えられる。

本稿の構成は次のとおりである。まず2節においてPKIの意義やPKIで利用される各種技術を紹介し、3節において、金融機関が参画するPKIや政府のPKIを取り上げ、各PKIの構造や情報セキュリティ対策の概要を説明する。4節では、3節の内容を踏まえ、今後金融機関が認証機関としてPKIに取り組む際に解決すべき課題を示し、その対応策として、情報セキュリティ対策の適切な選択と開示や、運用・管理体制に関するセキュリティ監査の実施とその結果の開示について説明する。5節では、簡単に結びを述べる。

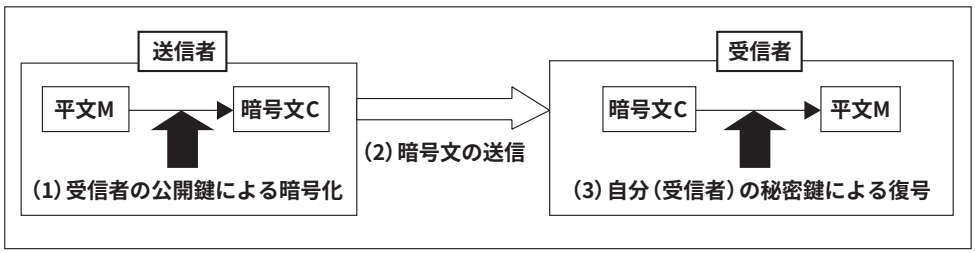
2．PKIの意義とそれを実現する技術

PKIは、一般的に、「デジタル署名技術を用いて、公開鍵暗号における公開鍵とそれに対応する秘密鍵の所有者を検証可能な形で結び付けるための機構」（ANS X 9.79-1、ANSI［2001］）と定義される。以下では、PKIの意義について説明したうえで、PKIとは何か、PKIはどのように実現されるのかについて説明する。

（1）公開鍵暗号とPKIの意義

公開鍵暗号は、暗号化用の鍵と復号用の鍵が異なる暗号方式であり、ある特定のデータが得られない状況において一方の鍵から他方の鍵を算出することが計算量的に困難である[1]ため、どちらか一方の鍵を公開することができる。通常、暗号に利用される鍵（公開鍵）が公開され、復号に利用される鍵（秘密鍵）が秘密に管理される。公開鍵暗号を利用した暗号通信では、まず、送信者が送りたい平文Mを受信者の公開鍵によって変換して暗号文Cを生成し、Cを送信する。暗号文Cを受信した受信者は、自分の秘密鍵によってCを変換し、平文Mを入手する（図2参照）。このように、暗号化用の鍵が公開されることから、不特定多数の者が、暗号化の鍵を秘密に共有することなく暗号通信を実施できる。

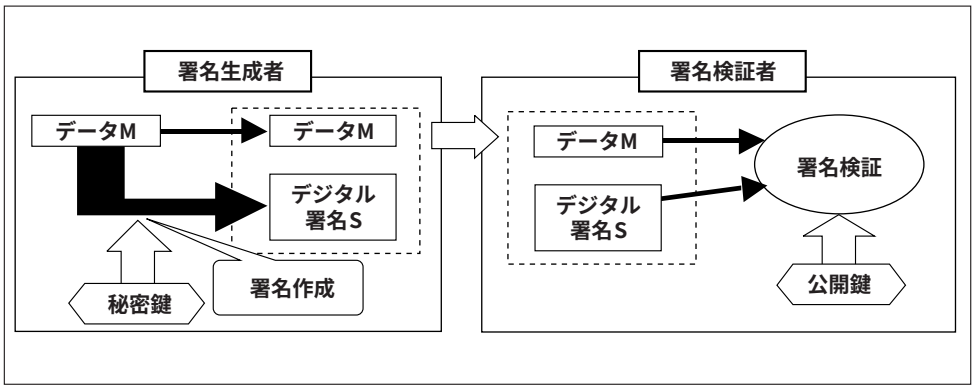
図2　公開鍵暗号による暗号通信の例



公開鍵暗号は、暗号通信だけではなく、デジタル署名の機能も実現する。あるデータMに対するデジタル署名Sは、秘密鍵を用いてデータMに一定の処理（署名生成処理）を施すことによって生成される（図3参照）。デジタル署名SとデータMを入手した第三者（署名検証者）は、これらのデータと署名生成者の公開鍵を用いて一定の処理（署名検証処理）を行い、①デジタル署名Sが生成された後にデータMが改ざんされていないかどうか（一貫性〈integrity〉が確保されているかどうか）

1 「計算量的に困難である」とは、その計算を行うことは理論的には可能であるものの、実際にその計算を実行するには計算量が非常に大量となり、膨大な費用と時間を必要とすることから、事実上不可能であることを意味する。どの程度の計算量が事実上不可能であるかは、その時々の技術条件等によって左右される。公開鍵暗号では、「一方の鍵から他方の鍵を導出することが計算量的に困難」という状況を、効率的に解を求めることが困難とみられている数学の問題を利用して実現している。

図3　デジタル署名の生成・検証



を確認する（メッセージ認証）ほか、②デジタル署名Sの署名者を確認する（ユーザー認証）ことができる。このように、秘密鍵と公開鍵はそれぞれ署名生成鍵、署名検証鍵に対応し、署名検証に用いる鍵が公開されることから、不特定多数の者が、事前に鍵を秘密に共有することなく署名検証を行うことができる。

こうした公開鍵暗号やデジタル署名を安全に実現するためには、暗号化や署名検証に用いられる公開鍵の所有者を特定すると同時に、公開鍵と秘密鍵が適切に生成され、管理されていることを確認する必要がある。

例えば、ネットワーク経由でAさんの公開鍵と称されるデータDを入手したときに、データDが確かにAさんの公開鍵であり、かつ、データDが受信途中で改ざんされていないことを検証できない場合が考えられる。こうした状況においては、Aさんが生成したと称されるデジタル署名SをデータDによって検証し、その検証が成功したとしても、データDはAさんの公開鍵ではなく、デジタル署名SはAさんが生成したものではない可能性がある。

一方、Aさんの秘密鍵が格納されているICカードが盗まれ、その直後にAさんがICカード盗難の事実に気づいたとする。この場合、盗難が発覚した後に、Bさんが Aさんの正しい公開鍵を用いてデジタル署名Sの検証に成功したとしても、AさんのICカードから秘密鍵が第三者に漏洩し、デジタル署名Sはその秘密鍵によって偽造されたものである可能性がある。

PKIは、こうした問題（公開鍵の所有者の特定、鍵管理の適切さの確認）に対応する手段を提供し、公開鍵暗号やデジタル署名を安心して利用できるようにする。具体的には、公開鍵の利用者から信頼されている第三者（認証機関、CA：certification authority）が、各公開鍵に対してその所有者および秘密鍵が適切に管理されていることを示すデータとして公開鍵証明書（public key certificate）を発行し、定期的または要求に応じて公開鍵証明書の有効性を示すデータを配布することによって実現される。公開鍵証明書の有効性に関しては、認証機関は、各公開鍵の所有者に対して、秘密鍵が第三者に漏洩した可能性等が発生した場合には認証機関に直ちに通知させることを要請する。公開鍵証明書には、公開鍵、公開鍵の所有者

のID、公開鍵証明書の有効期間、公開鍵証明書を発行した認証機関のID等が含まれるほか、それらに対する認証機関のデジタル署名が含まれる。公開鍵を利用する際には、その公開鍵に対する公開鍵証明書を認証機関から入手したうえで、以下の2点を実行する。

・公開鍵証明書の有効期間と、認証機関から入手する公開鍵証明書の有効性に関するデータを用いて、公開鍵証明書が有効であることを確認する。
・認証機関の公開鍵を入手したうえで、公開鍵証明書に含まれる認証機関のデジタル署名を検証する。

以上の手続によって、ある公開鍵に対応する秘密鍵が公開鍵証明書で特定される所有者によって適切に管理されていることが確認される[2]。

(2) PKIの形態

イ．金融分野におけるPKI関連の標準規格

PKIに関する具体的な説明に入る前に、金融分野を主たるターゲットとしたPKIに関してどのような標準規格が存在するか、また、標準化が進められているかについて説明する。代表的な標準規格および標準規格案として、ANS X9.57（ANSI［1997］）、ANS X9.79-1（ANSI［2001］）、ISO/DIS 15782-1（ISO/IEC［2001］）の3つが挙げられる。

まず、ANS X9.57とANS X9.79-1は、それぞれ1997年、2001年にANSIによって策定された米国の国内標準であり、多くの米国の金融機関において利用されている。ANS X9.57は金融業務において利用される公開鍵証明書の管理方法を規定する一方、ANS X9.79-1は、金融機関が認証業務を行う際に作成する証明書ポリシー・認証実施規程（詳細は(3)において説明）について規定している。なお、ANS X 9.79-1については、ANS X9.57のほか、証明書ポリシー（CP：certificate policy）・認証実施規程（CPS：certification practice statement）に関するIETF PKIX[3]の技術標準RFC 2527（Chokhani *et al*.［2001］）の内容を参考にして策定されたものである。

2 ただし、秘密鍵が漏洩し、秘密鍵の正当な所有者が漏洩の事実に気づくまでに長いタイムラグが存在した場合には、その間にデジタル署名が偽造され、秘密鍵の漏洩を知らない署名検証者が正当な署名であると誤認する可能性がある。こうした問題についてはPKIだけでは十分な対応が困難であり、別途対策を講じることが必要となる（小森・松浦・須藤［2001］、洲崎・松本［2001］）。本稿では取り上げないが、対応策として、ヒステリシス署名（松本ほか［2000］、洲崎ほか［2000］）、フォワード・セキュア・デジタル署名（Forward-Secure Digital Signature、Anderson［2000］、Bellare and Miner［1999］）、実行ハードウエア確認タグ認証方式（松本・田中［2000］）といった技術が提案されている。

3 IETF（International Engineering Task Force）：インターネットにおける技術上の諸問題を解決することを目的として設置された委員会（IAB：Internet Architecture Board）の下部組織であり、インターネットの技術標準RFC（Request For Comments）の策定等を担当する委員会。IETFは各分野に設置されたワーキング・グループによって構成されており、IETF PKIX（Public-Key Infrastructure［X.509］）は、インターネット上においてX.509に基づくPKIを実装する際に用いられるRFCの策定を担当するワーキング・グループである。

また、ISO/DIS 15782-1は現在ISO/TC68[4]において検討が進められている国際標準案であり、2001年5月作成の草案には、認証機関の役割、公開鍵証明書の管理方法、公開鍵証明書のデータ形式等について記載されている。ISO/DIS 15782-1はANS X 9.57をベースとして作成されており、証明書ポリシーや認証実施規程については詳しく記載されていない。このため、ISO/TC68では、米国国内標準であるANS X 9.79-1を参考にして証明書ポリシー・認証実施規程に関する国際標準を策定する方向で検討が行われている。

なお、本稿では、国際標準化に向けた検討が進められているISO/DIS 15782-1とANS X9.79-1の内容を主に参照することとする。

ロ．PKIの構成者

PKIの構成者（以下、エンティティという）として、ANS X9.79-1では、認証機関、ポリシー管理機関（policy authority）、公開鍵所有者（subscriber）、検証者（relying party）が想定されている。このうち、認証機関については、その各種機能を別々のエンティティが担うケースも想定されており、証明書発行機関（certificate issuer）、登録機関（registration authority）、証明書生成機関（certificate manufacturer）、リポジトリ（repository）の4つが規定されている。ANS X9.79-1に規定される各エンティティの役割は次のとおりである。

〈エンティティとその役割（図4参照）〉

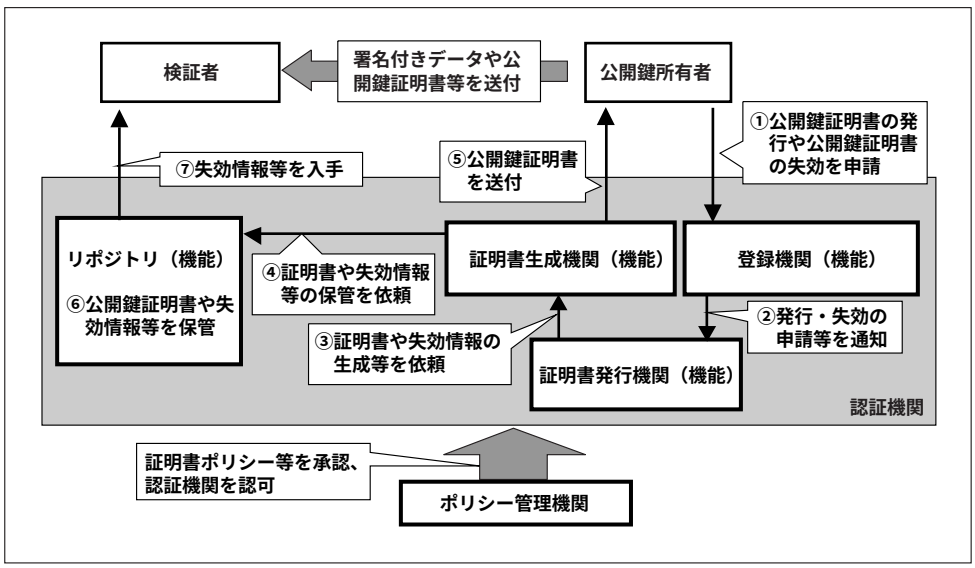
- **ポリシー管理機関**：認証機関を認可するほか、証明書ポリシーや認証実施規程等を承認する。また、セキュリティ上の脅威や基本方針に関する問題点等について対応する。
- **認証機関**：次の各機能を担う。
  - 〈1〉認証業務の基本方針や実施規程を作成し、公開鍵証明書の発行・失効処理の意思決定を行い、業務を統括する（証明書発行機関の機能）。
  - 〈2〉公開鍵証明書を生成して公開鍵所有者に送付するほか、公開鍵証明書の失効情報を生成し、公開鍵証明書や失効情報等の保管をリポジトリに依頼する（証明書生成機関の機能）。
  - 〈3〉公開鍵証明書の発行申請を受け付けて、公開鍵が適正に生成されていることや申請者の身元等を確認し、証明書発行機関に通知する。また、公開鍵所有者から公開鍵証明書の失効申請を受け付ける（登録機関の機能）。
  - 〈4〉公開鍵証明書、証明書の失効情報、証明書ポリシー等を保管し、検証者等に対して配布する（リポジトリの機能）。

4 ISO/TC68：国際標準化機構（ISO）の専門委員会の1つであり、「金融業務、証券業務およびその他の金融サービス」を対象とする国際標準規格の策定を担当している。

・**公開鍵所有者**：公開鍵と秘密鍵を生成し、公開鍵に対する公開鍵証明書の発行や公開鍵証明書の失効を登録機関に申請する。
・**検証者**：認証機関（リポジトリ）から失効情報等を入手し、公開鍵証明書の検証を行う。

なお、ISO/DIS 15782-1においては、認証機関の機能から登録機関を切り離し、認証機関を証明書発行機関、証明書生成機関、リポジトリの機能を有するエンティティとして記載している。ただし、以下では、認証機関を、証明書発行機関、証明書生成機関、登録機関、リポジトリの4つの機能をすべて具備した1つのエンティティとして扱うこととする。

図4　PKIを構成するエンティティ（ANS X9.79-1）



ハ．認証機関の信頼構造

複数の認証機関が存在する場合、他の認証機関が発行した公開鍵証明書を用いてデジタル署名を検証することが必要となり、検証に用いる公開鍵証明書を発行した認証機関が信頼できることを確認する手段が必要である。その手段として、認証機関間で公開鍵証明書を発行して信頼の連鎖（信頼構造と呼ばれる）を構築するという方法が一般的に採用されている。主な信頼構造として、階層型、相互認証型、ハイブリッド型が挙げられる（ISO［2001］）。

（イ）階層型

階層型では、上位の認証機関が下位の認証機関に公開鍵証明書を発行する形となり、各認証機関の関係はピラミッド構造になっている。ピラミッド構造の頂上に位置し、どの認証機関からも公開鍵証明書を発行されていない認証機関はルートCA

と呼ばれる。ルートCAの公開鍵に対しては、ルートCA自身が公開鍵証明書を発行するケースが多い。この公開鍵証明書には公開鍵所有者であるルートCAの署名が添付されることから、自己署名証明書と呼ばれる。なお、ルートCAの自己署名証明書は、予めCD-ROMに格納してオフラインで配布する等、正しい公開鍵あるいは自己署名証明書であることを公開鍵所有者や下位の認証機関が信頼できる形態で配布するケースが一般的である。

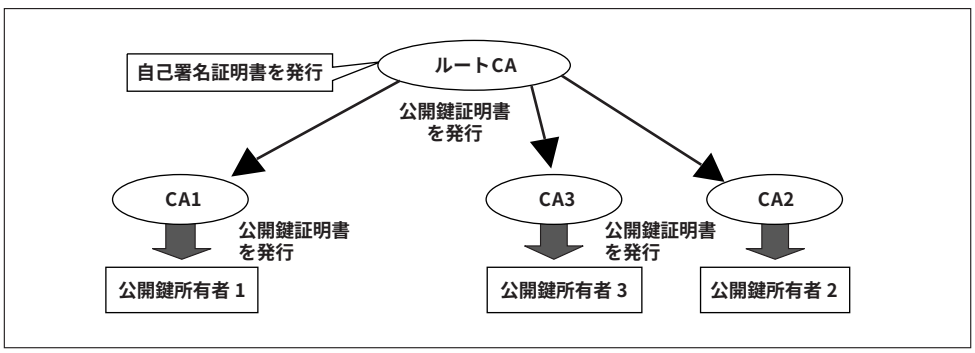
例えば、図5の例において、公開鍵所有者1が公開鍵所有者2の公開鍵証明書を検証する場合、次のような手順が取られる。公開鍵所有者1は、ルートCAの自己署名証明書を信頼できる手段によって既に入手しているものとする。

① 公開鍵所有者1は、CA2の公開鍵証明書を入手し、既に入手しているルートCAの自己署名証明書に含まれる公開鍵によってCA2の公開鍵証明書を検証する。

② 公開鍵所有者1は、CA2の公開鍵証明書に含まれる公開鍵を用いて、公開鍵所有者2の公開鍵証明書の検証を行う。

このように、「ルートCAの自己署名証明書→CA2の公開鍵証明書→公開鍵所有者2の公開鍵証明書」という公開鍵証明書の連鎖（認証パス、certification path）が形成され、これを辿って検証することとなる。階層型の場合、ルートCAがすべての検証者から信頼されていることが前提となっており、同一のセキュリティ・ポリシーのもとで認証パスの構築が容易であるという利点を有している。また、企業等における取引データの処理を行う際に階層構造が採用されるケースもあり、そうしたケースに適用しやすいと考えられる。ただし、ルートCAの秘密鍵が危殆化した場合[5]、その秘密鍵によるデジタル署名が付された公開鍵証明書がすべて信頼できなくなり、PKI全体が機能しなくなるという事態に陥る可能性がある。

図5　階層型の信頼構造例



5 一般的に、秘密鍵が危殆化するとは、何らかの要因（例えば、公開鍵から秘密鍵を効率的に計算できる可能性が判明した場合や、ハードウエア・モジュールの欠陥等によって秘密鍵の不正な読出しが容易になされうることが判明した場合）によって、①秘密鍵が無権限者である第三者の手に渡る可能性が高まり、（まだ渡っていないと考えられるものの）秘密鍵を利用するアプリケーションのセキュリティ受容度を超えたと判断された場合、または、②秘密鍵が既に第三者の手に渡った（もしくはその可能性が高い）と判断された場合を意味する。

（ロ）相互認証型

相互認証型では、2つの認証機関が相互に他の認証機関の公開鍵に対して公開鍵証明書を発行する。このようにして発行された2つの公開鍵証明書は、1セットで相互認証証明書と呼ばれる。公開鍵所有者は、相互認証証明書を用いて、当該公開鍵所有者に対して公開鍵証明書を発行している認証機関以外の認証機関が発行した公開鍵証明書を検証することができる。

