21-H006

「電子認証の民間制度・基盤確立に関する調査研究」

報告書

平成 22 年 3 月

財団法人日本情報処理開発協会

この事業は、競輪の補助金を受けて実施したものである。
http://ringring-keirin.jp/

序文

本報告書(事業)は、財団法人日本情報処理開発協会が財団法人ＪＫＡの補助金を受けて実施した平成 21 年度情報化の推進に関する補助事業「電子認証の民間制度・基盤確立に関する調査研究」の一環として作成したものである。

急速に発展するインターネット社会も、ビジネス活動環境としてみた場合、安心・安全面を裏打ちする社会的な環境の強化が求められている。情報化黎明期のおおらかさを残したインターネットの上で、適切な水準の安全性と信頼性を確保したビジネス活動環境を構築するためには、社会的なルールを伴った情報環境が必要であり、その整備が望まれている。また、そのような情報環境は、使いやすくストレスを感じさせないものでなければならない。

一方で、企業の人事情報や団体の登録情報等は、確実な本人確認/実在確認がなされており、また情報の更新もきちんとなされているものが多い。このような、最もフレッシュで信頼できる企業／団体（以下「企業等」）に軸をおいた認証環境を実現し、さらにグローバルな仕組みと連携することができれば、安心・安全で使いやすい社会的環境(以下「安信簡」情報環境)を実現でき、情報経済社会の変革が可能となると考える。

本事業では、上記に係る新たな民間の制度･基盤の確立に向けた調査研究を 2 年計画で行うものとし、初年度の平成 21 年度は、制度全体の認知拡大を目指した「ビジネスモデル」の整理/プロモーション活動（アンケート、シンポジウム）を行うとともに、制度･基盤に必要な「ポリシー」「基盤システム」「評価基準」を検討した。

また、事業の実施に当たっては、当協会役職員及び外部有識者で構成する「有識者委員会」とその下に「ビジネスモデル検討部会」「ポリシー/基盤システム検討部会」「評価基準検討部会」を設置し検討を行った。

なお、当協会は、電子署名及び電子認証に係る分野では、平成１３年４月に施行された電子署名法に基づく指定調査機関として長年の調査業務及び調査研究業務で培った技術と知見があり、これを活用して本調査研究を実施した。

平成 22 年 3 月

財団法人日本情報処理開発協会

－ 目　次 －

はじめに

(1) 背景

ネットワークにおいては、その情報の信憑性やなりすましなどの対策として公開鍵暗号に基づく電子認証･電子署名が利用されている。

特に、電子署名の分野においては「個人」を対象とした「電子署名法に基づく特定認証業務」や「地方自治体における公的認証サービス」等の我が国を代表する制度がある。

しかし、ビジネスにおいて、個人の電子証明書を使うことは、例えるなら実印と印鑑登録証明書を使って業務を行っているような違和感がある。

本来は、担当印や職印等と同じような運用ができる電子証明書が求められているものと考える。

また、現状では電子証明書が高価及び登録手続きの煩わしさも加わり“局所的な利用”に留まっているが、これをビジネスでインターネットを活用するすべての企業等内個人が安価で簡便な電子証明書を持てる状況になると情報経済社会の変革が起きるものと考える。

(2) 目的

安心・安全面を裏打ちする社会的な環境である「安信簡」情報環境の認証環境として、以下を特長とする民間の制度･基盤（以下「JCAN（Japan CA Network）」）を検討した。

・権限/資格等を正確に反映した電子証明書を発行する仕組み（内部統制の強化）
・企業等の信用力と情報管理力を担保に電子証明書を発行し実業務と同じ運用ができる仕組み（全体最適化/業務効率化）

なお、本電子証明書は、共通化された電子の名刺/社員証/担当印/部門印/角印/会員証等に相当する。

※実印/丸印相当の役割は、「電子署名法」等に基づく電子証明書が担う。

(3) 本書の構成

本書において、「事業化の検討」を第 1 章に、「ビジネスモデルの検討」を第 2 章に、「ポリシー/基盤システムの検討」第 3 章に、「評価基準の検討」第 4 章に、「認定制度の検討」を第 5 章に、「利用の手引き」を第 6 章に記載する。また、委員会活動及び広報活動の結果をそれぞれ第 7 章、第 8 章に記載した。

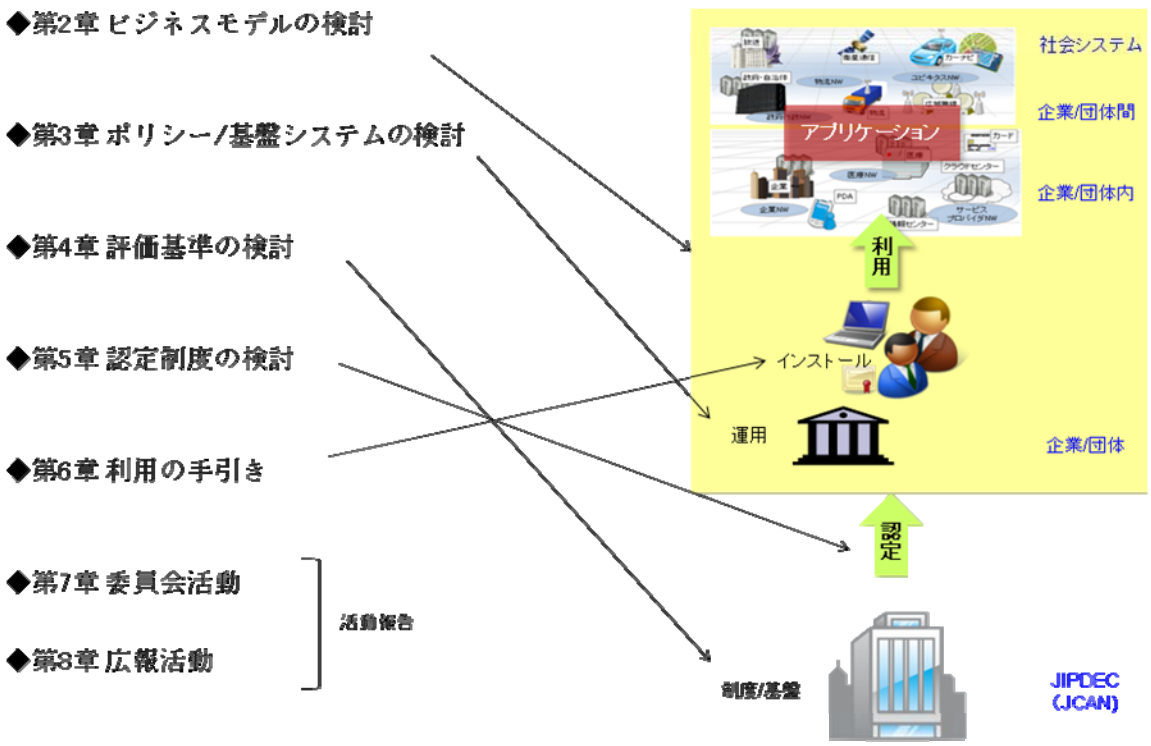


図 0-1　本書の構成

1. 事業化の検討

1.1 JIPDECが社会に果たすべき役割

(1) 背景

現代社会において、様々な領域，階層でネットワーク属性、利用方法が多様化し流通する情報の情報セキュリティに対する重要性が高まっている。

この背景の中で情報セキュリティ，情報連関性の分断を要因とした課題が山積となっている。

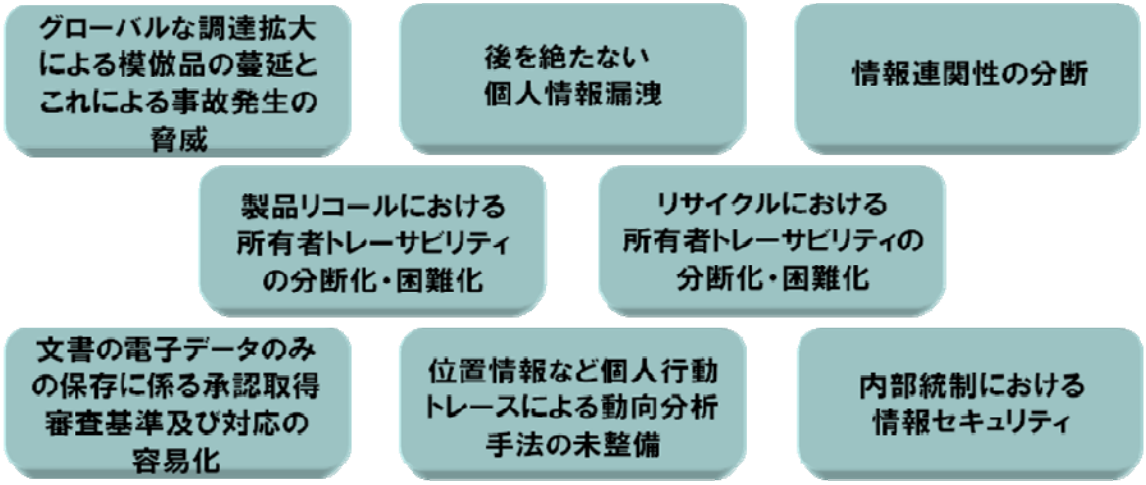


図 1-1　情報連関性の分断を要因とした課題

これらすべては、個人情報の守秘義務に遵守しつつ対処しなければならない課題であり、相手・情報の信頼性・真正性の確保・確認および情報流通の安全性があらゆる領域で必要不可欠な社会環境が求められている。

(2) JIPDECが社会に果たすべき役割

JIPDEC は、IT 社会基盤の根幹となる「情報認証センター」として中核の役割を果たし、セキュアな情報化社会の定着化に寄与することが求められている。

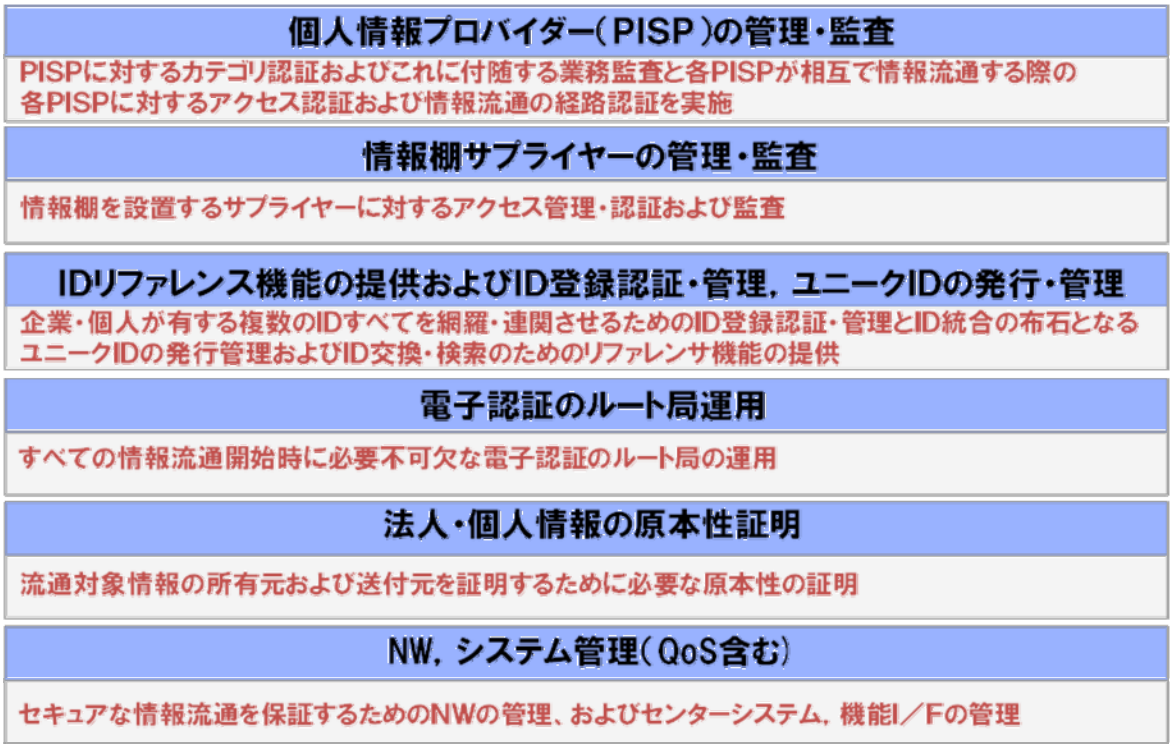


図 1-2　JIPDEC が社会に果たすべき役割

(3) コンセプト

以上より、多様化するネットワーク社会にかける情報セキュリティに関連する諸課題を解決するために必要不可欠な社会的環境である「安信簡」情報環境（安全・安心の「安」、信頼性の「信」、簡単・簡便の「簡」）というコンセプトを設定した。

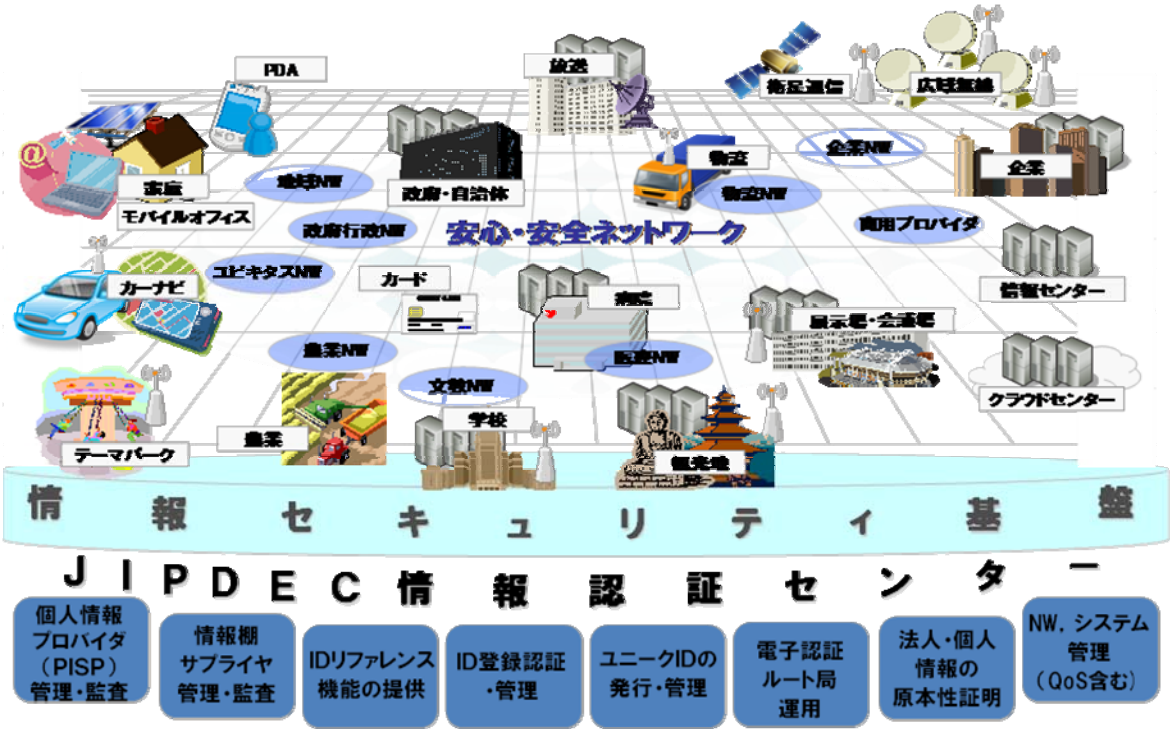


図 1-3　「安信簡」情報環境

1.2 「安信簡」情報環境

「安信簡」情報環境の構成要素は、次に示す４つから構成される。

① PS名情報環境

過剰な個人情報保護が、社会的な情報連関の阻害要因となっている。「PS 名情報環境」とは、確実な本人確認を前提とした PS 名（Pseudonym（シュードニム）の略称。なお、シュードニムは、擬名･仮名･別名と訳されることがあるが自身が命名者であることを意味する適切な訳語が定まっていない）を導入し、個人情報に配慮できる情報環境を実現するもの。

なお、本検討では、PS 名を更に名刺のようにビジネスの場で広く公開されて利用されるもの(以下「BN」(Business Name))と個人が私的に利用するもの(以下「PN」(Personal Name))に分けて検討した。

② 認証環境「JCAN」

認証環境の分断も、社会的な情報連関の阻害要因となっている。認証環境「JCAN」とは、共通のルールと認定制度に基づく認証環境で、組織が組織に属していることを組織の外に証明できる情報環境を実現するもの。

③ 企業ID連携環境

様々な企業 ID の乱立も、社会的な情報連関の阻害要因となっている。「企業 ID 連携環境」とは、これら複数の企業 ID を紐付け、企業の信用情報をより確かにできる情報環境を実現するもの。

④ 双方向情報交換環境

上記①～③の環境を利用し、「セキュアな情報交換環境」等を実現するもの。

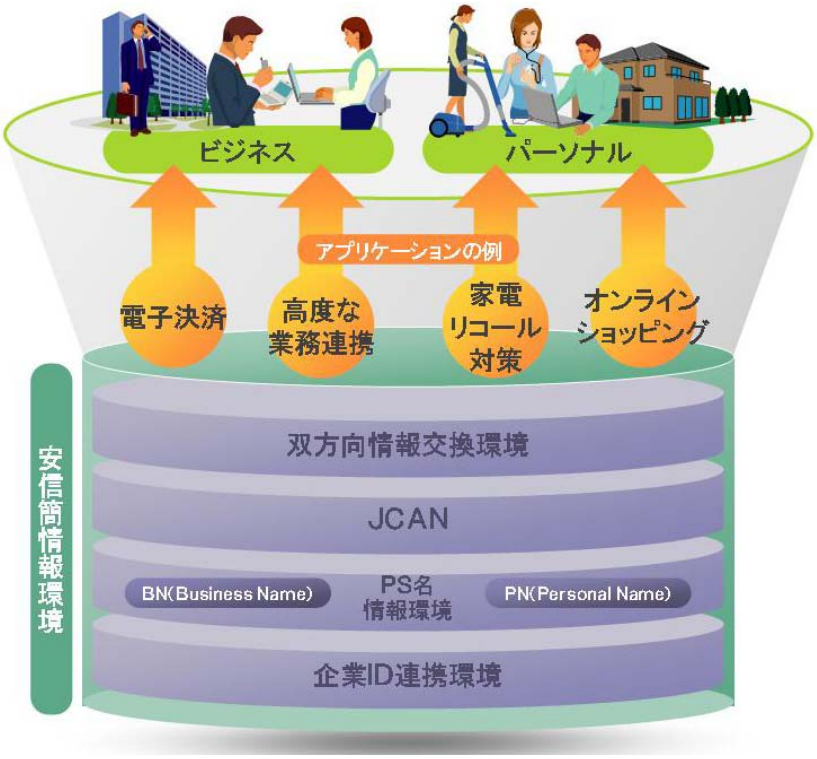


図 1-4 「安信簡」情報環境の構成要素

以下、認証環境「JCAN」についての検討を紹介する。

2. ビジネスモデルの検討

2.1 ビジネスシーンの検討

本検討では、JIPDEC が社会に果たすべき役割のひとつとして、安心・安全面を裏打ちする社会的な環境である「安信簡」情報環境の実現策を検討した。また、「安信簡」情報環境を活用したビジネスシーンを示す事により、多様な利用場面で「安信簡」情報環境が活用できることを示す。

本検討における成果は、企業等の認証環境に係る新しい民間制度・基盤の実現に向けた、啓蒙や必要性の認知の向上、今後の検討の下地として利用・活用されることを期待するものである。

なお、本検討の詳細については、添付資料 A「ビジネスシーンの検討」を参照のこと。

(1) ビジネスシーン

「安信簡」情報環境を活用したビジネスシーンを、BN の電子証明書を活用した場合のビジネスシーンと、PN の電子証明書を活用した場合に分けて、ビジネスシーンを検討した。

(a) BNを活用したビジネスシーン

①署名メール
②電子決裁
③電子投票
④模倣品対策

(b) PNを活用したビジネスシーン

①転職
②オンラインショッピング
③家電リコール

次に、BN を活用したビジネスシーン「署名メール」と PN を活用したビジネスシーン「オンラインショッピング」のイメージを示す。

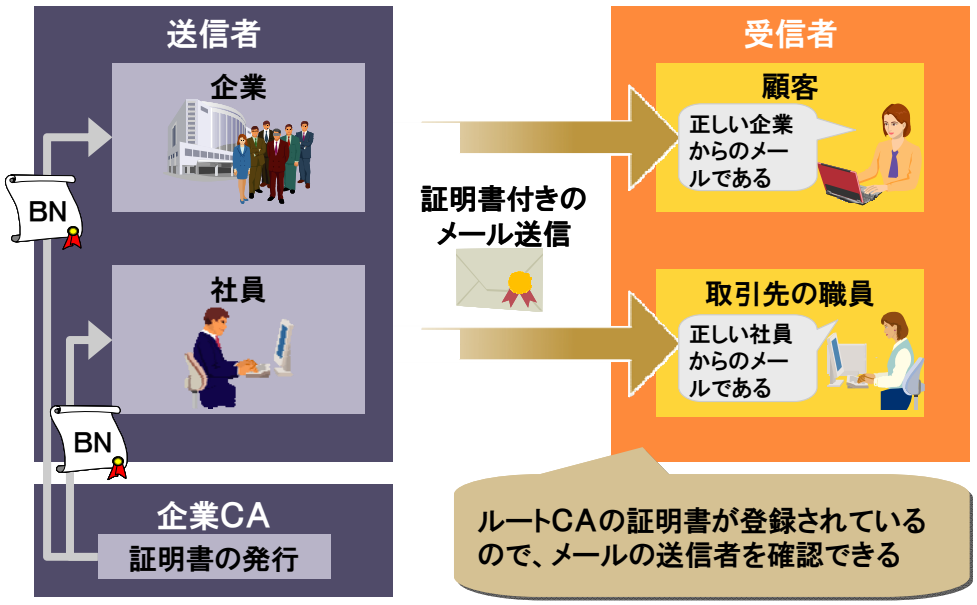


図 2-1　署名メール

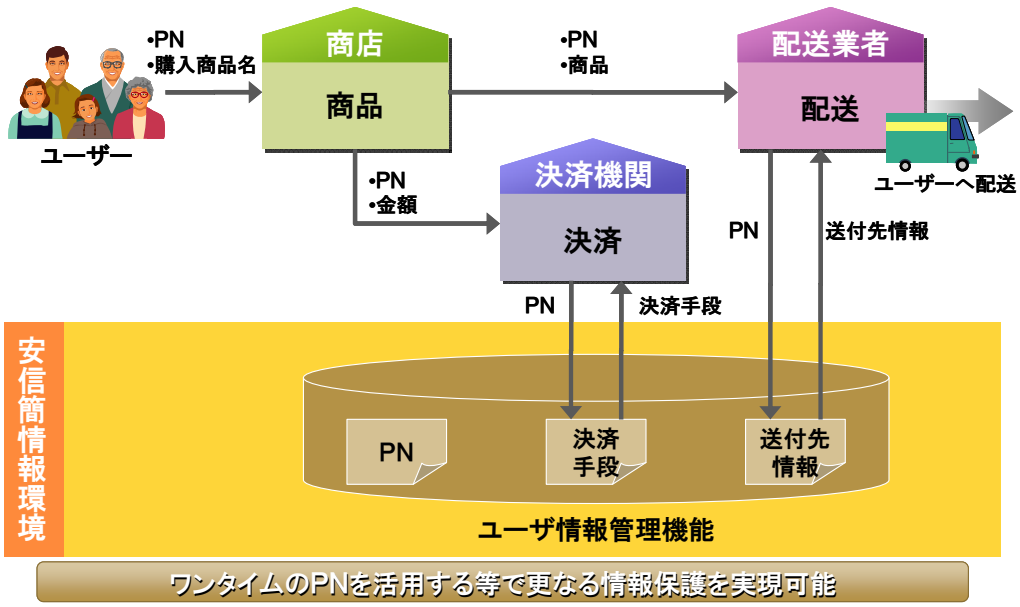


図 2-2　オンラインショッピング

(2) 今後に向けて

本検討では、安心・安全な社会環境である「安信簡」情報環境について検討を行い、その構成要素の一つである PS 名について、BN と、PN に分けて、それぞれを整理した。

また、これら BN や PN を活用した利用シーンをそれぞれ例示し、様々なビジネスシーンにおいて BN や PN をはじめとする「安信簡」情報環境が活用できることを示すことができた。

これら BN、PN の仕組みと、情報を交換させる環境が共通のルールと認定制度に基づいて推進されると、社会的な情報連関の活性化に貢献するものと考える。

プロセスとしては、BN が普及することで、企業活動における PKI の高度利用が促進され、同時に BN を信頼の起点とした PN の仕組みを導入することにより、社員の立場を離れた個人の活動に対しても、広く利用できるものになると考える。

2.2 普及に必要な環境の検討

2.2.1 マルチユース格納媒体のPKI対応の検討

本検討では、電子認証に必要な ID 情報（個人識別情報等）及び電子署名用秘密鍵の活性化共通鍵等情報（以下「共通鍵」）を持ち運び可能な格納媒体（以下「JCAN パス」）に格納するための方式や運用方法について調査検討した。

なお、本検討の詳細については、添付資料 B「マルチユース格納媒体の PKI 対応の検討」を参照のこと。

(1) JCANパスとは

JCAN パスは、分断された認証基盤をフロントエンドで連携することで業務の効率化を支える格納媒体であり、機能としては次を有するものである。

- ID 情報、共通鍵等を格納できる。
- 格納した情報には必要に応じて暗号化及び読み書き用 PIN 等のセキュリティ機能を備えている。
- 情報は必要に応じて、いつでも書き換えができる。
- 必要に応じて後から情報の追加、削除が行える。
- 基本的なルールを守れば、誰でも実装情報を利用できる。

(2) 格納媒体の種類

検討対象とする格納媒体の種類は、コスト、普及状況等を考慮し、今回は次の媒体とする。

・非接触 IC カード　（TypeA カード、FeliCa カード）

・USB メモリ

(3) 対象アプリケーション

既にマルチユース格納媒体を 60 万枚以上の発行している FeliCa 共通利用フォーマット推進フォーラム（通称：FCF フォーラム　http://www.fcf.jp/）の会員企業 113 社に調査した結果、ほぼ全社から「FCF フォーラムが提唱している共通フォーマットの考え方にそった考え方であれば、既存アプリケーションへの適用は可能」との意見があった。

また、電子証明書については、「手軽に証明書も発行処理が行えるのであれば利用価値はある」との意見であった。但し、「媒体上にある登録情報はなるべくシンプルな方がよく、複雑なものは適さない」との意見もあり、電子証明書のための PKI 情報はシンプルなものを利用することを考える必要がある。

以上より、FeliCa 共通利用フォーマットが利用できるアプリケーションを対象アプリケーションに含むものとする。

(4) 実装方式

JCAN パスの情報格納フォーマットは、60 万枚以上の発行実績がある FeliCa 共通利用フォーマットを参考に検討を行うものとする。

これにより、既存で利用されている技術や環境をうまく利用することが、時間とコストを押さえ、利用者からも受け入れ易いものになると考える。

具体的には、格納媒体として FeliCa カードを利用する場合の JCAN パス用フォーマットは、FCF に準拠し、FCF の追加サービス C1 領域を JCAN パス用の電子証明書に関する PKI 情報を格納する領域と定義し実現する。

一方、TypeA カード及び USB メモリについては、FCF のフォーマット構造を維持しながら、それぞれの格納媒体の特性を活かしたフォーマットを検討し、今後の実証実験等で開発・確認を行うものとする。

なお、JCAN パスでは、一般に電子証明書を扱う IC カードで格納している「電子証明書」及び「電子署名用秘密鍵」は格納しない。(「電子証明書」及び「電子署名用秘密鍵」は PC に格納する)

(a) JCANパス用共通フォーマット仕様

FCF は、次の図に示すように、大きく基本サービスエリアと追加サービスエリアの２つのエリアを持っている。

JCAN パス用は、この追加サービスエリアに電子証明書に関する PKI 情報を格納する仕様とする。

なお FCF の仕様上、追加サービスエリアを使う場合は、追加サービスエリアが必要となり、ここに各サービスエリアの使用事業者管理コードやサービスコードを記述する。これにより、誰が何の目的でどこのサービスエリアを使用しているかの管理を行うことができる。

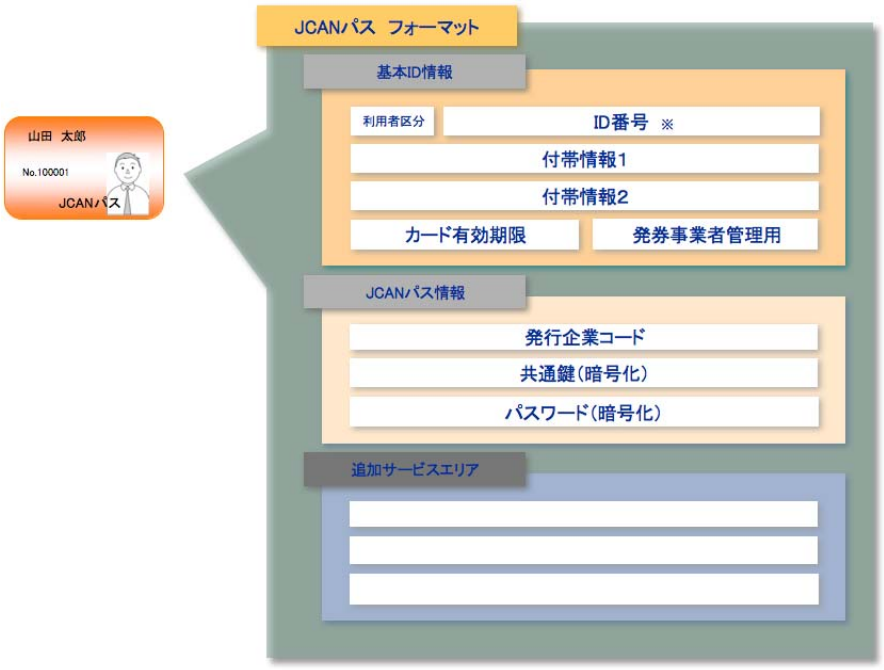


図 2-3　JCAN パス　フォーマット（案）

【基本 ID 情報】

ブロック数：4 ブロック　Write キーあり　Read キーなし

利用者区分	：2Byte	正社員、派遣、嘱託、部外者など別途定める区分
ID 番号	：12Byte	社員番号・学生番号・会員番号など
付帯情報 1	：16Byte	必要に応じて所有者の名前など
付帯情報 2	：16Byte	必要に応じて所有者の所属など
カード有効期限	：8Byte	カード有効期限の西暦年月日（YYYYMMDD 半角数字）
	発行事業者管理用：8Byte	発行事業者において、案件ごとの識別情報を記入（自由形式）

【JCAN パス情報】

ブロック数	：3 ブロック	Write キーあり　Read キーあり
発行企業コード	：16Byte	JCAN で定める企業コード
共通鍵	：16Byte	共通鍵（暗号化）
パスワード	：16Byte	JCAN パス認証パスワード（暗号化）

(b) JCANパス情報のアクセス用サービスキー

JCAN パス情報にはサービスキーを設置し、情報にアクセス時に使用する。

サービスキーは JCAN パスの利用規程に同意した企業のみ公開する。

なお、JCAN パス利用規程については、今後の検討課題となるため、当面は FCF フォーラムの利用規程に同意している FCF フォーラム会員を対象とすることを考えている。

(5) 利用イメージ

JCAN パスは、「(1)JCAN パスとは」で定義したように「必要に応じて後から情報の追加、削除が行える」ことから、例えば、初年度に社員証として JCAN パスを導入するが電子証明書の利用はせず「入退室管理」に用い、２年目から「勤怠管理」「ログイン」の利用を始め、３年目は「電子メール」「電子文書保存」「電子決裁」などのサービスを追加する運用を可能とする。

図 2-4　段階的なサービスの利用イメージ

(6) 今後に向けて

「マルチユース格納媒体における PKI 対応の検討」について、JCAN パスと言う考え方とその内容についての検討結果を検討した。

今後は、次の媒体を含めて共通フォーマットの検討を行いたいと考えている。

・非接触 IC カード　（Type B カード）
・RFID　（Radio Frequency IDentification「電波による個体識別」の略）
・SIM カード（携帯電話）

2.2.2 登録業務効率化の検討

本検討では、登録業務の効率化を目的に、電子証明書の発行等の処理と結び付いた JCAN パスの発行等の処理を調査検討した。

なお、本検討の詳細については、添付資料 C「登録業務効率化の検討」を参照のこと。

(1) システム概要

(a) 電子証明書申請発行管理システム（仮称）

電子証明書申請発行システムは、JCAN 提供する電子証明書の申請・発行手続きを行うためのシステムで、人事システム等の社員情報管理システムと連携して、社員や部門の電子証明書の申請及び取得・管理が行える。

主な機能としては、申請機能、更新機能、データベース機能、失効機能、他システム連携機能等を提供するものと考えている。

なお、このシステムを開発するために必要な、CA（認証局）等とデータ交換をするための API（Application Programming Interface)、人事情報を交換するための API、管理 DB フォーマットについては、今後の検討課題とする。

(b) JCANパス情報管理システム（仮称）

JCAN パス情報管理システムは、JCAN パス内の JCAN パス情報エリアに情報を書き込むシステムで、カード発行システムのオプションとして機能するものである。

なお、このシステムを開発するために必要な、ID 情報を元に電子証明書申請発行システムから JCAN パス情報を取得する API、情報を暗号化する API、JCAN パスエリアへの書き込みを行う API については、今後の検討課題とする。

(2) JCANパスのライフサイクル管理

(a) 発行

次の図は、JCAN パスの発行フローを示したもので、黒矢印が電子証明書の発行に関する流れ、緑矢印が JCAN パスの発行に関する流れとなる。

登録業務の効率化には、管理番号を中核に「既存人事システム等」「電子証明書申請発行管理システム」「JCAN パス情報管理システム」を連携させることが必要となる。

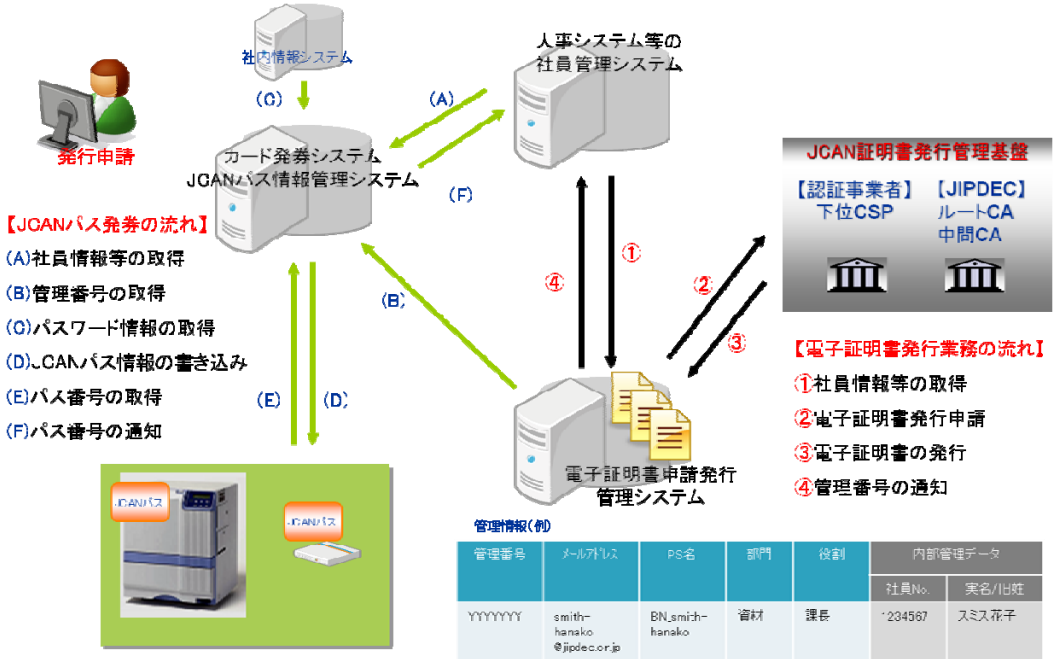


図 2-5　JCAN パスの発行フロー

(b) 再発行

次の図は、再発行フローを示したものである。

再発行の場合は、紛失した電子証明書及び JCAN パスの失効が必要となる。

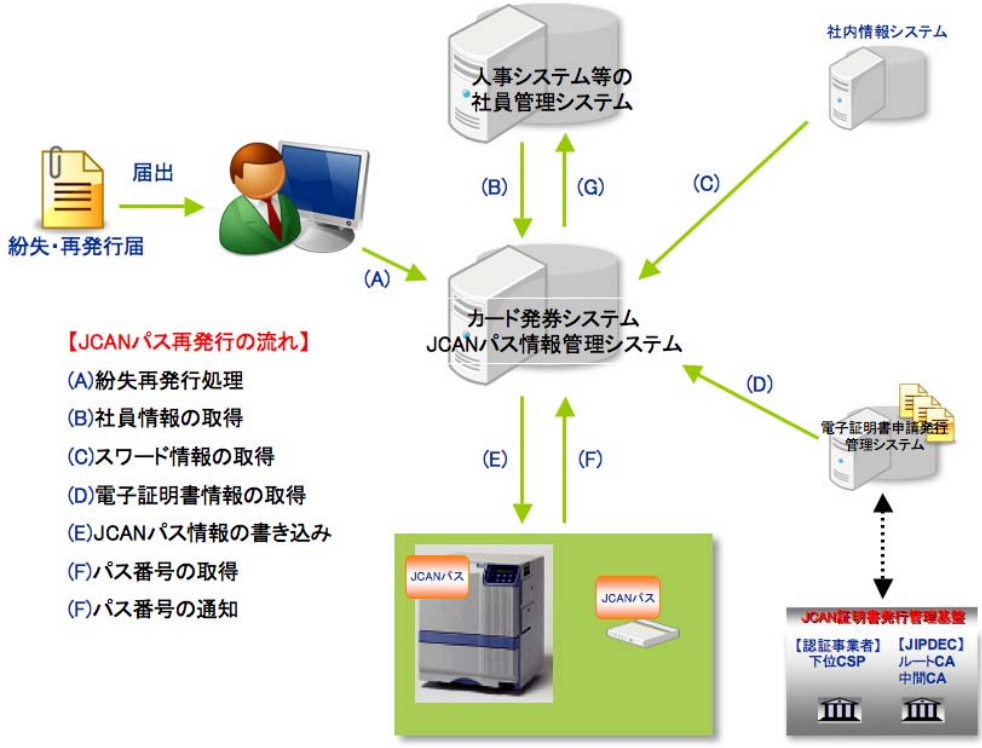


図 2-6　JCAN パス再発行フロー

(c) 失効

次の図は、失効フローを示したものある。

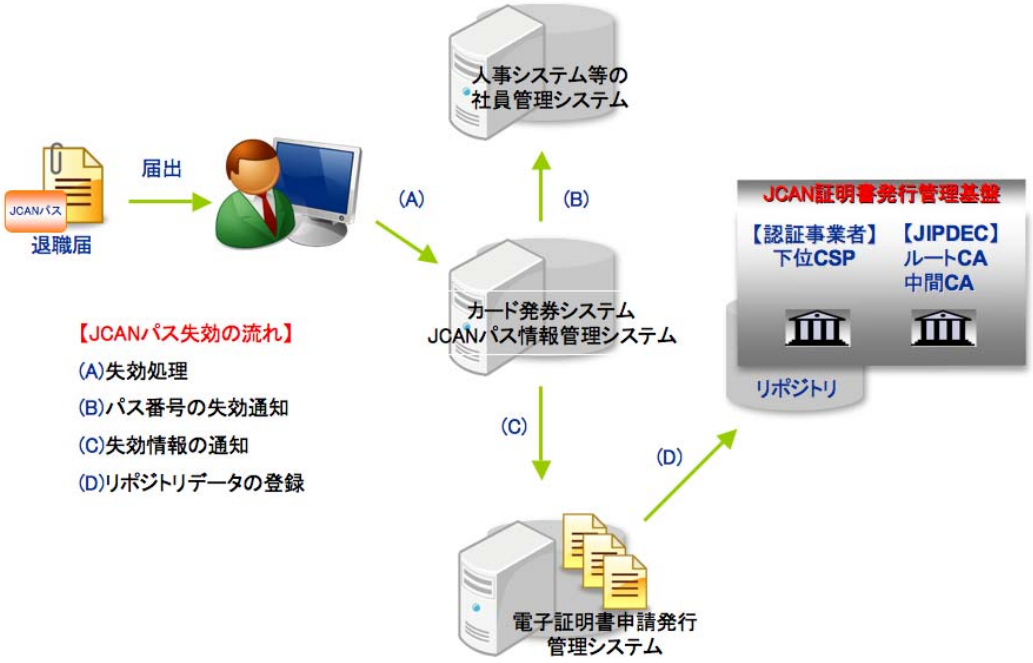


図 2-7　JCAN パス失効フロー

(3) 今後に向けて

今回は FeliCa カードをベースに JCAN パスの検討を行った。

今後は、FeliCa カード以外の媒体を含め、運用ルールやアプリケーションインターフェースの検討を行いたいと考えている。

2.3 3000 社アンケート調査

制度全体のプロモーションを目的に、JCAN の仕組み/メリットを訴求した冊子を作り、3000 社アンケートを実施する。

なお、冊子については、添付資料 D「プロモーション冊子」を参照のこと。

(1) 対象

次のデータから無作為に抽出及び電子取引に関係する団体の 3,000 社を抽出した。

・会社四季報　上場会社　約 4,000 社
・会社四季報　未上場会社　約 8,000 社

(2) アンケート票

調査表概要を次の表に示す。

表 2-1 アンケート調査票概要

分類	項目
・業務の電子化進展度合い	・ 情報システムインフラの整備状況 ・ 組織内情報・業務の電子化状況 ・ 社外との業務の電子化状況 ・ 業務の電子化に関して想定している脅威 ・ 企業コードの所有率
・電子署名/電子証明書の用途 ・業務における電子署名/電子証明書の利用状況	・ 電子署名/電子証明書の利用状況 ・ 電子署名/電子証明書を使わない理由 ・ 電子署名/電子証明書が必要な理由 ・ 電子署名/電子証明書の格納媒体 ・ 電子署名/電子証明書の有効期間 ・ 電子署名/電子証明書の発行元 ・ 電子署名/電子証明書の発行手続きの問題点 ・ 電子署名/電子証明書を配付したい対象 ・ 電子署名/電子証明書を利用したアプリケーションの利用実績と予定 ・ 電子署名/電子証明書を利用したアプリケーションの業務効率化・コスト削減への影響 ・ 電子署名/電子証明書が有効な理由 ・ 電子署名/電子証明書が有効でない理由 ・ 電子署名/電子証明書が仮にあった場合の利用用途
・冊子について	・ 冊子の反応 ・ 会員メンバー等への電子署名/電子証明書の発行 ・ 自社認証局のメリット ・ 自社認証局のデメリット ・ 自社認証局の所有
・企業属性	・ 業種 ・ 従業員数 ・ 資本金 ・ 年間売上高 ・ プライバシーマーク、ISMS の取得状況

(3) 調査実施スケジュール

調査実施スケジュールは以下の通りである。

表 2-2 アンケート調査実施スケジュール

作業内容	実施期間
印刷	2009 年 12 月 21 日～12 月 25 日
封入発送	2010 年 1 月 5 日～1 月 8 日
調査期間	2010 年 1 月 13 日～1 月 29 日
回収締切	2010 年 2 月 15 日
集計分析	2010 年 2 月 19 日

(4) 調査結果

アンケート送付数　3,000

アンケート実質到達数　2,812　（移転及び倒産等の不達による返送数　188）

回答数　200　（回答率　7.1%）

なお、集計に際しては以下のようなデータチェックをかけた。

・限定質問は親設問を優先、調査票で確認し矛盾回答は非該当とした

・数量データで異常に小さい値や大きい値は調査票で確認

・自由記入の整合性を確認

(5) 調査結果の分析

アンケート結果については、添付資料Ｅ「3000 社アンケート結果」を参照のこと。

なお、本調査において次の事実が認められた。

(a) 電子証明書の発行に興味がある企業数

電子証明書の発行を「実施したい 1 社(0.5%)」「検討できる 20 社(10.0%)」「興味がある 61 社(30.5%)」で合計 82 社(41%)であった。

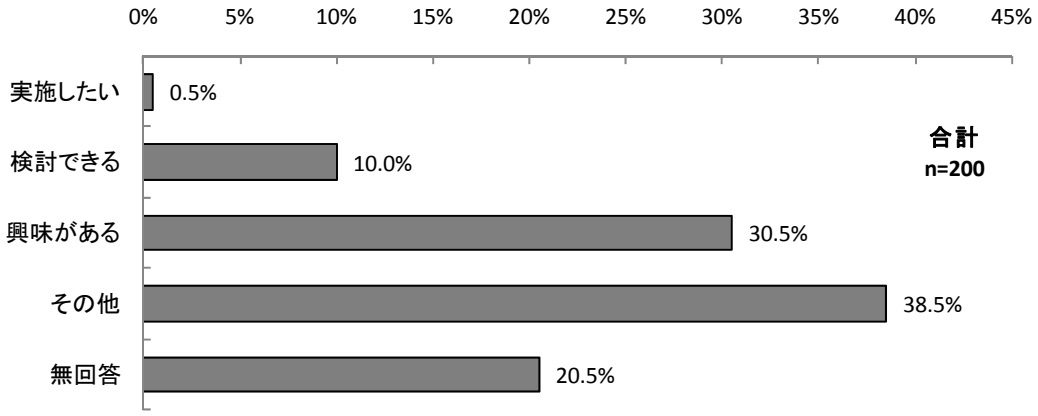


図 2-8 電子証明書の発行に興味がある企業数

(b) 上記 82 社における電子証明書の発行対象

「全社員 24 社(29.3%)」「管理職 18 社(22.0%)」「担当者 12 社(14.6%)」「取引先 10 社(12.2%)」「代表者 9 社(11.0%)」「グループ会社 5 社(6.1%)」「派遣 3 社(3.7%)」であった。

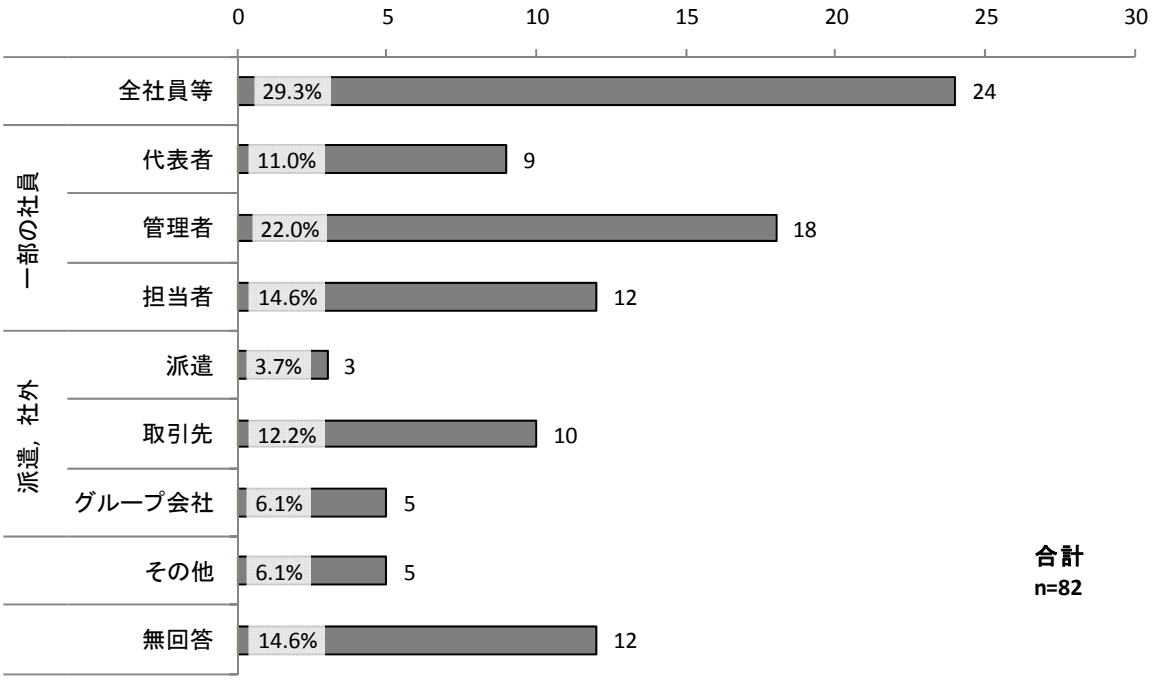


図 2-9 電電子証明書の発行対象

(c) 上記 82 社の社員数

「99 名以下 17 社(20.7%)」「100~199 名 14 社(17.1%)」「500~599 名 8 社(9.8%)」「1500~1999 名 6 社(7.3%)」「200~299 名 5 社(6.1%)」「400~499 名 5 社(6.1%)」であった。

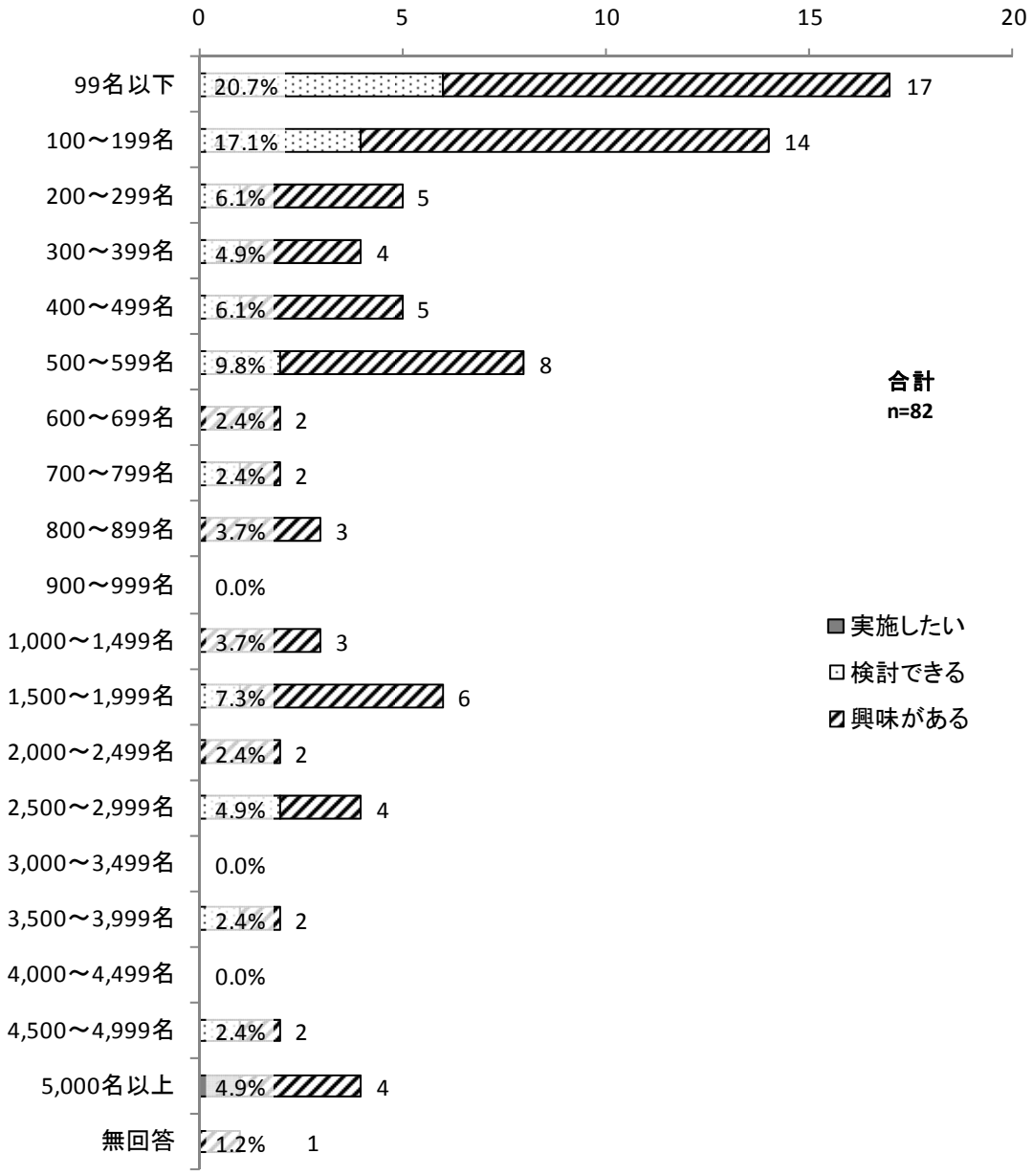


図 2-10 上記 82 社の社員数

3. ポリシー/基盤システムの検討

この検討は、「WebTrust for CA」の認定をうけて運用する「民間認証基盤」のルート認証局の組織、体制、構築、運用に関するポリシーの要点、ルート認証局をトラストアンカーとする認証局への発行申請方法をまとめたものである。

3.1 証明書ポリシー

電子認証及び電子署名に係る民間制度・基盤の確立及びその環境整備のために、社員証等の属性情報を扱う共通の電子証明書ポリシー案を検討した。

公開鍵暗号方式を使った電子証明書の規格の１つに X.509 がある。

X.509 をインターネットで利用することを目的に、IETF の PKIX 作業部会によって、その運用ルールが規定化された最新バージョンが RFC3647 でありデファクトスタンダードと言える。

RFC3647 では、第 3 章において、X.509 標準は、CP を特定のコミュニティ、かつ／または、共通のセキュリティ要件をもつアプリケーションのクラスへの証明書の適用可能性を示すルールの命名された集合」と定義しており、本報告書では、JCAN の認証ドメイン内で認証局に対する信頼性を示す CPS を作成するにあたり、電子証明書の適用性を指定する規則として RFC5280 に準じて証明書ポリシー（CP）を作成した。

JCAN で取り扱う証明書タイプは、以下のとおりである。

(1) 証明書タイプ

(a) パートナCA証明書

JCAN CA により認定されたパートナ CA の CA 証明書である。パートナ CA 証明書は以下の 2 通りで発行される。

・JCAN ルート CA 又は JCAN 中間 CA から発行される
・WeTrust の認定をうけているパブリック認証局から発行される

(b) JCANビジネス証明書（End Entity証明書）

JCAN の証明書は、認証サービス、セキュア電子メール、及び組織内、組織間、インターネットでの金額を伴わない取引で利用者を認証することに利用できる。JCAN が取扱う証明書（以下「JCAN 証明書」という）のタイプを下記に示す。

・企業／団体内個人及びそれに結びつく属性（肩書き等）を証明する証明書
・企業／団体の組織（部門名、役割）であることを証明する証明書
・企業／団体の設備であることを証する証明書

また、各証明書のタイプごとのプロファイルを、EE（End Entity）証明書、発行 CA 証明書、ルート CA 証明書の案を検討・作成した。また、関連する CRL プロファイルの案も検討・作成した。

3.2 共通運用ルール

企業において、グループ会社あるいは取引先を含めた業務連携の効率化を、安心・安全に進めることは経営力向上に資する重要な活動のひとつである。

具体的には権限・資格等（以下「属性情報」）に基づいた「アクセス」「決済」が規定どおり行われていることが求められることから、本事業では「社員等の属性情報を扱う電子認証（IDを含む）及び電子署名に係る民間制度・基盤の確立及びその環境整備」について調査研究を行うものである。

ここでは、証明書ポリシーの検討以外の以下の 2 点を検討した。

- MS-Windows、Java、Mozilla 等の「信頼されたルート認証機関」に求められる要件を、認証局運用に係る上位内部規程である「事務取扱要領」に仕様をまとめる。
- 発行申請業務の共通化を検討すること。

3.2.1 事務取扱要領

MS-Windows、Java、Mozilla 等の「信頼されたルート認証機関」リストに登録される場合の前提は「WebTrust for CA」の認定である。「WebTrust for CA」の認定をうけて運用する場合に必要な内部規定の要点を事務取扱要領仕様としてまとめた。

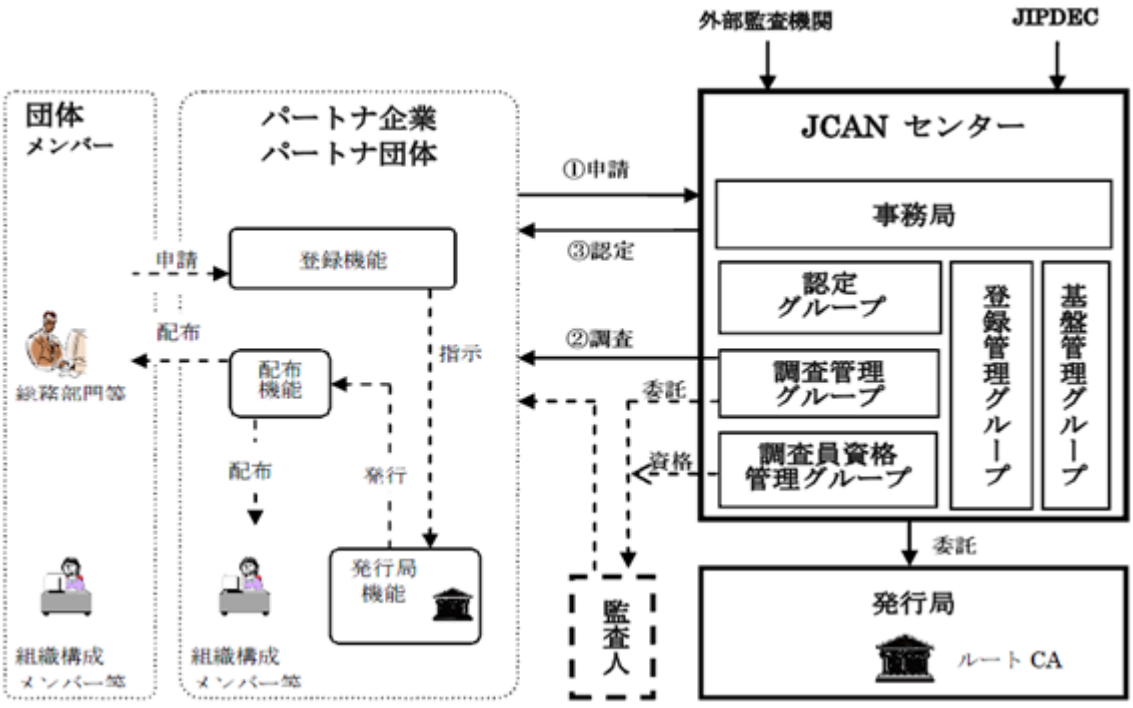


図 3-1　JCAN の構成要素

JCAN センター内には事務局、基盤管理グループ、登録管理グループ、認定グループ、調査管理グループ、調査員資格グループと役割を分け、パートナ企業・団体の CA の申請受付、認定可否の通知、認証局運用管理規程（CPS)、証明書ポリシー（CP）および情報セキュリティポリシー等の策定、パートナ CA の登録及び電子証明書の発行手続き、失効手続き等を WebTrust for CA の認定基準に準拠して運用を行い、外部監査機関の年次調査に備える体制をとる。監査人又は調査員はパートナ企業・団体がパートナとしての有資格者かどうかの調査を行い、認定を受けたパートナ企業・団体は証明書の申請のあった団体メンバーに対し、証明書発行業務を行う。尚、WebTrust の認定を受けた当初はルート証明書のブラウザ、メーラーへの普及率の度合いから外部の信頼済みルート CA の支援を受ける。

3.2.2 発行申請業務の共通化の検討

人事システムなど企業の既存システムと連携し、一括発行が可能なように、電子証明書のプロファイルの共通記載事項を検討した。またそれにより電子証明書の発行要求時に記載事項の登録に必要なデータ形式を整えることを検討した。

(1) 管理台帳

人事システムなど企業の既存システムと連携し、一括発行が可能なよう、証明書の共通記載事項を検討した。

共通部分

企業コード	企業名	メールアドレス	電話	ホームページ	操作責任者
1.2.392.200063	JIPDEC	ra@jipdec.or.jp	8133436xxxx	www.jipdec.or.jp／ra	山田太郎

管理番号対応部分

管理番号	メールアドレス	BN名	区分 1.企業内個人 2.部門/役割名	肩書き	部門/役割名	電話	承認日	状態	内部管理データ(提出不要)	
									社員No.	実名
YY. YYYY.	smith@jipdec.or.jp	Bn_smith_manager	1	課長	資材部	8133236XXXX	080401	貸与	123	スミス 花子
YYYY YYYY							090331	回収		

図 3-2 電子証明書発行要求データ形式

証明書の取得方法にはいくつか方法があるが、利用者が電子証明書のインストールを滞りなく、行えるよう PKCS#12 形式として配付することを検討した。PKCS#12 形式のファイルは、パスワード（PIN）に基づく暗号により保護された署名鍵（秘密鍵）と、それに関連する電子証明書を保管するために一般に利用されるファイルフォーマットである。PKCS#12 形式にすることで、ユーザまで署名鍵はパスワードにより秘匿されることとなる。

(2) 電子証明書貸与方法

証明書の取得方法にはいくつか方法があるが、利用者が証明書のインストールを滞りなく、行えるように且つ S/MIME 使用時に PKCS#7 形式を利用して上位 CA の証明書の配付を容易にするため PKCS#12 形式とした。

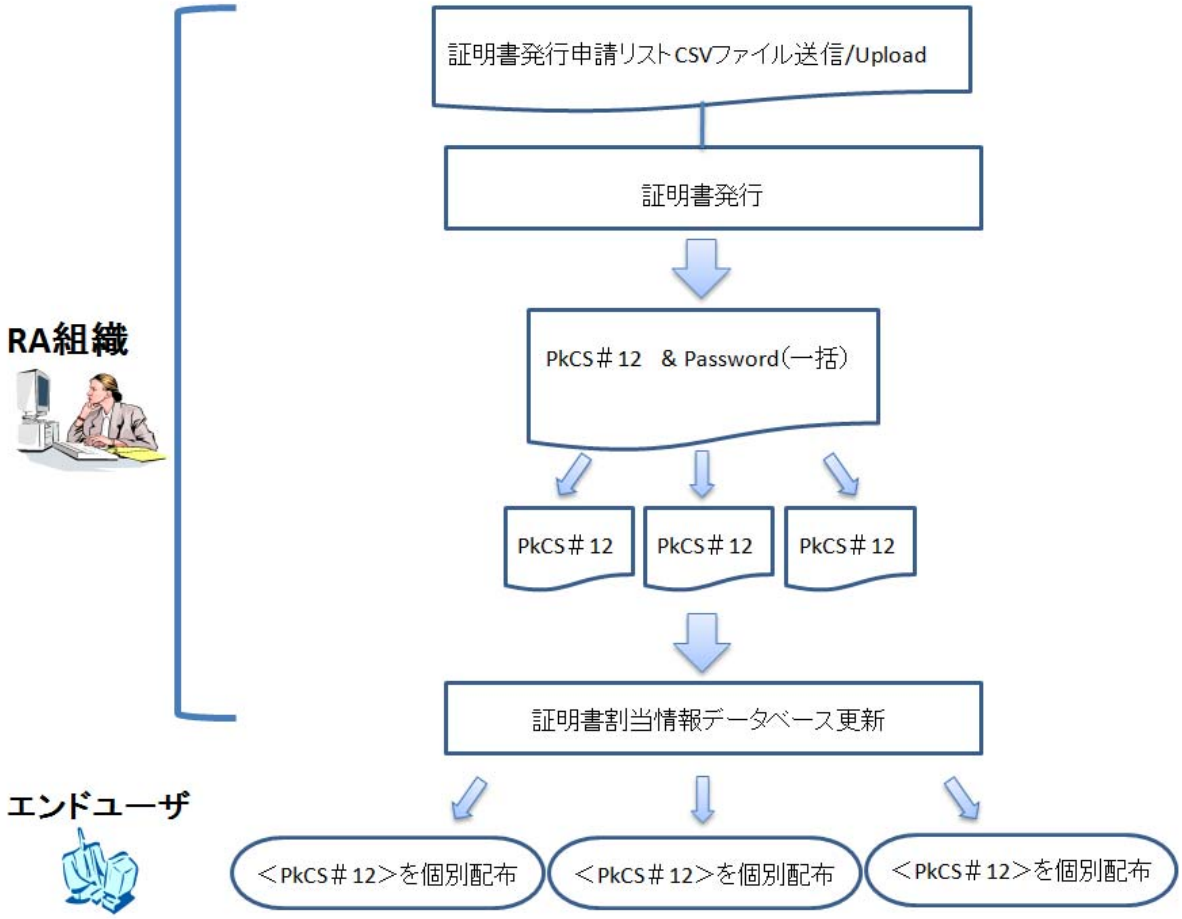


図 3-3　電子証明書貸与方法フロー

4. 評価基準の検討

4.1 登録業務の評価基準

(1) 登録業務の概要

(a) 登録業務フロー

登録業務とは、異動･退職等の情報に基づいて作成された管理台帳を発行業務に送って電子証明書の発行を受け、当該証明書を社員等に貸与･回収する業務である。登録業務のフローを次に示す。

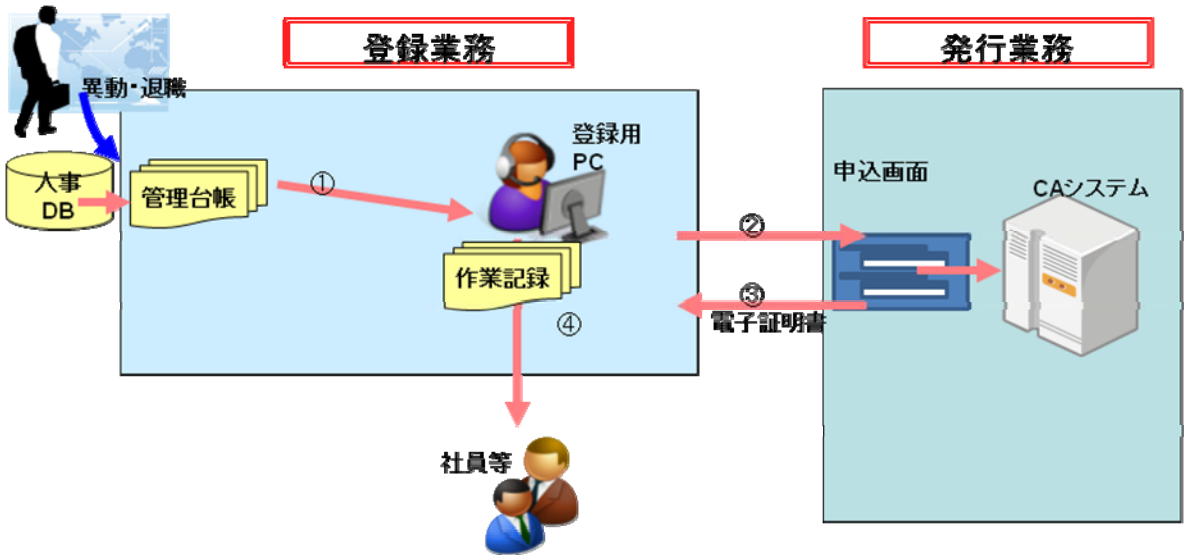


図 4-1　登録業務のフロー

(b) 管理台帳

管理台帳とは、電子証明書記載事項を含む電子証明書貸与者情報を記録した台帳である。台帳は、登録業務部門情報を記載する共通部分と貸与者情報を記載する管理番号部分がある。管理台帳の記載例を次に示す。

共通部分

企業コード	企業名	メールアドレス	電話	ホームページ	操作責任者
1.2.392.200063	JIPDEC	ra@jipdec.or.jp	8133436xxxx	www.jipdec.or.jp/ra	山田太郎

管理番号対応部分

管理番号	メールアドレス	PS名	区分 1.企業等内個人 2.部門/役割	部門	役割	内部管理データ(提出不要)	
						社員No.	実名
YYYYYYYY	smith-hanako@jipdec.or.jp	BN_smith	1	資材	課長	123	スミス花子
ZZZZZZZZ	supply@jipdec.or.jp	BO_supply	2	資材	担当	223	青木花子

◆管理番号
・社員No.と異なる番号を推奨する。
◆PS名には2つの付け方がある
・企業等内個人向け
旧姓等の場合は最初にBNをつける
・部門/役割向け
最初にBOをつける(例えばBO supply manager)

図 4-2　管理台帳の記載例

(2) 登録業務の評価基準

登録業務の評価基準の目的は、原則として電子証明書が人事台帳と結び付いて管理されていることを確認することにある。

具体的には、次に示すチェックシートに基づく内部監査を JCAN がサンプリング調査するやり方を考えている。

なお、レベルは、企業の人事管理のシステムと同程度のセキュリティレベルとする。

表 4-1 登録業務の評価基準用チェックシート

チェック項目		実施内容	提出資料
①登録用 PC のアクセス管理			
M-1	登録用 PC のログインパスワード管理を「登録業務事務取扱要領」に規定していますか。	□ 規定している。 （章節番号：　　） →具体的な方法は、 □ パスワード □ IC カード □ その他（　　） □ 規定していない。	
M-2	上記パスワード等の定期的な変更を行っていますか。	□ 変更している。 →定期的にパスワードを変更している （最近の変更日　　年　　月　　日） □ 変更していない。	
②スクリーンセーバーのパスワード設定			
M-3	スクリーンセーバーによるパスワードロックは、3 分以内に設定されていますか。	□ 設定している。 □ 設定していない。	
③ウイルス対策			
M-4	ウイルス対策ソフトが導入されて、パターンファイルが更新されていますか。	□ 導入している。 →パターンファイルの更新日は、 （　　年　　月　　日　：　） □ 導入していない。	
④登録業務			

チェック項目		実施内容	提出資料
M-5	電子証明書は、組織に属している対象（企業内個人、部門名、設備等）に貸与していますか。	□ 次の対象に貸与していることを管理台帳で管理している。 □人事 DB 登録者 □請負・派遣契約で指定された者 □組織体制表で管理されている部門名等 □その他管理簿で確認されている者／設備 □貸与先を管理台帳で管理していない。	
M-6	上記貸与者の異動・退職・変更に伴う管理台帳の内部監査を行っていますか。	□ 上記帳簿と突合せを行なっている。 □有効な電子証明書の総数 （約　　） □総貸与数 （約　　） □過去 1 年間のメンテナンス数 （約　　） □ 行っていない。	異動・退職者総数 失効総数
M-7	登録業務の作業記録を残していますか。	□ 残している。 □ 残していない。	
O-8	登録業務関係者に対して、年に一度又は任命の都度教育をし、教育記録を残していますか。	□ 残している。 □ 残していない。	

4.2 民間認証局の調査表案の検討 （発行業務の評価基準）

「社員等の属性情報を扱う電子認証（ID を含む）及び電子署名に係る民間制度･基盤の確立及びその環境整備」の一部として、「WebTrust for CA 監査基準」への準拠が必要と想定し、BtoG の電子認証に使える電子証明書を発行する民間認証局の調査表案の検討を行った。

(1) 民間認証局の調査表案の検討

わが国では、一定の電子署名をされた電子文書は、手書き署名や押印をされた文書と同程度の法的効力を持つことが期待されるようになった。これによりネットワークを用いた情報交換の信頼性、安全性が飛躍的に向上する上、電子署名の普及により情報流通の円滑化、手続きの簡素化により、電子商取引をはじめとする経済活動の発展を促すことが期待されている。片や電子署名、電子証明書の言わば現在のスタンダードとなっている PKI 技術を応用したデジタル署名及びデジタル証明書は、上位の認証局による認証を受けず、自らの正当性を自ら証明する認証局（ルート認証局）が発行するルート証明書を頂点とした信頼性が確保された枠組み（認証ドメイン）の中で運用される認証局で発行されたものである。したがってルート認証局は信頼の連鎖の頂点に位置することから厳しい監査を受け監査に通過したものだけが、広く利用されるルート認証局（パブリック認証局）と呼ばれることとなる。

JCAN はパブリック認証局を持つ認証ドメインを構成するため、パブリック認証局になるために、米国公認会計士協会およびカナダ勅許会計士協会が共同で開発・管理運営している WebTrust for CA 監査を受けることが必要となる。

「WebTrust for CA 監査基準」と電子署名法「特定認証業務の認定に係る調査表」を比較し、WebTrust for CA 認定を得るために必要な、設備、運用等の規定を明らかにした。続いて WebTrust for CA 監査基準の各項目について、認定認証業務の調査表における措置状況に相当する事項を検討しつつ、調査表案として作成を行った。

(2) 対応関係状況の調査

まず「WebTrust for CA 監査基準」の全項目(criteria)を和訳した。次いでその各項目について、「特定認証業務の認定に係る調査表」の、相当する項目を検索し

・用語、表現の相違の吟味
・米国、カナダの社会制度などと我が国の制度の相違の吟味

などを勘案し、適宜読み替えを行った。その結果、電子署名法側に存在しないと思われる項目が criteria 386 項目中 86 項目（PRINCIPLE1 に 45 項目中 8 項目､PRINCIPLE2 に 176 項目中 70 項目、PRINICPLE3 に 165 項目中 8 項目）存在した。このほかに電子署名法側の複数の項目で対応している項目（30 項目)、電子署名法側には明示されていないが認定調査

では確認される項目（90 項目）などが存在した。

(3) 対応関係の相違部分の検討

電子署名法側に存在しないと思われる項目について、WebTrust for CA 側の ILLUSTRATIVE DISCLOSURES 欄の記載事項を参考に、「社員等の属性情報を扱う電子認証（ID を含む）及び電子署名に係る民間制度･基盤」の認証業務を想定しつつ、既存事例を基に検討を行った。

(4) 調査表案の作成、報告

上記の準備作業の後、WebTrust for CA 監査基準の全項目(criteria)について、ルート/中間 CA 要件案、パートナ CA 要件案の検討を行った。なお、当初計画では「ルート CA」「中間 CA」「下位 CA」「利用者 RA」それぞれについて検討することとしていたが、「社員等の属性情報を扱う電子認証（ID を含む）及び電子署名に係る民間制度･基盤」に関する全体的な検討に合わせる形で、利用者 RA（その要件案はチェックリスト化された）を削除し、下位 CA をパートナ CA と名称変更し、CA に対する証明書発行を扱うルート CA と中間 CA をひとつにまとめた。各項目の要件案は、PKI 普及促進を重要目的のひとつとする「社員等の属性情報を扱う電子認証（ID を含む）及び電子署名に係る民間制度･基盤」の趣旨に沿って運用コスト低減を目指すため、既存事例のやや厳し過ぎるセキュリティ要件設定を排し、別に検討が進められていた「社員等の属性情報を扱う電子認証（ID を含む）及び電子署名に係る民間制度･基盤」の証明書ポリシー、CPS の検討に合わせる形で、両要件案を記していくこととした。

5. 認定制度の検討

JCAN ビジネス電子証明書は、JCAN に認定された企業等の信用力と情報管理力を担保に発行される。当該認定に係る制度の検討結果を次に示す。

(1) JCAN文書一覧

制度で用いる文書一覧を次に示す。なお、文書において、申請書類は「申」、規程は「規」、管理用様式は「管」、記録用様式は「記」と区分している。

表 5-1 JCAN 文書一覧

区分	文書番号	文書名称	版（Ver.）	改訂日
申	30-5000	JCAN 文書一覧表	0.1	
申	30-5010	申請の手引き（JCAN ビジネス CP 編）	0.1	
申	30-5020	申請書（JCAN ビジネス CP 編 登録業務編）	0.1	
申	30-5030	申請書（JCAN ビジネス CP 編 発行業務編）	―	
申	30-5040	利用の手引き（JCAN ビジネス CP 編）	―	
申	30-5050	JCAN ビジネス認定業務に係る秘密情報の取扱いに関する規約	―	
申	30-5060	JCAN ビジネス制度設置及び運営要領	―	
規	30-5100	JCAN ルート CA/中間 CA「CPS」	―	
規	30-5110	JCAN ルート CA/中間 CA「事務取扱要領」	―	
規	30-5150	JCAN ルート CA/中間 CA「CP」	―	
規	30-5200	JCAN 共通 CPS	―	
規	30-5210	JCAN 共通事務取扱要領（登録業務編）	―	
規	30-5250	JCAN 共通事務取扱要領（発行業務編）	―	
規	30-5300	JCAN 共通 CP「JCAN ビジネス CP」	―	
管	30-5500	JCAN ビジネス CP 登録業務 規程・記録一覧	0.1	
管	30-5510	JCAN ビジネス CP 登録業務 責任者体制表	0.1	
管	30-5550	JCAN ビジネス CP 発行業務 規程・記録一覧	0.1	
管	30-5560	JCAN ビジネス CP 発行業務 責任者体制表	0.1	
管	30-5600	JCAN ビジネス CP 電子証明書配付・回収管理台帳	0.1	
記	30-5700	JCAN ビジネス CP 教育記録	0.1	
記	30-5710	JCAN ビジネス CP 登録業務 作業記録	0.1	
記	30-5750	JCAN ビジネス CP 発行業務 作業記録	0.1	

(2) 認定手続き

初回認定までの手続きには、「予備調査」と「初回申請」がある。

また、更新認定の手続きには、「更新申請」がある。

次に「認定手続きの流れ」を示す。

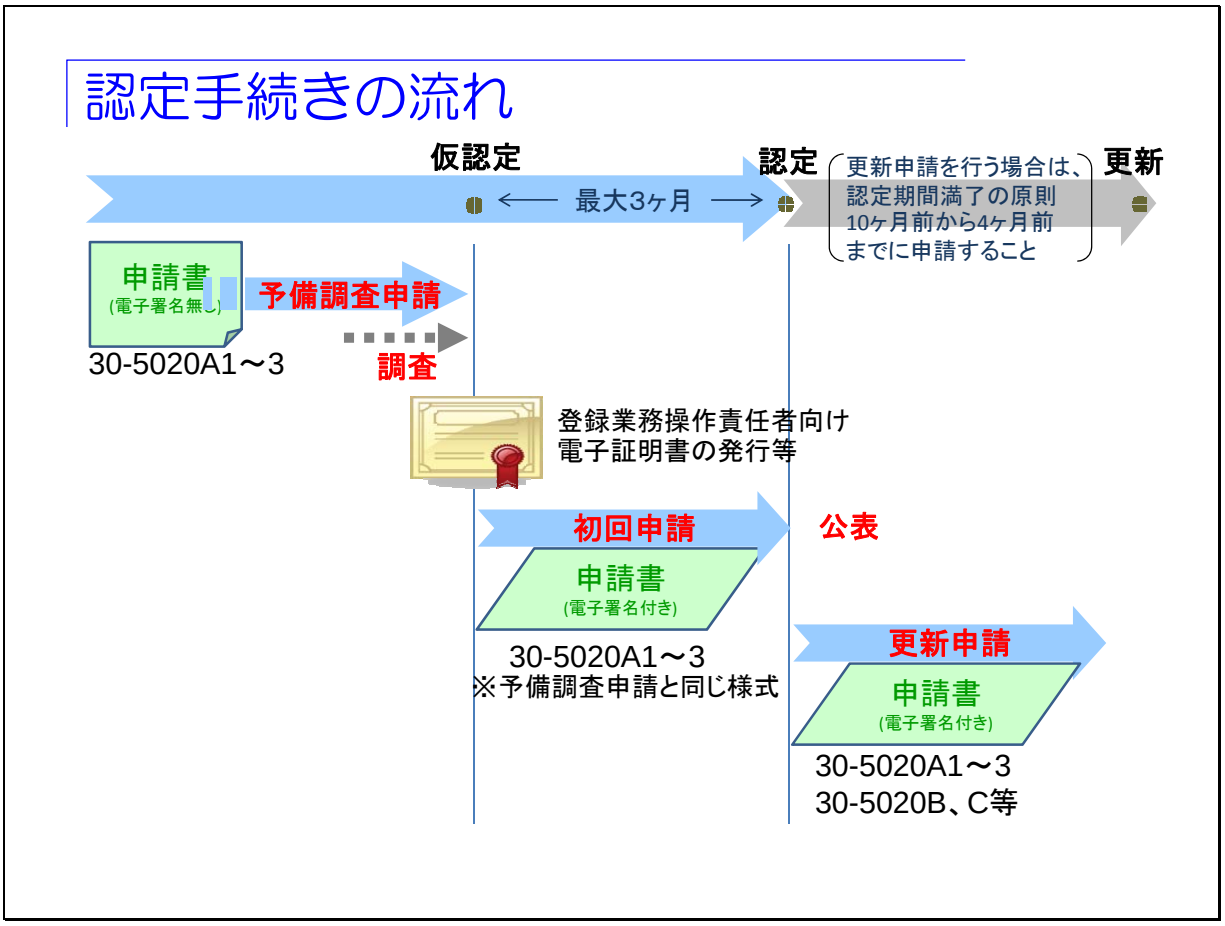


図 5-1　認定手続きの流れ

(a) 予備調査

予備調査の流れを次に示す。

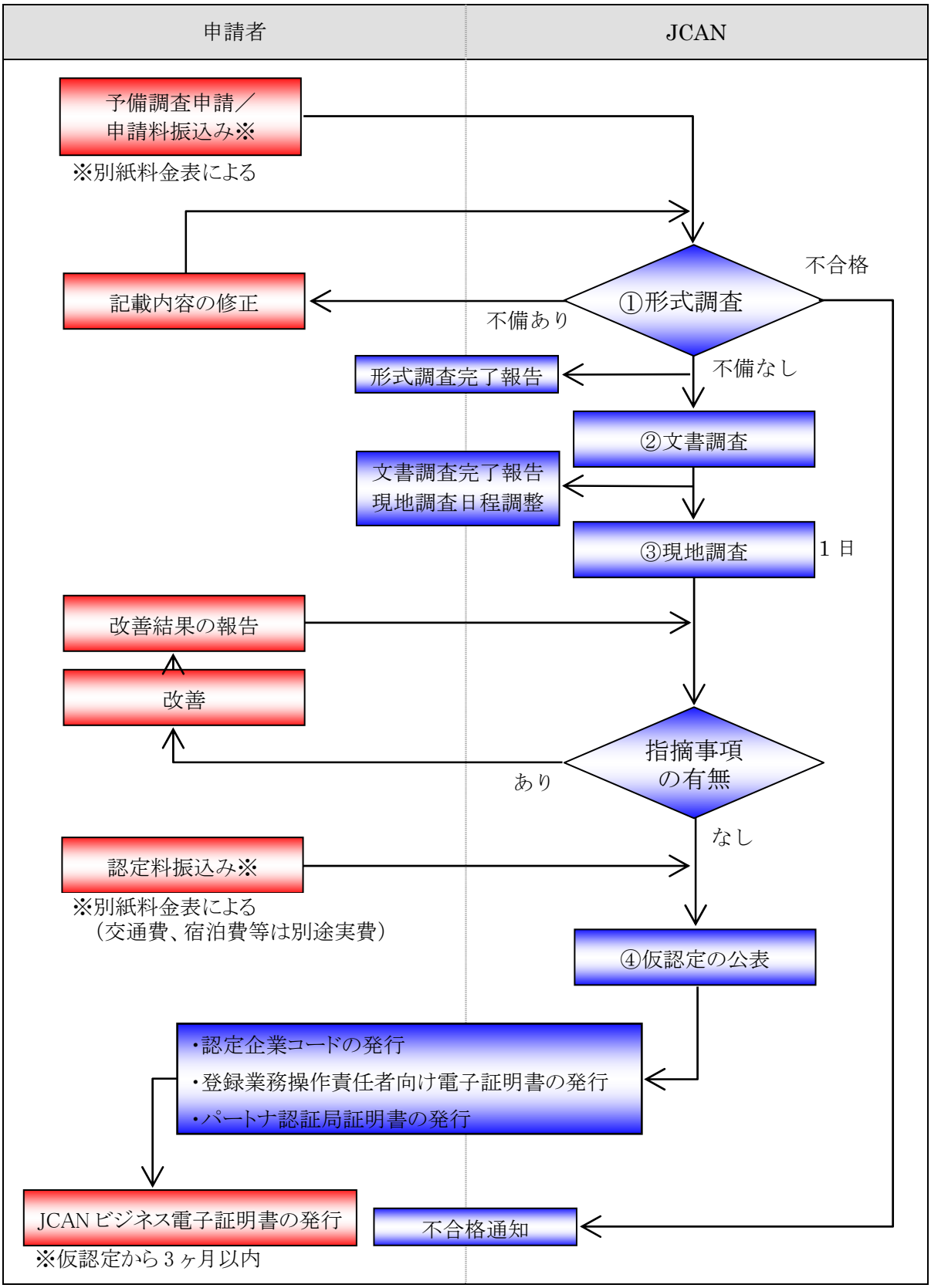


図 5-2　予備調査の流れ

①形式調査

「予備調査申請」及び「申請料振込み」が行われると形式調査が行われる。

形式調査に不備が無ければ「形式調査完了報告」が行われ、次のステップに進む。

②文書調査

文書調査に不備が無ければ「文書調査完了報告」が行われ、「現地調査日程調整後」次のステップに進む。

③現地調査

現地調査で指摘事項が無ければ「現地調査完了報告」が行われる。

④仮認定の公表

「認定料振込み」が受付けられると仮認定の公表、及び「認定企業コード」「登録業務操作責任者向け電子証明書」「パートナ認証局証明書」の発行が行われ、「JCANビジネス電子証明書の発行」ができるようになる。

