

# IMES DISCUSSION PAPER SERIES

金融業界におけるPKI・電子認証について  
技術面、標準化に関する最近の動向を中心に

谷口文一

Discussion Paper No. 99-J-30

## IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES  
BANK OF JAPAN

日本銀行金融研究所

〒100-8630 東京中央郵便局私書箱 203 号

**備考：** 日本銀行金融研究所ディスカッション・ペーパー・シリーズは、金融研究所スタッフおよび外部研究者による研究成果をとりまとめたもので、学界、研究機関等、関連する方々から幅広くコメントを頂戴することを意図している。ただし、論文の内容や意見は、執筆者個人に属し、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。

## 金融業界における PKI・電子認証について

技術面、標準化に関する最近の動向を中心に

谷口 文一\*

### 要 旨

近年、金融業界において、電子認証及び電子認証関連サービスのインフラである PKI(Public Key Infrastructure)が注目を集めている。PKI・電子認証は、インターネット上で行なう電子商取引を安全・確実なものにするためには欠かせない要素技術である。インターネットは、従来のクローズドなネットワークに比べて通信コストが圧倒的に低い、全国・全世界のユーザーと通信可能であるというメリットがある反面、通信相手やり取りするデータが本当に正しいのかどうか確認することができなかった。PKI・電子認証はこのインターネット上でクローズドなネットワークの場合と同等の安全性を可能とするものである。特に安全で確実な処理が求められる金融機関にとって、インターネットを通じたサービスの提供を可能にする PKI・電子認証は、顧客との関係を大きく変える契機となる可能性がある。

そこで本稿では、金融業界における PKI・電子認証に関する最近の動向について技術面・標準化面を中心とした検討を行うこととする。特に、PKI・電子認証では公開鍵証明書が発行等管理を行う認証機関(CA)が非常に大きな役割を果たすため、金融業務に利用される CA が認証サービスを提供する場合に関連する標準の内容や果たすべき技術的役割について検討することとする。なお、PKI・電子認証の実装技術の細部については未だ主流となる技術が確立していない部分も多い。このため、本稿では、今後注目していく必要があると思われる最新の技術動向についても紹介する。

キーワード：PKI、電子認証、認証機関、公開鍵証明書、デジタル署名、公開鍵暗号、

X.509

JEL classification：L86、L96、Z00

\* 日本銀行金融研究所 研究第2課 (E-mail: [fumikazu.taniguchi@boj.or.jp](mailto:fumikazu.taniguchi@boj.or.jp))

## 目 次

1 . はじめに .....	1
2 . 金融業・金融機関と PKI.....	3
( 1 ) PKI が有するポテンシャル.....	3
( 2 ) 金融業・金融機関への影響 .....	4
( 3 ) 金融機関による PKI・電子認証への取り組み方.....	6
( 4 ) 金融分野における PKI・電子認証の利用目的と利用状況 .....	7
3 . PKI・電子認証とは.....	11
( 1 ) 公開鍵暗号 .....	11
( 2 ) 公開鍵証明書.....	13
( 3 ) PKI の関連主体.....	14
( 4 ) CA の信頼構造 .....	15
( 5 ) 電子公証.....	18
4 . PKI・電子認証に関する標準化状況.....	19
( 1 ) 国際標準.....	19
( 2 ) 米国国内標準.....	22
( 3 ) 業界標準等 .....	23
5 . CA が果たす技術的役割 .....	27
( 1 ) 各種ガイドライン等の比較 .....	27
( 2 ) CA の秘密鍵の保護 .....	29
( 3 ) 公開鍵証明書廃棄の周知方法について .....	32
( 4 ) 認証ポリシー・CPS の作成 .....	33
6 . PKI に関する最近の技術動向 .....	36
( 1 ) 属性による認証 ( Attribute Certification ) .....	36
( 2 ) Secret Sharing Threshold Scheme.....	36
( 3 ) Proactive Signature .....	37
( 4 ) Public Key Validation .....	37
( 5 ) バイオメトリックスへの対応.....	38
( 6 ) Bridge CA.....	38
7 . 結び .....	39
【補論 1】 Secret Sharing の Threshold Scheme について.....	40
【補論 2】 Proactive Security について .....	42
【参考文献】 .....	45

## 1. はじめに

近年、金融業界において電子認証及び PKI (Public Key Infrastructure) が注目を集めている。米国フォレスターリサーチ社が 1998 年に米国の 51 金融機関に対して行ったアンケート調査では、今後 2~3 年の間における最も重要な技術として電子認証を挙げた金融機関は 43% と最大の割合を占めた (Forrester Research[1998])。実際、近年インターネット上でのショッピングやバンキング等が普及しつつある背景には、PKI・電子認証の実用化によりインターネット上でも安全な取引が可能となったことが挙げられる。

一般に「認証」と言う場合、英語の authentication と certification という 2 つの異なる概念を表わす言葉として使用されることがある。前者は、情報、物、人の真正性 (本物性) を確認するという意味を表わし、本人認証やメッセージ認証と呼ばれることがある。一方、後者は他者に対して何かを証明することを示す。「電子認証」と言う場合もその 2 つの概念を指すことがあり、前者の場合には、電子的な取引において、送信されたデータが確かに本人が送ったものであること及び途中で改竄されていないことを、電子的に作成された署名により検証することを意味する。通常「電子認証」と呼ぶ場合には前者を指すことが多いが、デジタル署名と呼ばれる電子的な署名 (詳細は第 3 章 (1) を参照) を検証するために必要な公開鍵 (詳細は第 3 章 (1) を参照) が確かに登録されていることを証明する機関は認証機関 (CA: Certification Authority) と呼ばれるように、後者の意味でも使用されることがある。また「PKI」とは、公開鍵暗号に基づく技術を広範囲に用いるために必要とされるサービスを提供するインフラである (Ford and Baum [1997])。

PKI・電子認証が注目される背景には、まずインターネットの発展が挙げられる。近年、誰でも自由にアクセス可能なインターネットが普及したことにより、不特定の顧客層を対象にデータ通信を行うことが可能になった。しかし、インターネットは、その自由度の高さとは裏腹にセキュリティを重要視したネットワークではないため、第三者が通信相手に「成りすまし」たり、送信データが途中で盗聴されたり、書き換えられることも想定される。したがって、電子認証の利用によりインターネット上で安全に商取引を行いたいというニーズが高まっている。

また、暗号関連技術の発達も、PKI・電子認証が注目される背景として挙げられる。近年、公開鍵暗号 (Public Key Cryptography) という暗号技術が発達したため、データを作成した本人やそのデータの真正性を電子的に確認することが可能となってきた (公開鍵暗号の概要については第 3 章を参照)。このような公開鍵暗号を用いた電子認証は、鍵の生成や保管、公開鍵の発行や廃棄等の維持管理等多くの作業を必要とし、全体として PKI という一種

のインフラを形成しているが、現在、PKIの実現のために様々な技術開発が行われ、各種サービスや製品が提供されるようになってきているほか、関連した標準化活動も盛んに行われている。

本稿では、技術面・標準化面を中心としたPKI・電子認証についての検討を行うこととする。これは、金融との関わりを中心にPKI・電子認証を解説した文献には、制度、法整備等の観点からの研究は散見されるものの、技術面・標準化面からの研究はさほど多くないか、あるとしても入門的な概要紹介に止まっているためである。まず、第2章でPKI・電子認証と金融業・金融機関の関わりについて述べることとする。第3章でPKI・電子認証に関する基礎的な事項について整理した後、第4章では、インターオペラビリティの確保が重要である電子認証にとって欠かすことのできない標準化動向について整理する。第5章では、金融機関が電子認証業務を行う場合に、技術面ではどのようなポイントが重要となるのかということについて説明する。最後に、第6章において電子認証に関する最近の技術動向についていくつか紹介することとする。

## 2. 金融業・金融機関と PKI

### (1) PKI が有するポテンシャル

PKI・電子認証の概要については第3章で説明することとするが、まず本章において、PKIと金融機関、金融業界との関係について考えることとする。PKI・電子認証が有する主なポテンシャルを列挙すると以下のとおり。

PKIは、セキュリティが低いと指摘されていたインターネット上で、取引相手の確認や送信する情報の真正性証明等を可能とする。これまでインターネットは商品案内やニュースの提供等さほど高セキュリティが要求されない業務を中心に使用されてきたが、PKIにより高度な信頼性や安全性が要求される商取引についてもインターネットを通して行うことが可能となるため、従来の face-to-face の取引や専用線によるオンライン取引に対して、取引コストの大幅な削減が期待される。

PKIにより、インターネット上で商取引を行うことが可能となるため、劇的に空間的制約が緩和される可能性がある。すなわち、従来のように顧客ベースが店舗の周辺に限定される必然性はなく、理想的には全国・全世界のインターネット利用者が対象となり得る。

PKIにより、商取引をインターネット上で行うようになれば、インターネット上の標準的なプロトコルを用いてデータ通信を行うこととなるため、エクストラネット<sup>1</sup>等を通じた外部企業とのシステム連携が容易となり、金融機関の M&A や業務提携等様々な環境変化に対してより迅速に対応することが可能となる。

PKIの実現には、公開鍵証明書を発行する CA が非常に重要な役割を果たす。公開鍵証明書への信頼性は、利用者による CA 自体に対する信頼に依存する面が大きく、その信頼が揺らいだ場合、当該 CA が管理する電子認証システム全体が崩壊する可能性がある。したがって、今後 PKI の普及に向けて、どのような組織が CA 業務の中心となっていくかが注目される。なお、CA への信頼は、ネームバリュー等組織自体に対する信頼に加えて、認証システムを安全に運営するための技術力に対する信頼が重要な役割を果たすものと考えられる（CA が果たすべき技術的な役割については、第5章を参照）。

---

<sup>1</sup> エクストラネット：本社と支店間や関連企業グループ間等、特定のグループ内でのみイントラネットを相互に接続した仮想的なプライベート情報システムのことであり、バックボーンにはインターネットを使用する。従来、このようなプライベートな情報システムを実現するためには各サイト間を専用線等で接続する必要があったため、構築コストが高くなりがちであったが、インターネットをバックボーンとして使用できるようになったことにより、比較的安価かつ柔軟にシステムの構築が可能となった。

## (2) 金融業・金融機関への影響

PKIによりインターネット上で金融取引が行われるようになれば、様々な影響が金融業・金融機関に及ぶものと考えられる。具体的な影響は以下のとおり。

### 他業態の企業による金融業への新規参入を促進する可能性

PKI・電子認証により多くの金融サービスを電子的に提供することが可能になると、金融業務のより多くの部分を情報システムを中心としたテクノロジーに依存することとなるため、そのようなテクノロジーに競争優位を有する他業態の企業による金融業務への参入が増えてくることが予想される。特に、当面、テクノロジーの有効活用によるコスト削減効果が大きい一般消費者向け金融商品の提供において他業態の企業の参入が増える可能性が高い。

Face-to-faceの取引により金融業務の多くが行われていた時には、店舗のロケーションや数、ネームバリュー等が取引先を選択する重要な要素であったが、電子的な取引においては技術力や技術面でのブランド力の重要性が増してこよう。実際、わが国でもソフトバンクやソニー等技術力に優れた非金融機関が金融業に参入してきている。

### 金融サービスの提供形態の変化

本来、預金や有価証券といった金融商品は、預金証書や証券の券面といった物理的な媒体に価値があるのではなく、その媒体に書かれた情報が価値を表象する性質を有するため、インターネット上での取引に適していると考えられる。したがって、電子認証を利用することにより、金融商品の紹介だけではなく、口座開設申請や決済等までもインターネット上で確実・安全に行えるようになれば、従来と比べて金融商品の販売が格段に低コストで行えるようになる可能性がある。例えば、株式売買手数料の自由化が進んでいる米国では、無店舗のオンライントレードが普及することにより、株式の平均売買手数料が2年間で約3分の1に下がった(<http://www.zdnet.co.jp>等)。

また、現在、電子認証の技術を応用することにより、電子マネーの実証実験が世界各地で行われているほか、CPやCDの電子化が各々大蔵省や法務省で検討されている。これらが実現すれば、各種金融サービスの提供がより低コストで行えるようになるほか、金融取引の最初から最後まで人手を介さ

ず全て自動化する STP<sup>2</sup> (Straight Through Processing) の実現により、よりスピーディーで効率的な金融取引の実現に繋がる可能性がある(宮田[1999])。

これまで金融機関にとっては、広い店舗網等既存の販売チャネルを有していることが新規参入業者に対する大きな優位性として作用してきたが、PKI・電子認証を利用することにより低コストで多くの顧客に対して金融サービスを提供することが容易になってくると、既存の販売チャネルを有することが必ずしも優位に働かない場合があることに留意すべきである。例えば、従来までであれば広い店舗網を有しない外国企業や他業態の企業が金融サービスを一般消費者を対象に広く提供することは非常に困難であったが、それが可能となってきたため、わが国でも小口株式売買手数料の自由化に向けて外国企業や他業態の企業がインターネットバンキングやインターネットトレーディングの形態で一般利用者向け金融サービスに新規参入しつつある。

#### 金融機関(銀行)による一般的な電子認証サービスへの進出

銀行は、企業や個人の預金口座等、各主体の特定の情報を保管・維持管理する主体として長年機能しているという実績がある。また、銀行はそもそも与信業務等において取引相手の審査を行っており、認証業務はその延長線上にあると捉えることも可能である。加えて、電子認証を行う主体は利用者から信頼される必要があるが、一般的に銀行は歴史的に信頼できる組織であると認識されているものと考えられる。このように、銀行は電子認証サービスを行うのに適したポジションにいると考えられる。

したがって、継続的な手数料収入を期待して、自社の金融サービスに付随しない一般的な電子認証サービスに金融機関が CA として進出することも考えられる。ただし、この点については、銀行法による他業禁止規定との兼ね合いが問題となる<sup>3</sup>。

この点に関して、米国では、ユタ州に本店がある Zions First National Bank of Salt Lake City が子会社の Digital Signature Trust (DST) を通じて行っている認証サービスの提供が、米国通貨監督庁(OCC: Office of the Comptroller of the

<sup>2</sup> STP: 証券取引を中心に、約定から決済に至るプロセスを、標準化されたメッセージ・フォーマットによりシステム間を自動的に連動させることによって、人手を介さずに一連の作業をシームレスに行うことであり、近年、欧米の金融機関を中心に STP の実現に向けた様々なプロジェクトが行われている。

<sup>3</sup> 大蔵省銀行局・国際金融局(事務局)[1997]による「電子マネー及び電子決済に関する懇談会報告書」では、「金融機関が電子決済に関連して認証サービスを行う場合には、この認証サービスは高い安全性を有していると考えられるため、こうした金融機関による認証サービスを電子決済に関連したものでない以外に活用することも考えられる。電子商取引の円滑な普及の観点から、金融機関の他業禁止の主旨にも配慮しつつ、金融機関による一般的な認証サービスの提供につ

