参考資料４

経済産業省委託調査

平成１４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）

属性認証の利用モデル

平成15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１４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１４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。

はじめに

本書は「属性認証の適用ガイドライン」の姉妹編として、属性認証の具体的な利用モデルについて考察した事例集である。「属性認証の適用ガイドライン」と併せてお読みいただき属性認証に関する考察を深めていただければ幸いである。

内容は、「インターネットショッピング」、商業登記証明書と社内の委任状を利用した電子申請について述べた「代理人による法人の電子申請」、個人が電子申請等において一時的に代理人を指定して行う届出について述べた「代理人による個人の届出」の３章構成になっており、それぞれについて、属性認証の利用適用場面と、運用上の特徴、さらには属性証明書の記述例を載せている。

なお、記載する利用例で、前提とする認証局/PKC の実現性等に課題もあるが、利用例の検討材料として提示する旨をお断りしておきたい。

「属性認証の適用ガイドライン」と同様に、本書の中で使用される略語について以下に明記しておく。

AA（題名等では属性認証局と記述）：Attribute Authority
AC（題名等では属性証明書と記述）：Attribute Certificate
CA（題名等では認証局と記述）：Certificate Authority
PKC（題名等では証明書と記述）：Public key Certificate
AC 保有者：Attribute Certificate Holder
AC 検証者：Attribute Certificate Verifier
AC 利用者（AC 保有者と AC 検証者を総称して使用）
AC 発行対象者（特定の章で、定義した上で使用）

平成 15 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

図表一覧目次

1. インターネットショッピング

本章ではインターネットショップでの属性証明書の利用事例を紹介する。

1.1 属性認証の利用

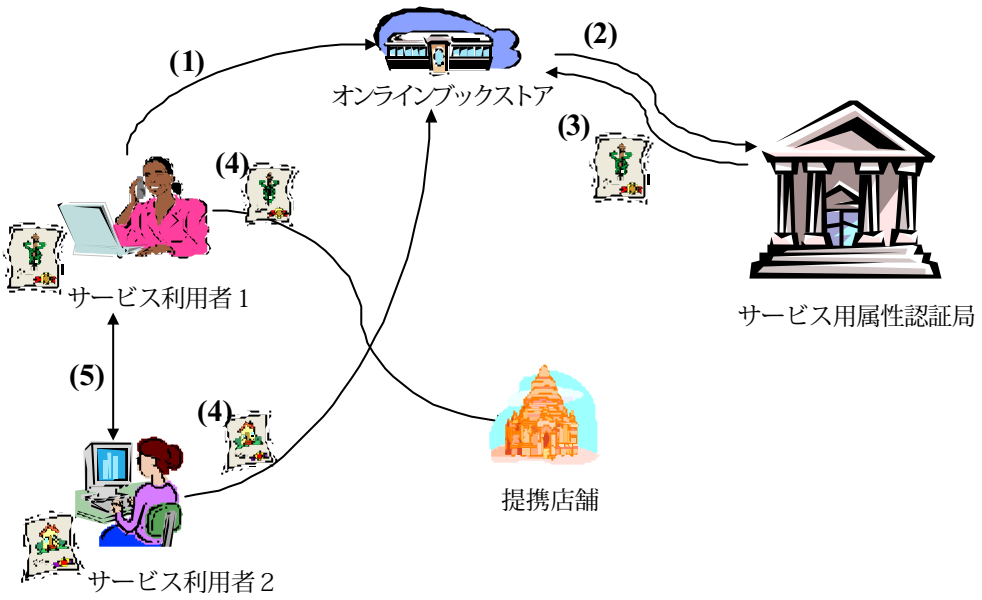

図 1-1 構成図

1.1.1 登場人物

本業務における登場人物を以下に示す。

- オンラインブックストア（サービス提供者）
  サービスサイトを持つ書店
- オンラインブックストア属性認証局（AA）
  オンラインブックストアが運営する属性証明書発行局
- 提携店舗（提携サービス提供者）
  オンラインブックストアが提携する店舗（例：CD 販売業者）
- サービス利用者（ユーザ）
  オンラインブックストアおよび提携店舗のサービスを受ける人

1.1.2　ビジネスフロー

基本的なビジネスフローは以下の通り。

1. サービス利用者はサービス提供者：オンラインショップのサイトに利用者登録する
2. オンラインショップはサービス用の属性認証局に対して利用者の属性（利用実績等）に応じた属性証明書の発行依頼を行う
3. サービス用属性認証局は、属性証明書の発行を行う
4. オンラインサービス利用者は本ショップにてあるいは提携オンラインショップにてオンラインサービスを受ける際に属性証明書を提示する事により会員制サービスや特典サービス、割引サービスが受けられる
5. また、オンラインサービス利用者間においても、この属性証明書を用いて、オンラインショップからのデジタルコンテンツのやりとりや情報交換が可能になる（例：利用者会員としてゴールド会員間であれば、利用者間で特定のコンテンツを期限限定で利用可能）

1.1.3 業務上の特徴

この業務の特徴は、以下の通り。

- 属性有効期間
  オンラインサービスからの属性は永続的な値ではなく、サービス利用実績やサービス提供側の都合に応じて変化する短期的なものであると考えられる。従って失効リストを用いない場合や失効そのものを行わない場合も考えられる。
- 属性の有効範囲
  発行したオンラインサービスあるいは提携業務を行っているサービス会社からのサービス、さらにはそれらから提供されたコンテンツに関するオンラインサービス利用者間での利用に限る。
- 属性証明書の申請および利用
  属性証明書の発行要求者と発行対象者、利用者は原則として同一である。なお、発行要求者、発行対象者、利用者の識別は公開鍵証明書をもって行う事を前提としており、本報告書では指紋照合等による個人の特定方法に関しては言及しない。
- 利用者公開鍵証明書と利用者属性証明書の多重度
  オンラインサービス利用者は、業務提供内にある複数のサービス提供者から、異なる属性値を持つ複数の属性証明書を発行される事が考えられる。

