22-H003

電子認証の民間制度・基盤の確立に関する調査研究報告書

平成 23 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す。
http://ringring-keirin.jp/

序文

本報告書は、財団法人日本情報処理開発協会が競輪の補助金を受けて実施した平成２２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・基盤の確立に関する調査研究」の成果を取りまとめたものである。

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、2 年目の平成 22 年度は、一般企業及び団体向けに電子証明書を発行する基盤を構築してプロトタイプ実証を行うとともに､電子証明書の環境要素あるいはアプリケーションである「マルチユース格納媒体」「登録業務」「電子認証応用領域」に関する検討及びプロトタイプ実証を行った。
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「電子認証等の民間制度・基盤の確立に関する委員会」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 23 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自然人である「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。

2 年目の平成 22 年度は、ビジネスにおいては「企業内個人」を対象とした電子証明書が求められていることから、対象を組織に属する個人(学生,被保険者等)に拡大し、次を共通化して一般的な OS やアプリケーション等で利用できる“扱いやすさ” を追求したパブリックな電子証明書である「JCAN ビジネス証明書」を設計しプロトタイプ実証を行って検証するものとする。

- 証明書発行業務
- 証明書プロファイル

(3) 本書の構成

本書において、「基盤のプロトタイプ実証調査」を第 1 章に、「団体向け認証基盤のプロトタイプ実証」を第 2 章に、「マルチユース格納媒体のプロトタイプ実証調査」を第 3 章に、「登録業務のプロトタイプ実証」を第 4 章に、「電子認証応用領域のプロトタイプ実証」を第 5 章に、「JCAN 文書」を第 6 章に、「電子証明書のインストール」を第 7 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 8 章、第 9 章に記載した。

1　基盤のプロトタイプ実証調査

1.1 事業の目的

公開鍵暗号に基づく電子認証・電子署名はネットワーク上において、認証、暗号、改ざんの防止といったセキュリティ面で認知されている。本事業では電子証明書が高価及び登録手続きの煩わしさといった面の軽減を主眼に置き、個人の電子証明書ビジネス活動環境として急速に発展しているインターネット社会における適切な水準の安全性と信頼性が確保された情報環境整備に向け「民間の制度・基盤の中核となる認証局に係る領域」で民間認証局がグローバルに所有する経験・ノウハウを最大限活用することにより、安心・安全で使いやすい社会的環境（「安信簡」情報環境）の実現による情報経済社会変革への貢献を図るものとする。

1.2 調査研究成果の概要

1.2.1 調査の目的

「平成 21 年度情報化推進に関する調査研究等補助事業」（電子認証の民間制度・基盤の確立に関する調査研究）の成果を受けて、プロトタイプ実証として、民間の制度・基盤の中核となる認証局に係る領域における「基盤のプロトタイプ実証調査」を実施する。

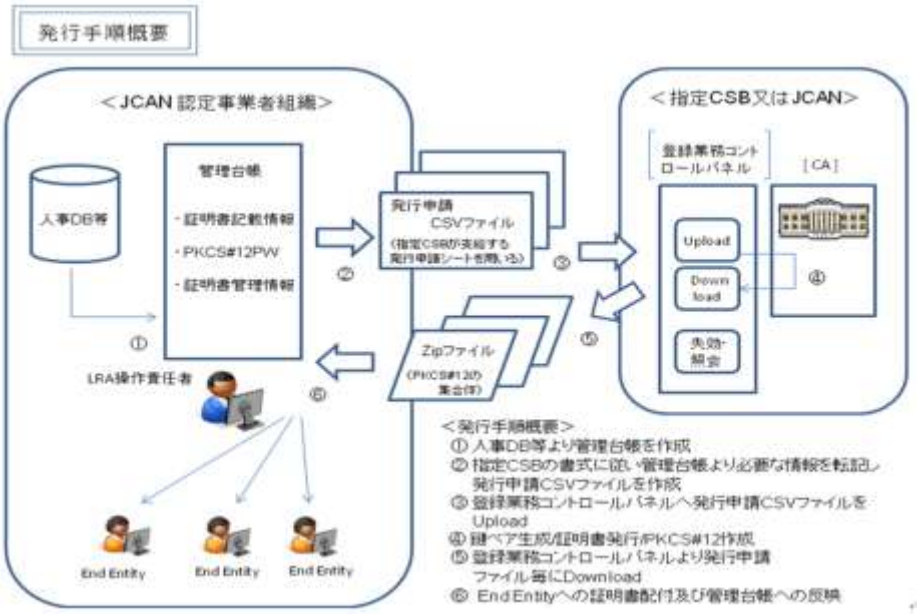
1.2.2 事業の内容

(1) 規程類の作成・整備

下記の規定類を作成又は整備した。

・ JCAN 認証局（一般向けクライアント証明書発行用）についての CP/CPS

・ 利用者の手引き



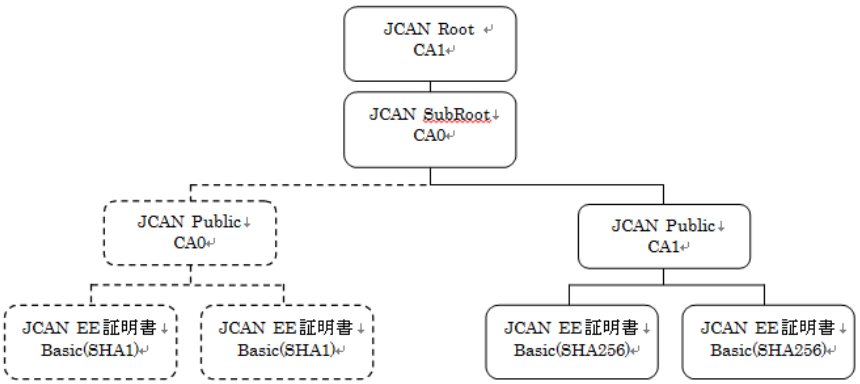
(2) 認証局（3 局）の構築

下記の 3 つの認証局を構築した。

・ JCAN ルート認証局

・ JCAN 認証局（SSL/オペレータ証明書発行用）

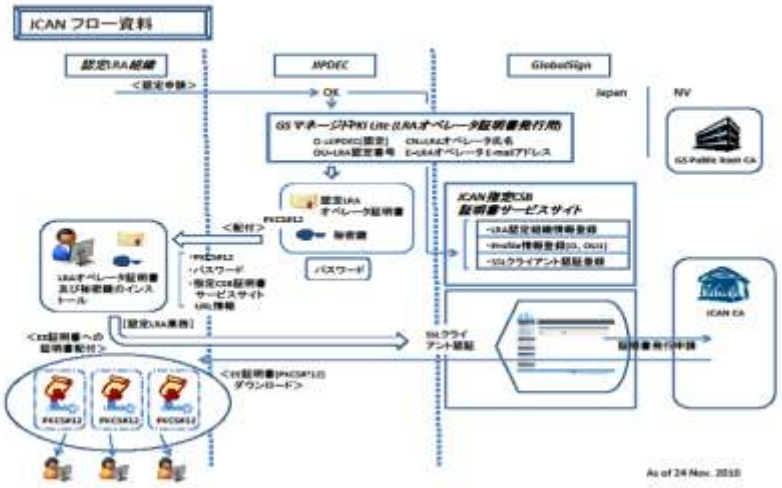
・ JCAN 認証局（クライアント証明書発行用）



(3) 発行システムの開発

上記認証局（3 局）について JIPDEC が指定する証明書プロファイルで証明書を発行する仕組みを構築した。

発行システムの概要



(4) 認証局の保守・障害対応

上記認証局（３局）について実証期間中の運用と保守及び障害対応を行った。

(5) 調査支援

構築した認証局に関する調査作業への支援を行った。

1.3 期待される成果の利用・活用方法

- 証明書プロファイル共通化を軸とする JCAN 構想と、ワールドワイドで通用するルート認証局を活用することにより、新たな市場創出の加速化が期待できる。
- 証明書発行の確認に企業の人事情報等を用いることで、信頼感を保ちつつ発行フローを簡素化することがでる。
- 証明書の申請・取得を一括して行う仕組みにより、エンドユーザ負担が軽減され、且つ社員全員での導入を想定した価格体系によりビジネスシーンでの普及拡大が見込まれる。
- 証明書に社員番号や PS 名といった情報を記載することにより実ビジネスでの利用シーンに即した形での証明書利用推進が期待できる。
- 証明書の具体的な活用シーンとして下記が見込まれる。

(1) クライアント証明書を用いた認証強化(Web サーバー、Web アプリケーション)

- 社員向け、パートナ向け

(2) 電子メールで S/MIME を用いた署名・暗号化、フィッシング対策

- 配信メール、取引先とのやり取り

(3) 電子文書の署名を用いた保存

- 保存文書の改竄検知

(4) 電子署名を用いた業務フロー(稟議書や決算書)

- 電子文書の署名、確認フロー

(5) 模倣品対策

- 模倣品対策の真贋判定とトレースのための模倣品対策システムに係るトレーサビリティのための電子認証

2　団体向け認証基盤のプロトタイプ実証

2.1 事業の目的

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。次の 10 年に向けたビジネス情報環境の変革を、企業のビジネススタイルに合った、発行しやすく使いやすい電子証明書の普及で実現していくことを目的に、電子認証の民間制度・基盤の確立に関する調査研究をスタートした。

2.2 調査研究成果の概要

2.2.1 調査の目的

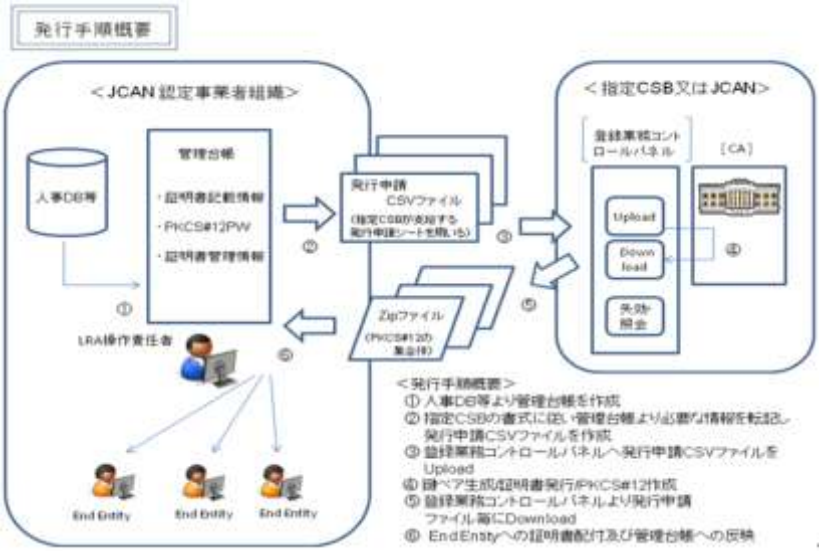
「平成 21 年度情報化推進に関する調査研究等補助事業」（電子認証の民間制度・基盤の確立に関する調査研究）の成果を受けて、プロトタイプ実証として、民間の制度・基盤の中核となる認証局に係る領域における「団体向け認証基盤のプロトタイプ実証」を実施した。

2.2.2　事業の内容

(1) 規程類の作成・整備

下記の規定類を作成又は整備した。

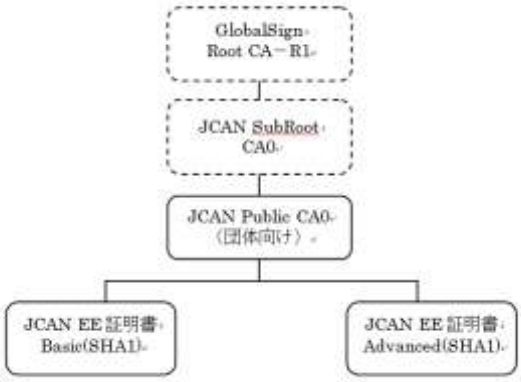
・ JCAN パブリック認証局（団体向け認証基盤）についての CPS



(2) プロトタイプ実証用認証局の構築

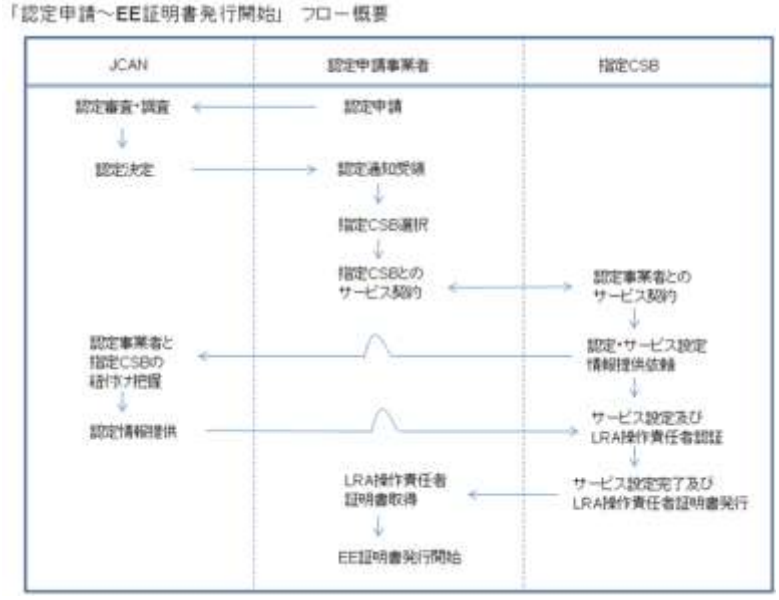
下記の認証局を構築した。

・ JCAN パブリック認証局（団体向け認証基盤）



(3) 発行システムの開発

上記認証局について JCAN が指定する証明書プロファイルで証明書を発行する仕組みを構築した。



(4) 認証局の保守・障害対応

上記認証局（1 局）について実証期間中の運用と保守及び障害対応を行った。

(5) 調査支援

構築した認証局に関する調査作業への支援を行った。

2.3 期待される成果の利用・活用方法

- 証明書プロファイル共通化を軸とするJCAN構想と、ワールドワイドで通用するルート認証局を活用することにより、新たな市場創出の加速化が期待できる。
- 証明書発行の確認に企業の人事情報等を用いることで、信頼感を保ちつつ発行フローを簡素化することがでる。
- 証明書の申請・取得を一括して行う仕組みにより、エンドユーザ負担が軽減され、且つ社員全員での導入を想定した価格体系によりビジネスシーンでの普及拡大が見込まれる。
- 証明書に社員番号やシュードニウム名といった情報を記載することにより実ビジネスでの利用シーンに即した形での証明書利用推進が期待できる。
- 証明書の具体的な活用シーンとして下記が見込まれる。

(1) クライアント証明書を用いた認証強化(Webサーバー、Webアプリケーション)
-社員向け、パートナ向け

(2) 電子メールでS/MIMEを用いた署名・暗号化、フィッシング対策
-配信メール、取引先とのやり取り

(3) 電子文書の署名を用いた保存
-保存文書の改竄検知

(4) 電子署名を用いた業務フロー(稟議書や決算書)
-電子文書の署名、確認フロー

(5) 模倣品対策
-模倣品対策の真贋判定とトレースのための模倣品対策システムに係るトレーサビリティのための電子認証

3　マルチユース格納媒体のプロトタイプ実証調査

3.1 プロトタイプ実証の目的

公開鍵基盤（PKI）は、信頼された電子証明書に基づく厳格な個人認証や、否認防止を確実にする電子署名など、高度なセキュリティを確保するソリューションとして知られている。公開鍵基盤（PKI）の信頼性を確保するために、電子証明書と署名鍵（プライベート鍵）は、本人以外の第三者が利用できないように安全に保管しておく必要がある。