Currency) により銀行の付随業務として 1998 年に認可されたという例が参考になる。

また、1999 年 6 月より米国の Wells Fargo 銀行が、サイバートラスト社の技術を用いて、口座を開設した商店に対してホームページの認証を行い自らのブランドで公開鍵証明書を発行するというサービスを開始したという例も存在する。当初は無料であるが、試行期間後は公開鍵証明書発行料を課す予定であり、現時点における公開鍵証明書発行の市場価格は年間約 350 ドルであると報じられている(1999 年 5 月 28 日付 American Banker)。

英国でも、1998 年よりパークレイズ銀行が、Barclays Endorse というデジタル署名の作成及び確認手段の提供を行っている。パークレイズ銀行は、デジタル署名を作成する際に必要な情報が搭載されている Barclays Endorse card という IC カードを利用者に発行し、これによって作成された署名が真正なものであるかどうかという確認サービスを署名の受信者に対してオンラインで提供している。1998 年 6 月から 1999 年 5 月にかけて、英国の税務当局は自営業者がインターネット経由で納税申告を行うために、本サービスを試行的に利用した。

公開鍵証明書の発行・管理等のための認証システムの構築には比較的大きな初期コストが必要である一方、個々の公開鍵証明書の発行に係るコストは大きくないと予想される。したがって、電子認証は装置産業的な側面が強く、規模の経済が働き易いサービスであり、一般的な認証サービスに進出する金融機関にとってはどれだけ採用される Web サイトや利用ユーザーを早く囲い込めるかということが重要となろう。

### (3) 金融機関による PKI・電子認証への取り組み方

このように、電子認証は、多くの金融機関にとって非常に重要な技術である。金融機関による電子認証の取り組み方法としては、以下のようにいくつかのオプションが考えられる。

自前で認証システムを構築し、自ら CA として機能。

認証サービス提供会社による公開鍵証明書作成機能を利用して、自らの名前で公開鍵証明書を発行してもらう。

認証サービス提供会社が発行する公開鍵証明書を利用。

取り組み方法は、大きく、自前で CA 機能を提供するか( )、認証サービス会社にアウトソースするか( )、( )に分類されるが、これらのメリッ

---

いても検討していくことが適当である。」としている。

ト・デメリットの比較については、いくつかのリサーチ会社が具体的に認証サービスを提供する際の TCO<sup>4</sup> ( Total Cost of Ownership ) を比較するレポートを公表している ( Aberdeen Group[1998]、Giga Information Group[1998] )。試算結果はレポートにより異なるが、定性的には概ね表 1 のように考えられる。

表 1 認証サービスの提供方法に応じた特徴の比較

自前で認証システムを構築・運営	認証サービスをアウトソース
<ul style="list-style-type: none"> <li>システム構築費用、ベンダーによるサポート費用が高い。</li> <li>公開鍵証明書の配布・廃棄の都度、費用がかからない。</li> <li>自らのセキュリティニーズに合わせた PKI を自由に構築できる。</li> <li>顧客から高い信頼を受ける企業は、その信頼の高さを電子認証業務での信頼確保に活かせる。</li> </ul>	<ul style="list-style-type: none"> <li>システム構築費用、ベンダーによるサポート費用は少ない。</li> <li>公開鍵証明書の配布・廃棄の都度、費用がかかる。</li> <li>初期コストが少なく済むため、将来の電子認証対応における自由度が高い。</li> </ul>

表 1 のとおり、自ら CA となって認証システムを構築・運営する場合には、公開鍵証明書を管理するためのシステム構築費用がかかる反面、電子認証におけるセキュリティレベルや運営において自らのセキュリティニーズにフレキシブルに対応しやすいと考えられる。公開鍵証明書の管理負担については、その規模が大きくなるほど、特に有効期限到来や秘密鍵の漏洩等に伴う公開鍵証明書の廃棄及び再発行に係る負担が大きいと指摘されることが多い。

また、PKI の構築に当たっては、情報セキュリティに関するスキルが要求され、組織的にそのスキルを高めていく必要があると考えられる。特に、金融機関自らが CA となって認証業務を行う場合、技術力は非常に重要であり、暗号関連技術 ( 鍵の管理・保管等、暗号アルゴリズムの安全性評価等 )、分散システム関連技術 ( オンラインディレクトリサービス等 ) 等、従来銀行が手がけてきた大型コンピュータによるオンラインシステムの場合とは異なる技術力が要求される。

#### ( 4 ) 金融分野における PKI ・電子認証の利用目的と利用状況

金融分野における PKI ・電子認証の利用は、以下のような利用目的に大きく分類することが可能である。

個人向けのインターネットバンキング ( 預金の振替、残高照会等 ) やイ

<sup>4</sup> TCO : 情報システム資産に関する直接コストだけでなく、維持管理や技術の習得、人件費なども含めた総合的なコスト。

インターネットトレーディング（株式、債券等の売買等）  
企業向けのインターネットバンキング（従来から存在するエレクトロニックバンキングのインターネット対応）  
個人向けのインターネットショッピングの決済（クレジットカード、銀行口座引き落とし等）  
一般的な電子商取引におけるオンライン店舗サーバーの認証  
金融機関社内ネットワーク（イントラネット及びエクストラネット）での相手認証及びデータの暗号化  
電子マネー、電子小切手  
～ における CA に対する認証（ルート CA 等）

これらの利用目的において、具体的には、  
（ア）Web ページ・サーバーが正当なものであることの確認、  
（イ）利用者が正当な顧客であることの確認、  
（ウ）データ、メッセージの真正性確認、  
（エ）秘密通信を行うための共通鍵方式のセッション鍵の交換、  
のために PKI・電子認証が使用されている。

上記 ～ の利用目的が Web 上でサービスされるように、近年の電子商取引の多くは Web を介して提供されるため、PKI・電子認証に関しても Web 上での技術に対する注目度が高い。Web 上でのクレジットカードやデビットカードの利用にあたっては、2、3 年前までは VISA と MasterCard が共同で開発した SET（Secure Electronic Transactions）というプロトコルにより認証や暗号化を行うことに注目が集まっていたが、SET では専用ソフトウェアを顧客が利用するパソコンにインストールする必要があることや、顧客のパソコンでの処理が重いことから、最近では SSL（Secure Sockets Layer）バージョン 3.0 というプロトコルを用いて加盟店や利用者の認証、クレジットカード番号の暗号化を行うことが主流になりつつある。なお、SSL における認証については、日本ベリサイン社やサイバートラスト社等の認証ベンダーに公開鍵証明書を発行してもらうという、本章（3）の のケースが多いようである。

また、本章（2）で紹介したとおり、米国の Wells Fargo 銀行のように、電子決済において電子認証サービスを提供するのみならず、一般のオンライン商店に対して電子認証サービスを提供する動きも見られる。

個々の金融機関が独自に PKI・電子認証を利用するという動きに加えて、欧米では、ABAecom<sup>5</sup>、GTA<sup>6</sup>（Global Trust Authority）、S.W.I.F.T.<sup>7</sup>（Society for

---

<sup>5</sup> ABAecom：米国銀行協会（American Bankers Association：ABA）の電子認証サービス子会社であり、米国国内で電子認証を行う銀行のルート CA となることを展望しているものと考えら

Worldwide Interbank Financial Telecommunications s.c.) のように、業界団体や複数の金融機関が集まって、金融取引のインフラとして電子認証を位置づけようとする動きも見られるようになってきた。これは、PKI・電子認証が個別金融機関内での利用が中心だった段階から企業間でのインターオペラビリティが求められる段階まで利用が進みつつあることを表わしているものと考えられる。

表2 金融業界における PKI・電子認証技術を採用したプロジェクト例 (1/2)

金融機関・団体名	利用目的	PKI・電子認証を採用するプロジェクト	利用プロトコル	認証ベンダー等	備考
住友銀行		個人向インターネットバンキング	SSL (128bit)	日本ペリサイン社	
三和銀行		個人向インターネットバンキング	SECE <sup>8</sup>	日本認証サービス社	
野村証券		個人向インターネットトレード	SSL (128bit)	サイバートラスト社	
日本興業銀行		企業向グローバルキャッシュマネジメントサービス	SSL	サイバートラスト社	暗号鍵や公開鍵証明書はPCカードで保管
JCB		個人向インターネットショッピング (J-Mall) でクレジットカード決済を可能化	SET		自社でCA機能を遂行
Wells Fargo 銀行		SureServer サービス: オンライン商店のWebページ・サーバの真正性を確認するための公開鍵証明書の発行		GTE Cybertrust (Wells Fargo 銀行の名で公開鍵証明書を発行)	電子決済における認証ではなく、一般的な認証サービスの提供
大和証券		社内国際ネットワーク	SSL (128bit)	日本ペリサイン社	インターネットを利用して国際基幹網を構築し、社内システムにおけるデータの暗号化と相手認証を実施

れる。これは、ノンバンクがオンラインサービスに本格参入する前に、オンラインでの決済サービスにおける銀行業界の優位性を強化したいという考えに基づいているものと考えられる。

<sup>6</sup> **GTA**: 国際金融の電子取引におけるインターオペラビリティを確保するために、階層構造で各参加金融機関の認証を行うルートCAを構築するために、欧州を中心に多くの大手銀行が参加して1999年に設立した組織。わが国からはさくら銀行が参加。

<sup>7</sup> **S.W.I.F.T.**: クロスボーダー銀行取引におけるペーパーレス化を、同一のネットワーク、標準化された手続きにより推進することを目的として1973年に欧米15カ国239銀行の出資により設立されたベルギーに本部を置く非営利協同組合。日本の金融機関は1976年より参加している。

<sup>8</sup> **SECE** (Secure Electronic Commerce Environment): インターネット上でのクレジットカード支払と銀行預金支払を対象とした共通プラットフォームの開発を目的とした日立、富士通、NECの3社によって開発中のソフトウェア開発プロジェクトである。クレジットカード支払についてはSETに準拠しているが、SETバージョン1.0に対して、ボーナス払い等の日本独特の商習慣や日本語のサポート等仕様の拡張が行われている。

表 2 金融業界における PKI・電子認証技術を採用したプロジェクト例 (2/2)

金融機関・団体名	利用目的	PKI・電子認証を採用するプロジェクト	利用フォーマット	認証ベンダー等	備考
ABAecom		銀行の Web ページ・サーバーの真正性を確認するための公開鍵証明書の発行		Digital Signature Trust (DST)	米国内で電子認証を行う銀行のルート CA となることを展望
Global Trust Authority (GTA)		国際的な CA の相互運用性の確保に向けた認証サービスの提供			国際的な金融業務で電子認証を行う銀行のルート CA となることを展望 階層型構造により、CA 間の相互運用性を確保
S.W.I.F.T.		E-Trust : SWIFT の新ネットワークインフラ ( Next Generation ) 上の業務やインターネット上の金融取引に対して電子認証サービスを提供する予定			

### 3 . PKI・電子認証とは

#### ( 1 ) 公開鍵暗号

PKI・電子認証の実現にあたっては、公開鍵の真正性を証明する公開鍵証明書が非常に重要な役割を果たす。そもそも、公開鍵暗号では、本人のみが保有する秘密鍵と他人にも広く公開する公開鍵という、数学的関係はあるが公開鍵からは秘密鍵を類推できない1組の鍵ペアを使用する。ここで、一方の鍵で暗号化したデータは、他方の鍵でしか復号化できないという性質を利用して、電子認証及び秘密通信を実現することができる<sup>9</sup>。

#### ( 電子認証 )

公開鍵暗号による電子認証を行う場合(図1を参照)、まず、データの送信者が鍵ペアを作成した上で、受信者がその一方の公開鍵を入手できるようにしておき、他方の秘密鍵のみを秘匿しておく。データの送信者は、送信したいデータを自らの秘密鍵で暗号化して暗号データを作成し<sup>10</sup>、元のデータと共に相手に送信する。この暗号データは、秘密鍵を保有している本人しか作成できないものという意味で、デジタル署名や電子署名<sup>11</sup>と呼ばれる。受信者は、送信者の公開鍵を用いてデジタル署名の検証処理を行い、その真正性が確認されれば、送信されたデータは正当な本人が作成したものであり、かつ途中で改竄されていないということが確認される。このような電子認証を利用することにより、メールの送信者やホームページの作成者が本当に正しい人物・企業であることを確認できる。

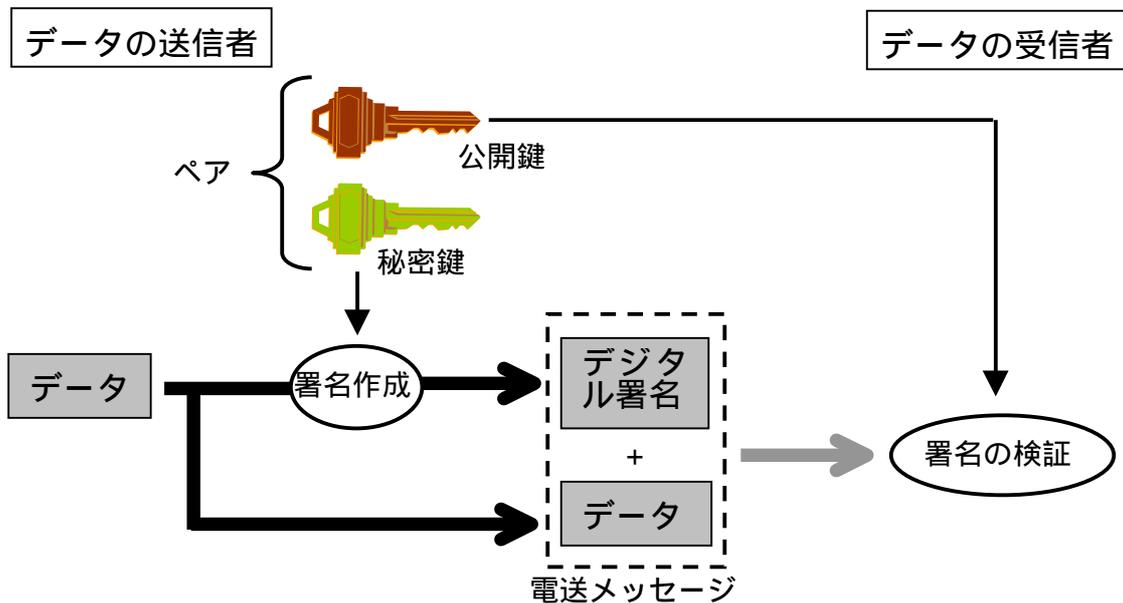
---

<sup>9</sup> 実際の公開鍵暗号方式には、電子認証と秘密通信の両方に使える方式の他に、電子認証にしか使用できない方式や秘密通信にしか使用できない方式も存在する。