1.2　運用手順

ここでは、本システムを属性証明書にて実装した場合の、運用手順について説明する。なお、PKC は既に各登場人物に発行されているものとする。

1.2.1　属性認証局及び属性証明書のモデル構成

以下に、本システムにおける、AC の発行と検証のモデルを示す。

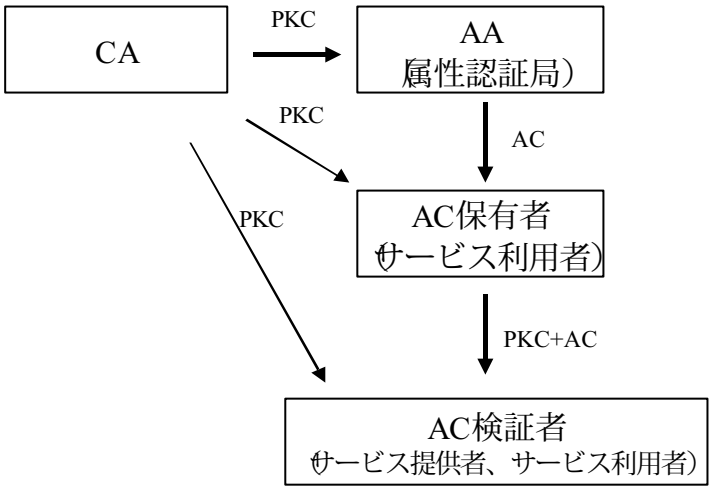

図 1-2　属性証明書モデル

1.2.2　属性証明書発行手順

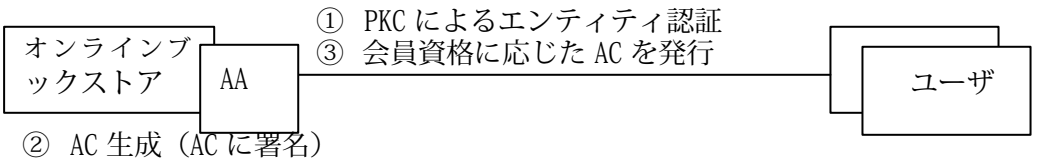

図 1-3　属性証明書発行手順

1.2.3 属性証明書利用手順

ケース1

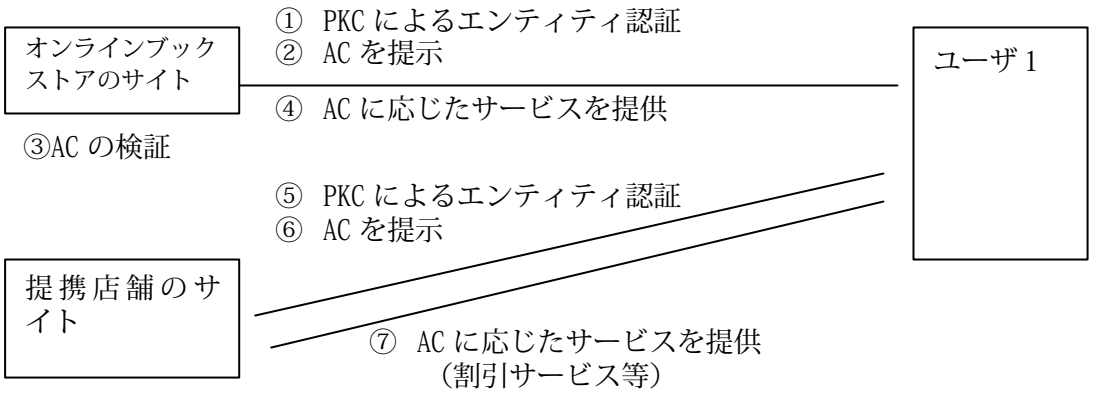

図 1-4 属性証明書利用手順（1）

ケース2

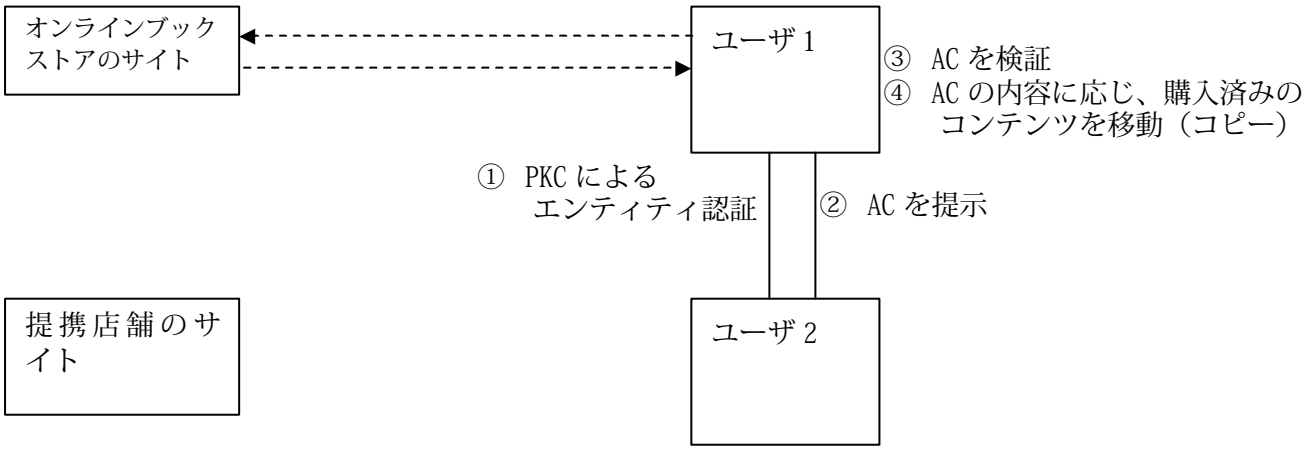

図 1-5 属性証明書利用手順（2）

1.2.4 失効

1.2.4.1 失効リストを利用するケース

1.2.3 において検証を行う際に失効リストのチェックを行う。失効されている場合は権限を認めず 1.2.2 の手順を用いて再発行を行なわせるものとする。

属性認証局は、定期的に失効リストの作成を行い、オンラインサービス提供者に送付する。

1.2.4.2 失効リストを利用しないケース

本ケースにおいては、属性認証局にて属性証明書を発行する際、属性証明書の有効期限を短く設定する。

1.2.3 において検証を行う際に失効リストのチェックは行わない。属性証明書の有効期限が切れている場合は権限を認めず、1.2.2 の手順を用いて再発行を行なわせるものとする。

