H13－認証・公証ＷＧ－２

証明書利用形態に関する考察

平成１４年３月

電子商取引推進協議会
認証・公証ＷＧ

連絡先

電子商取引推進協議会（ＥＣＯＭ）

認証・公証ＷＧ

〒 105-0011

東京都港区芝公園　機械振興会館 3 階

TEL. 03-3436-7500

FAX. 03-3436-7570

Ｅ-mail： info@ecom.or.jp

目次

図表目次

はじめに

ＩＴ革命という言葉が使われるようになって久しいが、その中でもっとも身近に利用されているものがインターネットである。インターネット社会から享受しているものとしては、ウエッブブラウザ利用による各種の情報入手、電子メール、インターネットショッピングあるいは企業間取引等様々なものがある。これらは、個人あるいは企業が必要に応じて組合せ活用している。

一方、インターネットは相手の顔が見えない形態での情報交換、取引を行うことから、その安全性、信頼性に対する不安が払拭されないでいることも周知のことである。このような状況から、顔の見えない相手が確かな相手であることを認証あるいは確認する手段として、平成１３年４月施行の「電子署名及び認証業務に関する法律（電子署名法）」に基づく本人性確認により、認証の証として発行される「電子証明書（以下“証明書”と記述する）」を含め、公開鍵基盤（ＰＫＩ：Public Key Infrastructure）を利用したシステムから発行される証明書の利用が有効なものとなってきた。

また、証明書の利用にあたっても、インターネット利用への不安と同様に、その利用形態について明確に示されたものがないことも実情である。

「認証・公証ＷＧ」下の「電子認証システム利用検討ＳＷＧ」として、「電子認証サービス約款作成ガイドライン」の作成（電子認証利用モデル約款検討タスクフォース：ＴＦ３）と「証明書利用形態に関する考察」作成（証明書利用形態検討タスクフォース：ＴＦ４）が設定された。ＴＦ３は平成１２年度成果報告として「電子認証サービス約款作成ガイドライン」を作成し、ＴＦ４は昨年度に引き続き証明書の利用形態についての検討活動を行い本書の作成を行った。

ＴＦ４の目的として、「ＩＤの認証と資格・権限等の属性認証を如何に組合せると、効率的で信頼性の高い認証が実現されるか（証明書の利用ができるか）を検討し提言としてまとめる。」ことである。以下、活動の経緯と本書の構成について記述する。

目的の意識あわせを行うために、「法務省法人代表者証明書の利用に関するガイドライン」の勉強会を行った。主な結果として、属性認証の証明対象の確認、電子商取引のためには、本人性・実在性が必要である等の確認ができた。

証明書利用のビジネスモデルについての検討から、「ＩＤ認証とは、個人／法人のＩＤを証明すること」、「属性証明とは、個人／法人の属性を証明すること」との確認ができ

た。

また、現在の流れは、電子商取引を行う場面で個別に証明書が発行され利用する方式が多く、証明書管理の利便性は決して良い方向ではない。そこで、国民一人一人に公的な証明書を１枚発行する方式、さらに両者の中間的な形態として業界ごとに証明書を発行・利用する方式についても検討対象とした。

このような検討から、「シングル証明書の世界」、「個別証明書の世界」および「マルチ証明書の世界」を想定した証明書の利用形態について、現実の世界に適用させた場合の比較を行うことになった。

３つの世界について、現実の社会システム[1]への適用比較項目を挙げ比較検討を行った。

以上の検討経緯から、電子商取引を主体とした証明書の利用形態の検討を行い、将来へ向けた更なる証明書の有効活用の一助となることを期待して本書をまとめている。

本書は、証明書の利用形態として次の３つの世界を想定し、各々の有効性、利便性、効率性等から信頼性の高い認証の実現に向けた証明書の利用形態について提言としてまとめた。

- シングル証明書の世界
- 個別証明書の世界
- マルチ証明書の世界

本書は以下の５章から構成されている。

第１章では、本書の作成にあたっての検討目的および背景について、第２章以降の概要と合わせて記述している。

第２章では、ＩＤと属性認証について、検討段階での共通認識としての確認および定義を記述している。

第３章では、証明書の利用形態として想定した３つの世界について記述している。

第４章では、３つの世界を社会的観点から見た比較を行い、その比較データと比較分析結果を記述している。

[1] 本書では、「現代の社会において広く浸透し必要不可欠となっているシステム」（出典：日経BP社デジタル大辞典）の総称として使用する。

第５章では、証明書の利用形態検討から得られた、今後の利用形態の提言について記述している。

なお、本書はＰＫＩの基礎知識を有している読者を対象として記述している。但し、理解を助けるため、用語集と参考文献リストを文末に付録として添付している。

1　証明書利用形態検討の目的

1.1　　目的

電子商取引において電子認証システムを利用する場合、本人認証を行う認証機関と取引当事者との関係、対象となる認証者と資格、権限等の認証範囲、ＩＤ認証と属性認証の関連等様々な取り決め事項が、認証の適用がオープンな環境であれ、クローズドな環境であれ必要となる。更に、取り決め事項の内、電子認証システムを利用した本人確認の結果として発行される証明書の利用にあたっては、効率的で信頼性の高い証明書の利用形態についての検討が必要と考えられる。

証明書は、発行機関による本人確認の結果、電子認証システムを利用して認証対象者へ発行される。現在は、第三者の発行機関から発行される証明書を含め、証明書を利用するサービスごとあるいは、各企業または企業グループごとに個別に発行されているのが現状である。今後想定される証明書を利用したサービスに対して、サービスごとに異なる証明書を個々に取得することは、証明書の管理を含め利用者から見た利便性、効率性に課題あるいは問題の発生が予想される。これらの解決方法の一つとして、サービス提供業界共通で１枚の証明書を発行する形態や、運転免許証相当の個人に１枚のみ証明書を発行する形態などが想定される。

「証明書利用形態検討タスクフォース」としては、電子認証システムにより発行される証明書の利用形態について、社会システムとして広く普及させる観点から見た場合、現実の世界で多く用いられているサービスごとに取得する「個別証明書」では利便性、効率性等の観点から社会システムには成り難いと考え、現実の世界では実現されていないが一人に 1 枚の「シングル証明書」およびサービス業界等で１枚の「マルチ証明書」を想定し、その利用形態を検討した。想定した３つの証明書について、その発行形態、利用形態ごとに有効性、効率性等から、信頼性の高い認証の実現に向けた証明書利用にあたっての課題・特徴等を抽出分析し、各証明書の適用分野についての検討を行った。

また、証明書を利用するインターネット社会では相手の顔が見えないという特性があることから、実名以外を名乗る匿名性を許容する場合についての検討も合わせて行っている。

将来の証明書発行と利用形態の指針として、今後の電子商取引の普及に向けた提言の一助となる「証明書利用形態に関する考察」を作成し、今後のＰＫＩ普及への貢献を目的とした活動を行った。

1.2　　背景

証明書利用形態検討の背景として、ＩＤ認証と属性認証の関連についての検討と効率的な証明書の利用方式をまとめる中で、証明書利用形態のビジネスモデルを明確化し各種証明書の利用形態として「シングル証明書の世界」、「個別証明書の世界」および「マルチ証明書の世界」の３つが提案され、現実の世界における社会システムへ適用した場合との比較検討を行うこととなった。以下にその概要を記述する。

1.2.1　ＩＤ認証と属性認証の関連

ＩＤ認証と属性認証について、検討タスクフォース共通認識として、確認および定義を行った。

認証（Authentication）とは、「対象者が、本物（本人）であることを確認する」ことを意味する。対象者が個人である場合は、本人認証とも呼ぶ。認証する人（第三者）により、何をもって本人を確認するかは異なる。

認証は単独では行われることはなく、通常それによって権限等の確認が行われる。認証によって、対象者に権限を与えることを、認可（Authorization）と呼ぶ。認証と認可は、厳密に異なる行為である。

「ＩＤ認証」とは、「ＩＤを提示してもらうことにより確認を行うこと」と考えることができる。これに対して、「属性認証」という概念は一般にはない。ここでは「属性認証」を「ＩＤに付与された属性情報により、認可を行うこと」としている。

1.2.1.1　リアル世界における例

ＩＤ、および属性情報のリアル世界における例としては、次のような情報、証明書が挙げられる。

(1) **ＩＤ**

個人を特定する情報としては、戸籍記載情報あるいは住民票記載情報等が挙げられる。具体的には､名前と本籍､あるいは名前と住所の組み合わせが考えられる．これらを基に作られたＩＤの例としては、運転免許証、パスポートおよび社員証等が挙げられる。

(2) **属性情報**

属性情報としては、住所、氏名、生年月日、顔写真、所属部署、資格および発行者情報等が挙げられる。

1.2.1.2 ネット社会における例

ＩＤ、および属性情報のネット社会における例としては、次のような情報、証明書が挙げられる。

(1) **ＩＤ**

ＩＤの例としては、秘密鍵の対となる公開鍵を含む証明書が相当する。

(2) **属性情報**

属性情報としては、発行者情報、所有者情報、および有効期限等が相当する。

1.2.2 証明書利用形態検討として想定される世界

証明書の利用形態を検討するにあたって、以下の３つの利用（発行）形態（証明書の世界）についてそれぞれ定義し、技術面および適用局面（アプリケーション）からの調査・分析を行った。

1.2.2.1 シングル証明書の世界

一人に一枚だけ発行され、社会全体でその証明書が通用する世界。

世界の中でユニークに個人を特定できるＩＤからなる証明書。

1.2.2.2 個別証明書の世界

各発行機関（サービス提供会社）は個人に対して一枚しか発行しないが、利用者一人に同種の証明書が結果的に複数枚発行される世界で、サービスを受ける時はサービス提供会社ごとに証明書を使い分ける。

利用するサービスごとにユニークに個人を特定できるＩＤを含む証明書。

1.2.2.3 マルチ証明書の世界

一人に複数枚発行されるが、それぞれの証明書が通用する領域が異なる世界で、一枚の証明書で複数のサービスが利用できる。

クローズドな世界（国、地域、業界、特定の世界）の中で、ユニークに個人を特定でき

るＩＤを含む証明書。

上記の 3 つの世界における証明書の利用形態のまとめを表 1-1 に示す。

表 1-1 証明書の利用形態

証明書の世界	証明書利用形態／ サービス登録	証明書発行形態 （発行単位）	利用者が持つ 証明書の数
シングル証明書	個別	個人単位	１枚
個別証明書	個別	サービス単位	複数枚
マルチ証明書	業界等クローズな 世界内個別	業界等クローズな 世界単位	複数枚

1.2.3 現実の社会システムへの適用比較

シングル証明書、個別証明書およびマルチ証明書の各証明書の世界における利用形態の比較検討を行うにあたって、具体的な活動およびサービスを選定し、社会的観点から見た３つの世界における証明書の利用形態についての比較検討を行った。

1.2.3.1 人間活動の抽象的な名称での比較検討

人間活動の抽象的な項目として、以下の３パターンを挙げ、シングル証明書とマルチ証明書の世界を想定して比較する。表 1-2 では、一例として証明書の枚数について記述する。

表 1-2 シングル証明書とマルチ証明書の世界比較

活動名称	シングル証明書の世界	マルチ証明書の世界
情報収集・提供	１枚の証明書で入手・提供	社会、業界毎に証明書１枚
購入（調達）	１枚の証明書で購入	社会、業界毎に証明書１枚
販売	１枚の証明書で販売	対象地域・市場毎に証明書１枚
送信	１枚の証明書で送信指示	対象地域・市場毎に証明書１枚
受信	１枚の証明書で受信確認	対象地域・市場毎に証明書１枚

1.2.3.2 具体的なサービス名称での比較検討

現実の世界に存在している具体的なサービス名称として、以下の５パターンを挙げ、マルチ証明書と個別証明書の世界を想定して比較する。表 1-3 では、一例として証明書の枚数について記述する。

表 1-3 マルチ証明書と個別証明書の世界比較

サービス名称	マルチ証明書の世界	個別証明書の世界（現実）
クレジット サービス	クレジット業界で 証明書 1 枚	カード会社毎に証明書 1 枚
銀行サービス	銀行業界で証明書 1 枚	銀行毎に証明書 1 枚
マイレージサービス	マイレージサービス提供 業界で証明書 1 枚	マイレージサービス提供会社毎 に証明書 1 枚
損害保険	保険業界で証明書 1 枚	保険会社毎に証明書 1 枚
会社毎の 情報提供サービス	全社共通情報提供サービス で証明書 1 枚	社内情報提供サービス毎に 証明書 1 枚

2　ＩＤと属性について

2.1　ＩＤ とは

2.1.1　ＩＤの定義について

本書では「ＩＤ」を、「対象者を識別(identify)するための情報、または、その情報を記録した物理的な物体」であると定義する[1]。ＩＤは、ユニークに特定するための情報であるだけでなく、ＩＤの所有を確認することにより、対象者が本物（人）であることを保証する効果を持つ。

ＩＤは、しかるべき発行者から対象者へ与えられる。対象者は、ＩＤを提示することにより、検証者に、自分が本人であることを示すことができる。本人であることが確認することにより、検証者は、サービス提供等を行うことができる。ＩＤの発行、利用について、その関与者との関係を図に示す。

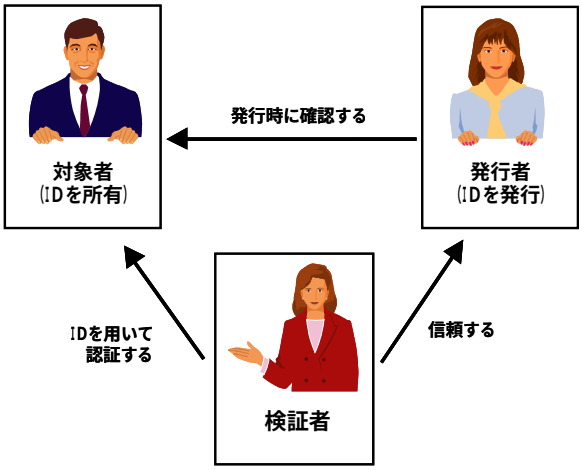


図 2-1 IDとその関与者

2.1.2　ＩＤ（識別情報）の表現方法

ＩＤには、その対象者を識別するための情報が含まれている。この識別情報は、発行者により、想定された範囲でユニークであることが保証される情報である。この識別情報の

[1]運転免許証そのものをIDとして扱う場合と、その部分情報をIDとして扱う場合がある。そのため、どちらも包含する定義としている。

表現として、シリアル番号等の数値や文字列で表現されるものがある。また、画像データや生体情報[2]が使用されることもある。これらの情報は、組み合わされることによりユニークに識別されることもある。

2.1.3 ＩＤの信頼性について

ＩＤは、発行時に、発行者により対象者(本人)と結びつけられる。ＩＤの信頼度は、発行者が、本人とＩＤの結びつけをどれだけ確実に行っているか、および、ＩＤの複製がどれだけ困難であるか、の２点に依存している。前者については、発行者が、他の（発行者が発行した）ＩＤをよりどころにして、新たなＩＤを発行することもある。新たに発行されたＩＤの信頼性は、参照した元のＩＤの信頼性を超えることは無い。後者については、物理的な性質や公開鍵暗号方式等により、ＩＤの複製を防ぐとともに、法的な規制によって複製を抑制することも行われている。

2.1.4 ＩＤの性質

ＩＤは、発行者やその保有情報により、資格や権限を意味することもある。すなわち、ＩＤは、後述の属性の性質も保持していると考えることができる

2.1.5 デジタル情報ＩＤと物理的なＩＤ

運転免許証に代表される物理的なＩＤと、電子証明書のようなデジタル情報ＩＤの違いは、その正当性の根拠にある。

例えば、運転免許証は、物理的に複製物との見分けが付きやすい作りになっていると同時に、法律によって複製を禁止されている。これに対して、電子証明書は、電子データであるため自由に複製できるが、それに対応する秘密鍵情報を対象者が安全に保持していることにより、正規の所有者しか使用することができない。また、電子証明書に記載された公開鍵と対応する秘密鍵をセキュアな（耐タンパー性のある）ハードウェアトークンに格納することにより、物理的に秘匿することも行われている。

以下の表に、デジタル情報ＩＤと物理的なＩＤの例をまとめる。

[2] 例えば、DNA等の遺伝子情報も、識別性についての手法が確立されると利用できる可能性がある.

表 2-1 デジタル情報IDと物理的なID

	発行時確認方法	記載項目	利用時識別情報	利用時確認方法
運転免許証	戸籍抄本等 顔写真と申請者の確認	免許証番号 氏名 本籍、住所 生年月日 顔写真 他	顔写真 免許証番号	・本人と見比べる ・免許証番号により確認
電子証明書	申請書類（多種） 秘密鍵の確実な所有	発行者情報 シリアル番号 所有者情報 公開鍵情報 他	(１)公開鍵情報 (２)発行者＋シリアル番号	・署名情報を公開鍵で複号して確認

2.2 属性とは

2.2.1 属性の定義について

ここでは、「属性」を、「対象者に与えられる資格や権限をあらわす情報」と定義する。属性は、ＩＤと結びつけられることによって、しかるべき対象者に対して、その資格や権限を示すことができる。また、属性は同じ権限を持った対象者に共通な情報であることがあり、一般的に識別性は持っていない。広義には、氏名や住所等の直接権限や資格と結び付けられていない情報も、属性として扱う。これは、資格や権限を検証する側の情報（利用者データベース等）により、権限や資格と結びついていることもあるからである。

2.2.2 ＩＤと属性の関係

属性は、単独(ＩＤ無し)で利用することはできない。また、ＩＤはそれ自体属性の性質を持つことから、単独で利用することができる。ＩＤと属性の組み合わせによって、認証

への利用可否は以下の通りである。

○ ＩＤ（単独）

○ ＩＤ＋属性

× 属性

ＩＤと属性の例として、パスポートとビザ（入国許可証）があげられる。パスポートは、旅行者自身を識別するＩＤであり、ビザは、旅行対象国によって必要となる属性である。旅行対象国によってビザが必要となるが、提示する際は、必ずパスポートを同時に提示する必要がある。パスポートを単独で利用できる国も存在するが、ビザを単独で提示することはない。

2.2.3 属性の動的性質(変更性)

属性には、本質的にＩＤ発行時に静的に決定するものと、動的に変化するものが存在する。例えば、氏名等の情報は、発行時にＩＤに含めることができる静的な属性である。動的に付与、変更される権限に対応する属性をＩＤに含めることはできない。このように動的に変更される属性を実現する方法として､以下の 2 つがある.

① 権限や資格を検証する側の情報（利用者データベース等）により、権限管理を行う。

② 属性証明書[3]のように、既発行のＩＤに対して属性を動的に結びつける。

[3] 「属性証明書(Attribute Certificate)」とは、公開鍵証明書と属性情報を紐付けたものである。属性証明書は、X.509 仕様にて規定されており、そのプロファイルについては、IETF PKIX WG で議論されている。

2.3 ＩＤ認証と属性認証

2.3.1 認証とは

認証(Authentication)とは、「対象者が、本物(本人)であることを確認する」ことを意味する。対象者が個人である場合には、本人認証とも呼ぶ。認証する人（第三者）により、何をもって本人を確認するかは異なる。

認証は単独で行われることはほとんど無く、通常それによって権限等の確認が行われる。認証によって、対象者に権限を与えることを、認可(Authorization)と呼ぶ。認証と認可は、厳密には異なる行為である。

2.3.2 ＩＤ認証と属性認証

本書では、「ＩＤ認証」は、「ＩＤを提示してもらうことより認証を行うこと」と定義する。これに対して、「属性認証」という概念は一般には無い[4]。本報告書では、「属性認証」とは、「ＩＤに付与された属性情報により、認可を行うこと」と定義する。

[4]「属性証明書」(前出)は、ここで述べている「属性認証」とはまったく違う概念である。

3　証明書利用形態における３つの世界

リアル社会では様々な ID（身分証明書、会員証、クレジットカード、キャッシュカード等々）を個人は使い分けている。しかしながら、ネット社会においてリアル社会を単に移行しただけの形態で ID が持ち込まれれば、それに対応した証明書は判別しづらく（リアル社会の証明書はデザイン、形状など多種多様だが、ネット社会の証明書は単なるデジタルデータのため）、個人にとっては利便性とても低いものとなってしまう。

本章では理想の世界（シングル証明書の世界）、リアル社会がそのままネット社会に移行した世界（個別証明書の世界）を考え、理想と現実の中間を模索した世界（マルチ証明書の世界）を導き出し、次章以降で具体例をまじえて解説を行なっていく。

3.1　シングル証明書の世界

3.1.1　シングル証明書について

(1) 定義

ネット社会においてユニークに個人を特定できる ID（個人特定ＩＤ）と基本的な属性情報からなる証明書。

(2) 特徴

住民票などに準じた個人一人一人に発行される公的な証明書[5]。

(3) 証明書記載事項

個人をユニークに特定する ID と氏名、生年月日、住所、性別など通常身分証明に必要な属性情報のみ。

(4) 発行審査

厳密な本人性確認手段と属性を証明する公的文書。

3.1.2　シングル証明書世界モデル

(1) 定義および特徴

シングル証明書があれば、利用したい全てのサービスへの利用・登録が可能となり、ネット社会でのオールマイティな身分証明書として使用できる。各個人はシングル証明書 1 枚のみを保有する。

