経済産業省委託調査

平成１５年度ＥＣ技術基盤の相互運用性に関する調査研究事業

（取引相手先の属性認証技術等の調査）

証明書利用ガイドライン

―属性情報の活用―

平成16年３月

電子商取引推進協議会

財団法人日本情報処理開発協会
電子商取引推進センター

この報告書は、平成１５年度受託事業として（財）日本情報処理開発協会電子商取引推進センターが経済産業省から委託を受けて、電子商取引推進協議会（ECOM）の協力を得て実施した「平成１５年度ＥＣ技術基盤の相互運用性に関する調査研究事業（取引相手先の属性認証技術等の調査）」の成果を取りまとめたものです。

序文

本ガイドラインは、電子認証における資格や権限の情報として利用される属性情報について、実社会での利用場面の分析や利用者からの要求要件整理を行い、その結果に基づきサービスを提供する側からの属性情報を活用するための指針をガイドラインとしてまとめたものである。

すでに、公開鍵証明書を用いることによりインターネット上で本人確認を行う仕組みができている。しかしながら、公開鍵証明書により本人性は証明されるものの、その本人の資格や権限の情報については統一的な記述方法はなく、多くの場合公開鍵証明書の拡張領域に利用するサービス毎にそれぞれの形式で属性情報を記述する方法が取られ、相互運用性が課題として残った。

この属性情報の利用に関して、公開鍵証明書とは別に属性証明書を発行する方法、信頼性の高いデータベースに属性情報を登録管理し公開鍵証明書にリンクさせておくことにより属性情報を取り出す方法などが検討されている。

このガイドラインは、属性情報の特性、実現方式の特長、利用者からの要求などの情報を総合的に検討して、属性情報を活用するモデルシステムの構築を提案する。

本報告書が、電子署名の利用を検討している企業、機関の方々にとって一助になることができれば幸いである。

平成 16 年 3 月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

目次

序文

まえがき

利用者がインターネット経由のサービス（特に有償サービス）を受けようとした場合、通信の秘匿と利用者権利の保証のために、PKI を利用した証明書による認証と暗号化を適用することが望まれる。しかしながら、証明書の発行手続きや、サービス利用手続きにおいては、サービス提供者から各種の個人情報等、属性情報の提示を求められている現実がある。

そこで、ネットワークを介して展開されているサービスを利用するにあたっての証明書利用の意義と個人情報提示における留意点をベースに、利用者に向けて証明書利用の有効活用を促進するためのガイドラインを提示する。

このガイドラインを作成するにあたり，以下を前提とする。

インターネットを利用したサービスは次々と新たな形態で現れており、利用者も増加の一途をたどっている。しかしながら一方ではクレジットカード番号の漏洩や、なりすましによる詐欺被害といった問題が継続的に発生しており、注意深い利用者を魅力的なサービスから遠ざける結果を招いている。飛躍的に拡大するネットワークの伝送容量という資源を有効に活用し経済の発展を図るためには、全ての利用者が少しの注意をすることで安心して多岐にわたるサービスを利用できる環境が整わなくてはならない。まずは利用者の負うリスクを許容範囲内に納めるための課題について考えてみる。

ネットワークを介した取引や情報交換における大きな課題は、通信相手の確認と通信経路の安全確保にある。現在、秘密鍵＋証明書を用いた暗号技術、署名技術を適用することにより、これらの課題にはひとつの回答が提示されている。

(1) 通信相手の確認に必要なこと

通信相手を確認するということは、通信相手のみが持つ情報を提示させることによって相手を認めることが一般的であり、パスワードもこの道具のひとつである。しかしながら、パスワードは他者に察知されたり予測されたりすることによってなりすましを許す可能性が高く、高度な情報を含む通信相手の確認手段としてはリスクが高いと言わざるを得ない。そこで秘密鍵と証明書を用いた方式が採用されている。通信相手間で通信に先立って証明書の交換を行っておき、お互い相手の証明書から取り出した公開鍵で電文を暗号化して送り出すため、相手が正しい秘密鍵を保有していれば電文を復号し相互の会話が成り立つことになる。

したがって、秘密鍵を持っていない限りなりすますことができないため、秘密鍵が利用者によってしっかりと管理されている限り、その安全性はパスワードを利用する場合に比較して、非常に高いものとなる。

(2) 通信内容の保証に必要なこと

通信内容の安全性を確保するということは、通信内容が第三者から参照できないこと、通信内容を第三者が改ざんできないこと、あるいは改ざんされたことがわかることにある。

このためにも秘密鍵＋証明書を用いることができる。

通信内容を第三者の参照から守るため、まず第三者からの参照を防ぐために通信内容を暗号化して送付する（実際には通信内容は共通鍵暗号方式で暗号化し、そのキーを相手の証明書を使って暗号化し相手に送り届ける）。

相手側では自分の秘密鍵を用いて通信内容を復号し利用することが可能となる（実際は自分の秘密鍵によって共通鍵暗号方式の鍵を復号し、この鍵によって通信内容を復号する）。

通信内容の改ざんを察知ためには、秘密鍵＋証明書で電子署名を利用することができる。送信側では、通信内容を決められたルールに沿って小さなビット列に変換し、このビット列を秘密鍵を用いて暗号化し通信内容に付加する。受信側では、通信内容に付加された情報を通信相手の証明書を用いて復号し、通信内容を決められたルールに沿ってビット列に変換したものと比較する。これが一致していれば通信内容は改ざんされていないと判断することができる。

上記の暗号、電子署名といった技術の複合的な利用で通信内容の保証が実現できる。

(3) 証明書利用の留意点

ショッピング Web サイトや、会員対応サービス Web サイトでは、SSL という通信プロトコルを利用してエンドエンティティとの秘匿通信を容易に実現しているが、多くの場合、Web サーバーのもつ秘密鍵と証明書のみを用いることにより、エンドエンティティとの間で暗号鍵を交換している。

しかしながら、この場合エンドエンティティを証明するものは、エンドエンティティの識別番号（会員番号）とパスワードというのが一般的であり、なりすましの危険性は高いと言わざるを得ない。

そこで利用者を特定し安全な通信を実現するために、利用者のもつ秘密鍵とサービス提供者が認識できる証明書を用いることで利用者認証を実現する。利用者は自分の秘密鍵を厳密に管理することで、なりすまされる危険を回避することができる。

よって心配事は秘密鍵の厳密な管理ということになるが、秘密鍵の保管方法には以下のような形態がある。

・コピー可能媒体での保管と利用
・PC の HDD 内での保管と利用
・IC カード等コピー不可能媒体での保管と利用

利用者の利便性と安全性を考慮した場合、3 点目の IC カード等コピー不可能媒体での保管と利用を推奨する。特に物理的媒体の利用は紛失・盗難が認識し易いため有効である。なお、いずれの場合にも秘密鍵の利用に際してはアクセスを制限するためのパスワードを知っていることが必要である。秘密鍵の安全性確保は全ての出発点であることを忘れてはならない。

(4) 証明書利用の準備

証明書という名称のみが先行してしまいがちなため、利用者として証明書を利用するためには何が必要であるかを確認する。なお下記の準備作業については、一般的にサービス提供者側から詳細な手順書が配布され、利用者はそれぞれのステップを容易に実行することができる。

① 鍵の生成

秘密鍵と公開鍵のペアを生成し、秘密鍵は厳重に保管する。

② 証明書の発行依頼

公開鍵と利用者を特定するための属性情報を安全な経路で認証局へ送付し、認証局の秘密鍵を用いた署名により、証明書の生成を依頼する。

③　証明書の受け取り

生成済みの証明書を受け取ると共に、サービスドメインで認識されている領域へ証明書を登録する。

本来、上記のような準備手順がとられるが、利用者の準備手続き負担を極力削減するために、秘密鍵と公開鍵のペア生成と証明書発行をサービス提供者が代行するケースが増えている。この場合には、サービス利用申し込みの後、サービス提供者から秘密鍵と証明書が安全なルートによって送付されてくる。しかしこの場合、サービス提供者が利用者の秘密鍵を知り得るわけで、サービス提供者の評価をきちんとしておく必要がある。また、秘密鍵は IC カード等複写のできない媒体を用いて配送される場合を除いて警戒を要することになる。

第 1 章「証明書利用形態概論」では、このガイドラインを作成するにあたり、基礎となる項目に関する調査検討結果を整理し紹介する。

すなわち、証明書利用形態についての考察、属性情報の分類・分析、属性情報を活用する場合に考えられるシステム形態、等について解説する。

第 2 章「証明書利用における要件ガイドライン」では、利用者側からの電子証明書を利用するにあたっての留意事項、すなわちサービス提供者に対して要求すべき要件について述べる。

第 3 章「サービス提供者から見た属性情報活用ガイドライン」では、1 章と 2 章の検討結果に基づき、属性情報を活用するシステムを 8 つのモデルに集約し、そのモデルを選択し活用するためのガイドラインを提案する。

第 4 章「今後の展望」において、このガイドラインの活用に向けた展望を述べる。

1．証明書利用形態概論

1.1　証明書の種別と利用モデル

1.1.1　目的

（1）検討の目的

インターネットでの電子商取引においては、リアルでの商取引と異なり、相手の顔が見えないという特徴がある。この中で、正当な相手との取引であることを確認するために電子認証システムを利用する場合がある。この場合、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、認証、認可の関係等の取り決めが必要となる。また、この取り決めの結果、電子認証システムでの本人確認の結果、発行される電子証明書については、信頼性が高く、利用しやすい利用形態の検討が必要と思われる。

電子証明書は、発行機関による本人確認の結果、電子認証システムを通じて電子証明書利用者に対して発行される。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毎に発行されている例が多い。今後想定される証明書を利用したサービスに対して、サービス毎に異なる証明書を個別に取得するのは電子証明書の管理を含めた利用者から見た利便性､効率性に課題もしくは問題が発生する可能性が予想される｡これらの解決方法の一つとして、サービスを提供する業界等で共通（複数サービスで利用できる）で１枚の電子証明書を発行する形態や、運転免許証、パスポートなど一人に一枚のみ発行され、公的な身分証明書として利用されているものに相当する電子証明書を発行する形態等が想定される。

本章では、電子認証システムから発行される電子証明書の利用形態について、社会インフラとして広く普及させる観点から見た場合に、個別のサービス毎に発行されている「単一目的証明書（Single Purpose Certificates）」､一人に１枚の「汎用目的証明書（Universal Certificates）」、サービス業界など複数サービス毎に１枚の「特定目的証明書（Specific Purpose Certificates）」を想定し、その利用形態を検討した。想定した３種類の電子証明書について、その発行形態、利用形態毎の有効性、効率性等から、信頼性の高い電子認証の実現に向けた電子証明書の利用にあたっての課題・特性等を抽出分析し、各電子証明書の適用分野について検討の結果を記述した。

（2）検討の背景

電子証明書の利用形態を検討する背景として、次のものがある。対象者をある情報を用いて識別する ID 認証と ID に付与された属性情報による認可との関連についての検討と効率的な電子証明書の利用方式をまとめた。この中で、電子証明書の利用形態のビジネスモデルを明確化し、各電子証明書の利用形態として「汎用目的証明書の世界」､「単一目的証明書の世界」、および「特定目的証明書の世界」の３つを提案し、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なうこととなった。以下にその概要を記述する。

ID 認証と認可についての検討結果の概要を示す。

認証（authentication）とは、「対象物が本物（本人）であることを確認する」ことを意味する。対象者が自然人である場合には本人の実在性と、対象者が本人であることの本人性の確認とを組み合わせて本人認証という場合がある。

認証の結果は権限の確認に利用される場合がある。この、対象者に権限を与えることを認可（authorization）と呼ぶ。認証と認可とは異なる行為である。

ID 認証、認可のリアル世界における例として次のようなものがある。

個人を特定する情報として、戸籍に記載されている情報あるいは住民票に記載されている情報等があげられる。具体的には、住所、氏名、生年月日、性別、本籍などの組み合わせがある。これらを元に作られた ID としては運転免許証、パスポート、社員証などがある。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、発行者情報等が挙げられる。

ID 認証、認可のネット社会における例として次のようなものがある。

ID として、利用者の持つ秘密鍵に対応する公開鍵を含む電子証明書がある。属性情報としては、発行者情報、利用者情報、有効期限などがある。

電子証明書の利用形態を検討するにあたって３つの利用形態（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からの調査・分析を行った。

汎用目的証明書の世界として、一人に１枚だけ発行され、社会全体でその電子証明書が通用する世界を想定した。ここでの電子証明書は、この世界の中で個人をユニークに特定できる。単一目的証明書の世界として、各発行機関（サービス提供会社）が個人に対して１枚しか発行しないが、利用者１人には同種の電子証明書が複数枚発行される。サービスを受けるときは利用者がサービス提供会社ごとに電子証明書を使い分ける。この電子証明書は利用するサービス毎にユニークに利用者を特定できる。特定目的証明書の世界は、一人に複数枚の電子証明書が発行されるが、それぞれの電子証明書が通用する領域が異なる世界で、一枚の電子証明書で複数のサービスが利用できる。この電子証明書は、閉じた世界（国、地域、業界等特定な世界）の中で、個人をユニークに特定できる。

次に、これらの電子証明書の利用形態についての検討結果を示す。

1.1.2 電子証明書利用形態における３つの世界

リアル社会ではさまざまな 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）を個人で使い分けている。しかしながら、ネット社会において、リアル社会の証明書に利用形態を単純に移行しただけの形態で ID を持ち込んでも個人の認証には使えない場合がある。リアル社会の証明書は証明書のデザイン、形状など多種多様であるが、ネット社会の電子証明書は単なるデジタルデータであることも理由の一つである。

ここでは、電子証明書の統合がなされた汎用目的証明書の世界、リアル社会がそのままネット社会に移行した世界（単一目的証明書の世界）を考え、これらの中間を模索した世界（特定目的証明書の世界）を示す。これら３つの世界の具体例を次章以降で示す。

（１）汎用目的証明書の世界

汎用目的証明書は、「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電子証明書」と定義できる。この電子証明書は、住民票等に準じた個人一人一人に発行される公的な電子証明書である。この電子証明書には、個人をユニークに特定するための ID と住所、氏名、生年月日、性別など、通常身分証明に必要な属性情報のみが記載される。また、厳密な本人確認（実在性、本人性確認）および属性を公的審査し、この結果に基づき証明するものとなる。

汎用目的証明書のモデルを図 1-1 に示す。

汎用目的証明書が１枚あれば、利用したいすべてのサービスの利用・登録が可能となり、ネット社会でのオールマイティの身分証明書として使用できる。各個人は汎用目的証明書１枚のみを保有する。

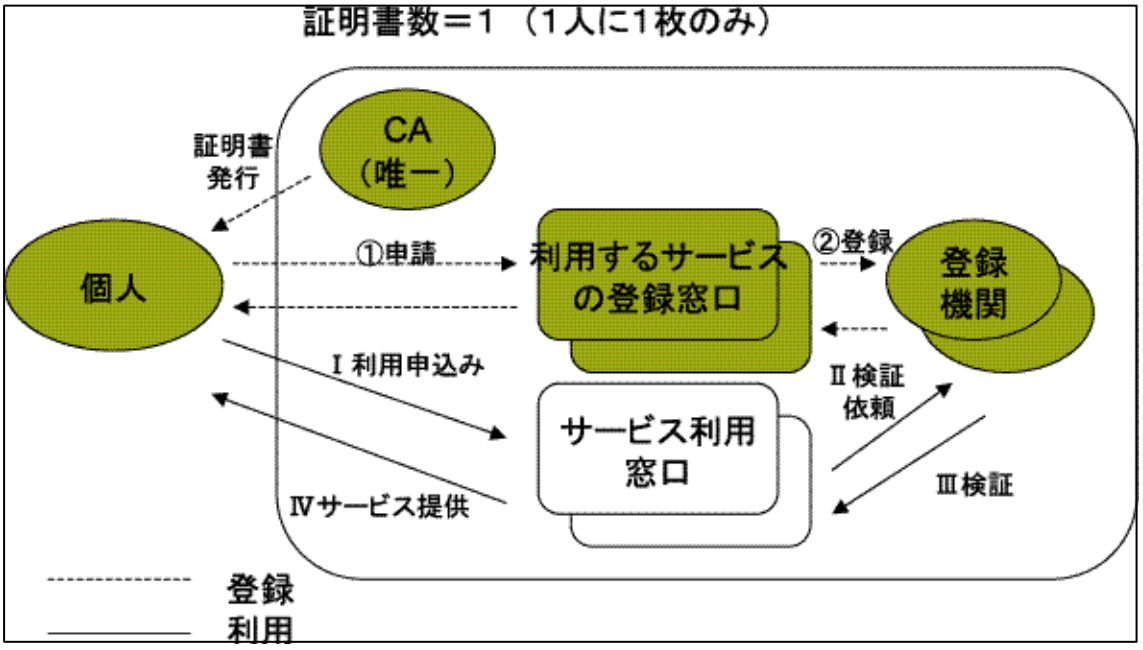


図 1-1 汎用目的証明書の世界

汎用目的証明書のモデルの前提は次のとおり。

個人に対して汎用目的証明書が１枚発行される。利用するサービス毎にサービス利用登録する窓口（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有効性確認を受け付ける機関（以下、登録機関）が存在する。

サービス利用前に、各個人のサービスへの登録が必要となる。汎用目的証明書には基本的な属性しか記載されていないために、基本的な属性以外の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汎用目的証明書を提示し、本人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汎用目的証明書とその他属性情報を登録機関に登録する。

サービス利用は次のフローとなる。

Ⅰ 個人は汎用目的証明書をサービス利用窓口に提示する。

Ⅱ サービス利用窓口は提示された汎用目的証明書が有効かどうかを登録機関に有効性確認を行う。

Ⅲ 登録機関において有効性が確認され、その確認結果とその他属性情報が応答される。

Ⅳ 有効性確認結果に基づきサービスが提供される。

（2）単一目的証明書の世界

単一目的証明書は、「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を含む電子証明書」と定義できる。

特徴として、個人がサービス・アプリケーション毎に申請登録し、複数の電子証明書を保有する。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できる。

電子証明書への記載事項としては、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のみを持つ。

発行審査はサービス・アプリケーション毎に異なる。決済行為など、本人性確認の厳密性を要求されるものから、チケット購入のような緩やかな本人性確認で、ニックネームを許容する、ものまで様々ある。

単一目的証明書のモデルを図1-2に示す。

現実のレンタルショップの会員証などをネット社会に置き換えた世界である。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が高いモデルである。

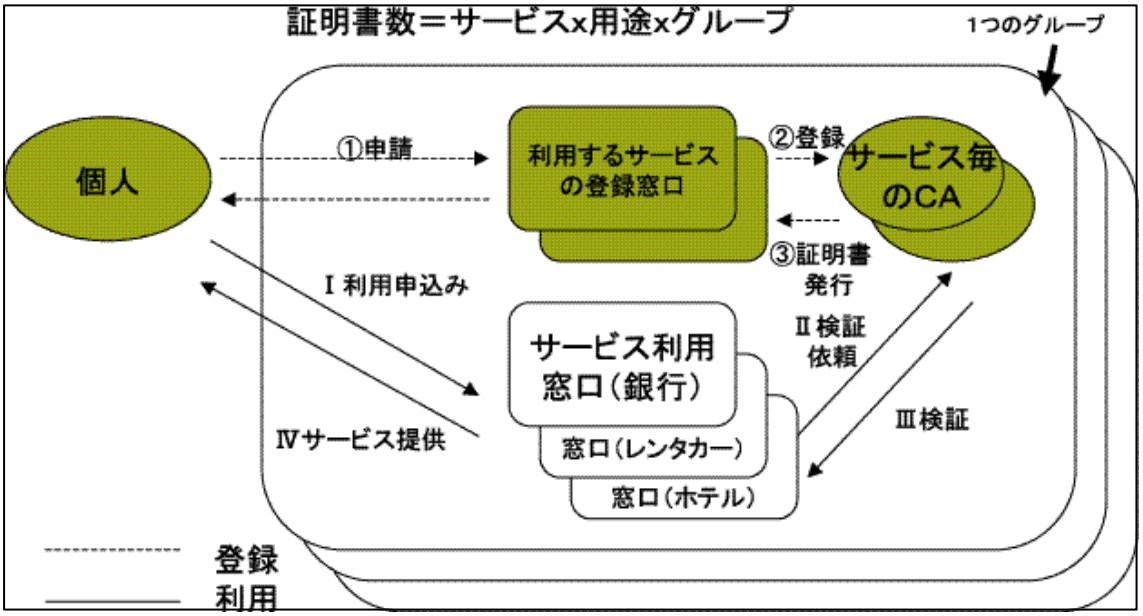


図 1-2 単一目的証明書の世界

単一目的証明書のモデルの前提を示す。

個人には単一目的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と登録をする窓口（以下、サービス登録窓口）とサービスの提供を受ける窓口（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有効性確認を受け付ける認証機関（以下、サービス毎の CA）が存在する。

サービスへの登録について次に示す。

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窓口に申請を行う。

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

③ サービス毎の CA は単一目的証明書の発行をサービス登録窓口経由で行う。

サービスの利用のフローは、以下のようになる。

Ⅰ 個人は単一目的証明書をサービス利用窓口に提示する。

Ⅱ サービス利用窓口は提示された単一目的証明書が有効であるかサービス毎の CA に有効性確認を行う。

Ⅲ サービス毎の CA にて有効性確認され、確認結果とその他属性情報が応答される。

Ⅳ 有効性確認結果に基づきサービスが提供される。

（3）特定目的証明書の世界

特定目的証明書は、「閉じた世界（国、地域、業界、或いは個人が決めた特定の世界などでも可能）の中で、ユニークに個人を特定できる ID を含む電子証明書」と定義できる。

特徴として、特定目的証明書があれば、その閉じた世界で利用するすべてのサービスの利用・

登録が可能である。電子証明書に記載される事項としては、基本的にはサービス・アプリケーション毎にユニーク性を確保するための ID のみ記述される。発行審査として、トレーサビリティを確保するための厳密な本人確認が必要となる。電子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を求められる。

特定目的証明書世界のモデルを図 1-3 に示す。

特定目的証明書は、汎用目的証明書の世界と単一目的証明書の世界の中間解である。利用者は、行政・業界（マーケットプレイス等）毎に発行された電子証明書を何枚かを使い分ける。

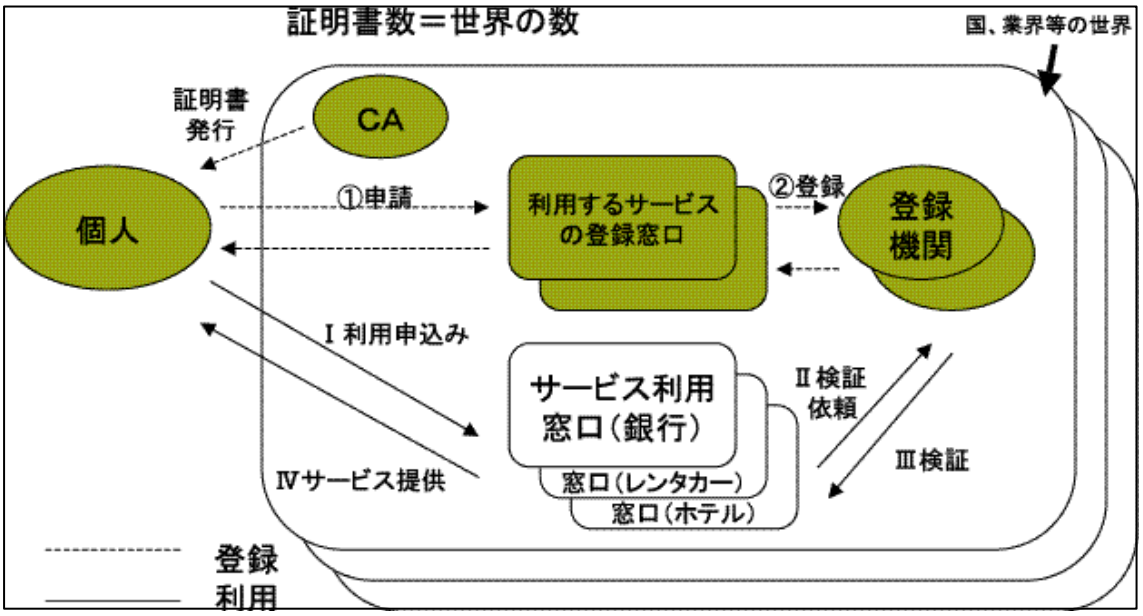


図 1-3 特定目的証明書の世界

特定目的証明書のモデルの前提を下記に示す。

個人には特定目的証明書が複数枚発行される。特定目的証明書の発行は、行政・業界毎に設立している認証局などから発行されることが多い。

利用され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）とがあり、リポジトリへの登録およびサービスからの有効性確認を受け付ける登録機関が存在する。

サービス利用の登録は、下記のフローとなる。

① 個人は利用するサービス登録窓口に特定目的証明書を提示し、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特定目的証明書とその他属性情報を登録機関に登録する。

サービス利用の際のフローは下記のとおり。

Ⅰ 個人は特定目的証明書をサービス利用窓口に提示する。

Ⅱ　サービス利用窓口は提示された特定目的証明書が登録されているか登録機関に有効性確認を行う。

Ⅲ　登録機関にて確認され、確認結果とその他属性情報が応答される。

Ⅳ　確認結果に基づきサービスが提供される。

1.1.3　利用モデル

近年、電子認証局の設置が進んでいる。認定認証局など法律に基づき認定されているものがあるが、主なものとして、次のようなものがある。

商業登記法などに基づく「商業登記に基づく電子認証制度」は、商業登記された会社の代表者に対して会社名を記載した電子証明書を発行する。地方自治体などの入札などに利用されている。

総務省の公的個人認証サービスは、住民基本台帳カードなどを媒体として住民票に記載される住所、氏名、生年月日、性別を都道府県知事が証明する電子証明書を発行するサービスである。個人のパスポート申請、税金の申告など、多種多様な申請、申告をインターネット経由で行う場合に利用される予定である。

利用モデルとして、リアル社会において実現しているサービスを、各種電子証明書を利用して実現できたものと仮定してモデル化した結果を示す。

リアル社会において実現されている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単一目的証明書と、また、企業グループや業界等の単位で提供されるサービスを特定目的証明書に対応させて検討した。サービスの流れとしては、当初、単一目的証明書にて提供し、提携などにより、特定目的証明書に移行しているが、実際には先に示した特定目的証明書のモデルを一部変形した形態となっている例がある。これらの例は、電子証明書の将来の利用形態についての示唆を与えるものと考えられる。

（1）クレジットカードサービス

クレジットカードには一般に、カード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締結しなくとも、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、特定の百貨店など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あるが、これは、個々の百貨店のサービスに閉じる単一目的証明書の世界から、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特定目的証明書の世界へ展開された例と言える。

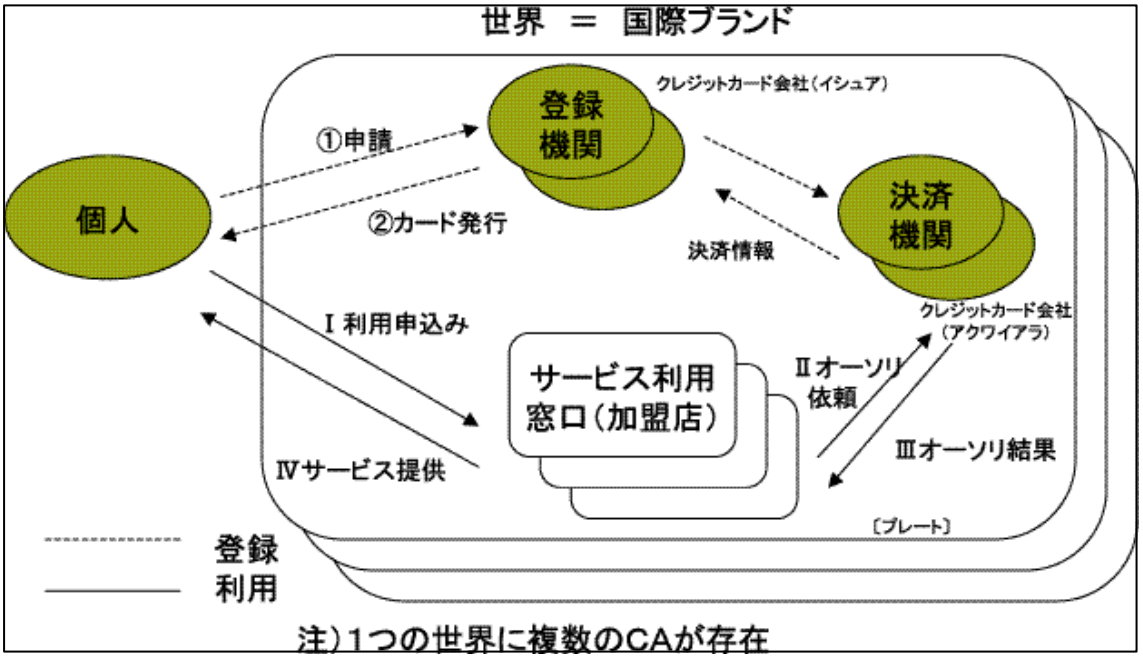


図 1-4 クレジットカードにおける特定目的証明書のモデル

この利用形態では、複数の世界（プレート）が存在する特定目的証明書の例であり、例えば一つの世界（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いるが、異なるサービス事業体（イシュア：カードを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。

この形態は先に示した特定目的証明書の世界で、一つのプレートに CA が複数（互いに認証された）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取ることができる。これは、特定目的証明書の新しい将来形態とも考えられる。

（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。

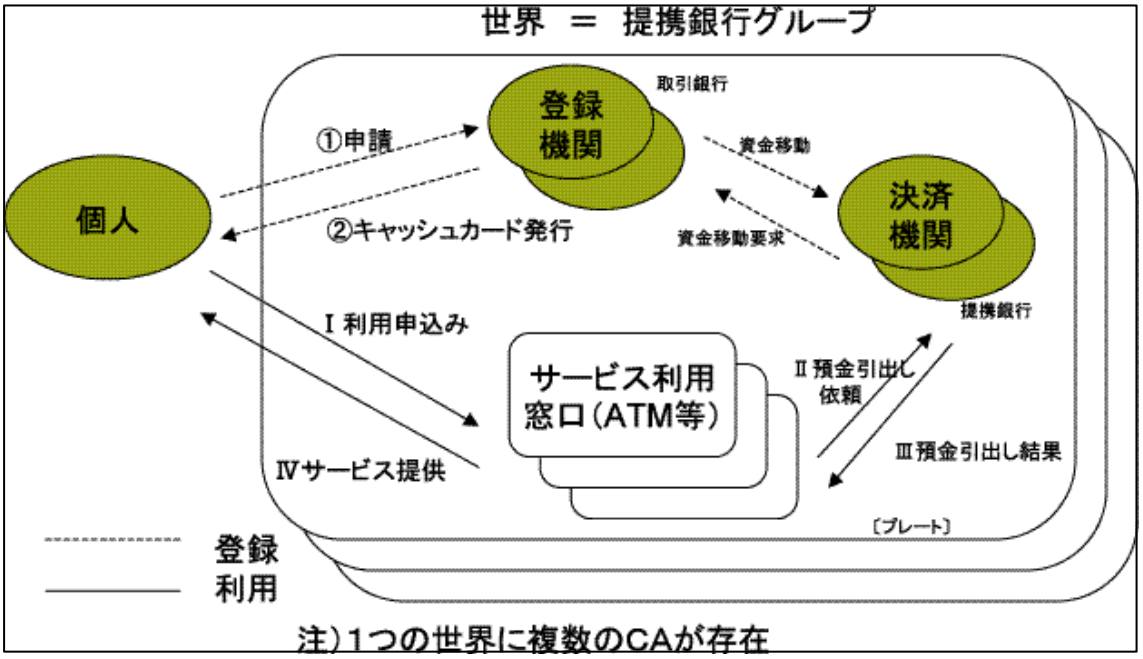


図 1-5 銀行における特定目的証明書のモデル

銀行のモデルは、一つの世界（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（手数料の有無などの差はあるものの）個人にとっては同一の世界としてサービス窓口への登録をすることなく、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。特定目的証明書の世界の拡張形であると言える。

（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など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サービスも出ている。また、クレジットカード会社と提携した場合、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同様に扱うことも出来る。

この形態は、提携各社の集合をドメインとする中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、特定目的証明書の拡張形態と考えられる。