1.3 運用上の特徴

1.3.1 属性証明書を使うメリット

本業務で取り扱うサービスを受けるための属性は、利用者の利用実績等に応じて変化するため頻繁に更新が発生する。また、永続的に利用するものである保証もないため、属性を証明する証明書の有効期限は短く設定するのが好ましい。従って、公開鍵証明書の属性での実装では、発行・失効手続きが頻繁に行われるため、速度を向上させることが難しい。また、一枚の属性証明書は複数のサービスに対して利用されることも想定されるため、サービスごとのデータベースを用いて属性管理を行うよりも汎用的な属性認証基盤を構築する方式が、より相互運用性が高まると考えられる。

1.3.2 属性証明書の内容

ここでは、本システムにおける属性証明書の一例を示す。

以下は、属性証明書の内容である。

表 1-1　属性証明書の内容例

項目名	説明	備考
holder	サービス利用者の公開鍵証明書の発行者とシリアル番号	属性証明書に永続性が求められないため、entityName などを使う必要はない。
issuer	属性認証局の DN 名	
attrCertValidtyPeriod	NotAfterTime：有効期間終了時刻	属性証明書の有効期限は、サービス利用者の公開鍵証明書の有効期限よりも一般的に短い。
attributes	属性情報	表 1-2 参照のこと

AC の attributes 属性内に書かれる情報としては、以下が考えられる。

表 1-2　属性値の内容例

項目名	説明	本ケースでの値例
Access Identity	アクセス識別子	対象となるサービス名
Charging Identity	課金識別子	サービス利用者がサービスを利用する際の課金のための識別情報（ID）
Group	グループ情報	サービス利用者が属するグループ（会員レベル）
Role	サービス利用者の役割	上記サービスにおいて提供されるコンテンツに関する操作権限を規定した役割
Clearance	サービス利用者に適用されるポリシーレベル	サービス利用者の個人情報などに対するアクセス権限などに対するポリシー
encAttrs	暗号化された属性値	サービス利用者の氏名その他の個人情報、サービスへのアクセス鍵等（データ内容を保護するために、暗号化して格納する）

2. 代理人による法人の電子申請

法人が行政（中央官庁系）に対して行う電子申請・電子調達等のオンラインサービスにおいて、法人代表者より委任を受けた代理人が、一括して代行するモデルを想定する。

本モデルは、法務省商業登記 CA が発行する法人代表者の証明書を用いて委任するための 1 つの解決案を示すものであるが、運用面、制度面においては課題が残されている。本事例では法務省商業登記 CA が AA の PKC を発行することを前提としているが、これは現在の法務省商業登記 CA では想定されていない。

現在、代理人による電子申請の業務形態の中には、代理人である業務担当者の PKC を申請受付側に事前に登録しておくことで、代理人とみなして業務が行われている例があるが、属性認証技術を用いることによって申請受付側での事前登録作業をなくし、利便性を高めることが目的である。

2.1 属性認証の利用

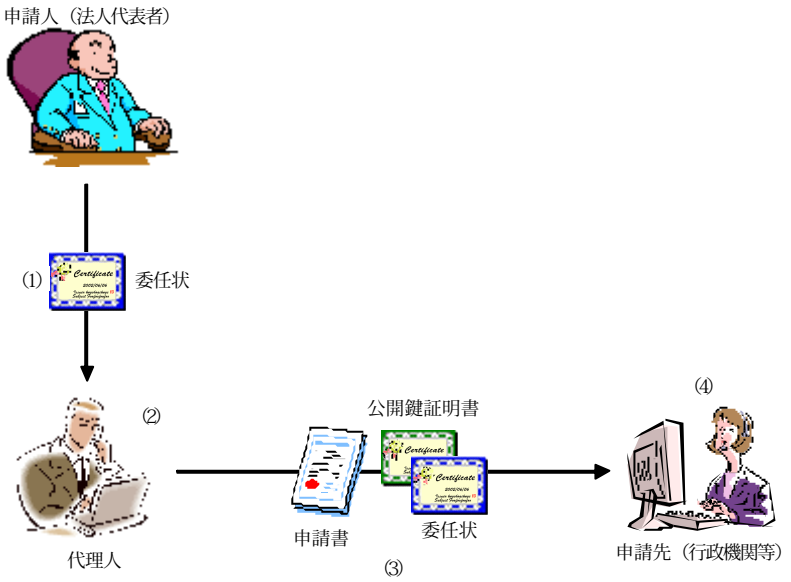

図 2-1 構成図

2.1.1 登場人物

本業務における登場人物を以下に示す。

- 申請人（法人代表者）
  電子申請・電子調達等の手続きを申請する企業の代表者である。申請人は、法務省商業登記 CA から発行された法人代表者用の PKC を所有しているものとする。
- 代理人（法人代理人）
  電子申請・電子調達等の手続きを代行して実施する者である。営業部長、資材部長等、申請人と同じ企業に属する人間、あるいは、司法書士、行政書士、税理士等の特有の資格を

有する人間などが代理人として想定される。代理人は、GPKI ブリッジ認証局と相互接続しており、電子署名法で定められた特定認証業務の認定を受けた民間 CA から発行された個人用の PKC を所有しているものとする。