<sup>10</sup> 実際には、データの送受信を効率よく行うために、一方向性ハッシュ関数(入力値から出力値を得ることは容易であるが、アルゴリズムを知っていても出力値から入力値を推定するのは困難であり、任意ビット長のビット列をある長さのビット列に変換する関数)により元のデータを圧縮した結果に対して秘密鍵で暗号化を行うケースもある。

<sup>11</sup> 「電子署名(electronic signature)」は、公開鍵暗号方式を利用したデジタル署名に加えて、手書きの署名の画像データ等、本人しか作成できない電子的に処理された情報全般を指すより広い概念を指す言葉として使用されることがある。

図1 公開鍵暗号による電子認証

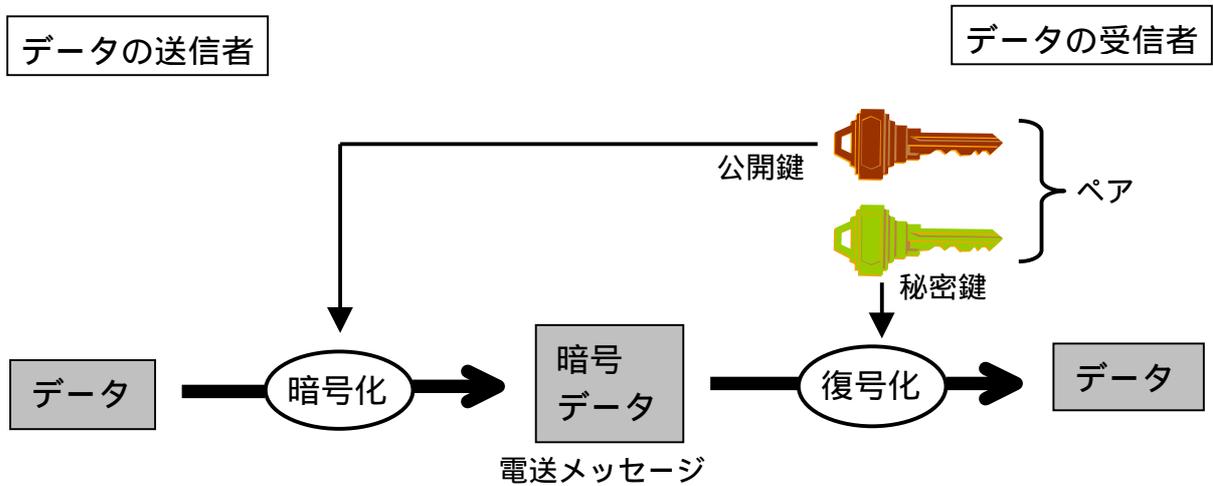


(秘密通信)

公開鍵暗号は秘密通信のためにも使用することが可能であり(図2を参照)、その場合、まず、データの受信者が鍵ペアを作成し、その一方の公開鍵をデータの送信者に渡し、他方の秘密鍵のみを秘匿しておく。データの送信者は入手した公開鍵によりデータを暗号化し、暗号データをネットワーク経由等で送信する。暗号化されたデータは、受信者が保有している秘密鍵でしか復号化できないため、秘密通信が可能となる。この場合、公開鍵は第三者に対して秘密にする必要がないため、特に不特定多数の主体と秘密通信を行う時に有用である。

一方、データの送受信者が予め共有している一つの暗号鍵を暗号化にも復号化にも使用するような暗号を共通鍵暗号と呼ぶが、公開鍵暗号は共通鍵暗号と比較すると暗号化や復号化に要する計算量が多く、処理に時間がかかるため、公開鍵暗号により共通鍵暗号の暗号鍵を送信し、その後は共通鍵暗号によりデータの送受信を行うことが多い。

図2 公開鍵暗号による秘密通信



(2) 公開鍵証明書

(1)で触れたとおり、公開鍵を利用した秘密通信や電子認証では、相手の公開鍵を使用することが前提となっているが、その公開鍵が正当な相手が保有する秘密鍵に対応した正しいものであることを証明するのが、公開鍵証明書である。

図3 公開鍵証明書の利用 (電子認証の場合)

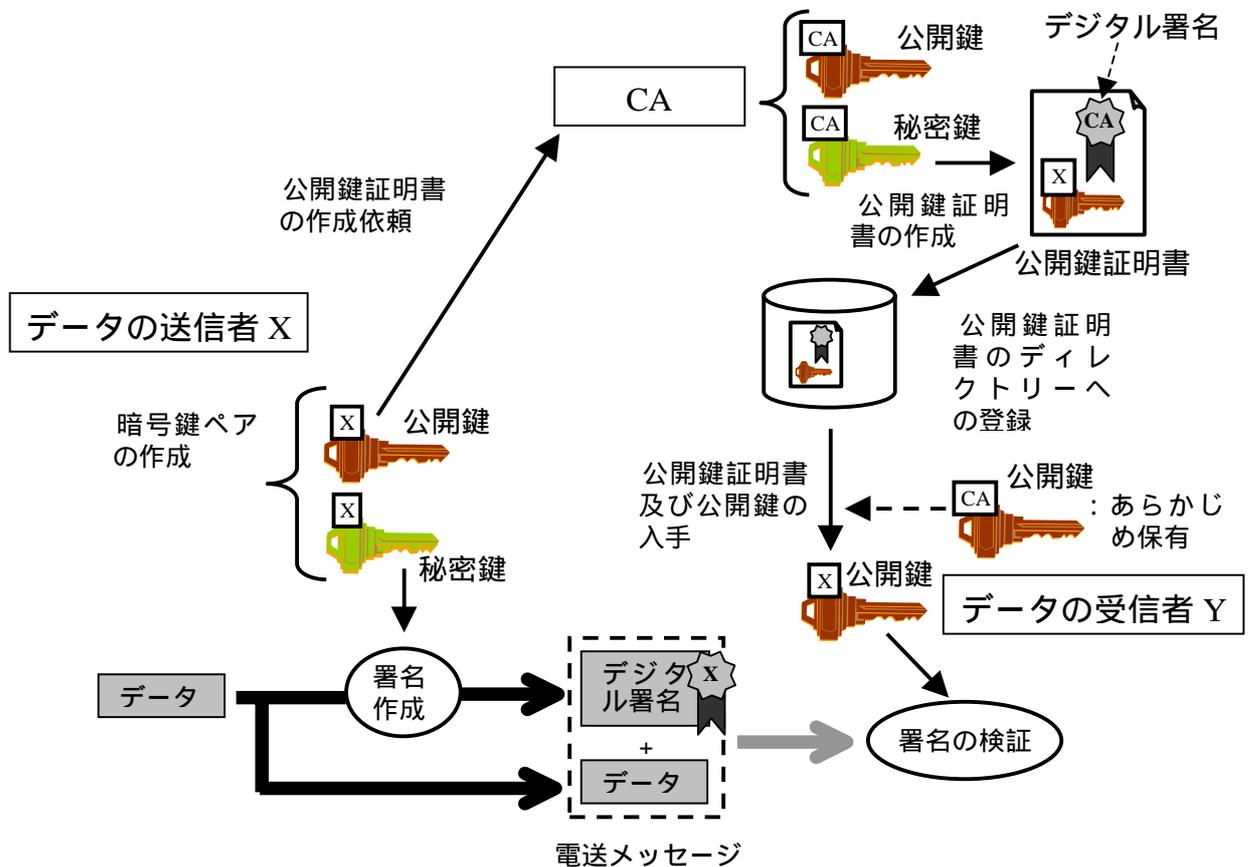


図3のとおり、公開鍵証明書は、各主体の公開鍵や関連情報に対して、CAが自らの秘密鍵によりデジタル署名を付したものである。Webブラウザに組み込まれていたり、郵送等の方法により、利用者はあらかじめCAの正しい公開鍵を入手しており、これにより公開鍵証明書がCAにより作成されたものであり、公開鍵証明書に付された取引相手の公開鍵も信頼できるものであることを確認することができる。公開鍵と秘密鍵は数学的関係があるとは言え、公開鍵から秘密鍵を推測することは非常に困難であるため、公開鍵証明書及び公開鍵は秘密にする必要がない。したがって、セキュリティ対策が十分とはいえないネットワークやシステムを使って公開鍵証明書を配布することが可能である。

次に、公開鍵証明書の作成、配布、廃棄といった一連の流れは以下のとおりである。

#### 公開鍵と秘密鍵のペアの作成

作成場所は、(ア)秘密鍵を使用する本人が保有するシステム(ICカードやパソコン上のソフトウェア)と、(イ)CAのセンターシステムに大別される。

公開鍵証明書申請者が公開鍵と必要な情報をCAに提出

CAが公開鍵証明書に記述する内容の正当性を確認

CAが公開鍵証明書を作成し、自らの秘密鍵により署名

公開鍵証明書を申請者に送付する他、第三者もアクセス可能な場所に保管  
必要に応じて公開鍵証明書の廃棄を行い、公開鍵証明書廃棄リストの形で  
廃棄した公開鍵証明書を周知

公開鍵証明書が廃棄されたことを確実に周知することは、電子認証にとって重要なポイントである。この点については、第4章で説明する。

### (3) PKIの関連主体

公開鍵証明書の作成や廃棄等の管理を行う主体はCAであり、PKIの確実な運用やその安全性に関して非常に重要な役割を果たしている。

公開鍵証明書の発行に際しては、実際に公開鍵証明書申請者とコンタクトをとり、ID等による本人の真正性の確認を行う必要がある場合もある。その場合、登録対象者数が多く、地理的に広がっている場合には、CAだけでは公開鍵証明書発行のための本人確認を行うことは困難である。したがって、本人確認及び公開鍵証明書に記載する事項の確認は、複数の登録機関(RA: Registration Authority)が実際に公開鍵証明書申請者とコンタクトをとりながら行うケースもある。この場合、RAは申請事項の確認後にCAに対して

公開鍵証明書を作成を要求し、その要求に基づいて CA が公開鍵証明書を作成することとなる。

加えて、近年、属性 (Attribute) による認証という概念が提案され、その認証を行う主体として属性認証機関 (AA: Attribute Authority) が今後一般的になる可能性がある。属性による認証の詳細に関しては、第 6 章の (1) を参照。

#### (4) CA の信頼構造

電子認証が幅広く使用されるようになると、一つの CA が全ての公開鍵証明書の発行・管理を行うのは不可能である。したがって、他の CA が公開鍵証明書を発行する主体と取引を行わなければならないケースもあるが、このため、相手の CA が発行した公開鍵証明書を使用するための相互運用の仕組みが必要になってくる。

複数の CA が各々公開鍵証明書を発行する状態での相互運用の仕組みは大きく以下の 3 つに分類することができる。

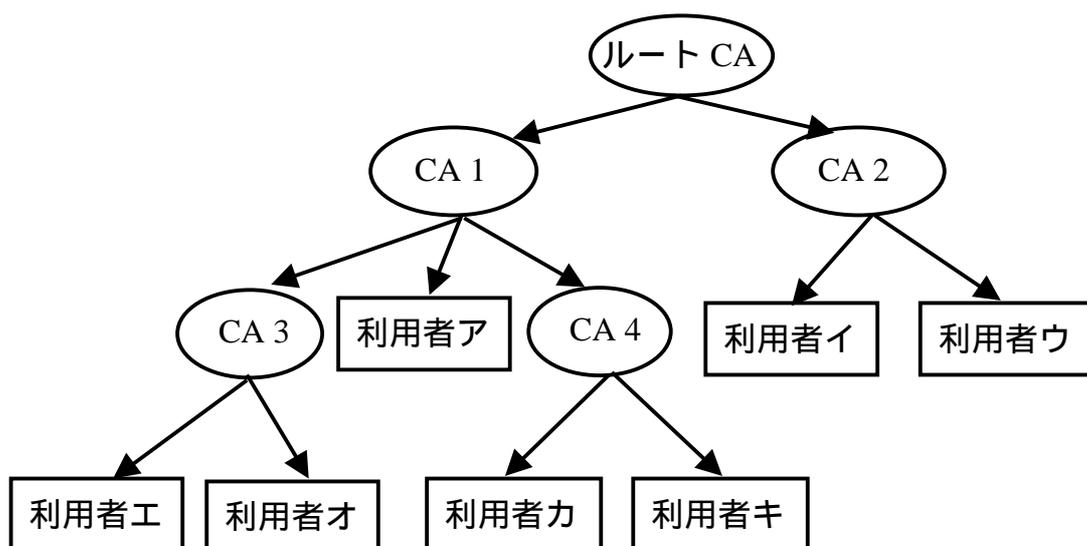
##### 階層型

階層型構造では、各 CA の公開鍵は他の CA により公開鍵証明書が発行されており、その関係は階層的なピラミッド構造になっている (図 4 を参照)。本構造では、上位の CA が下位の CA を認証する形となっている。本構造の最上位に位置し、どの CA からも認証されていない CA をルート CA と呼ぶ。ルート CA の秘密鍵が他者に漏れると、本 PKI 配下の全 CA 及び利用者の公開鍵の安全性が脅かされるため、ルート CA には非常に高い安全性が求められる。階層型構造では、ルート CA の公開鍵はどの CA からも認証されていないため、配下の全利用者がルート CA の正しい公開鍵を何らかの方法で確実に入手していることを前提としている。

図 4 の例で (利用者工) が (利用者力) と秘密通信を行いたい場合、まず、(利用者工) はルート CA の正しい公開鍵を保有しているため、ルート CA のデジタル署名が付された正当な CA1 の公開鍵証明書を電子的に入手する。CA1 の正当な公開鍵が入手できたため、(利用者工) は、次に CA1 のデジタル署名が付された正当な CA4 の公開鍵証明書を電子的に入手する。CA4 の正当な公開鍵が入手できたため、CA4 のデジタル署名が付された正当な (利用者力) の公開鍵証明書を電子的に入手できる。(利用者工) は、入手した (利用者力) の公開鍵でデータを暗号化して (利用者力) に送信することにより、秘密通信が可能となる。なお、この例において、(ルート CA) - (CA1) - (CA4) - (利用者力) という一連の信用の繋がりを認証パス (Certification Path) と呼ぶ。

階層型構造は、各主体に対する認証パスが一つしかないため見つけ易いというメリットがある反面、規模が大きくなるほど認証パスが長くなり処理負担が増えるというデメリットもある。そのため、後述（第4章）の公開鍵証明書に関する国際標準 ISO/IEC/ITU X.509 の Annex K において、CA 用の公開鍵証明書については利用できる認証パスの段数を制限（Path Constraint）できるように考慮されている。