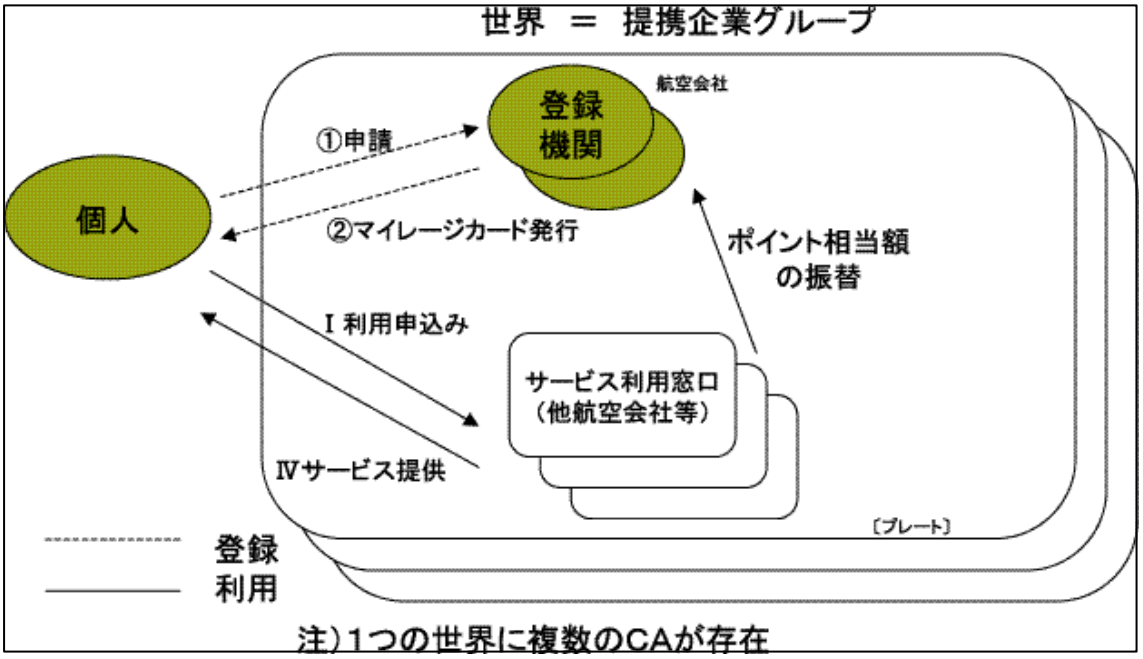


図 1-6 マイレージサービスにおける特定目的証明書のモデル

単一目的証明書がマイレージサービスの世界で利用される場合も想定されるが、この場合は独立した単一目的証明書が複数社間で互いに利用されることとなる。これも将来の電子証明書の利用形態の動向を示唆するものと考えられる。

1.2 属性の種類と利用場面

1.2.1 ID と属性

インターネットの世界では、顔の見えない本人のかわりとしてユニークに本人を特定できる情報がなければならない。一般に事物を表す情報として ID（identification）と属性（attribute）があるが、本節ではインターネットにおける本人確認の情報として ID と属性を考察する。

ID とは本人を確認（Authentication）するためのユニークな情報である。指紋・虹彩・DNA などのバイオメトリクス情報は代表的な ID 情報だが、一般的に ID は単一情報で構成されるとは限らない。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、一般的な個人は氏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、性別・生年月日・住所（氏名と合わせて住民基本４情報とよばれる）を加えて ID とすることがある。

属性とは対象者に与え（Authorization）られた資格や権限、職責、地位等をあらわす情報である。ID が単独で使用されることがあるのに対し、属性は単独で使用されることはない。ビザとパスポートの関係のように、属性は必ず ID とペアで使用される。

なお、本書では ID と属性を構成する個々の情報を「属性情報」とよぶ。

1.2.2 属性情報の分類

以下の観点から属性情報の分類を試みる。

（１）時間の経過に伴い変化する属性情報かどうか

属性情報には、生年月日など時間の経過に伴い変化しない情報と、権限・職責など変化する情報がある。

- 先天的に変わらない情報
  生年月日、バイオメトリクス情報など
- 後天的に付加され変わらない情報
  学歴・職歴などの経歴、賞罰など
- 時間的にあまり変化しない情報
  資格、免許、職業、住所など
- 時間的に変化しやすい情報
  所属、職責、権限、ランク、資産（預金残高等）など

前述の ID および属性との関係では、ID には時間的に変化しないか、あるいはあまり変化しない情報が必要であり、属性は時間的に変化しやすい情報から構成されるという特徴がある。

（２）オープンな属性情報かどうか（信頼できる属性情報かどうか）

属性情報には広くオープンな世界で通用する情報と、限られたコミュニティ内で通用する情報がある。

- オープンに通用する情報
  住民基本情報、商業登記情報、資格、免許（許認可）など
- コミュニティ内で通用する情報

所属部門、職責、ランク、会員資格など

属性情報は使用される世界と密接な関係があり、コミュニティごとに信頼される情報は異なる。

（3）センシティブな属性情報かどうか

属性情報には一般に知られてもよい（あるいは知らせたい）情報と、知られたくない情報がある。

- 知られてもよい（知らせたい）情報
  氏名、会社名、資格、免許（許認可）、賞など
- 知られたくない情報
  戸籍情報、住所・TEL、経歴、罰、診療情報、成績、年収など

属性情報には個人（私的）情報と組織人（公的）情報がある。個人（私的）情報は保護対象として特に厳重な管理が必要である。

（4）必要な属性情報かどうか

コミュニティやサービス毎に必要とする属性情報は異なるが、おおむね以下の３つに分類される。

- コミュニティやサービスに共通な属性情報（一次属性情報とよぶ）
- コミュニティやサービス毎に固有な属性情報（二次属性情報とよぶ）
- コミュニティやサービスで必要としない属性情報（非属性情報とよぶ）

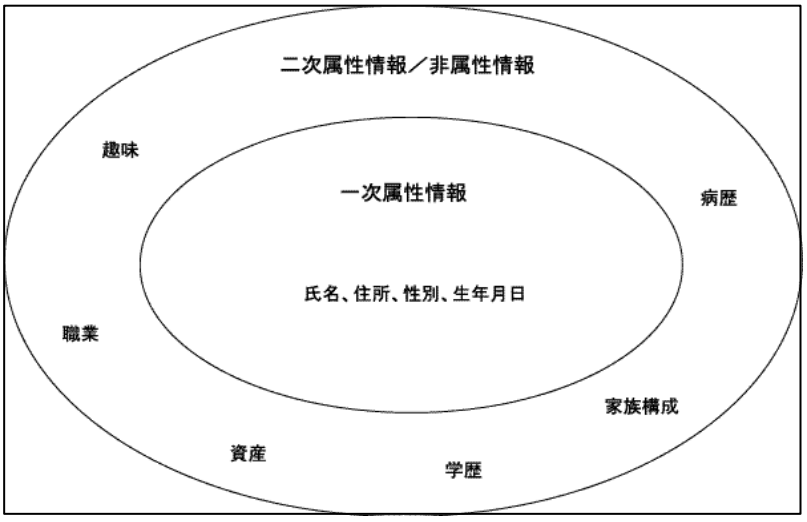


図 1-7 A さんの属性情報

例として A さんの属性情報を図 1-7 に表すと、氏名、住所等はどのコミュニティやサービスでも必要（一次属性情報）だが、病歴は診療サービスでは必要（二次属性情報）、金融サービスでは不要（非属性情報）である。

1.2.3 属性情報の利用場面

属性情報が利用される場面について考察する。

（1）加入（登録）時と利用時

コミュニティやサービスにおいては、加入（登録）時と利用時では属性情報に以下の違いがある。

- 加入（登録）時
  本人確認を目的とするため、あるレベルの信頼度を確立できていることが公に認識されている属性情報からなり、その数はコミュニティやサービスによってあまり異ならない。
- 利用時
  受け入れ側のリスクに対応しうる属性情報が必要であり、その数はコミュニティやサービスごとにかなり異なる。

（2）利用分野ごとの特徴比較

昨年の報告書「証明書利用形態に関する考察（2）属性情報の分析」では、医療・教育・行政・金融４分野の利用場面ごとに属性情報がどのように利用されるかを詳細に分析したが、これをサービス利用者の属性情報からみた各サービスの特徴をまとめると表 1-1 のようになる。

表 1-1 サービス利用者の属性情報からみた各サービスの特徴

項目	医療	教育	行政	金融
サービス利用者	患者	学生	組織人	顧客
主な属性情報	保険・診療情報	在籍・成績情報	法人の資格・許認可情報	契約情報
属性の有効期間	５年（カルテの保存期間）	数年	数年	数ケ月～数十年
属性情報登録機関	医療機関	教育機関	行政機関またはそれに準ずる公共機関	金融機関
同検証機関	同上	同上	同上	同上
同失効機関	同上	同上	同上	同上
権限の内容	特に権限はない	受講、施設利用、学割等	資格・許認可	契約内容による
権限の有効期間	―	属性の有効期間と同じ	属性の有効期間と同じ	属性の有効期間と同じ
権限の適用範囲	―	当該教育機関、学割サービス等	一般的に国内	契約内容による
属性のリスクレベル	大	小	資格・許認可内容による。	中
属性の信頼性	高い	高い	高い	高い

サービス提供者の主たる属性情報	資格（医師、看護師等）	教育機関名	行政機関長名	金融機関名
その他特記事項			サービス利用者は法人代表者名義が多い	

1.3 属性情報の実現方式

1.3.1 3種の実現方式

属性情報の実現方式には、いくつかの方法があるが3方式を紹介する

1.3.1.1 公開鍵証明書利用

公開鍵証明書（ID 証明書）を利用して利用者の属性情報を認証する方法である。

公開鍵証明書を利用する方法には、以下のように二つの方法がある。

（1）公開鍵証明書の発行対象者を限定することで、利用者がある属性及び属性値を有することを公開鍵証明書に暗示する方法

公開鍵証明書を属性とみなす方法である。属性を保証する団体が、属性を持つ個人に対してのみ公開鍵証明書を発行する。公開鍵証明書を用いた利用者認証が成功したら、利用者がその属性及び属性値を有していることを検証できたことになる。

例．弁護士会等、士業の団体が各加盟者に対して公開鍵証明書を発行。

公開鍵証明書の申請時に、各個人が属性情報を添えて申請するか、所属する組織がまとめて発行することが想定される。認証局の登録局（RA）が申請内容の確認を行い、発行局より公開鍵証明書が発行される。

（2）利用者がある属性及び属性値を有することを公開鍵証明書に明示する方法（拡張領域等に記載する）

利用者が保有する属性及び属性値を公開鍵証明書の extension に記載して公開鍵証明書を発行する。公開鍵証明書の extension を検証することによって利用者がある属性及び属性値を有していることを検証する。

公開鍵証明書発行時には、属性情報を確定する必要がある。

公開鍵証明書の申請時に、属性情報を添えて申請する。認証局の登録局（RA）が申請内容の確認を行い、発行局より公開鍵証明書が発行される。

図 1-8 に公開鍵証明書利用の際の運用イメージ例を示す。

①利用者は、ID 証明書の申請時に、登録する属性を記述して申請する。

②認証局では、登録局（RA）が申請内容の確認を行ない、発行局より公開鍵証明書が発行される。

③サービスを利用する際に、利用者がサービス提供者に公開鍵証明書を提示する。

④サービス提供者は、認証局の失効管理を前提に、提示された公開鍵証明書を検証し、サービスを提供する。

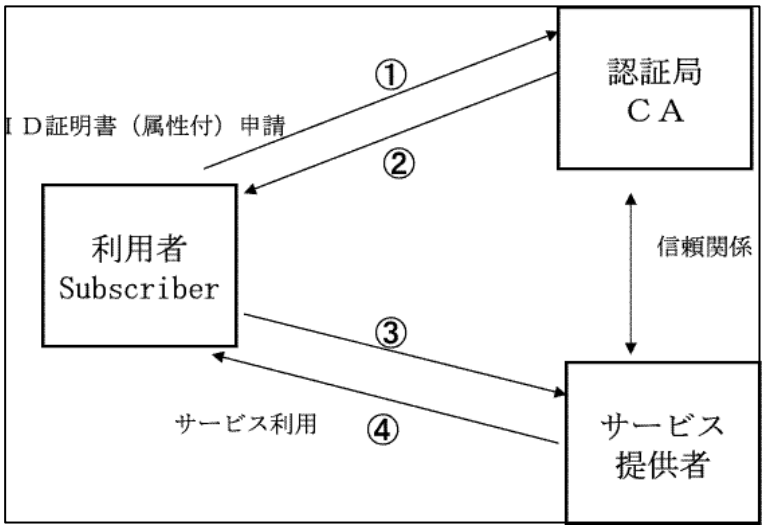


図 1-8 公開鍵証明書利用イメージ

申請書内容の確認を行なう登録局と、サービス提供者は、登録時の属性情報の確認や失効管理において、信頼関係を持つ。具体的な依存の仕方は、属性の種類により異なる。

(a) 属性が資格として扱われる場合

資格に対する権威者が、認証局を運営（登録局を担う）することが想定される。

(b) 属性が役割として扱われる場合

役割を決定する部署が、認証局を運営（登録局を担う）する。サービス提供者は、役割としての属性を信用する必要があり、限られた範囲での利用になる。

(c) 属性が許可として扱われる場合

サービス提供者が、登録時の確認を行なう。認証局は、サービス提供者の配下にあると考えられる。

公開鍵証明書を属性証明書として利用する場合は、サービス毎に公開鍵証明書を発行する必要がある。

属性情報及び属性値に変化があった場合には、公開鍵証明書が失効する。

1.3.1.2 属性証明書利用

既に発行されている公開鍵証明書（ID 証明書）を有する利用者に対して、属性及び属性値を記載した属性証明書を発行する方法である。属性証明書は、複数の属性及び属性値を取り扱うことができるので、必要に応じて複数の属性及び属性値を一つの属性証明書に記載しても良いし、複数の属性証明書に記載しても良い。

公開鍵証明書によって利用者を識別・検証し、検証したい属性を記載した属性証明書を用いて属性及び属性値を検証する。

図 1-9 に属性証明書利用の際の、運用イメージ例を示す。

①利用者は、公開鍵証明書を認証局に申請している。

②利用者に、公開鍵証明書が発行されていることが前提である。

③利用者は、属性認証局に対して、属性証明書を申請する。その際に、公開鍵証明書を提示する。

④属性認証局は、認証局を信頼し、またその運用ポリシーに従い、属性証明書を発行する。

⑤利用者は、サービス提供者に、公開鍵証明書と属性証明書を提示する。

⑥サービス提供者は、認証局と属性証明局を信頼し、その失効管理を前提に、属性証明書及び公開鍵証明書を検証し、サービスを提供する。

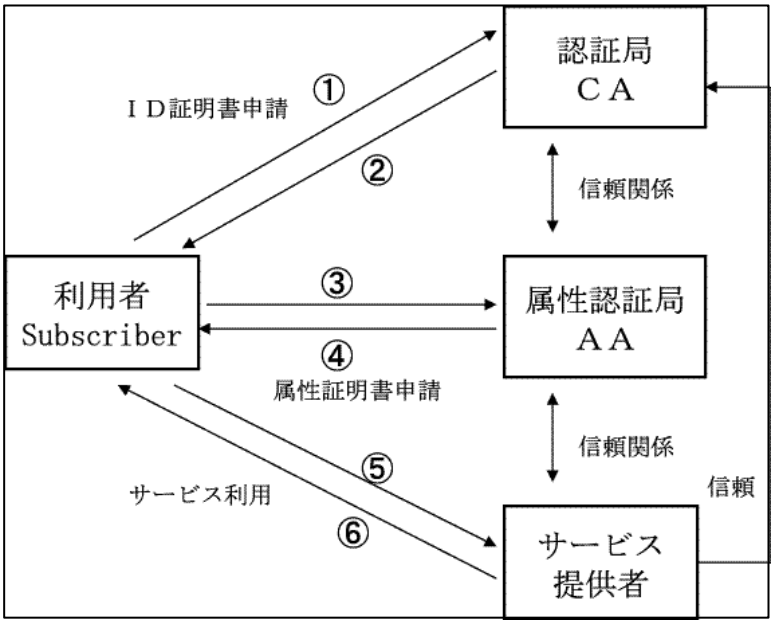


図 1-9 属性証明書利用イメージ

属性認証局は、属性を正しく公開鍵と結びつけて発行する義務を負う。

サービス提供者は、認証局と属性認証局のそれぞれと信頼関係を持つ。信頼の仕方は、属性の種類により異なる。

(a) 属性が資格として扱われる場合

資格に対する権威者が、属性認証局を運営（登録局を担う）することが想定される。その場合、権威者が信用できる公開鍵証明書を発行する認証局が存在する。

(b) 属性が役割として扱われる場合

役割が有効となる範囲で、属性認証局が運営されている。前提となる公開鍵証明書は、役割を決定、運用する組織で活用されていることが想定される。

(c) 属性が許可として扱われる場合

サービス提供者が、属性認証局を配下におき、属性証明書の発行を行なう。サービス提供者が信用できる公開鍵認証局が存在する。

属性証明書を使用する長所は、属性証明書を公開鍵証明書と独立して発行できるため、属性の追加、変更の度に公開鍵証明書を失効させ、再発行する必要が無い点である。

1.3.1.3 外部 DB 利用

属性認証サーバが、各利用者の属性及び属性値を格納した属性データベースを用いて属性認証

する方法である。属性情報は、証明書には記載されない。

属性データベースには、属性認証サーバの利用者情報テーブルに含める方法、ディレクトリサーバに含める方法等がある。

属性認証サーバは、公開鍵証明書を用いて利用者を識別・認証できたら、属性データベースを用いて、利用者がある属性及び属性値を有していることを検証する。

サービス提供者が属性の管理を行なう。

図 1-10 及び図 1-11 に外部 DB を使用する際の、運用イメージを示す。

①利用者は、公開鍵証明書を認証局に申請している。

②利用者が、公開鍵証明書の発行を受けていることが前提である。

③利用者は、サービス登録時に、公開鍵証明書をサービス提供者に提示する。

④サービス提供者は､公開鍵証明書によって検証､確認できる ID 情報と属性情報の結び付けを、データベースに登録する。

⑤サービスを利用する際に、利用者は、公開鍵証明書を提示する。

⑥サービス提供者は、認証局の失効管理を前提に、公開鍵証明書を検証し、さらにデータベース上の属性情報を確認してサービスを提供する。

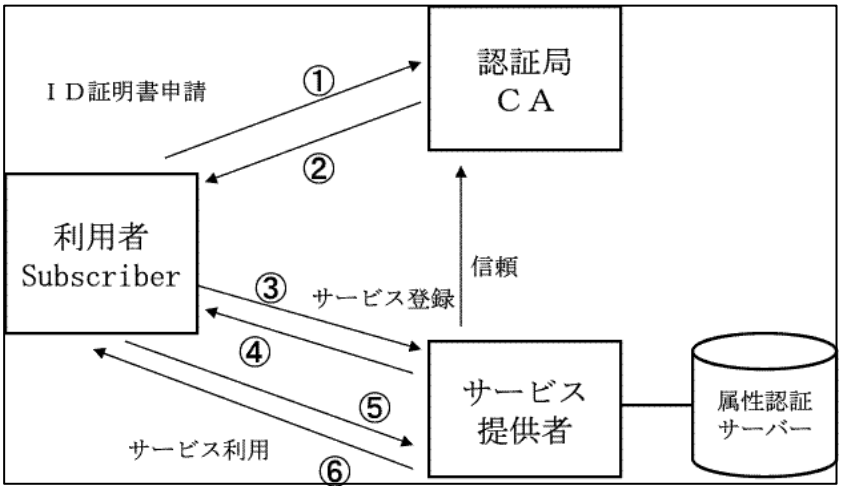


図 1-10 外部 DB 利用イメージ

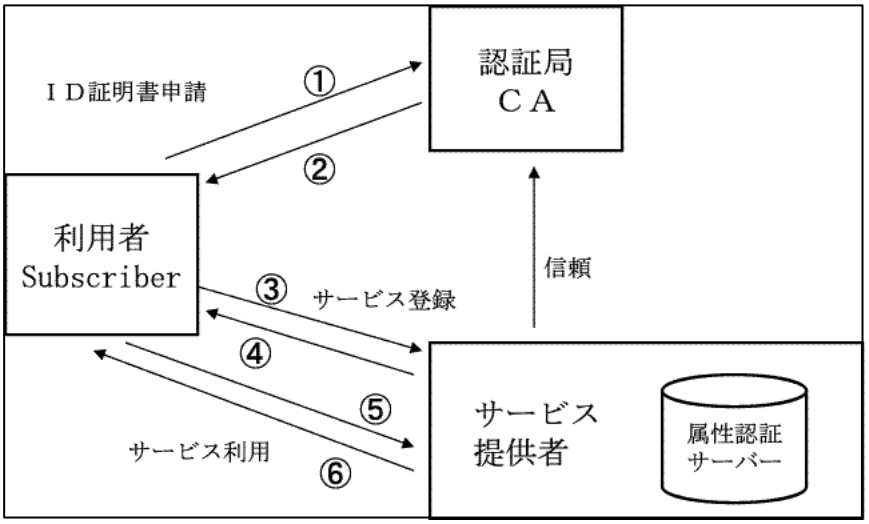


図 1-11 外部 DB 利用イメージ

(a) 属性が資格として扱われる場合

資格に対する権威者が、サービス提供者と一致することが想定される。資格保有者に対する閉じたサービスを提供する状況となる。

(b) 属性が役割として扱われる場合

役割が有効となる範囲で、ID と役割の対応付けがデータベース上で管理される。公開鍵証明書（ID 証明書）は、役割を決定、運用する組織で活用されていることが想定される。

(c) 属性が許可として扱われる場合

サービス登録時に、サービス提供者により、許可を与える。公開鍵証明書（ID 証明書）を前提として、サービス提供者が、ID 証明書とは独立して許可を与える運用が想定される。

外部 DB を使用する場合の、長所は、属性情報が変化しても証明書の再発行等で利用者の手を煩わせることなく、属性を変更できる点にある。短所は、サービス提供者の設備や、運用管理が複雑になる点である。

1.3.2 属性情報と実現方式

1.3.2.1 属性情報の管理形態

前項での属性情報の分類を基に各属性情報に推奨される管理形態を以下に示す。

(1) 時間軸による分類（時間の経過に伴い変化する属性情報かどうか）

①変化しない属性：

属性が変化しないことから、公開鍵証明書、属性証明書、外部 DB いずれも使用できる。証明書に一つの属性のみを持たせるのであれば、公開鍵証明書の使用が推奨される。

②変化する属性：

長期的に変化：公開鍵証明書の有効期間も１年間であるから、公開鍵証明書、属性証明書、外部 DB いずれでも使用できる。

短期的に変化：公開鍵証明書及び属性証明書は、属性が変化した場合、再発行が必要で

あるから、外部 DB の使用が推奨される。

(2) 適用範囲による分類（オープンな属性情報化どうか）

適用範囲の観点からは、推奨形態を選択できない。

(3) センシティブか否かによる分類（センシティブな属性情報かどうか）

①一般に知られてもよい情報：

公開鍵証明書、属性証明書、外部 DB いずれも使用できる。

②一般に知られたくない情報：

証明書に記入してあれば、サービス提供者に知られることになる。信頼できないサービス提供者のサービスを受けないことも重要である。外部 DB の使用が推奨される。

(4) 信頼度による分類

①公的機関で保証する情報：

公開鍵証明書、属性証明書、外部 DB いずれも使用できる。

②公的機関で保証しない情報：

信頼できる民間機関が保証する情報であれば、公開鍵証明書、属性証明書、外部 DB いずれも使用できる。信頼できる民間機関が保証しない情報であれば、サービス提供者の判断で使用することになるが、いつ変更があるかもしれないため、外部 DB の使用が推奨される。

1.3.2.2 属性情報の実現形式

属性情報を公開鍵証明書、属性証明書あるいは外部 DB で表現する場合の、詳細な標準仕様は、現在のところ存在しない。標準仕様の制定は、今後の対応となる。

「属性型証明書」という名称で公開鍵証明書に情報を追加して属性証明書として使用するサービスが開始されている。一例として紹介する。この例では、個人の識別情報に加えて表 1-2 のような企業等の在籍情報を証明している。

表 1-2 属性型証明書プロファイル概略

attribute	value
subject	C=JP CN=加入者氏名 UID=ユーザ ID
Subject AltName（C=JP を除き日本語）	C=JP O=法人名 OU=代表者氏名：法人代表者氏名 OU=法人所在地：法人登記所在地 OU=部門名：本支店名、事業所名等の部門名 OU=事業所所在地：本支店、事業所等の所在地 OU=コード：事業所コードまたは企業コード T=肩書名 CN=加入者氏名

このサービスの証明書有効期間は２年または３年である。証明書記載情報に変更があった時には利用者からの失効申請を受ける。

なお、新規にこのサービスを受ける場合には、以下の書類の提出を求められる。

①利用申込書

②在籍証明書

③履歴事項全部証明書（いわゆる商業登記の登記簿謄本）

④法人代表者印鑑証明書

1.3.2.3 属性情報のパターン分析

H14 年度の「証明書利用形態に関する考察（２）」ではリアル世界の属性情報を利用した認証を「医療分野」、「金融分野」、「教育分野」及び「行政・公共分野」の四つの分野ごとに検討した。検討の結果抽出された属性情報を多面的に分析した。また、属性情報を二次元でプロットし、パターン分析を行った。

分析の結果、属性情報は以下のような分類ができた。

(1) 論理的視点の分類

① 資格

広く認知された権威者によって付与される。被資格者についての客観的条件に基づく。

② 役割

ある組織内で決められた役割分担

③ 許可

２者間の取引において受け入れ側の判断により、権利者に付与される権利

④ 評判

実績に基づく。初回は、ある限られたリスクの範囲で許容される

(2) 何をもってその属性を信頼するかの分類

①身体的特徴

外観、年齢等

②持ち物（～証）

信頼できる第３者によって発行されたもの。２者間によって事前に渡されるもの。

③持ち物

身につけている物

④場所

存在する場所

(3) 属性の信頼性による分類

①高：なりすまし、偽造等の可能性が低い

②中：なりすまし、偽造等の可能性がありうる

③低：なりすまし、偽造等の可能性が高い

例えば、医療分野のリアル場面での分類を行うと表 1-3 のようになる。また、論理的視点と、何をもってその属性を信頼するかの視点で二次元でプロットすると図 1-12 のようになり、パターン１からパターン４の分類ができる。

表 1-3 医療分野リアル場面の属性分類

	論理的視点による分類				物理的視点による分類				属性の信頼性		
属性情報	A	B	C	D	a	b	c	d	高	中	低
1)医師資格	○					○			○		
2)勤務病院名			○			○				○	
3)医師氏名				○	○					○	
4)診療科目		○				○					○
5)紹介先病院名				○				○		○	
6)紹介先医師名				○				○		○	
7)紹介書				○			○				○
8)検査科目				○			○				○
9)患者本人の実体				○	○						○
10)患者の保険証			○			○				○	
11)患者の診察券			○			○				○	
12)対面での患者本人の希望				その他						○	
13)医師判断				その他							○
14)健康保険の被保険者			○			○				○	
15)診察券			○			○				○	
16)患者の氏名				○		○					○
17)患者の実体				○	○						○
18)待ち行列				○		○					○
19)顔型				○	○					○	
20)診察券番号			○			○					○
21)科目			○			○					○
21)看護師の名前				○	○					○	
22)看護師	○					○			○		
23)職員		○					○	○		○	
24)所属		○					○	○		○	
25)担当患者		○					○	○		○	
26)認印・サイン				その他	○					○	
27)経験				その他							○
28)得意分野				その他							○
29)スキル				その他							○

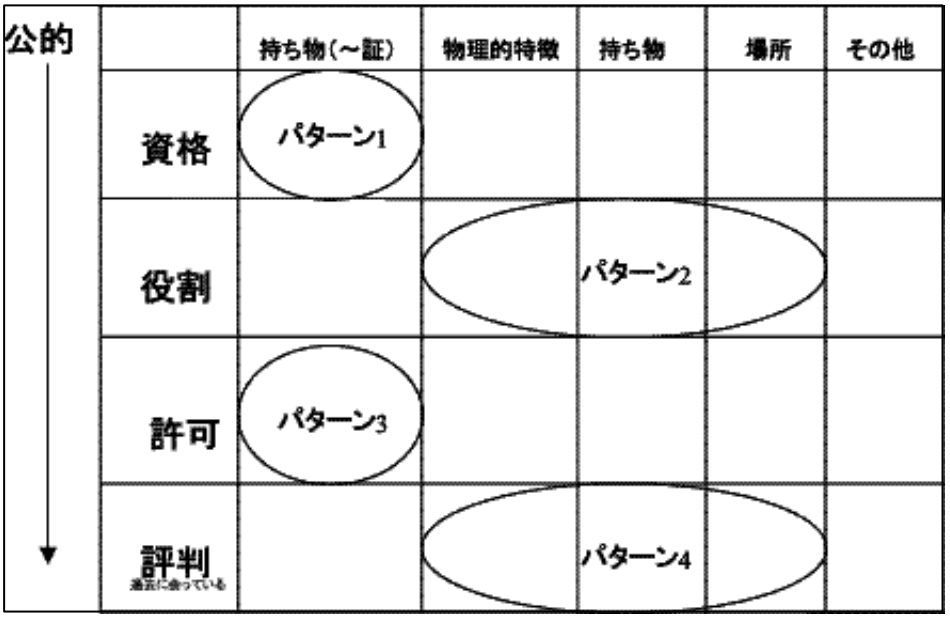


図 1-12 リアル場面のパターン分析

リアルの場面では、上記の分類のように各種の方法を用いて属性を推測できる。医療分野での属性の推測の例を以下に示す。

① 身体的特徴

直接会って相手の特徴（外観）を見る事により、相手を識別できる。過去に会ったことがあれば、顔かたちを見て、話をしてみて記憶と照合して本人と推測する。態度や言動により医師や看護師と推測している。また、同様に医師、看護師等は、患者を身体的特徴、声、雰囲気、本人しか知りえない知識等から患者本人であると推測する。

② 持ち物（～証）

信頼できる国家機関の発行する資格証や証明書を持っている事により属性を推測する場合である。医師免許証を持っていることより、医師と推測することができる。

同様に看護師免許証を持っている事より看護師と推測することができる。

③ 持ち物

患者が紹介書を持参してきた場合、病院所定の紹介書であるか、病院が紹介先病院リストにのっているか等により、紹介書が本物であると推定し、患者の属性を推測できる。また、患者は名札や服装から、応対している者が病院の職員であること及び所属を推測できる。

④ 場所

患者からみれば、応対している相手が存在する場所により、相手がそこの病院の職員であると推測したり、特定の所属であると推測できる。

以上のように、リアルの場面では、各種の方法で属性を推測している。

しかし、バーチャルな場面では、身体的特徴、持ち物及び場所で属性を推測することはできない。そのため、属性を推測することがむずかしくなる。何らかの証明書により、属性を推測することになる。この証明書が公開鍵証明書であったり、属性証明書であったり外部 DB であったりする。

電子的に送られてきた本人の申請のみでは、相手を推測できるのは、メールアドレス程度であり、これも偽造が可能であれば、信頼度が低い。何らかの証明書が無ければ属性の推測ができない。パターン分析を行うと図 1-13 のようになる。

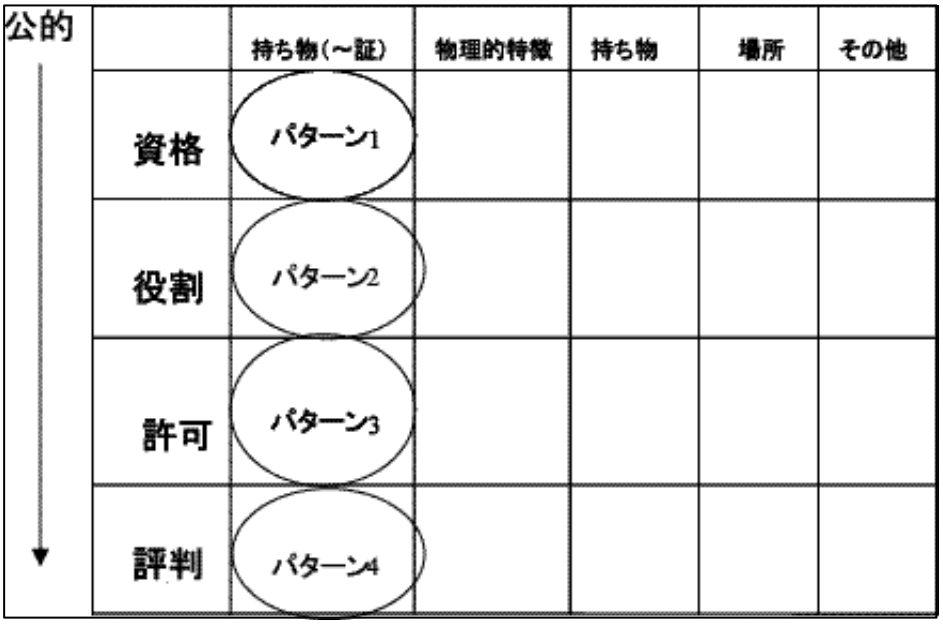


図 1-13 バーチャル場面のパターン分析

図 1-13 のパターン１～パターン４は、裏づけとなるものの種類による分類である。
パターン１～パターン４は、まとめると以下の定義が可能である。

①パターン１：公的証明のある属性
②パターン２：確かな裏づけのない属性
③パターン３：契約に基づく属性
④パターン４：覚書的合意に基づく属性

パターンによる分類を行ったものの管理形態は以下のようになる。

①パターン１：公的証明のある属性

このパターンの特徴は誰もが信頼できることである。非常に広範囲の分野における利用ができる。

公開鍵証明書、属性証明書、外部 DB いずれも使用できる。

②パターン２：確かな裏づけのない属性

このパターンの情報は、他のパターンの属性情報による補強がある場合にのみ、信頼することができる情報である。サービス提供者の判断によってのみ使用可能である。外部 DB の使用が推奨される。