---

[5] 理想的なモデルを想定しており、住基カードや公的個人認証等を想定しているものではない。

(2) **個人の利便性とプライバシー**

証明書を 1 枚のみ管理すれば良く、利便性は高い。しかし、基本的な属性情報は証明書に記載されるので必ずしも提示しなくても良い情報まで提示する場合がある。

(3) **認証局と登録機関**

認証局は一つであって登録機関はサービスに対応した数で複数存在可能。

(4) **モデル解説**

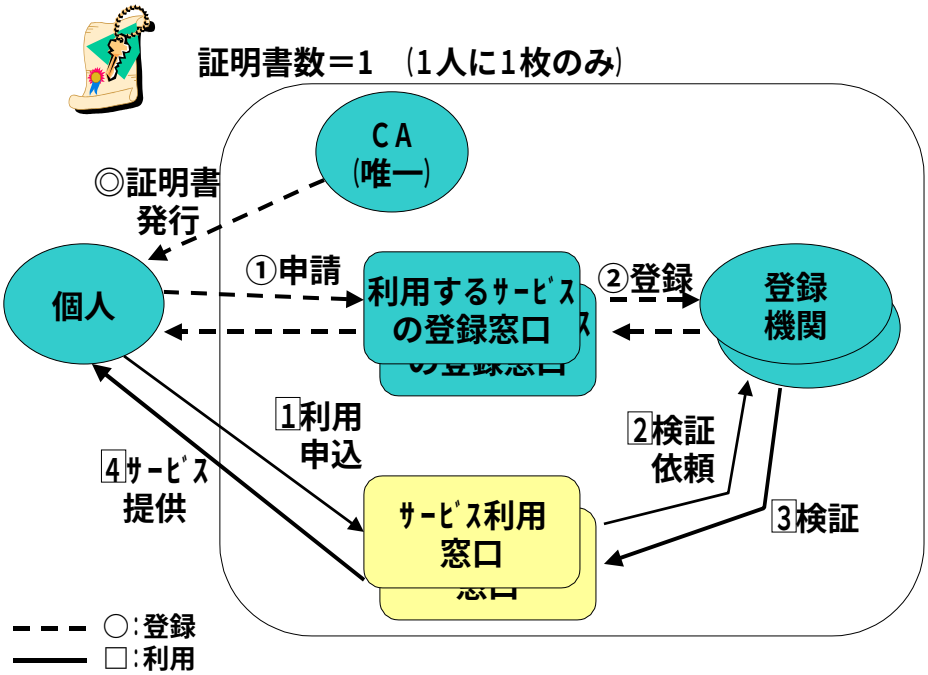


図 3-1 シングル証明書の世界

A. **モデルの前提**

個人にはシングル証明書が 1 枚発行される。

利用するサービス毎にサービスの利用登録をする窓口（以下、サービス登録窓口）とサービスの利用提供を受ける窓口（以下、サービス利用窓口）、リポジトリへの登録およびサービスからの検証を受付ける機関（以下、登録機関）が存在する。

B. **サービスへの登録**

個人はサービスを利用する前に登録が必要となる。シングル証明書には基本的な属性しか記載されていないために、その他サービス提供に必要な属性情報はここで確認される。

①個人は利用するサービス登録窓口にシングル証明書を提示し､本人性の確認およびサービス提供に必要な属性情報の確認を行う。

②サービス登録窓口は個人から申請のあったシングル証明書とその他属性情報を登録機関に登録する。

C. **＜サービスの利用＞**

個人がサービスを利用する際は以下のようなフローとなる。

1 個人はシングル証明書をサービス利用窓口に提示する。

2 サービス利用窓口は提示されたシングル証明書が登録されているか登録機関に検証依頼を行う。

3 登録機関にて検証され、検証結果とその他属性情報が応答される。

4 検証結果に基づきサービスが提供される。

3.1.3 社会システムとしての考察

唯一であるがゆえ使い分けが出来ず、匿名性も持てない。住民基本台帳法にて問題になった個人の情報管理につながるとの批判も受ける可能性があり実現性については疑問視される。

3.2 個別証明書の世界

3.2.1 個別証明書について

(1) 定義

利用するサービス･アプリケーション毎にユニークに個人を特定できる ID を含む証明書。

(2) 特徴

個人はサービス・アプリケーション毎に申請登録し、複数の証明書を保有する。属性情報を必ずしも必要とせず、ネット社会での匿名性も確保出来る。

(3) 証明書記載事項

基本的にサービス・アプリケーション毎にユニーク性を確保するための ID のみ。

（属性情報は記載されなくなる傾向にある。）

(4) 発行審査

サービス・アプリケーション毎に異なる。決裁行為など本人確認の厳密性を要求さ

れるものから、チャットの世界のように緩やかな本人確認でニックネームも許容するものまで様々である。

3.2.2 個別証明書世界モデル

(1) 定義および特徴

現実の世界をネット社会に置き換えていくスタイルとなる世界。サービスの提供条件によってはニックネームの使用が可能で匿名性を確保でき、ネット社会での自由度は高い。

(2) 個人の利便性とプライバシー

サービス・アプリケーション毎に証明書を管理する必要があるため利便性は低い。プライバシーの観点からは基本的に会員番号など ID のみなど必要最小限の情報が公開されるためプライバシーは確保される。

(3) 認証局と登録機関

サービス・アプリケーション毎に認証局が存在し、認証機関と登録機関が分離されていない。

(4) モデル解説

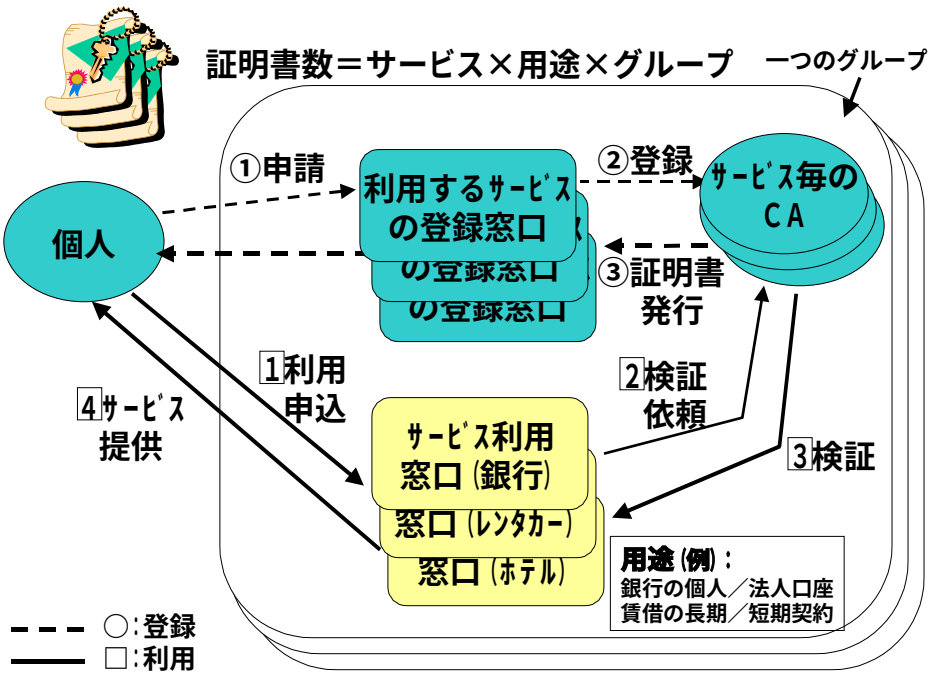


図 3-2 個別証明書の世界（現実の世界）

A. **＜モデルの前提＞**

個人には個別証明書が複数枚発行されている。

利用するサービス毎にサービスの利用登録をする窓口(以下､サービス登録窓口)とサービスの利用提供を受ける窓口（以下、サービス利用窓口）があり、レポジトリへの登録およびサービスからの検証を受付ける認証機関（以下、サービス毎のCA）が存在する。

B. **＜サービスへの登録＞**

個人はサービスを利用する前に登録が必要となり、以下のようなフローとなる。

①個人は利用するサービス登録窓口に申請を行い、

②サービス登録窓口は個人から申請のあった本人確認の情報をもとにサービス毎の CA に証明書発行依頼を行う。

③サービス毎の CA は個別証明書の発行をサービス登録窓口経由で行う。

C. **＜サービスの利用＞**

個人がサービスを利用する際は以下のようなフローとなる。

1 個人は個別証明書をサービス利用窓口に提示する。

2 サービス利用窓口は提示された個別証明書が有効であるかサービス毎の CA に検証依頼を行う。

3 サービス毎の CA にて検証され、検証結果とその他属性情報が応答される。

4 検証結果に基づきサービスが提供される。

3.2.3 社会システムとしての考察

証明書に記載されるのは会員番号などのサービス・アプリケーションで管理される ID のみであるため、一方で匿名性を確保出来る利点があるが、他方で他のサービス・アプリケーションで２次利用されることはない。個人で所有する証明書の枚数は各サービス・アプリケーション毎の認証局において相互認証などして少しは減らす工夫は可能である。

しかし、個別証明書の世界では効率的な証明書利用方式ではなく、工夫にも限界があるため社会システムにはなりにくい。

3.3 マルチ証明書の世界

3.3.1 マルチ証明書について

(1) **定義**

閉じた世界（国、地域、業界、あるいは個人が決めた特定の世界であっても良い）の中で、ユニークに個人を特定できる ID を含む証明書。

(2) **特徴**

マルチ証明書があれば、その閉じた世界で利用する全てのサービスの利用・登録が可能である。

(3) **証明書記載事項**

基本的にサービス･アプリケーション毎にユニーク性を確保するための ID のみ。(属性情報は記載されなくなる傾向にある。)

(4) **発行審査**

トレーサビリティを確保するための厳密な本人性確認手段は必要となる。証明書の記載事項になる属性情報の確認のため属性を証明する公的文書の提示が求められる。

3.3.2 マルチ証明書世界モデル

(1) **定義および特徴**

シングル証明書の世界と個別証明書の世界の中間解。利用者は行政・業界（マーケットプレイス）毎に発行された証明書を何枚か使い分ける。

(2) **個人の利便性とプライバシー**

業界毎に発行された証明書を数枚使い分けることとなるが利便性は個別証明書世界に比べると非常に高くなる。基本的に閉じた世界でプライバシー情報が共有されるため、利用者が意図していない事業者まで個人情報にアクセスする可能性がある。

(3) **認証局と登録機関**

認証局は業界毎に１つ存在し、その認証局に対応する登録機関が複数存在する。

(4) **モデル解説**

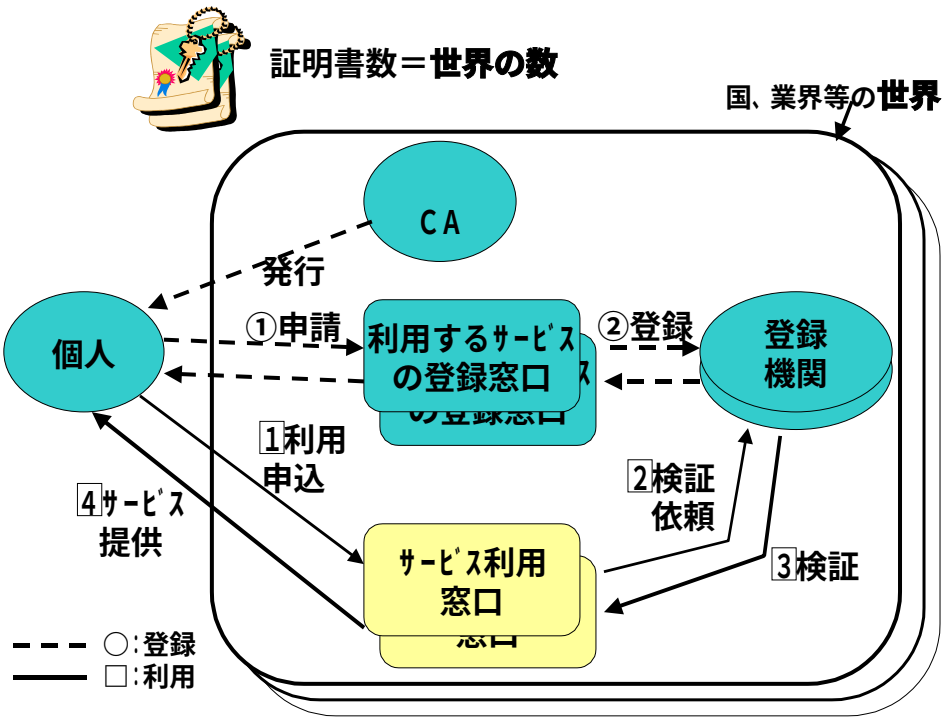


図 3-3 マルチ証明書の世界

A. **＜モデルの前提＞**

個人にはマルチ証明書が複数枚発行されている。

マルチ証明書の発行は行政･業界毎に設立している認証局もしくは特定認証業務の認証局から発行される。

利用するサービス毎にサービスの利用登録をする窓口(以下､サービス登録窓口)とサービスの利用提供を受ける窓口（以下、サービス利用窓口）があり、リポジトリへの登録およびサービスからの検証を受付ける登録機関が存在する。

B. **＜サービス利用の登録＞**

個人はサービスを利用する前に登録が必要となり、以下のようなフローとなる。

①個人は利用するサービス登録窓口にマルチ証明書を提示し､本人性の確認およびサービス提供に必要な属性情報の確認を行う。

②サービス登録窓口は個人から申請のあったマルチ証明書とその他属性情報を登録機関に登録する。

C. **＜サービスの利用＞**

個人がサービスを利用する際は以下のようなフローとなる。

1 個人はマルチ証明書をサービス利用窓口に提示する。

2 サービス利用窓口は提示されたマルチ証明書が登録されているか登録機関に検証依頼を行う。

3 登録機関にて検証され、検証結果とその他属性情報が応答される。

4 検証結果に基づきサービスが提供される。

3.3.3 社会システムとしての考察

業界毎に統一された認証が可能となり、個人情報保護の観点を網羅すれば社会システムとしての素地を満たす。

サービスの提供条件によってはニックネームの使用が可能で匿名性を確保でき、ネット社会での自由度は高くなる。（サービスの登録時に本人性の確認は行われているが、名前を名乗らなくても済むため、個人が安心して証明書を使えるようになる。）

4　社会的観点から見た３つの世界の比較

現状の人々の活動においては、運転免許証のように本来の運転に関する資格を証明する以外にも、公的証明書として個人の身分を証明するためによく用いられる証明書、クレジットカードのように複数の加盟店で種々のサービスを受けられる証明書、レンタルビデオショップの会員証のように個別のサービスのみで利用できる証明書がある。本章では、種々のサービスにおける証明書の使われ方を参考にしながら、３章で示したシングル証明書、マルチ証明書、および、個別証明書の利用形態を評価する。

具体的な比較は次のように進めた。評価の対象として抽象的なサービス、及び具体的なサービスを選択した。これらの概要を４．１項に、また、比較データを４．２項に示す。更に、これらについて以下の３つを評価した結果を４．３項に示す。

①　複数のサービスから利用されるシングル証明書の要件
　抽象的サービスを対象としてシングル証明書の概要を考察

② シングル証明書、マルチ証明書の比較
　抽象的サービスを対象として証明書の利用方法を考察

③ マルチ証明書、個別証明書の比較
　具体的サービスを対象として、証明書の利用モデルを考察

各証明書間の比較は、Ａ．概要／定義、Ｂ．特徴、Ｃ．ネット社会での自由度、Ｄ．運用性、Ｅ．セキュリティ、Ｆ．緊急時対応、Ｇ．コストの各項目について行った。これら項目の意味付けについては、証明書世界の比較項目の意味付け（表 4-1）の通りとした。

なお、本章での比較評価にあたっては、下記を想定した。

①　社会システムでの利用形態面から検討を行い、証明書の形式、有効性確認方法など技術面でのインプリメント方法との対応は考慮しない

②　社会システムとの対応を考える上で、シングル証明書：１人１枚、マルチ証明書：ドメイン内の複数サービス間で１枚、個別証明書：サービス毎に１枚、各々使われるものを想定した

③ ドメインとしては業界、地域などの領域を想定した

④ サービスとしては抽象的サービスについては利用方法を仮定し、また、具体的なサ

ービスについては実際のサービスの内容から証明書の利用モデルを想定し、特性を評価した。

表4-1 証明書世界比較項目の意味付け

比 較 項 目		内 容	
分類	項目	意味付け（例示）	備考
A.概要/定義	1.何を認証するか	自然人本人の特定、契約者の特定、決済手段との対応等の別。	
	2.証明書の持つ情報	格納情報の特徴	
	3.格納情報	住所、氏名、会員コード等具体的な格納情報	
	4.ＣＡの数	証明書所持者当たり、及び対象世界の中での CA 数	
	5.証明書枚数	証明書所持者当たりの枚数。類似目的のために、時期を区切って証明書が発行される場合で、１時期には１枚のみ利用可能な場合の枚数は１枚とする。	
	6.使用場面（限定する場合記入）	アプリケーション毎の利用場面	
B．特徴		各証明書の利用法の特徴	
C.ﾈｯﾄ社会での自由度	1.名義（仮名）を持てる	自然人本人の本名でなく、別名の利用可否	
	2.プライバシー	個人情報の分散範囲等	
	3.制御(利用側)	複数の別名証明書等の利用可否等	
	4.ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	不正発生時のトレース可否、要否／レベル等	
	5.サービス設計	サービス設計の影響範囲	
	6.ユーザ鍵ペアの有効期限	有効期限の目安、更新方法（自動更新の要否）等	
	7.審査/発行/更新	審査の厳密さ。対面手続き要否等。	
D.運用性	1.紛失時： 失効・削除・再発行	紛失時影響範囲、処理等	
	2.認証ｻｰﾋﾞｽ利用の課金	認証サービス利用（AP サービス利用）時の料金（事業者／利用者の負担）、課金方法等	
	3.証明書の配布	配布元（CA 等）、配布の際考慮すべき事項等	
	4.証明書の利用実績の通知	証明書の利用（AP サービスの利用）実績の通知方法、通知周期、通知内容等	
	5.約款の送付	送付方法、送付タイミング、内容等	
	6.メディア（格納デバイス）	媒体、所要容量、アクセス制限有無等	
	7.取り扱い留意点	秘密鍵の紛失時の影響、対処等留意点	
E.ｾｷｭﾘﾃｨ	1.運用 1.1.貸借 1.2.耐犯罪性	 禁止／許可の別（他人利用の可否） 発生しうる犯罪の種類、影響、対処等	
F.緊急時対応(ﾘｽｸの集中度)	1.検証局のダウン	証明書の有効性をリアルタイムに検証する検証局のダウン時の影響、対処方法等（ダウンすると証明書が紛失などのため失効されていても検証できない）	
	2.ネット上のサービス窓口	AP サービス窓口がダウンした場合の影響、対処方法等	
G.コスト	1.発行 1.1.審査/発行/ 1.2.更新/失効/削除	 審査、発行等に必要なコスト見積り。証明書を使う ことによるコストセーブ可能性等	
	2.運用 2.1.運用体制 2.2.ﾈｯﾄﾜｰｸ･ｷｬﾊﾟｼﾃｨ	 トラフィックの集中、利用時間帯の要件及びそれらの 観点から見た運用コスト、コストセーブ可能性等	

4.1 比較分析

4.1.1 シングル証明書とマルチ証明書の比較

人間活動の抽象的な名称として、情報収集・情報提供、購入（調達）・販売、送受信を選び､比較検討を行った。

4.1.1.1 情報収集・情報提供（選挙）

情報提供と情報収集として、選挙を例にして比較した。国政選挙もしくは地方選挙等の選挙において電子証明書が使用される場合に、シングル証明書とマルチ証明書、及び個別証明書の世界においてどのような差異が生じるかについて比較分析を行う。

投票においては、投票を行う者を証明書を用いて本人認証し、投票の権利を確認すると同時に、投票の秘密を守るという観点から、投票の内容が投票者と関連づけられないような仕組みの提供が求められる。これは一般に、利用者の認証を行うフェーズと、投票行為のフェーズを切り分ける等の方式により実現されるもので、アプリケーションを設計する際に特に注意が必要とされる部分である。

また、選挙は脅迫や買収などの不正行為の対象となりやすいため、その点についても十分な考慮が求められる。

(1) 「選挙」における証明書世界の比較

比較の前提とする選挙の仕組みとしては、インターネット等のネットワークを使用したオンライン投票、及び利用者が投票所に出向いて対面にて投票を行う方式(現在の方式)の両方のケースを検討の対象とする。ただし、この 2 つの方式は、利用端末が自宅に存在するか、投票所に存在するかという違いはあるものの、電子証明書の利用形態としては同一と考えられるため、ここでは特に区別を行わない。このうち、インターネット等のネットワークを使用したオンライン投票においては、特に脅迫や買収等の不正行為の脅威が大きくなるため、システムの設計には細心の注意が必要とされる。

① シングル証明書の世界

シングル証明書の世界としては、選挙に限らず、あらゆるサービスで利用される証明書が個人に対し 1 枚だけ発行される状況を想定する。結果として、すべての種類・時期の選挙においてこのシングル証明書が使用されることとなる。

シングル証明書には個人を特定するための最低限の属性情報（氏名等）のみ記載

されることが考えられ、選挙で必要となる付加情報は原則記載されない。よって、選挙を実行するにあたって必要な情報(年齢や転入年月日など)は、証明書以外の手段で提供する必要が生じる。

シングル証明書の世界では、すべての選挙において 1 枚の証明書が用いられるため、個人から見ると管理負担は小さいが、万が一その鍵が危殆化した場合や対象検証局がダウンした場合には、選挙を含めたあらゆるサービスが受けられなくなるというリスクがある。このため、より厳重な鍵の管理ならびに検証局の高信頼化対策が必要となる。

② マルチ証明書の世界

マルチ証明書の世界としては、選挙のみに使われる証明書が利用者に対して発行され、その 1 枚の証明書が公的に行なわれるすべての種類・時期の選挙において使用することができる状況を想定する。

この場合、証明書には個人を特定する情報に加えて、選挙に関する情報、例えば、年齢・住所・その住所への転入年月日等の情報が記載される。

マルチ証明書の世界では、それほど頻繁には行なわれない選挙のために専用の証明書が発行され、それを管理しつづければならないという点において利用者の負担が増大すると考えられる。

この選挙用の証明書に対応する鍵が危殆化した場合には選挙が実行できなくなるが、シングル証明書の世界に比較してリスクは分散されると考えることができる。

③ 個別証明書の世界

個別証明書の世界では、公的な選挙が行なわれる度に、一回だけ利用できる証明書が発行される状況を想定する。現在の選挙においては一回の選挙で複数の選挙(国政選挙と地方選挙等)が同時に行なわれることがあるが、それら一つ一つの選挙に対してそれぞれの証明書が発行されるという形式(つまり、一回の選挙において複数の証明書が利用される)もここに含めて検討する。

個別証明書の世界においては、証明書には、マルチ証明書の世界で記載される個人を特定する情報・年齢・住所・その住所への転入年月日等の情報に加え、その証明書が使われる対象となる選挙の情報(日付、場合によっては更に細かい選挙の種別)が記載されることとなる。

個別証明書の世界では、選挙が実施される前の一定期間(通常 2 週間程度)に利用者

に配布され、選挙当日までその証明書を管理することとなる。選挙が行なわれていないときも常に証明書を管理する必要があるマルチ証明書の世界よりは、利用者の管理負担は少ないと言うことができる。