図4 CAの信頼構造（階層型）



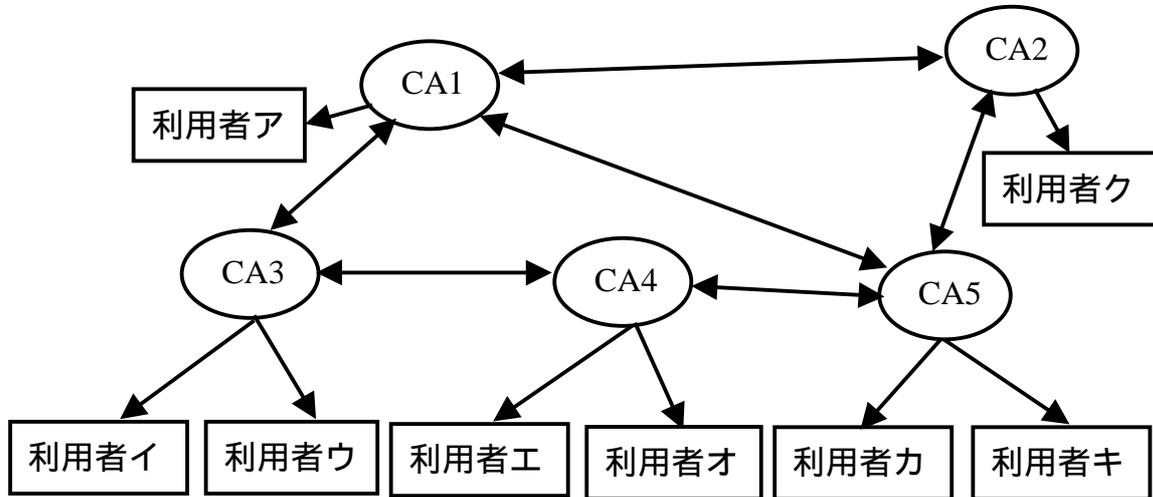
#### 相互認証型（非階層型）

相互認証型構造では、各利用者は自らの公開鍵を認証してもらっている CA の公開鍵を保有しており、他の CA による認証の有無に関わらずその公開鍵を信頼するということを前提としている。各 CA は他の CA と相互に認証を行っているが、そのパスを追うことにより他 CA 配下の利用者の公開鍵証明書の有効性を確認することができる。本構造では、ある CA の秘密鍵が他者に漏れた場合でも、その影響は当該 CA 配下の利用者にとどまるため、その利用者に公開鍵証明書を配布し直すことで対応できるため、秘密鍵漏洩時の負担は階層型と比較して小さい。

図5の例で（利用者ア）が（利用者キ）と秘密通信を行いたい場合、まず、（利用者ア）は自らの CA である CA1 の正当な公開鍵を保有しているため、CA1 のデジタル署名が付された正当な CA5 の公開鍵証明書を電子的に入手する。（利用者ア）は、CA5 の正当な公開鍵が入手できたため、CA5 のデジタル署名が付された正当な（利用者キ）の公開鍵証明書を電子的に入手できる。正当な（利用者キ）の公開鍵が入手できたため、（利用者ア）は、データを（利用者キ）の公開鍵で暗号化し、これを（利用者キ）に送信するこ

とによって秘密通信が可能となる。

図5 CAの信頼構造(相互認証型)



#### 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構造である。階層型構造のブロックが複数存在しており、各ブロックのルートCA同士が相互認証をしているというのが基本的な構造となっている。ただし、必要に応じてルートCAでなくとも他のCAと直接相互認証を行うことも考えられる。

例えば、米国のFPKI<sup>12</sup> (Federal Public Key Infrastructure) においては、各官庁や外部機関による複数のCA (及びその配下のCA、エンドユーザー) 間の信用をBridge CA (第6章を参照) が繋ぐというハイブリッド型の構造を採用している。

このような相互運用のための信頼構造のうち、どのような形態が主流となるか、まだ見極められる状況にはない。認証パスの検索技術の動向や公開鍵証明書の正当性チェック技術の動向に応じて、主流となる信頼構造も定まっていくものと考えられる。

<sup>12</sup> FPKI: 米国政府が情報資源を安全に使用する目的で利用するPKIを指し、現在、商務省の下部組織として科学技術全般の標準規格の策定を担当しているNational Institute of Standards and Technology (NIST) において、FPKIで採用する様々な認証関連技術やその使用法等について検討が行われている。FPKIの検討は、Part A: Requirements, Part B: Technical Security Policy, Part C: Concept of Operations, Part D: Interoperability Profiles, Part E: X.509 Certificate and CRL Extensions Profile という5つのPartで行われている。

## ( 5 ) 電子公証

電子公証とは、電子認証関連技術のアプリケーションの一つであり、当事者間に予想される紛争を解決するために、「誰が」「何を」「いつ」取引したかを、取引の第三者が証明する電子的な仕組みである。電子公証サービスを提供する主体は、信頼される第三者機関（TTP: Trusted Third Party）として第三者の立場で当事者間の取引の事実を電子的に保管し、その内容が正しいことを証明する機能を果たす。

電子商取引実証推進協議会（ECOM）の電子公証システムガイドライン（Ver.1.0）[1998]は、電子公証に要求される機能として、送受信者特定機能、到達確認機能、改竄検知機能、時刻付与機能、アクセス記録機能、プロセス記録機能、電子保存機能、を挙げている。このうち、送受信者特定機能は通常 CA により行われる。

公証と言えば、公的機関が行うサービスであるとイメージされることが多いが、必ずしもその必要はなく、第三者が取引の内容等を電子的な形で証明すれば、民間企業が行う場合も含めて電子公証と呼ぶことが多いようである。公的機関による電子公証への取り組みに関しては、現在、法務省が公証人役場で実施している確定日付の付与や公正証書の作成に関するサービスを電子データに対しても提供可能とする「電子公証制度」の開発を行っている。民間企業による電子公証への取り組みの一例としては、社内で行う重要データの保管等もその範疇に含まれる。

#### 4 . PKI・電子認証に関する標準化状況

PKI では、各主体間でのインターオペラビリティが確保されていることを前提としており、そのためにも標準化は非常に重要な役割を果たしている。したがって、本章では、PKI に関する標準化状況を紹介することとする（PKI に関する国際標準化活動の一覧は図 8、主な標準に関する具体的な対象分野は表 4 を参照）。

##### （ 1 ）国際標準

###### ITU-T X.509

PKI に関する基本的な標準の一つに、国際通信連合（ITU: International Telecommunication Union）下の通信標準セクター（ITU-T）で作成された ITU-T Recommendation X.509（Information technology – Open Systems Interconnection – The directory: Authentication framework）という標準がある。X.509 は、公開鍵証明書や公開鍵証明書廃棄リスト（CRL: Certificate Revocation List、詳細は第 5 章（2）を参照）のデータ構造等を定めており、他の多くの標準も本標準で定められた形式の公開鍵証明書を使用している<sup>13</sup>。現在有効な形式は 1996 年に定められたものであり、公開鍵証明書はバージョン 3、CRL はバージョン 2 と呼ばれている。ちなみに、X.509 は、国際標準化機構（ISO: International Organization for Standardization）と国際電気標準会議（IEC: International Electro-technical Commission）が共同で設立した ISO/IEC JTC1<sup>14</sup>（Joint Technical Committee 1）の SC6 においても同じ内容が標準化されており、その名称は ISO/IEC 9594-8 である。

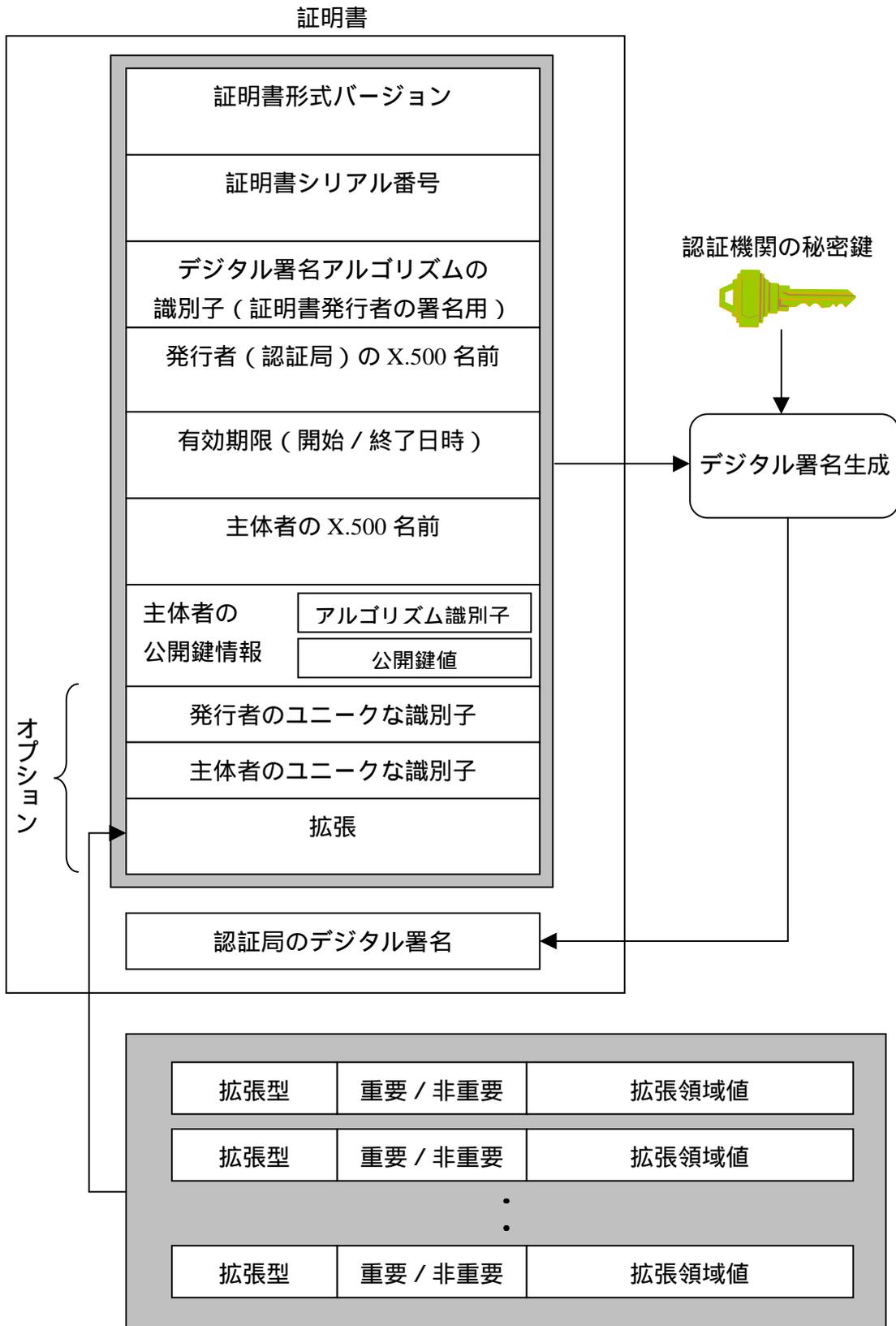
X.509 バージョン 3 による公開鍵証明書は、具体的には図 6 のような形式となっている。図 6 のとおり、X.509 バージョン 3 による公開鍵証明書には拡張フィールドが設けられており、暗号鍵と CA の運用ポリシー（詳細は第 5 章（3）を参照）、各主体と CA の属性、認証パス、CRL、に関する情報を追加的に記述するために使用されている。

---

<sup>13</sup> この他の公開鍵証明書の仕組みとしては、暗号学者の Rivest と Lampson が提案した SDSI（Simple Distributed Security Infrastructure）と Internet Society（ISOC）下の Internet Engineering Task Force（IETF）の作業部会によって開発された SPKI（Simple Public-Key Infrastructure）がある。いずれも、複雑な X.509 を簡単にする形で、より容易に PKI を実現することを企図しているが、X.509 と比較するとあまり利用されていない。

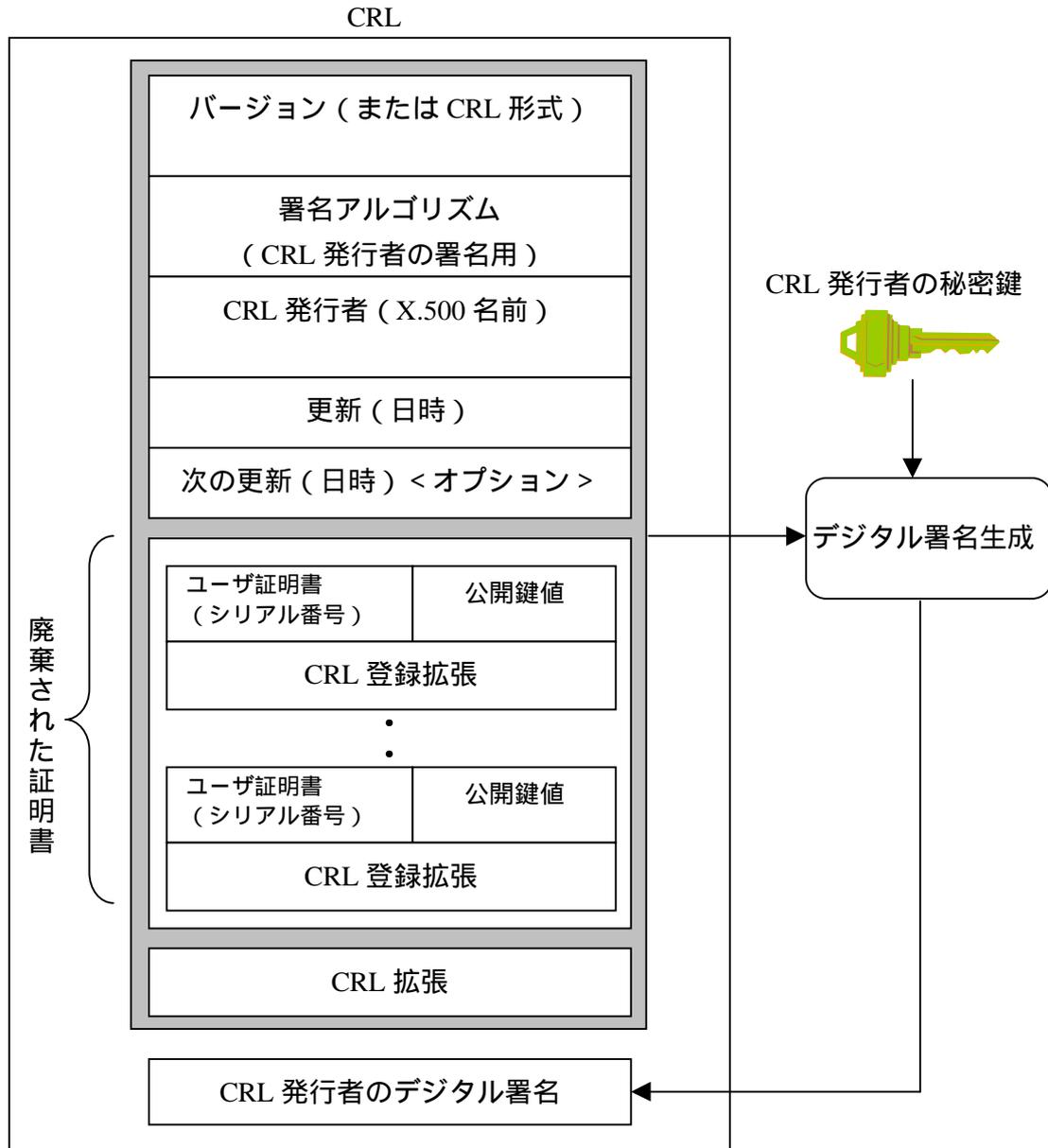
<sup>14</sup> JTC1：ISO と IEC が共同で設立した情報技術の国際標準化を担当する技術専門委員会。JTC1 では、プログラミング言語からシステム・デバイスまで、様々な技術標準を策定している。