③パターン３：契約に基づく属性

２者間の契約に基づくサービスの提供であり、公開鍵証明書、属性証明書、外部 DB のいずれも使用できるが、属性情報をサービス提供者が保持していることを考慮すれば、公開鍵証明書あるいは外部 DB の使用が推奨される。

④パターン４：覚書的合意に基づく属性

このパターンの情報は、信頼性のレベルが低く、サービス提供者の判断によってのみ使用可能である。外部 DB の使用が推奨される。

2．証明書利用における要件ガイドライン

2.1 基本方針

証明書の利用によって利用者が安心してインターネットの利便性を受け入れるようになるためには、利用者が証明書の利用を自ら望むサービスとはどのようなもので、そこへ提示し得る属性情報は何か､またこれらの情報管理に望む信頼性をどう確保すべきかといった検討を進めてきた。

この中では、証明書のライフサイクルおよび利用者が証明書発行に求める属性情報の信頼性、安全性に主眼をおき、証明書利用の有効性と利用における留意点について検討した。

これまでの PKI の説明資料（規約、本など）では、CA ベンダーや SI 業者、研究者/技術者からみたものが大半を占め、利用者の視点で見たものがほとんど存在しないことから、本章では利用者の視点に立ち、証明書利用の際に利用者が留意する事項、観点を記述することにより、証明書の利用に関する利用者の理解を深め、証明書利用の促進を目指すものである。

なお、証明書利用形態としては、以下の３形態を想定している。

・ 単一目的証明書

提供されるサービス毎あるいはサービス提供者毎に発行される証明書であり、その利用用途は非常に限定されたものであるが、サービス内容に見合った手続きやリスクレベルの設定が容易である。

・ 特定目的証明書

ワンストップサービスといった複合的なサービス連携や、特定業界のサービス連携に基づき、この連携グループによって発行される証明書であり、複数のサービスを１枚の証明書で利用することができるよう利便性を高めたものである。

・ 汎用目的証明書

あらゆる用途に利用可能な証明書であり、どのようなサービスを利用する場合にもこの証明書を利用することが可能となる。現時点では全てのサービス提供者がその利用を認めるような証明書は存在しないが、近い将来、証明書の利用拡大によって公的機関あるいは信頼される第三者機関によってこのような証明書が発行されることを期待したい。

2.2 利用モデル

本節では、利用者が証明書を利用する際に、利用者から見える人物ややり取り、情報について記述する。

利用者から見える主なものとしては以下の 3 つが考えられる。

- ライフサイクル（登録から証明書失効まで）
- 利用者と各人物との間にてやりとりする情報
- 認証局やサービス提供者にて公開する情報

なお、証明書利用とは、利用者が証明書に関わるやり取りを行う登録から証明書失効までの間のことを示す。

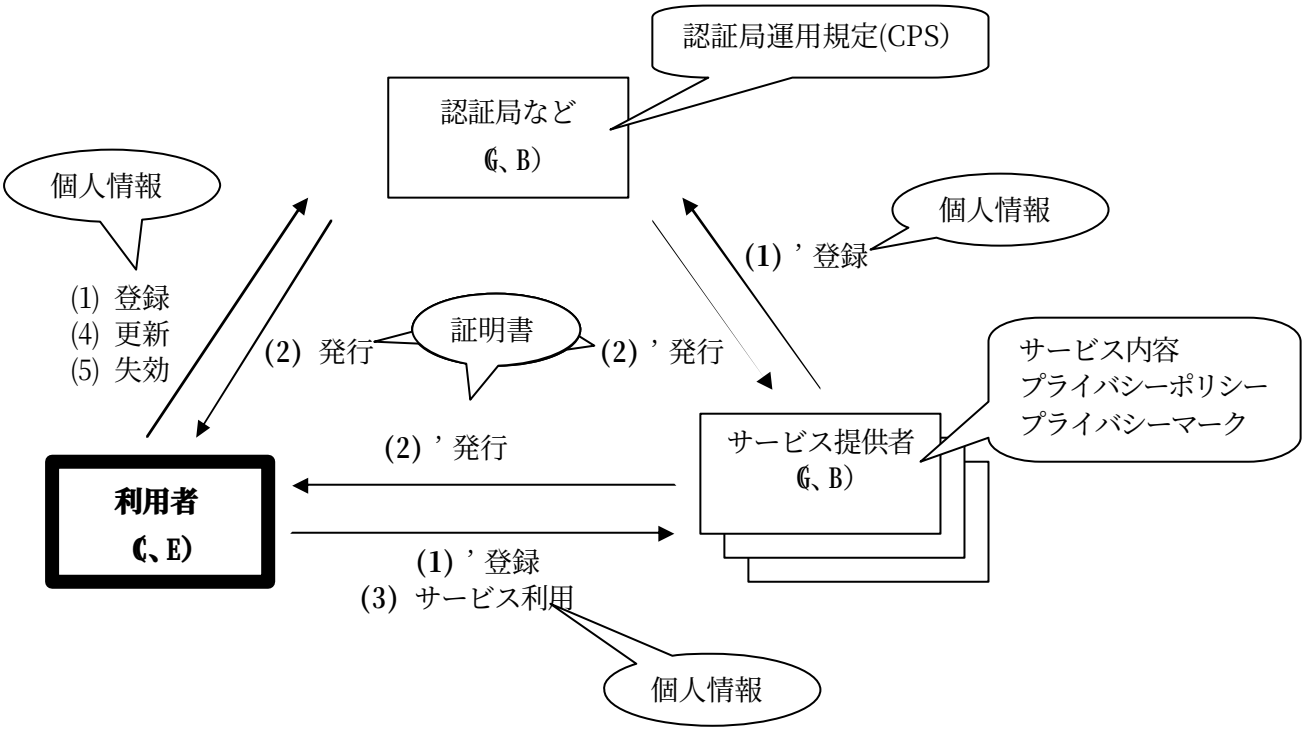


図 2-1 証明書利用サイクル

2.2.1 ライフサイクル

(1) 登録

利用者は認証局や属性認証局に対して自身を登録する。または、登録される。

この際、(1)のように利用者が自らの意思で認証局や属性認証局にアクセスして自身の公開鍵や属性を登録する場合や、(1)’のように利用者がサービス提供者にアクセスしてサービス提供者により利用者の公開鍵や属性を認証局や属性認証局に登録される場合などがある。

(2) 発行

認証局や属性認証局において公開鍵証明書や属性証明書が作成され、利用者に証明書が発行される。

(3) サービス利用

利用者がサービスを利用するためにサービス提供者にアクセスする際に、利用者が上記において発行された公開鍵証明書や公開鍵証明書と属性証明書を提示することで、サービス提供者が利用者に対して本人認証やアクセス制御を行い、利用者に各種サービスを提供することができる。

(4) 更新

利用者の持つ証明書の有効期限が切れた場合、有効期限が切れた証明書をサービス提供者に提示しても、サービス提供を許否されるため、サービスを継続して利用する場合には、新しい証明書を取得しなおす必要がある。

(5) 失効

秘密鍵が紛失や盗難の被害によって危殆化した場合や、利用者のサービス利用資格が剥奪された場合などに、公開鍵証明書や属性証明書を失効する必要が生じる。

2.2.2 利用者と各人物との間にてやりとりする情報

(1) 登録

登録時には、主に以下の情報をやり取りする。

利用者→認証局：住所、氏名などの個人情報

(2) 発行

発行時には、主に以下の情報をやり取りする。

認証局→利用者：公開鍵証明書

(3) サービス利用

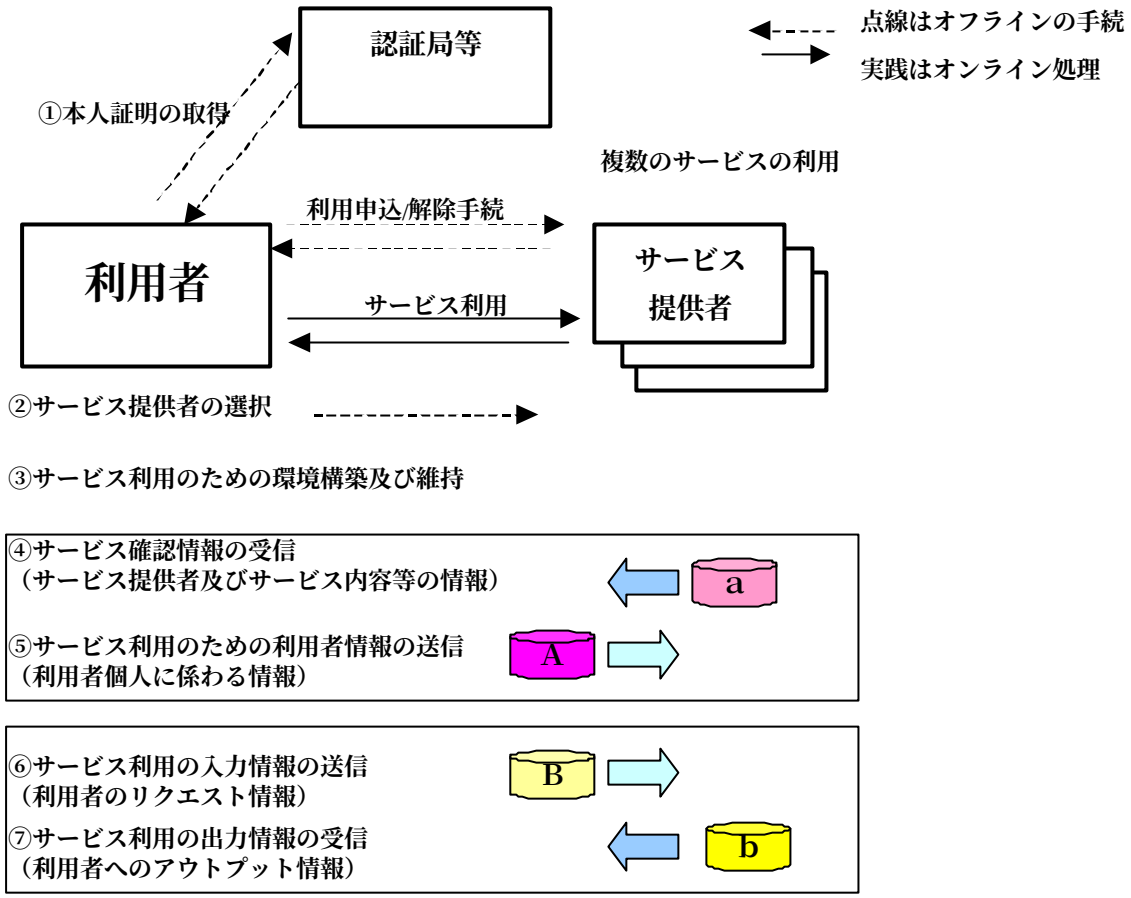


図 2-2 サービス利用手順

A．サービス利用の手順

利用者は以下のステップを経てサービスを利用する。

- 本人証明の取得

利用者は、利用者個人を識別する情報を送付し、認証局等（サービス提供者も含む）から、利用者個人を識別するための公的又は個別の証明（本人証明）を、取得する。

- サービス提供者の選択

利用者は、複数のサービス提供者から特定のサービス提供者を選択する。

- サービス利用のための環境構築及び維持

利用者は、サービスを利用するための装置・設備・ネットワーク環境等を構築する。

- サービス確認情報の確認

利用者は、サービス利用を開始する前に、サービス提供者のサービスにアクセスしサービス提供者自身の情報及びサービス内容の情報を確認する。

- サービス利用のための利用者情報の送信

利用者は、サービス利用のためにサービス提供者から要求される利用者個人の情報として公開鍵証明書や属性証明書等を送信する。

- サービス利用の入力情報の送信

利用者は、サービス利用におけるリクエスト情報を送信する。

- サービス利用の出力情報の受信

利用者は、サービス利用におけるアウトプット情報を受信する。

B．利用者からサービス提供者へ送信される情報

ａ）サービス利用のための情報

利用者個人の情報であり、以下の２つに大別される。

ｉ．利用者個人の固有情報（本人識別に使用される情報）：

氏名、生年月日、住所、生体情報等

ii．利用者が一時的に保有する属性情報（アクセス制御に使用される情報）：

資格、役職、所属、チケット、マネー、実績等

ｂ）サービス利用の入力情報

ｉ．サービス利用のためのリクエストに係わる情報

C．利用者がサービス提供者から受信する情報

ａ）サービス提供者の情報（利用者がサービス利用にあたって確認）

サービス提供者自身の本人証明の情報やサービス内容の情報。

ｂ）提供されるサービスの結果となる出力情報

（利用者のサービス利用の目的となるもの）

サービス提供者から提供されるサービス

例）インターネットショッピングであれば、商品（又は商品取得の権利情報）。

(4) 更新

更新時には、主に以下の情報をやり取りする。

利用者→認証局：更新理由、公開鍵証明書のシリアル番号など

認証局→利用者：公開鍵証明書

(5) 失効

失効時には、主に以下の情報をやり取りする。

利用者→認証局：失効理由、公開鍵証明書のシリアル番号など

2.2.3 認証局やサービス提供者にて公開する情報

主なものを以下に示す。

認証局

- 認証局運用規定（CPS：Certification Practice Statement）

サービス提供者

- サービス内容
- プライバシーポリシー
- プライバシーマーク

2.3 利用者の要件

ネットワークを介したサービスにはリスクが存在し、利用者は取引の安全性について注意を払う必要がある。利用者がこのリスクを認識しながらも利用するためには、利用者がサービスに求める要件を明確化し、その要件が満たされる必要がある。

信頼性、利便性、コストといった３つの観点で、利用者の要件を整理してみた。これら要件のバランス確保ができたサービスは継続的に利用者を確保することができよう。

2.3.1 信頼性

(1) サービス提供者が信頼できること
- サービス提供者を確認することができる
- 利用者登録情報等、入力情報の利用用途が明確であり、流用されることがない
- 出力情報はサービス提供者からのものであることが保証される
- 出力情報は求めたものに一致し正確である
- 入力情報、出力情報ともに盗聴や改ざんへの耐性を持つ
- 登録に際して提供されるサービスに見合った情報のみを求められる
- 期待したサービスが確実に履行される （過去に提供したサービスの実績）
- クレームの窓口が開いている
- システムの安全性を確認できる

(2) 認証局が信頼できること
- 唯一の秘密鍵が安全確実に手に入る
- 署名検証が容易く行える
- サービス提供者に対する証明書発行基準を確立している
- 秘密鍵紛失等の事故処理手順が明確にされている

2.3.2 利便性

(1) 簡単に証明書が取得できること
- サービス利用までの手順が少なく分かりやすい

(2) 使いたいときにサービスが利用できること
- サービスの提供品質が高い（高稼働率、即時性確保、継続的状況提示、等）

(3) どこからでもサービスが利用できること
- 特別なハードウェア、ソフトウェアを必要としない
- 低い通信レートでのサービスが可能

(4) ひとつの証明書で多くのサービスを利用することができること
- 一枚の証明書を保有すれば複数の魅力的なサービスが利用可能

(5) どのサービスを利用する場合でも、同様の使用方法で利用できること
- どのサービスも、同様のユーザ・インタフェースが実装されている

(6) 決済方法を選択できること
- クレジット、銀行振込み／振替、代引き、他が選択可能

2.3.3 コスト

(1) サービス内容と掛かる費用のバランスがとれていること

- ひとつの証明書が多くのサービスに長期間利用可能

(2) サービス利用のために特別な環境を準備する必要がないこと

- 標準的な PC、モバイルツール、からのサービス利用が可能
- 複数の証明書を使用する場合においても、同じ PC、モバイルツール等が利用可能

2.4 利用者の留意事項

前記のような要件を意識する利用者が、実際のサービスを利用するにあたり留意すべき事項を以下に提示する。

また、留意するべき事項とその対策を選択する際の判断基準を示す。

2.4.1 留意すべき事項

(1) サービス提供者の信頼性

- サービス提供者自身の提示情報
- サービス内容の提示情報
- サービスを利用するにあたってのリスク
- 利用者からサービス提供者へ提示する登録情報の妥当性
- 個人情報の保護（個人情報取扱ポリシー）
- 情報利用範囲・流用可能性の有無
- 評判
- 実績
- ドメイン名

(2) サービスの利便性

- サービスの保証内容
- サービス価格
- 利用環境構築費用
- 通信費・人件費等の経費
- リスクによる損害見積り
- サービス利用時間帯
- サービス利用手順
- 決済方法

(3) 認証局の信頼性

- 責任、補償、免責の範囲
- 利用者から認証局へ提示する登録情報の妥当性
- 取得条件

- 有効期限
- 証明書記載内容
- 電子署名法対応の可否
- 個人情報の保護
- 情報利用範囲・流用可能性の有無
- 申請受付時間帯
- 登録、発行申請、更新方法
- 証明書発行料金
- 決済方法
- 鍵ペア生成方法
- 秘密鍵格納方法
- PIN 送付方法

(4) 証明書取得の容易性
- 申請手順
- 証明書利用手順
- 証明書失効手順

2.4.2 対策と判断基準

利用価値が高く安全なサービスを有効に利用するため、証明書利用の各ライフサイクルにおける各種確認事項を以下に提示する。

(1) 登録～発行

認証局の提示事項

① CP/CPS

CP（CertificatePolicy）とは、証明書を使用する際に、認証局が示す規則集のことであり、CPS（CertificationPracticeStatement）とは、認証局が証明書を発行するときに採用する実践に関する声明文である。この内容によって、ネットワークを介して認証局の信頼性を把握するための情報は取得することが可能である。

② プライバシーポリシー

利用者から得た個人情報をいかに取り扱うかを宣言する文書であり、個人情報の利用や管理について、また利用者からの要求に対する処置等について記述されており、利用登録時に何らかの属性情報を提示する場合には一読すべきものである。

個人情報に関しては、JIPDEC（財団法人日本情報処理開発協会）の認定するプライバシーマーク制度があり、本認定を受けた事業者ではこれを公表しており、ひとつの判断材料とすることもできる。

③　証明書取得手順

利用者が証明書を入手するために必要な手順が記されているので、事前に準備すべきものや、提示を求められる情報の確認をするとともに、手続きの容易性を確認することができる。証明書の受け取り手段についても吟味することが求められる。たとえば秘密鍵と PIN が同一梱包で送付されるような場合には、「本人限定受取郵便（基本型）」といったルートで安全を確保する必要がある。

④　証明書格納媒体

ある人の秘密鍵は本人しか知らず、他人が知らないということが前提である。

そのため、秘密鍵が他人に覗かれないようにする必要がある。他人に秘密鍵を覗かれないようにして秘密鍵を格納しておくものとしては、IC カードや USB トークンなどがある。

利用者は、これらの情報をもとに認証局の信頼性を確認することができ、信頼できる認証局の証明書発行サービスを利用しているサービス提供者を再評価することもできる。信頼性を確認できないサービス提供者が仲介する認証局（第三者として独立したサービスを展開していない認証局）を利用する場合には、認証局の信頼レベルが、サービス提供者の信頼レベルを上回ることはないので、利用に際しては受容リスクについて十分な検討を行うべきである。

(2) サービス利用

サービス提供者の提示事項

①　サービス会員規約

サービス提供者が、サービス利用者に会員としての登録を求めるサービスにおいて、一般的に提示する規約であり、本規約によってサービスの利便性を判断することができる。多くの場合サービスの定義、費用、プライバシー、著作権、責任、義務、免責、決済、等に関する記述がなされており、利用者として一読すべきものである。信頼性判断の材料としては規約があることは最低条件であり、内容が整っていることは重要であるが、規約のみで信頼性を判断することはできない。

②　プライバシーポリシー

利用者から得た個人情報をいかに取り扱うかを宣言する文書であり、個人情報の利用や管理について、また利用者からの要求に対する処置等について記述されており、利用登録時に何らかの属性情報を提示する場合には一読すべきものである。なお、会員規約がある場合には、これに含まれる場合もある。

個人情報に関しては、JIPDEC（財団法人日本情報処理開発協会）の認定するプライバシーマーク制度があり、本認定を受けた事業者ではこれを公表しており、ひとつの判断材料とすることもできる。

③　著作権に関する情報

サービス対象となるコンテンツの著作権の保有者が誰で、利用者はこれらの著作物をどういった範囲で利用することができるかが記述されており、サービスの有効性判断や、誤使用を防ぐために一読すべきものである。なお、会員規約がある場合には、これに含まれる場合もある。

④　準拠法、裁判管轄

準拠法と、紛争が生じた場合の第一審専属管轄裁判所が明示される。なお、会員規約がある場合には、これに含まれる場合もある。

⑤　利用場所及び環境

サービス利用のための利用場所及び環境は、サービス提供者側が用意する場合と利用者が自ら構築する場合とがある。

利用場所及び環境をサービス提供者側が用意する場合は、利用場所及び環境の管理者がサービス提供者又は利用者に対しサービス提供者と同等の責任を負う者であることが前提条件となる。利用者は、利用場所が安全確保され、かつ利用者のライフサイクルに合致するかを確認するために、サービス仕様書に明記された利用場所に関する情報の机上確認だけでなく、利用場所の現地確認をすることが望ましい。利用場所及び環境を利用者自らが構築する場合は、利用者は、利用環境構築に係わる方式・手順及び費用を確認するために、サービス仕様書に明記された利用環境構築に関する情報を確認する。利用環境構築における費用の確認においては、構築費用だけでなく、ランニングコストも考慮に入れ、いつまでサービスを継続するかを含め総合的判断が必要となる。

利用者は、サービス提供者によるこれらの規約や宣言によって、いかなるサービスがどのようなサービスレベルで提供されているかを知ることができるが、信頼できるか否かの判断ではなく、信頼するか否かの判断をする必要がある。そのためには、サービス提供者の企業名、ドメイン名、実績、評判といった情報を収集すべきであり、サービス利用にかかる費用と、サービス内容からリスクを認識すべきである。このリスクが受容範囲内であった場合にサービス提供者を信頼して利用者となることができる。

⑥　サイトの証明書

サイトの証明書には、所有者、発行者及び有効期間等が記述されている。利用者はアクセスしたサイトが目的のサイトであることを確認するために、サイトの証明書を検証する。サイトの証明書の検証は、確実かつ迅速に行うためにシステムで自動的に実行されることが望ましい。

証明書検証の結果、証明書の所有者がサービス提供者であり、証明書の有効性確認が OK であった場合は、利用者はアクセスしたサイトが目的のサイトであることを確認することができる。

⑦　サービス結果の電子署名

サービス結果にサービス提供者の電子署名が付与されている場合がある。利用者は、サービス結果が正しいことを確認するために、サービス結果に付与された電子署名を検証する。サービス結果の署名の検証においては、利用者が電子署名を明示的に判別できるように、サービス結果に電子署名の画像イメージ等が表示されていることが望ましい。

サービス結果に付与された電子署名を検証した結果、署名者がサービス提供者であり、かつ署名検証が OK であった場合は､利用者はサービス結果が正しいところから送られてきた正しいものであることを確認することができる。

2.4.3　利用者の証明書利用形態に基づく留意点

(1) 単一目的証明書

サービス提供者ごとに証明書を発行する。紛失や盗難に対するリスクは小さいが、利用者が提示する属性情報の安全性はサービス提供者に依存するため、特にサービス提供者が提示する CP/CPS やサービス内容、プライバシーポリシーといった情報を十分確認の上、利用する必要がある。

また、複数のサービスを利用した場合には、秘密鍵ごとに PIN が必要となるので、それぞれの秘密鍵について PIN の管理（忘れない、PIN の定期的な変更等）を継続的に行う必要がある。

(2) 特定目的証明書

何らかの提携関係にあるサービス提供者が共同で証明書を発行する。複数のサービスを一枚の証明書で利用することができるため、利用者にとっての利便性は向上するが、利用者の意図しないサービスが付随していたり、利用者の属性情報が共有されたりすることがあるので、特にサービス提供者が提示するサービス内容やプライバシーポリシーといった情報を確認の上、利用する必要がある。

また、一枚の証明書が複数のサービス利用のキーとなり、紛失や盗難によるリスクが拡大することから、証明書の失効手続きに加えてリスクへの対応手続きについても認識しておく必要がある。

(3) 汎用目的証明書

信頼できる第三者が､あらゆるサービスの利用を可能とする証明書を発行するものであり、現時点では存在していない。利用者にとって管理する秘密鍵がひとつであることから利便性は高いが、サービスの提供を受けるには、各サービス提供者への利用者登録が必要となるので、サービス内容やプライバシーポリシーといった情報を確認すると共に、利用者の責任について確認しておく必要がある。

また、一枚の証明書が多くのサービス利用のキーとなり、紛失や盗難によって関連する全てのサービスが利用不可となることから、証明書の失効手続きに加えてリスクへの対応手続きについても認識しておく必要がある。

2.5　実現モデル例

利用者からみた証明書利用場面の具体例を記述する。

2.5.1　医療分野

医療分野におけるサービスは、利用者個人の情報を厳密に取扱う必要があるため、特に機密性、完全性及び信頼性が要求される。医師が利用する場合は、さらに緊急治療のためのいつでも使用できるという可用性、電子カルテなどの有効性、医師法等に対する遵守性が要求される。

2.5.1.1　証明書の利用例

医療分野におけるサービスとして診療記録閲覧サービスの利用例を想定する。本サービスにおいては、医療機関が認証局とサービス提供者を兼務するものとする。

- 提供サービス　：診療記録閲覧サービス
- 利用者　　：患者
- サービス提供者：医療機関
- 使用する証明書：患者の証明書、サイトの証明書、医師の証明書
- 認証局　　：医療機関が兼務

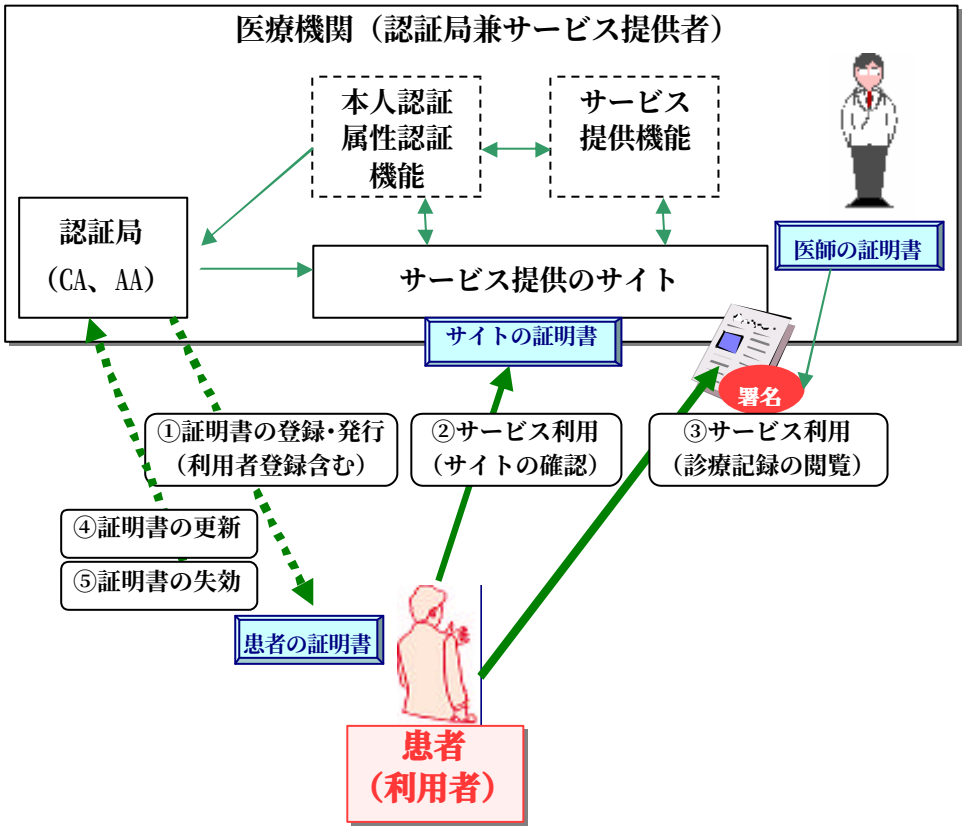


図 2-3 実現モデル例（医療分野）

(1) 証明書の登録・発行

患者は、サービス利用の申込みを行うことによって、本サービスを受けるための許可証となる「患者の証明書」を入手する。

(2) サービス利用（サイトの確認）

患者は、サービス提供のサイトにアクセスし、「サイトの証明書」を確認して正しいサイトであることを確認する。

(3) サービス利用（診療記録の閲覧）

患者は、自身の電子的な診療記録を閲覧し、医師の署名を検証して正しい診療記録であることを確認する。

(4) 証明書の更新

患者は、証明書の期限が切れる場合、「①証明書の登録・発行」と同様の申し込みで、証明書を更新する。

(5) 証明書の失効

患者は、サービス利用の解約を申込むことによってサービス利用の許可証となる「患者の証明書」を失効させる。また証明書の期限切れ又は診療終了による患者資格の失効等に伴い「患者の証明書」は失効される。

2.5.1.2 利用者の要件

(1) 証明書の登録・発行

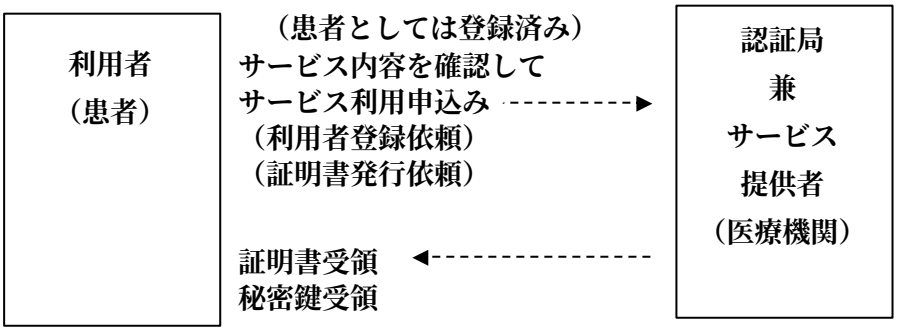


図 2-4 証明書の登録発行

証明書の登録・発行における利用者からの要件を以下に示す。

① サービス提供者の信頼性

診療情報を含む個人情報を既に診療等を通じて医療機関に提供済みであるから、サービス利用申込みの前に、これらの情報の保護を確実に行う管理がされているサービスであること。

ａ）運用管理規程の策定：運用管理規程が定められていること

ｂ）診療録の取扱い：診療録の適切に保護されていること

ｃ）証明書格納媒体の取扱い：サービスを利用する上での証明書が安全確保されていること。

② サービスの利便性

サービスの利用条件及びサービス内容から、利用できる時間や場所が、自身の利用スタイルを満足するものであること。

ａ）サービス時間：利用可能な時間が明確になっているか。工事等による利用不可の場合は、事前に連絡があるか。

ｂ）利用端末の設置場所：当該医療機関内だけか又は近隣の連携する医療機関内にも設置されているか。希望すれば利用者の自宅にも設置可能か。

ｃ）利用環境の構築：希望すれば利用者の自宅に利用環境（通信環境、PC 環境等）が構築できるか。比較的安価に構築できるか。

(2) サービス利用（サイトの確認）

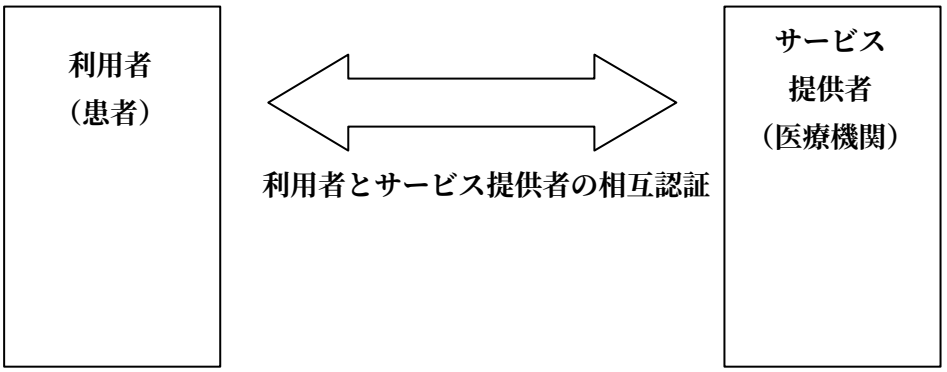


図 2-5 サービス利用（サイトの確認）

サービス利用（サイトの確認）における利用者からの要件を以下に示す。

① サービス提供サイトの信頼性

サービス利用を開始するために、サービス提供のサイトにアクセスし、サイトの証明書を検証して当該サイトが正しいサイトであることが確認できること。

ａ）サイトの証明書

ｂ）患者の証明書

② サービスの利便性

サイトのトップページ内容、利用者の識別結果の表示等から、視覚的に正しいサイトであることが確認できること。

ａ）ドメイン名：サービス提供者又はサービス内容を表すドメイン名か。

ｂ）サイトのトップページ：サービス提供者及びサービス内容がわかる内容か。

ｃ）利用者の識別：サイトにアクセス時、アクセスした利用者が、正しいサイトにアクセスできたことを確認できること。

(3) サービス利用（診療記録の閲覧）

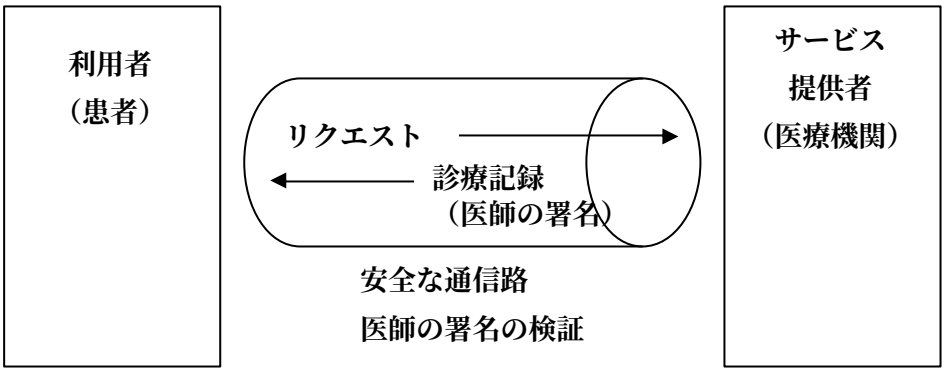


図 2-6 サービス利用（医療記録の閲覧）

サービス利用（診療記録の閲覧）における利用者の要件を以下に示す。

① サービス提供サイトの信頼性

医療機関の間で安全な通信路が形成され、情報の機密性が確保されていることまたサービス結果である診療記録の医師の署名を検証することによって、正確かつ最新の内容であること。

