

経済産業省補助事業

平成 17 年度情報基盤対策技術開発等推進事業  
(次世代型電子認証基盤の整備)

全体概要報告書

平成 18 年 3 月

財団法人日本情報処理開発協会

## 序

ブロードバンドの急速な普及、無線技術の進展などによりインターネットを介した電子商取引や情報交換が広く行われている。しかし、相手を確認する認証の手続きは、それぞれのサービス毎に個別に行われているのが現状である。また、認証の方法も ID とパスワードのレベルから PKI を用いたレベルまで、これもサービス事業者毎に個別に設定されている。

インターネットを介した電子商取引が一般的となった今、一人の利用者が複数のサービスを利用するのは、ごく普通のこととなっており、サービス毎に認証の手続きを踏むのは不便と感ずることが多くなっている。即ち、複数のサービスが連携したより高い価値のサービスが提供されることが望まれているのである。

海外に目を移すと米国では、行政サービスにおける電子認証の連携を実現するための電子認証基盤となる“ e-Authentication Initiative ”や民間・政府を含めた新たなビジネスモデルを開発するための“ Electronic Authentication Partnership ”が活動している。

本事業は、経済産業省の補助金を受けて、米国等の先進事例の調査から電子認証の連携技術、電子認証に関するポリシー、新しい電子認証に関するビジネスモデルの策定を行いその結果を以下の報告書として取りまとめている。

- ・ 電子認証ビジネスモデル策定報告書
- ・ 先進アプリケーション事例調査報告書
- ・ 電子認証に関する調査報告書
- ・ 電子認証ポリシーガイドライン（案）基準規範編
- ・ 電子認証ポリシーガイドライン（案）基準規範編 評価報告書
- ・ 次世代認証基盤ソフトウェア（開発成果報告書）
- ・ 評価報告書

これらの報告書が、電子認証を基盤とした新しいビジネスの創出、電子商取引の付加価値向上の一助となれば幸いである。

平成 18 年 3 月

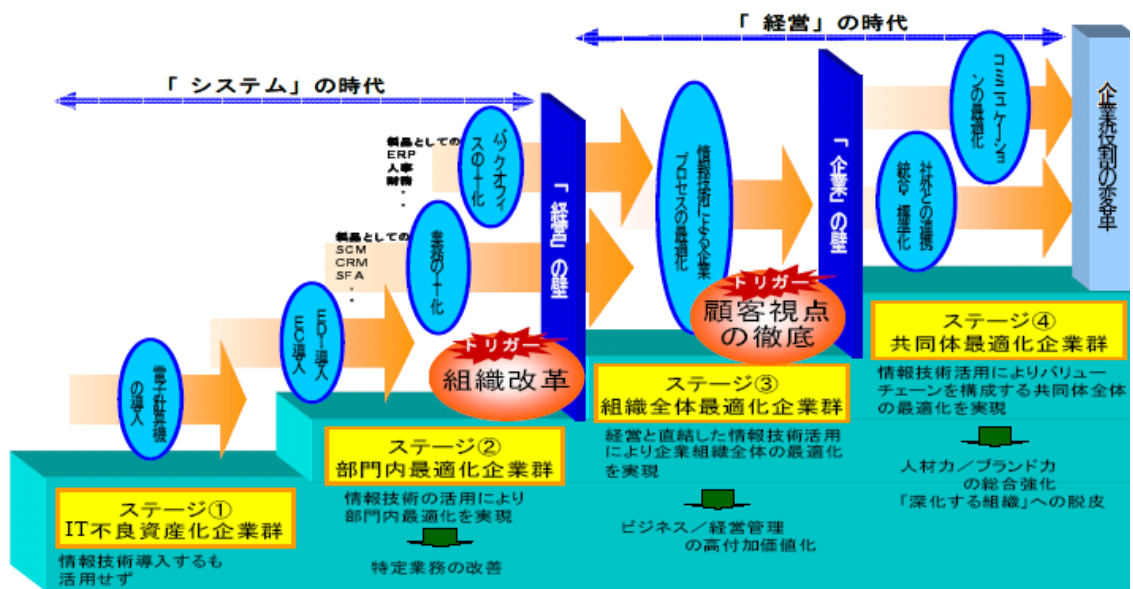
財団法人日本情報処理開発協会

- 目 次 -

1. 背景・目的	1
2. 実施期間	2
3. 推進体制	2
4. 全体概要	3
4.1 事業概要	3
4.2 実施方針	4
4.3 事業報告の構成	5
4.4 普及・啓発活動	7
5. 個別概要	7
5.1 電子認証ビジネスモデルの策定	7
5.1.1 電子認証ビジネスモデル策定	7
5.1.2 先進アプリケーション事例調査	8
5.2 電子認証ポリシーガイドラインの策定	9
5.2.1 電子認証ポリシーガイドライン（案）基準規範編策定	9
5.3 電子認証技術基盤確立	11
5.3.1 開発成果報告書	11
5.3.2 評価報告書	12