※仮認定は３ケ月以内に初回申請を行わないと中止の公表が行われる。

(b) 初回申請

初回申請の流れを次に示す。

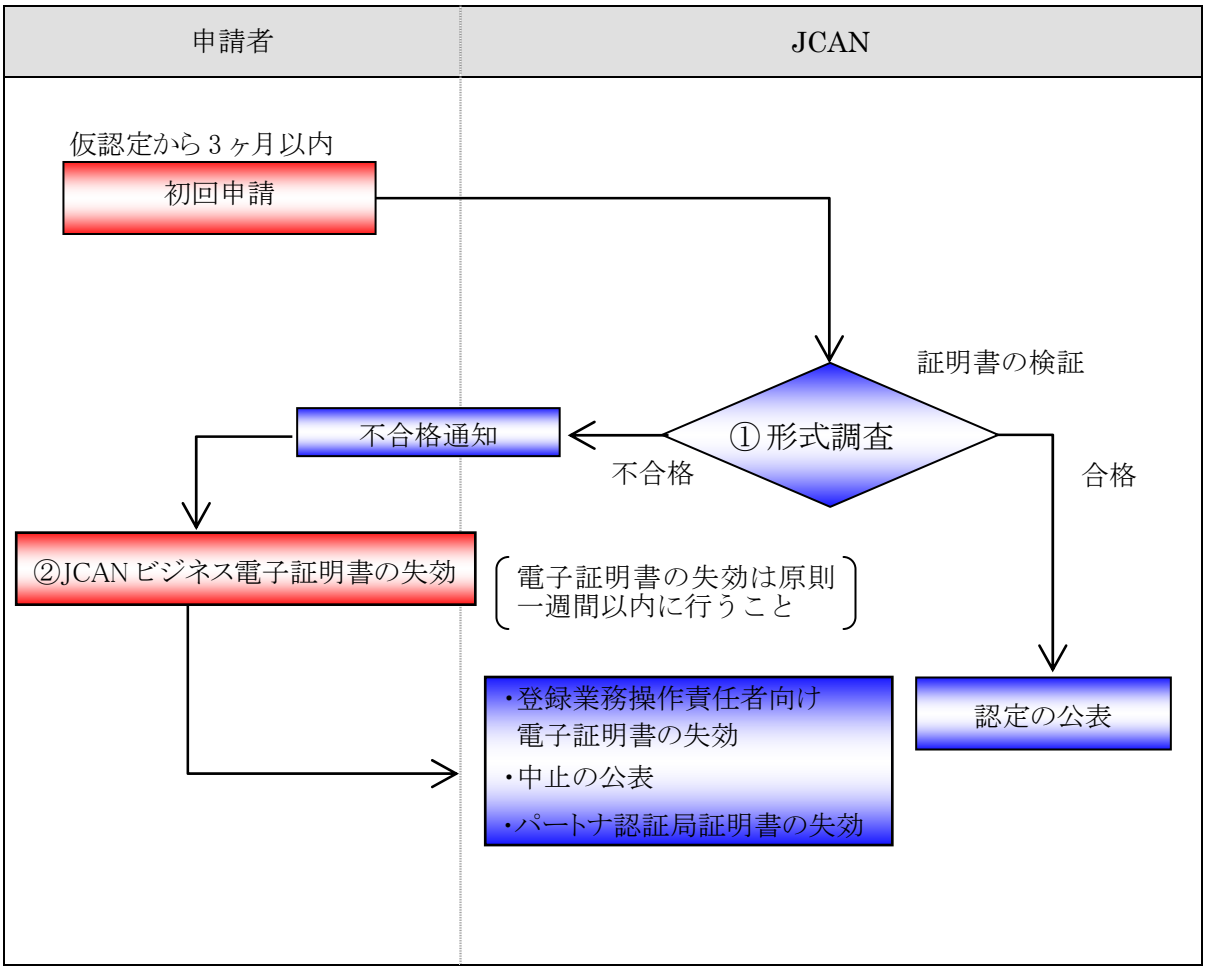


図 5-3　初回申請の流れ

①形式調査

仮認定は３ケ月以内に「初回申請」行われると形式調査が行われる。

形式調査に不備が無ければ認定の公表が行われる。

※形式審査で不合格になると「不合格通知」 が行われる。

②不合格

不合格通知が行われたら、原則１週間以内に「発行した全JCANビジネス電子証明書の失効」を行うこと。

その後、「登録業務操作責任者向け電子証明書」「パートナ認証局証明書」が失効され、中止の公表が行われる。

(c) 更新申請

更新申請の流れを次に示す。

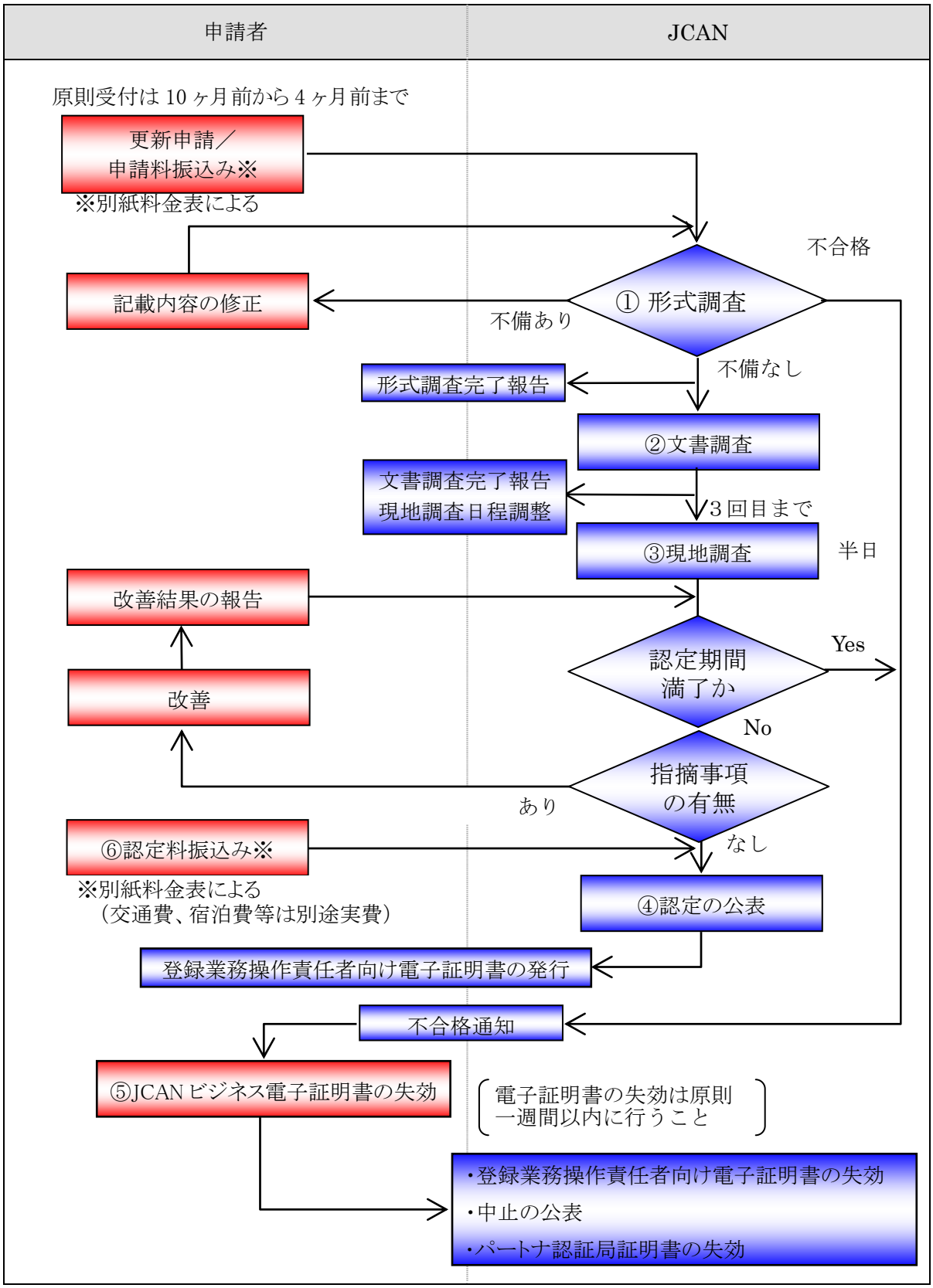


図 5-4　更新申請の流れ

①形式調査
「更新申請」及び「申請料振込み」が行われると形式調査が行われる。
形式調査に不備が無ければ「形式調査完了報告」が行われ、次のステップに進む。

②文書調査
文書調査に不備が無ければ「文書調査完了報告」が行われ、「現地調査日程調整後」次のステップに進む。
※現地調査を行わない場合がある。この場合は、その旨連絡する。

③現地調査
現地調査で指摘事項が無ければ「現地調査完了報告」が行われる。
※現地調査中認定期間が満了すると「不合格通知」が行われる。

④認定の公表
「認定料振込み」が受付けられると認定の公表、及び「登録業務操作責任者向け電子証明書」の発行が行われ、引き続き「JCANビジネス電子証明書の発行」ができるようになる。

⑤不合格
不合格通知が行われたら、原則１週間以内に「発行した全JCANビジネス電子証明書の失効」を行うこと。
その後、「登録業務操作責任者向け電子証明書」「パートナ認証局証明書」が失効され、中止の公表が行われる。

6. 利用の手引き（イメージ）

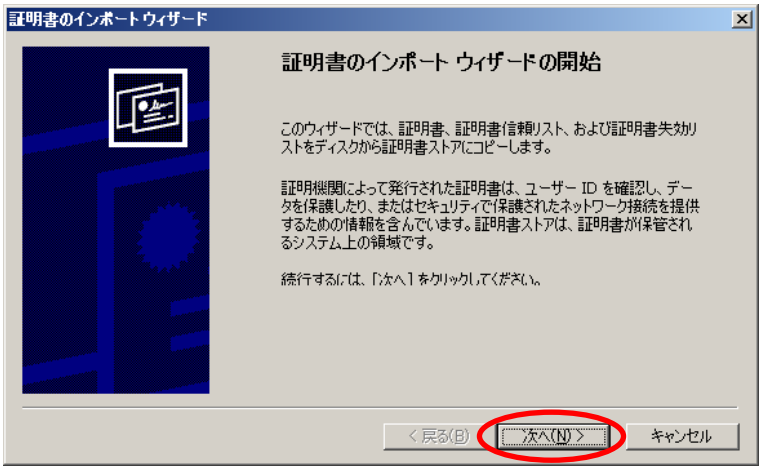
6.1 電子メール

6.1.1 Outlook 2007

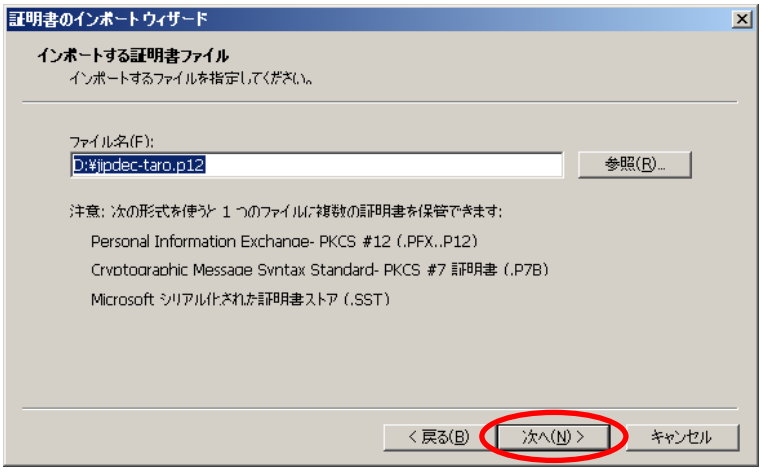
(1) 電子証明書のインストール方法

① 管理者から配布された証明書ファイルをダブルクリックし、「証明書のインポートウィザード」を開きます。

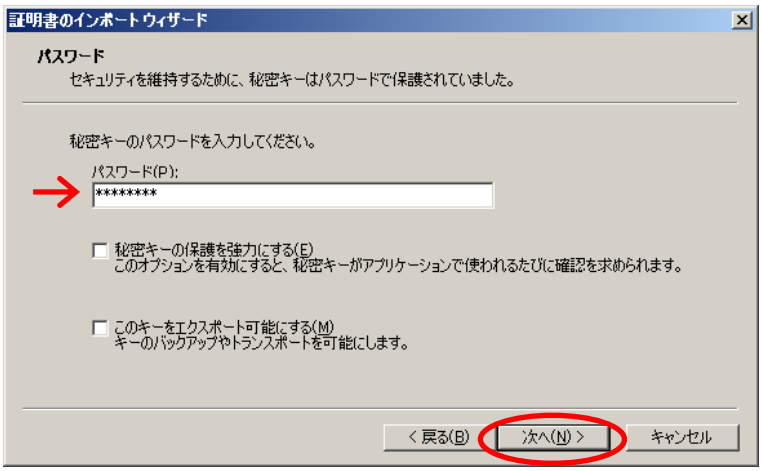
② そのまま「次へ」をクリックします。



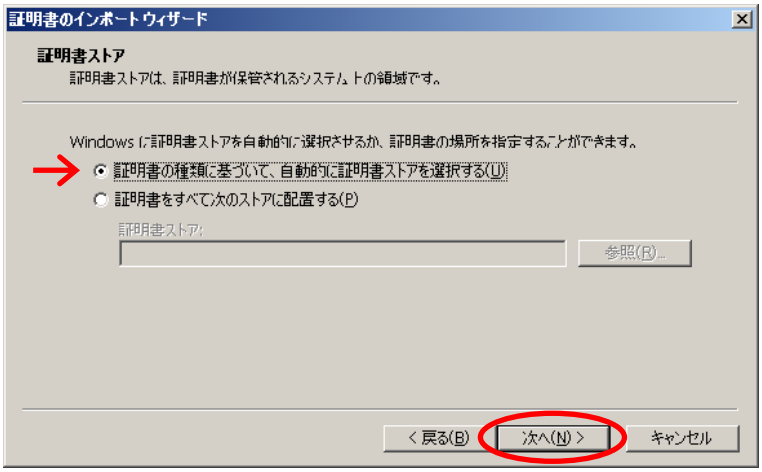
③ そのまま「次へ」をクリックします。



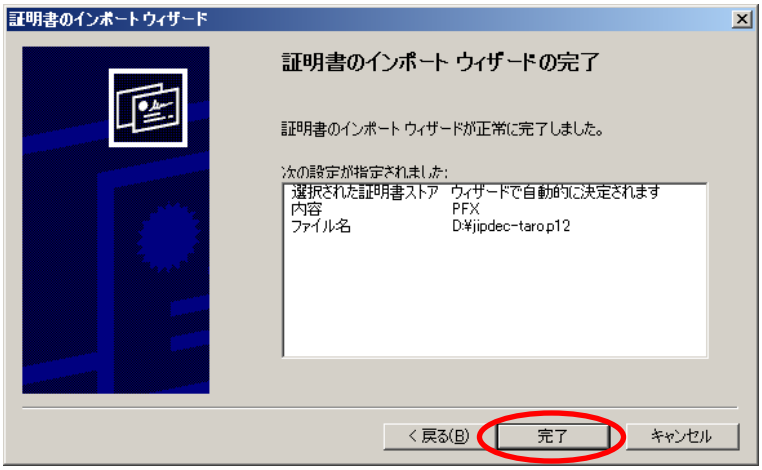
④　証明書ファイルと一緒に管理者から配布されたパスワードを入力し、「次へ」をクリックします。



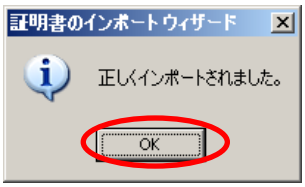
⑤　「証明書の種類に基づいて、自動的に証明書ストアを選択する」を選択し、「次へ」をクリックします。



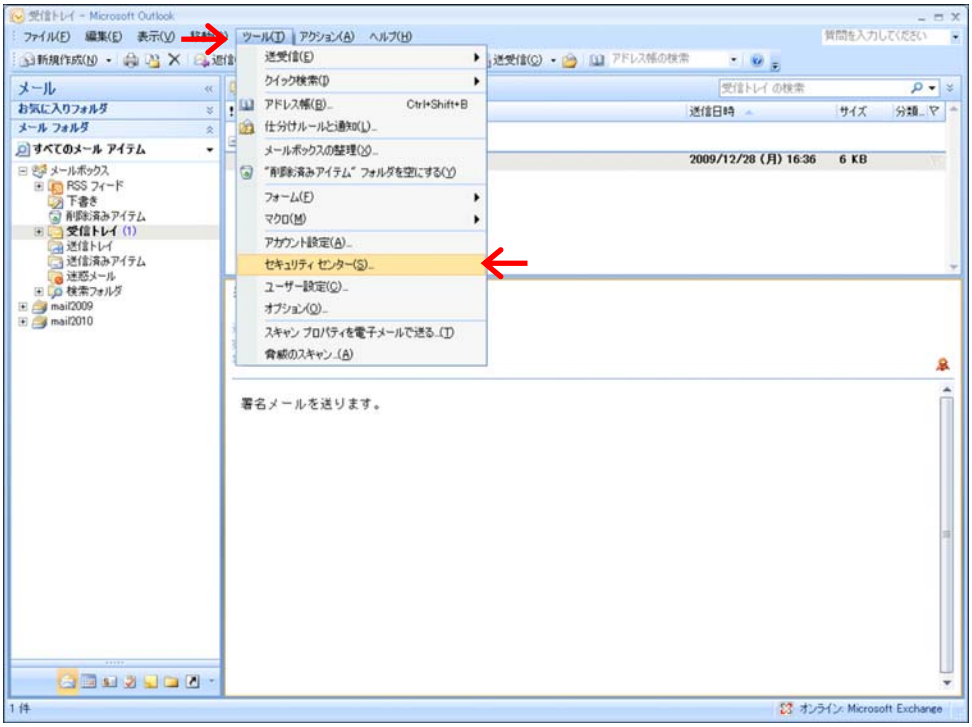
⑥　「完了」ボタンをクリックします。



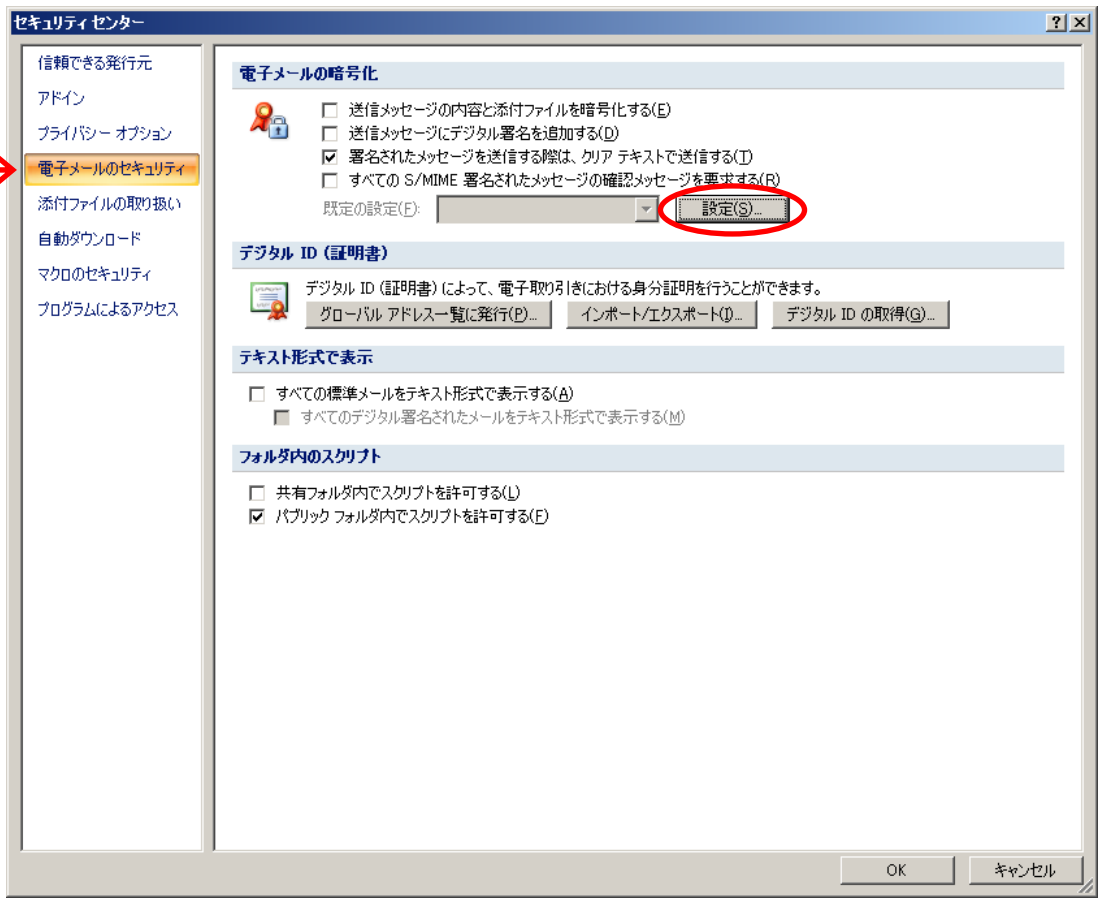
⑦　「正しくインポートされました」というメッセージが表示されたことを確認したら、「OK」ボタンをクリックして画面を閉じます。



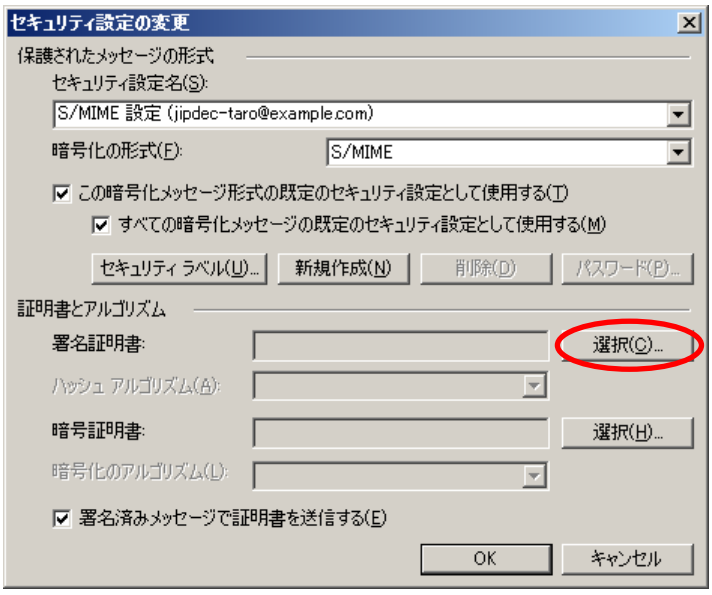
⑧　次に、Outlook 2007 の設定を行います。Outlook 2007 の上部メニューより「ツール」－「セキュリティセンター」を選択して「セキュリティセンター」画面を開きます。



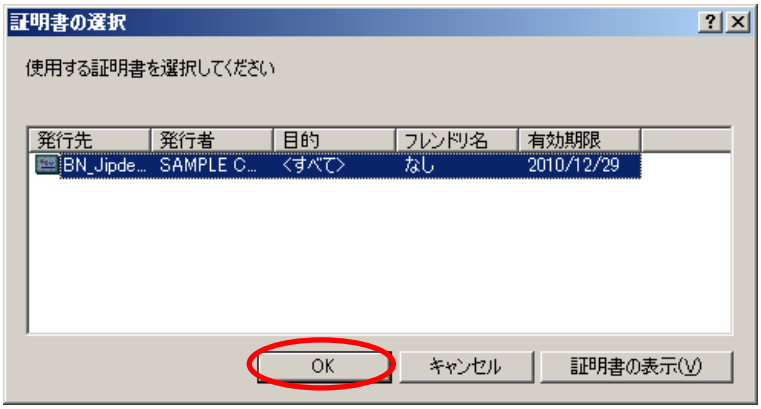
⑨　左のメニューで「電子メールのセキュリティ」を選択し「電子メールの暗号化」項目の中の「設定」ボタンをクリックします。



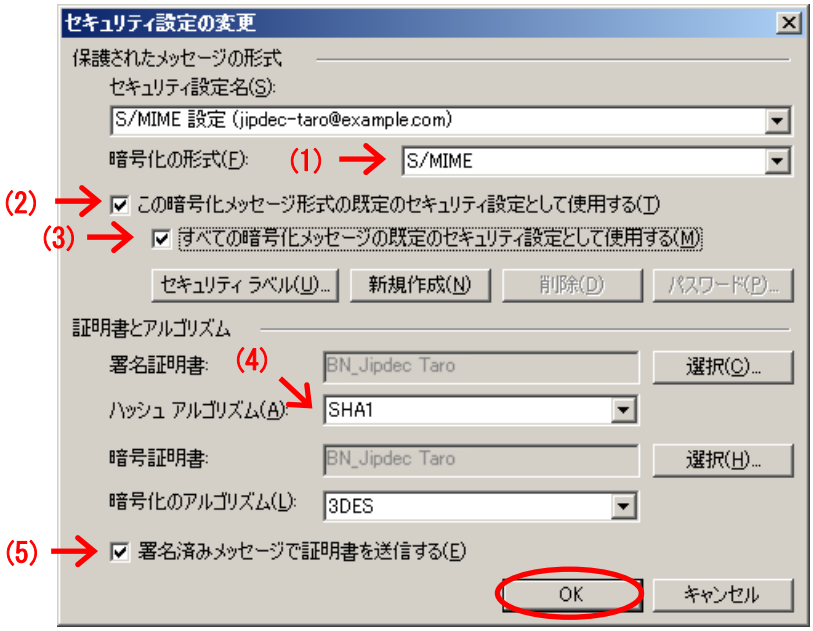
⑩　「署名証明書」欄にある「選択」ボタンをクリックします。



⑪　自分の証明書を選択し、「OK」ボタンをクリックします。

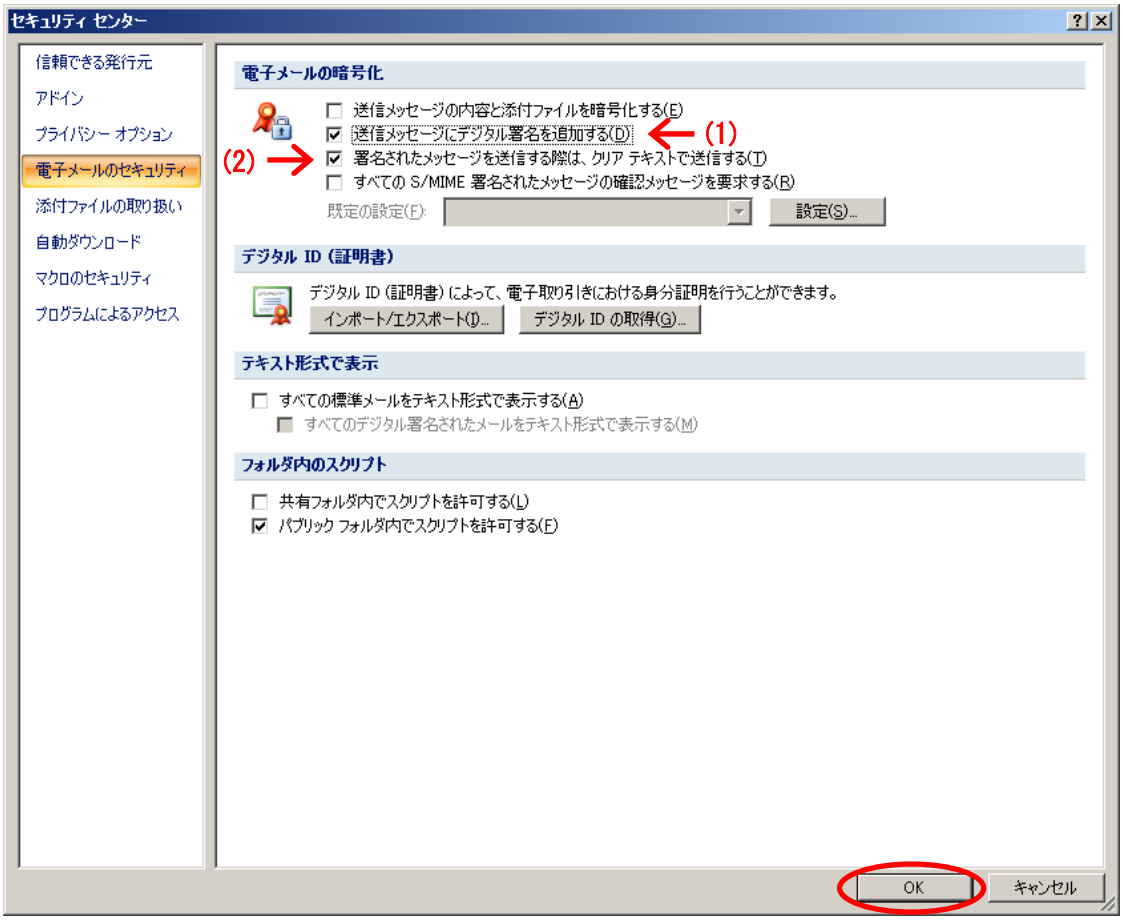


⑫　以下の通り選択し、「OK」ボタンをクリックします。



No.	項目	値
(1)	暗号化の形式	S/MIME
(2)	この暗号化メッセージ形式の既定のセキュリティ設定として使用する	チェック
(3)	すべての暗号化メッセージの既定のセキュリティ設定として使用する	チェック
(4)	ハッシュアルゴリズム	SHA1
(5)	署名済みメッセージで証明書を送信する	チェック

⑬　以下の通り選択し、「OK」ボタンをクリックします。

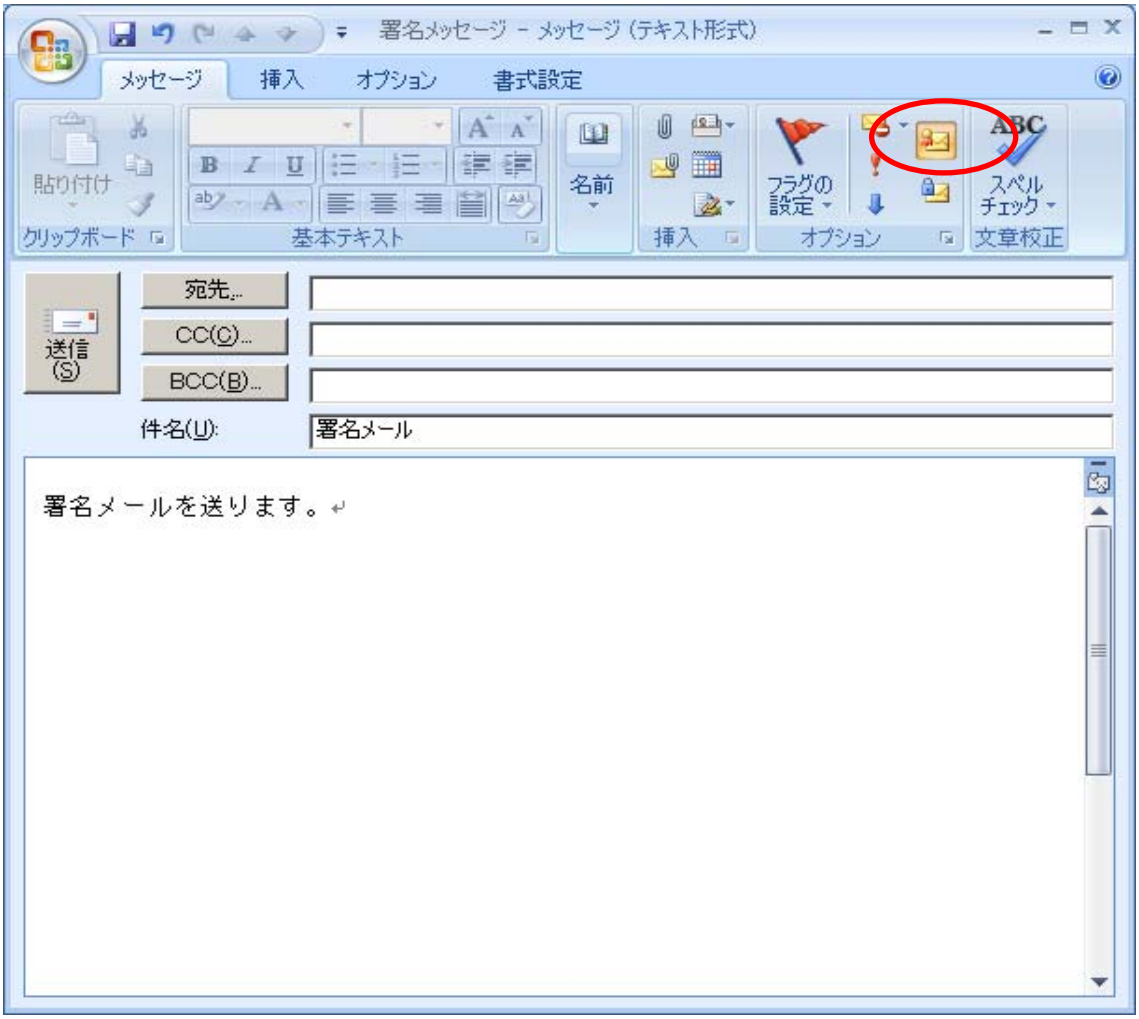


No.	項目	値
(1)	送信メッセージにデジタル署名を追加する	チェック
(2)	署名されたメッセージを送信する際は、クリアテキストで送信する	チェック

以上でインストール作業は終了です。

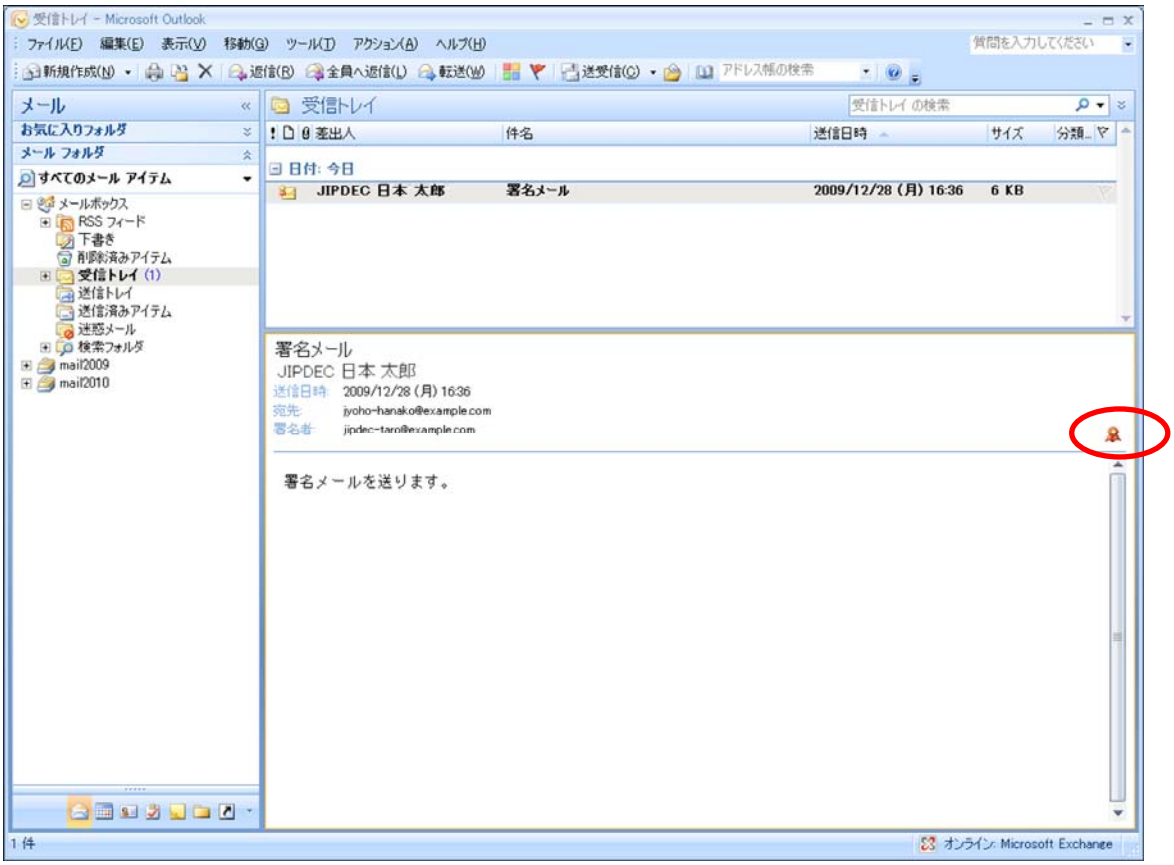
(2) 署名メールの送信方法

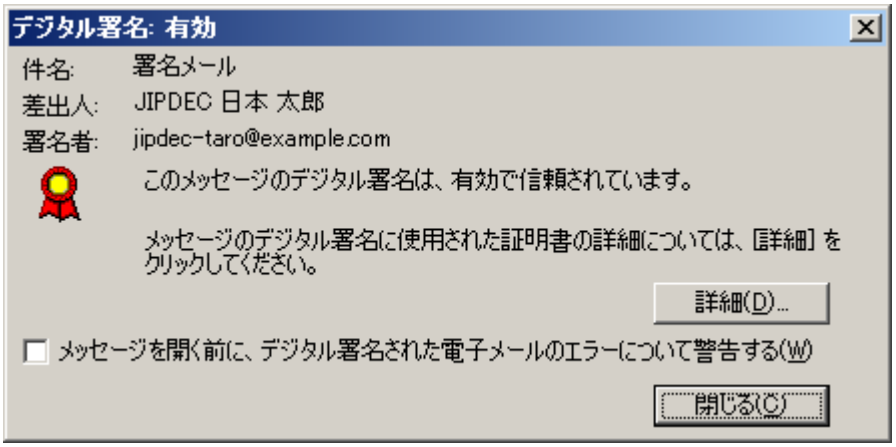
署名メールを送信する場合は枠で囲まれた部分にある署名のアイコンを選択します。



(3) 受信した署名メールの署名確認方法

受信メールの署名マークをクリックすることで署名確認ができます。





7. 委員会活動

7.1 ヒアリング活動

電子認証等の民間制度・基盤の確立に向けて、既存の認証局や利用企業、電子認証を用いたシステムベンダー、関係省庁等に、電子署名や電子認証における問題点の聞き込み、民間制度・基盤の説明や可能性の提言、要望等をヒアリング活動した。これらヒアリングは「電子認証等の民間制度・基盤の確立に関する委員会」の発足時や検討内容に大きく反映された。

以下にヒアリング活動を一覧で示す。

表 7-1 ヒアリング活動一覧

No.	日時	打合せ先	内　　容
1	2009/6/25 13:30～	・日本認証サービス(株)	ルート CA に関係する Web_Trust_forCA 監査について
	16:30～		上記を受けた内部打合せ
2	2009/7/2 13:00～15:00	・経済産業省 ・総務省 ・法務省	JIPDEC 民間認証制度の検討状況について
	2009/7/3 9:10～		上記を受けた内部打合せ
3	2009/7/2 16:10～	・アマノタイムビジネス(株)	JIPDEC 民間認証制度とアマノタイムビジネスとの連携について
	18:00～		上記を受けた内部打合せ
4	2009/7/6 13:30～15:40	・新日本監査法人 ・日本認証サービス(株)	JIPDEC 民間認証制度の検討状況について
	16:00～		上記を受けた内部打合せ
5	2009/7/7 13:30～15:30	・(株)帝国データバンク	JIPDEC 民間認証制度の検討状況について
6	2009/7/7 16:30～17:15	工学院大学	JIPDEC 民間認証制度の検討状況について
7	2009/7/9 14:00～15:30	・日本消費者金融協会 ・日本認証サービス(株)	CA ブラウザフォーラム、JCFA（日本電子認証協議会）との連携について
	15:30～		上記を受けた内部打合せ
8	2009/7/13 11:00～12:20	・ジャパンネット(株)	JIPDEC 民間認証制度の検討について
	13:30～		上記を受けた内部打合せ
9	2009/7/21 15:20～16:50	・東北インフォメーション・システムズ(株)	JIPDEC 民間認証制度の検討について
	17:15～		上記を受けた内部打合せ
10	2009/7/27 15:10～16:40	・シヤチハタ(株)	JIPDEC 民間認証制度の検討について
	17:00～		上記を受けた内部打合せ
11	2009/7/30 15:00～16:40	・三菱電機（株）情報技術総合研究所	JIPDEC 民間認証制度の検討について
12	2009/7/30 10:00～11:00	・セコム(株)	セコム ID カードサービスについて
13	2009/8/5 17:00～18:40	・大日本印刷(株)	JIPDEC 民間認証制度の検討について
14	2009/8/6 14:00～16:40	・(株)NTT データ	JIPDEC 民間認証制度の検討について

No.	日時	打合せ先	内　　容
15	2009/8/6 10:00～12:40	・国立情報学研究所	JIPDEC 民間認証制度の検討について
16	2009/8/7 17:00～19:00	・経済産業省	JIPDEC 民間認証制度の検討について
17	2009/8/17 11:00～12:00	・中電 CTI	JIPDEC 民間認証制度の検討について
18	2009/8/17 16:45～19:00	・(株)コスモラマ ・早稲田大学	JIPDEC 民間認証制度の検討について
19	2009/8/21 9:30～10:45	・(株)野村総合研究所	JIPDEC 民間認証制度の検討について
20	2009/8/25 16:00～18:30	・経済産業省	JIPDEC 民間認証制度の検討について
21	2009/8/27 13:30～14:45	・マイクロソフト(株)	Microsoft ルート証明書プログラムの登録について
22	2009/8/28 11:00～11:45	・アマノ(株)	JIPDEC 民間認証制度の検討について
23	2009/8/28 15:00～16:30	・内閣官房情報セキュリティセンター ・経済産業省 ・総務省	JIPDEC 民間認証制度の検討について
24	2009/9/1 16:35～17:30	・(株)オービック	JIPDEC 民間認証制度の検討について
25	2009/9/4 16:35～17:30	・GMO グローバルサイン(株)	JIPDEC 民間認証制度の検討について
26	2009/9/8 11:00～12:20	・日本ヒューレット・パッカード(株)	JIPDEC 民間認証制度の検討について
27	2009/9/9 11:00～12:20	・NTT 情報流通プラットフォーム研究所	JIPDEC 民間認証制度の検討について
28	2009/9/11 10:00～11:20	・日本 CA(株)	JIPDEC 民間認証制度の検討について
29	2009/9/15 17:00～19:30	・経済産業省	JIPDEC 民間認証制度の検討について
30	2009/9/25 13:00～14:05	・日本ベリサイン(株)	JIPDEC 民間認証制度の検討について
31	2009/9/25 15:00～16:30	・GMO グローバルサイン	JIPDEC 民間認証制度の検討について
32	2009/9/29 10:20～11:40	・東京工科大学	JIPDEC 民間認証制度の検討について
33	2009/9/30 16:00～17:10	・(株)イマーディオ	JIPDEC 民間認証制度の検討について
34	2009/10/1 10:20～11:45	・東京電機大学	JIPDEC 民間認証制度の検討について
35	2009/9/29 17:25～19:00	・(株)日立製作所	JIPDEC 民間認証制度の検討について
36	2009/10/16 10:00～11:30	・(株)コンストラクション・イーシー・ドットコム	JIPDEC 民間認証制度の検討について
37	2009/10/19 16:00～17:15	・(株)三菱総合研究所	11 月 24 日セミナー「市民と企業のための「安信簡」情報環境を目指して
38	2009/10/20 17:00～18:30	・日本商工会議所	JIPDEC 民間認証制度の検討について
39	2009/10/22 16:00～17:15	・日本電子認証(株)	JIPDEC 民間認証制度の検討について
40	2009/10/29 16:00～17:30	・経済産業省	JIPDEC 民間認証制度の検討について
41	2009/10/29 10:00～12:00	・セコム(株)	JIPDEC 民間認証制度の検討について

No.	日時	打合せ先	内　　容
42	2009/11/4 11:00～11:45	・弁護士　牧野	JIPDEC 民間認証制度の検討について
43	2009/11/25 16:00～18:30	・サイバートラスト(株)	JIPDEC 民間認証制度の検討について
44	2009/12/1 13:00～14:30	・セコムトラストシステムズ（株）	JIPDEC 民間認証制度の検討について
45	2009/12/2 16:10～18:30	・(社)日本ネットワークインフォメーションセンター ・日本ベリサイン(株) ・国立情報学研究所 ・セコム(株) ・NPO 日本ネットワークセキュリティ協会 ・日本電子認証協議会/クロストラスト(株) ・富士ゼロックス(株) ・筑波大学	JNSA　PKI 相互運用技術 WG
46	2009/12/9 13:45～14:30	・日本ベリサイン(株)	JCAN のルート認証局の運用について
47	2009/12/11 10:00～11:15	・経済産業省	「安信簡」情報環境プロジェクトについて
48	2009/12/16 16:00～16:45	・日本認証サービス(株)	JCAN プロジェクト実証実験について
49	2009/12/18 13:30～15:00	・アマノタイムビジネス(株)	JCAN プロジェクト実証実験等について
50	2009/12/18 10:30～12:00	・(株)イマーディオ	JCAN プロジェクト実証実験等について
51	2009/12/18 17:00～17:45	・日本商工会議所	JCAN プロジェクト実証実験等について
52	2009/12/18 17:00～18:30	・スマイルワークス(株) ・日本商工会議所	JCAN プロジェクト実証実験等について
53	2009/12/24 16:00～17:30	・経済産業省	JCAN 認証制度の検討について
54	2010/1/6 10:30～12:30	・(株)ミロク情報サービス	JCAN 証明書と会計ソフトとの関係
55	2010/1/6 14:30～16:30	・スマイルワークス(株)	JCAN 証明書と会計ソフトとの関係
56	2010/1/8 11:00～12:30	・日本ベリサイン(株)	JCAN の仕組みとニーズ、シーズについて
57	2010/1/18 15:20～17:30	・(株)NTT アプリエ ・NTT 情報流通プラットフォーム研究所 ・NTT(株)	JCAN の仕組みとニーズ、シーズについて
58	2010/1/20 18:30～19:30	・ネットワンシステムズ株式会社	電子認証の民間制度・基盤の確立に関するシンポジウム講演打合せ
59	2010/2/2 15:30～17:00	・東京工科大学	「安信簡」情報環境について
60	2010/2/16 10:00～12:00	・NTT コミュニケーションズ(株) ・NTT ソフトウェア(株)	JCAN プロジェクト実証実験について
61	2010/2/25 14:00～15:45	・(財)金融情報システムセンター	e-文書法に係る銀行業務での電子署名の利用について
62	2010/2/27 14:00～16:00	・BS 朝日 ・SOZOBUNKA bis	BS 朝日ヒアリング
63	2010/3/3 13:00～14:00	・NBS 研究所	JCAN の仕組みについて

No.	日時	打合せ先	内　　容
64	2010/3/4 16:00～17:00	・日経エレクトロニクス	日経エレ追加取材の件
65	2010/3/5 11:00～12:30	・経済産業省	「安信簡」情報環境の説明
66	2010/3/5 15:30～17:00	・(株)野村総合研究所	「安信簡」情報環境の説明

7.2 委員会活動

電子認証の民間制度・基盤の確立に向けた検討の場として、有識者、関係省庁、ベンダー等があつまる「電子認証等の民間制度・基盤にの確立に関する委員会」を立ち上げ、活動を行った。

(1) 委員会構成

「電子認証等の民間制度・基盤の確立に関する委員会」は、１つの委員会と３つの検討部会で構成されている。それぞれの活動内容は以下の通りである。

表 7-2 委員会構成

名称	活動内容
有識者委員会	・各作業部会からの報告もとに総合的な検討
ビジネスモデル検討部会	・ビジネスシーンの検討 ・マルチユース格納媒体の PKI 対応の検討 ・登録業務効率化の検討 ・プロモーション冊子の検討
ポリシー/基盤システム検討部会	・ポリシーの検討
評価基準検討部会	・民間認証局の調査表案の検討

(2) 委員会実施スケジュール及び内容

表 7-3 委員会構成

日程	時間	場所	委員会・検討部会 内容
2009 年 10 月 14 日(水)	16:00-18:00	JIPDEC 第 1 会議室	全体会議 ・委員長・主査・部会長、委員紹介 ・委員会設置について(目的、スケジュール)
2009 年 10 月 28 日(水)	13:00-15:00	JIPDEC 第 1 会議室	ビジネスモデル検討部会 ・プロモーション冊子について ・ビジネスシーン／マルチユース格納媒体等について
2009 年 11 月 10 日(火)	15:30-17:30	機械振興会館 6D-3	ポリシー／基盤システム検討部会 ・本制度の方向性 ・民間認証基盤の運用要件 ・WebTrust for CA と適合例のマッピング方式について
2009 年 11 月 11 日(水)	13:00-15:00	機械振興会館 B2-1	ビジネスモデル検討部会 ・プロモーション冊子の検討状況 ・ビジネスシーン/マルチユース格納媒体等の検討状況
2009 年 11 月 17 日(火)	10:00-12:00	機械振興会館 6-65	有識者委員会 ・作業部会活動概要 ビジネスモデル検討部会状況報告 ポリシー／基盤システム検討部会状況報告 ・公募結果と作業報告 プロモーション冊子 ビジネス・パスの検討状況 ルート/中間認証局の規程作業状況 ・評価基準検討部会活動予定
2009 年 12 月 9 日(水)	14:30-16:30	機械振興会館 B3-2	ビジネスモデル検討部会 ・プロモーション冊子の確定版の紹介 ・ビジネスシーン/マルチユース格納媒体等の検討状況

日程	時間	場所	委員会・検討部会 内容
2009 年 12 月 9 日(水)	17:00-18:30	機械振興会館 B3-2	評価基準検討部会 ・民間認証局の調査表案の検討 ・民間認証局の調査表に係る WebTrustforCA 認定基準と適合例等との比較検討状況 ・登録業務チェック項目の検討 ・申請手続きについて
2009 年 12 月 15 日(火)	10:00-12:00	JIPDEC 第 3 会議室	有識者委員会 ・作業部会活動概要 ビジネスモデル検討部会状況報告 評価基準検討部会状況報告 ポリシー／基盤システム検討部会活動予定 ・トピックス プロモーション冊子(確定版)及び JCAN 体制について JCAN 認証基盤に基づく模倣品対策における証明書プロファイルの ISO 化状況
2009 年 12 月 15 日(火)	13:00-15:00	JIPDEC 第 3 会議室	ポリシー／基盤システム検討部会 ・JCAN ルート CA/中間 CA のルール作成状況 ・JCAN ビジネス CP 証明書プロファイル案の検討
2010 年 1 月 18 日(月)	13:00-15:00	JIPDEC 第 3 会議室	ポリシー／基盤システム検討部会 ・JCAN ルート CA/中間 CA のルール作成状況 、JCAN ビジネス CP 証明書プロファイル案の検討 ・JCAN 体制の概要等について
2010 年 2 月 2 日(火)	10:00-12:00	JIPDEC 第 3 会議室	評価基準検討部会 ・民間認証局の調査表に係る WebTrustforCA 認定基準と適合例等との比較について ・その他 電子認証の民間制度・基盤の確立に関するシンポジウム 評価基準検討部会成果発表について 「JCAN」の取り組み
2010 年 2 月 2 日(火)	13:00-15:00	JIPDEC 第 3 会議室	ポリシー／基盤システム検討部会 ・JCAN センター事務取扱要領の内容 ARL/CRL が実際のフィールド上での動きについて 事業継続性に係るルート CA、中間 CA 以外のパートナ CA のベースラインとしての譲渡の扱い方 ・JCAN 電子証明書プロファイル案について CommonName のパターンの整理 ・その他 電子認証の民間制度・基盤の確立に関するシンポジウム ポリシー/基盤システム検討部会成果発表について 「JCAN」の取り組み
2010 年 2 月 10 日(水)	17:00-18:30	JIPDEC 第 3 会議室	有識者委員会 ・作業部会活動概要 評価基準検討部会状況報告 ポリシー／基盤システム検討部会状況報告 ・シンポジウム開催報告 ・「自社認証局の普及に関する調査」アンケート集計結果について ・次年度の活動予定

8. 広報活動

8.1 シンポジウムの実施

平成 22 年 2 月 4 日「電子認証の民間制度・基盤の確立に関するシンポジウム」を開催した。

本年度、平成 21 年 10 月より「電子認証等の民間制度・基盤の確立に関する委員会」を立ち上げ、さまざまな検討を行ってきた。

上記委員会での検討結果、活動報告をふまえて、電子認証や電子署名等に関わる民間制度･基盤の確立及びその環境整備の取り組みについて紹介した（詳しくは添付資料 G「シンポジウム実施報告」を参照のこと）

(1) プログラム

第 1 部：制度･基盤	
10:00-10:15	**電子認証等の民間制度・基盤**
1	講師：青木 尚（JIPDEC 電子商取引推進センター 主席研究員）
10:15-10:30	**ビジネスモデル検討部会**
2	講師：満塩 尚史（株式会社イマーディオ パートナ／環境省情報化統括責任者（CIO）補佐官／各府省 CIO 補佐官等連絡会議情報セキュリティ WG リーダー）
10:30-10:45	**ポリシー/基盤システム検討部会**
3	講師：手塚 悟（東京工科大学 コンピュータサイエンス学部 教授）
10:45-11:00	**評価基準検討部会**
4	講師：大木 栄二郎（工学院大学 情報学部情報デザイン科 教授）
11:00-11:05	**質疑応答**
11:10-12:00	**パネルディスカッション**
5	**テーマ：ポリシー（JCAN ビジネス CP）** 進　行：手塚 悟（東京工科大学 コンピュータサイエンス学部 教授） パネリスト：・佐々木 良一（東京電機大学未来学部 情報メディア学科教授） ・満塩 尚史（株式会社イマーディオ パートナ／環境省情報化統括責任者（CIO）補佐官／各府省 CIO 補佐官等連絡会議情報セキュリティ WG リーダー） ・阿藤 寿孝（アマノ株式会社 時間情報事業本部 副本部長） ・稲葉 厚志（GMO グローバルサイン株式会社 CA 戦略室 室長） ・岡部 寿男（京都大学学術情報メディアセンター ネットワーク研究部門 教授） ・西田 梢（シヤチハタ株式会社 IS 営業部開発課 主任） ・松永 隆司（東北インフォメーション・システムズ株式会社 法人ソリューション事業部 ソリューションサービスグループ副長） ・青木 尚（JIPDEC 電子商取引推進センター 主席研究員）
昼休憩（80 分）	
13:20-13:40	**ビジネスパス**
6	講師：福田 昭和（株式会社 HARTIN MARTIN 取締役）
13:40-13:45	**質疑応答**
第 2 部：海外動向	
13:50-14:30	**韓国における認証基盤について**
7	講師：Moon Sung-Eun《문성은》（Koscom Corporation《코스콤》, Team Manager）
14:30-15:10	**台湾における認証基盤について**
8	講師：Luke Lu《魯君禮》（National Information Infrastructure Enterprise Promotion Association《財團法人中華民國國家資訊基本建設產業發展協進會》, Information Risk Management Division《資訊風險管理組》Director）
15:10-15:40	**ドイツにおける認証基盤について**
9	講師：米丸 恒治（神戸大学大学院法学研究科 教授）
休憩（10 分）	

第 3 部：ビジネスシーン	
15:50-17:20　**パネルディスカッション**	
10	**テーマ：ビジネスモデル** 進　行：満塩 尚史（株式会社イマーディオ パートナ／環境省情報化統括責任者（CIO）補佐官／各府省 CIO 補佐官等連絡会議情報セキュリティ WG リーダー） パネリスト：・手塚 悟（東京工科大学コンピュータサイエンス学部 教授） ・中村 信次（株式会社日立製作所 公共システム事業部 公共ビジネス戦略室主任技師） ・福原 英之（ネットワンシステムズ株式会社 商品開発グループ　応用技術本部 DC プロダクト開発部 SaaS イネーブリングチーム 課長） ・米丸 恒治（神戸大学大学院法学研究科 教授） ・亀田 繁（JIPDEC 電子商取引推進センター 主席研究員）

(2) 申込者数及び参加数

Web による参加申込を行い、会場にて受付を行った。参加申込者数は 300 名を超え、当日は 200 名近くが参加した。

申込者：317 名

参加者：198 名（出席率 62%、当日参加 4 名）

(3) 講演資料

添付資料 F「シンポジウム講演資料」を参照。

(4) 広報活動

(a) Webによる開催案内・申込

当協会のホームページを利用した。

(b) ホームページへの掲載、メール広告

当協会のメーリングリスト、メールマガジン、ホームページ掲載に加えて、以下の一覧の組織へシンポジウムの参加案内、ホームページの掲載やメーリングリスト等での広報支援依頼を行った。

- 特定非営利活動法人 ITC-METRO
- アマノタイムビジネス株式会社
- 株式会社エス・エス・アイ・ジェイ
- 国立情報学研究所（NII）
- ｇコンテンツ流通推進協議会
- 社団法人電子情報技術産業協会
- システム監査学会（JSSA）
- 次世代 EDI 推進協議会（JEDIC）
- 次世代電子商取引推進協議会（ECOM）
- シヤチハタ株式会社
- 情報処理学会コンピュータセキュリティ研究会（CSES）
- 独立行政法人情報処理推進機構（IPA）
- 日本画像情報マネジメント協会（JIIMA）
- 社団法人日本経済団体連合会（経団連）

- 日本商工会議所
- 財団法人日本生産性本部情報化推進国民会議
- 日本セキュリティ監査協会（JASA）
- 日本セキュリティ・マネジメント学会（JSSM）
- 一般社団法人日本電子認証協議会
- 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）
- FeliCa 共通利用フォーマット推進フォーラム
- 有限会社ビジネス・サポートエム
- 株式会社日立製作所
- 牧野法律事務所
- UPKI イニシアティブ

(c) イベントカレンダーへの登録
- @IT イベントカレンダー
- scienceportal イベントカレンダー
- japan.internet.com　イベントカレンダー
- J-Net21　イベントカレンダー
- nikkeiBP events　イベントカレンダー

(5) アンケートの実施及び分析

シンポジウムの来訪者にアンケートを実施した。アンケート回答枚数は 108 枚であり、参加者 198 名からすると、回収率は 54.5%である。

(a) アンケート票

(b) 添付資料G「シンポジウム実施報告」を参照のこと

(c) アンケート分析

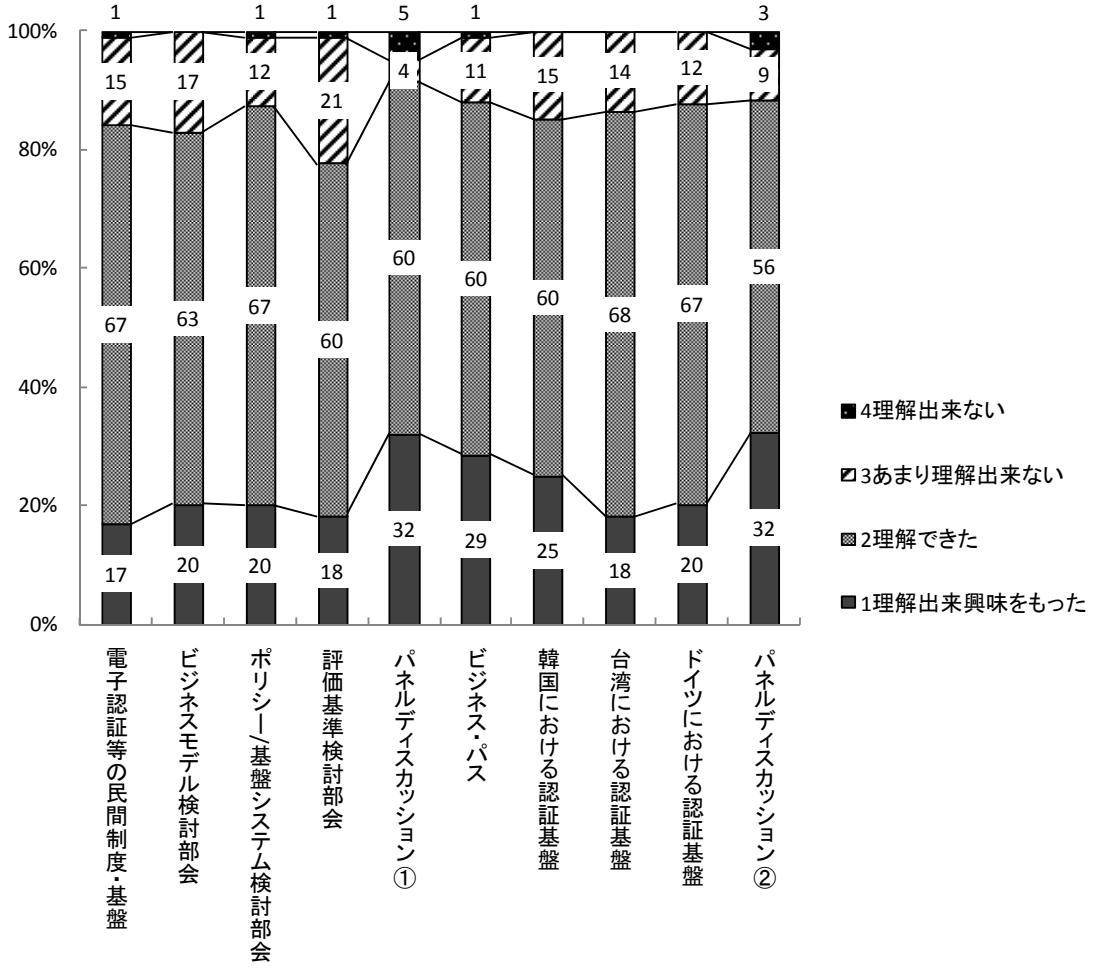
① シンポジウムの認知経路

シンポジウムを知るきっかけとなったのは主に当協会のホームページや案内メールであるが、その他のホームページや案内メールからという回答が全体の 3 割近く得られており、シンポジウム及び当事業への関心の高さが伺える。

項目	回答数
JIPDEC ホームページ	35
JIPDEC 案内メール	38
その他のホームページ	6
その他の案内メール	16
その他	16
無回答	3

② 理解と興味について

全ての講演について８割近くが「理解出来興味をもった」または「理解できた」との回答であった。



【評価】

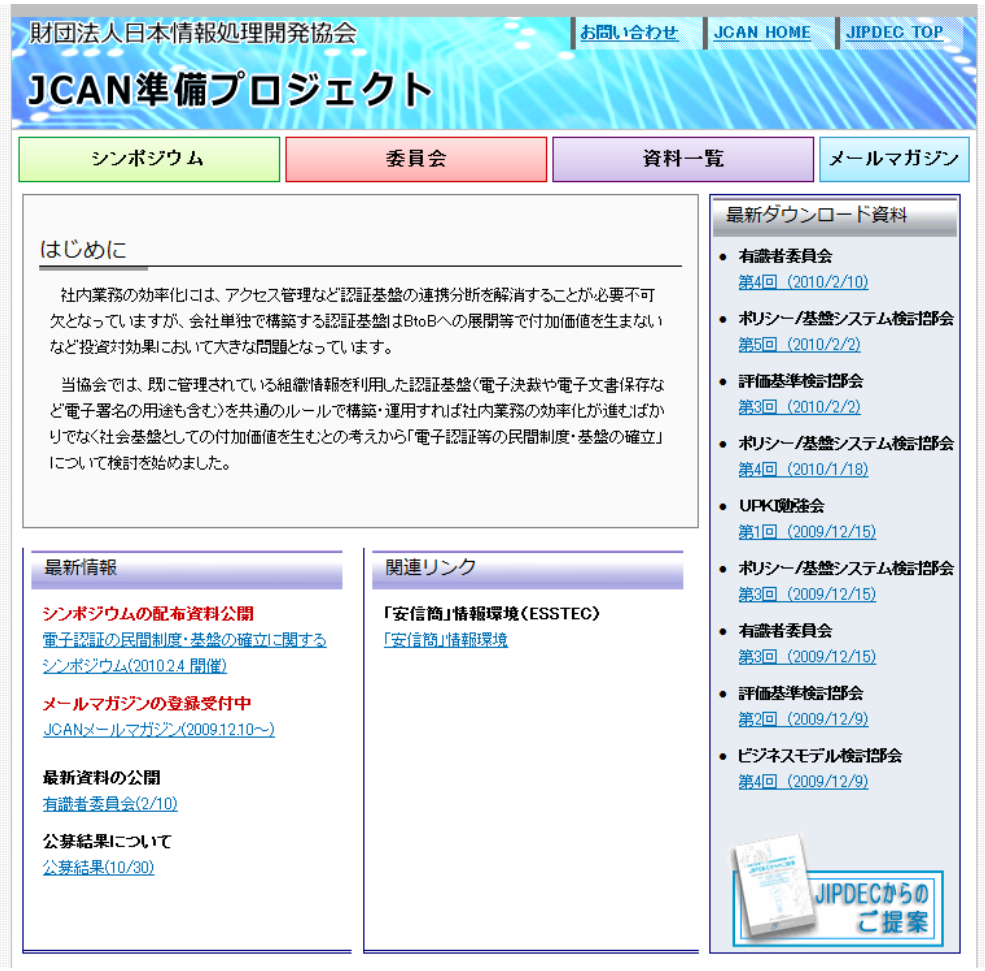
講演 / 項目	電子認証等の民間制度・基盤	ビジネスモデル検討部会	ポリシー/基盤システム検討部会	評価基準検討部会	パネルディスカッション ①
1 理解出来興味をもった	17.0%	20.2%	20.0%	18.1%	32.1%
2 理解できた	67.0%	62.8%	67.4%	59.6%	59.5%
3 あまり理解出来ない	14.9%	17.0%	11.6%	21.3%	3.6%
4 理解出来ない	1.1%	0%	1.1%	1.1%	4.8%

講演 / 項目	ビジネス・パス	韓国における認証基盤	台湾における認証基盤	ドイツにおける認証基盤	パネルディスカッション ②
1 理解出来興味をもった	28.6%	25.0%	18.2%	20.2%	32.4%
2 理解できた	59.5%	60.2%	68.2%	67.4%	55.9%
3 あまり理解出来ない	10.7%	14.8%	13.6%	12.4%	8.8%
4 理解出来ない	1.2%	0.0%	0.0%	0.0%	2.9%

8.2 Webコンテンツの作成

制度全体の認知拡大、委員会活動、シンポジウムの案内・参加申込を目的に、次の Web コンテンツの作成･公開を行った。

(1) トップページ



(2) アクセス数

月日	アクセス数
2009 年 10 月	13 アクセス
2009 年 11 月	1,653 アクセス
2009 年 12 月	3,798 アクセス
2010 年　1 月	6,361 アクセス
2010 年　2 月	5,687 アクセス
合計	17,512 アクセス

A「ビジネスシーンの検討」
B「マルチユース格納媒体の PKI 対応の検討」
C「登録業務効率化の検討」
D「プロモーション冊子」
E「3000 社アンケート結果」
F「シンポジウム講演資料」
G「シンポジウム実施報告」
H「ポリシーの検討」

A「ビジネスシーンの検討」

－ 目 次 －

※１：「PS 名」とは、Pseudonym（仮名・偽名・別名と訳されることがあるが自身が命名者である事を意味する適切な訳語が定まっていない）の略称である。

※２：PN は個人向け PS 名、BN はビジネス向け PS 名の略称である。

報告書概論

(1) 検討の実施内容

本検討では、仮名活用の検討として「安信簡情報環境」の検討を実施すると共に、これを活用したビジネスシーンの検討を実施した。

また、財団法人日本情報処理開発協会（JIPDEC）により立ち上げられた「電子認証等の民間制度・基盤の確立に関する委員会」において、ビジネスモデル検討部会や有識者委員会の対応を実施した。さらに、11/24 開催のセミナー「情報環境セミナー ～市民と企業のための「安信簡」情報環境構築を目指して～」の対応や、2/4 開催のシンポジウム「電子認証の民間制度・基盤の確立に関するシンポジウム」における本検討結果の報告を実施した。

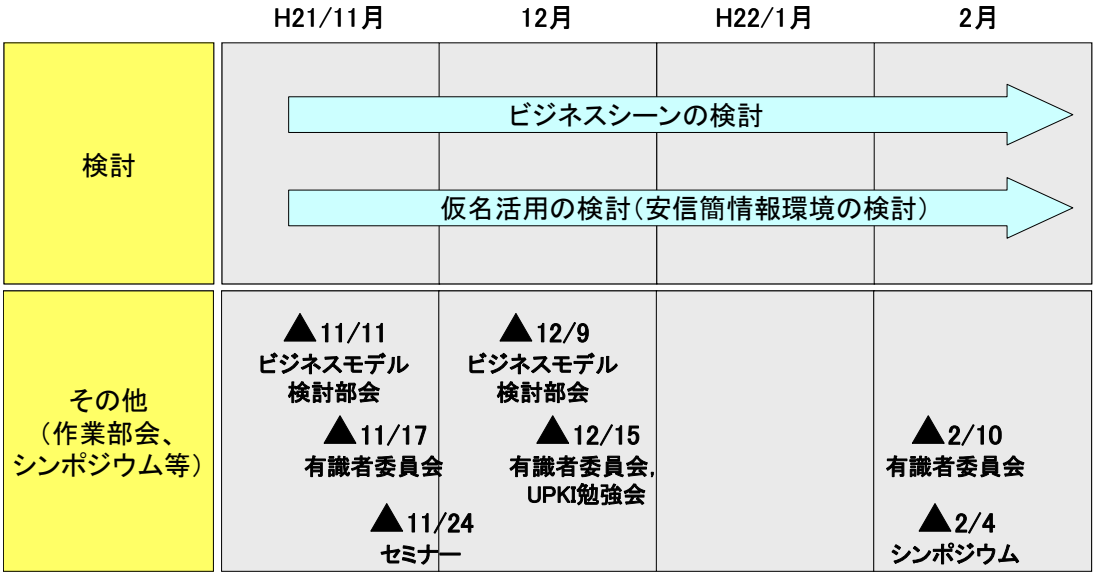


図 0-1　スケジュール

(2) 事業の目的

急速に発展するインターネット社会も、ビジネス活動環境としてみた場合、安心・安全面を裏打ちする社会的な環境の強化が求められている。情報化黎明期のおおらかさを残したインターネットの上で、適切な水準の安全性と信頼性を確保したビジネス活動環境を構築するためには、社会的なルールを伴った情報環境が必要であり、その整備が望まれている。また、そのような情報環境は、使いやすくストレスを感じさせないものでなければならない。

一方で、企業の人事情報や団体の登録情報等は、確実な本人確認／実在確認がなされており、また情報の更新もきちんとなされているものが多い。このような、最もフレッシュで信頼できる企業／団体に軸をおいた認証環境を実現し、さらにグローバルな仕組みと連携することができれば、安心・安全で使いやすい社会的環境を実現でき、情報経済社会の変革が可能となると考える。

本検討では、このような安心・安全な社会的環境「安信簡情報環境」の実現策を検討する。

また、「安信簡情報環境」を活用したビジネスシーンを示す事により、多様な利用場面で「安信簡情報環境」が活用できることを示す。

本検討における成果は、企業等の認証環境に係る新しい民間制度・基盤の実現に向けた、啓蒙や必要性の認知の向上、今後の検討の下地として利用・活用されることを期待するものである。

(3) 検討の概要

(a) 安信簡情報環境の構成要素

「安信簡」とは、安全・安心の「安」、信頼性の「信」、簡単・簡便の「簡」からなるもので、「安信簡情報環境」とは、これらを実現する社会的環境である。「安信簡情報環境」の構成要素は以下に示す４つから構成される。

① PS名情報環境

過剰な個人情報保護が、社会的な情報連係の阻害要因となっている。「PS 名情報環境」とは、確実な本人確認を前提とした PS 名（Pseudonym（シュードニム）の略称。なお、シュードニムは、偽名・仮名・別名と訳されることがあるが自身が命名者である事を意味する適切な訳語が定まっていない）を導入し、個人情報に配慮できる情報環境を実現するものである。

なお、本検討では、PS 名を更に名刺のようにビジネスの場で広く公開されて利用されるもの（以下「BN」（Business Name））と、個人が私的に利用するもの（以下「PN」（Personal Name））に分けて検討した。

② 認証環境「JCAN」

認証環境の分断も、社会的な情報連携の阻害要因となっている。認証環境「JCAN」とは、共通のルールと認定制度に基づく認証環境で、組織が組織に属していることを組織の外に証明できる情報環境を実現するものである。

③ 企業ID連携環境

様々な企業 ID の乱立も、社会的な情報連携の阻害要因となっている。「企業 ID 連携環境」とは、これら複数の企業 ID を紐付け、企業の信用情報をより確かにできる情報環境を実現するものである。

④ 双方向情報交換環境

上記(1)～(3)の環境を利用し、「セキュアな情報交換環境」等を実現するものである。

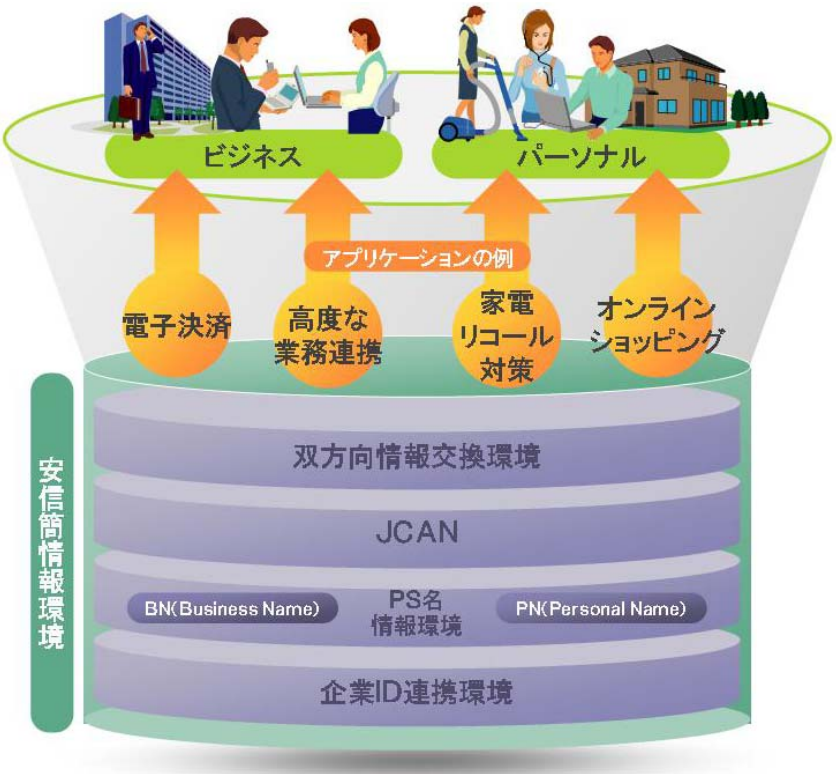


図 0-2　安信簡情報環境の構成要素

(b) ビジネスシーンの検討

「安信簡情報環境」を活用したビジネスシーンを、BN の電子証明書を活用した場合のビジネスシーンと、PN の電子証明書を活用した場合に分けて、ビジネスシーンを検討した。

① BNを活用したビジネスシーン

- 署名メール
- 電子決裁
- 電子投票
- 模倣品対策

② PNを活用したビジネスシーン

- 転職
- オンラインショッピング
- 家電リコール

下図に、BN を活用したビジネスシーン「署名メール」と、PN を活用したビジネスシーン「オンラインショッピング」のイメージを示す。

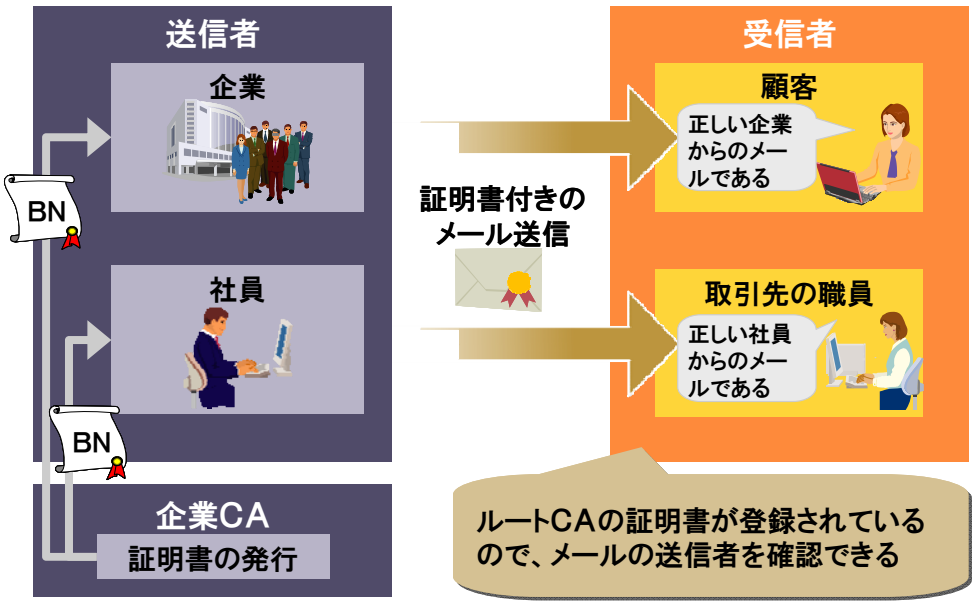


図 0-3　署名付きメール

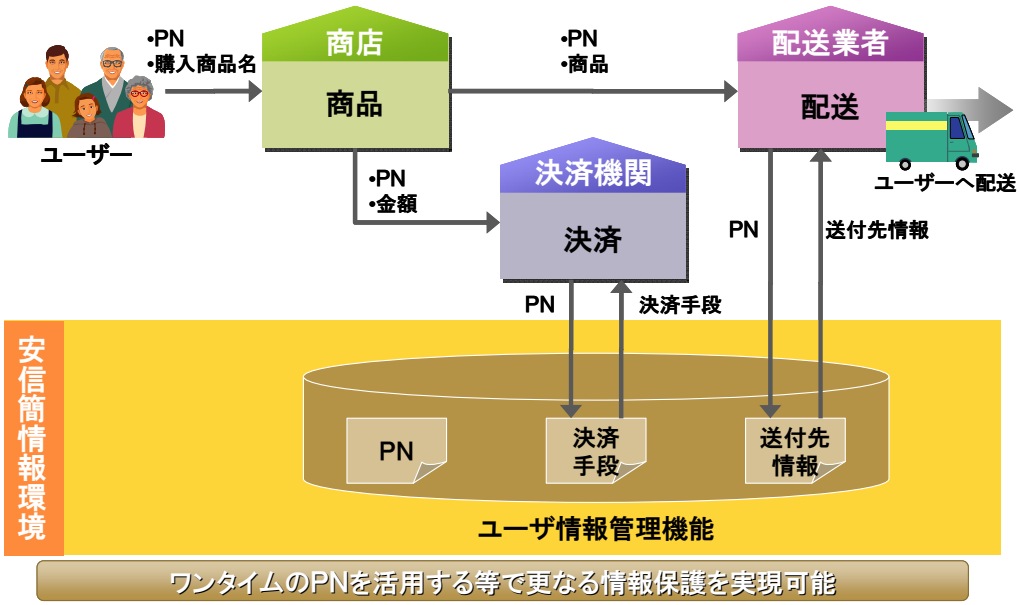


図 0-4　オンラインショッピング

(c) まとめ

① 本検討の成果

本検討では、安心・安全な社会環境である「安信簡情報環境」について検討を行い、その構成要素の一つである PS 名について、BN と、PN に分けて、それぞれを整理した。また、これら BN や PN を活用した利用シーンをそれぞれ例示し、様々なビジネスシー

ンにおいて BN や PN をはじめとする「安信簡情報環境」が活用できることを示すことができた。

② 今後に向けて

これら BN、PN の仕組みと、情報を交換させる環境が共通のルールと認定制度に基づいて推進されると、社会的な情報連関の活性化に貢献するものと考える。プロセスとしては、BN が普及することで、企業活動における PKI の高度利用が促進され、同時に BN を信頼の基点とした PN の仕組みを導入することにより、社員の立場を離れた個人の活動に対しても、広く利用できるものになると考える。

1. 安信簡情報環境の構成要素

「安信簡」とは、安全・安心の「安」、信頼性の「信」、簡単・簡便の「簡」からなるもので、「安信簡情報環境」とは、これらを実現する社会的環境である。「安信簡情報環境」の構成要素は以下に示す４つから構成される。また、これらの 4 つの構成要素について、その概要や論点を 1.1～1.4 節で説明する。

(1) PS名情報環境

過剰な個人情報保護が、社会的な情報連関の阻害要因となっている。「PS 名情報環境」とは、確実な本人確認を前提とした PS 名（Pseudonym（シュードニム）の略称。なお、シュードニムは、偽名･仮名･別名と訳されることがあるが自身が命名者であることを意味する適切な訳語が定まっていない）を導入し、個人情報に配慮できる情報環境を実現するものである。

なお、本検討では、PS 名を更に名刺のようにビジネスの場で広く公開されて利用されるもの(以下「BN」(Business Name))と個人が私的に利用するもの(以下「PN」(Personal Name))に分けて検討した。

(2) 認証環境「JCAN」

認証環境の分断も、社会的な情報連関の阻害要因となっている。認証環境「JCAN(Japan CA Network)」とは、共通のルールと認定制度に基づく認証環境で、組織が組織に属していることを組織の外に証明できる情報環境を実現するものである。

(3) 企業ID連携環境

様々な企業 ID の乱立も、社会的な情報連関の阻害要因となっている。「企業 ID 連携環境」とは、これら複数の企業 ID を紐付け、企業の信用情報をより確かにできる情報環境を実現するものである。

(4) 双方向情報交換環境

上記(1)～(3)の環境を利用し、「セキュアな情報交換環境」等を実現するものである。

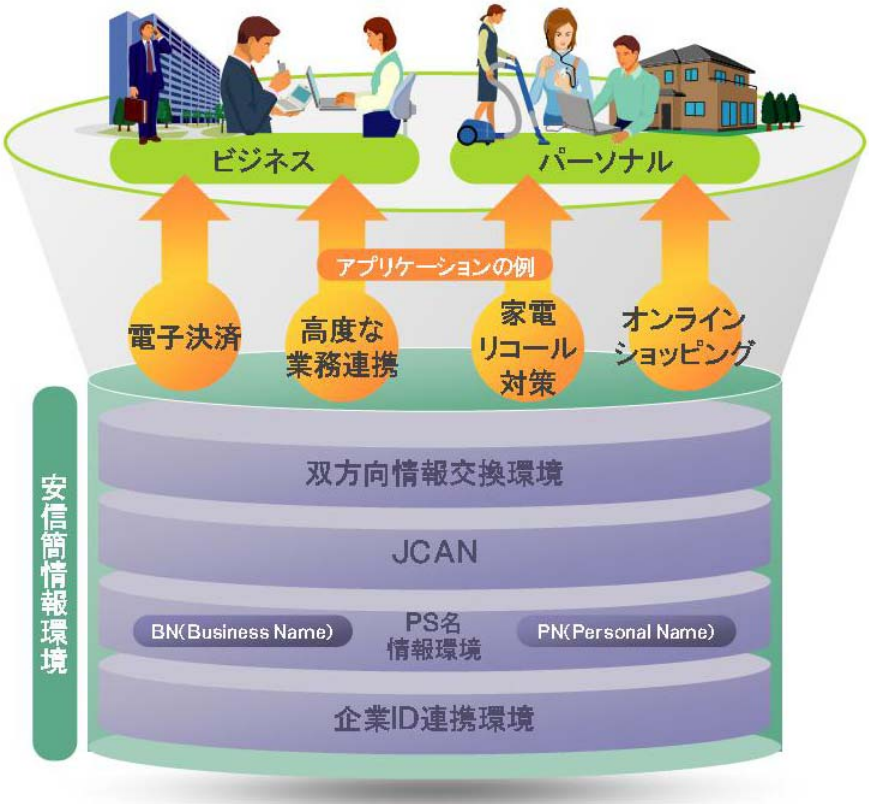


図 1-1　安信簡情報環境の構成要素

1.1 PS名情報環境

PS 名には、名刺のようにビジネスの場で広く公開されて利用される「BN（Business Name）」と、個人が私的に利用する「PN（Personal Name）」が存在する。これらの特徴を 1.1.1 節で示す。また、これを踏まえて、PS 名情報環境における主な論点を 1.1.2 説に記述する。

1.1.1 PS名の分類

BN と PN の特徴を、下図に示す。

BN は、名刺のようにビジネスの場で利用されるものであるため、広く公開して利用するのに対し、PN は個人が私的な場で利用するため、個人を特定する情報は含まないという特徴がある。

これら BN や PN は、次節で説明する JCAN における電子証明書の subject に記載されることを想定している。

		PS名	
		BN(Business Name)	PN(Personal Name)
1	目的	社会的にビジネス活動する為に広く公開して利用	個人がネット上のIDとして活用
2	表記内容 (証明書記載情報)	実名、旧姓、芸名、ペンネーム等	意味の無いID、自身が決めたニックネーム等(一意に識別可能なもの)
3	発行の由来	会社への所属	BNを所有していること等
4	主な利用シーン	BtoB、C、G	CtoC、B
5	同類の仕組み	名刺、メールのシグネチャ等	ドイツ市民ポータルのPseudonym
6	情報保護の考え方	氏名等は含まれるが、半ば公開され、流通可能と想定	個人情報を含まない
7	PS名の変更	人事異動や転職等で再発行(変更)となる	利用者が希望しなければ変更にならない

図 1-2　PS 名の分類

1.1.2 PS名情報環境における主な論点

PS 名情報環境における主な論点を以下に記述する。

(1) 個人情報保護法の対象となる情報について

・BNは実名等が含まれるため、現状個人情報保護法の対象となるが、この利用目的の性質上、個人情報保護法の対象外とすべきではないか。

・PNは個人情報を含まない番号等であるため、個人情報保護の対象外としても良いのではないか。

(2) 複数PS名の紐付けについて

(a) 同時に複数存在するPS名の紐付け

複数の企業や団体が 1 人のユーザに対して、PN や BN を発行する場合がありうる。これらは互いに紐付けされることにより、情報の連携を可能とし、サービス提供者側の高効率化や、利用者に対する利便性向上につながるのではないか。

(b) 過去と現在のPS名の紐付け

例えば転職などにより BN が変更になった場合に、過去の BN と現在の BN を紐付ける事

により、継続的に個人を識別することができる。転職のユースケースにおいては、どの企業にも属さない期間は BN が発行されない期間がありえる。このため、例えば PN を基点にして、過去の BN と現在の BN を紐付けることが考えられる。

(3) PS名の紐付け方法について

(2)で述べたような PS 名の紐付け方法として、例えば以下のような方法が考えられる。

(a) アプリケーションにおいて複数PS名の対応付けを行う

- アプリに対して、利用者が対応付けを登録する
- アプリ側で管理している属性情報から、アプリが PS 名の紐付けを行う

(b) 紐付けを行う環境を設ける

- 環境に対して、利用者が対応付けを登録する
- BN 証明書の拡張項目等に紐付け情報を記載する

(4) PNの匿名性について

PN は匿名性を高めるのに有効な環境となり得るものである。しかしながら、PN を個人情報と共にアプリに登録したり、PN と BN を紐付けて利用する場合、PN の匿名性は保てなくなってしまう。このため、PN を匿名のために利用する場合には、限られた範囲で利用するなど、考慮する必要がある。

[匿名性が保たれない場合の例]

- 商品送付先を登録する必要があるような、オンラインショップ等において PN を利用する場合、PN と商品送付先が紐付いてしまい、匿名性が損なわれる。
- BN には個人の氏名等が含まれる場合も想定されるため、PN と BN が紐付いている場合、PN に対する氏名がわかってしまう。

(5) PNの記述形態

PN の記述形態として、以下のようなものがありうる。

(a) 永続的に利用するもの

① ニックネームのような、ユーザが覚えやすいもの

② 機械的で意味の無いもの

(b) 一過性のもの（ワンタイムで利用するID）

1.1.3 プライバシに関する要件

PN は匿名性を高め、プライバシを守るのに有効な環境となり得るものである。ここでは、プライバシに関する要件について整理する。

(1) プライバシに対する要件の分類

※ドレスデン大学「PRIVACY AND DATA SECURITY」を参照して記載

(a) 匿名性（Anonymity）

・ある者が一意に識別されない状態

・利用者が自身を識別可能にする身元情報を開示せず（あるいは開示されず）情報やサービスの使用ができることを保証する

(b) 仮名（Pseudonymity）

・利用者が自身を一意に識別可能にする身元情報を公表する（あるいは公表される）ことなしに情報やサービスを利用できる

・その利用に対して責任があることを保証する

・リンク不能性を伴わない弱い匿名性といえる

(c) リンク不能性（Unlinkability）

・複数の情報をリンクすることができない状態

・複数の情報やサービスを利用した場合に、第三者がそれらの利用の相互の関連性を見出せないこと

(2) プライバシに対する脅威の種類

※JNSA「2008年情報セキュリティインシデントに関する調査報告書 Ver.1.3」(2009.11.4)を参照して記載

(a) 経済的損失

クレジット番号をオンラインショッピングサイトへ入力し、悪用されるなど。

[対策例]

楽天におけるオンラインショップサービス（クレジット番号は店へ渡さない）

(b) 精神的苦痛

個人の趣味や嗜好が漏洩し、差別等に利用されるなど。

[対策例]

mixi 年賀状サービス、ソフトバンクメルアド宅配便サービス（個人の氏名、住所を相手に渡さない）

1.2 認証環境「JCAN」

JCAN は、企業の認証局（CA：Certification Authority）がその社員等に対して電子証明書を発行するものである。まず、1.2.1 で JCAN の基本的な仕組みについて説明し、1.2.2 節で JCAN における証明書ポリシ（CP：Certificate Policies）の構成について説明する。

1.2.1 JCANの基本的な仕組み

JCAN は、JCAN センターが運用する「パブリックルート CA」が、各企業や団体が運営する認証局に対して電子証明書を発行し、これら企業 CA／団体 CA が社員や団体会員に対して電子証明書を発行することを基本とする。

パブリックルート CA は、WebTrust 認定という第三者にいよる信頼の裏づけがされており、このパブリックルート CA の証明書がブラウザ等の「信頼されたルート認証機関」に登録される。これにより、異なる企業や団体間での連携が簡単で低コストに実現できる。

企業／団体 CA は、各組織が管理する人事情報等を元に、社員や団体会員の登録業務を行い、BN を記載した電子証明書を発行する。

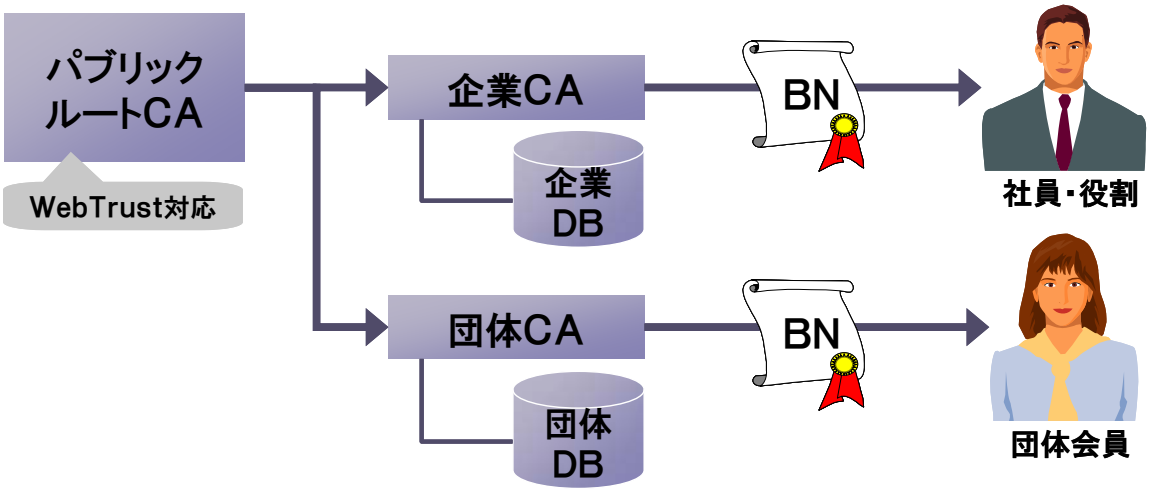


図 1-3 JCAN の基本的な仕組み

1.2.2 証明書ポリシ（CP）の構成

JCAN が提供する電子証明書には主に 2 種類あり、それぞれ異なる証明書ポリシ（CP）となる。これら CP の構成を、下図に示す。

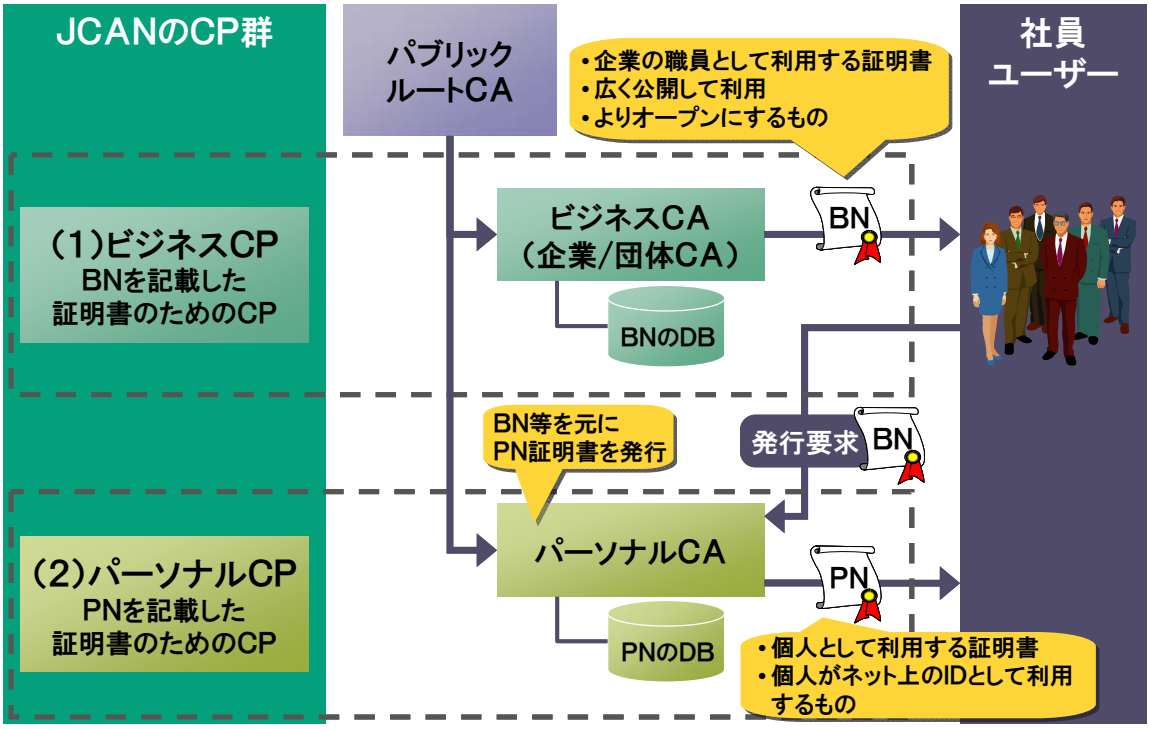


図 1-4 CP の構成

(1) ビジネスCP

BN を記載した証明書の為の CP。ビジネス CP の電子証明書は、企業の職員として利用する証明書であり、広く公開して利用するものである。ビジネス CP の電子証明書を発行する認証局を「ビジネス CA」と呼び、基本的には各企業がビジネス CA を運営する。

