Ｈ１１－認証・公証ＷＧ－３

認証局の責任に関する提言

平成１２年３月

電子商取引実証推進協議会
認証・公証ＷＧ

はじめに

背景

インターネットを利用した電子商取引は、昨年から大きな進展を見せ始めている。それは、規模の大小を問わず情報サービスプロバイダーが、経営資源をこの分野にシフトさせていることや銀行、商社、流通業等が業態をこえて新しいサービスに向けた提携を開始したこと等からも伺うことが出来る。又、一般消費者や企業も多様な情報の入手や利便性の向上や商品販売、調達コストの低減等が身近になりつつあるという電子商取引利用に対する意識変化も見られるようになった。

一方、このような事業改革や意識変化により電子商取引が拡大するにつれて、事故や犯罪も増加傾向にあることも否定できない事実である。インターネットの向こうにある今まで行ったこともなければ見たこともない店や店員から商品を購入する際に、前払いをしたりクレジットカード番号を教えたりして被害に遭うケースが繰り返されている。顔見知りの相手ならばいざ知らず、ネットワークの向こうにいる相手に対しては、例え名の通った店であろうと詐称の可能性がある限り、相手を確認する即ち認証する行為の重要性が再認識されている。

電子商取引実証推進協議会（ＥＣＯＭ）では、電子商取引における相手確認の重要性を設立当初から重視しており、本人認証技術、認証局運用等認証に関する研究を行い、評価基準やガイドラインを作成、公開してきた。特に、認証局については「認証局運用ガイドライン」として、利用者に信頼される認証局に必要な技術および運用に関する要件を取りまとめ、国内のみならず海外にも公開し認証サービスの普及に些細ではあるが、幾ばくかの貢献をしてきた。

しかし、認証局が如何に完璧な認証実施規定（ＣＰＳ）を用意していても、災害やミスや内外部の不正による事故から無縁であることはない。秘密鍵が盗難に遭うかもしれないし、システム障害で業務が停止するかもしれないし、事故が発生しそれにより認証書の利用者が何らかの被害を被る可能性は、人が設備やシステムを開発し使用する限り考慮しておく必要がある。一方、認証局が発行した認証書の利用者としても、自分の秘密鍵の管理に起因した盗難もしくは漏洩事故に遭遇する可能性もあるし、送られてきた認証書が失効されていたために事故に遭うこともあるかもしれない。

このような事故に対し、認証局としては事故防止策やコンテンジェンシー計画の準備、訓練が行われなければならないことは言うまでもないが、認証サービスが緒についたばか

りであり技術の完成度や登場する多くの当事者や知識の習熟度等を考慮すると、認証局、利用者、認証シムテムベンダー等の当事者がそれぞれの役割、義務、責任を認識した上で認証サービスを提供、利用することが重要であると考え、ＥＣＯＭとして本報告書を作成することにした。ＥＣＯＭがこうした考えに則り本報告書の検討に入った時点で、ＩＬＰＦ（Internet Law and Policy Forum）やＡＢＡ（American Bankers Association）が認証局の役割や責務の分析を行っていたり、ＥＵ指令等が法制度として認証局の責任について触れていたり時宜に適ったものであるとの認識にもある。

取り組みと構成

本報告書の作成にあたって、先ず認証局を中心として認証サービスに関連する当事者が取り扱う情報（この中には公開鍵、秘密鍵等の可視的ではないが義務や責任を検討する上で重要な情報を含む）について、それらの生成から廃棄に至る全プロセスに対し機密性、完全性、可用性の観点から想定される個々の事故について、事故の原因および被害を分析した。

次に、事故の原因と被害の大きさを考慮して責任の所在を検討したが、その際に基本的な考え方として認証局に対しては過失責任の立場を採用している。その理由は、消費者保護の観点から無過失責任であるべきだとの考え方もあるが、背景で記述したような状況にある電子商取引の環境において認証局に過度の責任を持たせることは、認証ビジネスの芽を積むばかりでなく認証そのものが定着しない恐れがあるからである。

又、本報告書においてはＰＫＩの適用を前提においているが、認証のモデルとしてはクローズドモデルとオープンモデルの双方を対象にしている。クローズドモデルでは、エンドエンティティが認証書加入者と認証書依存者の両方の役割を担い、且つ認証サービス事業者と約款等により責任、賠償等について契約関係にあるケースがほとんどであるが、消費者保護等の観点から整理が必要であると考えたからである。一方、オープンモデルのケースはほとんどビジネス事例がなく検討に苦労した。特に、認証書依存者は事前に認証局との間で契約関係にないため、双方の責任についてどのような合意を取れば良いのかが問題である。本報告書においては、依存規約（リライイングパーティアグリーメント）を有効にすべきであるとの考え方に立っているが、認証書の検証方法についても技術的手段が確立されていない現状において、検討の余地が残されているところであろう。

本報告書の構成は以下の通りであり、読者は自分の興味に応じて章を選ぶことが可能である。

１章：認証局の役割と機能

先ず、ＰＫＩサービスと認証局の機能について説明しているが、知識を持たれている人は以降の認証書の利用形態と認証局の置かれている立場と役割から読まれることを薦める。

２章：認証局の責任に関する基本的考え方

責任に触れる前に、認証局および認証書加入者、依存者等の関連者の果たすべき義務について説明している。認証局の責任については、過失責任の原則に立ち不法行為責任と債務不履行責任が問われるべきであるとしている。又、認証書依存者に対する責任は依存規約が有効であり、それを明確に依存者に提示すべきであるとしている。

更に、本章においては消費者保護と個人情報保護についても触れている。

３章：認証局と利用者の責任分担

本章では、先に述べた認証局および認証サービス関連当事者の取り扱うデータに起因して想定される事故、原因、被害の分析結果を報告し、その内の主な事故について認証局および利用者にどのような責任が生じるかについて記述した。事故の状況、原因の条件等詳細に触れることが難しく、今後の実例の積み重ねにより議論が発展して行くことが予想される。

４章：責任リスクの管理

認証局が責任リスクを管理するにあたって、本章では対象相手として認証書加入者、依存者および認証書発行委託先としてのＩＡ（Issuing Authority）を選び、対象相手毎にどのような対応を取れば良いかについて記述している。特に、消費者保護の観点におけるリスク管理については、その重要性を考慮し節を分けて記述している。又、認証局の責任について、ＣＰＳおよび認証書フォーマットでどの様に触れたら良いのかについても本章で記述している。

５章：損害賠償への対応について

損害賠償への対応方法として、責任限度額の設定、財務基盤の組込み、損害保険の加入の３つを取り上げ、それぞれの考え方について記述した。特に、損害保険の加入については、今後認証が電子商取引のインフラとして社会に定着していくために、保険が重要な役割を占めるとの観点から、保険金の支払限度、補償範囲、会社の選定、保険商品のあり方について記述した。

６章：付録

本章は、1997 年の 4 月にＩＬＰＦワーキンググループによりドラフトされた、「消費者取引における認証局の役割」をＩＬＰＦの好意を得て翻訳したものを掲載すると共に、その他本報告書を作成するにあたって参考にした内外の文献一覧、および検討メンバーリストを付けている。

今後の対応

当初、本報告書は電子商取引サービス事業者を含む民間の認証局に対する自主的なルールであるガイドラインとして取りまとめる計画であったが、上で述べたようなアプローチにより検討を重ねていくにつれて、事故の事例が乏しい中での（幸いなことではあるが）想定事故と被害、原因の分析を踏まえた責任所在の特定化に机上検討色が強すぎる懸念が生じてきた。勿論、認証のような新しいサービスについて、制度、技術、運用等の仕組みを構築して行くに際しては、先ず論理的な検討から入ることになる訳であり、ましてや認証サービス事業者や利用者を巻き込んだ実際のフィールドテストが困難であることを考慮すると止むを得ない面があるが、もう少し現実に即したシミュレーションが必要であろう。

更に、オープンモデルのように認証書の有効性確認が技術的な点からも依存規約のような運用面からも方式が確立されていない状況や、認証書加入者の秘密鍵管理も技術面や運用面で落ち着いてない状況があり、必ずしも責任を加入者や依存者に負わせることにはならない等個別課題がまだ多いと思われる。

従って、こうした課題を浮き彫りに出来たことは有益ではあったが、当初の目論見とは異なり認証サービス事業者や利用者に対する提言として取りまとめて公開することにした。

今後、事業者や利用者更には法律専門家、関連諸団体等から幅広くご意見を頂き、より実効的なものにして行きたいと考えておりますので、忌憚のないご意見等を下記までお寄せ願います。

電子商取引実証推進協議会(ECOM)
認証・公証ワーキンググループ
〒135-8073 **東京都江東区青海** 2-45 **タイム** 24 **ビル** 10 **階**
TEL：(03)5531-0061　FAX：(03)5531-0068
E-mail：info@ecom.or.jp
http://www.ecom.or.jp

目次

1.認証局の機能と役割

1.1　ＰＫＩサービスと認証局の機能

1.1.1 公開鍵基盤の概要

公開鍵基盤(ＰＫＩ：Public Key Infrastructure)は、電子商取引をはじめとして、情報処理システムのセキュリティやコミュニケーションシステムの信頼性を確保する上で必要となる様々なサービスのインフラストラクチャーとなるものである。

本書でいう認証書は、少なくとも利用者の名前と公開鍵(ビット列)を情報として含むデジタル文書で、認証局のデジタル署名を付したものを言う。従って認証をより正確に表現するならば公開鍵認証ということになる。

以下ではＰＫＩを構成するサービスについて概観する。

(1)　暗号サービス

ＰＫＩで利用される基本的な機能・技術として以下のものがある。

① 鍵ペアの生成・保管

公開鍵/秘密鍵のペアを生成するとともに､秘密鍵はパスワード等で保護されたファイルやＩＣカード等のハードウェア/ソフトウェアのモジュールに保存して他人に知られないように保管する機能。なお、鍵の用途として主に以下のものが挙げられる。

- デジタル署名
- 通信データ秘匿用共通鍵の暗号化
- 否認防止など。

② デジタル署名の生成

メッセージダイジェストを生成し、デジタル署名する機能。

③ デジタル署名の検証

メッセージとそれに対するデジタル署名が署名者のものであるかどうかを検証する機能。

④ 通信データ秘匿用共通鍵の生成･配布

通信文を暗号化するための共通鍵を生成し、それを相手に配布するための機能。

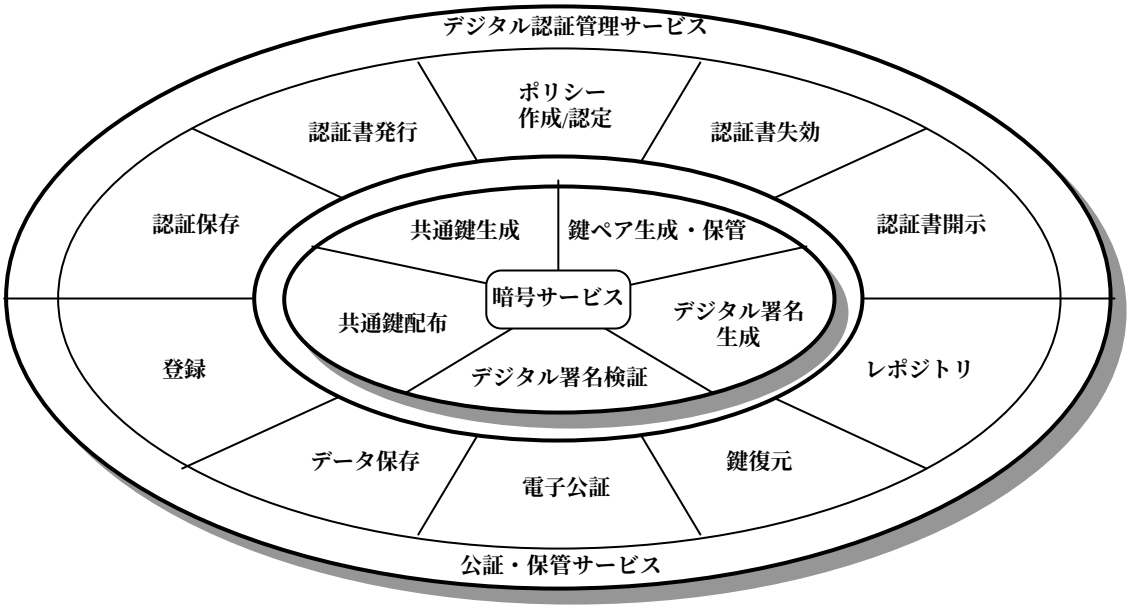


図 1-1 公開鍵基盤の構成

(2)　認証書管理サービス

ＰＫＩの中で核となる認証書の管理に関する以下のサービスであり、主として認証局によって提供されるものである。

① 認証書の発行(Certificate Issuance)

個人や法人等の加入者に対して認証書を発行する。発行する認証書には、階層構造の下位に位置する下位認証局(subordinate CA)、相互認証における相手の認証局等に対するものも含まれる。

② 認証書の失効(Certificate Revocation)

被認証者は、認証書に含まれる公開鍵と対になった秘密鍵をなくしたり、盗まれたり、あるいは解読されたりした場合、またはその可能性がある場合には、その認証書を無効にする必要がある。認証局は被認証者の確認を取った上で、認証書失効リスト(Certificate Revocation List: 失効リスト)等によって、失効情報を利用者等の関係者に知らせる。又、最近では、ＩＥＴＦ（Internet Engineering Task Force）によって失効リストを要求することをせずに、認証書の最新状況を問い合わせることを可能にするプロトコル（Online Certificate Status Protocol）が提唱されている。

失効の一種に一時失効(Certificate Suspension)がある。これは、ある期間だけ失効させるものであり、一時失効の期間が過ぎれば、通常自動的に失効は解除される。

一時失効は、漏洩等の可能性がある場合や、不在の場合等に利用される。

③ 認証書の開示(Certificate Publish)

発行済みの認証書を他の人が入手できるようにするため、レポジトリ(X.500 仕様のものやそれ以外のレポジトリなど)に登録する 。レポジトリは認証局が管理する場合もあるし、認証局以外の第三者が管理する場合もある。

なお、そのようなレポジトリとしては種々のアクセス制限の機能が用意され、プライバシーを守りたい場合には不特定多数に公開しないようになっているものもある。

④ 認証書の保存(Certificate Archiving)

発行済みの認証書や失効リスト等を長期にわたって保管する。これは、デジタル署名した文書自体が認証書の有効期限を超えて存在するため、それに対応させて有効期限が過ぎた認証書を、長期間保管しておく必要があるからである。

⑤ ポリシーの作成/認定(Policy Creation/Approval)

認証業務の実施に際して必要となる各種のポリシー(Policy)を定める。ポリシーには、認証局の運用に関わる要員、設備、各種手続き等を明確化した運用ポリシー、及び利用者や他の認証局等に対して認証を発行する際の審査基準等を定めた発行ポリシー等がある。

(3) 関連サービス

前記の認証書管理サービスに加えて、以下のような各種の関連サービスもＰＫＩの構成要素として考えられる。これらのサービスは、認証局が付加サービスとして提供することもあるし、別の機関が提供することもある。

① 登録(Registration)

個人情報等を登録・管理し、認証書の発行や失効に必要な本人確認を認証局に代わって行うサービス。実際の認証書発行等は認証局が行う。

② データ保管(Data Archiving)

デジタル文書等のデータを長期間にわたって保管･管理するサービス。書き換え不可能な媒体等に保管することで改竄等を防ぐとともに、媒体の陳腐化によるアクセス不能等が起こらないように適宜バックアップや保管媒体の更新等が行われる。

③ 電子公証(Notary)

事後のトラブルに備え、デジタル署名や文書の生成時刻の刻印、デジタル文書の存在等の公証を行う。

④ 鍵復元(Key Recovery)

鍵を無くしたり、あるいは鍵をアクセスするためのパスワードを忘れたりした場合に備えて、あらかじめ鍵の複製を預かっておき、利用者等の要請に応じて鍵の復元を行うサービス。鍵は公開鍵方式の秘密鍵の場合もあるし、共通鍵方式の鍵の場合もある。

⑤ レポジトリ(Repository)

個人等の属性情報を総合的に管理・提供するサービス。属性情報には、認証書ばかりでなく、電話番号、Ｅメールアドレス等の情報が含まれる。

⑥ その他

鍵の保管をＩＣカード等のハードウェアトークンで行うような場合、鍵の生成、ＩＣカードへの書き込みを行うサービス等のいろいろなサービスが想定される。

1.2　認証書の利用形態

認証書の利用は、利用に関して予め認証局と利用者間で何らかの契約もしくは約款が存在する場合と、利用時にはじめて何らかの約束を交わす場合があり、認証局の責任を規定するにあたってその相違を考慮する必要がある。

1.2.1 クローズドモデル

事前に契約関係にある当事者によって認証システムが設計され、運用されるモデルであり、ＳＥＴ（Secure Electronic Transaction）、ＳＥＣＥ（Secure Electronic Commerce Environment）における認証や企業グループ内ＳＣＭ（Supply Chain Management）における認証等が本ケースに該当する。下図における認証局は、クレジット会社、銀行、製造、流通会社等が登録局（ＲＡ：Registration Authority）を運営し認証書発行を発行局（ＩＡ：Issuing Authority）に委託する方式であり、この方式が市場で形成されつつある。

このケースでは、クレジット会社、銀行、製造、流通会社等の事業者が利用者である消費者やサイバーショップ運営者や従業員等の認証加入者、認証依存者との間で事前に認証書利用約款を取り交わす事により、各々の責任を明らかにしている。

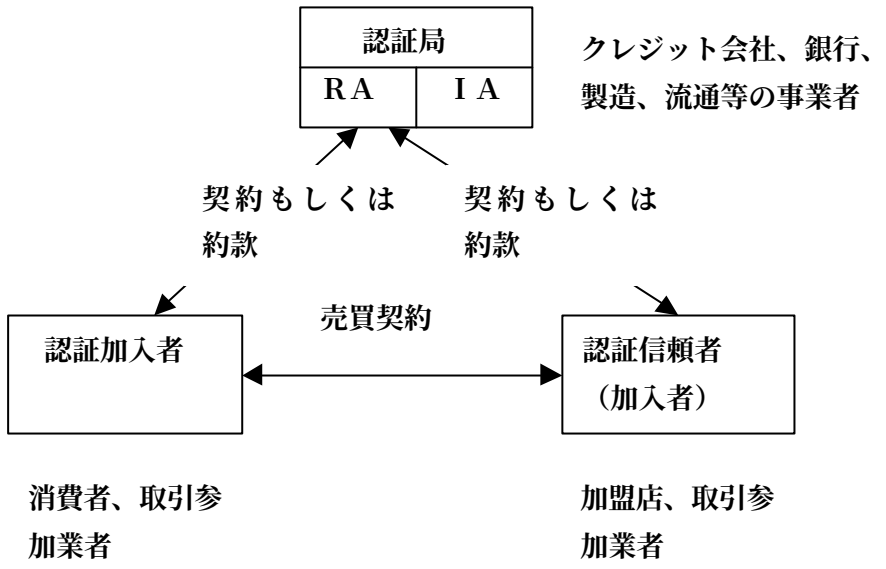


図 1-2 クローズドモデル

1.2.2 オープンモデル

事前に契約関係のない当事者に、ある認証局が発行した認証書が送付され、それを受け取った当事者がその認証書に基づいて取引活動を行うケースであり、現状ではサーバ認証、Ｅメール認証はこのケースに該当する。又、オークションや公開調達等の場合において、取引参加者が自分が所有する認証書（信頼出来る身分証明書に相当するもの）を提示する事によって取引への参加が認められるケースも想定される。

下図における認証局は、特定な取引に限定されないオープンな認証書（身分証明書の類）を発行し、加入者はその認証書を利用して公開取引やビジネス通信等に参加する。認証書を受け取った相手は、加入者の属する認証ドメインに参加していない事が想定され、従って自分の責任で認証書の有効性確認が必要になるが、この場合の認証局と認証依存者間の義務・責任を明確にする必要がある。