## 1. 背景・目的

近年、ブロードバンドの普及、高度な情報端末の小型化、無線技術の進展等によってIT環境が急速に変化しつつある。これを受けて、2005年4月に経済産業省は「情報経済・産業ビジョン」を発表した<sup>1</sup>。その中において、企業におけるIT投資を「ステージ」から「ステージ」までの4段階に分類し、IT投資の最大の効果を得るには、この4段階の最終段階である「ステージ 共同体全体の最適化」を実現することが必要であると述べている。IT化の進展において、インフラが整備されつつある今日の状況を、「ステージ」にあたるものと位置づけ、「ステージ」「ステージ」の実現に向け、今後目指すべきビジョンと戦略を取りまとめている。



(出典)「情報経済・産業ビジョン(産業構造審議会 情報経済分科会 平成17年4月)」

図 1.1 IT投資の4段階

本事業では、共同体全体の最適化に向けたプラットフォームとして、各サービスの連携による最適化を実現し、さらにはサービスの複合による価値の向上を実現するため、複数のサービスから共有可能な次世代型電子認証基盤の技術基盤を開発する。開発した技術基盤を採用した様々な企業間で認証の連携が行われることにより、新たな価値の創造、活力ある企業活動の実現を目的とする。

<sup>1</sup> 産業構造審議会情報経済分科会報告書「情報経済・産業ビジョン」の発表  
<http://www.meti.go.jp/press/20050427007/20050427007.html>

## 2. 実施期間

平成 17 年 7 月 19 日から平成 18 年 3 月 7 日

## 3. 推進体制

本事業の推進体制を「図 3.1」に示す。

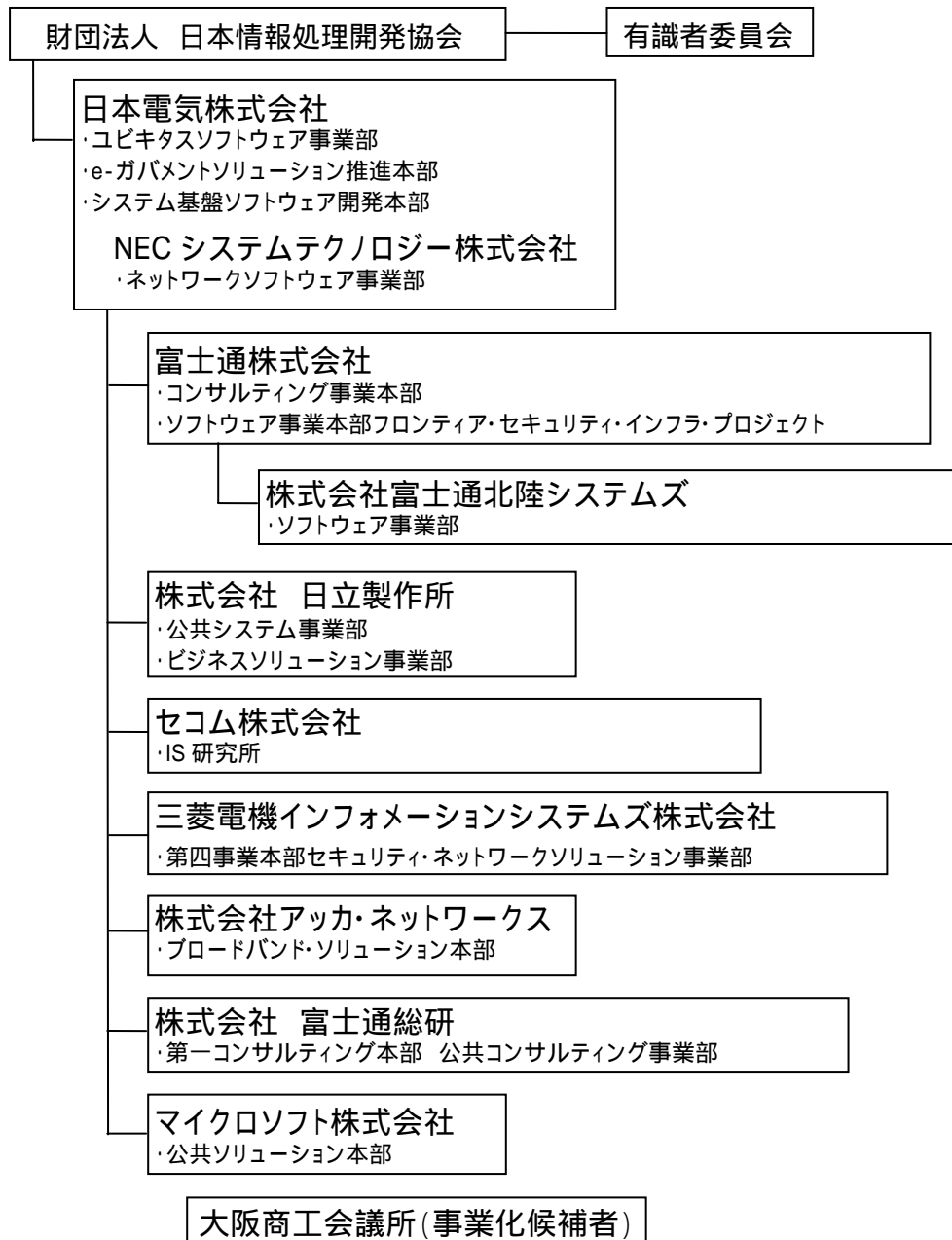


図 3.1 本事業の推進体制

#### 4. 全体概要

##### 4.1 事業概要

ビジネスモデルの策定では、異なる部門、企業間でのサービス連携を実現するため、次世代型電子認証基盤の関与者に対して、一定のビジネスルールに基づきビジネスを実現できるようビジネスモデルを策定した。ビジネスモデルとして、後述するポリシーガイドライン策定での基準を各クレデンシャルサービスプロバイダ（以下「CSP」という。）間で合意するための仕組みや、CSP が利用者の認証手段を提供するサービスプロバイダ（以下「SP」という。）や各関与者間の情報の流れと管理方法、利益分配方法、運用と責任範囲、契約及び制度について整理した。