また、ビジネス CA は、ユーザ（社員）が企業に属していることに基づき、電子証明書を発行する。

(2) パーソナルCP

PN を記載した証明書の為の CP。パーソナル CP の電子証明書は、個人がネット上の ID として利用するものである。パーソナル CP の電子証明書を発行する認証局を「パーソナル CA」と呼び、パーソナル CA をどのような組織が運営するかは今後検討が必要である。

また、パーソナル CA は、ユーザが BN を所持していることに基づき、電子証明書を発行する。すなわち、企業において厳格な本人確認を実施していることに基づき電子証明書を発行する。

1.3 企業ID連携環境

企業 ID 連携環境（略称「企業 ID リファレンサ」）は、複数の企業 ID を紐付け、その情報を提供するものである。まず 1.3.1 節で企業 ID 連携環境の概要について説明し、1.3.2 節で企業 ID 連携環境における主な論点を記述する。

1.3.1 企業ID連携環境の概要

企業 ID 連携環境は、電子証明書に記載された様々な種類の企業 ID から、企業の情報を提供するものである。具体的には、以下 2 つの機能を提供する。

(1) ユーザに対して法人登記情報等を画面に出力する（人間に対するサービス）

(2) サーバ等に対して、ある企業IDから別の種類の企業IDを提供する（機械的なサービス）

図 1-5 企業 ID リファレンサの概要

1.3.2 企業ID連携環境における主な論点

企業 ID 連携環境における主な論点を以下に記述する。

(1) 企業が統廃合した場合の継承関係について

企業の名称が変更したり、複数企業が一つの企業に合併する場合、企業 ID が変更になる可能性がある。このような場合において、過去の企業 ID と現在の企業 ID の関係がわかれば、様々な用途に活用できる可能性がある。

しかしながら、個人や物の ID と異なり、一つの企業が複数に分かれたり、複数の企業が一つに統合されるという特徴があるため、企業 ID の継承関係の管理方法には課題が多い。

(2) 確認可能な企業IDの範囲について

現状、多数の組織やサービス毎に企業 ID を発行しているため、一企業に対して数多くの ID が発行されている。企業 ID リファレンサにより企業 ID の変換を行うには、企業 ID を管理する組織同士が連携する必要があるため、全ての企業 ID をサポートするまでには時間がかかる。

このため、まずはニーズの大きい主要な企業 ID について連携を行い、対応情報を提供することが考えられる。例えば、まずは ISO6523 に登録されている組織の ID を対象にすることが考えられる。

1.4 双方向情報交換環境

1.1～1.3 の環境を利用し、「セキュアな情報交換環境」等を実現する環境が必要となる。1.4.1 節では、このような環境の概要を説明し、1.4.2 節ではその論点を記述する。

1.4.1 双方向情報交換環境の概要

PS 名情報環境、JCAN、企業 ID リファレンサを活用し、「セキュアな情報交換環境」を実現する。具体的には、個人（社員）の属性情報をセキュアに管理、閲覧できる機能や、長期保存を可能にする機能が必要となる。また、これらの情報にアクセス可能な者（個人、企業）を適切に管理するアクセスコントロール機能が必要となる。

企業等は、この環境を利用して様々なアプリケーションを実現することができる。また、ユーザは JCAN にて発行された電子証明書を使い、これらのアプリケーションを安全・安心に利用することができる。

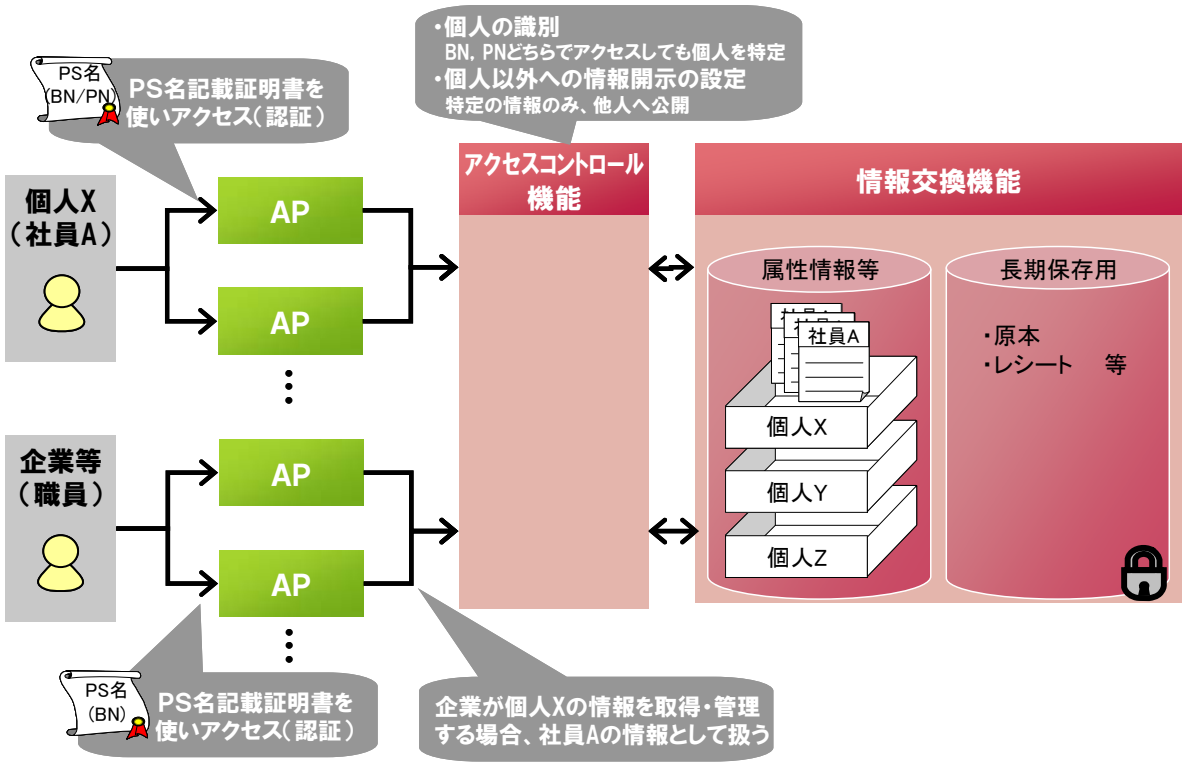


図 1-6 双方向情報交換環境

1.4.2 双方向情報交換環境における主な論点

双方向情報交換環境における主な論点を以下に記述する。

(1) 個人の情報を企業間で受け渡しする方法について

個人の情報を企業間で受け渡しする場合、以下の考え方がありえる。民間企業間でのやり取りの場合、「私書箱型」がよりマッチすると思われる。

(a) 私書箱型

個人を介して情報を受け渡しする。個人の了承を得て他機関へ情報を提供する。

(b) バックオフィス連携型

企業間で直接情報を受け渡しする。個人の了承は契約等で得る。

(2) 個人から企業への情報提供する場合の考え方について

個人から企業へ情報を提供する場合、以下 2 パターンの考え方がありえる。

(a) 個人の棚から企業の棚へ、情報を送付する

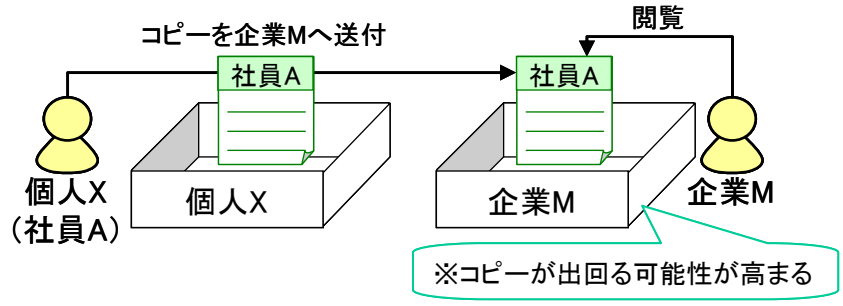


図 1-7 個人の棚から企業の棚へ情報を送付するパターン

(b) 個人の棚を企業が閲覧する

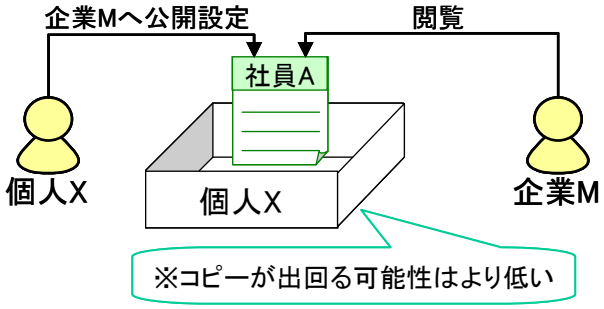


図 1-8 個人の棚を企業が閲覧するパターン

(3) PNと情報交換環境の関係について

PN が 1 つのみ取得可能な場合と、同時に複数取得可能な場合とで、情報交換環境における状態が異なる。それぞれのパターンを、以下に図示する。

(a) PNは 1 つのみ取得可能

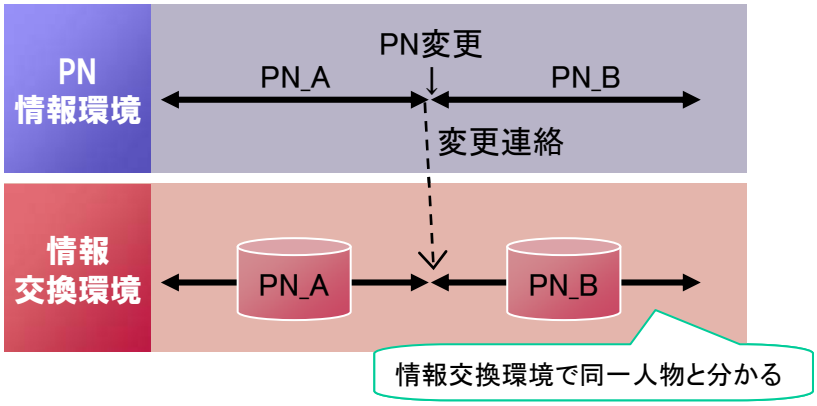


図 1-9 PN が 1 つのみ取得可能な場合

(b) PNは同時に複数取得可能

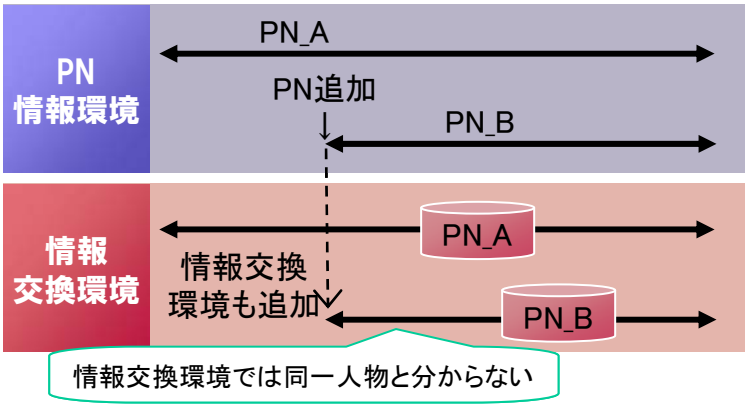


図 1-10 PN が同時に複数取得可能な場合

2. ビジネスシーンの検討

2 章で検討した「安信簡情報環境」を活用したビジネスシーンを検討した。本章では、BN の電子証明書を活用した場合のビジネスシーンと、PN の電子証明書を活用した場合のビジネスシーンに分けて、それぞれビジネスシーンを検討した。

(1) BNを活用したビジネスシーン

(a) 署名メール

(b) 電子決済

(c) 電子投票

(d) 模倣品対策

(2) PNを活用したビジネスシーン

(a) 転職

(b) オンラインショッピング

(c) 家電リコール

各ビジネスシーンの具体的な実現イメージを、それぞれ次節以降で記述する。

2.1 BNを活用したビジネスシーン

2.1.1 署名付きメール

異なる企業の社員同士でやり取りされるメールや、企業から顧客に対して送付するメールに対して、JCAN の BN 証明書を活用して電子署名を付与する。これにより、取引先の職員は、確かに正しい社員からのメールである事を確認でき、また顧客は正しい企業からのメールである事を確認できる。

なお、JCAN のパブリックルート CA の証明書が、取引先の職員や顧客のパソコンに登録されているため、自動的にメールの送信者を確認することが可能となる。

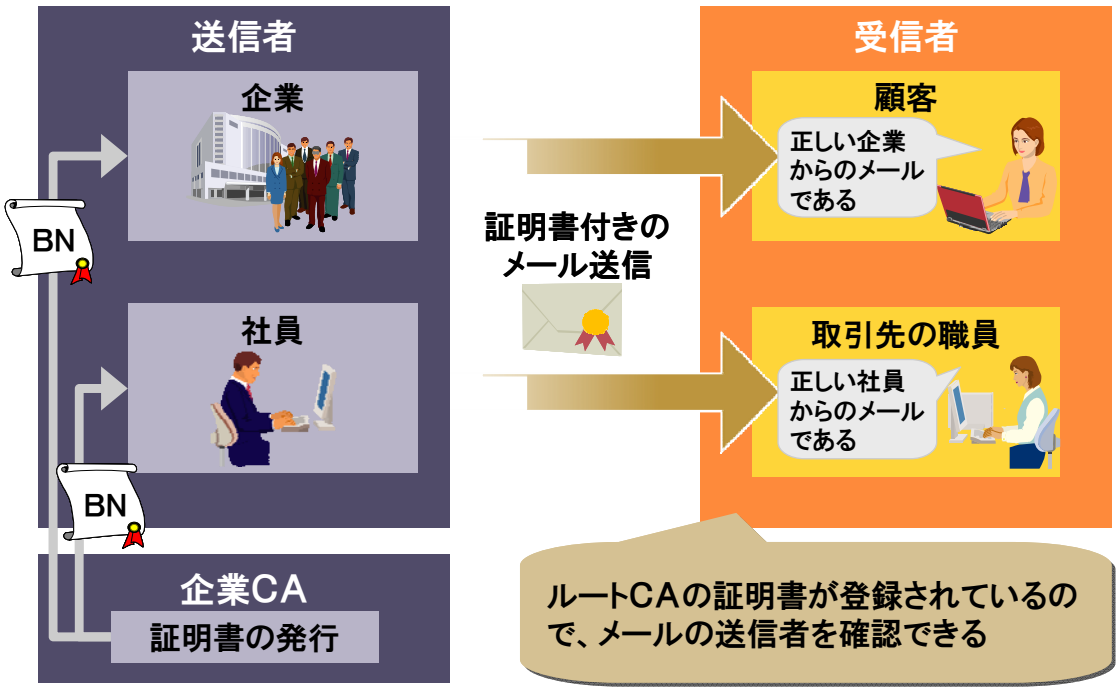


図 2-1 署名付きメール

2.1.2 電子決済

企業内等での決裁システムに、JCAN の BN 証明書を活用するビジネスシーンを示す。電子決済システムの実現方法としては、申請書に対して各担当者が電子署名した文書を回覧する方式と、電子決済システムにおける認証結果に基づき電子文書を回覧する方法の 2 パターンがありえる。以下に、それぞれのパターンを図示する。

(1) 電子署名を活用した電子決済

例えば旅費申請の書類等に対して、各担当者が電子署名を行うことにより、決裁システムを実現する。

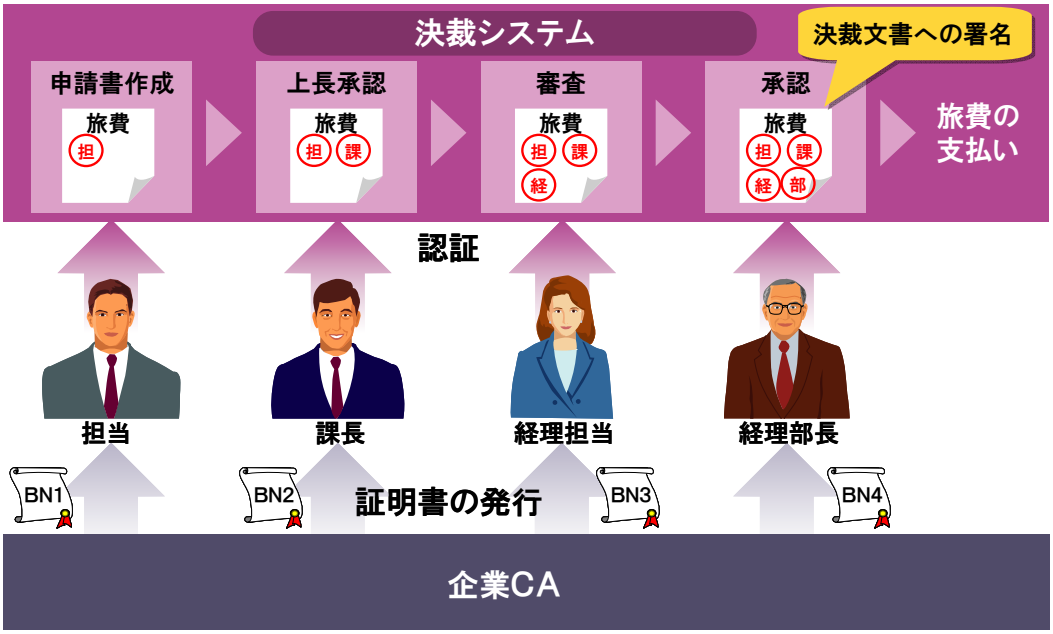


図 2-2 電子決済（電子署名）

(2) 電子認証を活用した電子決済

決裁システムにおいて、電子証明書を用いて各担当者のユーザ認証を実施し、認証結果に基づき旅費申請等の書類を回覧する。

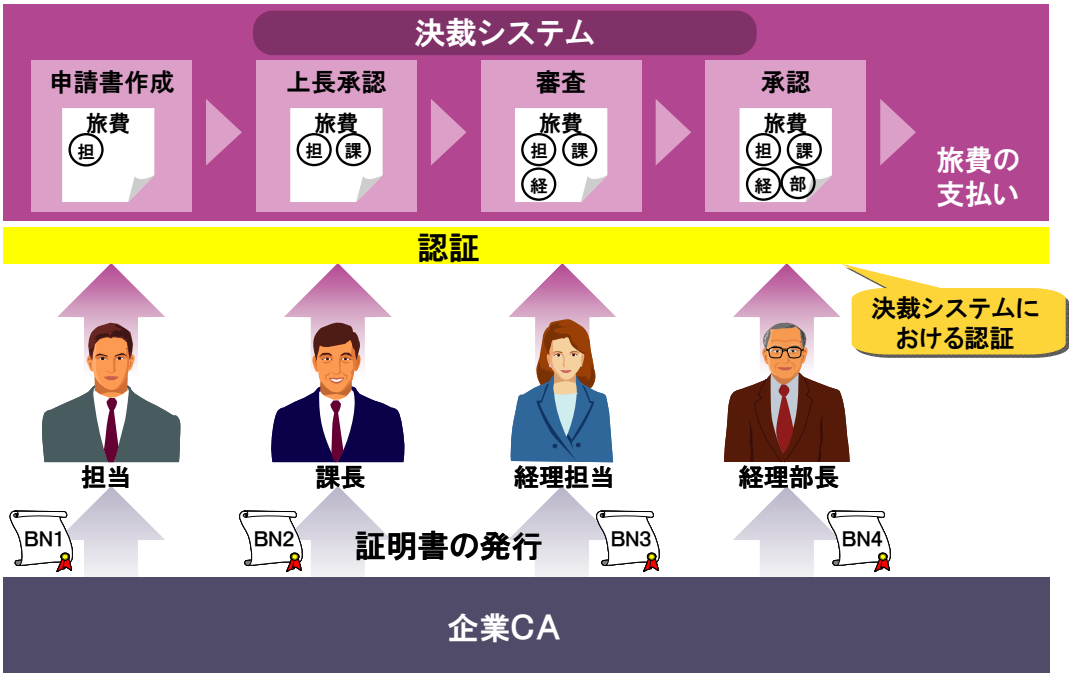


図 2-3 電子決済（電子認証）

2.1.3 電子投票

組織や団体内での役員投票や議案採決などを、BN 証明書を活用して電子的に行うことを可能とする。実現方法の一例を下図に示す。

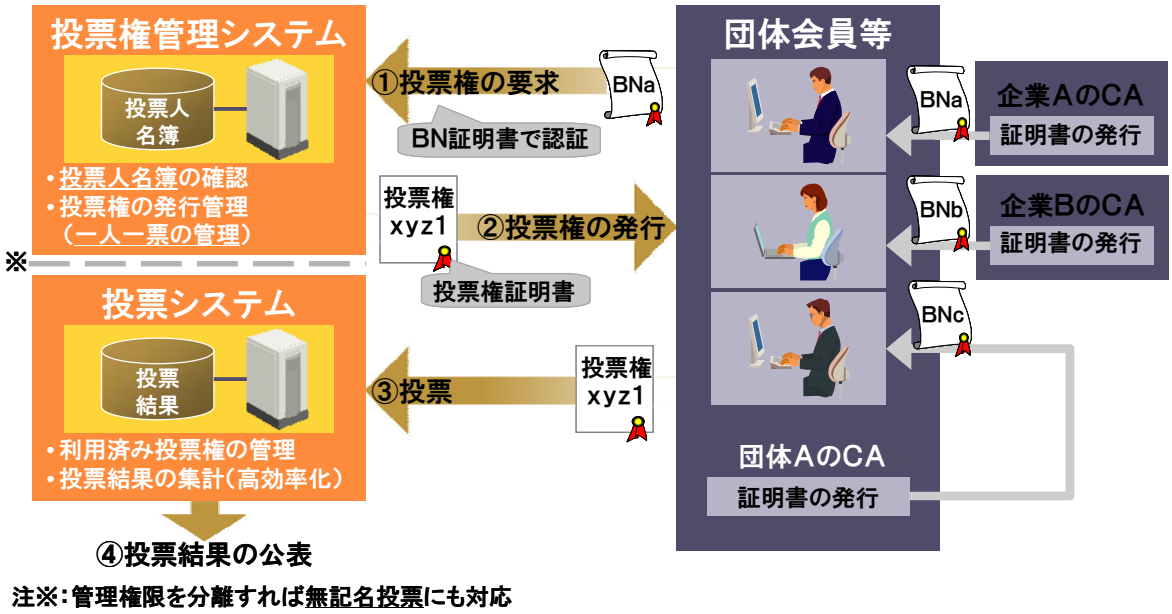


図 2-4 電子投票

団体会員は、あらかじめ団体から証明書を発行されているか、それぞれ自社の企業 CA から証明書を発行されていることを想定する。そして、投票権管理システムに BN 証明書を使ってアクセスし、投票権を取得する。このとき、投票権管理システムにおいて投票人名簿に基づき投票権の発行管理（一人一票の管理）を行う。また、無記名投票の場合、投票権には氏名を記載しない。団体会員は、取得した投票権を用いて投票システムにアクセスし投票を行い、投票システムはその結果を公開する。

このような電子投票システムを実現することにより、投票権の郵送コスト軽減、事務処理の負担軽減投票結果の収集時間短縮、無人化による透明性の向上が期待できる。

2.1.4 模倣品対策

半導体業界における LSI 製品等、模倣品の市場への出荷が広まってきており、問題となっている。この模倣品対策として、物が製造されていく段階におけるトレーサビリティを確保する手段として、BN を記載した電子証明書を活用する。

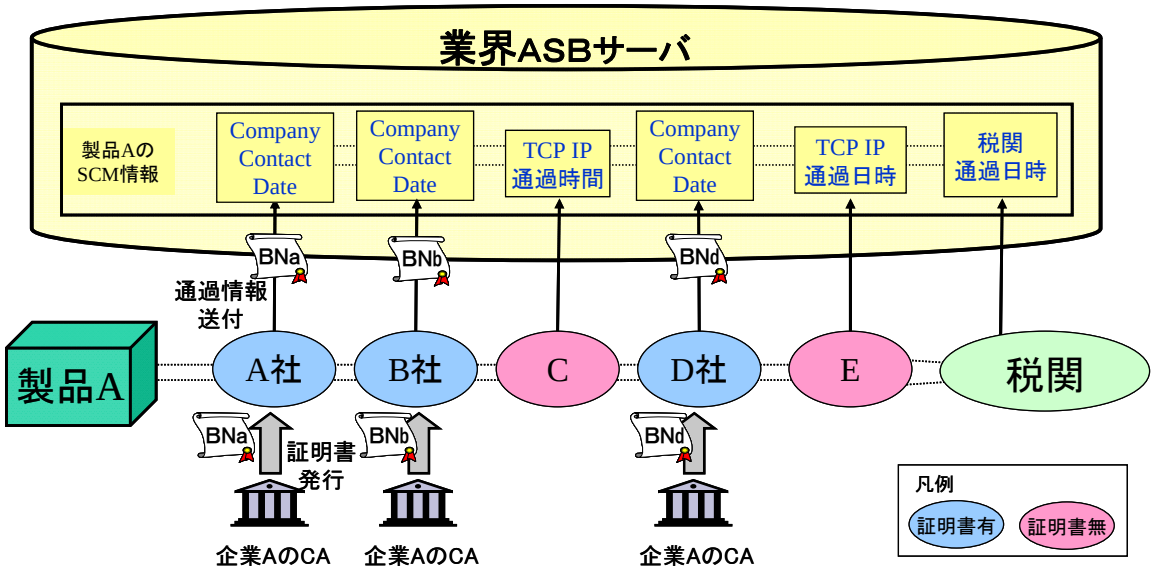


図 2-5　模倣品対策

製品を扱う複数の企業は、あらかじめ BN を記載した証明書を取得する。製品がこれらの企業を経由されて行くときに、各企業において製品に付与されたバーコードを読み取る等したタイミングで、業界 ASB サーバに対して製品の通過情報のログを送付する。このとき、電子証明書によるアクセスコントロールを実施すると共に、ログには証明書を含めた情報が記載される。これにより、問題が発生した場合に、それを扱った企業の電子証明書に記載された連絡先に連絡をすることにより、早期に問題解決につながることが期待される。

2.2 PNを活用したビジネスシーン

2.2.1 転職

転職のシーンにおいては、雇用保険番号や基礎年金番号等の転職前の企業が保持していたデータを、転職後の企業に対して提出する必要がある。これを、安信簡情報環境を利用して効率的に実施するために、PN を活用する例を下図に示す。

ユーザは、企業 A に属し BN を取得している。そして、この BN 証明書を用いてパーソナル CA から PN を取得する。これら BN と PN は、安信簡情報環境において紐付けが管理されることを想定する。

このような状態において、ユーザが転職する場合、ユーザの引継ぎ情報を安信簡情報環境を経由して転職後の企業 B へ送付する。これにより、効率的な情報のやり取りが可能となる。

また、企業 A で発行されていた BN は一度失効し、企業 B において新たに BN を発行されることになるが、この BN の引継ぎを、PN を用いて実現することができる。

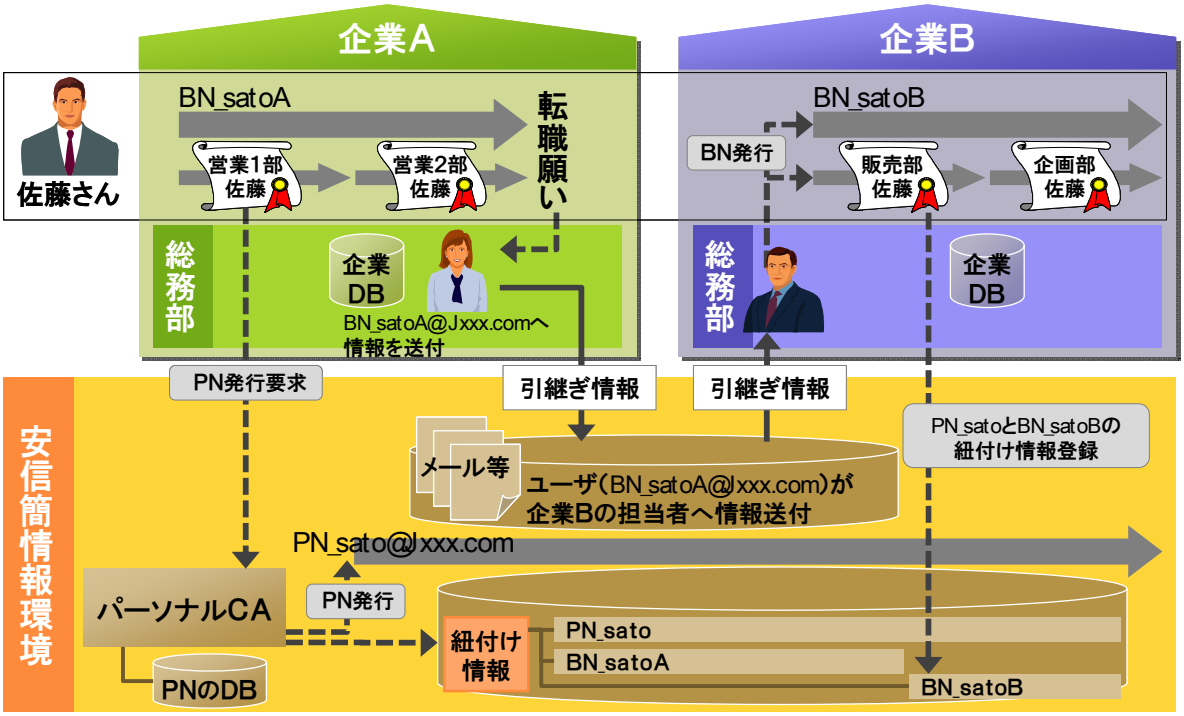


図 2-6 転職

2.2.2 オンラインショッピング

PN を活用して安心・安全なオンラインショッピングを実現する。実現方法としては、PN をそのまま活用する方法と、その都度発行されるワンタイム PN を活用する方法の 2 パターンを例示する。

(1) PNを活用したオンラインショッピング

ユーザは商店に対して、個人情報は入力せず、PN と購入商品名のみを入力する。商店は配送業者や決裁機関に対して、「PN と商品」、「PN と決済金額」を送付する。配送業者や決済機関は、それぞれ安信簡情報環境に対して PN を元に必要な情報のみ（住所、決済手段）を問い合わせ、商品の配送や決済手段を行う。

このような仕組みにする事により、各事業者に不必要な個人情報は送付されず、ユーザのプライバシが守られると共に、事業者における個人情報保護のコスト軽減が期待できる。

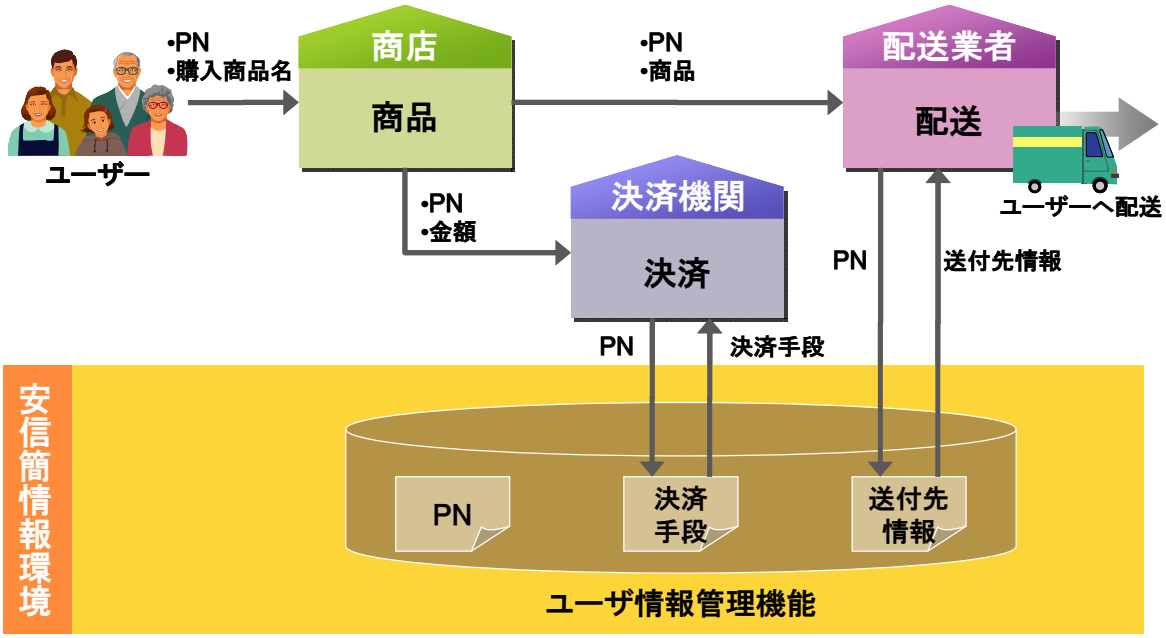


図 2-7 PN を活用したオンラインショッピング

(2) ワンタイムPNを活用したオンラインショッピング

ユーザは、予め安信簡情報環境へ PN を用いてアクセスし、ワンタイム PN を取得する。そして商店で商品を購入する場合、ワンタイム PN と購入商品名を入力する。商店は配送業者や決裁機関に対して、「ワンタイム PN と商品」、「ワンタイム PN と決済金額」を送付する。配送業者や決済機関は、それぞれ安信簡情報環境に対してワンタイム PN を元に必要な情報のみ（住所、決済手段）を問い合わせ、商品の配送や決済手段を行う。

PN のみを活用する場合に比べて、ワンタイム PN を活用することにより、各業者が PN をキーにして、PN に紐付く情報を蓄積できなくなるため、個人のプライバシ性を高める事が可能となる。

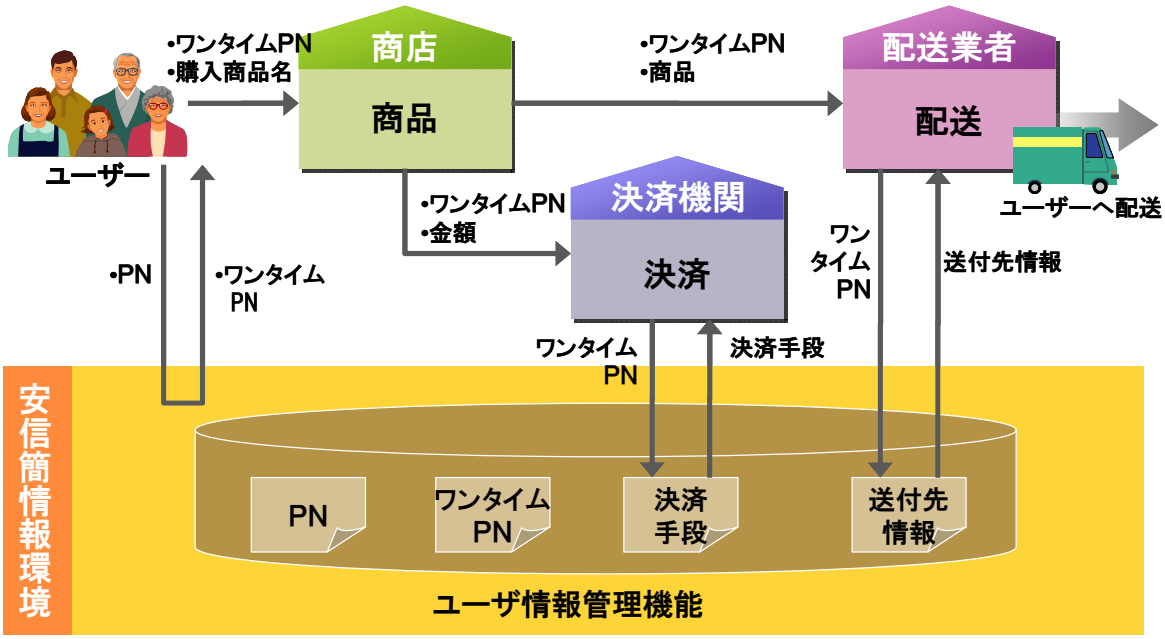


図 2-8 ワンタイム PN を活用したオンラインショッピング

2.2.3 家電リコール

PN を活用し、家電リコール時の連絡をユーザに対して抜け漏れなく実施する。家電製品の購入時と、リコール発生時に分けて説明する。

(1) 家電製品購入時

ユーザは、店舗において家電製品を購入する際に PN を提示し、店舗は情報連携局に対して PN と購買情報を登録する。もしくは、ユーザが自ら情報連携局に対して PN と購買情報の登録を実施しても良い。

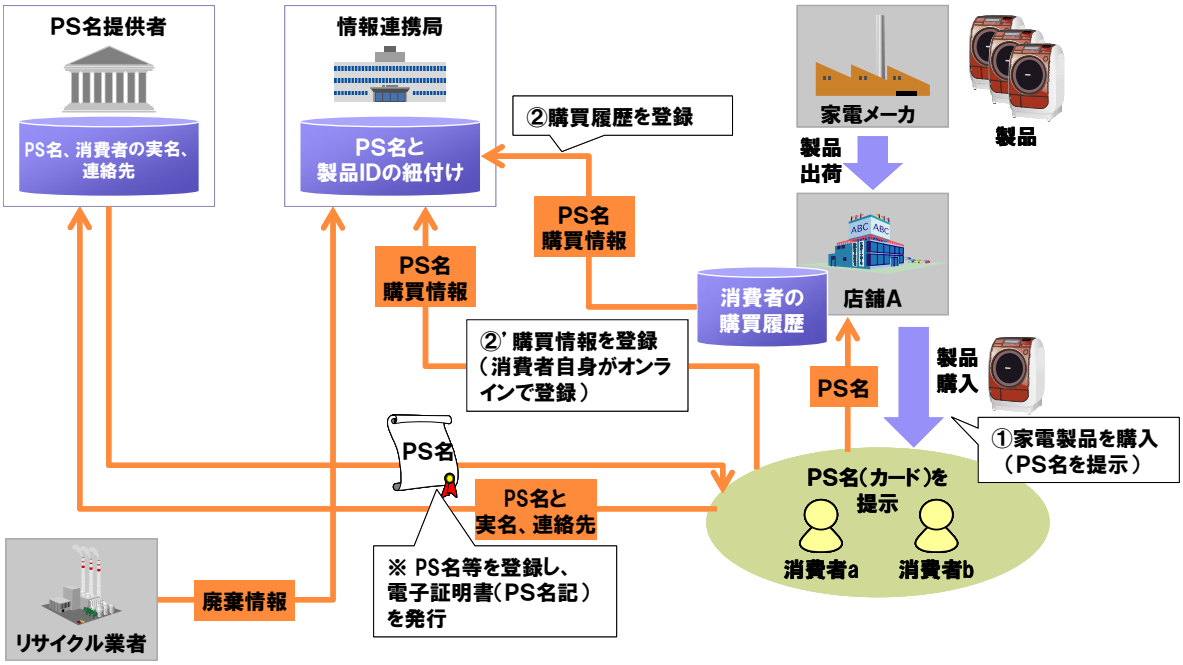


図 2-9 家電リコール（家電製品購入時）

(2) リコール発生時

リコールが発生した場合、家電メーカは制度推進機関等へリコール発生の報告を実施する。このとき、製品番号等を連絡する。制度推進機関は、情報連携局に対してリコールされた製品番号を元に、製品を所有する利用者の PN を問い合わせる。次に、取得した PN を元に、PN 提供者に対してユーザへの連絡を依頼する。PN 提供者は、ユーザに対してリコール発生の連絡を実施し、その後ユーザとメーカ間において製品回収等必要な対策を講じる。

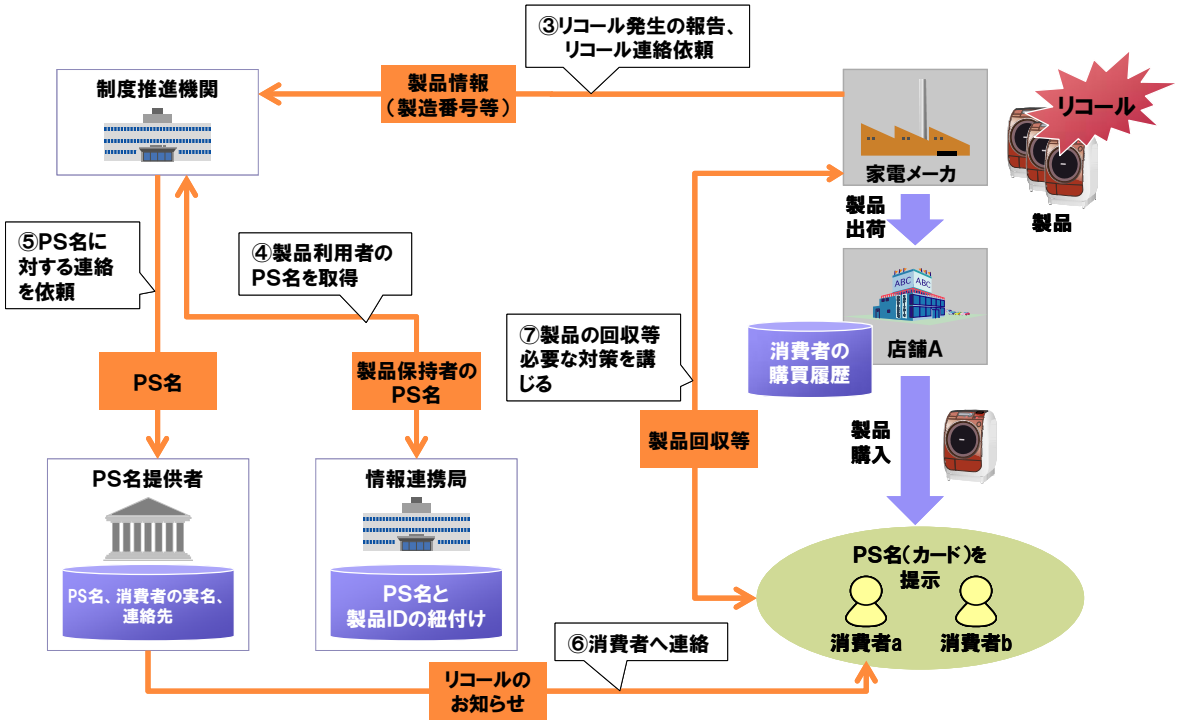


図 2-10 家電リコール（リコール発生時）

このような仕組みとすることにより、ユーザの個人情報は PN 提供者にのみ保持され、ユーザのプライバシが守られると共に、リコール情報の連絡を抜け漏れなくユーザへ連絡することができるという効果が期待できる。

3. まとめ

(1) 本検討の成果

本検討では、安心・安全な社会環境である「安信簡情報環境」の構成要素である「PS 名情報環境」、「認証環境 JCAN」、「企業 ID 連携環境」、「その他の安簡信情報環境」について、必要となる機能や論点を整理した。PS 名については、ビジネス活動で利用する「BN」と、個人がネット上の ID として活用する「PN」の２つに分け、それぞれを整理した。

また、これら BN や PN を活用した利用シーンをそれぞれ例示し、様々なビジネスシーンにおいて BN や PN をはじめとする「安信簡情報環境」が活用できることを示すことができた。

(2) 今後に向けて

これら BN、PN の仕組みと、情報を交換させる環境が共通のルールと認定制度に基づいて推進されると、社会的な情報連関の活性化に貢献するものと考える。プロセスとしては、BN が普及することで、企業活動における PKI の高度利用が促進され、同時に BN を信頼の起点とした PN の仕組みを導入することにより、社員の立場を離れた個人の活動に対しても、広く利用できるものになると考える。

B「マルチユース格納媒体の PKI 対応の検討」

－ 目 次 －

はじめに

この調査研究では、「社員等の属性情報を扱う電子認証（ID を含む）および電子署名にかかわる民間制度・基盤の確立およびその環境整備」の一環として、電子認証の基盤となる ID 情報（個人識別情報等）や電子署証明に必要な PKI 情報（共通鍵および属性情報等）を持ち運び可能な格納媒体に格納するための方式や運用方法について調査し、様々な認証サービスをいつでも利用出来るようにするための、格納媒体の選択及び媒体への情報格納方式について検討した結果の報告を行うものである。

具体的には、「マルチユース格納媒体への共通鍵及び属性情報の記録方式に関する検討」として、マルチベンダー環境でシステムの段階的な導入を可能とすることを特長とした、入退及び PC ログインに使われる格納媒体に、PKCS#7 対応共通鍵（16 バイト）及び属性情報（所属情報、権限情報或いは資格情報等）等を記録する方式を検討した。検討に際し、ID カードの共通フォーマットについて検討推進をしている FCF フォーラム（FeliCa 共通利用フォーマット推進フォーラム）会員企業 113 社を対象に認証サービスの関連アプリケーション調査を実施した。

尚、記録媒体への情報登録の方式については、別途調査研究を行っている「登録業務効率化の検討」に関する報告書も合わせて参照されたい。

1. マルチユース格納媒体への共通鍵及び属性情報の記録方式に関する検討に向けて

この調査研究を行う上で重要な役割を持つのが、電子認証情報を格納するマルチユース格納媒体である。ここではこのマルチユース格納媒体について、社会的な普及度やデータのセキュリティ性など様々な角度から検討を行った。

また、共通鍵及び属性情報の内容や記録方式については、関連アプリケーションの調査を踏まえて具体的方法について検討する事とした。

1.1 JCANパス

格納媒体には様々種類があるが、ここで言う格納媒体は電子認証基盤として様々な認証サービスに利用できると言うものと言う共通の目的をもつことから、わかりやすく総称として「JCAN パス」と呼ぶこととする。

1.2 JCANパスの定義

JCAN パスは様々な認証基盤の利用を一つの媒体に集約化し、認証・決済・保存とシームレスに連携、ビジネスを効率よく効果的に行うものであり、機能としては以下を有するものである。

- ID 情報（従業員番号窯、学籍番号など）や電子証明書を利用するための情報を格納できる。
- 格納した情報には必要に応じて暗号化及び読み書きに必要な PIN 等のセキュリティを備えている。
- 情報は必要に応じて、いつでも書き換えができる。
- 必要に応じて後から情報の追加、削除が行える。
- 基本的なルールを守れば、誰でも実装情報を利用できる。

2. JCANパスとしての格納媒体の選択

JCAN パスは、上記の基本概念お前提に認証サービスに必要な ID（Identification）情報として個人識別番号や電子証明書に関連した PKI（Public Key Infrastructure）情報を格納し、持ち運びが可能で、電子的に読み書きが可能な電子格納媒体無くてはならない。この条件を持つを格納媒体を選択した。

2.1 対象とした格納媒体

電子格納媒体には、様々な物があるが、コストや運用面での導入のし易さ、社会的な導入基盤の整備状況などを考慮して、今回は以下の媒体を対象として検討を進める事とした。

2.1.1 非接触ICカード　（TypeAカード、FeliCaカード）JCANパスとしての格納媒体の選択

非接触型とは、国際規格 ISO/IEC 14443 に準拠した非接触型の IC 搭載チップを搭載したカードで、カード情報読取装置（リーダ）とカード情報書込装置（ライタ）との通信距離に応じて「密着型」「近接型」「近傍型」「遠隔型」の 4 種類に区別される。近接型は「TypeA」「TypeB」に分類される。欧州では TypeA カード（フィリップスエレクトロニクスが開発。MIFARE カードとも言う）が普及している。米国では TypeB カード（モトローラが開発）も普及している。日本には FeliCa カード（ソニーが開発）があるが、国際規格には採用されず、現在は FeliCa カードと MIFARE カードの上位通信方式が ISO/IEC 18092（NFC, Near Field Communication）として標準化されている。

日本では社員証や入退出カードを中心に Type A カード（MIFARE カード）が多く利用されているが、住民基本台帳カード仕様は Type B カードであり、IC カード乗車券規格（日本鉄道サイバネティクス協議会による規格）は FeliCa カードである。FeliCa カードは読込み速度が速いことと他のカードに比べてセキュリティ性が高いことから、社員証や学生証などの ID カードとしても利用されている。

この状況から今回は、発行枚数が多く、民間企業での利用の多いこと、カードリーダーが複数の企業から発売され安価に購入できることなどから、Type A カードと FeliCa カードを対象とする。

2.1.2 USBメモリ

USB メモリは小型で持ち運びが容易なメモリ装置でほぼ全ての OS（オペレーティング・システム）の PC（パーソナル・コンピュータ）で利用が出来る。価格も安価であり、セキュリティ対策が施されていることから PC を利用を中心した場合の格納媒体として対象とすることにした。

2.2 今後の検討を必要とする格納媒体

今回は対象から外したが、今後の対象格納媒体として、以下の媒体も検討を継続して行く必要がある。

2.2.1 非接触ICカード　(Type Bカード)

Type B カードは日本では、住民基本台帳カードやパスポートなど国や自治体が発行する認証カードとして利用されており、それぞれが独自のフォーマットを利用し、公開性もないことから、既存カードとの親和性を考慮する観点から今回は検討対象から外したが、公共性と言う観点から見れば対象とすべき格納媒体であると考える。

検討にあたっては、多くの公的システムとの連携など考慮する必要性がある。

2.2.2 RFID

RFID（Radio Frequency IDentification「電波による個体識別」の略）は、主に物流品の管理などを主体に使われている電子格納媒体である。定義的には非接触 IC カードも RFID の一種となるが、通信方式やメモリの読み書き方式などからここでは区別する。

RFID には、通信方式が複数あり、それに伴い多くの媒体が存在するため、共通的な情報を格納するためには、利用目的を明確にした絞り込みが必要であり、今回は対象からは外したが、製造物や生産物を会社として証明するなどの利用を考えると対象とすべき格納媒体であると考える。

2.2.3 SIMカード（携帯電話）

SIM カード（Subscriber Identity Module Card）とは、GSM や W-CDMA などの方式の携帯電話で使われている電話番号を特定するための固有の ID 番号が記録された IC カードである。社会人の携帯保有率を考えるとほぼ全員が一台は携帯電話を保有している状態であり、この携帯電話に電子証明書のような公的な証明が付加できれば、認証基盤として活用の場面が増えると来たい出来る。ただし、現時点ではこの SIM カードに情報を格納するには多くの制約があるため、今回は対象から外したが、今後は、各関係機関との調整を行い検討を進めるべきものであると考える。

3. 関連アプリケーション調査と調査結果

JCAN パスへの情報登録内容を検討する上で、この JCAN パスを利用する可能性が高い認証サービス関連アプリケーションについて調査を行った。

3.1 関連アプリケーション調査の目的

この調査の目的は、JCAN パスを普及させるには、既存のサービス基盤でも利用できることを考える必要があるとの考えから、既存の認証サービス関連アプリケーションを調査しその実態から必要な機能や情報を調査するものである。

3.2 関連アプリケーション調査の方法

この調査は、この報告書をまとめる検討グループの所属する FeliCa 共通利用フォーマット推進フォーラム（通称：FCF フォーラム　http://www.fcf.jp/）の協力を頂き、会員企業 113 社からの情報をもとに実施した。

3.3 関連アプリケーション調査結果

調査結果は、添付資料１「関連アプリケーション調査結果」の「表 FCF 会員が提供するカード・認証関連アプリケーション一覧」の通り。

この情報を元に関連アプレイケーション提供企業からヒアリングを行った結果、ほぼ全社から「FCF フォーラムが提唱している共通フォーマットの考え方にそった考え方であれば、既存アプリケーションへの適用は可能」との意見があった。また、電子証明書については、「手軽に証明書も発行処理が行えるのであれば利用価値はある」との意見であった。また、「媒体上にある登録情報はなるべくシンプルな方がよく、複雑なものは適さない」との意見もあり、電子証明のための PKI 情報はシンプルなものを利用することを考える必要があると考える。

4. 情報格納フォーマット

JCAN パスの情報格納フォーマットは、JCAN パスの基本概念と既存の関連アプリケーションでの利用を実現するものでなくてはならない。そのためには、既存で利用されている技術や環境をうまく利用することが、時間とコストを押さえ、利用者からも受け入れ易いものになると考える。

そこで今回は、既に個人認証用の ID フォーマットとして、既に６０万枚以上が発券され、119 社に及ぶ企業が会員となっている FeliCa 共通利用フォーマット推進フォーラム（通称：FCF フォーラム　http://www.fcf.jp/）が提唱する共通フォーマット「FCF」を参考に検討を行う事

とした。

4.1 FCF（FeliCa Common-use Format）とは

FCF は、非接触 IC カード"FeliCa"の有する特長のひとつである、「マルチユース機能」を十分に活用することを目的として作られた、個人認証カード（ID カード）用フォーマットで、カード利用者（社員・学生など）の名前や ID 番号など、基本的な個人情報のファイルフォーマットをフォーラムに参加する会員企業内で共有し、お客様の同意に基づいて読み取れる仕組みを提供している。

4.1.1 背景

これまでの IC カードが、主にシングルユース（プリペイドカード、セキュリティカードなど）で使われてきたのに対して、FeliCa では、複数のサービスイシュアが 1 枚のカード上でサービス提供をするマルチアプリケーション環境を提供した。しかし、それぞれのアプリケーションが必要とする情報がカードの初期発行時に搭載されなかった場合、後からサービスを追加するためには、サービス提供事業者同士の鍵情報の公開や、対象となるカードの一斉回収などを必要とし、実質的に困難な場合が多く、実用的ではなかった。この問題を解決し、利用者にとっても、サービス提供事業者にとっても有意義な利用環境を提供するために、印刷会社、サービス提供事業者が集まり、共通フォーマットによる相互の利用環境を提唱した。

4.1.2 定義

FeliCa の共通利用領域上のサービス群であり、以下の 2 種のフォルダで構成

【基本 ID 情報フォルダ】

・券面記載相当の個人 ID 情報を記入

⇒この情報を活用して、各種アプリケーションシステムに対応させることが可能

【追加サービス用フォルダ】（オプション）

・後日ユーザーが、メモリを必要とするような追加サービスを希望する時に利用

⇒追加するサービスイシュア（事業者）が、利用できる

4.1.3 特長

FCF は、図 4-1、図 4-2 に示すように、利用者とサービス提供事業者の双方に対し以下の特長がある。

- 発券が簡単
  （顧客）　導入までに時間がかからない
  （事業者）事業者間の調整が最小限で済む
- ID 情報が使える
  （顧客）　サービスの段階的な導入が可能

（事業者）既存事業者にかわり、いつでのサービス提案が可

- メモリを使うサービスの追加ができる

（顧客）　顧客独自のサービスがいつでの実現可能

（事業者）様々な付加サービスの提案が可能

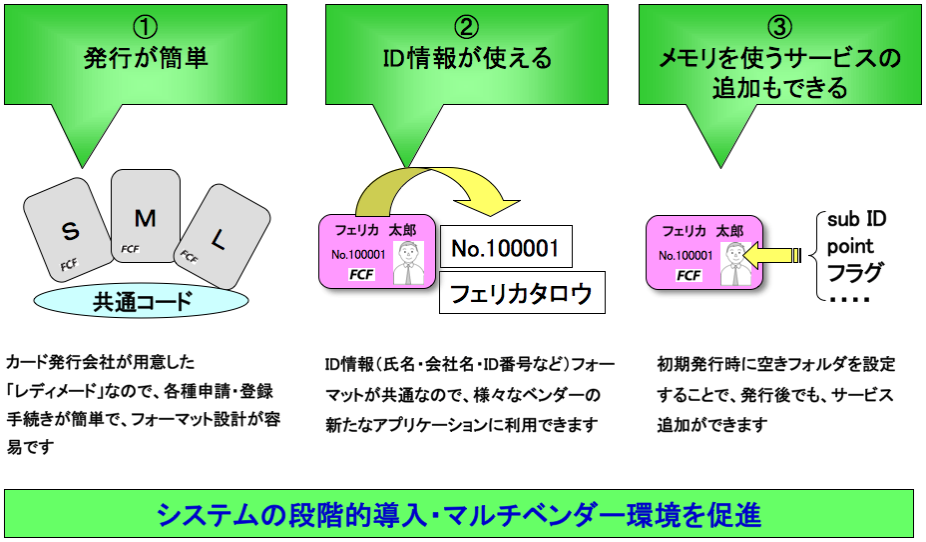


図 4-1　FCF の特長

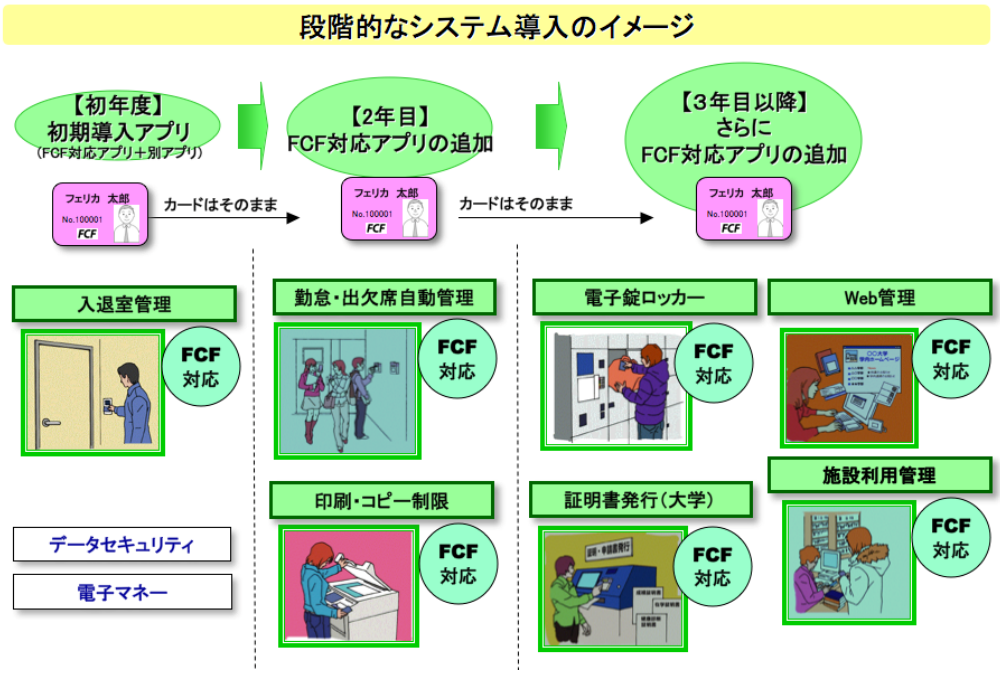


図 4-2　サービスの段階的導入イメージ

4.1.4 共通フォーマットイメージ

共通領域内の１サービスとして定義・登録し、フォーラム企業で共有する。基本 ID 情報領域と追加サービスのための空き領域を持つ構造となっており、空き領域はは顧客の利用状況により S、M、L の３タイプの境域確保が出来る。

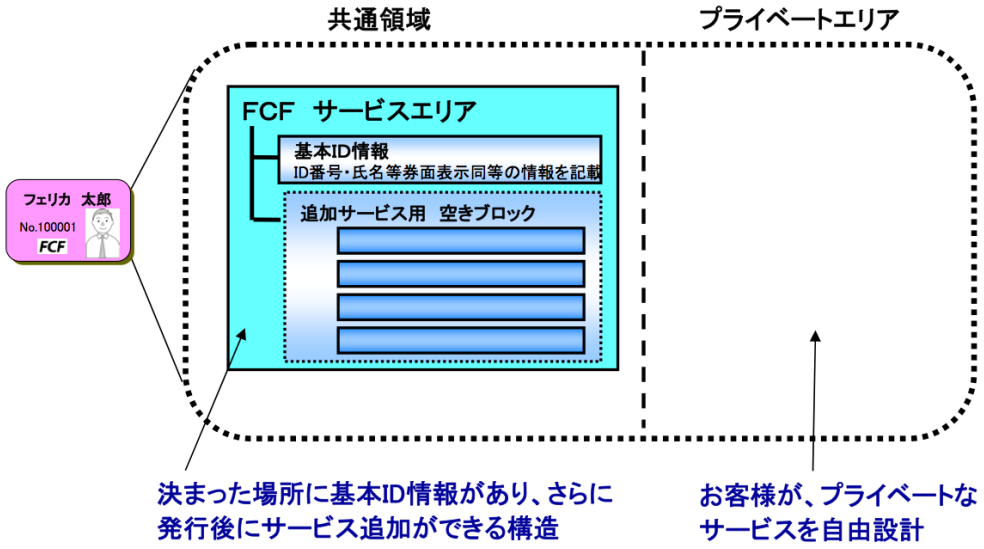


図 4-3　FCF フォーマットイメージ

詳細については、FCF フォーラムが発行する「FCF フォーマット情報　FCF-M03」を参照のこと。

4.2　JCANパス用共通フォーマット

格納媒体として FeliCa カードを利用する場合の JCAN パス用フォーマットは、FCF に準拠し、FCF の追加サービス C1 領域を JCAN パス用の電子証明書に関する PKI 情報を格納する領域と定義し実現する。

TypeA カード、USB メモリーについては、FCF のフォーマット構造を維持しながら、それぞれの格納媒体の特性を活かしたフォーマットを検討中であり、今後の実証実験等で開発・確認を行うこととする。

4.3　JCANパス用共通フォーマット仕様

FCF は、図 4-4 フォーマット仕様に示すように、大きく基本サービスエリア（エリア A）と追加サービスエリア（エリア C）の２つのエリアを持っている。

JCAN パス用はこの追加サービスエリア C1 に電子証明書に関する PKI 情報を格納する仕様とする。FCF の仕様上、追加サービスエリアを使う場合は、追加サービスエリア B が必要となり、ここに各サービスエリアの使用事業者管理コードやサービスコードを記述することで、誰が何の目的でどこのサービスエリアを使用しているかの管理が行える。

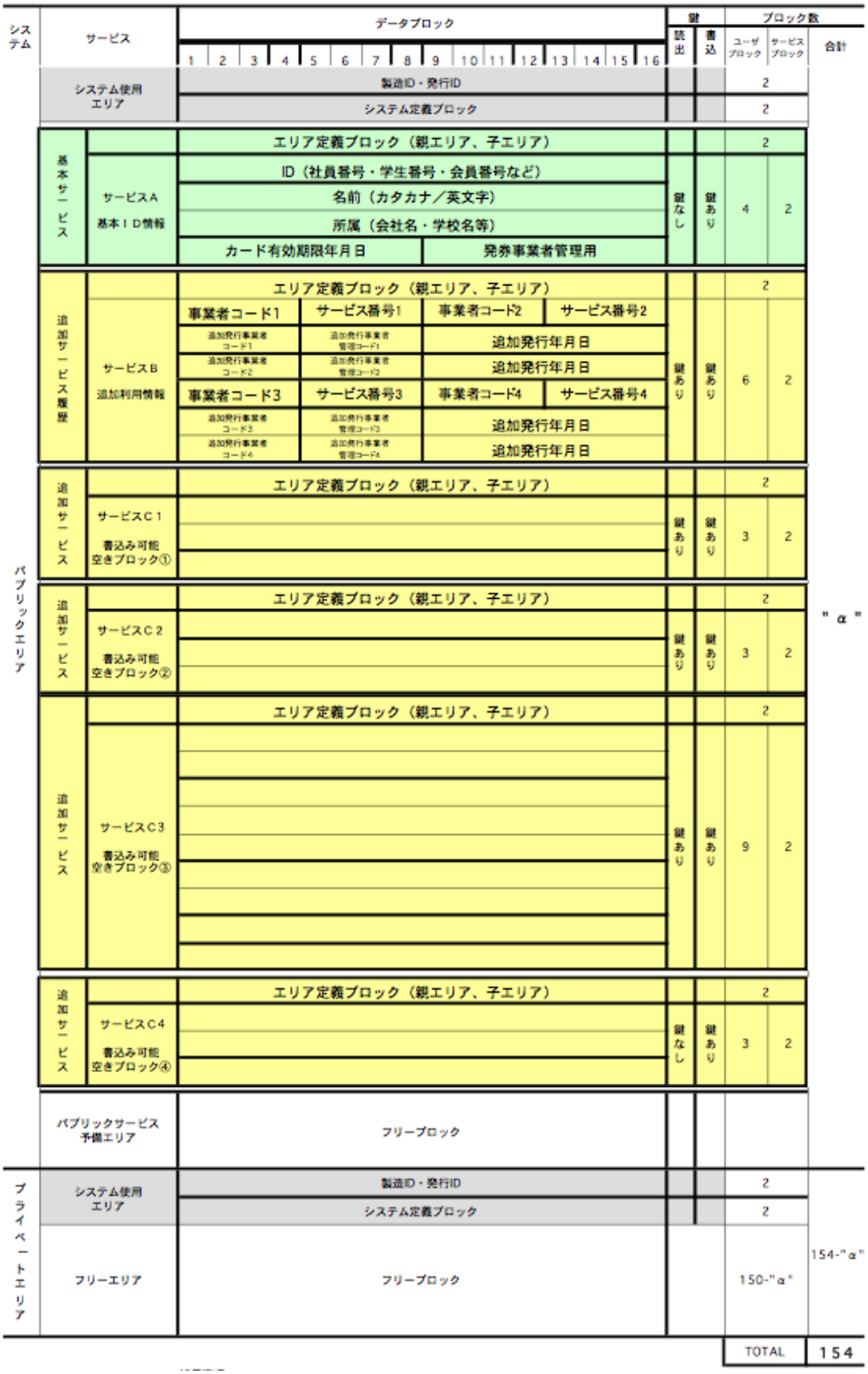


図 4-4 フォーマット仕様

4.3.1 サービス記載情報

4.3.1 サービス記載情報

サービス（Ａ）：基本 ID 情報　（必須）

カード券面に表示されている、カード所有者に関する開示可能な ID 情報を記入する。
情報を記入しないブロックには all'0'を入れる。

ブロック数：　4 ブロック　Write キーあり　Read キーなし
ＩＤ番号：　16Byte：社員番号・学生番号・会員番号など
名前：　16Byte：カード所有者の名前（半角カタカナまたは半角英字）
所属：　16Byte：カード所有者の所属（半角カタカナまたは半角英字）
有効期限：　8Byte：カード有効期限の西暦年月日（YYYYMMDD 半角数字）
属性情報：　8Byte：発券事業者において、案件ごとの識別情報を記入（自由形式）

サービス（Ｂ）：追加サービス履歴情報

使用した追加サービス（C1～C4）に関する属性情報を記入する。

ブロック数： 6 ブロック　Write キーあり　Read キーあり
初期発行時は all'0'
追加サービス情報（2 ブロック）
事業者コード：　4Byte：フォーラム会員コード番号
サービス番号：　4Byte：登録サービスコード番号
追加発行情報（4 ブロック）
追加発行事業者コード　：4Byte：事業者コード（発券事業者）
追加発行事業者管理コード：4Byte：各発券事業者が製造管理目的で自由に設定可
追加発行日　：8Byte：サービス追加の西暦年月日（YYYYMMDD 半角数字）

サービス（Ｃ１）、（Ｃ２）、（Ｃ３）、（Ｃ４）

追加サービスを行う際に使用するブロックで、自由な組み合わせで搭載可能。

ブロック数と鍵
C1：3 ブロック　Write キーあり　Read キーあり
C2：3 ブロック　Write キーあり　Read キーあり
C3：9 ブロック　Write キーあり　Read キーあり
C4：3 ブロック　Write キーあり　Read キーなし
初期発行時は all'0'
データは各追加サービス事業者が自由に設定できる。

4.3.2 鍵管理

共通フォーマットの鍵は、FeliCa においてはフェリカネットワークス株式会社（FNS）から FCF フォーラム事務局がエリアキー、エリア認証用縮退キー、サービス登録用縮退キーの提供を受けて組合企業および会員企業にて共有・管理している。

なお、縮退キーは、FeliCa の運用上きわめて重要な鍵情報であるため、**配布する場合には、配布先の会員企業名を FNS に報告する義務がありる。**また、カード発行者が縮退キーを取り扱なお、縮退キーは、FeliCa の運用上きわめて重要な鍵情報であるため、配布する場合には、配布先の会員企業名を FNS に報告する義務がありる。また、カード発行者が縮退キーを取り扱うには、フォーラム会員との守秘義務契約が必要である。

【サービスキーの管理・運用】

サービス（Ａ）

Read キー　：なし

Write キー　：FCF 事務局が初期の仮鍵を共有する。
各発券事業者はカード初期発行時、案件ごとに鍵を自社オリジナルキー（本鍵）に変更した上で管理・使用する。P 会員に発行業務を委託する際も自社オリジナルキーに変更した上で開示を行い、P 会員は責任を持って管理・使用する。

サービス（Ｂ）

Read キー　：FCF 事務局が管理し、フォーラム会員全体で共有・使用する。

Write キー　：FCF 事務局が初期の仮鍵を共有する。
追加サービス時、発行を担当する各発券事業者は発行者ごとに本鍵を決定し、フォルダＢへの書き込みを行う。

サービス（Ｃ１）、（Ｃ２）、（Ｃ３）、（Ｃ４）

Read キー　：FCF 事務局が初期の仮鍵を共有する。
サービスを追加する会員企業は、追加サービス時、初期仮鍵を FCF 事務局から取得し、自社のオリジナルキーに変更した上で組合企業から縮退キーを受け取り、管理・使用する。

Write キー　：Read キーの運用と同じ。

5. JCANパスに登録する電子証明書情報

電子証明書を実装した IC カードや USB メモリは既に何種類も存在する。その殆どが電子証明書自体（鍵情報や証明書情報など）を全て実装しているものが多い。また、実装方法は提供企業毎に独自の実装設計となっており、企業間で相互に利用はできない。

JCAN パスは、基本概念にあるように「基本的なルール」に従えば、どの企業でも認証情報

を読み書きできなくてはならない。また、一定のセキュリティ基準も守る必要がある。さらに電子証明書だけではなく、様々な企業が提供する認証関連サービス等を利用できなければならない。

この条件をクリアするための３つの基本方針について以下に述べる。

5.1 登録情報は必要最低限にする

ここで行った認証関連アプリケーションの調査で、各アプリケーションが必要とする個人識別情報を調べると、その多くが、社員番号や人事番号などその企業の構成員を識別する「個人識別番号」を必須として、その「個人識別番号」に対応した「所属」や「身分」、「権限」と言った付加情報をシステム上で管理してサービスを提供しているものが大半である。

サービスの提供方法を見ると、社員証等の格納媒体には、「個人識別番号」だけを登録し、その他の付加情報はシステム上に管理情報として持つものが殆どである。

既存のシステムとの融和性と共通利用を考えると、JCAN パスも認証に必要な個人識別情報など共通で利用が可能な情報のみを必要最小限で登録する。

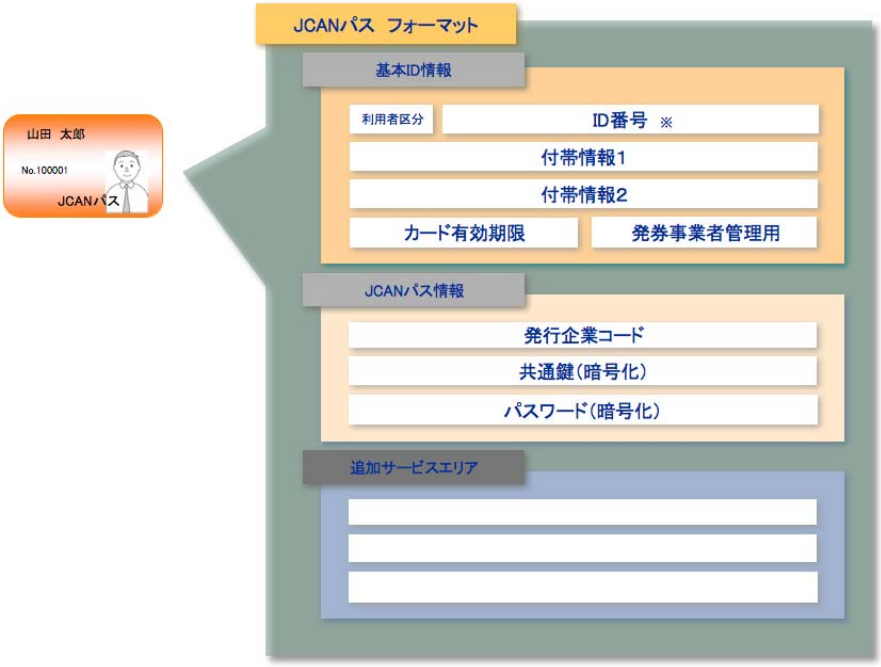


図 5-1 フォーマット仕様

【基本 ID 情報】

ブロック数：4 ブロック　Write キーあり　Read キーなし

利用者区分	：2Byte	正社員、派遣、嘱託、部外者など別途定める区分
ID 番号	：12Byte	社員番号・学生番号・会員番号など
付帯情報 1	：16Byte	必要に応じて所有者の名前など
付帯情報 2	：16Byte	必要に応じて所有者の所属など

カード有効期限　：8Byte　カード有効期限の西暦年月日（YYYYMMDD 半角数字）
発券事業者管理用：8Byte　発券事業者において、案件ごとの識別情報を記入（自由形式）

【JCAN パス情報】

ブロック数：3 ブロック　Write キーあり　Read キーあり
発行企業コード　：16Byte　JCAN で定める企業コード
共通鍵　　：16Byte　電子証明証の共通鍵（暗号化）
パスワード　　：16Byte　JCAN パス認証パスワード（暗号化）

5.2 各認証サービスで必要な付加情報はシステムで持つ

社員証等の格納媒体に付加情報を持たせないのは、「所属」や「身分」、「権限」は、頻繁に変わる可能性が高い情報のため、これを社員証等に持たせると社員証の回収、更新などの運用管理が大変にることが大きな要因と考える。

また、これらの付加情報はシステムによってデータ形式が違うため、利用するシステム毎の付加情報をそれぞれ管理するのは、運用的にも問題があると考える。

このことから、JCAN パスでは、認証に必要な個人識別情報など共通で利用が可能な情報意外は、各システム毎に持つか、あるいは、追加サービスエリアに個別に登録するようにし、「所属」や「身分」、「権限」についての共通化は行わない。

電子証明書についても、証明書自体は JCAN パスには持たず、JCAN パスから電子証明書を付加させる「JCAN パス認証プログラム（仮称）」を介して、電子証明書を必要とするサービスに電子証明書を渡す仕組みを提供することが望ましい。

JCAN パスでの電子証明書の利用方法については、「6.JCAN パスを用いた電子証明書の利用イメージ」で説明する。

5.3 情報のアクセスにはサービスキーを設置する

JCAN パスの各情報にはサービスキーを設置し、情報にアクセス時に使用する。サービスキーは JCAN パスの利用規程に同意した企業のみ公開する。なお、JCAN パス利用規程については、今後の検討課題となるため、当面は FCF フォーラムの利用規程に同意している FCF フォーラム会員を対象とする。

エリア毎のサービスキーの運用方法は以下の通り。

【基本 ID 情報エリア】

Read キー　　：なし
Write キー　　：FCF 事務局が初期の仮キーを共有する。
各発券事業者はカード初期発行時、案件ごとにキーを自社オリジナルキー（本キー）に変更した上で管理・使用する。P 会員に発行業務を委託する際も自社オリジナルキーに変更した上で開示を行

い、P 会員は責任を持って管理・使用する。

【サービス管理エリア】

Read キー　：FCF 事務局が管理し、フォーラム会員全体で共有・使用する。

Write キー　：FCF 事務局が初期の仮キーを共有する。
追加サービス時、発行を担当する各発券事業者は発行者ごとに本キーを決定し、フォルダＢへの書き込みを行う。

【JCAN パス情報エリア】

Read キー　：JCAN 事務局が初期の仮キーを共有する。
初期仮キーを FCF 事務局から取得し、JCAN サービスキーに変更した上でフォーラム会員で共有する。

Write キー　：JCAN 事務局が初期の仮キーを共有する。
各発券事業者はカード初期発行時、案件ごとにキーを自社オリジナルキー（本キー）に変更した上で管理・使用する。P 会員に発行業務を委託する際も自社オリジナルキーに変更した上で開示を行い、P 会員は責任を持って管理・使用する。

【追加サービスエリア】

Read キー　：FCF 事務局が初期の仮キーを共有する。
サービスを追加する会員企業は、追加サービス時、初期仮キーを FCF 事務局から取得し、自社のオリジナルキーに変更した上で組合企業から縮退キーを受け取り、管理・使用する。

Write キー　：Read キーの運用と同じ。

6. JCANパスを用いた認証サービスの利用イメージ

前項で説明した JCAN パスの情報を用いて認証サービスを利用した場合のイメージについて説明する。説明は電子証明書を利用する場合と利用しない場合に分けて行う。

また、様々な認証サービスを段階的に導入するイメージについても説明する。

6.1　電子証明書の利用イメージ

電子証明書を利用するシーンとして、電子メールへの電子証明書の付加、社内システムや EC システムなどが考えられる。これらのシステムを利用する場合、まず利用者はそのシステムを利用できる資格がるかの確認のため、システムへのログイン認証を行う。

このログイン認証を JCAN パスで行う場合は、「JCAN パス認証プログラム（仮称)」を使用しすることで、LDAP 等の社内共通ログイン認証に加え、その ID に付随した電子証明書を読み出すことができる。この「JCAN パス認証プログラム（仮称)」には、スタンドアロン型とネットワーク型の２つの形態を提供する。

スタンドアロン型は､利用する PC が利用者によって専用化されている場合のプログラムで、

初回のログイン認証時に「電子証明書申請発行管理システム（仮称）」から利用者の電子証明書を受け取り、専用 PC に設置したあとは、ログイン認証のみでいつでも証明書が利用できるものである。

ネットワーク型は、利用する PC が複数の人と共有する場合のプログラムで、ログイン認証の度に「電子証明書申請発行管理システム（仮称）」から利用者の電子証明書を取得し利用するものである。利用が終われば電子証明書も削除して PC には残さない。

それぞれのプログラムの詳細仕様は現在検討中である。

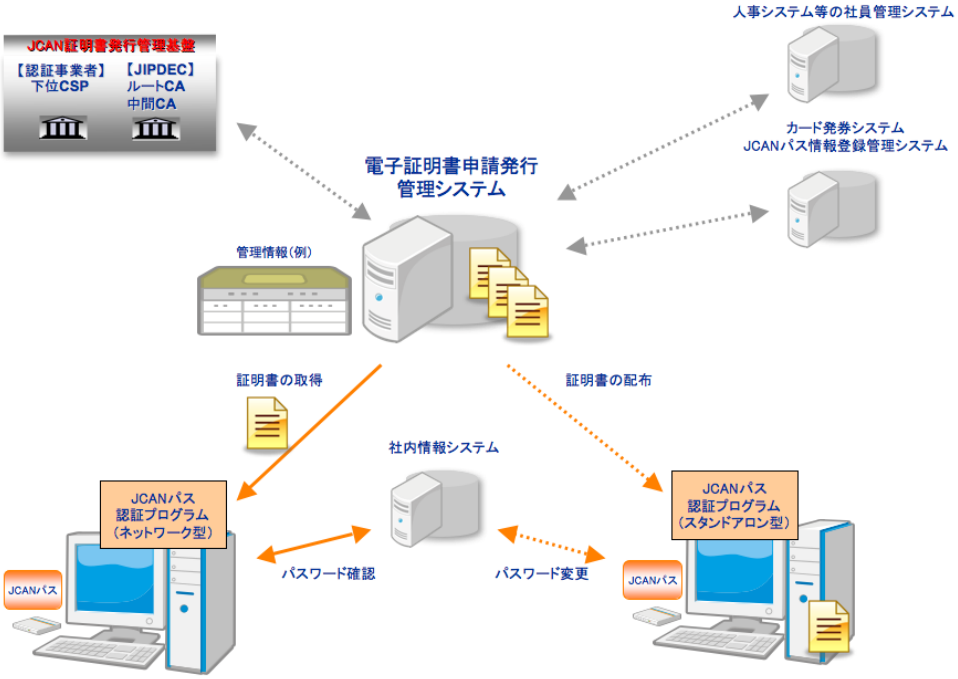


図 6-1　JCAN パスを用いた電子証明書利用イメージ

6.2　電子証明書を利用しない認証サービスでの利用イメージ

JCAN パスを利用するが、電子証明証を利用しない場合は、JCAN パスの中の基本 ID 情報を利用して ID 番号を用いた認証サービスや追加サービスを用いた認証サービスが利用でしる。

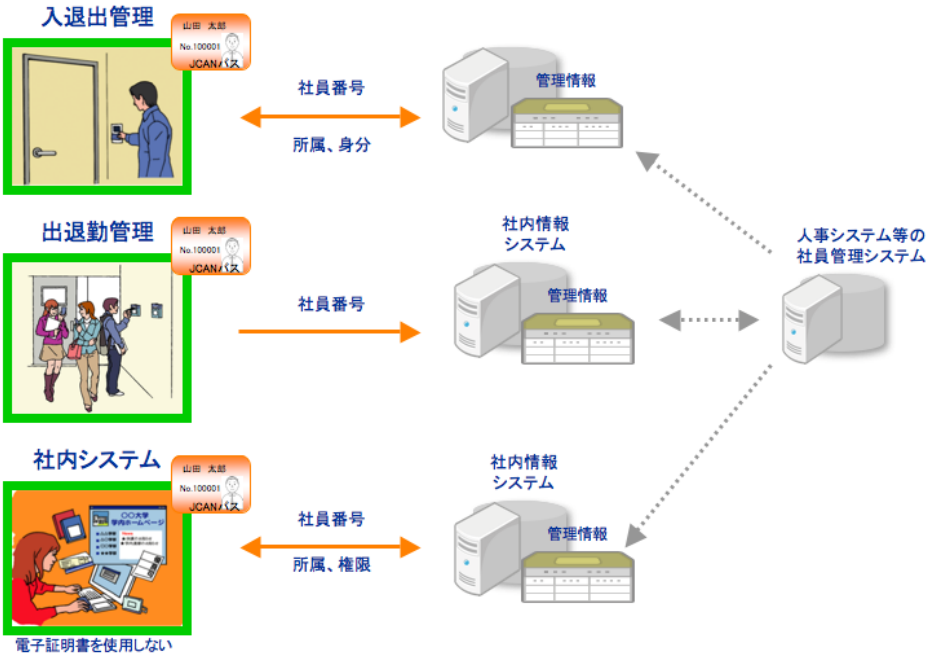


図 6-2　電子証明書を利用しない認証サービスの利用イメージ

6.3　段階的な認証サービスの導入イメージ

JCAN パスは、「1.JCAN パスの定義」にあるように「基本的なルールを守れば、誰でも実装情報を利用できる」、「必要に応じて後から情報の追加、削除が行える」ことから複数の認証サービスを段階的なに導入する事が出来る。

例えば、初年度は社員証を JCAN パスに替えるが、電子証明書の利用はせず、既存の認証サービスを利用する。２年目は社内システム及びメールで電子証明書の利用を始め、合わせて勤怠システムも新しいシステムに更新する。３年目は、新たに施設管理などのシステムを追加する。この場合、社員証の作り替えをする事無くシステムの導入が可能となる。

また、システムの更新も既存の導入企業にとらわれる事無く、JCAN パス対応の企業であればいつでも可能となる

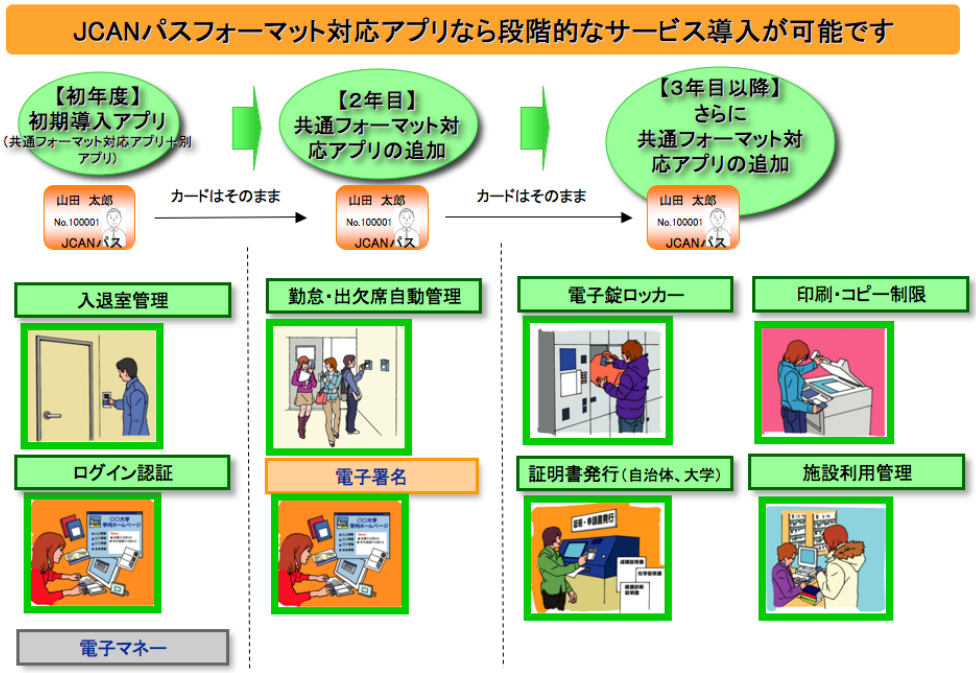


図 6-3　段階的な認証サービスの導入イメージ

7. 今後の検討課題

以上、「マルチユース格納媒体における PKI 対応の検討」について、JCAN パスと言う考え方とその内容についての検討結果を報告したが、具体的に JCAN パスを普及させるには、FeliCa カード以外の媒体についての JCAN パス共通フォーマットの検討、JCAN パスの運用ルールの検討、JCAN パスのためのアプリケーションインターフェースの検討など、今後も継続して行かなければならないと考える。特に下記の２点については、普及のためには必須と考えるので考慮が必要である。

7.1　継続的な検討組織の確立

今回は４ヶ月と言う期間で電子証明証の活用を促進するための JCAN パスについて検討をしてきたが、次年度の実証実験に向けて、まだまだ課題は多く残っている。特に既存の認証サービスとの融和性を持ちながら、電子証明書による認証サービスの普及を行うには、現実的に如何に簡単で安く利用できるかが焦点になると考える。また、利用者のみならず、認証サービスを提供する企業にとってもメリットのあるもので無くてはならない。この２つの点については、一企業や団体で進められるものではない。

これらの点を考慮して、継続的な検討組織の確立が急務であると考える。

7.2 JCANパス共通フォーマットの維持管理体制の確立

今回の検討でJCANパスと言う共通フォーマットの考え方を提言したが、このJCANパス共通フォーマットの普及を行うにはJCANパス共通フォーマットの維持管理体制を確立する必要がある。これは、今回、FeliCaカードでの共通フォーマットの参考とした、FeliCa共通利用フォーマット推進フォーラムの活動状況を見ても明白でる。

共通フォーマットを普及させるには、関係企業等に如何に公平に情報提供ができるか、意見を聞けるかが重要である。そのためには、開かれた運用組織と公平な意思決定が重要である。