- 申請先（府省が運用する業務用サーバ）
  代理人より送られた申請を受理し、申請人に関する各種手続きを行う。府省が提供する電子行政手続用のサーバ、あるいは、当該業務における担当官職などが想定される。申請先は、当該府省が運営する GPKI 府省 CA の自己署名証明書を信頼しているものとする。
- GPKI 府省認証局
  申請先の府省が運営する官職を証明する CA である。申請先の信頼点となる PKC は、当該 CA の自己署名証明書であるとする。
- GPKI ブリッジ CA
  GPKI 府省 CA と法務省商業登記 CA、民間 CA と相互認証を行い、各 PKI ドメイン間の橋渡しをする役割を担う CA である。
- 法務省商業登記 CA
  「商業登記に基づく電子認証制度」に基づいて、法人代表者に PKC を発行する CA である。
- 民間 CA
  「電子署名及び認証業務に関する法律」に基づいて認定された認証業務を運営する CA である。当該 CA は、認定認証業務であり、かつ、GPKI ブリッジ CA と相互接続できているならば、一般の民間認証事業者とは限らず、企業内の個人を認証することを目的とした企業が運用する CA（すなわち、企業内 CA）であってもよい。

2.1.2 ビジネスフロー

基本的なビジネスフローは以下の通り。

1. 申請者は、代理人が当該の申請に対する代行を許可することを表す委任状（AC）を発行する。
2. 代理人は、申請書を作成し、代理人の署名を付与する。
3. 代理人は、申請書、代理人の PKC、委任状（AC）を電子行政の申請窓口に送る。
4. 申請先は、委任状（AC）の検証を行い、代理人に申請の権限があることを確認する。確認後、申請先は申請書に基づき申請処理を行う。

代理人が、他の申請についても代行権限を有している場合には、2 および 3 を同様に行う。

2.1.3 業務上の特徴

この業務の特徴は、以下の通り。

- 委任期間
  手続き代行に伴う委任は、永続的な関係ではなく、例えば、営業部長という役職にある間、１ヶ月・１年など定められた期間、業務遂行完了までの期間、業務１回のみ等、申請する

業務内容や申請人と代理人との契約関係等により、委任期間は変わってくるものと想定される。しかしながら、これらの委任期間は、PKC の有効期間と比較すると短い場合が多いと考えられる。

- 委任範囲の限定
  申請する業務内容や申請人と代理人との契約関係等によって、全権委任の場合もあれば、特定の手続きに限定される場合もあると想定される。申請先は、代理人より提示された委任状の検証を行うだけではなく、申請の対象が委任権限範囲内であることを確認する必要がある。なお、手続きの性質に応じて、委任内容の表示に求められる明確性、具体性の程度が異なることも想定される。
- 法人代表者による AC の発行
  AC の発行者は、法人代表者であり、AC を発行する際に使用する秘密鍵は、法務省商業登記 CA によって発行された当該法人代表者用の PKC に対応したものである必要がある。委任状は、申請人本人から代理人に対して発行されなければならないため、申請人が法人代表者であるならば、法人代表者として公に認められた電子署名を委任状に付与する必要がある。現時点では、法人代表者を公に認めた認証基盤は、「商業登記に基づく電子認証制度」のみである。
- 代理人 PKC と委任状の多重度
  代理人は、複数の申請者からの代行業務を同時に委任されることや複数の異なる代行業務を同時に委任されることが考えられる。従って、一人の代理人に対して、多数の委任状が発行される場合がある。

2.2 運用手順

ここでは、本システムを AC にて実装した場合の、運用手順について説明する。なお、PKC は既に各登場人物に発行されているものとする。

2.2.1 属性認証局及び属性証明書のモデル構成

以下に、本システムにおける、AC の発行と検証のモデルを示す。

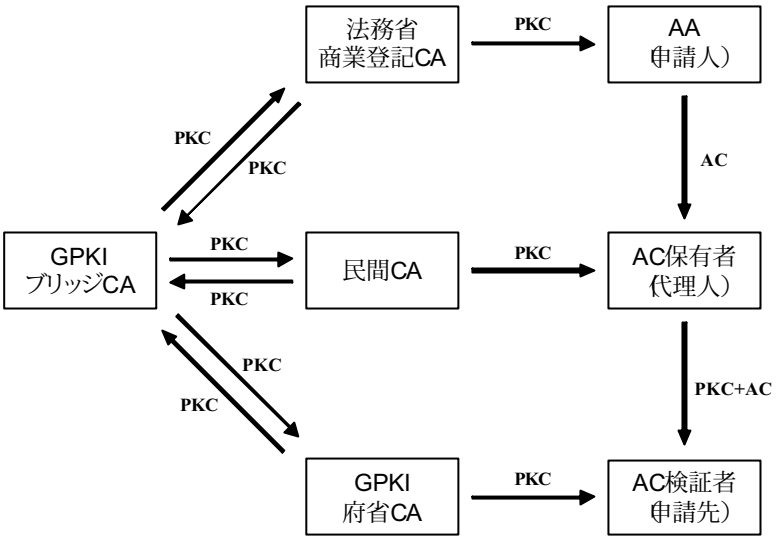

図 2-2　属性証明書モデル

ここでは、第一報告書「3.1 当事者とモデル」では記述していない相互認証を介したモデルとなっている。

2.2.2　属性証明書発行手順

AC の発行において、AC の発行を依頼する人が、申請人である場合と、代理人である場合が考えられるが、申請人が代理人に対して委任を行うので、通常は、申請人が AC の発行要求および発行を行うことになる。すなわち、第一報告書「3.2.1 属性証明書の発行手順 c)」の形式となる。この場合、申請人は、代理人の PKC（もしくは AC の holder フィールドに記載すべき情報）を事前に入手しておく必要がある。この入手方式についてはオンライン、オフラインのどちらでもよいが、入手した PKC が確実に委任しようとしている人の PKC であることを確認する。発行された AC は、申請人から代理人に渡される。渡す方法についてはオンライン、オフラインのどちらでもよい。

2.2.3　属性証明書利用手順

代理人は、電子申請の関わる申請書の作成を行い、申請先に送付する。申請書には、代理人の署名と PKC、申請人から発行された委任状相当の AC が含まれている。申請先は、受け取った申請書に付与されている代理人の署名の検証、代理人の PKC の検証、AC の検証を行う。代理人の PKC の検証や AC の検証上必要になる申請人の PKC の検証については、証明書検証サーバを用いて検証することができる。本モデルにおいては AC が失効されるケースもあるため、AC に noRevAvail 拡張が含まれていない場合については、AA に対して AC の有効性確認を行う。AC の検証後、AC に記載された委任内容を参照し、申請を行った代理人が代理権限を有していることを確認する。