図6　相互認証型の信頼構造例

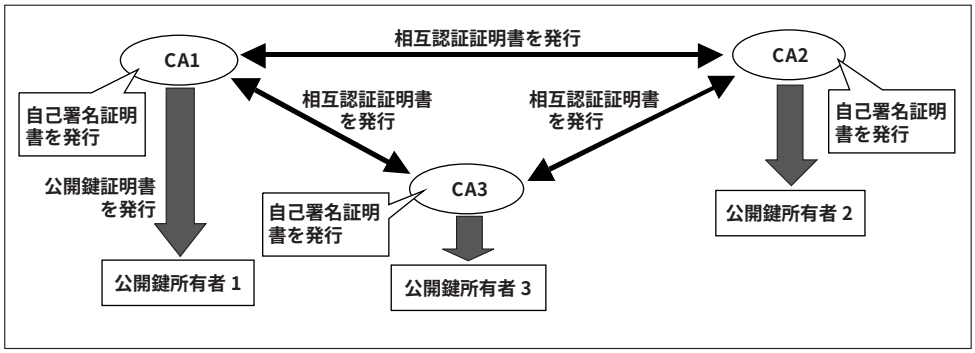


図6の例において、公開鍵所有者1が公開鍵所有者2の公開鍵証明書を検証する場合、以下の手順が取られる。公開鍵所有者1は、自分が信頼するCA1の自己署名証明書を信頼できる手段によって既に入手しているものとする。

① 公開鍵所有者1は、既に入手しているCA1の自己署名証明書に含まれる公開鍵を用いて、CA1がCA2の公開鍵に対して発行した公開鍵証明書を検証する。

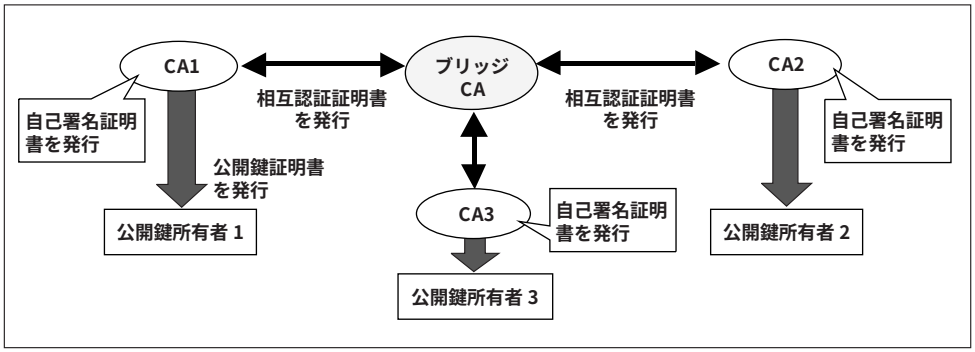
② 公開鍵所有者1は、CA2の公開鍵証明書に含まれる公開鍵を用いて、公開鍵所有者2の公開鍵証明書を検証する。

このように、「CA1の自己署名証明書→CA1がCA2の公開鍵に対して発行した公開鍵証明書→公開鍵所有者2の公開鍵証明書」という認証パスを検証することとなる。相互認証型の場合、ある認証機関の秘密鍵が漏洩した場合、信頼できなくなる公開鍵証明書はその認証機関が発行した公開鍵証明書のみであるため、階層型におけるルートCAの秘密鍵危殆時に比べ、認証機関の秘密鍵危殆時の影響は比較的小さいと考えられる。ただし、認証機関は相互認証証明書を発行する必要があるほか、信頼パスが階層型に比べて複雑になるといったデメリットがある。

なお、相互認証型のバリエーションとして、ブリッジCAと呼ばれる特殊な認証機関を利用する形態も提案されている（図7参照）。ブリッジCAは他のすべての認証機関と相互認証のみを行い、認証機関同士の信頼の橋渡しを行う役割を担う。

ブリッジCAを導入すると、ブリッジCA以外の認証機関は、ブリッジCAのみと相互認証を行うだけでよく、ブリッジCAを導入しない相互認証型の信頼構造を採用する場合に比べて相互認証に伴う負担を軽減させることができる。ただし、ブリッジCAのシステムの構築や運用・管理に伴う負担が新たに発生するほか、ブリッジ

図7　ブリッジCAを用いた信頼構造例

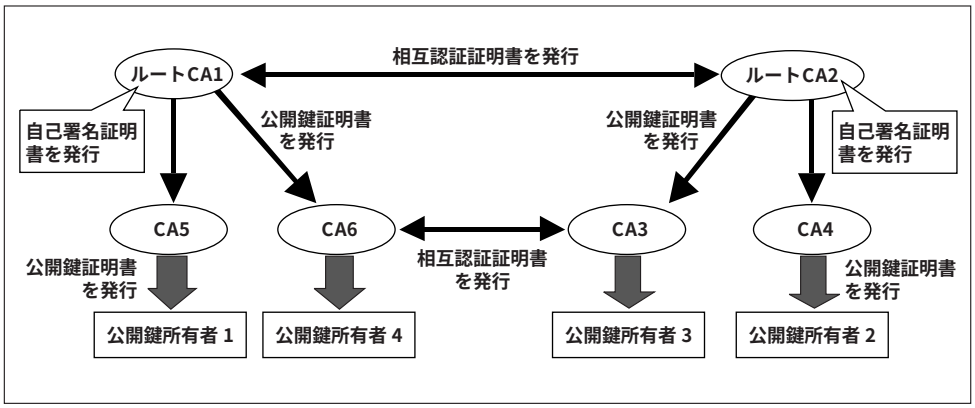


CAの秘密鍵が危殆化した場合には、ブリッジCAとその他の認証機関との間で発行された相互認証証明書がすべて利用不可能となる事態が発生する。

（ハ）ハイブリッド型

ハイブリッド型は、階層型と相互認証型を組み合わせたものであり、階層型の構造が複数存在し、各ルートCAが互いに相互認証するという形態となる（図8参照）。ただし、図8のCA3とCA6間の相互認証のように、ルートCAでなくとも必要に応じて他の認証機関と直接相互認証を行うケースも考えられる。

図8　ハイブリッド型の信頼構造例



ハイブリッド型では、信頼構造が他の構造に比べて複雑となる反面、利用する組織や組織間取引の形態に応じて信頼構造を柔軟に構築することが可能となっている。

以上で説明してきた各信頼構造の主な長所と短所を整理すると、表1のとおりである。

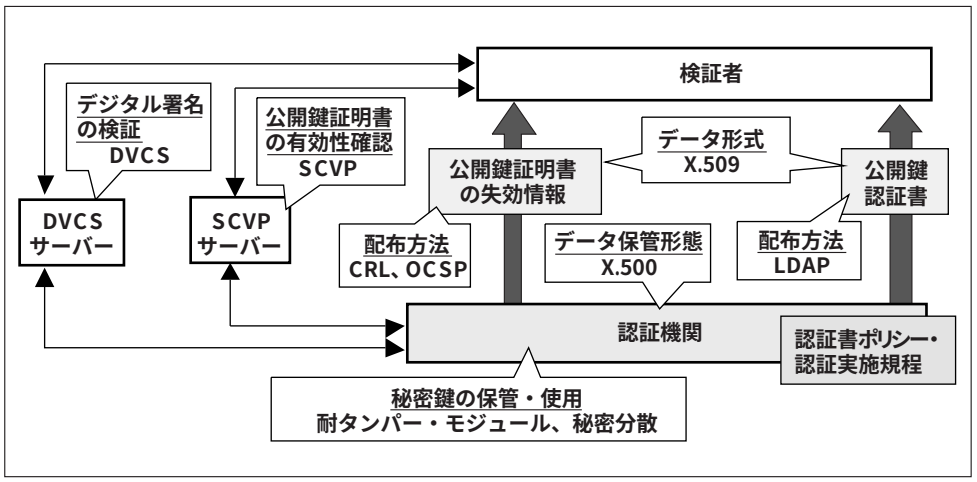
表1　各信頼構造における主な長所と短所

	長所	短所
階層型	・構造が相互認証型やハイブリッド型に比べて単純である。 ・企業等における取引データの処理を行う際に階層構造が利用されているケースがあり、そうしたケースに適用しやすい面がある。	ルートCAの秘密鍵が危殆化するとPKI全体が機能しなくなる可能性がある。
相互認証型	・ある認証機関の秘密鍵が危殆化しても、その認証機関が発行した公開鍵証明書と相互認証証明書は利用不可能となるが、PKI全体が機能しなくなることはない（ただし、ブリッジCAを利用する場合、その秘密鍵が危殆化するとすべての相互認証証明書が利用不可能となる）。 ・既存の認証機関が他の認証機関とリンクしようとする場合に適用しやすい面がある。	・認証機関の数が多い場合、構造が階層型に比べて複雑となる。 ・相互認証証明書の発行・管理が必要となる。 ・ブリッジCAを設置する場合、ブリッジCAのシステム構築や運用・管理等に伴う負担が新たに発生する。
ハイブリッド型	・利用する組織形態等に応じて柔軟に信頼構造を構築することが可能である。	構造が階層型や相互認証型に比べて複雑である。

（3）公開鍵証明書とその失効情報の管理等に用いられる主な技術

次に、PKIに用いられる各種技術の中でも認証機関の主な機能である公開鍵証明書とその失効情報の管理に用いられる技術に焦点を当て、主なPKIで採用されている技術を中心に紹介する（図9参照）。

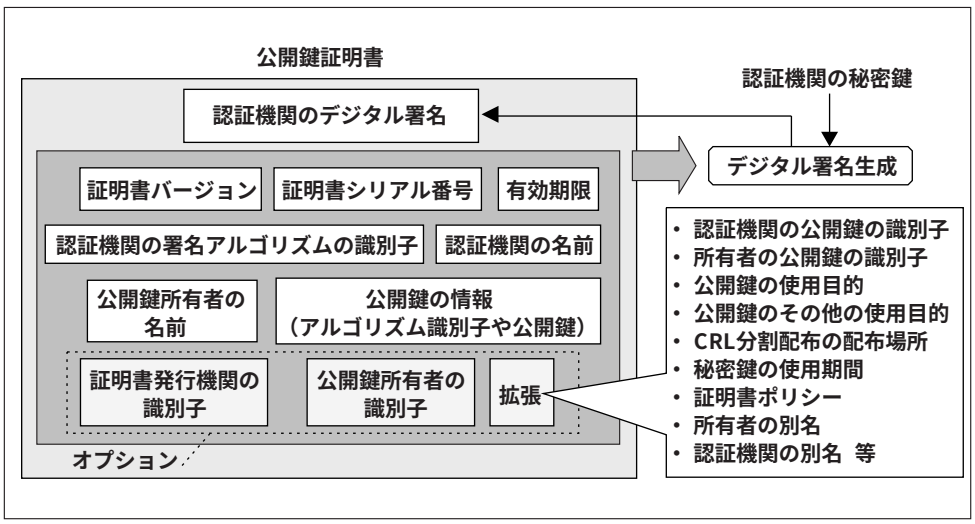
図9　PKIに利用される主な技術



イ．公開鍵証明書のデータ形式と保管・配布方法

公開鍵証明書のデータ形式は、ITU-T[6]によってX.509（バージョン3、ITU-T［1997b］）として国際標準化されている。X.509はISO/IEC 9594-8（ISO/IEC［1998a］）としても標準化されており、幅広い分野のPKIに利用されている。X.509の公開鍵証明書には、公開鍵、公開鍵所有者の識別子、署名アルゴリズムの識別子、有効期限、認証機関の識別子、認証機関のデジタル署名等が含まれる（図10参照）。金融分野におけるPKIの枠組み等について規定しているISO/DIS 15782-1やANS X9.79-1においても、公開鍵証明書のデータ形式としてX.509が採用されている。

図10　X.509公開鍵証明書（バージョン3）のデータ形式



公開鍵証明書を発行する際には、まず公開鍵所有者が、自分のICカードやパソコン上のソフトウエア等において公開鍵と秘密鍵のペアを生成する。ただし、認証機関等のシステムが鍵ペアの生成を代行するケースもある。公開鍵所有者は公開鍵や本人確認に必要な情報等を認証機関に提出し、認証機関は、本人確認、公開鍵が正しく生成されていることの確認、公開鍵証明書に記述する内容の正当性の確認等を行ったうえで、公開鍵証明書を生成する。生成された公開鍵証明書は公開鍵所有者に送付されるほか、認証機関内のリポジトリに保管される。

6 ITU-T（International Telecommunication Union - Telecommunication Standardization）：ITU（国際通信連合）は、電気通信に関する制度の検討、電気通信技術の標準化、電気通信サービスの運用に必要な情報収集・周知、電気通信インフラの開発・推進等を目的として設置された国際連合の専門機関の1つ（加盟国：189ヵ国＜2000年9月現在＞、本部：ジュネーブ）。ITUは、ITU-T（電気通信標準化部門）、ITU-R（無線通信部門）、ITU-D（電気通信開発部門）、事務総局から構成されており、このうちITU-Tでは、各種通信技術に関する国際標準の策定等の活動が行われている。

リポジトリにおける公開鍵証明書の保管形態に関しては、ITU-T X.500（ITU-T［1997a］）に準拠したデータベースが採用されるケースが一般的である。X.500は、DIT（directory information tree）と呼ばれる階層構造のディレクトリによるデータ保管方法等を規定する国際標準であり、ISO/IEC 9594シリーズとしても標準化されている。

X.500ベースのデータベースを有するリポジトリから公開鍵証明書等を入手するための技術としては、IETF PKIXにおいてRFC 2251として標準化されているLDAP（lightweight directory access protocol、Wahl, Howes, and Kille［1997］）が広く利用されている。LDAPは、X.500準拠のディレクトリにアクセスしてデータの検索を行い、検索条件に合致したデータを入手するためのプロトコルである。LDAPは、データの要求者と保管者との間で交信されるデータ形式を汎用的に規定しているため、公開鍵証明書の入手のほか、さまざまな用途に利用されている。LDAPによって公開鍵証明書を入手する場合、①まず、検証者はディレクトリを管理する認証機関（リポジトリ）のサーバーに対して公開鍵証明書の送付を要求するデータを送信する、②サーバーは要求データに応じて公開鍵証明書を検索する、③サーバーは公開鍵証明書を検証者に返信する、という手順となる。

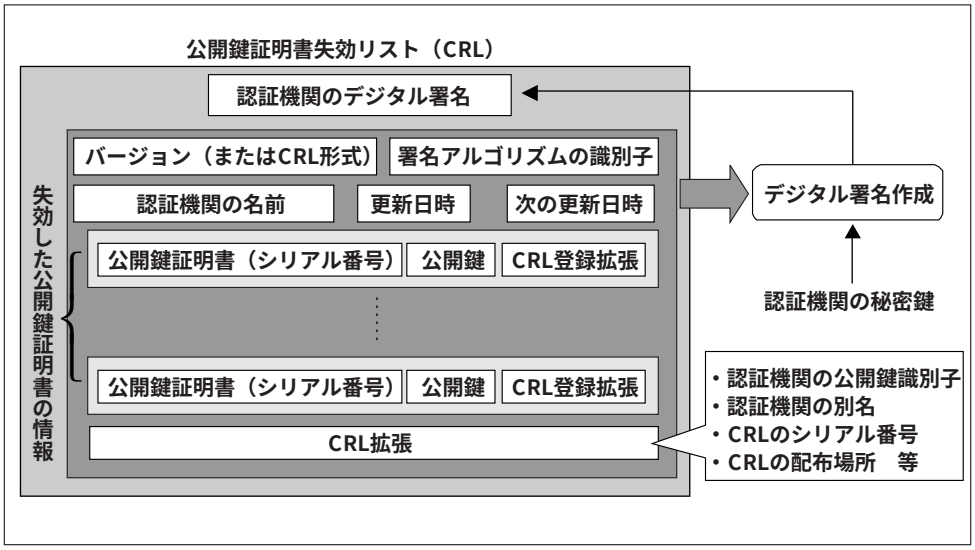
ロ．公開鍵証明書の失効情報のデータ形式と配布方法

公開鍵証明書の失効情報は、通常認証機関のリポジトリに保管される。失効情報の代表的な配布方法として、公開鍵証明書失効リスト（CRL：certificate revocation list）を配布する方法（Housley *et al.*［2001］）と、OCSP（online certification status protocol、RFC 2560）と呼ばれるプロトコルを利用する方法（Myers *et al.*［1999］）の2つが挙げられる。

CRLは、失効した公開鍵証明書の情報によって構成されるデータであり、そのデータ形式は、公開鍵証明書と同様にX.509において国際標準化されている（図11参照）。CRLとしては、X.509のバージョン2に準拠したものが利用されるケースが多い。CRLは認証機関によって作成され、一貫性を確保するために認証機関のデジタル署名を含む。CRLのなかでも、認証機関の公開鍵に対する公開鍵証明書の失効情報を扱うCRLはARL（authority revocation list）と呼ばれる。検証者がCRLやARLを入手する際には、LDAP、HTTP、FTP等のプロトコルが利用される。ただし、失効した公開鍵証明書が増加するとCRLのサイズが大きくなり、通信データ量が増大するというデメリットがあるほか、CRLは一定期間（例えば24時間）ごとに更新されるため、常に最新の失効情報がCRLに反映されているわけではないといった問題が指摘されている。

CRLのサイズを抑える主な方法として、CRL分割配布（CRL distribution points）とデルタCRLという方法が提案されている。CRL分割配布は、CRLを任意の数に分割して保管・配布する方法である。分割された各CRL（以下、分割CRLという）の配布場所の情報は公開鍵証明書の拡張フィールドに記述され、検証者はその情報を手がかりに分割CRLを入手する。この結果、CRL全体を入手する場合に比べて通信

図11　公開鍵証明書失効リスト（CRL）のデータ形式



データ量を削減可能となる。一方、デルタCRLは、前回のCRLの発行以降に失効した公開鍵証明書の情報のみから構成されるデータであり、CRLの更新時における差分のデータのみを交信することで通信データ量を削減可能にするものである。検証者は、デルタCRLのみを定期的に認証機関から入手することで最新のCRLを構成可能である。

CRLが一定時間ごとに更新され、常に最新の失効情報がCRLに反映されているわけではないという問題に対処する技術として提案されているのがOCSPである。OCSPは、公開鍵証明書を検証する際にその公開鍵証明書のステータスを認証機関に問い合わせるというものであり、公開鍵証明書の失効情報をリアルタイムで入手できる。認証機関から返信される失効情報には、認証機関のデジタル署名が含まれる。

ハ．秘密鍵の保管・使用方法

認証機関は、公開鍵証明書やその失効情報等に添付するデジタル署名用の秘密鍵を厳重に保管する必要がある。また、公開鍵所有者も、自分の秘密鍵を第三者に知られないように管理することが求められる。このため、通常秘密鍵は、特殊なセキュリティ対策が施されたハードウエア・モジュールに保管され、そのモジュールを利用して署名を生成する場合にはPINや秘密鍵所有者の生体情報等が必要とされる。特に、認証機関の秘密鍵を利用する場合には、複数の管理者が協力しなければならない仕組みが採用されるケースもある。

多くのPKIプロジェクトでは、秘密鍵を保管するハードウエア・モジュールのセキュリティ要件として、米国の政府機関が利用する暗号モジュールのセキュリティ要件を定めた米国連邦政府標準FIPS 140-1（Security Requirements for Cryptographic

Modules、NIST［1994］）の規定が利用されている[7]。FIPS 140-1は暗号モジュールについて4段階のセキュリティレベルを設定し、各レベルを達成するためのセキュリティ要件を規定している（表2参照）。

表2　FIPS 140-1における暗号モジュールの各レベルの要件

	各レベルのセキュリティ要件
レベル 1	・データを保護する特別な物理的対策は不要 （例）暗号化機能を備えたICカード、パソコン用暗号処理ボード、パソコン用暗号化ソフトウエア
レベル 2	・物理的攻撃を検知するための対策（コーティングやシール等）が必要 ・利用者の権限認証の機能が必要 ・ソフトウエアの場合、TCSEC C2レベル相当のOS上の実行が必要
レベル 3	・レベル2に加え、物理的に内部の重要データにアクセス不可能にする対策（例えば、アクセスを検知してデータを自動消去）が必要 ・レベル2の権限認証に加え、利用者の個人認証の機能が必要 ・入出力される重要データを暗号化する機能等が必要 ・ソフトウエアではTCSEC B1相当以上のOS上での実行が必要
レベル 4	・暗号モジュール全体を保護する機構を備え、物理的に内部の重要データにアクセス不可能にする対策（例えば、アクセスを検知してデータを自動消去）が必要 ・レベル3に加え、電圧や温度等の環境変化に対して内部の重要なデータを保護する機構を有していることが必要 ・ソフトウエアではTCSEC B2相当以上のOS上での実行が必要