これらの点を考慮して、JCANパスの維持管理体制の確立が急務である。

付録1　関連アプリケーション調査結果

表　FCF 会員が提供するカード・認証関連アプリケーション一覧

	名称	サービス内容	提供事業者
1	カード発行システム	FeliCa 二次発行およびフルカラープリンタおよび同発行ソフトウェアの販売および保守	日本データカード（株）
2	証明書自動発行システム「パピルスメイト」	大学向けｿﾘｭｰｼｮﾝ　学生証を操作するだけで、成績証明書や学割証等の各種証明書を自動発行	（株）内田洋行
3	ＮＳＡＳ	情報ｾｷｭﾘﾃｨｰ製品/FeliCa IC ｶｰﾄﾞを持ちいた(配布・発行済みも可 MicroSoft 社 ActiveDirectory の認証 また離席時の PC の画面ﾛｯｸ機能・端末稼働状況の収集(ﾛｸﾞ機能)・VPN-1 認証機能などを提供	（株）ｱｲ・ﾋﾞｰ・ｲｰ・ﾈｯﾄ・ﾀｲﾑ —
4	オフィスＩＴソリューション・勤怠管理	社員証と専用リーダでネットワーク上から勤怠データを入力　全国の拠点における勤怠状況をリアルタイムに集計管理	ソニーﾌﾞﾛｰﾄﾞﾊﾞﾝﾄﾞソリューション（株）
5	オフィスＩＴソリューション・在席管理	社員証と専用リーダでネットワーク上から入室・退室データを入力　Web 画面で社員の在席状況をリアルタイムで把握できる、ネット上のホワイトボードを提供	ソニーﾌﾞﾛｰﾄﾞﾊﾞﾝﾄﾞソリューション（株）
6	キャンパスＩＴソリューション・出欠管理	学生証と専用リーダで各教室から授業出席データを入力各種検索画面で生徒ごとや講義ごとの出席状況を即時に確認	ソニーﾌﾞﾛｰﾄﾞﾊﾞﾝﾄﾞソリューション（株）
7	入退管理ｼｽﾃﾑ	FeliCa で入退管理ｼｽﾃﾑをご提供する。各種品揃えを行うと共に他のｱﾌﾟﾘｹｰｼｮﾝと連携する。	日立情報通信ｴﾝｼﾞﾆｱﾘﾝｸﾞ（株）
8	Cyber Gatevision		—
9	PC アクセスセキュリティ Secure Aegis	PC ﾛｸﾞｲﾝ及び画面・入力の操作許可認証を、FeliCa に記載した認証情報を元に行う。	日立情報通信ｴﾝｼﾞﾆｱﾘﾝｸﾞ（株） —
10	情報漏洩防止ｼｽﾃﾑ Security　Platform	各ｱﾌﾟﾘｹｰｼｮﾝの利用権限に応じてｱｸｾｽを許可する。ﾃﾞｰﾀの流出防止の為、各種機能制限を行う。	日立情報通信ｴﾝｼﾞﾆｱﾘﾝｸﾞ（株） —
11	IP コミュニケーションプラットフォーム SIP：OFFICE	IP 電話によるｺﾐｭﾆｹｰｼｮﾝｼｽﾃﾑで、FeliCa に電話番号などの個人情報を登録し、使用する PC を自分の端末に設定	日立情報通信ｴﾝｼﾞﾆｱﾘﾝｸﾞ（株） —
12	ﾈｯﾄﾜｰｸ端末認証	ｾｷｭﾘﾃｨ機能付きﾈｯﾄﾜｰｸ端末の利用者認証を FeliCa にて行う。	日立情報通信ｴﾝｼﾞﾆｱﾘﾝｸﾞ（株）

13	ｹｰﾀｲｻｰﾊﾞｰ	携帯電話を利用した携帯ｻｰﾊﾞ AP の認証に使用。	日立情報通信ｴﾝｼﾞﾆｱﾘﾝｸﾞ（株）
14	POS ｼｽﾃﾑ	会員ﾎﾟｲﾝﾄｻｰﾋﾞｽや各業務に対する操作許可認証に使用する。	日立情報通信ｴﾝｼﾞﾆｱﾘﾝｸﾞ（株）
15	入退場セキュリティ管理システム	セキュリティゲート、タッチゲート及び電気錠で、スムーズな入退場管理を行なう	（株）高見沢サイバネティックス
16	キャンパス向けサービス	入退出管理・出欠席管理等学園内のサービス+Edy 機能	（株）シー・エス・イー
17	入退室管理システム（ＧＧ－１）	セキュリティゲート、デジタル録画装置と連携し、警備や鍵管理機能などトータルセキュリティシステムを提供	（株）クマヒラ
18	鍵管理	カード対応できない所等、鍵そのものを保管・管理し入退室管理システムと連携したシステムを提供	（株）クマヒラ
19	セサモＴＲⅡ	就業スペースの入退室管理、無人時の防犯管理機能を提供。オンライン契約を付加頂ければ警備員の緊急対処も可能。	セコム（株）
20	キャンパスカードソリューション	出欠管理、入退出管理、図書貸出し、証明書発行を中心としたキャンパス向けソリューション。	トッパン・フォームズ（株）
21	カードホルダ情報	カードホルダの情報を学外の端末にて読むために使用する。	大日本印刷（株）
22	キャンパスカードサービス	出席管理や入退室管理等キャンパス内のサービスを一括管理する。。	サクサ（株）
23	企業向け IC カードサービス	勤怠管理や入退室、警備の開始／解除等、社員証または専用カードとしてリアルタイムに管理する。。	サクサ（株）
24	ピットタッチ	ネットワーク対応 FeliCa R/W で、Standalone でも動作。標準的な３つのパッケージを用意したほか、ソフトウェアカスタマイズ、OEM も可能。	（株）ビー・ユー・ジー
25	POS 連動会員システム	POS システムと連動して、会員へのポイントサービスや FSP・CRM などのソリューションをご提供する。。	（株）寺岡精工
26	POS 連動電子決済システム	POS システムと連動して、Edy などの電子マネー決済やクレジットカードの電子決済をご提供する。。	（株）寺岡精工
27	入出退管理サービス	FeliCa 対応端末（自社、OEM、受託開発／製造）による勤怠管理、入出退管理、出席管理等の端末から管理サーバまでのトータルソリューションの提供。	コンピュータ・ハイテック（株）
28	セキュリティサービス	ネットワーク上の通信に関わるセキュリティサービス（ハードウェア／ソフトウェア）。	コンピュータ・ハイテック（株）

29	セキュリティ・プリンティングサービス	印刷システムのセキュリティ強化により、企業内や学内、省庁内の機密情報や、個人情報の外部漏洩を防止するシステムサービス。	コンピュータ・ハイテック（株）
30	WB-1S	FeliCa 対応リーダ／ライタ	ドコモ・システムズ（株）
31	入退管理システム	入退管理ゲートで入場者を管理し他システムと連携を行う。	日本コントロール（株）
32	入退管理システム	ネットワーク上で利用者のドア開錠、履歴を管理する。。	NECトーキン（株）
33	出席管理用：IC メッセンジャー出席ボード	データ記録・送信機能付マルチ IC カードリーダです。記録したタイムスタンプ、カード情報を出席管理等にご利用頂けます。	（株）ICブレインズ
34	Socratec (ソクラテック)	各座席に IC カードリーダを置き、座った所に IC カードを置くことで、どこに誰が着席しているのかを把握できます。出席が一瞬で取れるだけでなく、5 つのセレクトボタンを利用し授業にもお使い頂けます。	（株）ICブレインズ
35	トータル・キャンパス・インフォメーション	学生・教職員向けの出席管理システム	安田情報(株)
36	SmartOn	FCF の ID を使った、PC セキュリティソフトを開発、販売、サポート。	（株）ソリトンシステムズ
37	ポイントサービス	キャンパス内のポイントシステム	NRIﾈｯﾄﾜｰｸｺﾐｭﾆｹｰｼｮﾝｽﾞ（株）
38	入退室管理	弊社入退室管理装置での入退室・在室・身分証明管理サービス。	パナソニック電工（株）
39	就業管理システム	人事・給与システムともリアルに連携し、労働生産性向上を視野に分析データの提供も可能な HRM Solution です。	日通システム（株）
40	入退室管理システム	電気錠との連携で、ドアの開錠施錠管理、入室履歴管理が可能。出退勤管理との併用も可能です。	日通システム（株）
41	証明書自動発行機	各種証明書・学割証の自動発行システム	（株）エスアイインフォジェニック
42	ＴＥＣＳ	弊社入退室管理システムで使用。	ﾀﾂﾀ ｼｽﾃﾑ・ｴﾚｸﾄﾛﾆｸｽ（株）
43	キャッシュレスサービス	FCF 内の ID データに ReadOnly でアクセスし、キャッシュレス決済を行うことができる。（給与控除決済・クレジット対応 PostPay 決済）	グローリー（株）

44	企業･学校向けサービス	入退室管理、出欠席管理、証明書発行等企業・学校内の IC カードシステムに関係するサービス。	（株）ｴﾇ･ﾃｨ・ﾃｨ・ﾃﾞｰﾀ
45	キャンパスソリューション	ＦＣＦを利用した学生証や教職員証のＩＣカードソリューション	NECｼｽﾃﾑﾃｸﾉﾛｼﾞｰ（株）
46	MFP 認証・課金	MFP 本体、周辺機器でのカード認証、課金システムに使用	ｺﾆｶﾐﾉﾙﾀﾋﾞｼﾞﾈｽﾃｸﾉﾛｼﾞｰｽﾞ（株）
47	製造業向けサービス	製造業の生産現場における入退室管理等の個人認証をするサービス	三菱マテリアル（株）
48	R/W ドライバ・アプリ開発	FCF 準拠 R/W の採用を検討される機器メーカーに対する、ドライバやアプリの開発・提供	アイティアクセス（株）
49	図書館入館管理システム	図書館に入館管理のためのゲートを設け、ホストシステムと連携し、利用の可否、各種の利用実績統計を行う。	アイデックコントロールズ（株）
50	図書自動貸出返却システム	図書館における資料の貸出・返却を利用者自身が行い、利便性の向上やプライバシーの保護を提供する。。	アイデックコントロールズ（株）
51	出席管理	ガイダンス等の出席状況を把握する	大学生協中国・四国事業連合
52	カード発行	氏名、写真、バーコード等の印刷、及びＩＤ情報の書き込み	日本オフィスメーション（株）
53	入退室･警備システム ID コード	非接触カードを用いた入退室・警備システムの認証に使用する ID コード	アビニックス株式会社
54	収納セキュリティ	カードで認証された人だけが利用できる保管庫・キャビネット	株式会社イトーキ
55	アクセスコントロール	電気錠との連携でドアの開錠施錠管理、入退出履歴管理。また収納セキュリティとの連携も可能	株式会社イトーキ
56	入退室管理	入室・退室両方にカードリーダーを設置し、高度なセキュリティを実現する。。	株式会社大塚商会
57	勤怠管理	IC カードを読ませるだけで、日々の勤怠管理が行え、給与システムとも連携する。。	株式会社大塚商会
58	出席管理	学生証をリーダーにかざすだけでデータを収集。個々の出席率も把握できます。ﾊﾝﾃﾞｨ型も利用可。	株式会社大塚商会
59	プリンタセキュリティ	プリンタ据付のカードリーダーにかざしてから出力するので、他人に文書を読まれる心配がありません。	株式会社大塚商会
60	勤怠管理システム	FeliCa 社員証を使った勤怠の管理。上位アプリケーションを選ばず、接続が可能です。	株式会社ﾏｰｽﾃｸﾉｻｲｴﾝｽ
61	図書館用自動貸出返	自動貸出返却装置において、FeliCa 使用の図書館利用者	住友スリーエム株式会社

	却装置	カードに対応。	
62	IC カード認証	IC カードを用いた学内システムの認証を行う。この際 SSO などを用いシステム利用の利便性を向上させる。	株式会社ネットマークス
63	リーダ端末	読取部・表示部・操作部を一体化し、小型化を実現した Felica 用リーダ端末の開発・設計・製造及び販売	マイクロテクノ株式会社
64	マルチリーダモジュール	マルチ RFID リーダモジュール（組込用）の開発・設計・製造及び販売	マイクロテクノ株式会社
65	電子マネーチャージ	電子マネーのチャージ・残高照会・精算処理 及びカード発行	株式会社エルコム
66	チケット発行	食券や証紙など、引換券の発行	株式会社エルコム
67	入退場管理	フラッパーゲートを利用した入退場管理	株式会社エルコム
68	図書自動貸出返却装置	自動貸出返却装置において、FeliCa 使用の図書館利用者カードに対応	東急車輛製造株式会社
69	出席確認アプリ／モバイル版	先生のおサイフケータイを IC カード学生証出席確認リーダ端末として使用可能とするサービスです	株式会社コスモ・サイエンティフィック・システム
70	出席確認アプリ／ＰＣ版	先生の WindowsPC を IC 学生証出席確認リーダ端末として使用可能とするサービスです	株式会社コスモ・サイエンティフィック・システム
71	出入管理システム	カード認証による電気錠の解錠	ホーチキ株式会社
72	食堂決済	食堂キャッシュレスシステムの構築	エヌ・エス・システム株式会社
73	eyes	独自ポイントシステム	株式会社アイズ
74	カード受託発行	学生証・社員証等の受託発行サービス	株式会社ニプリック
75	カード発行用アプリケーション	大学・企業等現場にてカード発行するためのシステムの提供販売	株式会社ニプリック
76	出欠管理	IC カードを利用し出席情報を所得する。。取得した出欠情報はリアルタイムに確認できます	日本システム技術株式会社
77	出退勤管理	IC カードを利用し出退勤情報を取得する。。取得した情報を利用し教員の在学確認ができます	日本システム技術株式会社
78	情報ポータル端末	IC カードで情報ポータルに自動ログインすることができます	日本システム技術株式会社
79	図書館システム	図書館カウンターでの貸出業務における IC カード利用者証に対応	京セラ丸善システムインテグレーション株式会社
80	セキュリティシステム	IC カードを利用した入退室管理システム	株式会社デンソーウェーブ

81	キャッシュレスシステム	IC カードを利用した食堂での自動精算システム	株式会社デンソーウェーブ
82	AS-D1	IC ｶｰﾄﾞを認証キーとして実現する認証印刷製品	ｷｬﾉﾝｲﾒｰｼﾞﾝｸﾞｼｽﾃﾑｽﾞ株式会社
83	授業出欠席管理ｼｽﾃﾑ	ﾎﾟｰﾀﾌﾞﾙ IC ｶｰﾄﾞﾘｰﾀﾞを使用して、いつでもどこでも簡単に出欠管理が出来ます	日鋼情報ｼｽﾃﾑ株式会社
84	企業・学校向ｿﾘｭｰｼｮﾝ	入退館、出席管理から利用者の利便性を向上させる IC ｶｰﾄﾞを中心としたﾄｰﾀﾙｿﾘｭｰｼｮﾝ	株式会社DTS
85	ｾｷｭﾘﾃｨｼｽﾃﾑ	IC ｶｰﾄﾞを利用した各種ｾｷｭﾘﾃｨｼｽﾃﾑ	タカヤ株式会社
86	会員ﾛｯｶｰの施開錠ｼｽﾃﾑ	会員ﾛｯｶｰの施開錠方法として FCF を利用する	日本自動保管機
87	入退室管理システム	ｶｰﾄﾞを使った個人認識によるｹﾞｰﾄ（扉）制御と、上位ﾊﾟｿｺﾝからｹﾞｰﾄ制御と入退履歴管理を行う。。	株式会社エヌケーシー
88	入退室管理ｼｽﾃﾑ	IC ｶｰﾄﾞによる入退室管理ｼｽﾃﾑ。各種機器連携が可能	東急建設株式会社
89	出席管理ｼｽﾃﾑ	IC ｶｰﾄﾞによる出席管理ｼｽﾃﾑ	東急建設株式会社
90	IC ｶｰﾄﾞ発行	学生証・社員証等 IC ｶｰﾄﾞの受託発行ｻｰﾋﾞｽ	東急建設株式会社
91	自動貸出機	図書の自動貸出機	株式会社暁電機製作所
92	入退室ｼｽﾃﾑ	FeliCa ｶｰﾄﾞ使用の学校に於ける入退室ｼｽﾃﾑ	東京計器株式会社
93	IC ｶｰﾄﾞ認証ｺﾋﾟｰ/ﾌﾟﾘﾝﾄｼｽﾃﾑ	FCF を利用した社員証を使って個人認証し、ｾｷｭｱなｺﾋﾟｰ・ﾌﾟﾘﾝﾄ出来る仕組みを提供する。	富士ｾﾞﾛｯｸｽ株式会社
94	IC ｶｰﾄﾞ認証ｵﾝﾃﾞﾏﾝﾄﾞ課金ﾌﾟﾘﾝﾄｼｽﾃﾑ	FCF を利用した学生証を使って個人認証し、ｾｷｭｱなどこでも課金ﾌﾟﾘﾝﾄ出来る仕組みを提供する。	富士ｾﾞﾛｯｸｽ株式会社
95	ｵﾌｨｽｾｷｭﾘﾃｨｻｰﾋﾞｽ	機械警備、出入管理、PC ｾｷｭﾘﾃｨを組み合わせたｵﾌｨｽ向けｾｷｭﾘﾃｨｻｰﾋﾞｽ	綜合警備保障株式会社
96	講義出欠管理ｼｽﾃﾑ	大学等の講義で FeliCa を使用して出欠の取得・管理を行う。	大明株式会社
97	勤怠管理ｼｽﾃﾑ	企業の社員出退勤情報を FeliCa を使用して取得する。。	大明株式会社
98	IC ｶｰﾄﾞ読込みｼｽﾃﾑ	IC ｶｰﾄﾞの社員証・学生証等を貸出利用ｶｰﾄﾞとして使用出来るようにするｼｽﾃﾑです。	株式会社ブレインテック
99	就業システム	IC ｶｰﾄﾞ対応方式、指紋、静脈照合方式など、ﾈｯﾄﾜｰｸにつながる最新式ﾀｲﾑﾚｺｰﾀﾞｰを始めとして、就業情報ｿﾌﾄ、人事情報ｿﾌﾄといった各種情報ｼｽﾃﾑｿﾌﾄｳｪｱを紹介する。。	アマノ株式会社
100	入退室システム		アマノ株式会社
101	食堂システム		アマノ株式会社

102	入退室管理ｼｽﾃﾑ	入出退管理と警備ｼｽﾃﾑを同一ｶｰﾄﾞにより行う。。（ﾃﾅﾝﾄﾋﾞﾙ、自社ﾋﾞﾙ等）	ｺﾊﾞｯｸｽ株式会社
103	出席管理	電池駆動の IC ﾘｰﾀﾞで大学や研修所の講義出席者の FeliCa ｶｰﾄﾞを読み取り時間と共に記録する。。	株式会社ｹﾝﾌﾟﾗｽ
104	ﾀｲﾑﾚｺｰﾀﾞ	出勤時間、退勤時間を記録する。。	株式会社ｹﾝﾌﾟﾗｽ
105	巡回管理	巡回ﾎﾟｲﾝﾄの FeliCa ｶｰﾄﾞを電池駆動のﾘｰﾀﾞで読み取り、何時にどのﾎﾟｲﾝﾄを通過したか記録する。。	株式会社ｹﾝﾌﾟﾗｽ
106	IC ｶｰﾄﾞ発行	学生証・社員証等 IC ｶｰﾄﾞの受託発行業務	東京ｶｰﾄﾞｿﾘｭｰｼｮﾝｽﾞ株式会社
107	ｶｰﾄﾞ発行ｼｽﾃﾑ	自社でｶｰﾄﾞを発行する為のｼｽﾃﾑの販売	東京ｶｰﾄﾞｿﾘｭｰｼｮﾝｽﾞ株式会社
108	勤怠管理	勤怠管理用に出勤、退勤等の勤怠ﾃﾞｰﾀを収集出来ます。連動する勤怠管理ｿﾌﾄの紹介も可能です。	ｾｲｺｰﾌﾟﾚｼｼﾞｮﾝ株式会社
109	食堂管理	食費天引き用のﾃﾞｰﾀを収集出来ます。	ｾｲｺｰﾌﾟﾚｼｼﾞｮﾝ株式会社
110	入室管理	電気錠と連動させ、入室管理が行えます。	ｾｲｺｰﾌﾟﾚｼｼﾞｮﾝ株式会社
111	FeliCa 対応リーダライタ	FeliCa 対応リーダライタの製造/販売を行っています。	富士電機ﾘﾃｲﾙｼｽﾃﾑｽﾞ株式会社
112	複合機利用ｻｰﾋﾞｽ	複合機利用者 ID と利用権限、利用可能枚数、利用後枚数の保存	ｺﾆｶﾐﾉﾙﾀﾋﾞｼﾞﾈｽｿﾘｭｰｼｮﾝｽﾞ株式会社
113	健診カード	FeliCa に受診者属性と健診結果の書込みと読出しを行う	株式会社サン・プラニング・システムズ
114	ｶｰﾄﾞ発行ｼｽﾃﾑ	ｶｰﾄﾞﾌﾟﾘﾝﾀの販売・ｿﾌﾄｳｪｱの開発	株式会社D-WORK SOLUTION
115	受託発行	ｶｰﾄﾞ発行の受託処理	株式会社D-WORK SOLUTION
116	入退出管理ｼｽﾃﾑ	FCF の IC ｶｰﾄﾞ学生証を使用した、生徒の登下校を管理するｼｽﾃﾑ	株式会社ｻﾝ・ﾃﾞｰﾀｾﾝﾀｰ
117	警備システム	機械警備、鍵管理、入退室管理を一括管理するﾄｰﾀﾙｼｽﾃﾑを提供する。	キング通信工業株式会社
118	入退室管理ｼｽﾃﾑ	入退室管理ｼｽﾃﾑを提供する。	キング通信工業株式会社
119	TASKGUARD ID Printing	IC ｶｰﾄﾞ等を活用したﾌﾟﾘﾝﾀ・複合機の利用認証ｼｽﾃﾑ	京ｾﾗﾐﾀｼﾞｬﾊﾟﾝ株式会社
120	MiBeliCa Print	IC ｶｰﾄﾞを活用したｾｷｭｱﾌﾟﾘﾝﾄｼｽﾃﾑ	京ｾﾗﾐﾀｼﾞｬﾊﾟﾝ株式会社
121	出席管理ｼｽﾃﾑ	IC ｶｰﾄﾞ及びｲﾝﾃﾘｼﾞｪﾝﾄﾘｰﾀﾞｰをﾍﾞｰｽに構築したｷｬﾝﾊﾟｽ向け出席管理ｼｽﾃﾑ	株式会社蝶理コム
122	勤怠管理ｼｽﾃﾑ	IC ｶｰﾄﾞ及びｲﾝﾃﾘｼﾞｪﾝﾄﾘｰﾀﾞｰをﾍﾞｰｽに構築した企業及びｷｬ	株式会社蝶理コム

		ﾝﾊﾟｽ向け勤怠管理ｼｽﾃﾑ	
123	入退室管理ｼｽﾃﾑ	ICｶｰﾄﾞ及びｲﾝﾃﾘｼﾞｪﾝﾄﾘｰﾀﾞｰをﾍﾞｰｽに構築した企業及びｷｬﾝﾊﾟｽ向け入退室管理ｼｽﾃﾑ	株式会社蝶理コム
124	認証ﾌﾟﾘﾝﾄｼｽﾃﾑ	ICｶｰﾄﾞ及びｲﾝﾃﾘｼﾞｪﾝﾄﾘｰﾀﾞｰをﾍﾞｰｽに構築した企業及びｷｬﾝﾊﾟｽ向け認証ﾌﾟﾘﾝﾄｼｽﾃﾑ	株式会社蝶理コム
125	図書館ｶｳﾝﾀｰｻｰﾋﾞｽｼｽﾃﾑ	FeliCa を利用した図書館への入退管理、また図書貸出・返却ｻｰﾋﾞｽを提供する	株式会社シー・エム・エス
126	出欠管理ｼｽﾃﾑ	ICｶｰﾄﾞを利用して出席情報を取得。学生の動向変化を早期にｷｬｯﾁ、素早いﾌｫﾛｰにより休退学者の減少、目的意識向上を図ります。	株式会社SIGEL
127	ｷｬﾝﾊﾟｽｶｰﾄﾞ統合ｻｰﾋﾞｽ	ｷｬﾝﾊﾟｽｶｰﾄﾞﾌｫｰﾏｯﾄを利用した入退・出席、その他のｻｰﾋﾞｽを他社も含めてｷｬﾝﾊﾟｽ向けに統合して提供するｻｰﾋﾞｽ	（株）高見沢サイバネティックス
128	Ridoc IO Gate	印刷枚数上限の設定など、ﾌﾟﾘﾝﾀｰ管理業務の効率化を簡単に実現出来る統合ﾌﾟﾘﾝﾄ管理ｼｽﾃﾑ	ﾘｺｰITｿﾘｭｰｼｮﾝｽﾞ株式会社
129	IDｶｰﾄﾞ発行ｼｽﾃﾑ	社員証・学生証の受託発行ｻｰﾋﾞｽ	小林クリエイト株式会社
130	関連機器販売	FCF 関連機器の販売	小林クリエイト株式会社
131	関連ｼｽﾃﾑ販売	FCF 対応ｼｽﾃﾑの販売	小林クリエイト株式会社
132	出席管理ｼｽﾃﾑ	大学様向け FCF を用いた出席管理ｼｽﾃﾑ	株式会社ハイエレコン
133	教室端末予約ｼｽﾃﾑ	大学様向け FCF を用いた PC 教室端末の予約ｼｽﾃﾑ	株式会社ハイエレコン

C「登録業務効率化の検討」

－ 目　次 －

はじめに

この調査研究では、「社員等の属性情報を扱う電子認証（ID を含む）および電子署名にかかわる民間制度・基盤の確立およびその環境整備」の一環として、電子認証の基盤となる共通鍵および属性情報を記録媒体に効率的に登録するための登録フロー及びシステムの役割について調査し、マルチベンダー環境でも効率的かつ安全な PKI 情報の登録フローとそれに関わるシステムの役割につて検討した結果の報告を行うものである。

具体的には、「属性情報の連携方式に関する検討」として、電子証明書等のクレデンシャル発行のための登録業務の自動化を目的に、人事システム等と登録業務との属性情報の連携方式を検討し、まとめる。なお、方式には属性情報をマニュアル（CSV 等の利用）で連携する方法と自動（SAML 等の利用）で連携する方法を検討する。

尚、ここで扱う記録媒体及び登録方式については、別途調査研究を行っている「マルチユース記憶媒体の PKI 対応の検討」で検討された「JCAN パス」への情報登録を対象としているため、「マルチユース記憶媒体の PKI 対応の検討」に関する報告書も合わせて参照されたい。

1. 属性情報の連携方式に関する検討に向けて

この調査研究を行う上で重要な役割を持つのが、電子認証情報を格納するマルチユース格納媒体である。ここではこのマルチユース格納媒体について、社会的な普及度やデータのセキュリティ性など様々な角度から検討を行った。

1.1 JCANパス

格納媒体には様々種類があるが、ここで言う格納媒体は電子認証基盤として様々な認証サービスに利用できると言うものと言う共通の目的をもつことから、わかりやすく総称として「JCAN パス」と呼ぶこととする。

1.2 JCANパスの定義

JCAN パスは様々な認証基盤の利用を一つの媒体に集約化し、認証・決済・保存とシームレスに連携、ビジネスを効率よく効果的に行うものであり、機能としては以下を有するものである。

- ID 情報（従業員番号窯、学籍番号など）や電子証明書を利用するための情報を格納できる。
- 格納した情報には必要に応じて暗号化及び読み書きに必要な PIN 等のセキュリティを備えている。
- 情報は必要に応じて、いつでも書き換えができる。
- 必要に応じて後から情報の追加、削除が行える。
- 基本的なルールを守れば、誰でも実装情報を利用できる。

1.3 JCANパスとしての格納媒体

今回の検討では、格納媒体として非接触 IC カードとして、FeliCa カードと TypeA カード、さらに USB メモリを対象とするこになったが、本報告では、非接触 IC カードについて報告を行う。USB メモリにつては、今後の検討課題とする。

格納媒体の選択理由については、「マルチユース媒体への PKI 対応の検討に関する報告書」を参照されたい。

2. 情報格納フォーマット

JCAN パスの情報格納フォーマットは、「マルチユース媒体への PKI 対応の検討に関する報告書」で検討された。

2.1 JCANパス用共通フォーマット

格納媒体として FeliCa カードを利用する場合の JCAN パス用フォーマットは、FeliCa 共通利用フォーマット推進フォーラム（FCF）の提唱する共通フォーマットに準拠し、FCF の追加サービス C1 領域を JCAN パス用の電子証明書に関する PKI 情報を格納する領域と定義し実現する。

TypeA カード、USB メモリーについては、FCF のフォーマット構造を維持しながら、それぞれの格納媒体の特性を活かしたフォーマットを検討中であり、今後の実証実験等で開発・確認を行うこととする。

格納媒体の選択理由については、「マルチユース媒体への PKI 対応の検討に関する報告書」を参照されたい。

2.2 JCANパス用共通フォーマット仕様

電子証明書を実装した IC カードや USB メモリは既に何種類も存在する。その殆どが電子証明書自体（鍵情報や証明書情報など）を全て実装しているものが多い。また、実装方法は提供企業毎に独自の実装設計となっており、企業間で相互に利用はできない。

JCAN パスは、基本概念にあるように「基本的なルール」に従えば、どの企業でも認証情報を読み書きできなくてはならない。また、一定のセキュリティ基準も守る必要がある。さらに電子証明書だけではなく、様々な企業が提供する認証関連サービス等を利用できなければならない。

既存のシステムとの融和性と共通利用を考えると、JCAN パスも認証に必要な個人識別情報など共通で利用が可能な情報のみを必要最小限で登録する。

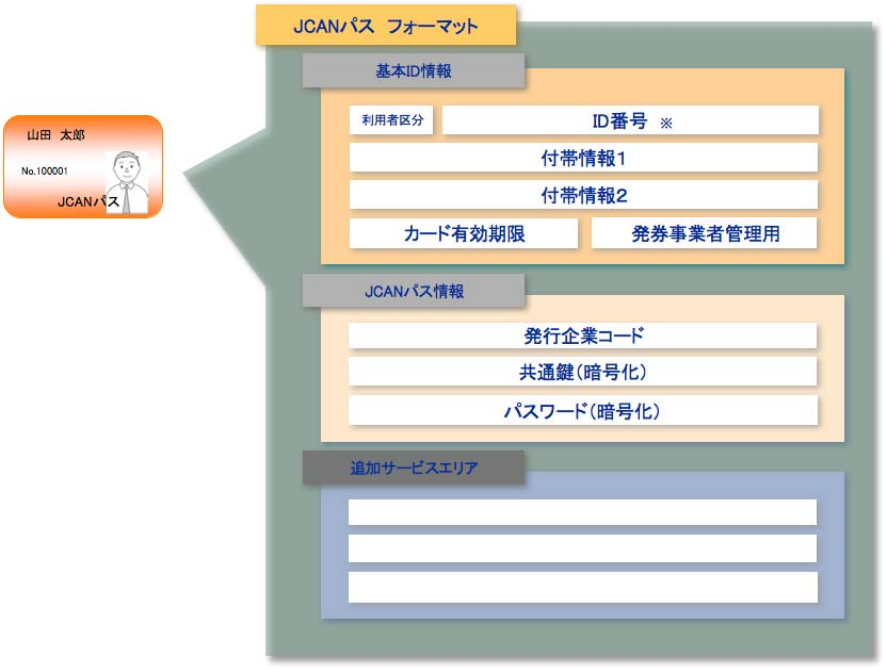


図 2-1　JCAN パスフォーマット（案）

【基本 ID 情報】

ブロック数：4 ブロック　Write キーあり　Read キーなし

利用者区分	：2Byte	正社員、派遣、嘱託、部外者など別途定める区分
ID 番号	：12Byte	社員番号・学生番号・会員番号など
付帯情報 1	：16Byte	必要に応じて所有者の名前など
付帯情報 2	：16Byte	必要に応じて所有者の所属など
カード有効期限	：8Byte	カード有効期限の西暦年月日（YYYYMMDD 半角数字）
発券事業者管理用	：8Byte	発券事業者において、案件ごとの識別情報を記入（自由形式）

【JCAN パス情報】

ブロック数：3 ブロック　Write キーあり　Read キーあり

発行企業コード	：16Byte	JCAN で定める企業コード
共通鍵	：16Byte	電子証明証の共通鍵（暗号化）
パスワード	：16Byte	JCAN パス認証パスワード（暗号化）

3. JCANパスの運用方法と情報管理システム

上記の JCAN パスへの情報登録を考える上で、登録業務だけを考えるれば良い訳ではない。JCAN パスの運用に関わる全ての処理について検討し、そのルールを定める必要がある。

ここでは、JCAN パスの発行から失効までの運用に処理フローを定義するとともに、そこで必要となる機能及び運用ルールについて検討した結果を報告する。

3.1 JCANパス発券フロー

ここではJCAN による電子証明書の発行からJCAN パスの発行までの処理の流れについての考え方を説明する。

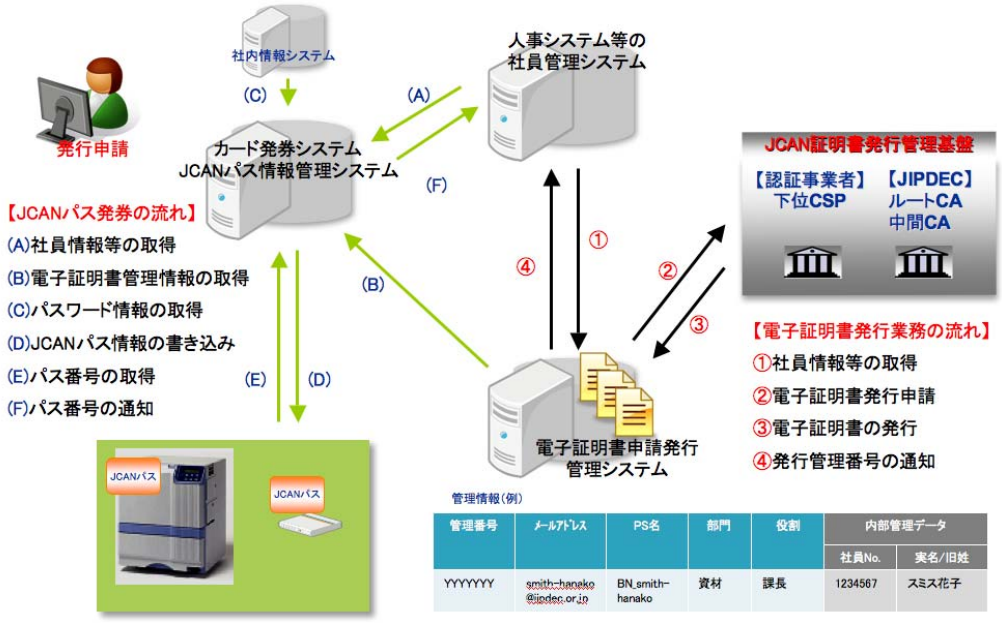


図 3-1　JCAN パスの発行フロー

図 4-1 はJCAN パスの発行フローを示したもので、黒矢印が電子証明書の発行に関する流れ、緑矢印が JCAN パスの発行に関する流れとなる。図にあるように発行処理には幾つかのシステムが連携して情報を扱うフローとなっている。これは既存システムとの連携や段階的なシステムの導入を可能にすることと、それぞれのシステムを複数の企業が構築でき、各システムの組み合わせを自由に行えるようにする事で、利用者にとっても、企業にとってもメリットがあるものにするためである。

多くの場合、企業では人事システム等の社員管理システムを有している。また、既に社員証の発行システムも導入している所もある。このような利用者には、システムを提供している企業がオプション機能として JCAN パスの発行機能を提供できれば、新規にシステムの導入を行うより、コストも時間も少なくて済むようになる。

JCAN 電子証明書の普及をはかるには、如何に安いコストで導入が出来るかが重要なポイントであると考えるからである。

3.2 情報管理と発行システム

ここではJCANパスを発行管理するためのシステムについて、その役割と機能概要について説明する。

3.2.1 電子証明書申請発行管理システム（仮称）

電子証明書申請発行システムは、JCAN 提供する電子証明書の申請・発行手続きを行うためのシステムで、人事システム等の社員情報管理システムと連携して、社員や部門の電子証明書の申請及び取得・管理が行える。

主な機能としては、申請機能、更新機能、データベース機能、失効機能、他システム連携機能等を提供するものと考えている。

JCANは、このシステムを開発するために必要な、CA（認証局）等とデータ交換をするためのAPI（Application Programming Interface)、人事情報を交換するためのAPI、管理DBフォーマットとそのAPIを提供する。提供する各種API仕様については、今後の検討課題とする。

3.2.2 JCANパス情報管理システム（仮称）

JCANパス情報管理システムは、JCANパス内のJCANパス情報エリアに情報を書き込むシステムで、カード発券システムのオプションとして機能するものである。

JCANは、このシステムを開発するために必要な、ID情報を元に電子証明書申請発行システムからJCANパス情報を取得するAPI、情報を暗号化するAPI、JCAN パスエリアへの書き込みを行うAPIを提供する。

JCAN パスエリアのアクセスにはアクセスキーが必要なため、このAPI が無いとJCANパスの発行は行えない。提供する各種API仕様については、今後の検討課題とする。

3.3 再発行フロー

ここでは、JCANパスを紛失した場合などのJCANパスの再発行処理の流れにつての考えを説明する。

図 4-2 は再発行フローを示したもので、基本的には発行処理と変わらないが、人事システム等の管理DBに再発行フラグが立つことと、カード毎に持つパス管理番号が変更されることで、紛失したカードが失効される処理が追加される。

具体的には、前項のJCANパス情報管理システムとカード発行システムにより再発行処理が行われる。

再発行については、紛失だけではなく、「身分」や「権限」、「所属」などの変更によっても行われるケースがあると考えるが、「2. JCANパスフォーマット」で説明したように、「身分」や

「権限」、「所属」などの変更がある情報は、パス情報としては扱わないことを原則とすれば、再発行処理行わず、各認証サービスで情報の更新をすることで対応できると考える。

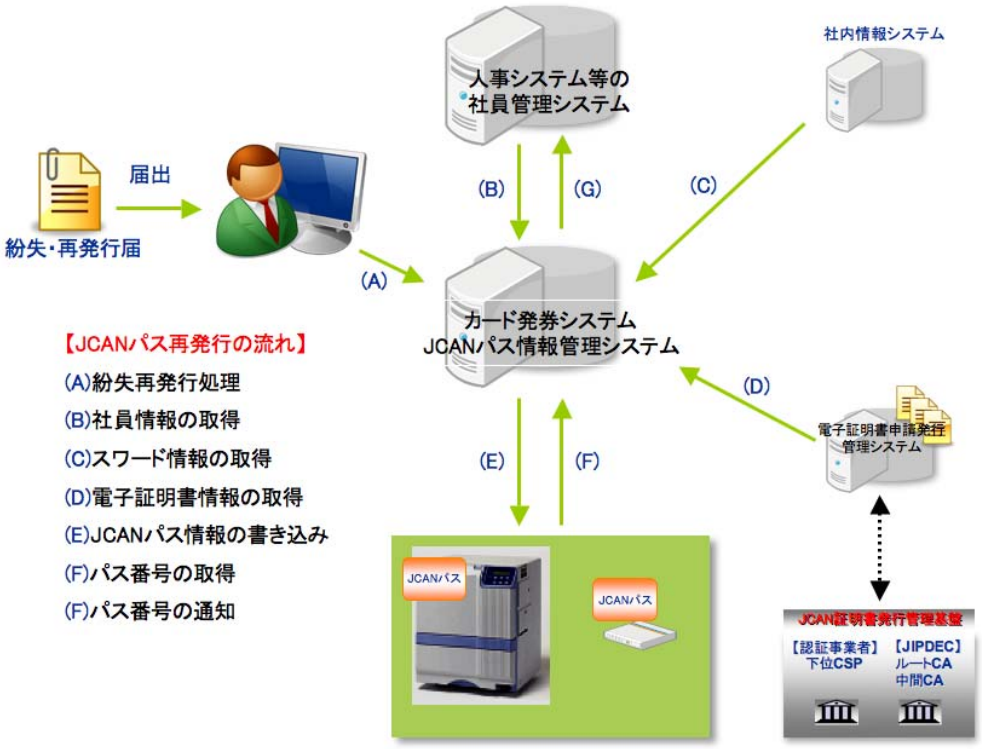


図 3-2　JCAN パス再発行フロー

3.4　失効フロー

ここでは、退職などにより JCAN パスを失効する場合の失効処理の流れにつての考えを説明する。

図 4-3 は失効フローを示したもので、人事システム等の管理 DB に失効フラグが立つことと、カード毎に持つパス管理番号がクリアされ、登録カードが失効される処理が行われる。

また、電子証明書申請発行管理システムに失効情報を通知し、CA（認証局）に対して証明書の失効（レポジトリ登録等）を依頼する。

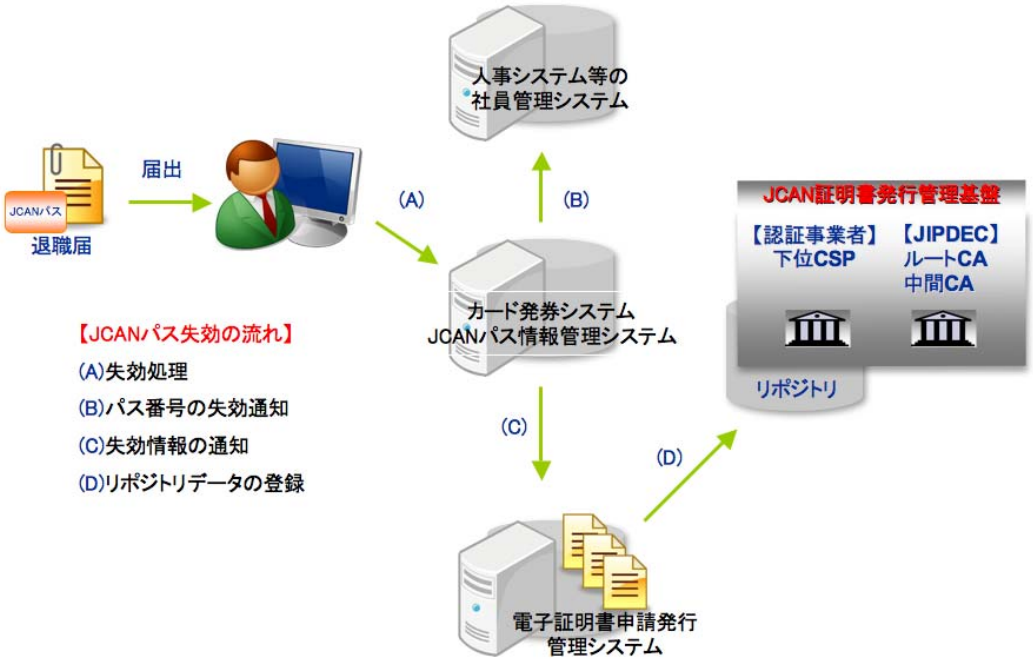


図 3-3　JCAN パス失効フロー

4. JCANパスの運用環境

JCAN パスへの情報登録管理については、上記で述べた通りであるが、各システムの詳細については、今後さらに検討を継続し詳細をつめる必要がある。さらにシステム利用に関するルールについても検討を進める必要がある。特に JCAN パスへの情報登録については、情報の扱い方に一定のルールが必要であり、このルールを守った上で、誰でもが簡単に情報のやり取りが出来るもので無くてはならない。

そこでシステムの仕様とともに、下記の２つの運用環境についても今後、検討する必要があると考えている。

4.1　登録関連システムの公認制度

前項で電子証明書申請発行管理システムや JCAN パス情報登録システムを開発するための API を JCAN が提供すると述べたが、この API を利用いてシステム開発を行うには JCAN が定める開発基準を満たした企業でなれればならない、さらに開発されたシステムは JCAN の示す品質基準をクリアしたて、公認されたものでなければ販売や使用は出来ないものとする。

理由は、JCAN パスに情報が書き込めると言う事は、故意的に同じ物を作りだす事ができると言う事でもあり、同じ JCAN パスが複数存在する可能性ができると言う事である。どんなにサービス側で対処を考えても、それを発行する側に問題があれば百々巡りとなりってしまい、

JCAN パスの信用が崩れることになる。このような状況を作り出さないためには、情報を書き込む際に、様々なルールを守らせる必要があると考える。

5. 今後の検討課題

以上、「登録業務効率化の検討」について、JCAN パスへの情報登録方法の検討結果を報告したが、具体的に JCAN パスを普及させるには、FeliCa カード以外の媒体についての JCAN パス共通フォーマットの検討、JCAN パスの運用ルールの検討、JCAN パスのためのアプリケーションインターフェースの検討など、今後も継続して行かなければならないと考える。特に下記の３点については、普及と運用管理のためには必須と考えるので考慮が必要である。

5.1 継続的な検討組織の確立

今回は４ヶ月と言う期間で電子証明証の活用を促進するための JCAN パスへの効率的な情報登録方法について検討をしてきたが、次年度の実証実験に向けて、まだまだ課題は多く残っている。特に既存の認証サービスとの融和性を持ちながら、電子証明書による認証サービスの普及を行うには、現実的に如何に簡単で安く利用できるかが焦点になると考える。また、利用者のみならず、認証サービスを提供する企業にとってもメリットのあるもので無くてはならない。この２つの点については、一企業や団体で進められるものではない。

これらの点を考慮して、継続的な検討組織の確立が急務であると考える。

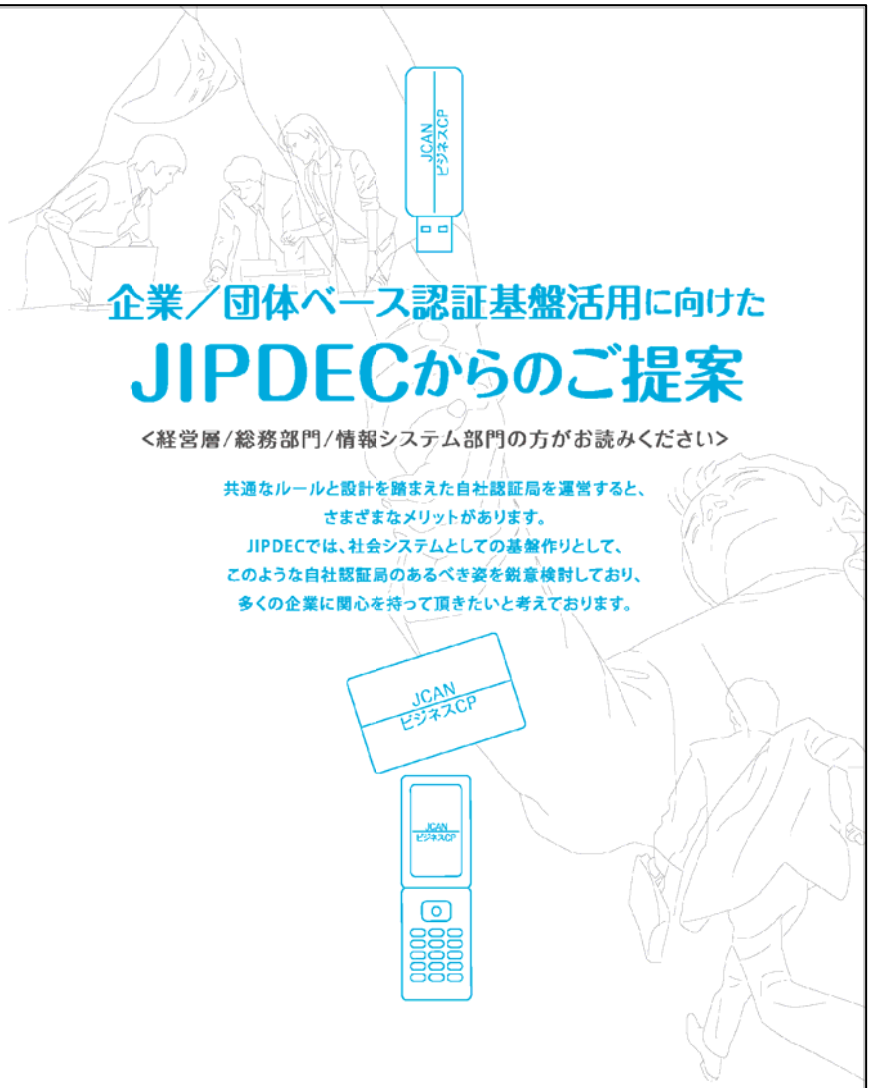
D「プロモーション冊子」

詳細は以下のURLをご覧ください

http://www.jipdec.or.jp/jcan

発行：財団法人日本情報処理開発協会（JIPDEC）JCAN準備プロジェクト
住所：〒105-0011東京都港区芝公園3丁目5番８号機械振興会館内
電話：03-3436-7513

2010年2月発行



企業／団体ベース認証基盤活用に向けた

JIPDECからのご提案

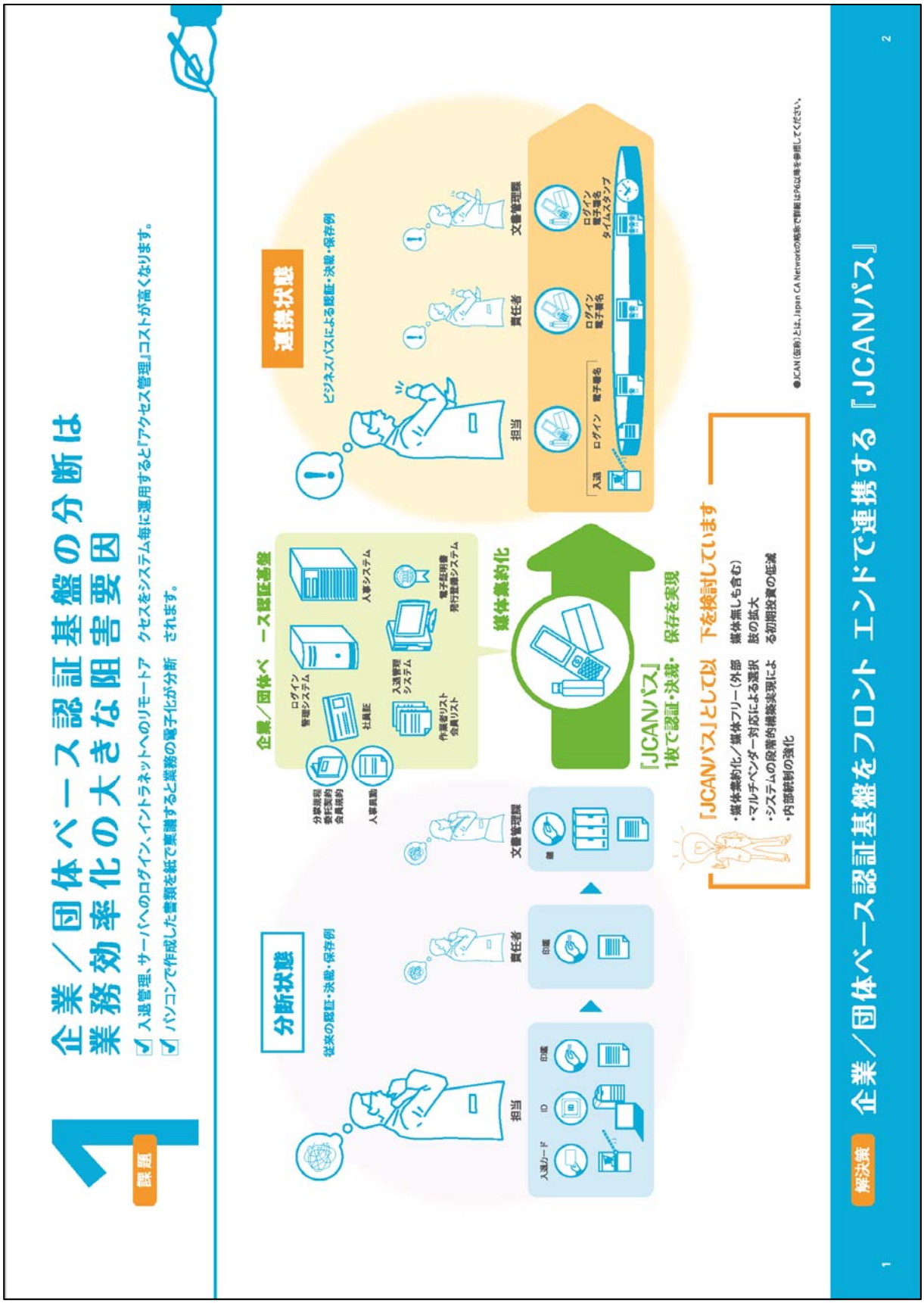
<経営層/総務部門/情報システム部門の方がお読みください>

共通なルールと設計を踏まえた自社認証局を運営すると、
さまざまなメリットがあります。
JIPDECでは、社会システムとしての基盤作りとして、
このような自社認証局のあるべき姿を鋭意検討しており、
多くの企業に関心を持って頂きたいと考えております。

2010年2月

財団法人日本情報処理開発協会（JIPDEC）

プロモーション冊子①（日本語版）　P1・P2



課題 2-1

企業／団体ベース認証　基盤を社会的 な仕組みに連携させると全体最適が生まれる

✓ 企業／団体ベースの認証基盤が社会基盤と連　携すると、取引先との業務効率化を促進します。

インターネットを介して行う情報交換には、企業／団体ドメインのメールアドレスを使うように、JCANの認定を取得した自社認証局から発行された電子署名／証明書を使うと、更に信頼されます。

社会的な仕　組み

有効性検証を行うに　は、ブラウザ等の「信頼　されたルート認証機　関」に登録されている　必要があります。

企業／団体

自社認証局

電子署名／証明書

会社が発信した電子メールのフィッシング対策が可能となります。

電子署名付き電子メール

消費者

電子認証

取引先

有効性検証

電子署名付き電子　メール・電子文書

保存

アクセス権限設定

Sausサービス
クラウドコンピューティング
共同利用システム

有効な取引情報として扱える電子署名付き電子メール・電子文書

●JCAN認定の自社認証局から発行され、かつその有効性が検証できる電子署名付きの電子メールや電子文書を使って情報交換を行うと、確かに当該企業の分掌に基づいて作成されたビジネス情報として扱うことができる。

共同利用システムの運用コスト削減

●例えば「販売会社」の電子証明書をそのままアクセス制御に使えるので、「メーカー」は、IDの発行業務が不要となりコスト削減ができる。

●電子署名には、改ざん検知等の機能があります。　●自社認証局とは、組織の認証基盤に基づく組織の構成メンバー及び役割等に電子証明書を発行する認証局　で、ここでは「企業認証局」及び「団体認証局」の総称として使います。

解決策 企業／団体ベース認証基盤を社会的 な仕組みにつなげる信頼の自社認証局

課題 2-2　自社認証局にすると付加価値が生まれる

✓ 証明責任が自社で閉じるので、改めて「本人確認」を行う作業が不要となります。

課題 3　相互に連携する認証基盤には第3者による信頼の裏付けが必要

✓ 取引先等に自社の内部統制を適切に行っていることを説明できることが重要です。

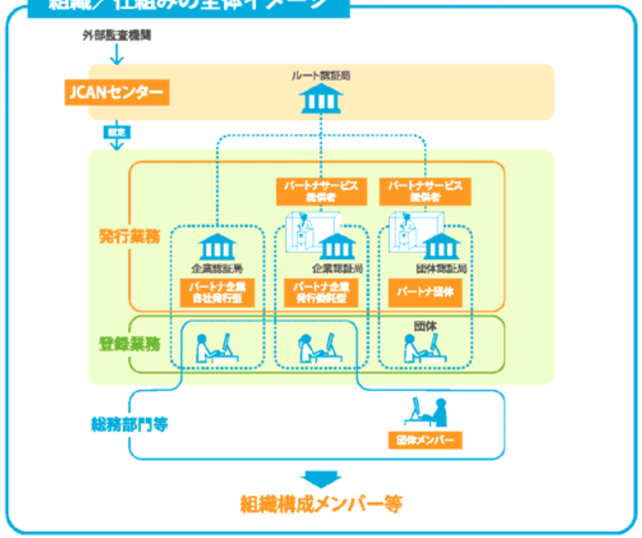
●内部統制では、分掌規程等に基づいた「アクセス管理」「決裁」「保存」が求められます。

こうした課題解決のための組織/仕組みとして JCANを提案します。

『JCANビジネスCP』
●JCANが規定する認証に関するルールの一つ
①「企業・団体が部門名或いは組織構成メンバーに電子証明書を発行する」を原則
②部門名或いは組織構成メンバーの登録は組織の総務部門等が実施
※企業・団体の審査はJCANまたはJCANが委託する者が実施

組織／仕組みの全体イメージ

●詳細は次頁を参照してください。



解決策　社会的な仕組みに連携した企業／団体ベース認証基盤で経営力アップ

まとめ

1 認証基盤をフロントエンドで連携する『JCANパス』

- 「入退管理システム」「ログイン管理システム」等の企業／団体ベース認証基盤は、そのまま『JCANパス』で連携できます。
- 『JCANパス』を使うと以下が可能となります。
  - ・媒体の集約化／媒体フリー（外部媒体無しも含む）
  - ・コスト削減につながるベンダー選択肢の拡大
  - ・初期投資を低減するシステムの段階的構築
  - ・内部統制の強化
- 『JCANパス』に社員証を券面印刷すると多目的な電子の社員証となります。

■JCANの電子署名／証明書は、企業内では電子認証、電子決裁、電子文書保存に、企業間では電子認証、電子メール、電子文書の署名に使えます。

2 企業ベース認証基盤を社会的な仕組みにつなげる信頼の自社認証局

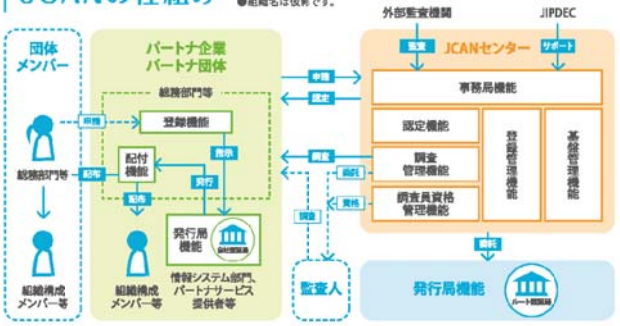
- 自社ドメインのメールアドレスのように、自社認証局は信頼の基本。さらに証明責任が自社で閉じるので迅速・低コスト・高信頼性への近道。
- ビジネス電子メールは電子署名付きがあたりまえに。
- 企業／団体ベース認証基盤が社会基盤と連携すると、取引先の業務効率化が進み、全体最適による利益が生まれます。

3 社会的な仕組みに連携した企業ベース認証基盤で経営力アップ

- 企業／団体ベース認証基盤に第3者による信頼の裏付けがあれば、自社の内部統制を適切に行っている証明になります。

JCANの仕組み

●組織名は仮称です。



●団体メンバーへの発行はパートナ団体が行います。

JCAN入会手続き

初回申請 ※基本合意書締結 → 会員（1年） → 更新申請（3ヶ月）

・登録業務：原則として書類調査（初回から2回目の更新までは実地調査を行います。）
・発行業務：書類調査及び実地調査

※両業務とも随時の実地調査を行う場合があります。
※自社認証局を認定パートナサービス提供者に委託している場合は発行業務の調査を行いません。

JCAN行程表（目標）

2009年12月 メールマガジン受付開始 → 2010年11月 入会手続き開始 → 2011年1月 パイロット運用スタート → 2012年4月 本格運用スタート

JIPDECからのお願い

メールマガジン登録のお願い

本冊子に掲載した課題解決のためには自社認証局を社会的な仕組みに連携するブラウザ等の「信頼されたルート認証機関」に登録されたルート認証局と接続させることが必要です。
このため、JCANはルート認証局等の基盤運用を含めた組織／仕組みの提供を検討しています。
詳細はメールマガジンでご案内いたしますので、以下のURLからのご登録をお待ちしております。

http://www.jipdec.or.jp/jcan

【JCAN情報】
・JCAN準備プロジェクトでの検討状況
・JCAN詳細情報（工程／手続き／組織）
・セミナー案内　等

関連プロジェクトのご紹介

～空気のように意識しないで使える「安信簡」情報環境～

●「安信簡」とは、安心・安全の「安」、信頼性の「信」、簡単・簡便の「簡」からなり、しばしばトレードオフの関係にある情報セキュリティと使い易さを、ともに向上させていこうという意味を込めた造語です。またその発音 は、安心感とも重なっています。

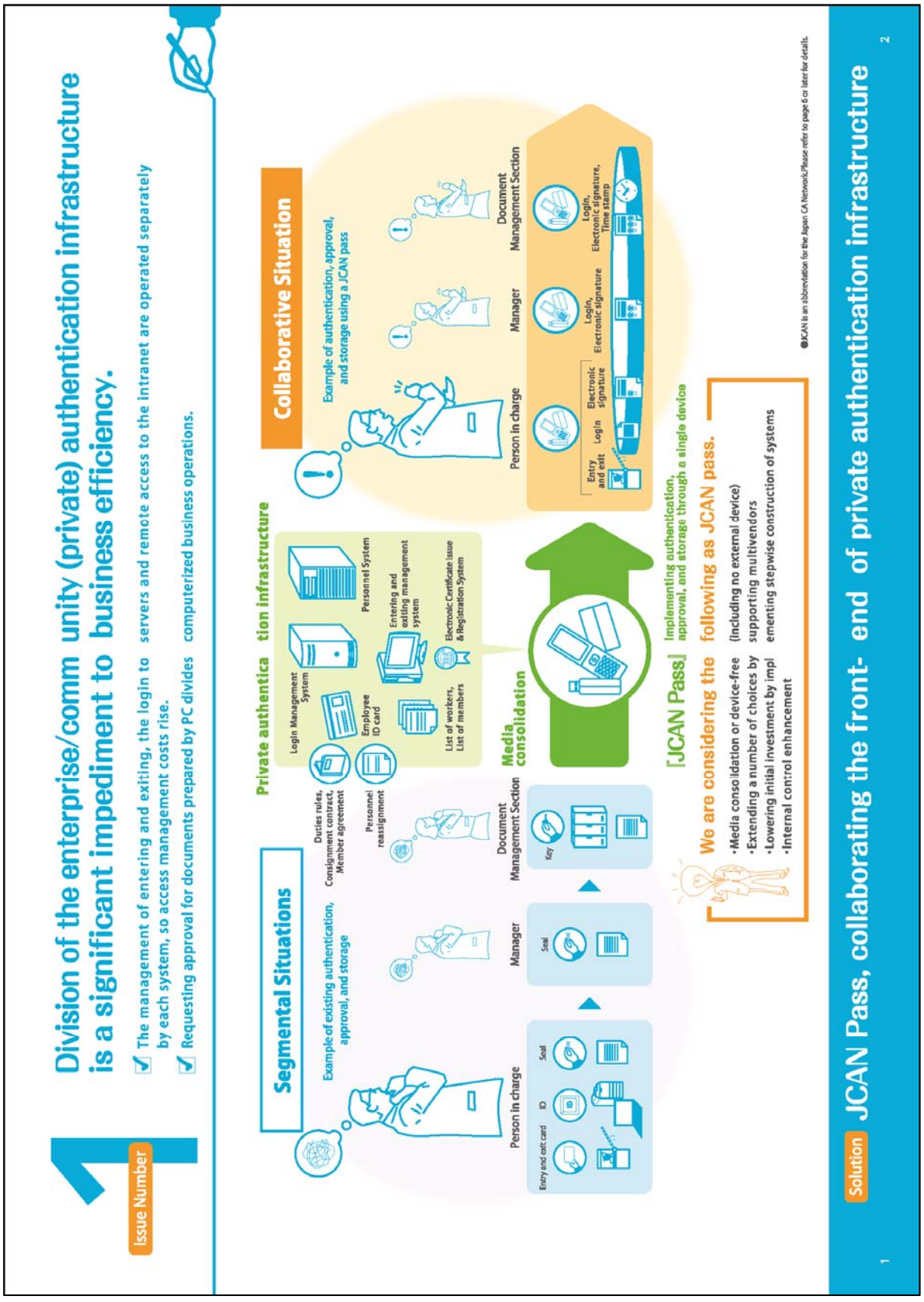
■急速に発展するインターネット社会も、ビジネス活動環境として見た場合、安心・安全面を裏打ちする社会的な基盤の強化が求められています。
情報化黎明期のおおらかさを残したインターネットの上で、適切な水準の安全性と信頼性を確保したビジネス活動環境を構築するためには、社会的なルールを伴った情報環境が必要であり、その整備が望まれます。しかし一方でそのような情報環境は、使いやすくストレスを感じさせないものでなければなりません。

■JIPDECでは、このような観点から、社会的な基盤として構築すべき4つの情報環境基盤を検討しています。

- ☑ 社会基盤との連携で付加価値を増す企業／団体ベース認証環境（JCAN）
- ☑ 確実な本人確認と個人情報保護を両立させ、C2B環境に画期をなす可能性を持つPS名(Pseudonym※)情報環境
- ☑ 信用に裏打ちされた既存の各種企業IDの連携環境
- ☑ 企業活動をオープンに結び付けるセキュアな双方向情報交換環境

※Pseudonymは擬名・仮名・別名と訳されることがありますが、適切な訳語が定まっていないため、PS名とします。

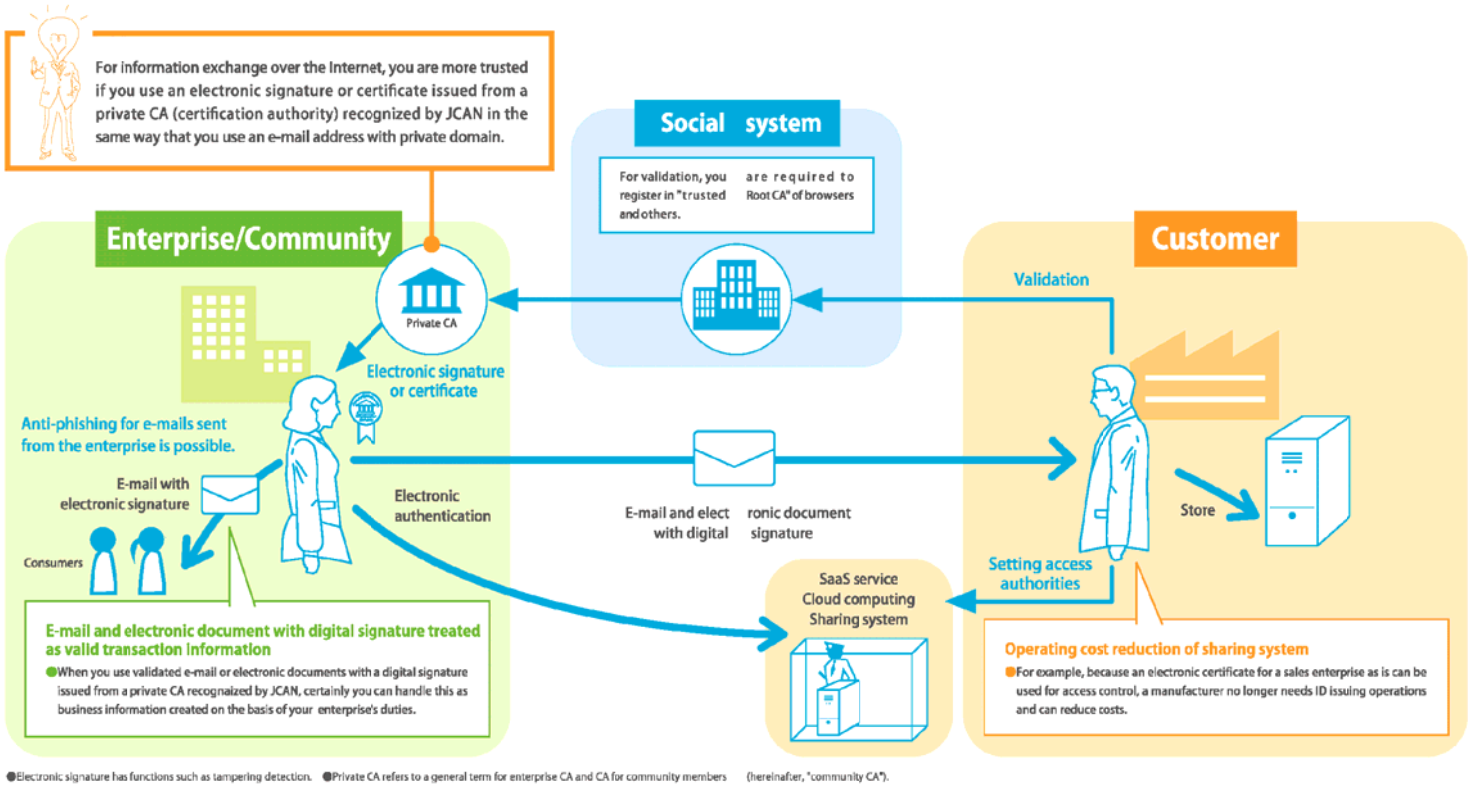
プロモーション冊子②（英語版）　表紙・裏表紙


Issue Number
Division of the enterprise/comm unity (private) authentication infrastructure is a significant impediment to business efficiency.
The management of entering and exiting, the login to by each system, so access management costs rise.
servers and remote access to the intranet are operated separately
Requesting approval for documents prepared by PC divides
computerized business operations.
Segmental Situations
Example of existing authentication, approval, and storage
Person in charge
Manager
Document Management Section
Duties rules, Consignment contract, Member agreement
Personnel reassignment
Private authentica tion infrastructure
Login Management System
Employee ID card
List of workers, List of members
Personnel System
Entering and exiting management system
Electronic-Certificate issue & Registration System
Media consolidation
Collaborative Situation
Example of authentication, approval, and storage using a JCAN pass
Person in charge
Manager
Document Management Section
Entry and exit
Login
Electronic signature
Login, Electronic signature
Login, Electronic signature, Time stamp
[JCAN Pass]
Implementing authentication, approval, and storage through a single device
We are considering the following as JCAN pass.
・Media consolidation or device-free (including no external device)
・Extending a number of choices by supporting multivendors
・Lowering initial investment by impl ementing stepwise construction of systems
・Internal control enhancement
●JCAN is an abbreviation for the Japan CA Network.Please refer to page 6 or later for details.
Solution
JCAN Pass, collaborating the front- end of private authentication infrastructure
1
2

Issue Number **2-1**

Collaboration of private authentication infrastructure with social systems would result in total optimization.

☑ When private authentication infrastructure collaborates with the social infrastructure is promoted.



●Electronic signature has functions such as tampering detection. ●Private CA refers to a general term for enterprise CA and CA for community members (hereinafter, "community CA").

Solution **Trusted private CA connects the private authentication infrastructure to social systems**

3

4

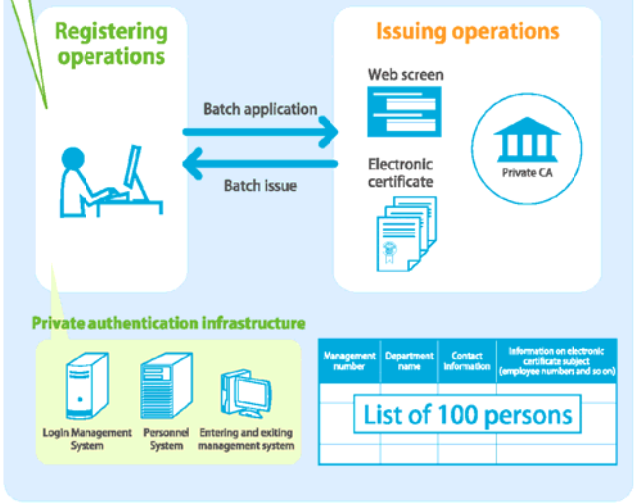
Issue Number 2-2

Private CA enables value added operations.

- [x] Identity verification would not be necessary because the responsibility for authentication is confined to the enterprise.

Speedy, low-cost, highly reliable registering operations

- Collaborating with an existing system, such as the personnel system, for instance, when a list of 100 persons in the table shown is sent to an issuing operation, all the electronic certificates can be issued at once.
- For instance, issued electronic certificate can be distributed by the following:
  - A person in the information system department stores an electronic certificate on an intranet server and allows an organization member to download it.
  - A person in the information system department stores an electronic certificate on the PC of an organization member.



Issue Number 3

Mutually collaborated private authentication infrastructure requires proof of trust from a third party.

- [x] It is important that one can explain to counterparties and others that internal control of the enterprise is executed appropriately.

● Internal controls require access management, approval, and storage based on rules of duties.

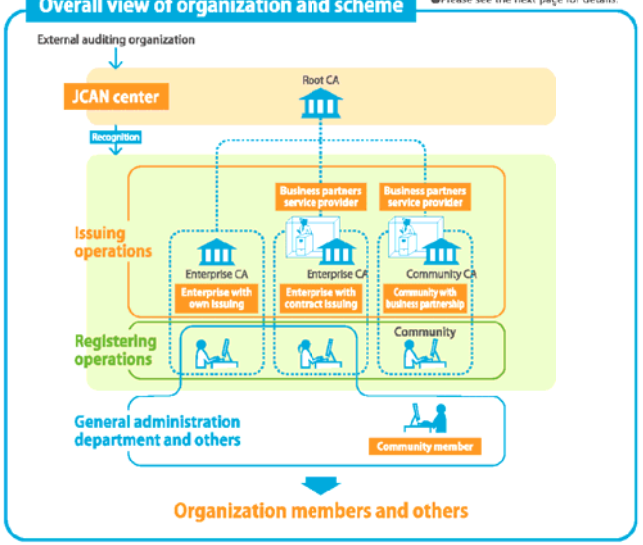
We propose JCAN as an organization and a scheme as a solution to the issues above.

『JCAN Business CP』

- One of the rules for authentication that JCAN stipulates.
- ①The rule makes "an enterprise or a community issues electronic certificates to department names or organization members" a principle.
- ②General administration department or other departments within an organization register department names or organization members.

※JCAN or a party commissioned by JCAN judges an enterprise or a community.

Overall view of organization and scheme ●Please see the next page for details.



Solution Private authentication infrastructure that collaborates with the social system would enhance the strength of management.

Summing it up...

1 JCAN Pass, collaborating front-end private authentication infrastructure

- Private authentication infrastructure such as the Entering and Exiting Management System, Login Management System, and others can collaborate directly with the JCAN Pass.
- The following would be possible using the JCAN Pass.
  - ・Media consolidation or device-free (including no external device)
  - ・Extending a number of choices of vendors, which may lead to cost reduction
  - ・Lowering the initial investment by implementing stepwise construction of systems
  - ・Internal control enhancement
- Printing Employee Identification on the face of the JCAN Pass would make an all-aspects electronic employee ID card.

■An electronic signature or certificate of JCAN can be used for electronic authentication, electronic approval, storing of electronic documents within an enterprise and electronic authentication, e-mail, and the signature for electronic documents between enterprises.

2 A trusted private CA that connects private authentication infrastructure to social systems

- A private CA is the basis for trust, like an e-mail address from the private domain. Because the responsibility for authentication is confined to the enterprise, such a private CA is a fast road to readiness, low costs, and high reliability.
- E-mail for business should normally have an electronic signature.
- When private authentication infrastructure collaborates with social systems, the business efficiency of counterparties is promoted and profits with total optimization would be produced.

3 With a private authentication infrastructure that collaborates with social systems, the strength of management would be enhanced.

- Trust from a third party for private authentication infrastructure would be proof that internal control of the enterprise is executed appropriately.

JCAN scheme

●The name of the organization is tentative.

External auditing organization　JIPDEC

Community member

Enterprise with business partnership, Community with business partnership

General administration department and others

Organization members and others

Application

Certification

Registering function

Distribution function

Issuing authority function

Information system department, business partners' system providers and others

Instruction

Issue

Confirmation

Organization members and others

Encryption

Decryption

Audit

JCAN center

Request

Office function

Recognition function

Research management function

Report

Collect

Evaluate

Research

Researcher qualification management function

Registering management function

Infrastructure management function

Consign

Issuing authority function

Root CA

Auditor

●Only a community with a business partnership issues certificates to community members.

JCAN admission procedure

Initial application

※memorandum of understanding

Membership (1 year)

Renewal application (3 months)

・Registering operations: documentary research in principle (Field research is conducted from the initial to the second renewal.)

・Issuing operation: documentary research and field research

※Occasional field research may be conducted for both operations.

※A research for issuing operations won't be conducted when a private CA is consigned to a recognized business partners service provider.

JCAN mile posts

Start accepting mail magazine requests December 2009

Start admission procedures November 2010

Start trial operations January 2011

Start full-scale operations April 2012

7

8

Request from JIPDEC

Request for signing up for mail magazine

To resolve issues stated in this brochure, a private CA should be connected to Root CA being registered in "trusted Root CA" of a browser and others that collaborates with social systems.
For the above reason, JCAN has considered providing an organization or scheme including infrastructure operations for the Root CA and others.
Details will be announced in our mail magazine. So please register for the mail magazine at the URL below.

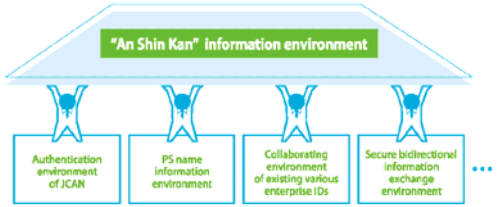
http://www.jipdec.or.jp/jcan

[JCAN information]

- The progress of discussions during the JCAN preliminary project
- Detailed JCAN information (schedule, procedures, organization)
- Seminar announcements and other news

A related project…

～"An Shin Kan"（安信簡）Information environment that can be used unintentionally like air～



●"An Shin Kan"（安信簡）is a coined Japanese word that consists of "An "（安）meaning "safe or security", "Shin"（信）meaning "trust," and "Kan"（簡）meaning "easy or simple." We gave the meaning to this word as we want to enhance both information security and ease of use that often have been in a trade-off relationship. Also "An Shin Kan"（安心感）using different characters, is an ordinary Japanese word meaning "relief".

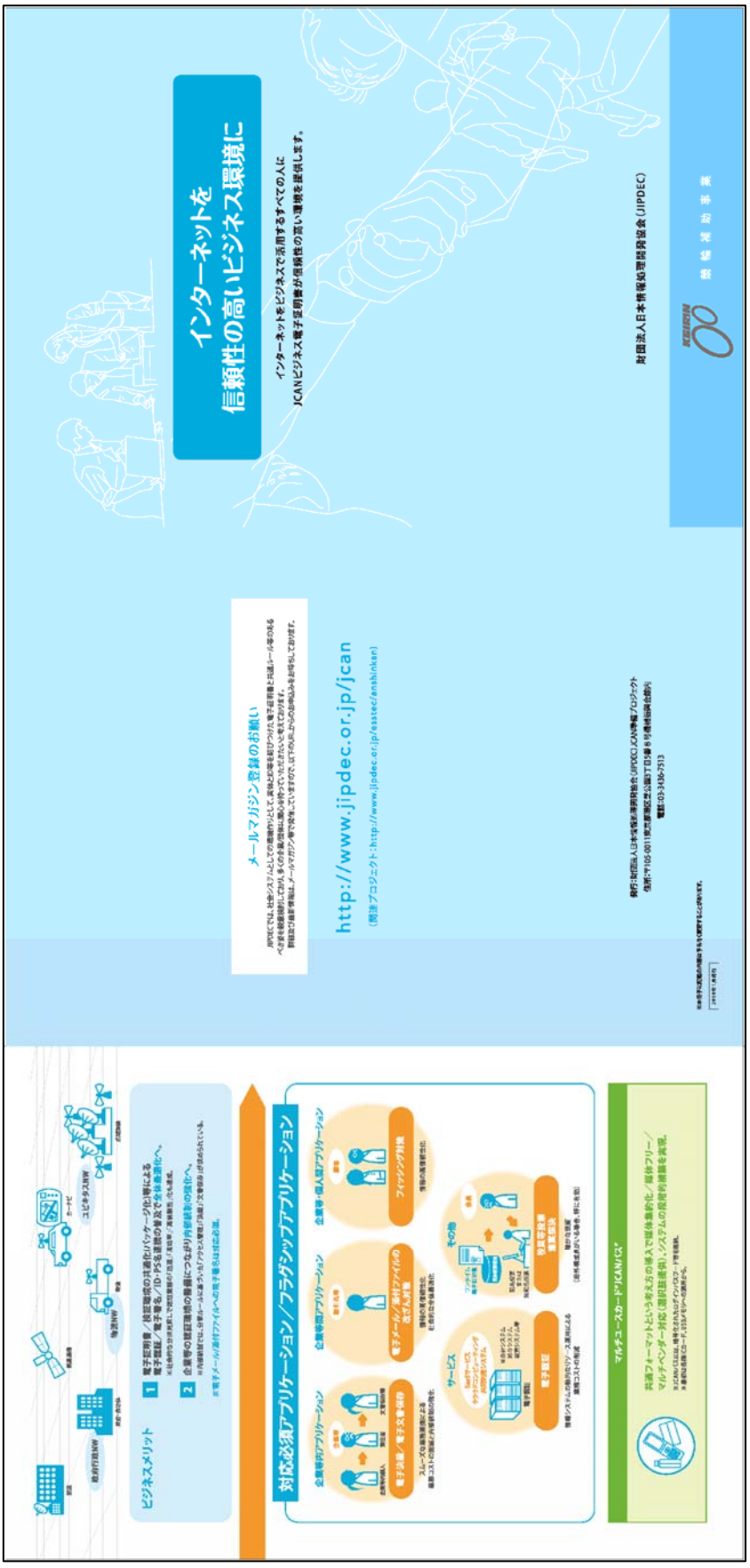
■From the viewpoint of the business activity environment, even a rapidly developing Internet society requires a strengthening of the social infrastructure that backs up ease and safety.
On the Internet with the remaining laid-back atmosphere of the earliest days of informatization, implementing a business environment that ensures the appropriate level of safety and trust requires an information environment with social rules and improvement of such an information environment is desirable. On the other hand, such an information environment must be easy to use and not stressful.

■From this viewpoint, JIPDEC has been considering four information environment infrastructures that should be implemented as social infrastructures.

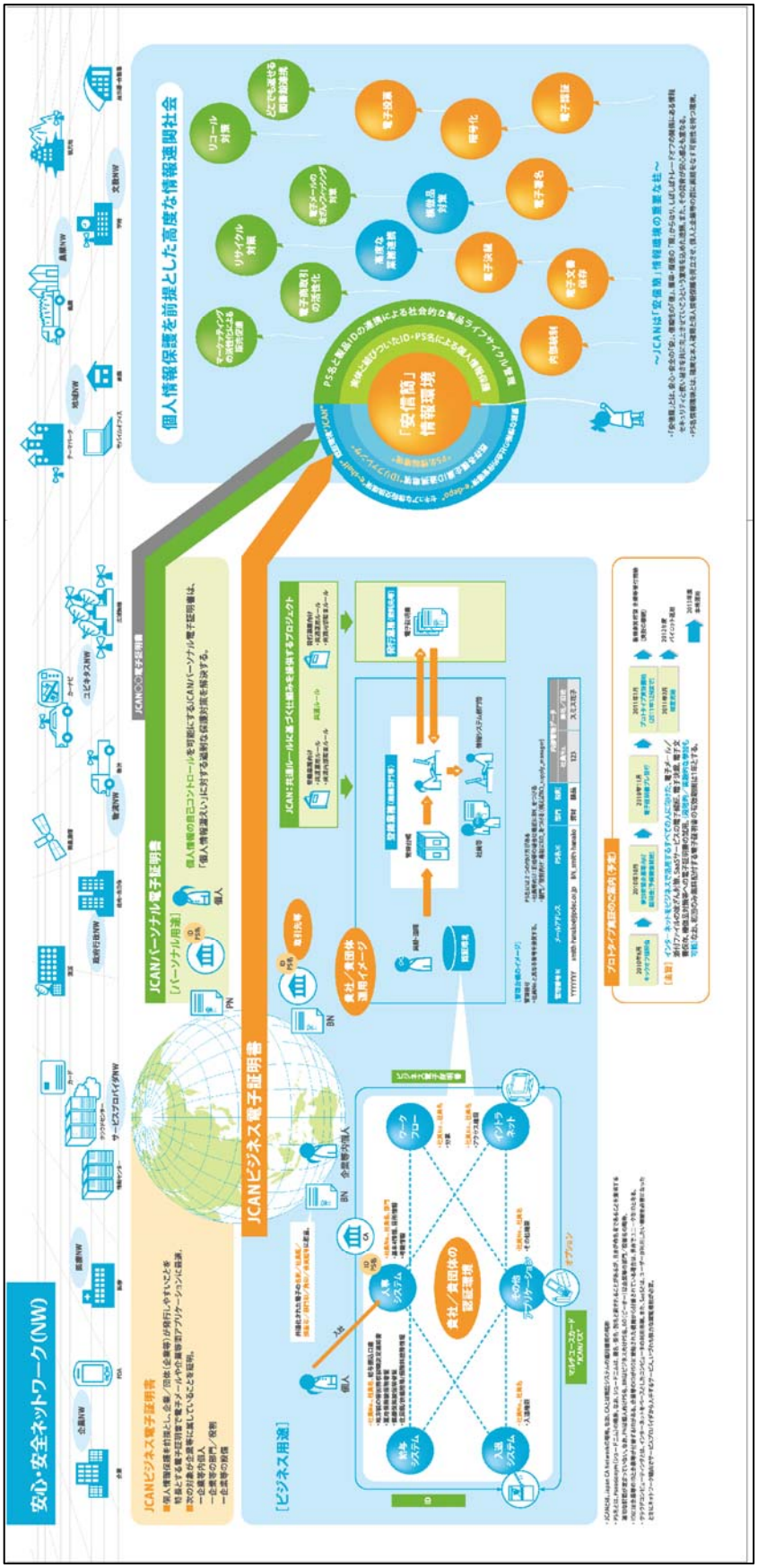
- ☑ Adding value to the enterprise authentication environment by collaborating with social systems (JCAN).
- ☑ PS name (pseudonym) information environment that satisfies both reliable identity verification and personal information protection with the possibility of an epoch-making C2B environment.
- ☑ Collaborating environment of existing enterprises IDs backed by trust.
- ☑ Secure bidirectional information exchange environment that would open up enterprise activities.

※Pseudonym may be translated into an anonymous false name or alias. Because an appropriate translation is not fixed, PS name will be used.