この選挙用の証明書に対応する鍵が危殆化した場合には該当する選挙が実行できなくなるが、別の種別、もしくは別の日に行なわれる選挙では別の証明書を利用して投票することができるので、シングル証明書及びマルチ証明書の世界に比較してリスクは分散されると考えることができる。

4.1.1.2 購入（調達）・販売

購入・販売というプロセスにおいて、シングル証明書、マルチ証明書といったものの利用形態を比較検討し、それぞれの証明書利用形態の特徴と方向性を抽出する。

比較は、シングル証明書を利用した購入と、マルチ証明書を利用した購入、およびシングル証明書を利用した販売（企業）、シングル証明書を利用した販売（個人）、マルチ証明書を利用した販売、といったケースを対象として行った。

(1) 購入

① シングル証明書を利用した購入

利用者から見たシングル証明書とは、自分の求めるサービスを 1 枚の証明書に集約することが可能なものとして理解することができる。

証明書自体は、住民票レベルの証明が限界であることから、シングル証明書を用いて購入行動をとる際には決済能力の提示が必須となる。したがって購入に際しては、販売者に対して何らかの確証を提示しなければならない。

デジタルコンテンツのダウンロード販売といった特定の分野（販売金額がさほど大きくない／物理的な運搬を要さない）においては、販売側にとって購入者確認の精度が上がる分の利用価値は考えられる。

属性情報の変化による証明書の頻繁な更新を避けるとともに、証明書利用における個人情報の流出を防ぐために証明書への格納情報は最低限に止めるべきである。基本的には「氏名＋個人特定ＩＤ」程度と考える

② マルチ証明書を利用した購入

利用するサービスの提供組織や業界に対応した範囲において、１枚の証明書で複数のサービスが利用可能となる。

マルチ証明書では、証明書発行母体が利用者を証明し保護することになる。また、証明書発行時点で利用者情報をもとに権利を付与されることも可能であり、証明書発行時点で利用者のサービス利用権限確立を完了できる。したがってマルチ証明書の申請から発行に際しては、利用者と証明書発行母体との間でサービスレベルに関する明確な契約を交わす必要がある。

証明書格納情報については、証明書発行母体における管理情報をも登録可能であることから、アプリケーションプログラムの柔軟性は向上する。たとえばポイントカード等、特典の適用範囲が特定の店舗ではなくマルチ証明書適用範囲まで拡大するといった利点が考えられる。

(2) 販売

① シングル証明書を利用した販売（企業）

企業のシングル証明書が証明することは、秘密鍵の保有組織が企業登記されているといったようなある時点での事実であり、その組織に対して何らの保証をするものではない。

販売業者にとってのシングル証明書は、購入者との信頼性の確立と決済機関との信頼性の確立に利用する。決済機関あるいは決済代行者に対し、シングル証明書と共に決済能力を提示することで決済を機能させることができる。

公的なディレクトリサービスにおいて、企業の活動状況や財務情報の提供が連携してくると、取引相手（購入者）にとって良い判断材料となろう。こういった展開がなければ購入者にとって、企業の持つシングル証明書といえども、ＳＳＬのサーバ証明書と変わりはない。

② シングル証明書を利用した販売（個人）

ネットを介して個人間の取引が発生することになるが、証明書のみで相手を信頼した取引は成り立たない。モールのようなサービスが介在することによって、この会員間での取引という形が現実的であろう。

販売者にとっても購入者にとってもリスクが高い上、簡略化できるプロセスもないことから、証明書を利用する利点がない。オークション等のサービスではエスクローといったものが出てきているが、個人間の取引が活発になってゆくためには、ネット上での認証以上に必要なサービスといえよう。

③　マルチ証明書を利用した販売

証明書発行母体となる組織や業界に対応した範囲において、１枚の証明書にて複数のサービスを提供可能となる。販売におけるマルチ証明書の利用は、基本的に複数の決済機関との取引がひとつの証明書によって実現できることから、販売業者の活性化が期待できる。

販売者にとってのマルチ証明書では、証明書発行母体となる組織や業界によって認定され、一定の保証レベルを維持できるものとなろう。

シングル証明書が実現できれば利用者の利便性は向上し、１枚のカードであらゆるサービスの利用・提供が可能となるが、紛失、なりすまし、結託という脅威から完全に逃れる術はなく利用者の自覚が重要なポイントとなる。また、サービス提供者としてはシングル証明書の場合、利用者の登録というプロセスが必要となり顧客の囲い込みにテクニックが必要となる。ここらは、新たなビジネスモデルを生み出す要素として考えられる。

マルチ証明書との直接的な比較としては、シングル証明書においては利用者責任が重く、マルチ証明書においては、証明書発行母体となる組織や業界によって、その責任が軽減できるといった利点が考えられるが、カードの使い分けは必要となる。

マルチ証明書においてはいかに利用者の求めるサービスをひとつのグループに纏め上げるかが勝敗を分けるポイントであろう。

(3) 各形態の証明書に対する考察

①　シングル証明書

シングル証明書とは、何もかも 1 つの証明書で購入や販売を行うべきもの、として捕らえてはいない。シングル証明書は、ある人を特定するためにたった１枚発行される証明書であり、あらゆるサービス事業者は、依頼主が個人の属性とシングル証明書を提示した場合に、この依頼主を顧客と認め、この顧客のシングル証明書による取引を認めるものとする。

したがって、利用者から見た場合にシングル証明書は、自分の求めるサービスを 1 枚の証明書に集約することが可能なものとして理解することができる。

②　マルチ証明書

業界やサービスグループといった、ある範囲の中で複数のサービスを受けること

ができる証明書であり、発行母体は業界やサービスグループであることを想定する。現状のクレジットカードとほぼ同等と考えることができる。ある範囲の中でのみ同じ証明書が利用可能となる。

③　個別証明書

非常に限定された範囲内での利用のみを許すカードで、現状のポイントカード、個別会員カードに近いものと考える。したがって発行母体も店舗、企業といった単位となろう。通常は個人情報を持つことはなく、証明書といった高度なセキュリティは必要ないが、たとえば病院の診察券として利用されたような場合には求められることとなろう。

これら証明書とはいっても、個人の所有する証明書は、通常何を保証するものでもなく、証明書を発行された個人がその時点で証明書を受け取る権利を有していたことが証明されるだけである。したがって、取引においては何らかの保証が必要となる。マルチ証明書や個別証明書では証明書発行母体がある程度のリスクを持つことと考えられるが、シングル証明書においては基本的に個人がそのリスクを負うこととなる。シングル証明書による個人間取引も可能ではあるが、ネットワークを介して遠隔地同士での取引が成り立つとは考えられない。

4.1.1.3　送受信

インターネットを利用したコンテンツの送信・受信業務におけるシングル証明書とマルチ証明書の世界の比較分析を行う。

まずここでの送信業務とは、リアルな世界における宅配便の発送業務をインターネットの世界に置き換えたコンテンツ配送サービスの送信処理を想定しており、そこでの証明書利用形態としてどのような特徴が見られるかを分析する。次に、ここでの受信業務とは、インターネットの世界でのコンテンツ配信等におけるコンテンツ受信に関わる処理を想定しており、そこでの証明書利用形態の特徴を分析している。

なお、インターネットを利用する送信・受信サービスといった場合、発注や決済処理のみインターネットで行い、送受信対象の商品は実際の物流として処理する形態も考えられる。しかし、ここでは対象の商品もすべてデジタルコンテンツとしてインターネット上で送受信される場合に検討対象を絞っている。

(1) 「送信」業務における証明書世界の比較

送信業務としては、インターネットを介してコンテンツを送信するサービスにおける送信処理を想定する。その送信処理においては、送信行為の主体者（送信者）を受信者に対して証明する必要があるため、証明書を用いた認証が行われる。

① シングル証明書の世界

シングル証明書の世界では、あらゆるサービスで利用される証明書が個人に対し１枚発行されている。すなわち、送信業務においてもあらゆるコンテンツの送信処理にこのシングル証明書が使用される。

シングル証明書には個人を特定する情報（個人特定 ID）と最低限の属性情報（氏名等）のみ掲載されることが想定され、外部アプリケーションで必要となる付加情報は原則掲載されない。よって、外部アプリケーションで必要となる情報は、証明書以外から提供する必要が生じる。

シングル証明書の世界では、送信業務においてもあらゆるコンテンツの送信処理に１枚の証明書が用いられるため、個人から見ると管理負担は小さいが、万が一その鍵が危殆化した場合や対象検証局がダウンした場合には、全ての送信業務が行えなくなるというリスクがある。このため、より厳重な鍵の管理ならびに検証局の高信頼化対策が必要となる。

② マルチ証明書の世界

マルチ証明書の世界では、送信対象のコンテンツの種別ごとにそれぞれ専用の証明書を持ち、ある種別（業界）のコンテンツ送信処理にはそれぞれの証明書を使い分けることを想定する。例えば、ソフトウェア（の送信）を 1 つの業界と考え、ソフトウェア送信にはそれ専用の証明書を用いて処理が行われる。

この場合、証明書には個人を特定する情報に加えて、コンテンツ種別（業界）を表す情報が掲載される。外部アプリケーションは必要に応じて証明書からこの情報を参照し、対象業界の識別や認証を行う。

マルチ証明書の世界では、業界ごとの複数の証明書を個人が所持するため、シングル証明書に比べて個人の管理負担は増加するが、ある業界用の鍵が危殆化したとしてもその特定業界の送信業務が実行できなくなるのみであり、リスクが分散されるメリットがある。

(2) **「受信」業務における証明書世界の比較**

受信業務としては、インターネットを利用したコンテンツ配信サービスにおいて、商品コンテンツを受信（受取）する際の業務を想定する。その受信処理においては、受信したという行為事実ならびに受信者を証明するために、証明書を用いた認証が行われる。

① シングル証明書の世界

シングル証明書の世界では、すべての受信業務に唯一１枚受信者が保持する証明書が使用される。「送信」業務と同様に、万が一鍵が危殆化した場合や検証局がダウンした場合すべての受信業務が行えなくなるというようにリスクが集中しているため、厳密な鍵の管理ならびに高信頼化対策が必要となる。

② マルチ証明書の世界

マルチ証明書の世界としては、「送信業務」と同様に、受信するコンテンツの種別ごとに業界があり、その業界ごとに専用の証明書を使い分けるという形態を想定する。例えば、ソフトウェア、音楽といったコンテンツ配信の業界ごとに個人は証明書を持ち、その業界内ではあらゆる受信にその証明書が利用できる。

この場合、証明書には個人を特定する情報に加えて、業界を識別するための情報が掲載される。外部アプリケーションは必要に応じて証明書からこの情報を参照し、業界の識別や認証を行う。

マルチ証明書の世界では、業界ごとの複数の証明書を個人が所持するため、シングル証明書に比べて個人の管理負担は増加するが、ある業界用の鍵が危殆化したとしてもその特定業界のコンテンツ受信ができなくなるのみであり、リスクが分散されるメリットがある。

4.1.2 個別証明書とマルチ証明書の比較

具体的サービス名称で比較検討を行った。

4.1.2.1 クレジットサービス

インターネット上で、代金決済を行う際に、クレジットカードを用いるという前提で個別証明書とマルチ証明書の世界の比較を試みる。リアルな世界では、ある特定の店舗でしか使えない「ハウスカード」と、カードフェイスにあるブランドのステッカーが貼ってあ

る店なら使える「汎用カード」がある。これらの機能をインターネット上で実現したらというイメージで比較してみる。

一般的に公開鍵証明書という観点から考えれば、双方の世界の証明書とも、利用の都度提示する証明書上にカード番号そのものを掲載することは、困難と言わざるを得ない。

① 個別証明書の世界

リアルな世界でのハウスカードをインターネット上で実現した場合を想定した世界である。証明書の発行者＝クレジットサービス提供者なので、証明者発行主体がリスクテイクでき、証明書の項目や発行基準の自由度はかなり高くなる。反面、同じクレジットサービスの証明書であってもユーザインタフェースがまったく異なったり、複数の個別証明書を保有する場合は使い分けを制御する機能が必要になるなど、クレジットサービス全体で見た場合は、使い勝手等が悪くなる可能性もある。

② マルチ証明書の世界

通用する範囲を、リアルな世界での汎用カードよりも少し広げ、本サービスに参加しているカード会社のカードならば、同じく本サービスに参加しているカード会社と契約している加盟店のどこでも通用するということを実現した場合を想定した世界である。この世界では、証明書の発行者とクレジットサービス提供者が異なる場合もある。異なる場合がある以上、本サービスに参加する者の間で合意された一定のルールが必要となる。従って、証明書の項目や発行基準といったものもこのルールに従わざるを得なくなり、その分自由度は制限される。しかし、本サービスに参加しているカード会社のカードであれば、何枚カードを保有していても使う証明書は 1 枚で済むことになるので使い勝手は良くなる可能性が高い。

複数のクレジットカードに一枚の証明書を関連付けるため、相対する秘密鍵の保管には、充分配慮しなければならない。

4.1.2.2 銀行サービス

使用場面は、一般個人のお客様が自身の電子証明書（「マルチ証明書」、「個別証明書」）をネット上で呈示することで振込を行う場面を想定。技術的な観点からは、現時点でこのスキームを確立することは可能なものと考えられる。

但し、お客様の囲い込みの観点から、銀行同士でお客様の情報をオープン・共有することについては課題が残る。

① 個別証明書の世界

現在、インターネットを利用して振込を行う銀行サービスは既に開始されている。このサービスは、

a) お客様が、銀行に口座番号、ログイン用パスワード、資金移動用パスワード、自身の口座番号、振替先口座番号、振込先口座番号、を事前に登録する。

b) 利用する銀行のホームページに、インターネットを利用して接続する。

c) ホームページ上で、口座番号、パスワードを入力して本人確認を行い、お客様の依頼する処理（振替、振込等）を行う。

というものである。

この口座番号とパスワード部分を「個別証明書」に置き換えることで、「個別証明書」の世界は成立する。

② マルチ証明書の世界

「個別証明書」と「マルチ証明書」の違いは、「個別 = 銀行毎」、「マルチ ＝ 業界毎 = 業界統一」という考えから、一枚の証明書でありながらどの銀行でも使える電子証明書を想定したことにある。

但し、この電子証明書については、上述のとおり銀行間での顧客情報の共有・オープンには課題があるため、必要最低限な個人情報の格納に留まり、決済情報（利用者が保有する銀行口座の銀行名、支店名、口座番号名）等の情報は含まれないものと想定する。

③ 「マルチ証明書」と「個別証明書」の比較

基本的には、「マルチ証明書」「個別証明書」ともに、必要最低限の情報しか包含せず、またそれぞれにおいても同等レベルなものになるものと推定される。

4.1.2.3 マイレージサービス

航空機の搭乗実績に応じ無料航空券などに交換できるマイレージサービスは、証明書を発行する場面と、発行された証明書を認証し搭乗実績を確認する場面が想定される。

マイレージサービスは、航空会社単独で実施している場合と、複数の航空会社が同盟（アライアンス）を結び実施している場合とがある。前者は証明書発行航空会社と搭乗航空会社が同一であり、後者では異なる事が大きな違いである。

インターネット上での利用を想定した場合、公開鍵証明書での運用が一般的に利用され

と思われる事から、証明書内には最小限の情報保有に留め、会員属性情報や搭乗実績情報の多くは証明書発行航空会社内で管理する必要がある。

① 個別認証書の世界

航空会社独自で完結するマイレージサービスが個別証明書の世界となる。航空会社は会員証明書の発行から、搭乗時の搭乗実績加算、交換時の搭乗実績減算までをクローズな環境で、独自の運用ルールに基づき行える事からオリジナルなサービス展開が可能となる。

しかし、複数航空会社のマイレージサービスを利用されている利用者にとっては、搭乗航空会社毎に異なる証明書の保有が必要であり、且つ異なった運用ルールで利用しなけれならず、マイレージ対象の搭乗エリアも航空会社に依存するなど不便さを感じられる事も想像される。

② マルチ認証書の世界

１つの航空会社が発行した会員証明書を、同盟関係にある複数の航空会社が共通会員として認識するマイレージサービスがマルチ証明書の世界となる。

異なる航空会社における会員証明書の相互認証の実現には、証明書内に発行航空会社を認識する情報保有と、ネットワーク化されたオンライン環境が必要であると共に、同盟航空会社間で合意された運用ルールに基づく証明書発行と会員属性情報や搭乗実績情報の管理を行う必要性がある。

会員の航空機搭乗時やマイレージ交換時に、搭乗航空会社は証明書の認証を行うと共に、証明書内の発行航空会社を判断する識別子から発行航空会社に問合わせを行い、保有される会員属性情報と搭乗実績情報を参照する必要がある。

利用者は１つの証明書で複数の航空会社からマイレージを獲得する事が可能であり、また獲得したマイレージを複数の航空会社で利用することが出来る事から、複数航空会社を利用する者にとっては利便性の向上が期待出来る。

4.1.2.4 損害保険

損害保険（以下、損保）のインターネットを利用した各種サービス（以下、損保サービス）では､既に様々な場面で電子証明書が利用されている。その理由の一つとして、各種保険締結時の告知項目（事故の有無、家屋の構造明細、家族の年齢、同居の有無、通院歴など）、事故情報（事故原因、過失の有無など）、損保サービスでは機密性の高い情報を取

り扱っていることをあげることができる。証明書を利用するケースが多い貨物保険でも同様に、企業秘密にかかわるデータ（保管倉庫、商品原価、事故情報など）を扱っている。

例えば誘拐身代金保険、役員賠償責任保険、リコール保険、製造物責任保険などのように、人命や社運にかかわるような情報を扱うことがあるのも損保サービスの特徴である。本項ではこれらの個別証明書利用に加えて、マルチ証明書の可能性について考察する。

①　個別証明書の世界

前述の通り、損保サービスが扱うデータの性格上、一般的には SSL で証明書を使ってアクセスコントロールして通信を行うか、PKI を利用して暗号化したデータをやり取りすることが一般的である。保険会社によっては、各社の情報管理規定に従って、PKI で暗号化したデータでのやり取りを義務づけている。具体的事例としては、大手会社と保険会社間で、支払保険金関連書類を市販のＰＫＩツールで作成した先方の公開鍵で暗号化しメールに添付して送信し、受信側は相対する自身の秘密鍵で複合化する方法が利用されているケースがある。また、保険会社が利用している貿易 EDI のボレロでは、IC カードに格納した X.509 に準拠した PKI 生成アルゴリズムを利用してネットワークに参加している。

このように、損保サービスで利用が始まっている電子証明書では、それぞれのサービス内容によって証明書の概要／定義、ネットでの自由度、セキュリティレベルはまちまちであるが、顧客の既存ネットワークに保険会社が参加する場合、そのネットワークが利用している証明書利用形態を受け入れていることが多い。　一方、保険会社が主体としてセキュリティ確保するケース、例えば、一般ユーザ向け電子保険取引や、代理店、自動車整備工場、医療機関などとのデータ交換については、各保険会社が自社のポリシーや情報管理規定に基づいて証明書利用形態を定義していくことが求められる。しかし、代理店とのデータ交換と異なり、不特定多数の整備工場からは画像データを暗号化せずに送受信しているのが実態である。

また、従来外資系損保会社のみが販売していたガン保険など疾病保険販売が国内損保に解禁になり、今後電子カルテ・疾病データなどを送受信するケースが増加することが想定されることから、損保各社がハイレベルな情報管理規定を作成し、そのルールを正しく守って運営することが必要であろう。

②　マルチ証明書の世界

大企業の職域契約に関して、複数の引受保険会社が乗合い各社員の希望する保険

会社を選択できる仕組みを導入しているケースがある。企業の福利厚生に関するカフェテリアプランのコンテンツとして、イントラネットによる保険申込みを実施している企業もある。このようなドメイン内のみで通用するマルチ証明書を使い、複数の生保損保に加入する利用形態が考えられる。職域を構成する個々人の保険リスクは様々だが、全体の損害率に基づいて次年度保険料が決まるレザルトレーティングという仕組みがあるため、このドメインに限って通用するマルチ証明書を利用できる可能性がある。

一方、不特定多数を対象としたドメイン、例えば保険アグリゲータや保険ポータルサイトの利用者がマルチ証明書を利用できる可能性を考えた場合に、上記ケースと違ってリザルトレーティングが適用できないという相違がある。大企業は基本的には、終身雇用制またはそれに準じた雇用形態があるので、構成メンバーが毎年大幅に変わることは考えられないが、ＷＥＢで入退会が随時出来る後者のドメインにおいてはその約束がない。従って、マルチ証明書を発行したとしても、その電子保険取引を利用するインセンティブになるようなメリット（保険料割引）をだすモデルは描きにくい。

未来の理想的な（人によっては迷惑な）世界では、個人の保険リスク・スコアリングができる可能性があり、リスクの少ない人が複数保険会社で割引利用できるマルチ証明書が実現できる可能性がある。現在、複数保険会社でゴールド免許割引制度があるのと同様に、例えば ITS による運転挙動データ解析により自動車事故を起こす可能性が低いこと、過去の診察データやゲノムの構造上疾病になる可能性が低いことなどにより、個人のリスクについて客観的にスコアリングできるようになる可能性があるからである。例えば、車の実走行軌跡を GPS でとらえてリスクを算出して毎月の保険料を決めるというビジネスモデルのように、損保が個人のリスクを客観的に判断して保険料を決める超リスク細分化を指向する傾向は、マルチ証明書実現の可能性を暗示している。

4.1.2.5　会社毎の情報提供等サービス

ここでは情報提供サービスで証明書が使用される場合を想定した。ここで言う情報提供サービスとは現在の紙を媒体として配信されている新聞などの文字情報をメインとする情報サービスとテレビに代表される映像による情報サービスが融合したものである。これらのサービスが現在のアナログメディアから完全にデジタル化され、ユビキタスネットワー

ク[6]環境が実現、そして、電池および表示デバイスの技術発展により、雑誌、新聞などと同等の手軽さでアクセス端末が実現された近未来を考える。

(1) 電子証明書が使用される理由

ユビキタスネットワーク環境の実現とアクセス端末の普及により、各種メディア業界のコンバージェンスはさらに進む。実際に現状の衛星放送チューナは IC カードをユーザの識別および視聴情報を保存するために使用している。各社が自社のマルチ化され、インターネットをインフラとする情報サービスへのユーザのアクセスコントロール手段として電子証明書を含む IC カードが一般的に使用される可能性がある。