ISO/DIS 15782-1では、秘密鍵の生成・保管は特殊なハードウエア・モジュール内で生成する必要があると規定し、そのセキュリティ機能として、外部からの物理的攻撃を検知する機構やカバー等がこじ開けられた場合に重要なデータが自動的に消去されるといった機構が例示されている。こうしたモジュールのセキュリティ要件はFIPS 140-1のレベル3に対応すると考えられる。

ハードウエア・モジュールに格納した秘密鍵を利用してデジタル署名を作成する際には、利用者が正当な権限を有しているかを確認するためにPINや生体情報等が利用されるケースが一般的である。特に、認証機関の秘密鍵の場合には、1人の管

7　FIPSは5年ごとに見直しが行われるため、1994年に成立したFIPS 140-1は既に改訂され、2001年11月からはFIPS 140-2（NIST［2001］）が有効となっている。主な改訂点は、①OSの評価基準がTCSEC*からISO 15408に変更されたこと、②ソフトウエアやハードウエアの管理方法に関する記述が拡充され、ソフトウエア等の配送やセットアップ方法の明確化、操作マニュアルの整備等の項目が追加されたこと、③タイミングアタックや電力差分攻撃等の新しい攻撃に関する記述が追加されたこと、④モジュールのセキュリティポリシーの雛形が付録として追加されたこと、の4点である（Snouffer, Lee, and Oldehoeft［2001］）。FIPS 140-1からFIPS 140-2への移行は2002年5月までに実施することとされており、それまでは移行期間としてFIPS 140-1も引続き有効となっている。なお、これまでに策定されている標準規格等においては、FIPS 140-1が専ら参照されている。

*TCSEC（Trusted Computer Security Evaluation Criteria）：米国の国防機関等において利用されるセキュリティ機器の評価基準。1985年に策定され、通称オレンジブックと呼ばれる。TCSECでは、セキュリティ機器の7つのセキュリティレベル（D, C1, C2, B1, B2, B3, A1）を規定しており、A1が最も高いセキュリティレベルとなっている。

理者の不正行為によって署名が偽造されることを防ぐために秘密分散技術が活用されるケースが多い。秘密分散技術を秘密鍵の管理に利用する際には、秘密鍵を利用するために必要なデータ（activation data）を複数のデータに分割してそれぞれを別々の管理者に配布しておき、分割されたデータ（以下、分割データという）のうち一定数以上が集まらなければ元のデータを復元できず秘密鍵を利用できない、という方法が一般的である。分割データの管理者の1人が秘密鍵を不正に利用しようとした場合でも、他の複数の管理者とも結託する、または、それらが管理する分割データを何らかの方法で入手する必要があり、秘密鍵管理の安全性向上が期待できる。

秘密分散技術の代表的な方式には、分割データをすべて集めないと秘密のデータを復元できないというシンプル・シェアド・コントロール・スキーム（simple shared control scheme）と、n個の分割データのうちいずれかk個（kはnより小さい自然数）を集めるとデータを復元できるという（k, n）しきい値秘密分散法の2つが挙げられる。このうち、シンプル・シェアド・コントロール・スキームの場合、1つの分割データが利用不可能になると秘密鍵を利用することができなくなるという問題点が存在する。一方、（k, n）しきい値秘密分散法の場合には、（$n-k$）個の分割データが利用できないケースにおいても秘密鍵を利用する余地がある反面、分割データの作成方法や秘密鍵を利用するために必要なデータの復元方法がシンプル・シェアド・コントロール・スキームに比べて複雑になる。

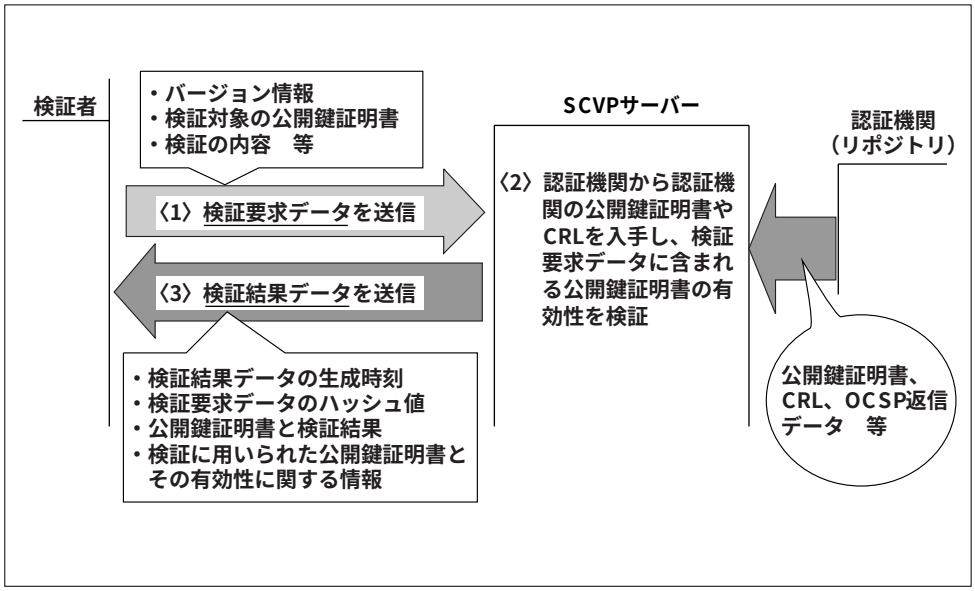
ニ．公開鍵証明書の有効性確認方法

公開鍵証明書の有効性を確認する基本的な方法は、LDAPによって公開鍵証明書を入手し、CRLやOCSPによって失効情報を確認するというものである。しかし、デジタル署名検証時に公開鍵証明書の信頼パスを辿る場合、信頼パス上に存在する複数の認証機関から公開鍵証明書を入手しおのおのの失効情報を確認しなければならず、認証パス上に多数の認証機関が存在するケースでは、通信および署名検証に関する検証者の負担が大きくなるという問題が存在する。

こうした負担を軽減するために、認証機関や他のエンティティが検証者の代わりに公開鍵証明書の有効性を確認し、その結果を検証者に通知するという機能がPKIの中に組み込まれる場合がある。例えば、3節で紹介するアイデントラスやスイフトのPKI、わが国の政府認証基盤（GPKI）では、認証機関が検証者に対して公開鍵証明書の有効性確認サービスを提供している。こうした仕組みに関する技術として、現在IETFで検討されているプロトコルSCVP（simple certificate validation protocol）が挙げられる（Malpani, Hoffman, and Housley［2000］）。

SCVPでは、SCVPサーバーと呼ばれるエンティティが認証機関とは別に準備される。まず、検証者はSCVPサーバーに対して検証対象の公開鍵証明書等のデータを送信する（図12参照）。SCVPサーバーは、検証パスを辿るために必要なすべての公開鍵証明書とその失効情報を各認証機関から入手し、それらを用いて各公開鍵証明書のデジタル署名の検証を代行する。最後に、SCVPサーバーは検証者に対して検

図12　SCVPにおけるデータ交信とデータ形式



証結果を通知する。ただし、検証者がSCVPサーバーを信頼できない場合、SCVPサーバーは検証に必要なすべての公開鍵証明書を入手して検証者に送信し、検証者が自分で信頼パスを辿る仕組みとなっている。

ホ．デジタル署名の検証方法

公開鍵証明書の有効性確認に加えて、デジタル署名検証アルゴリズムの実行も検証者が専用サーバーに依頼するプロトコルDVCS（data validation and certification server protocol、Adams *et al.*［2001］）がIETFにおいてRFC 3029として標準化されている。RFC 3029では、検証者と専用サーバー（DVCサーバー）との間の通信データ形式が規定されている[8]。

DVCSでは、まず検証者がデジタル署名付きデータをDVCサーバーに対して送信する。DVCサーバーは、認証機関から公開鍵証明書、CRL、OCSPの返信データ等を入手し、データ検証証明書（DVC：data validation certificate）を生成して検証者に送信する。データ検証証明書には検証結果を示すデータのほか、DVCサーバーのデジタル署名が含まれる。このように、DVCSのプロトコルの形態はSCVPとよく似ているものの、DVCSを実行するサーバー（DVCサーバー）を信頼できる第三者機関として想定する点がSCVPと異なる。

8　DVCSのほかに、検証対象の公開鍵証明書が期限切れとなった場合でも署名検証を可能とするプロトコルDSVP（delegated signature validation protocol、Pinkas［2001］）が現在IETF PKIXにおいて検討されている。

なお、RFC 3029は、デジタル署名の検証のほかに、データの所有の証明（certification of possession of data）や公開鍵証明書検証（certification of public key certificates）のサービスを行う場合の交信データ形式も規定している。

以上、紹介してきた技術を整理すると、表3のとおりである。

表3　PKI関連の主要な技術

適用分野		技術
公開鍵証明書	データ形式	X.509（バージョン3）準拠の公開鍵証明書：ITU-T X.509において規定されている公開鍵証明書。公開鍵、公開鍵所有者の識別子、有効期限、認証機関の識別子、署名アルゴリズムの識別子等のデータを含む。
	保管	X.500準拠のデータベース：ITU-T X.500において規定されているディレクトリを採用したリポジトリ用のデータベース。ディレクトリの形式としてDITと呼ばれる階層構造を利用する。
	配布	LDAP：X.500準拠のディレクトリを採用したデータベースにアクセスし、データを検索・入手するプロトコル。RFC 2251に規定されている。
	有効性確認	SCVP：証明書有効性確認用のサーバーとデータ交信を行い、公開鍵証明書の有効性確認を実行するプロトコル。
証明書失効情報	データ形式	X509（バージョン2）準拠の証明書失効リスト（CRL）：ITU-T X.509において規定されているCRL。認証機関の識別子、署名アルゴリズムの識別子、更新日時、失効した公開鍵証明書の情報等のデータを含む。
	配布	・CRL分割配布：CRLを複数に分割し、配布する技術。ITU-T X.509に規定されている。 ・デルタCRL：CRL更新時に新たに失効した公開鍵証明書のデータをデルタCRLとして配布する技術。ITU-T X.509に規定されている。 ・OCSP：要求された公開鍵証明書の失効情報をリアルタイムで配布する技術。RFC 2560に規定されている。
秘密鍵の保管・使用		＜秘密鍵を格納するモジュール＞ ・FIPS 140-1準拠のモジュール：FIPS 140-1に規定されたセキュリティ要件に沿って設計されたモジュール。 ＜秘密鍵の分散管理＞ ・シンプル・シェアド・コントロール・スキーム：秘密鍵の不正利用を防止するために、秘密鍵を利用する際に用いるデータを分割して複数の管理者に配布し、秘密鍵を利用する際には分割されたデータすべてを用いることが必要となるという技術。 ・（k, n）しきい値秘密分散法：秘密鍵の不正利用を防止するために、秘密鍵を利用する際に用いるデータを分割して複数（n人）の管理者に配布し、秘密鍵を利用する際には分割されたデータのうち一定数（k）のデータが必要となるという技術。
デジタル署名の検証		DVCS：デジタル署名検証用のサーバーとデータ交信を行い、デジタル署名の検証を行うプロトコル。RFC 3029に規定されている。

(4) 証明書ポリシーと認証実施規程

(3)で説明してきた各技術を活用してPKIを適切に構築するためには、認証業務の目的、公開鍵証明書の用途、利用環境等を考慮したうえで、PKIにおけるセキュリティ要件を適切に設定することが必要となる。こうした認証業務の全体像を記述する文書として、認証機関は証明書ポリシーと認証実施規程を作成するケースが一般的となってきている。金融分野では、米国において、証明書ポリシーおよび認証実施規程に関する国内標準ANS X9.79-1が2001年に策定されているほか、ISOにおいても、これらの文書に関する国際標準化の検討が進められている。

証明書ポリシーは、「どのような環境のもとで、どのような目的に利用される公開鍵証明書を発行・管理するか」を定める認証業務の基本方針である。ANS X9.79-1では、金融分野向けの証明書ポリシーの内容が規定されている。具体的には、証明書ポリシーの識別子や公開鍵証明書の利用条件のほか、証明書ポリシーの管理方法（証明書ポリシーの公表・変更手続等）、公開鍵所有者の責務（秘密鍵の管理、秘密鍵漏洩時の対応等）、検証者の責務（公開鍵証明書の有効性確認、デジタル署名の検証等）、認証機関の責務（公開鍵証明書の発行・失効の周知、証明書ポリシーの遵守等）等が規定されている。

一方、認証実施規程は、証明書ポリシーを実現する具体的な施策であり、認証機関等の各エンティティにおける業務運用の体制が詳細に規定される。ANS X9.79-1では、金融分野向けの認証実施規程のモデルが記述されている（表4参照）。

表4　認証実施規程のモデル（ANS X9.79-1）

モデルの章構成	内容
導入	準拠する証明書ポリシー、認証実施規程の識別情報、PKIを構成するエンティティ、公開鍵証明書を利用するアプリケーション、ポリシーの管理組織
一般規定	各エンティティの責任・義務、準拠法、公開鍵証明書の失効情報の公表タイミング、監査の実施タイミング、情報の機密管理方法
識別と認証	初期登録時の利用者の識別・認証手続、公開鍵証明書の発行申請・更新申請・失効申請時における申請者の識別・認証手続
運用要件	公開鍵証明書の発行・更新・失効手続、鍵寄託等に関する要件・手続、セキュリティ監査の内容・手続、各種ログの管理方法、認証業務の廃業時の手続
物理面、手続面、人事面のセキュリティ管理	認証機関の物理的な安全対策（建物、設備、入退室管理等）、認証機関のセキュリティ管理組織、認証機関の従業員の採用・研修手続
情報セキュリティ管理	鍵ペア生成・保管・更新方法、秘密鍵の管理方法、秘密鍵以外のデータ（公開鍵やPIN等）の管理方法、システム開発・メンテナンス時の管理方法、暗号モジュール管理方法
公開鍵証明書と公開鍵証明書失効リスト	公開鍵証明書・公開鍵証明書失効リストのデータ形式、公開鍵証明書の管理・配布方法、公開鍵証明書失効情報の管理・配布方法
変更管理	証明書ポリシーと認証実施規程の変更手続、通知方法、承認手続

証明書ポリシーや認証実施規程に関する各種標準の成立は、PKIサービスを開始したいと考えている金融機関にとって大きな意味をもっている。すなわち、ANS X 9.79-1やRFC 2527等を参考にしながら証明書ポリシー等を適切に作成し、これらに沿ってセキュリティ対策を講じることによって、ANS X9.79-1等を利用することができなかった従来に比べ、認証業務のセキュリティをより体系的かつ効果的に確保することが可能になると考えられる。

また、電子認証サービスを利用したいと考える利用者からみても、証明書ポリシーや認証実施規程が整備されている場合、それらの内容を参考にして公開鍵証明書の利用範囲や認証機関のセキュリティ要件が自分の利用条件に合致するかを判断することが可能となる。なお、証明書ポリシーや認証実施規程を公開するか否かについて、ANS X9.79-1では、これらに含まれる情報の機密度に応じて検討する必要があるとしている。

3．金融分野等における主要なPKI構築の動き

(1) 金融機関によるPKIへの取組み

従来の金融分野におけるPKIの利用形態は、各金融機関が電子認証サービスを提供する企業から発行された公開鍵証明書を活用し、インターネット・バンキングやオンライン証券取引等のサービスにおいて利用者の本人確認等に用いるといったものが大半であった（谷口［2000］）。米ジオンズ銀行が認証機関を運営する子会社デジタル・シグニチャ・トラストを設立した事例等、金融機関が認証業務に取り組むケースもみられたが、そうした事例は一部にとどまっていた。

これに対し、最近では、金融機関自らが認証機関となる、もしくは、複数の金融機関が共同で設立した組織が認証機関となるPKIを構築する事例がいくつもみられる。例えば、①わが国の全銀協、②欧米の金融機関等によって設立されたアイデントラス、③国際的な金融機関間メッセージ通信サービスを提供しているスイフト、④米国銀行協会（ABA：American Bankers Association）の電子認証サービス子会社ABAecom、⑤欧州の銀行が参加して設立されたGTA（Global Trust Authority）が、PKIの構築を進めている。

これらのPKIでは、金融機関が認証機関として参画しており、電子認証サービスを提供する企業によって発行された公開鍵証明書を活用するという従来のPKIの利用形態に比べ、金融機関がPKIのシステムに直接関与している。また、ルート認証機関が各金融機関に対して公開鍵証明書を発行する階層型のPKIが採用されており、従来に比べ高度な形態でのPKIの活用が図られている。例えば、アイデントラス のPKIでは、アイデントラスがルート認証機関、アイデントラスに参加する金融機関が下位の認証機関となり、各金融機関から公開鍵証明書の発行を受けた企業等がその公開鍵証明書を用いて企業間電子商取引において電子認証を行うという仕組

みとなっている。

このほか、わが国では政府認証基盤（GPKI）、米国政府ではFPKI（Federal PKI）の検討が進められている。GPKIやFPKIに関しては、金融機関がPKIの利用者として公開鍵証明書の発行を受け、政府への電子申請・届出を実行するというケースのほか、金融機関が認証機関としてGPKI等と相互認証するといったケースも考えられる。また、GPKIやFPKIではブリッジCAを用いたハイブリッド型のPKIが採用されており、これらのPKIの検討内容は、金融機関が今後PKIを構築・運用していく際に1つのモデルとなるという意味でも注目される。

本節では、こうしたPKIの中からその具体的な構造やセキュリティ対策に関する情報が公開されているものとして、全銀協、アイデントラス、スイフトのPKI、GPKI、FPKIを取り上げて説明するほか、金融機関が認証機関として機能するものではないが、金融機関が貿易金融取引の当事者として検討に関与している貿易金融EDI（TEDI）のPKIについても、金融分野に関連するPKIとして取り上げる。

なお、各PKIにおける情報セキュリティ対策に関する説明では、認証機関の秘密鍵の管理と、公開鍵証明書の失効情報の管理を中心に説明する。認証機関の秘密鍵の管理を強調する理由は、認証機関の秘密鍵の管理が不適切であり秘密鍵が第三者に漏洩した場合、その秘密鍵によって生成されたデジタル署名を含む公開鍵証明書がすべて信頼できなくなり、PKIの機能に深刻な影響をもたらすことが想定されるためである。また、公開鍵証明書の失効情報の管理に関しては、失効情報の管理が不適切であった場合、秘密鍵漏洩を理由とする公開鍵証明書の失効申請がなされていたにもかかわらずその事実が周知されないという状況が発生し、最悪のケースと

表5　各PKIの主な特徴点

金融機関・団体	認証機関	信頼構造	公開鍵証明書の主な用途	認証業務開始（予定）日
全銀協	全銀協（ルートCA）、加盟銀行（下位CA）	階層型	ICキャッシュ・カードやATM端末等による相手確認	2002年2月
アイデントラス	アイデントラス（ルートCA）、加盟金融機関（下位CA）		企業間電子商取引での相手確認、メッセージ一貫性確認	2000年12月
スイフト	スイフト		スイフトネット上における相手確認、メッセージ一貫性確認	2002年末（スイフトネット開発完了予定）
TEDI	一定基準を満足する民間の認証機関	未定	貿易取引関連データ交信での相手確認、メッセージ一貫性確認	未定
日本政府（GPKI）	ブリッジ認証局、各府省認証局	ハイブリッド型	電子申請・届出や結果通知等における相手確認、メッセージ一貫性確認	2002年度中（全府省の認証局の整備完了予定）
米国政府（FPKI）	ブリッジCA、各政府機関の認証機関			不明（2000年にブリッジCA実装実験を実施）