ポリシーガイドラインの策定では、トラストドメイン内及びトラストドメインを越えた認証連携を実現するため、CSP に対して、一貫した認証ポリシーのもとでクレデンシャルサービスを提供できるようガイドラインを策定した。又、SP に対しては、その保証レベルを決定するときに依拠するガイドラインを策定した。

認証技術の開発では、認証やサービス連携を実現するため、SP 及びポータルサーバに対して、必要なコア技術を開発した。コア技術として既に存在する製品やオープンソフトウェアが実現する機能はそれを使用し、基本的な電子認証技術として標準仕様や標準プロトコルを使い、標準的に他の組織・団体・利用者からも利用できるよう認証連携機能に関わる機能を開発した。

本事業の想定する関与者及び成果物の適用範囲について「図 4.1」に示す。

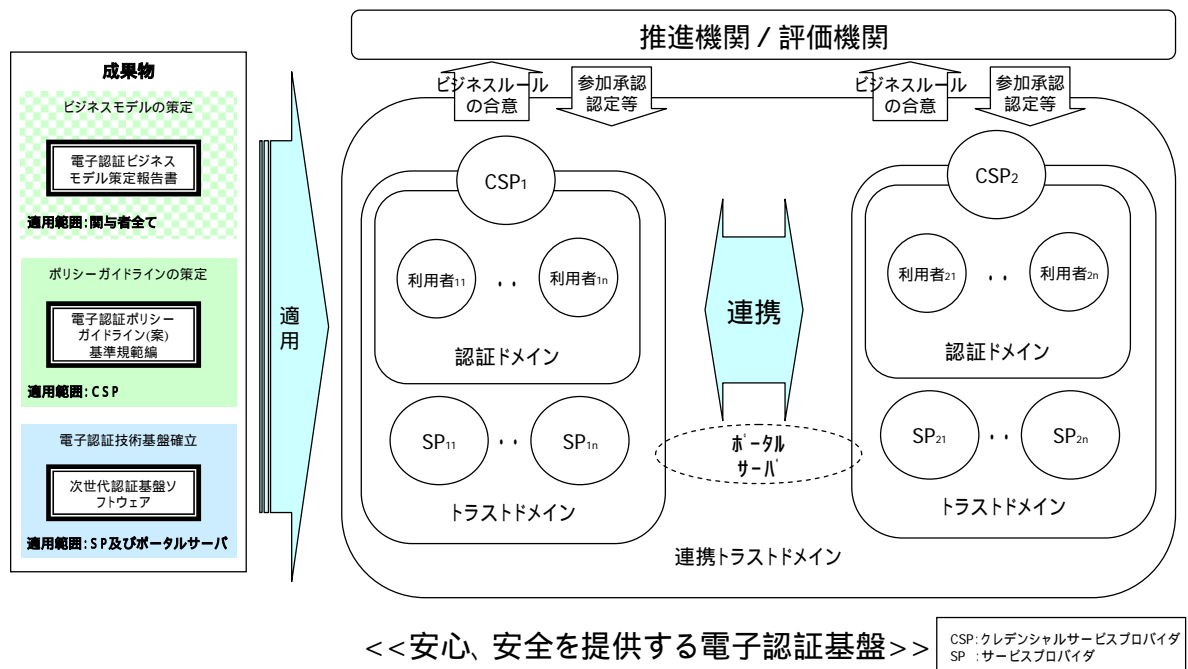


図 4.1 想定される関与者及び適用範囲

## 4.2 実施方針

本事業では、2 ヶ年にわたり段階的に活動することとし、初年度である平成 17 年度では、「電子認証ビジネスモデルの策定」、「電子認証ポリシーガイドラインの策定」、「電子認証技術基盤確立」を実施した。