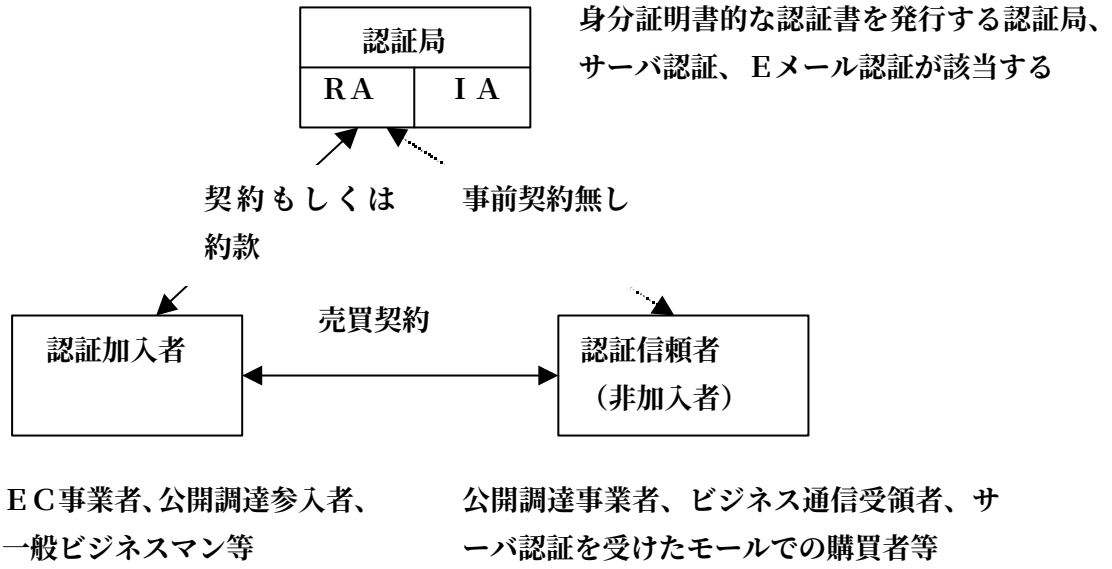


図 1-3 オープンモデル

1.3　認証局の置かれている立場と役割

インターネットなどオープンなネットワークを介して行われる電子商取引においては、電子的に相手を確認し、取引の成約を可能にするための認証書が重要な役割を果たす。認証によって、ネットワーク上を流れる取引情報に対する盗聴、改ざん、詐称などを排除しセキュリティを確保できるだけでなく、商取引に不可欠な信頼や信用を通有させることが可能になる。

それ故、認証局は認証書を発行する機関として、当該電子商取引の形態に合った認証書の位置づけおよび認証局の運用を明示するとともに、認証局自身の安全性、信頼性、中立性の向上につとめなければならない。また、認証局が果たすべき機能の重要性に鑑み、万一の事故や過失による当事者（加入者および依存者）ないしは社会に与える影響は大きいものと思われるため、認証局はその責任範囲を明確にし、万一の場合の補償（損害賠償）に備えなければならない。認証局は通常、これらをポリシーおよびＣＰＳとして明示しなければならない。

しかしながら、一方では認証局の責任範囲について一定の限度があることを認識しなければならない。例えば、認証局はショッピング決済において認証書を保有する消費者の支払能力やショップの信頼性を必ずしも保証するものではない。ましてや認証局は認証

書を使用するサービス、商品、提供する情報の品質や正当性を保証するものではない。

近年、認証局および認証書については各国とも電子署名法として法制化が盛んに行われており、日本においても２００１年度を目途に電子署名法の施行が準備されている。今後、ますます認証局の社会的な責任と義務が明確になっていくものとおもわれる。

2.認証局の責任に関する基本的考え方

2.1　認証局及び関連者の義務

2.1.1 認証局の果たすべき義務

認証局は認証書の発行にあたって、加入者ならびに依存者に、認証局のサービス・運用等に関する方針（ポリシー）および認証実施規定（ＣＰＳ：Certification Practice Statement）を公開しなければならない。認証局は自らのポリシーおよびＣＰＳに準拠することなく認証書を発行してはならないし、加入者や依存者はポリシーおよびＣＰＳを遵守することを要求される。

認証局は登録局(ＲＡ)、発行局（ＩＡ）およびリポジトリ（ＶＡ：Validation Authority として独立して存在することもある）からなる。各々の役割とその果たすべき基本的な義務は以下のとおりである。

(1)　登録局

登録局は認証書の発行審査をおこなう。発行審査にあたって、登録局は認証書発行対象者が本人であるかどうか確認しなければならない（本人確認）。

(2)　発行局

発行局は登録局の発行審査結果にもとづき認証書を発行する。即ち

－ 発行局は認証書発行対象者以外の者に認証書を発行してはならない。

－ 発行局は認証書発行審査を行わないで認証書を発行してはならない。

(3)　リポジトリ

リポジトリは加入者ならびに依存者に、認証書およびＣＲＬを公開する。リポジトリは認証書およびＣＲＬの更新状況にあわせ、ポリシー等で定めた期間内にその内容を更新しなければならない。

最近では認証書の失効状況をリアルタイムで確認するためＣＲＬにかわる機能としてＯＣＳＰ（Online Certificate Status Protocol）がサポートされたり、また、ある時点である認証書が有効だったかどうかを確認するＤＶＣＳ（Data Validation and Certification Server）が提唱されている。

2.1.2 関連者の果たすべき義務

(1)　加入者

―加入者は認証局が公開するポリシーやＣＰＳに記載されている範囲外の用途や相手（依存者）に認証書を提示してはならない。

―加入者は秘密鍵と対応する認証書（公開鍵）を確実に維持しなければならない。対応関係が不明になったり、秘密鍵が危殆化した場合、加入者は速やかに失効申請を行わなければならない。

―加入者は認証書記載事項に変更があったり、加入を止める場合は速やかに認証局（登録局）に届けなければならない。

(2)　依存者

―依存者は、認証局が公開するポリシーや CPS に記載されている範囲外の用途に、相手方の認証書を利用してはならない。

―依存者は、認証局が公開するリポジトリを利用して、相手方の認証書の有効性を確認しなければならない。

(3)　認証サービス製品提供者

認証サービスの提供、利用に際しては、サーバー、ＰＣ、耐タンパー装置等のハードウェアや、認証書の発行、失効、署名、検証等に用いられるソフトウェアに安全性、信頼性が求められる。認証サービス向けのハードウェア、ソフトウェア等の認証サービス製品を提供するベンダは、それら製品の安全性と信頼性に最大の注意を払うとともに、技術変化に対応した暗号強度等のセキュリティ向上に迅速に対応できるよう開発、サービス提供に努めなければならない。

そのために、ＩＥＴＦやＩＳＯ等の国際機関が提唱する技術仕様、品質基準等の標準に対する研究、提案、準拠等の活動はもとより、暗号の解読や製品へのウイルス混入等の事故の動向、原因追求、対応措置について、常に感度を高めておく必要がある。

2.2　認証局の責任に関する考え方

本項では、認証局の責任のあり方についてその基本的な考え方を示すこととしたい。なお、ここでいう責任とは、民事上の責任のことを指し、刑事上、行政上の責任については言及しないこととする。

2.2.1 民事上の責任について

民事上の責任とは、法律上の損害賠償責任のことである。つまり、被害者の受けた損害を公平の観点から誰が負担すべきかという問題である。法律上の損害賠償責任が発生する原因としては、不法行為に基づく責任、債務不履行に基づく責任そして損害担保契約に基づく責任がある。

不法行為責任とは、「故意または過失によって他人の権利ないしは利益を違法に侵害し、その結果損害を与えた場合、行為者はその損害を賠償しなければならない。」ことである。民法では、７０９条で過失責任に基づいた一般原則を定めており、これを一般的不法行為責任という。

債務不履行責任とは、債務者と債権者間に債権債務関係（契約関係）があることを前提とし、正当な理由がないにもかかわらず、債務者が「債務の本旨の従った給付をしない」場合、債権者は債務者に対して、損害賠償する権利が認められていることをいう。また債務不履行責任においては、契約関係を前提としていることから、その契約（あるいは約款）により特段の合意が可能である。例えば、契約によりある一定の損害については過失の有無にかかわらずにてん補することを約定したり、逆に（信義誠実、権利濫用、公序良俗等の一般原則に反しないことを前提として、）免責約款によって損害賠償責任を制限したりといったことも可能である。

不法行為責任と債務不履行責任は、いずれも加害事故の加害者が被害者対し、損害賠償責任を負うことになる点では異ならない。しかし、加害事故の当事者間の関係等が異なることなる。以下に簡単な比較を示す。

不法行為責任（民法７０９条）

○責任要件：過失（但し過失が推定されない→立証責任は被害者にある）、重過失、故意

○責任範囲：相当因果関係があって予見可能なもの

○契約による特段の合意は通常考えられない。

債務不履行責任（民法４１５条）

○責任要件：過失（但し過失は推定される→立証責任は加害者にある）、重過失、故意

○責任範囲：相当因果関係があって予見可能なもの

○契約（あるいは約款）において特段の合意が可能。但し公序良俗等一般原則による修正があり得る。

また、損害担保契約とは、当事者の一方がある事柄に関して被るかもしれない損害を賠償することを、相手方との間で約する契約のことである。

2.2.2 過失責任の原則（不法行為責任と債務不履行責任）

認証局においても、その業務に起因し、他人に損害を与えた場合には、前述のような不法行為責任あるいは債務不履行責任が発生することが考えられる。

ここで述べておきたいことは、どちらの責任を負うとしても、故意または過失が要件となっていることである。つまり、認証局に故意または過失がなければ、認証局が責任を負うことはないのである。

一方、消費者保護の観点から、認証局の過失の有無にかかわらず、一定の損害があれば、認証局がその損害について責任を負うべきであるという指摘も一部にある。しかし、現行法上では、当事者間の特段の合意がない限り、こうした主張は認められるべきでないだろう。電子商取引の発達、その信頼性・安全性の向上の観点から、認証局の存在は不可欠であるが、過失の有無にかかわらず認証局に責任を負わせることは、民法の大原則に反するものであるうえ、認証事業が成り立たなくなり、結果的に電子商取引の発展そのものを阻害しかねない。よって、認証局について無過失責任を取ることはあり得ないと考えられる。

2.2.3 注意義務

認証局が責任を負うのは認証局の行為に故意または過失があった場合であるが、それでは認証局の過失とは如何なるものであるのか。一般的に過失とは、注意を怠ること、すなわち注意義務違反のこという。そこで、認証局の注意義務の水準が問題となってくるが、認証サービスの提供の形態も様々であることから、一概に、サービスの全てが専門的なサービスということは困難であり、個別の判断が必要となるケースが多いと思われる。

2.2.4 損害賠償の範囲

(1)　通常損害と特別損害

一般的に、不法行為責任にしても債務不履行責任にしても、損害賠償の範囲は、予見可能な相当因果関係にある損害、つまり不法行為や債務不履行の結果、通常生じる損害が損害賠償の範囲であり、特別な事情によって生じた損害については債務者が予見でき

または予想すべきであった場合にのみ責任を負うこととなっている。

認証局の場合も損害賠償責任を負った場合には、通常損害及び予見可能な特別損害について責任を負うこととなる。

(2)　責任限度額の設定

認証サービスは、電子商取引の発展にとって不可欠なものであるが、電子商取引でさまざまなものが取り引きされるため、損害額が膨大なものになる可能性を秘めている。ところが、認証サービスといえども技術的要因あるいは人為的要因に起因する事故の発生は不可避であり、その損害の補填を予定しなければならない。そのため、認証局の過失に基づく損害をすべて認証局が負担しなければならないとすると、認証局がビジネスとして成り立たなくなり、電子商取引の発展を妨げることになる。あるいは、認証局が負担すべき損害賠償リスクを予め取りこんで料金を設定すると、極めて高い料金となることが予想され、やはり電子商取引の発展を妨げることになる。

そこで、責任限度額を設定し、認証局がおりこむべきリスクの限度額を明確にすると共に、利用者に対してもかかる責任限度額の設定されたサービスであることを明示することにより、その範囲内での認証サービスの利用を促し、利用者も合理的なリスクの範囲内で電子商取引を行うことになる。そのような意味において、責任限度額を設定することは、極めて合理性が高いものと考えられる。

現実にも、例えば、電気通信事業者の利用約款においては責任限度額が設定されており、この利用約款は上記と同様の理由により合理性が承認されている。即ち、損害をすべて電気通信事業者が負担しなければならないとすると、電気通信事業がビジネスとして成り立たなくなる反面、電気通信事業者が負担すべき損害賠償リスクを予め取り込んで料金を設定すると、極めて高い料金となってしまうことから、一定の限度で電気通信事業者が責任を負うとする利用約款に合理性があるとされているのである。

また、米国ユタ州のデジタル署名法においては「推奨信頼限度額」という概念が用いられ、認証局がその提供するサービスについて責任限度額を定めることが推奨されている。更に、1999 年１２月に採択された電子署名に関するＥＵ指令においても、適正な認証書は第三者による承認を前提とし取引額の限度を示すことが出来、認証局はこれを超えて生じる損害については責任を負わないとしている。

我が国においても、認証局がこうした責任限度額を設けることは否定されるべきではない。しかしその前提としては、加入者および依存者に対し、責任限度額が設定されて

いることを周知させることが必要である。また、その責任限度額の設定についても合理的な設定がなされるべきである。

2.2.5 依存規約による依存者に対する責任

(1) 依存規約に対する考え方

認証局の責任のあり方を考える上で、問題となるのが、依存者との関係である。いわゆるクローズドモデルにおいては、依存者＝加入者であり、加入時における認証局との契約において、その加入者が依存者となる場合の責任関係を予め定めておくことが可能である。

一方、いわゆるオープンモデルにおいては、依存者と間に予め契約を結ぶことは不可能である。一般的な解釈からすれば、このモデルにおいて認証局が依存者に損害を与えた場合は不法行為責任を負うこととなりそうである。しかし、認証局は加入者との間には予め結んだ契約により責任分担を定め、ある程度のリスク計算が可能であるのに対し、オープンモデルの依存者との責任分担が不明確ではリスク計算が困難となるという問題が発生する。

こうした問題への対処として、認証局によっては依存者が認証書を信頼する際に、依存者から合意を得る仕組みとして”依存規約”（リライイングパーティアグリーメント）を用意している。依存規約により、認証局および依存者ともに、予め自らのリスク計算が可能となるため、認証局は事業参入しやすくなり、依存者は認証書を利用した電子商取引を導入しやすくなるというメリットがある。依存規約の有効性については、今後議論が必要な部分もあるが、基本的には、依存規約の有効性を認めて行くべきである。

もちろんその際の依存規約は一般原則に反しないだけでなく、認証局の一方的な責任回避に利用されるべきではない。また合意に至る手続きについても、依存者が十分納得できる手段をとり、事後に否認されないような工夫が必要である。

(2) 依存規約の要件

認証局は依存規約を用意する場合には、その中に下記内容を記載し、また依存者が認証書を利用する際に、これを確認できるようにする必要がある。

① 記載すべき要件

A. 認証書の利用範囲

認証局は、依存者に対して認証書の認証レベル、使用目的、適用範囲を記載しな

ければならない。依存者が認証書をその目的や適用範囲外で利用したり、認証書の認証レベルを過度に信頼して損害を被ることのないよう注意を促す必要がある。

B. 認証書の有効性確認

認証局は、依存者が認証書を利用する際には、認証書の有効性を確認するよう注意を促す必要がある。よって認証書の有効性とは認証書が有効期間内であること、認証書が失効していないこと、発行機関名等の認証書記載項目が妥当であることを記載する必要がある。

C. 損害賠償および責任の範囲

万一の事故等により、依存者が損害を被った場合における認証局の責任や損害賠償の範囲を記載する必要がある。また依存者の損害に備えて、補償制度がある場合にはその内容を記載することが必要である。

② 伝達確認方法

依存規約は、依存者が認証書を利用する際、いつでも容易に見られるようにしなければならない。

また、依存規約は上記記載内容のように認証局のポリシー、ＣＰＳに関わる内容が多いが、徒にポリシー、ＣＰＳを引用するだけで内容がわからないことがないよう明確な記述が必要である。

2.2.6 他者の行為に対する責任

(1) 委託先ＩＡの行為に起因するＲＡの責任

債務不履行の一般原則として、他人の行為による責任としての履行補助者の過失による責任が認められている。

よって、ＲＡ（ブランド認証局）が認証書の作成業務をＩＡに委託している場合には、ＩＡはＲＡの履行補助者とみなされる。その場合、ＩＡの故意または過失についても、ＲＡが加入者に対して債務不履行責任を負うことになる。また、ＲＡが実際に損害賠償を行った場合には、ＲＡはＩＡにその損害賠償を求償することが可能である。

(2) ベンダーの行為に起因する責任

認証局のハード、ソフト等のシステムを開発、提供するベンダーの故意または過失により、利用者に損害が発生した場合においても、場合によっては、認証局は債務不履行責任を負うことがあり得ると考えられる。なお、認証局とベンダーの間の責任分担は、

その契約類型によって異なる。

(3)　電気通信事業者の行為に起因する責任

例えば、認証局自体に過失がなくとも、通信回線の中断により、本来の期日までに認証書の発行が間に合わないということは起こり得ると思われる。法的な解釈についていえば、様々な議論があり得るが、留意すべきは、一般的に電気通信事業者のサービス約款においては電気通信事業者の責任を限定しており、責任限定されていることはある程度周知されていると共に、合理性も一般に承認されていることである。通信途絶等において被る損害が基本的に利用者のリスクとして整理されている点を踏まえると、通信回線の中断による損害は、不可抗力によるものとして、認証局は責任を負わないと考えて良いのではないだろうか。

(4)　加入者の行為に起因する責任

加入者が自らの秘密鍵を故意に第３者に渡してしまったり、あるいは不注意で盗難されたりするとデジタル署名の偽造によるなりすまし損害等の発生のおそれがある。こうした場合、加入者には自らの秘密鍵を十分に注意深く管理する義務があり、その注意義務違反による損害については、認証局の責任はないものと考えられる。

一方で、認証局は顧客の管理責任等については十分な啓発を行うことが望ましい。

2.2.7 情報開示義務等

認証業務自体が揺籃期にある現状において、一般人の認証業務に対する理解も十分でないと思われる。このため、認証局は自らの業務内容、安全対策、責任分担、財務基盤等について十分な情報開示に努める必要がある。

またこれまで認証局の責任限定や依存規約の有効性について述べたが、認証局の情報開示等が不十分であれば、こうしたものの有効性が否定されるおそれがある。こうした意味からも、認証局はどこまでが認証局の業務なのか、責任を負える範囲はどこまでか、加入者が責任を負う範囲はどこまでかといったことを十分に周知させて行くべきである。

2.3　消費者保護の観点

2.3.1 消費者の適当な注意義務

認証局が認証書の発行、公開にあたって、加入者ならびに依存者に対して認証局のサービス・運用に関する方針（ポリシー）および認証実施の手続き（ＣＰＳ）を公開すること

が必要であることは述べた。しかし、消費者が加入者及び依存者の立場になる場合、電子商取引が十分普及するまでは、認証やデジタル署名の仕組み、暗号アルゴリズム等の技術面や、秘密鍵の管理、認証書の利用方法等の運用面について知識が十分にないことを前提に考えるべきである。従って、認証ポリシーやＣＰＳに対する消費者の理解に対して十分な配慮を払う必要がある。認証局としては、消費者の責任に帰す事故は適当な注意義務を怠らなければ生じ得ない範囲に止めるべきである。

消費者の適当な注意義務の範囲とはどこまでを指すのかは、認証サービスにおける事故事例が乏しい現在（残念ながらサービスの普及につれて事故が増えると思われる）、明確な規定を置くことは難しいが、加入者としての消費者の適当な注意義務範囲を想定する場合、公開鍵ペアの生成、管理、認証書の申請から受領、更新、失効、廃棄等消費者が行う一連の手続きを分析し、使用されるハード・ソフトを考慮した無理のない常識的なオペレーションの範囲を設定することになろう。

認証局がその責任を問われないために行うべき重要なことは、秘密鍵の漏洩の可能性、検証不能等の異常時や秘密鍵の安全な保管、属性変更時の失効申請等の確実な処理に対して、分かり易い説明資料の提供が、タイムリーに行われていることである。

また、認証局の負うべき責任限度額を明示することにより、消費者に責任限度額を越える取引きを行うことには慎重になるべきことを促すことも有効であろう。

2.3.2 個人情報保護

認証局はＲＡとＩＡが分離していようとも、いずれも加入者の個人情報を扱うことになるし、どのような依存者が認証書の有効性を問い合わせたかの情報も保有している。これら個人情報に対して、プライバシー保護の観点から法的な措置を講ずる動きが、ＥＵをはじめとして各国において見られるようになってきた。日本においても、インターネットによる電子商取引以前に個人情報漏洩問題が少なからず生じており、その対策が求められている。

個人情報の保護に関する法制化の動きに係らず、認証局はその業務を通して知り得た個人情報を内部においては、権限を有する職員以外が見てはならないし、見られない措置を講じなければならない。ましてや外部に不正な手段を用いて、漏洩したり販売してはならないことは言うまでもない。認証局が個人情報保護に対して、適切な措置を講じておらずその結果、個人情報が漏洩もしくは販売され、個人が被害を被った場合は、認証局は直接