新聞などの文字情報を中心とした配信を考えた場合、アクセス端末のコストを下げ、操作性を簡素化する為、アクセス端末には数個のボタンしか装備できず（タッチパネルも装備されていない）、ユーザ名、パスワードの入力を行う手段がないことから、衛星放送と同様に IC カードを購読者の識別用に使用することが想像できる。アクセス端末の標準化により喫茶店、ホテルなど何処にでも設置され、購読者は自分が加入しているサービスに対してカードを差し込むことによりアクセスできることが求められるのも普及要因と考えられる。

また、情報提供サービスの多様化により、各購読者に完全にカスタマイズされた情報が提供されることが予想される。従って、情報提供会社は購読者の年齢、配信内容の好み等に合わせた情報を提供しなくてはならない。購読者を特定する為にも電子証明書が有効な手段である。

また、広告収入によって配信されている無料サービスであっても、配信内容に関する購読者の合意を得る場合、契約内容に電子署名する為にも電子証明書が必要となる。有料サービスではペイ・パー・ビュー、週刊コンテンツの購入などより多くの場面で電子証明書による、セキュアな取引が行われる。

電子証明書により購読者が特定できるようになると、有料サービスの違法閲覧、コピー、違法な再配信も減少する為、情報提供サービス会社側でも積極的に採用することも考えられる。

① 個別証明書の世界

各情報提供サービス会社が証明書を発行するパターンが個別証明書の世界にな

---

[6] いつでも誰でもどこでもどんな端末からでもあらゆるコンテンツにアクセスできる環境

る。各会社がサービスごとに証明書を発行することは現実的でないので、情報提供サービス会社は購読者に対して証明書を一枚無償で発行する。従って、デジタル化された新聞的なサービスである場合、一般と経済専門の情報の提供会社が異なる可能性があり、購読者は複数の証明書を携帯しなくてはならない可能性がある。

証明書に記載される内容は購読者を特定する為の識別子が最小限必要となるが、契約者名義は記載される方が望ましい。なお、現状の新聞の購読形態を考えると法人契約も考えられる為、別名が記載されることも考えられるが、サービス加入時には支払い方法とそれで必要となる名義は提出する必要があると考えられる。

カードにはサービスに特化したその他の情報を格納することも考えられるが、ユビキタスネットワーク環境を想定した場合、その必要性もない。その理由は、サービスを提供する為に必要となるその他購読者情報（年齢、住所など）はサービス加入時に提供し、サーバ側で管理することができるので、証明書が格納される媒体内に保存する必要もない。

リスクの面では検証局のダウンはその会社のサービスのみに影響するので購読者にとっては迷惑であるが、社会全体に及ぶ影響ではない。

② マルチ証明書の世界

情報提供サービス会社が一般的に証明書を発行するようになると、各社の提供する情報を充実する為、別の会社の情報も提供する可能性がある。また、サービス会社間の提携、企業合併、又は情報流通と情報提供の役割分担が明確に分類されることも想像できる。このような状態を発展するとマルチ証明書の世界が考えられる。この場合、購読者は 1 枚の証明書を所有し、それにより、様々な会社の情報へ購読できるようになり、個別証明書で課題であった複数の証明書を携帯する必要がなくなる。

証明書に記載される内容は購読者を特定する為の識別子が最小限必要となるが、契約者名義は記載される方が望ましい。また、年齢制限のことを考慮した場合、生年月日の記載があることにより汎用性が増すが、バックエンドシステム側で対応することも可能である。

個別証明書の世界と比較した場合、バックエンドシステムがどのような形で提供されているかにより、運用システムの複雑度が変わる。例えば流通を担当している会社が CA を運用しているのであれば、その会社のみが購読者の詳細属性情報（住

所、支払い方法、利用記録など）を保有し、アグリゲータ[7]として機能できる。情報提供会社はそこから情報料を徴収すればよい。逆に CA を運用している会社が購読者の認証のみ担当した場合、各情報提供会社は独自で購読者の詳細属性情報を管理し、購読者も結果としては会社ごとの契約を行うことになるので一枚の証明書のメリットが薄れる。

個別証明書の世界と比較した場合、検証局の信頼性が非常に重要になり、原則 24 時間 365 日ノンストップのサービスが要求され、リスクが集中し、ダウンした場合、社会全体に影響を与える。

[7] 「集める、結合する」ことを行うサービス事業者

4.2 比較データ

4.2.1 シングル証明書とマルチ証明書の比較表

4.2.1.1 情報収集・情報提供（選挙）

比較項目		世界		
分類	項目	シングル証明書	マルチ証明書（あらゆる選挙で利用可能）	個別証明書（選挙日時、対象で利用可能）
A.概要/定義	1．何を認証するか	・個人認証（本人特定）	・個人認証（本人認証）、選挙有資格者（年齢、住所、転入年月日、等）	・個人認証（本人認証）、選挙有資格者（年齢、住所、転入年月日、対象選挙、等）
	2．証明書の持つ情報	・個人を特定する情報のみ	・個人の年齢、所在地（選挙区）を特定する情報	・個人の年齢、所在地（選挙区）、対象選挙を特定する情報
	3．格納情報	・属性情報：氏名、生年月日、性別、住所（住民４情報）	・属性情報：氏名、生年月日、性別、住所（住民 4 情報）、・・・	・ID 情報：選挙管理番号（対象となる選挙情報） 属性情報：氏名、生年月日、性別、住所（住民 4 情報）、・・・
	4．CAの数	1	自治体単位	自治体単位
	5．証明書枚数	1	1	1
	6．使用場面（限定する場合記入）	・投票において、個人の身分証明（有権者であること）に利用する。 ・選挙以外での利用も可能。	・投票において、個人の身分証明（有権者であること）に利用する。 ・あらゆる選挙への参加だけが可能。	・投票において、個人の身分証明（有権者であること）を行う。 ・一定期間、対象選挙における投票が可能
B.特徴		・個人に対し１枚の証明書が発行され、その１枚で全ての認証業務に利用される。	・選挙参加用として証明書が発行され、あらゆる選挙における認証用として利用される。	・特定選挙参加用として証明書が発行され、その該当選挙での認証用として利用される。
C.ネット社会での自由度	1．名義（別名・仮名）を持てる	・持てない（シングル証明書はあくまで個人（本人）に対して発行される）。	・基本は持てない（匿名性という観点で、割り振られる可能性もある）。	・基本は持てない（匿名性という観点で、割り振られる可能性もある）。
	2．プライバシー	・1 箇所で管理されるため、そこが信頼されれば守られる。 （証明書に氏名、生年月日等が含まれるならば、それらは公になる。）	・1 箇所で管理されるため、そこが信頼されれば守られる。 （アプリケーションが閉じた世界なので、証明書の利用でもプライバシーは守られる。）	・1 箇所で管理されるため、そこが信頼されれば守られる。 （アプリケーションが閉じた世界なので、証明書の利用でもプライバシーは守られる。）
	3．制御（利用側）	・1 枚なので使い分けはできない。	・選挙用なので、他サービスへの適用は不可である	・特定選挙用なので、それ以外の選挙、他サービスへの適用等は不可である

	4．ﾄﾚｰｻﾋﾞﾘﾃｨ(犯罪)	･個人特定の可能性は、そのプライバシー保護ポリシーに依存する。 秘密鍵格納媒体が、利用者によって厳重に管理されれば･犯罪は起こりにくい。 (投票したことは判断できるが、「誰」に投票したかはわからない仕組みが必要)	･個人特定の可能性は、そのプライバシー保護ポリシーに依存する。 ･秘密鍵格納媒体が、利用者によって厳重に管理されれば犯罪は起こりにくい。 (投票したことは判断できるが、「誰」に投票したかはわからない仕組みが必要)	･個人特定の可能性は、そのプライバシー保護ポリシーに依存する。 ･秘密鍵格納媒体が、利用者によって厳重に管理されれば犯罪は起こりにくい。 (投票したことは判断できるが、「誰」に投票したかはわからない仕組みが必要)
	5．サービス設計	･証明書にアプリケーション用の情報がないので、外部アプリケーション用の情報が必要である。 ･(上記を認識できれるアプリケーションならば、選挙以外でも動作する。)	･証明書には、選挙アプリケーションの識別情報が含まれていて、あらゆる選挙で利用可能となる。	･証明書には、投票アプリケーション、対象選挙の識別情報が含まれている。 ･同一機関(選挙、アプリケーション)でのみ、利用可能
	6．ユーザ鍵ペアの有効期限	･安全性の観点から、原則1年 ･自動更新(オンライン更新)されることが望ましい。	･安全性の観点から、原則1年 ･自動更新(オンライン更新)されることが望ましい。	･現状の投票期間の観点から、2 週間程度(不在者投票の期間を含む)
	7．審査/発行/更新	･初期発行、および属性変更は、安全性の観点から対面手続きが望ましい。 ･更新は、負荷削減の観点からオンライン手続きが望ましい。	･自治体が持つ情報で審査／発行される。 ･初期発行、および属性変更は、安全性の観点から対面手続きが望ましい。 ･更新は、負荷削減の観点からオンライン手続きが望ましい。	･自治体が持つ情報で審査／発行される。 ･発行は、自治体が持つ情報を利用して、送付される。 ･更新は、そもそも住民票の移動が伴う状況により選挙権がなくなるため、ありえない。
D.運用性	1．紛失時 ：失効・削除・再発行	･選挙を含む全てのサービスが利用できなくなるため影響大 ･再発行は、失効処理を行った後、再度対面手続きを行う必要がある。	･投票ができなくなるので、影響大。 再発行は、失効処理を行った後、再度対面手続きを行う必要がある。	･投票ができなくなるので、影響大。 ･再発行は、失効処理を行った後、再度対面手続きを行う必要がある。
	2．認証サービス利用の課金	･投票といったアプリケーションにおいては、課金は無い。 (認証機能提供側が、証明書発行時、もしくは検証時に、課金を行うこともありうる。)	･投票といったアプリケーションにおいては、課金は無い。 (民主主義における投票権の侵害の可能性)	･投票といったアプリケーションにおいては、課金は無い。 (民主主義における投票権の侵害の可能性)
	3．証明書の配布	･対面／郵送(書留等直接本人に渡る仕組み)	･郵送(書留等直接本人に渡る仕組みで、利用者にとって負荷を感じない仕組み)	･郵送(書留等直接本人に渡る仕組みで、利用者にとって負荷を感じない仕組み)
	4．証明書の利用実績の通知	･あらゆるアプリケーションで利用可能なため、利用実績を把握するためにも通知はあることが望ましい。 ･郵送、もしくはメールによる通知。	･対面の場合はない(現状の仕組み) ･オンラインは受領通知が必要	･なし
	5．約款の送付	･証明書発行時に、併せて配布されることが望ましい。 ･更新内容は、ホームページ等で公開されていることが望ましい。	･証明書発行時に、併せて配布されることが望ましい。 ･更新内容は、ホームページ等で公開されていることが望ましい。	･証明書発行時に、併せて配布されることが望ましい。 ･更新内容は、ホームページ等で公開されていることが望ましい。

	6．メディア (格納デバイス)	・格納される情報量により差が出るが、2～3Kbytes 程度の証明書と秘密鍵が格納できる媒体 ・容易にデータ書き込み／参照／更新ができない仕組みを持つ媒体	・格納される情報量により差が出るが、2～3Kbytes 程度の証明書と秘密鍵が格納できる媒体 ・容易にデータ書き込み／参照／更新ができない仕組みを持つ媒体	・格納される情報量により差が出るが、2～3Kbytes 程度の証明書と秘密鍵が格納できる媒体が望ましい。 ・容易にデータ書き込み／参照／更新ができない仕組みを持つ媒体
	7．取り扱い留意点	・問題が生じた際には利用サービス全てに影響がでるため、厳重な管理が必要	・問題が生じた際には選挙投票サービス全てに影響がでるため、厳重な管理が必要	・問題が生じた際には選挙投票サービス全てに影響がでるため、厳重な管理が必要
E.ｾｷｭﾘﾃｨ	1．運用 1.1 貸借 1.2 耐犯罪性	・秘密鍵は IC カード等へ格納の上、厳重な管理が必要 貸借は、自己の損失に繋がる可能性があるため禁止 ・1枚で実行できる業務処理の範囲／影響が大きいため、狙われる危険性が高い。 (アプリケーションとしては、2 重投票のチェック、投票者の匿名性を保つ、投票権の譲渡を禁止する等の仕組みが必要)	・秘密鍵は IC カード等へ格納の上、厳重な管理が必要 ・貸借は、自己の損失に繋がる可能性があるため禁止 ・不正投票が行われる可能性があり、狙われる危険性が高い。 (アプリケーションとしては、2 重投票のチェック、投票者の匿名性を保つ、投票権の譲渡を禁止する等の仕組みが必要)	・秘密鍵は IC カード等へ格納の上、厳重な管理が必要 ・貸借は、自己の損失に繋がる可能性があるため禁止 不正投票が行われる可能性があり、狙われる危険性が高い。 (アプリケーションとしては、2 重投票のチェック、投票者の匿名性を保つ、投票権の譲渡を禁止する等の仕組みが必要)
F.緊急時対応 (リスクの集中度)	1．検証局のダウン	・リスク集中 － 1枚のため対象検証局がダウンしたならば、全てのサービスが利用停止	・リスク集中 － 1枚のため対象検証局がダウンしたならば、全ての選挙サービスが利用停止	・リスク集中 － 1枚のため対象検証局がダウンしたならば、特定選挙のサービスが利用停止
	2・ネット上のサービス窓口	・リスク集中 － 1枚のためサービス窓口がダウンしたならば、全てのサービスが利用停止	・リスク集中 － 1枚のためサービス窓口がダウンしたならば、全ての選挙サービスが利用停止	・リスク集中 － 1枚のためサービス窓口がダウンしたならば、特定選挙のサービスが利用停止
G.コスト	1．発行 1.1 審査/発行/ 1.2 更新/失効/削除	・社会基盤であることから、発行は無料としサービス利用にコストをかけることが望ましい →現状の印鑑証明書は、登録は無料、利用は 300 円程度である (選挙は、特別扱い)。 ・発行の手間としては、発行の拠り所とする情報との連携がどのように実現されるかに依存する。	・選挙の性質上、利用者からはお金を徴収できない。 ・発行／更新の手間としては、拠り所とする情報との連携がどのように実現されるかに依存する。	・選挙の性質上、利用者からはお金を徴収できない。 発行／更新の手間としては、拠り所とする情報との連携がどのように実現されるかに依存する。 ・格納媒体を再利用できる仕組み、もしくは格納媒体自体の低コスト化が必要
	2．運用 2.1運用体制 2.2 ﾈｯﾄﾜｰｸ・ｷｬﾊﾟｼﾃｨ	・高性能、高信頼性をもった認証サービス、検証サービスを提供する必要がある。 ・CA は唯一であるため、独自の運用体制、運用時間を設定可能 ・あらゆるアプリケーションで利用可能なため、有効性確認の利用頻度が高い	・高性能、高信頼性をもった認証サービス、検証サービスを提供する必要がある。 ・CA は唯一であるため、独自の運用体制、運用時間を設定可能 ・選挙で利用するため、短期的に集中することを考慮する必要がある	・高性能、高信頼性をもった認証サービス、検証を提供する必要がある。 ・CA は唯一であるため、独自の運用体制、運用時間を設定可能 ・証明書の管理、サービス利用共に、短期的に集中することを考慮する必要がある

4.2.1.2 (1) 購入（調達）

比較項目		世界	
分類	項目	シングル証明書	マルチ証明書
A.概要/定義	1．何を認証するか	申請時点で要件を満たした申請者の存在 「要件例」 ･申請書にある住所･氏名･生年月日･性別が住民票のものと一致する ･身分証明ができる。例えば、運転免許書のように、サービスごとの証明書を得るための大元の証明書となる。	申請時点で要件を満たした申請者の存在 「要件例」 ･サービスを受けるための対価を支払う意思がある。 ･ある一定金額以上の支払能力を保持する。 ・　　銀行口座を持っている
	2．証明書の持つ情報	個人を特定するための基本情報	業界名と個人を特定する情報
	3．格納情報	ID･氏名 「ID」 ･住民番号（個人を特定するID番号） これ以上の情報格納を行うと、購入フェーズの中で不要な情報まで相手に渡ってしまう	ID･氏名＋個別属性 「ID」 ･サービスの業界名＋会員番号／会社識別子＋社員番号等
	4．CAの数	1	･業界ごと
	5．証明書枚数	1	･業界ごと
	6．使用場面（限定する場合記入）	･個人旅行に係る一連の購入行為を想定。 JR,航空各社、ホテル,旅館、各ツアー会社が提供する「パックサービス」ホームページ上で購入する。 ･事前に利用する会社を選択し、各社毎に個別に会員登録を行うことを前提とし、購入時、シングル証明書の提示と各社毎の会員番号を入力し購入権利を得る。 ※現実的には、サービス提供側で利用者が各会員番号を入力せずにすむ工夫（証明書ID と会員番号の紐付け）が必要になるのではないか…	･旅行サービス業界（JR,航空各社、ホテル,旅館、各ツアー会社が提携）におけるマルチ証明書を想定。 ･同左、「パックサービス」ホームページ上で購入する。購入時、マルチ証明書提示のみで購入権利を得る。
B.特徴		･証明書発行者は、地方公共団体（市区町村）が有望 ･住民登録と関連付けた証明書とすることが望ましい ･シングル証明書を利用する場合には、サービス利用に先だって利用者登録を要することになろう。ここで利用者属性がサービス利用者によって定義され、証明書利用が可能となるものと想定している。 ･シングル証明書とは、利用者が選択したサービス全てを1枚の証明書で受けることができるもの	･各業界で信頼できる個人情報にて管理する 銀行口座、所属企業、･･････ ･マルチ証明書の場合には、証明書取得段階で何らかの権限やサービスレベルが定義されているものと想定している。

C.ﾈｯﾄ社会での自由度	1．名義（別名・仮名）を持てる	・個人を特定するため別名や仮名は持てない	・組織としての別名は持ち得る
	2．プライバシー	・サービス利用登録に依存する ・利用者は規約／約款を確認し、個人の責任において利用者登録を実施	・利用業界に依存する ・サービス提供業者は各業界にて認定されるが、証明書取得時点でリスクが許容できることを確認する
	3．制御(利用側)	・証明書の使い分けはない	・業界によって固定
	4．ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	・あり（完全性を求める場合はバイオ連携が有望）	・同左
	5．サービス設計	・サービス利用登録におけるキーのアクティベートが標準化され、利用登録において最低限の情報を提示することによって、以降、該当サービスへのアクセスが可能となる	・業界内の標準化
	6．ユーザ鍵ペアの有効期限	・3～5年？ ICカードの耐久性からもこのあたりが適切と考える。（鍵の有効期限＝＜証明書有効期限）	・同左
	7．審査/発行/更新	・審査・発行：公的機関による対面手続き ・更新：実質的には再発行、申し込み手続きはネットで可	・利用業界に依存する
D.運用性	1．紛失時　：失効・削除・再発行	・失効：緊急（TEL）、標準（対面） ・再発行：発行と同等	・同左
	2．認証サービス利用の課金	・利用サービスに依存する ・認証に要する費用はサービス提供者が負担	・利用業界に依存する ・認証に要する費用はサービス提供者が負担
	3．証明書の配布	・IC カードで配布・郵送は好ましくない（PIN 別ルート）	・IC カードで配布・郵送可（PIN 別ルート）
	4．証明書の利用実績の通知	・必須	・同左
	5．約款の送付	・証明書に関しては証明書発行時に必要 ・サービスに関わるものはサービス利用登録時に必要	・同左
	6．メディア（格納デバイス）	・当面は IC カード	・同左
	7．取り扱い留意点	・利用者に、単なる証明書ではなく、自分の全ての財産に接近し得る鍵であることを徹底認識させる	・利用者に証明書ごとの接近可能資産を認識させる
E.ｾｷｭﾘﾃｨ	1．運用 1.1 貸借 1.2 耐犯罪性	・なし（利用者責任） ・生体情報とのコンビが有効	・なし（利用者・組織責任） ・生体情報とのコンビが有効
F.緊急時	1．検証局のダウン	・CA の冗長構成等は必須だが、ダウンに対してはサービス提供業者が担保する	・同左

対応 (リスクの集中度)	2・ネット上のサービス窓口	・緊急失効受付（24時間）・電話／Email	・同左
G.コスト	1．発行 1.1 審査/発行/ 1.2 更新/失効/削除	 ・初期発行費用 ・更新費用＝初期発行費用、再発行費用には失効費用を含む ・通常失効＝なし、緊急失効費用＝あり	 ・同左 ・同左
	2．運用 2.1 運用体制 2.2 ﾈｯﾄﾜｰｸ･ｷｬﾊﾟｼﾃｨ	 ・証明書発行代金＋認証代金にて運用をカバー ・ディレクトリサーバの冗長構成／地域分散	 ・同左 ・同左

4.2.1.2.（2） 販売

比較項目		世界		
分類	項目	シングル証明書（企業）	シングル証明書（個人）	マルチ証明書
A.概要/定義	1．何を認証するか	申請時点で要件を満たした申請業者の存在 「要件例」 ・企業登記情報と一致する	申請時点で要件を満たした申請者の存在 「要件例」 ・申請書にある住所・氏名・生年月日・性別が住民票のものと一致する ・身分証明ができる。例えば、運転免許書のように、サービスごとの証明書を得るための大元の証明書となる。	申請時点で要件を満たした申請業者の存在 「要件例」 ・サービスの提供能力を有する ・ある一定金額以上の支払能力を保持する ・銀行口座を持っている
	2．証明書の持つ情報	・業者の特定情報（登記情報→公証）	・個人を特定するための基本情報	業界種別と業者の特定情報
	3．格納情報	ID・住所・代表者氏名 「ID」 ・会社法人等番号	ID・氏名 「ID」 ・住民番号（個人を特定するID番号）	シングル証明書＋個別属性 「ID」 ・業界名　＋　会員番号／会社識別子
	4．CAの数	1	・同左	・業界ごと（業界はサービス提供企業で構成される。）
	5．証明書枚数	1	・同左	・業界ごと
	6．使用場面（限定する場合記入）	・「購入」と同様の場面、個人旅行に係る一連の販売行為を想定する。 ・JR,航空各社、ホテル,旅館、各ツアー会社が協力して「パックサービス」ホームページを提供し販売する。 ・販売側各社は、決済機関に対して、利用者情報とともに各社が各々シングル証明書を提示。各社は事前に、決済機関に対して銀行口座など入金に必要な情報を提示しておくか、申請毎に決済機関から問合せを受けることにより、入金処理が可能となる。	・「個人販売」においては個人対個人の販売行為を想定してみる。 ・ネットを介して単なる個人を信用した前払い取引は基本的に成り立たないものと考える。したがって、証明書を持っていることを確認するレベルにとどまり、実際の取引における入金は代引き（コンビニ決済含む）や着後振込みを求められる可能性が高い。→リスクも高く証明書を使う利点がない。 ・信用度の高いモールにおける個人出店で、モール側の決済機能利用のために証明書を利用するものとする。 →モールのエスクローサービス等も期待。	・旅行サービス業界におけるマルチ証明書を想定。販売側のマルチ証明書は、業界各社と決済機関との提携を前提とする。 /・決済機関に対して、各社が各々マルチ証明書を提示することにより入金処理が可能となる。