図 6 X.509 公開鍵証明書バージョン 3 のデータ形式



また、X.509 で定められている CRL のデータ形式は図 7 のとおり。

図 7 X.509 の CRL のデータ形式



秘密通信や電子認証を行う前に、各ユーザーは、正式な相手の公開鍵証明書と正式な CRL を入手しておく必要があるが、その配布のためにオンラインディレクトリサービスと呼ばれる各種情報を整理、貯蔵するための仕組みが利用されつつある。例えば、秘密通信を行いたい場合、データの送信者は、ディレクトリと呼ばれるデータベースに対してオンライン経由で受信者の公開鍵証明書を請求し、オンライン経由で受け取ることとなる。

オンラインディレクトリサービスの標準的な形式は、ITU が X.500 として、

ISO が同内容を ISO 9594 として定めており、近年、特に大企業を中心に使用されるようになってきた。ただし、X.509 公開鍵証明書バージョン 1 及び 2 では X.500 の使用が必須とされていたが、X.500 の名称だけでは各主体をユニークに特定しきれないケースがあることや、アプリケーションによっては X.500 の名称ではなく他の名称により特定した方が便利であることから、バージョン 3 では X.500 の名称以外に、インターネットドメイン名、電子メールアドレス、ウェブサイトの URL 等を、各主体を特定するための情報として利用できるようになった。また、X.500 以外に、LDAP( Internet Lightweight Directory Access Protocol ) と呼ばれる X.500 よりもシンプルな形式のディレクトリもよく使用されている。LDAP は 1997 年末に定められたバージョン 3 が最新版である。

## ISO 15782

X.509 で定められた公開鍵証明書や CRL を利用して PKI を実現するためには、金融機関が暗号鍵や公開鍵証明書等をどのように管理していくべきかということに関して、ISO の金融専門委員会である ISO/TC68 では ISO 15782 の標準化が進められている。ISO 15782 は、PKI に関する各種証明書の管理をテーマとしており、3 つのパートに分かれている。パート 1 は公開鍵証明書の管理、パート 2 は属性証明書の管理、パート 3 は証明書の拡張、がテーマである。1999 年 7 月現在、パート 1 は 2 回目の CD 投票、パート 3 は初めての CD 投票が終わった段階であり、いずれも今後 1~2 年かけて国際標準化の手続きが進められる予定である。本標準は、(ア)金融業務に利用される CA を対象に、採用すべき高度なセキュリティ要件を具体的に規定していること、(イ)金融機関が電子認証業務を行う場合の義務と責任範囲を明確にしていること、(ウ)技術力の高い米国のベンダーが標準策定に参画していること、(エ)ISO 標準として今後国際的に利用されていく蓋然性が高いこと、等の理由から、今後大きな影響力を持つ可能性が高いと考えられる。

## (2) 米国国内標準

金融分野における国際標準は、米国国内の標準化機関である ANSI (American National Standards Institute) 配下で米国金融業界内での標準化を行っている ANSI X9 が定める各種標準から影響を受けることが多い。PKI に関して、ANSI X9 は以下のような標準を定めている。

- ・ X9.30：非可逆型<sup>15</sup>公開鍵暗号アルゴリズム（DSA、SHA-1）
- ・ X9.31：可逆型公開鍵暗号を用いたデジタル署名（RSA）
- ・ X9.55：公開鍵暗号における公開鍵証明書と CRL の拡張
- ・ X9.57：公開鍵暗号における証明書管理
- ・ X9.62：楕円曲線暗号

特に、X9.57 は、米国主要銀行や連邦準備銀行及び主要ベンダーの代表者が集まり、公開鍵証明書の管理全般について詳細に纏めたものであり、その内容は ISO/CD 15782-1 の作成時にも利用された。

この他、米国では、NIST が政府機関向けに情報処理に関する標準（FIPS: Federal Information Processing Standards）を定めており、PKI に関しては FIPS140-1 と FIPS186-1 の 2 つが主な標準である。FIPS140-1 は、秘密鍵を保管するための暗号モジュールが満たすべき条件を記述した標準として 1994 年に定められたものであり、他の多くの標準で使用されている（詳細は第 5 章を参照）。FIPS186-1 は、電子認証に用いる暗号アルゴリズムを定めている標準であり、具体的には、DSA<sup>16</sup>と RSA<sup>17</sup>の 2 つが標準アルゴリズムとして定められている。

### （3）業界標準等

標準化機関が定めた標準ではないが、業界内で標準的に参照されたり、業界団体等が作成したガイドライン等も存在する。具体的には、RSA を利用した製品の開発・販売を行っている米国 RSA Data Security 社が作成する PKCS（Public Key Cryptography Standards）、認証サービスを提供する米国 Verisign 社が作成した認証実施規定（CPS: Certification Practice Statement、詳細は第 5 章（3）を参照）、IETF（Internet Engineering Task Force）下の PKIX<sup>18</sup>（Public-Key Infrastructure<X.509>）による各種技術仕様等が頻繁に参照されている。

特に、PKIX では X.509 による公開鍵証明書を用いた PKI をインターネット上で利用するために必要な具体的な規格を多く作成し、その多くが RFC（Request For Comments）と呼ばれる標準としてインターネット上で公開さ

<sup>15</sup> 秘密通信には使用できず、電子認証のみに使用できることを指す。これに対して、両方の目的に使用できる公開鍵暗号を可逆型と呼ぶ。

<sup>16</sup> DSA：NIST によって提案されたデジタル署名用の暗号アルゴリズムであり、暗号学者の ElGamal によって 1985 年に発表された ElGamal 署名を改良したものである。

<sup>17</sup> RSA に関しては、FIPS186-1 では単に標準アルゴリズムとして認定することが記述されているのみで、内容については「ANSI X9.31 を参照」と記述されており、詳細な説明はない。

<sup>18</sup> PKIX：X.509 に基づいた PKI をインターネット上で利用するための様々な規格化を行うためのワーキンググループ。

れており、様々なプロジェクトで頻繁に参照されている。PKIX により作成されたドキュメントの例は表 3 のとおり。

表 3 PKIX で作成されたドキュメントの例

ドキュメント名	内容
Internet X.509 Public Infrastructure PKIX Roadmap	PKIX で共有されている PKI に関する基本的な考え方や PKIX で作成されたドキュメントの概要の説明。
Internet X.509 PKI Certificate and CRL Profile (RFC 2459)	X.509 バージョン 3 の公開鍵証明書とバージョン 2 の CRL の具体的なデータ構造を説明。
Internet X.509 PKI Certificate Policy and Certification Practices Framework (RFC 2527)	CA が認証サービスを提供する際のポリシーについて記述。
Internet X.509 PKI Online Certificate Status Protocol – OCSP (RFC 2560)	CRL を使用せずに公開鍵証明書の現在の状態を確認するためのプロトコルに関する説明。

ここで挙げた標準以外にも PKI に関して多くの標準が存在するが、PKI の場合には他の主体とのインターオペラビリティが重要になる機会も多いことから、実際のプロジェクトで多く使用される標準を見極め、それを採用していくことが重要であろう。

図 8 情報セキュリティ技術、PKI技術に関する国際標準化活動の鳥瞰図

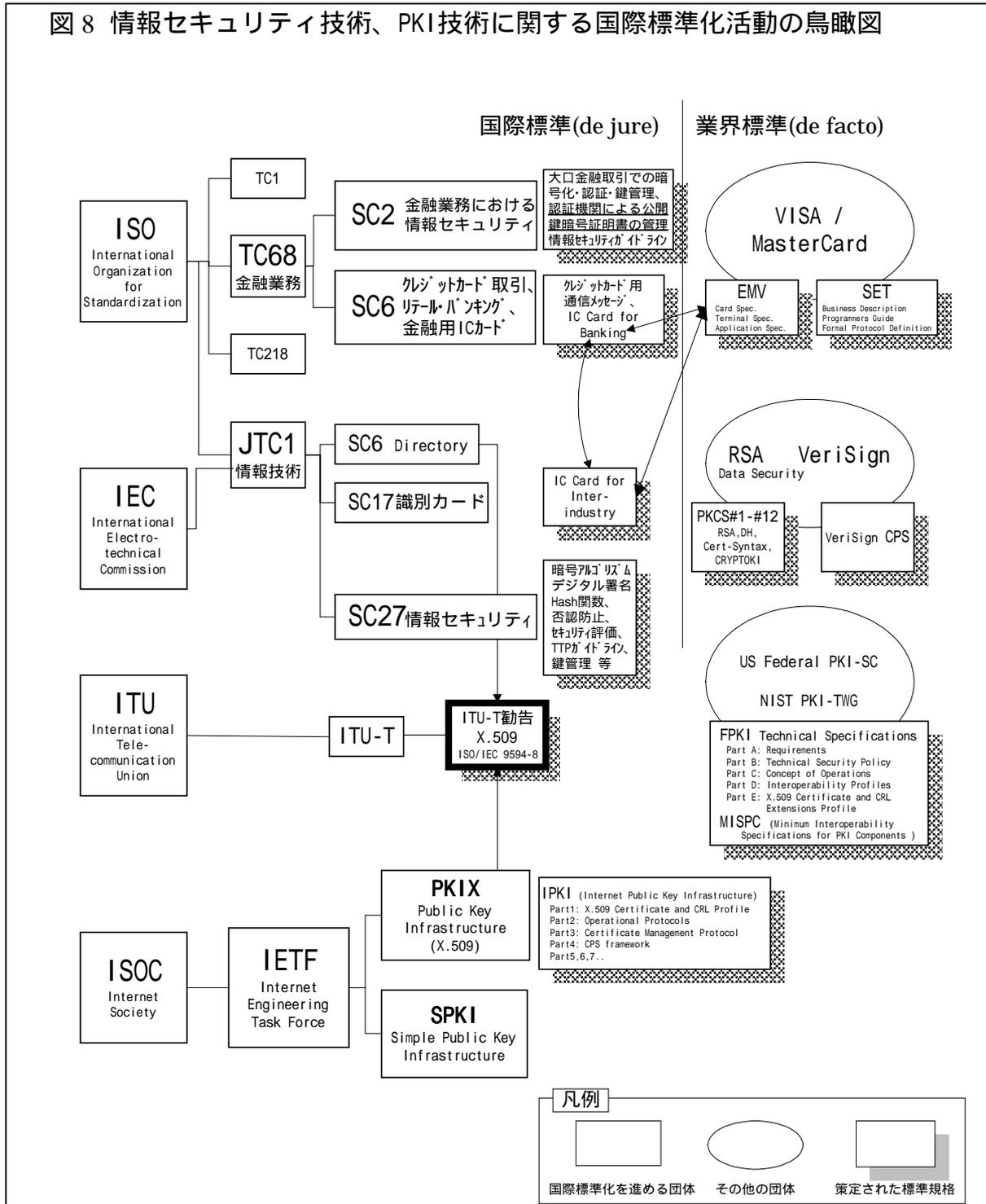


表 4 主な標準に関する具体的な PKI の対象分野

	国際標準		米国国内標準		業界標準等			
	ISO 15782 (Part 1 - 3)	ITU-T X.509 (ISO /IEC 9594-8)	ANSI X9 (各種)	FIPS (140-1, 186-1)	PKCS (#1 - 12)	Verisign CPS	PKIX (各種)	ECOM 認証局運 用ガイドライン
各主体(CA 等)の行動指針	(Part 1)		(X9.57)					
公開鍵証明書管理	鍵生成	(Part 1)					(Roadmap)	
	公開鍵証明書発行申請	(Part 1)						
	登録手続	(Part 1)					(Roadmap)	
	公開鍵証明書の発行	(Part 1)		(X9.57)			(Roadmap)	
	CA 公開鍵配布	(Part 1)		(X9.57)				
	公開鍵証明書の配布	(Part 1)						
	公開鍵証明書の使用	(Part 1)						
	公開鍵証明書の廃棄・中断	(Part 1)		(X9.57)			(Roadmap) (OCSP)	
データ構造	公開鍵証明書の更新	(Part 1)					(Roadmap)	
	公開鍵証明書申請データ	(Part 1)		(X9.57)		(PKCS#10)		
	公開鍵証明書	(Part 1)		(X9.57)			(Certificate and CRL Profile)	
	公開鍵証明書廃棄リスト	(Part 1)		(X9.57)			(Certificate and CRL Profile)	
	公開鍵証明書拡張フィールド	(Part 3)		(X9.55)		(PKCS#6)	(Certificate and CRL Profile)	
	公開鍵証明書廃棄リスト 拡張フィールド	(Part 3)		(X9.55)			(Certificate and CRL Profile)	
属性証明書	(Part 2)		(X9.57)			(Attribute Certificate Profile)		
属性証明	(Part 2)							
監査	(Part 1)							
アルゴリズム	DSA		(X9.30-1)	(FIPS 186-1)				
	RSA		(X9.31)	(FIPS 186-1)	(PKCS#1)			
組織・人事管理								
情報開示								
システム・設備要件								
秘密鍵保管用暗号モジュール のセキュリティ要件				(FIPS 140-1)				
PKI の構成(CA 間の相互関係)	(Part 1)		(X9.57)					
CPS の重要性							(Certificate Policy and CPS)	

: 記述されている。

: 簡単に記述されている。

## 5 . CA が果たす技術的役割

### ( 1 ) 各種ガイドライン等の比較

本章では、金融機関が自ら CA として認証サービスを提供する場合に果たすべき役割について、技術的な観点から検討する。検討にあたっては、既に CA 業務の安全対策について取り纏められたガイドライン等で共通的に強調されている点を取り扱うこととする（各標準の詳細な内容は表 5 を参照）。参照したガイドライン等は、ISO/CD 15782-1、Internet X.509 Public Key Infrastructure PKIX Roadmap、ECOM 認証局運用ガイドライン（1.0 版）、ベリサイン CPS バージョン 1.2 の 4 つ。