的な被害を補償する責任がある。但し、認証局がハード・ソフト面及び運用面等で十分な保護対策を講じていたにも係らず、外部からのハッキング等で個人情報が盗まれた場合などでは、その時点で十分な措置が施されていることを立証すれば、過失がないとされ、責任は問われない場合もあり得ると考えられる。

3.認証局と利用者の責任分担

3.1　想定される事故形態と原因

認証局の責任を考える上で、認証システムに係る当事者（エンティティ）自身及び当事者間で取り扱う、もしくは取り交わす情報の発生から廃棄に至る全プロセスにおいて、情報そのもの及びその処理の過程で生ずる事故と被害、更にはその原因を明らかにすることが重要である。

以下に、エンティティ内及びエンティティ間で想定される事故とそれによる被害、事故の原因について分析した結果を紹介する。

3.1.1 認証局独自データに起因する事故と被害、原因

(1)　署名用秘密鍵

① 秘密鍵の生成

秘密鍵の生成とは、生成システムを起動して、鍵ペアを生成し、保管媒体に格納するまでの一連のプロセスを行う事を言う。このプロセスで想定される事故とその原因としては以下があげられる。

- 鍵生成に用いられる秘密情報(その情報があれば鍵が容易に推定できる)、あるいは鍵そのものが漏洩する。原因としては、乱数初期値などの入力データを入力者以外に盗み見られたり、入力者が他人にその情報を漏洩する(この情報を元に、生成プロセスを再現して、鍵を発見する)事が想定される。原因追求は難しいが、複数人管理（Dual Control）及び入力データが再現できないようなシステム対応(例えば、マウスのランダム操作から乱数取得)によって、当該事故は回避する事が可能である。
- システムがウィルスやバグ、あるいはセキュリティが十分でないためによって秘密情報が漏洩する。原因としては、生成システムが不正プログラムを含む、あるいはバグ等を含んでいることによって、秘密情報を漏洩してしまう事が想定される。原因追求は難しいが、生成システムが所定のセキュリティ基準(例えばＣＣ：Common Criteria 等)を満たしている保証があれば、事故は極めて少なくなるであろう。
- 権限者以外の者が生成に携わることで、鍵情報の漏洩、鍵のすりかえ等で不正な鍵を生成する。権限者であることの確認が不十分であるために起きる事故であり、生成時の履歴情報や記録から、それらの情報、記録が改竄されていなけ

れば、不正の検出は容易である。

- 暗号学的に弱い鍵を生成したために鍵が解読されてしまう。これは、最新の暗号技術についてフォローがされていないために起きる事故であり、最新の解読プログラムを用いる事により原因追求が容易に行える。
- 第三者が偶然に暗号を解読したか、同一の鍵を生成した。この事故は偶然に起こる事が想定されるが、万が一発生した場合は、原因追求は難しく、解読者の通知を待つよりほかがない。
- 暗号解読につながる理論・アルゴリズムが発見され、誰でも暗号解読が可能となる。この場合は、別の暗号アルゴリズムに代替するしか対応方法はない。又、新理論が公表されれば原因追求が容易であるが、公表等がされず、密かに利用されるのであれば、発見は困難である。

上記事故の発生による被害は、利用者全員におよぶ可能性がある。被害としては、秘密鍵を入手する事により認証書を偽造する事が可能になり、その偽造認証書を信頼して取引した利用者の取引損害と、事故に気が付いた後の全認証書の失効と再発行のためのコストが対象となる。又、事故はこれら以外に次のものもある。

- 生成時に操作ミスによって対応しない鍵ペアが取り出されたり、生成システムのバグ等によって対応しない鍵ペアが生成されたり、という公開鍵と秘密鍵の対応がとられていない事故が発生する事も想定出来るが、初歩的な操作ミス、バグ及びその後の確認ミスの積み重ねが原因であり、実質的にはほとんどありえない。又、当該秘密鍵に対応するとされる公開鍵で認証局の署名を確認できないため、発行された認証書が有効とならないため実質的な被害は発生しない。

② 秘密鍵のロード

秘密鍵のロードとは、秘密鍵を保管媒体から暗号管理モジュールに移すプロセスを指し、このプロセスで想定される事故とその原因、被害としては以下があげられる。

- ロード時に、秘密鍵の情報が、操作者あるいはケーブルのタッピングや不正プログラム混入等のシステムセキュリティ上の問題によって漏洩する。原因追求としては、ケーブルのタッピング、不正プログラムの混入など、予め原因として想定されるケースについての究明は容易であるが、想定外の原因についての究明は難しい。偽造認証書を信頼して取引した利用者の取引損害、全認証書の

失効と再発行のためのコストが被害の対象となる。

- ロード時に操作ミスによって対応しない鍵が暗号鍵管理モジュールに入力されたり、ロードシステムのバグ等によって対応しない鍵ペアがロードされる。これは、誤った鍵をロードしようとしたか、知識分散（Split Knowledge）された鍵情報の一部を誤ってロードしたためかあるいは、ロードシステムがバグ等を含んでいることによって、対応した鍵ペアをロードできない等が原因として考えられるが、いずれも初歩的なミスが原因であり追究は容易である。この事故が発生しても認証局の署名を確認できないため、発行された認証書が有効とならず、実質的な被害は発生しない。

③ 秘密鍵の保管

秘密鍵の保管とは、暗号鍵管理モジュールを署名システム等での利用状態から、利用停止状態にして保管することを言う。このプロセスで想定される事故、原因、被害については以下の通りである。

- 秘密鍵の情報が知識分散されている場合に、知識保有者の共謀により秘密鍵の不正再生が行われる。複数の責任者の共謀による内部の組織的不正が原因であり、もし行われた場合その原因究明は難しい。偽造認証書を信頼して取引した利用者の取引損害、全認証書の失効と再発行のためのコストが被害の対象となる。
- 秘密鍵が暗号鍵管理モジュールに保管されている場合に、モジュールへの不正アクセスが行われ秘密鍵が漏洩する。外部あるいは内部の人間による、暗号鍵管理モジュールへの不正アクセスが原因であるが、暗号鍵管理モジュールには、不正アクセスがあった場合に、その証拠が残るようなメカニズムが装備されているため原因究明は容易である。但し、そのメカニズムは想定される不正アクセスに対抗できるだけであり、想定されていない不正アクセスに対しては、必ずしも原因究明が容易であるとは言えない。この事故による被害は、上記と同様に偽造認証書を信頼して取引した利用者の取引損害、全認証書の失効と再発行のためのコストである。
- 暗号鍵管理モジュールの故障により鍵が変化する。原因は、暗号鍵管理モジュール内のソフトの異常動作により鍵が変化したためであり、簡単なチェックで原因究明が可能である。万一変形した鍵で不良認証書が発行されても、対象は

新規の利用者に限定されるため被害は少ない。

- 部品やソフトの不良等による暗号鍵管理モジュールの故障、暗号鍵管理モジュールの災害で認証書への署名が行なえない。この事故が発生した場合、バックアップされた暗号鍵管理モジュールを使用するか、業務停止により新規発行を一時的に中断するかの対応により、他への影響が及ばないため被害は少ない。

④ 秘密鍵の利用

秘密鍵の利用とは、暗号鍵管理モジュールが認証書発行システム等と接続され、認証書の発行等に利用されるプロセスを言う。このプロセスで想定される事故、原因、被害については以下の通りである。

- 暗号管理モジュールへの不正アクセスにより秘密鍵が盗まれる。原因としては、認証書発行システム等と接続中に、ネットワークを経由して、あるいは物理的に暗号鍵管理モジュール内の秘密鍵を取り出す事が想定されるが、ネットワーク経由での不正アクセス等は、監査ログ等で究明が可能であるし、又物理的な不正アクセスは、外形的に認識が可能である事により究明が比較的容易である。しかし、万一この事故が発生した場合は、偽造認証書を信頼して取引した利用者の取引損害と全認証書の失効と再発行のためのコストが被害となる。
- 暗号鍵管理モジュールの故障により鍵が変化する。原因、想定被害等は、秘密鍵保管時の事故と同様である。
- 暗号鍵管理モジュールの故障、および暗号鍵管理モジュールの災害もこのプロセスで想定される事故である。原因、想定被害等は、秘密鍵保管時の事故と同様である。

⑤ 秘密鍵のバックアップ

災害や事故等の原因により認証局の運用に齟齬を来さないために、秘密鍵の消失に備えてバックアップを行なう。このプロセスで想定される事故、原因、被害については以下の通りである。

- 秘密鍵の保管、利用プロセス時と同様に、秘密鍵の情報が知識分散されている場合の知識保有者の共謀による鍵の不正再生、秘密鍵が暗号鍵管理モジュールに保管されている場合のモジュールへの不正アクセスが想定される。原因、被害等については、保管、利用時の場合と同様である。
- 暗号鍵管理モジュールの故障、暗号鍵管理モジュールの災害もこのプロセスに

おいて発生する可能性がある。原因、被害等については、他のプロセスで発生する事故と同様であるが、このプロセスで発生した場合、リカバリが不能となり万一オリジナルの秘密鍵が消失した場合は秘密鍵の再生成が必要となる。

⑥ 秘密鍵の廃棄

秘密鍵の廃棄とは、有効期間が終了あるいは利用しなくなった秘密鍵を消去することを指し、バックアップされている秘密鍵の消去も含まれる。このプロセスで想定される事故、原因、被害については以下の通りである。

- 適正な手続きで消去しなかったため、暗号鍵管理モジュールや､その他の媒体に残ってしまうケースが想定される。廃棄ミスが原因で、秘密鍵あるいは秘密鍵情報が存在していることが確認できれば被害が発生しないが、不正な意図を持って行われた場合、他のプロセスと同様に不正使用による被害が発生する。

(2) 復号用秘密鍵

認証局では文書等を暗号化して保管あるいは通信する場合、文書を暗号化する鍵を公開鍵で暗号化する。それを復号するために用いる秘密鍵を復号用秘密鍵と称する。復号用秘密鍵に関連する事故とその原因は、署名用秘密鍵のそれとほぼ同一である。

(3) 認証局認証書

認証局が階層構造をとる場合、下位に位置する認証局は上位認証局から自分の公開鍵に対応する認証書を発行してもらいそれをバックアップを含め保管・利用し、有効期間が過ぎたら適切な期間保存する必要がある。

① 認証書の生成

不正もしくは不適切な認証局認証書が発行されることが想定される。原因としては、当該認証局の申請時のミス、上位認証局における内部不正(審査、発行、機密漏洩等)、上位認証局の認証書発行システムにおける不正プログラム、上位認証局の秘密鍵の第三者解読等が考えられる。もし不正もしくは不適切な認証局認証書が発行され、それに基づいた不正もしくは成りすましの利用者認証書が発行された場合は、それら利用者認証書によって行われた取引が被害の対象となり大きな影響を及ぼすこともある。

② 認証書の保管、バックアップ

保管およびバックアップされている認証局認証書が、認証局の不注意によるレポジトリ等からの消去や災害による焼失等が原因で、全て失われてしまう事がこのプロセスにおける事故として想定される。認証局の署名の検証が行えないことにより利用者

間の取引、文書の有効性確認等に影響を及ぼすこともある。

(4)　監査関連データ

その他、認証局内部において取扱う情報の中で被害の対象となるものに、監査に関連する情報がある。監査ログと報告に使用される監査結果がその主なものであり、それらの漏洩もしくは改竄等は認証局のみならず加入者や依存者にも多大な影響を及ぼすことがある。

① 監査ログ

認証局の業務遂行状況をロギングする情報は、ほとんどが定期もしくは不定期の監査における対象データになるため、対象データの選定から生成、保管、廃棄等に至るまでの的確な管理基準が求められる。監査ログは、不正持出し、タッピング、改竄、消去等が認証局内の管理不充分や不正アクセスやウィルス等の不正プログラムや通信路の盗聴等の原因により発生する恐れがある。その結果、利用者の個人情報等の漏洩によるプライバシ侵害、認証局運用に関わる技術機密の漏洩等認証局自身もしくは利用者に及ぶ被害が生じる。

② 監査結果

監査結果があらゆる面で良好であれば、単なる漏洩事故によって被害が発生することはないが、監査人からの重要な指摘事項の不正な漏洩や結果の改竄等がなされると、それが悪用されることにより被害が発生する可能性がある。

3.1.2 認証局と加入者間データに起因する事故と被害、原因

(1)　申請データ

利用者が認証局に対して申請するデータには、認証書の新規申請、失効申請、更新申請等があり、それらが利用者から認証局に送付されるプロセスにおいて事故に遭う場合と、認証局内で保管・保存されるプロセスで発生する事故がある。前者のケースでは盗聴、漏洩、改竄等がセキュアな通信手段をとらなかったことにより生じたと考えられるが、ほとんどは認証局からの確認により事故が判明することで被害は局所的である。後者のケースでも盗聴、漏洩、改竄等の事故形態が想定されるが、認証局内部の人間による不正やセキュリティ対策不備等が原因として考えられ、被害も大きくなる可能性がある。

(2)　審査データ

認証局では、各種申請データの審査を行うが、審査の過程および審査結果データの保管・保存過程において、本人確認誤り、不正審査、審査結果の改竄、漏洩等の事故が起きる可能性がある。これらは、提出させるべき情報を含め適切な本人確認方法が取られていなかったり、設備やセキュリティに不備があったり、内部に不正者がいた等の原因による。結果として、成りすまし認証書や個人情報漏洩等による被害の発生に繋がる。

(3)　認証書

認証書に係る事故は、認証書の生成から加入者への配布、保管・保存等のプロセスにおいて発生する。例えば、認証書生成プロセスにおいては、人的な操作ミスやシステム不具合により誤った認証書を発行する可能性があるし、セキュリティ不備や内部不正により偽りの認証書が発行される可能性もある。又、認証書の配布プロセスにおいては、申請データの誤りや、操作ミスにより認証書が正しく配布されないこともある。

(4)　ＣＲＬ

ＣＲＬもその生成から廃棄に至るプロセスにおいて、上で述べた認証書と同様な事故が発生する可能性を持っている。

3.1.3 加入者独自データに起因する事故と被害、原因

認証書加入者の独自データとしては、認証書の発行や失効、更新等の申請時に使用するデータ、配布された後の認証書、認証書に対応する公開鍵・秘密鍵ペア等があるが、ここでは事故が生じた場合加入者にとって影響が大きいと考えられる署名用秘密鍵を取り上げる。

加入者の署名用秘密鍵の取扱において想定される事故は、基本的には認証局の署名用秘密鍵と同様に生成から廃棄までの一連のプロセスで生じるものとほぼ同様な事故がある。

しかし、根本的な違いとして認証局は専門知識、技術を有する要員による管理がなされ又、高度なセキュリティを備えた設備・システムが使われることが想定されるが、加入者自身および加入者の環境にはそのような条件が無いことがあげられる。

従って、不注意な秘密情報管理や操作ミス等加入者の運用が原因となる秘密鍵の漏洩、盗難事故が発生し、それによる成りすまし被害が発生することが考えられる。加入者の秘密鍵に関連するものとしてそれ以外に、加入者が使用するハード、ソフトのバグもしくはウイルス混入による強度の弱い鍵の生成や署名データのすり替え等の事故も想定されるが、

秘密鍵の漏洩、盗難等に比べ可能性および被害の影響は少ないと思われる。

3.1.4 加入者と依存者間データに起因する事故と被害、原因

加入者から依存者には本来の目的である通信電文に添付もしくは結合されて、デジタル署名と加入者の認証書等が送信される。それらの情報を受信した依存者は、デジタル署名の検証と認証書の有効性確認を行う事により、正当な相手から改竄等がなされていない有効な通信電文が到着したことを知る。

デジタル署名の検証は、送信者の公開鍵を用いて復号したハッシュ値と通信電文のハッシュ化結果を比較することにより行われ、値が一致していれば当該公開鍵に対応する秘密鍵を所有している人が署名をし、且つ電文が通信途上で改竄されていないことが判明する。

これらの手続きは、依存者の使用するシステムが自動的に行い、検証結果を表示することが一般的に行われており、システムのバグやウイルスによる事故もしくは依存者の誤用等による事故が想定されるが、その頻度、影響はさほどではないと思われる。

次に、依存者は送られて来た認証書が正当な認証局によって発行され、失効されておらず、有効期限内にあり、認められている用途内である等を確認する必要がある。これら一連の手続きは、依存者の使用するシステムが自動的に行う方向にあるが、現状では依存者のオペレーションに委ねられている部分もあるし、確認結果の判断を依存者に委ねる部分もある。又、上記認証書の有効性問い合わせに際しては、問い合わせ先認証局のＣＲＬ更新サイクルによって実態とのズレが生じることもあるし、問い合わせ時に認証局から提示される依存規約が理解し難いこと等も考えられる。

失効されている、有効期限が切れている、もしくは用途外である等の認証書を、認証局、依存者、システム等のミスで有効であると判断された場合、状況によっては依存者に多大な被害が生じる可能性がある。

3.2　認証局および利用者の責任について

本節においては、認証局及び認証書ユーザ自身と相互間におけるデータの取扱で発生する事故、原因、被害等の分析結果を基に、認証局及び認証書ユーザが負うべき責任について記述する。認証局及び認証書ユーザが取るべき責任に関する考え方としては、２．２の「認証局の責任に関する考え方」に基づく。

上記考え方をベースに事故形態別、発生原因別に認証局と利用者の責任のあり方を記す。

3.2.1 なりすまし事故

(1)　不正申請によるなりすまし

不正申請によるなりすまし発生時における認証局の責任を考える際には、まず認証局が認証のレベルに応じてクラス分けをして認証書を発行していることに留意すべきである。具体事例をあげれば、認証局が送信人のメールアドレスを認証しているのみで、本人の同一性について認証していない場合もある。このような場合では、そもそも認証局は送信人名義と実際の送信人が、同一であることを確認したわけではことを明らかにしており、送信人の名義と実際の送信人が異なったとしても、認証局は必ずしも責を負わないと考えられる。利用者は、認証書の認証レベルを考慮し、認証書の利用形態に応じた適正なレベルの認証書を利用すべきであり、認証局はその認証のレベルを開示する必要があるわけである。

よって、検討が必要になってくるのは悪意のあるものが他人になりすまし不正な申請をおこない結果、認証局が誤った認証書を発行してしまった場合、つまり本人の同一性確認を行ったあるいは行うべき場合において結果として同一性が確保できなかった場合である。

この場合はまず認証局が適正な本人確認を行っていたかどうかがポイントとなる。認証局は適正な本人確認を行う義務があると考えられるため、本人確認手続きにおける過失や、その本人確認方法が容易になりすましが行えるようなものであったことが原因でなりすましが発生した場合は、認証局は責を負うこととなろう。

しかし、例えば申請者が真正な実印と印鑑証明等を持参してきた場合などでは、認証局がその申請者が本人であると判断し、結果としてその申請者が本人でなかったとしても、認証局に過失があるとはいえず、こうした場合、認証局は責を負うものではないであろう。

なお、現在、電子署名に法的な効力を与えるべく検討がおこなわれているが、電子署名に法的な効力を与えるとすれば、より確実性の高い本人確認方法がとられている必要があり、電子署名に法的効力を与える場合おいては認証局がどのような本人確認方法をとるべきか具体的な検討が必要である。

(2)　内部不正によるなりすまし

認証局内部の人間の不正により、なりすましが発生した場合、認証局は使用者として責任を負うこととなる。

よって、認証局は、内部の不正がおこらないよう、権限・知識分割などを定めた内部管理規定を定め、それを忠実に実行する必要がある。

(3)　加入者の不正等によるなりすましまたは事後否認

加入者の不正または過失等によりなりすましが発生した場合、原則として認証局は責を負うべきではない。加入者は自らの秘密鍵の管理に十分な注意を払う必要があり、加入者の秘密鍵管理や本人確認時に必要な本人確認情報の管理に不備があり、なりすましが発生したとしても認証局に責はない。また、加入者が他人に認証書や秘密鍵を利用させた、あるいは自らが利用した場合においては、事後否認が認められるべきではないのは当然である。