B.特徴		・証明書発行者は、地方公共団体（市区町村）や法務局が有望 ・企業登記と関連付けた証明書とすることが望ましい ・販売におけるシングル証明書利用とは、販売業者が決済機関に対して提示する場面を想定する	・証明書発行者は、地方公共団体（市区町村）が有望 ・住民登録と関連付けた証明書とすることが望ましい ・販売側／購入側相互の信用を確保することは不可能→高額品の販売はは成り立たない（モールのエスクローサービス等の範囲内であれば成り立つ可能性有り）	各業界で信頼できる個人情報にて管理する ・銀行口座、所属企業、・・・・・・
C.ﾈｯﾄ社会での自由度	1．名義（別名・仮名）を持てる	・業者を特定するため別名や仮名は持てない	・個人を特定するため別名や仮名は持てない	・組織としての別名は持ち得る
	2．プライバシー	・サービス利用登録に依存する ・サービス提供業者として規約・約款の整備が必要 ・サービス提供に必要最低限の情報保持に努める	・保証がない。 ・販売側では購入側からの情報入手に際して、取引のために必要な最低限の情報で有る旨を提示する必要があろう。	・利用業界に依存する ・サービス提供業者は各業界にて認定する ・業界内で共通の機密保持レベルを維持する
	3．制御(利用側)	・証明書の使い分けはない	・同左	・業界によって固定
	4．ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	・あり（企業内部での運用にかかる比重が大）	・困難である	・あり（業界内での仕組みと連携）
	5．サービス設計	・各決済機関におけるキーのアクティベートを標準化	・同左	・業界内の標準化
	6．ユーザ鍵ペアの有効期限	・3～5年？（鍵の有効期限＝＜証明書有効期限）	・同左	・同左
	7．審査/発行/更新	・審査・発行：公的機関による対面手続き ・更新：対面は必須ではない（対面手続きが好ましい）	・同左	・利用業界に依存する
D.運用性	1．紛失時　：失効・削除・再発行	・失効：緊急（TEL）、標準（対面） ・再発行：発行と同等	・同左	・同左
	2．認証サービス利用の課金	・利用サービスに依存する ・決済機関への手数料に含まれるものと考える	・同左	利用業界に依存する ・認証に要する費用は販売価格でカバー
	3．証明書の配布	・ICカードで配布・対面受領	・ICカードで配布・郵送は好ましくない（PIN別ルート）	・ICカードで配布・郵送可（PIN別ルート）
	4．証明書の利用実績の通知	・必須	・同左	・同左
	5．約款の送付	・証明書に関しては証明書発行時に必要 ・サービスに関わるものはサービス利用登録者に送付	同左	・同左
	6．メディア（格納デバイス）	・当面はICカード	・同左	・同左

	7．取り扱い留意点	・利用者に、単なる証明書ではなく、企業の全資産に接近し得る鍵であることを徹底認識させる	・利用者に、単なる証明書ではなく、個人の全資産に接近し得る鍵であることを徹底認識させる	・利用者に証明書ごとの接近可能資産を認識させる
E.ｾｷｭﾘﾃｨ	1． 運用 1.1 貸借 1.2 耐犯罪性	・なし（利用者責任・法的罰則定義） ・企業登記＋決済機関のチェックでガード、また証明書保管に関する運用規定を罰則と共に設けるべきと考える	・同左	・なし（利用者・組織責任） ・該当業界の規定と審査でガード、顧客に対しては業界としての保証体制を準備すべき
F.緊急時対応(ﾘｽｸの集中度)	1．検証局のダウン	・CA の冗長構成等は必須だが、発行機能のダウンに対しては余裕がある。検証機能のダウンは決済の停止となり得るが、決済金額やその他条件により決済機関のポリシーにかかる	・同左	・同左
	2・ネット上のサービス窓口	・緊急失効受付（24時間）・電話／Email	・同左	・同左
G.コスト	1． 発行 1.1 審査/発行/ 1.2 更新/失効/削除	・初期発行費用 ・更新費用＝初期発行費用、再発行費用には失効費用を含む ・通常失効＝なし、緊急失効費用＝あり	・同左	・同左
	2．運用 2.1 運用体制 2.2 ﾈｯﾄﾜｰｸ・ｷｬﾊﾟｼﾃｨ	・証明書発行代金＋認証代金にて運用をカバー ディレクトリサーバの冗長構成／地域分散	・同左	・同左

4.2.1.3 (1) 送信

比較項目		世界	
分類	項目	シングル証明書	マルチ証明書
A.概要/定義	1．何を認証するか	・個人認証（本人特定）	・個人認証（本人特定）
	2．証明書の持つ情報	・個人を特定する情報のみ	・個人を特定する情報　と　コンテンツ種別（業界）情報（例えば“ソフトウェア（の送信）”）
	3．格納情報	・ID 情報：住民番号 ・属性情報：氏名、生年月日、性別、・・・	・ID 情報：住民番号 ・属性情報：氏名、生年月日、性別、コンテンツ種別（業界）情報、・・・
	4．CAの数	1	・複数（業界の数）。　例えば、ソフトウェアの送信を1つの業界と考える。
	5．証明書枚数	1	・複数（業界の数）。　例えば、ソフトウェアの送信を1つの業界と考える。
	6．使用場面（限定する場合記入）	・インターネットを利用したコンテンツ送信サービスを想定する。 ・あらゆるコンテンツ種別（業界）の送信処理に1枚の証明書を用いる	・送信するコンテンツの種別（業界）ごとに証明書各1枚を持ち、あるコンテンツの送信にはその業界用の証明書を用いる
B.特徴		・人に対し 1 枚の証明書が発行され、その1枚がすべてのコンテンツ種別（業界）の送信処理に用いられる。	・個人に対しコンテンツの種別（業界）数分の証明書が発行される。あるコンテンツの送信処理には、その業界用の証明書が使用される。
C.ネット社会での自由度	1．名義（別名・仮名）を持てる	・持てない（シングル証明書はあくまで個人（本人）に対して発行される）	・持てる（シングル証明書と異なり、送信業務用かつ各コンテンツ種別用証明書として複数持つので、名義（別名・仮名）を許容）
	2．プライバシー	・一箇所で管理されるため、そこが信頼されれば守られる。 （・証明書には不必要な属性情報は掲載しない。）	・名義はどこか一箇所で管理することとし、その信頼性に依存する。 ・証明書にはコンテンツ種別情報が掲載されるため、必要以上の配布は行わない。
	3．制御(利用側)	・1枚なので使い分けはない。	・コンテンツ種別ごとに証明書を使いわける
	4．ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	・個人 ID→個人の特定の可能性はそのプライバシー保護ポリシーに依存する。	・個人 ID→個人の特定の可能性はそのプライバシー保護ポリシーに依存する。 ・あるコンテンツ種別ごとのネガリスト対策は容易
	5．サービス設計	・証明書にアプリケーション用の情報がないので、外部アプリケーション用の情報を別途提供する必要あり	・証明書にコンテンツ種別情報を含むため、アプリケーションで利用可能
	6．ユーザ鍵ペアの有効期限	・原則 1 年　・自動更新	・1～3 年　・自動更新
	7．審査/発行/更新	・本人確認のため対面手続きが必要	・本人確認のため対面手続きが望ましいが、シングル証明書と比較すると簡易な手続きで発行が可能

D.運用性	1．紛失時　：失効・削除・再発行	・全サービスが利用できなくなるため影響大 ・再発行時は再度対面手続きを行う。	・ある特定のコンテンツ種別について送信業務が実行できなくなる ・シングル証明書に比べリスクは分散される
	2．認証ｻｰﾋﾞｽ利用の課金	・サービス契約時に金融機関の口座番号を提示して、口座引き落とし	・サービス契約時に金融機関の口座番号を提示して、口座引き落とし
	3．証明書の配布	・対面、または郵送（本人限定）	・対面、または郵送（本人限定）
	4．証明書の利用実績の通知	・利用実績を確認するために必要 ・郵送	・利用実績を確認するために必要 ・郵送
	5．約款の送付	・契約時の送付が必要	・契約時の送付が必要
	6．メディア（格納デバイス）	・基本は IC カード	・基本は IC カード
	7．取り扱い留意点	・影響が大きいため厳重な管理が必要	・厳重な管理が必要、かつ、複数管理する負荷がより大きい。
E.セキュリティ	1．運用 1.1 貸借 1.2 耐犯罪性	秘密鍵は IC カード等へ格納のうえ厳重な管理が必要 ・貸借は禁止 ・1枚で実行できる業務処理の範囲／影響が大きいため、狙われる危険性が大きい	秘密鍵は IC カード等へ格納のうえ厳重な管理が必要 ・貸借は禁止 ・シングルに比べてリスクは分散するが狙われる危険性は大きい。
F.緊急時対応（ﾘｽｸの集中度）	1．検証局のダウン	・リスク集中　－　1枚のため対象検証局がダウンした場合検証不可能	・シングルに比べてリスクは分散
	2・ネット上のサービス窓口	・リスク集中　－　サービス利用不可能	・シングルに比べてリスクは分散
G.コスト	1．発行 1.1 審査/発行/ 1.2　更新/失効/削除	・低い方がよい。 ・サービスの付加価値（信頼性の高低など）による料金のバリエーション	・低い方がよい。 ・サービスの付加価値（信頼性の高低など）による料金のバリエーション
	2．運用 2.1 運用体制 2.2　ﾈｯﾄﾜｰｸ・ｷｬﾊﾟｼﾃｨ	・CA は唯一であるため、独自の運用体制、運用時間を設定可能	・全コンテンツ種別統一の運用体制、運用時間が望ましい

4.2.1.3 （2） 受信

比較項目		世界	
分類	項目	シングル証明書	マルチ証明書
A.概要/定義	1．何を認証するか	・個人認証（本人特定）	・個人認証（本人特定）
	2．証明書の持つ情報	・個人を特定する情報のみ	・個人を特定する情報　と　コンテンツ種別（業界）情報（例えば“ソフトウェア（の受信）”）
	3．格納情報	・ID 情報：住民番号 ・属性情報：氏名、生年月日、性別、・・・	・ID 情報：住民番号 ・属性情報：氏名、生年月日、性別、コンテンツ種別（業界）情報、・・・
	4．CAの数	1	・複数（業界の数）。　　例えば、ソフトウェアの受信を1つの業界と考える。
	5．証明書枚数	1	・複数（業界の数）。　　例えば、ソフトウェアの受信を1つの業界と考える。
	6．使用場面（限定する場合記入）	・インターネットを利用したコンテンツの受信を想定する。 ・1枚の証明書であらゆる種別（業界）のコンテンツ受信処理を行う。	・インターネットを利用したコンテンツの受信を想定する。 ・受信するコンテンツ種別（業界）毎に証明書を1枚持ち、あるコンテンツの受信にはその業界用の証明書を用いて処理する。
B.特徴		・個人に対し 1 枚の証明書が発行され、その1枚がすべてのコンテンツ種別の受信処理に使用される。	・個人に対し利用するコンテンツ種別（業界）数分の証明書が発行される。ソフトウェア受信についてはその業界用の証明書が使用される。
C.ネット社会での自由度	1．名義（別名・仮名）を持てる	・持てない（シングル証明書はあくまで個人（本人）に対して発行される）	・持てる（シングル証明書と異なり複数持つので、名義（別名・仮名）を許容）
	2．プライバシー	・一箇所で管理されるため、そこが信頼されれば守られる。 （・証明書には不必要な属性情報は掲載しない。）	・名義はどこか一箇所で管理することとし、その信頼性に依存する。 ・証明書には業界識別情報が掲載されるため、必要以上の配布は行わない。
	3．制御(利用側)	・1枚なので使い分けはない。	・業界ごと（受信するコンテンツ種別ごと）に証明書を使いわける
	4．ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	・個人 ID→個人の特定の可能性はそのプライバシー保護ポリシーに依存する。	・個人 ID→個人の特定の可能性はそのプライバシー保護ポリシーに依存する。 ・ある業界ごとのネガリスト対策は容易
	5．サービス設計	・証明書にアプリケーション用の情報がないので、外部アプリケーション用の情報を別途提供する必要あり	・証明書に業界識別情報を含むため、アプリケーションで利用可能
	6．ユーザ鍵ペアの有効期限	・原則 1 年　・自動更新	・1～3 年　・自動更新
	7．審査/発行/更新	・本人確認のため対面手続きが必要	・本人確認のため対面手続きが望ましいが、シングル証明書と比較すると簡易な手続きで発行が可能

D.運用性	1．紛失時　：失効・削除・再発行	・全サービスが利用できなくなるため影響大 ・再発行時は再度対面手続きを行う。	・特定業界のコンテンツが受信できなくなる ・シングル証明書に比べリスクは分散される
	2．認証サービス利用の課金	・サービス契約時に金融機関の口座番号を提示して、口座引き落とし	・サービス契約時に金融機関の口座番号を提示して、口座引き落とし
	3．証明書の配布	・対面、または郵送（本人限定）	・対面、または郵送（本人限定）
	4．証明書の利用実績の通知	・利用実績を確認するために必要 ・郵送	・利用実績を確認するために必要 ・郵送
	5．約款の送付	・契約時の送付が必要	・契約時の送付が必要
	6．メディア（格納デバイス）	・基本は IC カード	・基本は IC カード
	7．取り扱い留意点	・影響が大きいため厳重な管理が必要	・厳重な管理が必要、かつ、複数管理する負荷がより大きい。
E.ｾｷｭﾘﾃｨ	1．運用 1.1 貸借 1.2 耐犯罪性	秘密鍵は IC カード等へ格納のうえ厳重な管理が必要 ・貸借は禁止 ・1枚で実行できる業務処理の範囲／影響が大きいため、狙われる危険性が大きい	秘密鍵は IC カード等へ格納のうえ厳重な管理が必要 ・貸借は禁止 ・シングルに比べてリスクは分散するが狙われる危険性は大きい。
F.緊急時対応(リスクの集中度)	1．検証局のダウン	・リスク集中　－　1枚のため対象検証局がダウンした場合検証不可能	・シングルに比べてリスクは分散
	2・ネット上のサービス窓口	・リスク集中　－　サービス利用不可能	・シングルに比べてリスクは分散
G.コスト	1．発行 1.1 審査/発行/ 1.2 更新/失効/削除	・低い方がよい。 ・サービスの付加価値（信頼性の高低など）による料金のバリエーション	・低い方がよい。 ・サービスの付加価値（信頼性の高低など）による料金のバリエーション
	2．　運用 2.1 運用体制 2.2 ﾈｯﾄﾜｰｸ・ｷｬﾊﾟｼﾃｨ	・CA は唯一であるため、独自の運用体制、運用時間を設定可能	・全業界統一の運用体制、運用時間が望ましい

4.2.2 個別証明書とマルチ証明書の比較表

4.2.2.1 クレジットサービス

比較項目		世界	
分類	項目	個別証明書	マルチ証明書
A.概要/定義	1．何を認証するか	･決済を行おうとしている人物が当該クレジットカードの正当な行使権利保有者であること	･決済を行おうとしている人物が、(業界の認めた)クレジットカードの正当な行使権利保有者であること)
	2．証明書の持つ情報	･証明書を発行する主体(=サービス提供者=カード会社)ごとにユニークとなるような個人を特定する情報。	･証明書を発行する主体(=カード業界)でユニークとなるような個人を特定する情報。
	3．格納情報	･シリアル NO、鍵/証明書の有効期限、署名アルゴリズム等の一般的な証明書格納情報 ･ＣＡ(=サービス提供者=カード会社)の情報･公開可能な個人の属性(氏名程度か?)	･シリアル NO、鍵/証明書の有効期限、署名アルゴリズム等の一般的な証明書格納情報 ･ＣＡ(=カード業界)の情報･発行カード会社の情報(一定の体系に則り、対象カードの発行会社が判別できるようなもの)、公開可能な個人の属性(氏名程度か?)
	4．ＣＡの数	･複数	･カード業界で１
	5．証明書枚数	･当該個人が利用するクレジット決済サービス数	･利用する個人にカードアプリとして１枚
	6．使用場面（限定する場合記入）		
B.特徴		･クレジット決済サービスごとに発行される。各クレジットサービス提供者が自分の会員に発行するものなので、証明書上の情報はほとんど自由に設定できるが、ネットワーク上でのクレジット決済を考える場合、カード NO は公開できないので、証明書に記載することはできない。	･クレジットカードの枚数に関らず、クレジット決済を利用する個人に対し 1 枚発行される。参加する各クレジットサービス提供者が合意した情報を一律設定する。ネットワーク上でのクレジット決済を考える場合、カード NO は公開できないので、証明書に記載することはできない。
C.ネット社会での自由度	1．名義（別名・仮名）を持てる	･現実的には不可	･現実的には不可
	2．ﾌﾟﾗｲﾊﾞｼｰ	･カード会社と利用者は予め取り決め事項に合意する。各カード会社に情報は保管されるので、比較的安全。	･一箇所で管理する為､そこが信頼されれば守られる。
	3．制御(利用側)	･サービス毎ごとに使い分け可能である反面、使い分け制御は必要。	･1 枚なのでクレジット決済という範疇では、証明書の使い分けは出来ない。
	4．ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	･発行主体のポリシーに依存する。 ･一般的には、有事の際の捜査機関等への提供は、利用規約等で事前の取り決めがなされる。	･発行主体のポリシーに依存する。 ･一般的には、有事の際の捜査機関等への提供は、利用規約等で事前の取り決めがなされる。

	5．サービス設計	・サービス提供者が自ら発行する証明書なので、自由度が高い。反面、ユーザインタフェースは各サービス毎に操作方法が異なるなどの問題が出る可能性はある。	・証明書には、(参加カード会社の合意した)規定項目のデータしかないため、独自のサービス展開をする場合は、アプリケーションに必要となるデータは別に供給しなければならない。
	6．ユーザ鍵ペアの有効期限	・自由に設定可能だが、リアルのカードと関連付けるとすれば2～4年程度の自動更新	・参加カード会社の合意した規定サイクル(2～4年)での自動更新
	7．審査/発行/更新	・各ＣＡ(=サービス提供者=カード会社) の判断で発行できる。 ・ポリシー次第で、対面手続き等を省略した使い勝手を重視した方法でも可能。 ・更新は、自動更新が現実的(?)	・参加カード会社が合意した規定基準の方法(公的書面確認・対面手続き?) での本人確認が必要。 ・更新も参加カード会社が合意した規定基準の方法(郵送?)
D.運用性	1．紛失時　：失効・削除・再発行	・当該サービスのみが利用不能となるため、影響は比較的小さい。但し、記憶媒体等に複数の証明書があって、一度にクラッシュしたような場合、1枚1枚再発行の手続きが必要となる。	・全クレジット決済が利用できなくなるので影響大。 ・再発行時は仮に複数枚のクレジットカードを保有している場合でも、証明書の再発行手続きは一回で済む。
	2．認証サービス利用の課金	・年額の一定費で、クレジット代金と併せて自動的に口座から引き落としが可能 (利用への課金というよりも、発行手数料イメージ)	・一定額で口座引き落としが可能ではあるが、複数枚のカードで証明書を共有している場合、どのカード分とするか取り決めが必要。
	3．証明書の配布	・郵送、またはパスワードチェックつきダウンロード形式	・対面／郵送／パスワードつきダウンロード形式
	4．証明書の利用実績の通知	・証明書利用時は、クレジット決済を前提にしているので、クレジットの請求書で代用可能 ・上記以外の分野での利用は、制限するものではないが通知の義務はないと考える。	・関連付けているクレジットカードの利用明細で代用可能ではあるが、複数枚のカードで証明書を共有している場合、どのカード分とするか取り決めが必要。
	5．約款の送付	・契約時に提示は必要。郵送時は同封、ダウンロード時は「合意する」ボタンを押させる形式か？	・契約時に提示は必要。郵送時は同封、ダウンロード時は「合意する」ボタンを押させる形式か？
	6．メディア（格納デバイス）	・証明書の情報量は、個人間で大差が出るほどではない。 ・証明書を行使する段階で、最低パスワードチェックが可能な媒体。	・証明書の情報量はほとんど一定。個人間で大差が出るほどではない。 ・証明書を行使する段階で、最低パスワードチェックが可能な媒体。
	7．取り扱い留意点	・相対の秘密鍵は厳重な管理が必要である。	・相対の秘密鍵は厳重な管理が必要である。
E.ｾｷｭﾘﾃｨ	1．運用 1.1 貸借 1.2 耐犯罪性	・何らかの理由により利用が不可能になった場合、代替クレジット決済を利用することは可能。 ・証明書の貸借は禁止。(秘密鍵の貸借を行わない限り事実上意味はない) ・利用者側の秘密鍵保管方法に依存する。	・何らかの理由により利用が不可能になった場合、全クレジットサービスが利用不能。 ・証明書の貸借は禁止。(秘密鍵の貸借を行わない限り事実上意味はない) ・利用者側の秘密鍵保管方法に依存する。

F.緊急時対応 (ﾘｽｸの集中度)	1．検証局のダウン	･他のクレジット決済にて代替することは可能。また自社のサービスに閉じているため、やろうと思えば、インターネット以外の通信媒体(例えば電話など)を用い、自社の会員 DB を参照して回答することは可能。	･クレジット決済は利用できなくなる。
	2･ネット上のサービス窓口	･復旧を待つか、リアルの手段(手続き書類等)に切り替える。	･復旧を待つ。
G.コスト	1．発行 1.1 審査/発行/ 1.2 更新/失効/削除	･安いに越したことはないが、現実的には各カード会社間のサービス競争により決定。	･安い方がよい
	2．運用 2.1 運用体制 2.2 ﾈｯﾄﾜｰｸ･ｷｬﾊﾟｼﾃｨ	･利用する局面の特性を考慮した運用時間、サービスの設定が可能	･基本的に 365 日、24 時間サービス提供