又、これらの評価にあたっては有識者を交え議論を行った。「図 4.2」に各活動の関連と流れを示す。

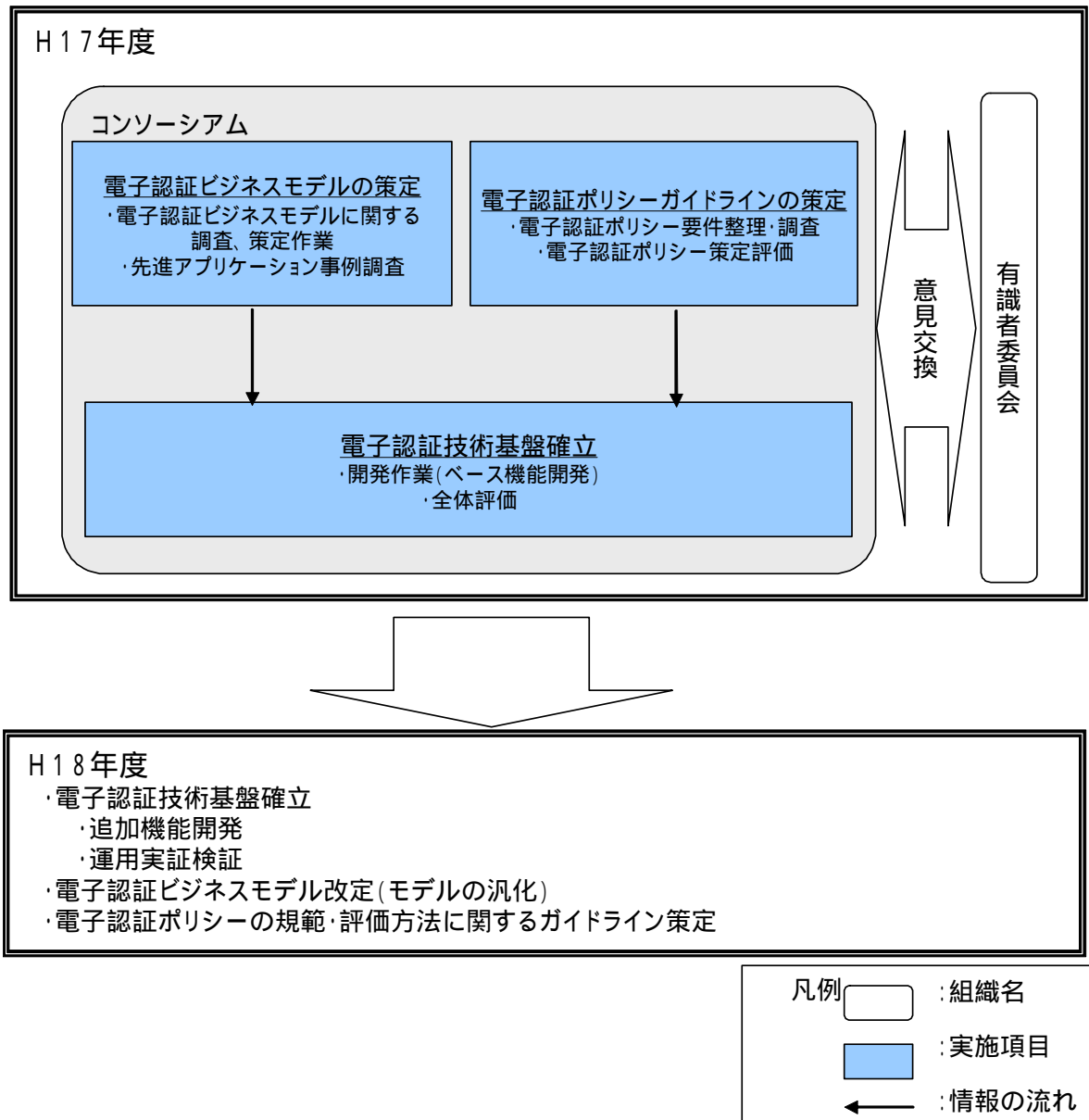


図 4.2 2 箇年活動全体図

### 4.3 事業報告の構成

電子認証ビジネスモデル策定については、海外国内の先進アプリケーション事例を調査した結果を踏まえ、「電子認証ビジネスモデルの策定報告書」を策定した。

電子認証ポリシーガイドライン策定について、海外の事例を調査した結果を踏まえ、「電子認証ポリシーガイドライン(案)基準規範」を策定し、海外先行プロジェクトの電子認証ポリシーとの互換性の視点と妥当性の観点から評価を行った。

電子認証技術基盤確立については、認証やサービス連携を実現する基本的な電子認証技術基盤として「次世代認証基盤ソフトウェア」を開発した。又、電子認証技術基盤確立では、開発したソフトウェアの評価実験、電子認証ビジネスモデル策定、電子認証ポリシーガイドライン策定の要件とのフィットギャップの検証、目的と達成度に対する客観的な評価、本プロジェクト全体評価及び次年度へ向けた改善点洗い出しを実施し、「評価報告書」としてまとめた。