電子証明書の導入の初期段階では、パソコンのハードディスク内の証明書ストアに電子証明書と署名鍵（プライベート鍵）を格納しておくところからスタートする事例が多く見られる。しかし、この方法では署名鍵（プライベート鍵）を利用して電子署名をしているユーザが電子証明書に記載された本人であることを保証できない。

そこで、公開鍵基盤（PKI）の信頼性を確実に担保するために、電子証明書と署名鍵（プライベート鍵）を安全に格納する媒体として IC カードが知られている。IC カードは、権限を持たない第三者に対して IC カード内部に格納された情報を漏えいさせない耐タンパー性を備えた媒体である。従来は、高度な公開鍵計算能力を備えた接触型 IC カードに、電子証明書と署名鍵（プライベート鍵）を格納しておき、IC カード内部で電子署名値を計算し、署名鍵（プライベート鍵）を IC カードの外へ出さないことにより、公開鍵基盤（PKI）の信頼性を確実にするという運用が行なわれてきた。この方法は、高度な信頼性を確保できる反面、公開鍵計算能力を備えた接触型 IC カードを必要とするため、コスト面からは電子証明書の普及を阻害する要因の一つとなっている。

JCAN ビジネス証明書は、JCAN から認定された企業／団体の総務部門等が社員／職員に配付し、自社の職員であることを証明する証明書である。手軽に導入でき、リーズナブルなコストで運用できる方法が求められる。JCAN ビジネス証明書は電子認証にも署名にも利用されることから、証明書を配付された社員／職員本人だけが利用できる仕組みを手軽に構築する必要がある。そこで、パソコンのハードディスク内に電子証明書と署名鍵（プライベート鍵）を格納しておき、なおかつ、その利用時には本人だけが所持する利用者認証用媒体を使うことを検討した。そのため、非接触 IC カードを使った ID 証カード・フォーマットとして広く普及している SSFC カードと FCF カードの双方のフォーマットを JCAN パスとして利用するための検討を行い、プロトタイプ実証用 JCAN パスを試作して実証実験を行なった。

3.2 JCAN パス・システムが備えるべき要件

JCAN パスの利用シーンを想定し、PKI 用途での妥当性、業務効率等の観点から、JCAN パス・システムが備えるべき要件を検討した。

JCAN パス・システムが備えるべき要件	要件の概要
(1) 1 枚の JCAN パスから複数の電子証明書へリンクできる	個人に対して発行される証明書と役職に対して発行される証明書がある。
(2) 電子証明書申請発行管理サーバ（仮称）へのアクセス情報	証明書利用時に電子証明書申請発行管理サーバ（仮称）へのアクセスが想定される。
(3) 取得した電子証明書（EE 証明書）の正当性検証	電子証明書申請発行管理サーバ（仮称）から取得した電子証明書の正当性を検証したいという要求に対応。
(4) ID 情報の読み出し効率が高いこと	個人が保持する現在有効な JCAN パスを特定するために必要な ID 情報項目を一度に読み取れることが望ましい。
(5) 1 枚の JCAN パスを物理的セキュリティ（入退室管理等）と PKI で連携利用できること	JCAN ビジネス証明書による電子署名が、どこで署名されたかを証明できる仕組みにより JCAN パスの付加価値を高める。
(6) 既存で流通し利用されている ID 証カード（SSFC カード、FCF カード）をそのまま JCAN パスとして利用できること	社員等に配付済み ID 証カードを回収して再発行する手間をかけずに、そのまま JCAN パスとして利用できることが望ましい。

3.3 JCAN パス・フォーマットの検討

JCAN パス･システムが備えるべき要件を念頭に、JCAN パス・フォーマットの検討を行った。その際に、SSFC カードと FCF カードの双方を JCAN パスとして利用できるようにするため、「JCAN パス・サービス（仮称）」を FeliCa プライベート領域に搭載する方式を検討した。

これによって、JCAN パス･システムが備えるべき要件(1)(2)(4)(5)を解決し、以下のいずれのケースでも JCAN パスとして発行できることを示した。

- SSFC カードを JCAN パスとして発行するケース
- SSFC カード（共通領域版）を JCAN パスとして発行するケース
- FCF キャンパスカードを JCAN パスとして発行するケース

今年度のプロトタイプ実証では、上記の中から SSFC カードをプロトタイプ実証用 JCAN パスとして発行して試作した。

JCAN パス･システムが備えるべき要件(3)と(6)については、引き続き検討していく JCAN パス用ドライバー・ソフトウェアの要求仕様としてインプットすることとした。

3.4 実証実験

試作したプロトタイプ実証用JCANパスを用いて、以下の3項目について実証実験を実施し、マルチユース格納媒体の有効性を確認した。

- 入退
- ネットワークログイン
- 電子署名

3.4.1 プロトタイプ実証用 JCAN パス

現在ID証カードとして市場で広く使われているSSFCカードをJCANパスとして発行するケースを採用し、プロトタイプ実証用JCANパスを試作した。FeliCaカード(RC-S962)のプライベート領域に「JCANパス・サービス(仮称)」、「SSFC」、「入退出ゲート・サービス」を搭載した。

3.4.2 入退

財団法人日本情報処理開発協会(JIPDEC)オフィスの入退室ゲートにて、プロトタイプ実証用JCANパスに搭載した前記入退室ゲートベンダー固有の「入退出ゲート・サービス」を利用して入退室できることを確認した。

3.4.3 ネットワークログイン

大日本印刷製PCセキュリティソフトウェア「Endpoint Saver F」をテスト機PCに搭載し、プロトタイプ実証用JCANパスをリーダライタ(R/W)にかざし、PCへのログオンに成功した。ログオン後、R/WからプロトタイプJCANパスを離すとスクリーンとキーボードがロックされ、JCANパスをR/Wに戻すと両方ともロック解除された。

3.4.4 電子署名

プロトタイプ実証用JCANパスを使って、JCANビジネス証明書による電子署名機能の実証を行った。プロトタイプ実証用に、JCANパス用ドライバー・ソフトウェアトウェアを設計・開発し、これを利用して電子証明書インストールデモ・アプリと電子署名デモ・アプリにより実証した。プロトタイプ実証用JCANドライバーは、プロトタイプ実証用JCANパスの「JCANパス・サービス(仮称)」と「SSFC サービス」にアクセスするライブラリである。今回開発したプロトタイプ実証用JCANドライバーは、FeliCa用R/Wとして広く普及しているPaSoRi及び、PC/SC仕様に準拠したR/Wをサポートしている。

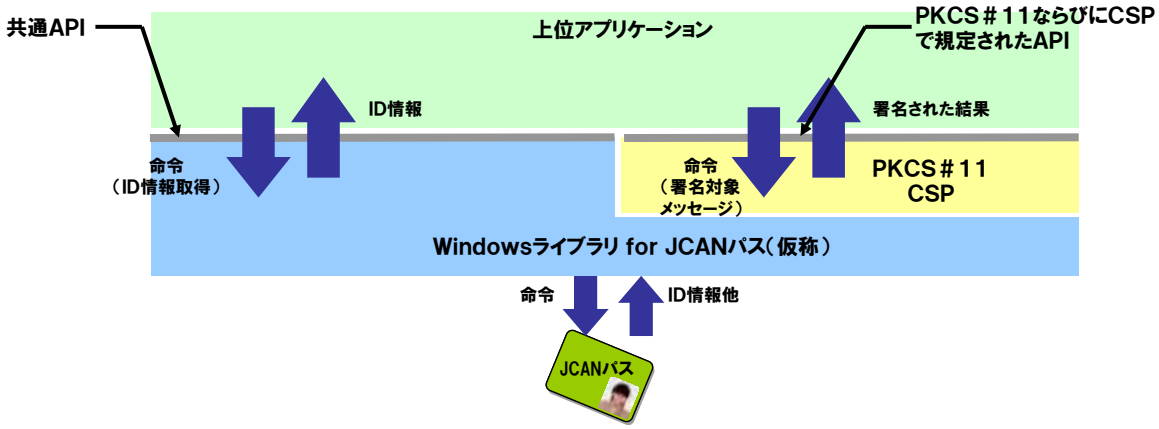
3.5 課題

今年度のプロトタイプ実証を通じて浮き彫りにされた JCAN パス事業化に向けた課題を整理した。

3.5.1 JCAN パス用ドライバー・ソフトウェア ／ PKI 標準 API の提供

電子メールソフトやブラウザが電子証明書格納媒体にアクセスする際に利用される PKI 標準 API (CSP, PKCS#11)を提供する JCAN パス用ドライバー･ソフトウェアが必要と思われるため、その要求機能、構成を検討した。

JCAN パスの媒体として FeliCa カード以外にも TypeA など複数種類の非接触 IC カード媒体に展開していくことが考えられる。このため、複数の非接触 IC カード媒体に対応した PKI ドライバーを効率良く開発するため、以下の 2 階層構造を企画提案した。



3.5.2 JCAN パス用ドライバー・ソフトウェア／既存カードをそのまま利用

既に利用されている SSFC カード、FCF カードをそのまま利用して、仮想化 JCAN パス(サブセット)として利用できるようにするための『仮想 JCAN パス化ドライバ』(仮称)構想を企画した。

4　登録業務のプロトタイプ実証

4.1 事業の概要

4.1.1 事業の背景

日本の労働力人口が減少する一方で、出産・育児・介護などで思うような就業ができず本来発揮できる能力を発揮できていない方も多くなっている。またインターネット社会においても未だ大多数の社会人は都市圏への通勤のためストレスを蓄積すると同時に、交通手段の過密化による CO2 の排出拡大、大都市圏への資源偏重という問題も抱えている。

昨今、既にビジネスにおいて当然にインターネットを活用するようになった。今後はビジネスへの活用を更に発展させ､社会全体の最適化を促すことができる環境が整ってきたと言える。

そこで特に日本全国で約 5500 万人強の給与取得者及び約 380 万件弱の従業員を雇用する事業者の双方にとってより合理的で生産性の高い、安心・安全なビジネスインフラを広く活用できる基盤の構築を目指した。

4.1.2 事業の内容

株式会社スマイルワークスで企画・開発・運用を行っている ClearWorks（財務会計・給与計算・販売管理の SaaS 型統合業務システムサービス）の「給与ワークス」をカスタマイズ・拡張した上で従業員がネットワークまたはインターネットを介して電子認証を通じて、勤怠管理・給与計算などの実務に活用できる基盤の実証を行った。

4.1.3 事業の期待

本事業は次のような点を期待している。

(1) 従業員管理と ID 管理・認証管理の統一による合理化
(2) 従業員の勤怠管理の合理化
(3) 従業員が利用する各種システムなどへの SSO などの実現
(4) （電子証明書を FeliCa などに格納すれば）入退出管理と勤怠管理の統一管理
(5) （更にカスタマイズは必要ですが）給与明細書を安心・安全に個別に PDF 配信
(6) 外部とのコミュニケーションや取引においても従業員認証情報の参照を実現
(7) その他、社会保険や労働保険、源泉取得税などとの連動を実現

4.2 プロトタイプ実証の目的と方法

企業の従業員と雇用する事業者の双方にとってより合理的で生産性の高い、安心・安全なビジネスインフラを広く活用頂ける基盤の構築を目指し、実際の業務システムに登録されている社員情報と JCAN ビジネス証明書申請情報を効率的に管理するシステムのプロトタイプ構築による実証実験を行った。

SaaS 型統合業務システムサービスである「ClearWorks」から、JCAN ビジネス証明書の登録業務で使われる「管理台帳」に必要なデータを生成する環境を試作し、実証する調査研究を

行うため、以下の方法を用いて行った。

- 財務会計・給与計算・販売管理の SaaS 型統合業務システムサービスである「ClearWorks」の機能拡張を行い、従業員マスター情報に JCAN ビジネス証明書の発行申請に必要な情報を格納できる拡張を試作する。

- 拡張された従業員マスター情報の管理画面から、業務管理者が JCAN ビジネス証明書の発行に必要なデータを所定の形式で出力できる機能を試作する。

- 発行された電子証明書を使って「ClearWorks」にログイン認証することができるように ClearWorks の認証機能を試作する。

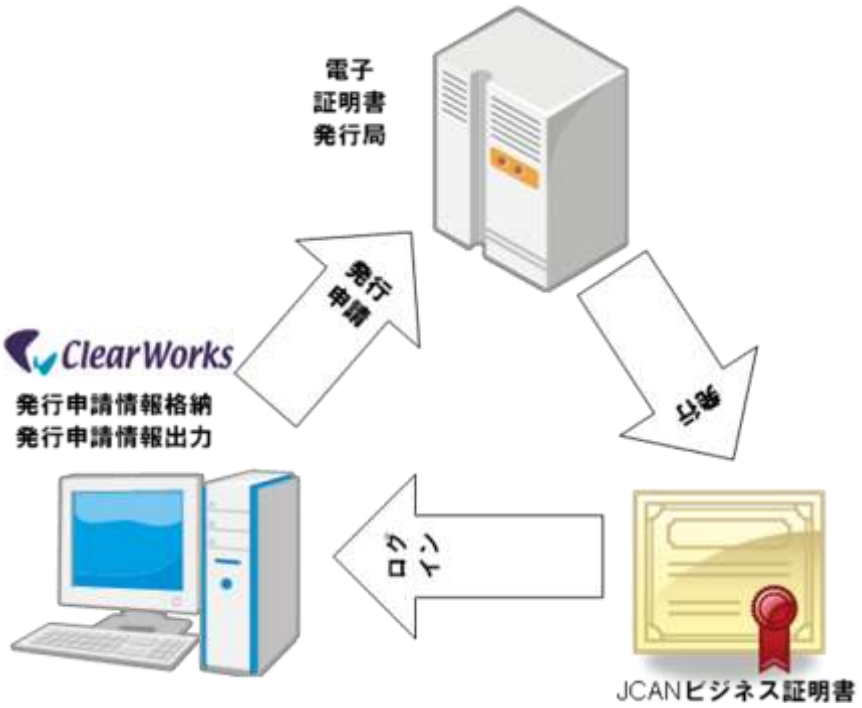


図 4-1　実証イメージ

4.3 JCAN ビジネス証明書発行申請情報保持機能

SaaS 型統合業務システムサービス ClearWorks の社員台帳マスターを拡張し、JCAN ビジネス証明書発行申請に必要な情報を登録、格納する機能を追加する。これにより、既存の社員マスター情報に JCAN ビジネス証明書発行申請情報をリンクさせることで、一元的な管理が可能となる。