(4)　加入者の秘密鍵の解読によるなりすまし

公開鍵暗号方式においては、公開鍵からその秘密鍵を解読するといったことは極めて困難であり、電子認証・電子署名はこうした特性を利用したものである。

しかし、暗号技術とその解読技術はいたちごっこのようなものであり、その時点において安全と考えられている暗号もいつまでも安全であるとは限らないし、また絶対に解読されない暗号はないというのも事実である。よって、解読技術が確立している暗号は利用すべきではなく、また利用している暗号技術について解読技術が確立してしまった場合は速やかにその利用を中止し、新たにより強度のある暗号方式を導入する必要がある。仮に暗号解読技術が確立している等により暗号の強度が相対的に低下しているにもかかわらず、認証局がその対策（古い暗号方式を利用している認証書の失効、新たな暗号方式の導入等）を怠った場合には認証局が責を負う場合もある。

しかし、絶対に解読されない暗号というものはないことから考えると、秘密鍵が解読されたら必ず認証局が責を負うというものではないだろう。たとえば、数学的には極めて低い確率であるが、加入者の秘密鍵が偶然に解読されてしまった場合、上述のように絶対解読されない暗号はないことを考えれば、認証局に過失があるとは言い難く、認証局が責を負うべきではない場合もあり得る。

また認証局が加入者の秘密鍵生成まで行っている場合において、認証局の情報管理不備により、暗号解読に係わる秘密情報を認証局が漏洩してしまい秘密鍵が解読されてしまった場合には認証局の責となりうる。

(5)　認証局の秘密鍵の解読によるなりすまし

認証局の秘密鍵が解読されてしまうと、電子認証制度及び電子商取引そのものの信頼

性が揺らぎかねない。またそれにより発生する損害も巨大なものになるおそれがある。認証局の秘密鍵の解読に関する責任については、暗号解読技術が確立している等により暗号の強度が相対的に低下しているにもかかわらず、認証局がその対策を怠った場合や秘密鍵の管理が不十分である場合など認証局が責を負う場合もある。損害額が巨大になり、且つ責任限度額の設定がなされていなければ、認証局としても損害の賠償能力の限界を超えることも想定され、被害者に十分な賠償が行われない可能性もある。よって、認証局はその秘密鍵が解読または不正利用されないための厳格な管理を行う必要がある。

3.2.2 サービスの利用不能

サービスの利用不能については、原則的に認証局の責となろうが、賠償の範囲については、責任限度額を設定することにより合理的に分担すべきである。（ただし、顧客サービスの一環として認証局が費用負担することを否定するものではない。）

(1)　自然災害等による利用不能

大規模な自然災害に起因するものなど、リスクが集積しかつ直接的には認証局に過失といえない原因による利用不能については、必ずしも認証局が賠償すべきものではない。

(2)　システムの不具合・セキュリティ対策不備による利用不能

システムに不具合等が生じる原因としては、システムが本来備えるべき安全性・信頼性を欠いていた場合と、本来備えるべき安全性・信頼性基準を充たしていたが、現状の技術レベルにおいては不可避な原因による場合があげられる。前者の場合は、認証局に責があろうが、後者の場合は認証局は責を負わないこととなる。

(3)　操作ミスによる利用不能

人的または自動による操作にミスが生じて、サービスが利用不能になった場合には認証局の責となろう。

3.2.3 個人情報漏洩事故

認証局は、認証書の発行、更新、失効、保存、廃棄等一連の業務に係る各種情報を改竄、漏洩等の事故から防ぐ管理が求められている。中でも加入者のプライバシーに係る個人情報は、外部は元より認証局内部においてもアクセス権限を有する者以外に漏れてはならない。個人情報が漏洩するケースとして、加入者自身が保有する情報がインターネット等を通じた外部からの不正アクセスにより漏洩する場合と、認証局が管理している個人情報が

外部、内部の不正アクセスにより漏洩する場合があるが、ここでは後者の場合における責任について記述する。

(1)　外部からの不正アクセスによる個人情報漏洩

外部からの不正アクセスが行われ個人情報が漏洩する原因として、認証局のセキュリティが不備である場合とその時点で十分なセキュリティを講じていたにも係らず外部から侵入される場合が考えられる。

認証局のセキュリティ不備が明らかな場合は当然認証局の責であるが、認証局から個人情報が漏洩したことは利用者が立証しなければならない。

その時点としては十分と思われるセキュリティ対策を設けていたにも係わらず、外部から侵入された場合、開発危険の抗弁的な考え方が認められるべきであるが、予めどのような要件を満たせば開発危険の抗弁が認められるか定めておくことは困難であり、個別事案に応じて判断されることととなろう。

(2)　内部の不正アクセスによる個人情報漏洩

本来であれば内部無権限者にはアクセス不能な情報が、認証局内部の管理体制の不備によって、アクセスされてしまうことが原因として考えられる。いずれにしても認証局内部の不正であり、原則認証局が使用者責任を負う事になる。

3.2.4 検証不具合事故

認証書の依存者が行う検証行為として、デジタル署名の検証と送付された認証書の有効性確認がある。デジタル署名の検証は、送付された文書を送信時と同一のアルゴリズムを用いてハッシュ化し、その結果と送信者のデジタル署名を送信者の公開鍵を用いて復号したハッシュ値と比較することによって行われる。結果が一致した場合、成りすましが行われていなければ、認証書に記載されている人が署名したことと改竄がなされていないことが判明する。結果が不一致の場合は、送付された文書が改竄されたか置き換えられたかの事故によるものと考えられる。

一方、認証書の有効性確認は、送信者の認証書が何らかの事情で一時失効もしくは失効により無効になっていないかどうかを確認することを意味し、認証書を発行した認証局の認証書失効リスト（ＣＲＬ）を問い合わせることやオンラインで認証局に認証書のステータスを問い合わせる（ＯＣＳＰ）等の手段を用いて行われる。又、最近はデジタル署名が認証書の有効期限内になされたものか等を検証するための仕組み（ＤＶＣＳ）も提唱され

ている。

これら２つの検証行為において想定される事故としては、失効情報公開のタイムラグや有効期限切れ等による無効認証書を有効であると判定されるケース等が考えられる。その原因としては、認証局もしくは依存者の検証システムのミスが想定される。又、利用者が認証書の適用範囲を逸脱して使用する場合やそもそも認証書の検証を行わなかった場合や依存規約の不備等が原因による事故も考えられる。

(1)　認証局の情報整備に係る検証不具合

依存者が、認証書の有効性を何らかの手段により問い合わせた時に、認証局のサービスが利用不能である場合、失効受け付けもしくは失効確定後の失効情報公開までのタイムラグ内にある場合、認証局が誤った失効情報を公開していた場合が原因となる検証不具合が考えられる。

① サービス利用不能

認証局のサービスが利用不能である場合は、基本的には 3.2.2 項が該当するが、依存者が問い合わせ不能であるからと言って認証書の検証を行わずに行動した結果の損害については、必ずしも認証局の責任に帰すとは思われない。このケースでは依存者は、サービス再開まで検証を保留するか、認証書送信者に検証不能の旨を伝える等の手段があるからである。

② 失効情報のタイムラグ

認証書の失効は、加入者側が登録情報の変動や加入者秘密鍵の危殆化等によって申請する場合と、認証局側で加入者の不正な情報登録の発見や認証局秘密鍵の危殆化等によって行う場合があるが、一連の手続きと失効登録のタイミングのズレにより実態との間にタイムラグが生じるケースがある。特に、ＣＲＬ運用の場合はタイムラグが生じることが認識されており、そのためにＯＣＳＰの必要性が言われている。

認証局では、タイムラグが生じることを依存規約に盛り込むことにより、依存者に注意を喚起することが可能であるが、ほんの僅かなタイミングにより失効された認証書を信頼して依存者が被害を被った場合、認証局が依存規約により免責されるかどうかは問題のあるところである。

③ 失効情報登録

所謂正当な失効申請に対して、失効処理をしなかったり別の人の認証書を失効したり等のミスは、認証局に責があることは言うまでもないが、悪意もしくは悪戯により

他人の認証書の失効申請を行う事が想定される。この場合、失効申請が申請者の秘密鍵によって署名される等の合理的な手段を採用しているのであれば認証局に責任はないが、信頼性の低い手続きを採用していれば責任を問われる場合もあり得る。

(2)　依存者の行為に係る検証不具合

依存者が、デジタル署名と認証書の検証行為を行ったにも係らず、その結果にそぐわない行動を取った場合の責任は言うまでもない。依存者が必要とされる認証書の検証を怠った場合も依存者がリスクを負うことになろう。

4.責任リスクの管理

4.1　加入者、依存者への対応

4.1.1 加入者への対応

認証局と利用者の責任分担に関する法制度が整備されていない現状において、認証事業の健全な発展を阻害しないためには、認証局は加入者に対して特定の責務を負わせることにより認証業務の健全性を確保すべきである。

そのため、認証局は、消費者保護の観点で適切な範囲において、自主的に加入者の責務を明確化し契約に盛り込むなど、自局の責任リスクを管理するべきである。

(1)　加入者の責務の明確化

認証局が加入者の責務について明確化するべき項目および内容は以下のとおりである。

① 正確な情報の提示

加入者は、認証書申請などに際して、正確な情報を認証局に提示する義務がある。

② 認証書発行の確認

加入者は、認証局により認証書発行に際して、認証書の記載情報を確認する義務がある。

③ 秘密鍵および認証書の保護

加入者は、公開鍵/秘密鍵ペアの生成において、信頼できるソフトウェアやハードウェア等を利用して安全な方法で生成し、秘密鍵および対応する認証書を管理する義務がある。

④ 迅速な失効手続

加入者は、秘密鍵が危殆化した場合や認証書記載の情報に変更が生じた場合等、迅速に失効手続を行う義務がある。

⑤ 認証書の利用範囲の遵守

加入者は、認証局が公開するポリシーやＣＰＳに指定した認証書の利用範囲および目的を遵守する義務がある。

また、クローズドモデルのように依存者も加入者となる場合には、認証局は以下の責務についても明確化するべきである。

⑥ 認証書の適格性のチェック

依存者は、受け取った認証書が目的に適したものであるかどうかを判断する義務がある。例えば、取引の金額的な限度は、認証の真正性保証レベルや補償レベルに応じて決める義務がある。

⑦ 認証書の確認

受け取った認証書の有効期限、利用目的、署名の正当性を確認する義務がある。

⑧ 認証書以外の情報の利用

取引の重要性に応じて、認証書だけに依存するのではなく他の手段も併用する必要があることを認識しておく義務がある。

⑨ 責任限度額

認証局が負担する責任には責任限度額が設定されていることを理解して、その範囲内で利用すべき義務がある。

(2) 認証局-加入者間の契約

認証局は、事前に加入者と契約または約款を取り交わすことにより、前項に記した加入者の責務を加入者自身に通知し、合意を得るべきである。

当該契約関係の発生により、認証局は、直接的に加入者との責任分担および認証局の加入者に対する責任範囲を明確化することができ、また、当該契約において、加入者と加入者の認証書に依存する依存者との取引上の契約に認証局の責任範囲を組み入れる旨を規定することで、加入者でない依存者との間でも、間接的に責任分担および責任リスク量の管理を図ることができる。

ただし、この場合の契約または約款の規定内容については、本書における認証局と加入者の責任分担の考え方および消費者保護の考え方に基づき、当事者間の権利・義務のバランスが取れたものであり、自局の免責を一方的に規定するものであってはならない。

また、これらの契約または約款の通知および合意の手段についても、認証局が提供する認証サービスレベルにより一概に評価することはできないが、認証局は、加入者（または場合によっては加入者の認証書に依存する依存者）との間で充分な合意を得ることが事後のトラブル防止に繋がるために、契約書面を加入者本人に郵送するなど、なるべく明示的な通知を実施することが望ましい。特にオンライン申請方式などにおいて、Web等に契約または約款条文を表示し加入者の合意を得る場合には、認証局は、適当な注意力を持つ加入者であれば容易に確認できる表示形態を採用し、かつ手続において充分に

確認できる時間が確保しなければならない。加入者の合意を得るうえでは、加入者が選択する同意確認機能等について、システム的に「同意する」が初期設定されていることは消費者保護および事後のトラブル防止の観点から望ましくない。

(3)　認証書発行審査における加入者への要求事項

認証局は、発行する認証書について、加入者の属性情報の真正性および当該認証書に記載される公開鍵の対となる秘密鍵が加入者に唯一属していることの信頼性を確保しなければならない。

また、加入者による認証書の申請方式としては、オンライン申請とオフライン申請に区分され、さらにオフライン申請についても書類送付申請や出頭申請等が想定される。各々の申請方式または提供する認証サービスレベルより認証局の責任リスクは変化すると考えられるが、以下に申請方法毎に加入者に対して要求するべき事項を例示する。

① オンライン申請

デジタルデータに基づいた本人確認を前提とした方式であるため、認証局は容易に成り済ましができないような方法を用意するべきであり、加入者に対しては以下のような情報を複数入力することを要求したうえで、予め保有する情報との突き合わせを実施するべきである。

- 生年月日
- 自宅住所
- 自宅電話番号
- クレジットカード番号／預金口座番号
- 暗証番号（PIN）
- 本人しか知り得ない情報等

この場合においても、認証局は審査結果を加入者の自宅住所宛てに郵送するなど、より一層の責任リスクの管理を実施するべきである。

② 書類送付申請

本申請方式において認証局は、加入者に対して認証局所定の申請書式に必要事項を記載させるとともに、加入者が本人であることを証明する以下のような書類（およびこれら書類の組み合わせ）の送付を要求したうえで、書類記載事項および捺印の確認を実施するべきである。

- 印鑑登録証明書（法人・個人）

- 住民票（個人）
- 商業登記簿謄本（法人）等

この場合においても認証局は、審査結果を加入者の自宅宛に郵送するなどにより、一層のリスク管理を実施すべきである。

③ 出頭申請

本方式において認証局は、加入者に対して出頭のうえ認証局所定の申請書式に必要事項を記載させるとともに、②の書類に加えて加入者が本人であることを証明する以下のような書類（およびこれら書類の組み合わせ）の提示を要求したうえで、書類に貼付された写真および記載事項並びに押印の確認を実施するべきである。

- 運転免許証
- パスポート
- 健康保険証等

(4) 加入者への情報開示

認証局は、自局の責任限定および加入者との間における責任分担を計画するうえで、加入者に対して「認証書およびＣＲＬのリポジトリ」をはじめとして、認証局における「経営情報」、「技術情報」、「安全対策実施状況」、「認証実施規定（ＣＰＳ）」等を開示するべきである。

認証局は、特に認証書およびＣＲＬのリポジトリを公開するにあたり、「誤ったリポジトリまたはＣＲＬを公開した場合」や「（システムの故障等により）リポジトリまたはＣＲＬを利用できない場合」には、自局の過失すなわち注意義務違反に起因して、加入者および依存者が取引上何らかの損害を被ることを併せて認識するべきである。

4.1.2 依存者への対応

認証書の利用形態がオープンモデルである場合、認証局と加入者でない依存者の間には事前の契約関係が存在しない。

そのため、認証局は加入者に対する場合と同様に、依存者との間でも責任分担を明確にすることで自局の責任リスクを管理する必要がある。一方、依存者の立場からも、認証局との責任範囲が不明確な状態においては、潜在的にリスクを負うことになる。つまり、認証局が依存者に損害を与えた場合、依存者が認証局の不法行為責任に基づき損害賠償を請

求する際には認証局の過失を自ら立証する必要がある。

そこで、認証局が依存者との責任分担を計画するにあたり、以下に例示する対応のいずれか（またはこれらの組み合わせ）取ることが考えられる。

- 依存者が認証書を信頼する際に、依存者より合意を得る「依存規約」により認証局の責任範囲を明示する。
- 目的範囲を超えて依存者が認証書に依存することを予防するために、認証書の目的範囲を制限するなど、認証局の責任範囲を加入者の認証書により依存者に通知する。
- 加入者に対し、加入者と依存者間の取引上の契約において、認証局の責任範囲を組み入れるよう要請する。

いずれの場合においても、認証局は、自局の一方的な免責を図るべきではなく、依存者との合意や通知方法についても適切な方法を用意するべきである。

4.2　ＩＡとの関係

認証局の発行する認証書は利用用途に応じて要求される信頼性が異なり、これに対応して認証局に要求されるマネージメント、運用、システム・設備要件も異なってくる。認証局に要求される信頼性が高いほど、認証局の初期コストや運用コストは増大し、また運用要員やセキュリティ要件の確保に困難が伴うであろう。このような場合、発行局（ＩＡ）を認証サービス事業会社に外部委託するのが一般的である。

ここではＩＡを外部委託する場合、委託契約等に盛り込むべき項目と内容について記述する。

4.2.1 認証書の位置づけ

ＩＡを外部委託する場合、委託元は認証書の利用範囲が企業内認証等のクローズドな領域（サービス）なのか、それともサーバ認証や電子メール認証等のオープンな領域（サービス）なのかを明確にしなければならない。

一般的に、クローズドなサービスで発行される認証書の発行対象者およびサービス利用者は、社員とか銀行・クレジット会社のカード所有者等のように、委託元に属している個人とか委託元と何らかの契約関係にある（「１．２．１ クローズドモデル」に相当）。この場合、認証書の発行主体は委託元であり、認証サービス事業会社は認証書の発行業務を請け負うに過ぎない。委託元は、発行主体として自らの認証局を運営する立場から、認証ポ

リシーおよびＣＰＳを作成し公開するのが望ましい。

これに対し、オープンなサービスで発行される認証書は、認証書の発行対象者のみならず委託元と直接、契約関係にないサービス利用者（認証依存者）が利用する（「１．２．２オープンモデル」に相当）。この場合、認証書の発行主体は、認証サービス事業会社になるのが一般的であり、委託元は認証サービス事業会社が運営する認証サービスを利用するという立場になる。よって委託元は、本サービスの利用者として認証サービス事業会社のポリシ ー、ＣＰＳに従わなければならない。本形態では、委託元は認証サービス事業会社より認証書の発行審査を委任されることになる。

上記をリスクマネージメントの観点からみれば、クローズドなサービスで発行される認証書は委託元、オープンなサービスで発行される認証書は認証サービス事業会社が、発行主体としてリスクマネージメントを実施していく必要がある。

4.2.2 義務と責任

委託元と認証サービス事業会社は委託契約を締結するにあたり、各々の義務と責任を明確にしなければならない。とりわけ、下記事項については運用時のトラブルになりやすいので契約書に明記することが望ましい。

(1)　事故と責任

認証局の事故でＲＡとＩＡ間でその責任を契約時に明確にしておくものとして、大別すると以下の３つのケースがあり、ＲＡ及びＩＡは契約時の留意事項として認識する必要がある。

①　認証書の瑕疵による事故

例えば、ＲＡが故意又は過失により誤った本人確認による認証書の発行をＩＡに指示したことにより、ＲＡに損害が発生した場合、ＲＡが自らその損害を負担することとなり、ＩＡに責任を負わせることは出来ない。一方、ＩＡが故意又は過失によりＲＡから指示されていないのに瑕疵ある認証書を発行し、ＲＡに損害が発生した場合、ＩＡはＲＡの損害を賠償しなければならない。

②　サービスの不具合による事故

ハードウェア、ソフトウェア、ネットワーク等のさまざまな障害が原因として考えられるが、ＩＡがＲＡに提供するハードウェア、ソフトウェアに原因がある場合には、契約に特段の免責の規定がない限りＩＡが責任を負うこととなる。

③ 秘密鍵の危殆化による事故

加入者の管理ミスにより加入者の秘密鍵の危殆化が生じた場合には、加入者の責任でありＲＡやＩＡに責任が発生するものではない。これに対し、認証局の管理ミスにより認証局の秘密鍵が危殆化した場合には、ＲＡやＩＡに責任が発生し、ＲＡとＩＡの間の責任分担は両者の契約内容によることとなる。

又、認証局の管理ミスによらずに、即ち例えば暗号が解読された事により秘密鍵が解読された場合には、認証局側に責任があるかどうかは個別事案によると考えられるが、認証局に責任があると認められる場合にはＲＡやＩＡに責任が発生し、ＲＡとＩＡの間の責任分担は両者の契約内容によることとなる。

(2) 機密保持義務

認証局が取り扱う機密情報として特に注意を要するものに、加入者の個人情報（審査情報）がある。委託元は認証サービス事業会社との委託に際し、加入者の個人情報の取扱いを充分に検討する必要がある。また、認証サービス事業会社は加入者の個人情報の取扱いについて充分なリスクマネージメントが必要である。

(3) 知的財産権

認証システムが第三者の特許権や著作権等の知的財産権を侵害した場合、通常，ＩＡが認証システムを提供するであろうからＩＡが責任を負うこととなる。但し、契約に免責の規定のある場合や当該認証システムをＲＡが自己の責任で準備してＩＡに運用のみを委託した場合のように、ＲＡがリスクを負うこともある。