シンポジウム用パンフレット　表面



シンポジウム用パンフレット　中面



E「3000 社アンケート結果」

アンケート調査票

平成 22 年 1 月
財団法人日本情報処理開発協会

「自社認証局*の普及に関する調査」
アンケートご協力のお願い

拝啓 時下ますますご清栄のこととお慶び申し上げます。
平素は、当協会事業に格別のご協力を賜り厚く御礼申し上げます。

さて当協会は、政府、産業界をはじめとする各界の幅広いご支援･ご協力のもと、昭和 42 年の設立以来、公益的中立機関として、経済産業省をはじめとする国の情報化施策に協力し、わが国の情報化の進展に貢献すべく、情報信頼性確保、電子商取引等の推進に関わる事業を幅広く展開しております。

今般、「共通なルールと設計を踏まえた自社認証局を運営すると全体最適の観点から業務の効率化、コスト削減、内部統制の強化等さまざまなメリットがある」ことが検討結果から解り、このような認証局の普及に向けてアンケート調査を実施することになりました。

つきましては、ご多用中誠に恐縮に存じますが、**同封の冊子をお読みの上**、アンケート調査にご協力下さいますよう何卒よろしくお願い申し上げます。

敬具

【回答期限】　平成２２年１月２９日（金）　投函締切
【調査目的】　企業における電子署名の利用実態を明らかにする
【調査対象】　･社内の情報戦略企画部門責任者の方
　　･総務部門等の責任者の方
　　･情報システム部門等の責任者の方
【設問数】　全 24 問

《お問合せ先》
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
担当（野村）
〒105-0011　東京都港区芝公園 3-5-8　機械振興会館内
TEL：03-3436-7513
お問合せは平日 9:30～17:00　（※12:00～13:00 は除く）

*自社認証局とは、自社の名前で自社の社員等を認証する電子証明書を発行する認証局のことで、ここでは企業及び団体の認証局の総称として使います。

自社認証局の普及に関する調査

2010 年 1 月実施

1. 調査目的

本調査は、「共通なルールと設計を踏まえた自社認証局を運営すると全体最適の観点から業務の効率化、コスト削減、内部統制の強化等さまざまなメリット」があることから、このような認証局の普及に向けて財団法人日本情報処理開発協会（JIPDEC）が実施するものです。

2. 調査項目

本調査は、主に以下の項目に関してお伺いします。

- ·業務の電子化進展度合い
- ·電子署名/電子証明書の用途
- ·電子署名を利用したシステムやサービス等の利用状況

3. ご回答をお願いしたい方

本調査は、会社四季報から無作為に抽出した企業、及び電子取引に関係する団体の約 3 千社にお送りしております。

貴社において、情報システム·情報サービスの企画·導入に当たられる企画·総務部門や情報システム担当部門等の責任者の方のご回答をお願いいたします。

なお、異なる部門で受け取られた場合、お手数ですが、ご担当の部門にお回しください。

4. ご回答要領

- 設問は全部で 24 問です。
- ご回答は、該当する選択肢の番号に○を付けるか、欄内に具体的な数値や文章をご記入ください。（欄内では記入スペースが足りない場合は別紙に記載の上添付してください）
- **ご記入後は、本アンケートの 3～8 ページを同封の返信用封筒に入れ、1月29日（金）までにご投函下さるようにお願いいたします。**

5. その他

- 集計·分析に利用するのは、総計、平均等の代表値のみです。個票の内容は集計後破棄します。
- 本調査の目的についてご不明の点などございましたら、以下までお問合せください。

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
担当（野村）
〒105-0011　東京都港区芝公園 3-5-8　機械振興会館内
TEL：03-3436-7513
お問合せは平日 9:30～17:00（※12:00～13:00 は除く）

【業務の電子化進展度合い】

問 1　貴社･貴団体で管理しているPC、業務用サーバ及び対外公開用サーバの台数は何台ですか。正確な台数が不明の場合は概算でお答えください。所有、リースの別は問いません。

(1) PCの台数（＿＿＿＿＿＿）台
(2) 社内業務用サーバの台数（＿＿＿＿＿＿）台
(3) 対外公開用サーバの台数（＿＿＿＿＿＿）台

問 2　貴社･貴団体における情報システムインフラの整備状況に関して、すでに整備されているものを全てお選び（○をつけて）ください。[複数回答]

1. 構内 LAN
2. 拠点間 ERP
3. 電子メール（S/MIME 等）
4. 電子会議システム
5. VoIP（IP 電話）
6. ファイルサーバ
7. その他（具体的に　　）

問 3　貴社･貴団体における組織内情報･業務の電子化状況に関して、電子化されているものを全てお選びください。ASP サービス等の利用も含みます。[複数回答]

1. 在庫管理
2. 財務会計
3. 生産/サービス管理
4. ロジスティクス管理
5. 顧客管理
6. 教育システム
7. 入退室管理
8. 外部からのリモートログイン
9. 勤怠管理
10. 電子決裁/稟議
11. 図面管理
12. 電子文書保存･管理
13. その他（具体的に　　）

問 4　貴社･貴団体における外部との業務の電子化状況に関して、電子化されているものを全てお選びください。[複数回答]

1. 在庫管理
2. 財務会計
3. 生産/サービス管理
4. ロジスティクス管理
5. 顧客管理
6. 法人営業
7. 販売（ｲﾝﾀｰﾈｯﾄｼｮｯﾌﾟ含む）
8. マーケティング
9. 調達
10. 見積もり
11. 契約
12. その他（具体的に　　）

問 5　貴社･貴団体における業務の電子化に関して、想定している脅威を全てお選びください。[複数回答]

1. 情報漏えい
2. 情報改ざん
3. 情報システムの障害･停止
4. コストの増大
5. 生産性の低下
6. その他（具体的に　　）

問 6　貴社･貴団体の電子取引等に使う「企業コード」について全てお選びください。[複数回答]

1. 帝国データバンクのコードを持っている
2. CII 標準企業コードを持っている
3. JAN コードを持っている
4. わからない
5. その他（具体的に　　）

【電子署名/電子証明書の用途】

問 7　「電子署名/電子証明書」を使ったことがありますか。

1. 使っている
2. 検討したことがある
3. 使わないことになっている

問 8　問 7 で「3. 使わないことになっている」とお答えの方にお尋ねします。使わないことになっている理由を全てお選びください。［複数回答］

1. メリットがない
2. コストがかかりすぎる
3. 利用の仕方が複雑
4. 従来の紙の方が利便性が高い
5. 対応アプリケーションが無い
6. その他（具体的に　　）

問 9　問 7 で「1. 使っている」もしくは「2. 検討したことがある」とお答えの方にお尋ねします。

(1)「電子署名/電子証明書」が必要と思われた理由（検討中を含む）を全てお選びください。［複数回答］

1. 成りすましの防止･本人確認
2. 文書の改ざん防止
3. 情報漏えい防止
4. 否認防止
5. 顧客からの要請
6. 法律上の要請
7. 特にない
8. その他（具体的に　　）

(2)「電子署名/電子証明書」の格納媒体（検討中を含む）を全てお選びください。［複数回答］

1. IC カード
2. USB メモリー
3. PC の内部ディスク
4. その他（具体的に　　）

(3)「電子署名/電子証明書」の有効期間（検討中を含む）をお選びください。

1. 1 年
2. 2 年
3. 3 年
4. その他(具体的に　　)

(4)「電子署名/電子証明書」の発行元（検討中を含む）を全てお選びください。［複数回答］

1. 一般の認証局
2. 取引先･グループ会社
3. 自社
4. その他(具体的に　　)

(5) 「電子署名/電子証明書」の発行手続きの問題点（検討中を含む）に関して全てお選びください。[複数回答]

1. 手続きがわかりづらい
2. 手続きが煩雑
3. 手続きに時間がかかりすぎる
4. 提出書類が多い
5. 提出書類の形式チェックが厳しい
6. 証明書記載事項の設定が難しい
7. 窓口への一括発行をしてくれない
8. 配付方法が煩雑
9. インストールが難しい
10. コストがかかりすぎる
11. 特にない
12. その他（具体的に　　）

問 10　電子署名/電子証明書を配付したい対象者（検討中を含む）を全てお選びください。[複数回答]

1. 全社員等
2. 一部又は全部の代表者・役員
3. 一部又は全部の管理職
4. 一部又は全部の担当者
5. 一部又は全部の派遣者
6. 一部又は全部の取引先
7. 一部又は全部のグループ会社
8. その他（具体的に　　）

【業務における電子署名/電子証明書の利用状況】

問 11　電子署名/電子証明書を利用したアプリケーション等、貴社・貴団体としての利用実績や利用予定等についてお答えください。

	(a) 既に利用している	(b) 利用予定有り	(c) 利用予定無し	(d) 不明
(A) 電子証明書を用いたユーザ認証				
(B) S/MIME・PGP を利用した電子メール				
(C) 署名つき PDF 文書				
(D) SSL による Web サーバ認証				
(E) 電子証明書を用いた VPN				
(F) 電子文書の保存				
(G) ダウンロード元の認証（コードサイニング）				
(H) 電子商取引（企業間取引）				
(I) 電子商取引（企業対消費者）				
(J) その他（具体的に：　　）				

問 15

問 12　問 11 で(a)を選択した項目についてお尋ねします。貴社・貴団体で利用した電子署名/電子証明書を利用したアプリケーションが、業務の効率化・コスト削減等の観点から、貴社・貴団体の業務にどの程度有効であったかについて、それぞれご回答ください（相当するところに○を記入）。[複数回答]

	(a) 非常に有効	(b) まあまあ有効	(c) あまり有効でない	(d) 全く有効でない
(A) 電子証明書を用いたユーザ認証				
(B) S/MIME･PGP を利用した電子メール				
(C) 署名つき PDF 文書				
(D) SSL による Web サーバ認証				
(E) 電子証明書を用いた VPN				
(F) 電子文書の保存				
(G) ダウンロード元の認証（コードサイニング）				
(H) 電子商取引（企業間取引）				
(I) 電子商取引（企業対消費者）				
(J) その他（具体的に: ）				

問 14

問 13　問 12 で(a)または(b)を 1 つでも選択した方にお尋ねします。電子署名/電子証明書を利用したアプリケーションが有効である理由を全てお選びください。[複数回答]

1. 利便性が高い
2. コストが削減できた
3. 売り上げが増加した
4. 安全性･信頼性が高まった
5. 利用の仕方が簡単
6. わからない
7. その他（具体的に　　）

問 14　問 12 で(c)または(d)を 1 つでも選択した方にお尋ねします。電子署名/電子証明書を利用したアプリケーションが有効でない理由を全てお選びください。。[複数回答]

1. メリットがない
2. コストがかかりすぎる
3. 利用の仕方が複雑
4. 従来の紙の方が利便性が高い
5. 対応アプリケーションが無い
6. その他（具体的に　　）

問 15　問 11 で(b)(c)(d)を選択した方にお尋ねします。もし電子署名/電子証明書が利用できれば何に使いますか全てお選びください。[複数回答]

1. 電子証明書を用いたユーザ認証
2. S/MIME を利用した電子ﾒｰﾙ
3. 署名つき PDF 文書
4. 署名付きワード/エクセル文書
5. SSL による Web サーバ認証
6. 電子証明書を用いた VPN
7. 電子文書の保存
8. ダウンロード元の認証（コードサイニング）
9. 電子商取引（企業間取引）
10. 電子商取引（企業対消費者）
11. わからない
12. その他（具体的に　　）

【冊子について】

問 16　添付した冊子の内容について全てお選びください。[複数回答]

1. だいたい理解できた
2. あまり理解できない　（該当箇所　　）
3. まったく理解できない
4. 意見がある　（該当箇所　　）

問 17　貴団体にお尋ねします。貴団体の会員メンバーであることの電子の証明書として、或いは情報共有の手段、業務ＩＴ化の支援として貴団体から貴団体の会員メンバー等へ電子署名/電子証明書を発行することについてお尋ねします。[複数回答]

1. 実施したい
2. 検討できる
3. 興味がある
4. その他（具体的に　　）

問 18　冊子の中の自社の認証局についてお尋ねします。

(1) 自社で認証局を持つメリットを全てお選びください。。[複数回答]

1. 人事システムなど既にある社員等のリストに基づいて電子署名/電子証明書を発行できるので改めて本人確認を行う作業が不要となる。
2. 自社ドメインのメールアドレスを使うように自社発行の電子署名/電子証明書は信頼される。
3. わからない
4. その他（具体的に　　）

(2) 自社で認証局を持つデメリットを全てお選びください。[複数回答]

1. コストがかかりすぎる
2. 利用の仕方が複雑
3. その他（具体的に　　）

(3) 自社の認証局の所有についてお尋ねします。

1. コストが妥当で有れば所有したい（おおよその予算　　万円）
2. 所属している団体から発行を受けたい（想定団体名　　）
3. その他（具体的に　　）

【企業属性】

Ｆ１ 貴社･貴団体が属する業種をお答えください。[当てはまるもの１つのみ]

1. 農林漁業･鉱業
2. 建設業
3. 製造業（品目：　　）
4. 電気･ガス･熱供給･水道業
5. 情報通信業
6. 運輸業
7. 卸売･小売業
8. 金融･保険業
9. 不動産業
10. 飲食店、宿泊業
11. 医療、福祉
12. 教育、学習支援業
13. その他のサービス業
14. 上記以外

Ｆ２ 貴社･貴団体の社員等人数をお答えください。　□□□□□□ 人

Ｆ３ 貴社の資本金をお答えください。　□□□□□□□ 百万円

Ｆ４ 貴社の直近年度の売上高※をお答えください。　□□□□□□□ 百万円

※貴社平成 20 会計年度における売上高。

Ｆ５ プライバシーマークについてお答えください。

1. 取得している　　2. 取得していない

Ｆ６ ＩＳＭＳについてお答えください。

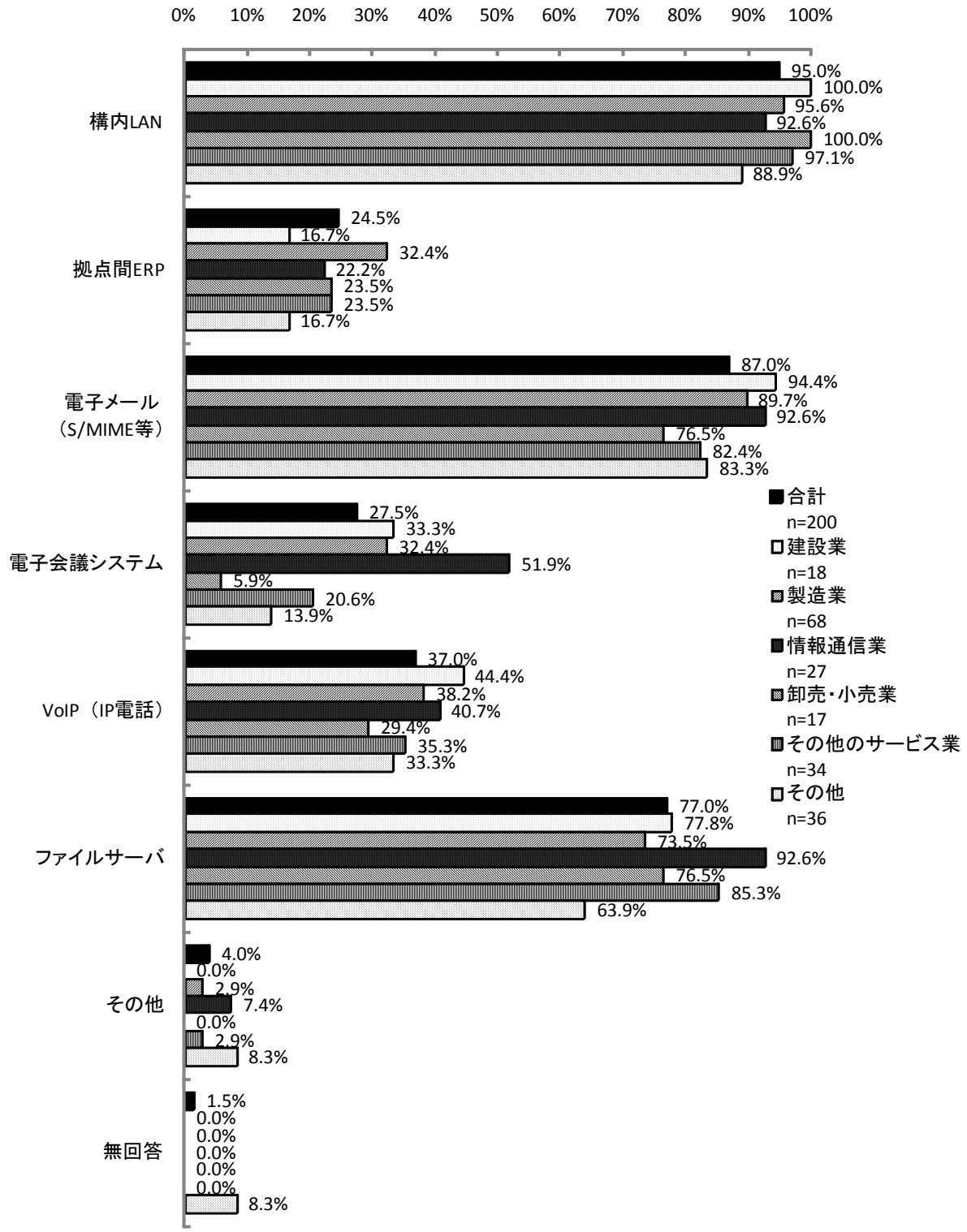
1. 取得している　　2. 取得していない

－ 設問は以上です。ご回答ありがとうございました －

貴社･貴団体名	
ご回答者部門名	
電話番号（内線）	

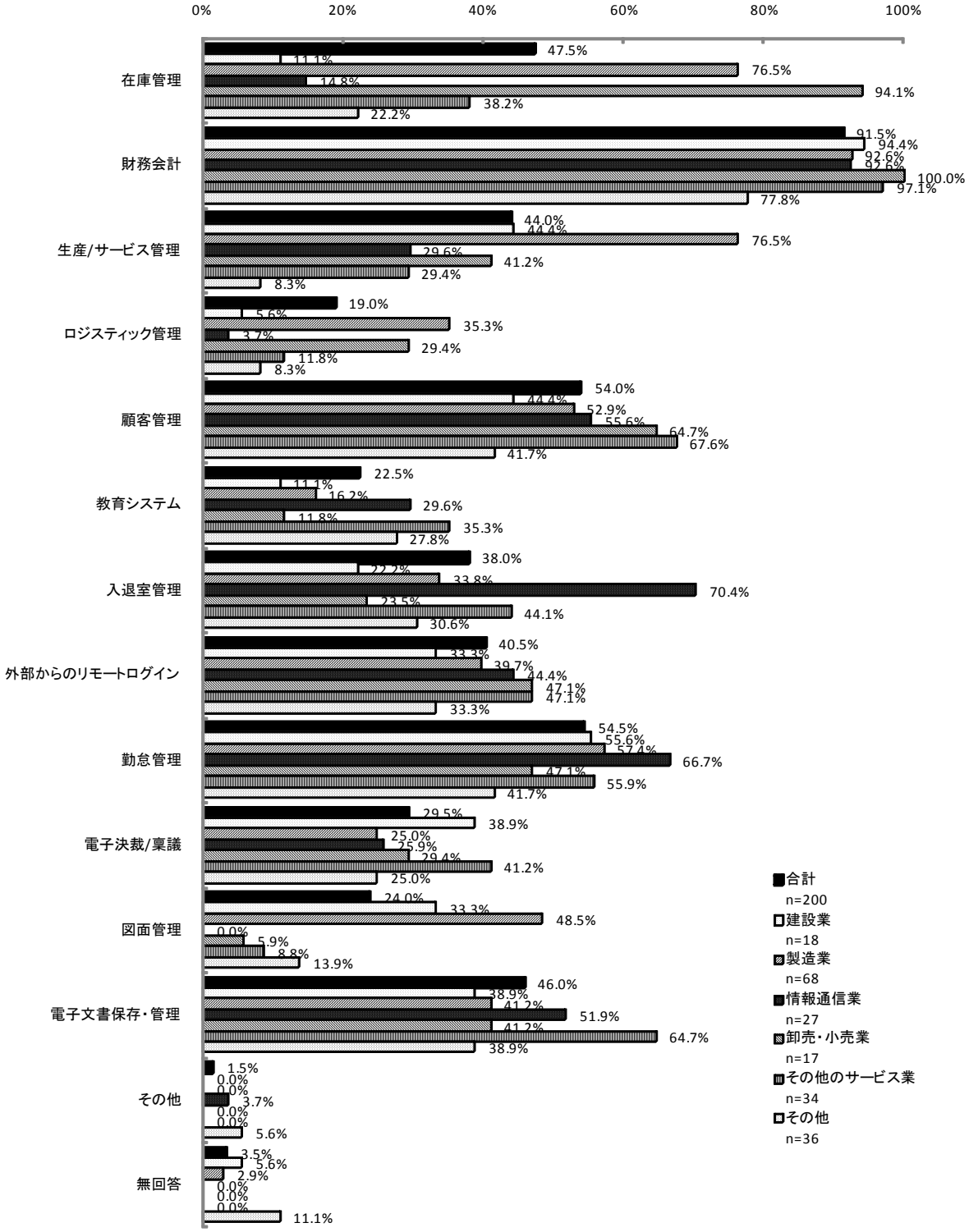
1 情報システムインフラの整備状況

社内の情報システムインフラの整備状況は、社内 LAN、電子メール、ファイルサーバの設置は業種によらずほとんど導入されている。しかしながら平成 19 年度の調査に比べると電子メール及びファイルサーバについては 10 ポイントほど減少している。その理由は定かではないが、自社ではなく、ネットワークを介した外部環境の利用も考えられる。



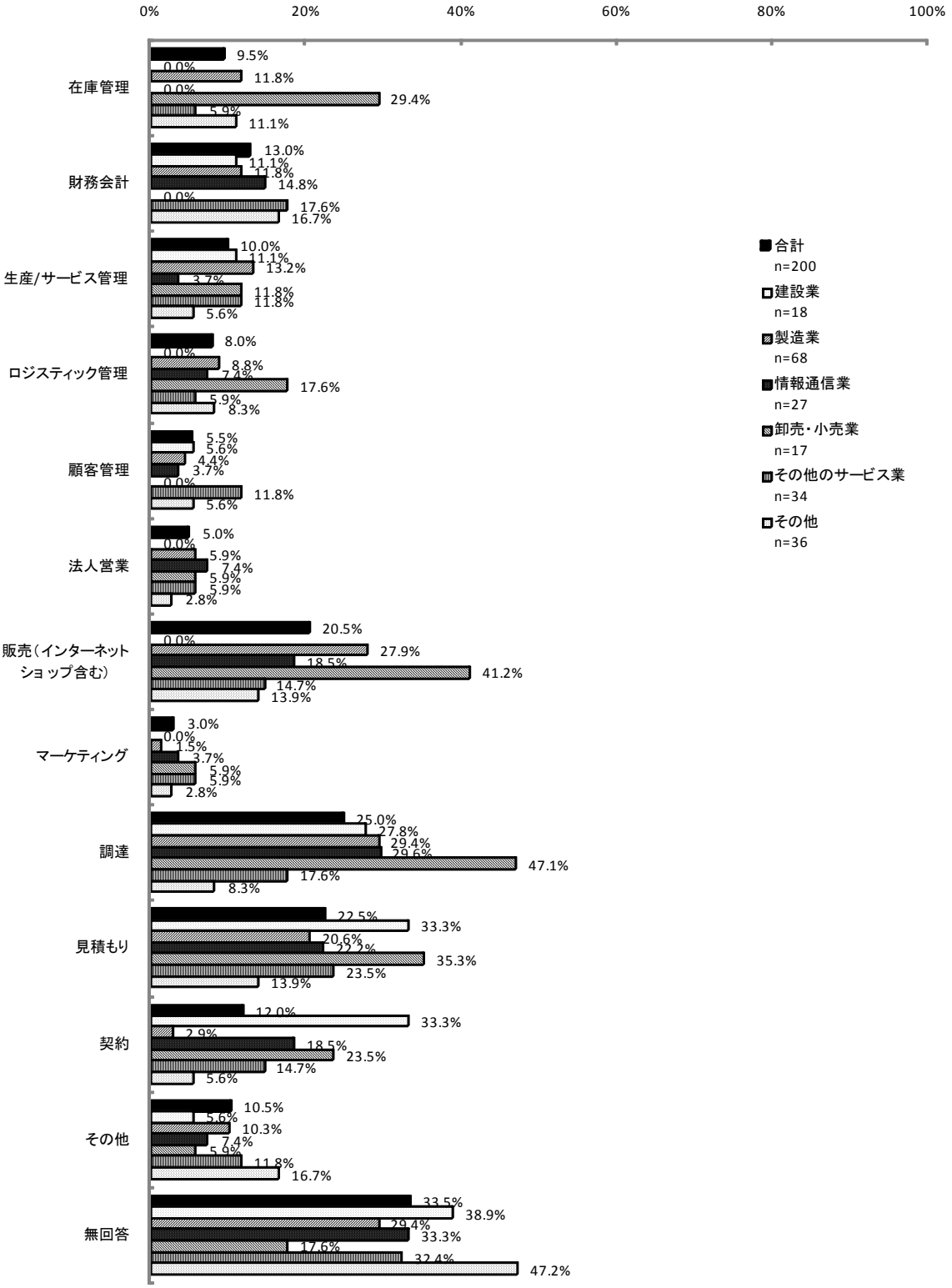
2 組織内情報・業務の電子化状況

社内情報・業務の電子化状況は、財務会計などの業種依存性が低いものと、在庫管理や図面管理などのきわめて業種依存性の高いものに分けることが出来る。業種依存性が低いものでもそれぞれの電子化状況に差がある。財務会計が 9 割近いが、電子文書保存・管理、電子決裁、入退室管理は半数近くは電子化されておらず、ひとつの会社でデジタルとアナログが混在している状況がわかる。効率や生産を高めるに総合的運用が望まれると考えられる。



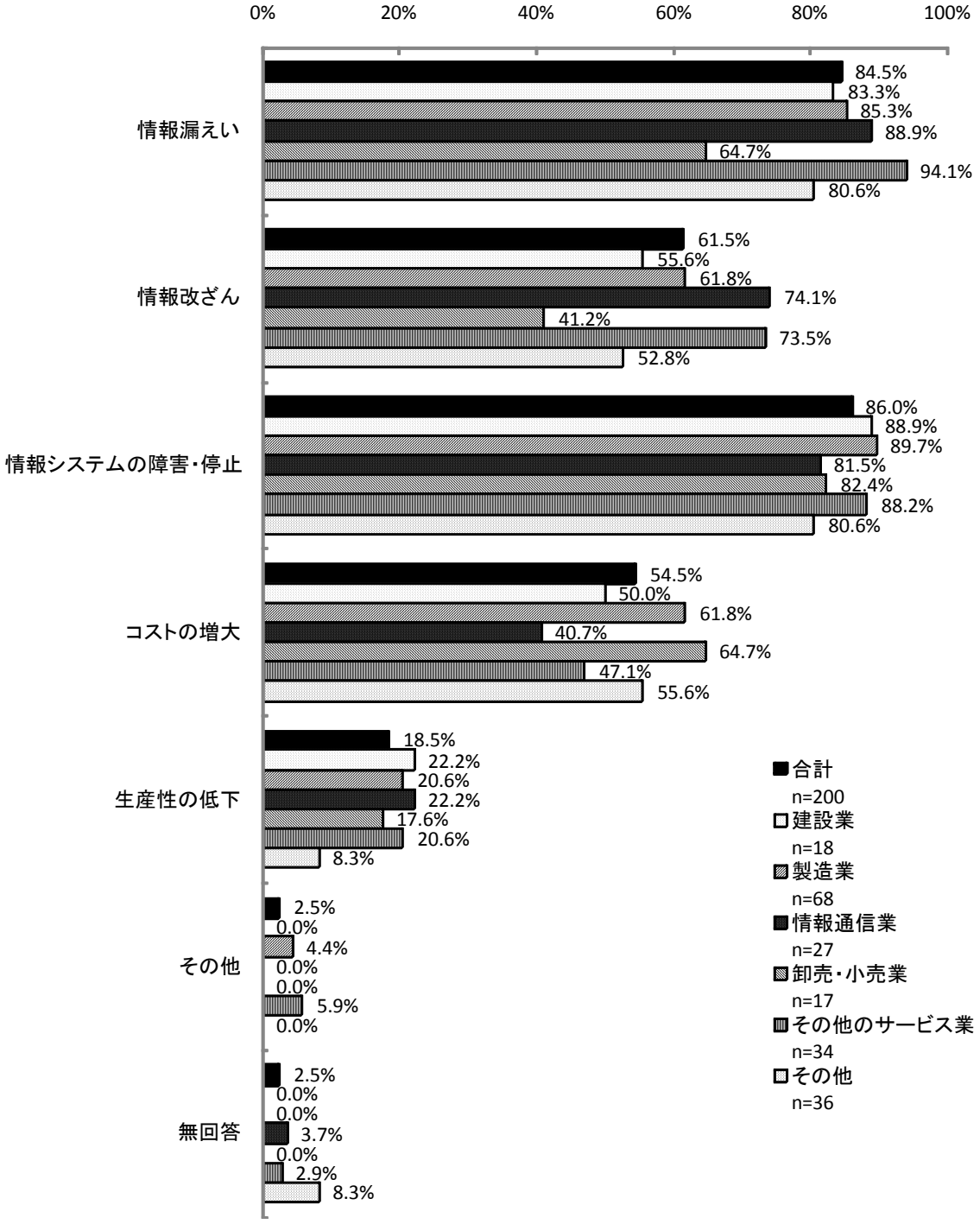
3 社外との業務の電子化状況

社内業務の電子化に比較して、社外とのやり取りについて電子化は進んでいない。普及度が比較的高いのは調達、販売、見積もりである。企業活動の促進及び効率化を促進させるためには他社を含めた情報基盤の統合が必要と考えられる。



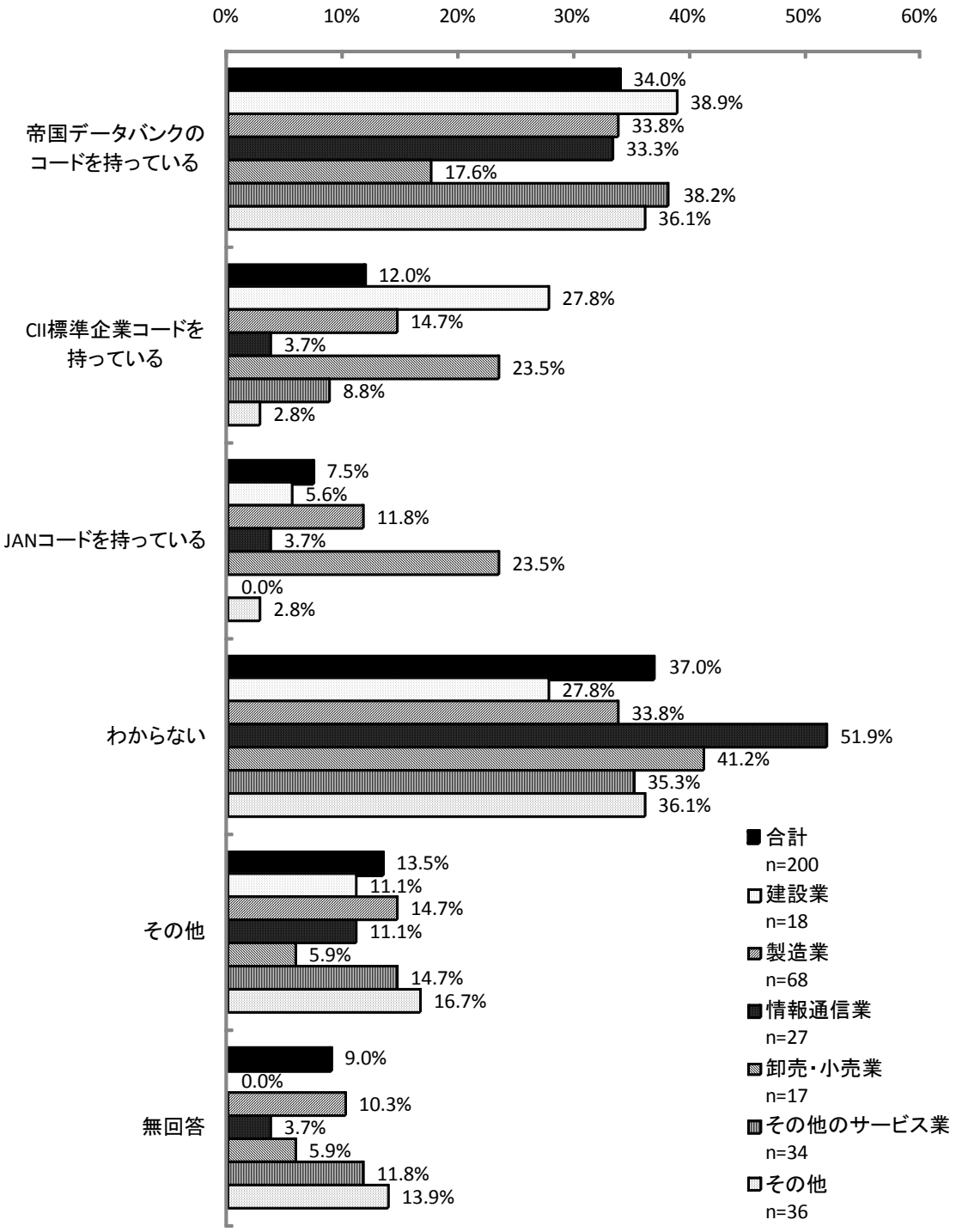
4　業務の電子化に関して想定している脅威

想定される脅威は、情報システムの障害・停止、情報漏えい、情報改ざんは合計で見ると半数以上が脅威と考えている。



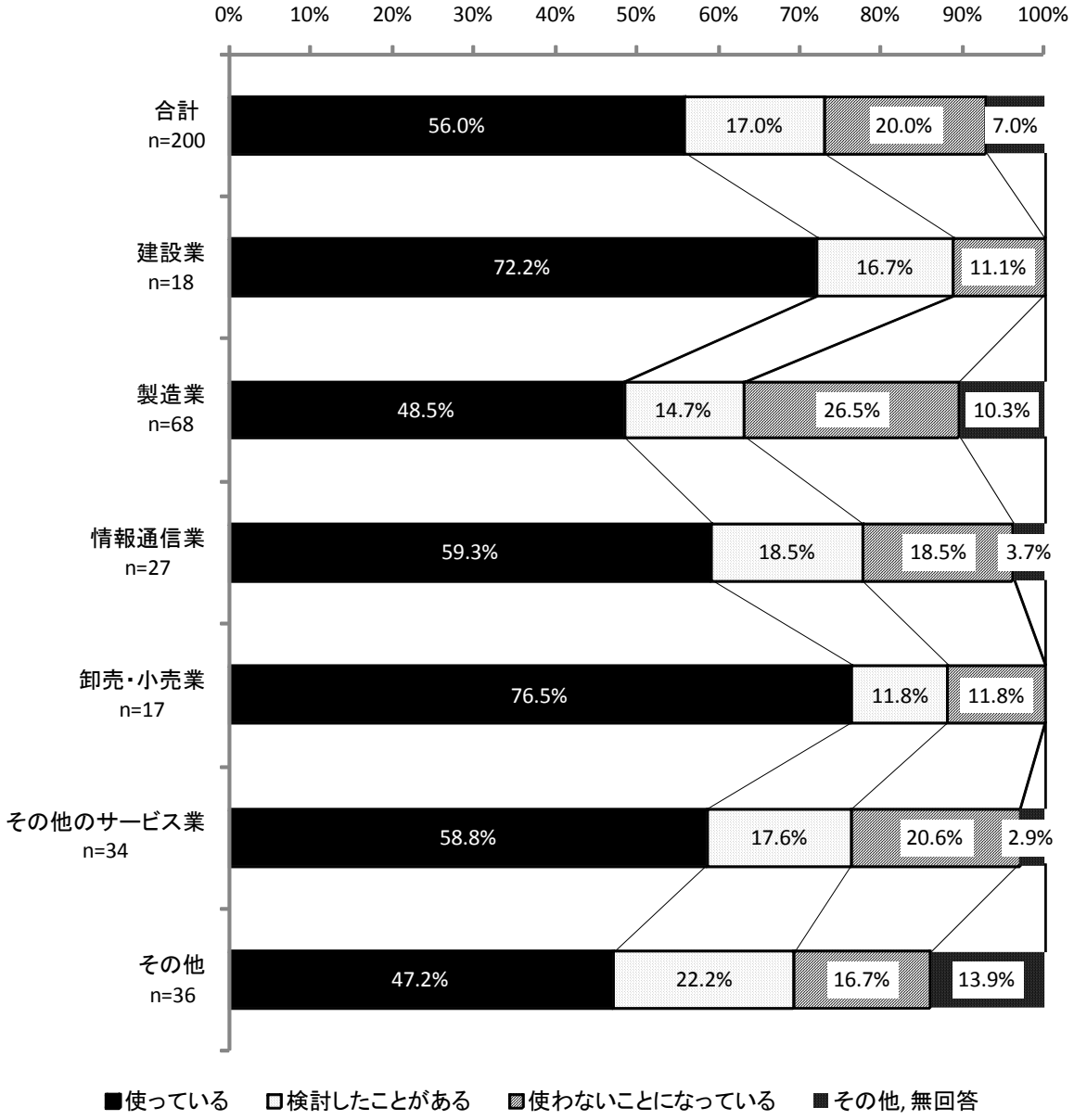
5　企業コードの所有率

企業コードについては 3 割近くが帝国データバンクのコードを持っている一方で、わからないと答えた企業が 3 割ほどある。自社の企業コードを認識していないことから、コードを利用した業務は少ないと思われる。



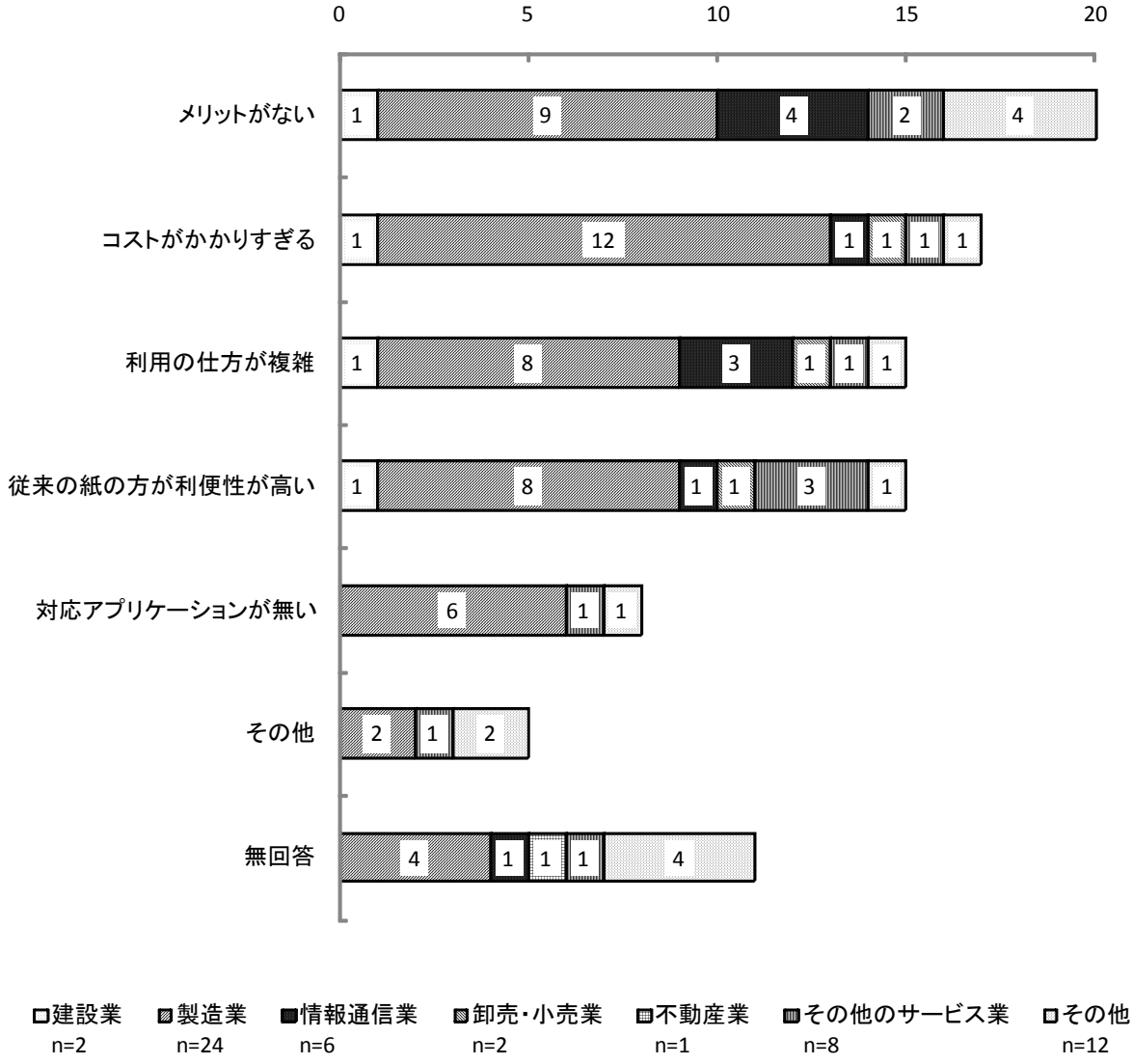
6　電子署名/電子証明書の利用状況

電子署名/電子証明書の利用はどの業種ともほぼ半数近くの企業が利用していることがわかる。建設業と卸売・小売業においては 7 割を超えている。



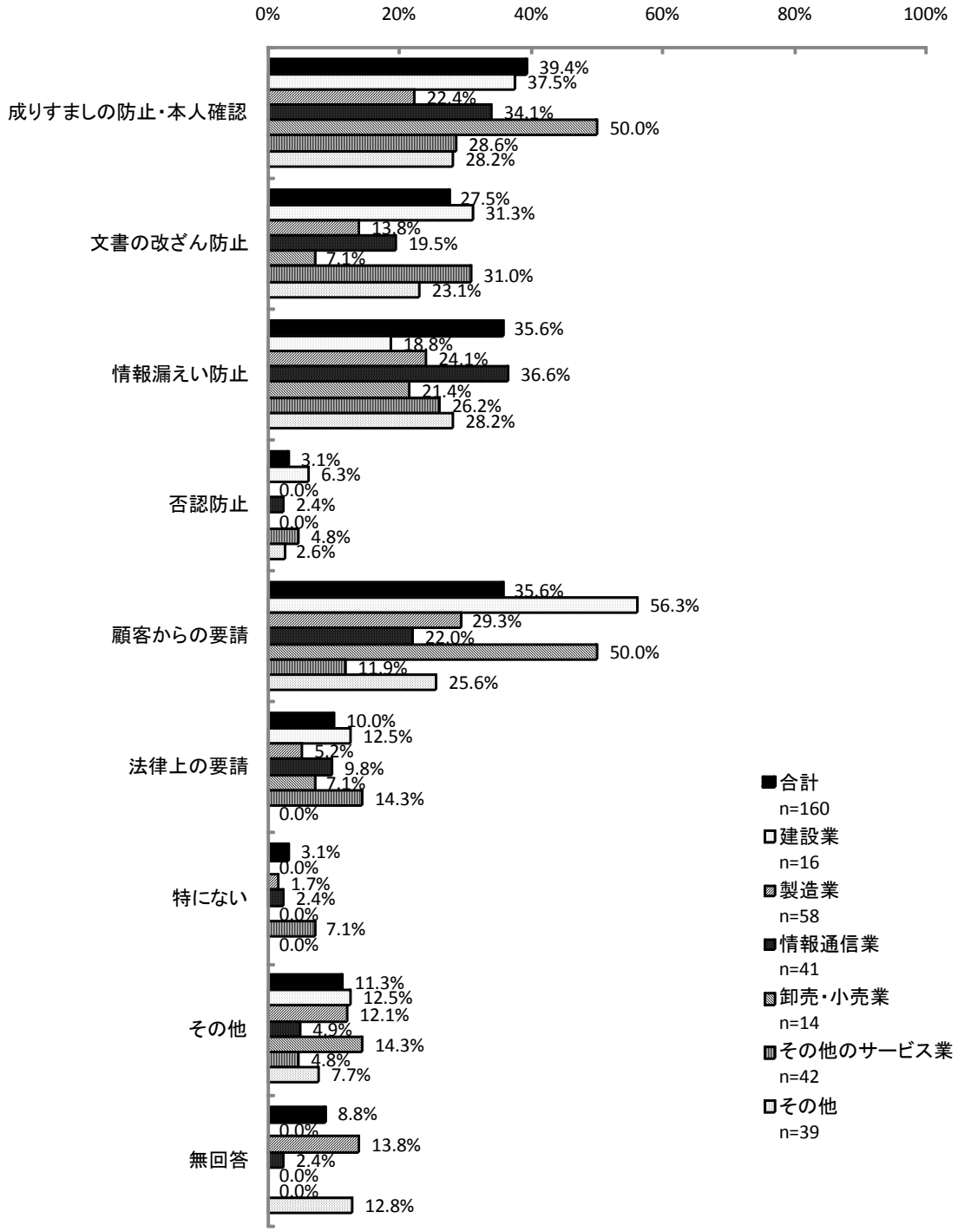
7　電子署名/電子証明書を使わない理由

回答の多い順では「メリットがない」そして「コストがかかりすぎる」であった。電子署名/電子証明書を普及させるには、利用することのメリットを提供すること、そして利用コストの低減が求められるだろう。



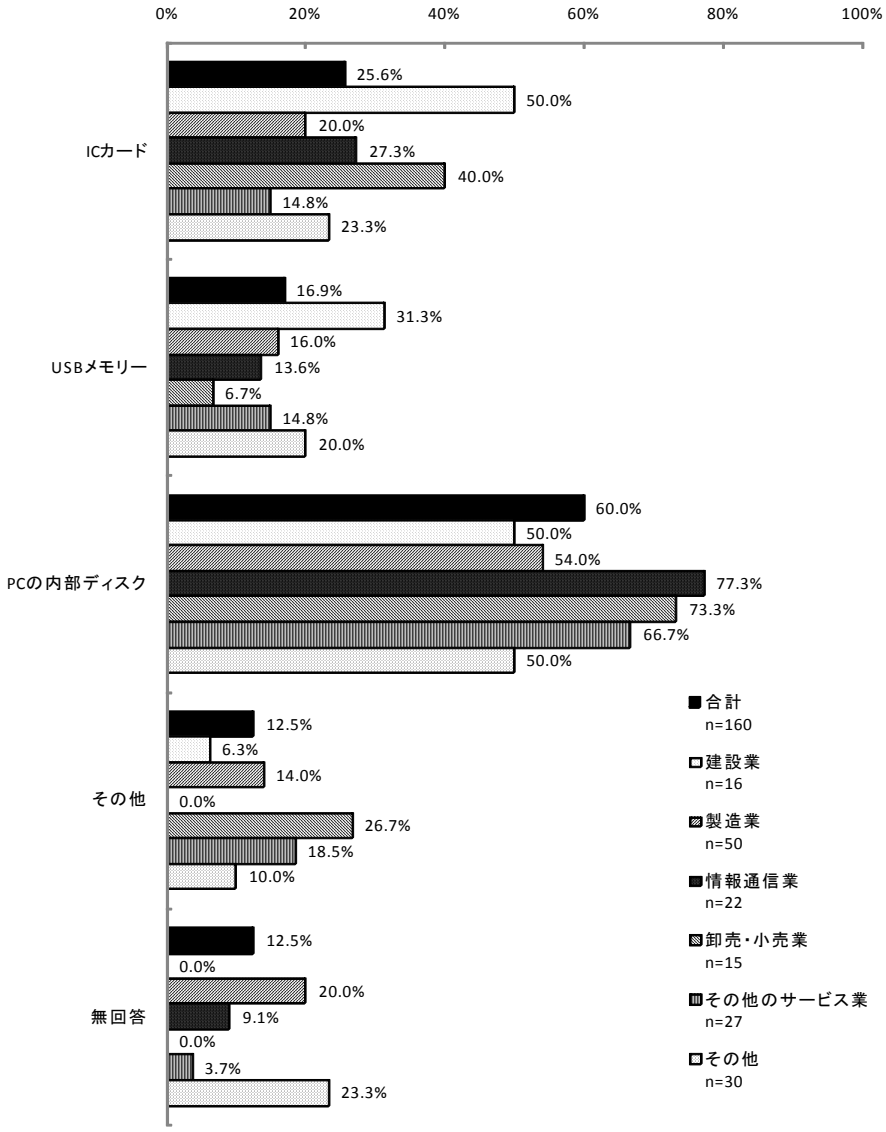
8　電子署名/電子証明書が必要な理由

電子署名/電子証明書が必要な理由として「成りすまし防止・本人確認」を挙げた企業が一番多いのは平成 19 年度と変わりがないが、前回の 72%に対し、39%と大幅に減っている。一方で「顧客からの要請」は前回の 14%に対し、35.6%と大幅に増えていた。特に建設業及び卸売・小売業で半数以上が必要な理由として挙げているのが特徴的である。なお、両業種とも前項目の電子署名/電子証明書の利用状況ではもっとも利用している業種である。



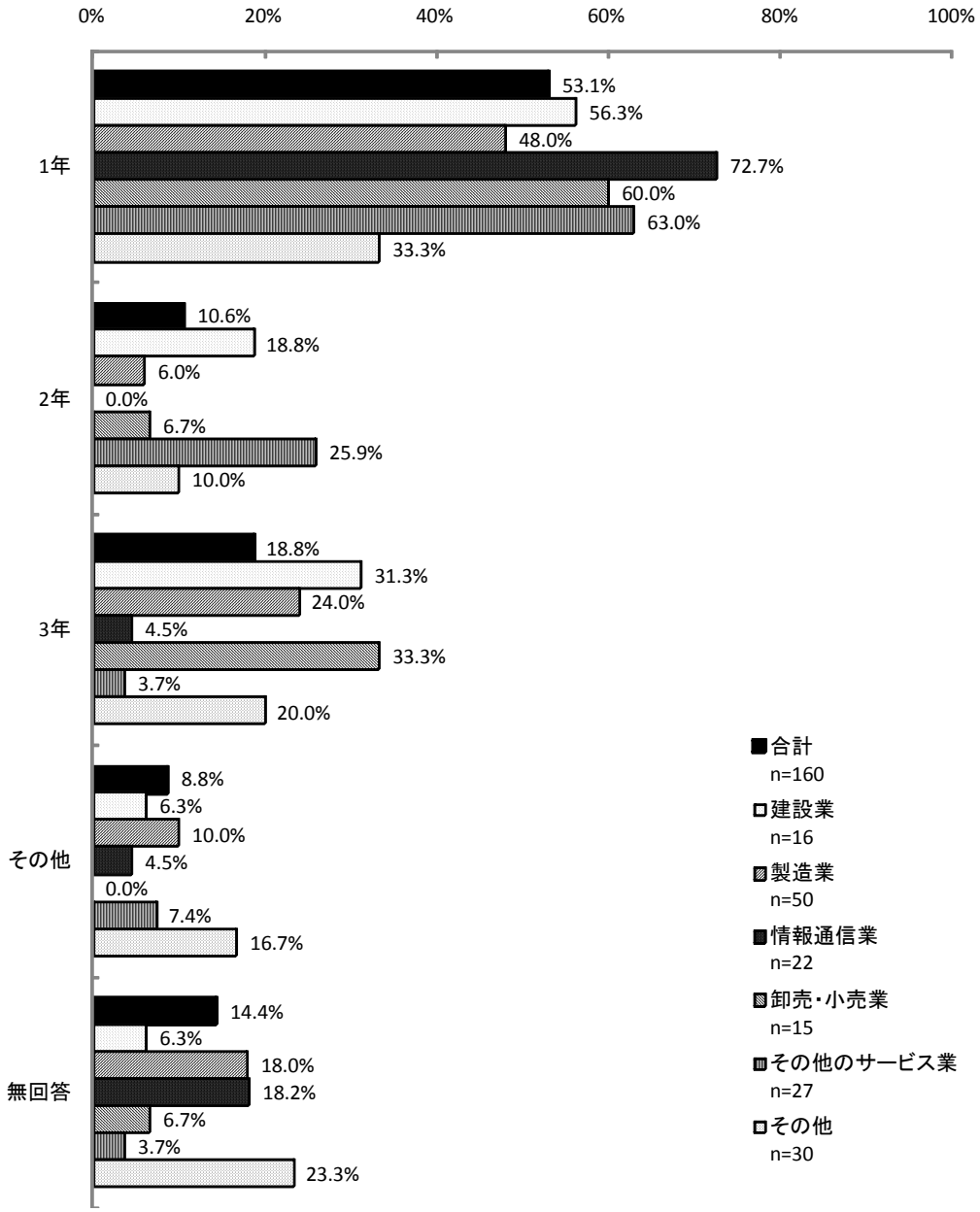
9　電子署名/電子証明書の格納媒体

電子署名/電子証明書の格納媒体は PC が多いが、IC カードや USB メモリーの利用もされている。



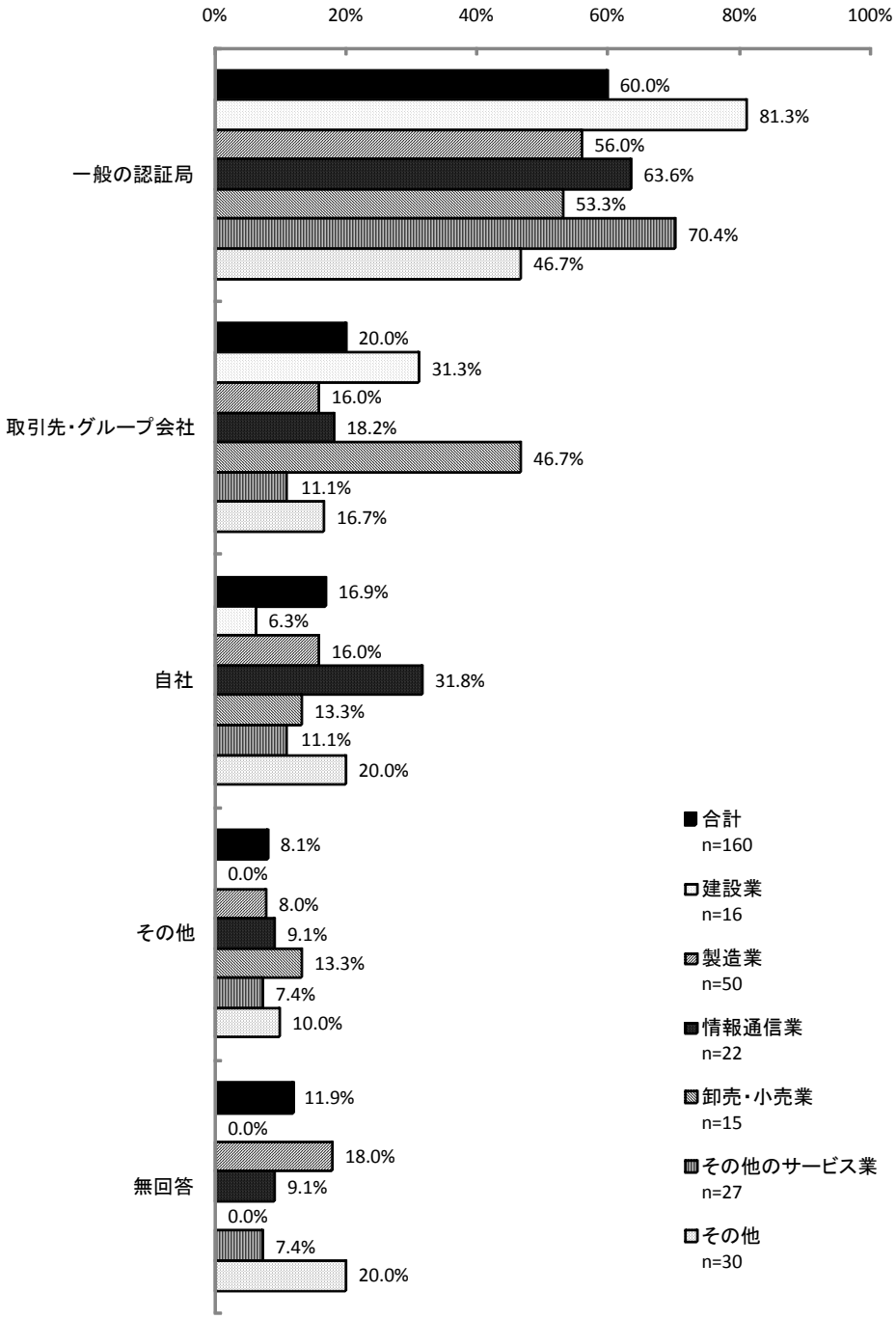
10　電子署名/電子証明書の有効期間

電子署名/電子証明書の有効期間は 1 年が最も多い。理由として、SSL サーバ証明書の利用、有効期間が長いものリスク（職員の異動に伴う失効、購入時にかかる予算高）が考えられる。



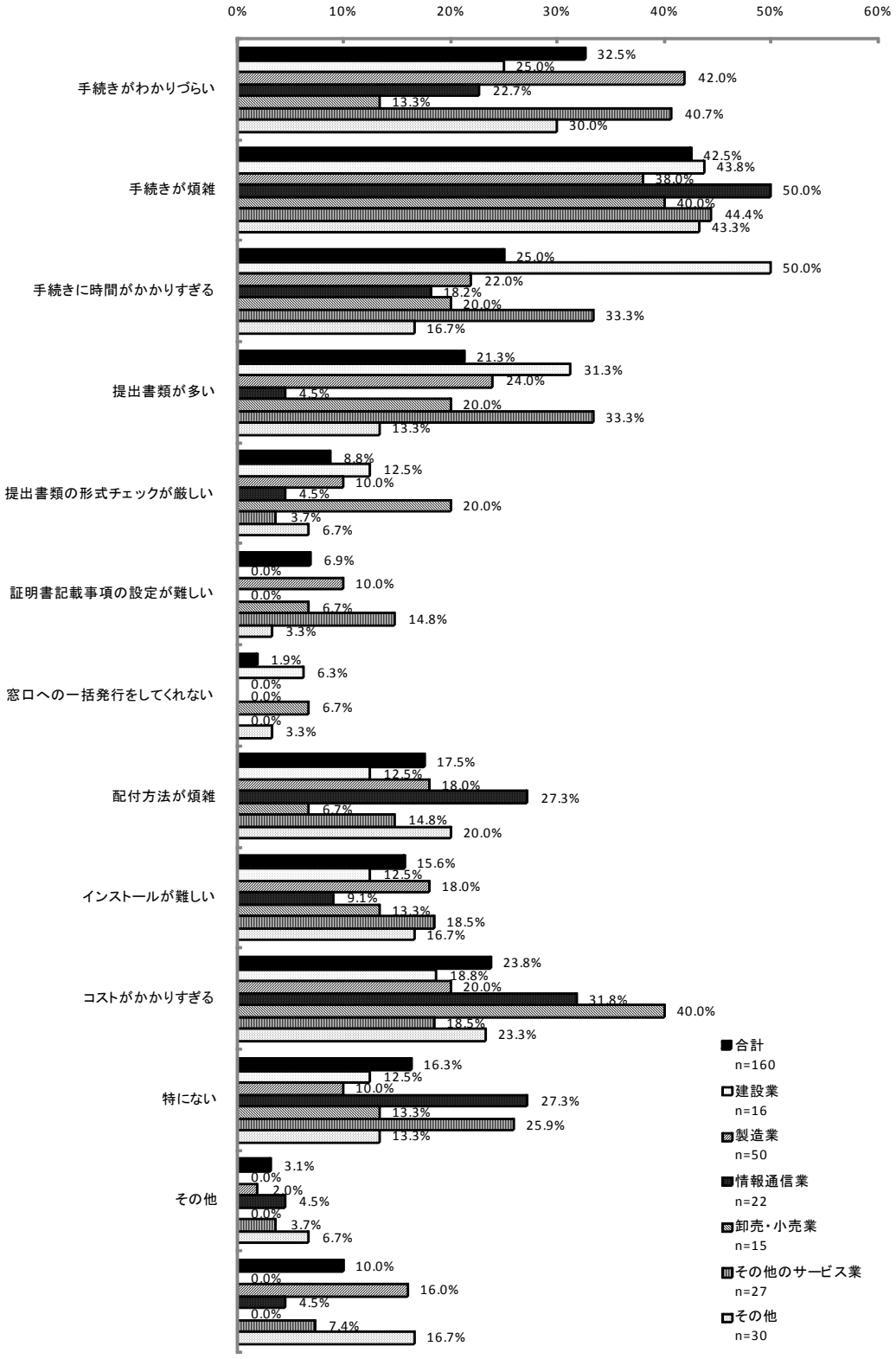
11　電子署名/電子証明書の発行元

電子署名/電子証明書の発行に関しては一般の認証局が 6 割を占める。

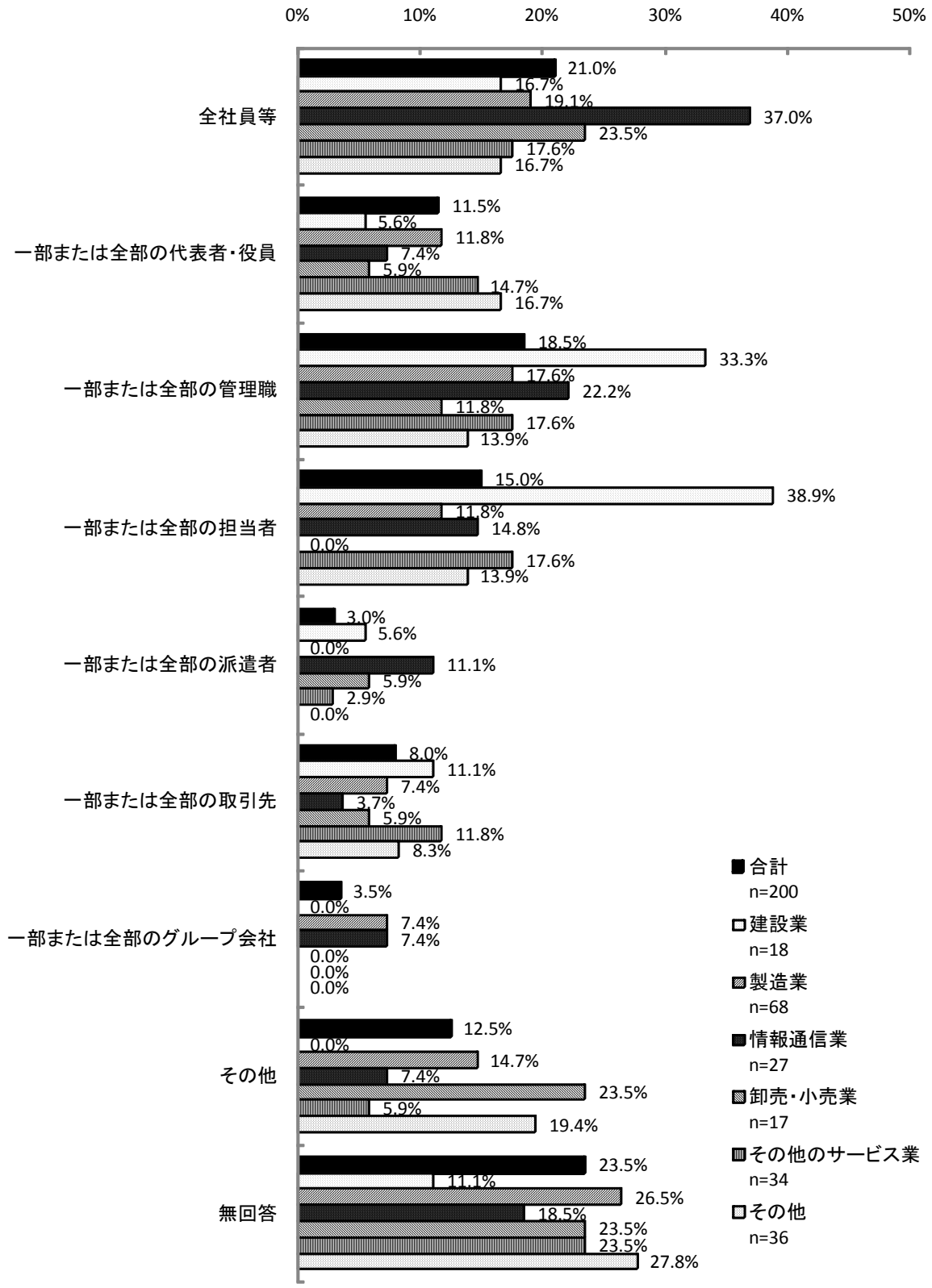


12　電子署名/電子証明書の発行手続きの問題点

電子署名/電子証明書の発行において「手続きが煩雑」であることが問題点として一番多く挙げられている。

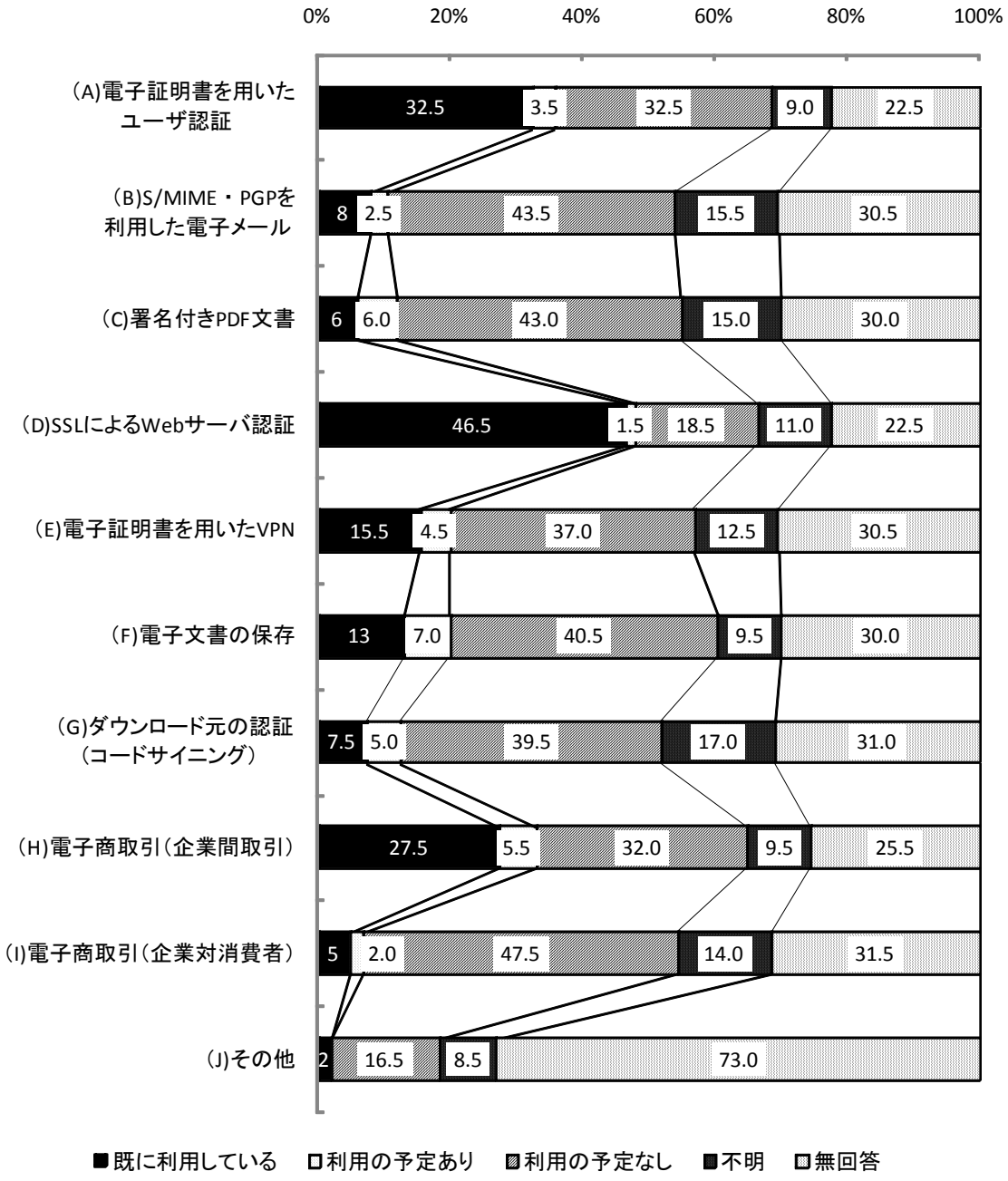


13　電子署名／電子証明書を配付したい対象



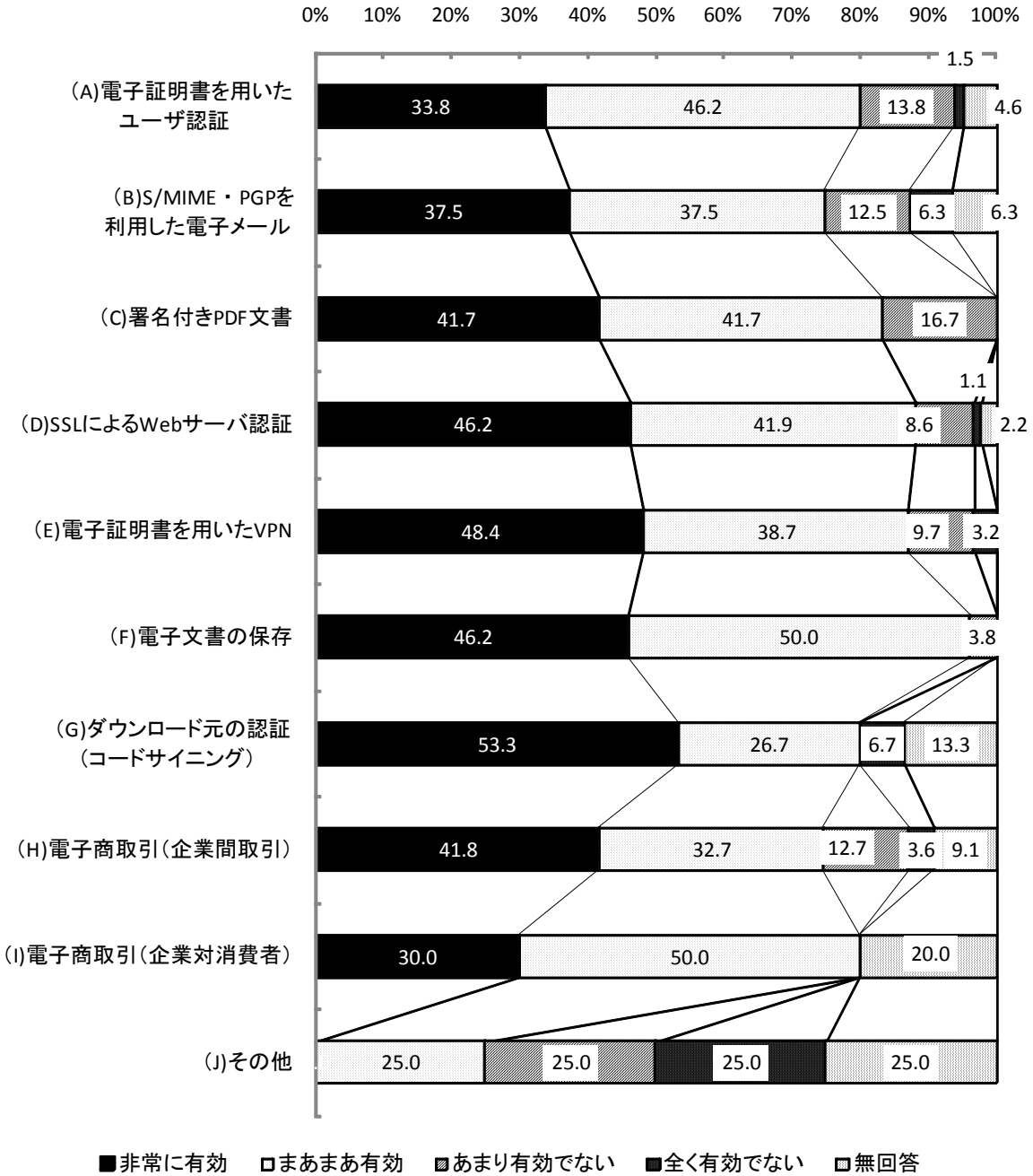
14　電子署名/電子証明書を利用したアプリケーションの利用実績と予定

電子署名/電子証明書を利用したアプリケーションとして最も利用されているのは、「SSL によるサーバ認証」であり、「電子証明書を用いたユーザ認証」と続く。「電子証明書を用いたユーザ認証」は平成 19 年度では「既に利用している」の(15.2%)に比べ、2 倍近く既に利用されている状態にある。

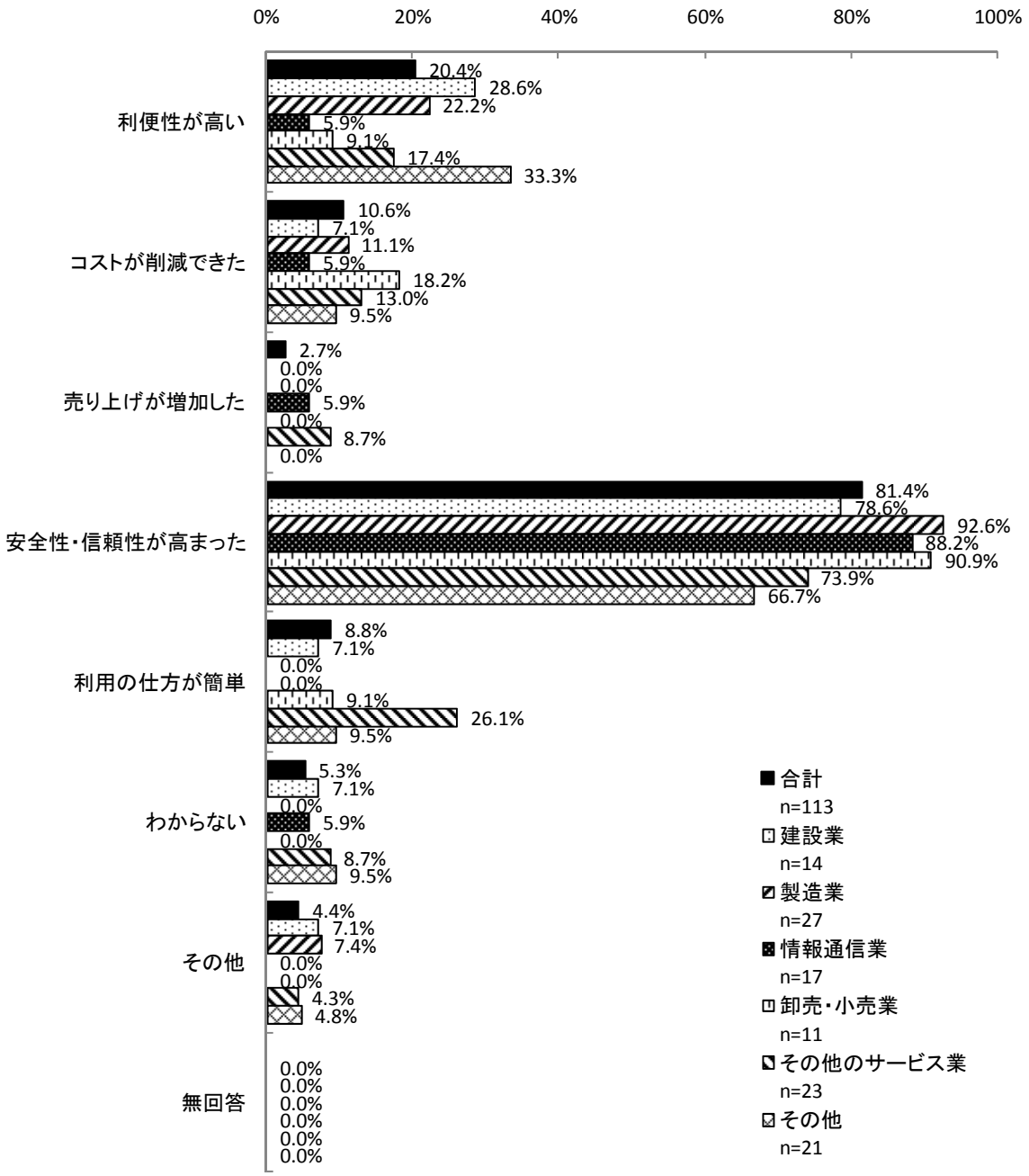


15　電子署名/電子証明書利用アプリケーションによる業務効率化・コスト削減への影響

電子署名/電子証明書を利用したアプリケーションとして最も利用されているのは、「SSL によるサーバ認証」であり、「電子証明書を用いたユーザ認証」と続く。「電子証明書を用いたユーザ認証」は平成 19 年度では「既に利用している」の(15.2%)に比べ、2 倍近く既に利用されている状態にある。

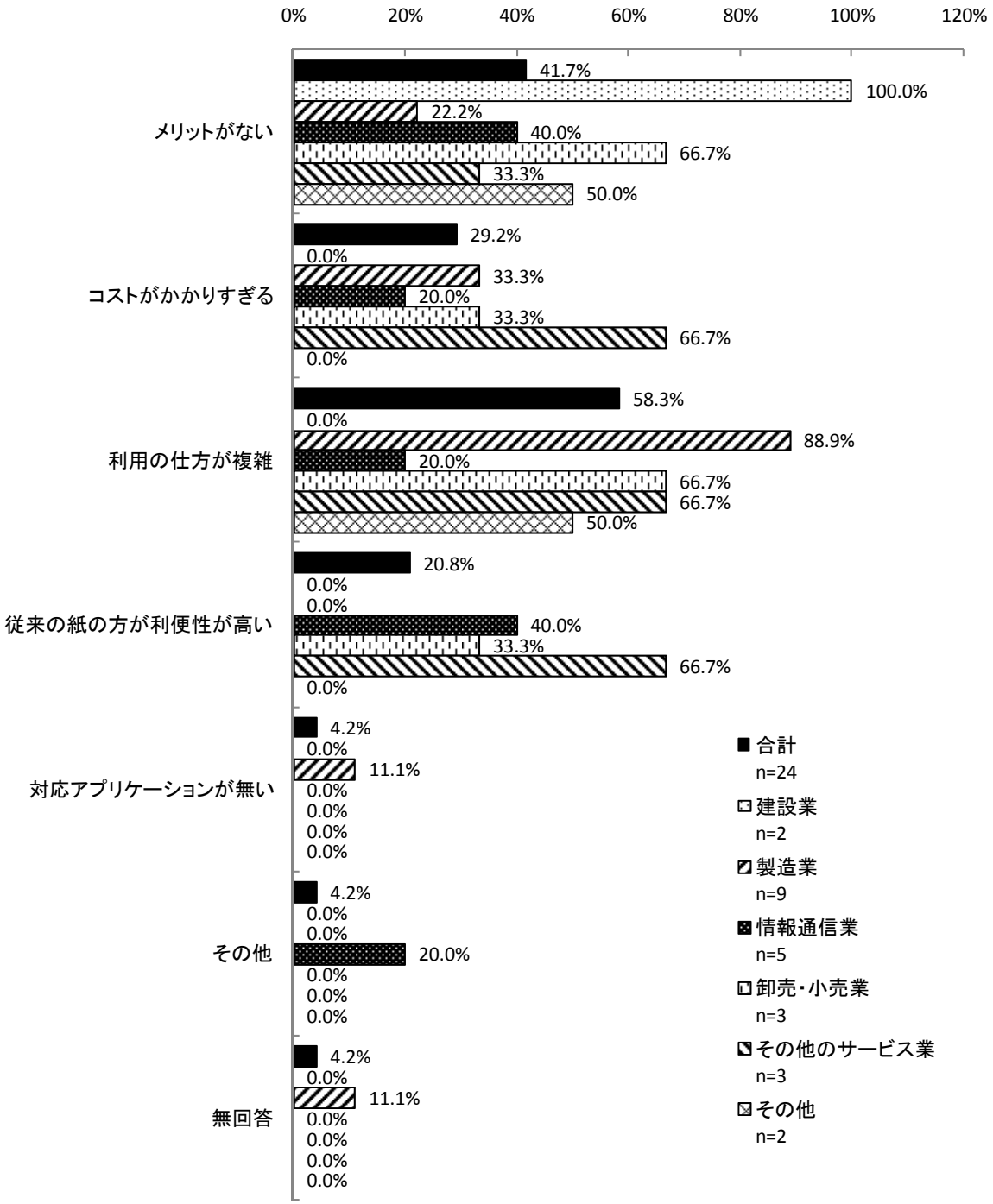


16　電子署名/電子証明書が有効な理由

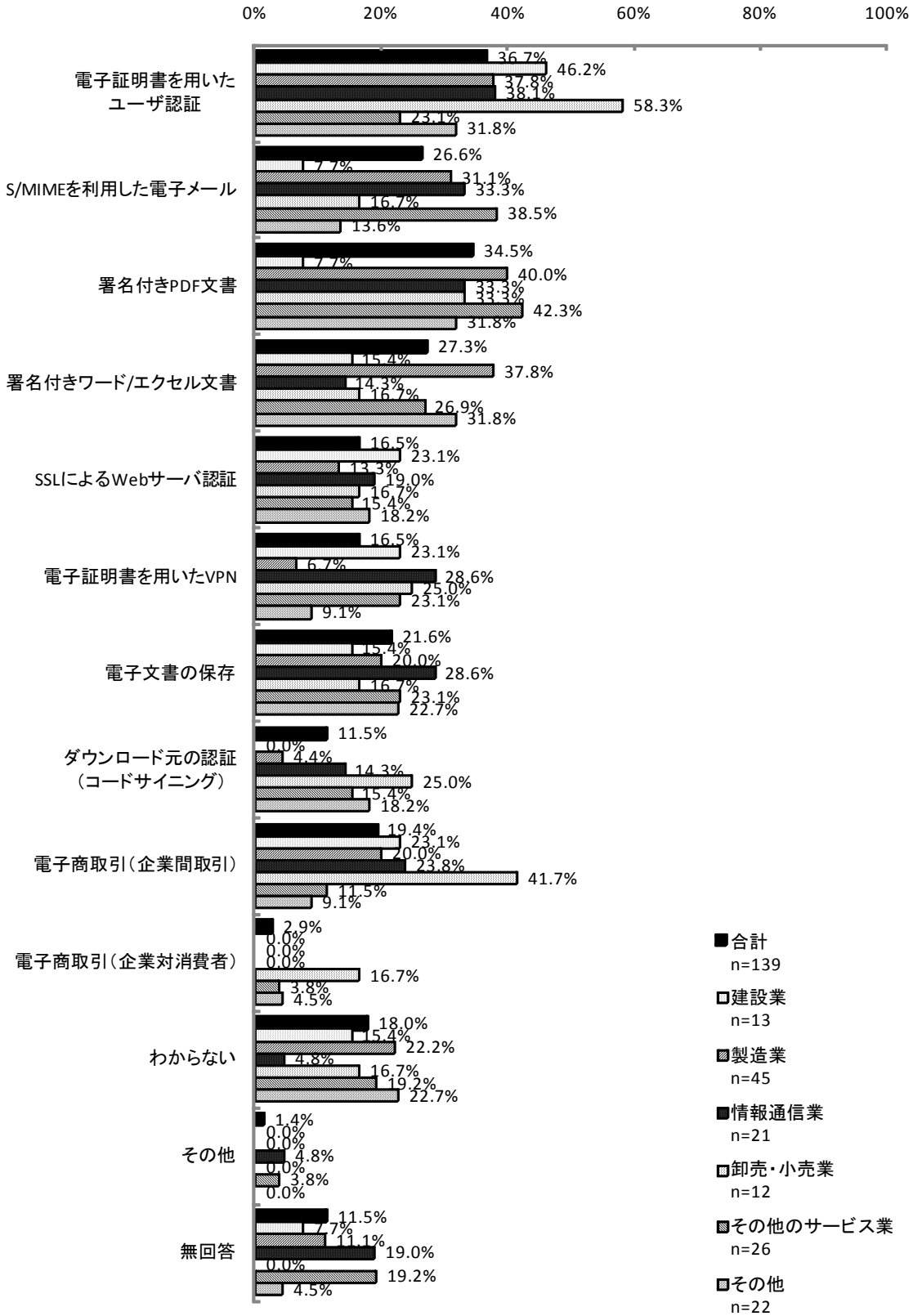


17　電子署名/電子証明書が有効でない理由

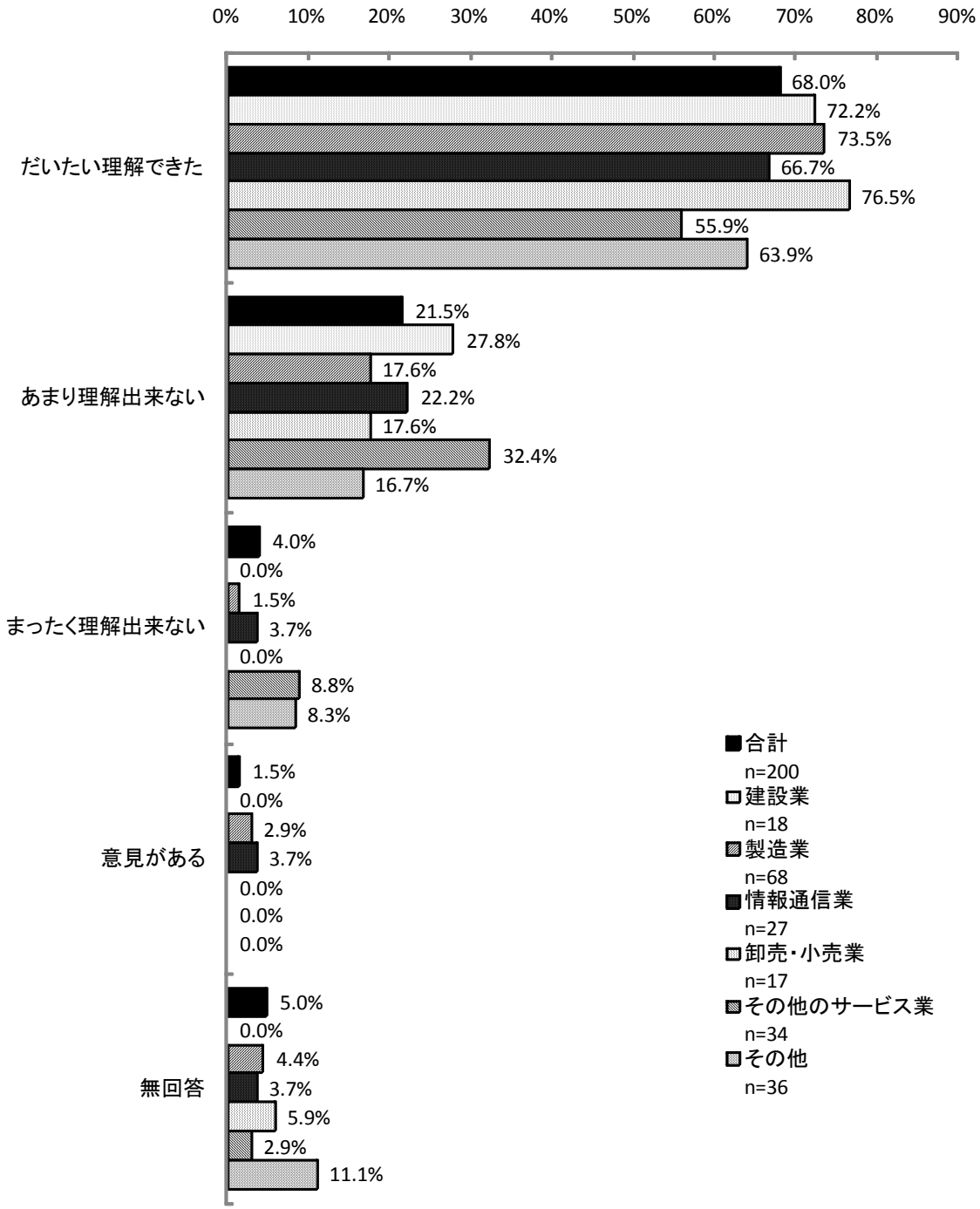
有効でない理由としては利用の仕方が複雑、コストがかかりすぎるなどが指摘されている。



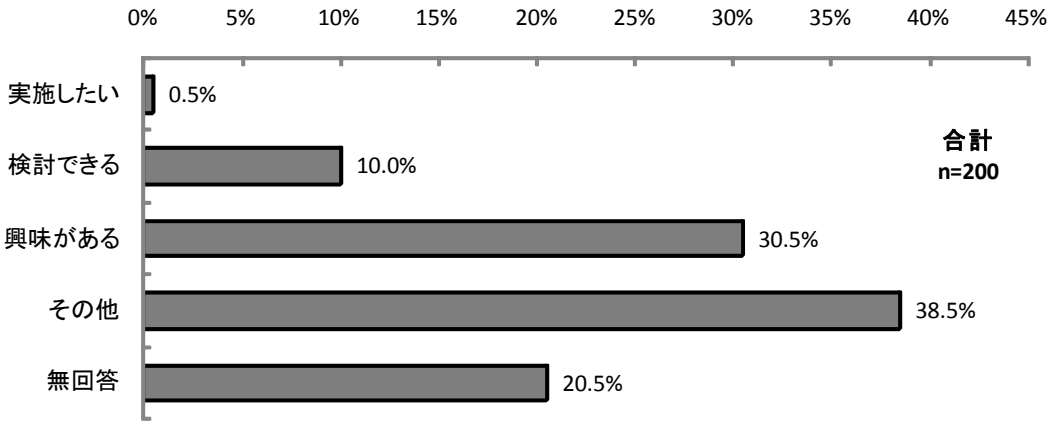
18　電子署名/電子証明書が仮にあった場合の利用用途



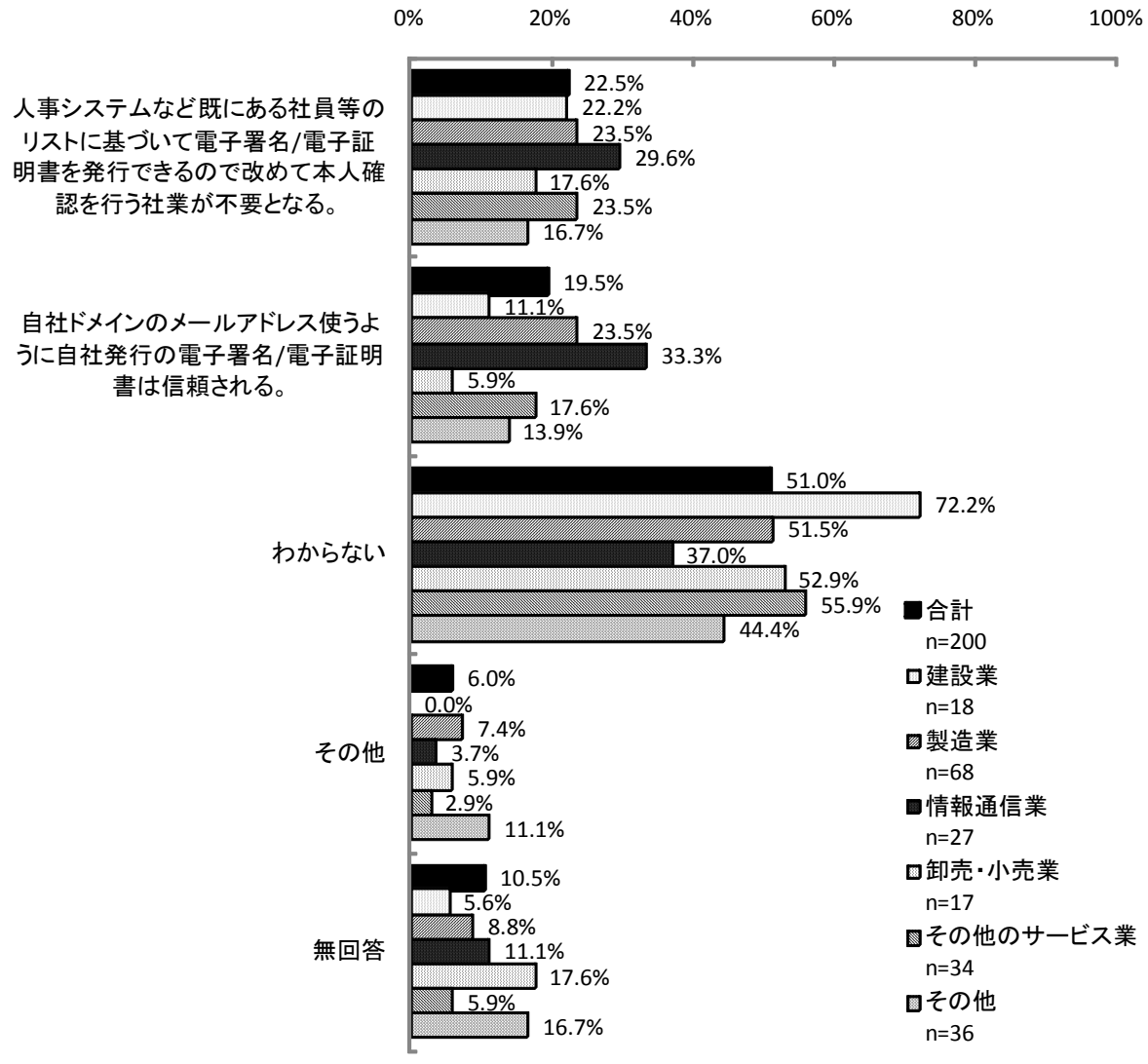
19　冊子の反応


0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
だいたい理解できた
68.0%
72.2%
73.5%
66.7%
76.5%
55.9%
63.9%
あまり理解出来ない
21.5%
27.8%
17.6%
22.2%
17.6%
32.4%
16.7%
まったく理解出来ない
4.0%
0.0%
1.5%
3.7%
0.0%
8.8%
8.3%
意見がある
1.5%
0.0%
2.9%
3.7%
0.0%
0.0%
0.0%
無回答
5.0%
0.0%
4.4%
3.7%
5.9%
2.9%
11.1%
合計
n=200
建設業
n=18
製造業
n=68
情報通信業
n=27
卸売・小売業
n=17
その他のサービス業
n=34
その他
n=36