ISO/CD 15782-1 は、公開鍵証明書の管理全般について取り纏められており、具体的には、公開鍵証明書の管理のために CA や RA が果たすべき機能、公開鍵証明書のライフサイクル、公開鍵証明書の詳細な設定内容等について説明されている。

Internet X.509 Public Key Infrastructure PKIX Roadmap は、IETF が 1999 年 3 月に作成したドラフトであり、PKIX の各ドキュメントの内容を実行に移す際の留意点が記述されている、CA にとってのガイドライン的なドキュメントである。

ECOM 認証局運用ガイドライン（1.0 版）は、電子商取引実証推進協議会（ECOM）により、CA を運営するためのガイドラインとして 1998 年 3 月に作成されたものである。その内容は、鍵や公開鍵証明書の管理だけでなく、組織管理やシステム・設備の管理等多岐にわたっている。

ベリサイン CPS バージョン 1.2 は電子認証サービスを提供しているベリサイン社が 1997 年 5 月に作成したものであり、ベリサイン社及びベリサイン社以外の主体が、「ベリサインパブリック証明サービス」における CA として機能するための行動指針が纏められている。本資料は、1 企業が作成した CPS であるが、CA の運用上の注意点として広く参照されている。

これらのガイドライン等を比較検討した結果、CA 業務を行う上で最も留意すべき技術的事項は、CA の秘密鍵の保護、公開鍵証明書廃棄の周知であると考えられる。これらの点については、(2)、(3) で詳細を説明することとする。また、いくつかのガイドライン等において、CA が CPS を作成して公表することの重要性が示されており、この点について(4)で説明することとする。

表 5 CA が果たすべき技術的な役割 (主な点のみを列挙)

各種ガイドライン等 項目	ISO/CD 15782-1	Internet X.509 Public Key Infrastructure PKIX Roadmap	ECOM 認証局運用ガイドライン (1.0 版)	ペリサイン CPS バージョン 1.2
公開鍵証明書管理	<ul style="list-style-type: none"> <li>公開鍵証明書の廃棄や中断は、時刻情報を付加した(Time-stamped)CRL の配布により周知する。</li> </ul>	<ul style="list-style-type: none"> <li>X.509 では、公開鍵証明書の廃棄を周知する方法として CRL の配布を定義しており PKIX でもその概要を説明しているが、CRL を配布する方法には常に最新の廃棄情報を得られるわけではないというデメリットもあるため、PKIX では CA に対して CRL の発行を要求していない。これに代わる方法として、オンラインで公開鍵証明書の状態をチェックするための OCSP と呼ばれるプロトコルを定義している。</li> </ul>	<ul style="list-style-type: none"> <li>公開鍵証明書の作成申請があった場合、証明書に記載される公開鍵に対応した正当な秘密鍵を保有していることを確認するために、申請情報に秘密鍵でデジタル署名させるか、チャレンジデータ (申請者が予め予想できないようなデータで通常は乱数を使用) にデジタル署名の上 CA に送付させる。</li> <li>秘密鍵の危瀕や重要な認証情報の変更等で失効した公開鍵証明書は、失効リストとして生成され保管、管理される必要があると共に、正当な利用者の問い合わせに適宜応じる必要がある。</li> </ul>	<ul style="list-style-type: none"> <li>公開鍵証明書の廃棄や中断に際しては、CA は以下の方法のうちどれかで周知しなければならない。</li> <li>廃棄または中断された公開鍵証明書のリスト</li> <li>CRL (高セキュリティ用 CA&lt;Class2 及び Class3&gt;と配下の CA に対しては毎日、各 Class の取り纏め CA に対しては月 1 回更新)</li> <li>各 CA 作成 CRL の合成 CRL</li> <li>ソフトウェア業者への公開鍵証明書に關しては、廃棄情報を記したメッセージ</li> </ul>
鍵管理	<ul style="list-style-type: none"> <li>CA の秘密鍵の保管・操作は、エンドユーザーがアクセス及び制御できない暗号モジュール中で行う必要。高レベルの保護を行う場合には、秘密鍵は最低限 FIPS140-1 のレベル 3 を満たす暗号モジュールで内部的に作成 (非常に高いリスクを有するアプリケーションの場合にはレベル 4)。</li> <li>重要なシステムでは、CA の秘密鍵を分割して複数の暗号モジュールに保管し、各々の暗号モジュールでは一部の署名しか作成できないようにすることも考えられる (Fragmentation)。この場合、Shamir が 1979 年に公表した Secret Sharing の threshold scheme のように、全ての鍵が揃わなくても、ある一定数以上の鍵が揃えば元の鍵を復元できるようにすることも可能。</li> <li>秘密鍵が一つの暗号モジュールで作成・分割された場合、分割された秘密鍵は暗号化して各モジュールに移動させる。移動後は、元の秘密鍵は廃棄する。</li> <li>秘密鍵を分割している場合には、どの主体も 2 つ以上の分割鍵にアクセスできないようにする。</li> <li>バックアップ及び高スループットのための二重化以外には秘密鍵は暗号モジュールの外では存在できないようにする。</li> </ul>	<ul style="list-style-type: none"> <li>秘密鍵・公開鍵ペアの作成は、CA のポリシーに応じて、利用者の手で行うケースと、CA によって行うケースがある。後者の場合、CA から利用者への鍵の配布はファイルを暗号化して送信するか、IC カードや PC の PCMCIA カードにより物理的に渡すことにより行う。</li> </ul>	<ul style="list-style-type: none"> <li>鍵ペアや共通鍵の生成は、信頼できる暗号鍵生成システムを利用して行う必要がある。なお、暗号鍵生成システムの機能は、暗号鍵管理モジュールの内部に実装されていることが望ましい。</li> <li>暗号鍵生成システムによって生成された鍵は、複数の鍵構成要素に知識分散 (2) (を参照) することによって単独では鍵に関する秘密情報を一切知り得ないように保管するか、あるいは暗号鍵管理モジュール内に保管する必要がある。</li> <li>鍵を知識分散して保管する場合には、知識分散された鍵の情報は各鍵構成要素について、権限を有する者が個別に保管する必要がある。さらに、暗号鍵管理モジュールあるいはそれを使用するシステムは、そこから暗号鍵等の秘密情報を出力する場合に、秘密情報を複数要素に知識分散し、単独の要素だけでは元の情報の 1 ビットをも知り得ないようにするメカニズムを備えている必要がある。</li> </ul>	<ul style="list-style-type: none"> <li>ルート CA の鍵の初期サイズは 2048bit、その他 CA の鍵サイズは 1024bit である。ただし、エンドユーザー用ソフトウェアの全てが 2048bit の鍵を認識できないためにルート CA はまだ設置せず、ルート CA 配下に存在する各クラスの第一次 CA がルート CA の機能を果たしている。</li> <li>CA の秘密鍵は、基本的には「信頼性のあるハードウェア (FIPS140-1 レベル 3 を満たすもの)」上で保管することとしているが、最も信頼性の低い証明書 (クラス 1) をエンドユーザーに対して発行するための秘密鍵に限っては、「信頼性のあるソフトウェア」での保管も認めている。</li> <li>なお、CA の秘密鍵については、信頼性を高め、かつ鍵の回収を可能にするため、秘密鍵を分割して、分割された各秘密鍵を別の保有者が保有する必要がある (Secret Sharing)。</li> <li>秘密鍵の分割を行う場合、各鍵の所有者を認証するために、パスワードを付与する (Challenge Phrase)。</li> </ul>
その他	<ul style="list-style-type: none"> <li>CA の運営は、CA の CPS に沿ったものでなければならない。</li> </ul>		<ul style="list-style-type: none"> <li>CA は、CA が果たすべき義務及び公開鍵証明書を取得または利用しようとする者が果たすべき義務を定めておく必要があると共に、双方の義務を前提とする CA の責任と保証に関するポリシーを定め、開示する必要がある (CPS の公開)。</li> </ul>	

## (2) CA の秘密鍵の保護

### FIPS 140-1

(1) で説明したガイドライン等で共通的に指摘されているのは、公開鍵証明書を作成する CA の秘密鍵は電子認証の要であり、外部に漏れないようにする必要があるということである。具体的な方法はガイドライン等によって異なるが、ソフトウェアで暗号化して保管するだけでなく専用のハードウェア内で保管することを要求しているものが多い。ISO/CD<sup>19</sup> 15782-1 とペリサイン CPS バージョン 1.2 で共に指摘しているのは、米国の FIPS 140-1 Security Requirements for Cryptographic Modules においてレベル 3 以上を満たすハードウェアにより秘密鍵を保護するということである。

FIPS 140-1 は、第 4 章 (2) で触れたとおり、情報システムで重要な情報を保護するための暗号モジュールが満たすべき要件を纏めたものである。本標準では、情報の重要度を 4 つに分け、これに応じて暗号モジュールが満たすべきセキュリティレベルも 4 つに分けている。具体的には以下のとおりである。

セキュリティレベル 1：最も低いセキュリティレベルであり、他のレベルと異なるのは、必ずしも情報を保護するための専用の物理的装置を必要としないことである。暗号化機能を備えた IC カードや、パソコンで使用する暗号処理ボードやソフトウェア等が、本レベルに該当する。

セキュリティレベル 2：レベル 1 に、タンパーエビデント<sup>20</sup> なコーティングやシール等を付加することによって、暗号モジュールに侵入があった場合、それが顕現化するようになっており、物理的なセキュリティが向上したものである。また、本レベルでは、職位等に応じた認証 (role-based authentication) によりオペレーターを認証する。これにより、オペレーターが行えるサービス内容を制限する。加えて、本レベルには、TCSEC<sup>21</sup> (Trusted Computer Security Evaluation Criteria) で C2 レベル相当のオペレーティングシステム (OS) 上であれば複数ユーザーのタイムシェアシステム上でのソフトウェアによる暗

---

<sup>19</sup> CD (Committee Draft)：ISO の国際標準策定プロセスにおける委員会原案段階。ISO では、通常、NP (New work item Proposal：新業務項目提案)、WD (Working Draft：作業原案)、CD (Committee Draft：委員会原案)、DIS (Draft International Standard：国際標準案)、FDIS (Final Draft International Standard：国際標準最終案)、IS (International Standard：国際標準) というプロセスを経て国際標準が作成される。

<sup>20</sup> タンパーエビデント：侵入を受けた場合、その事実が事後的に明らかになる性質。

<sup>21</sup> TCSEC：米国国防総省が国家安全保障に関する情報の管理を目的として定めたもので、通称オレンジブックと呼ばれる。製品の検定は、米国の NCSC (National Computer Security Center) が行い、下のレベルから、D、C1、C2、B1、B2、B3、A1 と分かれている。

号化も含まれる。

セキュリティレベル 3：侵入者が暗号モジュール内のデータにアクセスできないようにしたものである。例えば、侵入が発生した場合には暗号モジュール内の重要データが消滅するものや、暗号モジュールが嚴重に管理され、アクセスが極めて困難な製品も本レベルに該当する。また、本レベルでは、レベル 2 のような職位等ではなく、個人ベースによりオペレーターの認証を行い (identity-based authentication)、オペレーターの実施可能なサービス内容を制限する。加えて本レベルでは、暗号モジュールへのアクセス等に必要となる重要な暗号鍵等に関しては厳しい制限を設けている。具体的には、重要な暗号鍵等をやり取りするデータポートは他のデータポートとは物理的に別になければならない、暗号鍵等は暗号化して入出力するか、知識分散<sup>22</sup>(split knowledge、詳細は を参照) しなければならぬ、等である。本レベルでは、重要な暗号鍵等の入出力が信頼性の高いものであれば、TCSEC で B1 レベルの信頼できる OS の下で複数ユーザーのタイムシェアシステム上でのソフトウェアによる暗号化も認められている。

セキュリティレベル 4：本レベルは最も高いセキュリティを提供する。数は少ないが、本レベルを満たす製品も存在する。本レベルでは、暗号モジュールを包む形での保護を行うことにより、どのような形でも機器への侵入があった場合にはそれを検知できるようにしている。例えば、暗号モジュールを包む保護層に対して侵入しようとした場合には、それを検知し、全ての重要な暗号鍵等をゼロにするということが挙げられる。本レベルを満たす機器は、侵入が容易な、物理的に保護されていない環境での使用に適している。本レベルでは、TCSEC で B2 レベルの信頼できる OS の下で複数ユーザーのタイムシェアシステム上でのソフトウェアによる暗号化も認められている。

FIPS140-1 対応製品の認可は、米国の NIST とカナダの CSE (Communications Security Establishment) により定められた CMV (Cryptographic Module Validation) プログラムに基づき、CMT (Cryptographic Module Testing) 機関として認められた第三者の研究所が、定められた手続きに従って実際の製品の認可を行う。1999 年 6 月 21 日時点において、NIST のホームページ (<http://csrc.nist.gov/cryptval/140-1/1401val.htm>) では、55 の暗号製品 (レベル 1 : 18、レベル 2 : 25、レベル 3 : 10、レベル 4 : 2) が FIPS140-1 対応として認定されている。

---

<sup>22</sup> 知識分散：複数の主体が暗号鍵に関する情報 (各々の情報だけでは暗号鍵を復元することは不可能) を分散して保有している状態。

## 鍵の分割

CA の秘密鍵を保護するための方法として、秘密鍵を分割して作成する分割鍵を複数の暗号モジュールで別々に管理することにより、秘密鍵の外部への漏洩または紛失により秘密鍵が失われるリスクを軽減する方法がいくつかのガイドラインで指摘されている。この場合、各々の分割鍵だけでは元の秘密鍵を復元することができず、分割鍵の保有者が本来の業務外の目的でデジタル署名を作成するためには、全てまたは一定数以上の分割鍵保有者が共謀しなければならなくなるため、より安全性が高くなると考えられる。

このような秘密鍵の分割は、FIPS 140-1 や ECOM 認証局運用ガイドラインでは知識分散 (Split Knowledge)、ISO/CD 15782-1 では Fragmentation や Secret Sharing と呼ばれており、様々な標準や文書で異なる用語が使用されている。しかし、Menezes, Oorschot, and Vanstone[1997]は、様々な秘密鍵の分割方法を表 6 のように定義している。

なお、これらの方法のうち、ISO/CD 15782-1 でも参考文献として紹介されている threshold scheme の secret sharing については、第 6 章 (2) で説明することとする。