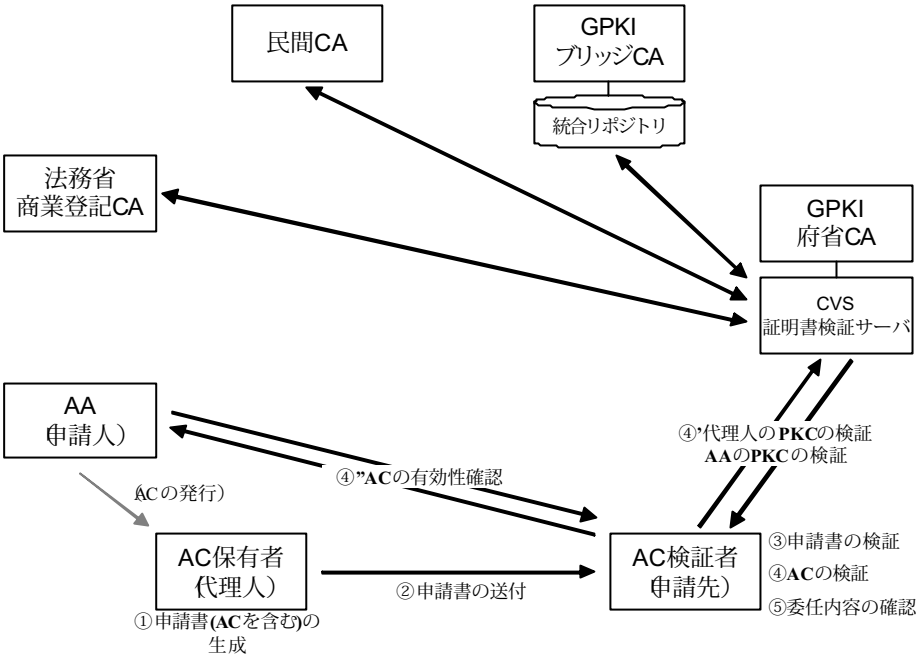

図 2-3　属性証明書利用手順

2.2.4　失効

委任期間の長い AC においては、有効期間が満了する前に AC の失効を必要とする場合がある。例えば、申請人による委任の中止や代理人の変更による委任権限の解除などの場合である。通常は、申請人が自身の権限に基づいて、代理人の AC を失効することになる。

2.3　運用上の特徴

2.3.1　属性証明書を使うメリット

本業務で取り扱う「代行権限」という属性は、委任する業務や委任先によって、その期間や範囲が決定されるが、通常は、一時的なものであり、公開鍵証明書の有効期間よりも短い場合が多い。従って、公開鍵証明書に属性を記載すると、発行・失効手続きが頻繁に行われるため、速度を向上させることが難しい。

また、一枚の属性証明書は複数のサービスに対して利用されることも想定されるため、サービスごとの DB を用いて属性管理を行うよりも汎用的な属性認証基盤を構築する方式が、より相互運用性が高まると考えられる。特に、本モデルでは、法務省商業登記 CA や民間 CA、GPKI といった既存の認証基盤を活用しており、これらの認証基盤の中に信頼点を置くユーザであれば AC の検証を行うことができるため、非常に広範な範囲で委任状を利用することができるようになる。

2.3.2　属性証明書の内容

ここでは、本システムにおける属性証明書の一例を示す。

以下は、属性証明書の内容である。

表 2-1　属性証明書の内容例

項目名	説明	備考
holder	代理人の発行者とシリアル番号	属性証明書に永続性が求められないため、entityName などを使う必要はない。
issuer	法人代表者の DN 名	
attrCertValidtyPeriod	NotAfterTime：有効期間終了時刻	属性証明書の有効期限は、委任期間より短くする場合も考えられる。
attributes	属性情報	表 2-2 参照のこと

AC の attributes 属性内に書かれる情報として、以下がある。

表 2-2 属性の内容例

項目名	説明	備考
Access Identity	アクセス識別子	委任対象となるサービス名などが入る。
Role	役割	上記サービスにおける委任上の役割などが入る。

3. 代理人による個人の届け出

引越し等に伴う、銀行や各種オンラインサービスなどに対する住所変更等の手続を、本人より委任を受けた代理人が、一括して代行する場合を想定し、属性証明書の利用事例（案）を紹介する。