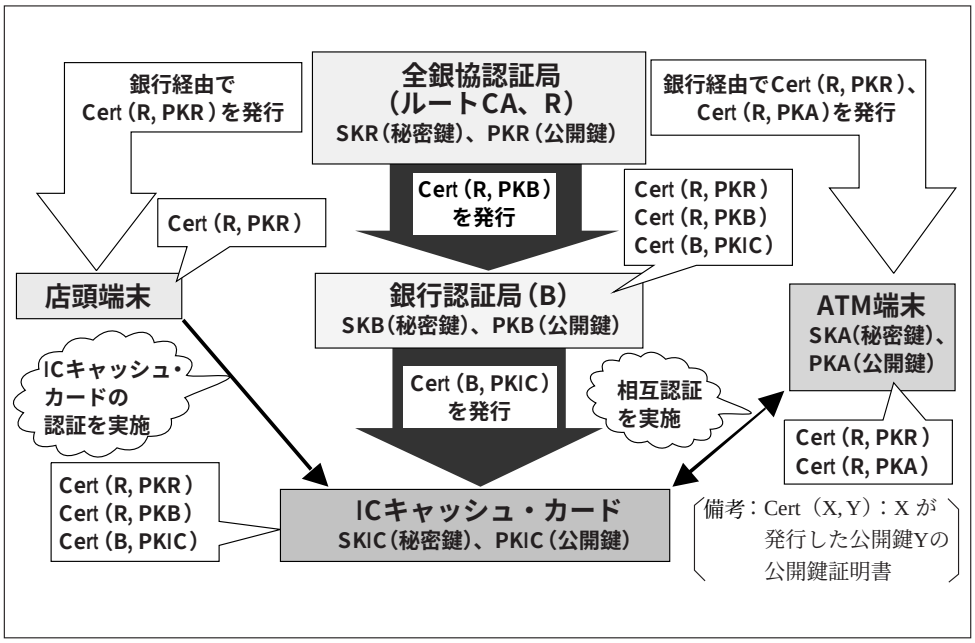
して、偽造された署名が正当なものとして誤認され、認証機関に対する信頼が大きく低下する事態につながるためである。

以下で取り上げる各PKIの主な特徴点を予め整理すると、表5のとおりである。

（2）全銀協のPKI

全銀協は、2001年3月に公表した「全銀協ICキャッシュ・カード標準仕様」（以下、全銀標準仕様という）に基づくICキャッシュ・カードのオフライン認証の実現を目指して、PKIの構築を進めている（全銀協［2001］）。全銀協のPKIの信頼構造は、全銀協が運営する認証局（以下、全銀協認証局という）がルートCAとなり、ICキャッシュ・カードを発行する銀行が下位CA（以下、銀行認証局という）となる階層型となっている（図13参照）。こうした階層型PKIの構築は、①ATM提携ネットワークを利用したICキャッシュ・カードと端末間の認証[9]において、ある銀行認証局が

図13　全銀協のPKIの構造



9　従来のキャッシュ・カード取引におけるATMでの認証方式は、キャッシュ・カードの磁気ストライプに書き込まれたデータや暗証番号等がATM提携ネットワーク経由でキャッシュ・カード発行銀行のホストに送られ、そのホストにおいてキャッシュ・カードの認証が行われるというものである。これに対し、全銀標準仕様のICキャッシュ・カードを利用する場合には、従来の認証方式よりも高度なオンライン認証方式が採用される予定である。ただし、ICキャッシュ・カード導入当初は、ATM接続ネットワークや銀行ホストが新しい認証方式に十分対応できないため、対応可能となるまでの経過期間中は、ICキャッシュ・カードの認証として、従来のオンライン認証方式と、公開鍵暗号方式を用いたオフライン認証方式の両方を用いることとされている。

発行したICキャッシュ・カードの公開鍵証明書を別の銀行のATM等でも検証可能にするほか、②今後オフライン・デビット取引等のサービスが利用可能となった場合に、ICキャッシュ・カードとATM端末との間でのオフラインによる相互認証[10]や、商店の店頭等に設置されるオフライン・デビット取引等の端末（以下、店頭端末という）におけるオフラインによるICキャッシュ・カードの認証を可能にすることを企図したものと発表されている。

本PKIにおける全銀協認証局の役割は、①おのおのの銀行認証局の公開鍵PKBに対する公開鍵証明書Cert（R, PKB）[11]の発行、②ATM端末の公開鍵PKAに対する公開鍵証明書Cert（R, PKA）の発行、③全銀協認証局の公開鍵PKRに対する自己署名証明書Cert（R, PKR）の配布、④各公開鍵証明書の失効情報の管理、の4つである。全銀協認証局では、公開鍵証明書の発行申請の受付・登録は東京銀行協会が担い、公開鍵証明書の生成はNTTコミュニケーションズに委託する形態となっている。一方、銀行認証局は、各ICキャッシュ・カードごとに秘密鍵SKICと公開鍵PKICを生成したうえで、PKICに対して公開鍵証明書Cert（B, PKIC）を発行し、SKIC、PKIC、Cert（B, PKIC）、Cert（R, PKR）、および、銀行の公開鍵に対する全銀協認証局が発行した公開鍵証明書Cert（R, PKB）をICキャッシュ・カードに格納・配布する。また、銀行認証局は、各ATM端末ごとに公開鍵PKAと秘密鍵SKAを生成し、各ATM端末に格納する。

ICキャッシュ・カードがATM端末の認証を行う場合には、予め入手している全銀協認証局の自己署名証明書Cert（R, PKR）と、ATM端末から入手するPKAおよびCert（R, PKA）を用いて「全銀協認証局の自己署名証明書→ATM端末の公開鍵証明書」という認証パスの検証が行われる。ATM端末がICキャッシュ・カードの認証を行う場合には、予め入手している全銀協認証局の自己署名証明書Cert（R, PKR）と、ICキャッシュ・カードから入手するCert（R, PKB）、Cert（B, PKIC）およびPKICを用いて「全銀協認証局の自己署名証明書→銀行認証局の公開鍵証明書→ICキャッシュ・カードの公開鍵証明書」という認証パスの検証が行われる。また、店頭端末がICキャッシュ・カードの認証を行う場合には、ATM端末によるICキャッシュ・カードの認証と同様の手順での検証が行われる。なお、各公開鍵証明書の失効情報については、全銀協認証局が銀行認証局等からの問い合わせに応じて失効情報を提供する仕組みとなっている。

10 ICキャッシュ・カードとATM端末でのオフラインによる相互認証は、オフライン・デビット取引におけるバリュー・チャージ処理の際に実施される。ただし、オフラインでの相互認証の実施は、ATM接続ネットワークや銀行ホストが新しいオンライン認証方式に対応可能となるまでの経過期間中に限定され、経過期間後はオンラインによる認証が行われることとされている。

11 Cert（X, Y）は、発行者Xが発行した公開鍵Yに対する公開鍵証明書を示す。Xの部分における各記号の意味は、R=全銀協認証局、B=銀行認証局である。

デジタル署名の生成にはRSA署名方式が採用されるほか、全銀協認証局の秘密鍵の管理に関しては、FIPS140-1のレベル4相当の機能を備えた耐タンパー装置であるハードウエア・モジュールによって秘密鍵が保管される。また、全銀協認証局については、電子署名法に基づく特定認証業務の認定指針（4節(3)において後述）に沿ってセキュリティ対策が講じられている。一方、銀行認証局に対しては、全銀協の定める認証局運営規則を遵守することが求められるほか、銀行認証局のセキュリティ対策の実施や業務運用に関する届出・報告義務などが課されている。

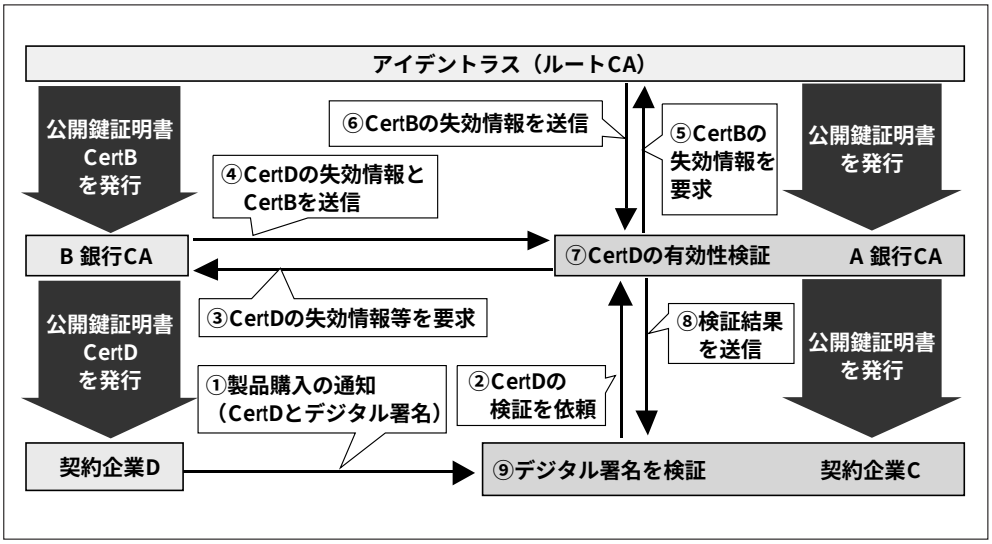
(3) アイデントラスのPKI

アイデントラスは、金融機関を認証機関とするPKIを構築し、グローバルな電子認証サービスを提供することを主たる目的として、金融機関の共同出資[12]によって1999年4月に米国において設立された有限会社である。アイデントラスのPKIでは、アイデントラスがルートCAとなり、アイデントラスと電子認証サービスに関する契約を締結した銀行が下位の認証機関（以下、銀行CAという）として参加する階層型の信頼構造が採用されている。銀行CAは、電子認証サービスの契約を行った企業（以下、契約企業という）に対して公開鍵・秘密鍵ペアおよび公開鍵証明書を生成・発行する。契約企業に対して発行される公開鍵証明書（X.509のバージョン3に準拠）は、インターネット上での企業間電子商取引における取引相手の確認や交信メッセージの一貫性確認等に利用される。

アイデントラスのPKIにおける公開鍵証明書を利用した取引相手確認の基本的な手順を図14によって説明する。例えば、B銀行CAから公開鍵証明書CertDの発行を受けている契約企業Dがインターネット経由で契約企業Cの製品の購入意思を通知し、A銀行CAから公開鍵証明書の発行を受けている契約企業Cが企業Dの相手確認を実施するケースを想定する。B銀行CAとA銀行CAはアイデントラスから公開鍵証明書の発行を受けているほか、アイデントラスの自己署名証明書を入手しているものとする。

12 1999年4月のアイデントラス設立時には、エービーエー・アムロ、バンク・オブ・アメリカ、チェース・マンハッタン、シティバンク等欧米金融機関8社が参加していたが、2002年1月現在、世界各国51の金融機関がアイデントラスに参加している（うち邦銀は、UFJ銀行、みずほコーポレート銀行、東京三菱銀行、三井住友銀行）。

図14　アイデントラスのPKIを利用した取引相手確認の基本的な手順



〈契約企業Dの本人確認手順〉

① 契約企業Dは、商品購入希望のデータを、公開鍵証明書CertD、商品購入希望データに対するデジタル署名とともにインターネット経由で契約企業Cに送信する。

② 契約企業CはCertDをA銀行CAに送信し、CertDの有効性の検証を依頼する。

③ A銀行CAは、CertDを発行したB銀行CAに対して、インターネット経由でCertDの有効性に関するデータ（失効情報等）を要求する。有効性に関するデータの入手方法としてはOCSPを利用する。

④ B銀行CAは、CertDの有効性に関する情報と、B銀行CAの公開鍵に対する公開鍵証明書CertBをA銀行CAに送信する。

⑤ A銀行CAは、アイデントラスのルートCAに対して、CertBの有効性に関するデータを要求する。有効性に関するデータの入手方法としてはOCSPを利用する。

⑥ ルートCAはA銀行CAに対してCertBの有効性に関するデータを送信する。

⑦ A銀行CAは、B銀行CAやルートCAから得た情報等に基づいてCertDの有効性の検証（認証パス「ルートCAの自己署名証明書→B銀行の公開鍵証明書CertB→契約企業Dの公開鍵証明書CertD」の検証）を実行し、その結果を契約企業Cに送信する。

⑧ 契約企業Cは、CertDの有効性に関する検証が成功した場合、CertDに含まれる契約企業Dの公開鍵を用いて商品購入希望データに対するデジタル署名を検証する。

このように、銀行CAは、取引相手確認を実行する契約企業に代わり、取引相手

の公開鍵証明書の有効性確認サービスを提供している点が特徴である。このほか、各銀行CAは、契約企業からの認証サービスの要求内容やその処理結果に関するログを保管し、例えば、特定のメッセージを送信した契約企業がそのメッセージ送信の事実を後日否認することを防ぐ否認防止（non-repudiation）サービスも提供している[13]。

アイデントラスのPKIにおけるセキュリティ管理については、契約企業に対して発行される公開鍵証明書に関する証明書ポリシー（Identrus［2001］）が公開され、その中に一部記述されている。ただし、ルートCAの証明書ポリシー等については非公開となっており、詳細な内容は公表されていない。契約企業に対して発行される公開鍵証明書に関する証明書ポリシーには、公開鍵証明書の用途、各エンティティの権限・責任、公開鍵証明書の発行手続、公開鍵証明書および秘密鍵の管理方法等の概要が記述されている。鍵管理に関しては、銀行CAが鍵ペアの生成をFIPS 140-1のレベル2相当の暗号モジュール内で生成・暗号化したうえで、FIPS 140-1のレベル2相当のICカード等に格納して契約企業に配布するとされている。また、秘密鍵を利用するために必要なデータ（PIN等）は、秘密鍵を格納したICカード等とは別の手段によって安全に契約企業に配布すると規定されている。なお、ルートCAや銀行CAにおけるセキュリティ監査に関しては、証明書ポリシーには規定されていない。

（4）スイフトのPKI

国際的な金融機関間取引のメッセージ通信サービスを提供しているスイフトは、独自の通信プロトコルを利用した従来の通信システムのスイフトII（SWIFT II）に代わる新しい通信システムとして、インターネットとの親和性が高いスイフトネット（SWIFTNet）の検討を1999年より進めている。スイフトネットでは、インターネットで利用されている通信プロトコルTCP/IPが採用されているほか、リアルタイム・双方向通信が可能とされており、リアルタイム双方向メッセージ通信サービスであるインターアクト（InterAct）や、数メガバイトの決済情報を格納したファイ

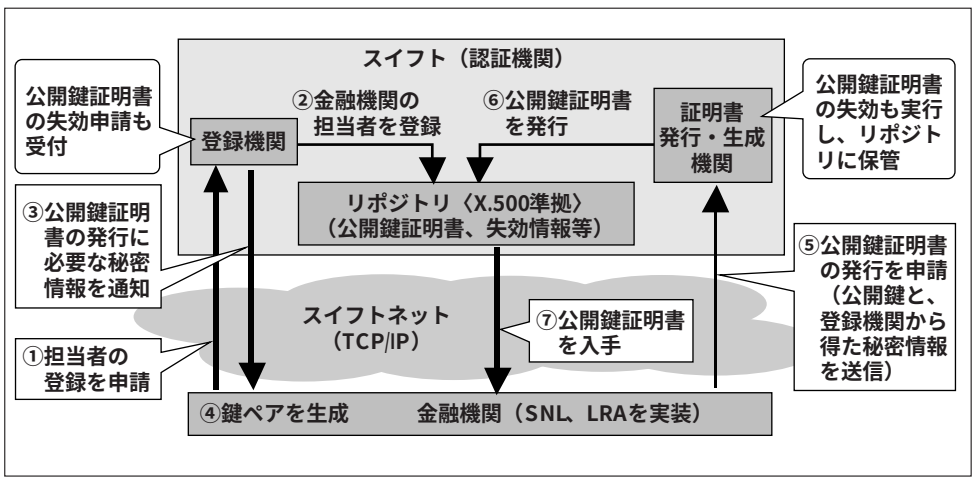
13 アイデントラスは、トラストアクト（TrustAct）と呼ばれる否認防止サービスをスイフトと共同で提供している。トラストアクトでは、スイフトが管理する専用サーバー（トラストアクト・サーバー）が設置され、トラストアクト・サーバーと各銀行CAとの間の通信は現在スイフトが開発を進めているスイフトネット上で行われる。例えば、A銀行CAから公開鍵証明書の発行を受けた契約企業Dが、B銀行CAから公開鍵証明書の発行を受けた契約企業Cに売買注文書を送信する場合に、トラストアクトにおける処理の流れを簡略化して説明する。まず、契約企業Dは自分の公開鍵証明書や売買注文書をインターネット経由でトラストアクト・サーバーに送信する。トラストアクト・サーバーは、契約企業Dの公開鍵証明書の有効性に関する情報をA銀行CAからスイフトネット経由で入手し、売買注文書のコピー（日時データ等を添付）をデータベースに保管する。その後、トラストアクト・サーバーは、 売買注文書を公開鍵証明書の有効性確認結果とともに企業Bにインターネット経由で送信する。後日売買注文書の内容に疑義が生じた場合、トラストアクト・サーバーに保管されているコピーを参照することによってその内容を確認することができる。

ル交換サービスであるファイルアクト（FileAct）等の新しいサービスが提供される予定となっている（SWIFT［2000］）。さらに、スイフトネットは、メッセージの送受信時に電子認証による通信相手の確認や通信メッセージの一貫性確認を実現する仕様となっており、スイフトネットにおける電子認証を実現する際に必要となるPKIの検討が行われている。

スイフトのPKIでは、スイフトが認証機関となり、スイフトネットの利用契約を締結した各金融機関の担当者に対して公開鍵証明書（X.509バージョン3準拠）を発行するという形態となっている。公開鍵証明書は、デジタル署名用と暗号化用の2種類が用意されている。スイフトの認証機関は主に3つのサーバーから構成されており、各サーバーは、ANS X9.79-1で規定されている証明書発行・生成機関[14]、登録機関、リポジトリに対応する機能をそれぞれ担う。スイフトの認証機関から公開鍵証明書の発行を受ける金融機関は、スイフトネットへの接続や鍵ペアの管理を行うソフトウエアSNL（SWIFTNet Link）と、スイフトの認証機関と連携して各金融機関の担当者の登録や公開鍵証明書の発行要求を行うソフトウエアLRA（local registration application）をインストールすることが要求される。なお、認証機関は、システムの信頼性を高める目的から二重化され、欧州および米国のスイフト・オペレーティング・センター内にそれぞれ設置される予定となっている。

デジタル署名用公開鍵証明書の発行手順は次のとおりである（図15参照）。

図15　スイフトネットのPKIの構造と公開鍵証明書の発行



14　スイフトの認証機関を構成するサーバーのうちの1つは、ANS X9.79-1で記述されている証明書発行機関と証明書生成機関の両方の機能を担っている。ここでは、本サーバーを証明書発行・生成機関と呼ぶ。

〈公開鍵証明書の発行手順〉

① 金融機関は、自社の担当者を公開鍵証明書の利用者として登録するための申請データをスイフトの登録機関にスイフトネット経由で送信する。
② 登録機関は、申請された者を審査し、公開鍵証明書の利用者としてリポジトリに登録する。
③ 登録機関は、金融機関に対して登録完了を通知するとともに、公開鍵証明書の発行申請に必要な秘密情報をスイフトネット経由で金融機関に送信する。
④ 金融機関は、公開鍵証明書の対象となる公開鍵と秘密鍵のペアを生成する。
⑤ 金融機関は、スイフトの証明書発行・生成機関に対して、生成した公開鍵や登録機関から得た秘密情報等を送信し、公開鍵証明書の発行を申請する。
⑥ 証明書発行・生成機関は、公開鍵証明書を発行してリポジトリに保管し、公開鍵証明書を発行したことを金融機関に通知する。
⑦ 金融機関は、スイフトネット経由でスイフトのリポジトリにアクセスし、公開鍵証明書を入手する。

スイフトのPKIにおける証明書ポリシーと認証実施規程は現時点で公開されていないものの、スイフトネットに関する公表資料（SWIFT［2000］）の中にPKIの仕組みやセキュリティ対策に関する記述がある。鍵管理に関しては、金融機関の担当者が所有するデジタル署名用の鍵ペアはその金融機関のSNLで生成される一方、暗号化用の鍵ペアはスイフトの証明書発行・生成機関によって生成されてSNLへ送付される仕組みとなっている。署名生成・検証やデータ暗号化にはRSA署名方式およびRSA暗号方式が採用され、鍵長は金融機関の担当者の鍵と認証機関の鍵においてそれぞれ1,024 bit、2,048 bitと定められている。金融機関の担当者の秘密鍵はそれぞれSNLにおいて暗号化され、FIPS 140-1のレベル2相当のICカードに別々に格納されるほか、認証機関の秘密鍵は耐タンパー・ハードウエア（FIPS 140-1のレベル3相当）に保管されることとなっている。

公開鍵証明書の失効に関しては、証明書発行・生成機関は公開鍵証明書の失効処理を行ったうえで、リポジトリに保管されているCRL（X.509バージョン2準拠）にその情報を反映する仕組みが採用されている。リポジトリはX. 500に基づいて構築されており、スイフトネットを利用する金融機関のみがアクセス可能となっている。