表 6 秘密鍵の分散方法

秘密鍵の分散方法		説明
Generalized secret sharing		秘密鍵から作成した分割鍵のうち、指定されたサブセットに含まれていればどの分散鍵からも元の秘密鍵が復元可能である方法。
Threshold schemes	(k, n) threshold scheme	秘密鍵から n の分散鍵を作成し、元の秘密鍵を復元するためには k (k < n) の分散鍵が必要となる方法。
	split knowledge scheme (dual control scheme)	秘密鍵から 2 つの分散鍵を作成し、元の秘密鍵を復元するためには 2 つの分散鍵全てが必要となる方法。
	unanimous consent control	秘密鍵から t (3 以上) の分散鍵を作成し、元の秘密鍵を復元するためには t の分散鍵全てが必要となる方法。
Simple shared control schemes		

### (3) 公開鍵証明書廃棄の周知方法について

通常、セキュリティ対策の一環として、公開鍵証明書には有効期限を設定するケースが多い。したがって、有効期限経過後には公開鍵証明書を廃棄する必要がある。また、秘密鍵の漏洩、運営停止等の場合にも、公開鍵証明書を廃棄する必要がある。CA は公開鍵証明書を廃棄した後は、その事実を他の CA や RA、エンドユーザーにも周知する必要がある。周知が確実に行われなければ、古い公開鍵証明書に基づき処理が行われる可能性があるため、公開鍵証明書廃棄の確実な周知は PKI 全体のセキュリティにとって非常に重要である。

#### CRL

公開鍵証明書廃棄の周知方法として最も一般的なものは、CA が CRL を作成し、定期的に配布することである。

ISO/CD 15782-1 は、CRL に関する留意事項として以下の 3 点を指摘している。

- その完全性と発行日時を確認できるようにするため、CA が CRL を作成し、これにデジタル署名を行う。
- 仮に廃棄情報に変更がなくとも、CRL を定期的に発行する。
- 当システム配下の全主体が CRL にアクセス可能とする。

また、CRL については、そのサイズが非常に大きくなり公開鍵証明書を利用するシステムにおけるオーバーヘッドが大きくなる可能性があることや、次の CRL 発行までのタイムラグがあるために常に正しい情報が得られるわけではないこと、等が問題とされている。

CRL のサイズを抑えるためにいくつかの方法が提案されている。まず公開鍵証明書の拡張フィールドで対応する「CRL 配布点」が挙げられる。X.509 バージョン 2 の CRL では、CA が、CRL 内の廃棄証明書を任意の数に分割し、CRL を複数保有することが可能となった。分割された各 CRL は 1 つの CRL 配布点によって関連付けられているため、公開鍵証明書の利用者は、その拡張フィールドに記述されている CRL 配布点情報に基づき対応する CRL を入手し、公開鍵証明書の正当性を確認する。分割した CRL 配布点は互いに異なる廃棄理由を持つことが認められているため、名称変更等通常の廃棄用の CRL、セキュリティが搾取された公開鍵証明書を廃棄するための CRL というように CRL を複数保有することができる。したがって、セキュリティ搾取用 CRL は発行頻度を高くする一方、通常用 CRL は発行頻度を落とすことにより、CRL 全体のサイズを削減することが可能である。

また、「デルタ CRL」も CRL サイズの問題に対応するための方法のひとつである。デルタ CRL は前回の CRL の発行以降に行われた廃棄分だけのリストであり、各主体は受け取ったデルタ CRL に基づいて最新の全 CRL データベースを作成する。これにより、CRL の送信に係る負荷を軽減することができる。

#### OCSP

Internet X.509 Public Key Infrastructure PKIX Roadmap では、上記のようなオーバーヘッドが大きいことや常に最新の廃棄情報を得られないという CRL の問題点を避ける方法として、公開鍵を使用する都度、オンラインで公開鍵証明書のステータスをチェックする方法（OCSP: Online Certificate Status Protocol）も併せて紹介している。OCSP では、デジタル署名の受信者が、デジタル署名の正当性チェックを行う際に、OCSP responder と呼ばれるサーバーにアクセスして、公開鍵証明書が廃棄されていないかどうかを含めて公開鍵証明書のステータスをチェックすることとなる。したがって、ネットワーク上を行き来する CRL の情報が大きいという問題も解決できると期待される。実際、主要セキュリティ会社の CertCo、Entrust、GTE CyberTrust と大手銀行である Bank of America、Citibank、Mellon Bank、Zion's Bank が共同で行う NACHA<sup>23</sup>（National Automated Clearing House Association）の CA 相互運用性に関するパイロットプログラムでは、OCSP のテストも行い正常な稼働が確認された。

ただし、OCSP では、公開鍵証明書の正当性チェックの結果にデジタル署名が付されて送付される必要があるため、高レスポンスが期待される大規模システムでは、運用が困難となる可能性も指摘されている（Adams and Zuccherato[1998]）。OCSP は新しい技術であり実例も少ないため、今後実現に向けて様々なテストや改善等が行われていくと考えられる。

#### （４）認証ポリシー・CPS の作成

CA は、セキュリティ上の要件を満たすために配下の各主体やアプリケーションに対して公開鍵証明書をどのように応用するかということを記述した一連のルールである認証ポリシーを作成し、その組織のシステム構成や組織運営手順の中でどのように本ポリシーを具体化するかということを CPS の形で公表することが重要である。認証ポリシーは「何を」行うかということとその組織の固有の状況とは独立して一般的な形で定めたものであるのに対

---

<sup>23</sup> NACHA：米国における、紙ベースの小切手を電子化する小口決済システムである ACH（Automated Clearing）の運営主体の連合会。

して、CPS には認証ポリシーの内容を「どのように」行うかということがその組織の状況に即してより具体的に記述されているという違いがある。したがって、認証ポリシーは一組織のみに止まるのではなく、より広く使用されることが意識される場合が多く、今後その内容が類型化され、共通的な認証ポリシーが使用されるようになれば、公開鍵証明書中で示された認証ポリシーのチェックが自動的に行われるようになる可能性もある。

PKIX の RFC2527 である Chokhani and Ford [1999]では認証ポリシー及び CPS の項目案について説明しているが、これによると、認証ポリシー及び CPS では、CA や RA の義務や責任、公開鍵証明書発行前の手続内容、各主体の運用要件（テクニカル及びノンテクニカル）、公開鍵証明書及び CRL のフォーマット等を記述すべきであるとされている。

X.509 バージョン 3 形式の公開鍵証明書には認証ポリシーやこれに対応する CPS に関する情報を記述する拡張フィールドが設けられており、利用者はその内容をチェックすることにより公開鍵証明書を信頼するかどうかを見極めることとなる。X.509 内で認証ポリシーや CPS に関する情報を記述する拡張フィールドは、具体的には以下の 3 種類である。

#### Certificate Policies extension

本拡張フィールドは、CA が設定する業務の重要性に応じてその目的が多少異なる。さほど重要ではないと CA が認めた場合には<sup>24</sup>、公開鍵証明書の使用はそのポリシーが示す目的には制限されない。一方、重要であると CA が指摘した場合には、公開鍵証明書は列挙したポリシー内容に従って使用される必要がある。これは、利用者が不適切な目的や方法で公開鍵証明書を使用した場合に被った被害から CA を守る効果を有する。

#### Policy Mappings extension

本拡張フィールドは、CA の公開鍵証明書のみで使用される。前述の CA 間での相互認証において、自らのドメインの認証ポリシーが他の CA のドメインのポリシーと同等のものであることを指摘するために使用する。

#### Policy Constraints extension

本拡張フィールドは 2 つの機能を有しており、1 つは CA が認証パスの下位の全証明書内に認証ポリシーを提示させるということであり、もう 1 つは CA が認証パスの下位の CA によるポリシーマッピングを不可能とすることである。

---

<sup>24</sup> 拡張フィールド内に、重要または非重要を記述する領域が存在する（図 5 を参照）。

認証ポリシー及び CPS については、上記 X.509 や PKIX の他、ISO/CD 15782-1 でも触れられており、CA、RA、利用者等各種主体は認証ポリシー及び CPS に記述した内容にしたがって、PKI に関する様々な活動を行うこととされており、非常に重要な位置付けが与えられている。

## 6 . PKI に関する最近の技術動向

本章では、第4章で参照したようなガイドライン等では、触れられていない、または詳しく説明されていない、PKIに関する新しい要素技術について紹介することとする。新しい技術としては、(1)属性による認証(Attribute Certification)、(2)Secret Sharing Threshold Scheme、(3)Proactive Signature、(4)Public Key Validation、(5)バイオメトリックスへの対応、(6)Bridge CAを取り上げる。

### (1)属性による認証(Attribute Certification)

公開鍵証明書では、取引相手が正当な本人であることは確認できるが、その本人が有している属性情報(企業内での役職や権限等)を利用するアプリケーションには適していない。公開鍵証明書の拡張フィールドに属性を記述することもできるが、この場合、属性は公開鍵に比べて変更される頻度が高いため、公開鍵証明書の廃棄、再発行を頻繁に行う必要が生じるほか、当該属性情報を使用しないアプリケーションもそのためにサイズが大きくなった公開鍵証明書を使用しなければならないというデメリットもある。これらの問題点を解決するために、本人の真正性確認は公開鍵証明書が行い、AAが公開鍵証明書にリンクづけられた属性証明書(Attribute Certificate)を発行し、この権限情報をアプリケーションで使用するという方法が実用化されつつある。属性による認証は、実際のプロジェクトで使用されているケースは少ないが、今後その利用が広がることが予想されており、ISO/WD 15782-2等各種標準において対応が進みつつある。

### (2)Secret Sharing Threshold Scheme

第5章(2)で説明したとおり、CAの秘密鍵はPKIの根幹であるため、秘密鍵の外部への漏洩または紛失により秘密鍵が失われるリスクを軽減するために、秘密鍵を分割・管理する方法が考案されている。しかし、分割する鍵の数が増えるほど紛失等により全ての分割鍵(Share)が揃わない危険性が増大するため、Threshold Schemeと呼ばれる、全ての分割鍵が揃わなくてもある一定数以上の分割鍵が揃えば元の秘密鍵を復元できるようにする方法が存在する。

Secret Sharingは、秘密鍵を1箇所に保管する際のリスク(コンピュータのダウン、パスワードの忘失等)を避けるために、元の秘密鍵からいくつか( $n$ 個)の分割鍵(Shares)を作成し、これらを複数人で管理する方法である。元の秘密鍵を復元するためにはこれらの分割鍵が一定数( $k$ 個)以上揃う必要があり、 $k-1$ 以下しか揃わなければ元の暗号鍵を得ることができないため、

電子署名や秘密データの復号化を行うことはできない。このように  $k$  という数字が秘密鍵を復元するためのしきい値 (Threshold) となっているため、 $(k, n)$  threshold scheme と呼ばれている。Secret Sharing Threshold Scheme における具体的な分散鍵の作成、秘密鍵の復元方法については、補論 1 を参照。

なお、Threshold Scheme を発展させた定期的に分割鍵を自動変更する Proactive Signature という方法も考案されている。

### ( 3 ) Proactive Signature

第 4 章では、CA の運営にとって秘密鍵の安全を確保することは最重要課題であり、その実現方法をいくつか説明したが、基本的には侵入者が秘密鍵にアクセスできないようにするという方法が中心であった。米国及びイスラエルの IBM 研究所で考案された技術である Proactive Security を応用した Proactive Signature は、侵入者に秘密鍵の入手を困難にするという対策を行いながら、同時に、頻繁に鍵情報を自動変更することにより安全性を高めるという方法である ( Proactive Security に関する詳細は補論 2 を参照 ) 。

具体的には、秘密鍵を複数のサーバー上に分割させた上で ( あるしきい値以上の数の分散鍵が揃わなければデジタル署名の作成は不可能 )、分割鍵を定期的に自動更新することにより、仮にいくつかの分割された秘密鍵が侵入者に漏れたとしても、その秘密鍵を長期間使用できないようにしている。この場合、定期的に変更するのは分割鍵だけであり、元の秘密鍵は変更しないままとすることにより、エンドユーザーに公開鍵証明書を配布し直す手間を省いている。また、Proactive Signature では、デジタル署名の作成時にある場所で元の秘密鍵を復元せずに署名を作成することにより、秘密鍵が漏洩することを防いでいる。

### ( 4 ) Public Key Validation

本技術は ISO/CD 15782-1 で若干触れられているが、公開鍵が、使用する暗号アルゴリズムにとって正しい形式を満たしているかどうかということ、数学的にチェックするための方法である。これにより、秘密鍵と公開鍵ペアの作成者が正しい鍵を作成できたかどうか、また、Secret Sharing のような正当な秘密鍵を誰も知らない場合に鍵ペアが正しく生成されているのか等をチェックする他に、攻撃者の自由度を極力低くするというセキュリティ上の目的がある。

Public Key Validation は、公開鍵の候補さえ保有していればオフラインで誰でも行えるのが望ましいが、RSA に対して Key Validation を行おうとする

と、秘密鍵の保有者が質問に答える形で秘密鍵に関する何らかの情報を提供する必要があるため、オンラインの形態で行わなければならないことが判っている。

また、ISO/CD 15782-1 の作成過程では、CA が公開鍵証明書を発行するには、対象公開鍵の Public Key Validation を行う必要性を記述することが検討されたが、現時点では公開鍵に対応する秘密鍵の保有を証明する一つの方法として紹介するに止まっている。

#### ( 5 ) バイオメトリックスへの対応

電子認証においては、IC カードまたはパソコンのソフトウェア内の秘密鍵は正当な本人が保有していることを前提としているが、これを確認する方法としては暗証番号・パスワードの入力が主流である。しかし、銀行のキャッシュカードの暗証番号の多くには誕生日や電話番号が使用されているという指摘もあるため、暗証番号・パスワードは他者に漏れる心配がある。このため、指紋、網膜、虹彩、声紋、筆跡等身体的特徴を用いて暗証番号・パスワードを代替・補完することにより、秘密鍵に紐付けられた正当な本人であることを確認しようとする検討が現在行われている。例えば ISO では、昨今、識別カードの国際標準化を担当している、ISO/IEC JTC1 の分科委員会である SC17 において、IC カード内に格納した音声データを利用してカード利用者の個人認証を行うための仕組みを標準化しようという提案がフランスより提出され、賛成多数で標準化が進められることが決定した。

#### ( 6 ) Bridge CA

FPKI において検討されている概念であり、複数の官庁や政府外の企業による CA ( 及び配下の CA やユーザー ) 間で信頼性の高いコミュニケーションを行うために、CA 間において認証パスを繋げる目的で機能する特別な CA である。これにより、各 CA が互いに相互認証を行うよりは、より単純・効率的に、バラバラに存在する官庁等の CA を接続<sup>25</sup>して大きな一つの FPKI として構築することが可能となる。Bridge CA は、FPKI 全体のポリシー管理機関 ( FPMA: Federal Policy Management Authority ) によって運営される。