本事業に関わる成果物の体系を「図 4.3」に示す。

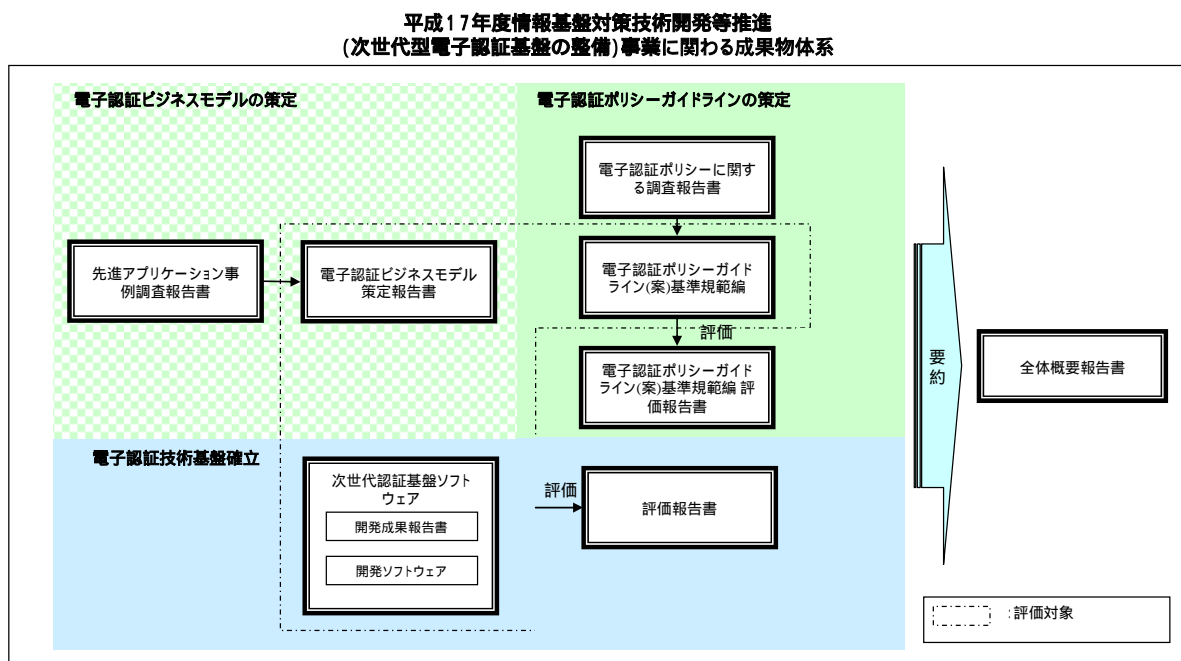


図 4.3 本事業に関わる成果物体系

以下に「図 4.3」で示した各成果物の位置づけについて記述する。

#### (1) 電子認証ビジネスモデル策定報告書

実ビジネスを構築する際に利用、並びに参照されるモデルとして想定される関与者及び関与者間の情報の流れと管理方法、利益分配方法、契約、制度、運用と責任範囲及び必要とされるシステムと機能について整理した報告書。

(2) 先進アプリケーション事例調査報告書

ビジネスモデル及び電子認証基盤の汎用性の確保の検討に必要な現状の事実認識のために、海外及び国内の先進事例の調査を行い、結果をまとめた報告書。

本書では、現状における利用状況も踏まえたうえで、問題点や課題を整理・分析し、ビジネスモデルの汎用性を確保するために必要な対策案を提起し、併せて、想定される関係者の具体的な候補（企業等）や新たに創生すべき組織等についても考察している。

(3) 電子認証ポリシーに関する調査報告書

「電子認証ポリシーガイドライン（案）基準規範編」を策定するため、海外先行プロジェクトの電子認証ポリシーが「どのような考え方で構成されているか」「どのような基準規範を規定しているか」について、及び国内 SP の事例を調査、整理し、要件をまとめた報告書。

(4) 電子認証ポリシーガイドライン（案）基準規範編

CSP が電子認証ポリシーを策定するとき及び SP が自身の提供するサービスの保証レベルを決定するときに依拠するガイドライン。本ガイドラインでは、保証レベルの定義及び基準、並びに保証レベル決定プロセスを規定している。

又、本ガイドラインは、CSP が内部監査を行うとき、認定機関及び推進機関がトラストドメインに加わろうとしている CSP や SP の評価を行うとき及び SP が利用するクレデンシャルサービスの妥当性を利用者が判断するときに依拠する。

(5) 電子認証ポリシーガイドライン（案）基準規範編 評価報告書

平成 18 年度に向けた全体最適化のために、策定にあたって調査した海外先行プロジェクトの電子認証ポリシーと策定したポリシーガイドラインを比較することでその妥当性を評価した結果をまとめた報告書。

(6) 開発成果報告書

開発したソフトウェア機能及び評価実験の成果をまとめた報告書。

(7) 評価報告書

本事業において実施される事業内容について、その実施内容の妥当性を評価した結果と今後に向けた課題をまとめた報告書。

評価対象範囲は、「電子認証ビジネスモデル策定報告書」、「電子認証ポリシーガイドライン（案）基準規範編」、次世代認証基盤ソフトウェア（「開発成果報告書」、開発ソフトウェア）であり、関連する部分について、「先進アプリケーション事例調査報告書」、「電子認証ポリシーに関する調査報告書」、「電子認証ポリシーガイドライン（案）基準規範編 評価報告書」を参照している。

#### 4.4 普及・啓発活動

本事業では、普及・啓発活動として以下の活動を実施した。

- ・ APKI-F 北京国際シンポジウムにて紹介（2005/11/5）
- ・ APKI-F 北京ミーティング相互運用 WG（E-Authentication Policy part）にて紹介（2005/11/3）
- ・ 日本ドイツ年（第 11 回日独シンポジウム～情報社会におけるセキュリティ～）にて紹介（開催期間：2005/9/13～2005/9/16）
- ・ NII セミナー（大学電子認証基盤シンポジウム）にて紹介（2006/2/15）
- ・ 日本 PKI フォーラム国内シンポジウムにて紹介及びデモを実施（2006/2/8）