4.2.3 監査

認証サービス事業会社は自らのポリシー、ＣＰＳに基づき最低、年１回、監査を実施し、委託元に報告する必要がある。また、委託元は契約により認証サービス事業会社の監査を実施することができる。この場合、監査内容については事前に双方、協議する必要がある。

4.2.4 提供情報と提供方法

ＩＡを外部委託する場合、委託元は下記の情報を認証サービス事業会社に提供する必要がある。

- 認証書発行情報：X.５０９V3.0 に準拠した認証書情報を通常、オンラインにて提供するのが一般的である。

- 認証書失効情報：ポリシー、ＣＰＳに規定された方法で提供する。
- その他：ＲＡ担当者名等、認証局運営に必要な情報等で通常、委託契約時に提供する。

4.3　認証ポリシー・ＣＰＳでの対応

4.3.1 認証ポリシー・ＣＰＳの策定

(1)　ポリシーとＣＰＳ（Certification Practice Statement）

認証局は、サービス・運用等に関する方針や規定、基準を定めたポリシーを策定し、信頼性・安全性・経済性に対する基本的考え方およびその実現方法等を規定する。

また、認証局は、そのポリシーに基づいて、認証の実施における手続き、遵守事項など、どのような実務慣行を採用しているのかを簡単に文書化したＣＰＳを策定することが要求される。

(2)　ポリシーおよびＣＰＳの遵守

認証局は、認証書を発行する際には、このポリシーやＣＰＳに記載された規定に従わなければならないし、利用者や他の認証局等が認証書を利用する際にもポリシーおよびＣＰＳを遵守させなければならない。

また、利用者としても、ポリシーやＣＰＳに定められた目的や利用範囲内で、認証書を利用したり提示することを遵守しなくてはならない。

ポリシーおよびＣＰＳは、利用者等の認証局の外部者が認証局を信頼性・安全性・経済性の面から評価できるように、開示あるいは公開することが要求される。そこで、認証局としては、利用者等が簡単にポリシーおよびＣＰＳにアクセスして利用できるようにしておくべきである。

(3)　認証局の責任範囲との関係

認証局は、ポリシーおよびＣＰＳにおいて、特定の制限やその責任範囲を明確に表現することにより、損害賠償等の万一の補償に備えることに役立つ可能性がある。認証書を利用する前に、関係者がポリシーおよびＣＰＳを参照するように契約において義務づけることで、認証局の責任範囲はより明確化することができる。

ポリシーが認証局としての基本的方針や考え方を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し、ＣＰＳは、そのポリシーに基づいた実施手続きをその組織の状況に応じ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、より広い範囲で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。

ポリシーとＣＰＳが当該認証ドメインのビジネスにおいて、共にその責任範囲について詳細に記述したものであると考えるなら、ポリシーとＣＰＳには密接な関係があり、相互に補完するべきである。

さらに、この両者はポリシーを共有する認証ドメイン内でビジネスの実践に先立って行われる契約で関係付けることも可能である。例えば、ビジネス契約の付帯条項あるいは付帯文書として参照させる方法であり、もし異なる表現があったなら、どちらを優先させるかを規定することも可能であろう。

(4)　ポリシー・ＣＰＳの記載方法

認証書が特定の規制や免責事項を前提としていることを明確にするには、認証書の本文中に明記したり、そのような情報を記載したポリシーまたはＣＰＳを参照させることが適切かもしれないが、依存者にとって分かり易くする事が必要である。

ポリシーまたはＣＰＳにおいて、認証局がその規制や免責条項をいくら視覚的に目立つように作成したとしても、膨大なページ数のポリシー・ＣＰＳが認証書に参照として組み込まれその中に免責条項が記載されていた場合、利用者にとって内容を把握することは難しいと考えられる。

免責条項等の主要な点を簡潔にまとめ、目立つように記載すれば、利用者にとっては認識し易いかもしれないし、ポリシーおよびＣＰＳがインターネット上において依存者からアクセスを受ける場合においても、免責条項等の重要な項目が常に最初に表示され、さらに全文を容易に参照できるように、認証局は配慮すべきである。

ＣＰＳの条項等を参照に組み込んだだけで、依存者に適切な通知をしたことになるのか、ＣＰＳを参照にしている通知が目立つようになっているのか、またその場所が指定されているかどうか、簡単にアクセスできるかどうかの要因が、免責条項等の有効性を考えるにあたって重要である。

4.3.2 認証局の責任に関するＣＰＳの内容

ＩＥＴＦ（The Internet Engineering Task Force）のＰＫＩＸでは、ＲＦＣ２５２７で認証ポリシーと認証実施フレームワークを規定している。その中で認証局の責任に関し、

以下の条項において記述することを薦めている。

一般条項（General Provisions）において、認証局の義務（Obligations）、認証局の責務（Liability）、認証局の財務上の責任（Financial Responsibility）、監査（Compliance Audit）に関する項目が規定されている。

また、認証ポリシーとＣＰＳの維持管理条項（Specification Administration）では、規定の更新手続（Specification Change Procedures）、公開と通知の手続（Publication and Notification Procedures）、ＣＰＳの承認手続（ＣＰＳ Approval Procedures）等の項目が記載されている。

その他、ＣＰＳには認証局の責任以外の条項として、本人認証手続（Identification and Authentication）、業務遂行要件（Operational Requirements）、建物・設備のセキュリティ管理、人事管理（Physical , Procedural , and Personnel Security Control）、鍵のセキュリティコントロール（Technical Security Controls）、認証書及びCRLフォーマット（Certificate and CRL Profile）等がある。

4.4　認証書フォーマットでの対応

認証書のフォーマットは、X.509と呼ばれるものが広く利用されている。このX.509は国際標準であり、ISO/IEC 9594-8（同じものがITU Rec. X.509）として発行されている。現在、バージョン３が正式登録されているが、それ以前のバージョン１及びバージョン２に対して、拡張領域が大幅に追加されたものになっている。

それら拡張領域のうちの一つに、当該認証書を発行した認証局のポリシー（certificate policies）を参照するためのポインターを指定できる項目がある。これを利用して、認証書の受け手は、所定のディレクトリから、ポインターによって示された認証局のポリシーを入手することが可能である。このディレクトリは、信頼される国際機関によって管理されているので、信用できるものである。

認証局のポリシーを参照する手段として、この拡張領域は利用可能であるが、認証書フォーマットとしてバージョン１を利用しているユーザに対しては別途考慮が必要である。

認証局は、認証ポリシーやＣＰＳを表現することにより、認証書の利用者に対し、その利用目的や利用制限等を明示する。一方、認証書の利用者は、その認証ポリシーやＣＰＳを参照することにより、認証書が信頼できるかどうかを判断したうえで、その利用を決めることになる。

通常、X.509 Ｖ3 認証書には拡張フィールドが設けられていて、そこに認証ポリシーやＣＰＳの情報が記述され、認証局が自らの認証ポリシーを表現することになる。X.509の拡張フィールドのうち、認証ポリシーやＣＰＳに関するものとしては、利用者に関わる「Certificate Policies Extension」と、認証局向けの「Policy Mappings Extension」「Policy Constraints Extension」の３つの拡張項目がある。

Certificate Policies Extensionには、認証局の業務に対し「重要」あるいは「非重要」のフラグを記述し、業務の重要度に応じてポリシーの利用を制限するフィールドが存在する。認証局が「重要」であると判断した場合には、認証書はポリシーの内容に従って使用される必要があり、ユーザーのアプリケションがこれを処理できなければ、認証書の利用は著しく制限されることになる。一方、認証局が「非重要」とする認証書は、そのポリシーの利用目的や利用制限等には限定されず、自由に利用することができることになる。

これは、認証局は認証書が不適切な目的や方法で使用された場合に、自らを守ることも可能となる必須項目である。

4.5 消費者保護への対応

4.5.1 消費者保護

インターネットの世界では、その取引が隔地間で行なわれる為、悪意をもった事業者が簡単に消費者と接触し、悪事を働いた後ネットから撤退するという不正が行われる可能性も秘めている。この為、消費者がなりすましや情報漏えいなどの事故に巻込まれる可能性も高い。

一方で、鍵の管理不徹底による盗難や、キーボード操作ミスなど、消費者自身に起因する事故も推測される。そもそも一般的な消費者は、認証システムや制度に関する情報はもとより、インターネットの公開性などの基本知識に関して、事業者より劣ることは否めない。消費者も知識不足を認識している上に、こうした事故に巻込まれることへの不安感を抱いており、電子商取引発展のためには消費者保護に対する環境整備が急がれるところである。

こうしたなか、認証局の責任リスク管理を考えるにあたり、消費者に係る事故や事故発生後の両者間のトラブルに対する防止策を充分に考えておくことは、重要な課題となっている。

(1)　消費者への啓発

認証局は、不正アクセス防止策などシステム環境の整備を行なうことは当然であるが、それ以外に消費者が巻き込まれ易い事故の防止に向けた教育や啓蒙といった取り組みを積極的に進める必要がある。

具体的には、消費者に認証システムや制度そのものを正しく理解してもらうことが重要であるのだが、単に仕組みや利用方法を理解するだけでなく、認証の利用に伴うリスクの予見や、消費者の利用時における義務や責任など、認証利用についての正しい認識をもってもらうことが重要である。

また、パスワードや秘密鍵の管理方法など、消費者の情報セキュリティに関する基本的なリテラシー向上に向けた努力も必要である。

こうした啓発活動の取り組みは、電子商取引サービス提供者や認証サービス提供者等の事業者が協力して行なっていくものであるが、少なくとも認証サービスの主要な役割を担う認証局としての努力義務は不可欠である。

(2)　適切な注意義務の喚起とトラブルへの対応

消費者が巻き込まれ易い事故について、認証局と消費者の間で予め締結される契約において、発生する可能性のある事柄全てを取り決めておくことは難しいが、予想し得る問題に対して、最大限の努力を払い、発生し得る事故、被害の説明や発生した場合の対応について取り決めを行なっておくことも認証局の信頼確保の為には重要である。

次に、事前説明、通知にもかかわらず事故が生じ、責任、損害問題等の交渉で消費者とトラブルが持ちあがることも考慮する必要がある。その際に備え、相談窓口を設置し事故状況や被害状況等を客観的に聴取し、責任の所在、損害負担等に関して、誠意を持った対応を行う等の手続きを明確にしておくことが必要である。

4.5.2 個人情報保護

認証局は、消費者から本人確認等の為に業務上必要な個人情報を入手できる立場にあるわけであるが、この個人情報の取り扱いについては、認証局として業界ごとに定めた個人情報保護に関するガイドライン等に基づいたコンプライアンスプログラムを制定するなど、積極的な個人情報保護に向けた管理が必要である。

特に、収集する個人情報の取り扱いについては、リスク管理上次のような注意を払う必要がある。

① 収集する個人情報については、業務上必要な最低限の情報に留める。

② 個人情報の収集に際しては、その利用または提供の目的を明確にした上で、顧客の同意を得る。

③ 次に掲げる個人情報については、これを収集し、利用し、又は提供してはならない。

イ) 人種及び民族

ロ) 門地及び本籍地

ハ) 信教、政治的見解及び労働組合への加盟

ニ) 保健医療及び性生活

④ 個人情報の収集は、適法かつ公正な手段によって行なうものとする。

⑤ 個人情報を第三者から収集するにあたっては、顧客の利益を不当に侵害しないようにする。

⑥ 入手した個人情報については、収集目的以外に提供されることがあってはならない。

⑦ 第三者への開示については、本人の同意または法律上の手続きに基づく司法当局の要求があった場合に限定されるべきである。

⑧ 個人情報を業務上必要な範囲内で、正確かつ最新の状態に管理する。なお、業務上必要な期間を経過した場合は、個人情報の破棄その他の処理を行なう。

⑨ 個人情報への不当なアクセスまたは個人情報の紛失、改ざん、漏えい等の危険に対して、必要な安全保護措置を講じる。

⑩ 個人情報の取り扱いを外部に委託する場合には、その委託先との契約において十分な個人情報保護に関する事項を加える。

⑪ 顧客から自己の個人情報についての開示請求があった場合や、訂正の請求があった場合、および利用又は提供の中止の請求があった場合には、これに応じる。

⑫ 個人情報を保護する為に管理体制の整備に努める。

5.損害賠償への対応について

認証局は法律上の損害賠償リスクを処理する手段を講じる必要がある。

一般的にリスクの処理手段としてはリスクコントロール（危険制御）[1]、リスクファイナンス（危険財務）[2]等の手法があるが、ここでは特にリスクコントロールとしての責任限度の設定、またリスクファイナンスとしての財務基盤の確保、賠償責任保険の加入について述べる。

5.1　責任限度の設定

あまりにも高額な損害賠償により認証局が破綻することとなれば、その事故自体には直接関係ないものにも悪影響がでるおそれがあり、そうなれば電子商取引発展そのものを阻害しかねない。よって電子商取引の安全性の確保に不可欠な存在である認証局を保護・育成する観点から、認証局が自らの損害賠償責任について責任限度を設けることは許容されるべきである。また、認証業務への参入時に予め責任限度を設定しておくことでリスクの算出がしやすくなるため、認証事業への新規参入が促されるという側面もある。責任限度を設ける際にには、その限度額が合理的なものである必要があるが、具体的な責任限度額の設定のあり方については、認証業務を外部から委託される場合の委託元との関係と、依存者や加入者との関係とについて場合分けが必要であろう。

まず、認証局と委託元の関係、（特にここで想定しているのは企業が自らの業務に電子認証を活用するため、認証書の発行業務を外部の認証局に委託する場合等のことである。）について述べる。この場合、責任限度額をどの程度で設定するのかということもサービス内容の一環と考えられ、低額な受託料金でサービス提供を行うのか、サービス料金を高めに設定する一方で、サービスの付加価値として責任限度額を高く設定するのかについては、原則的に当事者間の合意よって決定されるものであろう。ただし、その際には認証局の財務基盤や認証書の目的用途など考慮に入れる必要があろう。つまり、いくら責任限度額を

---

[1] 「リスクコントロール」とは危険の発生を防止し、万一発生した危険の結果たる損害を最小ならしめる手段の採用のことである。リスクコントロールには危険の回避（危険に係わる活動自体を行わないという消極的な危険処理手段）、危険の除去（危険を積極的に予防し、軽減する手段であり、危険の防止、分散、結合、制限）があるが、責任限度の設定は危険の除去の中の危険の分散あるいは危険の制限にあたる。

[2] 「リスクファイナンス」とは損害が発生した場合に必要な資金繰りをあらかじめ計画して準備することである。リスクファイナンスには危険の保有および危険の転嫁がある。危険の保有の典型的な手法としては準備金設定があり、また危険の転嫁の典型的な手法としては保険の活用がある。

高額に設定しても認証局に賠償資力がなければ意味はなく、一方、認証書の用途によってはあまり高額な賠償事故が起こりえないケースもあり、企業にとっては責任限度額を高額に設定するよりも、サービス料金が低く設定された方が好ましいという場合もあるからである。

他方、認証局と加入者や依存者との関係では、消費者保護の観点等から、その責任限度額は不当に低額に設定されるべきではない。また、認証局からみても、責任限度の設定額があまりにも低いと、かえってその有効性が否定されかねないという問題もあろう。認証局の対処としては、顧客が自らの用途に応じ、認証のレベルを選択できることとし、その認証レベルに応じた責任限度額の設定を行うという措置をとることも有効であろう。

なお、上記のいずれの場合においても、認証局は十分な情報提供により、消費者等に責任限度が設定されていることを周知させておくことが、責任限度の設定を有効たらしめる要件となる。具体的には、クローズドモデルにおいては、加入者の申込時にすくなくとも加入約款等を利用し、加入者にできるだけわかりやすい形式で情報提供を行う必要がある。また、オープンモデルにおける依存者との関係において、認証書の責任限度の設定を有効たらしめるためには、依存者が認証書に依拠し取引を行う際に、その認証書に責任限度が設定されていることを依存者が認識できる仕組みづくりが必要である。

5.2　財務的基盤

たとえ責任限度を設定したとしても、一定レベルの賠償金の支払いのためには、認証局は財務的な基盤を維持する必要がある。

財務的な基盤が貧弱であることにより、もしもの損害賠償事故が致命傷になり、認証局の業務に支障がでることになれば、電子商取引の発展を阻害しかねない。また、被害者の救済が困難になるという問題も起こり得る。

具体的な対策としては、まず、準備金を設定することなどが考えられよう。具体的な準備金の必要額については、責任限度額、認証書の発行枚数、認証書の利用目的等を総合的に勘案し決定される必要がある。

5.3　損害保険の加入

米国の認証局においては既に複数の保険会社から認証局向けの損害賠償責任保険が販売されており、認証局の中にはそうした保険に加入することで、もしもの際の損害賠償に備

えているものもある。

また日本に於いても認証局向けの賠償責任保険の発売が開始したところである。賠償責任保険の加入により、立ち上げ期であることから十分な準備金が設定しにくい認証局においても賠償資力の確保が図れ、ひいては被害者の救済が図られることから、認証局の賠償責任保険の加入が期待される。

認証局が損害賠償責任に加入する際には以下のような点に留意が必要である。

5.3.1 保険金の支払限度額

一般的な損害賠償責任保険においては、１請求毎、保険期間毎（通常１年間）に保険金の支払限度額の設定することになっている。支払限度額の設定程度について、基本的な考え方は、準備金の必要額と同じであるが、十分な準備金を用意するにはある程度の期間必要であるのに対し、損害賠償責任保険については、保険に加入すれば、当初から必要な賠償資力が確保できる。（もちろん、損害保険によって全てのリスクが転嫁できるわけではなく、保険の対象となる事故には制限がある。）

5.3.2 補償範囲等

現在、保険商品の自由化が進んでいることから、認証局向けの損害保険についても、オーダーメイド的に保険設計することが可能となっている。このため、補償の対象事故、支払われる保険金の種類等については、保険約款で十分確認するとともに、必要に応じて、補償内容の変更等も保険会社に依頼するべきである。

5.3.3 保険会社の選定

保険会社の選定にあたっては、十分な支払い余力を有している保険会社であることは当然であるが、電子認証業務自体が高度な専門性を有していることから、引受保険会社が電子認証業務やその法的な責任のあり方について十分な知識を有している必要がある。仮に保険会社にそうした知識がないと、保険加入時に十分な説明が受けられない、補償の内容の変更を依頼しても、認証局の要望に応じた変更ができない、事故の際の支払い時に、保険の有無責の判断ができないことから、スムースな損害処理が行われないといった問題が発生するおそれがある。

5.3.4 損害保険商品のあり方

ところで、保険に加入することにより、かえって保険契約者のモラルが低下し、事故が増加してしまうおそれあるのではと指摘されることがある。しかし、認証局の位置づけから鑑みるに、保険の加入が直接的に認証局のセキュリティ対策のモチベーション低下につながるとは考えづらい。とはいえ、今後の新規参入の増加により様々な認証局が現れることを想定すれば、高度なセキュリティ対策を講じているものから、必ずしもそうでないものまで現れてくることも考えられる。仮に、セキュリティ対策が不十分でそのため事故発生の可能性が高い認証局の契約を他のものと同じ条件引き受けるとすれば、善良な認証局の負担のもとに一部の認証局を優遇することとなり不適当である。特に賠償責任保険は、過失等ある程度は認証局の自助努力で改善できる要素を担保するため、引受に際してはモラルリスクの排除の視点が重要である。よって保険会社が認証局の賠償責任保険を引き受ける際には、適切なアンダーライティングが重要である。

また、引受を行う場合に於いては事故発生の可能性の大きさを考慮に入れ、保険料も相応の配慮が必要である。認証局のリスク評価を行い、リスク対策が十分な認証局に対しては保険料を引き下げることによって、社会的な公平性が保たれるともに、認証局にとってもリスク対策強化のインセンティブとなるというメリットがあるからである。

6.付録

6.1　消費者取引における認証局の役割（ＩＬＰＦワーキンググループ報告書）

本報告は、ＩＬＰＦの認証局実務に関するワーキンググループによって作成され、1997年4月にドラフトとして公開された「The Role of Certification Authorities in Consumer Transaction」を、ＩＬＰＦの好意及び許可を得てＥＣＯＭが翻訳したものである。従って、コピーライトはＩＬＰＦに属し、翻訳についてはＥＣＯＭが責任を負うものである。

原文においては、６．１．１まえがき以降の翻訳文以外に付録として、作成の目的と前提、オープンシステム対クローズドシステムの分析、デジタル署名の解説等が記述されているが、紙面の都合上それらを割愛している。興味ある読者は、http://www.ilpf.org/work/ca/draft.htmからご覧頂きたい。