なお、スイフトのPKIに関する公表資料（SWIFT［2000］）には、認証機関のセキュリティ監査に関する情報は記述されていない。

（5）TEDIのPKI

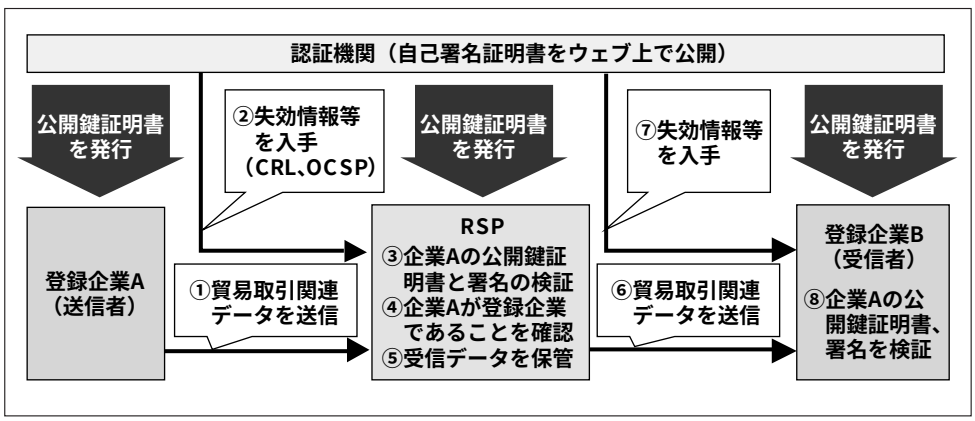
TEDIは、貿易手続に用いられる紙の書類を電子化し、ネットワーク経由で安全かつ迅速に授受できるようにすることを目的として、通商産業省（現経済産業省）の支援のもとで1998年に開始された貿易金融EDIのプロジェクトである。現在TEDI

の具体的な検討は、貿易取引当事者、銀行、保険会社、運輸会社等が参加する業界団体テディ・クラブ（TEDI Club）[15]によって進められており、TEDIに関する各種ガイドラインの作成、各種技術の標準化、TEDIと他の貿易EDIプロジェクトとの相互運用性に関する検討等の活動が行われている。これまでにTEDIのシステムの技術仕様や運用に関するガイドライン（TEDI Club［2001a］）が公開されている。

TEDIのシステムの主な特徴は、貿易取引関連データが取引当事者間で交信される際に、各データに送信者のデジタル署名および公開鍵証明書が添付され、RSP（repository service provider）と呼ばれる第三者機関を介して通信が行われる点にある。RSPは、TEDIの登録企業のリストを管理しており、ある企業からデータを受信すると、そのデータに添付される公開鍵証明書によって送信者がTEDIの登録企業であることを確認し、受信データに日時データ、送受信者名、RSPのデジタル署名等を添付したうえでデータベースに保管する役割をもつ。後日、TEDIのネットワーク上で交信された取引データの存在や内容が問題となった場合、RSPのデータベースに保管されているデータを検査することによって問題解決が図られる仕組みとなっている。

TEDIでは、電子化された貿易取引関連データの送信者を確認するとともに、送信されたデータの一貫性を確認する手段としてPKIを利用することが予定されている。TEDIのPKIでは、TEDI独自の認証機関を準備せず、既存の認証機関から公開鍵証明書の発行を受けることを想定している。TEDIの登録企業は、TEDIのガイドラインやモデル運用規程の仕様を満足する認証機関から公開鍵証明書の発行を受け、その公開鍵証明書をTEDIに利用することとなる（TEDI Club［2001a, b］）。ガイドラインによると、公開鍵証明書はデジタル署名用の公開鍵に対して発行され、X.509バージョン3に準拠することが必要とされている。また、デジタル署名の生

図16　TEDIのPKIの枠組みと電子認証



15　2002年4月時点でテディ・クラブに参加していた企業・団体は87先、そのうち銀行は、みずほコーポレート銀行、東京三菱銀行、三井住友銀行、UFJ銀行、あさひ銀行、東京都民銀行、信金中央金庫、ドイツ銀行東京支店、シティバンク東京支店であった。

成・検証にはRSA署名方式、ハッシュ関数にはSHA-1を利用することが定められているほか、認証機関とTEDIの登録企業が利用する公開鍵の鍵長はそれぞれ2,048 bit、1,024 bitと規定されている。

登録企業Aが認証機関から公開鍵証明書の発行を受け、登録企業Bに対してRSPを介して貿易取引関連データを送信する手順は以下のとおりである（図16参照）。

〈TEDIにおけるデータ通信の手順〉

① 登録企業Aは、貿易取引関連データにデジタル署名を添付し、公開鍵証明書とともにRSP経由で登録企業Bに送信する。
② RSPは、登録企業Aの公開鍵証明書の有効性に関する情報をCRLやOCSPによって認証機関から入手する。
③ RSPは、認証機関から得た有効性に関する情報と認証機関の自己署名証明書を用いて、登録企業Aの公開鍵証明書とデジタル署名の検証を行う。
④ RSPは、登録企業AがTEDIの登録企業であることを登録企業のリストを用いて確認する。
⑤ RSPは、登録企業Aが登録企業であり、企業Aから送信されたデータが改ざんされていないことを確認し、受信データに日時データや送受信者名等を添付するとともに、それらに対する自分のデジタル署名を生成して一緒にデータベースに保管する。
⑥ RSPは企業Aから受信したデータを企業Bに転送する。
⑦ 企業Bは、企業Aの公開鍵証明書の有効性に関する情報等をCRLやOCSPによって認証機関から入手する。
⑧ 企業Bは、認証機関の自己署名証明書や企業Aの公開鍵証明書の有効性に関する情報等を用いて、企業Aの公開鍵証明書とデジタル署名の検証を行う。

PKIにおけるセキュリティ対策等については、認証機関に関するガイドライン（TEDI Club［2001a］）に大枠が記述されているのみであり、各参加者が認証実施規程等を参考にして適切な認証機関を選択し、公開鍵証明書の発行を受けることが求められている。認証機関に関するガイドラインによれば、鍵ペアの生成は、登録企業やRSPが自分で専用ソフトウエアによって生成することとされている。認証機関の秘密鍵の生成・保管については、「現時点において秘密情報の改ざん、漏洩に対してハードウエア暗号装置の方が安全性が高く、ハードウエア暗号装置の使用が望ましい」と記述されており、ハードウエア・モジュール内での秘密鍵の生成・保管が推奨されている。また、秘密鍵の使用については、「全員がそれぞれの管理機能を遂行しなければその機能が働かないようにする合議制操作の機能や、1つの情報を複数の要素に分解し、所定の数がそろわないと元の情報の一部さえ再現できない分散保管等の機能を有することが望ましい」とされている。

公開鍵証明書の失効情報については、TEDIの登録企業は、認証機関に公開鍵証明書の失効を申請するだけでなく、RSPに対しても同様の申請を行う仕組みとなっ

ている。失効申請を受けたRSPは、登録企業のリストにおいて失効申請を行った企業の欄に無効を示すフラグを立てるという処理を行い、以後その企業宛のデータを受信した場合、無効になっている旨を送信元に通知する。認証機関のCRLやOCSPだけでなくRSPにおける登録企業リストの管理を行う理由について、テディ・クラブ作成の認証機関に関するガイドラインには、「登録企業がさまざまな認証機関から公開鍵証明書の発行を受けることが想定され、そのうちいくつかの認証機関がCRLを採用していた場合、リアルタイムでの失効情報の利用が困難となる可能性がある」としたうえで、「RSPの登録企業リストによる失効処理によって常にリアルタイムでの失効情報の利用が可能になる」と記載されている。

なお、認証機関のセキュリティ監査に関しては、認証機関に関するガイドラインに記載されていない。

(6) わが国の政府認証基盤（GPKI）

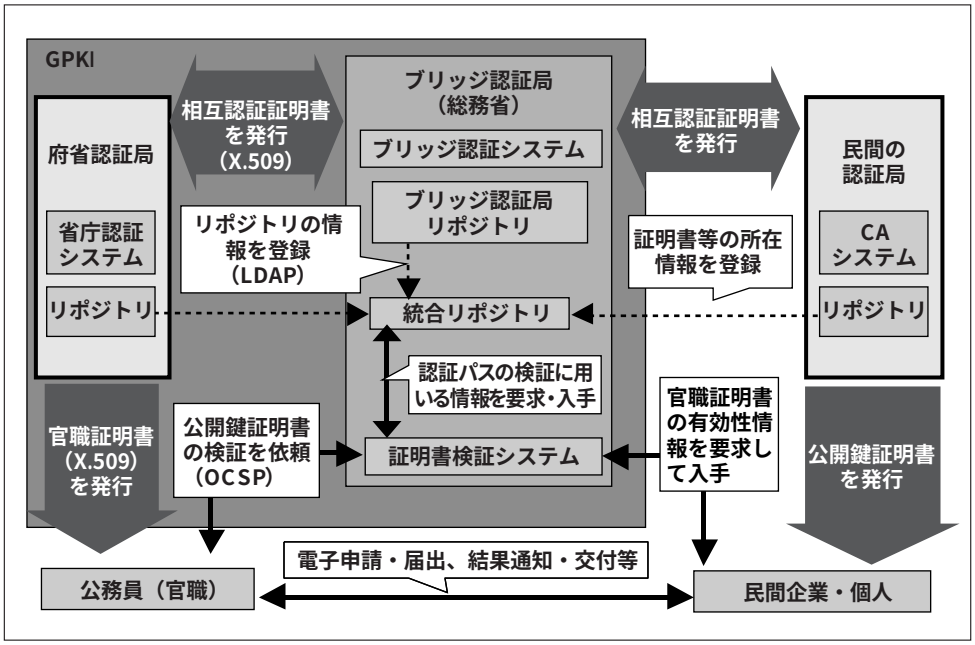
政府認証基盤（GPKI：Government Public Key Infrastructure）は、民間企業や個人が行政手続の申請や届出を電子的に行う場合や、政府が民間企業等に対して電子的に申請結果の通知や各種データの交付等を行う場合に、政府と民間企業・個人間における電子認証を実現するPKIである。わが国の政府は、政府部門の電子化を目標として掲げたe-Japan構想に基づき、2003年度中の電子政府実現に向けて各種電子化施策を推進している。GPKIは、そうした取組みの一翼を担うものであり、各府省において検討が進められている。

GPKIは、各府省の認証機関（以下、府省認証局という）とそれらを相互に接続するブリッジ認証局から構成される。府省認証局は下位の認証局をもつケースも想定されており、GPKIはハイブリッド型の信頼構造となっている（図17参照）。各府省認証局は、各官職に対して鍵ペアおよび公開鍵証明書（官職証明書）を発行するほか、ブリッジ認証局との相互認証証明書、自己署名証明書を発行する。一方、ブリッジ認証局は、各府省認証局との相互認証証明書、自己署名証明書を発行するほか、民間の認証局との間でも相互認証証明書を発行することが想定されている[16]。

ブリッジ認証局は、①ブリッジ認証システム（ブリッジ認証局の鍵管理、相互認証証明書の発行等を実行）、②ブリッジ認証局リポジトリ（各種証明書、失効情報等を格納）、③統合リポジトリ（ブリッジ認証局リポジトリおよび府省認証局リポ

16 府省認証局がブリッジ認証局と相互認証を行うためには、官職認証に関する府省認証局CP/CPSガイドライン（総務省［2001b］）に準拠し、GPKI相互運用性仕様書（総務省［2001a］）に規定される仕様を満足することが必要とされる（2001年12月現在、ブリッジ認証局と相互認証を完了している府省認証局は経済産業省認証局、国土交通省認証局の2つ）。また、民間認証局がブリッジ認証局と相互認証を行うためには、利用者認証に関する基準として電子署名法における特定認証業務の認定を受ける必要があることに加え、相互認証に関する基準としてGPKI相互運用性仕様書に規定される仕様を満足する必要がある。なお、商業登記認証局に対しては、府省認証局と同じ基準が適用される。

図17　GPKIの枠組み

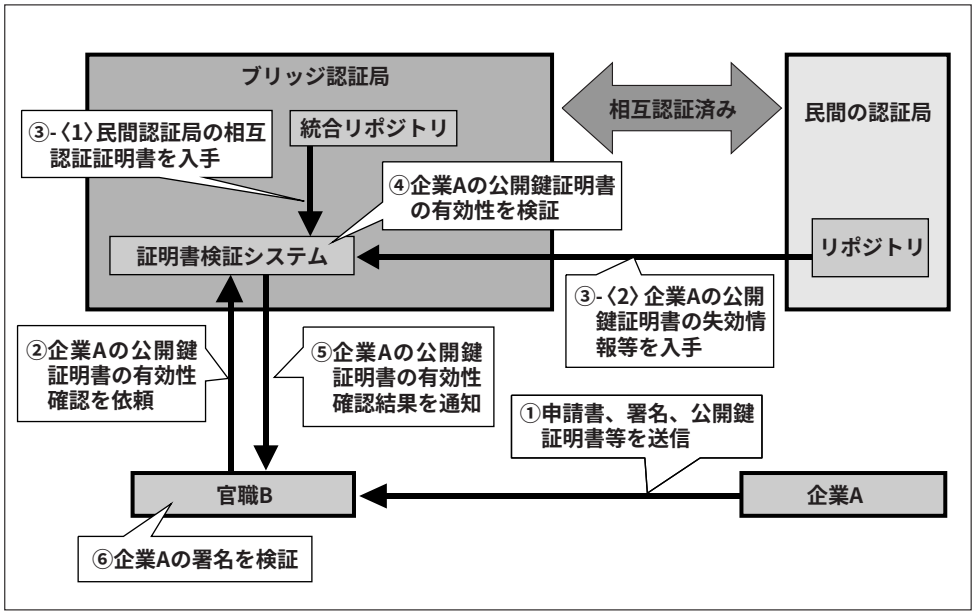


ジトリ等に格納される情報をLDAPによって吸い上げて管理）、④証明書検証システム（統合リポジトリ等から情報を入手し、要求された公開鍵証明書の有効性確認を実行）から構成される。証明書検証システムは、公務員側からの公開鍵証明書の有効性確認要求に対し、統合リポジトリの情報を用いて公開鍵証明書の有効性を確認するサービスを提供する[17]。これにより、公務員側では、民間企業等の公開鍵証明書やデジタル署名の検証処理の負担を軽減できる。また、民間企業側では、申請結果の通知や交付等とともに送信される官職証明書やデジタル署名の検証を行う際に、各種証明書やその失効情報を統合リポジトリから一括入手できる。

例えば、官職Bの公務員が民間企業Aの本人確認と申請データの一貫性を確認する場合について、その手順を説明すると次のとおりである（図18参照）。

17　ブリッジ認証局の証明書検証システムでは、現在IETFにおいてSCVPの評価が十分定まっていないことから、証明書検証要求とその応答のプロトコルとしてSCVPを採用せず、OCSPのプロトコルをベースとした独自方式を採用することとしている（総務省［2001a］）。

図18　GPKIにおける電子申請時の申請書の認証手順（例）



〈GPKIにおける電子認証の手順〉

① 企業Aは、申請書に自分のデジタル署名と公開鍵証明書を添付して官職Bの公務員にインターネット経由で送信する。

② 官職Bの公務員は、ブリッジ認証局に対して企業Aの公開鍵証明書の有効性確認を依頼する（プロトコルはOCSPをベースとする独自方式）。

③ ブリッジ認証局の証明書検証システムは、〈1〉企業Aに公開鍵証明書を発行した民間認証局の相互認証証明書を統合リポジトリから入手するほか、〈2〉民間認証局のリポジトリから企業Aの公開鍵証明書の失効情報等を入手する。

④ 証明書検証システムは、企業Aの公開鍵証明書の有効性を確認する。

⑤ 証明書検証システムは、企業Aの公開鍵証明書の有効性に関する確認結果を官職Bの公務員に通知する。

⑥ 官職Bの公務員は、企業Aの公開鍵証明書が有効であるとの回答をブリッジ認証局から入手したら、企業Aの公開鍵を用いて企業Aのデジタル署名を検証し、申請書の一貫性を確認する。

GPKIにおける証明書ポリシーと認証実施規程については、ブリッジ認証局、経済産業省認証局、国土交通省認証局が両者を1つにまとめた文書をCP/CPSとしてそれぞれ作成・公表している（総務省［2001c］、経済産業省［2001］、国土交通省［2001］）。いずれもIETF PKIXで作成されたRFC 2527に準拠している。これらの内容に関して認証機関の鍵管理、公開鍵証明書の失効情報の管理、セキュリティ監査を中心に、主な特徴点を整理すると次のとおり（表6参照）。

秘密鍵の管理に関しては、経済産業省認証局と国土交通省認証局ともに、官職証明書に対応する秘密鍵は各認証局にてソフトウエアで生成された後、FIPS 140-1のレベル2相当のICカードによって格納・配布されるほか、ブリッジ認証局と府省認証局の秘密鍵はFIPS 140-1のレベル3相当以上のハードウエア・モジュール内で生成・保管することとされている。デジタル署名の生成・検証についてはRSA署名方式を採用し、官職証明書に対応する鍵のサイズは1,024 bit、認証局の鍵のサイズは2,048 bitとされている。また、認証局の秘密鍵は、複数の管理者が協力しないと利用不可能な形態で管理され、モジュールを物理的に破壊することによって廃棄される形態となっている。認証局の秘密鍵が危殆化した場合には、直ちに認証業務を停

表6　ブリッジ認証局・府省認証局CP/CPSの主な項目と内容

項目	ブリッジ認証局CP/CPS	経済産業省認証局 運用管理規程	国土交通省 認証局CP/CPS
公開鍵証明書と有効期限	相互認証証明書：5年	・相互認証証明書：10年 ・下位CA証明書：10年 ・官職証明書：3年	・相互認証証明書：5年 ・官職証明書：3年
セキュリティ監査	認証局と利害関係のない監査人を選定し、CP/CPSに準拠した運営が行われているか等を監査（年1回の定期監査のほか、適宜監査を実施する場合もある）		
運用環境	・CRL/ARL：24時間ごとに更新し、秘密鍵危殆時は直ちに更新（LDAPによって統合リポジトリに反映） ・各種ログ：3年保管 ・アーカイブ・データ：30年保管 ・認証局の鍵ペア：5年更新 ・秘密鍵危殆時：その秘密鍵による署名が含まれるすべての証明書を直ちに失効させ、再発行	・CRL/ARL：24時間ごとに更新し、秘密鍵危殆時には直ちに更新（LDAPによって統合リポジトリに反映） ・各種ログ：3年保管 ・アーカイブ・データ：30年保管 ・鍵ペア：5年更新 ・認証局の秘密鍵危殆時：その秘密鍵による署名が含まれる証明書を直ちに失効させ、再発行	
ログ管理	各種ログを記録し、不正操作等異常な事象を確認するためにその内容の調査を行う		
鍵管理	・鍵ペアの生成・保管：FIPS 140-1レベル3相当のハードウエア・モジュールにおいて実施 ・鍵サイズ：RSA署名方式・2,048 bit ・秘密鍵の使用：操作は複数の管理人によって行われ、秘密鍵は複数の管理者の管理鍵によって利用可能な状態とされる ・秘密鍵のバックアップ：鍵を暗号化したうえで分割管理 ・秘密鍵の廃棄：ハードウエア・モジュールの破壊によって実施 ・鍵ペアの有効期間：10年	・CA鍵の生成・保管：FIPS 140-1レベル3相当のハードウエア・モジュールによる ・官職用鍵の生成・保管：各認証局がソフトウエアで生成し、FIPS140-1レベル2相当のICカードで保管 ・CA鍵サイズ：RSA署名方式・2,048 bit ・官職用鍵サイズ：RSA署名方式・1,024 bit ・CA秘密鍵の使用：操作は複数の管理人によって行われ、秘密鍵は複数の管理者の管理鍵によって利用可能な状態とされる ・CA秘密鍵のバックアップ：鍵を暗号化したうえで分割管理 ・CA秘密鍵の廃棄：ハードウエア・モジュールの破壊によって実施 ・鍵ペアの有効期間：10年	
証明書とCRL/ARL	・各種証明書のデータ形式：X509バージョン3 ・CRL/ARLのプロファイル：X509バージョン2		

止して秘密鍵を廃棄し、その鍵で生成された各種証明書をすべて失効させたうえで、改めて新しい秘密鍵を生成し、公開鍵証明書の再発行を行うとされている。

公開鍵証明書の失効情報の管理に関しては、CRLとARLを管理することとし、府省認証局、ブリッジ認証局ともに24時間ごとに更新を行うとともに、LDAPを用いて統合リポジトリに集約することとされている。認証局の秘密鍵が危殆化した場合には直ちに自己署名証明書や相互認証証明書を失効させたうえでARLに反映し、公開鍵証明書の再発行を行うこととされている。