ａ）患者の証明書

ｂ）サイトの証明書

ｃ）安全な通信路

ｄ）医師の署名の検証

② サービスの利便性

「(1)証明書の登録・発行」において机上で確認した要件が実機上で守られていることが確認できること。

ａ）サービス時間：サービス条件で示された時間に確実に利用できるか。

ｂ）利用場所：サービス条件で示された場所（当該医療機関、連携する医療機関、自宅等）で利用できるか。

ｃ）利用環境と構築：サービス条件に従って構築した利用環境（通信環境、PC 環境等）を使ってサービスが利用できるか。

ｄ）利用環境の構築費用：利用環境の構築に要した費用は想定した範囲内か。

(4) 証明書の更新

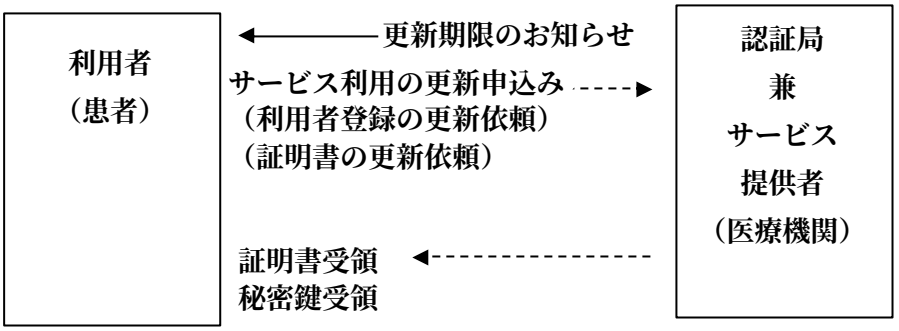


図 2-7 証明書の更新

証明書の更新における利用者の要件を以下に示す。

① サービス提供者の信頼性

継続してサービス利用を受けるにあたって、「(1)証明書の登録・発行」で確認した要件が、同様に守られることが確認できること。

ａ）運用管理規程

ｂ）個人情報保護

ｃ）診療記録の取扱い

ｄ）患者の証明書の要件

② サービスの利便性の確保

利用者（患者）が、継続してサービス利用を受けるにあたって、「(1)証明書の登録・発行」で確認した要件が、同様に守られることが再度確認できること。またサービスの更新処理では、十分な期間があり、簡便な手続でできること。

ａ）サービス時間

ｂ）利用端末の設置場所

ｃ）利用環境の構築：構築した利用環境が継続して利用できるか。

ｄ）利用端末の構築・維持費用：更新にあたって追加の費用が発生するか。

ｅ）旧証明書の取扱い

ｆ）証明書の更新期限

ｇ）証明書の更新手続

(5) 証明書の失効

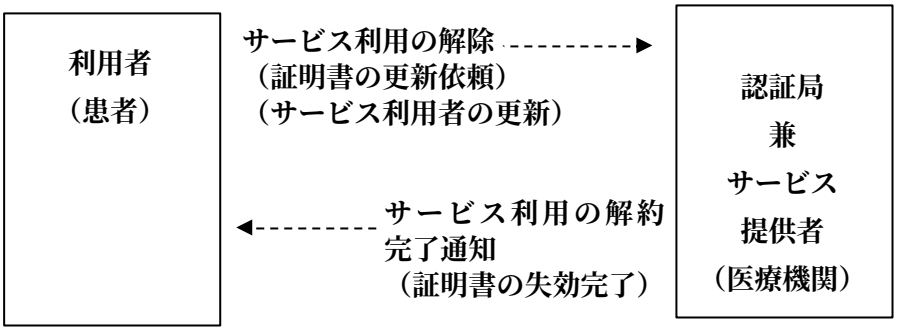


図 2-8 証明書の失効

証明書の失効における利用者の要件を以下に示す。

① サービス提供者の信頼性

サービス利用の解約によって、利用者登録が削除され、証明書の失効が確実に完了したことが確認できること。また将来的にサービス利用を再開する場合に対応してそれまで診療記録が保護され維持されることを確認できること。

ａ）患者の証明書

ｂ）Web サイトの証明書

ｃ）医師の証明書

② サービスの利便性の確保

サービスの失効では、簡便な手続でできること。

ａ）旧証明書の取扱い

ｂ）証明書の更新期限

ｃ）証明書の失効手続

2.5.1.3 利用者の留意事項

利用者（患者）は、前記にような要件において留意すべき事項を以下に提示する。

表 2-1 利用者の留意事項

	確認の視点	確認事項	脅威
①	サービスの運用	・運用管理規程の策定	・不正行為
②	利用者に求められる情報開示	・個人情報取扱いポリシー	・個人情報の流用 ・機密度が高い個人情報の流出
③	証明書の取扱い	・証明書格納媒体の取扱い ・患者の証明書	・経年劣化 ・許可使用、改ざん、紛失、盗難、
④	サイトの信頼性	・評判・実績 ・サイトの証明書	・実績作り後の詐欺行為 ・不正サイトへの誘い込み ・不正アクセス、改ざん、紛失 ・通信路からの侵入

① 運用管理規程の策定

診療録等を電子媒体で保存する場合には、平成 11 年 4 月の厚生省通達により、運用管理規程を定めることとなっている。利用者（患者）は、サービス提供者によって本サービスの運用管理規程が定められていることを確認すべきである。可能ならば当該運用管理規程が利用者にも公表されていることが望ましい。

（平成 11 年 4 月 22 日付け厚生省通知「診療記録等の電子媒体による保存について」3. 留意事項(1)(2)参照）

② 個人情報（診療録）取扱いポリシー

サービス提供者である医療機関が診療録を取扱うにあたっては、刑法及び医療関係法規によって診療に係る情報が保護されるように定められている。利用者はサービス提供者が提示する診療録取扱いポリシーを確認するとともに以下の項目がどのように実現されているかを確認するべきである。

- 正確性の確保：作成・更新の日時・医師名・内容等が確認できること
  （医師法第 24 条等参照）
- 目的外の使用制限：患者の同意なく診療以外の目的で使用されないこと
- 第三者提供の制限：患者の同意なく第三者へ提供しないこと
- 使用履歴の開示：患者の求めに応じて使用履歴を開示できること

③ 証明書の取扱い

ａ）IC カードの利用

利用者自身の秘密鍵及び証明書を格納する媒体は、安全性及び携帯性の高い IC カードであることが望ましい。

ｂ）証明書の取扱説明書の配布

利用者が証明書格納媒体を正しく使用できるようにするため、証明書格納媒体の使用に関する利用者向け取扱説明書が配布されることが望ましい。取扱説明書には適切な使用方法だけでなく、他人への貸与を禁止する等の禁止・注意事項も記載されるべきである。

ｃ）利用者向け教育の実施

利用者向け取扱説明書の配布だけでは利用者に正しい使用方法を十分徹底できない場合は、利用者向けの教育を実施することが望ましい。

ｄ）IC カードの使用に対するセキュリティ機能

利用者が IC カードを使用するにあたり、IC カードを挿入している時のみログオンを可能とするログオン制御機能、サービス利用中の離席時に IC カードを抜くことによりキーボードの操作や画面の盗み見などを防止するスクリーンロック機能、PC のシャットダウン時に IC カードの抜き忘れを知らせる警告機能などを選定することが望ましい。

④　患者の証明書

患者の証明書の記載事項は、患者の求めに応じて氏名非開示等が選択できることが望ましい。

⑤　サイトの証明書

利用者（患者）が、アクセスしたサイトが目的のサイトであることを利用者自身の知識にだけ頼って行うことは困難である。利用者が多種多様な患者であることを考えれば、利用者が意識せずに正しいサイトであることを確実かつ迅速に行うための機能が提供システムに組み込まれていることがいることが望ましい。

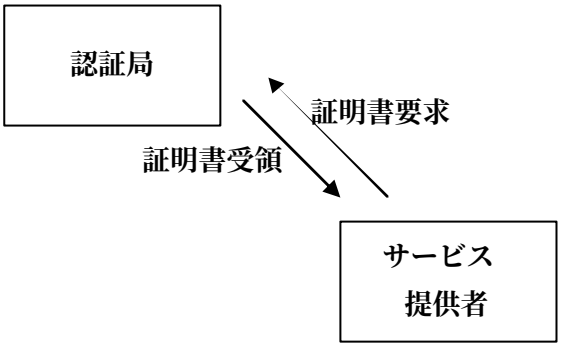
2.5.2 インターネットショッピング

(1) サーバ証明書のみを利用するサービス例

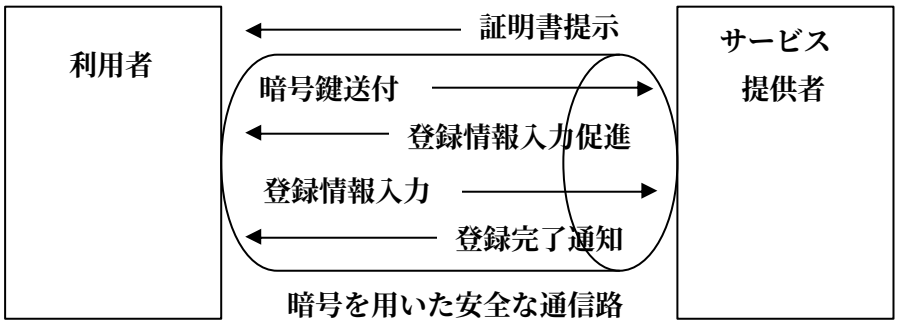
小額決済が中心のインターネットショッピングサイトにおける一般的な証明書の利用形態であり、証明書はサービス提供者側からのみの提示となる。

３つのフェーズからなり、第１フェーズは、サービス提供者が認証局から証明書を取得する。第２フェーズは利用者がサービス提供者に対して利用者登録を行う。第３フェーズは利用者がサービスを利用する。というものである。

・第１フェーズ（サービス提供準備）



・第２フェーズ（サービス利用者登録）



・第３フェーズ（サービス利用）

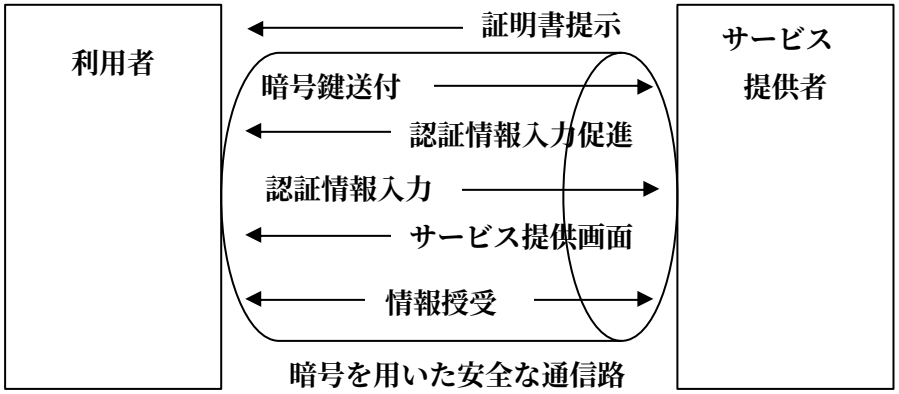


図 2-9 実現モデル例（インターネットショッピングその１）

サーバ証明書のみを用いたサービスの提供では、利用者の認証にはID＋パスワードで対応することが一般的であり、なりすましによるリスクは利用者、サービス提供者、決済確認者に分散され、それぞれ納得の上でサービスが成り立っている。

この方式によれば、利用者は個別のソフトウェアや認証情報を新たにインストールする必要もなく、ブラウザのみでサービスを受けることが可能であるため、利用者負担が少なく、サービス提供者にとっても利用者を集めやすいという利点がある。

このようなサービスの利用者が払うべき留意点を以下に述べる。

① サービス提供サイトの信頼性
- 評判、実績
- ドメイン名
- 証明書記載内容

② 利用者登録における登録情報の妥当性
- 個人情報取扱ポリシー
- 登録必須の属性情報項目

③ ID＋パスワードの厳密な保管
- メモ、通知メールの保存状態
- ブラウザ上の自動入力設定の有無

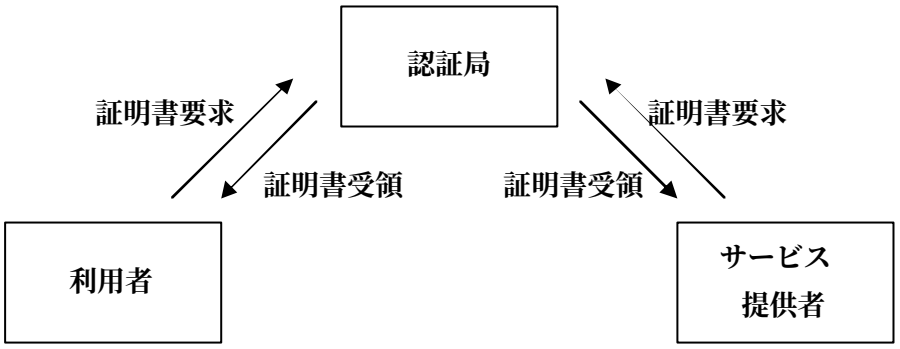
④ 決済方法の選択
- 現金送付
- クレジットカード番号入力
- 宅配業者の商品代引き

⑤ リスクの受容
- 商品の不着
- 決済のみの完了
- なりすまし被害
- 決済情報を含む個人情報の流用

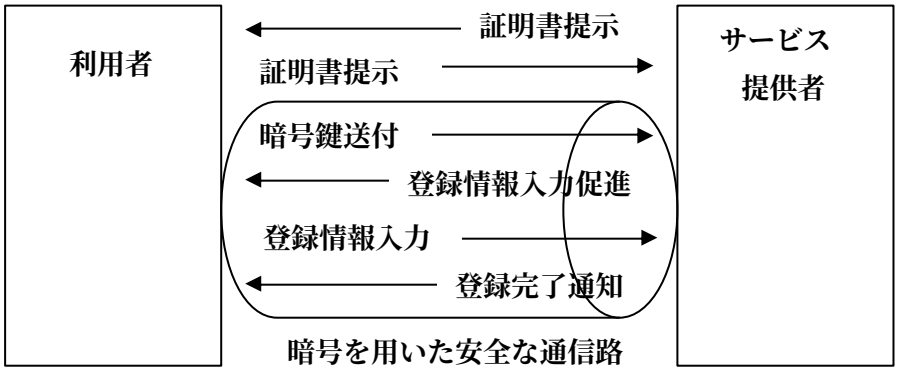
(2) 利用者、サービス提供業者がともに証明書を利用するサービス例

決済額が高額なサービスや機密情報に係るサービスにおいては、サービス提供者が利用者を限定したり、特定組織や提携相手のみをサービス範囲とすることがある。また、利用者にとっては信頼できるサイトのサービスをなりすましによる被害の心配なく利用したいという要望も多くある。利用者証明書による認証機構はこういった要望に応えるものである。

・第１フェーズ（サービス利用・提供準備）



・第２フェーズ（サービス利用者登録）



・第３フェーズ（サービス利用）

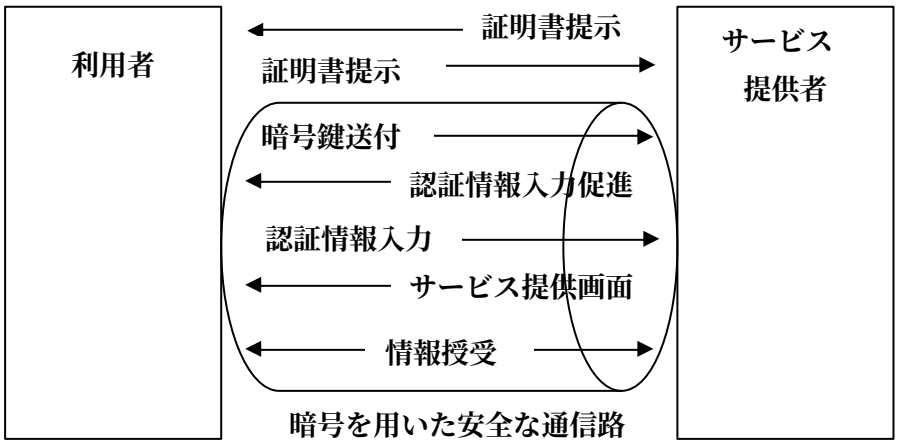


図 2-10 実現モデル例（インターネットショッピングその２）

サーバ証明書＋利用者証明書を用いたサービスの提供では、サービス提供サーバと、アクセスしてきた利用者との間で証明書の交換が行われ、互いに信頼できる認証局の発行する証

明書であることを確認する。秘密鍵の運営方法しだいで ID＋パスワード方式に比較して非常に高い安全性の確保が可能となる。

この方式によれば、利用者はサービス利用の前にサービス提供者の指示に従い、証明書の取得をする必要があり、取得した証明書と証明書に対応する秘密鍵をブラウザ等のアプリケーションプログラムから利用するための準備作業を行うことが必要となる。

PKI に基づく相互認証が行われるため、利用者が誤って不正サイトへアクセスしたり、利用者のアクセス権を､他人がなりすましによって不正利用することを防ぐことが可能となる。

秘密鍵の取り扱いによる安全性の振れを以下に示す。

表 2-2 秘密鍵の取り扱い

格納媒体	アクセスの必要条件	安全性
FD	FD 携帯 秘密鍵へのアクセスパスフレーズ	低：コピー可、書込み可
CD-ROM	CD-ROM 携帯 秘密鍵へのアクセスパスフレーズ	中：コピー可
HDD	秘密鍵へのアクセスパスフレーズ	低～中 :PC 利用権限に依存
IC カード等 （タンパフリー）	IC カード携帯 IC カードR/W デバイス 秘密鍵へのアクセスパスフレーズ	高：コピー不可 IC カード等を保有している限り安全が確保される

２つの代表的な証明書取得手続きについて以下に述べる

○ 利用者の鍵生成に基づく証明書取得手続き

- 利用者が自分の PC において鍵生成ツールを起動し秘密鍵と公開鍵の鍵ペアを生成する
- 秘密鍵を安全に保管した上で、公開鍵と求められる個人情報に署名を行い、認証局へ安全なルートで送付する
- 公開鍵に認証局の署名がついて証明書として返送される証明書を保管する

○ 証明書発行者による鍵生成に基づく証明書取得手続き

- 利用者が証明書発行者へ、求められる個人情報とともに証明書発行要求を行う
- 証明書発行者が、鍵ペアと証明書を生成の後、定められた媒体に格納し利用者へ安全に配送する。
- 利用者は秘密鍵及び証明書を受け取り保管する

このようなサービスの利用者が払うべき留意点のうち、サーバ証明書のみを利用するサービスにはないものを以下に述べる。

① 証明書取得手順

- 鍵ペアの生成方法

- 秘密鍵格納方法
- 証明書取得方法

② 証明書利用規程

- 証明書の取得（利用）価格
- 証明書の有効期限
- 証明書取得手続き
- 証明書更新手続き
- 証明書実行手続き

③ PIN（秘密鍵活性化に要するパスフレーズ）の厳密な保管

- メモ、通知メールの保存状態

(3) インターネットショッピング利用におけるリスクの低減

インターネットショッピング利用における現実的なリスクを以下に示す。

①個人情報の流出
②商品の不着
③不良品の受領
④未注文品の受領
⑤未注文品の決済

利用者はこれら現実的なリスクの存在を認識しながら、インターネットショッピングを利用する必要があり、購入等においては、これらのリスクに見合ったサービスを選択しリスクを受容しなければならない。

サービス利用に当たっては以下の視点で安全性の確認が必要となる。

①Web サイトの信頼性
②利用者に求められる情報開示
③証明書取得手順
④証明書利用規程
⑤利用者認証情報
⑥決済方法の選択

表 2-3 確認の視点

確認の視点	確認事項	脅威
Web サイトの信頼性	・評判、実績 ・サーバ証明書署名者	・実績作り後の詐欺行為 ・不正サーバへの誘い込み
利用者に求められる情報開示	・個人情報取扱ポリシー ・情報開示の必然性	・個人情報の流用 ・機密度が高い個人情報の流出
証明書取得手順	・鍵ペアの生成方法 ・利用者証明書署名者	・不正秘密鍵／証明書の配布 ・機密性、完全性の崩壊
証明書利用規程	・証明書利用範囲 ・利用者の責任 ・賠償と免責	・危殆化による被害範囲の拡大 ・紛失、不注意によるなりすまし ・利用者責任に対する賠償問題
利用者認証情報	・ID や PIN の配送と管理	・配送の落ち度による鍵の危殆化
決済方法の選択	・決済手段のﾊﾞﾘｴｰｼｮﾝ （現金送付、ｸﾚｼﾞｯﾄｶｰﾄﾞ、宅配代引き、ｴｽｸﾛｳ）	・支払いと引渡しの非同期

上表を参考に、存在する脅威が生むリスクを、確認事項に沿ってできるだけ低減させる努力をした上で、サービスの利用を決定するよう推奨する。このとき、サービス利用による恩恵と、リスクの大きさによって判断することも必要となろう。特に最悪の状況に陥った場合の対応を想定しておくことは重要である。なお上記のうち、利用者証明書を使わないインターネットショッピングにおいては、証明書取得手順及び証明書利用規程は確認対象とならない。

ここで再度、現実的なリスクについて考えてみる。もっとも大きなリスクは「未注文品の決済」である。「商品の不着」、「不良品の受領」、「未注文品の受領」は一過性のものと考えることができるが、「未注文品の決済」と「個人情報の流出」については、一過性とは考えられず、継続した被害の発生を想定しなくてはならない。しかし「個人情報の流出」は被害額に直結するものではないため、「未注文品の決済」により大きなリスクがあると考える。

これらをもとに、インターネットショッピング利用に当たっての安全確保に向けた確認手順を考えてみる。なお、利用者証明書を使わないインターネットショッピングにおける確認事項は（6）までである。

① Web サイトの評判・実績

非常に知名度の高いサイトであれば確認は容易であるが、一般的にはこの部分について絶対的な確認方法はない。したがって可能な限りの調査を実施することとなる。場合によっては実際に先方の会社を訪ねての確認も考えられる。

② 決済手段のバリエーション

一般的に信頼できるサイトは複数の決済手段を準備しており、各決済方法に応じた確認事項が存在する。

ａ）現金送付

一般的に支払い後の商品送付であるため、商品不着の可能性があり、十分信頼できるサイトでないかぎり利用を控えることを推奨する。特にオークションサイトにおいては十分な確認が求められる。ただし、エスクロウサービスが整備されている場合にはリスクの低下を計算することができる。（エスクロウサービスとは、個人間の取引の仲立ちにより、商品と代金が確実に交換できることを保証するシステムである）

ｂ）クレジットカード

クレジットカード番号をネットワークに流すため、渡す相手であるサービス提供者の信頼性はもちろんのこと、通信経路の安全性についても十分な確認が必要である。一度とられたクレジットカード番号は、繰り返し悪用される可能性が高く、利用者は事前の確認と共に、クレジット利用明細による事後の確認をおろそかにしてはならない。

ｃ）宅配代引き

商品受領と代金の支払いが同時でしかも直接受け渡しであるため、安全性は高いといえるが、「不良品の受領」というリスクは持っているため、サービス提供者の評判や実績を十分確認しておくことで、高い安全性を得ることができる。

③ 個人情報取扱ポリシー

何らかのサービスを利用する場合、ほとんどのケースで個人情報の登録といったことを求められる。その際、通常はこの集めた個人情報の取扱方法について宣言が提示してあるので、この内容を必ず熟読し個人情報の流用について確認しておく必要がある。なお、こういった宣言がないサイトの利用は控えることを推奨する。

④ 情報開示の必然性

前述した通り、サービス利用の前に求められる個人情報の登録に際しては、求められる情報の必然性と取扱方法について十分な確認をし、利用するサービスの恩恵に見合わない情報の開示を求められた場合にはその利用を控えることを推奨する。

⑤ ID や PIN の配送と管理

ID や PIN の配送方法では、これらの情報に対する重要性の認識が求められるが、ID と PIN を通常の電子メールにて送付するといったケースも見受けられるため、こういった意識の低いサービス提供者からのサービスを利用する際には、リスクを高めに見積もっておく必要がある。

⑥ サーバ証明書署名者

サーバ証明書については、一般的に信頼されている認証業者の署名がついていれば、サ

ービス提供者の存在等に対するチェックはなされていることから、ある程度の信頼性を認めることができる。独自に作成した証明書等が利用されているような場合には、警戒を要する。

⑦　鍵ペアの生成方法

証明書取得に当たって、鍵の生成から証明書作成までをサービス提供者側にて行い、利用者に秘密鍵と証明書が送付されてくるケースがあるが、同じ鍵が不当に使われていれば証明書を利用するシステムにおいて、けっしてあってはならない「なりすまし」が発生することになるため、配送方式に注意の上、信頼の確認できないサービス提供者への登録ではリスクを高めに見積もっておく必要がある。

⑧　証明書利用範囲

取得する証明書の利用範囲を確認し、利用範囲における最大のリスク額をもとに利用を考える必要がある。証明書を取得することにより、多くの必要以上のサービスが利用可能となった場合、何らかの事故・事件による利用者の被害額が飛躍的に拡大する恐れがあるので、利用範囲をコントロールできる場合には必要な範囲に留めることを推奨する。

⑨　利用者の責任

利用者の秘密鍵が利用者の過失により危殆化した場合､速やかな対処が図られない場合、それに基づく損害を被る可能性がある。一般的に秘密鍵の管理は利用者責任であるため、秘密鍵の危殆化が判明した場合の対処法（証明書の失効手続き）について明確な提示があることを理解しておく必要がある。

⑩　賠償と免責

秘密鍵の危殆化が原因となって他者に与えた損害への賠償や、自身の故意によって他者に与えた損害への賠償が発生することがあり得るため、規約等を熟読し納得のいくものであることを確認しておく必要がある。

⑪　利用者証明書署名者

利用者証明書が一般的に信頼されている認証業者の署名がついていれば、サービス提供者の存在等に対するチェックはなされていることから、ある程度の信頼性を認めることができる。独自に作成した証明書等が利用されているような場合には、警戒を要する。

以上のような確認項目に沿って、サービス提供者の信頼性を把握し、利用するサービスによる恩恵とリスクとを見比べることにより、リスクを受容することができればサービスの利用を開始することができる。もし、リスク値が期待値よりも高い場合にはリスク低減が確認できるまで利用を控えることを推奨する。

2.5.3 教育分野

(1) 想定する証明書利用場面

ここでは、大学における証明書利用場面を取り上げる。図 2-11 に大学における証明書利用場面を示す。

① IC カード学生証の発行

入学時あるいは学生からの申請などにより大学から学生に IC カード学生証を発行し、配布する。

② IC カード学生証の利用

IC カードには、氏名、生年月日、大学名、学部学科、有効期間などが記されている。IC カード内には、秘密鍵や証明書が入っている。

学生はこの IC カードを用いて大学の種々のサービスを利用する。大学においては学生に対して図書貸出、成績証明書などの各種証明書発行、オンライン試験などのサービスを提供し、大学側としては学生の出席管理、入退出管理などを行っている。

学生がこれらのサービスを受ける時に、IC カード内の証明書を用いて学生の本人認証が行われる。

③ IC カード学生証の更新

IC カード内の証明書の有効期間が切れたときなどに、証明書が更新され、新しい秘密鍵と証明書が入れられる。

④ IC カード学生証の失効

学生が退学、除籍、転学部、転学科などした場合は証明書が失効される。また、IC カードが盗難にあったり紛失した場合にも証明書が失効される。

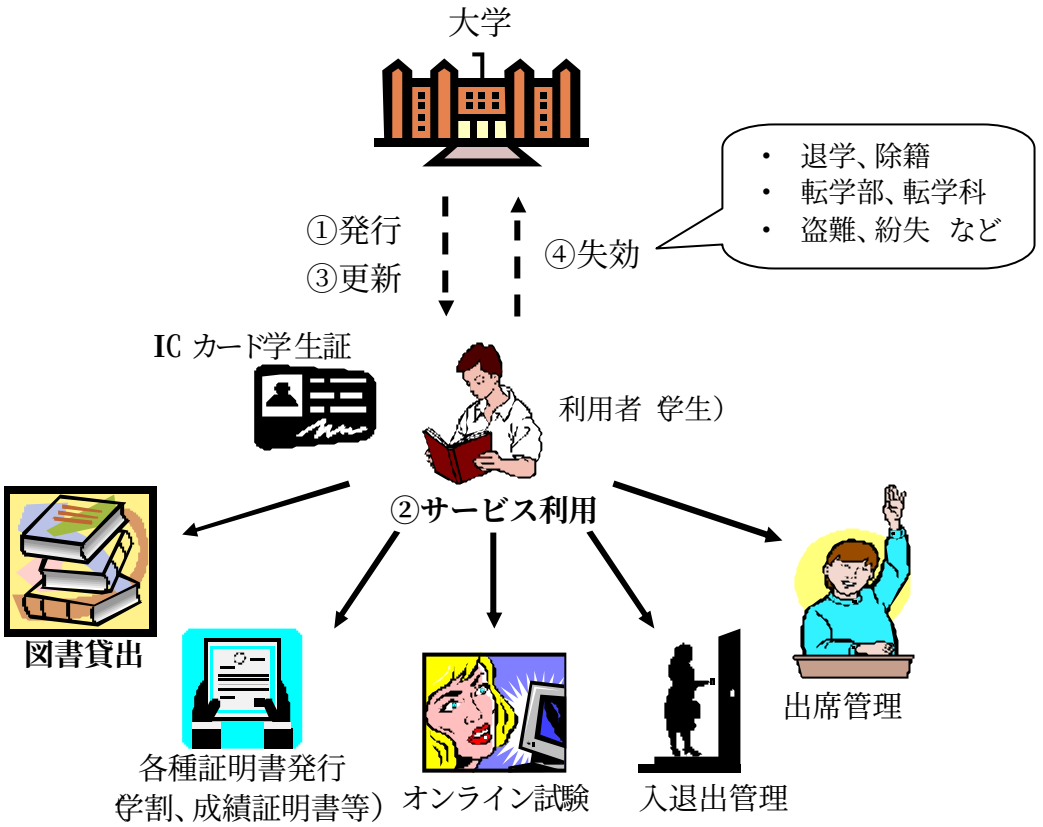


図 2-11 大学における証明書利用場面

(2) 留意点

利用者がサービスを受ける際の留意点を以下に示す。

① 現実的なリスク

利用者はこれら現実的なリスクの存在を認識しながら、サービスを利用する必要がある。

ａ）個人情報の流出

サービス提供者側（大学）から利用者（学生）の個人情報が漏れてしまう危険性がある。また、サービス提供者側からのみでなく、利用者自身が自分の個人情報を漏らしてしまう危険性がある。