4.3.1 社員台帳画面構成

ClearWorks 社員台帳画面に対し、「JCAN 発行申請情報項目」の追加を行った。

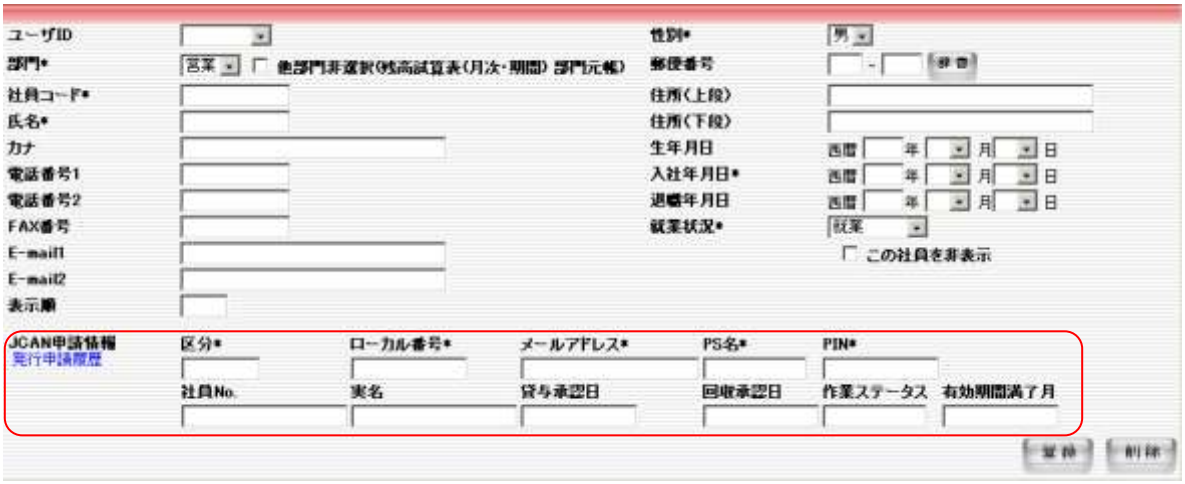


図 4-2 JCAN 申請情報項目

4.4 JCAN ビジネス証明書発行申請出力機能

JCAN ビジネス証明書発行申請情報保持機能により格納された発行申請情報を CSV ファイルとして出力し、自動的に Microsoft EXCEL にて表示する。これにより、管理台帳へのコピー／ペーストを可能にする。

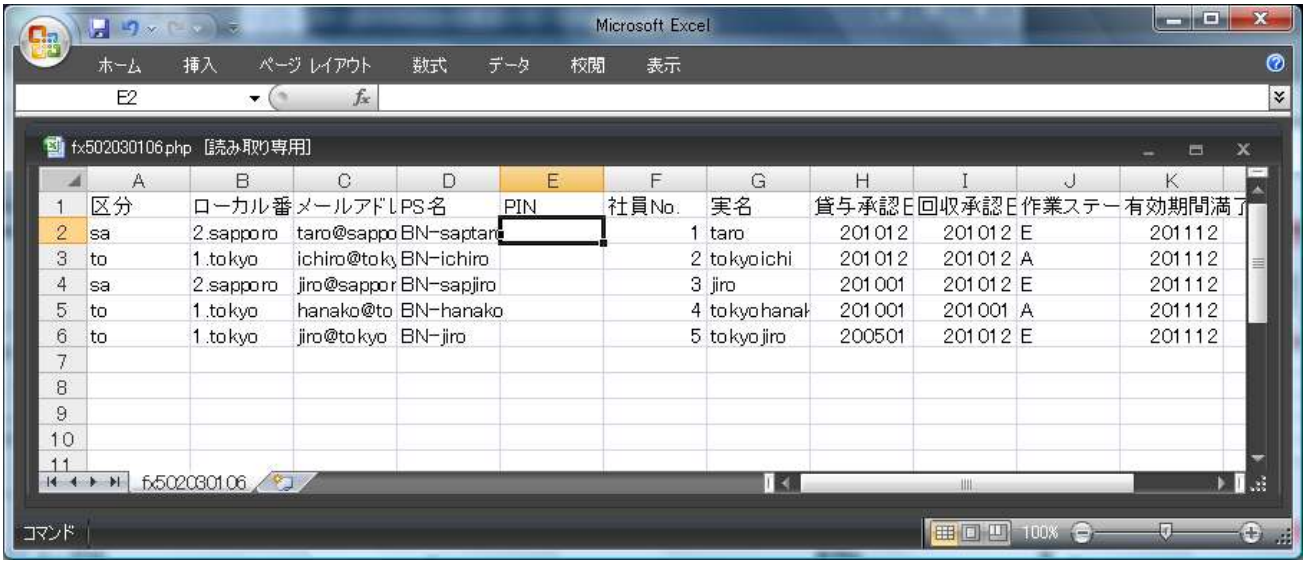
4.4.1 社員台帳画面構成

ClearWorks 社員台帳画面に対し、「発行申請情 CSV」ボタンの追加を行った。

図 4-3 発行申請 CSV ボタン

出力 CSV ファイルの EXCEL による表示

出力した CSV ファイルを、Microsoft EXCEL で表示し、操作を可能にする。



	A	B	C	D	E	F	G	H	I	J	K
1	区分	ローカル番	メールアド	PS名	PIN	社員No.	実名	貸与承認E	回収承認E	作業ステー	有効期間満了
2	sa	2.sapporo	taro@sappo	BN-saptaro		1	taro	201012	201012	E	201112
3	to	1.tokyo	ichiro@toky	BN-ichiro		2	tokyoichi	201012	201012	A	201112
4	sa	2.sapporo	jiro@sappor	BN-sapjiro		3	jiro	201001	201012	E	201112
5	to	1.tokyo	hanako@to	BN-hanako		4	tokyohanak	201001	201001	A	201112
6	to	1.tokyo	jiro@tokyo	BN-jiro		5	tokyojiro	200501	201012	E	201112
7											
8											
9											
10											
11											

図 4-4　発行申請 CSV ボタン

4.5 JCAN ビジネス証明書による認証ログイン

本実証実験でのプロトタイプシステムとしての「ClearWorks」へのログイン時には、通常の ID およびパスワード認証に加え JCAN ビジネス証明書による認証によるログイン機能を実装した。

4.6 実証結果と今後の課題

本プロトタイプシステムにより、EXCEL 上で社員台帳上の JCAN ビジネス証明書発行申請情報を「30-5600」管理台帳へペーストすることで発行申請が可能となり、社員情報と管理台帳情報の効率的な管理を実現することが実証された。

本実証研究において、実運用されている業務システムの社員情報と電子証明書情報を紐づけて管理することが可能であることの実証を行ったが、実運用に向けては以下のような課題について更なる検討を要する。

① 実運用時には、より効率的な発行申請を実現するために、今回の実装方法（B ルート）以外にも直接 CSB にアップロード可能なフォーマット（A ルート）での出力機能の実証

② 発行申請情報をより効率的に登録するための機能強化（OCR 用紙からの入力、電子メールなど電子情報からの自動登録など）の検討

③ 社員などの人事異動情報などと連動して、発行電子証明書の追加・変更・削減・失効・更新等の管理ができる機能の実証

④ 紙印刷コストの削減のために、業務システムが出力する帳票（見積書、請求書などの PDF）へ個人印の印影と合わせて電子証明書の添付機能の実装のための実証。また受発注に際して相手先認証による注文処理、注文請処理、受領確認、などインターネットを介した受発注ステータス管理機能の実証。

⑤ JCAN パス使用者の為の、JCAN パスドライバ対応実装の検討

5　電子認証応用領域のプロトタイプ実証

5.1 事業の目的

半導体　認証、トレーサビリティでは、SEMI 標準化 T20（Structure of Authentication / Verification Capability）に向け、SEMI-J と JEITA の協力のもとで、日本からの提案として Doc4845（CSB：人と組織の認証)、Doc4847（SASB，ASB：物の認証）として、SEMI での標準化を行っている。また、半導体に限らない全業界にまたがる ISO TC247（Fraud countermeasures and Controls ）に対しても、日本からの提案を進めている。

本調査では、日本からの認証、トレーサビリティの提案内容に沿った模倣品対策の真贋判定とトレースのための模倣品対策システムのプロトタイプを実証し、電子認証とトレーサビリティの仕組みを含めた実証・調査を行うことで、今後の本格的なシステム構築と運用に向けた課題から改善へとつなげる。さらに、電子証明書を活用したビジネスシーンにおいての応用領域で、その効果を明らかにすることを目的とする。

5.2 模倣品対策システムの概要

本章では、プロトタイプの基となる TC247 において日本が提案している模倣品対策システムの概要を示す。5.2.1 節で本システムに関連する役割とプレイヤを示し、5.2.2 節で本システムにおいて利用するコード体系を示す。

5.2.1 役割・プレイヤについて

本システムでは、3 種類の役割が存在する。これらの役割は、Doc4845（CSB：人と組織の認証）及び Doc4847（SASB、ASB：物の認証）として日本が提案している内容に則している。また、各役割で想定するプレイヤとその概要を以下に示す。

表 5-1 役割の定義

略称	名称	想定する団体	備考
SASB	Self Authentication Service Body	企業等を想定	
ASB	Authentication Service Body	任意の業界団体を想定	主に B to B に関連する
CSB	Certificate Service Body	認証機関（各国認証）を想定	主に B to C に関連する

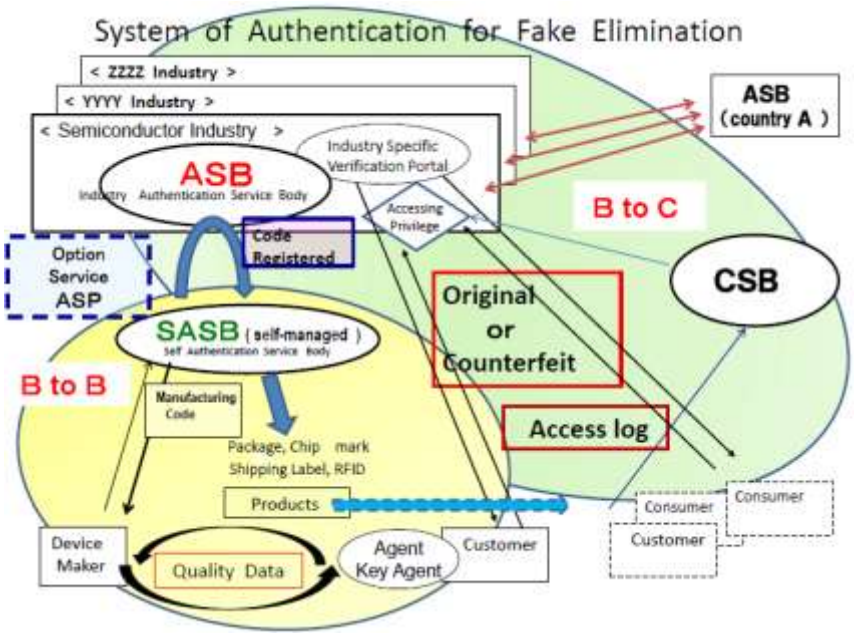


図 5-1 各役割の概要図

5.2.2 コード体系について

本システムでは、2 種類の認証コードが存在する。以下にその概要を示す。

- ライセンスプレート用認証コード(以下 LC)

  LC は、一般的に製品の箱やトレーなどに貼付／印字されることを想定している。

  ex）薬品の箱に貼れている製品識別のラベル

- デバイス認証用コード(以下 DC)

  DC は、一般的にデバイス自体に貼付／印字されることを想定している。

  ex）薬品のカプセル自体に印字されている製品識別情報

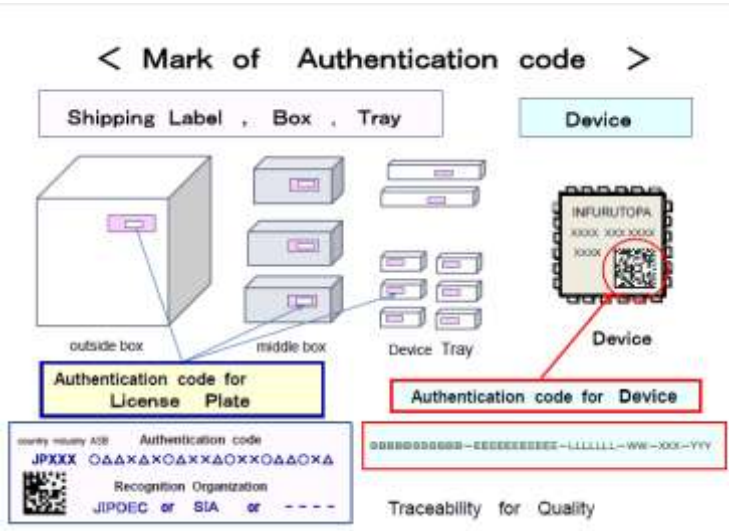


図 5-2 ライセンスプレート、デバイスコード概要

5.2.3 全体像

本システムでは、SASB が各種認証コードや物流のトレース情報を ASB に登録する。SASB や ASB の登録情報及び存在の確かさについては CSB が発行する電子証明書によって確認する。また、顧客は ASB に登録された情報を確認することで、真贋判定やトレースを実施できる。

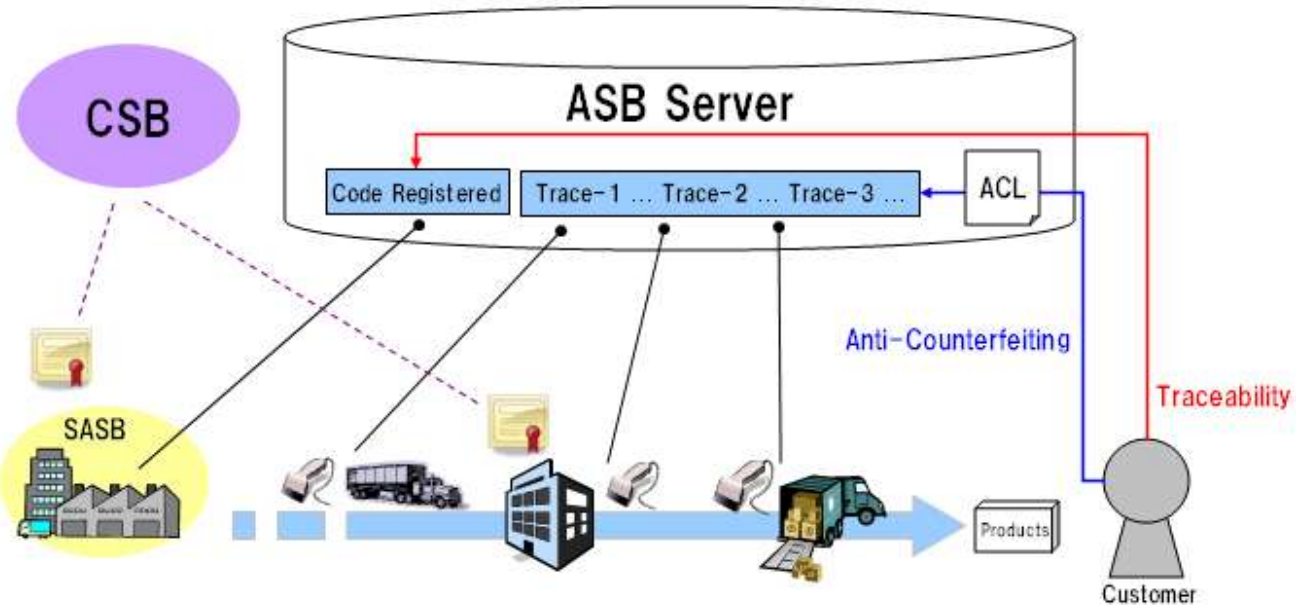


図 5-3 TC247 における日本提案の全体像

上記のシステムによって、ASB がユニーク性(一意性)を確認したコードに対する不正な関連付けの検出が可能である(コードと製品・物の不正な関連付け、コードと製品情報・物情報の不正な関連付け、コードとトレース情報の不正な関連付け等)。また、不正な関連付けを検出した場合は、購入先への問合せや返品等の事後対策によって解決することを想定している。