なお、ＩＬＰＦでは本ドラフトを作成したワーキンググループ以外にも多彩な活動を行っており、Self-RegulationやContent Liability等のワーキンググループがそれぞれの研究成果を公開している。電子認証関連では、認証局に関するワーキンググループの他、デジタル署名に関するワーキンググループがあり、電子署名・デジタル署名法の調査、分析報告や「電子認証のための国際的合意原則」(http://www.ilpf.org/digsig/intlprin.htm）を取り纏めて公開している。

6.1.1 まえがき

本レポート「消費者取引における認証局の役割」はインターネットロー&ポリシーフォーラムが作成したものである。このフォーラムは、欧州、アメリカ、アジアの企業のコンソーシアムによって設立され、インターネット社会の関係者や取引や政府がインターネットの困難な法的および政策的問題を解決するための中立的な論拠を与えることが目的である。本フォーラムに関する詳細情報は、インターネット上のwww.ilpf.orgで入手することができる。

本レポートは、本フォーラムの「認証局実務に関するワーキンググループ」によって書かれた。本レポートは、「認証局実務に関するワーキンググループ」の手順書と予定された作業計画書に従って作成されている。これらの文書は、http：//www．ilpf．org/work/ca/draft．htmのインターネットロー&ポリシーフォーラムにおいて入手可能である。本レポート、フォーラム、またはワーキンググループに関する質問は、info@ilpf.org

か以下のモントリオールのフォーラム事務所に連絡すること。

Internet Law & Policy Forum
World Trade Centre
Bureau 3280
380, rue Saint-Antoine Oues, bureau 3280
Montreal, Quebec H2Y 3X7
Canada
514.288.1966（電話）
514.288.1177（ファクス）
info@ilpf.org

ワーキンググループや、本レポートの作成に関わった企業その他の組織は以下の通りである。

ワーキンググループ

Bruce Hunter, General Electric Info. Services
Hong Kong Telecommunications
Colm Dobbyn, Mastercard Corporation
Barbara Fox, Microsoft Corporation
Peter Harter, Netscape Communications Corp.
David Schelhase, Premenos Corporation
John Makaryshyn, Telus Corporation
Jeffrey Ritter, ILPF 議長（職務）

追加参加者

CertCo
CommerceNet
DFN-CERT
Entegrity Solutions
IBM
Institut Jozef Stefan
Nortel Secure Networks

消費者政策に関する OECD 協議会

Signet Systems

UNINETT

法律関係報告者-- Cooley Godward LLP, Palo Alto, California。 Cooley Godward チームには Terrence P. Maher (Boulder, CO)、Eric Schalachter (Palo Alto, CA)、C.Bradford Biddle (San Diego, CA)が含まれる。アシスタントは Melissa Richards (Boulder, CO)および Janice Phillips (Palo Alto, CA)である。

技術関係報告者-- Manny Pasetes, Premenos Corporation

ドイツの法律問題に関する情報は、Gleiss Lutz Hootz Hirsch & Partners, Frankfurt, Germany の Matthias Karl 博士および Christopher Kuner によって提供された。

本レポートの根幹部分は 1997 年 1 月に完成したが、それ以降いくつかの部分を更新している。特に記載がないかぎり、読者は本レポートが 1997 年 1 月 1 日以降で最も新しいものであると見なすべきである。

6.1.2 概要

本レポートは、新しく出現している認証局のサービス業に関する法律問題、特に消費者取引に関していくつかの問題点を大まかに分析したものである。本レポートの扱う範囲は、意図的にアメリカ合衆国の法的環境に限定しているが、追加情報としてドイツの法律、欧州委員会の通達、およびその他の地域での法律も記載している。また本レポートは「オープンシステム」で発生する消費者取引だけを扱っている。オープンシステムでは、ＣＡは、サービスを要求する消費者には誰でもサービスを提供し、消費者や販売店と決済システムとの間の契約義務は考慮しない。これは本フォーラムの「パイロット」プロジェクトであるため、このプロジェクトの情報源からより広範囲の総合的分析を行うことは意図していない。

本レポートは、ＣＡ、販売店、消費者の間の複雑な関係を分析している。現在、特定の「デジタル署名法制度」があるわけではなく、既存の法律では次のような原則になっている。

- デジタル認証書を購入する消費者とＣＡとの関係は、既存の契約法が適用される可能性が高い。特に、デジタル認証書はあくまでサービスとして取り扱い、商品では

ないと考えられるため、（アメリカ統一商事法典やその他の「商品」関連規則の代わりに）コモン・ロー（普通法）が適用されるであろう。ただし、多くの理由から、ＣＡと消費者との間で成立した契約だけで両者の間で発生する可能性のある事柄をすべて完全に解決するのは無理があり、デフォルト規則が必要となる。

- 消費者からデジタル認証書を受け取る販売店とＣＡとの関係は、契約法ではなく、既存の不法行為法が適用される可能性が高い。特に、デジタル認証書が正しくなかった場合、販売店へのＣＡの責務を決定するルールとして、「過失による不実表示」の不法行為が適用される可能性が高い。

このようなことから、この構造から損失が生じた場合の当事者の責任は、その人物が適切に行動したかどうかに関係するのが普通である。このため、一般的に、一方が適切に行動し、もう一方が不適切に行動した場合、不適切に行動した方が損失の責任を負うべきである。しかし、全ての当事者が適切に行動したにもかかわらず損失が発生した場合、損失は販売店が追うべきであると我々は考えている。さらに、消費者が不適切に行動した場合、消費者の損失を制限するように配慮し、消費者が負担できない分は販売店が損失を負担するようにすべきであると考える。どちらのケースでも、販売店は、損失を防止したり、損失が全ての消費者に広がらないようにするのに最もよい立場にある。

本レポートは、どのような振る舞いが適切である見なされるのかについて、いくつかのパラメータを提案したい。本レポートで扱っている他の問題点と同様に、これらのパラメータについてもさらに深い研究が必要である。

6.1.3 はじめに

(1)　問題の要約

インターネットは、サイズや適用範囲や到達範囲が非常に広いのにも関わらず、まだ消費者取引の主要手段となっていない。これは、一部には、オンラインでのセキュリティ侵害が現実に発生しているため、それを心配する消費者がインターネットを商業取引に使うのをためらっているためである。販売店の方も、オンライン商取引を懸念する理由がいくつか存在する。電子メッセージが改竄されていないこと（完全性）、本人のものであること（本人性）、後から取引を否認できないようにしていること（否認防止性）が自動的に保証されているわけではない。

電子メッセージの完全性、本人性、否認防止性を改善する方法の１つは、頑強な公開

鍵基盤（PKI、「公開鍵認証フレームワーク」とも呼ばれる）を開発すること、特にデジタル署名を商取引に利用するように奨励することである。デジタル署名を利用する場合に発生する困難な問題の１つは、暗号鍵のペアを持つ人物のアイデンティティが正確にわかるようにすることである。認証局（ＣＡ、「媒介システム」とか「認証者」とも呼ばれることがある）と呼ばれる信頼できる第三者を使うことで、公開鍵が確かにその本人に属するものであることを確認できる。ＣＡは、ある個人と特定の公開暗号鍵を結びつけた認証書を発行することによって、確認ができるようにしている。

(2)　本レポートの焦点

本レポートは、消費者取引で認証書を利用した場合を取り扱っており、企業から企業へのやりとりで認証書を利用する場合（企業間電子商取引）の問題点に関しては扱っていない。ただし、消費者取引の枠組みの中でも、本レポートの対象範囲は限られている。デジタル署名に関係する問題点は範囲も広く複雑である。さらに認証書は、斬新で創意に富んだ方法で利用されつつある。

本レポートは、おおむね「オープンシステム」とか「オープンループ」モデルと呼ばれているものに焦点を当てている。オープンシステムモデルでは、消費者は独立した第三者ＣＡから１つの「アイデンティティ」認証書を入手し、次に多くの異なる販売店との取引を簡単にするのにその認証書を使う。

我々がオープンシステムモデルに焦点を絞ったのは、以下のようにいくつかの理由がある。

まず、オープンシステムモデルでは、当事者同士の複雑な関係を統御するルールに関して、非常に難しい問題や前例のない法的および政治的問題が発生するからである。これとは反対に、クローズドシステムでは、関連する当事者同士の関係は、契約法や既存の決済システム法制度および条例によって統御することができる。これは両方とも、内容が比較的よく知られており、分析しても意外性が少ない。しかし、適用される契約法やその他の法律がクローズドシステムのモデルに合わない場合、デフォルトの規則として、オープンシステムのモデルで議論された規則が適用される可能性が高い。

第二に、ＰＫＩの問題点を解決するために、今日まで続いているほとんど全ての法律上の努力は、暗黙のうちにオープンシステムモデルを前提としている。現在まで米国で制定された「デジタル署名」の法律は、おおまかに言って、このような独立した第三者ＣＡモデルをベースにしたＰＫＩを発展させようというねらいがある。同様に、米国政

府がＰＫＩ発達促進のために行っている施策もオープンシステムモデルを前提にしているし、アメリカ法曹協会科学技術部門の情報セキュリティ委員会が発行した「デジタル署名ガイドライン」もオープンシステムモデルが前提である。

第三に、このプロジェクトが最初に計画されたのは 1996 年春である。この当時、業界はもっぱらオープンシステムを開発することに努力を傾けており、したがってオープンシステムがビジネスモデルとして優勢であった。実際は、本レポートが執筆されている間に、オープンシステムはビジネスモデルとして成功する見込みが次第に薄れてきており、代わりに、認証書を利用する消費者取引は「クローズドシステム」または「クローズドループ」モデルで行われるだろうと考えられるようになった。

まず、クローズドシステムは２つのカテゴリーに分類することができる。1 つは、当事者同士が契約に合意することで決済メカニズムが「ループを閉じる」ようにするシステムである。もう 1 つは、認証書をアクセス制御デバイスとして使い、知的所有権の利用量を計測したり、自分が所有権を持つリソースへのアクセスを制限するために利用するようなシステムである。

消費者取引においてオープンシステムが本当に望ましいのか、実現可能なのかについては議論の余地があるが、本レポートは、このモデルに付随する難しい法律的および政策的問題のいくつかに焦点を絞っている。ただしクローズドシステムに関する議論も、それが解明に役立つと考えられる場合、本レポート内に挿入している。両モデルの境目が曖昧であるし、現在市場では新しいビジネスモデルが進化している最中なので、オープンシステムモデルに関する議論の一部は他の状況の中でも適用可能であると考える。

本レポートでは、オープンシステム型のＰＫＩに参加している両方のエンティティに関してどのような問題点があるか、またこのような基盤の継続的発展に関心を持つ政策立案者に関してどのような問題があるかを突き止めようとしている。これらの問題点としては以下のようなものがある。

- あるＣＡにおいて、そのＣＡの顧客である消費者とそのＣＡとの関係について、ＣＡはどのような実務が予想されるか。ＣＡがこれらの実務を適切に遂行できなかったことに関して、ＣＡが自分の責任を否認する能力を制限する必要がある場合、どのような制限を設定すべきか。
- ＣＡの提供するサービスに関して、消費者はどのような実務が予想されるか。これらの実務を遂行しなかった場合の潜在的責任をどのように制限すべきか。

- ＣＡが発行した認証書を信用している販売店には、どのような実務が予想されるか。ＣＡの発行する認証書を信用しているが、そのＣＡとはその他の関係を持たない販売店とＣＡとの間にはどのような法的関係が存在すべきか。ＣＡの販売店に対する潜在的責任は、何らかの方法で制限すべきか。責任を制限するには、どのようなメカニズムが使用できるか。
- この関係のうちの誰（ＣＡ、消費者、または販売店）が、損失リスクを見積り金額をつけるのに最適か。

(3)　本レポートの目標

本レポートは、オープンシステムで消費者にサービスを提供するＣＡに関する新しい法的ルールやビジネス実務について、簡単な要約を作成することを目的にしている。これが達成されているなら、本レポートは、問題点をさらに深く分析するため、および公共および民間の両方が参考にできるような法的および政策的ガイドラインの決定版を作るための基礎となるはずである。

最終的に本レポートが最も役に立つのは、この分野において実用的で一貫していて明解なルールを作り出すプロセスに使用される場合であろう。本文でも記載している通り、不明確なルールを寄せ集めつぎはぎして作っただけでは、ＰＫＩの参加者がそれらのルールを順守することは困難である。順守するためにそれらのルールを分析するということすらも困難だ。

一貫した明確なルールがないということは、ＰＫＩの発展を阻害する大きな要因となり、十分な数の参入企業を確保できないことになる。わかりやすい透明なルールを作ることは、がっちりした電子市場を発展させるために不可欠な１ステップであると我々は考えている。

ワーキンググループの全てのメンバーは、ＰＫＩを使った電子商取引の開発に商業的な関心を持っているが、本レポートは特定の標準、ベンダー、製品、またはビジネスモデルを故意に有利にしたり、評価したり、支持することは避けるようにしてきた。ＣＡおよびワーキンググループのメンバーは、本レポートに対するコメントを書面で提出するように要請された。

本レポートは、単なる参考用であり、弁護士と顧客の関係を規定することを意図したものではない。読者が特定の状況に関してアドバイスを受けたい場合、自分で職業的法律専門家を探すべきである。

本レポートは、ＩＬＰＦのパイロットプロジェクトであり、ＣＡに関する困難な問題や興味深い問題を全て取り扱ったり分析しているわけではない。これらの問題を解決するためには、この分野でさらに作業を続ける必要があるとワーキンググループは考えている。

6.1.4 背景

(1) 用語集

ＰＫＩに関する議論は、略語や専門用語のためにさらにわかりにくくなっている。本レポートで使われている主要な用語の一部を以下に解説する。

1. 「認証書」または「デジタル認証書」。デジタル認証書は、消費者に関する情報（消費者の公開鍵を含む）を持ちＣＡの秘密鍵を使って署名される。
2. 「認証失効リスト（ＣＲＬ）」。ある認証局から発行されたデジタル認証書の中で、取り消されたものの全てのリスト。
3. 「認証局（ＣＡ）」。認証局は、消費者に関する情報（たとえば消費者のアイデンティティ、金融機関での消費者の口座、クレジット支払いカード番号、等）と公開鍵をリンクするデジタル認証書を消費者に提供する。ＣＡは、タイムスタンプ、鍵管理サービス、および CRL サービスのような、その他のサービスを提供することができる。
4. 「認証実施規定（ＣＰＳ）」。ＣＡと、ＣＡが認証書を発行したエンティティ（本レポートでは、消費者であることが多い）との間の契約の基礎として使われる技術的、ビジネス的、法的な広範囲の問題に関して、ＣＡの実務について記載したもの。オープンシステムにおいては、消費者のＣＡのＣＰＳによって、販売店の権利や義務を支配するような契約的基礎がどの程度与えられるのかという問題については未解決である。クローズドシステムにおいて、ＣＡは、取引の全ての当事者との間で契約関係に入ることになると思われるので、ＣＡのＣＰＳはこのような契約の中に当然組み込まれることになる。
5. 「消費者」。商品やサービスをオンラインで購入する個人。オープンシステムでは、ＣＡから認証書を入手した消費者は「加入者」と呼ばれることが多い。しかし、販売店と消費者の両方が取引を締結するために使われるデジタル認証書を持っているような状況では、このような用語の区別は混乱のもとになる。この場合、

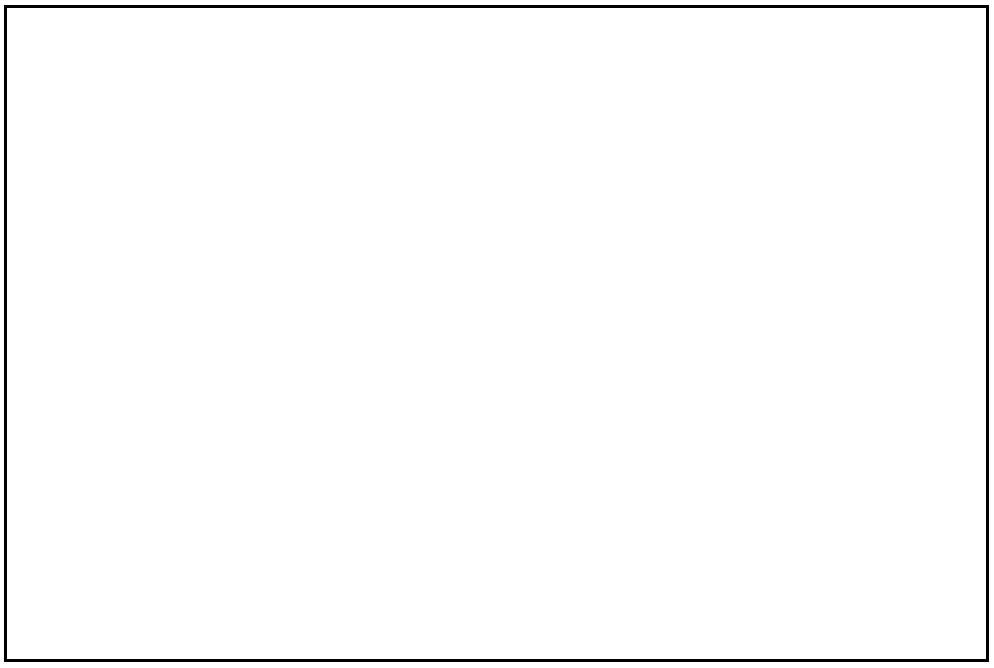
両方の当事者とも「加入者」になってしまうからだ。

6.「販売店」。商品やサービスをオンラインで提供するエンティティであり、消費者との取引を完了させるためのプロセスの一部として認証書を受け取る。オープンシステムでは、販売店は「依存する第三者」と呼ばれることが多い。

7.「秘密鍵」および「公開鍵」。デジタル署名の利用するためには、数学的に関連付けられた大きな素数のペアを作成する必要がある。この数の１つは公開鍵と呼ばれ、もう１つは秘密鍵と呼ばれる。秘密鍵は安全に保管するが、公開鍵は一般に入手可能である。公開鍵と秘密鍵の各ペアは完全に一意であり、したがって各秘密鍵に対応する公開鍵は１つしかない。

(2)　デジタル署名を使ったインターネット商取引のモデル

デジタル署名とＣＡを解説するのは、かなり難しい仕事であることが知られている。下図は、オンライン取引の一部として消費者が認証書を販売店に提出するという状況を、簡略化して図示したものである。この図は、たくさんの複雑な事柄が省略されていることに注意していただきたい。また、この図には、販売店が認証書を消費者に提示して自分の身元を認証するというケースは含まれていない。



要約すると、プロセスは一般的に次のように機能する。

ステップ１：消費者は、消費者のシステムに常駐する鍵生成システム（ソフトウェアかハードウェアと組み合わせたソフトウェアのどちらか）を使って公開鍵および秘密鍵を生成する。

ステップ２：消費者は、身元情報と消費者の公開鍵をＣＡに提示する。ＣＡはその消費者に認証書を提供する。

ステップ３：消費者と販売店がある関係に入る。すなわち、消費者は、消費者の秘密鍵でデジタル的に署名した支払い情報および注文情報（たとえば「貴社のオンライン雑誌を購読したいので、小生の現住所に請求書を送ってください」とか「以下の商品を送ってください。代金は口座番号 123456789 から引き落としてください」とか「この支払い契約と交換で貴社のレポートをダウンロードさせてください」等）、およびＣＡの秘密鍵で署名された認証書を提出する。

ステップ４：販売店は認証書（およびＣＡまたは自分のＣＡの認証書）を確認し、認証失効リスト（存在している場合）をチェックして認証書が取り消されていないことを確認する。

ステップ５：消費者および販売店は取引を完了する。

(3)　なぜ認証書を使うか？

ＰＫＩにより、本人認証、否認防止、メッセージ完全性という３つの主要目標を容易にすることができる。認証書は、これらの目標を達成するための役割を、様々な程度で果たすことができる。ＰＫＩの第４の目標は機密性であるが、これが提起する問題点は本レポートの対象外である。

本レポートは、認証書を使って本人認証を行うことに焦点を当てている。ここで、本人認証とは、ある当事者の身元を確認することを意味する。販売店は、取引相手の消費者が公開鍵の本当の所有者であることを確認するための一手段として、消費者の本人認証を行いたいと考えるであろう。これにより、取引が合法的に実施され、何か問題があった場合の頼みの綱となるので、販売店は安心することができる。

逆に、消費者が販売店のアイデンティティを確かめるために販売店に認証書を要求する場合もある。ただし、このケースは本レポートでは詳しく取り扱っていない。消費者は、取引相手の販売店が公開鍵の本当の所有者であることを確認するための一手段として、販売店の認証を行いたいと考える。これにより、注文情報（支払いメカニズムにつ