また、Bridge CA は、複数の暗号アルゴリズムによる公開鍵が使用されている PKI において、暗号アルゴリズムを使用しているユーザー間で公開鍵の正当性を確認できるようにする役割を果たす場合がある。

---

<sup>25</sup>一定の技術標準や業務要件の充足を条件に、全ての官庁等の CA が Bridge CA と相互認証することによって、Bridge CA が官庁等の CA の間でハブとして機能することが想定されている。

## 7. 結び

本稿で見てきたように、PKI・電子認証は確実性が求められる金融取引をインターネット上で行うことを可能とし、ひいては、金融業界のあり方や金融機関の経営に大きな影響を与える可能性がある。PKI・電子認証関連サービスの提供には様々なオプションがあるため、各金融機関は、PKI・電子認証について理解を深めながら、どのように PKI・電子認証関連サービスと関わっていくかというポリシーを固めていく必要がある。

いくつかのオプションの中でも、金融機関自らが CA として認証業務を行うという対応をとる場合には、暗号等情報セキュリティや大規模な分散処理型システムの運用ノウハウ等、これまで経験が蓄積されているオンラインシステムの場合とは異なった技術力が要求される可能性が高い。特に、第5章で検討した CA の秘密鍵の保護や公開鍵証明書廃棄の周知等については、正しく行われなかった場合の影響が大きいいため、その技術動向を十分フォローしていく必要がある。

以 上

## 【補論 1】 Secret Sharing の Threshold Scheme について

CA の秘密鍵については、変更時の負担が大きいため、事故等によって紛失してしまうことを防ぐために、そのバックアップを取りたいというニーズがある。一方で、秘密鍵は PKI の要であり、FIPS140-1 で認められた特別なセキュリティ対策を施した媒体に保存したとしても、バックアップを取り複数の秘密鍵を作成することは秘密鍵が漏洩するリスクを増大させてしまうため、セキュリティ上問題がある（勿論、必要に応じて各分割鍵を FIPS140-1 で認められた媒体に保存することとなる）。この問題を解決するために、単純に秘密鍵のバックアップを取るのではなく、秘密鍵を複数に分割し、各々の分割鍵を別々に管理する方法が考えられている。この場合、1 つの分割鍵からは元の秘密鍵を復元することは不可能である。このような方法は一般に Secret Sharing と呼ばれる。但し、全ての分割鍵が揃わなければ元の秘密鍵が復元できないというリスクがあるため、このリスクに対応する方法として Threshold Scheme と呼ばれる Secret Sharing の一方法がある。これは、秘密鍵から  $n$  個の分散鍵を作成しても、元の秘密鍵を復元するためにはそのうち  $k$  個 ( $k < n$ ) の分散鍵で十分であり<sup>26</sup>、デジタル署名の作成を行うためには必ずしも全ての分散鍵が揃う必要がないというものである。具体的な Threshold Scheme の実現方法としては、1979 年に暗号学者の Shamir が考案したものが有名であり、多項式の補間(polynomial interpolation)に基づき、 $k-1$  次の多項式は  $k$  個の点が判れば特定できるという性質を利用して鍵の分割を実現している。

秘密鍵である正の整数  $S$  を  $n$  人に分割する方法及び  $k$  個の分割鍵から秘密鍵  $S$  を復元する方法は以下のとおり。

### 秘密鍵の分割方法

$p > \max(S, n)$  である素数  $p$  を選択する。

$a_0 = S$  とする。

$k-1$  個の独立した係数  $a_1, \dots, a_{k-1}$  ( $0 \leq a_j \leq p-1$ ) をランダムに選択する。

上記により、多項式  $f(x) = \sum_{j=0}^{k-1} a_j x^j$  を定義する。

分割鍵は  $S_i = f(i) \bmod p$  ( $1 \leq i \leq n$ ) により計算される。分割鍵  $S_i$  を各々、分割鍵管理者  $P_i$  に対して  $i$  という情報と共に安全に引き渡すことにより、分割鍵の生成、配布が完了する。

---

<sup>26</sup> したがって、 $(k, n)$  threshold scheme とも呼ばれる。

### 秘密鍵の復元方法

$k$  個の分割鍵が入手できたため、 $k$  個の座標点  $(i, S_i)$  が集まることとなる。そもそも、 $k$  個の座標点  $(x_i, y_i)$  ( $1 \leq i \leq k$ ) で表わされる最大  $k$  次の多項式  $f(x)$

は、ラグランジュ補間方程式により  $f(x) = \sum_{i=1}^k y_i \prod_{1 \leq j \leq k, j \neq i} \frac{x - x_j}{x_i - x_j}$  と表わされる。

この場合、秘密鍵を生成した際の多項式  $f(x)$  は  $f(0) = a_0 = S$  であるため秘密

鍵  $S$  は  $S = f(0) = \sum_{i=1}^k c_i y_i$ , where  $c_j = \prod_{1 \leq j \leq k, j \neq i} \frac{x_j}{x_j - x_i}$  と表わされる。ここで、入手

した分割鍵  $(x_i, y_i) = (i, S_i)$  ( $1 \leq i \leq k$ ) から秘密鍵  $S$  を復元することが可能である。

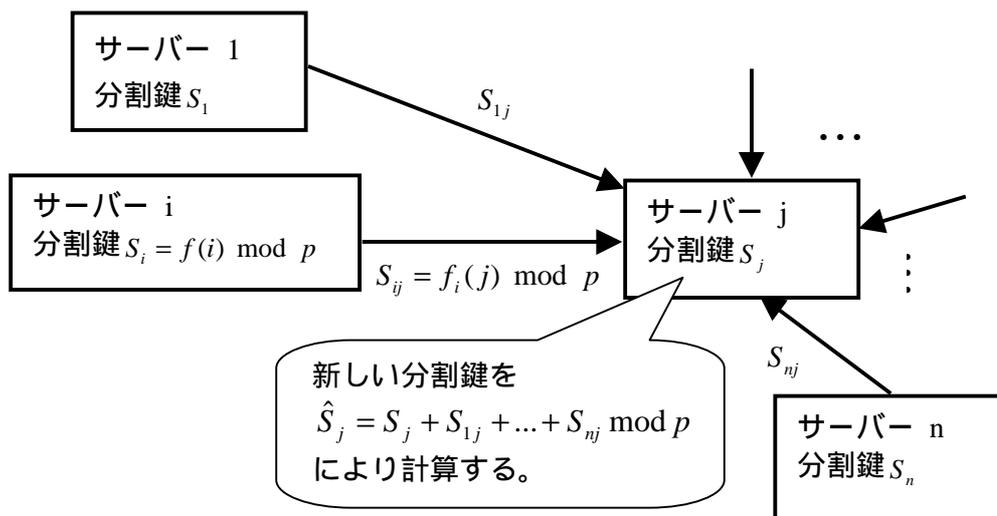
## 【補論 2】 Proactive Security について

Proactive Security は米国とイスラエルの IBM 研究所で考案されたコンピュータシステムのセキュリティを確保するための手法である。Proactive Security は、長期間にわたる攻撃から資源を保護するための方法であり、

$$Proactive = Distributed + Refresh$$

で表わされるように、複数のサーバーに秘密鍵に関する情報を分配した上で (Distributed)、それらを定期的に自動変更することにより (Refresh)、仮に複数のサーバーに対して侵入されたとしても、その場合の損失を短期間に抑えようとするものである。例えば、電子メールのパスワードを定期的に変更することも Proactive Security と類似の対応であり、Proactive Security ではセキュリティに関する情報の変更を自動で行おうとするものである。

図 Proactive Security における分割鍵の更新



分割鍵は、補論 1 で説明した Shamir の Secret Sharing により補間多項式を利用して作成し、各サーバーに分配するため (サーバー  $i$  が保有する分割鍵  $S_i$  は  $S_i = f(i) \bmod p$ )、ここでの説明は省略する。

分割鍵の定期的な更新は、以下の手順により行う (図参照)。

分割鍵を保有している各サーバーは、 $f_i(0) = 0$  を満たす  $k$  次の多項式  $f_i(x)$  を適当に選択する。

上記 で選択した多項式  $f_i(x)$  を利用して、各サーバーは他のサーバーに対して分割鍵を更新するための情報を送信する。ここで、サーバー  $i$  がサーバー  $j$  に対して送信する情報は  $S_{ij} = f_i(j) \bmod p$  である。

サーバー  $j$  は、元の分割鍵  $S_j$  と上記 で他のサーバーから受け取った情報

を元に、新しい分割鍵  $\hat{S}_j$  を  $\hat{S}_j = S_j + S_{1j} + \dots + S_{nj} \bmod p$  により計算する。その際、元の分割鍵は廃棄する。この場合、新しい分割鍵  $\hat{S}_j$  は多項式  $\hat{f}(x) = f(x) + f_1(x) + \dots + f_n(x)$  上にあるが、 $\hat{f}(x)$  は  $f(x)$  と同様に  $k$  次で、その定数項は  $S$  であるため ( $a_0 = S$ )、上記処理により分配鍵は更新されたものの秘密鍵自体は変更されていないことがわかる。

したがって、Proactive Security では、秘密鍵自体は変更しないまま、複数サーバーが連携することにより、分割鍵を自動的にかつ定期的に変更することが可能となる。

なお、上記の方法は、入手した情報を読み取るだけの受動的な攻撃者に対してのみ有効であり、情報を変更したり、サーバーの設定を変更する能動的な攻撃者には無効である。このような攻撃者に対しては、Feldman が考案した Verifiable Secret Sharing (VSS)を利用することが有効であると考えられている。

Proactive Security の応用分野としては、Proactive Signatures と Proactive Secure Communication の 2 つが考えられている。

### Proactive Signatures

単なる Secret Sharing の Threshold Scheme では、鍵を分散保管していても、電子署名を行う際にはある 1 ヶ所で秘密鍵を復元する必要があるため、その際に侵入者が秘密鍵を入手するチャンスが生じる。これに対して Proactive Signatures は、秘密鍵を 1 つの場所で復元することなく、分散鍵を保有する複数のサーバーが共同でデジタル署名を作成する方式であり、侵入者が秘密鍵を入手できるチャンスを少なくすることにより、より安全にデジタル署名を作成しようとするものである。

また、Proactive Signatures 用のサーバーに対して侵入することにより第三者がデジタル署名を作成しようとしても、予め決められた数以上のサーバーに対して次の分散鍵更新までの限られた期間に侵入しなければならないため、単なる Secret Sharing の Threshold Scheme に比して安全性が高められていると考えられる。

### Proactive Secure Communication

通常、通信データを暗号化する場合、データの暗号化を行う Session 鍵は割合頻繁に定期的な変更を行うのに対して、Session 鍵の送受信を行うための Master 鍵は非常に重要であるものの、これをネットワーク上で送信することにはリスクが伴うことから、頻繁に変更しないケースが多い。

現在、Master 鍵の変更時には相手の公開鍵で暗号化して送信することが多いが、その公開鍵の交換時に不正が起こる可能性があるため、Proactive Signature により複数の分配鍵保有者が共同でその公開鍵に対してデジタル署名を行うことにより、正当な公開鍵が使用されるようにすることが考えられている。

## 【参考文献】

- ・岩下・谷田部、「金融分野における情報セキュリティ技術の国際標準化動向」、金融研究第 18 巻第 2 号、日本銀行金融研究所、1999 年
- ・宇根・岡本、「公開鍵暗号の理論研究における最近の動向」、金融研究第 18 巻第 2 号、日本銀行金融研究所、1999 年
- ・大蔵省銀行局・国際金融局（事務局）、「電子マネー及び電子決済に関する研究会報告書」、1997 年
- ・電子商取引実証推進協議会（ECOM）、「『認証局運用ガイドライン（1.0 版）』」、1997 年
- ・電子商取引実証推進協議会（ECOM）、「『電子公証システムガイドライン（Ver.1.0）』」、1998 年
- ・日経デジタルマネーシステム、「『電子商取引のセキュリティ技術』」、1998 年
- ・宮田、「証券取引の STP 化を巡る動きについて」、日本銀行金融研究所 ディスカッションペーパーシリーズ、No. 99-J-29、1999 年
- ・Aberdeen Group, “Evaluating the Cost of Ownership for Digital Certificate Projects”, *White Paper*, 1998
- ・C. Adams and R. Zuccherato, “A General, Flexible Approach to Certificate Revocation”, <http://www.entrust.com>, 1998
- ・American National Standards Institute, "X9.57-1997, Public Key Cryptography for the Financial Services Industry: Certificate Management", 1997
- ・A. Arsenault and S. Turner, “Internet X.509 Public Key Infrastructure PKIX Roadmap”, Internet Draft, 1999
- ・M. Branchaud, “Internet Public Key Infrastructure Caching the Online Certificate Status Protocol”, Internet Draft, 1998
- ・W. Burr, “Public Key Infrastructure (PKI) Technical Specifications: Part A – Technical Concept of Operations”, Working Draft, 1998
- ・———, “Multiple Algorithms and the Bridge CA Concept”, Working Draft, 1998
- ・R. Canetti, R. Gennaro, A. Herzberg, and D. Naor, “Proactive Security: Long-term protection against break-ins”, *CryptoBytes* RSA Laboratories Newsletter, 1997
- ・S. Chokhani and W. Ford, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, RFC2527, 1999
- ・S. Farrell and R. Housley, “An Internet AttributeCertificate Profile for Authorization”, Internet Draft, 1999

- W. Ford and M. Baum, 『デジタル署名と暗号技術』(山田慎一郎訳、日本ペリサイン株式会社監修), プレンティスホール出版, 1997年
- Forrester Research, "Money & Technology Strategies", *The Forrester Report*, Volume Three, Number Seven, 1998
- Giga Information Group, "A Total Economic Impact Analysis of Two PKI Vendors: Entrust and Verisign", 1998
- R. Housley, W. Ford, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, 1999
- International Organization for Standardization, "ISO/CD 15782-1 Banking Certificate Management Part 1: Public Key Certificates", 1998
- , "ISO/WD 15782-2 Banking Certificate Management Part 2: Attribute Certificates", 1997
- , "ISO/DIS 15782-3 Banking Certificate Management Part 3: Certificate Extensions", 1999
- ITU-T, ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1997
- A. Menzes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, 1997
- National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules", FIPS PUB 140-1, 1994
- , "Digital Signature Standard (DSS)", FIPS PUB 186-1, 1998
- RSA Laboratories, PKCS #1: RSA Encryption Standard Version 1.5, 1993
- , PKCS #6: Extended-Certificate Syntax Standard Version 1.5, 1993
- , PKCS #10: Certification Request Syntax Standard Version 1.0, 1993
- A. Shamir, "How to Share a Secret", *Communications of the ACM*, 1979
- L. Stein, 『Web セキュリティガイド』(株式会社クイック訳), アスキー, 1998年
- Verisign, Certification Practice Statement Version 1.2, 1997