### 5. 個別概要

#### 5.1 電子認証ビジネスモデルの策定

##### 5.1.1 電子認証ビジネスモデル策定

###### (1) 電子認証ビジネスモデルの関与者

電子認証ビジネスモデルに登場する主たる関与者は利用者、SP、CSP、推進機関 / 評価機関である。

###### (2) 対象とする市場

対象とする市場を電子商取引の場である BtoB 市場及び BtoC 市場とし、導入容易性の高い市場は BtoB 市場と分析した。

###### (3) 策定した電子認証ビジネスモデル

「認証連携型モデル」と「認証連携型 + 属性利用型モデル」の 2 つを策定した。「認証連携型モデル」における電子認証サービスが CSP 事業の基軸となり、事業性が確保できることを確認した。それぞれのモデルの特徴は以下のとおりである。

###### 【認証連携型】

CSP の収益の基軸となるモデルである。

電子認証に関わる利用者情報を CSP で管理し、これまで SP が独自で行っていた電子認証業務から SP が解放される。SP は電子認証業務以外の自サービスの提供に必要な情報のみを利用者から収集・管理し、サービスを提供する。

###### 【認証連携型 + 属性利用型】

CSP のさらなるビジネス展開のために考えられたモデルである。

電子認証サービスの提供に加え、CSP の保有する利用者属性情報を利用するサービスや、サービスへのアクセス制御、統計情報の提供等 SP に対する付加価値サービスの提供を想定したモデルである。

次世代型電子認証基盤における CSP と SP への便益は以下のとおりである。

- ・ CSP は提供する電子認証サービスを帰属する SP 及び利用者が利用することによって得られる対価が基本収益となる。
- ・ SP は利用者が安全安心なサービスを利用できること、異なるトラストドメイン間でサービス連携が可能となることに起因する利用者のサービス利用機会の増加によって得られる利益増が便益となる。さらに CSP の提供する電子認証サービスを利用することのコストダウン効果によって便益を得ることができる。

#### (4) 次世代型電子認証基盤普及の鍵となる関与者

次世代型電子認証基盤における電子認証ビジネスモデルが事業性を持つためには CSP の存在が鍵となり、以下の CSP の事業候補者を想定した。

##### 【BtoB 市場における CSP 事業候補者】

- ・ 金融業・クレジット会社・保険会社等、利用者登録時に厳格な利用者確認を既に実施している企業
- ・ 認証局（CA）業者
- ・ 地域の商工業界を推進する団体（商工会議所等）

##### 【BtoC 市場における CSP 事業候補者】

- ・ BtoB 市場において記述した CSP 候補者のうち BtoC 向けサービスが提供可能な候補者
- ・ 大規模オンラインショッピングモール等、既に電子認証業務を保有しており、顧客サービスを継続しながら運用可能な企業

#### (5) 関与者間の運用留意事項

電子認証ビジネスモデルの関与者について、その関係、契約並びに制度の所在、契約の際に留意する事項や運用に関わる利用者属性情報の管理と責任範囲、及び必要となるシステムと機能について記述した。

#### (6) 電子認証ビジネスモデルの適用分析

事業候補者である大阪商工会議所が運営し、企業間取引を支援するポータルサイトである「ザ・ビジネスモール」に対し、策定した電子認証ビジネスモデルの適用可能性について分析を行い、適用可能との結果を得た。

### 5.1.2 先進アプリケーション事例調査

#### (1) 調査分野

今後の我が国において電子認証ビジネスの展開が期待できる「健康サービス関連」「中小企業金融関連」「デジタルコンテンツ配信と知的財産権管理関連」「電子商取引関連」の4分野を中心に調査を行った。

## (2) 4 分野の現状

### ・健康サービス関連

サービスプロバイダが日本においては医療機関に限られているのが現状である。

### ・中小企業金融関連

クレジットカードの仕組みが多くの特約者を持つ実ビジネスモデルとして参考になる。

### ・デジタルコンテンツ関連

利用者が個人に限られているのが現状であり、サービスプロバイダであるコンテンツ権利者との契約関係が複雑な点が特徴的である。

### ・電子商取引関連

利用者として個人を対象としたものと企業を対象としたものに大別されるが、企業を対象としたサービスでは特定の業界に限定しているのが現状である。

## (3) まとめ

このような現状を踏まえたうえで、次世代型電子認証ビジネスにおいて想定される関与者（利用者、SP、CSP、推進機関・評価機関）を挙げ、特に推進機関・評価機関として創設すべき組織の要件を挙げた。又、電子認証ビジネスを展開するうえでの有望な分野は、電子商取引関連と中小企業金融関連である点を指摘した。

最後に、電子認証ビジネス展開のための課題をまとめている。

## 5.2 電子認証ポリシーガイドラインの策定

### 5.2.1 電子認証ポリシーガイドライン（案）基準規範編策定

#### (1) 目的

CSP が電子認証ポリシーを策定するとき、及び SP が保証レベルを決定するときに依拠するガイドラインとして保証レベルの定義、保証レベルに基づく基準及びレベル決定プロセスを規定したものである。

#### (2) ガイドライン策定方針

本ガイドラインに規定する「電子認証ポリシー」及びリスク分析から保証レベルを導出するプロセスである「レベル決定プロセス」に関する体系的な事例が国内にないことから、海外先行プロジェクトの調査結果を参考に策定することとし、グローバルなトラストドメインの連携に資するガイドラインにすることを策定方針とする。