認証局のセキュリティ監査については、各認証局と利害関係を持たない監査人を指名し、年1回の定期監査等を実施して監査報告書を作成するほか、各種ログを記録して不正行為等が行われていないか否かをチェックすることとされている。

（7）米国連邦政府のFPKI

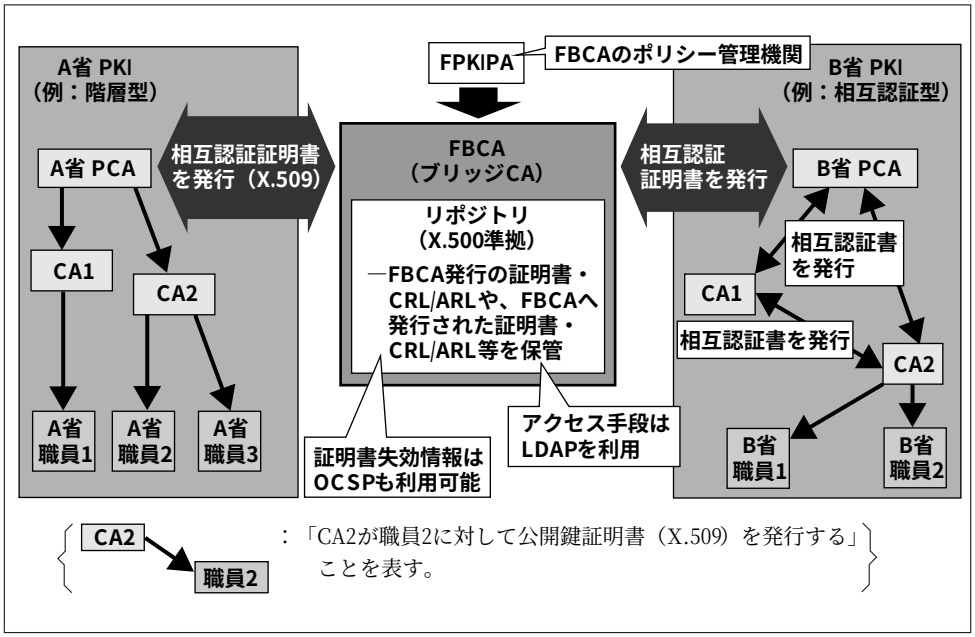
FPKIは、政府機関間、および、政府機関と民間企業・個人間において、公開鍵暗号方式による暗号通信やデジタル署名等の利用を実現するために、米国連邦政府機関の各PKIを相互に接続し、政府部門全体をカバーするPKIである。米国政府がFPKIを進める背景の1つとして、2000年10月に施行されたGPEA（Government Paperwork Elimination Act）が挙げられる。GPEAは、米国政府が民間企業・個人から電子申請・届出を受理する体制を2003年10月までに整備することを要求している。

FPKIの検討の焦点は、各政府機関のPKI間における相互運用性をどのようにして確保するかという点にある。米国政府内でも国防総省や商務省等一部の政府機関において既に独自のPKIが実装されており、それらのPKIの仕様になるべく変更を加えない方法で各政府機関のPKIを相互に運用できるようにすることが課題となっている。その解決策として、ブリッジCA（FBCA：Federal Bridge Certification Authority）を設置して各政府機関のPKIを相互接続させる方法が採用されており、FPKIの信頼構造はハイブリッド型となっている。

FBCAと相互認証を行う認証機関（APCA：Agency Principal Certification Authority）は、各PKIにおけるルートCAやブリッジCAが候補となり、FBCAのポリシー管理機関に相当するFPKIPA（FPKI Policy Authority）の認可によって相互認証が実施されるという体制となっている（図19参照）。FPKIPAはFBCAの証明書ポリシー（FPKIPA［2000b］）等をインターネット上に公開しており（例えばBurr［1998］）、各政府機関のCAはそれらを参考にしてFBCAと相互認証を行う体制の整備を進めている。2000年には複数の政府機関CAと民間企業CAが参加してFPKIのプロトタイプの実装実験が行われており、複数の政府機関のPKIをまたがる認証パスの検証やCRL/ARLの入手可能性等、主に相互運用性の観点から検証が行われた。なお、その結果をまとめたレポートも公表されている（FPKIPA［2000a］）。

FBCAの証明書ポリシーによると、FBCAは、各APCAに対して相互認証証明書を発行するほか、CRL/ARLを作成してX.500準拠のデータベース構造を有するリポジ

図19　FPKIの枠組み



トリに格納する。リポジトリへのアクセスにはLDAPが採用されるほか、証明書失効情報を配布する際にはOCSPの利用も可能にしている。デジタル署名を検証する際には認証パスを辿る必要があるが、FPKIでは、認証パス検証に必要な公開鍵証明書、相互認証証明書、失効情報等を検索・入手する仕組みとして、FBCAのリポジトリのディレクトリと各政府機関のリポジトリのディレクトリとを連鎖（chaining）させるという方法を採用している。例えば、検証者がFBCAのリポジトリに対して認証パス検証に必要なデータを要求すると、FBCAのリポジトリから他の認証機関のリポジトリに対してもデータ検索の実行が要求される。この結果、検証者は、各リポジトリに個別にアクセスする場合に比べて効率よくデータを検索で

表7　4つの管理レベルと想定される利用環境

管理レベル	利用環境
初歩 （rudimentary）	不正行為が発生する可能性が非常に低いと考えられる環境を想定 ―本管理手段は、通信データの一貫性確保のためのアプリケーションにのみ適用可能、本人確認やデータ守秘目的には適用不可能
基本 （basic）	利用者が不正行為を行う可能性が低く、その他のエンティティによる不正行為（例えば秘密情報への不正アクセス）が発生したとしても重大な被害にはつながらないと考えられる環境を想定
中位 （medium）	機密情報への不正アクセスが発生する可能性を無視できないほか、ある程度の金銭的被害を伴う不正行為が発生する可能性のある環境を想定
上位 （high）	機密情報への不正アクセスが発生する可能性が高く、大きな金銭的被害を伴う不正行為が発生する可能性が高い環境を想定

きるとされている。

FPKIの情報セキュリティ対策に関しては、個々の政府機関が公開鍵証明書を発行する環境がそれぞれ異なることから、4つの利用環境が想定されている点が特徴である。各利用環境に対して、初歩（rudimentary）、基本（basic）、中位（medium）、上位（high）という異なるレベルの管理手段がそれぞれ準備されている（表7参照）。これらの基準の定義はやや曖昧であるが、各政府機関の認証機関がFBCAと相互認証を行う際に、両者の間でどの管理レベルが適当かについて検討が行われ、4つの管理レベルのいずれかが選択される。こうした手法によって、FPKIに参加する各政府機関のPKIの管理レベルが統合化される。なお、FBCAの管理レベルは、すべての管理レベルに対応可能となるように上位の管理レベルが適用される。

FBCAの証明書ポリシーでは、FBCA自身、および、FBCAと相互認証を行うAPCAの責務、業務内容、各種管理方法が4つの管理レベルに分けて記述されている。監査・ログ管理、新規登録、鍵管理、証明書管理といった情報セキュリティ管理項目をみると、各レベルによって管理方法が細かく設定されている（次頁表8参照）。まず、認証機関の秘密鍵の管理に関しては、鍵の生成および保管を行うモジュールについて、各管理レベルに対してそれぞれ異なるFIPS 140-1のレベルが適用され、上位レベルに対応するFBCAはFIPS 140-1のレベル3相当のハードウエア・モジュールを採用することとされている。デジタル署名の生成・検証はいずれの管理レベルもFIPS 186規定のRSA署名方式もしくはDSAを利用することとされており、鍵長は1,024 bit以上に設定されている。秘密鍵の利用に関しては、暗号技術による論理的な保護対策と物理的な保護対策と組み合わせるほか、秘密鍵を利用可能にするデータには管理者の身体的特徴によるデータ（バイオメトリック・データ）等の利用が望ましいとされている。

認証機関の秘密鍵が危殆化した場合の対応に関しては、まずその秘密鍵を直ちに失効させCRL/ARLに反映したうえで、新しい秘密鍵を生成し、その鍵を用いて公開鍵証明書を再発行する。さらに、秘密鍵が危殆化した原因等について調査し、FPKIPAに報告しなければならないこととされている。

公開鍵証明書の失効情報の管理に関しては、失効の申請を受理して実際に失効処理が完了するまでの時間が細かく設定され、基本、中位、上位の各管理レベルに対してそれぞれ6時間以内、2時間以内、30分以内とされている。CRLやARLの更新頻度についても、認証機関の秘密鍵が危殆化した場合、中位、上位においてそれぞれ18時間以内、6時間以内とされている。

セキュリティ監査については、基本、中位、上位の管理レベルに対応する認証機関の場合、民間の監査人を指名する、または、監査対象の認証機関とは独立した別の組織（例えば、行政監査局）の監査人を指名することが規定されており、第三者機関による監査の実施を意識した内容となっている。

表8　FPKIの認証機関における各管理レベルの差（FPKIPA［2000b］）

項目		利用環境に応じた認証機関の管理レベル			
		初歩	基本	中位	上位（FBCAが対応）
セキュリティ監査・ログ管理	監査人	（監査不要）	セキュリティ監査に精通し、FPKIの構造に深い理解がある監査人であり、民間部門、または、偏った監査の防止のために監査対象の政府機関とは独立した別の組織（例えば行政監査局）の監査人であること。		
	監査頻度		2年に1度以上	1年に1度以上 ―FBCAやAPCAは、相互認証先や下位の認証機関に対して監査の実施を要求可能。	
	ログの主な内容	鍵ペアの生成記録、秘密鍵のロード記録、公開鍵証明書の発行申請・失効申請の審査記録、利用者・操作者管理記録等 ―基本・中位・上位のみ：ログの削除・変更記録、本人確認結果、セキュリティ関連データ入力・出力記録、ハードウエア暗号モジュール管理記録、システム変更記録等			
	ログ調査頻度	問題発生時		2ヵ月に1度以上	1ヵ月に1度以上
	アーカイブ・データ	FBCAやCAの承認記録、CPS、契約書、システム仕様書、システム構成変更記録、公開鍵証明書発行申請記録、公開鍵証明書、ログ ―基本・中位・上位のみ：公開鍵証明書失効記録・申請者本人確認資料、公開鍵証明書・暗号トークン受領書、ARL/CRL、監査用資料			
新規登録	申請者の本人確認方法	メールアドレスで登録	申請者がRA等に出向き、信頼できる情報との照合や信頼できる人物の証言によって確認	申請者がRA等に出向き、提出情報を法令に則って確認、また、政府発行の写真付IDカード等を用いて本人を確認	申請者がRAに出向き、提出情報を法令に則って確認、また、政府発行の写真付IDカード等を用いて確認
鍵管理	鍵有効期間	5年		3年	
	鍵の生成・保管用のモジュール	FIPS140-1レベル1	FIPS140-1レベル2	FIPS140-1レベル2（ハードウエアに限定）	FIPS140-1レベル3（ハードウエアに限定）
	署名方式	RSA署名方式もしくはDSA（FIPS 186に規定される方式）			
	鍵長	1,024 bit以上			
	秘密鍵利用データ	暗号による保護と物理的な保護の組合せを利用。バイオメトリック・データ等が望ましい。また、誤入力の回数によって秘密鍵の利用を不可能にするメカニズムも組み込むことが望ましい。			
証明書管理	証明書有効期間	10年		6年	
	失効申請から失効処理までの時間	設定不要	6時間以内	2時間以内	30分以内
	CRL/ARL更新頻度	設定不要	通常時は認証機関が個別に設定、秘密鍵危殆時は24時間以内	通常時は24時間以内、秘密鍵危殆時は18時間以内	通常時は24時間以内、秘密鍵危殆時は6時間以内（PCAの場合は直ちに更新）

（8）各PKIの情報セキュリティ対策の整理

これまでみてきた各PKIの情報セキュリティ対策を、主な項目ごとに改めて整理すると、以下のとおり（表9参照）。

証明書ポリシーと認証実施規程の作成・公表に関しては、アイデントラスのPKIにおいては銀行CAの証明書ポリシーは公表されているが、認証実施規程は非公表となっている。GPKIにおいては証明書ポリシーと認証実施規程を一体化させた文書が公表されている。FPKIではブリッジCAの証明書ポリシーが公表されている。全銀協のPKIでは証明書ポリシー等の作成・公表については検討中とされている。スイフトのPKIにおいては、PKIの構造に関する資料のみが公表されている。

秘密鍵の管理に関しては、認証機関の秘密鍵はFIPS 140-1レベル3以上に相当するハードウエア、公開鍵所有者の秘密鍵はICカードやFIPS 140-1レベル2相当のハードウエアに保管するとされているPKIが多い。また、GPKIやFPKIでは、認証機関の秘密鍵の使用時において秘密分散技術が採用されている。秘密鍵の危殆時の対応については、GPKIとFPKI以外のPKIでは具体的な対応が明らかとされていない。

デジタル署名の生成・検証に関しては、スイフトとTEDIのPKI、GPKI、FPKIにおいては、RSA署名方式が採用されており、FPKIではRSA署名方式とDSAの利用が可能とされている。ただし、RSA署名方式の具体的な利用方法はいずれのPKIでも明らかとされていない。鍵長については、スイフトとTEDIのPKI、GPKIにおいては、認証機関用の鍵が2,048 bit、公開鍵所有者用の鍵が1,024 bitに設定されている。FPKIのブリッジCAでは、鍵長が1,024 bit以上に設定されている。

公開鍵証明書の失効情報の管理については、アイデントラス、スイフト、TEDIのPKI、FPKIにおいてはCRLやOCSPが利用されている。全銀協のPKIでは、全銀協認証局が問合せに応じて失効情報を提供する仕組みとなっている。また、アイデントラスのPKIとGPKIでは、公開鍵証明書の有効性確認を認証機関が行う形態となっている。

認証機関のセキュリティ監査やログ管理に関しては、TEDIのPKI、GPKI、FPKIの公表資料では、監査人や監査の頻度等が記述されている。このうち、GPKIでは、監査対象となる認証局と利害関係のない監査人を選定することが定められており、FPKIでは、監査対象の機関とは独立の組織に属する監査人を選定することとされている。その他のPKIでは、セキュリティ監査等に関する情報は公表されていない。

なお、全銀協のPKIにおいては、電子署名法に基づく特定認証業務の認定指針に沿って認証機関のセキュリティ対策が講じられている。

こうしてみると、現状、金融機関等が参画して構築を進めているPKIにおいては、情報セキュリティ対策に関する公開情報が限定的なものにとどまっているように窺われる。特に、秘密鍵危殆時の対応やセキュリティ監査に関する情報は、ほとんど公開されていない。

表9　各PKIにおける鍵管理・公開鍵証明書失効情報管理・セキュリティ監査

金融機関・団体	証明書ポリシー等の作成・公開	秘密鍵の生成・保管・使用・廃棄	秘密鍵の危殆時の対応	デジタル署名方式と鍵長	公開鍵証明書の失効情報の管理	認証機関のセキュリティ監査・ログ管理
全銀協	いずれも検討中	＜秘密鍵生成・保管＞ ・全銀協認証局用：FIPS 140-1レベル4相当のハードウエアで保管 ・ICキャッシュカード・ATM端末用：銀行認証局が生成、保管	・全銀協認証局：電子署名法に基づく特定認証業務の認定指針に沿って対策が講じられている ・銀行認証局：全銀協が定める認証局運営規則に沿って対策が講じられている			
アイデントラス	銀行CAの証明書ポリシーのみ公表、他の証明書ポリシーや認証実施規程は非公表の扱い	＜契約企業用の秘密鍵の生成・保管＞ 銀行CAがFIPS 140-1レベル2相当のハードウエア内で生成し、暗号化したうえでFIPS 140-1レベル2相当のICカード等に保管 ＜契約企業用の秘密鍵の使用＞ 秘密鍵を使用する際にはPINによる本人確認を実施し、PINは秘密鍵を格納したハードウエアとは別の手段によって契約企業に配送	銀行CAの証明書ポリシーには記載されていない		公開鍵証明書の有効性確認は銀行CAが実施し、銀行CA間における失効情報の配信にはOCSPを利用	銀行CAの証明書ポリシーには記載されていない
スイフト	現時点ではいずれも公表されていない	＜金融機関用の秘密鍵の生成・保管＞ 暗号化用、署名用をそれぞれスイフトの認証機関とSNLが生成し、ICカードに保管 ＜スイフトの認証機関用秘密鍵の生成・保管＞ 暗号化用、署名用いずれもFIPS 140-1レベル3相当のハードウエア内で生成・保管	公表資料には記載されていない	RSA署名方式 ・スイフト：2,048 bit ・金融機関：1,024 bit	CRL（X.509バージョン2）を利用	公表資料には掲載されていない
TEDI	独自の認証機関を設置せず、認証機関のガイドラインを公表	＜秘密鍵の生成・保管＞ ハードウエア・モジュール内での生成・保管を推奨 ＜秘密鍵の使用＞ 秘密鍵を利用するために必要な情報の分散管理を推奨	ガイドラインには記載されていない	RSA署名方式 ・認証機関：2,048 bit ・登録企業：1,024 bit	CRLやOCSPの利用を推奨	ログの一貫性を確保するための対策（デジタル署名付与等）の実施を推奨
日本政府（GPKI）	CPとCPSを一体化した文書を公表済み	＜秘密鍵の生成・保管＞ ・ブリッジ認証局用、府省認証局用：FIPS 140-1レベル3相当のハードウエア内で生成・保管 ・官職用：府省認証局がソフトウエアで生成し、FIPS 140-2レベル2相当のICカードに格納・保管 ＜ブリッジ認証局・府省認証局の秘密鍵の使用・廃棄・バックアップ＞ 複数の管理者がそれぞれ管理鍵を持ち寄り、それらによって秘密鍵を使用可能にするほか、秘密鍵の廃棄はハードウエアの破壊によって実行し、秘密鍵のバックアップは暗号化および分割によって実施	危殆化した秘密鍵を直ちに失効させ、CRLやARLに反映し、新しい鍵ペアを生成して公開鍵証明書を再発行	RSA署名方式 ・ブリッジ認証局：2,048 bit（有効期間10年） ・府省認証局：2,048 bit（有効期間10年） ・官職用：1,024 bit	公開鍵証明書の有効性確認はブリッジ認証局の統合リポジトリにおいてOCSPを参考に開発された独自のプロトコルによって実行	各認証局と利害関係のない監査人を選定し、年1回の定期監査を実施するほか、各種ログの調査も適宜実施
米国政府（FPKI）	＜ブリッジCA＞ CPは公表済み、CPSについては不明	＜ブリッジCAの秘密鍵の生成・保管＞ FIPS 140-1レベル3相当のハードウエア内で生成・保管 ＜ブリッジCAの秘密鍵の使用＞ 秘密鍵を利用する際に必要とされるデータには管理者のバイオメトリック・データ等を利用するほか、そのデータは暗号技術による保護手段（暗号化や秘密分散等）と物理的な保護手段（耐タンパー・ハードウエア等）を組み合わせて保護	30分以内に秘密鍵を失効させ、6時間以内にARLに反映し、鍵ペアを生成して公開鍵証明書を再発行	RSA署名方式、DSA ・1,024 bit以上（有効期間3年）	CRLとOCSPを利用し、公開鍵証明書の有効性確認に必要なデータは、各CAのディレクトリの連鎖によって検索・入手	監査人は監査対象の機関とは独立した組織に属し、監査頻度は年1回以上とするほか、各種ログ調査は1ヵ月に1回以上の頻度で実施

4．PKIにおける今後の課題と対応策

(1) 課題と対応策

金融機関が認証業務に取り組むことについては、金融機関、とりわけ銀行は認証機関として認証業務を行うのに比較的適したポジションにいるとの見方が多い（American Banker［2001］、谷口［2000］）。銀行は、企業や個人の預金口座等、他者の重要な情報を管理する主体として長年機能しているという実績をもっていることに加え、与信業務等において取引相手の審査を行っており、認証機関の業務をそれらの延長線上に捉えることができるためである。また、認証機関は利用者からその業務・運用管理に関して信頼される必要があるが、銀行は一般的に「信頼できる組織」として認識されてきていると考えられる。