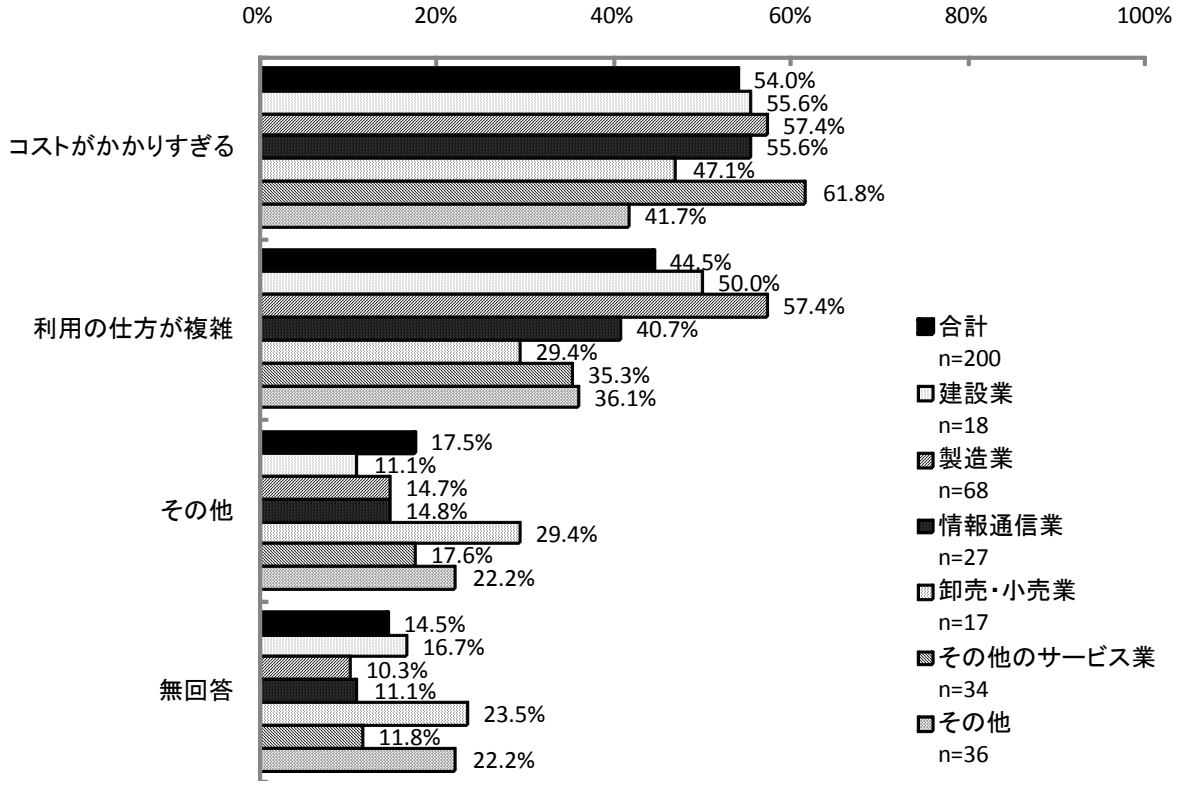
20　電子署名/電子証明書を団体の会員メンバー等への発行



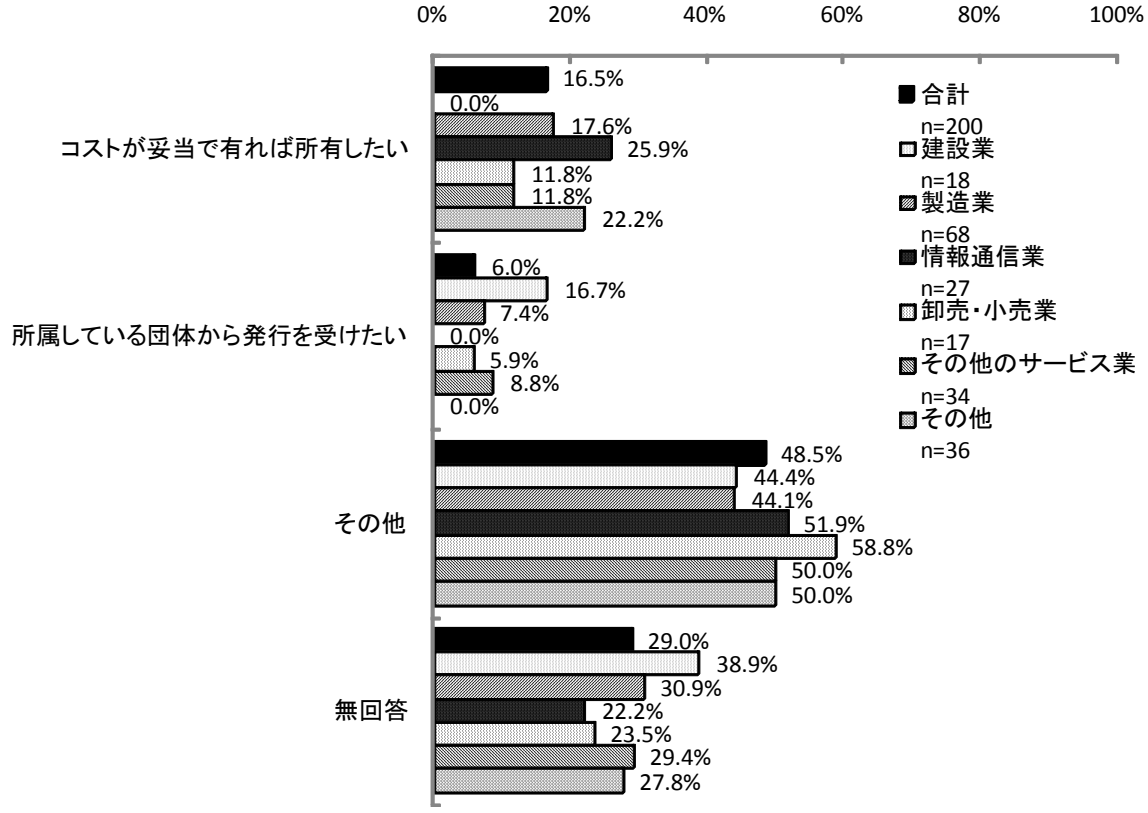
21　自社認証局のメリット



22　自社認証局のデメリット



23　自社認証局の所有



F「シンポジウム講演資料」

講演１　電子認証等の民間制度・基盤

2010年2月4日
シンポジウムプログラム講演内容について

第1部：制度･基盤	
10:00-10:15	**電子認証等の民間制度･基盤**
1	**講師：青木 尚**（JIPDEC 電子商取引推進センター　主席研究員） 本日のシンポジウムの各講演内容やパネルディスカッションのポイントを紹介します。
10:15-10:30	**ビジネスモデル検討部会**
2	**講師：満塩 尚史**（株式会社イマーディオ パートナー） [ビジネスモデル検討部会　部会長] ビジネスモデル検討部会の設置の目的、検討結果のご報告をします。認証基盤の分断は業務効率化の大きな阻害要因（JCANの必要性、目的）、認証基盤のフロントエンドでの連携、自社認証局と相互連携等について記された冊子の作成過程での検討内容についてご紹介します。
10:30-10:45	**ポリシー/基盤システム検討部会**
3	**講師：手塚 悟**（東京工科大学 コンピュータサイエンス学部　教授） [有識者委員会 主査･ポリシー/基盤システム検討部会　部会長] ポリシー/基盤システム検討部会の設置の目的、検討結果のご報告をします。共通CPプロファイル、ポリシーの統一について等、検討部会での討議内容についてご紹介します。

1

10:45-11:00	**評価基準検討部会**
4	**講師：大木 栄二郎**（工学院大学 情報学部情報デザイン科　教授） [評価基準検討部会　部会長] 評価基準検討部会の設置の目的、検討結果のご報告をします。WebTrustforCA監査を受けた認証局の評価等、検討部会での討議内容についてご紹介します。
11:00-11:05	**質疑応答**
11:10-12:00	**パネルディスカッション**
5	JCANビジネスCPについての説明後、その内容も含めて、パネリストの皆様とともに民間認証基盤の現状と方向性等について討論します。
13:20-13:40	**ビジネスパス**
6	**講師：福田 昭和**（株式会社HARTIN MARTIN　取締役） ビジネス･パスのID、証明書情報の取り扱い、共通フォーマットの仕様案について等、委員会での研究結果についてご報告します。
13:40-13:45	**質疑応答**

2

第2部：海外動向	
13:50-14:30	**韓国における認証基盤について**
7	韓国Koscom CorporationのMoon Sung-Eun氏をお招きし、韓国における電子署名のinB、BtoBの普及状況について等、韓国の認証基盤のご紹介をいただきます。
14:30-15:10	**台湾における認証基盤について**
8	台湾、NII 産業発展協進会のLuke Lu氏をお招きし、台湾における電子署名のinB、BtoBの普及状況について等、台湾の認証基盤のご紹介をいただきます。
15:10-15:40	**ドイツにおける認証基盤について**
9	欧州、特にドイツにおけるPseudonymの使われ方、IDとの関係、連携について等、ドイツにおける認証基盤のご紹介をいただきます。
15:40-15:45	**質疑応答**

第3部：ビジネスシーン	
15:50-17:20	**パネルディスカッション**
10	テーマ：ポリシー（JCANビジネスCP） 複数のCPを位置づける認証基盤、PS情報環境、情報交換機能について等、事例として転職、電子投票（役員選挙）等、SaaS/クラウド型の電子認証について（発表者調整中）の発表内容を踏まえて、安心・安全な社会的な基盤、適切な水準の安全性と信頼性の確保に係るビジネス活動環境の構築等について討論します。

3

講演２　ビジネスモデル検討部会

電子認証の民間制度・基盤の確立に関するシンポジウム

ビジネスモデル検討部会検討内容について

電子認証等の民間制度・基盤の確立に関する委員会
ビジネスモデル検討部会部会長　満塩 尚史
（株式会社イマーディオパートナー／環境省情報化統括責任者（CIO）補佐官／
各府省CIO補佐官等連絡会議情報セキュリティWGリーダー）

2010年2月4日

財団法人日本情報処理開発協会

1

ビジネスモデル検討部会検討内容

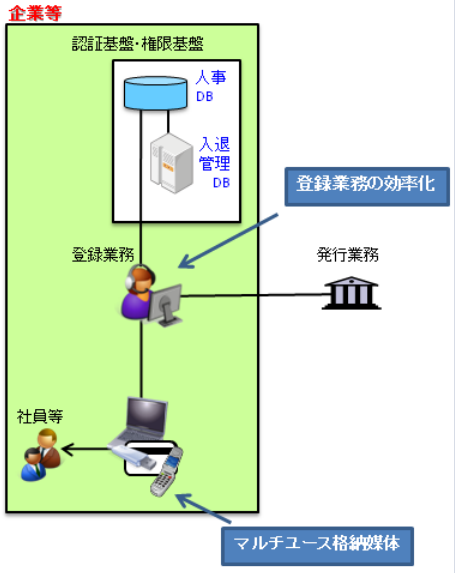
設置の目的

・ビジネスシーンの検討
企業/団体（企業等）内、グループ会社或いは取引先等を含めた業務連携への民間制度･基盤の適用例の検討

・プロモーション冊子の検討/アンケートの実施
民間制度・基盤の創成を目的としたプロモーション冊子の作成及び3000社アンケートの実施。

・登録業務効率化の検討
電子証明書等のクレデンシャル発行のための登録業務の自動化を目的に、人事システム等と登録業務との属性情報の連携方式の検討。

・マルチユース格納媒体のPKI対応の検討
企業等が導入しやすい環境整備の一環として、ICカードにPKCS#7対応共通鍵及び所属情報等を記録する方式の検討。



2

開催日	主な意見等
第1回(10/14)	◆JCANプロジェクトへの取り組み紹介 ・普及に向けた登録業務まわりの環境整備を検討する。 ・今年度はプロモーション活動、来年度は認証局の構築を行う。 ・UPKI(University Public Key Infrastructure)について、一緒に検討していきたい。
第2回(10/28)	◆ビジネスシーンについて ・本制度・基盤の利用者を集めるためにプロモーション冊子にまとめ、3000社アンケートに添付する。 ◆電子署名の使用用途について ・電子認証及び電子署名(暗号は利用者に任せる)。 ・企業等内用途をベースに企業等間用途まで広げる。 ・企業等間用途は電子メールや電子文書への電子署名が必須と考える。 ◆電子署名を使うメリットについて ・社会的な全体最適化(業務効率化)、内部統制の強化。

3

開催日	主な意見等
第3回 (11/11)	◆ビジネスシーンについて ・冊子案に対する「JIPDECのメッセージ」の追加、表現の見直し等のコメントへの対応。 ◆証明書プロファイルについて ・企業等が発行しやすいビジネススタイルに合った電子証明書の普及 ①次の対象が会社/団体に属していることの証明 ・企業等内個人(肩書き) ・企業等の部門・役割名 ・企業等の設備 ②実名をオプションとすることで次を実現 -事前の作り込みを可能 -証明書記載事項の変更による失効を減らし有効期限まで使いきることを可能 ※サーバ証明書(SSL証明書等)については今は検討しない ◆認証業務について ・社会全体としての分担見直しで「迅速」「高効率」「高信頼性」化を可能とする ◆JCANパス(マルチユースカード)について ・共通フォーマットという考え方の導入で媒体集約化/媒体フリー/マルチベンダー対応(選択肢提供)、システムの段階的構築の実現を可能

・ PS名とは、擬名・仮名・別名と訳されることがあるが適切な訳語が定まっていないPseudonymの略称。

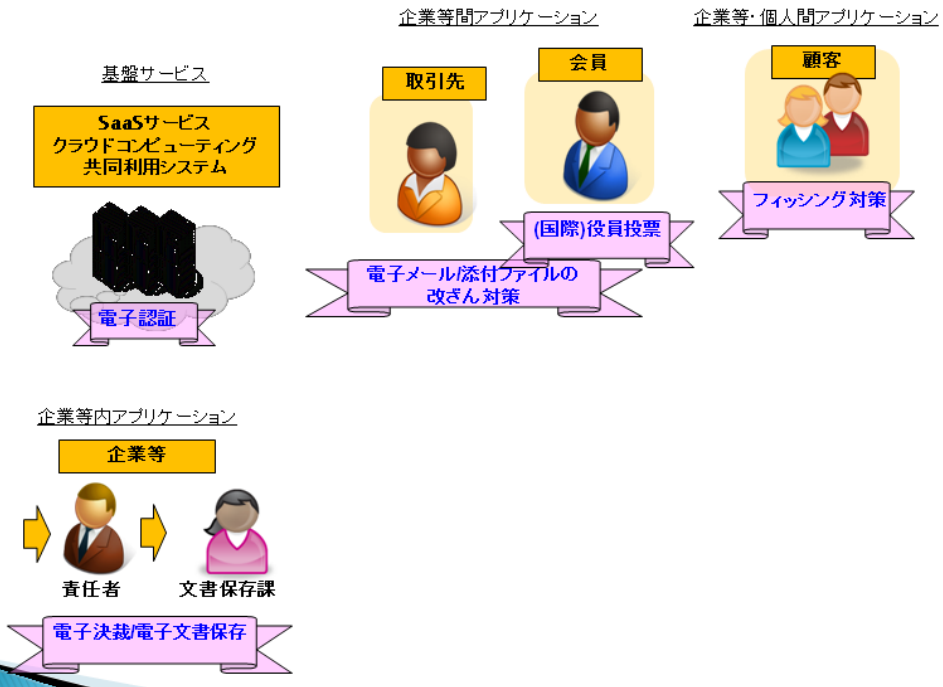
4

委員会名	主な意見等
第4回(12/9)	◆JCANパス(マルチユースカード)について ・最初はTypeA、フェリカカード、USBメモリへの適用を考えている。 ・暗号化についてはドライバでの適用を考えている。 ◆ISO化について ・ISO/TC247等でインターネット上での物流トレースを行うタイプの模倣品対策が検討され始めている。 ・アクセスした企業等情報を当該物流トレースにログする方法として、電子証明書をセキュアな封筒として使う案を提案したところ採用になった。 →Subject等の標準化提案をまとめている。 ◆今後について ・実体とID・PS名を結びつけ個人情報に配慮したグローバルな仕組みについてはメーリングリスト/シンポジウムで検討結果を報告する

5

参考資料

フラグシップ(キラー)アプリケーション・対応必須アプリケーション例



6

講演３　ポリシー/基盤システム検討部会

電子認証の民間制度・基盤の確立に関するシンポジウム

ポリシー/基盤システム検討部会検討内容について

電子認証等の民間制度・基盤の確立に関する委員会
ポリシー/基盤システム検討部会部会長　手塚 悟
（東京工科大学 コンピュータサイエンス学部 教授）

2010年2月4日

財団法人日本情報処理開発協会

1

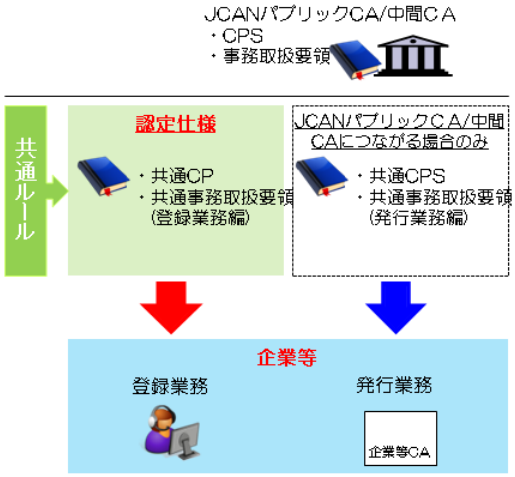
ポリシー/基盤システム検討部会検討内容

設置の目的

・制度/基盤のあり方の検討
企業/団体（企業等）ベース認証基盤に基づいて企業等が企業等に属する対象（企業等内個人、部門名等）に発行する電子証明書に係る制度/基盤のあり方の検討からスタート。

・証明書プロファイル
企業等が発行しやすくビジネススタイルに合った電子証明書の普及が目標。

・規程の検討
ブラウザ等のトラストリストに登録されたルート認証局（パブリックCA）につなげることが前提。



2

開催日	主な意見等
第1回（10月14日）	◆JCANプロジェクトへの取り組み紹介 ・企業等ベース認証基盤に基づいて企業等が企業等に属する対象（企業等内個人、部門名等）に発行する電子証明書を企業等内用途及び企業等間用途（金銭取引は保証しない）に使用する。 ・電子メール/添付ファイルの改ざん対策は対応必須と考えており、そのためにブラウザ等のトラストリストに登録されたパブリックCAにつなげる。

3

開催日	主な意見等
第2回　（11/10）	◆JCANについて ・本プロジェクトを仮にJCAN（日本認証局ネットワーク）と名付ける。 ◆方向性について（パブリックCA） ・インキュベーション基盤としてJIPDECが新しいパブリックCAを構築。（来年度） ・同時に、既存パブリックCAとの共存を探る。 ◆方向性について（企業等CA） ・自社認証局の普及と認定。 ・次の仕組みでCSPの責任を取り除きコスト削減につなげる -自社認証局から発行された全ての電子証明書の責任は企業等の責任者が担う。 -企業等の確認はJCANが行う。 -発行対象の確認は企業等が行う。

4

委員会名	主な意見等
第3回　（12/15）	◆認定について ・この仕組みのポイントは企業等が人事情報に基づいた電子証明書を発行しているということである。 ・共通のルールと内部監査を調査対象とする民間認定制度に基づいて上記運用を行うと社会的な信頼連携を可能とする。 ◆証明書プロファイルについて ・企業等が発行しやすいビジネススタイルに合った電子証明書の普及 ①次の対象が企業等に属していることの証明 ・企業等内個人(肩書き) ・企業等の部門・役割名 ・企業等の設備 ②実名をオプションとすることで次を実現 -事前の作り込みが可能 -証明書記載事項の変更による失効を減らし有効期限まで使いきることが可能 ※サーバ証明書（SSL証明書等）については今は検討しない ※JCANの証明書は個人を証明するのではなく、企業等に属していることを証明するものである。従って人事情報を持っていない他社の人へ電子証明書を発行できない。

5

委員会名	主な意見等
第4回　（1/18）	◆ISO化について ・ISO/TC247等でインターネット上での物流トレースを行うタイプの模倣品対策が検討され始めている。 ・アクセスした企業等情報を当該物流トレースにログする方法として、電子証明書をセキュアな封筒として使う案を提案したところ採用になった。 →電子証明書の一部の標準化提案をまとめている。 ◆位置付けについて ・共通化された電子の名刺/社員証/担当印/部門印/角印/会員証等に相当する電子証明書。 ※実印/丸印相当の役割は、「電子署名法」等に基づく電子証明書が担う。

6

講演４　評価基準検討部会

電子認証の民間制度・基盤の確立に関するシンポジウム

評価基準検討部会検討内容について

電子認証等の民間制度・基盤の確立に関する委員会
評価基準検討部会部会長　大木 栄二郎
（工学院大学 情報学部情報デザイン学科 教授）

2010年2月4日

財団法人日本情報処理開発協会

1

評価基準検討部会検討内容

設置の目的

①登録業務の評価基準

適用範囲：

共通ルールに基づくパートナーの登録業務の認定基準

活動内容：

内部監査チェックシート案の検討

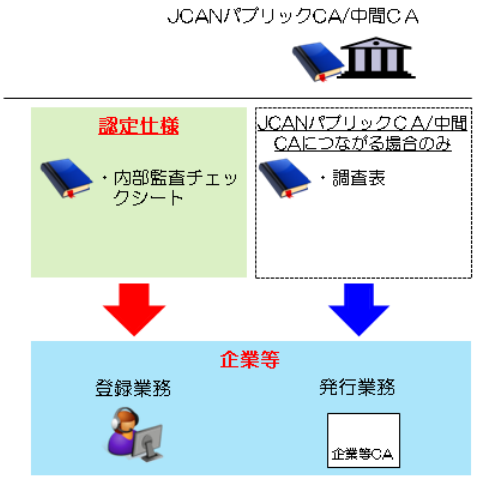
②発行業務の評価基準

適用範囲：

- 共通ルールに基づくパブリックCAの運用の評価基準
- 共通ルールに基づくパートナーCAの運用の評価基準

活動内容：

WebTrust for CAの監査基準と電子署名法に基づく認定制度の適合例を入れ込んだ調査表案の検討



・パブリックCAとは、ブラウザ等の「信頼されたルート認証機関(=トラストリスト)」に登録されたルートCAを指す
・Webtrust(米国公認会計士協会およびカナダ勅許会計士協会が共同で開発・管理運営している認定制度)とは、ブラウザ等のトラストリストに登録の際に要求される基準。
・CA(Certification Authority)は、認証システムの運用機関の略称。

2

開催日	主な意見等
第1回(10月14日)	◆JCANプロジェクトへの取り組み紹介 WebTrustの認定取得を目指す本格運用の検討開始

・JCAN(仮称)とは、Japan CA Networkの略称。

3

開催日	主な意見等
第2回 (12/9)	**①登録業務の評価基準** ◆原則 ・原則として電子証明書が人事台帳と結び付いていることの確認。 ◆調査方法の形式 ・基本的には、内部監査の形式になるのだろう。 チェックシートには規程名だけ出させる。 その確認は内部監査で行ったとして、責任は内部監査を行った担当者に持たせるべきである。 ・チェックシートは自社内の担当者のセルフチェック項目だろう。 内部の人が予め確認したことを記録させる。 ◆調査方法について ・サンプリング調査と制度上言って問題はないと思う。 **②発行業務の評価基準** ◆方針 ・電子署名法の認証局の運用コストの半分以下を目指す ◆企業の存在確認について ・企業の実在性確認はJIPDECで行うのでここでの議論の対象ではないと考えている。 ・企業コードを持っているか、1部上場、2部上場なのか、TDBに登録されているのかという確認手段を複数組み合わせて確認することは可能だと思う。 ◆スケジュール ・12月末までに比較表は埋めて、1月～2月に確認、修正作業を行う。 ・作業結果は2月の次回検討部会で提示する。

4

開催日	主な意見等
第3回（2/2）	**①登録業務の評価基準** ◆登録業務のチェックについて ・企業の人事管理のシステムと同程度のセキュリティを保つとすれば良い。 **②発行業務の評価基準** ◆民間認証局の調査表に係るWebTrustforCA認定基準と適合例等との比較について ・JCANの証明書は企業の証明書であり、企業に属している証明書で社員個人の証明書ではない。それを貸し与えているだけである。ダウンロードされたPKCS#12をどの形にするかは、そこのRAで決めて渡すという方向で検討したい。

参考資料

参考資料A　内部監査チェックシート案

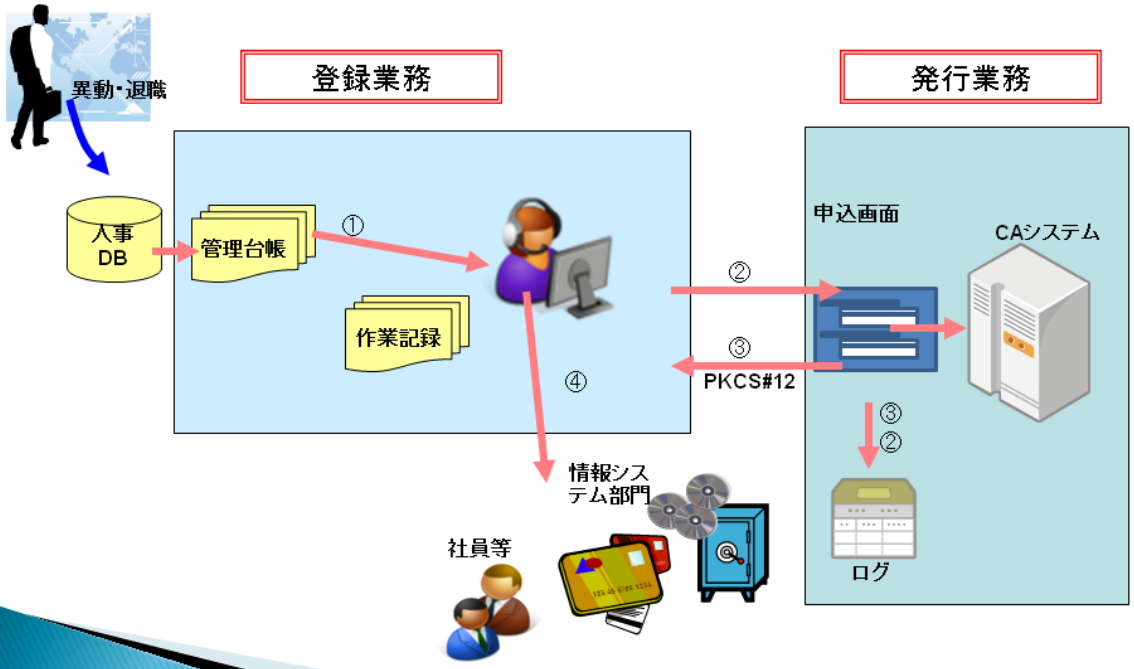
参考資料B　「WebTrust Principles and Criteria for CA」の構成

参考資料C　調査表案

参考資料A

内部監査チェックシート案

◆登録業務の運用イメージ



・ PKCS#12とは、電子証明書等のダウンロードの形式の1つ

参考資料A

内部監査チェックシート案

①登録用PCのアクセス管理			
M-1	登録用PCのログインパスワード管理を「登録業務事務取扱要領」に規定していますか。	□ 規定している。 （章節番号：　　） →具体的な方法は、 □ パスワード □ ICカード □ その他（　　） □ 規定していない。	
M-2	上記パスワード等の定期的な変更を行っていますか。	□ 変更している。 →定期的にパスワードを変更している （最近の変更日　　年　　月　　日） □ 変更していない。	
②スクリーンセーバーのパスワード設定			
M-3	スクリーンセーバーによるパスワードロックは、3分以内に設定されていますか。	□ 設定している。 □ 設定していない。	
③ウイルス対策			
M-4	ウイルス対策ソフトが導入されて、パターンファイルが更新されていますか。	□ 導入している。 →パターンファイルの更新日は、 （　　年　　月　　日　　：　　） □ 導入していない。	

参考資料A

内部監査チェックシート案

④登録業務			
M-5	電子証明書は、組織に属している対象（企業内個人、部門名、設備等）に貸与していますか。	□ 次の対象に貸与していることを管理台帳で管理している。 □人事DB登録者 □請負・派遣契約で指定された者 □組織体制表で管理されている部門名等 □その他管理簿で確認されている者／設備 □貸与先を管理台帳で管理していない。	
M-6	上記貸与者の異動・退職・変更に伴う管理台帳の内部監査を行っていますか。	□ 上記帳簿と突合せを行なっている。 □有効な電子証明書の総数（約　　） □総貸与数　　（約　　） □過去1年間のメンテナンス数（約　　） □ 行っていない。	異動・退職者総数 失効総数
M-7	登録業務の作業記録を残していますか。	□ 残している。 □ 残していない。	
O-8	登録業務関係者に対して、年に一度又は任命の都度教育をし、教育記録を残していますか。	□ 残している。 □ 残していない。	

参考資料B

「WebTrust Principles and Criteria for CA」の構成

PRINCIPLE No.	概要
PRINCIPLE 1 CA Business Practices Disclosure 事業実践の開示	The Certification Authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices. 認証局ははその鍵と証明書のライフサイクル管理事業と情報プライバシーの実践を公開し、またその公開された実践に従って、サービスを供給する。
PRINCIPLE 2 Service Integrity サービスの完全性	The Certification Authority maintains effective controls to provide reasonable assurance that: ・Subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and ・The integrity of keys and certificates it manages is established and protected throughout their life cycles. 認証局は効果的な管理を維持し、以下について適切な保証を提供する。 ・利用者情報を適正に認証する（その認証局により実施される登録業務に向けて） ・その管理する鍵と証明書の完全性を確立し、そのライフサイクル全体を通して保護する
PRINCIPLE 3 CA Environmental Controls 認証局環境管理	The Certification Authority maintains effective controls to provide reasonable assurance that: ・Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure; ・The continuity of key and certificate management operations is maintained; and ・CA systems development, maintenance and operation are properly authorized and performed to maintain CA systems integrity. 認証局は効果的な管理を維持し、以下について適切な保証を提供する。 ・利用者と依存者の情報（へのアクセス）を認証された人にのみ限定し、認証局の業務実践として指定されていない利用から保護する ・鍵と証明書の管理運用の継続性を維持する ・認証局システムの開発、維持、運用を適正に認証し、認証局システムの完全性を維持する

WebTrust for CA 監査基準は、３つの原則と、それぞれについて複数の基準(criteria)から成ります。criteriaは階層構造をもつこともあります。認証局はそれぞれのcriteriaに対して、自認証局での実践を開示(disclose)し、criteriaに合致していることを主張(assert)します。監査人はその主張の内容と合致について第三者として意見を表明します。

参考資料C

調査表案

sample

PRINCIPLE 1

WebTrust for CA	RFC 3647	電子署名法JIPDEC適合例ver2.3	調査表案
1.1.1.CAが証明書を発行するためのCPとCPSの識別 Identification of each CP and CPS for which the CA issues certificates	4.1.2. 文書名と識別 Document Name and Identification	対象外	JCANルートCAおよび中間CAはポリシーXXX、CPS XXXに従って証明書を発行する。
1.1.2.CAによって発行された証明書のPKIと適用可能性の中で、当事者のタイプ及び適用可能性の記述を含むコミュニティと適用可能性 Community and applicability, including a description of the types of entities within the PKI and the applicability of certificates issued by the CA	3.1. 証明書ポリシー（CP） Certificate Policy	項番3712 項番3903	JCANルートCAは配下の中間CAに対してのみ証明書を発行する。 JCANルートCAはJCANとして設置が意思決定された中間CAを証明する。設置された中間CAにより証明されるパートナーCAが発行する総てのE／E証明書のsubjectとなる利用者、およびそのE／E証明書を提示される相手となる依存者は、いずれも証明書パス検証の目的でのみ、ルートCAおよび中間CAのコミュニティを形成する。
1.1.3.下記を含む連絡先の詳細と管理規程の作成 ・連絡先 ・ポリシー機関の識別 ・番地 ・CPとCPSのバージョンと有効期限 Contact details and administrative provisions, including: ・Contact person ・Identification of Policy Authority ・Street address ・Version and effective date(s) of each CP and CPS	4.1.5. ポリシー運用管理 Policy Administration	項番3902	JCANルートCAおよび中間CAの連絡先：ＪＣＡＮ係, 03-3436-7513, ra@jipdec.or.jp ポリシー機関名称：ＪＩＰＤＥＣ ポリシー機関所在地：東京都港区芝公園3-5-8 ポリシーとCPSの有効な版と日付：001版、2010.06.01

11

参考資料C

調査表案

sample

PRINCIPLE 2

WebTrust for CA	RFC 3647	電子署名法JIPDEC適合例ver2.3	調査表案
2.1.1 CA鍵生成 CA Key Generation CAは、CA鍵対が、業界標準によって生成されることについて妥当な保証を得るための制御を維持する。 The Certification Authority maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with industry standards.	4.6.1. 鍵ペアの生成と導入 Key Pair Generation and Installation 4.6.2. プライベート鍵の防護と暗号モジュールエンジニアリングコントロール Private Key Protection and Cryptographic Module Engineering Controls	項番1311-5, 1411-, 3422, 3E12-3	CA鍵の生成は、CAのビジネス実践(原則1、アイテム18参照)で開示されている様に、FIPS PUB 140-2レベル3に合致した安全な暗号デバイスの中で行われる CAによるCA鍵の生成は、予め指名された複数人による合議制操作を要求する CAは、その鍵対を署名に使用する暗号化デバイスで生成する ：
2.1.2 CA鍵保管、バックアップ、復旧 CA Key Storage, Backup and Recovery CAは、CA秘密鍵が秘匿され、それらの完全性が維持されるための妥当な保証を得るための制御を維持する。 The Certification Authority maintains controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity.	4.6.1. 鍵ペアの生成と導入 Key Pair Generation and Installation 4.6.2. プライベート鍵の防護と暗号モジュールエンジニアリングコントロール Private Key Protection and Cryptographic Module Engineering Controls	項番3712 項番3903	CAの署名用秘密鍵は、CAのビジネス実践(原則1、アイテム17)に開示されたFIPS 140-2レベル3に合致した安全な暗号デバイス暗号化デバイスに格納される CAの秘密鍵は、同じ暗号化モジュールで生成され使用され、バックアップおよび回復の目的以外で暗号化モジュールの外にエクスポートされることは無い バックアップおよび回復のため、CAの秘密鍵が、安全な暗号化モジュールからエキスポートされて、安全なストレージに移動される場合には、CAの秘密鍵は、「合議制操作による暗号テキスト」を含む安全な鍵管理スキームに従って、エクスポートされる ：

12

参考資料C

調査表案

sample

PRINCIPLE 3

WebTrust for CA	RFC 3647	電子署名法JIPDEC適合例ver2.3	調査表案
3.1 認証実務規定と証明書ポリシー管理 Certification Practice Statement and Certificate Policy Management CAはその認証実務規定(CPS)と証明書ポリシー(CP)の管理監督が効果的であることを合理的に保証するための支配権を維持する The Certification Authority maintains controls to provide reasonable assurance that the CA's CPS and Certificate Policy (CP) management controls are effective.	4.1.5. ポリシー運用管理 Policy Administration	項番3C01-3C03	JCANルートおよび中間CAにかかるCPSおよび証明書ポリシーは、JCAN内に設置されるxxxx委員会および事務局にて制定し、遵守されていることを監督する。
3.2 セキュリティ管理　Securty Management CAは情報セキュリティに関する管理者の指示と支援が供給されることを合理的に保証するための支配権を維持する The Certification Authority maintains controls to provide reasonable assurance that management direction and support for information security is provided.	4.5. マネジメントコントロール、運用的コントロールおよび物理的コントロール Management, Operational, and Physical Controls	項番3C11-54	JCANルートおよび中間CAにかかる情報セキュリティ方針を定めた文書「xxxx」を制定し、維持管理し、公開しすべての作業者に適切に周知する。 情報セキュリティ方針文書「xxxx」は、その定義、目的と適用範囲、情報共有にかかるセキュリティの重要度の記述を含んでいる。 ：

13

講演５　パネルディスカッション①

電子認証の民間制度・基盤の確立に関するシンポジウム

次の10年に向けた「安信簡」の認証基盤“JCAN”の取り組み（中間報告）

2010年2月4日

財団法人日本情報処理開発協会

1

◆次の10年に向けたビジネス情報環境の変革

最もフレッシュで信頼できる企業/団体（企業等）ベース認証基盤がグローバルな仕組みに連携すると社会情報環境を刷新する。
ビジネスでインターネットを使う全ての人への発行を目指す共通の電子証明書が次の10年を切り開く。

◆企業等が発行しやすくビジネススタイルに合った電子証明書を目指して

①次の対象が会社/団体に属していることを証明
－企業等内個人（肩書き）
－企業等の部門/役割名

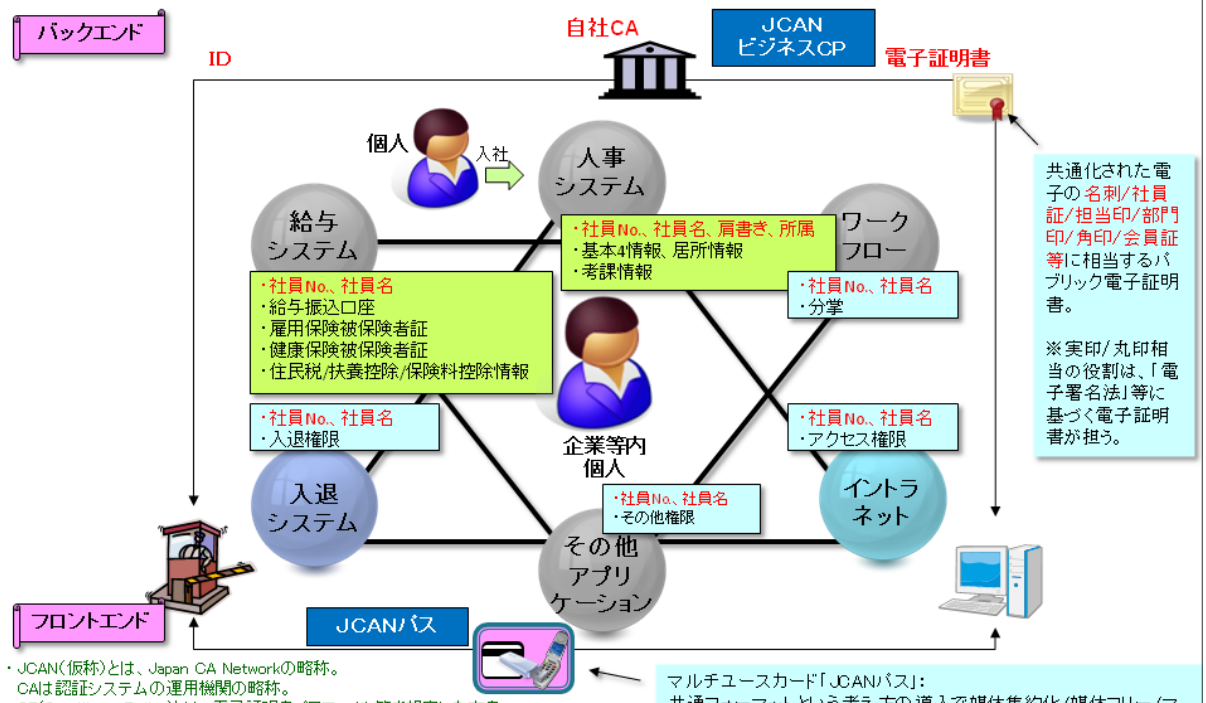
②実名とID・PS名を結びつけた電子証明書とし、肩書き、部門名、役割をオプションとすることで次を実現
－事前の作り込みを可能
－証明書記載事項の変更による失効を減らし有効期限まで使いきることを可能

◆目次

・「安信簡」とは、安心・安全の「安」、信頼性の「信」、簡単・簡便の「簡」からなり、しばしばトレードオフの関係にある情報セキュリティと使い易さを共に向上させていこうという意味を込めた造語。また、その発音が安心感とも重なる。
・PS名とは、Pseudonym（擬名・仮名・別名と訳されることがあるが適切な訳語が定まっていない）の略称。

2

1.JCANビジネスCP



・JCAN(仮称)とは、Japan CA Networkの略称。
CAは認証システムの運用機関の略称。
・CP(Certificate Policy)とは、電子証明書プロファイル等を規定した文書。
・パブリック電子証明書とは、ブラウザ等の「信頼された認証機関」(トラストリスト)でパス検証ができる電子証明書。
・PKCS#12とは、暗証番号(PIN)により保護された秘密鍵と電子証明書を保管するためのファイルフォーマット

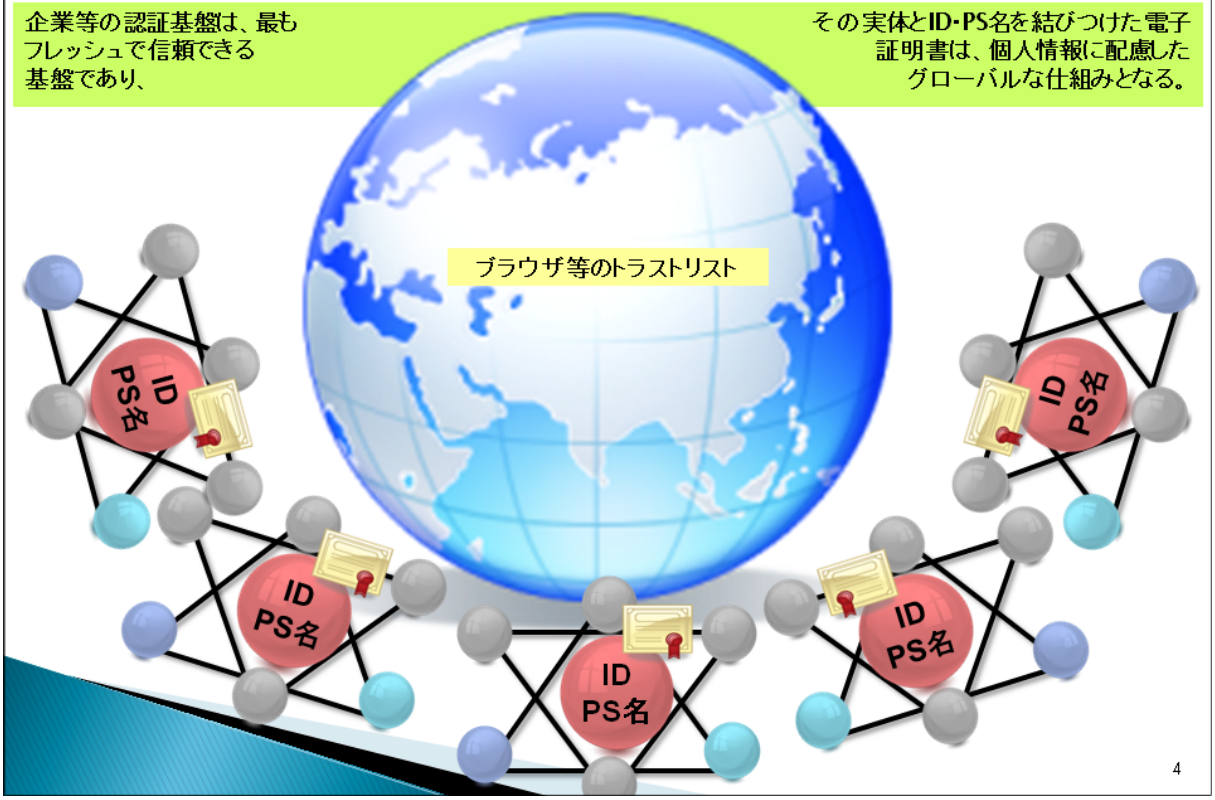
マルチユースカード「JCANパス」:
共通フォーマットという考え方の導入で媒体集約化/媒体フリー/マルチベンダー対応(選択肢提供)、システムの段階的構築を実現。
※JCANパスには、暗号化されたログインパスワードを格納。
(PKCS#12等はPCに格納)
※最初は各種ICカード(TypeA等)、USBメモリへの適用から。

3

狙い

企業等の認証基盤は、最もフレッシュで信頼できる基盤であり、

その実体とID・PS名を結びつけた電子証明書は、個人情報に配慮したグローバルな仕組みとなる。



4

ビジネスメリット

Ⅰ CP/検証環境の共通化(パッケージ化)等による電子認証/電子署名/ID・PS名連携の普及で全体最適化を実現。

※社会的な分担見直しで認証業務の「迅速」「高効率」「高信頼性」化も達成。

Ⅱ 企業等ベース認証基盤の整備による内部統制の強化。

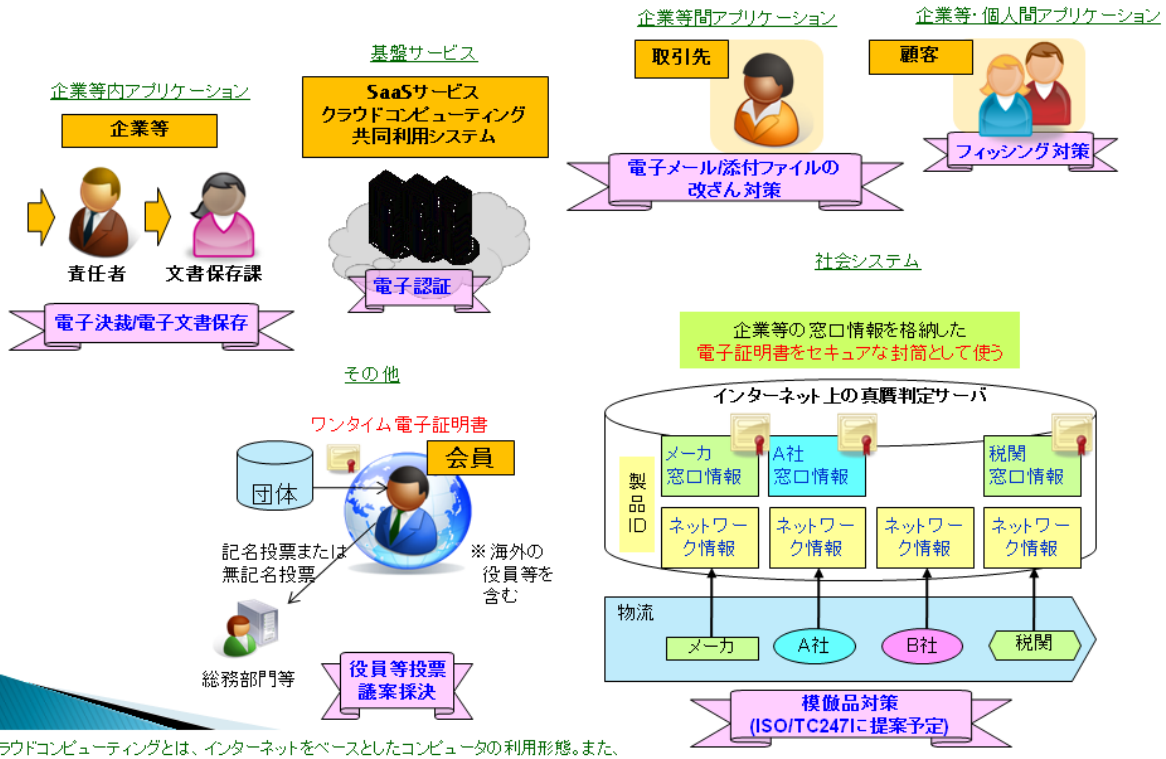
※分掌ルールに基づいた「アクセス管理」「決裁」「文書保存」が求められている。

Ⅲ 共通のルールと認定制度に基づく企業等ベース認証基盤の運用は、社会的な信頼連携を加速する。

※認定制度は、民間ならではの柔軟な運用で企業等の内部監査を調査する。

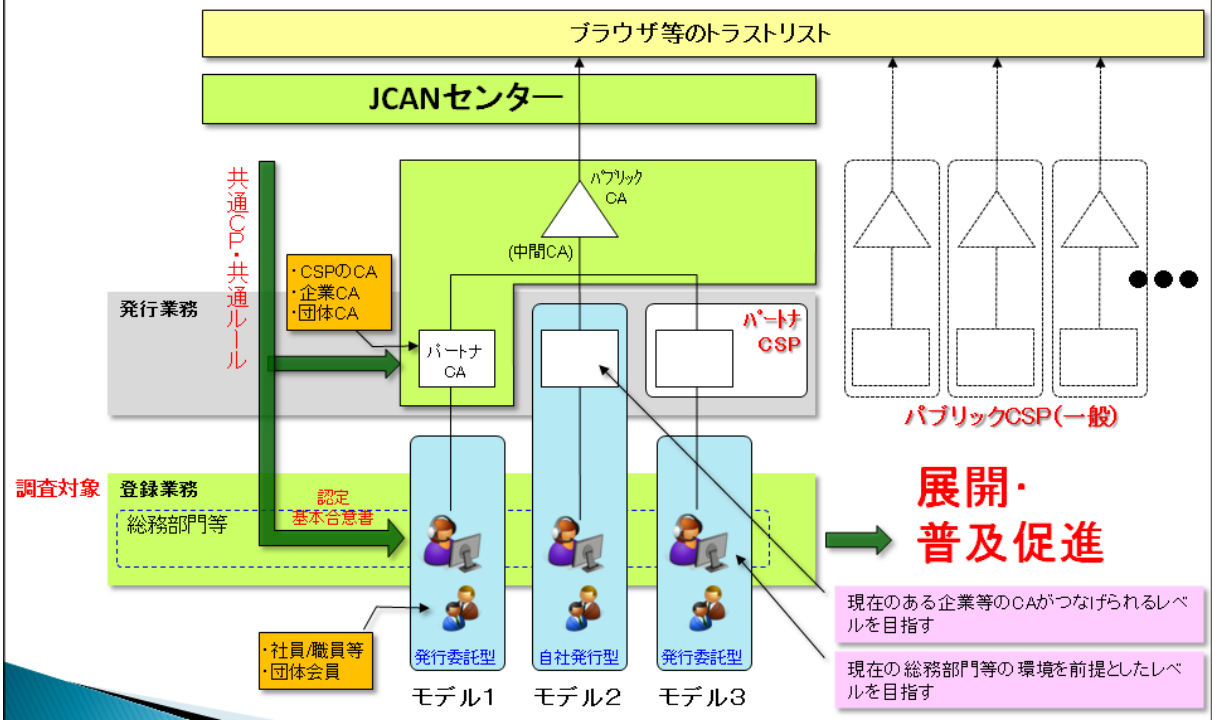
※用途は電子認証及び電子署名。(暗号は利用者に任せる)
※電子メール/添付ファイルへの電子署名は対応必須。
※企業等が専用ドメインアドレスを持つように、自社認証局の普及を目指す。

フラグシップ(キラー)/対応必須アプリケーション



・クラウドコンピューティングとは、インターネットをベースとしたコンピュータの利用形態。また、SaaSとは、ユーザーが利用したい機能を必要になったときにネットワーク経由でサービスプロバイダから入手するサービス。いづれも強力な認証機能が必要。

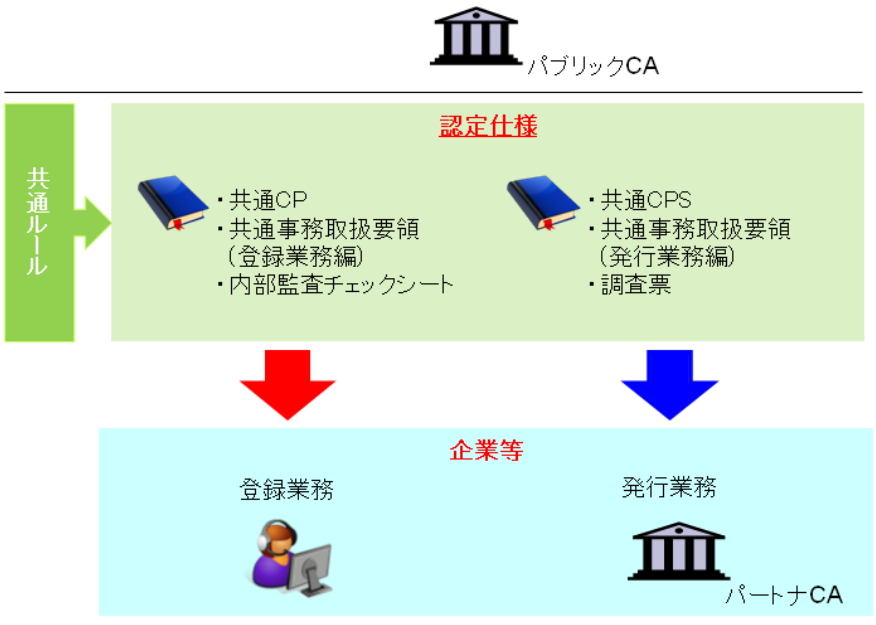
2.基盤イメージ



・CSPは、認証サービス事業者の略称。
・登録業務とは、自社の社員等向け電子証明書の発行失効を指示し貸与/回収する業務。

7

3.JCANビジネスCPに係る共通ルールと認定制度



・ CPS(Certification Practice Statement)とは、認証局運用規程の略称。

8

4.JCANビジネスCPに基づく申請企業の実在確認

標準企業コード
→②で確認

- 証券（銘柄）コード →①で確認
- TDB企業コード →②で確認
- 指定団体発行コード →（検討中）

✓ いずれかの証券市場に上場している → OK

✓ TDB企業コードが登録されている → OK

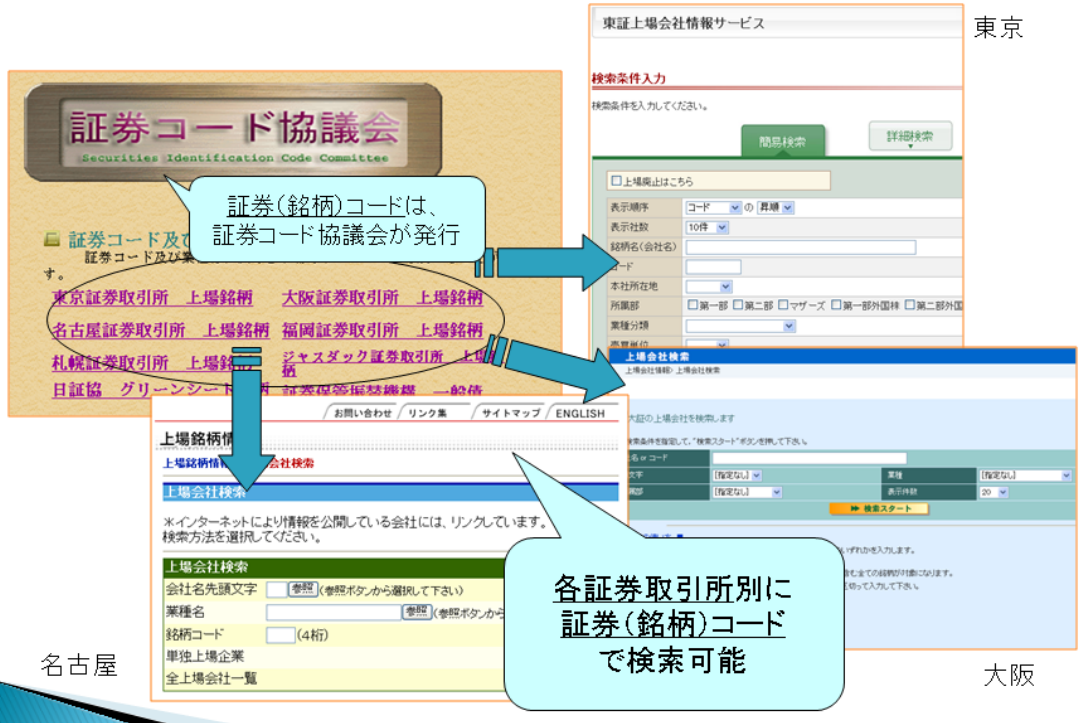
✓ 3年以上指定団体の会員となっている（会費を払っている） → OK

24,188件（2010.1現在）
http://jedic.ecom.jp/code/documents/code_list.pdf

9

4.JCANビジネスCPに基づく申請企業の実在確認

① 証券（銘柄）コード検索



東京

名古屋

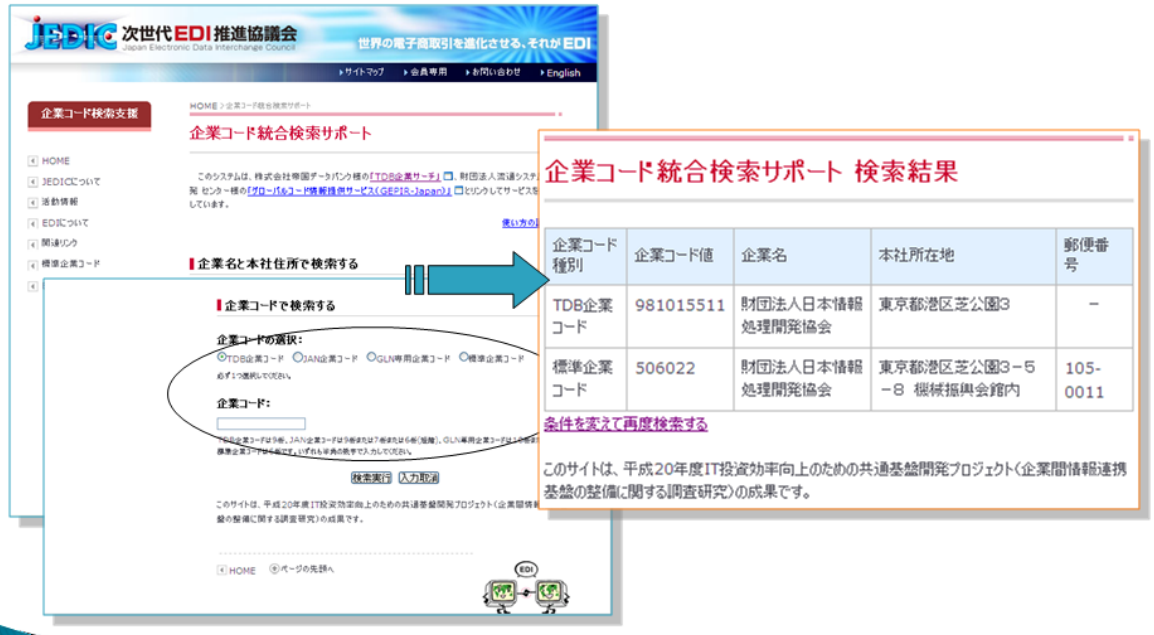
大阪

出典）http://www.tse.or.jp/sicc/

10

4.JCANビジネスCPに基づく申請企業の実在確認

② 企業コード統合検索サポート(JEDIC)



出典)http://jedic.ecom.jp/CodeKensaku/ 11

5. JCANビジネスCPの証明書プロファイル

◆デンマークの証明書プロファイル

社員証明書	
必須	国番号
必須	企業のフルネーム。できる限りCVR（デンマーク中央商用登録）番号を含める。
オプション	部門名
必須	職員ID
オプション	企業の住所
	職員（名）
	職員（姓）
必須	職員のフルネームまたは登録されているPS名、可能な限り肩書も。
オプション	職員の肩書
	職員のPS名
オプション	職員の電子メールアドレス

会社証明書	
必須	同左
必須	同左
オプション	同左
必須	・Qualifier CVR:CVR及び可能で有ればUID:, SE:, P:と連携されていること ・DS 844, section 6.1のIDと連携されていること
オプション	企業の住所
必須	名前、可能であれば他の文字列を-で区切ったもの
オプション	
オプション	会社の電子メールアドレス

13

5.JCANビジネスCPの証明書プロファイル

検討案（抜粋）

■Basic Certificate Fields　　設定例

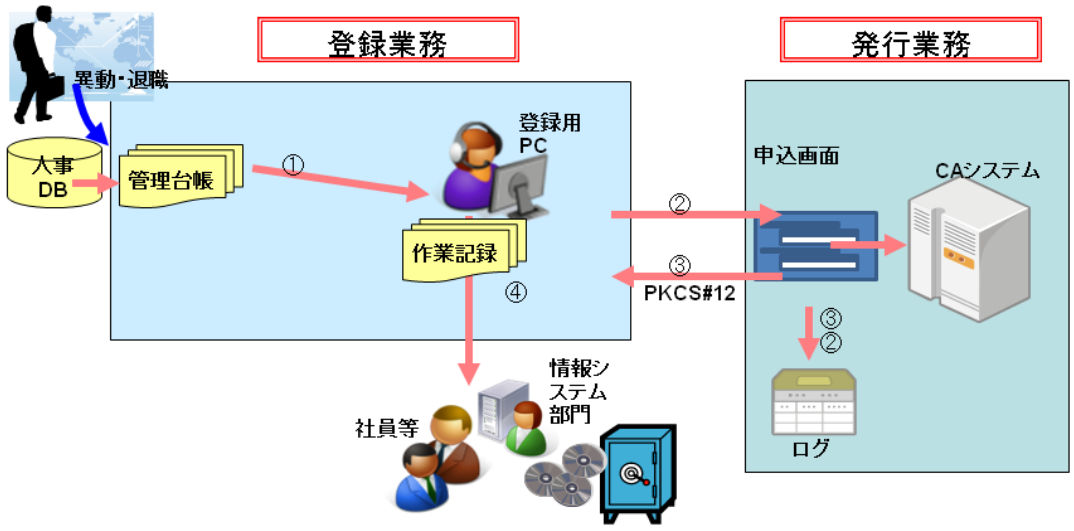
項目 Certificate Fields		データタイプ	企業等内個人向け	部門/役割名向け	
Subject					
	CountryName(C)	PrintableString	JP		必須
	StateName(S)	PrintableString	Tokyo		オプション
	LocalityName(L)	PrintableString	Minato-Ku		オプション
	OrganizationName(O)	PrintableString	ID_1.2.392.200063_JPDEC		必須（企業コード・企業名略称）
	OrganizationUnitName (OU)	PrintableString	8133436XXXX_www.jpdec.or.jp/ra		必須（総務部またはCNの所属部門の電話番号・ホームページ（企業/団体のトップページでも可））
	CommonName(CN)	PrintableString	BN_smith_manager	BN_supply	必須（PS名）
	e-Mail(E)				設定しない（rfc822Nameで設定）
	SerialNumber	INTEGER	YY.YYYY.YYYYYYY	ZZ.ZZZZ.ZZZZZZZ	必須（管理番号）

■Standard Certificate Extensions

subjectAltName					必須
	rfc822Name	IA5String	smith@jpdec.or.jp	supply@jpdec.or.jp	必須（CNまたはCNの所属部門のメールアドレス）

6.JCANビジネスCPの登録業務

◆イメージ



6.JCANビジネスCPの登録業務

管理台帳

共通部分

企業コード	企業名	メールアドレス	電話	ホームページ	操作責任者
1.2.392.200063	JIPDEC	ra@jipdec.or.jp	813343 6xxxx	www.jipdec.or.jp/ra	山田太郎

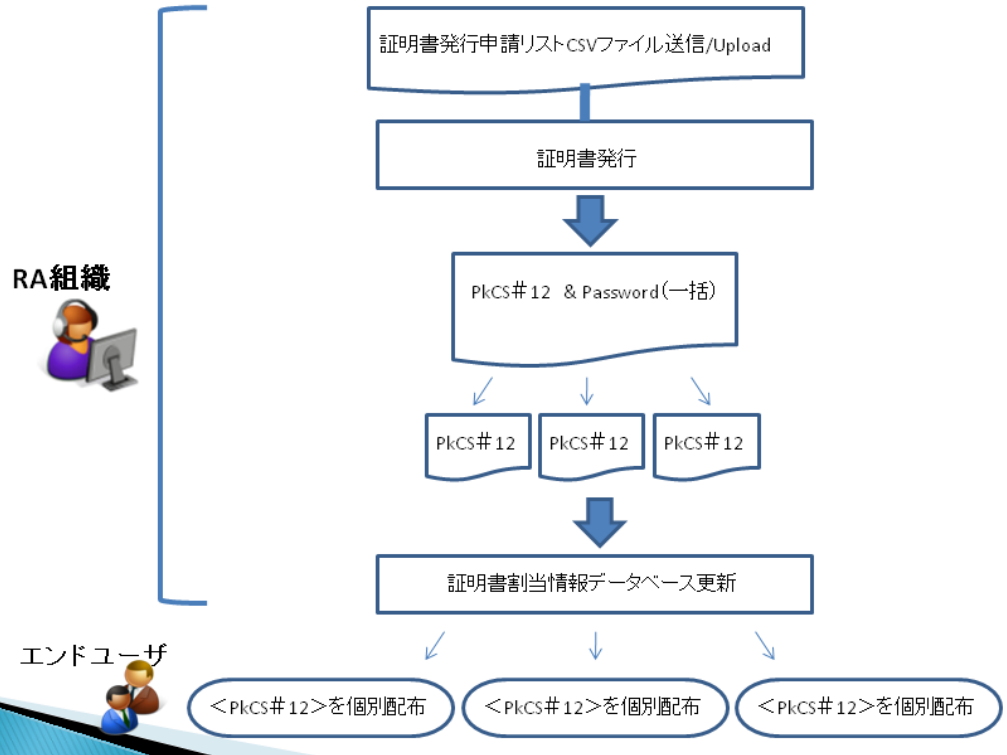
管理番号対応部分

管理番号	メールアドレス	BN名	区分 1.企業内個人 2.部門/役割名	肩書き	部門/役割名	電話	承認日	状態	内部管理データ(提出不要)	
									社員No.	実名
YY.YYYY.YYYY YYYY	smith@jipdec.or.jp	BN_smith_manager	1	課長	資材部	813323 6xxxx	080401	貸与	123	スミス花子
							090331	回収		

16

6.JCANビジネスCPの登録業務

電子証明書貸与方法



17

7.JCANビジネスCPの内部監査チェックシート（1/2）

①登録用PCのアクセス管理			
M-1	登録用PCのログインパスワード管理を「登録業務事務取扱要領」に規定していますか。	□ 規定している。 （章節番号：　　） →具体的な方法は、 □ パスワード □ ICカード □ その他（　　） □ 規定していない。	
M-2	上記パスワード等の定期的な変更を行っていますか。	□ 変更している。 →定期的にパスワードを変更している （最近の変更日　　年　　月　　日） □ 変更していない。	
②スクリーンセーバーのパスワード設定			
M-3	スクリーンセーバーによるパスワードロックは、3分以内に設定されていますか。	□ 設定している。 □ 設定していない。	
③ウイルス対策			
M-4	ウイルス対策ソフトが導入されて、パターンファイルが更新されていますか。	□ 導入している。 →パターンファイルの更新日は、 （　　年　　月　　日　：　） □ 導入していない。	

19

7.JCANビジネスCPの内部監査チェックシート

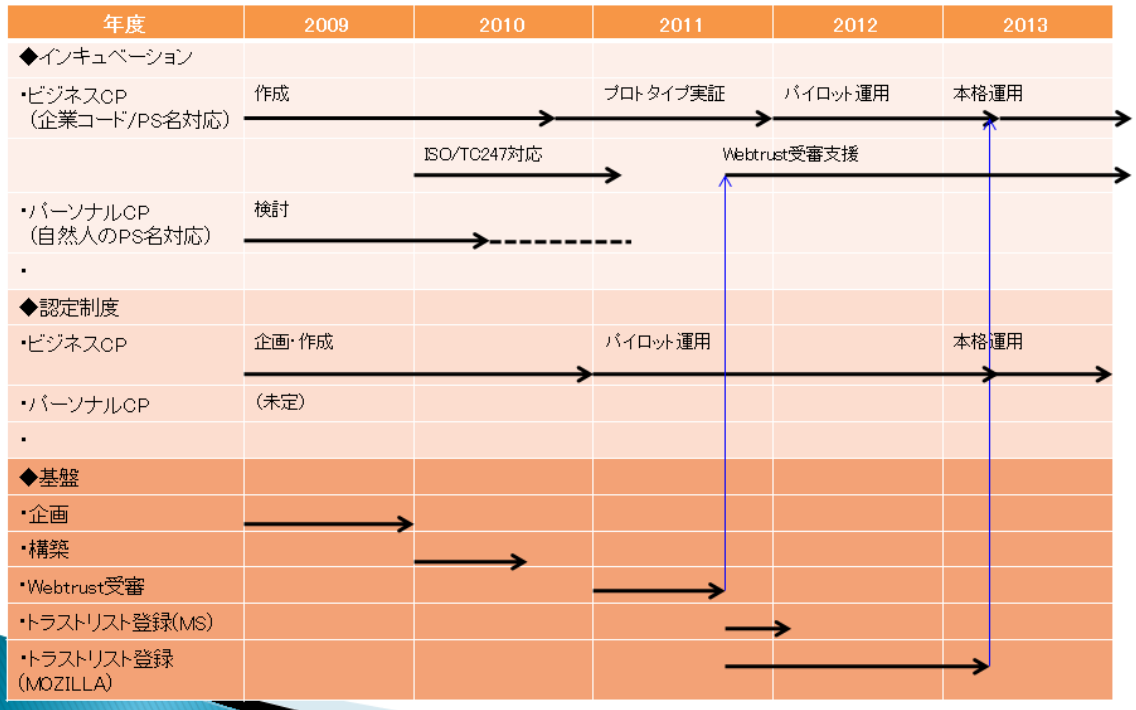
(2/2)

④登録業務			
M-5	電子証明書は、組織に属している対象（企業内個人、部門名、設備等）に貸与していますか。	□ 次の対象に貸与していることを管理台帳で管理している。 □人事DB登録者 □請負・派遣契約で指定された者 □組織体制表で管理されている部門名等 □その他管理簿で確認されている者／設備 □貸与先を管理台帳で管理していない。	
M-6	上記貸与者の異動・退職・変更に伴う管理台帳の内部監査を行っていますか。	□ 上記帳簿と突合せを行なっている。 □有効な電子証明書の総数（約　　） □総貸与数　　（約　　） □過去1年間のメンテナンス数（約　　） □ 行っていない。	異動・退職者総数 失効総数
M-7	登録業務の作業記録を残していますか。	□ 残している。 □ 残していない。	
O-8	登録業務関係者に対して、年に一度又は任命の都度教育をし、教育記録を残していますか。	□ 残している。 □ 残していない。	

20

8.JCANインキュベーション（ベンチャーを支援するサービス・活動）

◆行程表



8.JCANインキュベーション

ビジネスCPプロトタイプ実証

◆目的

電子メール/添付ファイルの改ざん対策、SaaSサービスの電子認証、電子決裁、電子文書保存、模倣品対策等への利用促進

◆施策と目標

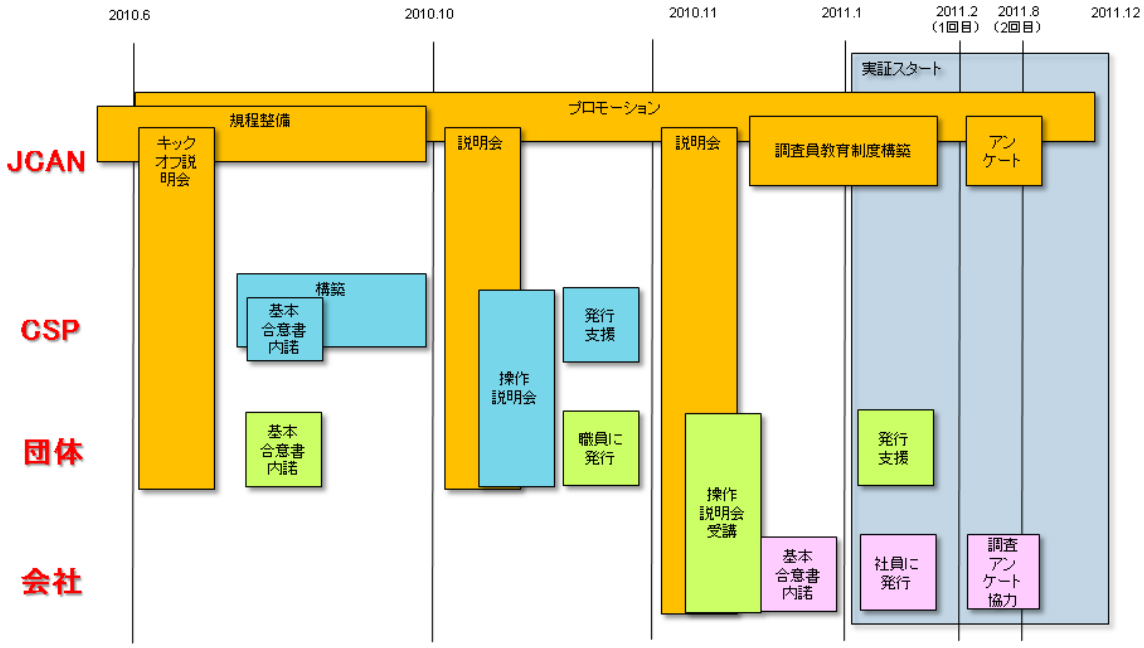
- 電子証明書の発行
- アプリケーションソフトウエアの提供
- パートナCSP、パートナCAへのプロモーション
- 調査員教育制度の準備

◆条件

- 電子メールへの使用に関するアンケート回答
- アプリケーションソフトウエア使用に関するアンケート回答

8.JCANインキュベーション

ビジネスCPプロトタイプ実証のスケジュール（予定）



23

参考：JCANと「安信簡」情報環境プロジェクト

- JCANは、「安信簡」情報環境プロジェクトの重要な柱
- 「安信簡」情報環境プロジェクトは、JIPDECが2009年度から取り組みを開始した新しい民間ベースプロジェクト
- 「安信簡」情報環境プロジェクトとは、インターネット環境における安心・安全、信頼性、簡易性の向上を社会システムの形で実現していこうとするもの

25

参考：「安信簡」情報環境とは？

安全・安心の「安」　信頼性の「信」　簡単・簡便の「簡」

しばしば**トレードオフ**の関係にある**「情報セキュリティ・信頼性」**と**「使い易さ（利便性）」**を、ともに向上させていこうという意味を込めた造語

あんしんかん 安心感

社会システム構築という切り口から全体を高めていく、というアプローチ
目指す方向が**「安信簡」情報環境**

ESSTEC：
an Environment of Safety, Security, Trustworthy, Ease and Convenience

2009/11/24　26

参考：「安信簡」情報環境の構造

「安信簡」情報環境プロジェクトを構成する要素的情報環境には以下のようなものがある。

①商習慣の電子化を支える企業ベースの民間認証環境（JCAN）

②確実な本人確認と個人情報保護を両立させ、C2B環境に画期をなす可能性を持つPS名(Pseudonym)情報環境

③信用に裏打ちされた既存の各種企業IDの連携環境

④企業活動をオープンに結び付けるセキュアな双方向情報交換環境

⑤重要な情報の社会的な保管環境

これらの要素的情報環境・情報基盤は、組み合わさることによって、様々なサービスの土台となる。

Original:
2009/11/24　27

ありがとうございました

http://www.jipdec.or.jp/jcan

連絡先

財団法人 日本情報処理開発協会（JIPDEC）

〒105-0011 東京都港区芝公園3丁目5番8号
機械振興会館 3階

TEL:03-3436-7513

電子商取引推進センター JCAN準備プロジェクト

主席研究員
青木 尚
aoki-takashi@jipdec.or.jp

28

講演６　ビジネスパス

電子認証の民間制度・基盤の確立に関するシンポジウム

JCAN ビジネスパス

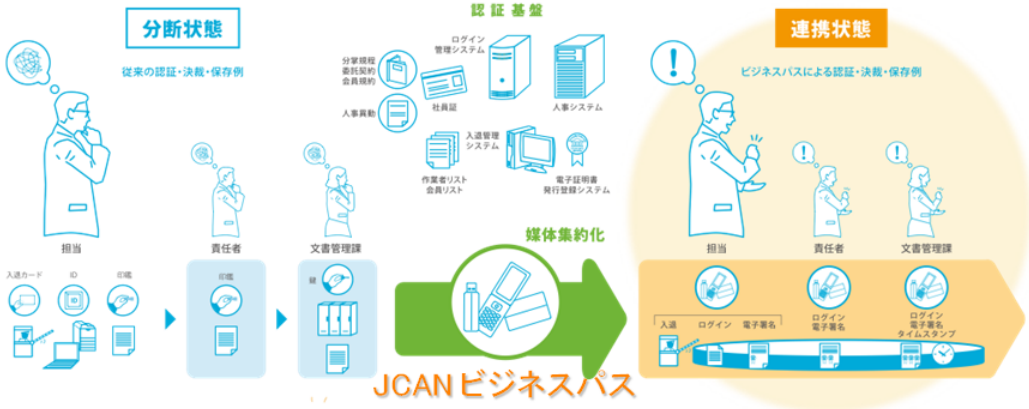
2010年2月4日

マルチユース格納媒体のPKI対応の検討及び
登録業務効率化の検討ワーキンググループ
プロジェクトリーダ　福田昭和
（HARTIN MARTIN CORPORATION）
E-mail: fukuda@hartinmartin.com

1

JCANビジネスパスとは

さまざまな認証基盤の利用を一つの媒体に集約化し、認証・決済・保存とシームレスに連携、ビジネスを効率よく、効果的に行うためのパス



一枚で認証・決済・保存を実現

2

ビジネス・パスの考え方

- 認証に必要なID番号（従業員番号、学籍番号など）や鍵情報、企業情報などを共通フォーマットとして格納し、マルチベンダー環境でも「誰でも、いつでも、安全に」認証サービスを利用できるようにする
- さらに、共通フォーマット内に「空き地」となるエリアを設定しておくことで、後日メモリを必要とするような新たなアプリケーション追加も行いやすくする
- 媒体は、以下のものを検討中
  - 非接触ICカード
  - RFID
  - USBメモリ
  - 携帯電話（SIM）

3

JCAN共通フォーマット

JCAN共通フォーマットはそれぞれの媒体毎にフォーマットを用意するが、格納する基本項目は同一とする

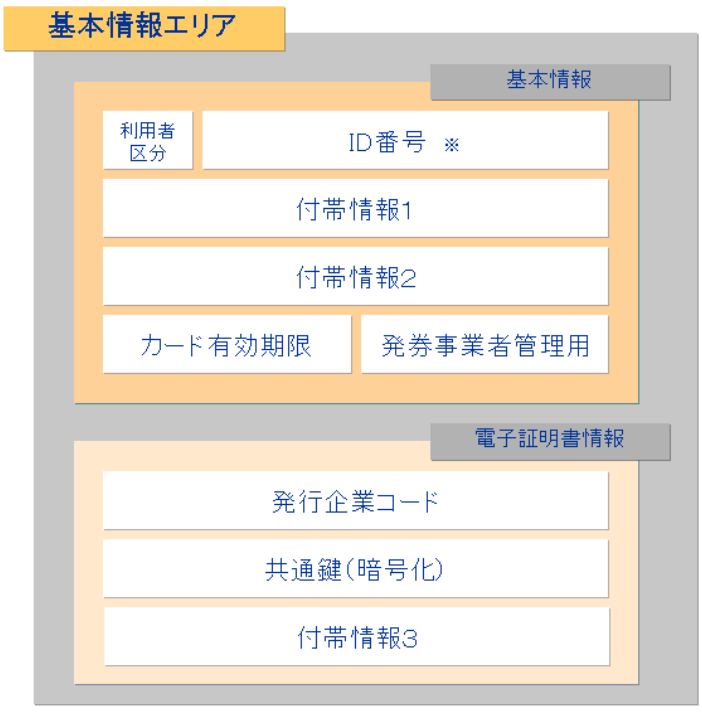
【対象と考える媒体】

- 非接触ICカード
- FeliCa
- TypeA

RFID

- USBメモリ
- 携帯電話（SIM）

共通フォーマット内には電子証明書本体は持たず、電子証明書を呼び出すための共通鍵を格納する。電子証明書の呼び出しは、共通フォーマットに対応したPCアプリで行うことができる

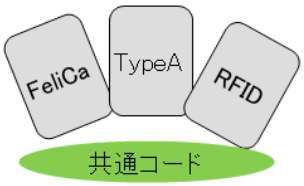


※ID番号：従業員番号、教職員番号、学籍番号など企業や団体で一意の番号

4

共通フォーマット採用のメリット

発行が簡単

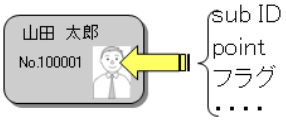


カード発行会社が用意した「レディメード」なので、各種申請・登録手続きが簡単で、フォーマット設計が容易です

ID情報や共通鍵情報が使える

ID情報や電子証明書情報などの実装フォーマットが共通なので、様々なベンダーの新たなアプリケーションに利用できる

メモリを使うサービスの追加ができる



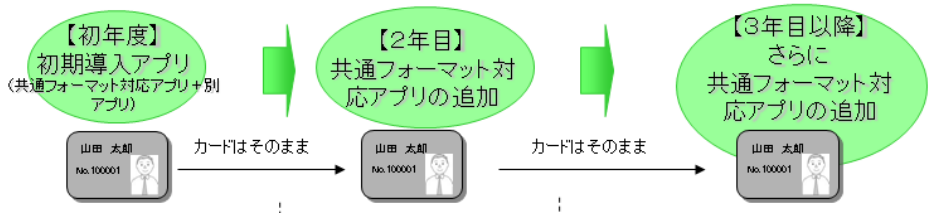
初期発行時に空きフォルダを設定することで、発行後でも、サービス追加ができます

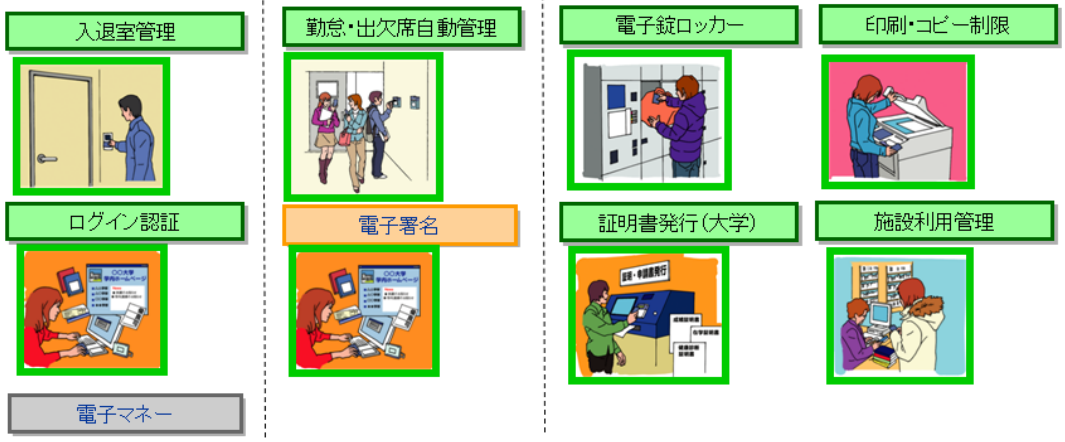
システムの段階的導入・マルチベンダー環境を促進

5

段階的なサービスの導入

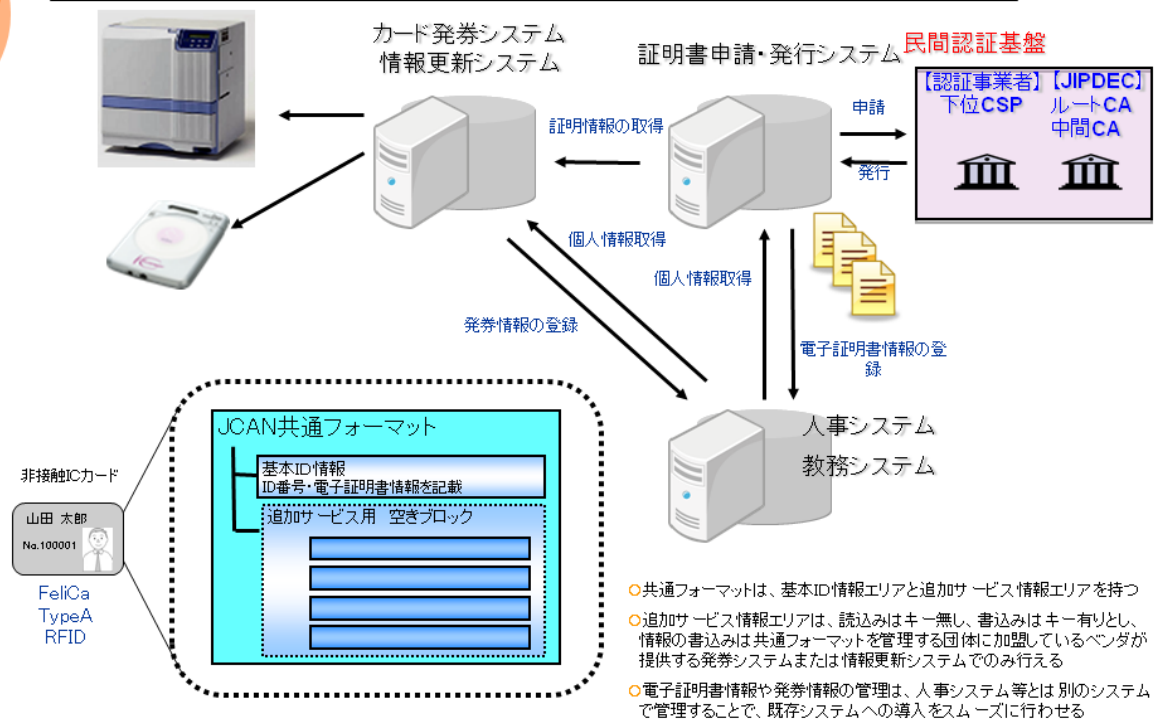
共通フォーマット対応アプリなら段階的なサービス導入が可能です





6

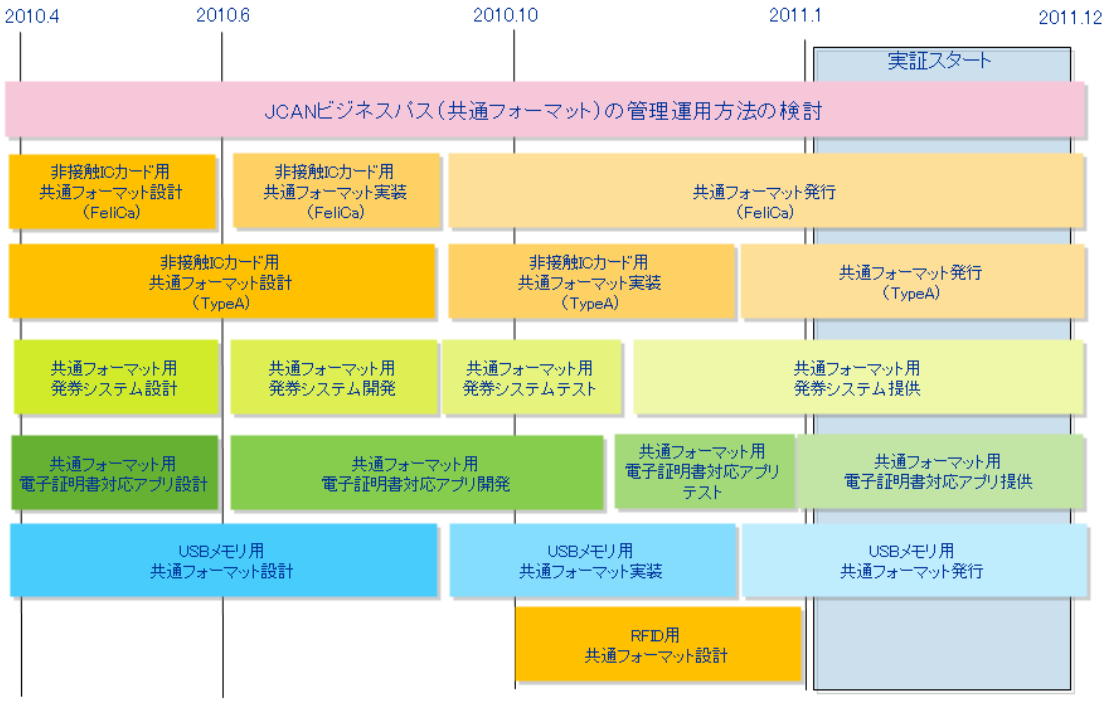
JCANビジネスパスへの情報登録（案）



- 共通フォーマットは、基本ID情報エリアと追加サービス情報エリアを持つ
- 追加サービス情報エリアは、読込みはキー無し、書込みはキー有りとし、情報の書込みは共通フォーマットを管理する団体に加盟しているベンダが提供する発券システムまたは情報更新システムでのみ行える
- 電子証明書情報や発券情報の管理は、人事システム等とは別のシステムで管理することで、既存システムへの導入をスムーズに行わせる