4.2.2.2 銀行サービス

比較項目		世界	
分類	項目	個別証明書	マルチ証明書
A.概要/定義	1．何を認証するか	･個人認証	･個人認証
	2．証明書の持つ情報	･個人特定情報	･個人特定情報
	3．格納情報	･個人情報（口座新約に必要な情報････氏名、住所、電話番号、生年月日）	･個人情報（口座新約に必要な情報････氏名、住所、電話番号、生年月日）
	4．CAの数	･複数	･1
	5．証明書枚数	･複数	･1
	6．使用場面（限定する場合記入）	･インターネットを利用したﾈｯﾄﾊﾞﾝｷﾝｸﾞでの振込	･インターネットを利用したﾈｯﾄﾊﾞﾝｷﾝｸﾞでの振込
B.特徴		･利用会社毎に一枚発行	･利用者に対し一枚発行
C.ネット社会での自由度	1．名義（別名･仮名）を持てる	･不可	･不可
	2．プライバシー	･各銀行に依存。お客様情報の管理に対するセキュリティは従来業務と同じ（またはそれ以上）	･一箇所で管理するため、そこが信頼されれば守られる
	3．制御(利用側)	･利用銀行毎に使い分け	･1 枚なので証明書の使い分けは出来ない
	4．ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	･振込、振替であれば資金の移動先は追求可能。現金化なればトレース困難。	･振込、振替であれば資金の移動先は追求可能。現金化なればトレース困難。
	5．サービス設計	･証明書にアプリケーション用の情報がないので、サービスの登録時には、外部のアプリケーション用の情報を提供する必要がある。	･証明書にアプリケーション用の情報がないので、サービスの登録時には、外部のアプリケーション用の情報を提供する必要がある。
	6．ユーザ鍵ペアの有効期限	･ユーザ鍵ﾍﾟｱの有効な限り	･ユーザ鍵ﾍﾟｱの有効な限り
	7．審査/発行/更新	･審査：口座保有者で、本人確認問題なければ対応。	･審査：口座保有者で、本人確認問題なければ対応。
D.運用性	1．紛失時　：失効･削除･再発行	･手順：喪失に伴う届け出　→　無効化　→　再発行 （印鑑喪失と同様）	･手順：喪失に伴う届け出　→　無効化　→　再発行 （印鑑喪失と同様）

	2．認証サービス利用の課金	・無料	・無料
	3．証明書の配布	・書留郵便	・書留郵便
	4．証明書の利用実績の通知	・銀行の口座明細（通帳等）で代用可能	・銀行の口座明細（通帳等）で代用可能
	5．約款の送付	・契約書に添付（手交）	・契約時に呈示（手交）
	6．メディア（格納デバイス）	・IC ｶｰﾄﾞ等	・IC ｶｰﾄﾞ等
	7．取り扱い留意点	・厳重管理	厳重管理
E.ｾｷｭﾘﾃｨ	1．運用 1.1 貸借 1.2 耐犯罪性	・何らかの理由により利用が不可能になった場合、全振込サービスが利用不能。 1.1　貸借：禁止。 1.2　本人に成りすまし、振込を利用した資金の払出。	・何らかの理由により利用が不可能になった場合、全振込サービスが利用不能。 1.1　貸借：禁止。 1.2　本人に成りすまし、振込を利用した資金の払出。
F.緊急時対応（ﾘｽｸの集中度）	1．検証局のダウン	・他のサービス提供者（銀行）を利用する。	・利用不可となる
	2・ネット上のサービス窓口	・利用不可となり、代わりに銀行窓口・ＡＴＭを利用することで対応。	・利用不可となり、代わりに銀行窓口・ＡＴＭを利用することで対応。
G.コスト	1．発行 1.1 審査/発行/ 1.2 更新/失効/削除	1.1　審査、発行･･･無料 1.2　更新･･･無料、失効･･･有料（再発行ｺｽﾄ 800 円）、削除･･･無料	1.1　審査、発行･･･無料 1.2　更新･･･無料、失効･･･有料（再発行ｺｽﾄ 800 円）、削除･･･無料
	2．運用 2.1 運用体制 2.2 ﾈｯﾄﾜｰｸ・ｷｬﾊﾟｼﾃｨ	・365 日、24 時間。 ・STP 化によるコストセーブ	・365 日、24 時間。 ・銀行間ﾈｯﾄﾜｰｸによるコスト負担

4.2.2.3 マイレージサービス

比較項目		世界	
分類	項目	個別証明書	マルチ証明書
A.概要/定義	1．何を認証するか	・マイレージサービス会員の個人認証	・マイレージサービス会員の個人認証
	2．証明書の持つ情報	・個人を特定する情報	・個人を特定する情報と証明書発行航空会社の企業情報
	3．格納情報	・属性情報：氏名（最小限）、その他属性情報については航空会社の任意	・属性情報：氏名 ・企業情報：証明書発行航空会社の識別子
	4．CAの数	・航空会社毎に1つ	・航空会社毎に1つ
	5．証明書枚数	・マイレージサービス提供会社毎に1つ	・同盟航空会社単位に1つ
	6．使用場面（限定する場合記入）	・航空券発券時とマイレージ交換時	・航空券発券時とマイレージ交換時
B.特徴			
C.ネット社会での自由度	1．名義（別名・仮名）を持てる	・持てない	・持てない
	2．プライバシー	・航空会社と利用者は入会時の取決め事項に合意する ・航空会社内で情報管理される為、航空会社の管理状況に依存する	・航空会社とは利用者は入会時の取決め事項に合意する ・証明書発行航空会社内で保管される為、証明書発行航空会社の管理状況に依存する
	3．制御(利用側)	・マイレージサービス提供会社毎に必要	・同盟航空会社内であれば必要ない
	4．トレーサビリティ（犯罪）	・航空会社と利用者間は入会時の取決め事項に準じ可能である	・証明書発行航空会社と利用者間は入会時の取決め事項に準じる可能である ・同盟航空会社間は業務提携契約内で可能である
	5．サービス設計	・マイレージサービス提供会社が自由に設計出来る為、自由度が高い	・同盟航空会社間のインターフェイスを考慮する必要があり自由度は低い
	6．ユーザ鍵ペアの有効期限	・鍵の安全性が保証出来る期間（2年程度の自動更新が妥当）	・鍵の安全性が保証出来る期間（2年程度の自動更新が妥当）
	7．審査/発行/更新	・申込情報に基づき航空会社の判断で審査／発行／更新できる	・同盟航空会社のルール遵守を前提に、申込情報に基づき証明書発行航空会社の判断でじ審査／発行／更新できる
D.運用性	1．紛失時　：失効・削除・再発行	・個人属性情報を基づくオフライン処理が整備されておれば影響は少ない	・同盟航空会社間でオフライン処理が整備されておれば影響は少ない

	2．認証サービス利用の課金	・自社航空機利用促進のサービスであり、再発行等以外での会員課金は困難である	・自社航空機利用促進のサービスであり、再発行等以外での会員課金は困難である
	3．証明書の配布	・初回のみ郵送、次回以降はオンラインダウンロード	・初回のみ郵送、次回以降はオンラインダウンロード
	4．証明書の利用実績の通知	・都度の利用実績はインターネット等を用いた照会サービスで問題無いと思われるが、インターネット接続環境が無い利用者も想定し、年に1回程度の有効マイレージの失効通知に合せた郵便による通知が必要	・都度の利用実績はインターネット等を用いた照会サービスで問題無いと思われるが、インターネット接続環境が無い利用者も想定し、年に1回程度の有効マイレージの失効通知に合せた郵便による通知が必要
	5．約款の送付	・マイレージサービス入会タイミングで郵送	・マイレージサービス入会タイミングで郵送
	6．メディア（格納デバイス）	・ICカードを想定（但し、限定するものでは無い） ・会員毎の情報量変動は無い	・ICカードを想定（但し、限定するものでは無い） ・会員毎の情報量変動は無い
	7．取り扱い留意点	・相対の秘密鍵は厳重な管理が必要である	・相対の秘密鍵は厳重な管理が必要である
E.ｾｷｭﾘﾃｨ	1．運用 1.1 貸借 1.2 耐犯罪性	・貸借禁止 ・利用者側の証明書保管方法に依存する	・貸借禁止 ・利用者側の証明書保管方法に依存する
F.緊急時対応（ﾘｽｸの集中度）	1．検証局のダウン	・利用出来なくなるが、個人属性情報に基づくオフライン処理が整備されておれば影響は少ない	・利用出来なくなるが、個人属性情報に基づくオフライン処理が整備されておれば影響は少ない
	2・ネット上のサービス窓口	・利用出来なくなるが、個人属性情報に基づくオフライン処理が整備されておれば影響は少ない	・利用出来なくなるが、個人属性情報に基づくオフライン処理が整備されておれば影響は少ない
G.コスト	1．発行 1.1 審査/発行/ 1.2 更新/失効/削除	・再発行以外は航空会社での負担となる ・航空会社での負担となる	・再発行以外は証明書発行航空会社での負担となる ・証明書発行航空会社での負担となる
	2．運用 2.1 運用体制 2.2 ネットワーク・ｷｬﾊﾟｼﾃｨ	・365日／24時間 ・大量のトランザクション発生が見込まれる。また、閑散期や繁忙期なども考慮する必要がある	・365日／24時間 ・大量のトランザクション発生が見込まれる。また、閑散期や繁忙期なども考慮する必要がある

4.2.2.4 損害保険

比較項目		世界	
分類	項目	個別証明書	マルチ証明書
A.概要/定義	1.何を認証するか	・保険契約者（申込者）であることの認証	・特定できる個人・法人であることの認証
	2.証明書の持つ情報	・保険契約者（申込者）を特定する情報（被保険利益の有無は問わない）	・被保険利益のある保険契約を保有する個人を特定する情報
	3.格納情報	・住所、氏名（または名義）、包括予定証券または特約書番号等	・住所、氏名（または名義＊1）、既存契約の保険会社コード、会員番号
	4.ＣＡの数	・複数	・1つ
	5.証明書枚数	・利用する保険契約の数	・1名義（＊1）につき1枚
	6.使用場面（限定する場合記入）	・その利用する保険種目以外では使えない。	・各社で割引保険料率を適用できる、または簡便に保険加入が出来る(ゴールド免許割引の様なもの)
B.特徴			
C.ネット社会での自由度	1.名義（別名・仮名）を持てる	・職域や団体の一員としての名義を持つこともあり得る。（＊1）	・職域や団体の一員としての名義を持つこともあり得る。（＊1）
	2.プライバシー	・各社が守秘義務によって保護する。	・各社が守秘義務によって保護する。ただし、他社切替え時点で事故歴等一部データが引き渡される。
	3.制御(利用側)	・複数名義があれば、都合の良い証明書を選択可能。	・複数名義があれば、都合の良い証明書を選択可能。
	4.ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	・原則トレース可能。しかし、職域や団体の一員として利用した場合等で困難なケースもありうる。	・原則トレース可能。しかし、職域や団体の一員として利用した場合等で困難なケースもありうる。
	5.サービス設計	・各々保険会社で自由に設計できる。	・各々保険会社で自由に設計できる。
	6.ユーザ鍵ペアの有効期限	・2,3年程度。	・保険申し込み時から保険終期まで。次年度からは保険期間にリンク。
	7.審査/発行/更新	・個人の場合はクレジット口座情報等、法人の場合は調査会社情報等を利用して審査。自動更新。	・既存保険契約情報がある場合は簡便な審査で発行、純新規の場合は＋αの審査が必要。自動更新。
D.運用性	1.紛失時　：失効・削除・再発行	・鍵を変えて再発行する	・鍵を変えて再発行する
	2.認証サービス利用の課金	・保険証券・約款印刷費、郵送費セーブになるので課金しないが、保険解約時は500円程度相殺する。	・保険証券・約款印刷費、郵送費セーブになるので課金しないが、保険解約時は500円程度相殺する。

	3.証明書の配布	・「郵送＋オンライン」作業の組み合わせによる配布。	・「郵送＋オンライン」作業の組み合わせによる配布。
	4.証明書の利用実績の通知	・使用した月は一ヶ月分の明細をまとめて郵便（ハガキ等）で送付。	・使用した月は一ヶ月分の明細をまとめて郵便（ハガキ等）で送付。
	5.約款の送付	・郵便（ハガキ等）にて概要を送付。全文は Mail で配布。	・郵便（ハガキ等）にて概要を送付。全文は Mail で配布。
	6.メディア（格納デバイス）	・IC カードまたは PC 本体	・IC カード。
	7.取り扱い留意点	・利用者側の保管方法に依存する。	・厳重な保管。
E.ｾｷｭﾘﾃｨ	1.運用 1.1 貸借 1.2 耐犯罪性	・禁止 ・契約者が被害を受ける可能性低いが、他人の不正請求により保険会社が被害を受ける危険はある。	・禁止 ・契約者が被害を受ける可能性低いが、他人の不正請求により保険会社が被害を受ける危険はある。
F.緊急時対応 (ﾘｽｸの集中度)	1.検証局のダウン	・海外旅行総合など至急証券発行のいるものは被害大きいが、年建契約はバッチ処理等で対応できる。	・海外旅行総合など至急証券発行のいるものは被害大きいが、年建契約はバッチ処理等で対応できる。
	2.ネット上のサービス窓口	・保険会社のコールセンター等である程度の対応は出来るが、トラブル規模によっては捌ききれない。	・保険会社のコールセンター等である程度の対応は出来るが、トラブル規模によっては捌ききれない。
G.コスト	1.発行 1.1 審査/発行/ 1.2 更新/失効/削除	・既存 IC カードへ鍵等ダウンロードする場合、保険証券郵送に合わせて仮 ID のメモを同封するなどすれば、コスト低く抑えることが可能。IC カード希望者には実費をもらいコストセーブする。 ・更新時も契約あれば郵送代が別途かからないのでよいが、無い場合には郵送代等の実費請求をする。	・既存 IC カードへ鍵等ダウンロードする場合、保険証券郵送に合わせて仮 ID のメモを同封するなどすれば、コスト低く抑えることが可能。IC カード希望者には実費をもらいコストセーブする。 更新時も契約あれば郵送代が別途かからないのでよいが、無い場合には郵送代等の実費請求をする。
	2.運用 2.1 運用体制 2.2 ﾈｯﾄﾜｰｸ･ｷｬﾊﾟｼﾃｨ	・各保険会社のオンライン」稼働時間に拘束される。 ・月末、月初、オンライン」終了時間間際に負荷集中が予想される。	・各保険会社のオンライン」稼働時間に拘束される。 ・月末、月初、オンライン」終了時間間際に負荷集中が予想される。

4.2.2.5 会社毎の情報提供等サービス

比較項目		世界	
分類	項目	個別証明書	ﾏﾙﾁ証明書
A.概要/定義	1．何を認証するか	･情報サービス加入者の個人認証	･情報サービス加入者の個人認証
	2．証明書の持つ情報	･個人を特定する情報と情報提供サービスの利用者識別子	･個人を特定する情報と情報提供サービスの利用者識別子
	3．格納情報	･ID 情報:情報提供サービスの利用者識別子 ･属性情報:氏名(最低)、サービスに特化した属性(オプション)	･ID 情報:情報提供サービスの利用者識別子 ･属性情報:氏名(最低)、生年月日(オプション)
	4．CAの数	･会社、サービスに応じて複数。最大 1 サービス毎の CA	･対象地域、サービスの種類に応じて 1 つ
	5．証明書枚数	･利用する情報提供サービス数	･対象地域、サービスの種類であるが、利用者は 1 枚
	6．使用場面 (限定する場合記入)		
B.特徴		･情報提供サービス会社ごとに発行される	･情報提供サービス加入者に対し一枚発行される
C.ネット社会での自由度	1．名義 (別名･仮名) を持てる	･持てる(法人契約も考えられる為)	･持てない(サービスポリシーによっては可能)
	2．ﾌﾟﾗｲﾊﾞｼｰ	･利用会社毎に管理されるのでサービス提供会社のﾎﾟﾘｼｰおよび運用体制に依存	･一箇所で管理する為、そこが信頼されれば守られる
	3．制御(利用側)	･使い分け可能	･1 枚なので使い分けは出来ない
	4．ﾄﾚｰｻﾋﾞﾘﾃｨ (犯罪)	･個人 ID→個人(例.住所、氏名)の特定の可能性はｱﾌﾟﾘｹｰｼｮﾝとそのﾌﾟﾗｲﾊﾞｼｰ保護ポリシーに依存する。	･個人 ID→個人(例:住所、氏名)の特定の可能性はそのﾌﾟﾗｲﾊﾞｼｰ保護ポリシーに依存する
	5．サービス設計	･新たな情報を提供することなく、同社が提供する関連サービス共通で利用できることが可能	･新たな情報を提供することなく、共通で利用できることが望ましい
	6．ユーザ鍵ペアの有効期限	･有効期限は 1 年間、自動更新	･有効期限は 1 年間、自動更新
	7．審査/発行/更新	･情報提供サービスの判断	･情報提供サービス･ﾄﾞﾒｲﾝ(地域、又はサービス業種)の判断

D.運用性	1．紛失時　：失効・削除・再発行	・ﾏﾙﾁﾙ証明書に比べ、ﾘｽｸは分散されるが、同じような情報サービスに複数加入している利用者も少ないと想定されるので利用者にとっては影響大	・全情報サービスが利用できなくなるので影響大 ・再発行時は上記と同じ手続き
	2．認証サービス利用の課金	・サービス料金に含まれる	・サービス料金に含まれる
	3．証明書の配布	・郵送又はオンライン」	・郵送又はオンライン」
	4．証明書の利用実績の通知	・不必要(利用明細がある)	・不必要(利用明細がある)
	5．約款の送付	・契約時に必要	・契約時に必要
	6．メディア（格納デバイス）	・IC カード	・IC カード
	7．取り扱い留意点	・厳重な管理が必要であり、かつ、複数管理する必要があり、管理負荷がより大きい	・厳重な保管が必要
E.ｾｷｭﾘﾃｨ	1．運用 1.1 貸借 1.2 耐犯罪性	・サービスポリシーによる ・紛失した場合、他人が使用してしまう可能性がある	・サービスポリシーによるが原則禁止 ・紛失した場合、他人が使用してしまう可能性がある
F.緊急時対応（リスクの集中度）	1．検証局のダウン	・リスクが分散される	・利用できなくなる
	2・ネット上のサービス窓口	・リスクが分散される	・利用できなくなる
G.コスト	1．発行 1.1 審査/発行/ 1.2 更新/失効/削除	・無料(サービス料金に含まれる）。紛失の場合の再発行は実費。 ・更新、失効、削除は無料	・無料(サービス料金に含まれる)。紛失の場合の再発行は実費。 ・更新、失効、削除は無料
	2．運用 2.1 運用体制 2.2 ﾈｯﾄﾜｰｸ・ｷｬﾊﾟｼﾃｨ	情報提供サービスのポリシーに依存 負荷はマルチと比較して低い	・独自の運用時間帯を設定するのはサービスの性質上困難 ・負荷は高い

4.3 比較結果

4.3.1 シングル証明書の要件

シングル証明書は１枚の証明書で種々のサービスを受けることを想定している。これら各サービスに必要なシングル証明書に対する要件から、シングル証明書に必要な共通的な項目について評価した。

人間活動の抽象的な項目について、シングル証明書として共通に利用できる項目／内容および、サービス毎のバリエーションを表 4-3-1 に示した。シングル証明書は利用者、利用企業を特定する証明書をサービスに係らず共通に使用することを想定していることから、サービス色のない、サービス間で共通に利用できる要件が多い。

シングル証明書としての要件のうち、サービス間で内容が異なり、今後の検討が必要となる項目を課題として以下に示す。

① プライバシー：１箇所での管理のため、そこの信頼度により個人情報は守られるが、証明書に記載された項目は原則公開となる。サービス登録の方法が複数あれば、信頼度の度合いは一定にならない恐れあり。

② 課金：考え方はサービス毎に異なる。証明書毎に課金する認証書利用料としてではなく、サービス毎に独立した、サービス利用料としての課金が必要と考えられる

③ セキュリティ：耐犯罪性については種々の手法があげられている。サービス間で共通に利用できるもの、および、サービス固有なものの両方が有る

④ ユーザ鍵ペアの有効期限：サービスにより、１年もしくは３～５年の差がある。

⑤ 更新／失効：費用の負担の考え方がサービスにより異なる

表4．3－1 シングル証明書世界の比較

比較項目				
分類	項目	シングル証明書概要	シングル証明書バリエーション	特徴
A.概要/定義	１．何を認証するか	個人認証（本人特定）	（１）個人認証（本人特定） （２）申請時点で要件を満たした申請者の存在 「要件例」 ・申請書にある住所・氏名・生年月日の一致 ・身分証明が出きる、例えば、運転免許証のようにサービスごとの証明書を得るための大元の証明書となる （３）申請時点で要件を満たした申請者の存在 「要件例」 ・企業登記情報と一致する	
	２．証明書の持つ情報	個人／企業を特定する情報に制限	（１）個人を特定する情報／基本情報のみ （２）事業者の特定情報（登記情報→公証）	
	３．格納情報	最小限の属性情報に限定	（１）属性情報：氏名、生年月日、性別、住所（住民４情報）・・・ （２）ID情報：住民番号 属性情報：氏名、生年月日、性別・・・ （３）ID・氏名 ID：住民番号（個人を特定するID番号） （これ以上の情報格納を行うとサービスに不要な情報まで相手に渡ってしまう） （４）ID・住所・代表者氏名 ID：会社法人等番号	
	４．ＣＡの数	１	数：1	
	５．証明書枚数	１	数：1	
	６．使用場面（限定する場合記入）	（省略）	（省略）	
B.特徴		個人に対して１枚発行される。	（１）個人に対し１枚の証明書が発行され、その１枚で全ての認証業務に利用される。 （２）住民登録と関連付けた証明書とするのが望ましい シングル証明書は、利用者が選択したサービス全てを１枚の証明書で受けることが出きるもの （３）企業登記と関連付けた証明書とすることが望ましい	