5.3 プロトタイプ実証結果

5.3.1 プロトタイプ実証の結果概要

想定する関係者に対して、プロトタイプのデモを行い、処理フローや機能を説明し、実用性及び模倣品対策として期待する効果等を確認した。以下にその結果の概要を報告する。

表 5-2 プロトタイプ実証の結果概要

主なヒアリング先	・JEITA の各種委員会 ・ISO PC246/ TC247 の国内審議委員会 ・ISO PC246 ベルリン ・ISO TC247 フランス ・SEMI：Semicon Japan トレーサビリティ委員会 ・JIPDEC 主催の PC246/ TC247 セミナー （2010 年 12 月 1 日開催）

	・その他、説明希望のあった印刷業界、試験関係、認証会社等に対して個別に説明を実施
主なコメント	・認証コードが強制でないことを賛同する。 ・プロトタイプの機能や処理フローは実用に耐える仕様である。 ・コストが問題である。（認証コード発番、システム登録、トレース取得、真贋判定等にかかるコストを抑える必要がある。）

5.3.2 プロトタイプ実証による課題の整理

本節では、電子認証応用領域のプロトタイプ実証の課題について示す。各課題について検討し、プロトタイプの改良や運用上の取り決めによって解決した内容については、課題と共にその解決方法も報告する。

表 5-3 主な課題

課題項目	解決策	
	システム対応	運用対応
(1) トレース情報の管理コスト		○
(2) 物と情報の接合時点での管理ミスの可能性		○
(3) 製品情報登録と管理工数の増大について	○	
(4) ID の使い回しによる SASB の管理ミス		○
(5) SASB の罰則について		○
(6) コードに対する耐性の問題		○
(7) トレース情報の閲覧制御	○	
(8) トレース情報の閲覧の多様性	○	

5.3.3 電子証明書利用の効果について

プロトタイプ実証で確認できた電子証明書利用による効果について報告する。

表 5-4 プロトタイプ実証による効果の確認結果

信頼性･セキュリティに関する効果	・ 電子証明書の組織情報は TTP で識別されているため信頼できる。 ・ 電子証明書を用いたアクセス制御が可能。
システム構築､運用に関する有効性	・ X.509 電子証明書は、OS や一般的なアプリケーションで既にサポートされているため、特別なソフトウェアを必要とせず、システムに利用できる。 ・ 電子証明書により、機械読取が可能であり、管理工数等の削減が期待で

	きる。 ・ X.509 のプロファイルを共通書式にすることで、トレース時のログをコンパクトにすることが可能。 ・ 変更されやすい属性情報を記録しないことで期限満了まで証明書を利用することが可能(変更されやすい属性情報は、CSB のリポジトリで公開する等の運用が考えられる)。
国際相互運用で期待できる効果	・ 以下の要件を適用することで CSB の国際相互運用が可能となり海外製品の真贋判定にも利用可能。 ➢ 各国の法による CA 及び下位 CA の認可 ➢ ISO による CA 及び下位 CA の認定 ➢ ESTI-TS-102042 による CA 及び下位 CA の認定 ➢ Web Trust for CA による CA 及び下位 CA の認定

5.4 成果と期待される利活用について

本調査では、トレーサビリティの提案内容に沿った模倣品対策の真贋判定とトレースのための模倣品対策システムのプロトタイプを実証し、電子認証とトレーサビリティの仕組みを含めた実証・調査を行うことで、今後の本格的なシステム構築と運用に向けた課題整理と改善策の検討を実施した。さらに、電子証明書を活用したビジネスシーンにおいての応用領域で、その効果を示した。

本調査の結果が電子証明書を活用した模倣品対策システムの実現に向けた検討に活用されることを期待する。

6 JCAN 文書

JCAN ビジネス証明書は、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。JCAN ビジネス証明書の運用の詳細については、本報告書の資料 F「認定 LRA 運用マニュアル」またはホームページ（http://www.jipdec.or.jp/repository/）を参照のこと。

表 6-1 JCAN 文書一覧

区分	文書番号	文書名称
共通	30-5300	JCAN ビジネス証明書ポリシ□
	30-5800	教育記録□
	30-5900	内部監査実施記録□
認定 LRA 向け	30-5010	認定 LRA 運用マニュアル
	30-5020	LRA 認定調査申請書
	30-5210	認定 LRA 共通事務取扱要領
	30-5510	認定 LRA 責任者体制表
	30-5600	管理台帳
	30-5700	認定 LRA 作業記録

7 電子証明書のインストール

電子証明書の利用を普及、推進を目的に、OS やメーラーへのインストール、利用方法等を解説したインストールガイドを作成した。インストールガイドの詳細は本報告書の資料 G「電子証明書インストールガイド」またはホームページ（http://www.jipdec.or.jp/repository/）を参照のこと。

8 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・基盤の確立に関する委員会」活動を行った。

(1) 委員会の構成

名称	活動内容
電子認証等の民間制度・基盤の確立に関する委員会	・「登録局の監査・認定」など制度・基盤に関する検討 ・格納媒体(JCAN パス)に関する検討

(2) 委員会実施スケジュール及び内容

日程	時間	場所	内容
2010 年 11 月 9 日(火)	14:00-16:00	JIPDEC 第 1 会議室	・ 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) ・ JCAN プロジェクトの進捗 ➢ 構築の状況 ➢ 文書整備の状況 ➢ プロトタイプ実証の状況 ➢ 公募の進捗状況 ・ JCAN プロジェクトの関連プロジェクトの紹介 ・ 今年度のテーマについて ➢ 「登録局の監査・認定」など制度・基盤に関する検討 ➢ 格納媒体(JCAN)パスに関する検討
2010 年 12 月 21 日(火)	14:00-16:00	JIPDEC 第 1 会議室	・ プロトタイプ実証の状況 ・ SHA256 証明書の試用経過 ・ JCAN パス
2011 年 2 月 8 日(火)	14:00-16:00	JIPDEC 第 1 会議室	・ JCAN ビジネス証明書の実証実験の報告 ・ マルチユース格納媒体のプロトタイプ実証の報告 ・ 登録業務のプロトタイプ実証の報告 ・ 電子認証応用領域のプロトタイプ実証の報告

9 広報活動

(1) 説明会の実施

平成 22 年 11 月 4 日「JCAN ビジネス証明書 説明会」を開催した。

本説明会では、電子証明書の理解を広めるとともに、上記プロトタイプ実験への参加希望者に向けて「JCAN ビジネス電子証明書」の「概要」や「発行の仕方」等について説明をした。

(2) 日時・場所

日　時：平成 22 年 11 月 4 日（木）　開演 13:00 - 17:10

場　所：ベルサール九段　ホール A・B

東京都千代田区九段北 1-8-10 住友不動産九段ビル 3･4F

(3) プログラム

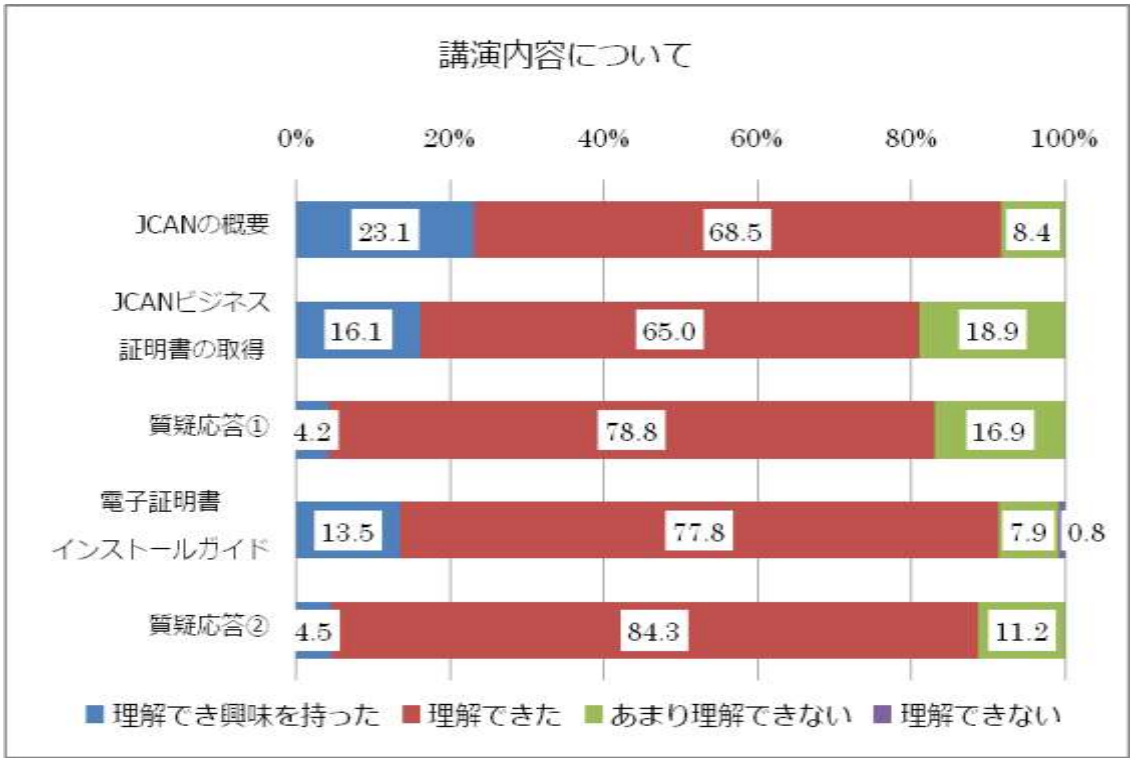
開催挨拶　13:00～13:10	
1	**開催挨拶** 講師：小林 正彦（財団法人日本情報処理開発協会（JIPDEC） 常務理事）
講演 1-1　13:10～13:20	
2	**JCAN の概要** 講師：小林 正彦（財団法人日本情報処理開発協会（JIPDEC） 常務理事）
講演 1-2　13:20～14:30	
3	**JCAN ビジネス証明書の取得** 講師：青木 尚（JIPDEC 電子商取引推進センター 主席研究員）
質疑応答　14:30～14:50	
4	**質疑応答**
休憩(10 分)	
講演 1-3　15:00～16:20	
5	**電子証明書インストールガイド** 講師：御田村 瑞恵（有限会社ビジネスサポートエム 代表取締役）
質疑応答　16:20～17:10	
6	**質疑応答**

(4) 申込者数及び参加者数

申込者：302 名

参加者：207 名（出席率 69%、うち当日参加 2 名）

(5) アンケート結果



回答項目	理解でき 興味を持った	理解できた	あまり 理解できない	理解できない
JCAN の概要	33 (23.1%)	98 (68.5%)	12 (8.4%)	0 (0%)
JCAN ビジネス証明書の取得	23 (16.1%)	93 (65.0%)	27 (18.9%)	0 (0%)
質疑応答①	5 (4.2%)	93 (78.8%)	20 (16.9%)	0 (0%)
電子証明書インストールガイド	17 (13.5%)	98 (77.8%)	10 (7.9%)	1 (0.8%)
質疑応答②	4 (4.5%)	75 (84.3%)	10 (11.2%)	0 (0%)

資料一覧

A「基盤のプロトタイプ実証調査」
B「団体向け認証基盤のプロトタイプ実証」
C「マルチユース格納媒体のプロトタイプ実証調査」
D「登録業務のプロトタイプ実証」
E「電子認証応用領域のプロトタイプ実証」
F「認定 LRA 運用マニュアル」
G「電子証明書インストールガイド」

A　「基盤のプロトタイプ実証調査」

目次

1　背景

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。次の 10 年に向けたビジネス情報環境の変革を、企業のビジネススタイルに合った、発行しやすく使いやすい電子証明書の普及で実現していくことを目的に、電子認証の民間制度・基盤の確立に関する調査研究をスタートした。

2　事業の内容

2.1 調査の目的

「平成 21 年度情報化推進に関する調査研究等補助事業」（電子認証の民間制度・基盤の確立に関する調査研究）の成果を受けて、プロトタイプ実証として、民間の制度・基盤の中核となる認証局に係る領域における「基盤のプロトタイプ実証調査」を実施する。

2.2 事業の内容

(1) 規程類の作成・整備

下記の規定類を作成又は整備した。

- JCAN 認証局（一般クライアント証明書発行用）についての CP/CPS
- 利用者の手引き

(2) 認証局（3 局）の構築

下記の３つの認証局を構築した。

- JCAN ルート認証局
- JCAN 認証局（SSL/オペレータ証明書発行用）
- JCAN 認証局（クライアント証明書発行用）

(3) 発行システムの開発

上記認証局（３局）について JIPDEC が指定する証明書プロファイルで証明書を発行する仕組みを構築した。

(4) 認証局の保守・障害対応

上記認証局（３局）について実証期間中の運用と保守及び障害対応を行った。

3　期待される成果の利用・活用方法

- 証明書プロファイル共通化を軸とする JCAN 構想と、ワールドワイドで通用するルート認証局を活用することにより、新たな市場創出の加速化が期待できる。
- 証明書発行の確認に企業の人事情報等を用いることで、信頼感を保ちつつ発行フローを簡

素化することがでる。

- 証明書の申請・取得を一括して行う仕組みにより、エンドユーザ負担が軽減され、且つ社員全員での導入を想定した価格体系によりビジネスシーンでの普及拡大が見込まれる。
- 証明書に社員番号やシュードニウム名といった情報を記載することにより実ビジネスでの利用シーンに即した形での証明書利用推進が期待できる。

証明書の具体的な活用シーンとして下記が見込まれる。

(1) クライアント証明書を用いた認証強化(Web サーバー、Web アプリケーション)
-社員向け、パートナ向け

(2) 電子メールで S/MIME を用いた署名・暗号化、フィッシング対策
-配信メール、取引先とのやり取り

(3) 電子文書の署名を用いた保存
-保存文書の改竄検知

(4) 電子署名を用いた業務フロー(稟議書や決算書)
-電子文書の署名、確認フロー

(5) 模倣品対策
-模倣品対策の真贋判定とトレースのための模倣品対策システムに係るトレーサビリティのための電子認証

4 規定類の作成・整備

4.1 JCAN ルート認証局の規定類

(1) JCAN ルート認証局の CP

JCAN ルート認証局の証明書ポリシを“JCAN ルート CA 証明書ポリシ“としてまとめた。本文は「7.1 JCAN ルート CA 証明書ポリシ」を参照のこと。

(2) JCAN ルート認証局の CPS

JCAN ルート認証局の認証業務運用規程を、“JCAN ルート CA CPS (認証業務運用規程)”としてまとめた。本文は「7.2 JCAN ルート CA CPS」を参照のこと。

4.2 利用の手引き

LRA 管理者向けに、証明書の発行及び失効手順に関する「利用の手引き」を纏めた。本文は「7.3 利用の手引き」を参照のこと。

5　認証局（3 局）の構築・運用

(1) JCAN ルート認証局の構築

JCAN ルート認証局を下記プロファイルにてキーセレモニーを実施（2010/12/20）、ルート認証局を構築し、パス検証のための片方向相互認証証明書及び CRL を発行した（2011/01/20）。

(2) JCAN 認証局（SSL/オペレータ証明書発行用）の構築

グローバルサインルートの下、JCAN 認証局（SSL/オペレータ証明書発行用）を下記プロファイルにて構築（キーセレモニーの実施、オンライン発行局の設定）後、発行システム（今回開発）と接続した。詳細は「7.4 JCAN の証明書チェーン階層図と証明書プロファイル」を参照のこと

(3) JCAN 認証局（クライアント証明書発行用）の構築

上記 JCAN 認証局に、JCAN 認証局（クライアント証明書発行用）を下記プロファイルにて追加構築し、発行システム（今回開発）と接続した。詳細は「7.5 JCAN 認証局（クライアント証明書発行用）のプロファイル」を参照のこと。