いての条件などが含まれる）を悪用したいと考えている相手が注文情報を収集しているわけではないことを確認し、安心する。

否認防止とは、意図を表明した人物（たとえば、注文をした消費者）がその意図表明を否認することが不可能であることを示す。アイデンティティを確認するメカニズムが正しく機能している場合、否認防止の目標は容易になる。アイデンティティが確認されると、消費者に属する言明が実際には行われていなかったと消費者が主張する根拠はほとんど失われる。デジタル署名は、否認防止のための強力な方策となることが立証されているが、秘密鍵は現在のところ特定の環境（パスワードで保護されたネットワークやハードドライブのようなもの）で維持されており、理論的に言えば、暴力的に攻撃して鍵そのものを突き止めるのよりずっと少ない努力で鍵を奪うことが可能である。秘密鍵をスマートカードに格納するなどのハードウェアトークンにより、秘密鍵のユーザーが確かにその権限を与えられていることを確認することができる。バイオメトリクス装置と結びつけられたハードウェアトークンは、さらに確実性を高めることができる。

本人認証だけを提供するだけでも不正を減らすことに役に立つ。少なくとも、問題が生じた時の頼みの綱になる。否認防止は、実際に行った声明を当事者が不正に否認することを防止することにより、さらに不正を減らす。ただし、現在のところ完全に不正を排除した既存システムはほとんどない。せいぜいシステムは不正を減らすだけであり、排除できなかった不正がビジネスの必要経費の一部となる。

最終的に、認証書に記載された公開鍵は、メッセージダイジェスト（デジタル署名を添付した文書の内容を数値で表現したもの）の妥当性を検証するのに使うことができる。これにより、メッセージ（および認証書）の受取人は、内容が改竄されていないことを知る。また、これにより、メッセージ内容が送信された通りであることを送り手が立証することができる。両方のケースで、消費者および販売店は、メッセージ内容を信頼できると見なすことができる。

6.1.5 事務取扱の提案

オープンシステムにおいてデジタル署名を使った消費者取引を行う場合、（本レポートで記載している通り）消費者、ＣＡ、販売店の３つの主要エンティティがあり、これらの権利や責任が取引に影響する。その他のエンティティも重要な役割を果たすことができる。たとえば、ソフトウェアおよびハードウェアのプロバイダ、タイムスタンプ業者、認証プ

ロセスにおいてＣＡを助ける公証人、その他の補助サービスのプロバイダなど。

まず本セクションは、オープンシステムで３つの主要エンティティ（ＣＡ、消費者、および販売店）間の関係を分析するのに、どのような法的枠組みが最も適切かという問題を扱う。本セクションにおける我々の結論は、ＣＡと消費者との関係は契約によって支配するのが最も適切であり、ある程度の制限はあるものの、消費者はこの関係の条件について自由に交渉できるようにすべきだという提案を基本的に支持する。ただしＣＡと販売店の関係については、義務や責任範囲の割当を分析するのに最もよい枠組みは不法行為法であろうと主張したい。我々は、参照によって認証書に盛り込まれた契約条件と販売店を結びつけようとすることは、基本契約法の事例として当てはまらなくなる可能性があり、経済的に見ても非効率であり、健全な公共施策にも反すると考える。

次に我々は、ＰＫＩの参加者は理に叶った行動をすることが義務づけられており、理に叶った行動をした当事者が、理に叶っていない行動をした当事者により蒙った損害を負担すべきではないという我々の主張を解説する。この提案は２つの問題点が含まれる。１つは、「理に叶った」振る舞いとはどのようなことを指すのか。もう１つは、全ての当事者が理に叶った行動をしたのに損失が発生した場合、誰が損失を負担するのか。我々はこれらの問題のそれぞれを扱うが、まず我々は、消費者、販売店、ＣＡ、包括的な用語で言えば補助サービス提供者が行うものと予想される振る舞いについて考察する。次に、我々は「過ちのない」状況において誰が損害を負担すべきかという問題を取り上げる。消費者保護法制度の長い歴史から見て、消費者が理に叶った行動をしなかった場合でも、消費者の責任範囲を限定すべきであると我々は考える。

本セクションは、さらに総合的な研究や討議を行うための骨格を記載する。

(1)　不法行為対契約

①　ＣＡ/消費者関係

我々は、ＣＡと消費者との間の関係は契約によって支配するのが最上であると考える。効率と競争が優先する市場においては、消費者はＣＡの業績、サービス条件、経費などのパラメータをもとにＣＡを選ぶことができる。多くの場合、これらのパラメータは契約書に記載されており、消費者はこれを見て選ぶか止めるかを決めることができる。したがって、一般的な契約の強制力には制限があり、マーケットが効率的に機能できないような契約条項が少なからず存在する可能性があることを認めた上で、ＣＡと消費者との関係は一般的に契約がベースになるだろうと我々は予測する。

ＣＡが直面する技術的、ビジネス的、法的問題点は非常に多く、したがって特定の状況では、ＣＡは長くて極端に複雑な契約書を作成する必要に迫られる。これによって、市場が正しく機能しているにも関わらず望ましい結果が得られないという事態に結びつくわけではないが、これらの契約書を分析し理性的な判断を下すために消費者は大きな負担を強いられるという事実は理解しておくべきである。このような大きな負担があるために、消費者がＣＡを正しく見分けることができないという事態が発生する恐れがある。この場合、契約法によってＣＡと消費者との関係を統御するという代替手段を検討してみるのが適切であろう。

ＣＡ/消費者の関係を契約によって支配するというのは魅力的ではあるが､契約の成立に関して明らかな問題が多数存在しており、ギャップを埋め合わせたり、他の原則を導入することが必要である。（社会的弱者など）契約を締結する資格がないことに苦しむ消費者が発生するかもしれない。契約書の言語を話さない消費者がいるかもしれない（下の「国際的問題」を参照のこと）。非良心的であるが、適用法のもとでは違法にならないような契約があるかもしれない。結局のところ、契約の色々な部分でローカル法と矛盾を起こし、このため公共政策が無力になる可能性がある。

このため、この関係に対しては、デフォルト契約条件（たとえば、アメリカ商事法典など）や不法行為原則など、一連のデフォルトルールが絶対的に必要である。これらのルールは自己規制法典として作成し、参照または成文法により契約に組み込むことができる。電子市場は統一性や予測可能性を必要としているので、あまり形式化されていない代替手段が採用される可能性は低い。

② ＣＡ/販売店の関係

ＣＡと販売店の関係が自動的に契約によって支配されるべきかどうかは、あまり明確ではない。販売店は、認証書に含まれた情報の正確さだけを追求する（おそらく、このような情報を確認するのに必要な基礎サービスの成績も）。販売店が締結予定の各契約について、販売店側に調べる義務を課した場合、このプロセスに大きな取引コストがかかってしまう。販売店は複数のＣＡと取引を行うことがあり、それぞれのＣＡが実施規定を作成しているだけでなく、その実施規定も時間とともに改訂されることがあるので、受け取った認証書のそれぞれについて実施規定をチェックする必要がある。ＣＡは、自社のサービスを繰り返し使ってくれる販売店に関しては、特別に相互締結の契約をその販売店と取り決めるようにすると経費効率がよい。ただし、これ

はルールというより例外である

ＣＡと販売店の間に特別に取り決められた契約がない場合、最も効率的な責任割当方法は、既存の過失不実表明の不法行為である。これにより、ＣＡは自社の行動のコストを内部で負担するようになり、当事者に大きな取引コストを課すことがない。さらに、これにより、ＣＡが行き過ぎた条件を課して契約成立プロセスを悪用できないようにすると同時に、ＣＡは「理に叶った」行動をすることで責任を回避できるようにする。ただしＣＡは、自分たちがどのような事実を提供するか、それらの事実を確認するためにＣＡがどのような努力をしたかを明確にすることで、自社の立場を述べることができるようにすべきである。このように、ＣＡが約束したサービスを理に叶った方法で実行した場合、そのＣＡには責任を負わせるべきではない。ＣＡが誤った行動をした場合、ＣＡは販売店への責務を負担する可能性がある。ただし、この方法は、合衆国法の不法行為法と根本的に全く異なる不法行為法の原則を持つ大陸法には、限定的な適用しかできない。

(2)　理に叶った行動をする義務

損失割当の出発点として、各当事者は理に叶った行動をする義務を持つ。ある当事者が理に叶った行動をせず、その他の当事者が理に叶った行動をした場合、理に叶った行動をしなかった当事者が損害を負担するようにすべきである。したがって、これ以降の議論は理に叶った振る舞いに関して焦点を絞り、可能なら、当事者の振るまいが理に叶ったものかどうかを決定するために考慮すべき基準を提示したい。ただし、このプロセスにおいて消費者の役割が非常に大きいことを考慮して、消費者が理に叶った行動をしなかった場合でも消費者の損害を限定するように検討すべきであると我々は考える。また、全ての当事者が理に叶った行動をしているにも関わらず、ある当事者に損害が発生する可能性がある。このような状況については後述のセクション（７）で扱う。ただし、複数の当事者が理に叶った行動をしなかった場合の損失割当に関しては特に注意を払っていない。

(3)　消費者

消費者が以下の振る舞いを行った場合には理に叶った振る舞いと見なされる。

- 適切な情報を提供する：消費者が誤った、または不完全な情報を提供することは理に叶った行動ではない。消費者が認証の対象となっている情報を更新しないことは理に叶った行動ではない。

- 注意に反応する：消費者が認証書の確認または受入を行う機会を与えられたシステムでは、消費者は適切な時間内に認証書を見直し、誤りを迅速に修正するための適切な努力をすべて行う必要がある。
- 秘密鍵を安全に保管する：消費者は、自分の秘密鍵を安全にするために最大限の努力をすべきである。認証書が消費者のアイデンティティに関して異なるレベルの保証を提供している場合、消費者のアイデンティティを認証書が保証している度合いに応じて、秘密鍵を安全に保管するための努力も増やす必要がある。しかし現在、多くの消費者は自分の秘密鍵を、パスワードを入力してアクセスできるようなシステム上に保存している。パスワードは、無理矢理に鍵自身を突き止めるより簡単に入手できる。ハードウェアトークン（パスカードやスマートカードなど）またはバイオメトリックデバイスにより秘密鍵を格納する場合のセキュリティは向上するだろうが、これらの技術はまだ世界的に導入されているわけではない。さらに消費者は、ハードウェア、ソフトウェア、その他の装置プロバイダの指示を全て厳格に守るべきである。したがって、ハードウェアおよびソフトウェア製品を提供するエンティティは、明解で簡潔な指示を消費者に提供し、秘密鍵を安全に保管するために消費者が守らなければならない手順を詳しく解説すべきである。
- 鍵を安全に生成する：消費者が自分の鍵のペアを生成する場合、十分に信頼できるシステム上で安全な方法を使って実行しなければならない。繰り返しになるが、暗号ハードウェアおよびソフトウェアのサプライヤは、この目標を達成するために必要な手順を明解かつ簡潔に消費者に示さなければならない。
- 侵害された鍵を速やかに取り消す：消費者の秘密鍵が侵害された場合、その消費者は、侵害の事実に気が付いたらすぐに、対応する認証書を取り消すための手順を迅速に実行しなければならない。

(4)　販売店

販売店が以下の振る舞いを行った場合には理に叶った振る舞いと見なされる。

- 正しい認証書を要求する：消費者が様々な事実を主張したり、ＣＡが色々なレベルの保証をしていることを表すために「クラス」（認証書のタイプ）を設定すると、全ての当事者に都合がよい。ＣＡが、異なる事実の表明に合わせて認証書のクラスを設定したと仮定すると、販売店は適切なクラスの認証書を要求すること

に責任を持つべきである。たとえばＣＡが、消費者から提供された未確認の情報を、未確認であることをはっきりと断った上で記載しているような認証書のクラスがあったとすれば、その認証書の情報の正確さをＣＡが保証するように販売店が要求するのは理に叶っていない。逆に、消費者の識別情報を確認するために多大な努力を払ったことを明記した認証書のクラスでは、この認証書に含まれた情報が真実であると販売店が信じることは、一般的に言って理に叶っている。販売店が自分に最も適した認証書のクラスを選ぶようにさせれば、市場の効率性から考えて、ＣＡは自然に販売店のニーズに合わせた認証書クラスを提供するようになるであろう。ＣＡは、目的が限定された認証書や目的が特化された認証書を発行することも可能である。このような場合、認証書の特化された目的がアイデンティティ目的と違っている場合、販売店がこのような特化された目的の認証書をアイデンティティ目的に使うのは理に叶っていない。運転免許証や社会保険証のような、物理的な空間を占める証明書は、アイデンティティ証明の目的のために作られたものではないが、現在身元を証明する目的で使われている。

- 認証書を確認する：同様に、販売店は、有効期限が切れた認証書やＣＡ（またはＣＡのＣＡ）の署名を確認できなかった認証書（自己証明型のＣＡの場合は除く）を信用するのは理に叶っていない。また販売店は、異なる目的のために作られた認証書（たとえば、企業が社内の出入り管理に発行した認証書）を信用するのは理に叶っていない。
- 使用可能なＣＲＬをチェックする：ＣＲＬが基盤の一部として含まれていないような方式もインプリメント中であるが、もしＣＲＬが存在する方式の場合、取り消された認証書はＣＲＬに記載されるはずである。この場合、使用可能なＣＲＬをチェックしなかったことによるリスクは販売店自身が負うべきである。ＣＡは、ＣＲＬへのアクセスにサービス料金を徴収することを検討している。これが実現すると、ＣＡは販売店に契約条件を課すことができるようになり、販売店がＣＲＬをチェックする時の金銭的障害となるので、当事者同士の関係が大きく変化する。このシナリオへの対処は、まだ検討していない。
- その他の情報をもとに行動する：認証書に含まれている情報が正しくないことを販売店が知っていた場合、または知っておくべきだった場合、その販売店が認証書を信用するのは理に叶っていない。販売店側が当然払うべき合理的な注意義務

は、取引のサイズや当事者の「帯域外」（すなわち、インターネット以外の）関係の範囲に応じて増大する。

(5)　ＣＡ

ＣＡが以下の振る舞いを行った場合には理に叶った振る舞いと見なされる。

- 最初の消費者認証：ＣＡが消費者のアイデンティティを最初に確認する方法が多数存在する。最低限適用する必要があるような基準は存在しない。ただし、ＣＡはどのような方法で消費者の本人認証を行うかを指定すべきである。もしこれらの手順を正常に実行しなかった場合、ＣＡは理に叶っていない行動をしたことになる。最も基本的なレベルとして、ＣＡは消費者から提供された情報だけをもとに認証書を作成することができるようにすべきである。ただし、ＣＡは、認証書に含まれた情報は第三者によって確認されたものでないことを明確に表記する。代わりに、ＣＡが厳格なチェックのシステムを使ってアイデンティティを確認することを約束している場合、このようなチェックを実現することができなかったら理に叶っていないことになる。（これは、ＣＡがアイデンティティの絶対的な保証人になるべきであるという意味ではない。自分が自分に制定した義務は実行すべきであるという意味である。）上記の通り、市場の効率性が発揮され、販売店の要求によってＣＡが十分な消費者認証義務を引き受けるようになることを我々は期待している。
- 信頼できるシステム/鍵管理：ＣＡは、自分の業務のほとんどを自動的に行うので、コンピュータによるリスク、内部と外部の両方の脅威にさらされることになる。システムの欠陥による損失は範囲が広く、大きいものと考えられる。第三者がＣＡの秘密鍵を突き止めた場合、問題は非常に深刻になる可能性がある。ＣＡの秘密鍵を発見した人間は、表向きは有効だが実際は偽造された認証書を無制限に作成することができる。さらに、ＣＡの秘密鍵が危殆化し、対応する公開鍵が取り消された場合、そのＣＡから発行された認証書はすべて無効となる。そのＣＡを利用している全ての消費者は、新しい認証書を入手することを強いられる。ＣＡと消費者との契約関係によっては、ＣＡはシステム欠陥のコストを強制的に引き受けないでもよい場合がある。特に各消費者によって発生する個別コストが少額であり、ＣＡに請求するための通信コストの方が高くつく場合である。ただし、正しいシステム運転を確保することは重要であるが、まったくエラーのない完全

な運転を期待するのは公平ではない。基礎技術がダイナミックに進化しているので、特に最低限の技術標準を制定するのは意味がない。したがってＣＡは、システムが信頼できるようなものにするために、理に叶った努力をすべきである。このため、時間が経過して技術が向上するにつれて、理に叶った努力や信頼性の基準も高くなる。鍵管理の問題は特に悩ましいので、ＣＡが自分の暗号鍵を生成したり、保管したり、使用する場合、細心の注意を払うようにしなければならない。特に鍵を生成したり管理するための技術的環境は変化が激しいので、鍵管理に関してどのように振る舞えば理に叶った注意を払ったことになるのか、現在のところ明確に断定することができない。秘密鍵を秘密にしておくためにどのようなことをすれば理に叶った努力をしていることになるのか、秘密鍵が第三者に突き止められたことや鍵が秘密でなくなったことを発見した場合にＣＡはどのような義務を持つかを示唆するためには、さらに研究を重ねる必要がある。業界標準作成団体を設立して、この団体が技術的進歩を動的に評価し、適切な技術を導入するための標準を作成して信頼を向上させるようにするのがよい。業界がこのような標準を作成しない場合、政府で規定を作ってライセンス方式を実施することになるだろう。最低限我々が期待するのは、ＣＡがどのような段階を経て自分のシステムを信頼できるものにするのかを自由に開示してくれることである。システムは、一般大衆の注目を集めるだけでも信頼度が上がるものである。

- 監督上の義務：従業員の雇用や管理、記録の保管、契約や保険、その他の職務機能などに関する問題は、本レポートでは扱わない。このような問題はＰＫＩの運用を成功させるのに重要であるが、これらの問題点に関してはさらに研究が必要であると思われる。
- 認証書の失効/一時失効：ＣＡは、消費者から通報があれば、すぐに認証書を失効させることが期待される。多くの場合、ＣＲＬを保守することによって失効が行われる。このＣＲＬは、販売店が認証書を受け取る前に簡単にＣＲＬを確認できるようになっていなければならない。認証された事実に関して、それを継続して確認する義務をＣＡだけに負わせるのは公平ではない。認証された事実が間違っていることを第三者がＣＡに通報した場合、その問い合わせを確認するのはＣＡの義務であるが、ＣＡ独自で継続的に確認させるようにすべきではない。ただし、認証書の条件としてそれが定められていたり、消費者との間にそのような契約を

結んでいる場合は別である。誤った認証書を発行した場合の危害は、発行されるはずの認証書を発行しなかった場合の危害より大きいと考えられるため、何か疑わしいことがあれば認証書を発行しないようにＣＡに推奨するのがよい。したがって、認証書を発行すべきでないと信じるに足るような理由があった場合、選定されたＣＡが認証書を発行しなかったことによって損害が発生してもＣＡが責任を免れるように適切な原則を作っておくのがよい（当事者同士の契約内容によっては、このように認証書の発行をしないことは契約違反になる可能性がある）。ただし、ＣＡが認証書を発行できないと判断したら、迅速に消費者に連絡し、消費者側に誤解のないようにするのが適切であろう。

- 実施規定の発行：ＣＡは、認証書を発行する際にどのような実務慣行を採用しているのかを簡潔かつ明解に記載した実施規定または同等の文書を、簡単にアクセスして利用できるようにしておくべきである。ＣＡは、この実施規定に記載された規定に従うべきである。
- 認証書を入手可能にする：ＣＡは、消費者の認証書を確認したい人のために、自分の公開鍵に関する認証書を入手できるようにしなければならない。
- 財政的責任：ＣＡの潜在的責任に関連した損失をＣＡが負担できるように確保するための方法に関しては、本レポートの分析対象外である。ただし、ＣＡが自分の義務を果たさなかった場合、非常に多くの無実の当事者に対して大きな損害を与えることになることを指摘しておきたい。このような当事者に損害の補償を与えられるように確保することは、公共政策の重要な関心事である。同様に、ＣＡが突然ビジネスを止めた場合、消費者その他に大きなコストがかかってくる。実際問題として、破産や債務超過に陥っているエンティティに対して実施可能な義務を課すことは困難な場合がある。適切な情報公開があれば、自分に責任のある損失を負担するだけの余裕のないＣＡとビジネスを行った場合にどれだけのリスクがあるかを市場が適切に評価できるようになる。政策的観点として、このアプローチのためには適切な情報開示が実施されるようなメカニズムが必要である。