しかし、金融機関が認証機関として認証業務を行う際に必要とされるセキュリティ技術は、金融機関が従来利用してきた大型コンピュータによるメインフレーム・システム等におけるセキュリティ技術とは異なるものが少なくない。金融業務で従来利用されてきたメインフレーム・システムやクローズドなネットワークでは、堅固なコンピュータ・センターの構築や、システム制御室等への入退室管理等、物理的なセキュリティ対策が中心であった。これに対してPKIでは、物理的な対策のみならず、オープンなネットワークを前提としたセキュリティ対策が必要とされる。例えば、証明書発行申請時等に用いられるバイオメトリック認証等の本人確認技術、デジタル署名に利用される公開鍵暗号技術、公開鍵証明書等をインターネット上で提供する場合にリポジトリのシステムへの不正侵入等を防止するネットワーク・セキュリティ技術等である。

また、3節においてみてきたように、現状、金融機関等が参画して構築を進めているPKIにおいては、情報セキュリティ対策に関する情報が必ずしも十分には公開されていないように思われる。こうした状況においては、PKIを利用したいと考えている者にとって、認証機関やPKIの情報セキュリティについて独自に評価を行い、そのPKIのサービスが自己の要求するセキュリティ要件に合致しているか否かを判断することが困難である可能性がある。

こうした現状を踏まえると、金融機関が認証機関としてPKIの運営に参画するに際しては、認証業務に必要な情報セキュリティ対策を適切に講じたうえで、これを利用者に効果的に示していくことが最も重要な課題であると考えられる。

こうした課題への対策については、①PKIシステム構築時の対策、②PKIサービス開始後の対策に分けて考えることができよう。

まず、上記①に関しては、PKIシステム構築時に、定評ある情報セキュリティ技術を適切に採用し、その内容を証明書ポリシー・認証実施規程等に反映したうえで、セキュリティを損なわない範囲でそれらの文書の内容を開示することや、情報セキュリティ技術の選択に当たり第三者機関によるセキュリティ評価の結果を活用しその旨を開示すること等が考えられる。

また、上記②については、まず、PKIサービス開始後に、認証業務の運用・管理体制に関するセキュリティ監査の実施や第三者機関によるセキュリティ認定の取得等によって、認証機関のセキュリティ対策を一層実効的なものにすることが考えられる。さらに、これに加えて、こうしたセキュリティ監査の方法や結果を開示していくことも考えられよう。

以下では、これらの対応策について、最近の標準化動向や技術研究動向を踏まえ、具体的に説明する。

（2）情報セキュリティ技術の適切な選択と開示

イ．情報セキュリティ技術の適切な選択

認証業務に利用するセキュリティ技術やその管理方法については、専門家から一定の評価を得たものを採用することが重要である。暗号技術をはじめとする情報セキュリティ技術は高度な情報技術や数学理論等に基づくものが多く、情報システムのセキュリティを評価するためには、専門的な知識や経験が必要とされる。また、ある情報セキュリティ技術が「致命的な欠陥がなく、実際に利用可能である」と広く認められるためには、その技術が公開され、多くの研究者による評価に耐え得ることが求められる。例えば、公開鍵暗号方式の「事実上の標準」といわれているRSA暗号／署名方式は、提案後20年以上もの間に数多くの研究者の研究対象とされ、それらの研究成果によってRSA暗号／署名方式を安全に実装するために必要な事項が次第に明らかにされてきた経緯がある。このように、多くの研究の積み重ねを経て、専門家による十分な評価が行われている技術を活用することが、安全性の観点から望ましいといえる。

具体的にどのような技術を選択するかを検討するに当たっては、ISOやITU-T等の国際標準、ANSI等の各国国内標準、IETF等の技術標準等が参考になる。特に、金融分野における証明書ポリシー・認証実施規程に関する米国国内標準ANS X 9.79-1のAnnex B（Certification Authority Control Objectives）には、「認証機関が検討すべき最低限の管理項目」が規定されており、検討を行うべき項目のほか、各項目を検討する際に参照することができる各種標準が紹介されている（表10参照）。

例えば、鍵の生成・保管・復元に関しては、鍵生成用暗号モジュールの選択、鍵長等のパラメータの設定等について検討すべきであるとされており、参考になる国際標準としてISO/DIS 15782-1のほか、金融分野で利用される暗号鍵の管理に関する国際標準ISO 11568-5（Key life cycle for public key cryptosystems、ISO/IEC［1998b］）や米国連邦政府標準FIPS 140-1が挙げられている。また、ログ管理の項目では、ログを作成する業務範囲の設定、ログの管理形態・検査内容・頻度、ログの検査者の選定等について検討すべきであると規定されており、その際に参考となる指針として、情報セキュリティ管理に関する英国の国内標準BS 7799-1（BSI［1999］）[18]、国

18 BS 7799-1は、2000年にISO/IEC 17799（ISO/IEC［2000］）として国際標準化されている。

表10　認証機関が検討すべき主な項目と各種標準（ANS X9.79-1 Annex B）

分野	検討すべき主な項目	紹介されている標準
手続的・物理的管理	証明書ポリシー・認証実施規程の管理	RFC 2527
	セキュリティ管理	BS 7799-1
	資産の分類と管理	
	人事管理	BS 7799-1、RFC 2527
	施設や機器の管理	
	運用管理	
	認証機関システムへのアクセス管理	
	システム開発・維持	
	監視・法律遵守	
	業務継続管理	BS 7799-1、 ISO/DIS 15782-1、RFC 2527
	ログ管理	
鍵管理	鍵生成	ISO/DIS 15782-1、ISO 11568-5、FIPS 140-1
	鍵の保管・復元・アーカイブ	
	認証機関の公開鍵の配布	ISO/DIS 15782-1、ISO 11568-5
	認証機関の鍵の利用	ISO 11568-5
	認証機関の鍵の廃棄	ISO 11568-5、RFC 2527
	ハードウエア・モジュールの管理	ISO/DIS 15782-1
公開鍵証明書管理	初期発行の申請	ISO/DIS 15782-1、 RFC 2527
	再発行の申請	
	公開鍵証明書の発行	X.509、 ISO/DIS 15782-1、RFC 2527
	公開鍵証明書の配布	ISO/DIS 15782-1
	公開鍵証明書の失効	ISO/DIS 15782-1、 RFC 2560

際標準ISO/DIS 15782-1、IETF PKIXの技術標準RFC 2527が挙げられている。

また、利用する情報セキュリティ技術を選択し、それらを基に証明書ポリシーや認証実施規程を作成する際には、採用する技術がどのような標準等に準拠しているのかを明確にすることも大切である。例えば、3節で紹介したPKIの大半がデジタル署名方式としてRSA署名方式を利用するとしているものの、RSA署名方式をどのように利用するのかに関しては鍵長を除いて明らかにされていない。RSA署名方式には、RSA-PSS署名方式、RSA-FDH署名方式、PKCS #1 Version 1.5をはじめとしてさまざまな利用方法が提案されており、利用方法によって安全性に差が生じる場合があることが知られている[19]。したがって、RSA署名方式の中でも利用方法によって

19 例えば、RSA-PSS署名方式といった場合でも、具体的なアルゴリズムについてはさまざまなバージョンが提案されている。RSA署名方式のさまざまな利用方法と安全性については宇根・岡本［2000］および齊藤［2002］を参照。

は、PKIのセキュリティ要件を満足することができない可能性も否定できない。このように、情報セキュリティ技術に複数の利用方法が存在し、それらの差異がセキュリティのレベルに影響を及ぼす可能性がある場合には、具体的な利用方法を含めて、準拠する標準等を明らかにしておくことが重要であると考えられる。

ロ．情報セキュリティ対策等の開示

以上の点を考慮して作成した証明書ポリシーや認証実施規程の内容は、PKIのセキュリティを損なわない範囲で開示することが、利用者をはじめとする外部からの信頼を得るうえで重要である。情報セキュリティ技術を利用したシステムの仕組みを適切に開示することは、PKIのサービス利用者の信頼向上に資するだけではなく、そのシステムのセキュリティを多くの専門家が評価するきっかけとなり、セキュリティ対策の有効性を高め、開発当初は気が付かなかったセキュリティ上の欠陥による被害を未然に防ぐ効果があるとの見方が多い（松本・岩下［1999］）。

情報セキュリティ対策に関する情報開示は不正行為の助長につながるとの見方もある。しかし、情報セキュリティ対策に関する情報を開示しない扱いとした場合でも、そのシステムに関わった技術者等は内部情報を知っているわけであり、セキュリティに関する情報が外部に漏洩する可能性は排除できない。ハイテク犯罪の多くに内部者が関与しているといった指摘も多い[20]。そうであれば、一部の内部者が不正を行おうとした場合であっても、それが有効な攻撃に結びつかないように予め対策を講じておくことが必要であり、情報セキュリティ対策の適切な開示は、むしろ、そうした問題への対策の1つにもなり得るものと考えられる。例えば、システム上に重大な欠陥が存在し、ある1人の関係者が他の関係者に気づかれないように不正行為を行うことが可能であったとしたら、関係者の1人がその事実に気づいた時点でシステムが重大な脅威に晒されることになる。これに対して、情報セキュリティ対策を適切に開示しておけば、専門家等による助言や評価を受けることを通じて、こうした問題を未然に防ぐ道が開かれるものと考えられる。

ハ．第三者機関によるセキュリティ評価・認定の活用

高い技術力を有する第三者機関が認証業務に利用される情報セキュリティ製品・システムの評価を実施しており、その評価に対する信頼が確立されている場合には、PKIのセキュリティ要件を勘案したうえで、そうした第三者機関から一定の評価を得ている製品・システムを採用し、その旨を開示することも有用と考えられる。

20 こうした指摘を行っている文献の1つとして、Anderson［2001］が挙げられる。本書では、これまでの各分野における情報セキュリティ対策の歴史や事例が紹介されており、内部者が関与して発生したセキュリティ侵害の事例も数多く記述されている。また、本書には、オープンな場でのセキュリティ侵害に関する議論や対策に向けた取り組みが各種のアプリケーションにおけるセキュリティ対策の高度化に大きく貢献してきた事例が多数掲載されている。

（イ）ISO/IEC 15408と最近の動向

欧米諸国で検討が進められてきたセキュリティ評価基準Common Criteriaは、1999年にISO/IEC 15408（Evaluation criteria for IT security、ISO/IEC［1999a］、［1999b］、［1999c］）として国際標準化された。ISO/IEC 15408は、ある業務を実行するためのハードウエア、ソフトウエア、アプリケーション・システム等のセキュリティ機能やその品質を、第三者機関が統一化された尺度によって評価・認定する際に用いられる。セキュリティ製品のベンダーは、製品が利用される分野のプロテクション・プロファイル[21]を参考にしてセキュリティ製品の設計仕様書（セキュリティ・ターゲットと呼ばれる）[22]を作成し、それに基づいて製品の製造を行った後、評価機関に対してその製品のセキュリティ評価を依頼する。評価依頼を受けた評価機関は、プロテクション・プロファイルやセキュリティ・ターゲット等を用いて製品の評価を行い、その結果を報告書として作成する。評価機関が行った評価結果の正当性は評価機関とは別の組織によって検証され、適正な評価であることが認められた場合、その製品にISO/IEC 15408に基づくセキュリティ認定が付与される。

ISO/IEC 15408の国際標準化に伴って、ISO/IEC 15408に基づく評価・認定体制を整備するための各種国際標準の検討も進められている。各種プロテクション・プロファイルの登録手続に関する国際標準ISO/IEC 15292（Protection profile registration procedures、ISO/IEC［2001］）の策定が完了し、プロテクション・プロファイルの登録局がISO/IEC JTC1[23]において設置されることとなった。また、ISO/IEC 15408に基づく評価手法CEM（Common Evaluation Methodology）に関する国際標準化がISO/WD 18045（Methodology for IT Security Evaluation）として進められているほか、プロテクション・プロファイルおよびセキュリティ・ターゲットの作成指針についてもISO/WD 15446（Guide for Production of Protection Profiles and Security Targets）として国際標準化が進められている。

わが国でも、ISO/IEC 15408に基づくセキュリティ評価・認定の実施に向けた検討が本格的に進められている。2000年にISO/IEC 15408の国内標準化（JIS化）が完了したほか、2001年4月からは、わが国政府が、ISO/IEC 15408に基づく評価・認定を受けたセキュリティ製品・システムの調達を行うための枠組みである「情報セキュリティ評価認証体制」の運用を開始している[24]。情報セキュリティ評価認証体制は、

21 プロテクション・プロファイル（protection profile）：ISO/IEC 15408に基づくセキュリティ評価の対象となる製品やシステムのセキュリティ要件等を特定用途向けに整理した文書。セキュリティ要件仕様書とも呼ばれ、評価対象となる製品・システムのユーザーが作成することが想定されている。プロテクション・プロファイルの形式はISO/IEC 15408-1に規定されている。

22 セキュリティ・ターゲット（security target）：ISO/IEC 15408に基づくセキュリティ評価の対象となる特定の製品やシステムの設計仕様書。セキュリティ製品・システムのベンダーが作成することが想定されている。セキュリティ設計仕様書とも呼ばれ、その形式がISO/IEC 15408-1に規定されている。

23 ISO/IEC JTC1（Joint Technical Committee 1）は、情報技術の国際標準化を担当する技術専門委員会であり、ISOとIECによって設立された。JTC1傘下には各種の下位委員会（SC：sub-committee）が存在し、情報セキュリティ技術（SC27が担当）をはじめとする各分野の標準化について審議している。

24 情報セキュリティ評価認証体制については、情報処理振興事業協会のウェブサイト（http://www.ipa.go.jp/security/ccj/index-j.html）に関連する情報が掲載されている。

政府から認定を受けた民間評価機関が、政府機関作成のプロテクション・プロファイルに準拠したとされるセキュリティ製品・システムの評価を行い、その評価プロセスが適正か否かを独立行政法人・製品評価技術基盤機構が認証する、というものである。現時点で評価・認証の対象とされているのは電子政府において利用される製品・システムであり、民間部門で利用される製品は直接の対象とはされていない。しかし、電子政府での利用を前提とした製品・システムの評価は、金融分野をはじめとする民間部門での利用を検討するに当たっても活用できる可能性がある。また、本制度を発展させる形で、民間部門でも利用可能なセキュリティ評価・認証制度が整備されていくことが予想されるため、今後の動向に注目していく必要があろう。

（ロ）金融分野向けプロテクション・プロファイルの評価

金融分野においてISO/IEC 15408に基づくセキュリティ評価を経た製品・システムを利用するためには、金融業務向けのプロテクション・プロファイルを作成することが必要である。こうした観点から、ICカード等セキュリティ製品に関する既存のプロテクション・プロファイルが金融分野において適用可能かどうかを評価するプロジェクトが、ISO/TC68/SC2/WG5[25]において進められている（宇根・中原［2000］）。これまでにICカード、ファイアウォール、ATMに関するプロテクション・プロファイルが評価の対象として提出され、それらの内容に関する検討が行われているほか、金融分野にISO/IEC 15408に基づくセキュリティ評価を導入した場合にどのような問題点があるかについても議論がなされている。これまでの議論の中では、特に、すべての評価機関がICカード等の評価を行う能力を有しているかどうかという点について問題提起がなされ、評価機関間のセキュリティ評価の整合性を確保する観点から、既に公知となっているセキュリティ上の脅威に関するデータベースを作成するよう、CCIMB[26]に対する働きかけが行われている。

（ハ）認証業務用システムのプロテクション・プロファイルの作成

この他注目される動きとして、米国政府（NIST、NSA）が進めている認証業務用システム向けプロテクション・プロファイルの策定プロジェクトが挙げられる。プロテクション・プロファイルの草案（Lee［2001］、2001年10月公表）が対象としている認証業務用システムは、ANS X9.79-1で定義されている4つの機能（登録機

25 ISO/TC68/SC2/WG5：ISO/TC68/SC2は、ISO/TC68の分科委員会であり、「セキュリティ管理と一般銀行業務」に関連する分野の標準化を担当している。ISO/TC68/SC2/WG5はその分科委員会の下に置かれた作業グループの1つである。本作業グループは、ISO/IEC 15408に基づいて作成されたICカード等のプロテクション・プロファイルが金融分野向けに利用できるかどうかを評価するプロジェクトを担当している。

26 CCIMB（Common Criteria Interpretation Management Board）：ISO/IEC 15408の基になっている評価基準Common Criteriaの解釈の統一化や規格のメンテナンスを行う国際的な委員会であり、1998年に設立された。オーストラリア、カナダ、フランス、ドイツ、英国、オランダ、米国のメンバーによって構成されている。

関、証明書発行機関、証明書生成機関、リポジトリ）を具備するシステムに概ね対応している。ただし、認証機関の秘密鍵を格納するハードウエア・モジュールやデジタル署名方式等のアルゴリズムについては本プロテクション・プロファイルの対象外とされている。

本プロテクション・プロファイルは金融分野を直接の対象としているわけではないものの、こうした検討の成果は、金融分野で利用される認証業務用システムの評価にも活用することができると考えられる。

（3）運用・管理体制の監査とその結果の開示

イ．セキュリティ監査とその結果の開示

各種標準規格等を参照して適切な情報セキュリティ対策を選択したとしても、適切な運用・管理がなされない場合、予期せぬセキュリティ上の問題が発生する可能性がある。認証業務を適切に運用・管理していくことは容易なことではない。このことを強く印象付ける最近の事例として、ベリサインが公開鍵証明書を誤発行した事例が挙げられる。その概要は以下のとおりである。

〈ベリサインの公開鍵証明書の誤発行事件〉

ベリサインは、2001年3月22日、マイクロソフトの社員を詐称した個人に対して同年1月29、30日に2通の公開鍵証明書（有効期限は1年）を誤って発行した事実を発表した（定期的に実施される監査によって発見されたと説明）[27]。ベリサインが誤って発行した公開鍵証明書は、ブラウザー上で動画を再生したり、ウェブサーバーと通信したりするためのプログラムをインターネット上でダウンロードする際に、プログラムの作成者確認や一貫性確認に用いられるものであった。このため、不正に公開鍵証明書を入手した攻撃者は、公開鍵証明書に含まれる公開鍵に対応する秘密鍵によって任意のプログラムに対して署名を生成し、そのプログラムの署名があたかもマイクロソフトが生成した正規の署名であるかのようにして第三者に配付する可能性がある。

ベリサインは誤発行された公開鍵証明書を失効させたほか、マイクロソフトは、同社の証明書が添付されたプログラム等の利用者に対して次の2つの対応方法を示した[28]。

27 本件については、2001年3月22日、ベリサインのウェブサイトにプレス・リリース“VeriSign Security Alert Fraud Detected in Authenticode Code Signing Certificates”が掲載された。

28 2001年3月29日、マイクロソフトのウェブサイト（http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd =MS01-017）に「VeriSign発行の誤ったデジタル証明書による、なりすましの危険性（MS01-017）」と題する技術情報が掲載された。

- **対応方法1**：プログラムに添付されている公開鍵証明書の有効期間を目視によって確認し、不正な証明書であるか否かを識別する。不正な証明書が発行された1月29日と30日にはベリサインからマイクロソフトに対して正当な証明書が発行されていなかったため、この両日から有効期間が開始する証明書が不正なものであることを検知可能である。
- **対応方法2**：誤発行の証明書が失効していることを示すCRLを含むアップデート・プログラムをインストールする。このアップデート・プログラムは、ダウンロードするプログラムに誤発行の証明書が添付されていた場合、証明書が失効していることを知らせる機能をもつ。

ベリサインの認証実施規程（CPS Version 1.2、VeriSign［1997］、［2001a］、［2001b］）には、今回問題となったタイプの公開鍵証明書を企業向けに発行（企業の職員名での申請を受付け）する場合の本人確認手続が規定されている。その手続は、①その企業が実在することを確認するために企業の名称や住所等を検証するほか、②申請者がその企業において公開鍵証明書の申請を行う権限を有する職員であることを確認するために、申請者の個人情報の提出を求め、その企業に電話をかけて申請者が正当な権限を有する職員であること等を検証するというものである。公開鍵証明書の誤発行は、こうした手続が適切に実行されなかった可能性を示唆している[29]。ベリサインは、これまでに金融分野をはじめとする幅広い分野において認証サービスを提供してきた実績をもち、認証機関として一定の評価を受けてきた企業である。こうしたベリサインにおいて公開鍵証明書の誤発行という問題が発生したという事実は、認証業務の適切な運用・管理を継続して行うことの難しさを物語っている。