6　発行システムの開発

「基盤のプロトタイプ実証調査」で使用する JCAN ビジネス証明書を、発行、更新、失効するための「発行システム」を開発した。

LRA の管理責任者は、管理台帳に基づき、証明書記載情報及び各証明書インストール用 PKCS#12 パスワード情報を発行申請シートに転記し、発行申請 CSV ファイルを作成、本システムを用いて、当該 CSV ファイルをアップロードして発行申請を完了する。

7　資料一覧

7.1 JCAN ルート CA 証明書ポリシ

文書番号：30-5150

JCAN ルート CA 証明書ポリシ

財団法人日本情報処理開発協会

改訂履歴

版（Ver）	改訂日付	変更内容	担当者	責任者

－ 目 次 －

1　はじめに

JCAN(Japan CA Network)は、財団法人日本情報処理開発協会（所在地：東京都港区芝公園３丁目５番８号、以下「JIPDEC」という）が主体的に運用する民間認証プロジェクトである。

1.1　概要

JCAN ルート CA 証明書ポリシは、JCAN ルート CA 及びサブルート CA（以下「JCAN ルート」という）が発行する CA 証明書の利用目的、適用範囲、及び利用者手続き等、JCAN ルートが発行する CA 証明書に関するポリシを規定するものである。

JCAN ルートの運用に関する諸手続きは、JCAN ルート CA「CPS」に規定する。

JCAN ルート CA 及びサブルート CA は、JIPDEC が運営する認証局である。

1.2　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。

1.2.1　JCAN ルート CA 証明書

JCAN 領域の証明書階層における最上位の証明書（トラストアンカーとも呼ばれる）であり、自己署名される。JCAN ルートからは、パートナ CA 等の発行認証局（Issuing CA）の CA 証明書が発行される。

1.2.2　JCAN サブルート CA 証明書

JCAN ルート CA 直下の中間 CA の CA 証明書である。本中間 CA からは、パートナ CA 等の発行認証局（Issuing CA)の CA 証明書を発行する。

1.2.3　パートナ CA 証明書

パートナ CA 証明書とは,JCAN により認定されたパートナ CA に発行する 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 ルートから発行される
- 指定 CSB の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 CA 証明書の発行に当たっては、本 CP が規定する証明書プロファイルに準拠することが条件となる。

1.2.4　JCAN パブリック CA 証明書

JCAN パブリック CA 証明書とは、1.2.3 に記載のパートナ CA 証明書のうち、JCAN 内部で使用するエンドエンティティ証明書（以下「EE 証明書」という）を発行する JCAN パブリック CA の CA 証明書である。本 CA 証明書は、JCAN ルートから発行される。

1.2.5　相互認証証明書

JCAN ルートから発行する一方向の相互認証証明書である。要請に応じて、指定 CSB の JCAN 用サブルート CA に対して発行する。

1.3　文書名と識別

本 CP の正式名称は、JCAN ルート CA 証明書ポリシである。

本書及び関連するポリシを参照するための識別子は下記のとおりである。

1.2.392.200063.30.5100	JCAN ルート CA CPS
1.2.392.200063.30.5150	JCAN ルート CA 証明書ポリシ
1.2.392.200063.30.5300	JCAN ビジネス証明書ポリシ

1.4 PKI の関係者

1.4.1 JCAN ルート

JCAN 認証サービスの信頼の拠り所となるトップルート認証局である。本認証局は、本 CP 含む証明書ポリシと関連する JCAN のポリシを起草する権限と責任を負う JCAN のポリシ管理局である。

1.4.2 JCAN ルート RA

JCAN ルートの登録局である。パートナ CA 等、CA 証明書を申請する利用者（認証局）の実在性と本人確認の審査を行い、CA 証明書の発行と失効のための登録業務を行う。

1.4.3 認定 LRA

LRA とは、認証局から本人認証を任された機関であり、JCAN が認定する LRA を認定 LRA という。JCAN ビジネス証明書に記載する DN の真正性の審査と利用者の本人認証を行い、JCAN ビジネス証明書の発行と失効の登録業務を行う。

1.4.4 パートナ CA

パートナ CA は、JCAN ビジネス証明書等の EE 証明書を、1.3 に記載の JCAN ビジネス証明書ポリシに準拠して発行する認証局である。EE 証明書の利用者への連絡は、認定 LRA を通じて行う。

1.4.5 JCAN パブリック CA

1.4.3 に記載のパートナ CA のうち、JCAN が運営するパートナ CA を、JCAN パブリック CA という。

1.4.6 指定 CSB (Certificate Service Body)

指定 CSB とは、JCAN が指定する、パートナ CA を運用する事業体である。

1.4.7 利用者

JCAN ルートから発行される CA 証明書の利用者は、CA 証明書の発行をうけるパートナ CA である。

1.4.8 サブジェクト（利用者識別情報）

JCAN ルートから発行される CA 証明書のサブジェクトは、JCAN から CA 証明書の発行を受けるパートナ CA である。

1.4.9 CA 証明書申請者

CA 証明書申請者は、サブジェクトに指名され、サブジェクトの代わりに JCAN ルートの利用者規約に同意する個人である。

1.4.10 検証者

検証者は、前記 1.4.7.利用者の CA 証明書を信頼するもの、又は利用者の電子署名を信頼するものである。

CA 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。

1.5　CA 証明書の用途

1.5.1　適切な証明書の用途

JCAN ルートから発行される CA 証明書は、1.2 に記載される範囲での適切な用途の利用に限る。

1.6　ポリシ管理

JCAN ルートは、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管理局である。JCAN ルートが本 CP を管理する。

2　公開とリポジトリの責任

2.1　リポジトリ

JCAN ルートは、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 ルートは、本 CP を含み、その業務手続及び特定のポリシの内容について、リポジトリに一定の開示を行う。

2.2　証明書情報の公開

JCAN ルートは、次の内容をリポジトリに公開し、CA 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
- CA 証明書
- 最新の CP、CPS
- JCAN ルートが発行する CA 証明書に関するその他の情報

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。

3　識別と認証

JCAN ルートは、CA 証明書の発行の前に、CA 証明書の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。

3.1　名前決定

JCAN ルートは、利用者を本人識別するため、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。

CA 証明書を申請する場合、利用者の名前は、利用者表す正式な名称でなければならない。

3.2　初回の本人確認

3.2.1　組織の認証

(1) JCAN の認証

JCAN は、パートナ CA 及び認定 LRA が設置された組織の認証を行う。当該組織の実在性は、標準企業コード、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）等を用いて、JCAN が、信頼性があると判断する方法によって実施する。

3.2.2　認定 LRA の認定

JCAN は、認定 LRA の申請があった場合、「3.2.1　組織の認証」に記載の方法による組織の認証後、申請組織の資格審査を行う。

資格審査に適合する場合、申請組織を認定 LRA として認定する。

3.2.3　LRA 操作責任者の認証

パートナ CA は、認定 LRA の LRA 操作責任者の証明書の発行に際し、「3.2.1　組織の認証」に記載の方法による組織の認証後、当該申請における利用者の本人確認と権限確認を行う。

3.2.4　利用者の登録の記録

JCAN ルート RA は、組織の認証に使用した本人識別を検証するための全ての情報を記録する。このとき、上記に示した記録を証明書の有効期限が切れた後、少なくとも 7 年間保存する。

3.3　鍵の再生成申請時の利用者の本人確認

3.3.1　通常の鍵更新における本人性確認と認証

鍵更新におけるパートナ CA の本人確認は、「3.2 初回の本人確認」に準拠する。

3.4　失効申請時の本人性確認と認証

パートナ CA 証明書の失効要求における本人識別と認証手続は、管理責任者への本人確認と、管理責任者証明書によるの署名入り失効要求を検証する。

4　証明書のライフサイクルに対する運用上の要件

パートナ CA、認定 LRA は、JCAN ルートが発行した CA 証明書の運用期間中、当該 CA 証明書に記載される情報の全ての変更について、JCAN ルート又は JCAN ルート RA に報告する継続的な義務を負う。

4.1　JCAN パブリック CA 証明書の証明書申請

JCAN パブリック CA 証明書の申請には、JCAN の事前の認定が必要である。JCAN ルートに JCAN パブリック CA 証明書を申請する場合は、申請者は CA 証明書に含むべき登録データを、JCAN ルートに安全な方法で送付する。JCAN ルートは JCAN パブリック CA 証明書を発行する前に、提出された信用証明にもとづいて、申請者の本人識別を検証する。

4.2　CA 証明書の申請手順

JCAN ルート RA は証明書申請を受けて、申請者の本人識別を検証する。

4.3　CA 証明書の発行

CA 証明書申請者の検証後、JCAN ルート RA は CA 証明書の発行登録を行い、パートナ CA 証明書が発行される。

4.3.1　CA 証明書生成

CA 証明書の発行及び更新に関して、JCAN ルート RA は、全ての当事者に対し、以下に規定される条件に従って、CA 証明書を安全に発行する。

- JCAN ルート CA は、JCAN ルート CA 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、適切な手段によって保証される。

4.4　CA 証明書の受領

発行された CA 証明書は、JCAN ルートが発行する CA 証明書の受領を JCAN ルート RA が確認した時点で、利用者により受領されたと見なす。

4.5　鍵ペアと証明書の用途

4.5.1　利用者による秘密鍵、及び CA 証明書の使用

(1) 利用者の義務

利用者の義務は以下の通り。

- 本 CP の諸条件を承諾し、本 CP と利用規約に従って許可された用途にのみ CA 証明書を使用すること
- CA 証明書を合理的な環境下で使用し、不正な操作から防御すること。また CA 証明書が有効でなくなった場合は、使用をやめること。
- CA 証明書の信頼性に重大な影響を及ぼす情報の変更は、JCAN ルート RA に、速やかに知らせること。
- CA 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 CA 証明書の失効を JCAN ルート RA に要求すること
- 秘密鍵を適切に保護し、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

(2) CA 証明書のライフサイクル運用要件

利用者は、CA 証明書の有効期間中における、CA 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があれば、これを直接 JCAN ルート RA に知らせる継続的義務を負う。

(3) 自己責任での信頼

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。

4.5.2　検証者による公開鍵、及び CA 証明書の使用

検証者の義務は以下の通り。

(4) 検証者の義務

CA 証明書の検証者の義務は以下の通り。

- 本 CP で規定したリポジトリで公開する証明書ステータス情報を使用して CA 証明書を検

証し、CA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CA証明書を信頼すること

・ CA証明書を、合理的な環境下でのみ信頼すること

(5) リポジトリとウェブサイトの条件

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、及びリポジトリで公開された他の使用条件を承諾する必要がある。

4.6 CA証明書の更新

JCANルートは、鍵更新を伴わないCA証明書の更新には対応しない。鍵更新を伴うCA証明書の更新は、「3.3 鍵の再生成申請時の利用者の本人確認」による。

4.7 CA証明書の失効

JCANルートRAは、次のような場合にCA証明書を失効する。

・ CA証明書サブジェクトの秘密鍵の紛失、盗難、改ざん、不正開示、その他の危殆化があった場合

・ CA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

・ CA証明書に含まれる、証明書サブジェクトの情報に変更があった場合

・ その他、JCAN ルートRAが必要と認めた場合

4.8 CA証明書のステータス確認サービス

JCANルートは、CRLによりCA証明書ステータスを提供する。

4.9 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。

5 設備上、運営上、運用上の管理

本章では、鍵生成、サブジェクトの認証、CA証明書発行、CA証明書失効、監査、及びアーカイブを実施するためにJCANルートが使用するセキュリティ管理について説明する。

5.1 物理的管理

JCANルートは、認証局の設備の重要性に対応して、人的・物理的なアクセス制御と、電子的なセキュリティメカニズムをもつ高度なセキュリティコントロールを、データセンター内に設置する。データセンターは、水害、地震、火災、その他の災害を容易に受けない構造と防災措置を講じる。

5.2 手続的管理

JCANルートは、要員の信頼性と適性及び技術分野における十分な遂行について、合理的な保証

を提供できる人事を実施する。

5.3　人事的管理

5.3.1　資格、経験及び身分の要件

5.2　手続的管理に記載の信任された役職につく要員は、本認証局の採用基準に基づき採用された従業員とする。

5.3.2　研修要件

JCAN ルートは、認証業務を実行するために、その要員に研修を実施する。

5.3.3　再研修の頻度及び要件

手続についての知識の更新と維持を目的に、定期的な再研修をその要員に実施する。

5.3.4　認められていない行動に対する懲戒

JCAN ルートは、認められていない行動、認められていない権限の使用、認められていないシステムの使用をした要員に対し、適切でないと判断した時は懲戒を行うことがある。

5.3.5　要員に提供する資料

JCAN ルートは、初回の研修とその他の研修の期間、要員に対し資料を提供する。

5.4　監査ログの手続

監査ログの手続には、安全な環境を維持する目的で実装されたイベントログと監査ツールのログを含む。JCAN ルートは、以下の管理を実装する

5.4.1　監査するイベントの種類

JCAN ルートは、以下の記録を監査する。

(1) システム関するログ

- CA 証明書の発行
- CA 証明書の失効
- CRL の公開
- その他（ログイン記録等）

(2) 入退室と秘密鍵の操作に関する記録

- CA を設置する室への入退室記録
- 秘密鍵の操作に関する記録

5.4.2　監査ツールのログに含まれる項目

- 操作の識別
- 操作の日時、時刻
- 操作に含まれる証明書の識別
- 操作を実施した人の識別
- 操作要求に関する参照情報

5.4.3　監査ログを処理する頻度

一定の間隔で、指命された要員がログファイルを点検し、異常事象を検知し、報告できるようにする。

5.4.4　記録の保存と保護、及びバックアップ

JCAN ルートの任命された者、及び指定された監査人による検査のため、ログファイルと監査証跡は保存される。これらは、アクセス制御機構により適切に保護され、バックアップされる。

5.5　記録のアーカイブ

5.5.1　アーカイブされる記録の種類

JCAN ルートは、CA 証明書、CA 証明書の発行・失効の監査データ、CRL、CA 証明書申請情報、ログファイル、及び CA 証明書申請の裏付け資料の記録を、信頼性のある方法で保持する

5.5.2　アーカイブ保存期間

JCAN ルートは、CA 証明書の記録を、有効期限切れ後、又は失効後、最長 7 年間、信頼のある方法で保持する。

5.6　危殆化、及び災害からの復旧

JCAN ルートは、インシデント及び危殆化が発生した場合の報告と取り扱い手続を、内部文書として文書化する。JCAN ルートは、コンピュータ資源、ソフトウェア、又はデータが破損した場合に使用する復旧手続を文書化する。（災害復旧計画）

5.7　認証局又は登録局の終了

認証局としての活動を終了する前に、JCAN ルートは指定された組織に以下の情報を、段階を踏んで譲渡する。

- JCAN ルートに関するすべての情報、データ、文書、リポジトリ
- アーカイブデータ、監査証跡

6　技術的セキュリティ管理

本章では、暗号鍵及び活性化データを保護するために採用するセキュリティ対策を説明する。

6.1　鍵ペアの生成、及びインストール

6.1.1　CA 鍵生成のデバイス

CA の秘密鍵の生成と管理には、秘密鍵を安全に保護する署名暗号装置であるハードウェアセキュリティモジュール（以下「HSM」という）を用いる。

6.1.2　CA 秘密鍵の生成

JCAN ルート及び下位 CA は、文書化された手続に従って CA 秘密鍵を生成する。CA の秘密鍵の生成は、信任された役職 2 名以上の要員による管理を必要とする。この行為は相互牽制を伴い、秘密鍵は、秘密シェアーとして管理され配付される。鍵生成アルゴリズムは RSA SHA-256 を使用する。