又、ISO / IEC17799 ( ISO / IEC27002 ) 等の既存の標準に対しては補完関係の位置づけとし、相互に干渉しあうことを避ける、あるいは組合せによる相乗効果を期待できるようにすることを策定方針とする。

## (a) 認証ポリシー

### (i) レベル

#### (I) 定義対象

「アイデンティティの有効性に対する信用度」及び同じ意味で「アサーションの信用度」に係る「保証レベル」を定義しているプロジェクト（米国 EAI、米国 EAP 及びオーストラリア）が多いことから、本ガイドラインでは「アサーションの信用度」をさらに一般化した「クレデンシャルの信用度」に係る「保証レベル」を定義することにした。

#### (II) レベル数

全ての調査対象においてレベル数は 4 であったので、本ガイドラインで規定するレベル数についても 4 とした。

#### (III) 信用度の定義

信用度はリスク分析から導出されるという考え方で信用度を定義しているプロジェクト（米国 EAI、米国 EAP、英国、オーストラリア及び IDA）が多いことから、本ガイドラインでは総合的な推進を行っている米国 EAI の定義を参考にすることにした。

### (ii) 基準

基準については、策定方針で示した補完関係の位置づけとするために、クレデンシャルの取扱いに限定した次の 4 領域に関する管理策を規定することにする。

なお、レベル 4 の基準は、電子署名の分野において高い信用度を要求している特定認定認証業務とレベル感を合わせることを目的に、当該認定に係る調査表を参考にすることにした。

#### (I) 登録

実在性及び本人性を確認する管理策を規定する。

#### (II) クレデンシャルの管理

クレデンシャルのライフサイクルに係る管理策を規定する。

#### (III) トークン

トークンに関する技術的管理策を規定する。

#### (II) 認証プロトコル

トークンの所持及び管理を検証するための認証プロトコルに係る技術的管理策を規定する。

## (b) レベル決定プロセス

リスク分析の重要な要素である潜在的影響度の定義が類似しているプロジェクト（米国 EAI、米国 EAP、英国及びオーストラリア）が多いことから、本ガイドラインではその中から唯一「レベル決定プロセス」を規定している米国 EAI を参考に規定することにした。

## 5.3 電子認証技術基盤確立

### 5.3.1 開発成果報告書

電子認証技術基盤確立ワーキンググループ（WG）では、「表 5.1」のエンティティの機能を開発し、「図 5.1」の評価実験システムを構築して 9 つの評価を実施した。

各エンティティの機能開発では、既存の製品やオープンソースを使用することで必要な機能開発に注力する方針をとり、PC と CSP は既存の製品を使用した。又、SP とポータルサーバは、オープンソースをベースに必要な機能を開発した。

表 5.1 エンティティ機能一覧

項目名	機能概要
PC	Web ブラウザを使用した。PC は、ポータルサーバ、CSP、SP にアクセスし、それぞれの提供サービスを受ける。
CSP	既存の製品を使用した。CSP は、PC の利用者を認証して利用者の認証・属性情報（アーティファクト、アセッション等を含む）を発行する。
SP (開発対象)	SP は、CSP が発行した利用者の認証・属性情報を用いて利用者の認証結果と権限を判断し、権限に応じたサービスを SP に提供する。
ポータルサーバ (開発対象)	ポータルサーバは、認証・属性情報を基に CSP や SP の認証連携を行う。又、利用者の要求に応じて SP 間のサービスの連携をカスタマイズできる。

評価実験では、トラストドメイン 2 に所属する PC がポータルサーバを介してトラストドメイン 1 に所属する SP1、SP2、SP3 の提供サービスを利用可能にするシナリオを基にシステムを構築した。トラストドメインとは、CSP を信頼点とする PC と SP の集合のことである。ポータルサーバは、異なるトラストドメインの認証とサービスをつなげるための認証とサービスの基盤の役割を持つ。

評価実験システムでは、実際の適用環境を考慮してインターネットに接続する 2 つのネットワークを用意した。又、3 つのドメイン名を用意し、2 つのトラストドメインと 1 つのポータルサーバに分けてそれぞれに割り当てた。