ｂ）なりすまし

他人が自分の名前をかたってサービスを受ける危険性がある。

ｃ）IC カード学生証の紛失

IC カード学生証を紛失すると、大学からのサービスが受けれなくなるため、大学生活に重大な支障が出る。

また、a)b)に関係あるが、IC カード学生証を紛失することにより、誰かが利用者になりすましてサービスを受けたり、利用者が不利になる行動をされる危険性がある。

② サービス利用時の注意点

サービス利用に当たっては以下の視点で安全性の確認が必要となる。

ａ）証明書利用規程

ｂ）利用者認証情報

ｃ）Web サイトや機器の信頼性

ｄ）証明書取得手順

ｅ）利用者に求められる情報開示

ｆ）決済方法の選択

表 2-4 確認の視点２

	確認の視点	確認事項	脅威
a)	証明書利用規程	・証明書利用範囲 ・利用者の責任 ・賠償と免責	・危殆化による被害範囲の拡大 ・紛失、不注意によるなりすまし ・利用者責任に対する賠償問題
b)	利用者認証情報	・ID や PIN の配送と管理	・配送の落ち度による鍵の危殆化
c)	Web サイトの信頼性	・評判、実績 ・サーバ証明書署名者	・実績作り後の詐欺行為 ・不正サーバへの誘い込み
d)	証明書取得手順	・鍵ペアの生成方法 ・利用者証明書署名者	・不正秘密鍵／証明書の配布 ・機密性、完全性の崩壊
e)	利用者に求められる情報開示	・個人情報取扱ポリシー ・情報開示の必然性	・個人情報の流用 ・機密度が高い個人情報の流出
f)	決済方法の選択	・決済手段のﾊﾞﾘｴｰｼｮﾝ（現金送付、ｸﾚｼﾞｯﾄｶｰﾄﾞ、宅配代引き、ｴｽｸﾛｳ）	・支払いと引渡しの非同期

上表を参考に、存在する脅威が生むリスクを、確認事項に沿ってできるだけ低減させる努力をした上で、サービスの利用を決定するよう推奨する。このとき、サービス利用による恩恵と、リスクの大きさによって判断することも必要となろう。特に最悪の状況に陥った場合の対応を想定しておくことは重要である。なお上記のうち、利用者証明書を使わないサービスにおいては、証明書取得手順及び証明書利用規程は確認対象とならない。

ここで再度、現実的なリスクについて考えてみる。もっとも大きなリスクは「個人情報の流出」である。「なりすまし」や「IC カード学生証の紛失」は IC カード学生証や証明書を失効すれば良く、一過性のものと考えることができるが、「個人情報の流出」については、一過性とは考えられず、継続した被害の発生を想定しなくてはならない。

(3) 安全確保に向けた確認手段

これまでの検討をもとに、大学におけるサービス利用に当たっての安全確保に向けた確認手順を考えてみる。

インターネットショッピングの確認手順とほぼ同様であるが、大学から学生に向けたサービスであるため、ほとんどのサービスにて決済が発生しない点が特徴的なものである。

① 個人情報取扱ポリシー

何らかのサービスを利用する場合、ほとんどのケースで個人情報の登録といったことを求められる。その際、通常はこの集めた個人情報の取扱方法について宣言が提示してあるので、この内容を必ず熟読し個人情報の流用について確認しておく必要がある。なお、こういった宣言がないサイトの利用は控えることを推奨する。

② 情報開示の必然性

前述した通り、サービス利用の前に求められる個人情報の登録に際しては、求められる情報の必然性と取扱方法について十分な確認をし、利用するサービスの恩恵に見合わない情報の開示を求められた場合にはその利用を控えることを推奨する。

③ ID や PIN の配送と管理

ID や PIN の配送方法では、これらの情報に対する重要性の認識が求められるが、ID と PIN を通常の電子メールにて送付するといったケースも見受けられるため、こういった意識の低いサービス提供者からのサービスを利用する際には、リスクを高めに見積もっておく必要がある。

④ サーバ証明書署名者

サーバ証明書については、一般的に信頼されている認証業者の署名がついていれば、サービス提供者の存在等に対するチェックはなされていることから、ある程度の信頼性を認めることができる。独自に作成した証明書等が利用されているような場合には、警戒を要する。

⑤ 鍵ペアの生成方法

証明書取得に当たって、鍵の生成から証明書作成までをサービス提供者側にて行い、利用者に秘密鍵と証明書が送付されてくるケースがあるが、同じ鍵が不当に使われていれば証明書を利用するシステムにおいて、けっしてあってはならない「なりすまし」が発生することになるため、配送方式に注意の上、信頼の確認できないサービス提供者への登録ではリスクを高めに見積もっておく必要がある。

⑥ 証明書利用範囲

取得する証明書の利用範囲を確認し、利用範囲における最大のリスク額をもとに利用を考える必要がある。証明書を取得することにより、多くの必要以上のサービスが利用可能となった場合、何らかの事故・事件による利用者の被害額が飛躍的に拡大する恐れがあるので、利用範囲をコントロールできる場合には必要な範囲に留めることを推奨する。

⑦　利用者の責任

利用者の秘密鍵が利用者の過失により危殆化した場合､速やかな対処が図られない場合、それに基づく損害を被る可能性がある。一般的に秘密鍵の管理は利用者責任であるため、秘密鍵の危殆化が判明した場合の対処法（証明書の失効手続き）について明確な提示があることを理解しておく必要がある。

⑧　賠償と免責

秘密鍵の危殆化が原因となって他者に与えた損害への賠償や、自身の故意によって他者に与えた損害への賠償が発生することがあり得るため、規約等を熟読し納得のいくものであることを確認しておく必要がある。

⑨　利用者証明書署名者

利用者証明書が一般的に信頼されている認証業者の署名がついていれば、サービス提供者の存在等に対するチェックはなされていることから、ある程度の信頼性を認めることができる。独自に作成した証明書等が利用されているような場合には、警戒を要する。

以上のような確認項目に沿って、サービス提供者の信頼性を把握し、利用するサービスによる恩恵とリスクとを見比べることにより、リスクを受容することができればサービスの利用を開始することができる。もし、リスク値が期待値よりも高い場合にはリスク低減が確認できるまで利用を控えることを推奨する。

2.6　まとめ

この章では、利用者の視点に立ち、証明書の利用に関する利用者の理解を深め、証明書利用の促進を目指すために、証明書利用の際に利用者が留意する事項、観点、利用者の要件、要件と留意する事項に対する対策を選択する判断基準を示した。

3．サービス提供者から見た属性情報活用ガイドライン

3.1　基本方針

本章では、サービス提供者が実現する証明書を用いたシステムを、ビジネスに合致したシステムにするため、証明書の利用方法とシステム設計のガイドラインを示す。

本章を読むに当たって、システムで利用する証明書は、例えば「単一目的証明書」にすると既に仮決定しているかもしれない。そして本ガイドラインは、その仮決定を決定に導くかもしれないし、他の証明書、例えば「特定目的証明書」に導くかもしれない。本ガイドラインによって導きだされた証明書の活用方法を、属性情報を効果的に活用する方法として参考にしてほしい。

本章は、まずサービス提供者が証明書を利用する場面である「加入（登録）時」と「利用時」での証明書の活用方法の組み合わせにより、属性情報活用パターンを整理する。次に、利用場面毎に運用手順を分析し利用される属性情報種別を整理する。そして、属性証明書活用パターンと属性情報種別から属性情報活用の実現モデルを提示する。最後に、これらの実現モデルをもとにしたシステム設計のガイドラインを提示する。

3.2　実現モデル

ここでは、１章で記述した属性の利用場面毎で、証明書を利用する登場人物と証明書の運用方法について整理し属性情報活用パターンを整理する。また利用場面毎に、サービス提供者側で行う運用手順を分析し活用される利用者の属性情報を分類する。そして、属性情報活用パターンと分類した属性情報から８つの実現モデルを提示する。

3.2.1　サービス提供者における属性情報活用パターン

１章や２章では、証明書を利用するときの役割を明確にするため、登場人物として「利用者」「認証局など」「サービス提供者」の三者を用いていた。しかし、サービス提供者が利用者の属性情報を活用するモデルには、図 3-1 および図 3-2 に示すように、証明書を発行する機関（認証局など）を、サービス提供者とは異なる第三者が運用している場合と、サービス提供者が運用している場合が考えられる。

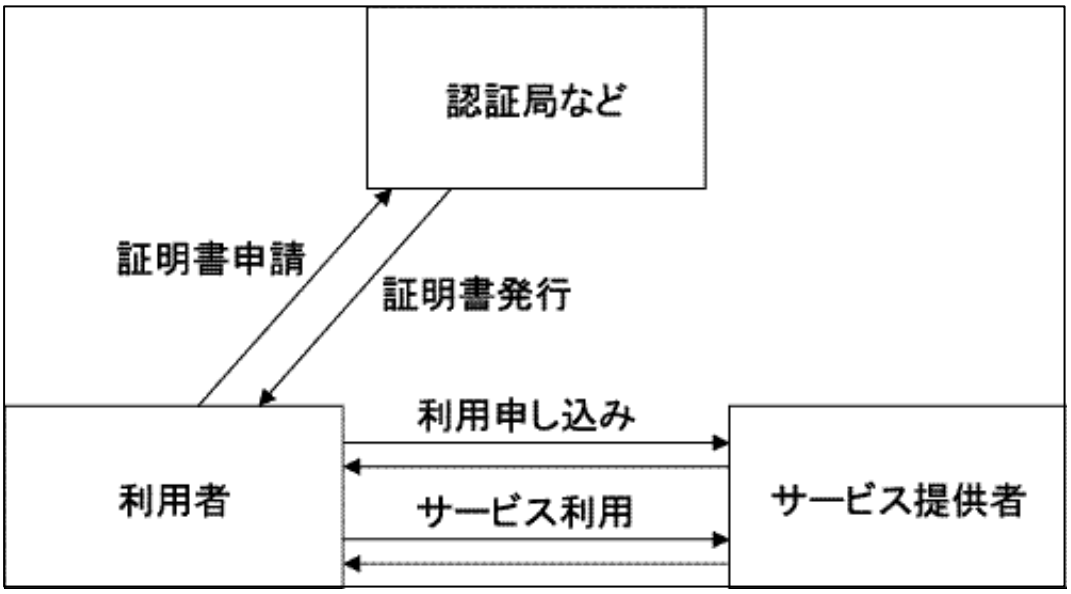


図 3-1 サービス提供者と認証局が異なる組織で利用者の属性情報を活用する場合

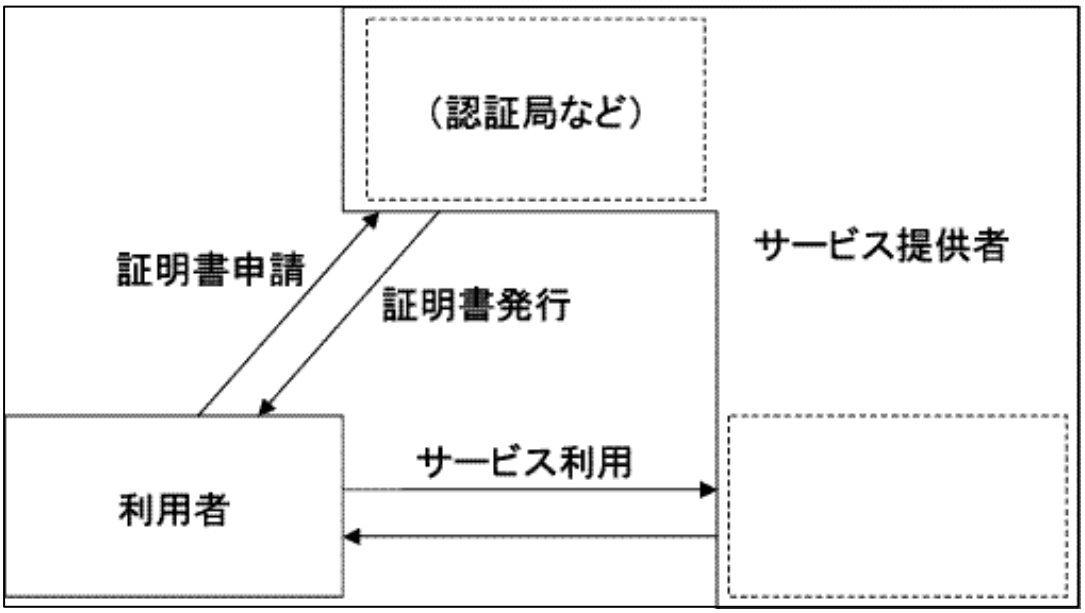


図 3-2 サービス提供者が認証局を運用して利用者の属性情報を活用する場合

一方、1.2 節で記述したように、サービス提供者が証明書を利用する場面として「加入（登録）時」と「利用時」がある。

このことから、利用者における証明書の活用方法は、表 3-1 に示すように３つの方法がある。ここで各活用方法を属性情報活用パターンとする。

表 3-1 認証局と証明書の利用場面の関係

		証明書の利用場面		利用者における証明書の活用方法	属性情報活用パターン
		加入（登録）時	利用時		
証明書を発行する認証局	第三者が運用	×	○	利用者は事前登録なしに所有している証明書を利用する	パターン１
		○	○	利用者は所有する証明書をサービス提供者に事前登録してから、サービス利用時に証明書を利用する	パターン２
	サービス提供者が運用	○	○	利用者はサービス提供者が発行した証明書を利用する	パターン３

次に、サービス提供者で活用される利用者の属性情報を整理するため、属性情報活用パターンでの「加入（登録）時」「利用時」それぞれに対して、証明書の運用から内容を詳細に検討する。

「加入（登録）時」に関しては、利用者の加入（登録）目的によって、「サービスの利用ができる証明書を入手するため」の加入（証明書を発行する運用）と「既存の証明書をサービスで利用できるようにするため」の登録（証明書を登録する運用）に分類する。

また「利用時」に関しては、利用者がサービスを利用する前提条件によって、「証明書のみで利用者を確認する運用」と「証明書と事前情報により利用者を確認する運用」に分類する。

属性情報活用パターンとこれら４つの関係を表 3-2 に示し、各パターンについて詳細を以下に示す。

表 3-2 属性活用パターンと利用場面の関係

属性活用パターン	証明書の利用場面	
	加入（登録）時	利用時
パターン１	－	証明書のみで利用者を確認する運用
パターン２	証明書を登録する運用	証明書と事前情報により利用者を確認する運用
パターン３	証明書を発行する運用	

3.2.1.1 証明書を発行する運用

この「証明書を発行する運用」は、後日利用者がサービスを利用するため、サービス提供者がサービス専用の証明書発行を行う運用である。

利用者とサービス提供者との手順、フロー図および手順に必要となる利用者の属性情報を以下に整理する。なおサービス提供者が利用者の本人確認を行う場合、サービスに関係しない本人認

証用の証明書が利用されても良い。

(1) 利用者とサービス提供者との手順

証明書を発行する運用における、利用者とサービス提供者との手順を以下に示す。

1．利用者はサービス提供者へ証明書発行申請を行う

2．サービス提供者は申請書により利用者の本人性・資格を確認する。さらに必要な場合は申請書をもとに外部から利用者情報を取得することにより利用者の本人性・資格を確認する

3．サービス提供者は申請書によりサービス利用における登録情報を確認（審査）する

4．サービス提供者は証明書を作成する

5．サービス提供者は利用者からの申請書および審査で付加した情報を保存する

6．サービス提供者は利用者に対して 4.で作成した証明書を発行する

(2) フロー図

証明書を発行する運用における、利用者とサービス提供者とのフロー図を以下に示す。

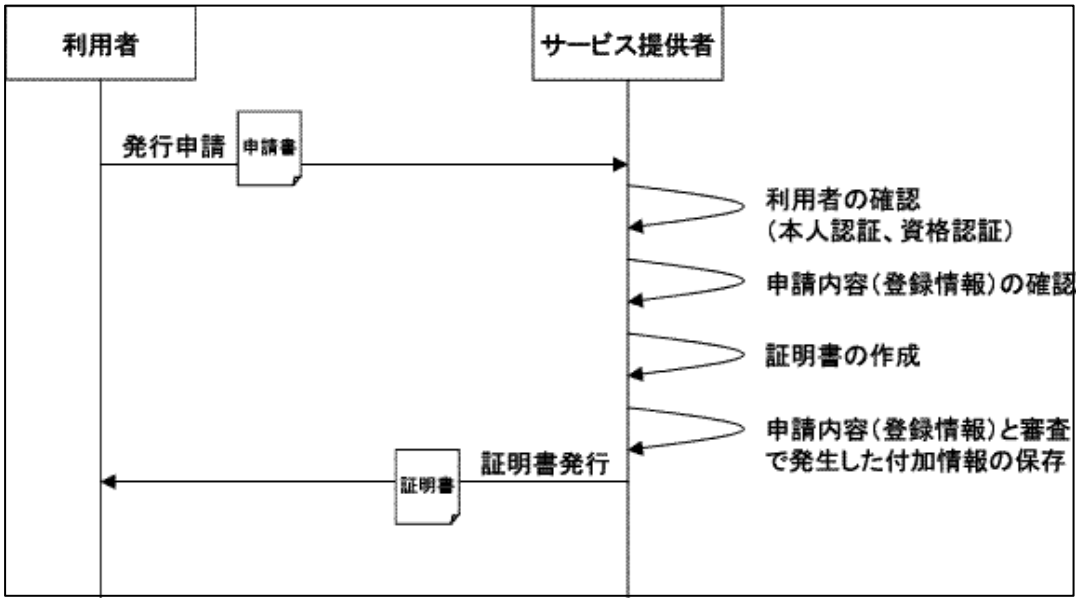


図 3-3 証明書を発行する運用フロー

(3) 手順に必要となる利用者の属性情報

証明書を発行する運用で必要となる属性情報を以下に示す。なお本運用における利用者の本人証明情報、資格情報の入手先は、経路の違いにより利用者本人と外部機関が考えられる。

表 3-3 証明書を発行する運用で必要となる利用者の属性情報

項番	運用フェーズ	属性情報	概要
1	発行申請	本人証明情報、資格情報	利用者がサービス提供者へ提示する本人証明情報や資格情報
2		証明書発行に関する登録情報	上記以外の証明書発行に必要となる情報
3	審査	本人証明情報、資格情報	サービス提供者が外部機関から入手する利用者の本人証明情報や資格情報
4		審査で発生した付加情報	サービス提供者内で発生した利用者情報
5	証明書発行	利用者の証明情報	利用者のサービス利用時に、サービス提供者が管理する利用者情報と利用者を関連づける情報

3.2.1.2　証明書を登録する運用

この「証明書を登録する運用」は、後日利用者がサービスを利用するため、サービス提供者が利用者から保有する証明書の登録を行う運用である。

利用者とサービス提供者との手順、フロー図および手順に必要となる利用者の属性情報を以下に整理する。

(1) 利用者とサービス提供者との手順

証明書を登録する運用における、利用者とサービス提供者との手順を以下に示す。

1．利用者は保有する証明書とともにサービス提供者へ証明書登録申請を行う
2．サービス提供者は証明書を確認し利用者の本人性・資格を確認する。さらに必要な場合は証明書や申請書をもとに外部から利用者情報を取得することにより利用者の本人性・資格を確認する
3．サービス提供者は申請書によりサービス利用における登録情報を確認（審査）する
4．サービス提供者は利用者からの申請書、証明書および審査で付加した情報を保存する
5．サービス提供者は利用者に対して登録結果を通知する

(2) フロー図

証明書を発行する運用における、利用者とサービス提供者とのフロー図を以下に示す。

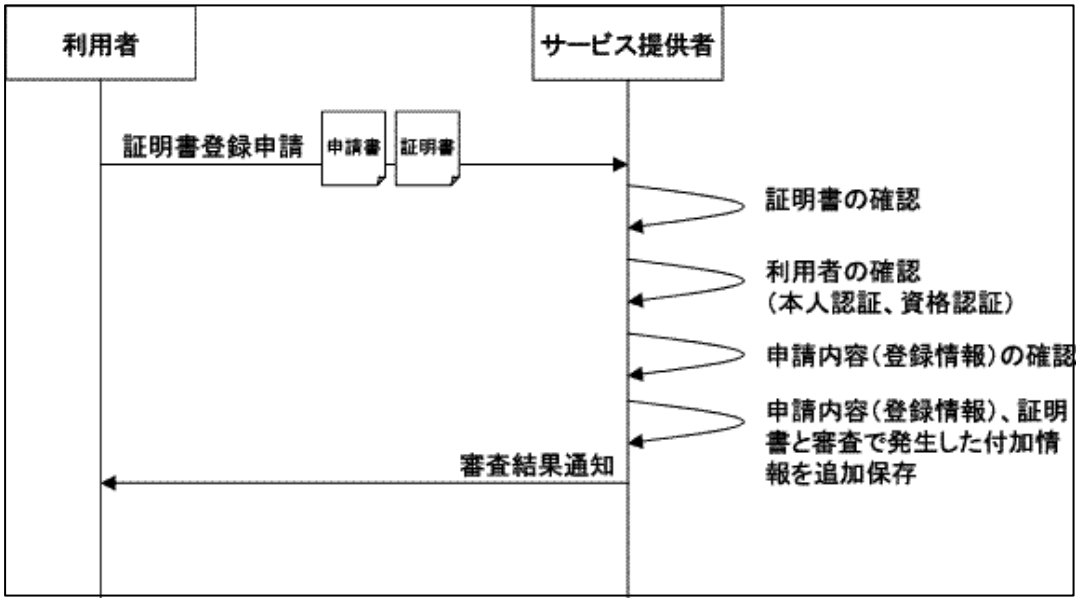


図 3-4 証明書を登録する運用フロー

(3) 手順に必要となる利用者の属性情報

証明書を登録する運用で必要となる属性情報を以下に示す。なお本運用における利用者の本人証明情報、資格情報の入手先は、経路の違いにより利用者本人と外部機関が考えられる。

表 3-4 証明書を登録する運用で必要となる利用者の属性情報

項番	運用フェーズ	属性情報	概要
1	証明書 登録申請	本人証明情報、資格情報	利用者がサービス提供者へ提示する本人証明情報や資格情報
2		証明書登録（サービス利用）に関する登録情報	上記以外の証明書登録（サービス利用）に必要となる情報
3	審査	本人証明情報、資格情報	サービス提供者が外部機関から入手する利用者の本人証明情報や資格情報
4		審査で発生した付加情報	サービス提供者内で発生した利用者情報

3.2.1.3 証明書のみで利用者を確認する運用

この「証明書のみで利用者を確認する運用」は、利用者がサービスを利用する際に、サービス提供者が初めて利用者の証明書の確認を行う運用である。

利用者とサービス提供者との手順、フロー図および手順に必要となる利用者の属性情報を以下に整理する。

(1) 利用者とサービス提供者との手順

証明書のみで利用者を確認する運用における、利用者とサービス提供者との手順を以下に

示す。

1．利用者は保有する証明書とともにサービス提供者へサービス提供申請を行う
2．サービス提供者は証明書を確認し利用者の本人性・資格を確認する。さらに必要な場合は証明書や申請書をもとに外部から利用者情報を取得することにより利用者の本人性・資格を確認する
3．サービス提供者は申請書により提供するサービスを確認する
4．サービス提供者は自ら管理する情報を参照し、利用者へのサービス提供の可否を判断する
5．サービス提供者は利用者からの申請書および 4.で発生した情報を保存する
6．サービス提供者は利用者に対してサービスを提供する

(2) フロー図

証明書のみで利用者を確認する運用における、利用者とサービス提供者とのフロー図を以下に示す。

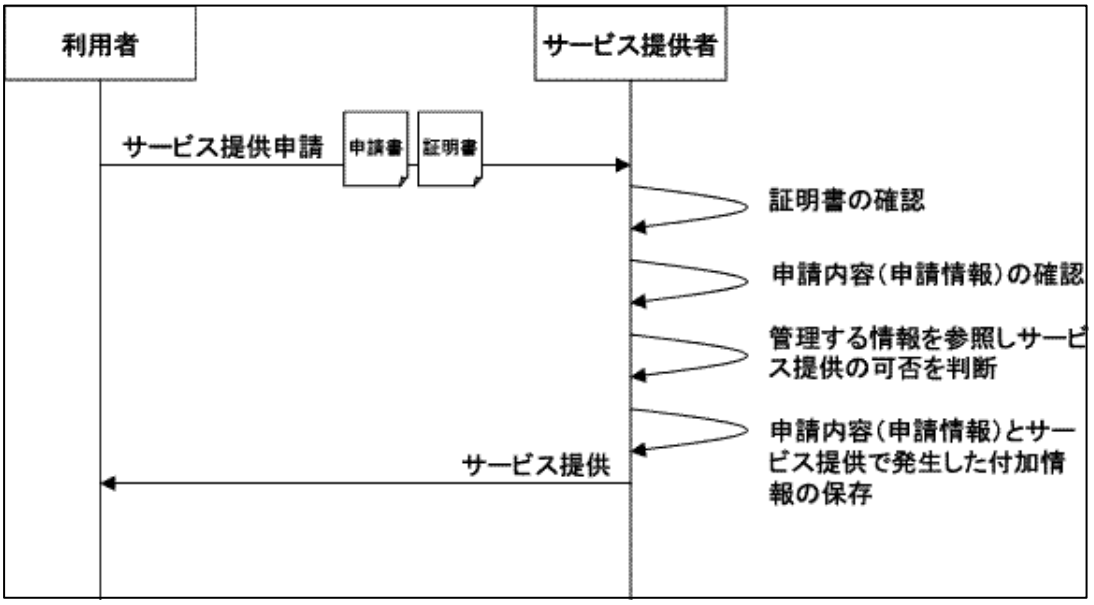


図 3-5 事前登録を行わない運用フロー

(3) 手順に必要となる利用者の属性情報

証明書のみで利用者を確認する運用で必要となる属性情報を以下に示す。なお本運用における利用者の本人証明情報、資格情報の入手先は、経路の違いにより利用者本人と外部機関が考えられる。

表 3-5 事前登録を行わない運用で必要となる利用者の属性情報

項番	運用フェーズ	属性情報	概要
1	サービス提供申請	本人証明情報、資格情報	利用者がサービス提供者へ提示する本人証明情報や資格情報
2		サービス利用に関する申請情報	上記以外のサービス利用に必要となる情報
3	サービス提供の判断	本人証明情報、資格情報	サービス提供者が外部機関から入手する利用者の本人証明情報や資格情報
4		サービス提供で発生した付加情報	利用者のサービス利用履歴情報

3.2.1.4 証明書と事前情報により利用者を確認する運用

この「証明書と事前情報により利用者を確認する運用」は、利用者がサービスを利用する際に、サービス提供者が発行した証明書もしくは事前登録された証明書の確認を行う運用である。

利用者とサービス提供者との手順、フロー図および手順に必要となる利用者の属性情報を以下に整理する。

(1) 利用者とサービス提供者との手順

証明書と事前情報により利用者を確認する運用における、利用者とサービス提供者との手順を以下に示す。

1．利用者は保有する証明書とともにサービス提供者へサービス提供申請を行う
2．サービス提供者は証明書を確認する
3．サービス提供者は申請書により提供するサービスを確認する
4．サービス提供者は自ら管理する情報を参照し、利用者の資格を確認するとともに利用者へのサービス提供の可否を判断する
5．サービス提供者は利用者からの申請書および 4.で発生した情報を保存する
6．サービス提供者は利用者に対してサービスを提供する

(2) フロー図

証明書と事前情報により利用者を確認する運用における、利用者とサービス提供者とのフロー図を以下に示す。

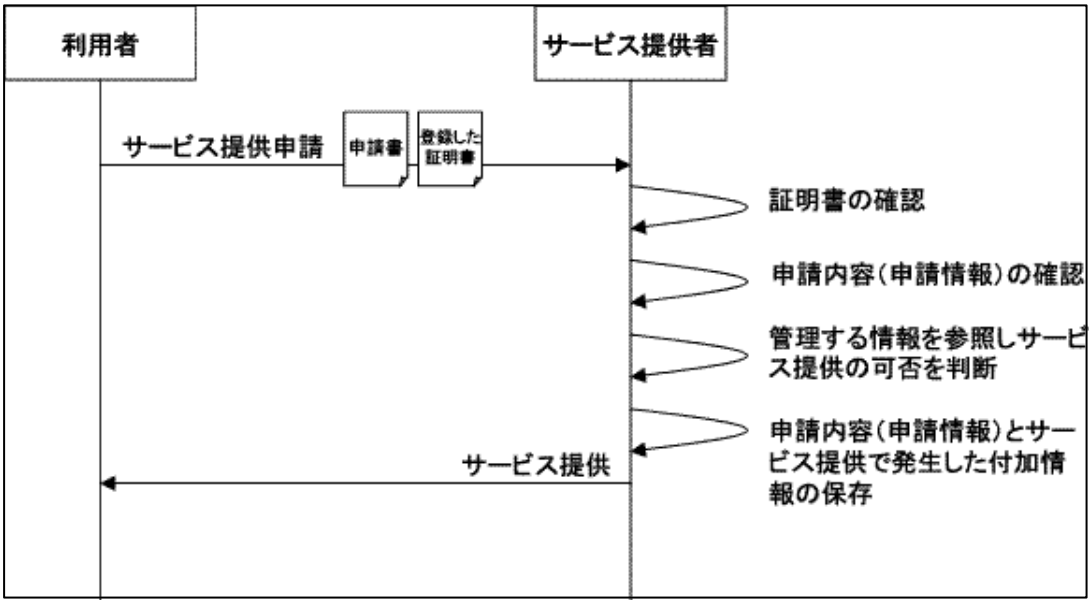


図 3-6 事前登録を行う運用フロー

(3) 手順に必要となる利用者の属性情報

証明書と事前情報により利用者を確認する運用で必要となる属性情報を以下に示す。なお本運用においては、他運用と異なり利用者の本人証明情報、資格情報の入手先は利用者本人のみと考えられる。

表 3-6 事前登録を行う運用で必要となる利用者の属性情報

項番	運用フェーズ	属性情報	概要
1	サービス提供申請	事前登録した証明書情報	事前に利用者へ発行した証明書情報、もしくは利用者から登録された証明書情報
2		サービス利用に関する申請情報	上記以外のサービス利用に必要となる情報
3	サービス提供の判断	事前登録情報	証明書発行もしくは証明書登録によって、事前に取得した利用者情報
4		サービス提供で発生した付加情報	利用者のサービス利用履歴情報

3.2.1.5 各運用で活用される属性情報

4つの運用において活用される利用者の属性情報を表 3-7 に整理する。表中には属性情報を活用方法も合わせて記す。

表 3-7 活用される利用者の属性情報

運用 / 属性情報	証明書を発行する運用	証明書を登録する運用	証明書のみで利用者を確認する運用	証明書と事前情報により利用者を確認する運用
本人証明情報、資格情報	○（利用者、外部機関から取得）	○（利用者、外部機関から取得）	○（利用者、外部機関から取得）	×
証明書発行に関する登録情報	○（利用者から取得）	×	×	×
審査で発生した付加情報	○（サービス機関が生成）	○（サービス機関が生成）	×	×
利用者の証明情報	○（サービス機関が生成し利用者へ発行）	×	×	×
証明書登録（サービス利用）に関する登録情報	×	○（利用者から取得）	×	×
サービス利用に関する申請情報	×	×	○（利用者から取得）	○（利用者から取得）
サービス提供で発生した付加情報	×	×	○（サービス機関が生成・管理）	○（サービス機関が生成・管理
事前登録した証明書情報	×	×	×	○（サービス機関が管理）
事前登録情報	×	×	×	○（利用者から取得）

3.2.2 属性情報活用パターンの実現モデル

実現方式には、1.3 節での記述より「公開鍵証明書利用」「属性証明書利用」「外部 DB 利用」の３つある。前節で整理した利用者の属性情報ごとに実現方式を適用し、属性情報活用パターンに合わせこれらを組み合わせ、属性情報活用パターンの実現モデルを整理する。さらに属性情報活用業務への実現モデル適用を検討する際の留意点を整理する。

3.2.2.1 実現モデルの整理

前節表 3-7 から、利用者の属性情報ごとに実現可能と思われる属性情報の電子化を表に整理する。各属性情報の電子化方法の適用を検討するにあたり、ここでは運用フローを考慮し、電子化方法を３つの実現方式に「申請書」「サービス提供者が管理する DB」の方式を加え５つとした。そして以下の観点から各属性情報の電子化方法を整理した。

- 利用者からサービス提供者へ提出する利用者確認のための属性情報は、申請書、公開鍵証明書、属性証明書とする
- そのうちサービス提供者の事前発行する属性情報は、公開鍵証明書、属性証明書とする
- また利用者確認以外のための属性情報は、申請書とする
- 外部機関からの入手する属性情報は、外部 DB とする
- サービス提供者で生成・管理する属性情報は、サービス提供者が管理する DB とする

表 3-8 属性情報の電子化の方法

項番	属性情報	属性情報の電子化の方法
1	本人証明情報、資格情報	【利用者から取得】申請書、公開鍵証明書 【外部機関から取得】外部 DB
2	証明書発行に関する登録情報	申請書
3	審査で発生した付加情報	サービス提供者が管理する DB
4	利用者の証明情報	公開鍵証明書、属性証明書
5	証明書登録（サービス利用）に関する登録情報	申請書
6	サービス利用に関する申請情報	申請書
7	サービス提供で発生した付加情報	サービス提供者が管理する DB
8	事前登録した証明書情報	公開鍵証明書、属性証明書
9	事前登録情報	サービス提供者が管理する DB