6.1.3　CA 秘密鍵の利用方法

CA の秘密鍵は、CA が発行する CA 証明書と証明書失効リストの署名に使用される。その他の利用方法は禁止されている。

6.1.4　CA 秘密鍵のタイプ

ルート CA の秘密鍵は、鍵長 2048 ビットで、RSA アルゴリズムを使用する。その他の CA 秘密鍵は、鍵長 2048 ビットで、RSA アルゴリズムを使用する。

6.2　鍵ペアの再生成と再インストール

JCAN ルートはライフサイクルの終了後、過去に使用された全ての鍵、使用中の耐タンパデバイス、及びバックアップ又はキーエスクローされた秘密鍵の複写を全て破棄する。

6.2.1　CA 鍵生成の管理

6.1.2 に準じる。

6.2.2　CA 秘密鍵の保管

CA の秘密鍵は HSM に保管し、HSM の外では CA の秘密署名鍵は常に暗号化される。

6.2.3　CA 公開鍵の交付

ルート CA 自身の公開鍵配付は、本認証局自身の業務手続に従って実行される。

6.2.4　CA 秘密鍵の破壊方法

CA の秘密鍵は、ライフタイムの最後に、信任された役職 2 名以上の要員の立会いの下に破棄される。鍵の破棄の処理は文書化し、関連する記録は保存する。

6.3　秘密鍵の保護、及び暗号モジュール技術の管理

JCAN ルート及び下位 CA は、FIPS140-1 レベル 3 相当の認定を取得した HSM を使用する。

6.4　活性化データ

JCAN ルートは、自己の秘密鍵と業務に関連する活性化データを安全に保管する。

6.5　コンピュータのセキュリティ管理

JCAN ルートは、必要なコンピュータセキュリティ管理を実装する。

6.6　ライフサイクルの技術上の管理

JCAN ルートは、定期的なセキュリティ管理レビューを実施する。

6.7　ネットワークセキュリティ管理

JCAN ルートと外部のネットワークとは遮断し、秘密鍵を保護する。

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および CRL のプロファイルを規定する。

7.1　証明書プロファイル

JCAN ルートが発行する CA 証明書は、X.509 フォーマット証明書形式により作成される。

フィールド	値、又は値制約
シリアルナンバー	CA が割り当てる一意な番号

署名アルゴリズム	証明書に署名するために使用されたアルゴリズムのオブジェクト識別子
証明書発行者	電子証明書を発行した CA の名前、X.500 識別名(DN)で記述
有効期間開始日	証明書の有効期間開始日
有効期間終了日	証明書の有効期間終了日
サブジェクト DN	電子証明書の所有者の名前
サブジェクト公開鍵	証明書所有者の公開鍵に関する情報

7.1.1 Authority Key Identifier 拡張

JCAN は、エンドユーザ証明書と中間認証局証明書に対し、X.509 バージョン 3 の Authority Key Identifier 拡張を挿入する。証明書発行者が subjectKeyIdntifier 拡張を含む際、Authority 鍵識別子は、証明書を発行する認証局の公開鍵の 160 ビットの SHA-1 ハッシュから構成される。

7.1.2 Authority Information Access 拡張

JCAN は、エンドユーザ証明書、及び適当であれば中間認証局証明書に対し、X.509 バージョン 3 の Authority Information Access 拡張を、検証者が発行認証局証明書を取得できる URL と共に挿入する。

7.1.3 CRL Distribution Points 拡張

JCAN のエンドユーザ証明書と中間認証局証明書は、検証者が認証局証明書のステータスを確認するための CRL を取得できる URL を含む、X.509 バージョン 3 の cRLDistributionPoints 拡張を含む。

7.1.4 Subject Key Identifier 拡張

JCAN が subjectKeyIdentifier 拡張を X.509 バージョン 3 証明書に挿入する場合、証明書のサブジェクトの公開鍵にもとづく keyIdentifier は、160 ビットの SHA-1 ハッシュ値から構成される。

7.1.5 Subject Alternative Name 拡張

JCAN が subjectAlternativeName 拡張を X.509 バージョン 3 証明書に挿入する場合、subjectAlternativeName は、RFC 5280 に記述された方法の 1 つに従って生成される。

7.2 CRL プロファイル。

JCAN ルートが発行する CRL は、X.509 バージョン 2 フォーマットにより形成され、cRLDistributionPoints 拡張を含む。

フィールド	値、又は値制約
バージョン	RFC 5280 に従って、V2
証明書発行者	CRL に署名し発行したエンティティ
発効日	CRL の発行日。CRL は発行次第有効になる。

次回更新	次回の CRL が発行される期限日
署名アルゴリズム	証明書に署名するために使用されたアルゴリズムのオブジェクト識別子－RFC3279 に従って、sha1RSA
Authority Key Identifier	証明書を発行する認証局の公開鍵の 160 ビットの SHA-1 ハッシュ
CRL 番号	RFC 5280 に従って、単調増加のシーケンス番号
今回更新	発行
次回更新	発行日付＋6 か月と数日

7.3

8　準拠性監査とその他の評価

8.1　監査の頻度あるいは条件

JCAN ルートは、年に 1 回以上、本サービスが、CPS 及び CP の要件、標準、手続、及びサービスレベルに適合していることを保証するために、準拠性監査を受諾する。

8.2　監査人の身元・資格

準拠性監査は、十分な監査経験を有する監査人が行うものとする。

8.3　監査人と被監査部門の関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるものとする。

8.4　監査で扱われる事項

監査は、JCAN ルートの運用における CP 及び CPS の準拠性を中心に行われる。

9　他の業務上の問題、及び法的問題

9.1　料金

JCAN ルートから発行される CA 証明書には、適正な料金が課金される。

9.2　財務的責任

JCAN ルートは、本サービスの提供にあたり、十分な財務基盤を維持する。

9.3　業務情報の機密性

JCAN ルートが保持する業務情報は、証明書、CRL、CP 及び CPS の一部として明示的に公表されるものを除き、機密保持対象として取扱われる。

9.4　個人情報のプライバシー保護

JCAN ルートが保持する個人情報は、証明書、CRL、CP 及び CPS の一部として明示的に公表されるものを除き、機密保持対象として取扱われる。

9.5　知的財産権

本 CP 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。

9.6　表明保証

JCAN ルートは、本 CP に規定した内容を遵守して証明書申請に関する審査、証明書の登録、発行、失効を含む認証サービスを提供し、ルート CA 秘密鍵の完全性を含む認証業務の信頼性を確保する。

9.7　無保証

JCAN ルートは、本 CP に規定された保証を除き、一切の保証を行わない。

9.8　責任の制限

JCAN ルートは、認証サービスに関する以下の損害について、利用者、検証者又はその他の第三者に対して、一切の責任を負わないものとする。

- JCAN ルートに起因しない一切の損害
- 利用者又は検証者の義務の履行を怠ったため生じた一切の損害
- 利用者又検証者のシステムに起因する一切の損失
- JCAN ルート及びその他の当事者のハードウェア、ソフトウェアの瑕疵・不具合による損害
- 証明書又は電子署名に関連して発生する、二次的、間接的、遺失利益の一切の損害
- JCAN の責に帰することの出来ない事由で、証明書及び CRL に公開された情報に起因する損害
- 現時点での予想を超えた、暗号アルゴリズム解読技術の向上に起因する損害
- JCAN ルート CA の終了に起因する一切の損害
- 天変地異、その他の自然災害、戦争、動乱、テロ、その他の不可抗力に起因するルート CA サービスの停止に起因する一切の損害

いかなる場合においても、JCAN ルートが負担する賠償責任は、利用者から受け取った金額を上限とする。

9.9　補償

利用者及び検証者は、本 CP に記載の義務または責任の不履行に起因する JCAN ルートが被る損害を補償するものとし、かつこれらに起因するクレーム、異議若しくは訴訟が提起された場合には、自らの費用と責任において当該クレーム、異議及び訴訟等に対応し解決するものとする。

9.10　期間と終了

本 CP は、JCAN ルートのリポジトリ上に効力がなくなったと通知されるまで、効力を持ち続ける。

9.11　関係者間の個別通知と連絡

JCAN ルートは、電子署名されたメールで本 CP に関連する通知を受領する。JCAN から有効

に電子署名された受領確認を受信したことを受けてその連絡が有効であったと見なす。

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 のポリシ管理局が、付与するバージョン番号を決定する。

9.13　紛争解決手続

JCAN ルートのサービスの利用に関し、JCAN ルートに訴訟、仲裁を含む法的、またはその他の解決手段を訴えようとするばあい、JCAN に対し、事前にその旨を通知するものとする。

9.14　準拠法

本 CP の解釈及び、JCAN ルートのサービスに関わる紛争については、日本国の法律が適用され、東京地方裁判所を第一審の専属的合意管轄裁判所とする。

9.15　適用法の遵守

JCAN は、適用可能な日本国の法律を遵守する。

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
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。

キーエスクロー：鍵預託
暗号化したデータの復号鍵を第三者に預けることをいう。

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。

パートナ CA：パートナ認証局
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
デジタル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。

サブルート 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付する責任を負う主体をいう。

法的エンティティ

法人

平成 23 年 2 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 丁目 5 番 8 号
機 械 振 興 会 館 内
ＴＥＬ　03（3432）6597

7.2 JCAN ルート CA CPS

文書番号：30-5100

JCAN ルート CA CPS
（認証業務運用規程）

財団法人日本情報処理開発協会

改訂履歴

版（Ver）	改訂日付	変更内容	担当者	責任者

－ 目 次 －

1　はじめに

JCAN(Japan CA Network)は、財団法人日本情報処理開発協会（所在地：東京都港区芝公園３丁目５番８号、以下「JIPDEC」という）が主体的に運用する民間認証プロジェクトである。

1.1　　概要

JCAN ルート CA CPS は、JCAN ルート CA 及びサブルート CA（以下「JCAN ルート」という）が行う証明書の発行、失効、及び関連する公開鍵基盤（Public Key Infrastructure:以下「PKI」という）の維持運用に係わる諸手続きとポリシを規定する文書である。

JCAN ルートが発行する CA 証明書のポリシは、JCAN ルート CA 証明書ポリシに規定する。

JCAN ルートは、JIPDEC が運営する認証局である。なお、JIPDEC から委託をうけて、GMO グローバルサイン株式会社（所在地：東京都渋谷区桜丘町 20-1）が本認証局を運用する。

1.2　　ルート認証局が取り扱う証明書タイプ

1.2.1　パートナ CA 証明書

パートナ CA 証明書とは,JCAN により認定されたパートナ CA に発行する 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 ルートから発行される

・ 指定 CSB の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 CA 証明書の発行に当たっては、 JCAN ルート CA 証明書ポリシが規定する証明書プロファイルに準拠することが条件となる。

1.2.2　JCAN パブリック CA 証明書

JCAN パブリック CA 証明書とは、1.2.1 に記載のパートナ CA 証明書のうち、JCAN 内部で使用するエンドエンティティ証明書（以下「EE 証明書」という）を発行する JCAN パブリック CA の CA 証明書である。本 CA 証明書は、JCAN ルートから発行される。

1.2.3　相互認証証明書

JCAN ルートから発行する一方向の相互認証証明書である。要請に応じて、指定 CSB の JCAN 用サブルート CA に対して発行する。

1.2.4　テスト用下位 CA 証明書/テスト証明書

JCAN ルートの稼働確認を目的にテスト用下位 CA 証明書を発行する。テスト用下位 CA からは、テスト用の EE 証明書を発行する。テスト証明書には以下の 2 種類がある。

(1) SSL サーバ証明書

(2) クライアント証明書

1.3　　文書名と識別

本 CPS の正式名称は、JCAN ルート CA「CPS」である。

本書及び関連するポリシを参照するための識別子は下記のとおりである。

1.2.392.200063.30.5100	JCAN ルート CA CPS
1.2.392.200063.30.5150	JCAN ルート CA 証明書ポリシ
1.2.392.200063.30.5300	JCAN ビジネス証明書ポリシ

1.4 PKI の関係者

1.4.1 JCAN ルート

JCAN 認証サービスの信頼の拠り所となるトップルート認証局である。本認証局は、本 CPS、及び JCAN ルート CA 証明書ポリシを含む証明書ポリシと関連する JCAN のポリシを起草する権限と責任を負う JCAN のポリシ管理局である。

1.4.2 JCAN ルート RA

JCAN ルート CA の登録局である。パートナ CA 等、CA 証明書を申請する利用者（認証局）の実在性と本人確認の審査を行い、CA 証明書の発行と失効のための登録業務を行う。

1.4.3 認定 LRA

LRA とは、認証局から本人認証を任された機関であり、JCAN が認定する LRA を認定 LRA という。JCAN ビジネス証明書に記載する DN の真正性の審査と利用者の本人認証を行い、JCAN ビジネス証明書の発行と失効の登録業務を行う。

1.4.4 パートナ CA

パートナ CA は、JCAN ビジネス証明書等の EE 証明書を、1.3 に記載の JCAN ビジネス証明書ポリシに準拠して発行する認証局である。EE 証明書の利用者への連絡は、認定 LRA を通じて行う。

1.4.5 JCAN パブリック CA

1.4.3 に記載のパートナ CA のうち、JCAN が運営するパートナ CA を JCAN パブリック CA という。

1.4.6 指定 CSB (Certificate Service Body)

指定 CSB とは、JCAN が指定する、パートナ CA を運用する事業体である。

1.4.7 利用者

JCAN ルート CA から発行される CA 証明書の利用者は、CA 証明書の発行をうけるパートナ CA である。

1.4.8 サブジェクト（利用者識別情報）

JCAN ルート CA から発行される CA 証明書のサブジェクトは、JCAN から CA 証明書の発行を受けるパートナ CA である。

1.4.9　CA 証明書申請者

CA 証明書申請者は、サブジェクト（パートナ CA 又はその他の CA）に指名され、サブジェクトの代わりに JCAN ルート CA の利用者規約に同意する個人である。

1.4.10　検証者

検証者は、前記 1.4.7.利用者の CA 証明書を信頼するもの、又は利用者の電子署名を信頼するものである。

CA 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。

1.5　証明書の用途

JCAN ルート CA「証明書ポリシ」に規定する。

1.6　ポリシ管理

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管理局である。JCAN ルート CA が本 CPS を管理する。

2　公開とリポジトリの責任

2.1　リポジトリ

JCAN ルート CA 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 ルート CA は、本 CPS を含み、その業務手続及び特定のポリシの内容について、リポジトリに一定の開示を行う。

2.2　証明書情報の公開

JCAN ルート CA 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
- CA 証明書
- 最新の CP、CPS
- JCAN ルートが発行する証明書に関するその他の情報

2.3　公開の時期と頻度

CPS 及び CP 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。

3　識別と認証

JCAN ルートは、パートナ CA 証明書の発行の前に、パートナ CA 証明書の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。

3.1　名前決定

JCAN ルートは、利用者を本人識別するため、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。

CA 証明書を申請する場合、利用者の名前は、利用者を表す正式な名称でなければならない。

3.2　初回の本人確認

3.2.1　組織の認証

(1) 認定 LRA の認証

JCAN は、パートナ CA 及び認定 LRA が設置された組織の認証を行う。当該組織の実在性は、標準企業コード、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）等を用いて、JCAN が信頼性があると判断する方法によって実施する。