7

スケジュール



2

共通フォーマット推進体制

- 検討組織：FeliCa共通利用フォーマット推進フォーラム （FCF）
  - 2004年2月設立
  - FCFを活用した、ID認証カードの普及促進・各会員のビジネス活性化・顧客へのサービス向上を目的とした非営利団体
  - 参加企業：116社（2010年1月現在）
    - 共同印刷（株）／昌栄印刷（株）／ソニー（株）／大日本印刷（株）／ 凸版印刷（株）／トッパン・フォームズ（株）／ソニーブロードバンドソリューション（株）
    - FeliCa発券ライセンスを有する全企業とカードソリューション企業
  - URL:http://www.fcf.jp/
  - e-mail: fcf.adm@sbs.sony.co.jp
  - 共通フォーマット普及状況
    - 企業向け採用数　　30社　約16万枚
    - 教育機関向け採用数　72機関（大学、高校、中学）　約40万枚

※現在、FCFは任意団体から法人組織への移行を検討中です。法人化後は、媒体に捕われないIDの共通フォーマットを定義・運用・普及を行う計画です。

FCF http://www.fcf.jp/

講演７　韓国における認証基盤について

The Practical use of Electronic Signature in PKI

Moon, Sung Eun
KOSCOM Co. ,

February 4, 2010

PKIに基づく電子署名の利用状況

Moon, Sung Eun
KOSCOM Co.,

2010年2月4日

Index

目次

1. PKI status in Korea

1. 韓国におけるPKIの現状

Related Law

Electronic Trade Basic Law	• **Ministry of Knowledge & Economy** • Established in 1999 / revised in 2002, 2005, 2007 • Legal effectiveness for electronic documents
Electronic Signature Law (NPKI)	• **Ministry of Public Administration and Security (MOPAS)** • Established in 1999 / revised in 2001, 2005 • Legal force clarification for a electronic signature
Electronic Government Law (GPKI)	• **Ministry of Public Administration and Security** • Established in 2001 • Regulation for official document in government

関連法

電子商取引基本法	•大韓民国知識経済部 (Ministry of Knowledge Economy) • 1999年に成立 / 2002年, 2005年, 2007年 に改正 • 電子文書の法的効果
電子署名法 (NPKI)	•大韓民国行政安全部 (MOPAS) • 1999年に成立 / 2001年, 2005年に改正 • 電子証明の法的効力
電子政府法 (GPKI)	•大韓民国行政安全部 (MOPAS) • 2001年に設立 • 政府公文書の規制

Stages of Korea PKI

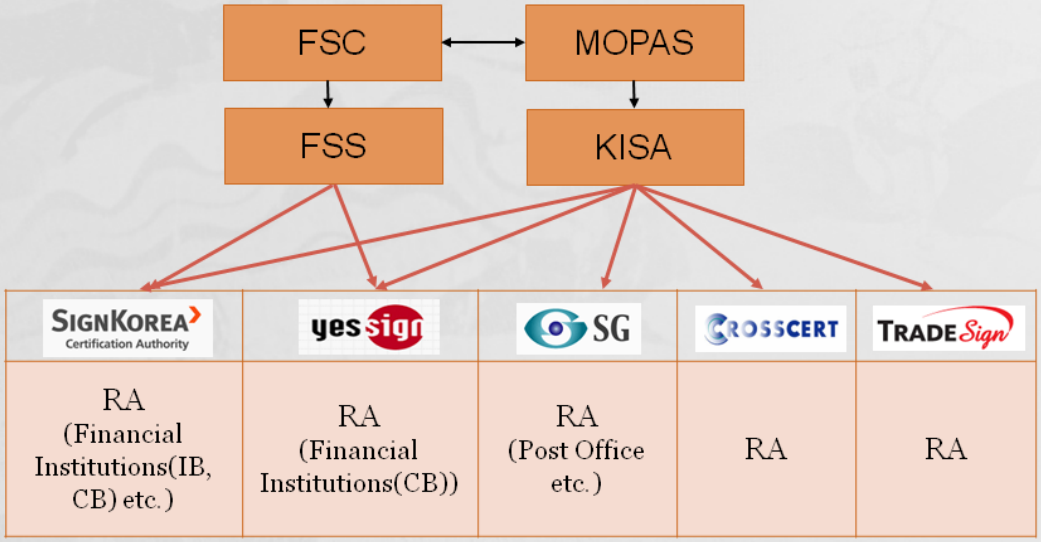
- **Introduction : 1999 ~ 2001**
  - Electronic Signature Law, Accredited CAs
  - Interoperability among Accredited Cas
- **Take-off : 2002 ~ 2005**
  - Providing User-friendliness, Increase in certificates and applications
  - Mandatory use of certificates (Banking, Stock)
  - Cross Certification for NPKI and GPKI
- **Maturity : 2006 ~ 2008**
  - Upgrading of PKI technologies(RFC3280, RSA 2048)
  - Addition of Root CA Certificate to Microsoft IE for secure web server
  - Providing users with secure environment (HSM)
- **Reinforcement : 2009 ~ 2011**
  - Enhancement of electronic Signature Cryptosystem
  - improvement of certificate storage and reissuance procedures

韓国PKIの発展経緯

- **導入期: 1999～2001年**
  - 電子署名法、認定認証局
  - 認定認証局連携
- **進化期: 2002～2005年**
  - 使いやすさの向上、電子証明書およびアプリケーションの普及
  - 電子証明書の使用の義務化（金融、株式）
  - NPKIとGPKIの相互認証
- **成熟期: 2006～2008年**
  - PKIテクノロジーのアップグレード（RFC3280、RSA 2048）
  - セキュアWebサーバーに対応したMicrosoft IEへのルートCAの追加
  - ユーザーに向けた安全な環境（HSM）の提供
- **強化期: 2009～2011年**
  - 署名暗号方式の強化
  - 電子証明書保存と再交付手続の改善

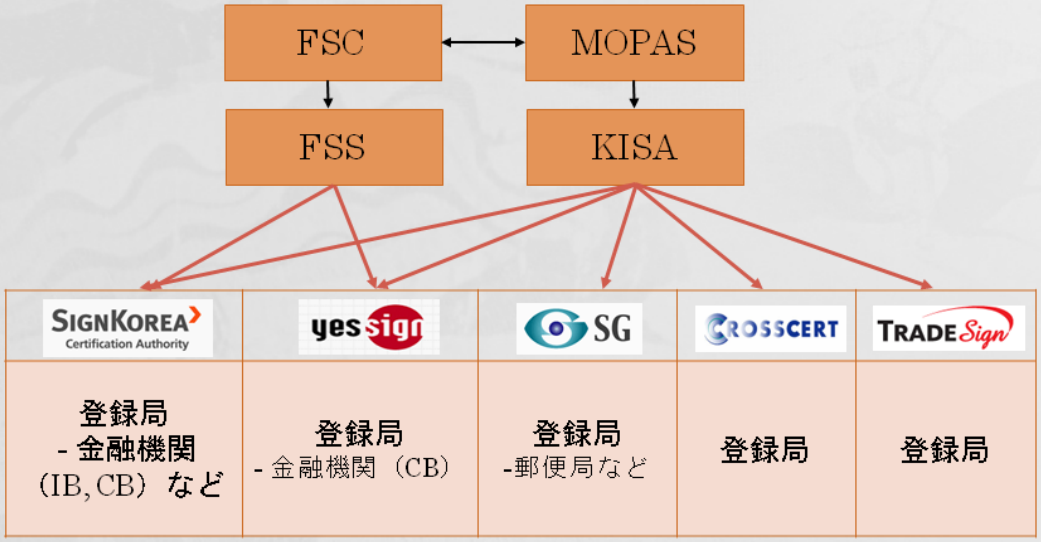
Accredited CA

- 5 CAs are accredited by MOPAS until now



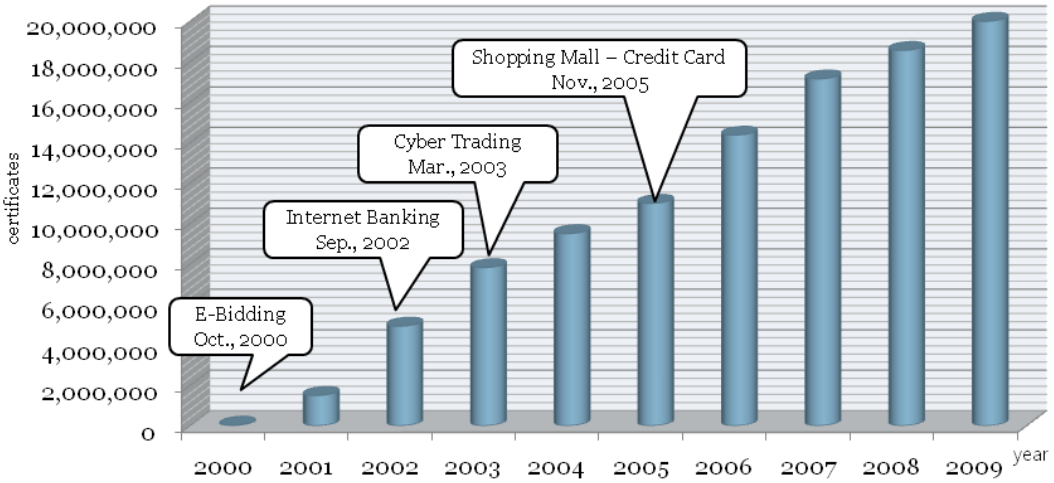
認定認証局

- 現在までにMOPASより5つの認証局が認定済み



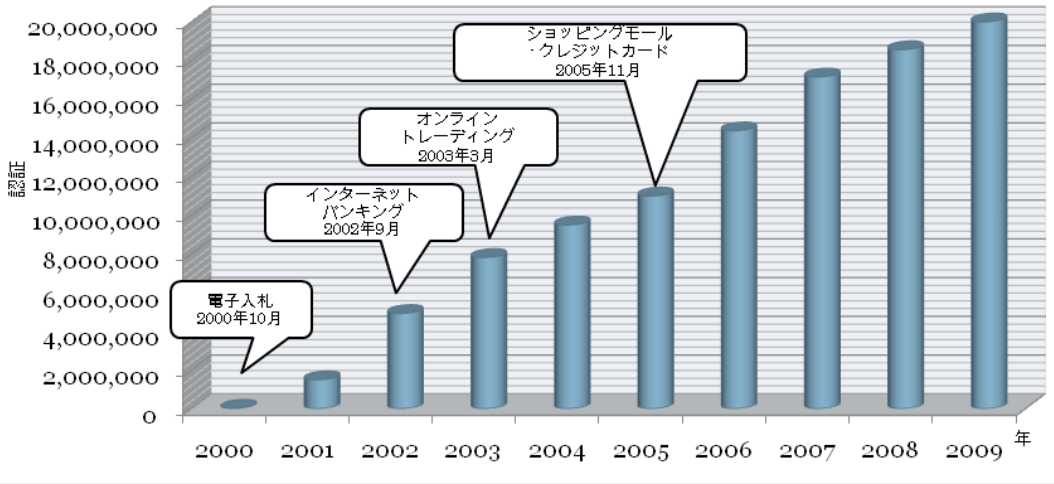
Number of accredited certificates

5 Accredited CAs issued accredited certificate to subscriber around 20million in total

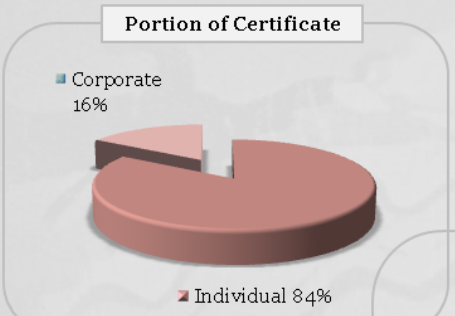


認定電子証明書の数

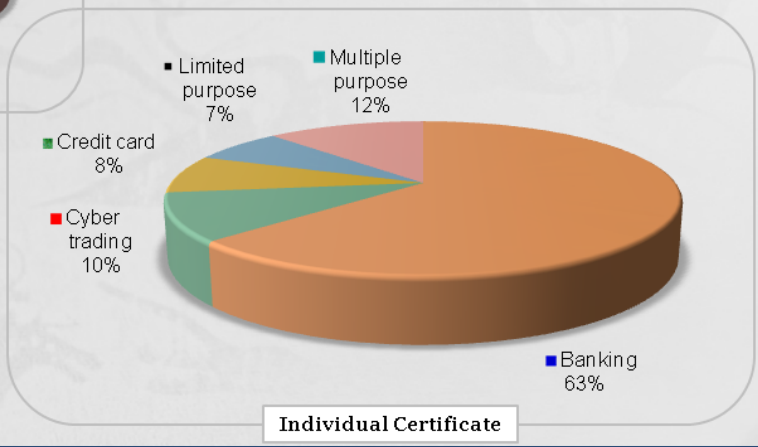
5つの認定認証局から加入者に発行された認定電子証明書数は、
合計で2000万前後に



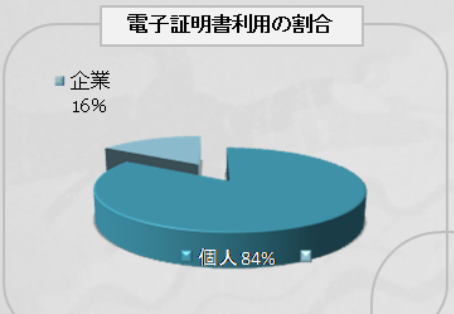
Status of certificate usage



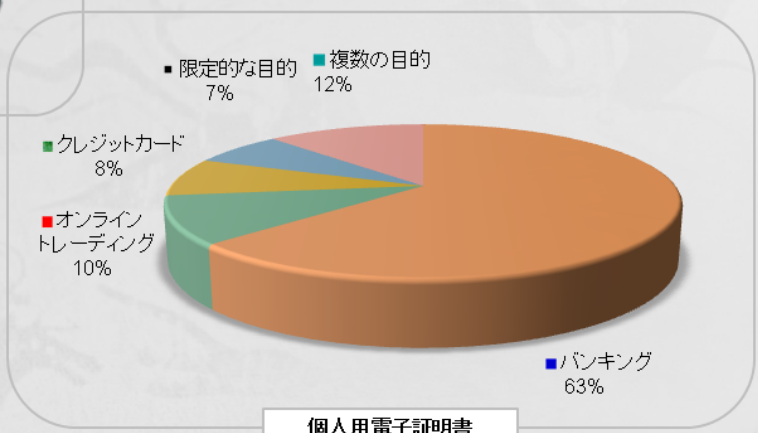
- Multiple purpose : Used for all e-transaction by a corporation or an individual
- Limited purpose : Used only for special purpose (banking, cyber trading) by a corporation or an individaul



電子証明書利用の現状



- **複数の目的**:企業や個人による全ての電子取引に使用
- 限定的な目的:企業や個人による特別な目的 (バンキング、オンライントレーディング)にのみ使用



2. Practical use of Electronic Signature in PKI

2. PKIに基づく電子署名の利用状況

Financial Business

Cyber Securities Trading

- Securities corporations provide online stock service based on accredited certificate
- Online stock users must use the accredited certificate for secure online transaction ('03. 3)

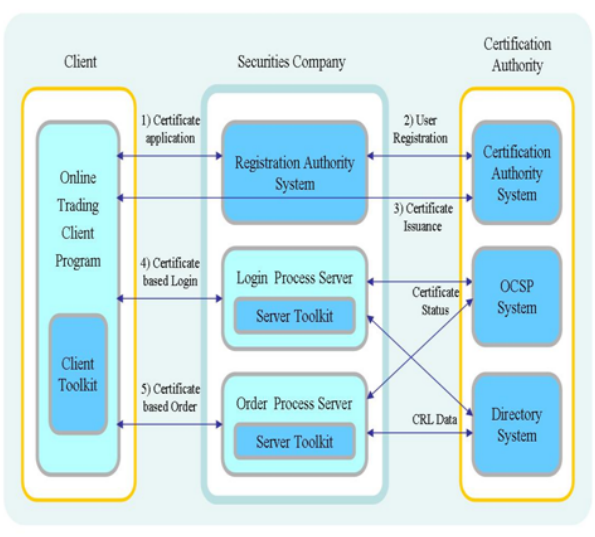
金融

電子証券取引

- 証券会社は、認定電子証明書に基づいてオンライン株取引を提供
- オンライン株取引のユーザーには、安全なオンライン取引のために認定電子証明書の使用が義務付けられる（2003年3月）

Financial Business

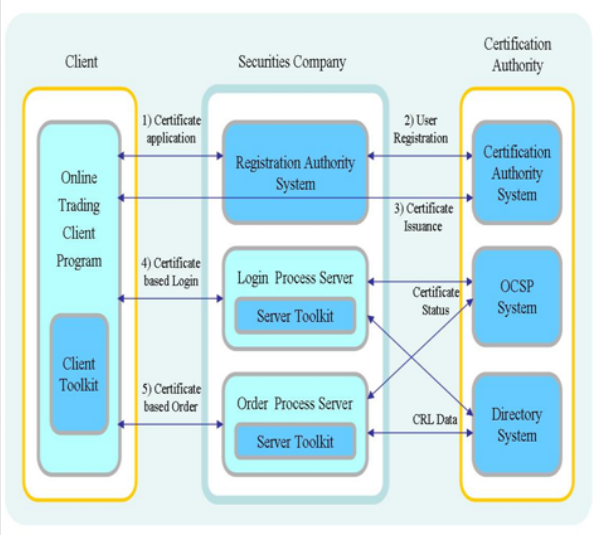
Cyber Securities Trading : Service Process



1) The Client applies a certificate to the CA via the RA in order to execute online trading transactions.
2) The RA requests User Registration to the CA.
3) The Client connects to the CA and receives a certificate.
4) "Login Process Server" executes the certificate verification and electronic signature verification via OCSP or CRL.
5) After the certificate verification, the online order transactions are executed electronic signature and verification automatically.

金融

電子証券取引: サービスプロセス



1) 顧客は登録局を介して認証局に電子証明書を適用し、オンライントレーディングを実施する
2) 登録局は認証局にユーザー登録を要求する
3) 顧客は認証局に接続し、電子証明書を受け取る
4) 「ログインプロセスサーバー」が電子証明書の内容を確認し、OCSPまたはCRLを通じて電子署名の検証を実行する
5) 電子証明書の内容確認後、オンラインオーダートランザクションで電子署名の検証が自動的に実行される

Financial Business

Cyber Securities Trading : Security Features

Certification and Sections to be encrypted

- Certificate issuance/reissuance/renewal via RA system
- User registration, system login-in and online transter

Method of authentication and encryption

- C/S type-enctypted communication using plug-in security modules
- Certificate validation via OCSP and CRL
- Secure certificate password linked with keyboard security modules
- As 2 factor-authentication, electronic certificate is used with security card and OTP (One Time Password)

Expected effects

- Integrity, confidentiality and non-repudiation of financial transaction's hitories
- Online-certification of users
- Secure financial transactions via End-to-End security

金融

電子証券取引: セキュリティ機能

認証と暗号化対象のセクション

- 登録局システムによる電子証明書の交付/再交付/更新
- ユーザー登録、システムログイン、オンライン転送

認証方式と暗号化

- プラグインセキュリティモジュールによるC/S型の暗号化通信
- OCSPおよびCRLを介した電子証明書の妥当性チェック
- キーボードセキュリティモジュールにリンクした安全な電子証明書パスワード
- 二因子認証として電子証明書とセキュリティカード、およびOTP（ワンタイムパスワード）を併用

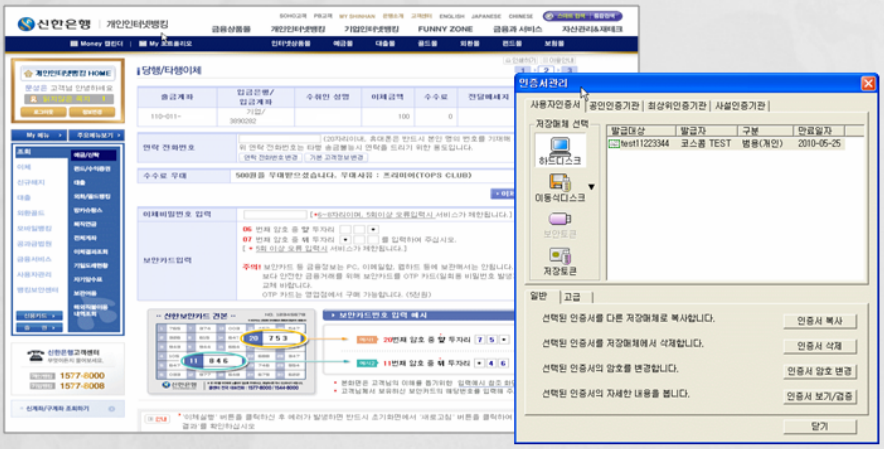
期待される効果

- 金融取引の履歴に関する完全性、機密性、否認拒否
- ユーザーのオンライン認証
- エンドツーエンドセキュリティによる安全な金融取引

Financial Business

Internet Banking

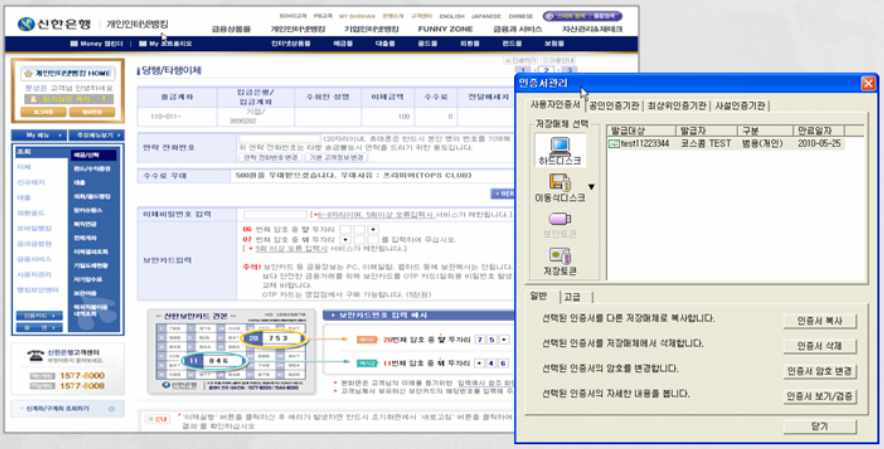
- 19 Banks and Post Office provide internet banking service based on accredited certificate
- Internet banking users must use the accredited certificate for secure online transaction ('02. 9)



金融

インターネットバンキング

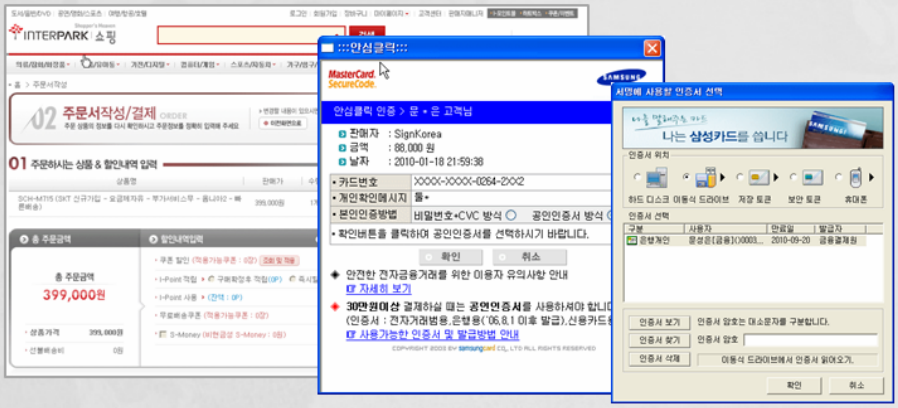
- 19の銀行と郵便局が認定電子証明書に基づくインターネットバンキングサービスを提供
- インターネットバンキングユーザーには、安全なオンライントランザクションの保証のために認定電子証明書の使用が義務付けられる（2002年9月）



e-Payment Business

Internet Shopping : Credit Card

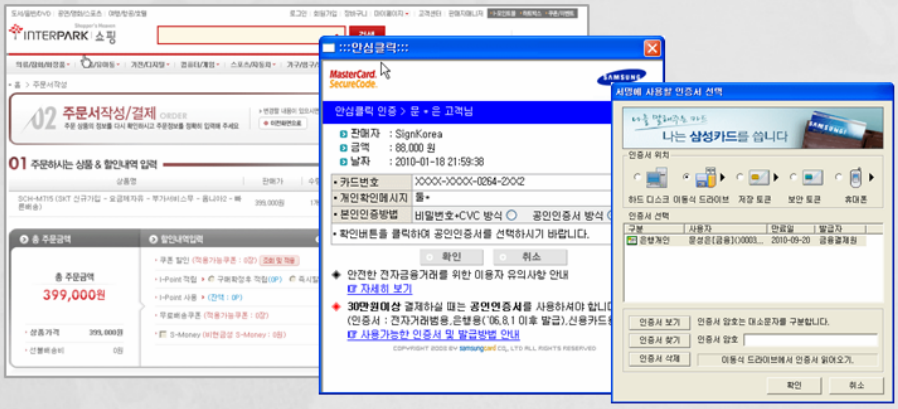
- Credit card should be used with accredited certificate to enhance the security of digital payment process
- Regarding the transaction of over 300,000 won internet shopping, purchasers are required to use accredited certificate ('05. 11)



電子決済

インターネットショッピング: クレジットカード

- デジタル決済プロセスの安全性強化のためにクレジットカードと認定電子証明書の併用を義務化
- 30万ウォンを超えるインターネットショッピングの取引について、購入者には認定電子証明書の使用が義務付けられる（2005年11月）



e-Tax Business

e-Tax invoice

- To reduce taxpayers' compliance cost and to enhance transparency of business transaction between business companies, the e-Tax Invoice is to be commenced from January 1st, 2010
- The e-Tax Invoice is an online tax invoice system which enables online issuance and distribution of a tax invoice, and transmission to the NTS

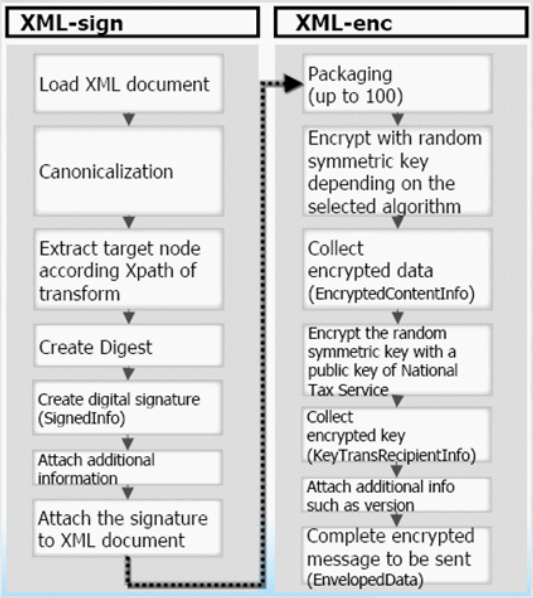
電子申告・納税

e-Tax Invoice

- 納税者の規制遵守コストを低減し、企業間取引の透明性を強化することを目的として、2010年1月1日よりe-Tax Invoiceを開始
- e-Tax Invoiceは、国税庁に申請する税還付請求書のオンラインでの交付、配布、および転送を支援するオンライン税金払い戻しシステム

e-Tax Business

e-Tax invoice : Security Features



Certification and Sections to be encrypted

- Applying detached signature to e-tax invoice
- Encyption is used for transferring e-tax invoice to NTS securely

Method of authentication and encryption

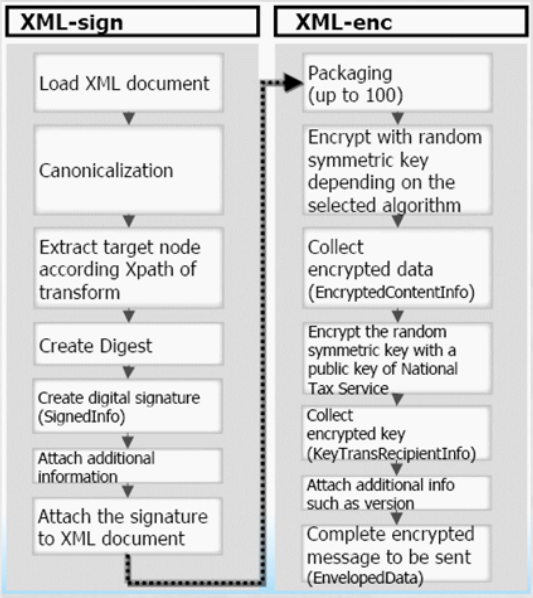
- W3C XML Signature Syntax and Processing (RFC 3275)
- IETF RFC 3852 CMS (Cryptographic Message Syntax)
- Issuer identification of e-Tax Invoices using certificates

Expected effects

- Integrity, confidentiality and non-repudiation of e-tax invoice
- Monotonous work and failures in manual handling decreased
- Face-to-face confrontation between taxpayers and officials decreased
- Increasing use of e-tax invoices which are reliable and secure

電子申告・納税

e-Tax Invoice: セキュリティ機能



認証と暗号化対象のセクション

- e-Tax Invoiceへの分離署名の適用
- 暗号化によりe-Tax Invoiceを国税庁へ安全に送信する

認証方式と暗号化

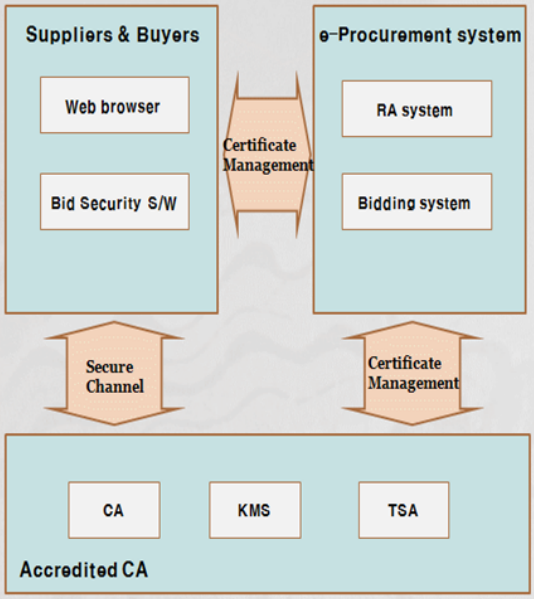
- W3C XML Signature Syntax and Processing (RFC 3275)
- IETF RFC 3852 CMS (Cryptographic Message Syntax)
- 電子証明書によるe-Tax Invoice発行者の身元確認

期待される効果

- e-Tax Invoiceに関する完全性、機密性、否認拒否
- 単純作業と手作業の処理に伴うエラーを低減
- 納税者と局員の間での対面的なやり取りが減少
- 信頼性と安全性を約束するe-Tax Invoiceの利用が拡大

e-Procurement Business

e-Procurement : Service Process



Certification and Sections to be encrypted

- 5 accredited Cas issue certificate to suppliers and buyers
- User registration, system login-in and submitting and opening application documents

Method of authentication and encryption

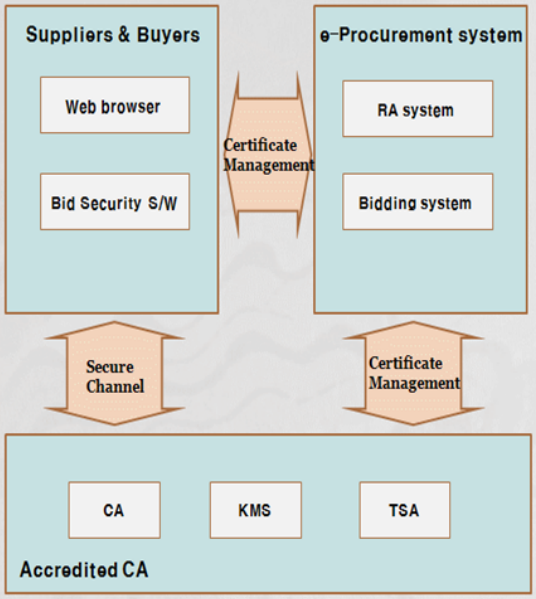
- Applying XML Signature and XML Encryption to application document to application documents
- Online identification of suppliers and buyers who use electronic certificates
- TSP (Time Stamping Protocol)
- KMS (Key Management System)

Expected effects

- Verifying forgery and modification of bid document
- Company identity and ban a bid of illegal company
- Prevention of opening problems caused by loss or damage of encryption private key
- Prevention of troubles for the bidding deadline
- Proof of existence of bid document at certain time

電子調達

電子調達: サービスプロセス



認証と暗号化対象のセクション

- 5つの認定認証局が供給業者や購入者に電子証明書を交付
- ユーザー登録、システムログイン、申請書類の提出と表示

認証方式と暗号化

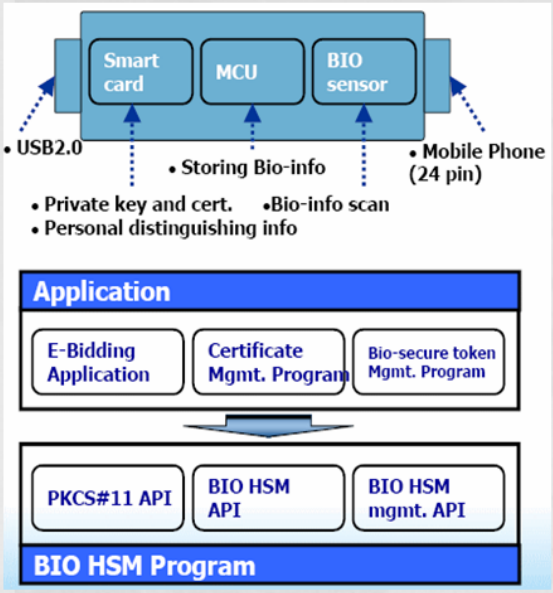
- 申請書類にXML署名とXML暗号化を適用
- 電子証明書を使用した供給業者と購入者のオンライン身元確認
- TSP（タイムスタンププロトコル）
- KMS（キーマネージメントシステム）

期待される効果

- 入札文書の偽造、および改ざんの検証
- 企業の識別と違法企業による応札の禁止
- 暗号用秘密鍵の喪失、または損傷が原因で起きる問題の防止
- 応札期限に伴うトラブルの防止
- 特定時点における入札文書の有無の証明

e-Procurement Business

e-Procurement : Bio HSM



Certification and Sections to be encrypted

- Using Suppliers' and Buyers' certificates stored in Bio HSMs
- Promoting mandatory use of BIO HSM on joining in wireless environment such as PDA and mobile phone
- User registration, system log-in and submitting and opening application documents

Method of authentication and encryption

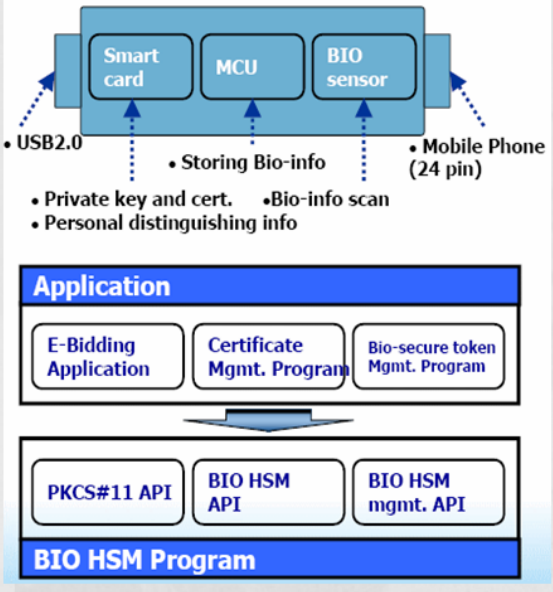
- PKCS#11 API as interface of PKI application and BIO HSM
- BIO HSM API to manage HSMs

Expected effects

- Certificate owners can create their electronic signature via verifying fingerprint information stored in BIO HSM and prevent problems caused by lent or lost certificates
- BIO HSM offers dedicated hardware-based key management to protect personal certificate from attack
- All electronic signing operations are performed within the BIO HSM to increase performance and maintain

電子調達

電子調達: BIO HSM



認証と暗号化対象のセクション

- BIO HSMに保存された供給業者、および購入者の電子証明書を使用
- PDAや携帯電話などのワイヤレス環境に入る際にBIO HSM使用の義務付けを強化
- ユーザー登録、システムログイン、申請書類の提出と表示

認証方式と暗号化

- PKIアプリケーションとBIO HSMのインタフェースとして使用するPKCS#11 API
- HSMを管理するBIO HSM API

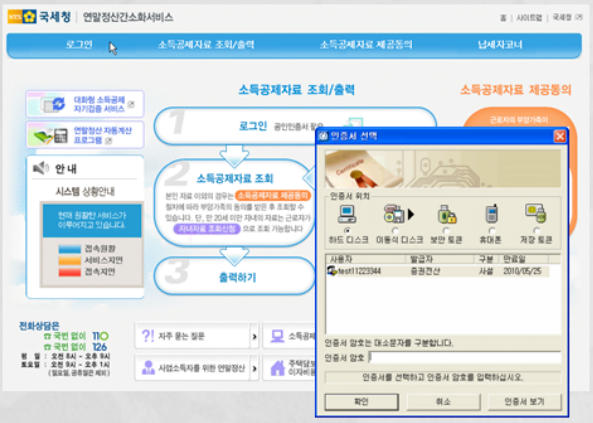
期待される効果

- 電子証明書の所有者は、BIO HSMに保存された指紋情報を検証して、電子署名を作成したり、電子証明書の貸与や紛失が原因で生じる問題を防止したりできる
- BIO HSMにより、ハードウェアベースのキーマネージメントが可能になるため、個人の電子証明書を攻撃から守ることができる
- 電子署名の処理はすべてBIO HSM内部で実行されるため、パフォーマンスの改善とセキュリティの維持が可能になる

Public Business

Public Service

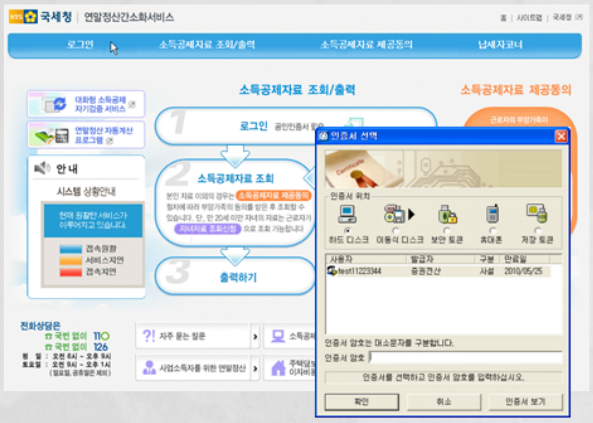
- Housing subscription deposit system, Education, Medical Information, e-bidding ('06)
- Housing subscription, the year-end tax adjustment, NEIS, National health Insurance, etc.



公共事業

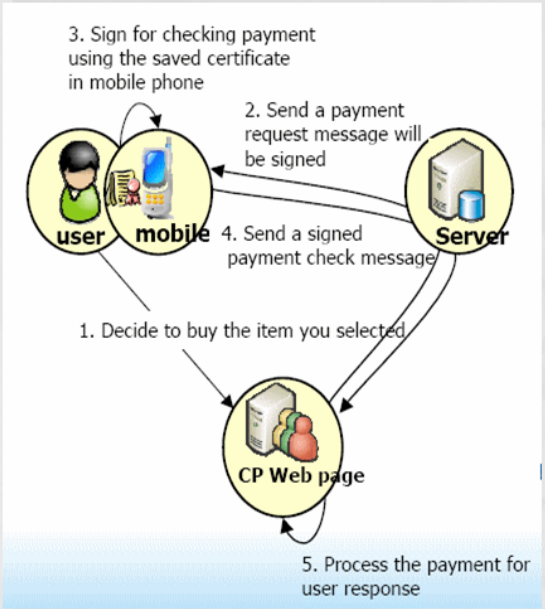
公共サービス

- 住宅予約金システム、教育、医療情報、電子入札（2006年）
- 住宅予約金、年末調整、NEIS、国民医療保険など



Mobile Business

Mobile e-Signing



Authentication and Sections to be encrypted

- Certification service via mobile phone where user's certificate is stored
- Able to use in 3 mobile service providers' environment (SKT, KT, LGT)

Method of authentication and encryption

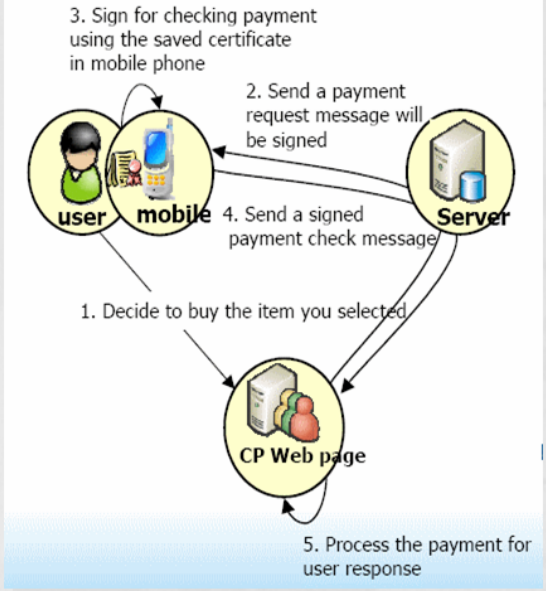
- Sending encrypted or signed data by performing computing operation inside mobile phone
- Service VM is installed in mobile phones in order to use certificates
- Storing certificates into a mobile phone to prevent memory hacking

Expected effects

- User have control to save and sign anywhere, anytime
- Expand the PSE to mobile phone

モバイル

モバイル電子署名



認証と暗号化対象のセクション

- ユーザーの電子証明書を保存した携帯電話による認証サービス
- 3つのモバイルサービスプロバイダ環境（SKT、KT、LGT）で使用可能

認証方式と暗号化

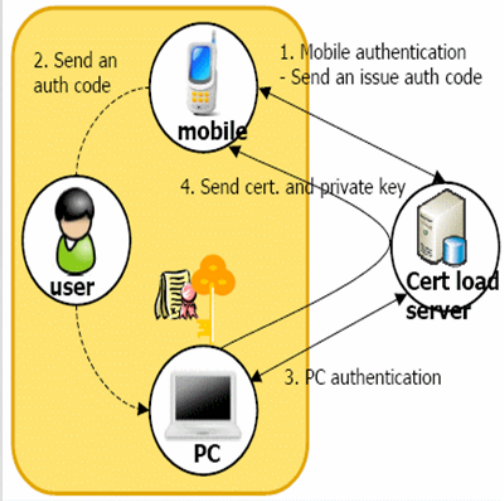
- 携帯電話内で計算を実行することにより、暗号化データや署名付きデータを送信
- 携帯電話にService VMをインストールして、電子証明書を使用する
- 電子証明書を携帯電話に保存することにより、メモリハッキングを防止する

期待される効果

- ユーザーは場所や時間に制約されることなく保存と署名を制御できる
- PSEを携帯電話にも拡大

Mobile Business

Certificate Moving to Mobile



Authentication and Sections to be encrypted

- Certification service via mobile phone where user's certificate is stored
- Able to use in 3 mobile service providers' environment (SKT, KT, LGT)

Method of authentication and encryption

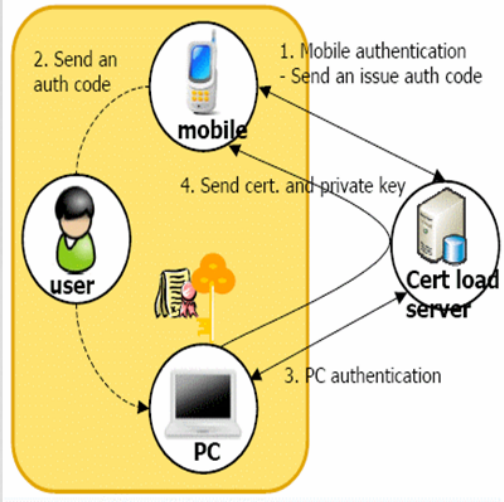
- Sending encrypted or signed data by performing computing operation inside mobile phone
- Service VM is installed in mobile phones in order to use certificates
- Storing certificates into a mobile phone to prevent memory hacking

Expected effects

- User have control to save and sign anywhere, anytime
- Expand the PSE to mobile phone

モバイル

モバイル化に伴う電子証明書



認証と暗号化対象のセクション

- ユーザーの電子証明書を保存した携帯電話による認証サービス
- 3つのモバイルサービスプロバイダ環境（SKT、KT、LGT）で使用可能

認証方式と暗号化

- 携帯電話内で計算を実行することにより、暗号化データや署名付きデータを送信
- 携帯電話にService VMをインストールして、電子証明書を使用する
- 電子証明書を携帯電話に保存することにより、メモリハッキングを防止する

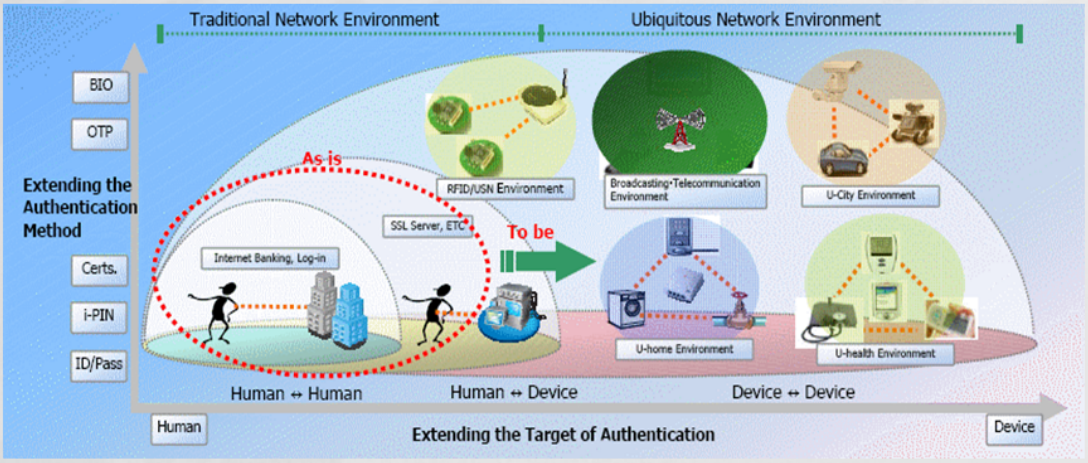
期待される効果

- ユーザーは場所や時間に制約されることなく保存と署名を制御できる
- PSEを携帯電話にも拡大

Ubiquitous Business

Device Authentication

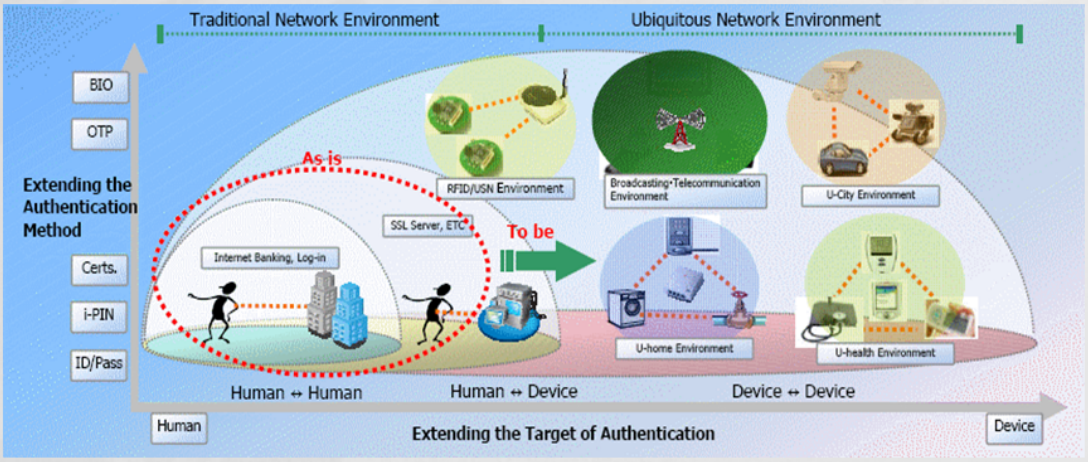
- Due to the developments of IT services, variety of authentication methods are invented and the needs are still growing
- Not just networks and humans but variable devices also



ユビキタス

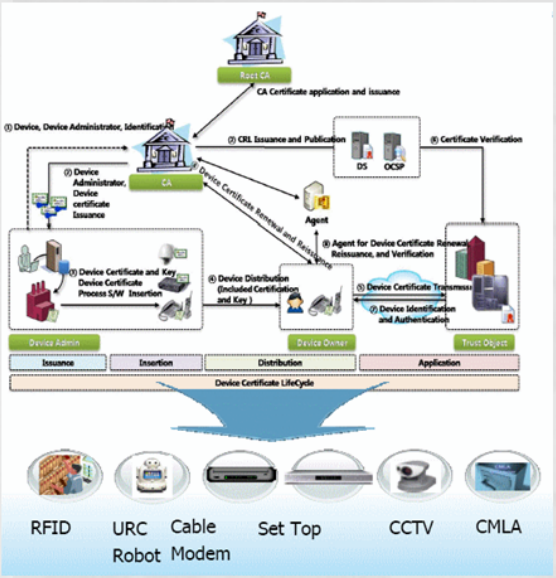
デバイスの認証

- ITサービスの発展に伴い、さまざまな認証方式が開発され、そのニーズも拡大している
- ネットワークや人だけでなく、多様なデバイスにも波及



Ubiquitous Business

Device Authentication



Sections to be encrypted

- Devices accessible via network
- Interconnect devices

Method of authentication and encryption

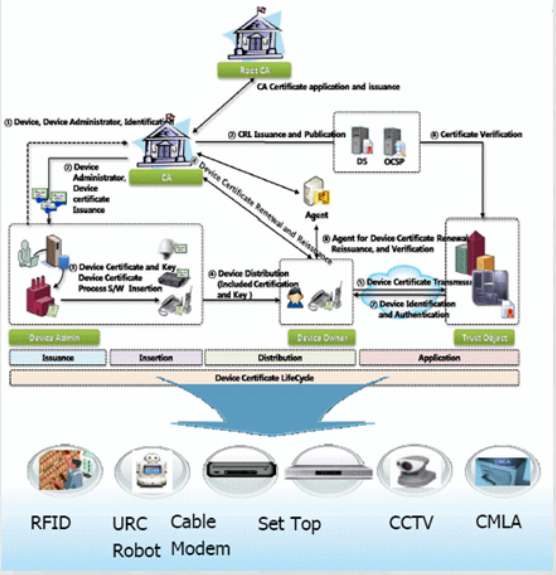
- Authenticaton based on device identity information such as MAC and serial number
- Device certificates to confirm that a device has passed authentication tests and approved
- Key management and encryption such as Diffie-Hellman key exchange, electronic signature and encryption (for integrity of data tranferred)

Expected effects

- Enhance security of device-based service and improve reliabilities
- Ensured services via device identity and authentication
- Raise reliability of services via certification services
- Integrity of a diverse of transferred information and encryption
- Able to extend certification services of diverse devices

ユビキタス

デバイスの認証



暗号化対象のセクション

- ネットワークを介してアクセス可能なデバイス
- デバイスの相互接続

認証方式と暗号化

- MACや通し番号などのデバイス識別情報に基づく認証
- デバイスが認証テストに合格し、承認済みであることを確認するデバイスの電子証明書
- Diffie-Hellman鍵交換、電子署名、および暗号化など、キーマネージメントと暗号化（転送データの完全性を保証）

期待される効果

- デバイスベースサービスのセキュリティ強化と信頼性の向上
- デバイスの識別と認証によりサービスを保証
- 認証サービスによるサービス信頼性の向上
- 転送された多様な情報の完全性維持と暗号化
- 多様なデバイスの認証サービスを拡張

3. Problems and Improvement Measures

3. 問題点と改善策

Problems Overview

- 7 certificate Hacking Incidents from 2005 ~ 2009
  - Total damage (in USD) : 0.1 Million
- 2007 ~ 2008 : Certificate Stolen
- 2008 ~ 2009 : Certificate Online illegal Reissuance

	2005	2006	2007	2008	2009
Cerfiticate Stolen	-	-	2	2	-
Illegal Reissuance	1	-	-	1	1

問題の概要

- 2005～2009年の間に起きた電子証明書のハッキング事件: 7件
  - 被害総額: 10万ドル
- 2007～2008年: 電子証明書の盗難
- 2008～2009年: 電子証明書のオンライン違法再交付

	2005	2006	2007	2008	2009
Cerfiticate Stolen	-	-	2	2	-
Illegal Reissuance	1	-	-	1	1

Hacking Incidents Analysis

- **Certificates Stolen**
  - Most Internet Banking users store certificates in PC hard disk instead of portable storage such as USB memory
    - about 74% of users store certificates in PC hard disk
  - Because the security of PC hard disk is weak, the information of certificates and secret cards can be easily stolen by hacking

ハッキング事件の分析

- **電子証明書の盗難**
  - 大部分のインターネットバンキングユーザーが、ポータブルストレージ（USBメモリなど）ではなく、PCのハードディスクに電子証明書を保存している
    - ユーザーの約74%が電子証明書をPCハードディスクに保存
  - PCハードディスクのセキュリティは脆弱であるため、電子証明書や機密カードの情報がハッキングにより盗み出される

Hacking Incidents Analysis

- **Illegal online reissuance of certificate**
  - Personal ID information requred for online reissuance is exposed to hacking due to careless handing etc.
    - Personal ID information : Social Security Number, Account Number, Account Password, Secret Card
  - Online personal ID information can be hacked through keyboard hacking programs (e.g. keylog) as user types the information in using a keyboard

ハッキング事件の分析

- **電子証明書のオンライン違法再交付**
  - オンライン再交付に必要な個人のID情報が、不注意な取り扱いなどによりハッキングの対象となる
    - 個人のID情報: 社会保険番号、口座番号、アカウントパスワード、機密カード
  - オンラインの個人ID情報は、ユーザーがキーボードでシステムに情報を入力するときにキーボードハッキングプログラム（例: keylog）でハッキングされることがある

PKI Security Improvement Measures

- Adopt Safer Certificate Storages
  - Build secure storage infrastructure e.g. security tokens, cellphone(USIM) etc.
  - Encourage public to use portable storage device
  - Secure mobile banking and revitalize using certificate in mobile banking
- Improvement of Reissuance Process
  - Enhancement of online authentication method
  - Notice of event of certificate issuance
- Upgrade the Digital Signature Algorithm
- Publicity Activity for Safe Use of Certificates

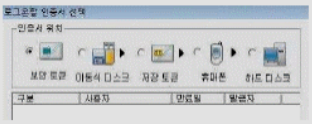
PKIセキュリティの強化策

- 安全な電子証明書保存方法の採用
  - 安全な保存インフラストラクチャの構築: セキュリティトークン、携帯電話（USIM）
  - 一般向けにはポータブルなストレージデバイスの普及を促進
  - モバイルバンキングでの電子証明書の使用により、モバイルバンキングの安全確保と活性化
- 再交付プロセスの改善
  - オンライン認証方法の強化
  - 電子証明書の再交付に伴うイベント通知
- デジタル署名アルゴリズムのアップグレード
- 電子証明書の安全な使用に向けた広報活動

Adopt Safer Certificate Storage

- Build secure storage infrastructure e.g. security token(HSM), cellphone(USIM)
  - Replace PKI user S/W employing HSM

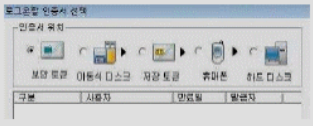
- Encourage using portable storage
  - Emodify certificate storage device selection window to encourage users to store certificates in potable storage instead of hard disk drive in PC
  - As the number of security tocken users increase, delete save in hard disk option from the storage device selection window



安全な電子証明書保存方法の採用

- 安全な保存インフラストラクチャの構築: セキュリティトークン（HSM）、携帯電話（USIM）
  - HSM対応のPKIユーザーソフトウェアへの置き換え

- ポータブルストレージの使用の促進
  - 電子証明書保存デバイスの選択ウィンドウを変更して、自分の証明書はPCのハードディスクドライブではなく、ポータブルなストレージに保存するように働きかける
  - セキュリティトークンユーザーの数が増えるに伴い、ストレージデバイスの選択ウィンドウからハードディスクへの保存オプションを除去する



Improve reissuance procedures

- Fortify online identification procedure
  - When identifying online, confirm additional information including personal information (Social security Number, Account Number, Account Password) and one time password (Sercret Card, OTP Token) etc
    - ➢ Authentication through cellphone SMS and landline phone
  - Provice accredited CAs with internet banking incident information (IP Address, MAC, Resident Registration Number etc.) to prevent illegal online reissuance

再交付手順の改善

- オンライン身元確認手順の強化
  - オンラインで身元を確認するときに、社会保険番号、口座番号、アカウントパスワード、ワンタイムパスワード（機密カード、OTP Token）などの個人の関連情報を確認する
    - ➢ 携帯電話SMS、および固定電話による認証
  - 認定認証局にインターネットバンキング事件の情報（IPアドレス、MAC、住民登録番号など）を提供して、違法なオンライン再交付を防止する

Improve reissuance procedures

- Fortify online identification procedure (continued)
  - User to choose whether to be identified online or in person
    - Encourage identifiction in person to prevent illegal reissuance of certificates
- Notice users in the event of certificate issuance
  - Send notice on reissuance to the user's cellphone(SMS) or landline phone
  - Build and operate 24-hour service system in accredited CA for users to file damage reports on illegal reissuance

再交付手順の改善

- オンライン身元確認手順の強化（続き）
  - ユーザーが身元確認をオンラインで行うか、対面で行うかを選択できる
    - 電子証明書の違法な再交付を防ぐために対面による身元確認を推奨
- 電子証明書の再交付に関するユーザーへのイベント通知
  - ユーザーの携帯電話（SMS）、または固定電話に再交付の旨を通知する
  - 認定認証局における24時間サービスシステムの構築と運用により、ユーザーが違法再交付に関するファイル損害報告を届け出られるようにする

Upgrade the Electronic Signature Algorithm

- RSA 1024 bit and SHA1 algorithm no longer safe after 1 year
- Change of Key size and Electronic Signature Algorithms
  - Increase User Certificate Key size of RSA Algorithms from 1024 to 2048
  - Change of hash algorithm from SHA1 to SHA2
- Modification of PKI user SW
  - for PKI application to support new algorithms and new certificates

電子署名アルゴリズムのアップグレード

- RSA 1024ビットおよびSHA1のアルゴリズムは、1年後には安全性が低下
- 鍵サイズと電子署名アルゴリズムの変更
  - RSAアルゴリズムのユーザー証明書鍵のサイズを1024から2048に増やす
  - ハッシュアルゴリズムをSHA1からSHA2に変更する
- PKIユーザーソフトウェアの変更
  - PKIアプリケーションが新しいアルゴリズムと新しい電子証明書をサポートできるようにする

Upgrade the Electronic Signature Algorithm

■ Change of Electronic Signature Algorithm

	~ Dec. 2010		
	Digital Signature	Hash	Validity Period
Root CA	2048 bit	160 bit	20 years
CA	2048 bit	160 bit	10 years
User	**1024 bit**	160 bit	1 year

	Jan. 2011 ~		
	Digital Signature	Hash	Validity Period
Root CA	3072 or 2048 bit	256 bit	20 years
CA	2048 bit	256 bit	10 years
User	**2048 bit**	256 bit	1 ~ 2 years

電子署名アルゴリズムのアップグレード

■ 電子署名アルゴリズムの変更

	~ Dec. 2010		
	Digital Signature	Hash	Validity Period
Root CA	2048 bit	160 bit	20 years
CA	2048 bit	160 bit	10 years
User	**1024 bit**	160 bit	1 year

	Jan. 2011 ~		
	Digital Signature	Hash	Validity Period
Root CA	3072 or 2048 bit	256 bit	20 years
CA	2048 bit	256 bit	10 years
User	**2048 bit**	256 bit	1 ~ 2 years

33
koscom Global IT Solution Leader

4. Introduction to KOSCOM

4. KOSCOM社の紹介

Introduction to KOSCOM

- Established by MoFE and Korea Exchange
  - To computerize the Securities Market and the Member Systems (in 1977)
  - Organization : 5 Headqurters, 16 Departments, 1 Office (17 Divisions)
  - Staffs : 4 Corporate Directors and 574 Employees
- Main Businesses of Koscom
  - Exchange IT Services, Financial Information Services, Financial IT Solution Services, IT Infrastructure Services
    - IT Infrastructure Servicess : Security Service (Certification Service, Information Sharing and Analysis Center, Certified e-Document Authority), Network Service, DR & BCP Center
- SignKorea
  - Issuers 4,5000,000 Certificates for Investment Banks (38 Securities Companies, 10 Futures Companies) and 5 Commercial Banks
  - Issues 1,200,000 General Purpose Personal Certificates (fee-charging)

KOSCOM社の紹介

- 韓国財務経済部と韓国証券先物取引所により設立
  - 証券市場とメンバーシステムのコンピュータ化を推進（1977年以来）
  - 組織: 拠点5個所、16部門、1オフィス（17課）
  - スタッフ: 企業取締役4名、従業員574名
- 主な事業
  - ITサービス、金融情報サービス、金融ITソリューションサービス、ITインフラストラクチャサービスの提供
    - ITインフラストラクチャサービス: セキュリティサービス（認証サービス、情報共有/分析センター、Certified e-Document Authority: CeDA）、ネットワークサービス、DR/BCPセンター
- SignKorea
  - 投資銀行（証券会社38社、商品先物会社10社）および商業銀行5行にむけて、4,500,000の電子証明書を交付
  - 一般の個人向けに1,200,000の電子証明書（有料）を交付

Thank You

e-mail : mse@koscom.co.kr
homepage : www.koscom.co.kr www.signkorea.com
address : Koscom Corporation
33, Yeouido-dong Yeongdeungpo-gu Seoul150-9777, Korea
tel : +82-2-767-7348
fax : +82-2-767-7390

ありがとうございます

e-mail : mse@koscom.co.kr
homepage : www.koscom.co.kr www.signkorea.com
address : Koscom Corporation
33, Yeouido-dong Yeongdeungpo-gu Seoul150-9777, Korea
tel : +82-2-767-7348
fax : +82-2-767-7390

講演８　台湾における認証基盤について

臺灣電子簽章現況與展望

報告人： 魯君禮

February 2010

財團法人中華民國國家資訊基本建設產業發展協進會

1

台湾における認証基盤について

－電子署名の現状と展望－

魯君禮

2010年2月

財団法人中華民国国家資訊基本建設産業発展協進会

1

大綱

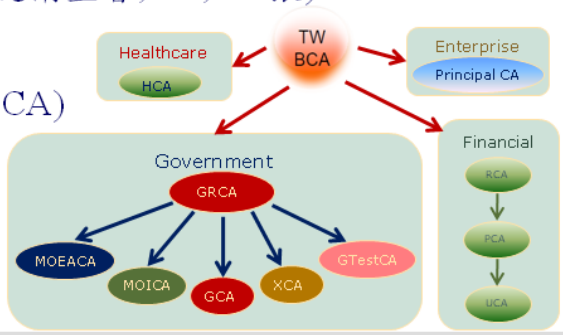
- 前言
- 電子簽章在電子郵件之應用
- 電子簽核之應用現況
- 電子發票之應用與挑戰
- 電子病歷之發展與願景
- 結語

目次

- はじめに
- 電子メールにおける電子署名の利用
- 電子認証利用の現状
- 電子インボイスの利用と課題
- 電子カルテの発展と未来の姿
- まとめ

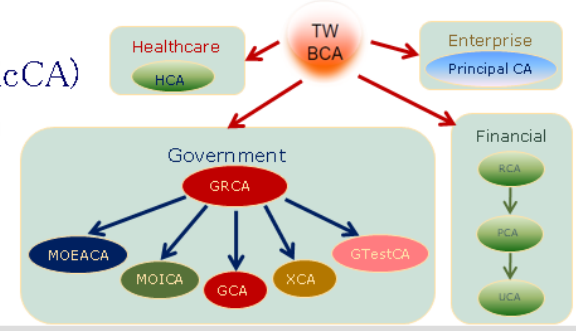
前言

- 台灣政府之憑證機構
  - 政府憑證總管理中心(GRCA,自簽憑證)
  - 政府憑證理中心(GCA,53,368張)
  - 內政部憑證管理中心(MOICA,簽發「自然人憑證」,1,770,596張)
  - 工商憑證管理中心(MOEACA,經濟部,489,778張)
  - 組織及團體憑證管理中心(XCA,行政院研考會,53,280張)
  - 醫療憑證管理中心(HCA,行政院衛生署,255,462張)
- 民間經營之憑證機構
  - 中華電信(eCA, GHTCA, PublicCA)
  - 銀行公會(FRCA,FPCA,FUCA)
  - …



はじめに

- 台湾政府の認証機関
  - 政府認証総管理センター(GRCA,自主認証)
  - 政府認証センター(GCA,53,368件)
  - 内政部認証管理センター(MOICA,「自然人認証」発行,1,770,596件)
  - 工商認証管理センター(MOEACA,経済部,489,778件)
  - 組織及び団体認証管理センター(XCA,行政院研考会,53,280件)
  - 医療認証管理センター(HCA,行政院衛生署,255,462件)
- 民間認証会社
  - 中華電信(eCA, GHTCA, PublicCA)
  - 銀行公会(FRCA,FPCA,FUCA)
  - …



電子簽章在電子郵件之應用

- 在電子郵件(email)上使用數位簽章之單位
  - ✓ 立法院
  - ✓ 行政院國家資通安全會報技術服務中心
  - ✓ 中央氣象局氣象資訊中心
  - ✓ 台灣電力公司
  - ✓ 聯邦銀行
  - ✓ 大華期貨
  - ✓ 金融單位如銀行、證券期貨業較多
- 推廣困難之原因
  - ✓ 所有使用者必須申請取得憑證並安裝在PC端
  - ✓ 企業資訊安全觀念宣導與落實執行不易
  - ✓ Webmail不接受數位憑證

電子メールにおける電子署名の利用

- 電子メール(email)で電子署名を利用している機関
  - ✓ 立法院
  - ✓ 行政院国家情報通信安全技術サービスセンター
  - ✓ 中央気象局気象情報センター
  - ✓ 台湾電力公司
  - ✓ 聯邦銀行
  - ✓ 大華期貨
  - ✓ 銀行、証券先物取引業などの金融機関が多い
- 普及が進まない原因
  - ✓ すべての使用者が認証取得を申請してPC端末に取り付ける必要があること
  - ✓ 企業の情報通信に対する安全の意識を指導し、着実に実行させることが容易でないこと
  - ✓ Webmailがデジタル認証を受け付けないこと

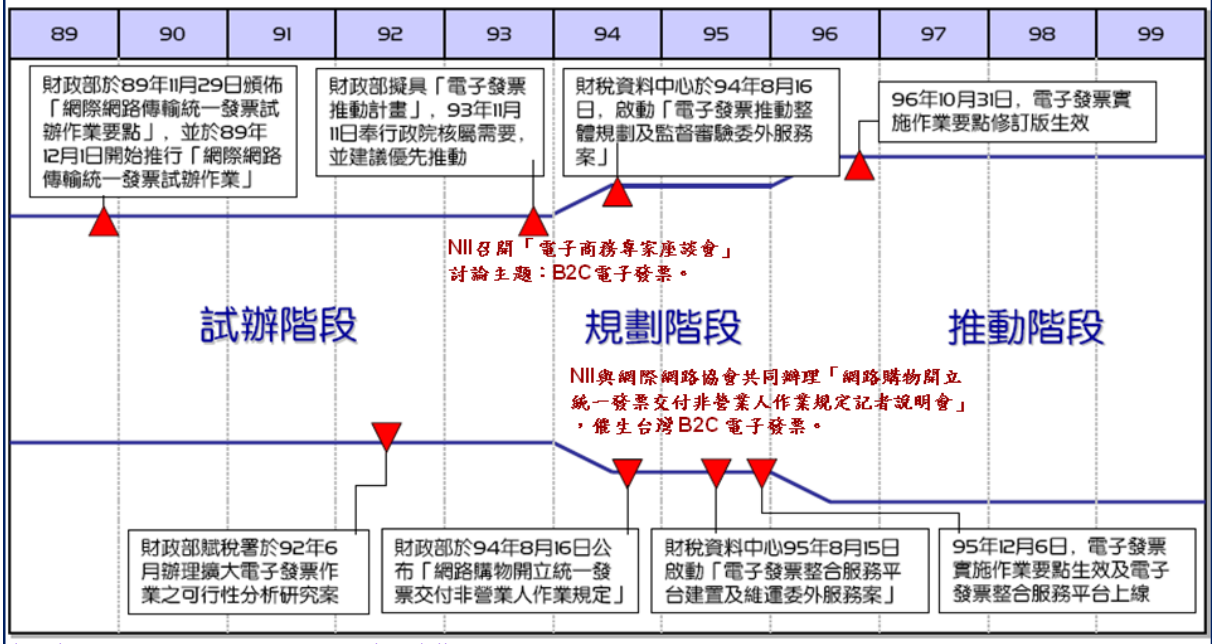
電子簽核應用現況

- 政府單位
  - ✓ 中央部會採用電子公文比例已有85%，地方單位有70%
  - ✓ 國家通訊傳播委員會(NCC)電子簽核比例達97%
  - ✓ 行政院研考會已規畫試辦「公務員電子識別證」，結合「自然人憑證」用於公文線上簽核、安全電子郵件、網路權限管理等資訊安全應用。(研考會2009/4/18新聞稿)
- 民間企業
  - ✓ 已導入ERP之企業(Acer, TSMC, Asus…)、中小企業之Workflow Software(EIP)
- 可能面臨之困難
  - ✓ 法律效力、保管之安全性、可閱讀性

電子認証利用の現状

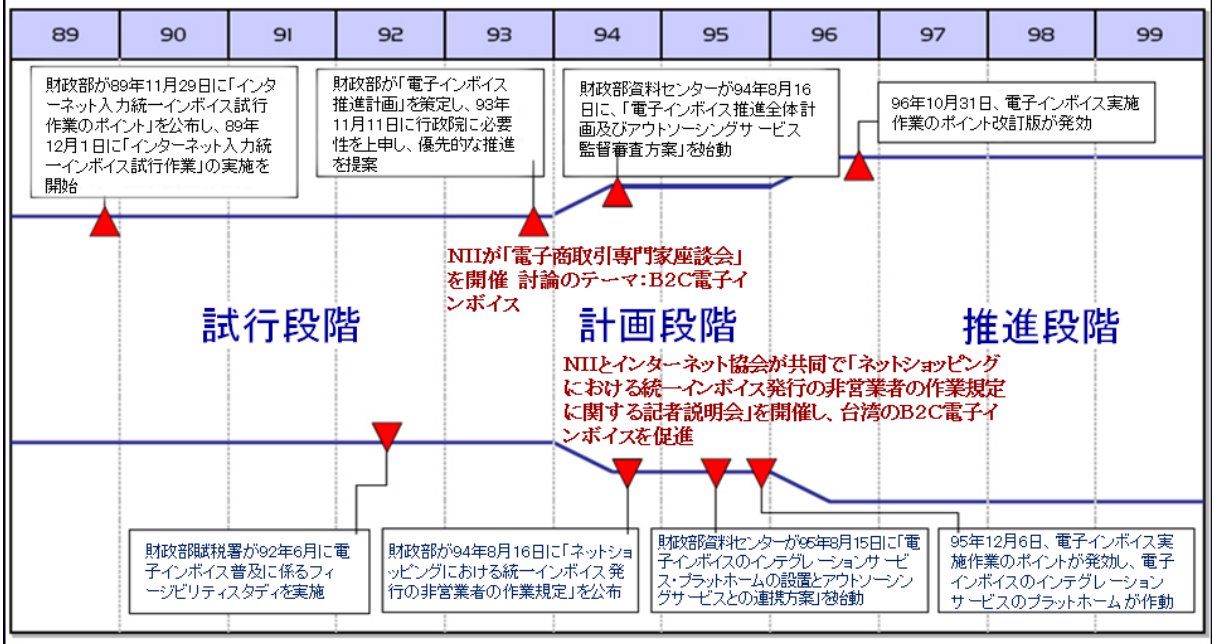
- 政府機関
  - ✓ 中央の部署の電子公文書の比率は85%に、地方機関では70%に達している。
  - ✓ 国家通信放送委員会(NCC)の電子認証比率は97%に達している。
  - ✓ 行政院研考会では「公務員電子識別証」を試行し、「自然人認証」と合わせて、公文書のオンライン認証、電子メールの安全管理、ネットワーク上の権限管理等の情報通信のセキュリティーに利用することを検討している。(研考会2009/4/18プレスリリース)
- 民間企業
  - ✓ ERP導入済み企業(Acer, TSMC, Asus…)、中小企業のWorkflow Software(EIP)
- 当面の課題
  - ✓ 法的効力、保存の安全性、閲読性

電子發票之應用－ 發展過程



資料來源：電子發票 e世代 (2009) 徐世豪，資策會。

電子インボイスの利用－ 発展のプロセス

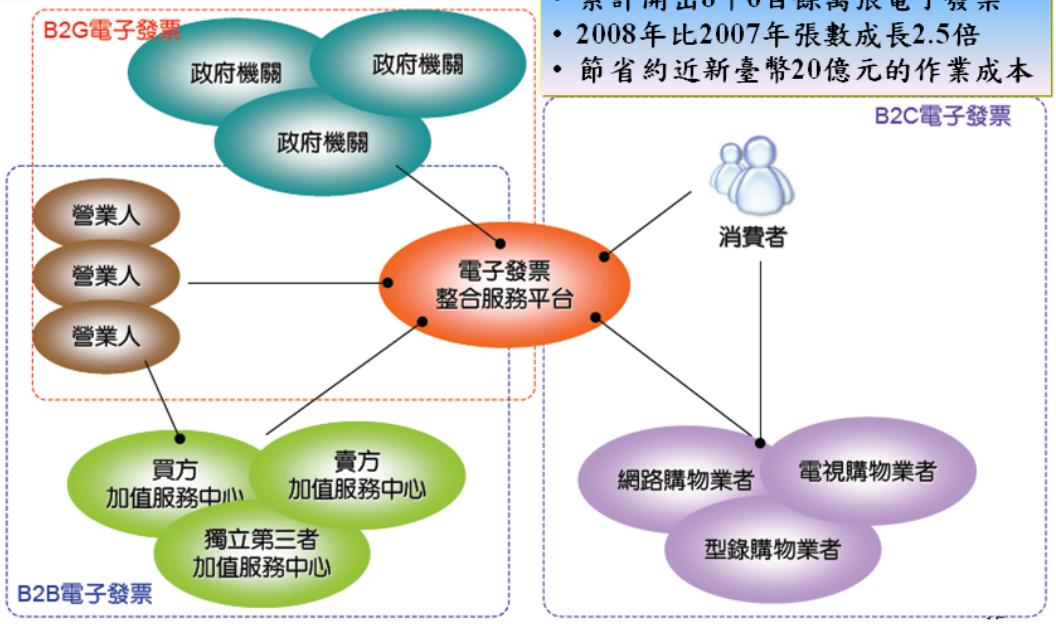


出典：電子インボイス e世代 (2009)徐世豪、資策会

電子發票之應用－ 現況

使用經濟部「工商憑證」提出申請

- 1萬3千家企業使用
- 累計開出8千6百餘萬張電子發票
- 2008年比2007年張數成長2.5倍
- 節省約近新臺幣20億元的作業成本

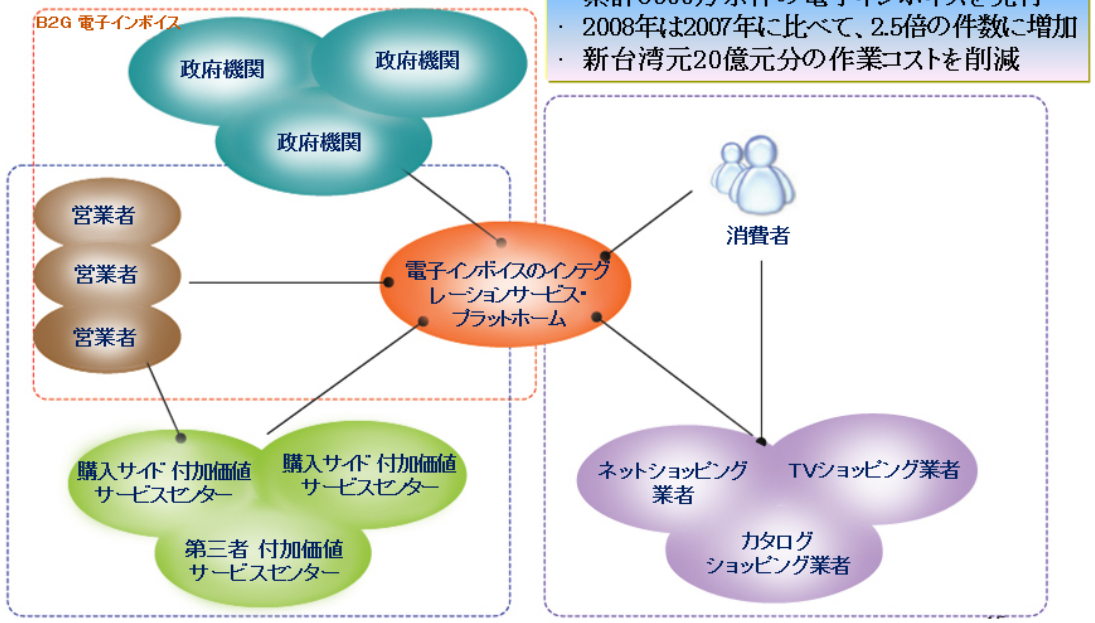


資料來源: 智慧台灣願景(2009/12)行政院科顧組副執秘鐘嘉德,研考雙月刊；電子發票 e世代 (2009) 徐世豪，資策會。

電子インボイスの利用－ 現状

経済部の「工商認証」を利用して申請

- 1万3000社の企業が使用
- 累計8600万余件の電子インボイスを発行
- 2008年は2007年に比べて、2.5倍の件数に増加
- 新台湾元20億元分の作業コストを削減



出典: 智慧台湾願景(2009/12) 行政院科顧組副執秘 鐘嘉徳、研考隔月刊;電子インボイス e世代 (2009) 徐世豪、資策会

電子發票之應用－ 面臨之挑戰

- **整體環境**
  - 電子商務發展快速，政府須提供更多誘因及配套措施以提高電子發票使用率。
- **B2C**
  - 消費者
    - 擔心退貨不易、個資外洩
  - 網路購物業者
    - 保證金過高：網購業者78%屬中小型（實收資本額低於新台幣5百萬），2百萬保證金門檻過高。
  - 實體通路業者
    - 網購、電視購物、型錄購物僅佔零售市場6.2%(2007年)，應擴及實體通路業者，但面臨以下問題
      - ✓ 結帳時間延長
      - ✓ 兌獎機制變更

資料來源:2008中華民國電子商務年鑑

電子インボイスの利用－ 直面する課題

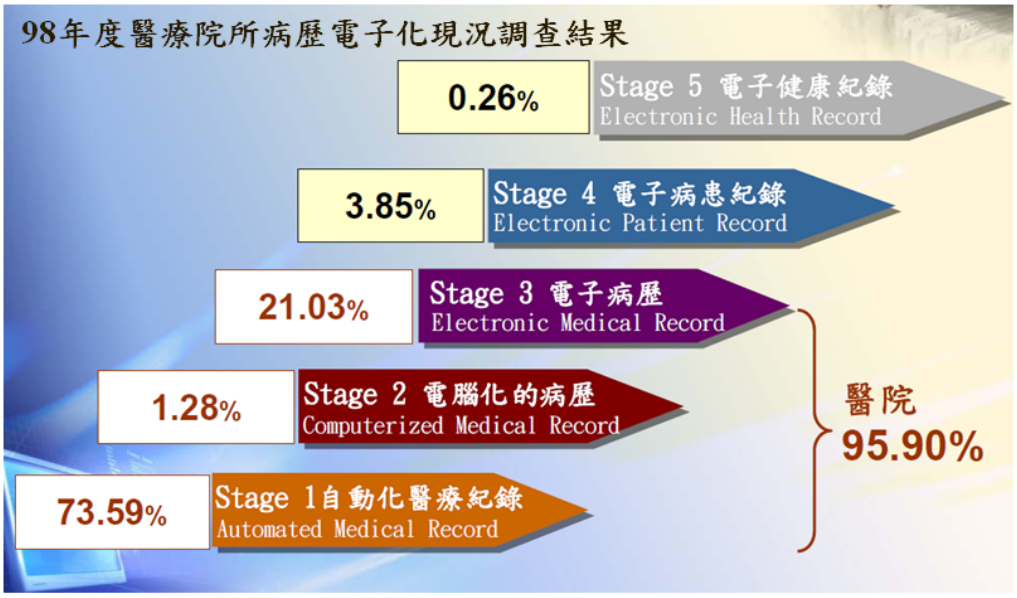
- **全体の環境**
  - 電子商取引は急速に発展しており、電子インボイスの利用率を向上させるためには、政府は一層のインセンティブと一連の施策を講じる必要がある。
- B2C
  - 消費者
    - 返品が困難なこと、および個人情報の漏洩が心配。
  - インターネットショッピング事業者
    - 保証金が高すぎる:インターネットショッピング事業者の78%は中小事業者(払込資本金は5百万新台湾ドル未満)であり、2百万の保証金はハードルが高すぎる。
  - 実店舗事業者
    - 小売マーケットに占めるインターネットショッピング、TVショッピング、カタログショッピングのシェアは6.2% (2007年)で、実店舗事業者に広がっているが、以下の問題に直面している。
      - ✓ 決済期間が延びる
      - ✓ 景品メカニズムの変更

出典:2009年中華民国電子商取引年鑑

電子病歷之應用－ 發展過程

◆2005年衛生署開始協助醫院導入

◆2009年底計100家醫院宣告實施電子病歷，進入電子病歷元年

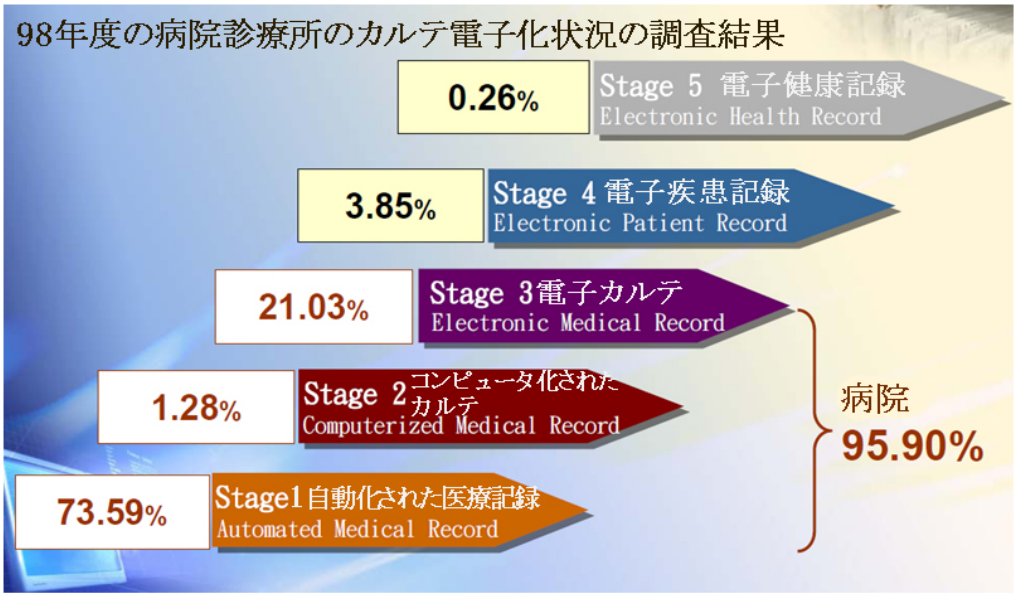


資料來源:我國電子病歷政策及發展(2009)行政院衛生署徐嫦娥參事兼資訊中心主任

電子カルテの利用－ 発展プロセス

◆2005年に衛生署が病院の導入への協力開始

◆2009年末に100件の病院が電子カルテの実施を宣言し、電子カルテ元年に

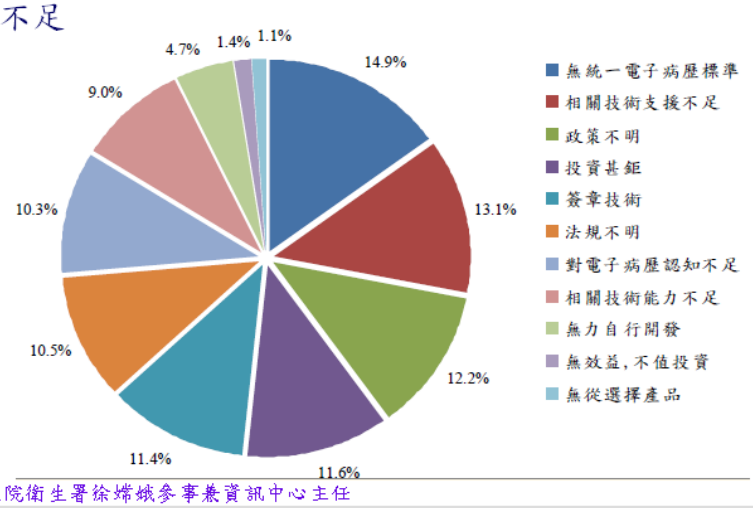


出典:電子カルテの政策と発展(2009) 行政院衛生署　徐嫦娥参事兼情報通信センター主任

電子病歷之應用－ 面臨之挑戰

◆ 當前執行問題

- 醫院資訊化及病歷電子化程度待提升
- 醫院實施電子病歷與病歷互通的誘因不足
- 尚無完善的院際電子病歷互通機制
- 醫院的資訊人員與經費不足

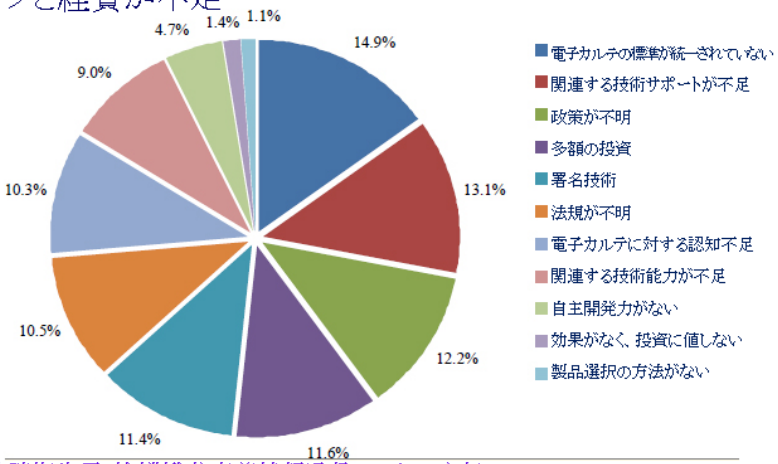


資料來源:我國電子病歷政策及發展(2009)行政院衛生署徐婦娥參事兼資訊中心主任

電子カルテの利用－ 直面する課題

◆ 実施に当たっての課題

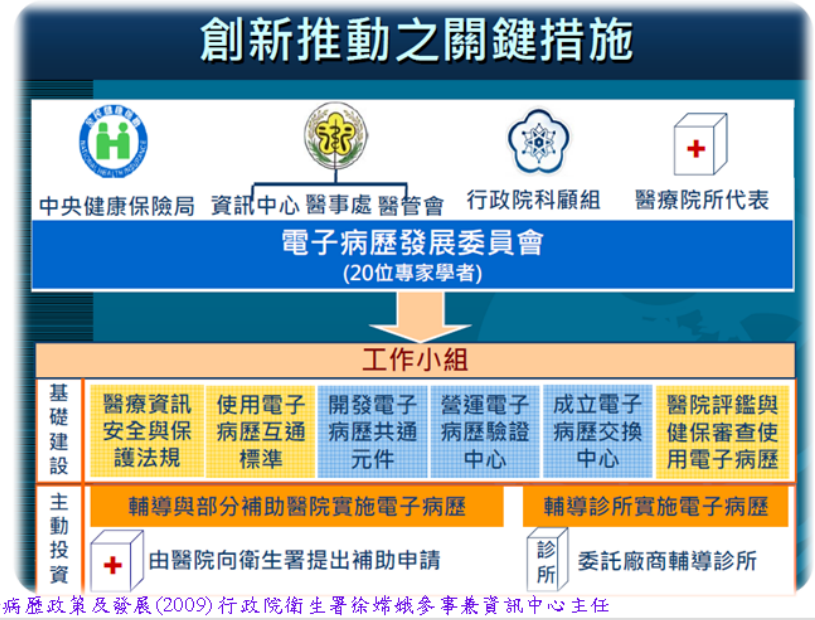
- 病院の情報通信化及びカルテ電子化レベルのアップが必要
- 病院の電子カルテ及びカルテ交換実施のインセンティブが不足
- 病院間の電子カルテ交換についての整備されたメカニズムが存在しない
- 病院の情報通信スタッフと経費が不足



出典: 電子カルテの政策と発展(2009) 行政院衛生署 徐婦娥参事兼情報通信センター主任

電子病歷之應用－ 願景

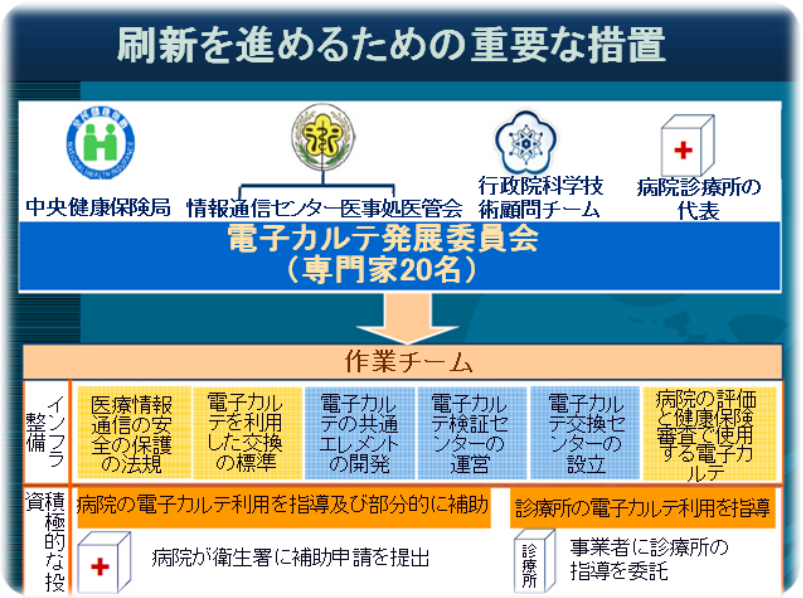
- 2010~2012年「加速醫療院所實施電子病歷系統計畫」
- 2014年預計醫療院所全面實施電子病歷與病歷交換系統



資料來源:我國電子病歷政策及發展(2009)行政院衛生署徐嫦娥參事兼資訊中心主任

電子カルテの利用－ 未来の姿

- 2010~2012年「病院診療所の電子カルテシステム実施加速計画」
- 2014年に病院診療所が電子カルテ、およびカルテ交換システムを全面的に実施する予定



出典：電子カルテの政策と発展(2009) 行政院衛生署　徐嫦娥参事兼情報通信センター主任

結語

- 台灣之PKI及電子認證技術已經成為發展電子商務之重要基礎。
- 台灣推動個人資料保護時，可採行電子認證技術與服務以強化資訊安全管理。
- 台灣PKI廠商除持續深化國內技術應用外，亦應積極拓展國際合作商機。

まとめ

- 台湾のPKIおよび電子認証技術は、今や電子商取引を展開するための基本要件である。
- 台湾は個人情報保護の推進において、情報通信の安全管理を強化するために、電子認証の技術とサービスを採用すべきである。
- 台湾のPKI事業者は、国内で技術の利用を進めながら、海外におけるビジネスチャンスを積極的に開拓しなければならない。

~Thank You for Your Participation~

財團法人中華民國國家資訊基本建設產業發展協進會

13

~ご清聴ありがとうございました~

財団法人中華民国国家資訊基本建設産業発展協進会

13

ドイツにおける認証基盤について
署名・認証基盤と仮名

2010年2月4日

米丸恒治
(神戸大学大学院法学研究科教授)

講演の概要

１　ドイツ電子署名法とその署名・認証基盤

２　ドイツeIDカードを利用した署名・認証基盤

３　市民ポータル構想（案）における認証基盤

４　ドイツの認証基盤からの示唆ーおわりにー

1-1 ドイツ電子署名法制の経緯・特徴

■1997年　デジタル署名法　＋30年の長期検証保証(連邦引継)
　タイムスタンプも法定　　〃
＜安全性の高い免許事業者の証明書を普及させ安価にと構想＞
★仮名(pseudonym)利用の署名も個人情報保護の観点から承認
　(機関認証、法人認証にも利用　→行政機関の証明書等)

↓　1999年EU電子署名指令(仮名利用を承認)

■2001年　電子署名大綱法（現行法）
　法的に手書き署名・押印に相当する電子署名は、下記の2種
①認定署名（＋30年の署名検証可能性確保：連邦の引継ぎ検証）
②適格署名　SSCDを用いたセキュリティー要件等を限定した署名
③先進署名については、署名法上の規制がない。

■97年デジタル署名の安全性、一律普及可能性が99年指令で規制緩和され、当初の免許(認定)CAによる統一的な体系が緩んだ。

(参考)EU電子署名指令の概要

- 事前の許認可制度排除　→　ドイツ法改正へ
- 任意の認定制度の導入

※先進署名・適格署名・認定署名の三区分導入
　適格電子署名「適格証明証に基づき安全署名作成装置により作成された先進電子署名」の法的効果の承認
　(手書き署名と同等、証拠として承認)

- CAの賠償責任の明示
　(立証責任転換＋過失責任原則)
- データ保護、仮名の証明証の利用保障
　(仮名の利用を禁止してはならない)

1-2 ドイツ署名法(現)の認証業務等

◎適格署名に関する認証業務(届出＆認定事業者)
―先進署名(advanced sig.)は規制なし

- 認証機関の免許から自由化―4条1項
- 監視システム(届出制)の導入―4条3項4項
  適格証明書を発行する事業者の届出義務
  ※日本の認定を受けない特定認証業務との相違点
- 任意認定制度の導入－15条以下
  従来の免許事業者を認定事業者として維持
  ＋新規参入、統廃合
- 責任規定の導入―11条

仮名(pseudonym)利用の署名を個人情報保護の観点から承認
(機関認証、法人認証にも利用 →行政機関の証明書等)
基本は旧法から変更なし。
法的には安全な仮名利用した署名可能

(参考)ドイツ署名法の区分

認定認証事業者の適格証明書利用(いわゆる認定電子署名)	適格証明書利用の電子署名(いわゆる適格署名)	先進電子署名 advanced. sig
任意の認定制度による第三者証明	適格であるとの自己宣言	
署名法上の要件の事前審査 技術的装置の事前審査 定期検査をともなう監督	要件を満たす旨の届出義務 技術的装置の製造者宣言 監督権は及ぶ	要件なし 監督なし
連邦ネットワーク庁(BNA=トラストアンカー)によるルートCAによるCA用証明書の発行 証明書失効後も、+30年の検証保証 CA廃業等の後も、業務引継保証＋連邦引継 ・文書保存も+30年	ネットワーク庁のルートCAがトラストアンカーにならない。 ＋5年間の検証保証 ・文書保存+5年	商用サービスの場合は契約条件により決定

適格証明書を利用した署名の普及が途上！(欧州の全体的傾向)
ドイツでは、法制度上、適格証明書に表見証明を与える等法的支援もしているが。

(参考)ドイツのCAの状況　士業CAの統合

- 認定CA(署名+タイムスタンプ)
  - 6CA　←　24CA（士業CA19→2、非士業団体5CA）
- 認定CA(署名のみ)
  - 3CA　　※新たにヘルスケア関係、金融関係が増加
- 認定CA(タイムスタンプのみ)
  - 1CA　　認定CA総計＝10CA
- 休廃止認定CA
  - 1CA廃止(承継)、1CA認定撤回(法人形式変更)
- 届出CA　5CA　(年金保険関係新規参入例)
  ←　2CA　(貯蓄金庫)
  うち2CAはタイムスタンプも供給
  ※届出CAでも適格証明書を発行するCAは把握され監督

(参)アルゴリズム適性公示への対応

◆連邦ネットワーク庁
連邦ネットワーク庁のルートCAの鍵長変更・ハッシュ変更
2007年8月17日完了。RSA2048＋SHA512で証明書発行
OCSPレスポンス、CRLも、上記で。

- 法令の規定により、SHA-1、RSA 1024を利用した適格証明書、認定CAの証明書発行用証明書には、再署名した。タイムスタンプによる再署名は、LDAPの"署名リニューアル"にて読みだし可能としている。

◆認定CA、TSA等
08年3月末までに、RSA1024の入れ換え、SHA1の入れ換えを実施。

◆ユーザーへもCA等をつうじて、法令上、再署名、タイムスタンプの重ねうちを求める段階にある!!