表 3-8 で整理した属性情報の電子化の方法をもとに、表 3-2 と表 3-7 から各属性情報活用パターンで利用する属性情報の組み合わせから属性情報活用パターンの実現モデルを整理する。つまり各属性情報活用パターンにおいて、加入（登録）や利用の利用場面で必要となる利用者の属性情報に対する電子化の方法を組み合わせたモデルを考え、全ての組み合わせの中から証明書を利用したモデルを実現モデルとする。対象とする実現モデルを表に整理する。

表 3-9 属性情報活用パターンの実現モデル

項番	実現モデル	概要	適用可能な属性情報活用パターン
1	実現モデル１	利用者が既に保有している証明書のみで、利用者の本人性や属性を確認するモデル	パターン１
2	実現モデル２	利用者が既に保有している証明書と、外部機関から取得した情報から、利用者の本人性や属性を確認するモデル	
3	実現モデル３	利用者が既に保有している証明書を、サービス提供者に登録するモデル	パターン２
4	実現モデル４	利用者が既に保有している証明書だけでなく、外部機関から取得した情報を登録するモデル	
5	実現モデル５	サービス提供者が、利用者に対して証明書として公開鍵証明書を発行するモデル	パターン３
6	実現モデル６	サービス提供者が、外部機関から取得した情報をもとに利用者を確認し、利用者に対して証明書として公開鍵証明書を発行するモデル	
7	実現モデル７	サービス提供者が、利用者に対して証明書として属性証明書を発行するモデル	
8	実現モデル８	サービス提供者が、外部機関から取得した情報をもとに利用者を確認し、利用者に対して証明書として属性証明書を発行するモデル	

なお実現モデルで利用される公開鍵証明書において、１章で記述した３種類の証明書（「単一目的証明書」「汎用目的証明書」「特定目的証明書」）の適用性を表 3-10 にまとめる。評価にあたり実現モデルに適すると考えられる証明書を「○」、運用によっては適用可能と考えられる証明書を「△」とした。

表 3-10 実現モデルと証明書の関係

実現モデル	単一目的証明書	汎用目的証明書	特定目的証明書
実現モデル１	×	×	○
実現モデル２	×	○	△
実現モデル３	×	○	○
実現モデル４	×	○	○
実現モデル５	○	×	△
実現モデル６	○	×	△
実現モデル７	×	○	△
実現モデル８	×	○	△

3.2.2.2 実現モデル１

このモデルは、サービス提供者が、利用者から取得した証明書のみで利用者の本人性や属性を確認するモデルである。

モデルで利用する公開鍵証明書はサービス提供者が必要となる全ての利用者の属性情報が記載されることから、あるグループで共通で使用する「特定目的証明書」が適すると考える。

モデルの特徴、留意点を以下に示す。

- PKI 技術による認証基盤で、サービス提供者は利用者の本人認証や属性認証が可能である
- 利用者の公開鍵証明書（PKC）には、サービス提供者が利用者の確認やサービス提供の可否で判断するための属性情報の記述が必要である
- 利用者の公開鍵証明書に記載される属性情報について、漏洩防止や個人情報保護の観点での管理や対策が必要である
- 利用者が利用できる公開鍵証明書(PKC)について､サービス提供者は規定や制限を設定し、利用者に提示する必要がある

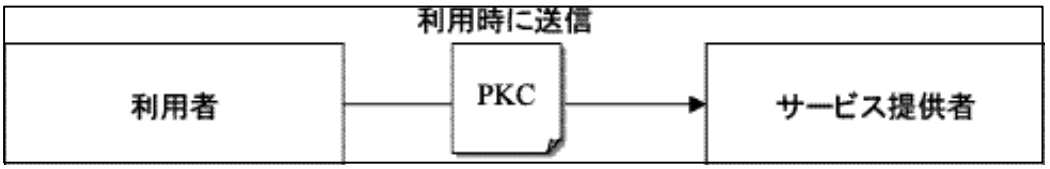


図 3-7 実現モデル１

3.2.2.3　実現モデル２

このモデルは、サービス提供者が、利用者から取得した証明書と外部機関から取得した利用者情報から利用者の本人性や属性を確認するモデルである。

モデルで利用する公開鍵証明書は外部 DB にある利用者の属性情報を特定するための情報が記載されることから、汎用的に利用者を特定できる「汎用目的証明書」が適すると考える。また外部 DB があるグループ内で共有する場合はグループで利用者を特定する「特定目的証明書」が適すると考える。

モデルの特徴、留意点を以下に示す。

- PKI 技術による認証基盤で、サービス提供者は利用者の本人認証が可能である
- 利用者の公開鍵証明書（PKC）には、サービス提供者が利用者の確認やサービス提供の可否で判断するための属性情報、もしくは外部 DB 情報の記述が必要である
- 利用者の公開鍵証明書に記載される属性情報について、漏洩防止や個人情報保護の観点での管理や対策が必要である
- 外部 DB との連携が必要である
- 利用者が利用できる公開鍵証明書(PKC)について､サービス提供者は規定や制限を設定し、利用者に提示する必要がある

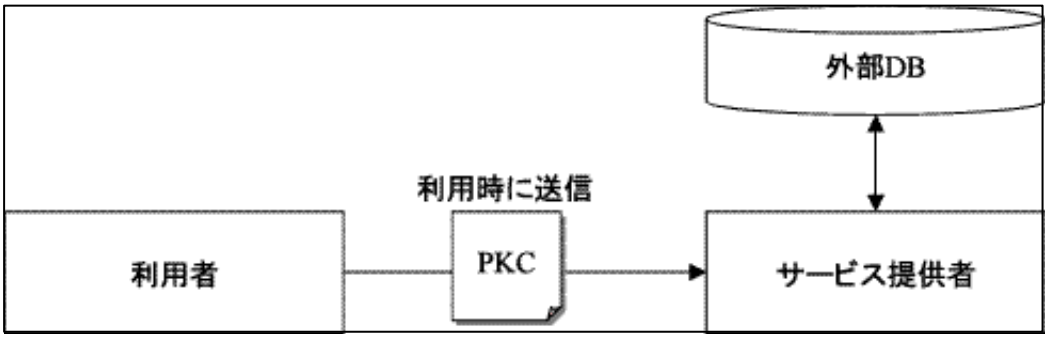


図 3-8 実現モデル２

3.2.2.4　実現モデル３

このモデルは、利用者がサービスを利用する前に利用者が既に保有している公開鍵証明書をサービス提供者へ登録することにより、サービス提供者が公開鍵証明書と登録情報から利用者の本人性や属性を確認するモデルである。

モデルで利用する公開鍵証明書は利用者が加入（登録）時にサービス提供者へ登録した属性情報を特定する情報が記載されることから、汎用的に利用者を特定できる「汎用目的証明書」もしくはあるグループで利用者を特定する「特定目的証明書」が適すると考える。

モデルの特徴、留意点を以下に示す。

- 利用者の公開鍵証明書（PKC）に含まれていない属性情報に対して必要に応じてサービス提供者に登録することにより、柔軟な対応が可能である
- PKI 技術による認証基盤で、サービス提供者は利用者の本人認証や属性認証が可能である
- 登録してある利用者の公開鍵証明書の失効、有効期限切れ、更新などに対する対応が必要である
- 公開鍵証明書を保有していない利用者に対する対策が必要である
- 複数の公開鍵証明書に対応する場合、それぞれの認証局と連携しかつ認証局が提供する失効確認サービスへの対応が必要である
- 利用者が利用できる公開鍵証明書(PKC)について､サービス提供者は規定や制限を設定し、利用者に提示する必要がある

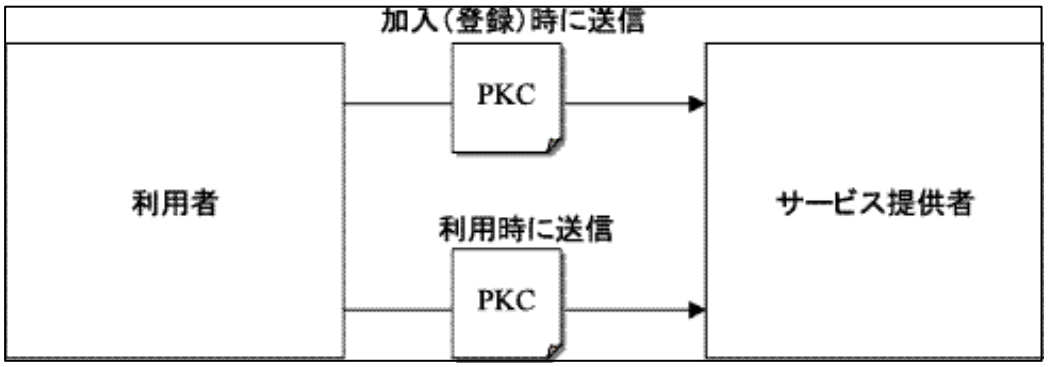


図 3-9 実現モデル３

3.2.2.5　実現モデル４

このモデルは、利用者がサービスを利用する前に利用者が既に保有している公開鍵証明書をサービス提供者へ登録することにより、サービス提供者が公開鍵証明書、登録情報さらに外部機関から取得した情報から利用者の本人性や属性を確認するモデルである。

モデルで利用する公開鍵証明書は利用者が加入（登録）時にサービス提供者へ登録した属性情報や外部 DB にある利用者の属性情報を特定するための情報が記載されることから、汎用的に利用者を特定できる「汎用目的証明書」もしくはあるグループで利用者を特定する「特定目的証明書」が適すると考える。

モデルの特徴、留意点を以下に示す。

- 利用者の公開鍵証明書（PKC）に含まれていない属性情報に対して必要に応じてサービス提供者に登録することにより、柔軟な対応が可能である
- PKI 技術による認証基盤で、サービス提供者は利用者の本人認証や属性認証が可能である
- 登録してある利用者の公開鍵証明書の失効、有効期限切れ、更新などに対する対応が必要である
- 公開鍵証明書を保有していない利用者に対する対策が必要である
- 複数の公開鍵証明書に対応する場合、それぞれの認証局と連携しかつ認証局が提供する失効確認サービスへの対応が必要である
- 外部 DB との連携が必要である
- 利用者が利用できる公開鍵証明書(PKC)について、サービス提供者は規定や制限を設定し、利用者に提示する必要がある

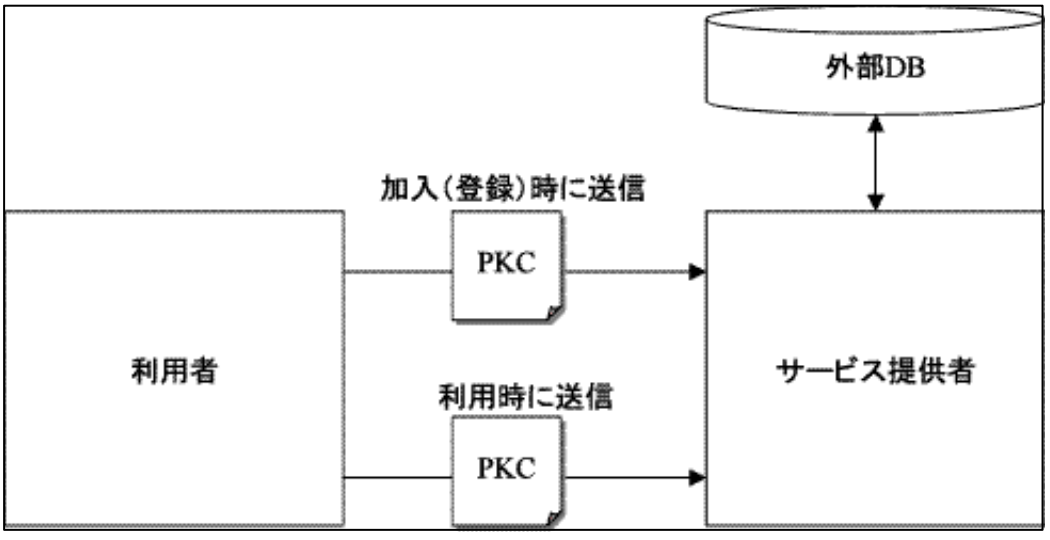


図 3-10 実現モデル４

3.2.2.6　実現モデル５

このモデルは、利用者がサービスを利用する前にサービス提供者が利用者に対して公開鍵証明書を発行することにより、サービス提供者が公開鍵証明書と登録情報から利用者の本人性や属性を確認するモデルである。

モデルで利用する公開鍵証明書はサービス提供者に応じて情報を記載されることから、「単一目的証明書」が適すると考える。またあるグループで公開鍵証明書に記載する情報を共通する場合は「特定目的証明書」が適すると考える。

モデルの特徴、留意点を以下に示す。

- サービス提供者が自由に公開鍵証明書（PKC）に属性情報を記述することが可能である
- 発行した利用者の公開鍵証明書の失効、更新に対する対応が必要である
- 発行した公開鍵証明書を他の目的で利用されることへの対策が必要である
- サービス提供者は、利用者へ公開鍵証明書の格納媒体（セキュアトークンなど）を発行し管理することが必要である
- サービス提供者は、サービスに応じた公開鍵証明書の信頼性を確保するため認証局の運用規定を設定し、利用者に提示する必要がある

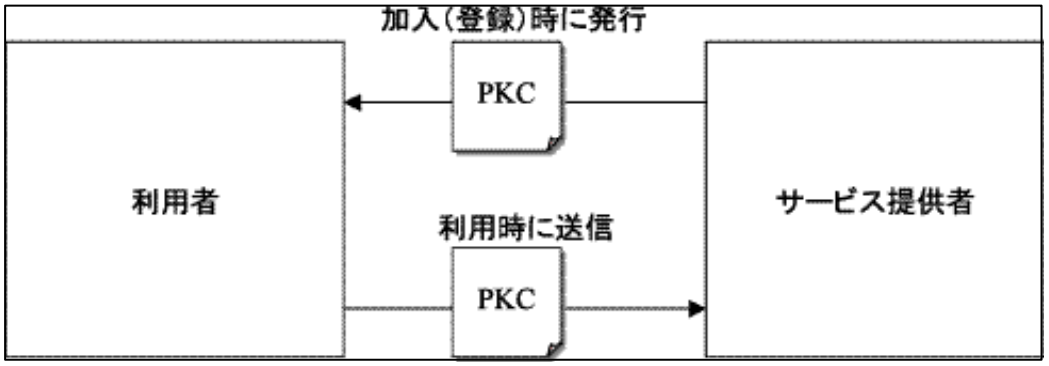


図 3-11 実現モデル５

3.2.2.7　実現モデル６

このモデルは、利用者がサービスを利用する前にサービス提供者が外部機関から取得した情報をもとに利用者に対して公開鍵証明書を発行することにより、サービス提供者が公開鍵証明書、登録情報から利用者の本人性や属性を確認するモデルである。

モデルで利用する公開鍵証明書はサービス提供者に応じて情報を記載されることから、「単一目的証明書」が適すると考える。またあるグループで公開鍵証明書に記載する情報を共通する場合は「特定目的証明書」が適すると考える。

モデルの特徴、留意点を以下に示す。

- サービス提供者が自由に公開鍵証明書（PKC）に属性情報を記述することが可能である
- 発行した利用者の公開鍵証明書の失効、更新に対する対応が必要である
- 発行した公開鍵証明書を他の目的で利用されることへの対策が必要である
- サービス提供者は、利用者へ公開鍵証明書の格納媒体（セキュアトークンなど）を発行し管理することが必要である
- 外部 DB との連携が必要である
- サービス提供者は、サービスに応じた公開鍵証明書の信頼性を確保するため認証局の運用規定を設定し、利用者に提示する必要がある

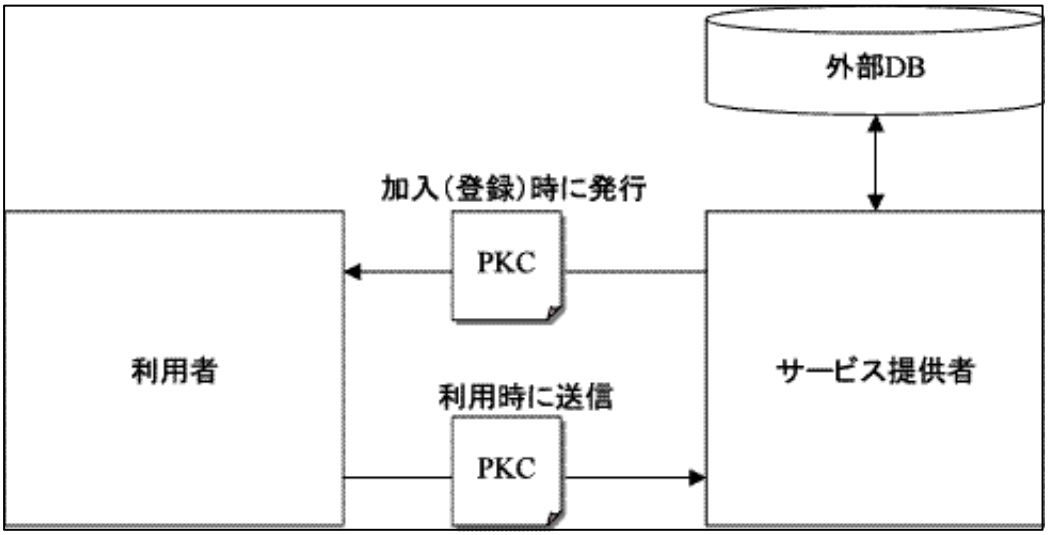


図 3-12 実現モデル６

3.2.2.8　実現モデル７

このモデルは、利用者がサービスを利用する前にサービス提供者が利用者に対して属性証明書を発行することにより、サービス提供者が公開鍵証明書と登録情報から利用者の本人性や属性を確認するモデルである。

モデルで利用する公開鍵証明書は汎用的に利用者を特定できれば良いことから「汎用目的証明書」が適すると考える。またあるグループ内において利用者を特定できれば良い場合には「特定目的証明書」が適すると考える。

モデルの特徴、留意点を以下に示す。

- PKI 技術による認証基盤で、サービス提供者は利用者の本人認証や属性認証が可能である
- サービス提供者が自由に属性証明書（AC）に属性情報を記述することが可能である
- 発行した属性証明書が紐づいている利用者の公開鍵証明書の失効、有効期限切れ、更新などに対する対応が必要である
- 発行した属性証明書の失効、更新に対する対応が必要である
- 属性証明書対応のソフトウェアが必要である
- サービス提供者は、サービスに応じた属性証明書の信頼性を確保するため属性認証局の運用規定を設定し、利用者に提示する必要がある
- 利用者が利用できる公開鍵証明書(PKC)について､サービス提供者は規定や制限を設定し、利用者に提示する必要がある

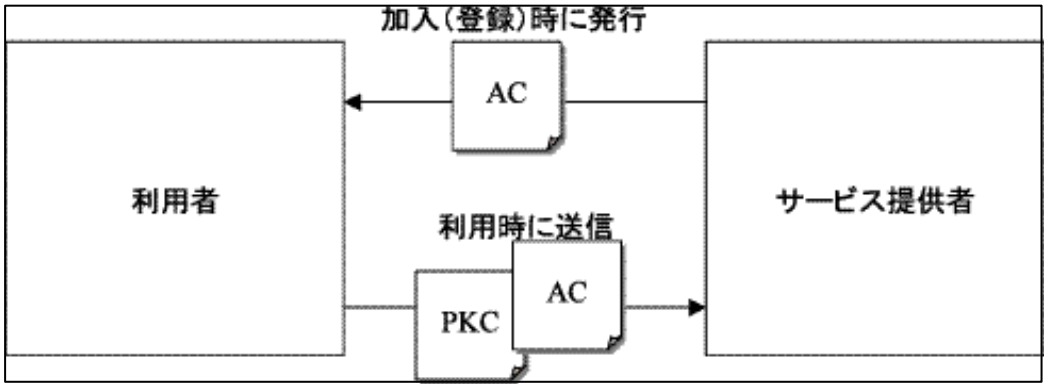


図 3-13 実現モデル７

3.2.2.9　実現モデル８

このモデルは、利用者がサービスを利用する前にサービス提供者が外部機関から取得した情報をもとに利用者に対して属性証明書を発行することにより、サービス提供者が公開鍵証明書、登録情報から利用者の本人性や属性を確認するモデルである。

モデルで利用する公開鍵証明書は汎用的に利用者を特定できれば良いことから「汎用目的証明書」が適すると考える。またあるグループ内において利用者を特定できれば良い場合には「特定目的証明書」が適すると考える。

モデルの特徴、留意点を以下に示す。

- PKI 技術による認証基盤で、サービス提供者は利用者の本人認証や属性認証が可能である
- サービス提供者が自由に属性証明書（AC）に属性情報を記述することが可能である
- 発行した属性証明書が紐づいている公開鍵証明書の失効、有効期限切れ、更新などに対する対応が必要である
- 発行した属性証明書の失効、更新に対する対応が必要である
- 属性証明書対応のソフトウェアが必要である
- 外部 DB との連携が必要である
- サービス提供者は、サービスに応じた属性証明書の信頼性を確保するため属性認証局の運用規定を設定し、利用者に提示する必要がある
- 利用者が利用できる公開鍵証明書(PKC)について､サービス提供者は規定や制限を設定し、利用者に提示する必要がある

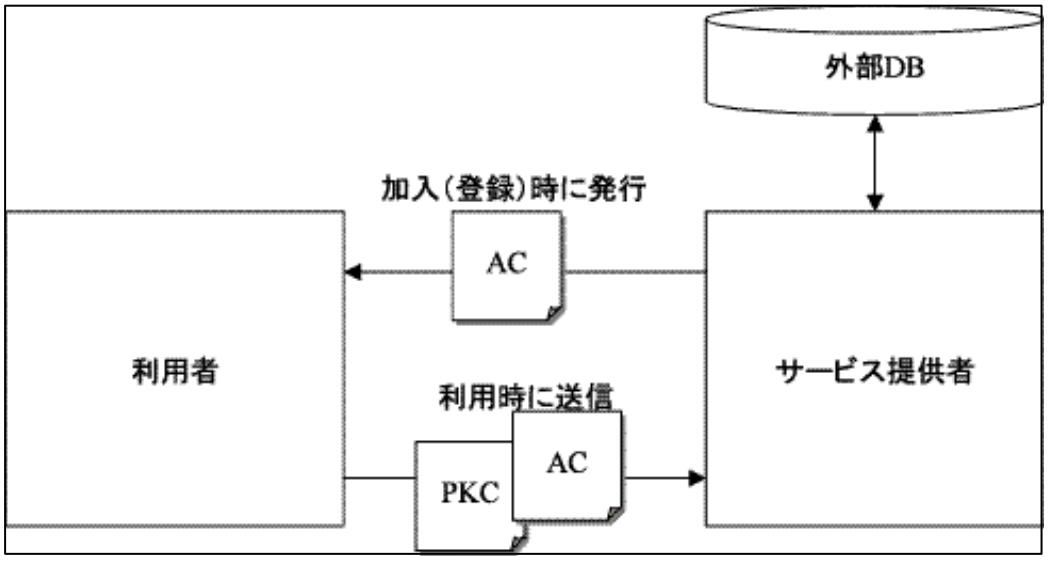


図 3-14 実現モデル８

3.3 属性情報活用ガイドライン

属性情報を活用するシステムの設計を行うには、構築するシステム要件を整理しその要件をもとに前節の８つの実現モデルから適用するモデルを選択し、さらに具体的に実現方式を検討する必要がある。そこで本節では、要件抽出、適用モデル選択、モデル詳細化の検討手順と検討ポイントに関して指針を示す。手順は以下の通りである。各手順での検討ポイントを紹介する。

STEP１　提供サービスの明確化
STEP２　実現上の要件定義
STEP３　実現モデルの選択
STEP４　設計の詳細化

3.3.1 提供サービスの明確化

システム設計を行うにあたり、最初に以下の観点で業務や社会・業界動向を調査検討し、システムで実現するサービスを明確にする。サービスの明確化を行うためには以下の観点からアプローチを取ると良い。

また 2.3 節に記述した利用者の要件を参考にし、利用者の利便性やコストを考慮して提供サービスを検討することが望ましい。

- サービス内容・提供形態の整理

提供するサービスの内容と提供形態を整理する。観点として 1)リアルなサービスの電子化。2)既存サービスとの連携・比較。3)社会・業界での提供サービスの動向。がある。

また、2.3.1 項に記述した利用者への信頼性要件や 2.3.2 項に記述した利用者の利便性要件を考慮し、サービス内容・提供形態を整理することが望ましい。

- 利用者の想定

利用者環境を設定する。観点として 1)証明書の保有状況。2)マシン環境（認証用トークンの有無など)。3)情報リテラシ。がある。

また、2.3.2 項に記述した利用者の利便性要件を考慮し、サービス利用者を整理することが望ましい。

- 環境条件の調査

外部環境を整理する。観点として 1)自ら証明書を発行するのか、認証基盤を利用するのか。2)業界、アライアンスやパートナーで利用できる認証基盤があるか。3)利用できる認証基盤はどのような方式なのか。がある。

- コスト要件の検討

サービス内容および後述するリスクを考慮し、サービス提供のためのシステム稼動やメンテナンスの運用、また社会的責任に応じた体制の維持管理のコスト要件を整理する。

また、2.3.3 項に記述した利用者のコスト要件を考慮し、サービス提供に必要となるシステム保守・管理のコスト要件を整理することが望ましい。

- リスク（セキュリティ、信頼性）要件/制約の検討

サービス内容を考慮し、システムで扱う属性情報やシステムの社会的責任に応じて、システムが確保しなければならないセキュリティ要件や対策を必要とするリスクを整理する。

- 法令遵守の調査

サービス実現において遵守しなければならない法令を調査する。法令には業務に関わる法令と、電子化に関わる法令（電子署名法など）がある。

- ビジネスストーリの検討

企業戦略、市場動向やビジネス展開を考慮し、システム構築・運用後のシステム拡張や機能拡充、サービスの拡大を検討する。

3.3.2 実現上の要件定義

提供サービスを明確にしたサービス提供における基本的な要件をもとに、システム要件を定義する。要件定義を行うためには以下の観点からアプローチを取ると良い。

- 属性情報の整理

提供サービス全体で必要となる属性情報を整理する。サービスで必要となる属性情報を洗い出し、1.2 節および 3.2 節を参考に属性情報を時間、信頼性、目的などの軸で分析し体系化する。

- サービス利用シナリオの検討

各属性情報のフローに着目し、利用者の利便性（属性情報の取得方法、管理方法、安全性など）やシステムの実現性（社会的責任、法制度など）に注意しながら、シナリオを整理する。

- 認証から認可のシナリオの検討

ビジネスストーリなどからサービス提供を長期的な視点で捉え、利用頻度の変化やセキュリティ強度の変化を考慮し、利用者の認証から認可までのフローを精査する。

- システム性能の検討

サービスの利用頻度、提供形態およびコスト要件からシステムの実現性を再整理し、システムの性能要件を整理する。

- 登場人物の整理

利用者環境や環境条件からサービス提供で必要となる登場人物を整理する。さらに登場人物との役割や責務を明確にする。

- **利用インフラ/サービスの整理**

サービス内容や環境条件から利用するインフラ/サービスを整理する。さらに利用要件を明確にする。

3.3.3 実現モデルの選択

定義した要件をもとに、3.2 節で整理した実現モデルの中から適用するモデルを選択する。選択するには以下のアプローチを取ると良い。

- **属性情報活用パターンの実現方式から選択**

登場人物や利用インフラ/サービスなどの要件に従い属性情報のライフサイクルを調査・分析し実現可能な実現モデルを整理する。次にコスト、リスクやビジネスストーリなどの要件を考慮し実現モデルを選択する。

- **バリエーションの検討**

選択した実現モデルを、利用するシステムとの連携方法の検討や認証方式の具体的な検討を通して、実現モデルのバリエーションを洗い出し、要件をもとにモデルを精査する。

例えば、既存システムや利用インフラがある場合、それらの認証方式（ID/パスワードなど）との連携（併用、変更など）を検討する。一方、属性証明書を利用する場合は、プッシュ型モデル/プル型モデルの検討や属性証明書から見た公開鍵証明書の位置付け（ポリシー等）の検討などを行う。

3.3.4 設計の詳細化

システム設計に向け、サービス内容や外部機関との連携を考慮し選択したモデルを精査する。精査するには以下のアプローチを取ると良い。

- **前提となる認証局の決定**

実現モデルをもとに、コスト要件、利用者の想定や利用インフラ/サービスを考慮して証明書を発行する認証局を決定する。外部の認証局を利用する場合、システムとの連携方法を整理する。サービス提供者が認証局を運用する場合、認証局の運用規定を策定する。

- **セキュアトークンの設計・選択**

利用者の想定や外部インフラ/サービス、もしくはコスト要件からサービスで利用するセキュアトークンを決定する。サービス提供者がセキュアトークンを発行する場合、ビジネスストーリを考慮した設計を行う必要がある。

- **開発環境の設定**

利用ソフトウェアの仕様や利用インフラ/サービスの仕様・インターフェースを調査し、システム開発における開発ソフトウェアや利用ソフトウェアを決定する。また提供形態や性能要件から、システム構成やネットワーク構成を検討しプロトコルや方式の検討を行う。

- 外部連携の再整理

設計の詳細化をうけ登場人物を整理し、最終的な利用インフラ/サービス、既存サービスを行い、必要な事務処理を調査する。

3.4 実現モデル例

本節では、表に示す４つの分類ごとに利用場面を想定し、利用場面ごとに前節に示した手順にしたがいシステム設計を行う。

表 3-11 利用場面

項番	分類	概要	利用場面
1	BtoC	民間企業と住民の間で行われるオンラインサービス	オンラインショッピング
2	BtoG	民間企業と行政機関の間で行われるオンラインサービス	電子申請
3	CtoG	住民と行政機関の間で行われるオンラインサービス	電子投票
4	MtoC	医療機関と患者のように、ある閉じられた空間（ドメイン、コミュニティなど）で行われるオンラインサービス	健康診断情報の共有サービス

3.4.1 オンラインショッピング

民間企業と住民の間で行われるオンラインサービスとして、オンラインブックストアを想定し設計を行う。ここでは「ブックストアの登録会員」という属性情報に着目する。

3.4.1.1 提供サービスの明確化

表 3-12 提供サービスの明確化

項目	検討結果
サービス内容・提供形態の整理	● インターネット経由で、会員に対して電子本（コンテンツ）を提供する
利用者の想定	● 会員は自宅などからインターネットにアクセスできる環境がある ● 会員は本人認証用の公開鍵証明書を持っている
環境条件の調査	● インターネット上でのオンラインブックストアの実在を証明する第三者機関がある ● インターネット上に利用者（会員）の本人性を保証する認証局がある
コスト要件の検討	● システム運用管理コストは必要最低限に抑える（目標：＊＊＊円/年程度）
リスク（セキュリティ、信頼性）要件/制約の検討	● 会員の成りすまし、事後否認 ● 購入要求時での要求者以外による改ざん

	● 会員情報（登録情報や購買履歴など）の漏洩 ● ブックストア内での購入要求の改ざん
法令遵守の調査	● 電子署名法 ● 個人情報保護法
ビジネスストーリの検討	● 提携企業、グループ企業間での会員割引や会員サービスを実現

3.4.1.2 実現上の要件定義

表 3-13 実現上の要件定義

項目	検討結果
属性情報の整理	● オンラインブックストアが認めた会員であること 時間：有効期間＊年 信頼性：公開は可能だが、サービス利用時のみ有効であるが、サービス以外での利用時には証明効力はない 目的：事前登録していること
サービス利用シナリオの検討	● 利用者は、サービス利用前にオンラインブックストアに会員登録を行う。その際に利用者の公開鍵証明書を提示する ● オンラインブックストアは、利用者に対して会員情報を発行する ● 利用者が、サービス利用時にオンラインブックストアに会員情報を提示する ● オンラインブックストアは提示された情報（必要であれば会員登録時の情報も合わせ）をもとに会員であることを確認し、同時にサービス利用が可能か判断する ● 購入要求情報をもとに、電子本を検索し利用者へ提供する ● 提供を確認できたら課金を行う
認証から認可のシナリオの検討	● 利用者から提示された会員情報をもとに、オンラインブックストア内で管理している登録情報を検索し、会員であることを確認する ● さらに、利用履歴や支払い状況などを確認し、会員へサービス利用の許可を判断する ● 支払い状況では、過去の課金時での与信情報も合わせて判断する ● 定期的に会員情報を利用者に確認する

システム性能の検討	● 365 日、24 時間のサービス提供 ● ＊＊＊件/日。コンテンツの送信時間は＊秒以下。
登場人物の整理	● 認証局：購入要求者の実在性を保証する ● 会員：オンラインブックストアのサービスを利用する ● オンラインブックストア：サービスを提供する、会員情報を管理する ● 決済サービス：利用者から料金を徴収する代行サービス
利用インフラ/サービスの整理	● 利用者の認証局が提供する公開鍵証明書検証サービス ● 課金を行うための決済サービス