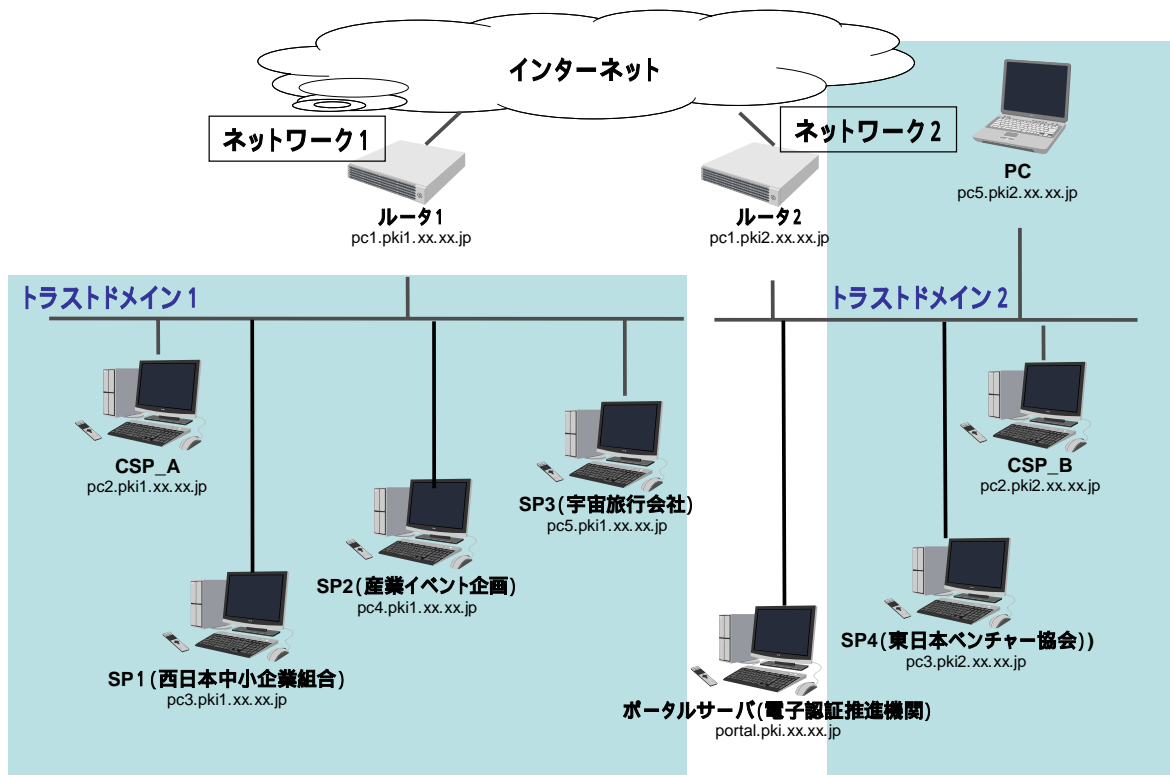


図 5.1 評価実験システム図

評価実験では、4つのエンティティ機能の達成度と、5つの評価項目（個人情報管理、安全性、利便性・操作性、適用効果・実用性、導入容易性・利用容易性）において評価を実施した。4つのエンティティの機能は、2005年度に設計、開発を予定していたものについては達成を確認した。又、5つの評価項目は、各項目において課題や考慮する点が残されているが、今年度は2箇年計画の初年度であり、課題を解決する基本機能が実現されていることから達成できていると考えられる。評価結果と有識者の意見から、次の2項目が来年度に対応する主な課題であることがわかった。

- ・ CSPにおいて異なる認証手段の提供（認証レベルの対応）
- ・ メッセージへのXML署名の付与（メッセージのセキュリティ対応）

### 5.3.2 評価報告書

本事業は「情報経済・産業ビジョン」における「共同体全体の最適化」に向けたプラットフォームとしての次世代型電子認証基盤の開発を目的として、以下の3つの活動を中心に行われた。

- ・ 電子認証ビジネスモデルの策定
- ・ 電子認証ポリシーガイドラインの策定

- ・電子認証技術基盤確立

評価にあたり、以下に示す 8 つの評価軸を設定した。これらに基づき評価項目を作成したうえで、成果物である「電子認証ビジネスモデル策定報告書」、「電子認証ポリシーガイドライン（案）基準規範編」、「次世代認証基盤ソフトウェア」につき評価した。

- ・サービスの連携・共有
- ・サービスの複合による付加価値の向上
- ・安心・安全なプラットフォームの提供
- ・プラットフォームの実用性（企業、利用者から考えて）
- ・ユニバーサルデザイン（操作性、利便性等）
- ・導入・運用・維持・管理
- ・国際標準等との整合性
- ・基盤・サービスの普及・発展

又、各成果物については、有識者委員会にてご意見をいただいたが、評価においては、その結果も考慮にいれている。有識者委員会では、次世代型認証基盤の適用領域・市場、属性情報の取扱い、ビジネスモデル検討の方向性等につきご意見をいただいた。

プロジェクトは、それぞれを担当するワーキンググループ間で意見交換をしつつ実施されたものの、並行作業となったため初年度末での成果の間には、必ずしも適用範囲が一致していないものも含まれている。これらの検討結果の整合は、今後の課題として検討されるべきものである。この観点より、次年度に向けた課題の整理も行った。

主な課題としては以下のものがある。

- (1) ビジネスモデルにおける対象領域、特に、BtoB における検討の拡充、又は各関係者間の具体的な契約内容
- (2) 認証ポリシーにおいては、認証対象は個人を前提にしたが、組織に適用する場合の検討
- (3) 技術基盤においては、複数の認証手段をサポートした場合の異なる保証レベルの間での連携

評価の結論として、初年度の各成果物の品質は、事業目的を達成するという観点で設定した評価項目を満たしており、当初の目的を達成している。

禁 無 断 転 載

平成 17 年度情報基盤対策技術開発等推進事業  
(次世代型電子認証基盤の整備)  
全体概要報告書  
平成 18 年 3 月発行

発行所 財団法人日本情報処理開発協会  
〒105-0011 東京都港区芝公園 3 丁目 5 番 8 号  
機械振興会館内  
TEL. 03 ( 3436 ) 7500

印刷所 新高速印刷株式会社  
〒105-0004 東京都港区新橋 5 丁目 8 番 4 号 柴田ビル 6 階  
TEL.03 ( 3437 ) 6365