(2) パートナ CA の認証

JCAN ルートは、パートナ CA 証明書を発行する前に、当該組織を認証する。国や地方公共団体が発行する公的書類、QGIS、QIIS 等を用いて、当該組織の実在性と本人確認を実施する。

3.2.2　認定 LRA の認定

JCAN は、認定 LRA の申請があった場合、「3.2.1　組織の認証」に記載の方法による組織の認証後、申請組織の資格審査を行う。

資格審査に適合する場合、申請組織を認定 LRA として認定する。

3.2.3　LRA 操作責任者の認証（パートナ CA）

パートナ CA は、認定 LRA の LRA 操作責任者の証明書の発行に際し、「3.2.1　組織の認証」に記載の方法による組織の認証後、当該申請における利用者の本人確認と権限確認を行う。

3.2.4　利用者の登録の記録

JCAN ルート RA は、組織の認証に使用した本人識別を検証するための全ての情報を記録する。このとき、上記に示した記録を証明書の有効期限が切れた後、少なくとも 7 年間保存する。

3.3　鍵の再生成申請時の利用者の本人確認

3.3.1　通常の鍵更新における本人性確認と認証

鍵更新におけるパートナ CA の本人確認は、「3.2 初回の本人確認」に準拠する。

3.4　失効申請時の本人性確認と認証

パートナ CA 証明書の失効要求における本人識別と認証手続は、管理責任者への本人確認と、管理責任者証明書によるの署名入り失効要求を検証する。

4　証明書のライフサイクルに対する運用上の要件

パートナCA、認定LRAは、JCANルートが発行したCA証明書の運用期間中、当該CA証明書に記載される情報の全ての変更について、JCANルート又はJCANルートRAに報告する継続的な義務を負う。

4.1　パートナCA証明書の証明書申請

パートナCA証明書の申請には、JCANの事前の認定が必要である。JCANルートにパートナCA証明書を申請する場合は、申請者はCA証明書に含むべき必要な登録データを、JCANルートRAに安全な方法で送付する。JCANルートRAは、提出された信用証明にもとづいて、申請者の本人識別を検証する。

4.2　CA証明書申請手順

JCANルートRAは証明書申請を受けて、申請者の本人識別を検証する。

4.3　CA証明書発行

CA証明書申請者の検証後、JCANルートRAはCA証明書の発行登録を行い、パートナCA証明書が発行される。

4.3.1　CA証明書生成

CA証明書の発行及び更新に関して、JCANルートRAは、全ての当事者に対し、以下に規定される条件に従って、CA証明書を安全に発行する。

- JCANルートCAは、JCANルートCA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、適切な手段によって保証される。

4.4　CA証明書の受領

発行されたCA証明書は、JCANルートが発行するCA証明書の受領をJCANルートRAが確認した時点で、利用者により受領されたと見なす。

発行されたCA証明書の受領に異議を申し立てる場合は、5営業日以内に、JCANルートRAに通知しなければならない。それ以後は、CA証明書は受領されたと見なす。

4.5　鍵ペアと証明書の用途

4.5.1　利用者による秘密鍵、及び証明書の使用

(1) 利用者の義務

利用者の義務は以下の通り。

- 本CPSの諸条件を承諾し、本CPSと利用規約に従って許可された用途にのみCA証明書を使用すること
- CA証明書を合理的な環境下で使用し、不正な操作から防御すること。またCA証明書が有効でなくなった場合は、使用をやめること

・ CA証明書の信頼性に重大な影響を及ぼす情報の変更は、JCANルートRAに、速やかに知らせること
・ CA 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 CA 証明書の失効をJCANルートRAに要求すること
・ 秘密鍵を適切に保護し、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

(2) CA証明書のライフサイクル運用要件

利用者は、CA 証明書の有効期間中における、CA 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があれば、これを直接 JCAN ルートRAに知らせる継続的義務を負う。

(3) 自己責任での信頼

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。

4.5.2 検証者による公開鍵、及びCA証明書の使用

検証者の義務は以下の通りである。

(4) 検証者の義務

CA証明書の検証者は、以下を実施する。

・ 本CPSで規定したリポジトリで公開する証明書ステータス情報を使用してCA証明書を検証し、CA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CA証明書を信頼すること
・ CA 証明書を、合理的な環境下でのみ信頼すること

(5) リポジトリとウェブサイトの条件

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 CPS の条項、及びリポジトリで公開された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。

・ 証明書情報を取得し、証明書のステータスを検証すること、及び対応する電子署名を検証すること
・ 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

4.6 CA証明書の更新

JCANルートは、鍵更新を伴わないCA証明書の更新には対応しない。鍵更新を伴うCA証明書の更新は、「3.3 鍵の再生成申請時の利用者の本人確認」による。

4.7 CA証明書の失効

JCANルートRAは、次のような場合にCA証明書を失効する。

・ CA証明書サブジェクトの秘密鍵の紛失、盗難、改ざん、不正開示、その他の危殆化があった場合

- CA 証明書サブジェクト又はその指名した利用者が、本 CPS の下の重大な義務に違反した場合
- 本 CPS 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
- CA 証明書に含まれる、証明書サブジェクトの情報に変更があった場合

4.8 証明書のステータス確認サービス

JCAN ルートは、CRL により CA 証明書ステータスを提供する。

4.9 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。

5 設備上、運営上、運用上の管理

本章では、鍵生成、サブジェクトの認証、CA 証明書発行、CA 証明書失効、監査、及びアーカイブを実施するために JCAN ルートが使用するセキュリティ管理について説明する。

5.1 物理的管理

JCAN ルートは、認証局の施設に物理的な制御を実践する。サービスプロバイダが提供する施設を利用して認証サービスを提供する場合、認証局は同様の物理的な制御をサービスプロバイダに要求する。

JCAN ルートは、認証局の設備の重要性に対応して、人的・物理的なアクセス制御と電子的なセキュリティメカニズムをもつ高度なセキュリティコントロールを備えるデータセンター内に設置する。データセンターは、水害、地震、火災、その他の災害を容易に受けない構造と防災措置を講じている。

認証局設備へのアクセスは、監査対象であるアクセス制御リストに記載された任命された者に制限し、メディアはセキュアに保管する。

5.2 手続的管理

JCAN ルートは、要員の信頼性と適性及び技術分野における十分な遂行について、合理的な保証を提供できる人事を実施する。

- JCAN ルートは、個人データの機密性と保護について対策を講じる
- JCAN ルートは、信任された役職につく要員の審査を実施する
- JCAN ルートは、実行された行為の全ての実行者について説明責任を追求する
- JCAN ルートは、重要な認証局機能には相互牽制を実装する

5.3 人事的管理

5.3.1 資格、経験及び身分の要件

5.2 手続的管理に記載の信任された役職につく要員は、本認証局の採用基準に基づき採用された従業員とする。

5.3.2　研修要件

JCAN ルートは、認証業務を実行するために、その要員に研修を実施する。

5.3.3　再研修の頻度及び要件

手続についての知識の更新と維持を目的に、定期的な再研修をその要員に実施する。

5.3.4　認められていない行動に対する懲戒

JCAN ルートは、認められていない行動、認められていない権限の使用、認められていないシステムの使用をした要員に対し、適切でないと判断した時は懲戒を行うことがある。

5.3.5　要員に提供する資料

JCAN ルートは、初回研修とその他の研修の期間、要員に対し資料を提供する。

5.4　監査ログの手続

監査ログの手続には、安全な環境を維持する目的で実装された、イベントログと監査ツールのログを含む。JCAN ルートは、以下の管理を実装する

5.4.1　監査するイベントの種類

JCAN ルートは、以下の記録を監査する。

(1) システム関するログ

- CA 証明書の発行
- CA 証明書の失効
- CRL の公開
- その他（ログイン記録等）

(2) 入退室と秘密鍵の操作に関する記録

- 基盤システムを設置する室への入退室記録
- 秘密鍵の操作に関する記録

5.4.2　監査ツールのログに含まれる項目

- 操作の識別
- 操作の日時、時刻
- 操作に含まれる証明書の識別
- 操作を実施した人の識別
- 操作要求に関する参照情報

5.4.3　監査ログを処理する頻度

一定の間隔で、指命された要員がログファイルを点検し、異常事象を検知し、報告出来るようにする。

5.4.4　記録の保存と保護、及びバックアップ

JCAN ルートの任命された者、及び指定された監査人による検査のため、ログファイルと監査証

跡は保存される。これらは、アクセス制御機構により適切に保護され、バックアップされる。

5.5　記録のアーカイブ

5.5.1　アーカイブされる記録の種類

JCAN ルートは、CA 証明書、CA 証明書の発行・失効の監査データ、CRL、CA 証明書申請情報、ログファイル、及び CA 証明書申請の裏付け資料の記録を、信頼性のある方法で保持する。

5.5.2　アーカイブ保存期間

JCAN ルートは、CA 証明書の記録を、有効期限切れ後、又は失効後、最長 7 年間、信頼のある方法で保持する。

5.6　危殆化、及び災害からの復旧

JCAN ルートは、インシデント及び危殆化が発生した場合の報告と取り扱い手続を、内部文書として文書化する。JCAN ルートは、コンピュータ資源、ソフトウェア、又はデータが破損した場合に使用する復旧手続を文書化する。（災害復旧計画）

5.7　認証局の終了

認証局としての活動を終了する前に、JCAN ルートは指定された組織に以下の情報を、段階を踏んで譲渡する。

- JCAN ルートに関するすべての情報、データ、文書、リポジトリ
- アーカイブデータ、監査証跡

6　技術的セキュリティ管理

本章では、暗号鍵及び活性化データを保護するために採用するセキュリティ対策を説明する。

6.1　鍵ペアの生成、及びインストール

6.1.1　CA 鍵生成のデバイス

CA の秘密鍵の生成と管理には、秘密鍵を安全に保護する署名暗号装置であるハードウェアセキュリティモジュール（以下「HSM」という）を用いる。

6.1.2　CA 秘密鍵の生成

JCAN ルート及び下位 CA は、文書化された手続に従って CA 秘密鍵を生成する。CA の秘密鍵の生成は、信任された役職 2 名以上の要員による管理を必要とする。この行為は相互牽制を伴い、秘密鍵は、秘密分散方式で管理される。鍵生成アルゴリズムは RSA SHA-1 又は SHA-256 を使用する。

6.1.3　CA 秘密鍵の利用方法

CA の秘密鍵は、CA が発行する CA 証明書と証明書失効リストの署名に使用される。その他の利用方法は禁止されている。

6.1.4　CA 秘密鍵のタイプ

ルート CA の秘密鍵は、鍵長 2048 ビットで、RSA アルゴリズムを使用する。その他の CA 秘密鍵は、鍵長 2048 ビットで、RSA アルゴリズムを使用する。

6.2　鍵ペアの再生成と再インストール

JCAN ルートはライフサイクルの終了後、過去に使用された全ての鍵、使用中の耐タンパデバイス、及びバックアップ又はキーエスクローされた秘密鍵の複写を全て破棄する。

6.2.1　CA 鍵生成の管理

6.1.2 に準じる。

6.2.2　CA 秘密鍵の保管

CA の秘密鍵は HSM に保管し、HSM の外では CA の秘密署名鍵は常に暗号化される。

6.2.3　CA 公開鍵の交付

ルート CA 自身の公開鍵配付は、本認証局自身の業務手続に従って実行される。

6.2.4　CA 秘密鍵の破壊方法

CA の秘密鍵は、ライフタイムの最後に、信任された役職 2 名以上の要員の立会いの下に破棄される。鍵の破棄の処理は文書化し、関連する記録は保存する。

6.3　秘密鍵の保護、及び暗号モジュール技術の管理

JCAN ルート及び下位 CA は、FIPS140-1 レベル 3 相当の認定を取得した HSM を使用する。

6.4　活性化データ

JCAN ルートは、自己の秘密鍵と業務に関連する活性化データを安全に保管する。

6.5　コンピュータのセキュリティ管理

JCAN ルートは、必要なコンピュータセキュリティ管理を実装する。

6.6　ライフサイクルの技術上の管理

JCAN ルートは、定期的なセキュリティ管理レビューを実施する。

6.7　ネットワークセキュリティ管理

JCAN ルートと外部のネットワークとは遮断し、秘密鍵を保護する。

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、及び CRL のプロファイルを規定する。

7.1　証明書プロファイル

JCAN が運用するルート証明書は、X.509 フォーマット証明書形式により作成される。

フィールド	値、又は値制約

シリアルナンバー	CA が割り当てる一意な番号
署名アルゴリズム	証明書に署名するために使用されたアルゴリズムのオブジェクト識別子
証明書発行者	電子証明書を発行した CA の名前、X.500 識別名(DN)で記述
有効期間開始日	証明書の有効期間開始日
有効期間終了日	証明書の有効期間終了日
サブジェクト DN	電子証明書の所有者の名前
サブジェクト公開鍵	証明書所有者の公開鍵に関する情報

7.1.1 Authority Key Identifier 拡張

JCAN は、エンドユーザ証明書と中間認証局証明書に対し、X.509 バージョン 3 の Authority Key Identifier 拡張を挿入する。証明書発行者が subjectKeyIdntifier 拡張を含む際、Authority 鍵識別子は、証明書を発行する認証局の公開鍵の 160 ビットの SHA-1 ハッシュ値から構成される。

7.1.2 Authority Information Access 拡張

JCAN は、エンドユーザ証明書、及び適当であれば中間認証局証明書に対し、X.509 バージョン 3 の Authority Information Access 拡張を、検証者が発行認証局証明書を取得できる URL と共に挿入する。

7.1.3 CRL Distribution Points 拡張

JCAN のエンドユーザ証明書と中間認証局証明書は、検証者が認証局証明書のステータスを確認するための CRL を取得できる URL を含む、X.509 バージョン 3 の cRLDistributionPoints 拡張を含む。

7.1.4 Subject Key Identifier 拡張

JCAN が subjectKeyIdentifier 拡張を X.509 バージョン 3 証明書に挿入する場合、証明書のサブジェクトの公開鍵にもとづく keyIdentifier は、160 ビットの SHA-1 ハッシュ値から構成される。

7.1.5 Subject Alternative Name 拡張

JCAN が subjectAlternativeName 拡張を X.509 バージョン 3 証明書に挿入する場合、subjectAlternativeName は、RFC 5280 に記述された方法の 1 つに従って生成される。

7.2 CRL プロファイル。

JCAN のルート CA 証明書は検証者及び CA 証明書が証明書のステータスを確認するための CRL を取得できる URL を含む、X.509 バージョン 2 の cRLDistributionPoints 拡張を含む。

フィールド	値、又は値制約
バージョン	RFC 5280 に従って、V2

証明書発行者	CRL に署名し発行したエンティティ
発効日	CRL の発行日。CRL は発行次第有効になる。
次回更新	次回の CRL が発行される期限日
署名アルゴリズム	証明書に署名するために使用されたアルゴリズムのオブジェクト識別子－RFC3279 に従って、sha1RSA
Authority Key Identifier	証明書を発行する認証局の公開鍵の 160 ビットの SHA-1 ハッシュ
CRL 番号	RFC 5280 に従って、単調増加のシーケンス番号
今回更新	発行
次回更新	発行日付＋6 か月と数日

8　準拠性監査とその他の評価

8.1　監査の頻度あるいは条件

JCAN ルートは、年に 1 回以上、本サービスが、CPS 及び CP の要件、標準、手続、及びサービスレベルに適合していることを保証するために、準拠性監査を受諾する。