(6)　サードパーティサプライヤ

ＣＡ業界で見過ごされがちなのは、ハードウェア、ソフトウェア、インターネット接続、タイムスタンプおよび本人認証ベンダーなどの補助サービスのサードパーティ業者である。我々は、ＣＡがサプライヤを選ぶ時に適切な注意を払う義務について考慮すべ

きであることを指摘したい。場合によっては、ＣＡ自身が特に損失を引き起こすような行動をしていない場合でも、ＣＡとサードパーティ業者とが責任を共同で分担する場合もあり得る。多くのサードパーティサプライヤはＣＡとの間で契約関係を結んでいるので、サードパーティの過誤によってＣＡにも責任が及ぶような事態に備えるため、ＣＡはサプライヤに誓約、保証、損害賠償を明確に要求しておくべきである。

ＣＡのコントロールが全く及ばないような状況では、サードパーティサプライヤに損失の責任を負わせることができる。このような損失は、既存の法的原則によって支配される。ただし、サプライヤの種類は非常に多いので、全てのサプライヤに対して一般的に適用されるルールを要約することは不可能である。

公証人などの認証確認提供者には、特に難しい問題がある。ＣＡは、加入者が公証人の公証済み申請書を提出することが本人確認の方法の１つとなると実施規定に記載する可能性がある。もし公証人がニセの申請書を公証し、その結果としてＣＡが不正な認証書を発行してしまった場合、結果として生じた損失を負担するのはＣＡなのか公証人なのか。不正な申請者に主な責任があることは確実だが、このような状況では、ＣＡが公証人に訴訟申し立てをすると同時に、販売店もＣＡに損害賠償を請求できるようにすべきである。公証人への損害賠償請求を販売店に行わせるのは不公平である。公証人は地理的にも販売店から離れており、販売店の地方裁判所の裁判管轄にならない可能性がある。さらに、このようにリスクを割り振ることで、ＣＡは公証人やその他のローカルな本人認証代行業者と提携する時に十分な注意を払うようになり、公証人より厳格な本人認証手順を課すように仕向けることができる。

ＰＫＩに必要なハードウェアやソフトウェアを納入するサードパーティのサービス提供者に関しては、その他にも問題点がある。デジタル署名の基礎となる暗号方式や技術を実現するのは簡単な仕事ではない。上記のように、ハードウェアおよびソフトウェアの納入業者は、自社のシステムを納入すると同時に、システムを安全にするための方法を明確かつ簡潔に記述し、これを正確に守ることによって消費者は約束されたレベルのセキュリティを達成できるようにすることが要求される。

一部の法体系では、これらのサードパーティサプライヤに適用される特定ルールを規定しようとしている。重要性の高いサプライヤに関しては、これが適切かもしれない。

(7)　全ての当事者が理に叶った行動をした場合の責務の制限

上記のような基準を適用した場合でも、全ての当事者が理に叶った行動をしたにも関

わらず損失が発生することが十分に起こり得る。この損失の割り振りをどうするかということは、デジタル署名を広く普及させるために重要であるし、消費者取引を支援するという認証局の役割を強固にするためにも重要である。

「電子資金移動法」には、いくつかの点で興味深い類似がある。クレジットカード保有者は全く理に叶った振る舞いをしていても、クレジットカード番号を盗まれて損失を蒙ることがある。クレジットカード保有者の責務を制限するために、ＥＦＴＡ法では、クレジットカード保有者が番号盗難を届け出る前に発生した損失に関しては、多くの場合保有者は 50 ドル以上は責任を持たなくてもよく、番号盗難を届け出た後は損失責任がないものと規定されている。これと同様の構造をデジタル署名に適用できるようにした場合、デジタル署名を使いたいと考える消費者は非常に増加するであろう。したがって、ＥＦＴＡの類似および、理に叶った振る舞いをした当事者は損失リスクを負うべきでないという我々の根本原則に照らしてみて、消費者が上記の通り理に叶った振る舞いをしたら消費者の責務を少額またはゼロに制限すべきであると我々は考える。

ＣＡが理に叶った振る舞いをした状況では、我々は多くの理由からＣＡは損失の責任を負うべきではないと考える。全体的な見方をすれば、契約の違反や過失による責務が厳しいと市場に参入するのを躊躇するＣＡが増えるのは確実である。この時点では、業界全体にリスクを分散できるような効率的な市場は成立していない。このことは、ＣＡが多大な損失を蒙るリスクが数量化できないくらい大きいことを意味する。ＣＡが理に叶った行動をした場合の損失のリスクをＣＡに与えると、これらのリスクが当然のことと見なされるようになり、ＣＡ業界の発展を大きく阻害する可能性がある。しかし、全ての当事者が理に叶った行動をした場合、ＣＡは関連当事者の間でコストを配分するのに最も適した当事者であるので、保険市場および料金モデルが整備されていくにつれてＣＡの責務を見直すのがよい。

消費者とＣＡが理に叶った行動をしている場合、両方の責務を制限すべきであると述べたので、この構造での損失リスクは必然的に販売店にかかってくる。これにより販売店は、自分に重要な取引については「理に叶う以上の」注意を払うようになる。その取引が自分にとってどれだけ重要かを知っているのは販売店だけなので、販売店に責任を負わせると、自分の行動とリスク限度との測定を行うように促進される。消費者取引においては、販売店は消費者から料金を払ってもらう立場にあるので、販売店は料金モデルにビジネスリスクを組み込むことができる。例を挙げると、通信販売や電話注文の販

売店は、損失を顧客の間に割り当てることのできる立場にあるので、多くの場合彼らが損失リスクを引き受けているのが現状である。

損失割当メカニズムとは無関係に、業界発展を促進するための最も重要なステップは、当事者に対して明解でわかりやすいルールを設定することである。消費者が理に叶った行動をすれば消費者の責務は常に限定すべきであり、実際にそうなると考えられるので、ルールが明解でわかりやすければ、ＣＡおよび販売店は、規制や法的枠組みの下で適切な料金設定メカニズムを作り出す方法を見つけるであろう。下記（11）のような国際的な議論において、このことは易しい問題ではない。

(8)　「理に叶っていない」振る舞いに対する消費者の責務の制限

当事者間でのリスクの割当を分析する時に、 類似しているＥＦＴＡ法では、消費者が理に叶った行動をしなかった場合でも消費者の責務を限定していることに我々は注目した。消費者が理に叶った行動をした場合でも理に叶った行動をしなかった場合でも、ＥＦＴＡ法は消費者の責務を限定している。ただし後者の場合は、消費者はより大きなリスクを持つことになる。

消費者保護は、デジタル署名の利用を促進するために不可欠なステップであると我々は考えている。前に述べた通り、一般的なルールとして、ＰＫＩの参加者は、理に叶った行動をしなかった場合には責務を負い、理に叶った行動をした場合には責務を負わないようにすべきである。消費者が自分の秘密鍵を適切に保護せずに不正につながった場合を想定してみよう。理に叶っていない行動をした当事者が損失結果を負担するという我々の原則を適用すれば、消費者は不正による損失をほぼ無制限に引き受けることになる。無制限の損失が発生する可能性があれば、消費者がシステムに参加するのを躊躇することが懸念される。したがって、消費者が理に叶った行動をしなかった場合でも消費者の責務は制限するように考慮すべきであると考える。

我々は、ＥＦＴＡをそのままＰＫＩに使うべきだと言っているのではない。デジタル署名において消費者が理に叶った行動をしなかったことによる結果は、クレジットカードのモデルにおいて消費者過失による結果よりずっと大きい。ＰＫＩが成功するかどうかは、秘密鍵のセキュリティにかかっている。我々は特定金額とドルキャップ（上限額）を対応させることを推奨する立場にはないが、以下の３つの原則は検討する価値がある。まず、ＥＦＴＡ構造と同様に、消費者の行動の重要度に応じて、いくつかの階層レベルのドルキャップを設けるのが適切かもしれない。第二に、ドルキャップは、消費者が理

に叶った行動をするくらい高く、PKI への参加を躊躇させないくらい低くすべきである。第三に、意図的に不正を行った消費者にはドルキャップは存在しないようにすべきである。

消費者とＣＡの責務を制限した場合、販売店は、理に叶った行動をしていても、潜在的に返済されない損失を抱えることになる。販売店がデジタル署名を信用しようとする場合、このリスクを考慮して損得計算を行うのが前提である。大きなドル取引では、販売店は帯域外の保証を入手したいと考えるであろう。少額の取引では、販売店はこの危険負担を受け入れたいと考えるかもしれない。

返済されない損失の問題を最終的に解決するのは保険であろう。ただし、損失実績のパターンを作るだけのデータがないし、既存の法的枠組みではこれらの損失を予測するには不十分であるため、民間保険市場がすぐに発達するわけではない。それまでの間、上記の推奨事項を実施することで、ＰＫＩの参加者は適切な程度の確実性を与えることができ、消費者保護の方針を放棄しないでも理性的で経済的な選択を行うことができるようになる。

(9)　黙示の担保

本セクションは、黙示の担保の既存枠組みとその枠組みがあるべき姿について考える。

①　消費者向け

ＣＡは認証書を消費者に提供する。認証書が単なる実施サービスの請願書であっても、これは黙示の担保の対象となる。契約ベースの救済手段があっても、消費者はＣＡの過失に対して訴訟を起こすことができる。ＣＡは消費者との契約において黙示の担保を拒絶することができるようにすべきであるが、契約で過失を拒絶する可能性がある企業は設立が困難であり、したがって黙示の担保は存続することになる。したがって、消費者/ＣＡ関係には「新しい」黙示の担保は不要である。

②　販売店向け

我々は、ＣＡと販売店の間に契約関係を成立させるべきであると主張する。この場合、黙示の担保は形成されない。ただし、上記の通り、ＣＡと販売店で損失を割り当てるためには、不実表明の不法行為が効果的なメカニズムとなるように思える。その他の状況と同様に、ＣＡがこの不法行為を事前に拒絶することは困難である（契約がない場合は多分不可能である）。

(10)　契約違反/過失に対するＣＡの責務の制限

ＣＡは、ＣＡの労力のレベルや料金の多寡をベースに、いくつかのクラスの認証書を設定したいと考えた場合、責務についていくつかのドルキャップを与えることになる。この論理的根拠は完全に理解可能である。消費者から提供された未確認の情報を記載しただけの安い認証書は、十分に確認された高価な認証書と同じにすることはできない。消費者に関して、ＣＡが正当な認証書について自分の責務を制限するのは理に叶っているが、不当な認証書を発行したことに対して自分の責務を制限するのは不合理である。販売店に関しては、ＣＡと販売店の間に契約が成立していないので、販売店が既存の不法行為原則で自分の損害を賠償してもらおうとする場合に、ＣＡがこのようなドルキャップを適用して賠償額を制限しようとするのは根拠に乏しい。しかし、一部の状況では、記載されたドル制限が認証書への信頼に影響することを裁判所が認定することがあるかもしれない。

ほとんど全てのＣＡは、派生損害や同様の損害に対する責務を拒絶しようとする。消費者に関して、これらの責務を拒絶する能力に既存の制限が加えられないかぎり、この問題は契約で扱われるべきである。販売店に関しては、ＣＡと販売店の間に契約が成立していない場合、ＣＡが責務を制限するための契約ベースの原則は存在しない（派生損害の判定に関する制限のように、不法行為の責務に関する制限は存在する場合がある）。販売店との間に契約が成立している場合、不当性の原則により、ＣＡが不当に自分の責務を制限すること、特に過失に対して責務を制限することが厳しく制限される。

試験やデモンストレーションの場合は除き、ＣＡが直接損害に対する責務をすべて拒絶したり、原告側の金銭的損害の救済を実質的に拒否したのと同じくらい低いドルキャップを設定することは不合理である。

（11） 国際的問題点

裁判管轄、裁判地、法律の選択、法の抵触のような難しい問題は、本レポートの対象外である。消費者/ＣＡ/販売店の関係の多くが国際的になることは確実である。これらの国際的関係には複雑で難解な法原則に関係する。

ＣＡと消費者との契約が消費者の母国語で作成されない可能性があることから、契約関係が浸食されるのは確実である。消費者/ＣＡ契約書を外国語に翻訳するコストは大きい。契約成立に関する一般的なローカルルールを契約書に反映させて作成すると、コストはさらにかかる。多くの法体系では特定条項に対して契約で同意することを禁止しているものもある。このような関係から派生した訴訟が世界中で起こっているため、多様

なエンティティが、つぎはぎして作った一貫性のないルールに従わなければならないという事態が予測される。ＣＡは訴訟の弁護のために遠い裁判管轄地をいくつも担当する可能性があるので、この問題をさらに悪化させている。

わかりやすい規制枠組みを作ることで、このような結果を大幅に減らしたり取り除くであろうと考えられる。ＰＫＩおよびデジタル署名は電子商取引における基本ツールになる可能性がある。全ての当事者は、消費者のニーズを保護すると同時に市場に受け入れられるような標準を作成することで、本レポートで扱っている問題点を解決できるように投資をすべきである。

6.1.6 次のステップ

本レポートは「インターネットロー&ポリシーフォーラム」のパイロットプロジェクトとして開始されたものである。パイロットという言葉が示す通り、本レポートの対象は限られており、オープンマーケットの消費者取引における認証局の役割を全ての法体系に照らして議論したり検討することは意図していない。これらの体系については概観しているだけであり、またフォーラムやその他の手続きの裁判地における検討分野を以下のように限定している。

- 法的な分析においては、オープンシステムとクローズドシステムの間に明確な区別を定義する必要がある。クローズドシステムでは、全ての当事者が契約によってお互いを結びつけていると推定され、クローズドシステム内でどのように損失を配分するかも分析を行う必要がある。
- 国境を越えた消費者取引に影響を及ぼす可能性のある法的議題に関して、他の法体系、特に新興国の法体系の典型的な例を選んで分析する。
- 制定される法体系に既存のＣＡがどの程度準拠しているかに関して、分析を行う。
- １つの裁判管轄内において重複した法的原理がお互いにどのように影響しあうかを分析する。
- 消費者の機密情報やプライバシー情報に関するＣＡの取扱の標準化を行う。
- 分析を認証書の他の用途（たとえば販売店間の商業取引またはアクセスコントロールデバイスなど）に拡張する。
- 既存の立法制度で現行法に存在する法的曖昧さを解決できるかどうかを分析する。
- 販売店が消費者に認証書を渡した場合の損失配分をどうするかを分析する。

- ＣＡはどのようなシステムを利用すれば信頼できると見なされるのかについての標準を作成する。特に、ＣＡによる鍵管理や、第三者が秘密鍵を突き止めたことを発見した場合のＣＡの義務の問題を取り扱う。
- 従業員の雇用と管理、記録の保管、契約や保険、その他の職務機能など、ＣＡの監督義務に関する標準を作成する。
- ＣＡに対するサードパーティ業者（特に公証人、タイムスタンプ業者、ＰＫＩハードウェアおよびソフトウェア提供者、このプロセスにおけるその他の関係者）の責務を分析する。
- ＣＡ、販売店、消費者の間の損失配分に対する決済企業の影響を分析する。
- ＰＫＩの１当事者が理に叶った行動をしなかった場合の損失配分を分析する。
- ＣＲＬにアクセスするための料金が当事者の権利や責任に及ぼす影響を分析する。
- サードパーティのハードウェアおよびソフトウェア業者がＰＫＩで使われるリソースを納入した場合、責務または保証を拒絶する権限を分析する。
- 理に叶った行動をしない場合の消費者の責務にキャップを与えるための、適切なドルの価値やルールを設定する。

6.2　参考文献

1. 認証局運用ガイドライン：
   電子商取引実証推進協議会（ＥＣＯＭ）認証局検討WG　1998．4
   http：//www．ecom．or．jp/about-wg/wg08/phase1-result/final-guide．pdf
2. 認証に係る諸外国の法制度調査報告：
   電子商取引実証推進協議会（ＥＣＯＭ）認証局検討WG　1998．3
   http：//www．ecom．or．jp/about-wg/wg08/phase1-result/swg3-fin．pdf
3. 金融業界におけるＰＫＩ・電子認証について：谷口文一　　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　1999.8
   http://www.imes.boj.or.jp/jdps99/99-J-30.pdf
4. 金融機関等における個人データ保護のための取扱指針（改正版）：
   金融情報システムセンター　1999．4　http://www.fisc.or.jp/ippan_3.htm
5. 民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン:
   通産省 1996．12　http://www.miti.go.jp/past/d61203a.html
6. オンラインマーク制度の課題について-電子商取引における信頼性確保のために(1.0版)：電子商取引実証推進協議会（ＥＣＯＭ）消費者WG　1999．3
   http://www.ecom.or.jp/seika/rink/hyousi-1.htm
7. 電子商取引における個人情報保護に関する調査研究報告書：
   電子商取引実証推進協議会（ＥＣＯＭ）消費者WG　1998．3
   http://www.ecom.or.jp/about_wg/wg12/privacy-report1.html
8. 電子商取引における消費者取引に関する調査研究報告書：
   電子商取引実証推進協議会（ＥＣＯＭ）消費者WG　1998．3
   http://www.ecom.or.jp/about_wg/wg14/cr/consumer-report-index.html
9. ２１世紀デジタル社会の暗号政策への提言：暗号通信のあり方に関する研究会
   1999．6
10. 電気通信事業における損害賠償制度のあり方に関する調査研究会報告書：1986．7
11. ＰＬ法の製品別適用－判例と判決－：長瀬二三男　一橋出版
12. インターネット法（新版）：内田晴康、横山経通　1999．11　商事法務研究会
13. ベリサイン CPS: VeriSign Japan 1998.7
   http://www.verisign.co.jp/repository/CPS1.2/CPS1_2.pdf

14.日本認証サービス　SecureSign サービス標準規程　2000.3
http://www2.jcsinc.co.jp/repository1/policy1/SecureSign-CPS1_0.PDF
15.プライバシー保護ガイドライン：OECD　1980　http://www.oecd.org
16.消費者保護ガイドライン：OECD　1999　http：//www. oecd.org
17.The Role of Certification Authorities in Consumer Transaction:
Internet Law and Policy Forum 1997.4 http://www.ilpf.org/work/ca/draft.htm
18.Certification Authority Liability Analysis: American Bankers Association 1998.2
19.Digital Signature Guidelines: American Bar Association 1996.8
http://www.abanet.org/scitech/ec/isc/dsg-toc.html
20.Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527): Internet Engineering Task Force 1999.3
ftp://ftp.isi.edu/in-notes/rfc2527.txt
21.X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560): Internet Engineering Task Force 1999.6
ftp://ftp.isi.edu/in-notes/rfc2560.txt
22.Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols Internet Engineering Task Force 1999.10
http://www.ietf.org/internet-drafts/draft-ietf-pkix-dcs-03.txt
23.Directive of the European Parliament and of the Council on a Community framework for electronic signatures : 1999.11
http://bscw2.ispo.cec.be/eif/policy/diresen.doc
24.Utah Digital Signature Act: 1995.5
http://www.le.state.ut.us/~code/TITLE46/46_03.htm
25.Model Law on Electronic Commerce with Guide to Enactment: UNCITRAL 1996.12
http://www.uncitral.org/en-index.htm
26.Draft Uniform Rules on Electronic Signatures: UNCITRAL 1999.12
http://www.uncitral.org/english/sessions/wg_ec/wp-84.pdf
27.Common Criteria V2.1: Common Criteria Project 1999.8
http://csrc.nist.gov/cc/ccv20/p1-v21.pdf

6.3　メンバーリスト

事務局

米倉　昭利	電子商取引実証推進協議会　主席研究員
加藤　寛之	電子商取引実証推進協議会　主席研究員

顧問

大山　永昭	東京工業大学　像情報工学研究施設　教授
須藤　修	東京大学　社会情報研究所　教授
岩下　直行	日本銀行　金融研究所研究第二課　調査役

リーダー

船越　亘	株式会社富士通総研　研究開発部　主席研究員
長嶋　潔	東京海上火災保険株式会社　公務開発部電子商取引プロジェクトチームリーダー

メンバー

井関　勝博	電子商取引実証推進協議会　主席研究員
市川　卓	株式会社ジェーシービー　情報ネットワーク部ＩＣ事業開発グループ主任
春田　克治	日本認証サービス株式会社　営業担当部長
横山　恒一郎	財団法人金融情報システムセンター　調査企画部　研究員

監　修

横山　経通	森綜合法律事務所　弁護士

禁無断転載

平成１２年３月発行

発行：電子商取引実証推進協議会

東京都江東区青海２－４５

タイム２４ビル１０階

Tel　　03-5531-0061

E-mail　info@ecom.or.jp