3.1 属性認証の利用

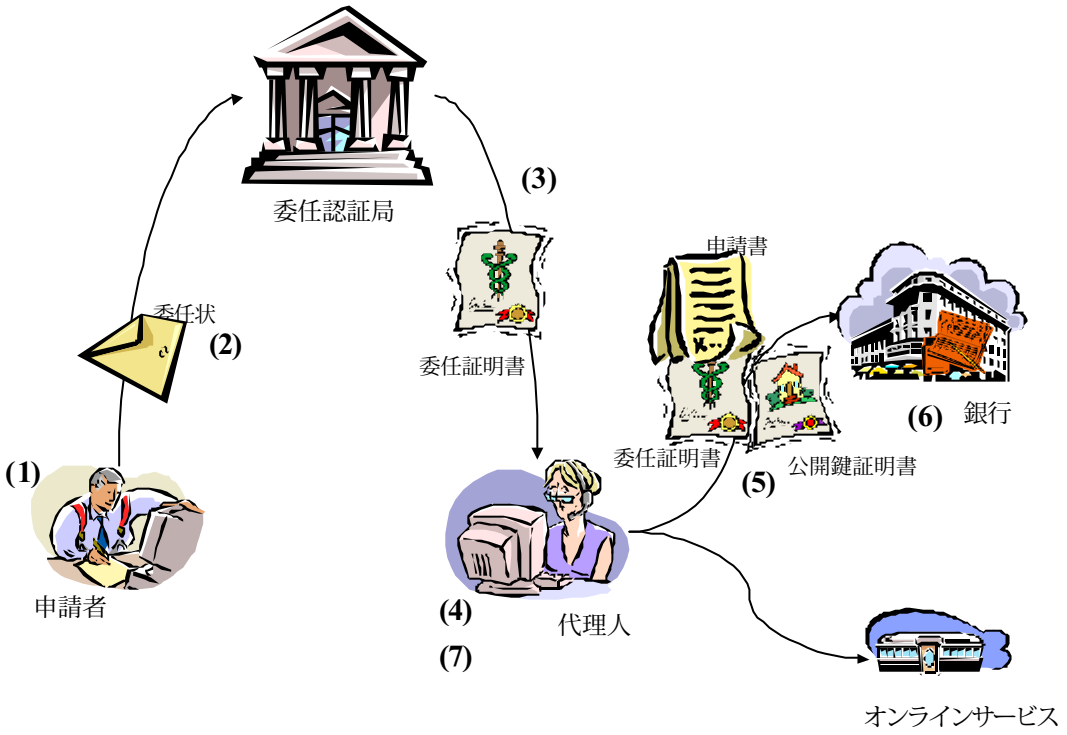

図 3-1 構成図

3.1.1 登場人物

本業務における登場人物を以下に示す。

- 申請人
  住所の変更に伴う、手続きを行う。
- 代理人
  住所変更に伴う各種申請を代行して行う。ポータルサービスや引越し業者などが想定される。
- 申請先
  代理人より送られた申請を受理し、申請人に関する住所変更など手続きを処理する。銀行やショッピングサイトなどが想定される。

- 委任認証局
  申請者が代理人に対し委任したことを確認し、委任証明書を発行する。

3.1.2 ビジネスフロー

基本的なビジネスフローは以下の通り。

1. 申請者は、代理人が当該の申請に対する代行を許可することを表す、委任状を作成する。
2. 申請者は、委任状を委任認証局に対し送信し、委任証明書の発行を要求する。
3. 委任認証局は、委任状の署名を検証し、内容を審査する。次に、代理人の資格等を確認した後、代理人に対し委任証明書を発行する。
4. 代理人は、申請書を作成し、代理人の署名を付与する。
5. 代理人は、申請書、代理人の公開鍵証明書、委任証明書を申請窓口に送る。
6. 申請先は、委任証明書の検証を行い、代理人に申請の権限があることを確認する。確認後、申請先は申請書に基づき申請処理を行う。

代理人は、他の申請について、4 および 5 を同様に行う。

3.1.3 業務上の特徴

この業務の特徴は、以下の通り。

- 委任期間
  手続き代行に伴う委任は、永続的な関係ではなく、引越しに伴う短期的な関係であると考えられる。従って、通常引越し手続き終了までの期間は非常に短いと考えられる。
- 委任範囲の限定
  全権委任と異なり、委任状を使って代行できる範囲は引越しに伴う住所変更等の手続きに限定されると考えられる。代理人より提示された申請先は、委任状の検証を行うだけではなく、申請の対象が委任権限範囲内であることを確認する必要がある。
- 委任証明書の申請
  委任証明書の発行要求者（ここでは申請者）と発行対象（ここでは代理人）が異なる。
- 代理人公開鍵証明書と委任証明書の多重度
  代理人は、複数の申請者からの代行業務を同時に行うことが考えられる。従って、一人の代理人に対して、多数の委任状が発行される。

3.2 運用手順

ここでは、委任認証局が属性認証局を運用し、委任証明書として属性証明書を用いることによって実装した場合の、本システムの運用手順について説明する。なお、公開鍵証明書は既に各登場人物に発行されているものとする。

3.2.1 属性認証局及び属性証明書のモデル構成

以下に、本システムにおける、属性証明書の発行と検証のモデルを示す。

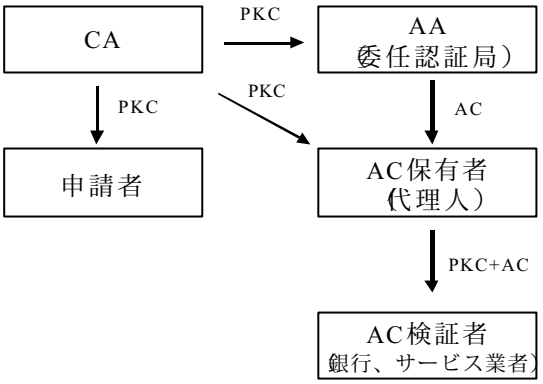

図 3-2 属性証明書モデル

ここでは、第一報告書「3.1 当事者とモデル」における Push 型モデル 1 を基本としている。

3.2.2 属性証明書発行手順

属性証明書の発行において、属性証明書の発行を依頼する人物が、申請者である場合と、代理人である場合が考えられる。通常、申請者が代理人に対し委任を行うことを委任認証局に対し発行依頼申請を行い、委任認証局が申請者本人による発行依頼申請であることを確認することで、代理人に対し属性証明書が発行される。一回の申請に対し一つのの属性証明書が発行されるだけではなく、変更手続きの数だけ複数の属性証明書が発行されることが考えられる。

代理人は、複数の手続きを平行して行い、また代行処理は緊急を要する場合が多いため、属性証明書発行手続きの効率化が重要になると考えられる。従って、発行手続きはオンラインで行われるほうが妥当であると考えられる。

3.2.3 属性証明書利用手順

代理人は、申請書に対し、代理人の公開鍵証明書と属性証明書委任証明書) を送付する。本システムでは、有効期限を短期間とし失効確認の必要性をなくし、属性証明書を添付することで属性認証局への問い合わせの必要性をなくす。

申請先が申請書を受け取った際には、代理人署名の検証、代理人証明書の検証及び、属性証明書の検証を行う。属性証明書の検証後、属性証明書内に記載された権限内容を参照し、代理人が申請の代行権限を有することを確認する。