3.4.1.3 実現モデルの選択

表 3-14 実現モデルの選択

項目	検討結果
属性情報活用パターンの実現方式から選択	● 要件をもとに実現モデルは別図のようになる。 ● 会員情報の信頼性確保、ビジネスストーリを考慮し実現モデル１を採用する
バリエーションの検討	● 属性証明書の利用はプッシュ型モデルとする

(1) モデル１

オンラインショッピング実現モデル１のフローを示す。

１．会員は認証局から公開鍵証明書（PKC）を入手する

２．会員はサービス利用前にブックストアへ公開鍵証明書の登録を申請する

３．ブックストアは申請をもとに会員審査を行い、属性証明書（AC）を会員へ発行する

４．会員は購入要求、公開鍵証明書および属性証明書をブックストアに送信して、電子本を購入する

５．ブックストアは属性証明書から会員であることを確認する

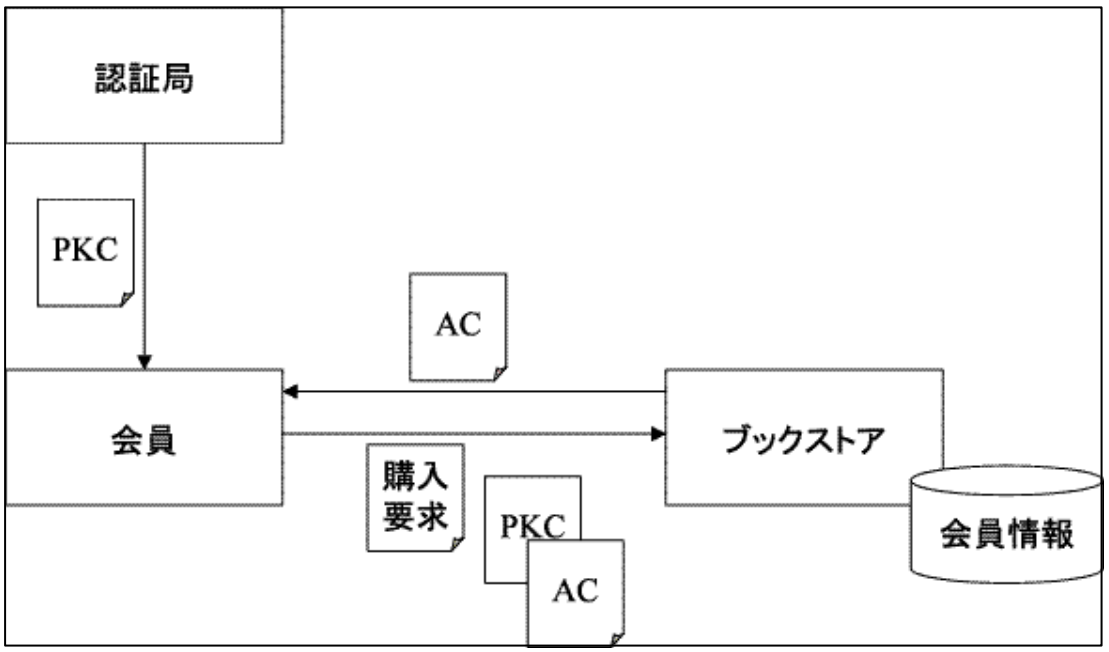


図 3-15 オンラインショッピング実現モデル１

(2) モデル２

オンラインショッピング実現モデル２のフローを示す。

１．会員は認証局から公開鍵証明書（PKC）を入手する

２．会員はサービス利用前にブックストアへ公開鍵証明書情報の登録を申請する

３.ブックストアは申請をもとに会員審査を行い会員情報として DB に公開鍵証明書情報を登録する

４．会員は購入要求および公開鍵証明書をブックストアに送信して、電子本を購入する

５．ブックストアは公開鍵証明書と会員情報中の情報を参照し、会員であることを確認する

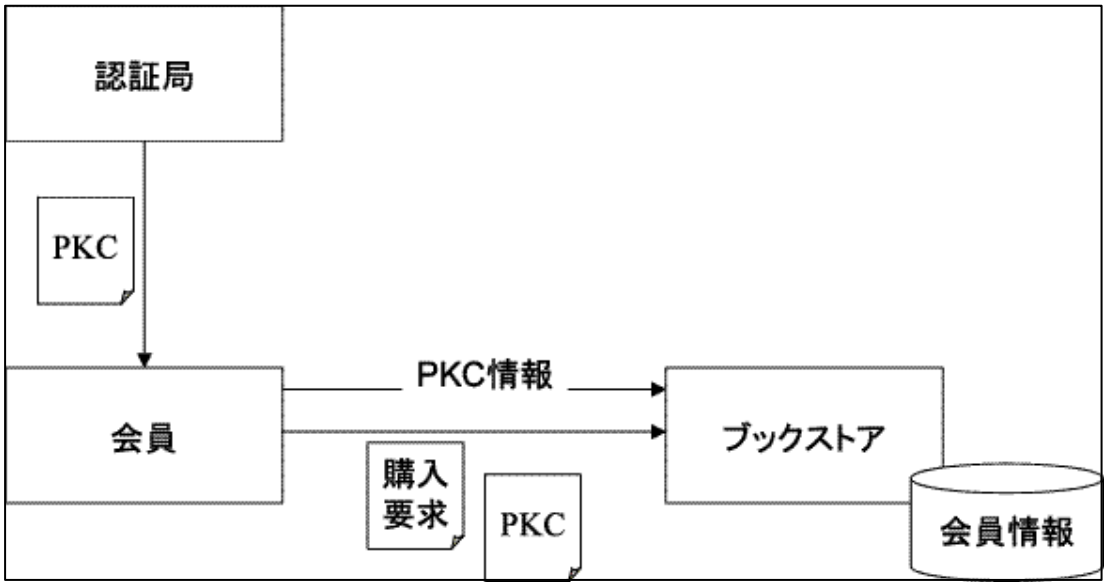


図 3-16 オンラインショッピング実現モデル２

3.4.1.4　設計の詳細化

表 3-15 設計の詳細化

項目	検討結果
前提となる認証局の決定	● 認証局：社会的に信頼のある認証局（特定認証業務認定認証局など） ● 属性認証局：オンラインブックセンタで登録業務、発行業務はアウトソース
セキュアトークンの設計・選択	● 公開鍵証明書を発行する認証局の運用に依存 ● 公開鍵証明書を格納するトークンに属性証明書が格納できない場合、属性証明書を管理するトークンが必要
開発環境の設定	● 属性証明書を表示、解析するソフトウェアが必要
外部連携の再整理	● 認証局は＊＊＊ ● 属性証明書発行サービスは＊＊＊ ● 決済サービスは＊＊＊

3.4.2　法人登記の電子申請

司法書士等が株式会社の登記の代理申請を法務省に対してオンライン申請することを想定し設計を行う。ここでは発起人、取締役、監査役、および司法書士の本人確認と関連する属性情報に着目する。

3.4.2.1　提供サービスの明確化

表 3-16 提供サービスの明確化

項目	検討結果
サービス内容・提供形態の整理	● インターネット経由で、発起人、取締役、監査役、および司法書士が株式会社登記の書類を準備し、登記所へ電子申請する
利用者の想定	● 利用者はインターネットにアクセスできる環境がある ● 利用者は本人認証用の公開鍵証明書を持っている
環境条件の調査	● 通常使用されているインターネット接続端末環境に対応する必要がある
コスト要件の検討	● システム運用管理コストは必要最低限に抑える（目標：＊＊＊円/年程度）
リスク（セキュリティ、信頼性）要件/制約の検討	● 申請情報の改ざんに対する担保 ● 申請情報に対する本人の意思証明
法令遵守の調査	● 電子署名法 ● 個人情報保護法
ビジネスストーリの検討	● 申請のオンライン化による効率化および利便性の向上

3.4.2.2 実現上の要件定義

表 3-17 実現上の要件定義

項目	検討結果
属性情報の整理	● 発起人、取締役、監査役の本人確認 ● 代理申請する司法書士の本人確認、資格および代理権の証明
サービス利用シナリオの検討	前提条件： ● 登記所が電子申請による登記を受け付けている ● 発起人、取締役、監査役は本人確認用と認められる電子証明書を保持している ● 司法書士は本人確認および司法書士であることを証明する電子証明書を保持している 発起人から見た利用シナリオ： ● 発起人は登記申請を行う司法書士のホームページ経由で会社登記の手続きを申し込む ● 司法書士は発起人に契約の過程で代理人として委任したことを証明してもらう ● 司法書士は必要な書類一式を用意する ● 発起人、取締役、監査役は用意された書類に電子署名する ● 司法書士は登記書類を登記所へ申請する
認証から認可のシナリオの検討	● 発起人、取締役、監査役を認証する認証局は本人の実在性を認証しなくてはならない ● 司法書士を認証する認証局は司法書士である資格認証を行わなくてはならない ● 登記所は発起人、取締役、監査役、および司法書士の認証、司法書士の資格の確認、司法書士が委任を受けた代理人であるかの属性を確認しなくてはならない
システム性能の検討	● 365 日、24 時間のサービス提供 ● ＊＊＊件/日。コンテンツの送信時間は＊秒以下。
登場人物の整理	● 本人確認認証局：本人であることを認証する電子証明書を発行 ● 司法書士認証局：司法書士であることを認証する電子証明書を発行
利用インフラ/サービスの整理	● 司法書士ホームページ：発起人と登記申請用書類をやりとりするホームページ ● オンライン法人登記申請ホームページ：登記所が法人登記の電子申請を受け付けるホームページ

3.4.2.3 実現モデルの選択

表 3-18 実現モデルの選択

項目	検討結果
属性情報活用パターンの実現方式から選択	● 要件をもとに実現モデルは図 3-17 のようになる。 ● モデル１の課題は委任状が機械処理できる形式のものであるかという点である ● モデル２では SAML による属性情報の証明を想定している
バリエーションの検討	● 属性証明書を使用する場合、モデル１の委任状に対して代理権を証明する AC を適用することにより実現可能

(1) モデル１

法人登記の電子申請実現モデル１のフローを示す。本モデルでは公開鍵証明書（PKC）のみを使用したモデルである。

１．発起人等は認証局から本人であることを証明する公開鍵証明書（ PKC）を所有している（①）
２．発起人は公開鍵証明書（PKC）を使用し、委任状および申請書類に電子署名を行う（②）
３．司法書士は認証局から本人であることおよび司法書士であることを証明する公開鍵証明書（PKC）を所有している（③）
４．司法書士は公開鍵証明書（PKC）を使用し、申請書類に電子署名を行う（④）
５．司法書士は登記所に電子申請を行う（⑤）
６．登記所は（A）と（B）の認証局で署名者の確認を行い、申請書類に含まれる委任状により司法書士の代理権を確認する

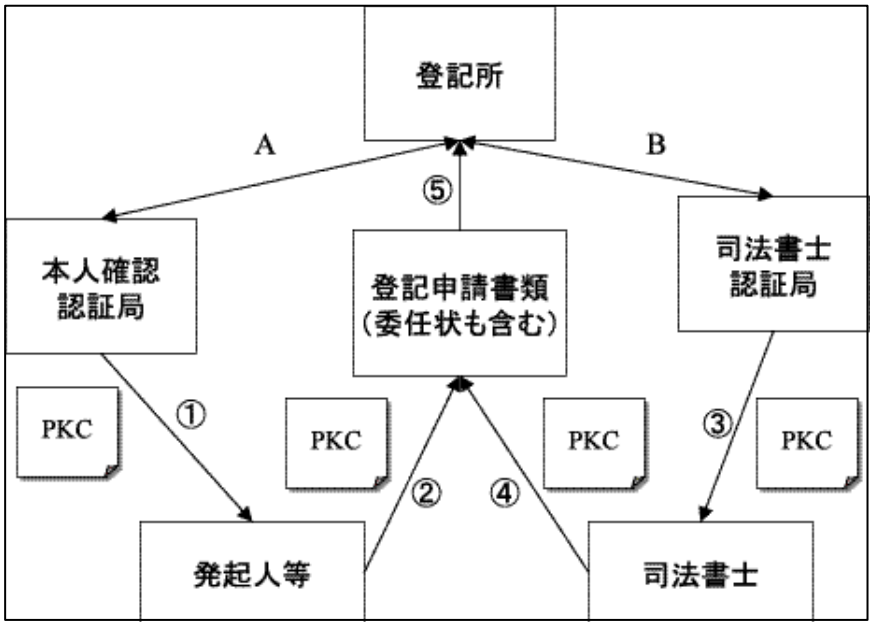


図 3-17 法人登記の電子申請実現モデル１

(2) モデル２

法人登記の電子申請実現モデル２のフローを示す。本モデルではデータベースに対して属性情報を照会するモデルである。

１．発起人等は認証局から本人であることを証明する公開鍵証明書（PKC）を所有している（①）

２．司法書士は認証局から本人であることおよび司法書士であることを証明する公開鍵証明書（PKC）を所有している（②）

３．発起人および司法書士は公開鍵証明書（PKC）を使用し、電子署名による契約を行い代理権限が司法書士に与えられる（③、④）

４．顧客データベースに司法書士が代理権限を持っていることが登録される（A）

５．発起人等は登記申請書類に電子署名を行う（⑤）

６．司法書士は公開鍵証明書（PKC）を使用し、申請書類に電子署名を行う（⑥）

７．司法書士は登記所に電子申請を行う（⑦）

８．登記所は（B）の認証局で署名者の確認を行い、また、(C）で司法書士の本人確認および代理権を確認する

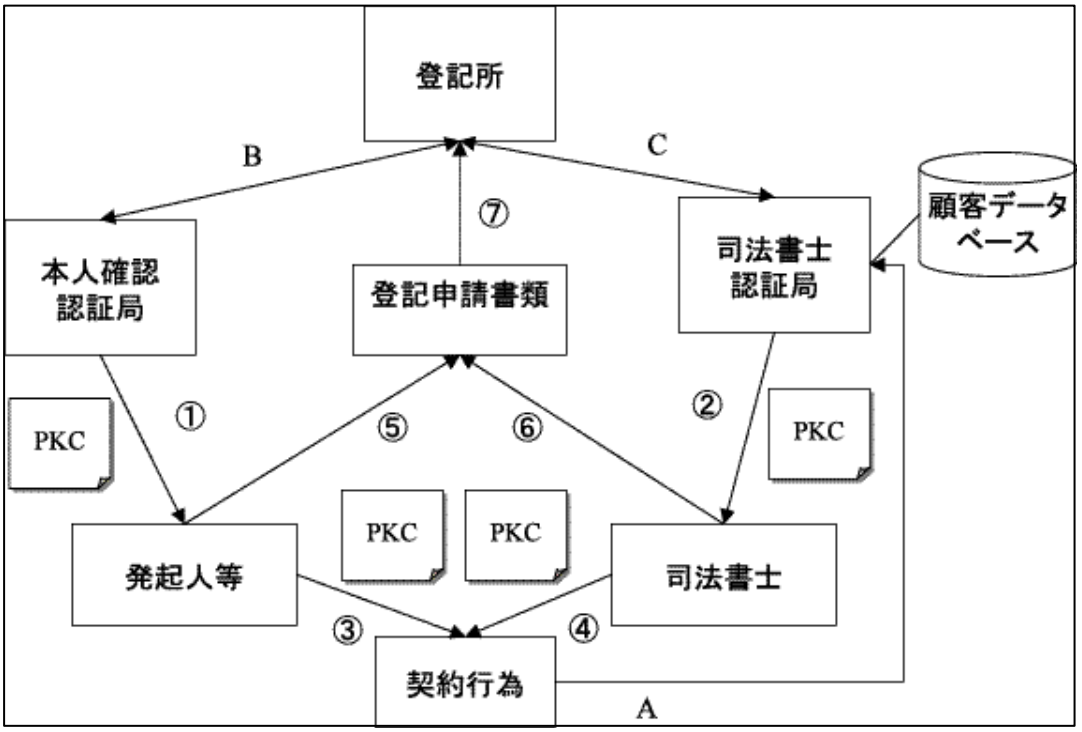


図 3-18 法人登記の電子申請モデル２

3.4.2.4　設計の詳細化

表 3-19 設計の詳細化

項目	検討結果
前提となる認証局の決定	● 本人確認用認証局：特定認証業務認定認証局を利用
セキュアトークンの設計・選択	● 本人および司法書士向け：認証局のポリシーに依存
開発環境の設定	● SAML 又は AC に対応した仕組みが必要
外部連携の再整理	● 本人確認用認証局はブリッジ接続された特定認証業務認定認証局を想定。公的個人認証局は司法書士が有効性確認を行えない為、活用しにくい

3.4.3　電子投票

住民と行政機関の間で行われるオンラインサービスとして、電子投票を想定し設計を行う。ここでは「住民の投票権」という属性情報に着目する。

3.4.3.1　提供サービスの明確化

表 3-20 提供サービスの明確化

項目	検討結果
サービス内容・提供形態の整理	● インターネット経由で、投票を行う
利用者の想定	● 投票者（選挙人）は自宅などからインターネットにアクセスできる環境がある ● 投票者（選挙人）は本人認証用の公開鍵証明書を持っている
環境条件の調査	● 選挙管理委員会が投票者（選挙人）の情報を管理している ● インターネット上に投票者（選挙人）を認証する認証局がある ● インターネット上に投票所（サイト）の実在を保証する第三者機関がある
コスト要件の検討	● システム運用管理コストは必要最低限に抑える（目標：＊＊＊円/年程度）
リスク（セキュリティ、信頼性）要件/制約の検討	● 投票者（選挙人）名と投票内容の漏洩 ● 投票者（選挙人）の成りすまし ● 重複投票 ● 投票結果の改ざん
法令遵守の調査	● 公職選挙法 ● 電子署名法
ビジネスストーリの検討	● 順次投票の種類を拡大する ● 順次投票者（選挙人）を拡大する

3.4.3.2 実現上の要件定義

表 3-21 実現上の要件定義

項目	検討結果
属性情報の整理	● 日本国民で年齢満 20 年以上の者（衆議院議員及び参議院議員の選挙権） ● かつ引き続き３箇月以上市町村の区域内に住所を有する者（地方公共団体の議会の議員及び長の選挙権） 時間：年齢は先天性、住所はあまり変化しない情報 信頼性：公的な裏づけや社会的な信頼性が必要 目的：正当な有権者であること
サービス利用シナリオの検討	● 選挙管理委員会が、投票時前に投票者に対して投票権情報を発行する ● 投票者は投票時間中に投票所サイトにアクセスし、投票権情報を提示する ● 投票所サイトは投票権情報をもとに本人確認と投票権の有効性を確認し、まだ投票していないことを確認する ● 投票者は、匿名で投票を行う
認証から認可のシナリオの検討	● 選挙管理委員会が毎年３月、６月、９月、12 月および選挙を行う場合に、区域内の投票人（選挙人）を把握しシステム登録を行う ● 投票者から提示された投票権情報をもとに、システム登録の有無を確認する ● さらに、投票者の投票状況を確認し、未投票の場合に投票を許可する
システム性能の検討	● 投票日の午前７時から午後８時 ● ＊＊＊件/時。１処理当り＊秒以下。
登場人物の整理	● 選挙管理委員会：投票者（選挙人）および投票者の投票権の有無を管理する ● 投票所（サイト）：投票者からの投票を匿名で受付け、投票内容の保証を行う ● 投票者（選挙人）：投票を行う
利用インフラ/サービスの整理	● 投票者の認証局が提供する PKC 検証サービス

3.4.3.3　実現モデルの選択

表 3-22 実現モデルの選択

項目	検討結果
属性情報活用パターンの実現方式から選択	● 要件をもとに実現モデルは別図のようになる ● 投票者の成りすましを防止するために、実現モデル３を採用する
バリエーションの検討	

(1) モデル１

電子投票の実現モデル１のフローを示す。

１．投票者は認証局から公開鍵証明書（PKC）を入手する

２．選挙管理委員会は選挙人名簿をもとに、投票者に投票用の公開鍵証明書（PKC）を発行する

３．投票者は投票所へ投票用紙と投票用公開鍵証明書を送信し、投票を行う

４．投票所は選挙管理委員会へ投票用公開鍵証明書の有効性を問合せ、有効であれば投票用紙を投票情報として DB で管理する

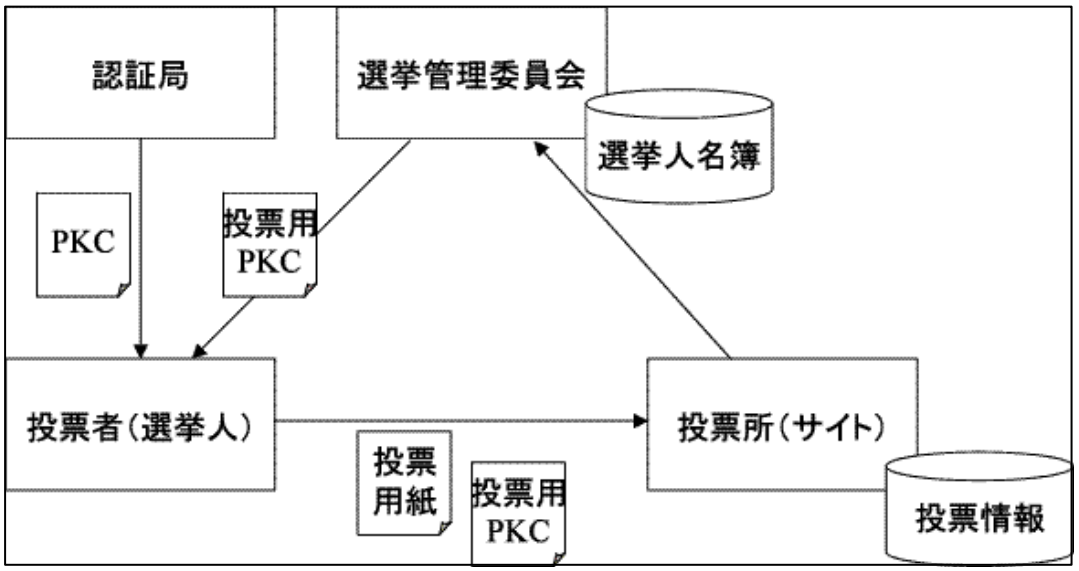


図 3-19 電子投票の実現モデル１

(2) モデル２

電子投票の実現モデル２のフローを示す。

１．投票者は認証局から公開鍵証明書（PKC）を入手する

２．選挙管理委員会は選挙人名簿をもとに、投票者に投票用の属性証明書（AC）を発行する

３．投票者は投票所へ投票用紙、公開鍵証明書および属性証明書を送信し、投票を行う

４．投票所は選挙管理委員会へ属性証明書の有効性を問合せ、有効であれば投票用紙を投票情報として DB で管理する

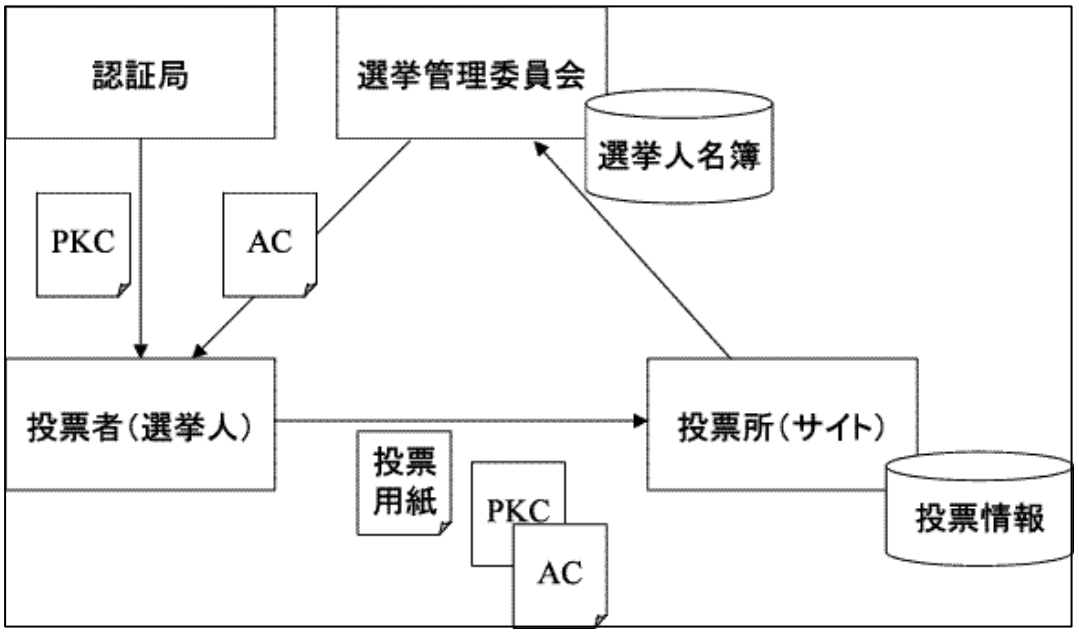


図 3-20 電子投票の実現モデル２

(3) モデル３

電子投票の実現モデル 3 のフローを示す。

１．投票者は認証局から公開鍵証明書（PKC）を入手する

２．投票者は投票所へ投票用紙、公開鍵証明書を送信し、投票を行う

３．投票所は選挙管理委員会へ投票人の投票権を問合せる

４．選挙管理委員会では投票所からの問合せに対して、選挙人名簿を参照し回答する

５．投票所は選挙管理委員会の回答が有効であれば、投票用紙を投票情報として DB で管理する

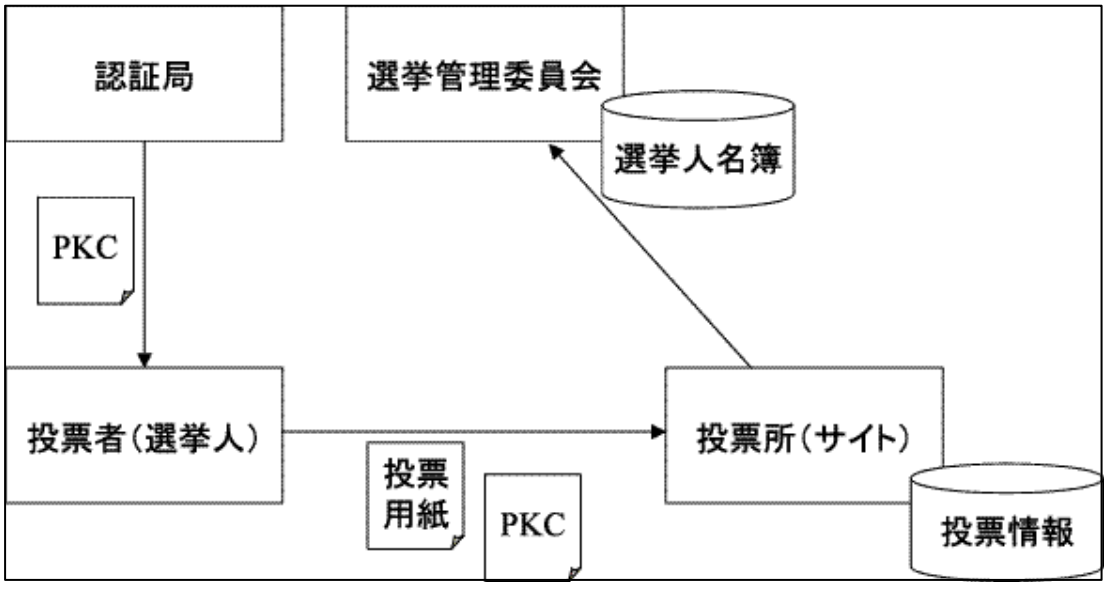


図 3-21 電子投票の実現モデル３

3.4.3.4　設計の詳細化

表 3-23 設計の詳細化

項目	検討結果
前提となる認証局の決定	● 認証局(1)：投票者（選挙人）の本人性を公的に保証する認証局（公的個人認証サービス） ● 認証局(2)：選挙管理委員会を保証する認証局、既存流用
セキュアトークンの設計・選択	● 公開鍵証明書を発行する認証局の運用に依存
開発環境の設定	● 投票用紙に選挙管理委員会がブラインド署名を行う場合、ブラインド署名を行うソフトウェアが必要
外部連携の再整理	● 投票者の認証局は＊＊＊

3.4.4　健康診断情報の共有サービス

社員、健康保険組合、医療機関、医師の間で行われる情報共有オンラインサービスとして、健康診断情報開示サービスを想定し設計を行う。ここでは情報開示に伴う本人確認（社員および医師）と関連する属性情報に着目する。

3.4.4.1　提供サービスの明確化

表 3-24 提供サービスの明確化

項目	検討結果
サービス内容・提供形態の整理	● インターネット経由で、健康保険組合、医療機関、診断担当医、社員、および医師に対して本人の健康診断結果を開示するまでの一連の作業に関して検討する
利用者の想定	● 利用者はインターネットにアクセスできる環境がある ● 利用者は本人認証用の公開鍵証明書を持っている
環境条件の調査	● 通常使用されているインターネット接続端末環境に対応する必要がある
コスト要件の検討	● システム運用管理コストは必要最低限に抑える（目標：＊＊＊円/年程度）
リスク（セキュリティ、信頼性）要件/制約の検討	● 診断情報の改ざんに対する担保 ● 診断情報の漏洩防止
法令遵守の調査	● 電子署名法 ● 個人情報保護法
ビジネスストーリの検討	● 健康診断情報のオンライン化による情報処理の効率化 ● 情報開示による診察の効率化

3.4.4.2 実現上の要件定義

表 3-25 実現上の要件定義

項目	検討結果
属性情報の整理	● 社員は自分の健康診断情報閲覧権限をもっている 時間：有効期間は生涯通して 信頼性：開示は許可した場合のみ 目的：健康管理の為参照 ● 健康診断担当医師は診断を担当した社員の健康診断情報の編集権限をもっているが、後日の修正は履歴が残る形でしかできない ● 診察担当医師は社員に許可されれば健康診断情報の閲覧権限が与えられる
サービス利用シナリオの検討	前提条件： ● 健康保険組合は複数の健康診断医療機関と契約している ● 医療機関はオンラインで社員からの健康診断の申込みを受け付け、健康診断を実施し、その結果をオンラインで閲覧可能にする ● 社員は健康保険組合員としての電子証明書を所有している ● 健康診断担当医師は担当した診断に関する編集権限をもっている。医師は医師であることを証明する公開鍵証明書（PKC）を保持している ● 診察担当医師は社員が診察を受けに来た場合、社員の承諾を得た後、過去の健康診断の記録を閲覧する。医師は医師であることを証明する公開鍵証明書（PKC）を保持している 利用シナリオ１（健康診断の予約、診断、結果の閲覧）： ● 社員は健康診断を受ける為、健康組合のホームページから契約診療所を探し、その医療機関に予約する。 ● 社員は、健康診断を受ける ● 社員にはメール等にて健康診断の結果通知を受け取り、医療機関のホームページに用意された専用ページで結果、過去の結果との比較、健康診断担当医師からのアドバイスなどを受けられる 利用シナリオ 2（診察）： ● 社員が出張先で急病になった場合、診察担当医師に過去の健康診断の結果を開示する。医師は豊富な情報を元に正しい診断ができ、社員も早期回復。

認証から認可のシナリオの検討	● 健康保険組合は社員が契約組合員であることを認証（証明）しなくてはならない ● 医療機関は、社員が健康保険組合員であることの認証、健康診断担当医師および診察担当医師の認証を行い、各自の属性に伴う権限の付与を行わなくてはならない
システム性能の検討	● 365 日、24 時間のサービス提供 ● ＊＊＊件/日。コンテンツの送信時間は＊秒以下。
登場人物の整理	● 健康保険組合認証局：健康保険組合が組合員（社員）を認証する電子証明書を発行 ● 医師認証局：医師であることを認証する電子証明書を発行 ● 社員：健康診断を受ける組合員 ● 健康診断担当医師：健康診断の結果をレビューする医師 ● 診察担当医師：社員が病気の際、治療する医師
利用インフラ/サービスの整理	● 健康保険組合ホームページ：健康保険組合が組合員に対するサービスを提供するウェブサイト ● 健康診断ホームページ：医療機関が予約受付、健康診断情報開示サービスを提供するウェブサイト

3.4.4.3　実現モデルの選択

表 3-26 実現モデルの選択

項目	検討結果
属性情報活用パターンの実現方式から選択	● 要件をもとに実現モデルは図 3-22 のようになる。 ● 一見モデル１の方が簡単に見えるが実際には複数の医療機関がある為、実装は複雑になる。また、既存の技術では簡単に他人の PKC を受け取ってその他サイトに提示する方法が存在しない為、モデル２を選択する。 ● モデル２ではSAMLによるSSOの権限および属性情報の受け渡しを想定している
バリエーションの検討	● 属性証明書を使用したモデルはモデル１と同等である為、検討の対象外にした