C.ネット社会での自由度	１．名義（別名・仮名）を持てる	持てない。	（１）持てない（シングル証明書はあくまで個人（本人）に対して発行される）。 （２）業者を特定するため別名や仮名は持てない	
	２．プライバシー	１箇所で管理し、そこの信頼性に依存、もしくは、複数のサービス登録方法を許し、信頼性のバラツキを許容する。	（１）１箇所で管理されるため、そこが信頼されれば守られる。 （証明書に氏名、生年月日等が含まれるならば、それらは公になる。） （証明書に不必要な属性情報は掲載しない） （２）保証が無い （３）サービス利用登録に依存する 利用者は規約／約款を確認し、個人の責任において利用者登録を実施 （４）サービス利用登録に依存する ・サービス提供業者として規約・約款の整備が必要 ・サービス提供に必要最低限の情報保持につとめる	１箇所での管理か、登録方法の多様性を許容するかで異なる
	３．制御 （利用側）	使い分けは出来ない	１枚なので使い分けはできない。	
	４．ﾄﾚｰｻﾋﾞﾘﾃｨ（犯罪）	あり	（１）　個人特定の可能性は、そのプライバシー保護ポリシーに依存する。 秘密鍵格納媒体が、利用者によって厳重に管理されれば犯罪は起こりにくい。 （投票したことは判断できるが、「誰」に投票したかはわからない仕組みが必要） （２）個人 ID→個人の特定の可能性は、そのプライバシー保護ポリシーに依存する （３）困難 （４）あり（完全性を求める場合はバイオ連携が有望） （５）あり（企業内部での運用にかかる比重が大）	
	５．ｻｰﾋﾞｽ設計		（１）　証明書にアプリケーション用の情報がないので、外部アプリケーション用の情報が必要である。 （２）　各決済機関におけるキーのアクティベートを標準化 （３）　サービス利用登録におけるキーのアクティベートが標準化され、利用登録において最低限の情報を提示することによって、以降、該当サービスへのアクセスが可能となる	
	６．ユーザ鍵ペアの有効期限	１年もしくは３～５年	（１）原則１年、自動更新（オンライン更新）されることが望ましい。 （２）原則１年、自動更新 （３）３～５年？（鍵の有効期限＝証明書有効期限？） （４）３～５年？（鍵の有効期限＝＜証明書有効期限？）	

	７．審査/発行/更新	審査・発行は対面にて実施。更新はオンラインでも可能。	（１）初期発行、および属性変更は、安全性の観点から対面手続きが望ましい。 更新は、負荷削減の観点からオンライン手続きが望ましい。 （２）本人確認のため対面手続きが必要 （３）審査・発行：公的機関による対面手続き 更新：対面は必須ではない（対面手手続きが好ましい？） （４）審査・発行：公的機関による対面手続き 更新：実質的には再発行、申込み手続きはネットで可	
D.運用性	１．紛失時　：失効・削除・再発行	影響は大。セキュリティ確保のため、再発行は対面にて実施。	（１）全てのサービスが利用できなくなるため影響大 再発行は、失効処理を行った後、再度対面手続き（発行と同じ）を行う必要がある。 （２）失効：緊急（Tel）、標準（対面） 再発行：発行とおなじ対面手続き	
	２．認証サービス利用の課金	無料、口座引き落とし、決済期間への手数料に含める、もしくはサービス提供者が負担。	（１）投票といったアプリケーションにおいては、課金は無い。 （認証機能提供側が、証明書発行時、もしくは検証時に、課金を行うこともありうる。） （２）サービス契約時に金融機関の口座番号を提示して、口座引き落とし （３）利用サービスに依存する。決済機関への手数料に含まれるものと考える （４）利用サービスに依存する。認証に要する費用はサービス提供者が負担	課金に対する考え方はサービス毎に大きく異なる
	３．証明書の配布	対面、郵送（書留、本人限定郵便）など本人に確実に渡す方法	（１）対面／郵送（書留、本人限定等直接本人に渡る仕組み） （２）IC カードで配布・対面受領 （３）IC カードで配布。郵送は好ましくない（PIN 別ルート）	
	４．証明書の利用実績の通知	アプリケーション利用実績として必要	（１）あらゆるアプリケーションで利用可能なため、利用実績を把握するためにも通知はあることが望ましい。 郵送、もしくはメールによる通知。 （２）利用実績を確認するために必要。郵送 （３）必須	
	５．約款の送付	証明書発行時の共に配布	（１）証明書発行時に、併せて配布されることが望ましい。 更新内容は、ホームページ等で公開されていることが望ましい。 （２）契約時の送付が必要 （３）証明書に関しては証明書発行時に必要。サービスに係るものはサービス利用登録時に送付	
	６．メディア（格納デバイス）	IC カード等容易に秘密情報の書込み／参照／更新が出来ない仕組みが必要	（１）格納される情報量により差が出るが、2～3Kbytes 程度の証明書と秘密鍵が格納できる媒体 容易にデータ書込み／参照／更新ができない仕組みを持つ媒体 （２）基本は IC カード （３）当面は IC カード	

	７．取り扱い留意点	利用者に、自分／企業の全資産に接近しうる鍵であることを認識させ、厳重に保管させる。	（１）問題が生じた際には利用サービス全てに影響がでるため、厳重な管理が必要 （２）影響が大きいため厳重な保管が必要 （３）利用者に、単なる証明書でなく、自分、企業の全資産に接近しうる鍵であることを徹底認識させる	
E.セキュリティ	１． 運用 1.1 貸借 1.2 耐犯罪性	1.1 秘密情報は IC カードに格納し、貸借は禁止する。 1.2 対犯罪性は種々の手法が種々提案されている。	秘密鍵は IC カード等へ格納の上、厳重な管理が必要 1.1 禁止 1.2 （１）１枚で実行できる業務処理の範囲／影響が大きいため、狙われる危険性が高い。 （アプリケーションとしては、2 重投票のチェック、投票者の匿名性を保つ、投票権の譲渡を禁止する等の仕組みが必要） （２）企業登記＋決済機関のチェックでガード、また証明書保管に関する運用規定を罰則とともに設けるべき （３）生体情報とのコンビが有効	耐犯罪性の手法についてサービス間で共通に利用できるもの、サービス固有なものが種々挙げられている。
F.緊急時対応 (リスクの集中度)	１．検証局のダウン	CA のダウンについては余裕があるが、検証局のダウンについての影響は広範囲にわたる	（１）リスク集中　－　１枚のため対象検証局がダウンしたならば、全てのサービスが利用停止 （２）ＣＡの冗長性は必須だが、発行機能のダウンに対しては余裕がある。検証機能のダウンは決済の停止となりうるが、決済金額やその他の条件により決済期間のポリシーにかかる。	
	２・ネット上のサービス窓口	サービス窓口のダウンの影響は大きい。証明書の失効については２４時間受付体制が必須。	（１）リスク集中　－　１枚のためサービス窓口がダウンしたならば、全てのサービスが利用停止 （２）緊急失効受付（２４時間）・電話／Email	
G.コスト	１．発行 1.1 審査/発行/ 1.2 更新/失効/削除	初期費用は低いことが望ましい。更新／失効費用はサービス付加価値により多様な要件が示されている。	（１）社会基盤であることから、発行は無料としサービス利用にコストをかけることが望ましい →現状の印鑑証明書は、登録は無料、利用は 300 円程度である（選挙は、特別扱い）。 発行の手間としては、発行の拠り所とする情報との連携がどのように実現されるかに依存する。 （２）１．１：低い方がよい １．２：サービスの付加価値（信頼性の高低など）による料金のバリエーション （３）１．１：初期発行費用 １． ２：更新費用＝初期発行費用、再発行費用には失効費用を含む。 通常失効＝なし、緊急失効費用＝あり、	シングル証明書の更新／失効費用は証明書の発行ポリシーなどで統一が望ましい。
	２．運用 2.Ｉ運用体制 2.2 ﾈｯﾄﾜｰｸ･ｷｬﾊﾟｼﾃｨ	あらゆるアプリケーションで利用されることから、冗長構成／地域分散が必要。	（１）高性能、高信頼性をもった認証サービス、検証サービスを提供する必要がある。 ２．１：CA は唯一であるため、独自の運用体制、運用時間を設定可能 ２． ２：あらゆるアプリケーションで利用可能なため、有効性確認の利用頻度が高い （２）２．１：証明書発行代金＋認証代金にて運用をカバー ２．２：ディレクトリサーバの冗長構成／地域分散	

4.3.2　抽象的サービスにおけるシングル証明書、マルチ証明書の比較

各サービス共通な､個人のみを特定して提供するシングル証明書と､各サービス毎に、サービス（業界）と個人の両方を特定して提供するマルチ証明書について必要な要件を抽出した。「選挙」については、実社会で使われている投票券が、サービスと個人の両方を特定（個別証明書）して提供しているため、個別証明書として必要な要件も抽出した。これらアプローチの違いが証明書の要件に現れる差異を評価する。この節では、サービスそのものに着目した証明書への要件を検討した。複数の互いに提携する事業体が混在することにより生じる要件については次項にて検討を進める。

4.3.2.1　情報提供と情報収集（選挙）

情報提供と情報収集として、選挙を例にして比較した。選挙での投票管理を、「個人を特定し任意の選挙への参加を管理」、「個人を特定し複数の選挙への参加を管理」及び「選挙を特定しこれに参加する個人を管理」の各面について検討した。これらをそれぞれ、サービスによらないシングル証明書､選挙用のマルチ証明書及び、１選挙に特化した個別証明書に対応させた｡現状の投票券は、１つの選挙と投票者とを特定しているため、個別証明書に対応する。

シングル証明書と比べたマルチ証明書の主な特徴は次のとおりである。選挙の枠組みで見た場合にはこれらの差は小さい。

[A．概要]：　利用は選挙のみ。年齢、選挙区を特定する情報が追加

[B．ネット社会での自由度]：　選挙用の識別情報が含まれる

[G．コスト]：　利用者からの利用料徴収の考え方が異なる

マルチ証明書と比べた個別証明書の主な特徴は下記のとおりであり、１選挙に利用可能対象を限定していることが現れている。

[A．概要]：　特定の選挙にのみ利用可。対象選挙を特定する情報が追加。

[C．ネット社会での自由度]：　投票期間にあわせて２週間程度に短縮。

[D．運用性]：　証明書の利用実績の通知を削除。

4.3.2.2 販売（個人対個人の販売）

(1) 購入

購入におけるシングル証明書と比較したマルチ証明書は、購入者本人の存在より、対価を支払う意思の確認、銀行口座との対応等決済可否に重点が置かれている。

シングル証明書と比較したマルチ証明書の主な特徴を下記に示す。

[A．概要]： 個人を特定するより、決済口座との対応が必要

[B．特徴]： 地方公共団体の発行ではなく、口座のある銀行、会社等による証明が必要。

(2) 販売

① 企業による販売

販売においては、「販売／購入時に相手を追跡できること」、もしくは「品物と販売代金を確実に渡してくれること」の２面がある。前者がシングル証明書、後者が銀行、マーケットプレイスなどが発行するマルチ証明書に対応する。前者は、販売者企業の存在の証明、後者は決済口座との対応（振込先確認）が要求されている。

当然ながら、シングル証明書でこのサービスを実際に受ける時には取引口座等の情報を別途相手方に通知するか、決済サービスに別途加入しておくなどの必要がある。

シングル証明書と比較したマルチ証明書の主な特徴を下記に示す。

[A．概要]： 企業の特定ではなく、決済口座との対応が必要

[B．特徴]： 法務局の発行ではなく、口座のある銀行による証明が必要。

② 個人対個人の販売

「①企業による販売」に示した分析と同様、シングル証明書と比較したマルチ証明書は、個人の存在の証明ではなく、個人の決済口座との対応の確認に重点が置かれている。

シングル証明書と比較したマルチ証明書の主な特徴を下記に示す。

[Ａ．概要]：　個人の特定ではなく、決済口座との対応が必要

[Ｂ．特徴]：　地方公共団体の発行ではなく、口座のある銀行による証明が必要。

4.3.2.3　送信

コンテンツ送信の例である。マルチ証明書の場合、コンテンツ種別毎に証明書を使い分けるものと想定している。マルチ証明書では、使い分けを行うため、仮名を許容し、リスクも分散されるため、鍵の有効期限を長期化している。

シングル証明書と比較したマルチ証明書の主な要件を下記に示す。

[Ａ．概要]：　ＣＡ数、証明書枚数がコンテンツ種別の数に応じて増加

[Ｃ．ネット社会での自由度]：　ユーザ鍵ペアの有効期限が１年から、１～３年と長期化。仮名を使用可能。

4.3.2.4　受信

コンテンツ配信サービスを受ける例である。マルチ証明書では、受信するコンテンツの業界毎に証明書を使用するものと想定している。

配信サービスの受信での仮名の扱いについて、次のような意見があった。

１）受取場所、受取人が特定できれば仮名の利用は可能

２）郵便の場合でも郵便局私書箱を利用しての郵便物受け取りに仮名が使える

３）オンラインでのデジタルデータ販売では決済が確実なら仮名の利用は可能

シングル証明書と比較したマルチ証明書の主な要件を下記に示す。

[Ａ．概要]：　ＣＡ数、証明書枚数が対象となる品物の業界に応じて増加

[Ｃ．ネット社会での自由度]：　ユーザ鍵ペアの有効期限が１年から、１～３年と長期化。仮名を使用可能。

4.3.3　具体的サービス毎のマルチ証明書、個別証明書の比較

実サービスにモデルが存在する具体的サービスについて検討した。実サービスにおいては、もともと事業主体が独立に提供していたサービスを、事業主体間の提携関係により企業グループ、業界等の単位で拡張してゆく流れがある。

事業主体が独立に提供しているサービスを個別証明書、企業グループ、業界等の単位で提供されるサービスをマルチ証明書に対応させて検討した。サービスの流れとして、当初、個別証明書にて提供し、提携などにより、マルチ証明書に移行しているが、3章で示したマルチ証明書の一部変形した形態となっている例がある。これらの例も含め、証明書の将来の利用形態について、示唆を与えてくれるものと考えられる。

4.3.3.1　クレジットサービス

クレジットカードには一般に、カード発行会社のマークだけでなく、国際ブランドマークも記載されている。加盟店は、カード会社と加盟店契約を締結すると、そのカード会社と対応する国際ブランドマークの記載された他社クレジットカードも利用可能となる。これにより、カード発行会社が個別に加盟店と契約を結ばなくとも、同じ国際ブランドに属するカード会社が契約している加盟店であればカードの利用が可能となっている。

たとえば、特定の百貨店のみで使えるカード（ハウスカード）等にクレジットカードの機能を新たに追加する例が多いが、これは、個々の百貨店のサービスに閉じる個別証明書の世界から、クレジット会社が契約する加盟店のドメインでも利用できるマルチ証明書の世界へ展開される例と言える。

図4．3－1　クレジットカードにおけるマルチ証明

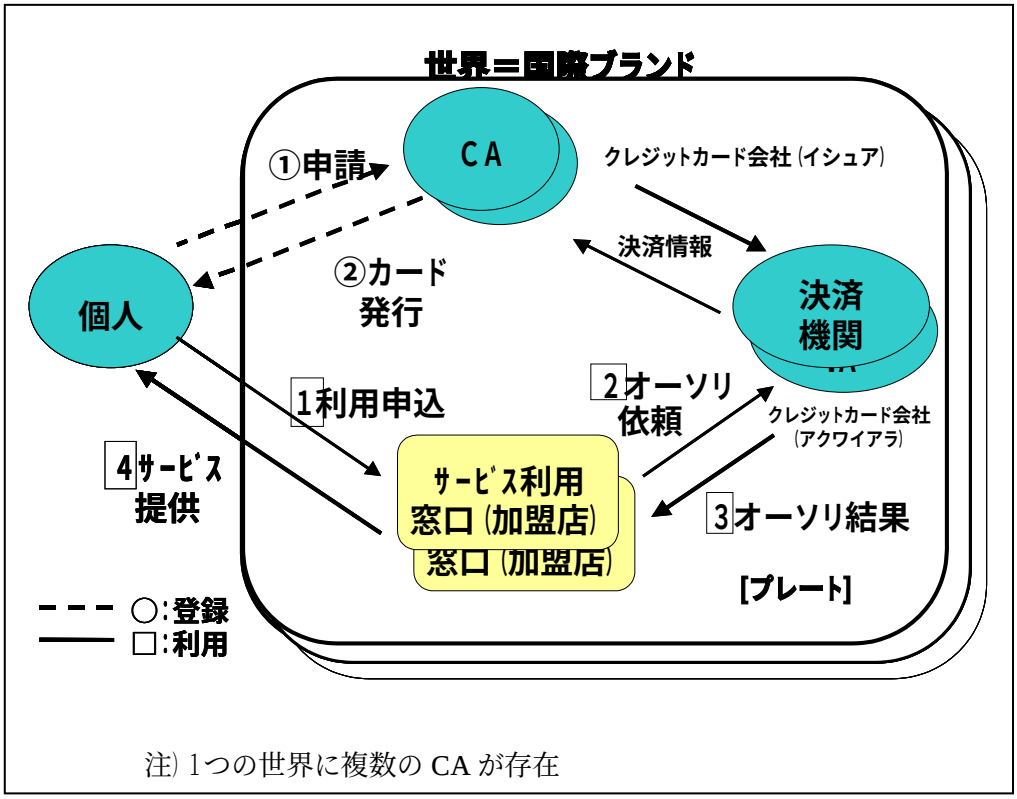


図4-3-1　クレジットカードにおけるマルチ証明書のモデル

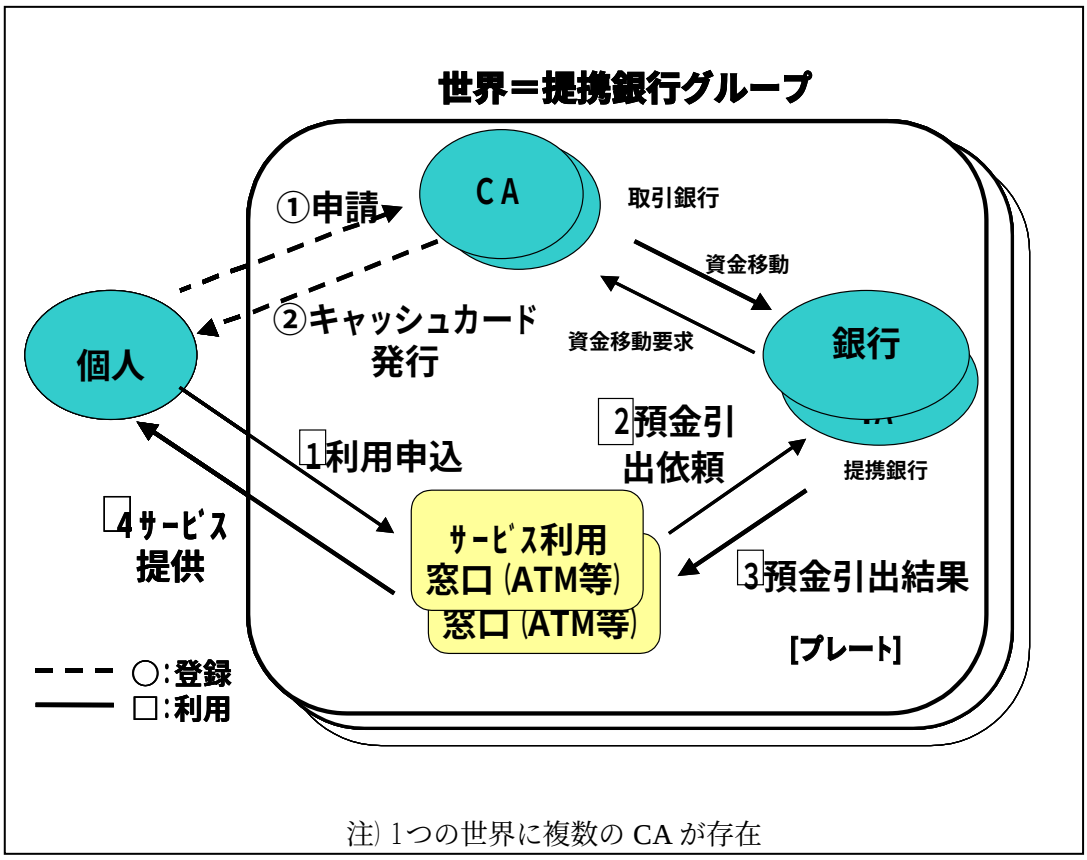
この利用形態では、複数の世界（プレート）が存在するマルチ証明書のモデルであり、例えば１つの世界(図ではプレートに相当)には､同一の国際ブランドが対応してはいるが、異なるサービス事業体（イシュア：カード発行するクレジットカード会社）が本人確認を経た証明書（クレジットカード）を発行する。この証明書は複数のサービス利用窓口（加盟店）で利用できる。加盟店はこの証明書の検証をアクワイアラ（加盟店と契約しているクレジットカード会社）に対して行う。

この形態は、第３章に示すマルチ証明書の世界で、１つのプレートに CA が複数（互いに相互認証された）存在し、かつ、個人は利用するサービス登録窓口ではなく、証明書の発行窓口にのみ登録すればプレート上のサービスを全て受けることができる。これは、マルチ証明書の世界の新しい将来形態とも考えられる。

4.3.3.2　銀行サービス

銀行のキャッシュカードは他の銀行のＡＴＭにおいても自分の口座からの預金引き出しに利用できる。利用者の口座のある銀行のキャッシュカードが、その銀行が提携している他

の銀行で、あたかも利用者の口座との対応を証明してくれているように利用できる。



注）1つの世界に複数の CA が存在

図4-3-2　銀行におけるマルチ証明書のモデル

銀行のモデルは、１つの世界（図ではプレートに相当）に独立した CA が複数存在し、提携関係にある銀行間であれば（手数料の有無の差等はあるが）個人にとっては同一の世界であればサービス窓口への登録することなく、キャッシュカード発行銀行と ATM 設置銀行との間で互いに利用可能としている。マルチ証明書の世界の拡張形であるといえる。

4.3.3.3　マイレージサービス

従来のマイレージサービスは利用者が自社の航空サービス等を受けた場合に利用者にポイントを付与し、利用者が蓄積したポイントに応じて自社の他のサービスを無料もしくは割り引いて提供するものである。近年、マイレージサービスに関する会社間の提携が進み、提携各社のサービスを利用した場合でも、自社の利用者にポイントを付与することとしている。また、クレジットカードと提携した場合、クレジットカードの利用代金に応じて付与された