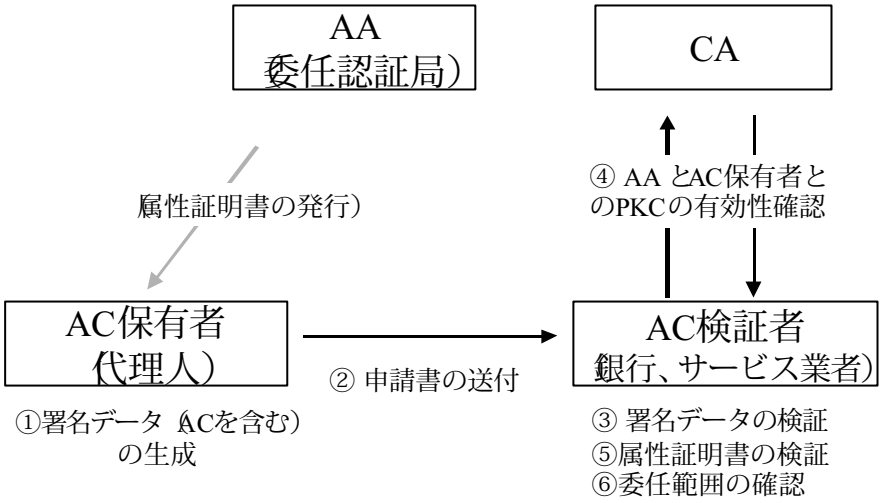

図 3-3 属性証明書利用手順

3.2.4 失効

本システムでは属性証明書の有効期限を短く設定しているため、当初の予定より代行手続きに時間がかかる場合、属性証明書が期限切れとなることが考えられる。この場合は、申請者が発行手続きを再度行うのではなく、代理人が再発行手続きを行うことも考えられる。

3.3 運用上の特徴

3.3.1 属性証明書を使うメリット

本業務で取り扱う「代行権限」という属性は、資格のような半永続的な属性と異なり、一時的なものであり、申請手続き終了後にその委任権限を速やかに失う。代理人を中心としてその権限管理の仕組みを考えた場合、一人の代理人は多数の申請者に対する代行権限を所有し、またその更新が頻繁に行われるため、属性証明書の利用が適している。また、一枚の委任証明書は複数のサービスに対して利用されることも想定されるため、汎用的な属性認証基盤を構築する方式を採用することで、より相互運用性が高まると考えられる。

3.3.2 属性証明書の内容

ここでは、本システムにおける属性証明書の一例を示す。

以下は、属性証明書の内容である。

表 3-1 属性証明書の内容例

項目名	説明	備考
holder	代理人の発行者とシリアル番号	属性証明書に永続性が求められないため、entityName などを使う必要はない。
issuer	委任認証局の DN 名	
attrCertValidtyPeriod	NotAfterTime：有効期間終了時刻	属性証明書の有効期限は、委任期間より短くする場合も考えられる。
attributes	属性情報	表 3-2 参照のこと
NoRevAvail	AC 破棄をサポートしていないことを示す。（拡張属性）	本システムでは AC の失効確認を行わないため、これを明示する。

AC の attributes 属性内に書かれる情報として、以下が考えられる。

表 3-2 属性値の内容例

項目名	説明	本ケースでの値例
Access Identity		代理申請可となるサービス名などが入る。
Role	代理人の役割	上記サービスの中から、代理申請可能な手続き名などが入る。
Clearance	代理人に適用されるポリシーレベル	申請人の個人情報などに対するｱｸｾｽ権限などに対するポリシーが格納されると考えられる。
encAttrs	暗号化された属性値	申請人氏名、申請人の公開鍵証明書など、申請者の個人情報を保護するために、暗号化して格納する。

本書の用語集

1. ＰＫＩ（Public Key Infrastructure）

公開鍵インフラ／公開鍵基盤とも呼ばれる。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。認証局（CA：Certification Authority）、登録局（RA：Registration Authority）、ディレクトリ（公開鍵証明書などを保管・開示する手段）、証明書有効性検証機関（VA：Validation Authority）、証明書を利用する利用者側のシステムなどが要素として含まれる。利用者側のシステムで行われる電子署名は、署名対象となる電子文書、あるいはそのハッシュ値を署名者の秘密鍵で暗号化する行為である。

2. GPKI、LGPKI（Government PKI, Local Government PKI）

各種申請・届出等の行政事務の電子化において基盤となる、政府及び自治体の PKI システム。

1999 年 12 月にミレニアム・プロジェクトが発表され、電子政府（行政事務の効率化、申請手続き軽減、情報公開、電子商取引促進）及び教育情報化に関する計画が明らかにされた。政府と民間の間のやり取りはインターネットが前提となっており、セキュリティを確かなものとすることは不可欠となっている。これら各種システムを安全に運用するために、GPKI 及び LGPKI の構築が進められている。

3. 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。

公開鍵暗号方式では「鍵ペア」と呼ばれる対となった二つの鍵が利用され、これらは公開鍵と秘密鍵と呼ばれる。公開鍵は、広く一般に開示する鍵で、検証者が署名検証を行う際に使用し、秘密鍵は署名を行う者自身が秘密に保持する鍵で、電子署名する際に使用する。

4. 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。

運用に際しては、認証局運用規定という、証明書発行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を作成する。それをＣＰＳ（Certification Practice Statement）とも呼び、一般に、利用者等に対して開示される。

5. リポジトリ（Repository）

加入者の証明書やＣＲＬおよびこれらに関連するその他の情報を保管しておき、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。

6. 登録局、登録機関

公開鍵証明書発行の申請者の本人性を確認し、主として登録業務を行う機関。

7. 発行局

電子証明書の作成･発行を主として発行業務を行う行う機関。

8. 公開鍵証明書

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。電子証明書、あるいは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があれば検出される形式となっており、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、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。

また、秘密鍵の危殆化、紛失等が生じた場合、証明書の所有者（署名者、または認証局）の指示に基づいて､有効期間内であっても証明書の効力を失わせることがあるが､これを証明書の失効と呼ぶ。

9. 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。ＣＲＬは、署名の検証者が、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場合に用いる。この他に､OCSP（Online Certificate Status Protocol）と呼ばれるプロトコルを使用してオンラインで失効確認する方法もある。