(参考)日独欧署名法比較資料

	日本署名法	独・署名法	EU署名指令
監督権	(認定業務にのみ)?	届出制＋監督権	監督権要求
事前規制	なし(認定のみ)	届出＋認定	認定制度
署名の効果	(排他)署名に	適格署名に	適格署名に
認証業務の要件	認定業務のみ(設備・本人確認・業務の各基準)	設備・本人確認・業務／財務要件賠償準備／	付属書Ⅱ(適格証明書・認証機関の要求事項)
タイムスタンプ	規定なし(デ協認定)	適格ﾀｲﾑｽﾀﾝﾌﾟ	(立法趣旨言及)
仮名の利用	規定なし(不可?)	**承認(機関・仮名)**	**承認**
無過失の立証	規定なし	認証機関	認証機関
検証可能期間	(+10年)(認定業務)	+30年(認定署名 +5年(適格署名	
資料等引継ぎ	休廃止時規定なし	他機関or監督庁	

1-3 電子署名の普及と課題

・法制度は整備、標準化、相互運用性確保の基準等も整備

■署名利用マーケット拡大途上

EU全体でも、適格電子署名の利用思うように拡大せず。

★電子政府アプリケーションによる牽引。 ・・

★署名カード普及施策

ドイツ： 適格署名の普及によるコスト削減、効率性を追求

標準的なSSCD搭載チップカード普及を推進

(◎eIDカード、ジョブカード、ヘルスケアカード)

☆電子政府 v.2 ＋ドイツ・ハイテク戦略

→ Identification ID戦略として、eIDの利用環境整備

→eIDカードなど署名利用可能なカード戦略推進

IDカード(公的証明)の官民・リアル＆オンラインでの利活用

→ 市民ポータル(ドイツ版電子私書箱)構想(法案)

安全で信頼できる使いやすい通信基盤の整備

1-4 電子署名とデータ保護(仮名利用含)

- 認証機関に対する監督
- 認証機関に対するデータ保護規制
- 仮名利用によるデータ保護 本人確認が確実にされた仮名

第5条〔適格証明証の付与〕(3) 認証事業者は、申請者の求めに応じて、適格証明証に、申請者の名前に代えて仮名を取り込まなければならない。適格証明証が、第三者のための代表権または職業関連もしくはその他のその者についての表示を含むときは、仮名の利用のためには、その第三者のまたは職業関連もしくはその他の表示について権限ある機関の承認を必要とする。

第7条〔適格証明証の内容〕 ・証明書中の仮名としてみわけのつく仮名を表示

(法的責任追及のための仮名の本人開示手続)

「犯罪または秩序違反の訴追のため、公共の安全と秩序に対する危険の防止のためまたは連邦および州の憲法保護行政機関、連邦諜報局、軍事諜報機関もしくは税務行政機関の法律上の任務の遂行に必要な限りにおいて、または、裁判所が係属中の手続の範囲内でそこで適用される規定の基準によりそれを命じる限りにおいて」 仮名の本人情報を提供

(参考)DASITプロジェクト 概要

デジタル署名法上の仮名を利用した商取引実験

- DASIT(テレサービスにおけるデータ保護)
- 1998年～2001年
- 連邦機関による補助事業
- 参加組織

・DGバンク/ドイツ組合銀行株式会社/GMD情報技術研究センター/PROVET

モデル: 仮名証明証を用いた仮名署名 (＋SET方式支払)

CAは、仮名証明証、仮名メールアドレス提供

ユーザは、ショップで仮名で購入 SET決済

商品は、発送IDをつけて運送事業者へ

運送事業者は、発送IDと送付先のみで配送へ

個人情報を最小限に押さえた商取引モデルを実証実験したプロジェクト

個人が、仮名を利用して個人情報最小化・仮名化しつつ法的に責任ある商取引を実現することの可能性が示された。

※法制度上承認された仮名の利用を実証実験するプロジェクト

適格証明書への仮名のとりこみのうち、個人情報保護最小限化は重要

Pre2　新たな認証基盤整備の動向

■eIDカードの導入　　eIDカード法改正成立(09年)　11月より切替
　・国民のeID・電子署名利用環境の全体的な整備
■市民ポータル　(技術指針、パブコメ、市民ポータル法案動向??)
　◆認証を受けた民間により提供・官民共通の利用基盤
　●本人確認・認証サービス
　　– 信頼性あるID管理、シングルサインオン
　　– ユーザー側のコントロールによる個人情報提供
　　– 仮名の利用もオプション
　●信頼性ある私書箱　　de-mail構想
　　– 一義的なアドレス、電子メール等の送受・保存管理
　●送達機能・送受信証明等各種証明サービス　日時証明可
　　– プロバイダによる秘密保持した送達機能・配達証明付メール
　　– 電子文書保存、第三者への管理されたID公開機能付
○長期署名・ﾀｲﾑｽﾀﾝﾌﾟ、信頼性ある安全なID利用環境構築着々と

2-1　eIDカード導入とeID、電子署名基盤整備

・前提：署名カード普及不十分

■eIDカードの3機能
　①本人証明（文書、旅券代替）
　②eID(電子本人証明)-ｵﾌﾟｼｮﾝ
　　自販機、ネット上での本人証明
　③適格電子署名機能-ｵﾌﾟｼｮﾝ
　　共通の適格電子署名用チップカード
　・非接触型ICチップ登載の標準規格カード(e-Card-API)

■官民共用、共通の本人確認データ・認証基盤の普及
■eIDを利用して、認定認証事業者に電子署名証明書申請可能
　eIDカード法により、電子署名の利用促進のため証明書本人確認がeIDで可能になった。eIDとeIDカードを利用して、署名利用拡大を
■多様な電子署名・認証に共通利用するための相互運用可能性

2-2　eIDカードと個人情報保護・仮名

■ドイツにおいては、共通番号制度、共通IDは、法的に禁止

■利用する個別行政機関、個別民間事業者ごとの主務官庁による審査と許可の際に与えられるアクセス権限証明書のデータから、個別ID(個人識別符号)を生成する。

○電子的な行政手続における確実な本人確認

○電子署名法による認定認証局への証明書の申請にも利用可

○オンラインバンキング等での口座開設・アカウント開設にも可

○市民ポータル(独版電子私書箱(仮))の開設、アクセス手段としても利用

その他のアプリケーション例：年齢制限サービス、地域限定サービス提供、電子商取引時の最初の本人確認、Webフォームへの入力など

仮名情報を利用できるサービスの例：

個人情報を必要としないが、アクセス者が同一であるか確認するサービス、など　例：SNSやWeb上のサービスの利用

2-3　ドイツeIDカードの特徴

・eIDの利用を民間にも開放：　官民共用の認証基盤に
公的証明を出発点にした、統一的標準的証明の民間への開放
電子的な証明データの官民での利用を想定

・民間企業利用には、事前のeIDアクセス権限審査を制度化
事業者によるアクセス用証明書により、ユーザID情報参照可に
個人情報保護監査を伴う

☆ユーザの個人情報コントロール：

①eIDの利用は任意＋個別の場面ごとの選択が可能

①アクセス権限証明書のチェック　→　相互当事者の認証可能
＋選択した情報のみアクセス承認。

③サービス毎、カード毎の仮名(自ら設定は不可？)利用可能
先発国のeIDにみられない個人情報保護措置

④個人情報の範囲についてユーザ選択して送信可能

☆電子署名利用可能（民間の適格証明書を選択して利用可）

eIDカードのみで6500万枚普及見通し
(署名用は伸びない？　500万人予測？　Cfベルギー全数配布)

3-1 市民ポータル構想の制度設計

■キーワード: 電子メール同様の簡便さと郵便同様の確実さ

■市民ポータル: 民間事業者による官民共用の通信基盤
09年4月に政府決定、連邦議会へ法案提出(新政権の動向まち)

■市民ポータルの機能:

①電子私書箱(自然人・法人用)の開設＆安全確実なアクセス
認証済みアドレス(de-mail.de)の付与　安全なアドレス
☆ユーザの希望により仮名アドレスも(本人確認済み仮名)
ex. pn_gustaf.mueller@t-online.de-mail.de

②メールの送受信証明機能(de-mail書留)　署名付き証明
☆電子政府の送達、裁判の送達など、法的送達機能承認

③ID管理・提供サービス(オプショナル de-Ident)→single-sign-on
☆ユーザのID管理、属性情報提供、第三者提供(署名つき)

④レジストリ・サービス(暗号通信、本人確認検証用)

⑤データ保管(オプショナル de-mail safe; Data safe)
☆(暗号化された)安全なデータ保管　将来的に長期署名保管

4 ドイツの認証基盤からの示唆

- 電子社会(官民共通)の文書/通信のセキュリティ要素
  署名＋ﾀｲﾑｽﾀﾝﾌﾟ(or/and第三者による証明)が不可欠。
- 郵便同様の確実で証明力ある通信基盤サービス必要
- 個人情報最小化のための「仮名(pseudonym)」重要！
  確実に本人確認がされた仮名をドイツでは重視。
- 多様な認証基盤を長期的な安全性・信頼性とともにどう確保するかの解決が課題
- 本人確認＋署名＋ﾀｲﾑｽﾀﾝﾌﾟの長期的検証可能性確保のための制度構築が急務(安全安心の長期的確保)
- 長期的な検証のための資料・ﾃﾞｰﾀの引継・保存・利用
- 長期的(将来的)なｼﾐｭﾚｰｼｮﾝと制度設計が重要
- (官民の)多様なｻｰﾋﾞｽ、ｱﾌﾟﾘｹｰｼｮﾝの標準化と相互運用性の確保が重要。 基盤整備とビジネスモデル
- 長期的な展望・指針・責任の重要性(国？民間？)

講演 10　パネルディスカッション②

電子認証の民間制度・基盤の確立に関するシンポジウム

クラウド事業者から見た電子認証の必要性／重要性

Cloud Business Alliance

Net One Systems

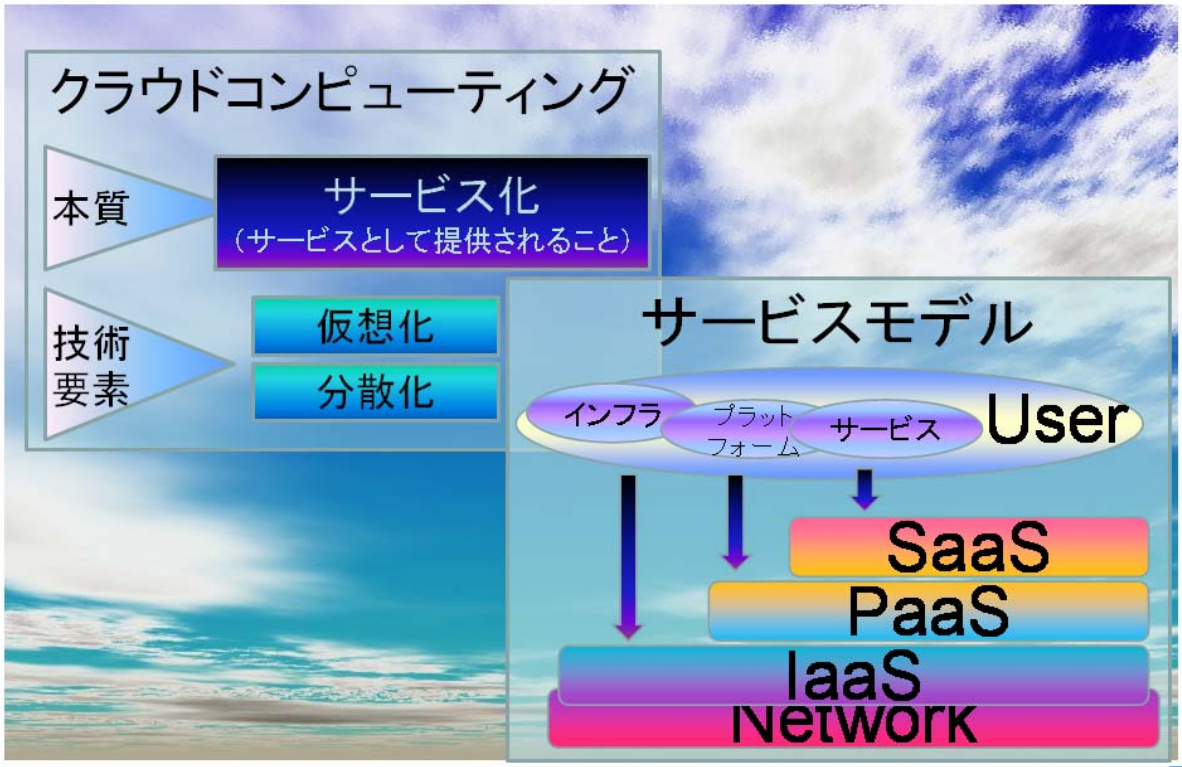
平成22年2月4日
ネットワンシステムズ株式会社
クラウド・ビジネス・アライアンス
福原　英之

バックグラウンド

- ネットワンシステムズ（株）
  - 1988年設立
  - コンピューター・ネットワーク市場を中心とするソリューションプロバイダー
  - 企業などに対してID管理やID連携のソリューション提供の実績あり
- クラウド・ビジネス・アライアンス
  - 2009年10月に、クラウド関連事業者を中心に発足
  - 「クラウド」を活用した新たなビジネスモデルの創出やそのための技術検証などを会員が相互に協力するための「場」を提供
  - SaaS事業者を中心に発足したが、その後IaaS/PaaS/SaaS事業者やイネーブラーが多数参加

Cloud Business Alliance

クラウドとは？



ID管理の重要性

- SaaS提供には「認証」が必須
  - オンラインサービスを前提としている
  - ほとんどの場合Multi-tenant
- 認証もサービスで
  - SaaS事業者は「本業」に注力したい
  - 共通サービスは統合した方がスケールメリットがある
  - シングルサインオン環境も提供が可能

認証は必須

認証は別管理にしたい

（メモ）
本資料では、ID管理のモデルとして、Idp／Sp　モデルを使用します。
Idp (ID Provider)：アイディー提供者、Authenticationの主体
Sp (Service Provider)：サービス提供者、Authorizationの主体

ID管理の運用課題

- 認証という言葉には2つの機能がある
  - Authentication
  - Authorization
- 認証機能の共有
  - Authentication の共有可能だが、Authorizationは共有が困難？
- 権限管理は誰が実施する？
  - Authorizationはアプリ内部の動作に直結
  - 企業ユーザー側でポリシーを管理・決定する必要がある
  - 個別のサービスごとに管理するとSSOのメリットが・・・

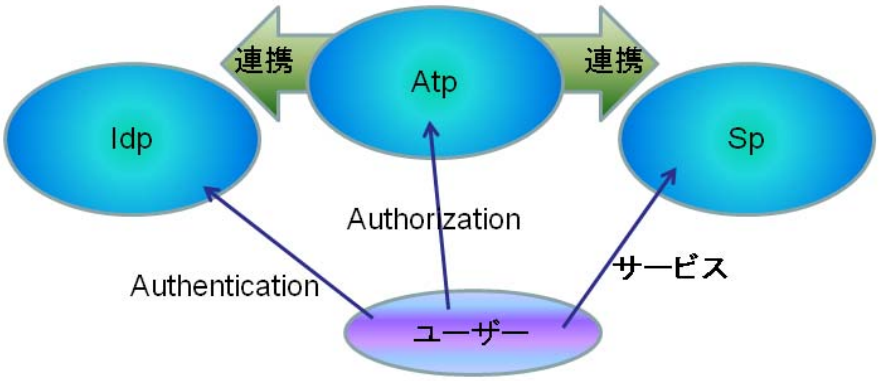
（メモ）
Idpの仕組みとしてPKIを採用すると、
- 24時間稼働を保証する「認証サーバー」の負荷は軽減される。
- セキュリティー上のリスク管理も軽減される。

クラウド環境でのID管理（権限管理）の改善アイデア

- Atpサービス

  権限を紐づける「属性」（Attribute）を提供する役割を作る

  Atp： Attribute Provider
  - ユーザー企業の管理者が社員の権限を管理
  - システム設置の形態
    - 社内に権限管理システムを設置しSaaSとオンラインで連携
    - Atp事業者が権限管理サービスとして提供




Business
Cloud
Alliance
Net One Systems

JCANを活用したビジネスシーンの検討

2010/02/04
株式会社 日立製作所
公共システム事業部　公共ビジネス戦略室
中村 信次

uVALUE

Contents

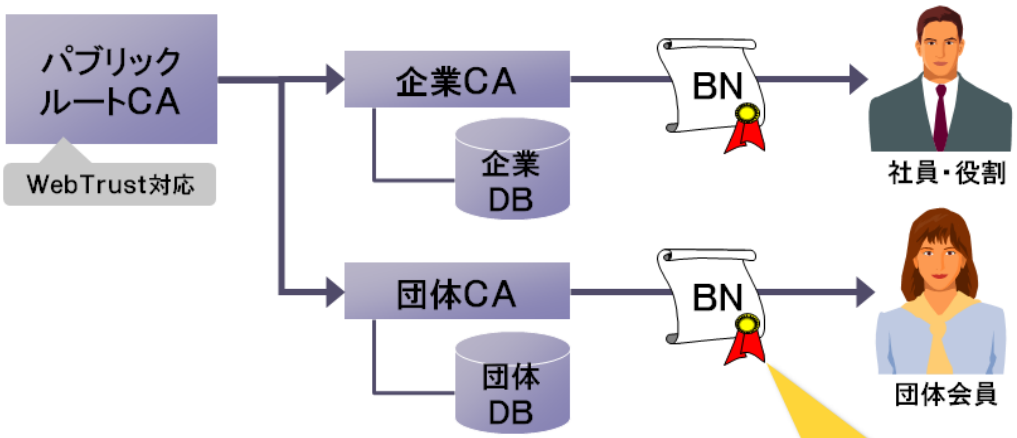
uVALUE

©Hitachi、Ltd. 2010. All rights reserved.

1. JCANの基本的な仕組み

HITACHI Inspire the Next

組織の構成メンバーおよび役割等に対して電子証明書を発行する仕組み



- 企業の社員として利用する電子証明書。
- 電子証明書は広く公開して利用するものとなる。
- 証明書には、名刺と同様の情報が記載される。

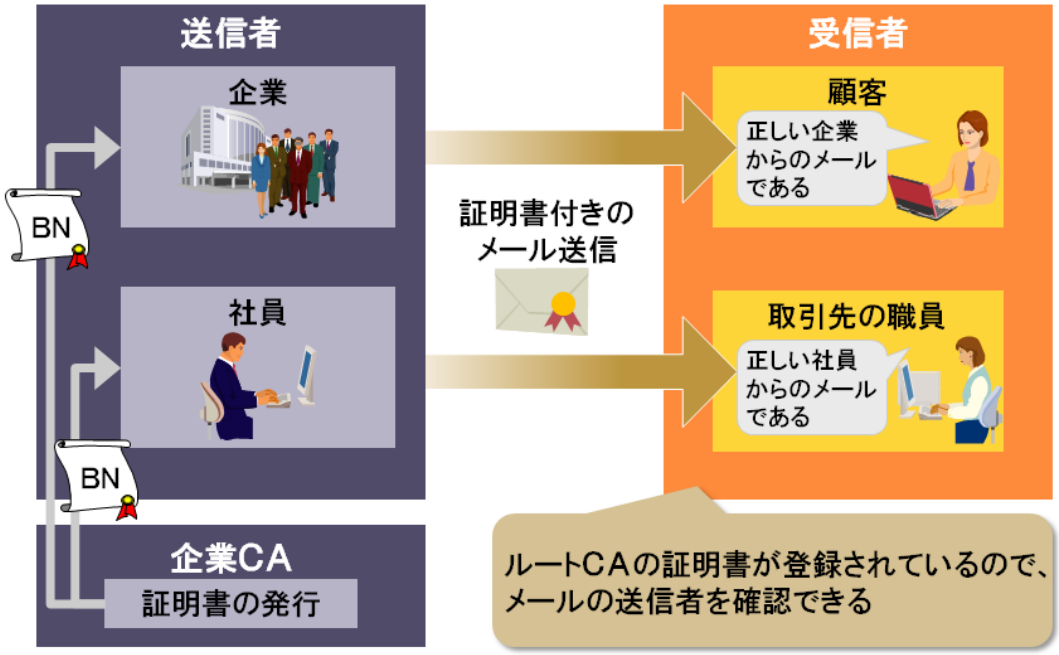
・Business Nameの略
・ペンネームや旧姓など、実名でない場合もある

uVALUE

2. JCANを活用したビジネスシーン

HITACHI Inspire the Next

2.1 電子メール／添付ファイルの改ざん対策（署名付きメール）



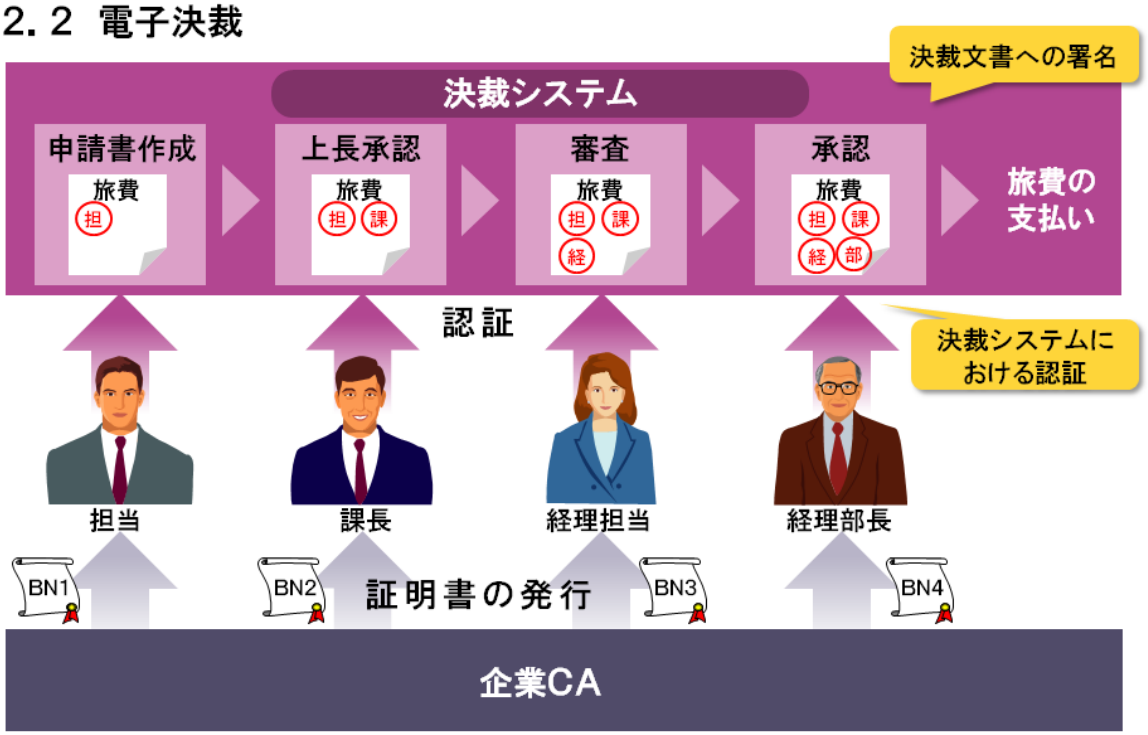
ルートCAの証明書が登録されているので、メールの送信者を確認できる

uVALUE

2. JCANを活用したビジネスシーン

HITACHI Inspire the Next

2. 2 電子決裁



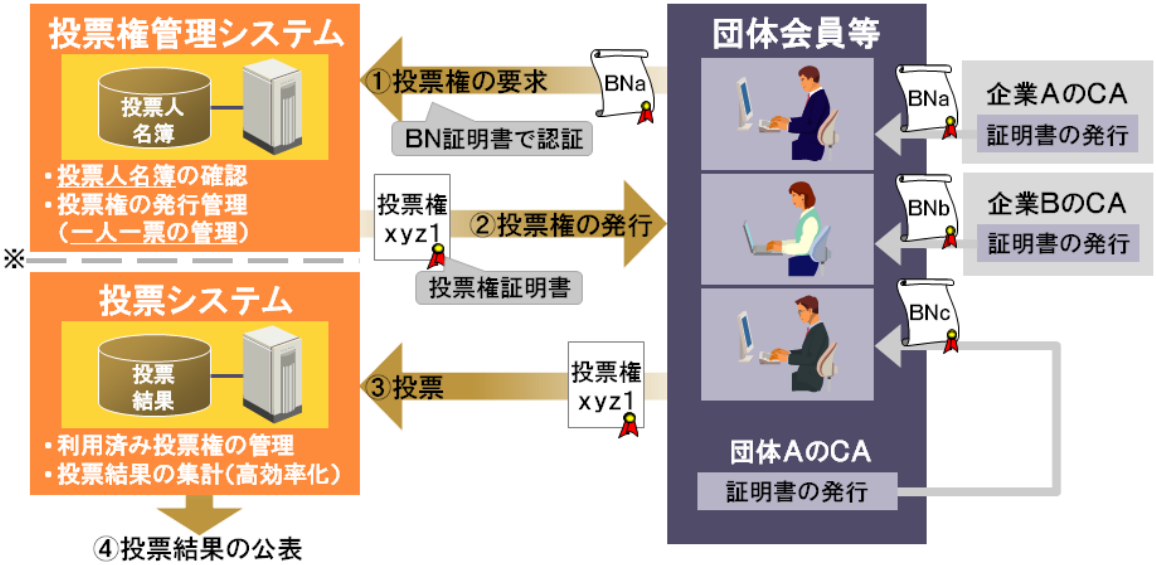
uVALUE

2. JCANを活用したビジネスシーン

HITACHI Inspire the Next

2. 3 投票での利用(役員投票・議案採決等)

1. 投票権郵送コストの軽減
2. 事務処理の負担を軽減
3. 投票結果の収集時間を短縮
4. 無人化による透明性の向上



uVALUE 注※:管理権限を分離すれば無記名投票にも対応

3. PS名の分類

HITACHI
Inspire the Next

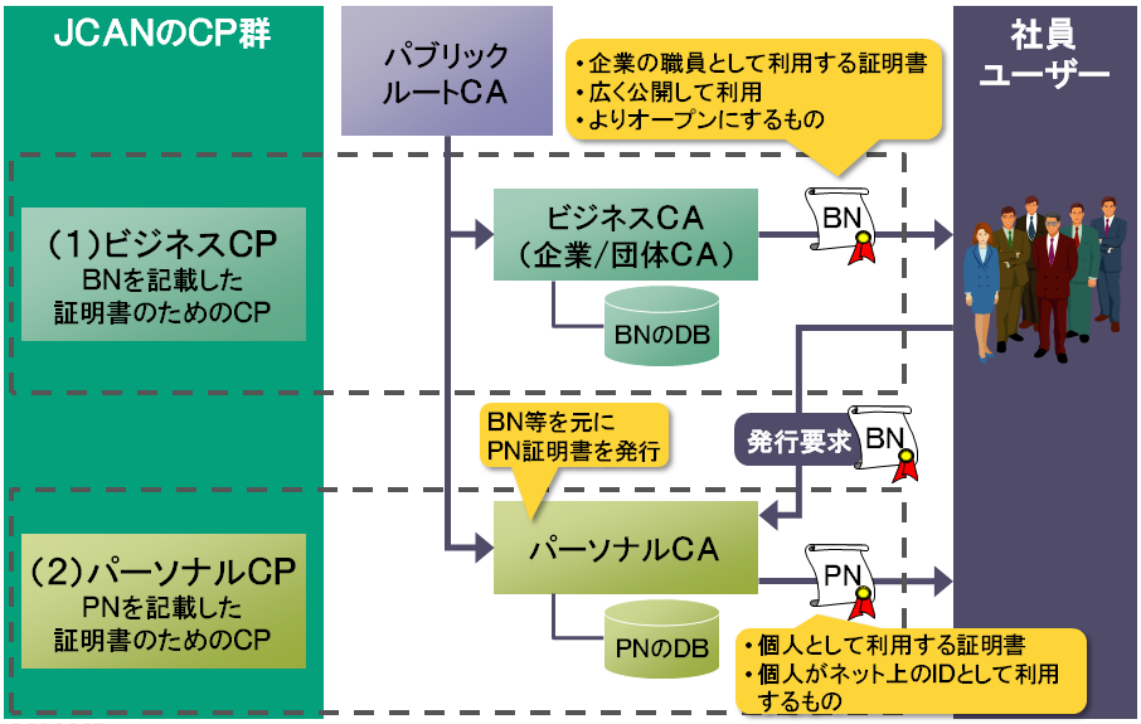
		PS名	
		BN(Business Name)	PN(Personal Name)
1	目的	社会的にビジネス活動する為に広く公開して利用	個人がネット上のIDとして活用
2	表記内容（証明書記載情報）	実名、旧姓、芸名、ペンネーム等	意味の無いID、自身が決めたニックネーム等（一意に識別可能なもの）
3	発行の由来	会社への所属	BNを所有していること等
4	主な利用シーン	BtoB、C、G	CtoC、B
5	同類の仕組み	名刺、メールのシグネチャ等	ドイツ市民ポータルのPseudonym
6	情報保護の考え方	氏名等は含まれるが、半ば公開され、流通可能と想定	個人情報を含まない
7	PS名の変更	人事異動や転職等で再発行（変更）となる	利用者が希望しなければ変更にならない

uVALUE

 6

4. JCANの応用機能

HITACHI
Inspire the Next



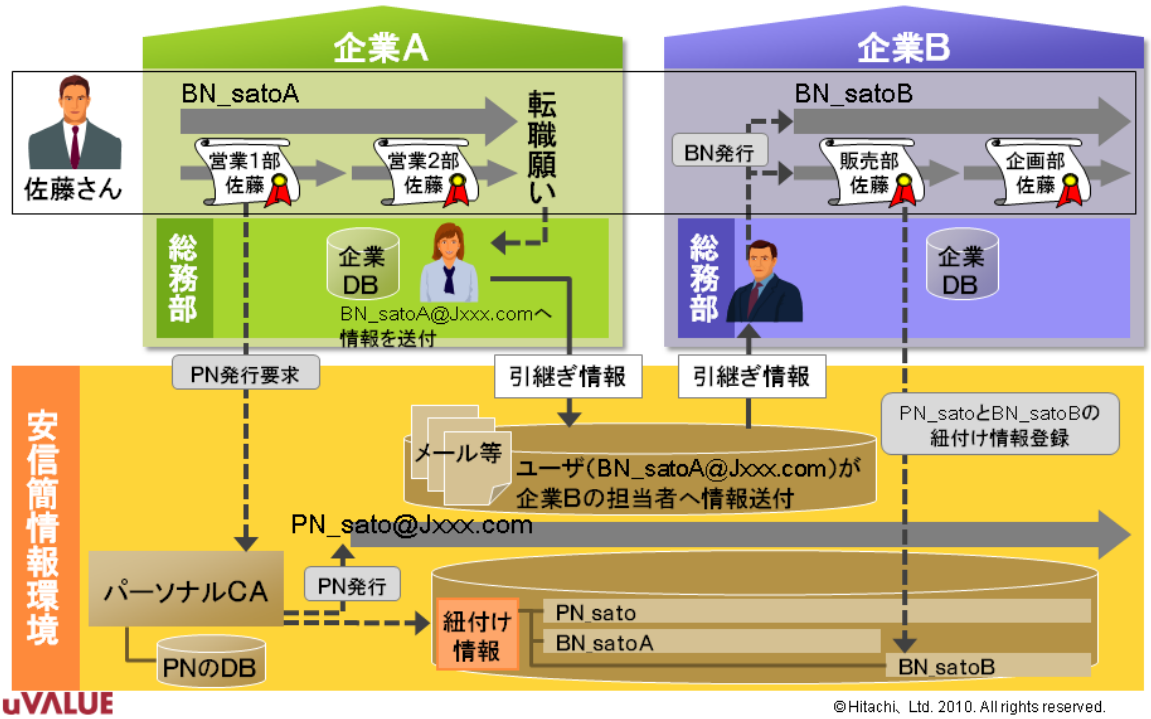
uVALUE

 7

5. JCANを応用的に活用したビジネスシーン

HITACHI Inspire the Next

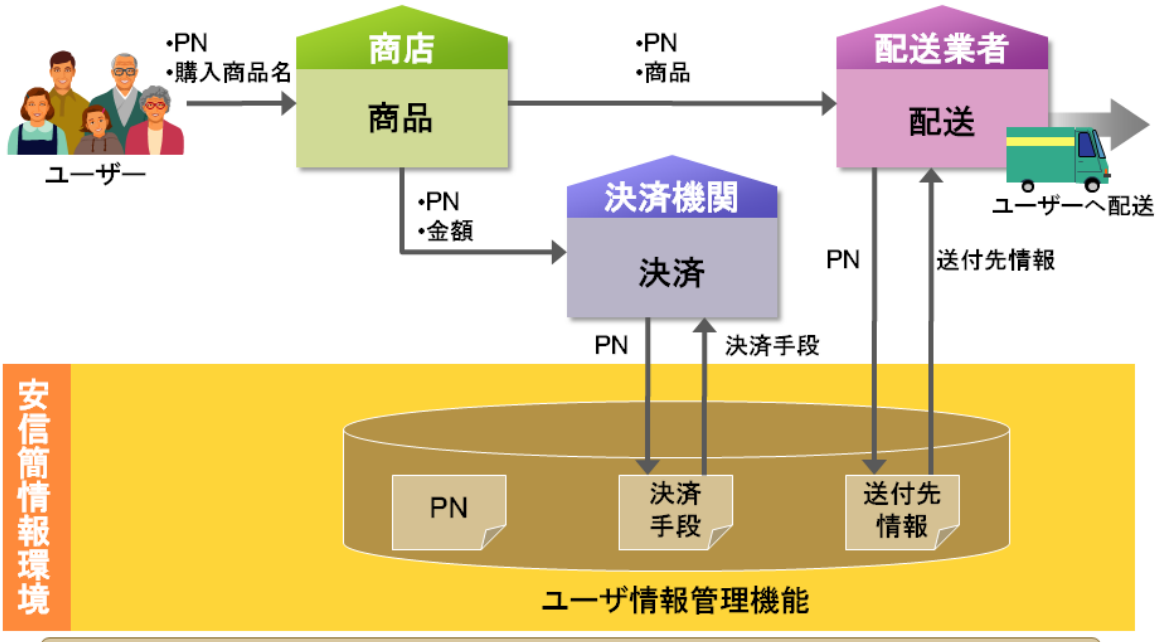
5.1 安信簡情報環境を利用したPS名のライフサイクル



5. JCANを応用的に活用したビジネスシーン

HITACHI Inspire the Next

5.2 オンラインショッピング



ワンタイムのPNを活用する等で更なる情報保護を実現可能

6. まとめ

HITACHI
Inspire the Next

1. PS名として、ビジネス活動で利用するBNと、個人がネット上のIDとして活用するPNの2つに分類し、それぞれの利用シーンを例示した。

2. BNが普及することで、企業活動におけるPKIの高度利用が促進されていくものと考える。
一方、BNを信頼の基点としたPNの仕組みを導入することにより、社員の立場を離れた個人の活動に対しても広く利用できるものになると考える。

3. これらBN、PNといった個人を証明する仕組みと、情報を交換させる基盤の具体化は、経済の活性化に貢献するものと考える。

4. JIPDECを中心として、「安信簡」情報環境の具体化が推進されることを期待する。

uVALUE

uVALUE


HITACHI
Inspire the Next

G「シンポジウム実施報告」

電子認証の民間制度・基盤の確立に関するシンポジウム　実施報告

日　時：平成 22 年 2 月 4 日（木）　実施期間 10:00 - 17:30

場　所：秋葉原コンベンションホール（東京都千代田区外神田 1-18-13 秋葉原ダイビル 2F）

プログラム：

第 1 部：制度･基盤	
10:00-10:15	**電子認証等の民間制度・基盤**
1	講師：青木 尚（JIPDEC 電子商取引推進センター 主席研究員）
10:15-10:30	**ビジネスモデル検討部会**
2	講師：満塩 尚史（株式会社イマーディオ パートナー／環境省情報化統括責任者（CIO）補佐官／各府省 CIO 補佐官等連絡会議情報セキュリティ WG リーダー）
10:30-10:45	**ポリシー/基盤システム検討部会**
3	講師：手塚 悟（東京工科大学 コンピュータサイエンス学部 教授）
10:45-11:00	**評価基準検討部会**
4	講師：大木 栄二郎（工学院大学 情報学部情報デザイン科 教授）
11:00-11:05	**質疑応答**
11:10-12:00	**パネルディスカッション**
5	**テーマ：ポリシー（JCAN ビジネス CP）** 進　行：手塚 悟（東京工科大学 コンピュータサイエンス学部 教授） パネリスト：・佐々木 良一（東京電機大学未来学部 情報メディア学科教授） ・満塩 尚史（株式会社イマーディオ パートナー／環境省情報化統括責任者（CIO）補佐官／各府省 CIO 補佐官等連絡会議情報セキュリティ WG リーダー） ・阿藤 寿孝（アマノ株式会社 時間情報事業本部 副本部長） ・稲葉 厚志（GMO グローバルサイン株式会社 CA 戦略室 室長） ・岡部 寿男（京都大学学術情報メディアセンター ネットワーク研究部門 教授） ・西田 梢（シヤチハタ株式会社 IS 営業部開発課 主任） ・松永 隆司（東北インフォメーション・システムズ株式会社 法人ソリューション事業部 ソリューションサービスグループ副長） ・青木 尚（JIPDEC 電子商取引推進センター 主席研究員）
昼休憩（80 分）	
13:20-13:40	**ビジネスパス**
6	講師：福田 昭和（株式会社 HARTIN MARTIN 取締役）
13:40-13:45	**質疑応答**
第 2 部：海外動向	
13:50-14:30	**韓国における認証基盤について**
7	講師：Moon Sung-Eun《문성은》（Koscom Corporation《코스콤》, Team Manager）
14:30-15:10	**台湾における認証基盤について**
8	講師：Luke Lu《魯君禮》（National Information Infrastructure Enterprise Promotion Association《財團法人中華民國國家資訊基本建設產業發展協進會》, Information Risk　Management Division《資訊風險管理組》Director）
15:10-15:40	**ドイツにおける認証基盤について**
9	講師：米丸 恒治（神戸大学大学院法学研究科 教授）
休憩（10 分）	
第 3 部：ビジネスシーン	
15:50-17:20	**パネルディスカッション**
10	**テーマ：ビジネスモデル** 進　行：満塩 尚史（株式会社イマーディオ パートナー／環境省情報化統括責任者（CIO）補佐官／各府省 CIO 補佐官等連絡会議情報セキュリティ WG リーダー） パネリスト：・手塚 悟（東京工科大学コンピュータサイエンス学部 教授） ・中村 信次（株式会社日立製作所 公共システム事業部 公共ビジネス戦略室主任技師） ・福原 英之（ネットワンシステムズ株式会社 商品開発グループ　応用技術本部 DC プロダクト開発部 SaaS イネーブリングチーム 課長） ・米丸 恒治（神戸大学大学院法学研究科 教授） ・亀田 繁（JIPDEC 電子商取引推進センター 主席研究員）

申込者：317 名

参加者：198 名（出席率 62%、当日参加 4 名）

アンケート回答：108 枚（回収率 55%）

プログラム内容：

第 1 部：制度･基盤

◆「電子認証等の民間制度・基盤」講演者：青木尚氏（JIPDEC 電子商取引推進センター主席研究員）

本シンポジウムについての目的、主旨、プログラム構成の説明によるガイダンスを行った。

◆「ビジネスモデル検討部会」講演者：(株式会社イマーディオ パートナー/環境省情報化統括責任者（CIO）補佐官/各府省 CIO 補佐官等連絡会議情報セキュリティ WG リーダー)

ビジネスシーンの検討、電子認証等の民間制度・基盤に係るプロモーション冊子の検討/アンケートの実施、登録業務効率化の検討等についての検討結果を紹介した。

◆「ポリシー/基盤システム検討部会」講演者：手塚 悟（東京工科大学 コンピュータサイエンス学部 教授）

企業/団体（企業等）ベース認証基盤に基づいて企業等が企業等に属する対象（企業等内個人、部門名等）に発行する電子証明書に係る制度/基盤のあり方の検討等についての検討結果を紹介した。

◆「評価基準検討部会」講演者：大木 栄二郎（工学院大学 情報学部情報デザイン科 教授）

WebTrust for CA の監査基準と電子署名法に基づく認定制度の適合例を入れ込んだ調査表案の検討等についての検討結果を紹介した。

◆パネルディスカッション「ポリシー（JCAN ビジネス CP)」パネリスト：手塚 悟（東京工科大学 コンピュータサイエンス学部 教授）〔進行〕、佐々木 良一（東京電機大学未来学部 情報メディア学科教授)、満塩 尚史（前述参照)、阿藤 寿孝（アマノ株式会社 時間情報事業本部 副本部長)、稲葉 厚志（GMO グローバルサイン株式会社 CA 戦略室 室長)、岡部 寿男（京都大学学術情報メディアセンター ネットワーク研究部門 教授)、西田 梢（シヤチハタ株式会社 IS 営業部開発課 主任)、松永 隆司（東北インフォメーション・システムズ株式会社法人ソリューション事業部ソリューションサービスグループ副長)、青木 尚（前述参照）

企業等の認証基盤に係る共通ルールの必要性、使用用途等についてパネルディスカッションを行った。

◆「ビジネス・パス」講演者：福田 昭和（株式会社 HARTIN MARTIN 取締役）

さまざまな認証基盤の利用を一つの媒体に集約化し、 認証・決済・保存とシームレスに連携、ビジネスを効率よく、効果的に行うためのパス等について等についての検討結果を紹介した。

第 2 部：海外動向

◆「韓国における認証基盤について」講演者：Moon Sung-Eun（Koscom Corporation, Team Manager）

韓国での PKI の現状、金融、電子決済、電子申告・納税、電子調達、モバイル等について紹介した。

◆「台湾における認証基盤について」講演者：Luke Lu （National Information Infrastructure Enterprise Promotion Association, Information Risk Management Division Director）

台湾での電子認証利用の現状、電子インボイスの利用と課題、電子カルテの展望の姿等について紹介した。

◆「ドイツにおける認証基盤について」講演者：米丸 恒治（神戸大学大学院法学研究科 教授）

ドイツでの電子署名法とその署名・認証基盤、ドイツ eID カードを利用した署名・認証基盤、市民ポータル構想（案）における認証基盤等について紹介した。

第 3 部：ビジネスシーン

◆パネルディスカッション（テーマ：ビジネスモデル）パネリスト：満塩 尚史（前述参照）〔進行〕、手塚 悟（前述参照）、中村 信次（株式会社日立製作所公共システム事業部公共ビジネス戦略室 主任技師）、福原 英之（ネットワンシステムズ株式会社 商品開発グループ応用技術本部 DC プロダクト開発部 SaaS イネーブリングチーム 課長）、米丸 恒治（前述参照）、亀田 繁（JIPDEC 電子商取引推進センター 主席研究員）

クラウド事業者から見た電子認証の必要性、重要性、ビジネスシーン（電子決裁、電子投票（投票での利用（役員投票・議案採決等））、Pseudonym に使われ方についてパネルディスカッションを行った。

電子認証の民間制度・基盤の確立に関するシンポジウム
参加者アンケート

本日は、当シンポジウムにご参加いただき、誠にありがとうございます。
今後のセミナー開催の参考にするため、ご参加された皆様にご意見を伺いたいと存じます。
お手数ですが、下記のご質問にお答えいただき、お帰りの際にアンケート回収箱にお入れ下さい。
何卒、よろしくお願い申し上げます。

質問１　本シンポジウムの開催をどのようにお知りになりましたか？　該当するものに「○」をつけてください。(複数回答可)
・JIPDEC ホームページ
・JIPDEC 案内メール
・その他のホームページ　（　　）
・その他の案内メール　（　　）
・その他　（　　）

質問２　(1)～(4)に該当するものに「○」をつけ、本シンポジウムのプログラムの中で参考になった事項や今後のシンポジウム等で説明して欲しい事項などありましたら、「ｺﾒﾝﾄ」覧にご記入ください。

プログラム等	参考になった事項や説明して欲しい事項など
1. 電子認証等の民間制度・基盤	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：
2. ビジネスモデル検討部会	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：
3. ポリシー/基盤システム検討部会	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：
4. 評価基準検討部会	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：

1

裏頁に続く

5. パネルディスカッション：JCAN ビジネス CP	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：
6. ビジネスパス	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：
7. 韓国における 認証基盤について	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：
8. 台湾における 認証基盤について	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：
9. ドイツにおける 認証基盤について	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：
10. パネルディスカッション：ビジネスモデル	(1)理解出来興味をもった　(2)理解できた　(3)あまり理解できない　(4)理解出来ない ｺﾒﾝﾄ：

質問 3　その他、シンポジウムに関すること、あるいは社会的な基盤として構築すべき新しい情報環境のあり方等に関して、ご意見ご要望がございましたら、ご記入ください。

ご協力ありがとうございました。

H「ポリシーの検討」

－ 目 次 －

1章 電子証明書ポリシー

1. 章　電子証明書ポリシー

1.1 はじめに

JCAN 共通 CP「JCAN ビジネス CP」は、JCAN 及び JCAN パートナー認証局（以下「JCAN パートナーCA」という）が発行する証明書の利用目的、適用範囲、利用者手続き等、JCAN が取り扱う証明書に関する共通のポリシーを規定するものである。

JCAN パートナーCA の運用に関する諸手続きは、JCAN 共通 CPS に規定する。

1.1.1 概要

本 CP は、JCAN 及び JCAN パートナーCA 及び JCAN パートナーCA から発行されるすべてのエンドエンティティ証明書（以下「EE 証明書」という）に適用される。本 CP の目的は、JCAN の証明書の利用目的、適用範囲、証明書の種類と用途を示し、証明書の発行に付随する要件を示すことである。

1.1.2 JCANが取り扱う証明書タイプ

本 CP で取り扱う証明書タイプは、以下のとおりである。総称して「JCAN 証明書」と呼ぶ。

(1) **パートナーCA証明書**

JCAN CA により認定されたパートナーCA の CA 証明書である。パートナーCA 証明書は以下の 2 通りで発行される。

- JCAN ルート CA 又は JCAN 中間 CA から発行される
- WebTrust の認定をうけているパブリック認証局から発行される

何れの場合も、パートナーCA 証明書の発行に当たっては、本 CP が定める証明書プロファイルに準拠しなければならない。なお、パートナーCA 証明書の発行に当たっての諸手続きは、パートナーCA 証明書の発行元認証局が個別に CPS に規定する。

(2) JCAN**ビジネス証明書**

JCAN は、幾つかのタイプの個人及び組織が使用する EE 証明書を提供する。これらの証明書は、認証サービス、セキュア電子メール、及び組織内、組織間、インターネットでの金額を伴わない取引で利用者を認証することに利用できる。JCAN が取扱う証明書（以下「JCAN 証明書」という）のタイプを下記に示す。

(a) **企業／団体内個人及びそれに結びつく属性（肩書き等）を証明する証明書**

(b) **企業／団体の組織（部門名、役割）であることを証明する証明書**

(c) **企業／団体の設備であることを証する証明書**

1.1.3 文書名と識別

本 CP の正式名称は“JCAN 共通 CP「JCAN ビジネス CP」”である。

1.1.4 PKIの関係者

(1) JCANルート認証局

JCAN ルート認証局（以下「JCAN ルート CA」という）は、本 CP を含め、JCAN が取り扱う証明書の全てのポリシーを起草する責任を負うポリシー管理局である。

(2) パートナー認証局

パートナーCA は、本 CP が定めるポリシーに従い、2.1.2.に記載の証明書（以下「JCAN 証明書」という）を、その利用目的、適用範囲、手続き等に準拠して発行する JCAN が認定する認証局である。

(3) 登録局

パートナーCA は登録局を通じて利用者に連絡をする。登録局は本 CP の下、証明書を申請する利用者の実在性確認と本人性確認の審査を行い、証明書の発行と失効のための登録業務を行う。

(4) 利用者

JCAN 認証サービスの利用者は、認証局から 2.1.2.の（2）に記載の EE 証明書の発行をうける主体である。なお、証明書の発行をうける主体が組織または設備である場合は、利用者は指定された組織内の個人である。

(5) サブジェクト（利用者識別情報）

JCAN 認証サービスの EE 証明書のサブジェクトは、企業／団体に属する、個人、部門、及び設備である。

(6) 証明書申請者

証明書申請者は、サブジェクトの代わりに認証局の利用者規約に同意し、証明書を申請する者である。

証明書申請者は、以下の通りである。

- サブジェクトが個人である場合は、サブジェクト自身である。
- サブジェクトが組織である場合は、組織・法人に属する個人である。
- サブジェクトが設備である場合、設備を管理する組織・法人に属する個人である。

(7) 検証者

検証者は、利用者の証明書を信頼する者、又は利用者の電子署名を信頼する者である。証明書の有効性を検証するために、検証者は必ず認証局失効情報を参照しなければならない。

1.1.5 証明書の用途

(1) 用途

JCAN 証明書は、1.2.2 に記載される範囲で、認証サービス、セキュア電子メール、及び組織内、組織間、インターネットでの金額を伴わない取引で利用者を認証することに利用できる。

(2) **適切な証明書の用途**

JCAN 証明書は、本 CP に記載の範囲での適切な用途に利用できる。その他の許可されない用途への利用は、認証局が提供する保証の対象から外れる場合がある。

1.1.6 ポリシー管理

JCAN ルート CA は、JCAN の領域内の証明書サービスを管理する最上位のポリシー管理局（トラストアンカーとも呼ばれる）である。JCAN ルート CA が本 CP を管理する。

1.2 公開とリポジトリの責任

1.2.1 リポジトリ

JCAN は、発行する証明書に関する情報をリポジトリに公開する。JCAN は、本 CP を含む、その業務手続、特定のポリシーの内容について、リポジトリに一定の開示を行う。

1.2.2 証明書情報の公開

JCAN は、次の内容をリポジトリに公開し、証明書利用者及び検証者がオンラインで参照できるようにする。

- CRL
- 本 CA 証明書
- 最新の CP、CPS
- 本 CA が発行する証明書に関するその他の情報

1.2.3 公開の時期と頻度

本 CP 及び CPS は更新の都度、公開される。CRL は失効情報に変更がある都度と、CRL の有効期限内で定期的に更新される。

なお、証明書の有効期限を過ぎたものは CRL から削除される。

1.3 識別と認証

JCAN CA 及びパートナーCA は、証明書の発行の前に、認証局への証明書申請者の本人識別と他の属性を審査し、認証する業務手続文書を保持する。

1.3.1 名前決定

JCAN は、利用者を本人識別するために、例えば X.500 の Distinguished Names、RFC 822 の Names、及び X.400 の Names のように、サブジェクトに割り当てられた名前のタイプを含む、特定の命名と本人識別の規則に従う。

パートナーCA 証明書を申請する場合、申請者の名前は、申請者を表す正式な名称でなければならない。

1.3.2 初回の本人確認

(1) 秘密鍵の所有を検証する方法

証明書利用者が鍵ペアを生成する場合、秘密鍵を所有していることの検証は以下の方法で行う。証明書署名要求ファイル（以下「CSR」という）の署名検証を行い、CSR の公開鍵に対応する秘密鍵で署名されていることを確認する。

(2) 組織の認証

JCAN は、組織の認証を、標準企業コード（証券コード、TDB 企業コード、指定団体発行コード）と、国や地方公共団体が発行する公的書類、国や地方公共団体が管理する信頼できるデータベース（以下「QGIS」という）、JCAN が信頼する第三者データベース（以下「QIIS」という）、JCAN が独自に保有する組織に関するデータベース、その他 JCAN のポリシー管理局が同等の信頼性があると判断した方法によって実施する。

(3) パートナーCA証明書申請時の権限確認

JCAN は、パートナーCA 証明書の申請があった場合、「3.2.2　組織の認証」に記載の方法による組織の認証後、当該申請における申請者と承認者の権限確認を行う。

(4) RA管理者の認証

JCAN CA は、パートナーCA の RA 管理者用証明書の発行に際し、「3.2.2　組織の認証」に記載の方法による組織の認証と、当該組織の代表者による RA 管理者の指名の事実を確認する。

(5) パートナーCAから発行するEE証明書の本人確認

エンドエンティティ証明書の発行に際しては、パートナー登録局にて本人確認を行う。本人確認は企業/団体で保有する人事台帳、体制表、資産台帳での確認を行う。

- 台帳、体制表による確認
- EE 証明書の申請者の確認

(6) 利用者の登録に必要な情報

(a) 企業／団体内個人及びそれに結びつく属性（肩書き等）を証明する証明書

個人、肩書きの正式名称

(b) 企業／団体の組織（部門名、役割）であることを証明する証明書

部門名、役割名の正式名称

(c) 企業／団体の設備であることを証する証明書

設備の名称、管理番号等、設備を特定する情報

(7) 利用者の登録の記録

認証局は、検証に使用した文書に記載された参照番号と、その有効性に関する制限を含む、利用者の本人識別を検証するために使用した全ての情報を記録する。

認証局は上記に示さされた記録を証明書の有効期限が切れた後、少なくとも 5 年間保存する。

1.3.3 鍵の再生成申請時の利用者の本人確認

(1) 通常の鍵更新における本人性確認と認証

鍵更新における証明書利用者の本人確認は、「3.2 初回の本人確認」に準拠する。

1.3.4 失効申請時の本人性確認と認証

証明書の失効要求における本人識別と認証手続として、失効要求をする利用者の署名入り依頼書を要求する。

1.4 証明書のライフサイクルに対する運用上の要件

登録局、利用者、その他 JCAN 領域内の全てのエンティティは、証明書が有効期限切れになるか、失効されるまでの運用期間中、かかる証明書に記載される情報の全ての変更について、登録局を介して当該認証局に報告する継続的な義務を負う。

認証局は、登録局により提出される署名入りの要求に従って、証明書を発行／失効する。

パートナーCA は、その業務を実施するため、第三者の代理人を使用することがある。この場合、パートナーCA は、認証局業務のサービス提供に関する代理人の作為と不作為に対する全責任と説明責任を負う。

1.4.1 証明書申請手順

登録局は証明書申請を受けて、申請者の本人識別を検証する。続いて、登録局は証明書申請を承認又は棄却する。

1.4.2 証明書発行

証明書申請の検証後、登録局は、認証局に証明書発行要求を送信する。登録局からの要請は、有効に作成され、有効な利用者データが含まれ、認証局の仕様に合致していれば、承認される。発行された証明書は、サブジェクトに配送される。

(1) 証明書生成

証明書の発行及び更新に関して、認証局は、全ての当事者に対し、以下に規定される条件に従って、証明書が安全に発行する。

- 認証局は、認証局の領域内において利用者に割り当てられた識別名の唯一性を保証する。
- 登録データの機密性と完全性は、常時、適切な手段によって保証される。
- 登録機関の認証は、その機関に発行される適切な信用証明を通じて保証される。

1.4.3 証明書の受領

発行された証明書は、認証局が発行する証明書の受領を登録局が確認した時点で、利用者により受領されたと見なされる。

1.4.4 鍵ペアと証明書の用途

(1) 利用者による秘密鍵、及び証明書の使用

(a) 利用者の義務

利用者の義務は以下の通り。

- JCAN リポジトリに公開された本 CP の諸条件を承諾すること
- 証明書の信頼性に重大な影響を及ぼす情報の変更は、認証局又は登録局に、速やかに知らせること
- 証明書が有効でなくなった場合は、使用をやめること
- 証明書を、合理的な環境下で使用すること
- 秘密鍵を危殆化、紛失、不正開示、改ざん、その他の不正使用から防護すること
- 秘密鍵を適切に保護すること
- 証明書の完全性に重大な影響を及ぼす事象が発生した場合、当該証明書の失効を要求すること
- 証明書を不正操作から防護すること
- CP 及び利用規約に従って法例を遵守し、許可された用途にのみ、証明書を使用すること
- 利用者は、常に上記に述べた認証局に対する義務を負う。

(b) 電子証明書のライフサイクル運用要件

利用者は、認証局証明書の有効期間中における認証局証明書に記載された情報についての全ての変更、又は証明書の有効性に重大な影響を及ぼす事実を、直接登録局に知らせる継続的な義務を負う。

(c) 自己責任での信頼

JCAN CA リポジトリに掲示される情報を適切に評価し信頼することは、当事者自身の責任である。

(2) 検証者による公開鍵、及び証明書の使用

検証者の義務は以下の通りである。

(a) 検証者の義務

証明書の検証者は、以下を実施する。

- 認証局が公開する証明書ステータス情報を使用して、認証局証明書を検証する。
- かかる検証手続により、証明書に記載された情報が正しく、最新であると検証できたときに限り証明書を信頼する。
- JCAN CA 証明書を、合理的な環境下でのみ信頼する。

(b) JCAN CAリポジトリとウェブサイトの条件

認証局のリポジトリ及びウェブサイトにアクセスする利用者及び検証者は、本 CP の条項、及び認証局が供する他の使用条件を承諾する必要がある。

リポジトリの使用により、以下のことが可能になる。

- 認証局証明書の検索の結果、情報を取得すること
- 証明書に含まれる公開鍵に対応する秘密鍵を使用して生成された電子署名のステータスを検証すること

・ 認証局のウェブサイトに公開される情報を取得すること

1.4.5 証明書の更新

JCAN の証明書は、鍵更新を伴わない証明書の更新には対応しない。鍵更新を伴う証明書の更新は、「2.3.3　鍵の再生成申請時の利用者の本人確認」による。

1.4.6 証明書の失効

登録局からの要請を受けて、認証局は、次のような場合に認証局証明書を失効する。

・ 証明書サブジェクトの秘密鍵の紛失、盗難、不正開示、その他の危殆化があった場合
・ 証明書サブジェクト又はその指名した利用者が、本 CP の下の重大な義務に違反した場合
・ 本 CP の義務の履行遂行が、自然災害、コンピュータ又は通信障害、その他制御不能な事象により妨げられ、情報が重大な脅威に晒され危殆化した場合
・ 証明書に含まれる、証明書サブジェクトの情報の変更があった場合

1.4.7 証明書のステータス確認サービス

認証局は、CRL、及び適当なウェブインタフェースを含む、証明書ステータス確認サービスを提供する。

1.4.8 利用の終了

利用者の加入は、証明書の失効、有効期限切れ、又はサービスが終了したとき、終了する。

1.5 設備上、運営上、運用上の管理

“規定しない”

1.5.1 物理的管理

“規定しない”

1.5.2 手続的管理

“規定しない”

1.5.3 人事的管理

“規定しない”

1.5.4 監査ログの手続

“規定しない”

1.5.5 記録のアーカイブ

“規定しない”

1.5.6 危殆化、及び災害からの復旧

“規定しない”

1.5.7 認証局又は登録局の終了

“規定しない”

1.6 技術的セキュリティ管理

“規定しない”

1.6.1 鍵ペアの生成、及びインストール

“規定しない”

1.6.2 鍵ペアの再生成と再インストール

“規定しない”

1.6.3 秘密鍵の保護、及び暗号モジュール技術の管理

“規定しない”

1.6.4 その他の鍵ペア管理

“規定しない”

1.6.5 活性化データ

“規定しない”

1.6.6 コンピュータのセキュリティ管理

“規定しない”

1.6.7 ライフサイクルの技術上の管理

“規定しない”

1.6.8 ネットワークセキュリティ管理

“規定しない”

1.7 証明書、及びCRLのプロファイル

このセクションは、証明書フォーマット、CRL を規定する。

1.7.1 証明書プロファイル

添付資料-1 を参照。

（EE 証明書プロファイル、subCA 証明書プロファイル、RootCA 証明書プロファイル）

1.7.2 CRLプロファイル

添付資料-2 を参照。（CRL プロファイル）

1.8 準拠性監査とその他の評価

“規定しない”

1.8.1 監査の頻度あるいは条件

“規定しない”

1.9 他の業務上の問題、及び法的問題

“規定しない”

1.9.1 料金

“規定しない”

1.9.2 財務的責任

“規定しない”

1.9.3 業務情報の機密性

“規定しない”

1.9.4 個人情報のプライバシー保護

“規定しない”

1.9.5 知的財産権

本 CP 及び CPS を含み JCAN が発行するすべての刊行物の知的財産権について、JCAN はその権利を留保する。

1.9.6 表明保証

“規定しない”

1.9.7 無保証

“規定しない”

1.9.8 責任の制限

“規定しない”

1.9.9 補償

“規定しない”

1.9.10 期間と終了

“規定しない”

1.9.11 関係者間の個別通知と連絡

“規定しない”

1.9.12 改訂

本 CP の変更は、適切に付与する番号を通じて表示する。

JCAN CA のポリシー管理局が、付与するバージョン番号を決定する。

1.9.13 紛争解決手続

“規定しない”

1.9.14 準拠法

“規定しない”

1.9.15 適用法の遵守

“規定しない”

1.9.16 雑則

“規定しない”

1.10 定義語

CA（Certification Authority）：認証局

証明書の発行・更新・失効、CA 鍵の生成及び証明書利用者のを行う主体をいう。

CP（Certificate Policy）：証明書ポリシー

CA が発行する証明書の種類、適用範囲、発行対象、用途等、証明書に関する規程文書をいう。

CPS（Certification Practice Statement）：認証業務運用規程

CA を運用するうえでの運用手続きやセキュリティ基準を明示した規定文書をいう。

CRL（Certificate Revocation List）:証明書失効リスト

証明書の有効期間内にも拘わらず失効された証明書情報を記載したリストをいう。

CSR(Certificate Signing Request)：証明書署名要求

申請者から認証局へ、証明書を要求する際に送られる機械可読の申込書式をいう。

QGIS(Qualified Government. Information Source)：行政機関の信頼情報源

EV ガイドラインで認められている「信頼できる行政機関の情報源」をいう。オンラインで公開され、定期的に更新される、行政機関が運営するデータベースで、データの報告が法律で義務付けられ、虚偽の報告には刑事罰または民事罰が科せられるものをいう。

QIIS(Qualified Independent Information Source)：第三者機関の信頼情報源

EV ガイドラインで認められている「信頼できる独立した第三機関の情報源」をいう。オンラインで公開され、定期的に更新される民間機関が運営するデータベースをいう。

X.400

ITU-TS の勧告の一つで電子メールについての標準を定めたもの。

X.500

ITU-T が定めた、ネットワーク上での分散ディレクトリサービスに関する規格。X.509 は公開鍵認証の標準形式を規定している。

アーカイブ
複数のファイルを一つのファイルにまとめたファイルをいう。

サブジェクト（利用者識別情報）
利用者を識別するための情報をいう。

タイムスタンプ
ファイルなどの電子データにおいて、その作成や更新などが行われた日時を示す情報。PKI の仕組みによって正確な日時、存在証明、非改ざん証明を行える。

パートナーCA：パートナー認証局
JCAN ルートによる認証を受け、JCAN エンドエンティティ証明書を発行するサービスを行う認証局をいう。

証明書プロファイル
汎用的な x.509 証明書に対して、証明書の使用方法が明記されていることをいう。

リポジトリ
証明書及び他の関連情報を列挙する、オンラインで利用できるデータベース及び/又はディレクトリをいう。

ルート CA：ルート認証局
電子証明書の認証局の種類の一つで、上位の認証局による認証を受けず、自分の正当性を自ら証明する認証局をいう。

中間 CA：中間認証局
上位の認証局による認証を受けることにより自らの正当性を認証する認証局をいう。

登録局
CA の業務のうち、利用者(申請者)の本人識別と登録業務を行い、発行した証明書を利用者に安全に配布する責任を負う主体をいう。

1.11 添付資料-1 （証明書プロファイル）

EE証明書プロファイル（1/2）

■証明書プロファイル(Basic Certificate Fields)

項目 Certificate Fields		設定	データタイプ	説明	JCANチェック欄		
					形式	内容	
Version			INTEGER	v3 のため「2」			必須
SerialNumber			INTEGER	CAが割り当てる一意な番号			必須
Signature			AlgorithmIdentifier	SHA-256withRSAEncryption （ 1.2.840.113549.1.1.11）			必須
Validity			Validity	証明書の有効期間（1年、他任意）要検討			必須
	NotBefore		UTCTime	YymmddhhmmssZ(年月日時間分秒Z) ※発行判断を行った時から6カ月以内の任意の日時			必須
	NotAfter		UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須
Issuer			Name	電子証明書を発行した機関(CA) の名前、X.500 識別名 (DN) で記述 CA 証明書に含まれる subject と同じDNを記述			CA証明書に依存？
	CountryName		PrintableString	JP			必須？
	StateName		PrintableString	Tokyo			オプション？
	LocalityName		PrintableString	Minato-Ku			オプション？
	OrganizationName		オブジェクト識別子（OID）	2.5.4.10			
			PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code（0147506022） or ISO/IEC8824_OID（1.2.392.200063）			必須？
	OrganizationUnitName		オブジェクト識別子（OID）	2.5.4.11			
			PrintableString	Head Quarter			必須？
	CommonName		オブジェクト識別子（OID）	2.5.4.3			
			PrintableString	JIPDEC Head Quarter CA1			必須？
Subject			Name	電子証明書の所有者の名前 ユーザの名前やサーバ名などを記述			
	CountryName		PrintableString	JP			必須
	StateName		PrintableString	【OP：Option】 Tokyo			オプション
	LocalityName		PrintableString	【OP】 Minato-Ku			オプション
	OrganizationName		オブジェクト識別子（OID）	2.5.4.10			
			PrintableString	ID_1.2.392.200063_JIPDEC			必須
	OrganizationUnitName		オブジェクト識別子（OID）	2.5.4.11			
			PrintableString	+81-3-3436-7500,www.jipdec.or.jp ※64文字以内に制限			必須
	CommonName		オブジェクト識別子（OID）	2.5.4.3			
			PrintableString	BN_shunin_shizaibu			必須
	SerialNumber		INTEGER	10.1023.20100137 ※管理番号			必須
SubjectPublicKeyInfo				証明書所有者（主体者）の公開鍵に関する情報			
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1（rsaEncryption）			必須
	SubjectPublicKey		BIT STRING	2048bitの公開鍵			必須

EE証明書プロファイル （2/2）

■証明書プロファイル(Standard Certificate Extensions)

項目	設定 criticality	データタイプ	説明	JCANチェック欄 形式	JCANチェック欄 内容	
authority Key Identifier	FALSE	オブジェクト識別子（OID）	2.5.29.35			
		OCTET STRING	RFC5280 4.2.1.2 に基づくSHA-1ハッシュ値			必須
subjectKeyIdentifier	FALSE	オブジェクト識別子（OID）	2.5.29.14			
		OCTET STRING	RFC5280 4.2.1.2 に基づくSHA-1ハッシュ値			必須
KeyUsage	TRUE	オブジェクト識別子（OID）	2.5.29.15			必須
DigitalSignature		BIT STRING	1			必須
NonRepudation		BIT STRING	1			必須
KeyEncipherment		BIT STRING	1			必須
DataEncipherment		BIT STRING	1			必須
KeyAgreement						
KeyCertSign						
CRLSign						設定しない
EncipherOnly						
extendedKeyUsage	FALSE	オブジェクト識別子（OID）	2.5.29.37			必須
clientAuth		オブジェクト識別子（OID）	1.3.6.1.5.5.7.3.2			必須
emailProtection		オブジェクト識別子（OID）	1.3.6.1.5.5.7.3.4			必須
msSmartcardLogin		オブジェクト識別子（OID）	1.3.6.1.4.1.311.20.2.2			オプション
msEncryptionFileSystem		オブジェクト識別子（OID）	1.3.6.1.4.1.311.10.3.4			オプション
certificatePolicies	FALSE	オブジェクト識別子（OID）	2 .5 .29 .32			必須
policyIdentifier						
certPolicyId		オブジェクト識別子（OID）	1.2.392.200121.1.1.1			必須
policyQualifiers						
policyQualifierID		オブジェクト識別子（OID）	1.3.6.1.5.5.7.2.1(id-qt-cps)			必須
qualifier		IA5String	https://www.iipdec.or.jp/ra/repository/			必須
policyQualifierID		オブジェクト識別子（OID）	1.3.6.1.5.5.7.2.2(id-qt-unotice)			必須
qualifier		UTF8String	JCAN Business CP			必須
subjectAltName	FALSE	オブジェクト識別子（OID）	2.5.29.17			必須
DirectoryName						
countryName		PrintableString	JP			オプション
organizationName		UTF8String	一般財団法人日本情報経済社会推進協会			オプション
organizationalUnitName		UTF8String	資材部、主任			オプション
commonName		UTF8String	日本太郎			オプション
rfc822Name		IA5String	nihon-taro@jipdec.or.jp			必須
OtherName						
UPN(プリンシパル名)		オブジェクト識別子（OID）	1.3.6.1.4.1.311.20.23			オプション
UPN(プリンシパル名)		UTF8String	ActiveDirectoryのプリンシパル名			オプション
issuerAltName	FALSE	オブジェクト識別子（OID）	2.5.29.18			必須
DirectoryName						
countryName		PrintableString	JP			必須
organizationName		UTF8String	一般財団法人日本情報経済社会推進協会			オプション
organizationalUnitName		UTF8String	本部			オプション
subjectDirectoryAttributes	FALSE					
attrType						将来使う？
attrValues						
cRLDistriburionPoints	FALSE	オブジェクト識別子（OID）	2.5.29.31			必須
distributionPoint						
FullName		オブジェクト識別子（OID）	2.23.42 .2 .0			必須
uniformResourceIdentifier		IA5String	http://*********			必須
authorutyInfoAccess	FALSE	オブジェクト識別子(OID)	1.3.6.1.5.5.7.1.1			必須
AccessMethod		オブジェクト識別子(OID)	1.3.6.1.5.5.7.48.2			必須
AccessLocation UniformResourceIdentifier		IA5STRING	“http://*****”			必須
netscape-cert-type	FALSE	オブジェクト識別子(OID)	2.16.840.1.113730.1.1			
		BIT STRING	SSL client, S/MIME			SUNIに確認中 当面入れておく

subCA証明書 (1/2)

■証明書プロファイル(Basic Certificate Fields)

項目 Certificate Fields		設定	データタイプ	説明	JCANチェック欄		
					形式	内容	
Version			INTEGER	v3 のため「2」			必須
SerialNumber			INTEGER	CAが割り当てる一意な番号			必須
Signature			AlgorithmIdentifier	SHA-256withRSAEncryption (1.2.840.113549.1.1.11)			必須
Validity			Validity	証明書の有効期間(10年？) CA階層を考慮			必須
	NotBefore		UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須
	NotAfter		UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須
Issuer			Name	電子証明書を発行した機関(CA) の名前、X.500 識別名 (DN) で記述			必須
	CountryName		PrintableString	JP			必須
	StateName		PrintableString	【OP:Option】 Tokyo			オプション
	LocalityName		PrintableString	【OP】 Minato-Ku			オプション
	OrganizationName		オブジェクト識別子(OID)	2.5.4.10			
			PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code(0147506022) or ISO/IEC8824_OID(1.2.392.200063)			必須
	OrganizationUnitName		オブジェクト識別子(OID)	2.5.4.11			
			PrintableString	JCAN Root CA1			必須
	CommonName		オブジェクト識別子(OID)	2.5.4.3			
			PrintableString	JCAN Root Certificate Authority			必須
Subject			Name	電子証明書の所有者の名前			必須
	CountryName		PrintableString	JP			必須
	StateName		PrintableString	【OP:Option】			オプション
	LocalityName		PrintableString	【OP】			オプション
	OrganizationName		オブジェクト識別子(OID)	2.5.4.10			
			PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code(0147506022) or ISO/IEC8824_OID(1.2.392.200063)			必須
	OrganizationUnitName		オブジェクト識別子(OID)	2.5.4.11			
			PrintableString	Head Quarter			必須
	CommonName		オブジェクト識別子(OID)	2.5.4.3			
			PrintableString	JIPDEC Head Quarter CA1			必須
	e-Mail						
	SerialNumber						
SubjectPublicKeyInfo			SubjectPublicKeyInfo	証明書所有者(主体者)の公開鍵に関する情報			必須
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1(rsaEncryption)			必須
	SubjectPublicKey		BIT STRING	2048bitの公開鍵			

subCA証明書 (2/2)

■証明書プロファイル(Standard Certificate Extensions)

項目	設定 criticality	データタイプ	説明	JCANチェック欄 形式	JCANチェック欄 内容	
authority Key Identifier	FALSE	オブジェクト識別子(OID)	2.5.29.35			必須
		OCTET STRING	RFC5280 4.2.1.2に基づくSHA-1ハッシュ値			
subjectKeyIdentifier	FALSE	オブジェクト識別子(OID)	2.5.29.14			必須
		OCTET STRING	RFC5280 4.2.1.2に基づくSHA-1ハッシュ値			
KeyUsage	TRUE	オブジェクト識別子(OID)	2.5.29.15			必須
DigitalSignature						
NonRepudation						
KeyEncipherment						
DataEncipherment						
KeyAgreement						
KeyCertSign		BIT STRING	1			必須
CRLSign		BIT STRING	1			必須
EncipherOnly						
extendedKeyUsage						
certificatePolicies	FALSE	オブジェクト識別子(OID)	2.5.29.32			必須
policyIdentifier						
certPolicyId		オブジェクト識別子(OID)	ポリシーのOID			
policyQualifiers						
policyQualifierID		オブジェクト識別子(OID)	1.3.6.1.5.5.7.2.1(id-qt-cps)			
qualifier		IA5String	URL			
policyQualifierID						
qualifier						
policyMapping						使用しない
Basic Constraints	TRUE	オブジェクト識別子(OID)	2 5 29 19			必須
CA		BOOLEAN	CA:TRUE PathLenConstraint:0			
subjectAltName						
DirectoryName						
countryName						
organizationName						使用しない
organizationalUnitName						
commonName						
e-Mail						
issuerAltName						
DirectoryName						
countryName						使用しない
organizationName						
organizationalUnitName						
subjectDirectoryAttributes	FALSE					
attrType						使用しない
attrValues						
cRLDistriburionPoints	FALSE	オブジェクト識別子(OID)	2.5.29.31			
distributionPoint						
FullName		オブジェクト識別子(OID)	2.23.42.0			必須
uniformResourceIdentifier		IA5String	URL			
subjectInfoAccess	FALSE					使用しない
authorutyInfoAccess	FALSE	オブジェクト識別子(OID)	1.3.6.1.5.5.7.1.1			
AccessMethod		オブジェクト識別子(OID)	1.3.6.1.5.5.48.2			必須
AccessLocation		IA5String	URL			
netscape-cert-type	FALSE	オブジェクト識別子(OID)	2.16.840.1.113730.1.1			
			SSL CA 、 S/MIME CA			必須

RootCA証明書 (1/2)

■証明書プロファイル(Basic Certificate Fields)

項目 Certificate Fields		設定	データタイプ	説明	JCANチェック欄		
					形式	内容	
Version			INTEGER	v3 のため「2」			必須
SerialNumber			INTEGER	CAが割り当てる一意な番号			必須
Signature			AlgorithmIdentifier	SHA-256withRSAEncryption (1.2.840.113549.1.1.11)			必須
Validity			Validity	証明書の有効期間(30年) ～2030年まで			必須
	NotBefore		UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須
	NotAfter		UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須
Issuer			Name	電子証明書を発行した機関(CA) の名前、X.500識別名 (DN) で記述			必須
	CountryName		PrintableString	JP			必須
	StateName		PrintableString	Tokyo			オプション
	LocalityName		PrintableString	Minato-Ku			オプション
	OrganizationName		オブジェクト識別子(OID)	2.5.4.10			
			PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code(0147506022) or ISO/IEC8824_OID(1.2.392.200063)			必須
	OrganizationUnitName		オブジェクト識別子(OID)	2.5.4.11			
			PrintableString	JCAN Root CA1			必須
	CommonName		オブジェクト識別子(OID)	2.5.4.3			
			PrintableString	JCAN Root Certificate Authority			必須
Subject			Name	電子証明書の所有者の名前			必須
	CountryName		PrintableString	JP			必須
	StateName		PrintableString	Tokyo			オプション
	LocalityName		PrintableString	Minato-Ku			オプション
	OrganizationName		オブジェクト識別子(OID)	2.5.4.10			
			PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code(0147506022) or ISO/IEC8824_OID(1.2.392.200063)			必須
	OrganizationUnitName		オブジェクト識別子(OID)	2 5 4 11			
			PrintableString	JCAN Root CA1			必須
	CommonName		オブジェクト識別子(OID)	2 5 4 3			
			PrintableString	JCAN Root Certificate Authority			必須
	e-Mail						
	SerialNumber						
SubjectPublicKeyInfo			SubjectPublicKeyInfo	証明書所有者(主体者)の公開鍵に関する情報			必須
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1(rsaEncryption)			
	SubjectPublicKey		BIT STRING	2048bitの公開鍵			必須

RootCA証明書 (2/2)

■証明書プロファイル(Standard Certificate Extensions)

項目	設定 criticality	データタイプ	説明	JCANチェック欄 形式	JCANチェック欄 内容	
subjectKeyIdentifier	FALSE	オブジェクト識別子(OID)	2.5.29.14			
		OCTET STRING	RFC5280 4.2.1.2に基づくSHA-1ハッシュ値			必須
KeyUsage	TRUE	オブジェクト識別子(OID)	2.5.29.15			必須
DigitalSignature						
NonRepudation						
KeyEncipherment						
DataEncipherment						
KeyAgreement						
KeyCertSign		BIT STRING	1			必須
CRLSign		BIT STRING	1			必須
EncipherOnly						
Basic Constraints	TRUE	オブジェクト識別子(OID)	2.5.29.19			
CA		BOOLEAN	CA:TRUE PathLenConstraint:NULL			必須

1.12 添付資料-2 （CRLプロファイル）

■CRLプロファイル

項目			設定	データタイプ	説明及び記載情報例	
Version				INTEGER	1 v2	必須
Signature					署名アルゴリズム	
	algorithm			OID	1.2.840.113549.1.1.11 sha256RSA	必須
Issuer						
	CountryName			PrintableString	JP	必須
	StateName			PrintableString	【Option】Tokyo	オプション
	LocalityName			PrintableString	【Option】Minato-Ku	オプション
	OrganizationName			PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code（0147506022） or ISO/IEC8824_OID（1.2.392.200063）	必須
	OrganizationUnitName			PrintableString	Head Quarter	必須
	CommonName			PrintableString	JIPDEC Head Quarter CA1	必須
ThisUpdate				UTCTime	YymmddhhmmssZ 今回の更新日時 例） 2010年1月20日 09:00:00	必須
NextUpdate				UTCTime	YymmddhhmmssZ 次回の更新日時 例） 2010年1月27日 09:00:00	必須

Revoked Certificates					失効される証明書	
	userCertificate			INTEGER	失効される証明書のシリアルナンバー	必須
	revocationDate			UTCTime	失効日時	必須
crlEntry Extensions					失効される証明書毎の拡張領域	
	reasonCode		FALSE		理由コード(コードの説明はIPA:PKI関連技術解説より引用)	
		unspecified		0	未指定	
		keyCompromise		1	鍵漏洩（鍵危殆化）	
		cACompromise		2	CA弱体化（CA危殆化）	オプション
		affiliationChanged		3	所属変更	（ただし 0、6、8
		superseded		4	破棄	は使用しない）
		cessationOfOperation		5	運用停止	
		certificateHold		6	証明書保留	
		removeFromCRL		8	CRLからの削除	
	holdInstructionCode		FALSE		保留指示コード	
		id-holdinstruction-none		1	何もしない	使用しない
		id-holdinstruction-callissuer		2	発行者に連絡する	
		id-holdinstruction-reject		3	証明書を受け付けない	
	invalidityDate		FALSE		推定無効日 GeneralizedTime	使用しない
	certificateIssuer		TRUE		証明書発行者 間接CRL使用時に設定	使用しない

crlExtensions						
	AuthorityKeyIdentifier		FALSE	OCTET String	SHA1ハッシュ値	必須
	issuerAltName		FALSE		CRL発行者の別名	使用しない
	cRLNumber		FALSE	INTEGER	CRLの通し番号（シーケンシャル）	必須
	deltaCrlIndicator		TRUE		デルタCRL使用時に設定	使用しない
	issuingDistributionPoint		TRUE		間接CRL使用時に設定	
		distributionPoint			配布点	
		onlyContainsUserCerts			EE証明書のみ	使用しない
		onlyContainsCACerts			CA証明書のみ	
		onlySomeReasons			特定の失効理由	
		indirectCRL			間接CRL	
	freshestCRL		FALSE		デルタCRL使用時に設定	使用しない

平成 22 年 3 月発行

発行所　財団法人日本情報処理開発協会
東京都港区芝公園３－５－８
機械振興会館３階
TEL：０３（３４３６）７５１３

印刷所　株式会社美行企画
東京都千代田区神田錦町２－５
TEL：０３（３２１９）２９７１