(1) モデル１

健康診断情報の共有サービス実現モデル１のフローを示す。本モデルでは公開鍵証明書（PKC）のみを使用したモデルである

健康診断の予約、診断、結果の閲覧

１．社員は健康保険組合認証局から組合員であることを証明する公開鍵証明書（PKC）を所有し

ている（①）

2．社員は公開鍵証明書（PKC）を使用し、健康保険組合ホームページへアクセスし（②）健康保険組合が契約している医療機関のホームページへアクセスする

3．医療機関の健康診断ホームページでは契約している健康保険組合の会員の公開鍵証明書（PKC）でログインできるように事前に設定されている（A）

4．社員は公開鍵証明書（PKC）を使用し健康診断の予約を行う（③）

5．健康診断担当医師は医師認証局から医師であることを証明する公開鍵証明書（PKC）を所有している（④）

6・医療機関の健康診断ホームページでは契約している健康診断担当医師の公開鍵証明書(PKC)でログインできるように事前に設定されている（B）

7．健康診断担当医師は公開鍵証明書（PKC）を使用し、社員の健康診断結果に対する診察を行い、コメント等を追加する（⑤）

8．社員は PKC を使用し、健康診断結果を閲覧する（⑥）

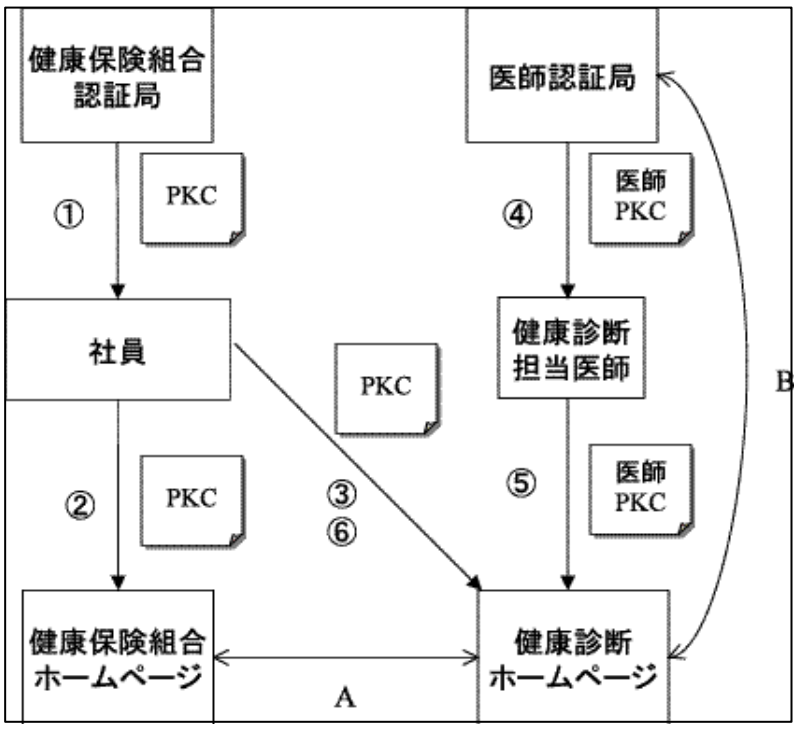


図 3-22 健康診断情報の共有サービス実現モデル１（予約・診断・結果閲覧）

診察

1．診察担当医師は医師認証局から医師であることを証明する公開鍵証明書（PKC）を所有している（①）

2．社員（患者）は病院で医師から過去の健康診断結果を参照したいと申請を受け、医師の公開鍵証明書（PKC）を得る（②）

3．社員は自分の公開鍵証明書（PKC）で健康診断ホームページへアクセスし、医師の公開鍵証明書（PKC）に対して閲覧許可の権限を付与する（③）

4．医師は公開鍵証明書（PKC）を使用し、健康診断ホームページへアクセスし、社員の健康診断結果を閲覧する

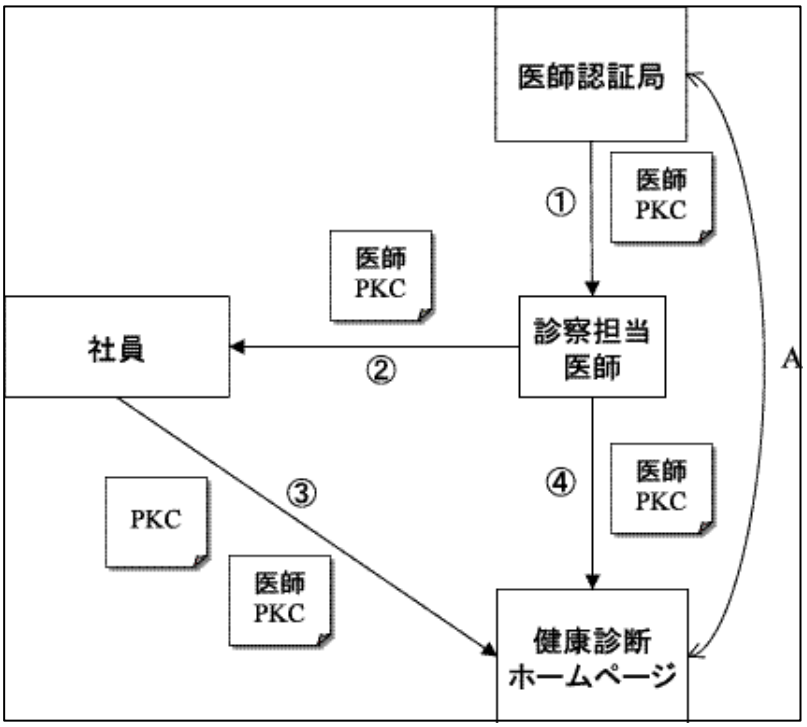


図 3-23 健康診断情報の共有サービス実現モデル１（診察）

(2) モデル２

健康診断情報の共有サービス実現モデル２のフローを示す。本モデルではデータベースに対して属性情報を照会するモデルである。

健康診断の予約、診断、結果の閲覧

1．社員は健康保険組合認証局から組合員である証明する公開鍵証明書（PKC）を所有している（①）
2．社員は公開鍵証明書（PKC）を使用し、健康保険組合ホームページへアクセスし（②）、健康保険組合が契約している医療機関のホームページへアクセスする
3．医療機関の健康診断ホームページでは契約している健康保険組合の会員であればログイン（SSO）できるように事前に設定されている（A）
4．社員は健康診断の予約を行う（③）。この場合公開鍵証明書（PKC）を再度提示する必要はない
5．健康診断担当医師は医師認証局から医師であることを証明する公開鍵証明書（PKC）を所有している（④）
6．医療機関の健康診断ホームページでは契約している健康診断担当医師がログインできるように事前に設定されている（B）
7．健康診断担当医師は社員の診断担当になった時点で社員の担当である属性情報が医師・患

者データベースに記録され、書込み権限も付与された状態になる（C）

8．健康診断担当医師は公開鍵証明書（PKC）を使用し、社員の健康診断結果を診察し、コメント等を追加する（⑤）

9．社員は PKC を使用し、健康診断結果を閲覧する（⑥）

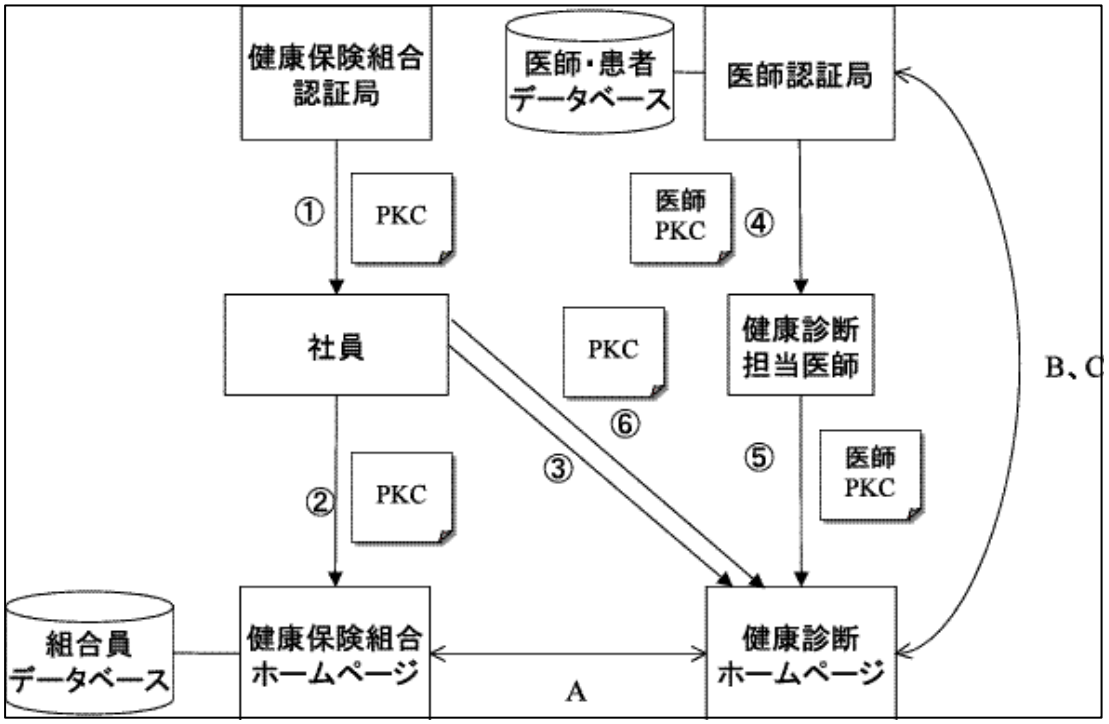


図 3-24 健康診断情報の共有サービス実現モデル２（予約・診断・結果閲覧）

診察

1．社員（患者）は病院で受付時に自分の公開鍵証明書（PKC）を提示し、また医師が過去の健康診断結果を参照してもいいという許可を出す（①）

2．社員を診療中であることおよび健康診断情報の閲覧許可を持っている属性情報が医師・患者データベースに記録される（A）

3．診察担当医師は医師認証局から医師であることを証明する公開鍵証明書（PKC）を所有している（②）

4．医師は公開鍵証明書（PKC）を使用し、健康診断ホームページへアクセスし、社員の健康診断結果を閲覧する（③）。この際、権限は医師・患者データベースの情報を元に付与される（B）

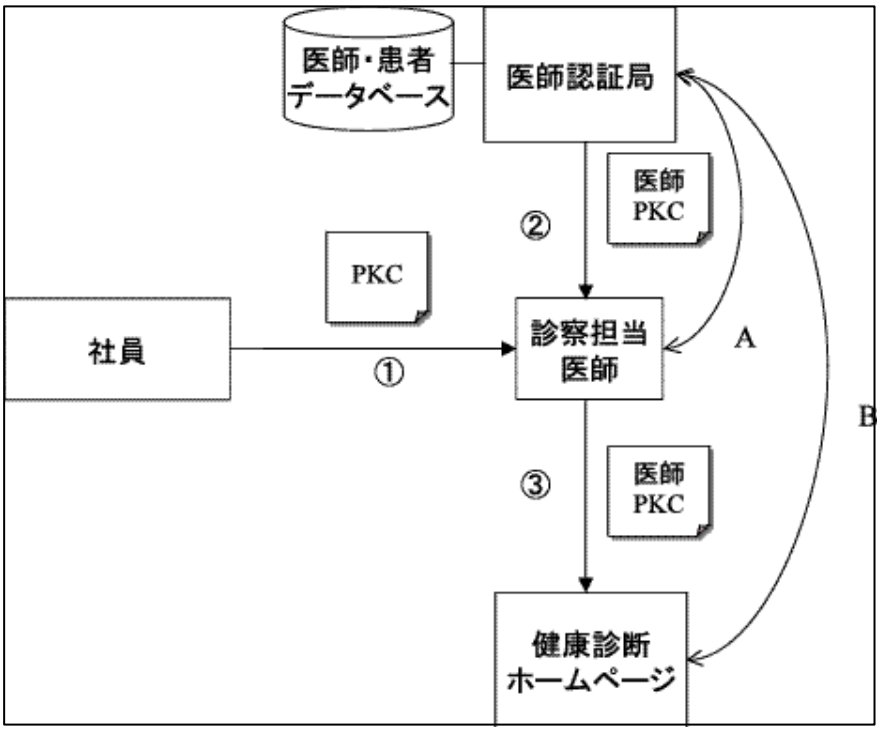


図 3-25 健康診断情報の共有サービス実現モデル２（診察）

3.4.4.4 設計の詳細化

表 3-27 設計の詳細化

項目	検討結果
前提となる認証局の決定	● 認証局：既存のものがない場合は新たに立ち上げる
セキュアトークンの設計・選択	● 健康組合員向け：既存の健康保険書を兼ねた IC カードなどが妥当 ● 医師向け：医師認証局のポリシーに依存
開発環境の設定	● SAML に対応した仕組みが必要
外部連携の再整理	● 健康保健組合の認証局は健康保健組合業界として供用し、コスト削減が可能

4．今後の展望

e-Japan 戦略Ⅱの発表に見られるように、世界最先端の IT 国家実現に向けた推進が政府主導で行われている。その中で、IT 国家の中核となるセキュリティ基盤として PKI（公開鍵基盤）の利活用が重要視されている。特に、サイバー空間における文書の改ざん・なりすまし・秘匿、及び電子商取引等における相手認証等を目的として電子署名、暗号化に使用される電子証明書の役割が重要となっている。

２章、３章で電子証明書の利用に関するガイドラインとして利用者の立場及びサービス提供者の立場での記述がなされているが、本章では証明書の利用動向及び証明書利用促進のための提言を今後の展望として記述している。

4.1 証明書利用動向

(1) インターネットショッピング

インターネットを用いたオンラインショッピングの多くの Web サイトでは、利用者にクレジットカード番号などの個人情報の入力を求める際､その情報が他に漏れることのないよう、Web サーバと消費者のブラウザ間でデータ通信を暗号化している。そのため Web サーバ用電子証明書を導入するのが最も一般的な方法である。

さらに最近では、利用者に本人確認用の電子証明書を発行して、成りすまし、改ざんを防ぐ仕組みをもったサービスが導入され始めている。

(2) オンラインバンキング

インターネットを利用した銀行のオンラインバンキングサービスがあたりまえになりつつある。ほとんどの Web サイトは、Web サーバ用電子証明書を用いて、利用者と Web サーバの間を SSL 通信によりデータを暗号化している。また、インターネットショッピング業者と提携し、インターネット上で決済が出来るようにするため、電子証明書を認証用に用いるサービスもある。

(3) e-Japan 戦略

2001 年 1 月に e-Japan 戦略が政府の IT 戦略本部で決定された。e-Japan 戦略には、「5 年以内（～2005 年）に世界最先端の IT 国家実現」目標が掲げられている。

2003 年 7 月、e-Japan 戦略に代わる新たな e-Japan 戦略Ⅱが発表された。旧戦略ではブロードバンド環境などの IT インフラ整備を重点に進められ、ADSL などのサービスが普及したことで、目標は達成しつつあると評価されている。

新戦略では、IT インフラを活用し、社会経済システムの積極的な変革を理念とし、さらに「医療」「食」「生活」「中小企業金融」「知」「就労・労働」「行政サービス」の 7 分野で IT 活用の先導的取り組みを実施する予定となっている。電子政府については、「行政サービス」の分野で取り上げられており、総合的なワンストップサービスの仕組み、利用者視点に立っ

た行政ポータルサイト整備（2005 年度末まで）などの実現を目指している。

(4) 電子政府および政府認証基盤（GPKI）

政府は、1999 年の「ミレニアム・プロジェクト」によって、政府と民間の間の行政手続きをインターネットを用いてペーパレスで行える電子政府構想を発表した。この構想に基づき、2003 年度中に政府認証基盤（GPKI）の構築を完了することになっている。

GPKI は、総務省が設置するブリッジ認証局（以降、BCA）と中央府省が設置する認証局（以降、府省 CA）により構成され、現在、BCA、府省 CA とも運用を始めている。

府省 CA から官職へ証明書が発行されている。各種の電子申請に対する申請者側の検証に利用されている。

国土交通省では、工事および建設コンサルタント業務などにおいて、平成 15 年度から電子入札を全面的に実施している。入札参加者は、決められた民間認証局から電子証明書を取得し、電子入札システムを利用することができる。

(5) 電子自治体

地方公共団体の行政サービスの電子化を実現するために、総合行政ネットワークの整備、住民基本台帳ネットワークシステムの稼動、組織認証基盤の整備、住民が電子申請を行う上で本人確認のための公的個人認証サービスの運用開始、電子窓口の整備などが進められている。

(6) 総合行政ネットワーク

総合行政ネットワーク（以下、「LGWAN」）は、全国の地方公共団体を相互に接続するとともに、国の府省間のネットワークである霞ヶ関 WAN とも相互に接続するネットワークである。「e-Japan 重点計画」によると、2003 年度までに全ての市区町村に対しネットワークへ接続を要請するとなっている。

LGWAN は 2003 年度中に開始される予定の公的個人認証サービスに利用されることが考えられている。さらに電子文書による許認可等行政処分の通知や行政文書の電子交換を行うための、地方公共団体における組織認証基盤（以下、「LGPKI」（Local Government Public Key Infrastructure））も 2003 年度中に整備され、LGWAN はインフラとして利用されることになっている。LGPKI では、地方公共団体の処分権者が行った電子署名を確認することになる申請者等に対して、当該公開鍵が本人（当該処分権者）のものであることを証明する職責証明書を発行する。

(7) 住民基本台帳ネットワークシステム

1999 年 8 月、「住民基本台帳法の一部を改正する法律」が公布され、この法律に基づき住

民基本台帳ネットワークシステム（以下、「住基ネット」）が整備されることになった。

住基ネットとは、住民票の記載事項として新たに住民票コードを加え、住民票コードを基に、行政機関に対する本人確認情報の提供、市町村の区域を越えた住民基本台帳に関する事務処理を行うための、各市町村の住民基本台帳のネットワークシステムである。

住基ネットにより、市区町村の区域を越えて国の機関などへ本人確認情報の提供が可能になる。2003 年 8 月から第二次稼動が始まり、国あるいは地方自治体の行政事務の中で住民票の写しの提出が必要とされている事務のうち、恩給や児童手当の支給、パスポートの交付申請など法律で定められた約 100 件の事務で、住民票の写しの提出が不要になった。

2003 年 8 月、住基ネット第二次稼動により、住民基本台帳カード（以下、「住基カード」）の配布が開始された。住基カードは高度なセキュリティ機能を有する IC カードを用いることとされており、住基ネット端末での本人確認に使われる他、電子証明書の格納が可能となる等の機能を持つ。市区町村の条例で規定することにより、住基カードを様々な目的に応じて利用することができるとされており、今後は電子証明書を用いた様々なサービスへの展開が期待される。

(8) 公的個人認証サービス

「電子署名に係る地方公共団体の認証業務に関する法律」（以下「公的個人認証法」）が 2002 年 12 月に成立し、都道府県及び市町村が連携して公的個人認証サービスの提供を行うこととされた。今後、公的個人認証サービス都道府県協議会において、制度構築及び全国実用試験に向けた作業が進められ、全国実用試験での検証を踏まえて、2003 年度中のシステム稼動が予定されている。住民に対しては、市町村窓口が本人確認を行い、都道府県知事名義で電子証明書を発行する。これにより、国および地方公共団体の行政手続きのオンライン申請・届出等に必要な個人認証サービスを地理的条件等による格差を生じることなく、低廉な費用で提供されると言われている。

また、電子商取引などのインフラとなる民間認証事業においては、信頼性が確保された本人確認を効率的に行うインフラとしての役割を果たすと考えられている。

(9) 海外事例　IPAI/SEC　PKI 関連技術解説資料から引用

＜アメリカ＞

連邦政府機関毎に PKI を導入。BCA を設置。政府職員のセキュリティ確保が主眼。証明書クラスが５段階存在している。

＜カナダ＞

政府 PKI は階層方式（シングルルート CA）。民間 CA とはピアツーピア方式で相互認証。外国 PKI との接続も考慮。政府が企業や市民に発行する認証書は、政府に対してのみ有効とさ

れており、企業や市民間での利用は認められていない。証明書クラスが 4 段階存在している。

＜オーストラリア＞

外国 PKI との接続も考慮。GPKA には政府公認の CA と非公認の CA を接続。

Gatekeeper という PKI に関する詳細な基準に従って実施しており、実際の運用は Gatekeeper 認定を受けた組織が行っている。個人のプライバシーに対する意識が強く日本のように住基ネットのようなものもないので地方自治体を含めた証明書の相互運用は現時点では行われていないが、オーストラリア企業番号電子署名証明書（ABN-DSC）のような共通の証明書を用いた相互運用方式の検討が行われている。

＜イギリス＞

米国のようなブリッジ認証局は設置せず、最上位認証局（ルート CA）を頂点としたピラミッド型の階層構造をもつ。PKI を利用した相互運用性を持つ多国間軍事情報システムを開発している。

4.2 証明書利用促進に向けた課題

本ガイドラインでは述べきれなかった今後の課題について下記にまとめた。

(1) 証明書のバリエーションを減らすための体制

単一目的証明書から特定目的証明書更に、汎用目的証明書が利用可能になることによって、証明書のバリエーションを減らすことが可能と考えられるが、そのためのサービス提供側（公共団体、業界他）における証明書利用に対する検討体制の設置が望まれる。

(2) 属性情報データベースを利用するための標準化および運用ガイドライン作成

サービス提供者が共通で利用できる属性情報データベースを想定し、アクセスのためのインターフェースの標準化が必要となる。PKI における LDAP、OCSP などに相当するプロトコルの取り決めも今後の課題となるだろう。さらに運用に関するガイドライン作成も望まれる。

(3) 個人情報登録のためのプライバシーポリシーの標準化

個人の属性情報の取扱については、個人情報保護法を遵守したプライバシーポリシー策定ガイドライン等の策定も今後必要と考える。

(4) PKC 拡張領域の利用ガイドライン作成

PKC の拡張領域の利用については、サービス提供者が個々のサービスに対応した証明書ポリシー（CP：Certificate Policy）で取り決めている。個別に作成することは、証明書検証者の負担が多くなることが想定され、証明書の利用拡大の観点からみると標準的な利用方法を記述したガイドライン作成も課題と捉えている。

(5) クウォリファイド証明書／属性型証明書の検討

本ガイドラインでは、PKC 及び AC を主に証明書利用の提言を行なってきたが、ESSSI で提案されている「クウォリファイド証明書」や、従来の証明書に法人名、部門名、肩書きなどの属性情報を追記した「属性型証明書」についての検討は行っていない。各標準化団体の動向にあわせて検討が必要である。

4.3 証明書利用促進のための提言

２章、３章では、利用者、サービス提供者それぞれの観点から証明書を利用するモデルを検討してきた。それぞれの立場で利用モデルを活用することにより、電子証明書活用の場面が一層広まることが期待される。インターネット社会が定着した今日、電子証明書普及の足がかりが出来たと言える。ここでは、今後、電子証明書利用が促進されるための提言を試みる。

２章では利用者の観点から証明書利用場面の実現モデル例を提示した。また、証明書を利用する際のサービスやシステムへの要求事項を信頼性、利便性、コストの３つの観点から整理した。利用者はサービスの中にこれら 3 要素がバランスよく取り込まれていなければ、証明書を使いたいとは思わないだろう。

利用者から見ると、サービス提供者の信頼性、認証局の信頼性を客観的にわかりやすく判断できる基準が欲しいところである。そのために、第三者機関による評価・格付け（レィティング）があると便利である。現在でも、オンラインショップの格付けや、企業の個人情報保護に関する認定制度などがあるが、利用者のわかる言葉でサービス業者の信頼度を総合的な情報として提供されるようになると､利用者のネット利用に対する不信感を払拭するのに役立つものと思われる。また、多くの利用者はサービス業者の指定する認証局の電子証明書を取得することになる。サービス業者は、利用者が最良の認証局を選択できるように情報を提供する役割も負うものと考えられる。

利便性向上の１つとして、使いやすいアプリケーションの充実が挙げられる。現在のアプリケーションは他のアプリケーションとの間の互換性が無かったり、操作やインストールの際、専門知識が要求されたりするなど、課題も少なくない。使い勝手の良いアプリケーションが世の中に出てくることで、証明書利用に加速がつくと期待される。

３章ではサービス提供者の観点から、証明書利用場面の実現モデルをいくつかのパターンに整理し提示した。サービス提供者は、提供したいサービスの要件から実現モデルを選択し、システム実現方式を導くことができるだろう。

システム実現の上で、PKI は標準が定まっていないことや、参考にできるものが少ないことが一つ障壁となっていると考えられる。そこで、PKI ベンダーや標準化団体などが集まって、小規模でも利用できる PKI を実現するための標準モデルが作成されると、敷居が低くなって普及にはずみがつくのではないだろうか。

さらに、PKI 普及促進団体などが中心になり、低コストで生産性の高い PKI の事例を収集、整理して、希望するサービス業者がこの資料を簡単に手に入れられるようしてはどうだろう。

証明書の利用形態が拡大していく中、利用者及びサービス提供者双方による、本ガイドラインを参考にした安全で安心できる証明書利用環境の実現は、更なる証明書の利用促進となることに期待して提言とする。

あとがき

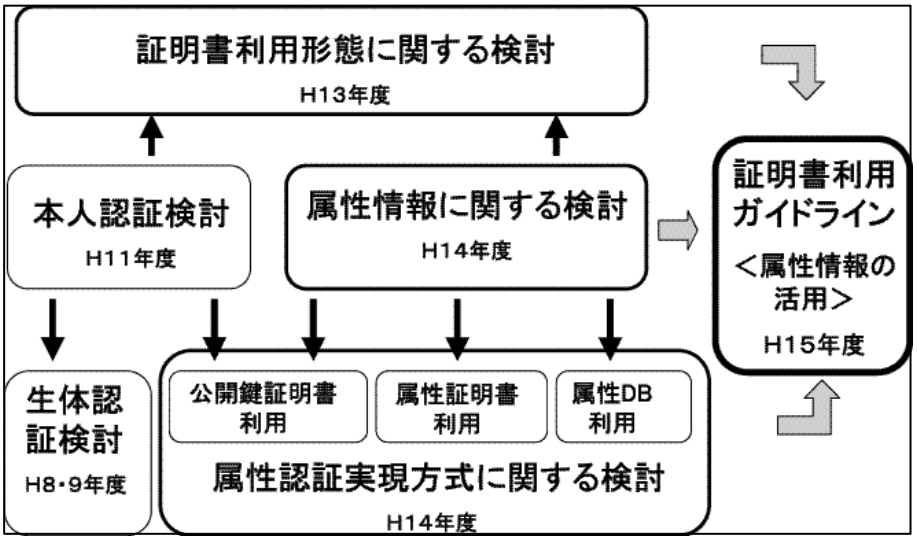
インターネット上で、成りすましを防止するシステムとして PKI の利用が広がりつつある。同時に、本人確認に加えて、その人の役割、権限を示す属性情報の活用もシステムごとに検討が進められている。

属性情報の活用も含めた認証システムの相互運用性を考えると、多くの企業がひとつのガイドラインに沿ってシステムの設計を行うことが望ましい。

認証公証 WG の電子認証利用検討 SWG では、1999 年度に、「認証のレベルと本人確認方式に関する提言」としてリアル社会で行われている本人認証の分析を多面的に行い、2001 年度には「証明書利用形態に関する考察」として、「利用者はどのような利用範囲の証明書を何枚持つようになるのか」といった分析を、いくつかの利用場面を想定して行った。また 2002 年度には、「証明書利用形態に関する考察　その２」として、いくつかの利用場面を想定し、属性を用いて認証する場合について、詳細な分析を行った。

今年度は、2001 年度、2002 年度に行った「証明書利用形態に関する考察」、「証明書利用形態に関する考察　その２」の検討結果に基づき、属性情報の利用を含む利用者が使いやすい証明書のあり方について、システム構築者が検討する際のガイドラインとして本報告を作成した。

属性認証に関する検討の枠組みを下図に示す。



属性認証に関する検討の枠組み

今回、企業の個別の利害を離れて、利用者の立場にたって電子証明書の利用のしやすさの検討を行い、特に属性情報を認証システムの枠組みに組み入れるかを検討・整理し、本ガイドラインとしてまとめることができた。

今後、このガイドラインの利活用を推奨していくとともに、国内外の関係機関にも普及していきたいと考えている。

本ガイドラインが、多くの人に参考にされ、活用されることを願ってやまない。

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.ID（Identification）

ID とは本人を確認（Authentication）するためのユニークな情報である。

指紋・虹彩・DNA などのバイオメトリクス情報は代表的な ID 情報だが、一般的に ID は単一情報で構成されるとは限らない。

3.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。

4.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。

5.PKC 拡張領域

X.509v3 公開鍵証明書において標準領域以外に追加された領域。鍵使用目的のような標準拡張と独自拡張がある。

6.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。

7.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。

8.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）。

9.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。

10.検証者

署名検証を行う人。

11.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。

12.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。

13.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。

14.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。

15.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。

16.証明書利用形態（本 SWG で作成した用語）

（1）単一目的証明書（Single Purpose Certificates）

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 を含む電子証明書。

（2）特定目的証明書（Specific Purpose Certificates）

閉じた世界（国、地域、業界、或いは個人が決めた特定の世界などでも可能）の中で、ユニークに個人を特定できる ID を含む電子証明書。

（3）汎用目的証明書（Universal Certificates）

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電子証明書。

17.証明書ポリシー

認証局が証明書を発行するにあたって設定するサービスや運用等に関する方針や規定。CP（Certificate Policy）とも呼ぶ。

18.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。

19.署名者

署名生成を行う人。

20.署名生成

電子文書に対して、署名者の秘密鍵を用いて暗号化することにより電子署名を施し、署名付き電子文書を生成する行為のこと。紙の文書に捺印する場合に相当する。

21.信頼点、信頼点情報

利用者が信頼する認証局の証明書。通常は、自分の証明書を取得した認証局のルート認証局であることが多い。信頼点は、検証者が署名者証明書の正当性を確認する際に利用される。

22.属性（Attribute）

属性とは対象者に与え（Authorization）られた資格や権限、職責、地位等をあらわす情報である。ID が単独で使用されることがあるのに対し、属性は単独で使用されることはない。

23.属性証明書（Attribute Certificate）

属性認証機関（AA）が発行し、証明書に添付する主体者の属性を指定するもの。公開鍵証明書がパスポートのようなもので、属性証明書は添付する査証（ビザ）のようなものである。属性証明書で定義する属性は、グループ名、組織名、セキュリティ区分などがある。

24.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。

25.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、本ガイドラインでは、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。

26.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。

27.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。

28.なりすまし

他者のふりをする不正行為。

29.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。

30.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。

31.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。

32.ハッシュ関数

電子文書に電子署名を施す際などに、その電子文書をある一定の大きさまで圧縮するための計算手順。ハッシュ関数の計算結果である圧縮データをハッシュ値、あるいはメッセージダイジェストと呼ぶ。ハッシュ関数には、あるハッシュ値が与えられたときに、それと同じハッシュ値となるような電子文書を求めることが困難であるという性質（一方向性）と、同じハッシュ値となる二つの異なる電子文書を探し出すことが困難であるという性質（衝突回避性）がある。

33.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。

34.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。

35.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。

36.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。

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
松山　博美	電子商取引推進協議会（ECOM）	主席研究員
川松　和成	電子商取引推進協議会（ECOM）	主席研究員

顧問

大山　永昭	東京工業大学　教授
菅　知之	関西大学　　教授
平田　健治	大阪大学　大学院　教授
米丸　恒治	神戸大学　大学院　教授

TF４メンバー（執筆メンバー）

氏名	会社名
相原　敬雄	日本ベリサイン株式会社
小田原　秀幸	日本電信電話株式会社
斉藤　幹男	富士電機情報サービス株式会社
篠原　秀直	三菱電機株式会社
田中　　稔　　（リーダ）	三菱電機株式会社
千葉　寛之	株式会社日立製作所
中山　　亮	株式会社 NTT データ
春田　克治	日本認証サービス株式会社
東山　栄一　　（リーダ）	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
守　　隆之	川鉄情報システム株式会社

SWG２メンバー（上記以外）

氏名	会社名
川島　慶一	株式会社 UFJ 銀行
河田　悦生	株式会社 NTT ドコモ
久保田　信也	KDDI 株式会社
関野　公彦	株式会社 NTT ドコモ
高橋　健司	株式会社損害保険ジャパン
土居　武宏	株式会社オーエムシーカード
冨岡　直樹	株式会社帝国データバンク
仲村渠　　剛	三菱電機情報ネットワーク株式会社
西谷　研ニ	株式会社 UFJ 銀行
野口　一宙	KDDI 株式会社
能勢　健一郎	株式会社東芝
横井　雅彦	NTT コミュニケーションズ株式会社

平成 15 年度　経済産業省　委託事業
ＥＣ技術基盤の相互運用性に関する調査研究事業
（取引相手先の属性認証技術等の調査）
証明書利用ガイドライン
―属性情報の活用―
平成 16 年３月発行

発行所　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園３丁目５番８号
機械振興会館３階
TEL：03(3436)7500
印刷所　新高速印刷株式会社
東京都港区新橋 5-8-4
TEL：03(3437)6365

この資料は再生紙を使用しています。