10. 相互認証

２つの認証機関（ＣＡ）が他方の認証機関を信頼することを証明し、安全に鍵情報を交換できるプロセス。

11. 電子署名法

2000 年 5 月に成立し､2001 年 4 月より施行された「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る旨が記述されている他､認証業務のうち一定要件を満たすものを特定認証業務と定義し認定を受けることができる、任意的な認定制度について記述されている。

12. 署名生成、署名検証

署名生成とは、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。紙の文書に押印する場合に相当する。

署名検証とは、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。

13. 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。

14. 属性証明局

公開鍵証明書の保有者が持つ属性を確認、審査し、属性証明書を発行する機関。AA（Attribute Authority）とも呼ぶ。

15. 属性証明書

公開鍵証明書が主に証明書利用者の特定に利用するのに対して、属性証明書はアクセス制御等に利用する。公開鍵証明書に記載された証明書所有者の名前によるアクセス制御も可能であるが、それのみならず、組織・団体における役職や役割などの属性情報によりアクセス制御を行うことも大いに考えられる。これら証明書所有者の属性情報を記載した証明書を、属性証明書と呼ぶ。これは、属性認証局（AA：Attribute Authority）により発行される。

16. 電子公証

電子認証と並んで、電子申請・企業間取引・電子文書長期保存等を支えるプラットフォームであり、一般的には、第三者（TTP：Trusted Third Party）による電子的記録の原本性を保証するサービス、として捉えられている。電子公証の意味合いは立場により解釈が異なる場合もあるが、共通的な認識としては、電子的記録の非改竄を保証し証拠能力を担保する為の一要素、非改ざんの保証は当事者ではなく第三者により行われる、電子公証の提供者が誰であるかは特に問わない、といった特徴を持つと言える。

本書の参考文献

[X.509-2000]

ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001,
"Information technology - Open Systems Interconnection -
The Directory: Public-Key and Attribute Certificate Frameworks".

[RFC2437]

B. Kaliski and J. Staddon, "PKCS #1: RSA Cryptography
Specifications Version 2.0", RFC2437, October 1998.
http://www.ietf.org/rfc/rfc2437.txt

[RFC2560]

M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams,
"X.509 Internet Public Key Infrastructure -
Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.
http://www.ietf.org/rfc/rfc2560.txt

[RFC3280]

R. Housley, W. Polk, W. Ford and D. Solo,
"Internet X.509 Public Key Infrastructure
Certificate and Certificate Revocation List (CRL) Profile",
RFC3280, April 2002.
http://www.ietf.org/rfc/rfc3280.txt

[RFC3281]

S. Farrell and R. Housley, "An Internet Attribute Certificate
Profile for Authorization", RFC3281, April 2002.
http://www.ietf.org/rfc/rfc3281.txt

[RFC3369]

R. Housley, "Cryptographic Message Syntax (CMS)",
RFC3369, August 2002.
http://www.ietf.org/rfc/rfc3369.txt

[OCSPv2]

M.Myers, A. Malpani and D.Pinkas,
"X.509 Internet Public Key Infrastructure
Online Certificate Status Protocol, version 2
draft-ietf-pkix-ocspv2-ext-01.txt", December 2002.
http://www.ietf.org/internet-drafts/draft-ietf-pkix-ocspv2-ext-01.txt

[XACML]

http://www.oasis-open.org/committees/xacml/index.shtml

http://www.xmlconsortium.org/websv/kaisetsu/C11/content.html

[SAML]

http://www.oasis-open.org/committees/security/docs/cs-sstc-core-00.doc

http://www.xmlconsortium.org/websv/kaisetsu/C10/content.html

http://www.atmarkit.co.jp/fsecurity/rensai/webserv04/webserv01.html

[XrML]

http://www.contentguard.com/

[XMCL]

http://www.xmcl.org/

[ODRL]

http://odrl.net/

[関連]

「代理申請の制度的・技術的課題について
～電子申請における代理申請のあり方について」
代理申請に関する制度的・技術的課題研究会

「電子申請業務における X.509 属性証明書を用いた資格確認技術の開発」
日立ソフトウェアエンジニアリング株式会社

メンバーリスト

事務局

松山　博美　電子商取引推進協議会　主席研究員
川松　和成　電子商取引推進協議会　主席研究員
前田　陽二　電子商取引推進協議会　主席研究員
小祝　香織　電子商取引推進協議会

リーダー

山下　真　　富士通株式会社

TF1/2 メンバー（編集メンバー）

氏名	会社名
高村　昌興	株式会社ＮＴＴデータ
小黒　博昭	株式会社ＮＴＴデータ
今枝　直彦	日本電信電話株式会社
手塚　優	エントラストジャパン株式会社
松山　科子	ソニー株式会社
洲崎　誠一	株式会社日立製作所
笈川　光浩	株式会社日立製作所
金谷　延幸	株式会社富士通研究所
佐伯　正夫	三菱電機株式会社
坂上　勉	三菱電機株式会社
鍛治俊彦＊	株式会社日本電子貿易サービス

（注）＊はオブザーバー

SWG1 メンバー（参加メンバー）

氏名	会社名
荻原　利彦	NTT コミュニケーションズ株式会社
宍倉　勝仁	シャチハタ株式会社
中原　康	株式会社東芝
島田　毅	株式会社東芝
中村　逸一	株式会社ＮＴＴデータ
立石　広治	株式会社ＮＴＴデータ
河田　悦夫	株式会社エヌ・ティ・ティ・ドコモ
関野　公彦	株式会社エヌ・ティ・ティ・ドコモ
内海　雅俊	川鉄情報システム株式会社
鈴木　良信	コンピュータ･アソシエイツ株式会社
佐藤　正康	コンピュータ･アソシエイツ株式会社
雨宮　隆征	セイコーインスツルメンツ株式会社
米倉　昭利	（財）日本品質保証機構（JQA）
星野　　理	株式会社帝国データバンク
岩本　光恵	日本電気株式会社
本間　史夫	日本認証サービス株式会社
塚田　孝則	日立ソフトウェアエンジニアリング株式会社
手塚　　悟	株式会社日立製作所
西谷　研次	株式会社 UFJ 銀行
保田　昌宏	中央青山監査法人

平成 14 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）
属性認証の利用モデル
平成 15 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