こうした問題に対応する手段としては、セキュリティ監査の厳格な実施が考えられる。ベリサインの事例においても、定期的に実施されていた監査によって公開鍵証明書の誤発行が発見されたと発表されている。仮に、何らかのセキュリティ侵害が発生した際にセキュリティ監査が有効に機能していなかったとすると、認証機関およびPKIの信頼を大きく損なう事態につながる可能性がある。例えば、公開鍵証明書の誤発行という事態が判明しないまま時間が経過した場合、誤発行された公開鍵証明書を用いて正規のメーカーを装った不正プログラムが広く配布され、多くの利用者が重要なデータを破壊される等の損害を被ることにもなりかねない。このように、公開鍵証明書を管理する認証機関の運用・管理が公開鍵所有者や検証者に及ぼす影響は大きく、認証機関においては、セキュリティ対策が有効に機能しなかった場合の問題の発生を最大限回避する観点から、専門的なノウハウをもつ外部の第

29 誤発行の原因・背景については、ベリサインやマイクロソフトのウェブサイト上では明らかにされていない。

三者機関にセキュリティ監査の実施を依頼するといった対応が考えられる[30]。

さらに、こうしたセキュリティ監査の結果を開示することも、認証機関の運用・管理体制に対する利用者の信頼を向上させる手段として検討することが考えられる。「認証機関に対するセキュリティ監査を行った結果、証明書ポリシーや認証実施規程に沿った適切な運用が行われていたことを確認した」といった情報が開示されれば、利用者の認証機関に対する信頼は一層向上すると予想される。また、セキュリティ監査において問題点が発見された場合でも、適切な対応を実施したうえでその旨を公表すれば、認証機関に対する利用者の信頼を確保しうるものと考えられる。さらに、不適切な運用・管理がセキュリティ監査において発覚した場合にその事実が外部に公表されるということになれば、認証機関の職員や関係者に対して適切な行動を促すことにもなるものと考えられる。

ロ．第三者機関による認定の活用

セキュリティ監査を適切に実施し、その結果を開示するほかに、認証機関のセキュリティ対策の運用・管理について、公的機関や高度な専門性を有する第三者機関から評価・認定を受けることも考えられる。こうした制度として、わが国では、電子署名法に基づく特定認証業務の認定制度が開始されている。また、情報セキュリティ管理が予め定められた運用・管理の規程に沿った形で適切に実施されているか否かを第三者機関が検証し、認定を付与する制度として、情報セキュリティマネジメントシステム適合性評価制度の検討が進められている。

（イ）電子署名法に基づく特定認証業務の認定

特定認証業務の認定は、政府が認証機関からの申請に応じて認証サービスやその運用体制等を審査し、一定の基準を満足した認証サービスを「特定認証業務」として認定するものであり、認定期間は1年に設定されている。民間の認証機関が、3節で紹介したGPKIのブリッジ認証局と相互認証を行おうとする場合には、その認証機関の電子認証サービスについて特定認証業務の認定を受けることが必要とされている。この認定制度における実際の審査は、政府から指定調査機関として承認された日本品質保証機構が、特定認証業務の認定指針（平成13年総務省・法務省・経済産業省告示第二号）に沿って実施する仕組みとなっている（日本品質保証機構［2001］）。

特定認証業務の認定指針の項目は具体的かつ多岐に亘っており、認定を受けようとする認証機関は、各項目についてどのような対策が講じられているかを整理した

30 なお、セキュリティ監査を適切に実施するには、監査の対象となる各種ログ等のデータの一貫性を確保する必要もある。これに関連する技術として、「あるデータがいつ存在したか」を証明するタイムスタンプ技術や、「だれがどのデータをいつ所有していたのか」を証明する電子公証技術が提案されており、こうした技術の活用について検討することも有用であろう。タイムスタンプのサービスについては、現在、ISOにおいて標準化が進められているところである（宇根・松浦・田倉［2000］、Une［2001］を参照）。

文書を作成し、指定調査機関である日本品質保証機構に提出する。日本品質保証機構は、その提出書類の審査を行ったうえで、提出文書の内容に沿って認証業務の運用・管理が適正に実施されているか否かについて実地調査を行い、その結果を踏まえて認定するか否かを判定する[31]。

特定認証業務の認定指針の中で掲げられている情報セキュリティ対策に関連する項目を整理すると、表11のとおりである。これらの項目は、ANS X9.79-1や

表11　特定認証業務の認定指針における情報セキュリティ関連項目とその概要

項目	概要
電子署名方式	・RSA署名方式（鍵長1,024 bit以上） ・ESIGN（鍵長1,024 bit以上、検証時に利用されるベキ指数8以上） ・DSA（鍵長1,024 bit以上）、ECDSA（鍵長160 bit以上）
認証業務用設備	・業務の重要度に応じた認証業務用の**設備への入退室管理**（バイオメトリック認証、遠隔監視・映像記録装置、各種警報等）の実施 ・通信回線経由による**不正アクセスへの対策**（ファイアウォール、不正アクセス検知システム）の実施、通信内容の盗聴・改変防止措置の実施 ・**無権限者による不正利用防止策**（操作者の権限設定、権限の確認）の実施、**各種処理ログ**（操作要求者、操作内容、操作日時、結果等）の記録
認証機関による利用者用の鍵生成	・利用者に対する鍵ペアの安全かつ確実な送付 ・利用者用に生成した鍵ペアをその利用者に送付した後における、その鍵ペアの確実な消去
証明書の管理	・有効期間：5年を超えない期間 ・公開鍵証明書に記載する情報：発行者名、発行番号、発行日、有効期間満了日、利用者名、公開鍵、署名アルゴリズム識別子 ・発行者を確認する手段に関する情報の開示 ・利用者からの証明書失効請求に応じての**迅速な失効処理の実施**
失効情報の配信	・検証者に自動的に**証明書失効情報を配信する手段の提供** ・公開鍵証明書の**失効処理完了の利用者への迅速な通知**
認証業務の実施に関する規程	**認証業務の実施規程**（認証機関名称・連絡先、認証の目的・対象、認証機関の責任、利用申込方法、本人確認方法、失効請求方法、失効情報の確認方法、セキュリティ管理、帳簿書類の保管、業務停止時の対応等）**の開示** ―帳簿書類は、**①利用申込に関するもの**（利用申込書、利用者の本人確認用資料等）、**②証明書失効に関するもの**（失効請求、失効情報の作成・管理記録等）、**③認証機関の組織管理に関するもの**（規程、業務手順、組織体制記録、委託契約、監査記録）、**④設備や安全対策に関するもの**（入退室管理記録等）から構成される。
帳簿書類の保管	・利用申込、証明書失効、認証機関の組織管理に関するものは、公開鍵証明書の有効期間満了日から10年間保管しなければならない。 ・設備や安全対策に関する帳簿書類は、作成日から認定の更新の日（1年後）まで保存しなければならない。

31　2002年1月現在で特定認証業務の認定を受けている電子認証サービスは、日本認証サービスのAccredited Signパブリックサービス（日本認証サービス［2001］、2001年7月13日認定）とAccredited Signパブリックサービス2（2001年10月19日認定）、帝国データバンクの電子入札用電子認証サービス（帝国データバンク［2001］、2001年9月6日認定）、日本電子公証機構の認証サービスiPROVE（2001年12月14日認定）の4つである。

ISO/DIS 15782-1等と同様に、認証機関の情報セキュリティ対策を検討するうえでも有用であると考えられる。ちなみに、3節で紹介した全銀協のPKIでは、本認定指針に沿って認証機関のセキュリティ対策が講じられている。

（ロ）情報セキュリティマネジメントシステム適合性評価制度

認証機関に限定されるものではないが、情報システムのセキュリティ運用・管理体制を評価・認定する制度として、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）適合性評価制度の検討が進められている。本制度は、情報セキュリティ管理の英国国内標準BS 7799に基づく評価・認定制度をベースとして検討されているものである。

BS 7799による評価・認定制度においては、評価・認定を受けようとする企業が情報システムのセキュリティ管理に関する実施規程を作成し、第三者機関が書類審査および実地調査を実施して認定を付与するか否かを決定するという手順が採用されている[32]。BS 7799は、英国の国内標準ではあるが、欧州を中心に多くの国々において採用されている。また、2000年には、BS 7799のうち、認定制度の枠組みを除く評価基準の部分（BS7799-1）がISO/IEC 17799として国際標準化されている。

こうした中で、わが国でも、ISMS適合性評価制度委員会（事務局：日本情報処理開発協会）が2000年9月に設置され、ISMS適合性評価制度の本格的な検討が開始された。その後、2001年4月にはISMS適合性評価制度における評価基準（日本情報処理開発協会［2001a］）が公表されたほか、2001年9月には評価・認定制度のガイド（日本情報処理開発協会［2001b］）が公表された。公表されているガイド等によると、本制度における評価・認定のプロセスは、BS 7799のそれとほぼ同様となっている。また、2001年4月からは、評価・認定のパイロット事業が開始されている。パイロット事業における評価・認定の対象は、情報処理サービス事業者の情報システムに限定されているものの、今後は情報システムを有する一般事業者にも対象が拡大される見通しとなっている。

5．おわりに

本稿では、まず、最近の金融機関によるPKIへの取組みについて整理したうえで、金融機関が認証機関としてPKIのサービスを提供する際に今後留意すべき事項を指摘した。すなわち、適切な情報セキュリティ対策の確保と利用者の信頼の向上を図るために、①PKIシステム構築時においては、情報セキュリティ技術を適切に選択したうえでANS X9.79-1等を参考にしながら証明書ポリシー・認証実施規程を適切に作成し、セキュリティを損なわない範囲でそれらの内容を開示すること、および、

32 BS 7799に基づく情報セキュリティ管理の評価・認定の仕組みについては、宇根・中原［2000］を参照。また、最近のBS 7799等の動向については、金融情報システムセンター監査安全部［2001］を参照。

②PKIサービス開始後においては、認証業務が適正に運用・管理されていることを第三者によるセキュリティ監査等によって確認し、その結果を開示することが有効であることを説明した。

PKIが有効に機能するためには「信頼の連鎖」が不可欠であり、認証機関はその信頼の源である。認証機関が利用者からの信頼を得ることができなくなった場合、信頼の連鎖が断ち切られ、PKIが機能しなくなる可能性が高い。なぜなら、信頼を失った認証機関については、「秘密鍵が適正に管理されていないのではないか」、さらには、「その認証機関の秘密鍵によって生成されたデジタル署名は偽造されたものであるかもしれない」といった不信感が生まれ、その認証機関が発行した公開鍵証明書が意味をなさなくなるためである。

金融機関が認証機関としてPKIに取り組む際には、こうした点について十分に認識し、PKI関連技術の最新動向を十分フォローしながら情報セキュリティ対策を適切に講じていくことが重要であると考えられる。

参考文献

宇根正志・岡本龍明、「最近のデジタル署名における理論研究動向について」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年4月、55～104頁

――――・中原慎一、「最近の金融業務における情報セキュリティ評価・認定を巡る動向について」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年4月、193～238頁

――――・松浦幹太・田倉 昭、「デジタルタイムスタンプ技術の現状と課題」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年4月、105～153頁

金融情報システムセンター監査安全部、「英国における、BS 7799を中心とした情報セキュリティへの取組み動向」、『金融情報システム』No.252、金融情報システムセンター、2001年12月、92～107頁

経済産業省認証局運営委員会、『経済産業省認証局運用管理規程（CP/CPS）』、2001年7月（http://www.meti.go.jp/application/ninsho/cpcps130529.pdf）

国土交通省CAポリシ委員会、『政府認証基盤（GPKI）国土交通省認証局CP/CPS（証明書ポリシ／認証実施規程）』、2001年4月（http://www.goa.mlit.go.jp/ mlitca/mlitcp_cps.pdf）

小森 旭・松浦幹太・須藤 修、「PKIに基づくC/S型アプリケーションの安全性分析と証拠性評価」、『コンピュータセキュリティシンポジウム2001論文集』、情報処理学会シンポジウムシリーズ、Vol.2001、No.15、情報処理学会、2001年10月、319～324頁

齊藤真弓、「RSA署名方式の安全性を巡る研究動向について」、『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年6月、285～324頁（本号所収）

洲崎誠一・松本 勉、「電子署名の偽造に関する一考察」、『コンピュータセキュリティシンポジウム2001論文集』、情報処理学会シンポジウムシリーズ、Vol.2001、No.15、情報処理学会、2001年10月、211～216頁

――――・宮崎邦彦・宝木和夫・松本 勉、「暗号ブレイク対応電子署名アリバイ実現機構（その2）―詳細方式―」、『情報処理学会研究報告』、2000-CSEC-8、情報処理学会、2000年3月、18～23頁

全国銀行協会、「ICキャッシュカードに関する認定制度の創設および全銀協認証局の設置について」、『金融』2001年11月号、全国銀行協会、2001年11月、16～25頁

総務省行政管理局、『政府認証基盤（GPKI）相互運用性仕様書』、2001年4月a（http://www.gpki.go.jp/session/010514_2.pdf）

――――、『政府認証基盤（GPKI）府省認証局CP/CPSガイドライン』、2001年4月b（http://www.soumu.go.jp/gyoukan/kanri/010514_5.pdf）

――――、『政府認証基盤（GPKI）ブリッジ認証局CP/CPS』、2001年4月c（http://www.gpki.go.jp/cpcps/cpcps.pdf）

谷口文一、「金融業界におけるPKI・電子認証について ―」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年4月、15～54頁

TEDI Club、『貿易金融EDI（TEDI）実施ガイドライン』、2001年a

――――、『TEDI認証機関モデル運用規則』、2001年b

帝国データバンク、『電子入札用電子認証局運用規程 Ver.1』、2001年7月（http://www.tdb.co.jp/ca/CPSver1.pdf）

電子商取引実証推進協議会認証・公証ワーキンググループ、『認証局の責任に関する提言』、H11－認証・公証－3、2000年3月

日本情報処理開発協会、『ISMS・情報セキュリティマネジメントシステム適合性評価制度－ISMS認証基準（Ver.0.8）－』、2001年a

――――、『ISMSガイド（Ver.0.8）－パイロット審査に向けて－（基本編・事例編）』、2001年b

日本認証サービス、『AccreditedSign™ パブリックサービス標準規程（V1.0）』、2001年4月（http://www2.jcsinc.co.jp/repository2/A_SignCPSv1.0-ja.pdf）

日本品質保証機構電子署名・認証調査センター、「電子署名および認証業務に関する法律に基づく指定調査機関の調査について」、2001年12月（http:// www.jqa.or. jp/j/esaec/eval_f0.html）

松本 勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」、『金融研究』第18巻第2号、日本銀行金融研究所、1999年4月、17～32頁

――――・岩村 充・佐々木良一・松木 武、「暗号ブレイク対応電子署名アリバイ実現機構（その1）－コンセプトと概要－」、『情報処理学会研究報告』、2000-CSEC-8、情報処理学会、2000年3月、13～17頁

――――・田中直樹、「計算の実行ハードウェアを確認する方法」、『コンピュータセキュリティシンポジウム2000論文集』、情報処理学会シンポジウムシリーズ、Vol.2000、No.12、情報処理学会、2000年10月、199～204頁

Adams, Carlisle, Peter Sylvester, Michael Zolotarev, and Robert Zuccherato, *RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocol*, February 2001(http://www.ietf.org/rfc/rfc3029.txt).

American Banker, “VeriSign Security Breach Said Fixed; Banks Wary,” *American Banker*, April 2, 2001.

American National Standards Institute, American National Standard for Financial Services, *ANS X9.57: Public Key Cryptography For the Financial Industry: Certificate Management*, 1997.

――――, *ANS X9.79 Part 1: PKI Practices and Policy Framework*, 2001.

Anderson, Ross, “Two Remarks on Public-Key Cryptology,” Manuscript, 2000.

――――, *Security Engineering—A Guide to Building Dependable Distributed Systems*, Wiley Computer Publishing, John Wiley & Sons, Inc., 2001.

Bellare, Mihir, and Sara K. Miner, “A Forward-Secure Digital Signature Scheme,” *Proceedings of CRYPTO ’99*, LNCS 1666, Springer-Verlag, August 1999, pp. 431-448.

British Standard Institution, *BS 7799*: *Information Security Management, Part1: Code of Practice for Information Security Management Systems*, 1999.

Burr, William E., *Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations*, Working Draft TWG-98-59, September 1998(http://csrc.nist.gov/pki/).

Chokhani, Santosh, Warwick Ford, Randy Sabett, Charles Merrill, and Stephen Wu, *RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, July 2001(http://www.ietf.org/rfc/rfc2527.txt).

FPKI Policy Authority, *Report of Federal Bridge Certification Authority Initiative and Demonstration*, Draft 101500, August 2000a (http://csrc.nist.gov/pki/documents/emareport_ 20001015.pdf).

————, *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.12*, December 2000b.

Housley, Russell, Warwick Ford, Tim Polk, and David Solo, *Internet X.509 Public Key Infrastructure: Certificate and CRL Profile*, January 1999 (http://www.ietf.org/internet-drafts /draft-ietf-pkix-new-part1-09.txt).

Identrus, *Identity Certificate Policy, Operating Rules and System Documentation*, Release 1.7, March 1, 2001.

International Organization for Standardization, *ISO/TR 13569: Banking and related financial services — Information security guidelines, Draft*, August 1999.

————, *ISO/DIS 15782-1: Banking — Certificate Management Part 1: Public Key Certificates*, May 13, 2001.

————, and International Electrotechnical Commission, *ISO/IEC 9594-8: Information technology - Open Systems Interconnection — The Directory: Authentication framework*, 1998a.

————, and ————, *ISO/IEC 11568-5: Banking — Key Management (retail)— Part 5: Key life cycle for public key cryptosystems*, 1998b.

————, and ————, *ISO/IEC 15408-1: Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general models*, 1999a.

————, and ————, *ISO/IEC 15408-2: Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999b.

————, and ————, *ISO/IEC 15408-3: Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999c.

————, and ————, *ISO/IEC 17799: Information technology — Security techniques — Code of practice for information security systems*, 2000.

————, and ————, *ISO/IEC 15292: Information technology — Security techniques — Protection profile registration procedures*, 2001.

International Telecommunication Union, Telecommunication Standardization Sector, *ITU-T Recommendation X.500: Information Technology — Open Systems Interconnection — The Director: Overview of concepts, models and services*, 1997a.

————, *ITU-T Recommendation X.509: Information Technology — Open Systems Interconnection — The Directory: Authentication Framework*, 1997b.

Lee, Annabelle, *Certificate Issuing and Management Components Family of Protection Profiles, Version 1.0*, October 2001(http://csrc.nist.gov/pki/secreqmts/wel-come.html).

Malpani, Ambarish, Paul Hoffman, and Russell Housley, *Simple Certificate Validation Protocol (SCVP)*, November 2000 (http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp -04.txt).

Myers, Michael, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, *RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol — OCSP*, June 1999 (http://www.ietf.org/rfc/rfc2560.txt).

National Institute of Standards and Technology, *FIPS PUB 140-1: Security Requirements for Cryptographic Modules*, January 11, 1994 (http://csrc.nist.gov /publications/fips/fips1401.pdf).

――― , *FIPS PUB 140-2: Security Requirements For Cryptographic Modules*, May 25, 2001 (http://csrc.nist.gov/publications/fips/fips1402.pdf).

Pinkas, Denis, *Delegated Signature Validation Protocol Requirements*, November 2001 (http://www.ietf.org/internet-drafts/draft-ietf-pkix-dsv-req-00.txt).

Souffer, Ray, Annabelle Lee, and Arch Oldehoeft, "A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2," *NIST Special Publication* 800-29, June 2001.

SWIFT, *SWIFTNet Security: Security and trust provided to SWIFTNet customers*, Release 1, September 2000 (http://www.swift.com/temp/2763/865/SWIFTNet_ Sec_WP_200009_v1.pdf).

Une, Masashi, "The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies," IMES Discussion Paper Series, No.2001-E-18, Institute for Monetary and Economic Studies, Bank of Japan, December 2001.

VeriSign, Inc., *VeriSign Certification Practice Statement*, Version 1.2, May 1997 (http://www.verisign.com/repository/CPS1.2/).

――――, *VeriSign Trust Network Certificate Policies*, Version 1.0, April 2001a.

――――, *VeriSign Certification Practice Statement*, Version 2.0, August 2001b.

Wahl, Mark, Tim Howes, and Steve Kille, *RFC 2251 Lightweight Directory Access Protocol (v3)*, December 1997 (http://www.ietf.org/rfc/rfc2251.txt).