ポイントをマイレージとして振り替えることもできる。

この形態は、提携各社の集合をドメインとするなかで個別の会社の発行するマイレージカードを利用できるもので、マルチ証明書の世界の拡張形態と考えられる。

（互いに提携関係にある、独立した個別証明書の世界と解釈すると、他社の証明書を認識できているという矛盾が生じる）

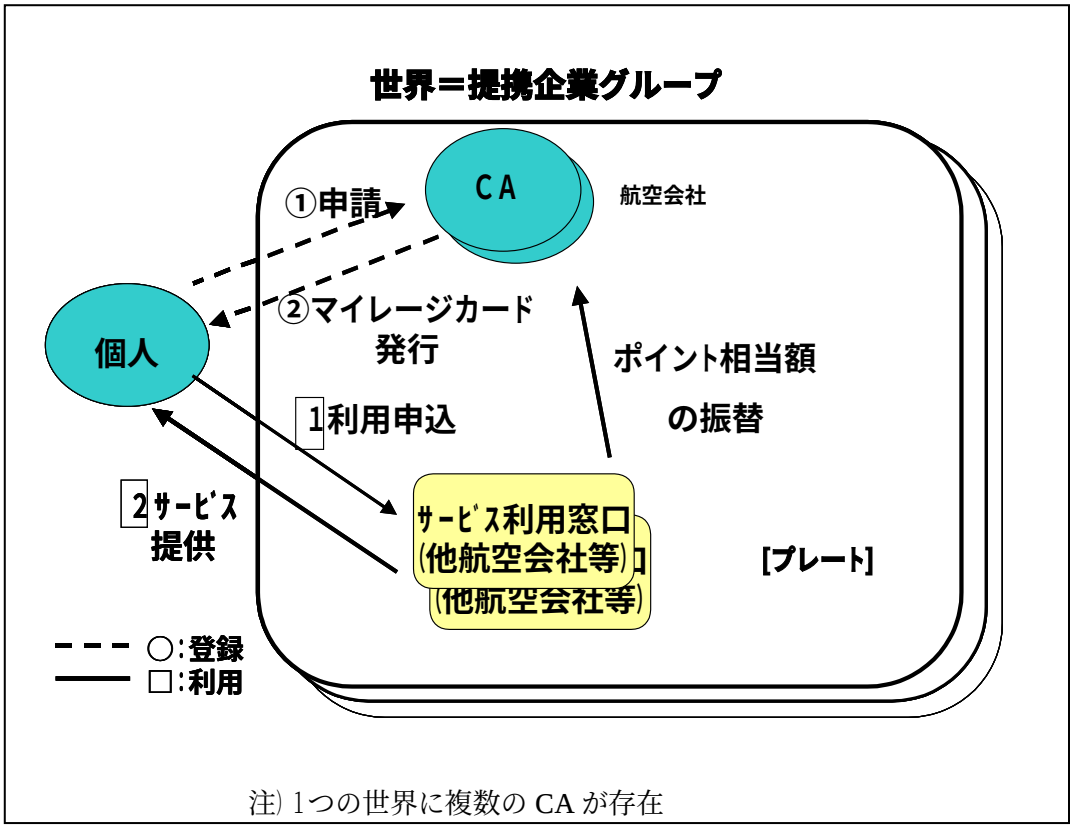


図4-3-3　マイレージにおけるマルチ証明書のモデル

個別証明書の世界のマイレージサービスは、ドメイン内で複数の証明書が互いに利用されるモデルである。これも、将来の証明書の利用形態の動向を示唆するものと考えられる。

4.3.3.4　損害保険

１つの損害保険は、実際には複数の保険会社が引き受けているケースがある。保険は１社で排他的に独占する必要が無く、逆に危険分散のために、この形態が採用されることが多い。保険業法の制限から、割引をする場合には客観的な根拠が必要であるため、将来的には個人、行動を特定して危険率を客観的に算出することも考えられる。

個人特定のための地域共通な地域マルチ証明書、危険率の算出根拠としての職域に固有な職域マルチ証明書など他の業界では見られない利用法が考えられる。

4.3.3.5　会社毎の情報提供（新聞・テレビ）サービス

現状の情報提供サービスは、各社が各サービス毎に個人を特定する証明書（会員番号／パスワードの払い出し等）により、サービス毎の囲い込みを行っている段階にある。このため、情報提供サービスにおける証明書の利用形態は、個別証明書の形態である。

マルチ証明書と比較した、個別証明書に対する要件は次の通り。

[A. 概要／定義]：　CA の数、証明書枚数は会社、サービス毎。

[C. ネット社会での自由度]：　別名を持て、使い分け可能。サービス設計では証明書に AP 用情報が記載されているため、新たな情報の提供は不要。

[D. 運用性]：　取扱いにおける留意点として、厳重な管理に加え、複数管理が必要。

[F. 緊急時対応]：　サービス毎に証明書が異なるため、リスクが分散される。

[G. コスト]：　運用体制は情報提供サービスのポリシー毎に異なる。ネットワークに対する負荷はマルチ証明書と比べて低い。

5　利用形態に対する提言

インターネット社会の発展に伴い、電子認証システムは今後ますます普及していくものと思われるが、本書では「利用者はどのような形で電子証明書を利用するのがよいのか。」について検討してきた。まず、最初に

- 人はどのような形で自己の証明、権限の証明を行っているのだろうか。
- 運転免許証やクレジットカードのように利用場面（サービス）ごとに複数の電子証明書を使いわけるのだろうか。
- 実印と認め印のように電子証明書にもレベル分け、使い分けが必要なのだろうか。

といった論点を整理するなかで、本書のテーマとしては「ＩＤと属性」の分析と、証明書の利用形態については現実に利用する場面（アプリケーション）を想定し、「シングル証明書の世界」、「個別証明書の世界」、「マルチ証明書の世界」の比較を行った。また、本書では全体を通して特に

- 証明書の発行・所持の観点からはどうだろうか。
- 安全など管理上の観点からはどうだろうか。
- 使用する観点からはどうだろうか。

を重点に検討を進めてきた。

最後に、本章では証明書が今後どのように利用されるのかを予測し、またどのように利用されるべきなのかの提言を試みたい。考察にあたり、以下の論点を整理した。

１）ＩＤと属性をいかに組み合わせるべきか。

２）個人のプライバシーが保証されるためにはどのようにすべきか。

３）マルチ証明書の世界を構築するには何をすべきか。

以下、それぞれの論点から証明書の利用形態を予測し、最後に証明書の利用形態に関する今後の課題を考察する。

5.1　ID と属性をいかに組み合わせるべきか

第 2 章で考察したように、ＩＤとは対象者を識別するためのユニークな情報であり、属性とは対象者に与えられた資格や権限、所属等をあらわす情報である。証明書はＩＤ単独で利用することもあればＩＤと属性を組み合わせて利用することもあるが、属性のみで利用することはない。

ＩＤは単一情報とは限らない。例えば、企業の従業員であれば社員番号のみで従業員をユニークに識別できるが、通常、一般個人や企業は氏名、企業名だけではユニークに識別することはできない。このため、住所などその他の情報を付加してユニークに識別できるようＩＤを設定しなければならない。

属性は証明書が利用される世界毎に必要な情報は異なるであろう。企業内の利用ならば従業員の所属や役職、電子入札での利用ならば企業の入札参加資格など様々である。また、一般に属性は度々、変更されることも考慮しなければならない。

証明書の利用にあたっては属性の取扱いは厄介な問題である。属性の変更が証明書の失効を伴うことを考慮すれば認証局の運用やコストの観点からは、なるべく証明書には属性を入れないほうが望ましい。一方、証明書が利用される世界からは、利用目的に応じた属性は証明書に入れたいとのニーズは強い。

ＩＥＴＦではこの問題を解決する方法として、証明書をＩＤ証明書と属性証明書に分け、ペアで利用することを検討している。即ち、利用者は証明書を利用する世界に応じて複数の属性証明書を使い分けることによりＩＤと必要な属性を提示する。

また、属性はサービス提供者がディレクトリなどの属性データベースで提供すべきであり、証明書には入れるべきではないとの意見も強い。

以上から、ＩＤと属性をいかに組み合わせるかの観点では、今後の証明書利用の世界が個別からマルチへ展開することを考慮すれば、少なくとも「ＩＤ＋証明書利用世界で必要最小限の属性」を持つ証明書とするべきであろう。

5.2　個人のプライバシーを保護するためには何をすべきか

証明書のＩＤ、属性には第三者に知られたくない情報がある。紙媒体等の証明書は、通常、本人のみが所有し、本人の意思により利用されるが、電子証明書は電子データとして公開されると、本人の意思にかかわらずＩＤ、属性情報がインターネットを通じて流れる危険性がある。

「マルチ証明書の世界」では複数のサービス提供機関と不特定多数の証明書利用者がいて、悪意の第三者により証明書のＩＤ、属性情報が犯罪等に利用される危険性も高い。

証明書の世界が広がれば広がるほど個人のプライバシーが危険にさらされることを考慮し、認証局は証明書が利用される世界を定義し、例えば目的外使用を禁ずるとかの対策を講じなければならない。また、ＩＤも仮名等を利用するなどの考慮も必要であろう。但し、ＩＤに仮名等を利用する場合でも認証局は、ネット社会での行為の責任を追及する上から、証明書所有者の実名および実存性は確保していなければならない。

5.3　マルチ証明書の世界を構築するには何をすべきか

業界、地域などに展開される「マルチ証明書の世界」には１つの認証局と複数のサービス提供機関が存在する。「マルチ証明書の世界」を構築するには業界、地域毎に認証局の設立が必要である。認証局設立のためには、運営主体と責任を明確にしなければならないので各サービス提供機関のあいだで充分な検討が必要である。また、認証局の運用については発行審査条件の統一および第４章で分析したように各アプリケーション毎の「マルチ証明書の世界」の特質を参考にして検討していく必要がある。これらの検討を進めるにあたっては各業界団体、行政等の公的機関が調整役を果たすことも必要だろう。

「マルチ証明書の世界」の構築には証明書利用の利便性向上や各サービス提供機関個別のメリットに止まらず、業界・地域全体の新たなサービスニーズを掘り起こす可能性を秘めている。業界、地域での積極的な検討をお願いするものである。

5.4　課題

本書では証明書の利用形態について実際の利用場面を想定し、３つの世界の比較を行ったが、マルチ証明書の世界を構築するには利用者、サービス提供者、認証局それぞれの観点から更に検討を深める必要がある。

属性認証については証明書の利用面からみた属性の洗出しと属性の認証責任は誰にあるのか（利用者なのか、サービス提供者なのか、認証局なのか）を検討しなければならない。実際に、電子署名法における特定認証業務では「住所、氏名、生年月日以外の属性情報は電子署名法に係わらない旨を明記しなければならない。」とある。また、ＩＥＴＦが提唱する属性証明書については実際のアプリケーションへの実装が可能なのか技術的な課題とともに利用面の課題も検討しなければならない。

一方、電子署名法の施行とともに、電子証明書の利用目的は電子認証（本人確認またはアクセスコントロール）から電子署名に重点が移りつつある。ビジネス領域においては単独の文書かつ単独の署名で成立する業務はあまりない。多くは単独の文書でも業務プロセス（ワークフロー）に従い複数人の署名（多重署名）が必要であったり、複数の署名文書をとりまとめて成立する業務である。業務によっては開始から完了まで数ヶ月を要するものもあり、当然ながらその間に、ある人の証明書の有効期間が満了したり、証明書が失効した場合、その文書あるいは業務の有効性をどう判断するかという課題がある。また、委任および代理業務における証明書の利用および電子署名の運用ルールについても検討が必要である。

証明書の利用形態については、利用世界の拡大に伴い、今後ますます新たな課題が提起されることが予想される。今後継続的に本テーマを検討することが重要であると認識している。

おわりに

当初、企業内などのクローズドモデルから始まった証明書の利用は、現在、徐々に電子申請、電子入札などのオープンモデルへと拡大している。また、法務省が発行する商業登記認証局や総務省が検討している公的個人認証など公的証明書の普及も始まろうとしている。電子署名法では電子署名の法的効果（推定効）を明らかにするとともに、民間認証局および民間認証事業者については、厳密な本人確認を行いセキュアな認証設備を有する認証業務については特定認証業務の認定制度を制定し、一般の認証業務と区別できるようにした。

当面、これらさまざまな認証局から発行される証明書は、サービス提供機関毎の「個別証明書の世界」での利用を経て業界、地域などで共通に利用される「マルチ証明書の世界」へと発展していくであろう。更に将来の姿としては、これら複数の「マルチ証明書の世界」がブリッジ認証局による相互認証で緩やかな認証ドメインを形成していくことも予測される。

また、公的証明書は政府・自治体への電子申請など、本来の利用目的のほかに、リアルな世界では、運転免許証などを本人確認の手段として民間の各種証明書、会員カード等が発行されているように、民間認証業務では本人（法人）確認の手段として住民票（商業登記簿謄本）などのかわりに利用することも検討されるであろう。

証明書の利用が普及するには利便性の向上が最大の課題である。本書では証明書利用形態の観点から利用者の利便性向上のためには、「個別証明書の世界」から「マルチ証明書の世界」への移行が重要であるとした。「マルチ証明書の世界」を目指す業界および関係各位に本書が参考になれば幸いである。

付録

付録. 1 用語集

1. ＣＲＬ（Certificate Revocation List）
   証明書失効リスト。認証局が発行するデータで、有効期限内に失効された証明書のシリアル番号の一覧が記載されている。ＣＲＬは、認証局の電子署名によって改ざんできない形式となっている。
2. ＯＣＳＰ（Online Certificate Status Protocol）
   検証局等に対して、証明書が失効されているかどうかという確認をオンラインで問い合わせるためのプロトコル。
3. ＰＫＩ（Public Key Infrastructure）
   公開鍵暗号を利用して各種情報通信システムの安全性を確保するための一連の技術およびサービス。
4. 改ざん(改竄)
   データを自分の都合のいいように改変する不正行為。
5. 鍵ペア
   公開鍵暗号方式で利用する組となる二つの鍵。公開鍵と秘密鍵とからなる。
6. 危殆化
   秘密鍵等の秘密情報が盗難、漏洩、解読などといった様々な原因によって、その機密性を失うこと（失ったものと想定されること）。
7. 検証局
   証明書が失効されているかどうかという検証者からの問い合わせを受け付け、応答する機関。ＶＡ（Validation Authority）やＯＣＳＰ Responder とも呼ぶ。
8. 検証者
   署名検証を行う人。
9. 公開鍵
   公開鍵暗号方式で利用する鍵ペアのうち、広く一般に開示する鍵。検証者が署名検証を行う際に使用する。
10. 公開鍵暗号方式

電子文書を暗号化する際に使用する鍵と、暗号文を復号する際に使用する鍵とが異なる暗号方式。公開鍵暗号方式には、どちらか一方の鍵からもう一方の鍵を算出することが非常に困難であるという性質と、二つの鍵は１対１対応であって、どちらか一方の鍵で暗号化したデータはもう一方の鍵でのみ復号可能であるという性質とがある。公開鍵暗号方式は、電子署名を実現する手段として利用される。

11. 証明書

公開鍵とその所有者（署名者、または認証局）とを対応付けるために、認証局が生成する電子データ。認証書、電子証明書、あるいは公開鍵証明書などとも呼ぶ。証明書は、認証局の電子署名によって改ざんできない形式となっており、所有者の名前や公開鍵の値だけでなく、発行した認証局の名前や有効期限や利用目的などといった情報も含まれている。市区町村役場や登記所で発行される印鑑証明書に相当する。

12. 証明書の失効

秘密鍵の危殆化等のため、有効期間内の証明書の効力を失わせる行為。証明書の所有者（署名者、または認証局）の指示に基づいて行われる。

13. 証明書の有効性確認

検証者が、署名検証に使用する証明書が失効されていないかを確認する行為。確認の方法として、ＣＲＬに記載されているかどうか調べる方法や、検証局にＯＣＳＰでオンライン問い合わせをする方法などがある。

14. 署名検証

署名付き電子文書を、署名者証明書に含まれる署名者の公開鍵を用いて復号することにより、当該電子署名の正当性（署名者によって生成された電子署名であることや、署名付き電子文書が改ざんされていないこと）を検証する行為。紙の文書に付された印影を印鑑証明書等に記された正しい印影を用いて照合する場合に相当する。

15. 署名者

署名生成を行う人。

16. 耐タンパ性

装置を分解するなどして、中にある秘密情報等を不正に入手しようとする行為（Tamper）に対する耐性。

17. 電子署名

署名対象となる電子文書、あるいはそのハッシュ値を秘密鍵で暗号化したもの。一般には、タブレット等によって入力された手書きサインも含めて電子署名と呼び、前記秘密鍵で暗号化したものをディジタル署名と呼びわける場合もあるが、本書では、公開鍵暗号方式に基づいて生成されたものだけを電子署名、あるいは単に署名と呼んでいる。

18. 電子署名法

平成１３年４月より施行される「電子署名および認証業務に関する法律（平成 12 年 5 月 31 日法律第 102 号）」の略称。電子署名に対して印鑑と同等の推定効を与えている法律。

19. 電子認証システム

電子署名を用いて、通信相手の確認や通信メッセージの改ざんチェックなどを行うシステム、および証明書の発行など、電子署名を正しく利用するために必要な処理を行うシステム。なりすましや改ざん、否認などといった不正を防ぐ目的で用いられる。

20. なりすまし

他者のふりをする不正行為。

21. 認証局

公開鍵とその所有者とを対応付けるために、署名者または他の認証局に対して証明書を発行する機関。ＣＡ（Certification Authority）とも呼ぶ。また、自己の証明書を自分自身で発行する認証局をルート認証局とも呼ぶ。

22. 認証局運用規定

証明書ポリシーに基づいて、認証の実施における手続きや遵守事項等を文書化したもの。ＣＰＳ（Certification Practice Statement）とも呼ぶ。一般に、利用者等に対して開示される。

23. 認証情報

ある利用者を他の利用者と区別するために用いられる情報。パスワードや生体情報等。

24. 否認

取引などを行った後に、当該取引に関与したことそのものを否定する不正行為。事後否認とも呼ぶ。

25. 秘密鍵

公開鍵暗号方式で利用する鍵ペアのうち、署名者自身が秘密に保持する鍵。署名生成時に使用する。

26. 本人確認（**Identification & Authentication**）

個人、法人､装置等の認証対象者に関する情報が真正であることを審査する行為。

27. リポジトリ

証明書やＣＲＬ等を保管しておき、利用者からの要求に応じてそれら情報を配布する仕組み。

28. 利用者

電子署名技術を利用する人。署名者と検証者に区分される。

付録. 2 参考文献

1. 小松文子他、PKI ハンドブック、ソフト・リサーチ・センター, 2000.11

2.「法務省法人代表者証明書の利用に関するガイドライン」

3. http://www.bolero.net/japan/

メンバーリスト

事務局

前田　陽二	電子商取引推進協議会（ECOM）	主席研究員
米倉　早織	電子商取引推進協議会（ECOM）	主席研究員
紙田　政典	電子商取引推進協議会（ECOM）	主席研究員

顧問

菅　　知之	関西大学　教授
平田　健治	大阪大学　大学院　教授

TF４メンバー（編集メンバー）

役割	氏名	会社名
	東山　栄一	NEC ソフト株式会社
	武藤　裕	NTT コミュニケーションズ株式会社
	関　　信雄	NTT コムウェア株式会社
	小熊　慶一郎	株式会社ＮＴＴデータ
	高村　昌興	株式会社 NTT データ
	石井　正光	共同印刷株式会社
	宮嵜　善史	国内信販株式会社
	高岸　辰哉	株式会社第一勧業銀行
	石井　範康	日本信販株式会社
	今仲　江美	日本電気株式会社
	村田　祐一	日本電信電話株式会社
	春田　克治	日本認証サービス株式会社
	相原　敬雄	日本ベリサイン株式会社
	立川　雅章	三井住友海上火災保険株式会社
リーダ	千葉　寛之	株式会社日立製作所
リーダ	田中　稔	三菱電機ｲﾝﾌｫﾒｰｼｮﾝｼｽﾃﾑｽﾞ株式会社

SWG２メンバー（上記を除く）

氏名	会社名
森田　純生	株式会社イーアイティー
熊木　克巳	株式会社エヌジェーケー
河田　悦生	NTT ドコモ株式会社
関野　公彦	NTT ドコモ株式会社
島田　晃	株式会社 NTT データ
後藤　啓一	株式会社 NTT データ
高村　昌興	株式会社 NTT データ
長谷川　亮	株式会社ｵﾘｴﾝﾄｺｰﾎﾟﾚｰｼｮﾝ
保倉　豊	グローバルフレンドシップ株式会社
久保田　信也	KDDI 株式会社
鈴木　良信	コンピュータ・アソシエイツ株式会社
森　　宣彦	コンピュータ・アソシエイツ株式会社
大西　雅春	佐川急便株式会社
吉岡　賢宏	佐川急便株式会社
安江　洋	株式会社 UFJ 銀行
藤本　正代	三井住友海上火災保険株式会社
三原　裕ニ	社団法人　日本鉄鋼連盟
松山　科子	ソニー株式会社
渡辺　秀明	ソニー株式会社
小林　由幸	株式会社第一勧業銀行
星野　理	株式会社帝国データバンク
長嶋　潔	東京海上火災保険株式会社
吉野　貴男	東京海上火災保険株式会社
中原　康	株式会社東芝
北折　昌司	株式会社東芝
佐々木　哲治	株式会社テプコシステムズ

岩渕　充	東北電力株式会社
長谷　容子	日本アイ・ビー・エム株式会社
松本　恵	日本アビオニクス株式会社
織　　晃一郎	社団法人日本航空宇宙工業会
石田　正夫	日本コムシス株式会社
角田　紳吾	日本ボルチモアテクノロジーズ株式会社
古寺　薫	日本ユニシス株式会社
原田　素子	東日本電信電話株式会社
板垣　敬介	日立キャピタル株式会社
久米本　文哉	株式会社日立情報システムズ
永倉　俊	富士通株式会社
石丸　誠孝	富士通株式会社
大竹　範明	富士電機株式会社
高田　修一	ﾏｲｸﾛｿﾌﾄ　ﾌﾟﾛﾀﾞｸﾄ　ﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ　ﾘﾐﾃｯﾄﾞ
青木　尚	三菱電機株式会社
三沢　康行	安田火災海上保険株式会社

平成１４年３月発行
発行：電子商取引推進協議会
東京都港区芝公園３－５－８
機械振興会館 3 階
Tel　　03-3436-7500
E-mail　info@ecom.or.jp