8.2　監査人の身元・資格

準拠性監査は、十分な監査経験を有する監査人が行うものとする。

8.3　監査人と被監査部門の関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるものとする。

8.4　監査で扱われる事項

監査は、JCAN ルートの運用における CP/CPS の準拠性を中心に行われる。

9　他の業務上の問題、及び法的問題

9.1　料金

JCAN ルートから発行される CA 証明書には、適正な料金が課金される。

9.2　財務的責任

JCAN ルートは、本サービスの提供にあたり、十分な財務基盤を維持する。

9.3　業務情報の機密性

JCAN ルートが保持する業務情報は、証明書、CRL、CP 及び CPS の一部として明示的に公表されるものを除き、機密保持対象として取扱われる。

9.4　個人情報のプライバシー保護

JCAN ルートが保持する個人情報は、証明書、CRL、CP 及び CPS の一部として明示的に公表

されるものを除き、機密保持対象として取扱われる。

9.5　知的財産権

本 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。

9.6　表明保証

JCAN ルートは、本 CPS に規定した内容を遵守して証明書申請に関する審査、証明書の登録、発行、失効を含む認証サービスを提供し、ルート CA 秘密鍵の完全性を含む認証業務の信頼性を確保する。

9.7　無保証

JCAN ルートは、本 CPS に規定された保証を除き、一切の保証を行わない。

9.8　責任の制限

JCAN ルートは、認証サービスに関する以下の損害について、利用者、検証者又はその他の第三者に対して、一切の責任を負わないものとする。

- JCAN ルートに起因しない一切の損害
- 利用者又は検証者の義務の履行を怠ったため生じた一切の損害
- 利用者又は検証者のシステムに起因する一切の損失
- JCAN ルート及びその他の当事者のハードウェア、ソフトウェアの瑕疵・不具合による損害
- 証明書又は電子署名に関連して発生する、二次的、間接的、逸失利益の一切の損害
- JCAN ルートの責に帰することの出来ない事由で、証明書及び CRL に公開された情報に起因する損害
- 現時点での予想を超えた、暗号アルゴリズム解読技術の向上に起因する損害
- JCAN ルート CA の終了に起因する一切の損害
- 天変地異、その他の自然災害、戦争、動乱、テロ、その他の不可抗力に起因するルート CA サービスの停止に起因する一切の損害

いかなる場合においても、JCAN ルートが負担する賠償責任は、利用者から受け取った金額を上限とする。

9.9　補償

利用者及び検証者は、本 CPS に記載の義務または責任の不履行に起因する JCAN ルートが被る損害を補償するものとし、かつこれらに起因するクレーム、異議若しくは訴訟が提起された場合には、自らの費用と責任において当該クレーム、異議及び訴訟等に対応し解決するものとする。

9.10　期間と終了

本 CPS は、JCAN ルートのリポジトリ上に、効力がなくなったと通知されるまで、効力を持ち続ける。

9.11　関係者間の個別通知と連絡

JCAN ルートは、電子署名されたメールで本 CPS に関連する通知を受領する。JCAN から有効に電子署名された受領確認を受信したことを受けてその連絡が有効であったと見なす。

9.12　改訂

本 CPS の変更は、適切に付与する番号を通じて表示する。

JCAN ルートのポリシ管理局が、付与するバージョン番号を決定する。

9.13　紛争解決手続

JCAN ルートのサービスの利用に関し、JCAN ルートに、訴訟、仲裁を含む法的、またはその他の解決手段を訴えようとするばあい、JCAN ルートに対し、事前にその旨を通知するものとする。

9.14　準拠法

本 CPS の解釈及び、JCAN ルートのサービスに関わる紛争については、日本国の法律が適用され、東京地方裁判所を第一審の専属的合意管轄裁判所とする。

9.15　適用法の遵守

JCAN は、適用可能な日本国の法律を遵守する。

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

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。

HSM(Hardware Security Module)：ハードウェアセキュリティモジュール

デジタルキー管理をセキュアに生成、保管し、物理的、論理的な防御を提供するデバイスのことをいう。

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。

SSL（Secure Sockets Layer）：
現在では後継の TLS という名称に変更されたが、一般的には SSL という語句には TLS も含まれる。暗号化、認証、改竄検出の機能を提供する通信のプロトコルをいう。

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。

キーエスクロー：鍵預託
暗号化したデータの復号鍵を第三者に預けることをいう。

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。

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。

パートナ CA：パートナ認証局
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。

バックアップ

複製（コピー）をあらかじめ作成し、たとえ問題が起きてもデータを復旧出来るように備えておくことをいう。

ライフタイム
有効期間をいう。

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
デジタル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。

サブルート 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付する責任を負う主体をいう。

法的エンティティ
法人

平成 23 年 2 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 丁目 5 番 8 号
機 械 振 興 会 館 内
ＴＥＬ　03（3432）6597

7.3 利用の手引き

利用の手引き

（LRA 管理者向け）

（第３編　証明書の発行及び失効手順）

10　発行･失効手順

3　発行･失効手順

3.1　概要

登録業務コントロールパネルは、JCAN ビジネス認定（登録業務）を取得した組織の LRA 操作責任者のみが操作可能な、Web ページより EE 証明書の申請・取得・状況照会・失効等を行うシステムである。

LRA 操作責任者は指定 CSB が提供する LRA 操作責任者証明書を使用することにより指定 CSB が提供する登録業務コントロールパネルへのアクセスが可能となる。LRA 操作責任者端末と登録業務コントロールパネルの間の通信は SSL により暗号化される。

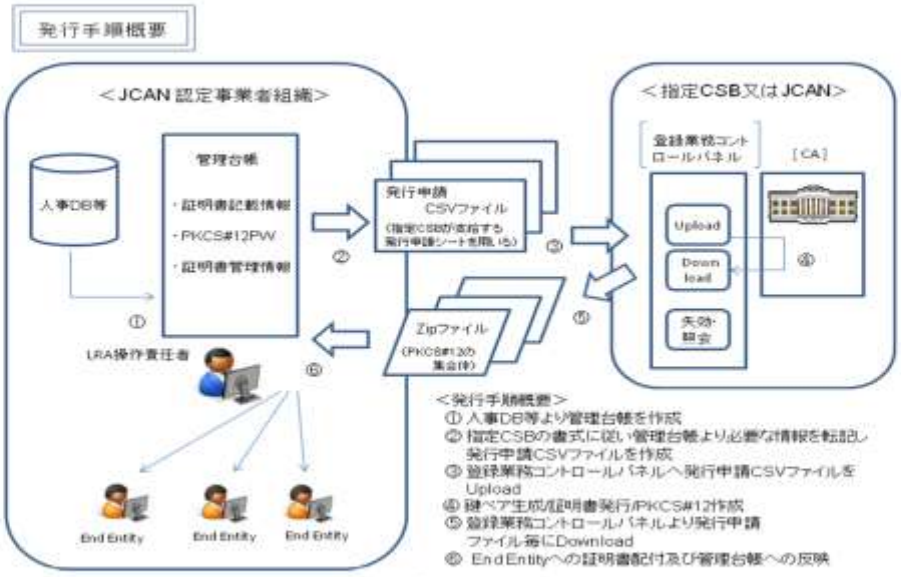
EE 証明書の申請～取得プロセスは下記を基本とする。

(1) LRA 操作責任者は自組織管理台帳に基づき発行申請 CSV ファイルを準備する。

(2) LRA 操作責任者は登録業務コントロールパネルにアクセスし、発行申請 CSV ファイルをアップロードする。発行申請 CSV ファイルには証明書記載情報、証明書インストール用 PKCS#12 パスワード等が記載される。

(3) 証明書が発行された後、LRA 操作責任者は登録業務コントロールパネルへアクセスし証明書を PKCS#12 形式で取得する。

(4) LRA 操作責任者は自組織管理台帳の EE 証明書管理情報を更新したうえ、証明書を配布する。JCAN は、PC ハードディスクやトークン等 EE 証明書の格納媒体及配布型式について規定しない。



3.2 証明書の申請

(1) 発行申請 CSV ファイルの準備

① 指定 CSB が提供する発行申請シートの取得

② 管理台帳に基づく証明書記載情報及び各証明書インストール用 PKCS#12 パスワード情報を発行申請シートに転記し、発行申請 CSV ファイルを作成する。

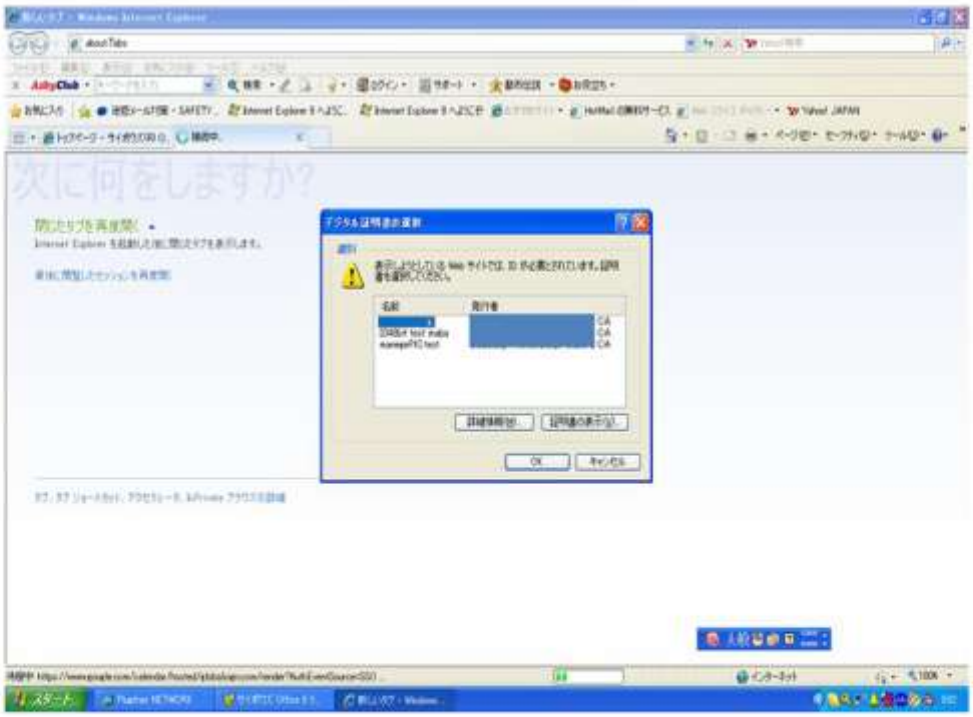
(2) 登録業務コントロールパネルへの発行申請 CSV ファイルアップロード

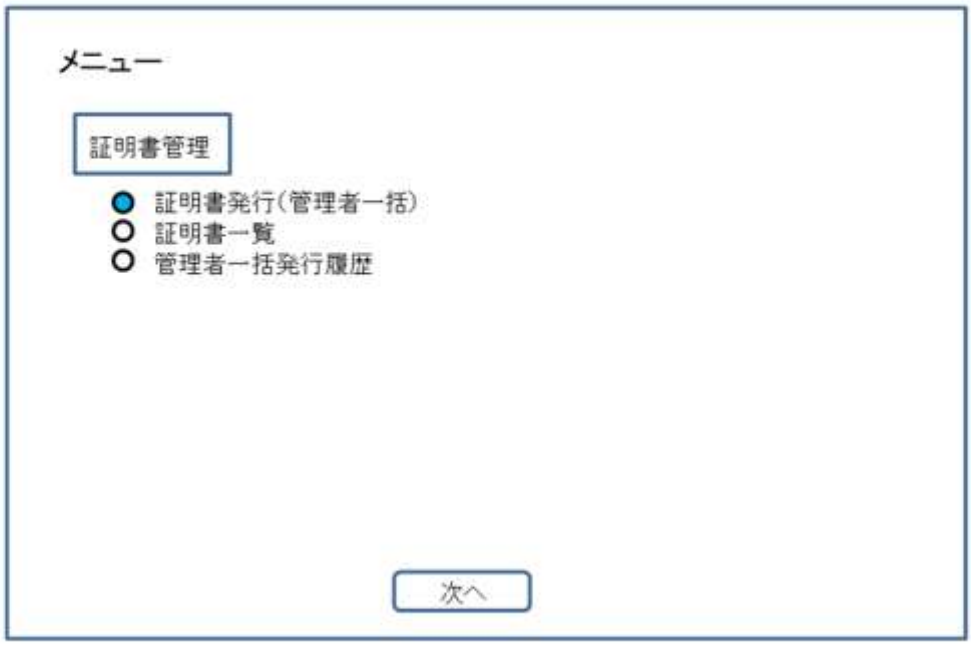
① LRA 操作責任者証明書を使用し登録業務コントロールパネルへアクセスする。

② メニューより証明書管理→証明書発行（管理者一括）を選択する。

③ 申請する証明書タイプ（Advanced, Basic）を選択した後、該当する発行申請 CSV ファイルをアップロードする。１つの発行申請 CSV ファイルでの最大申請件数は 100 件とし、これを超える申請は複数の発行申請 CSV ファイルをアップロードすることで行う。管理台帳に基づく証明書記載情報及び各証明書インストール用 PKCS#12 パスワード情報を発行申請シートに転記し、発行申請 CSV ファイルを作成する。

④ 発行申請 CSV ファイルをアップロードすると、個々の証明書申請に対し申請を特定するための情報が付与される。




メニュー
証明書管理
証明書発行(管理者一括)
証明書一覧
管理者一括発行履歴
次へ


証明書発行申請
プロファイル
Advanced
Basic
有効期間
1年 (証明書発行日から1年)
次へ

3-3


証明書発行申請
発行申請CSVファイル
対象ファイル
参照
アップロード
前へ
次へ


証明書発行申請
EE証明書プロファイルSubject情報共通領域(固定値)説明
項目
説明・例
制限事項
CountryName
国名
JP
ASCII文字2字以下
StateName
都道府県名
Tokyo
ASCII文字32字以下
LocalityName
市区町村名
Minato-ku
ASCII文字32字以下
OrganizationalName
申請事業者英字名
JIPDEC
ASCII文字56字以下
OrganizationalUnitName1
JCAN認定番号
1.2.392.200063.81.12345678
ASCII文字56字以下
OrganizationalUnitName3
LRA窓口URL
www.jipdec.or.jp
ASCII文字56字以下
OrganizationalUnitName4
LRA電話番号
81334329371
ASCII文字56字以下
前へ
次へ

証明書発行申請

確認(例)

OU 2	E-mail address(rfc822)	Common Name	(OU 5)	PKCS#12 password
B05 1.1,.1	○○○○@○○	○○○○○	81334367513	・・・・・・・・・・・・
A01 1.1,.2	△△△△@△△	△△△△△	81334327513	・・・・・・・・・・・・
A01 1.1,.3	××××@××	×××××	81334327513	・・・・・・・・・・・・

EE証明書プロファイル個別領域説明

項目	説明・例	制限事項
OU 2	ローカル管理番号　B05 1.1.1	ASCII文字56字以下
E-mail address(rfc822)	メールアドレス　○○○○@○○	ASCII文字100字以下
Common Name	PS名　○○○○○	ASCII文字56字以下
(OU 5)	EE所属部門電話番号(LRA毎任意)	ASCII文字56字以下
PKCS#12 password	発行申請CSVファイルにのみ記述(証明書には記載されない)	

前へ　次へ

証明書発行申請

完了

PKCS#12一括申請No.	××××××××××××

メニュー画面へ　次へ

3.3 証明書の取得

(1) 登録業務コントロールパネルでの証明書発行完了確認

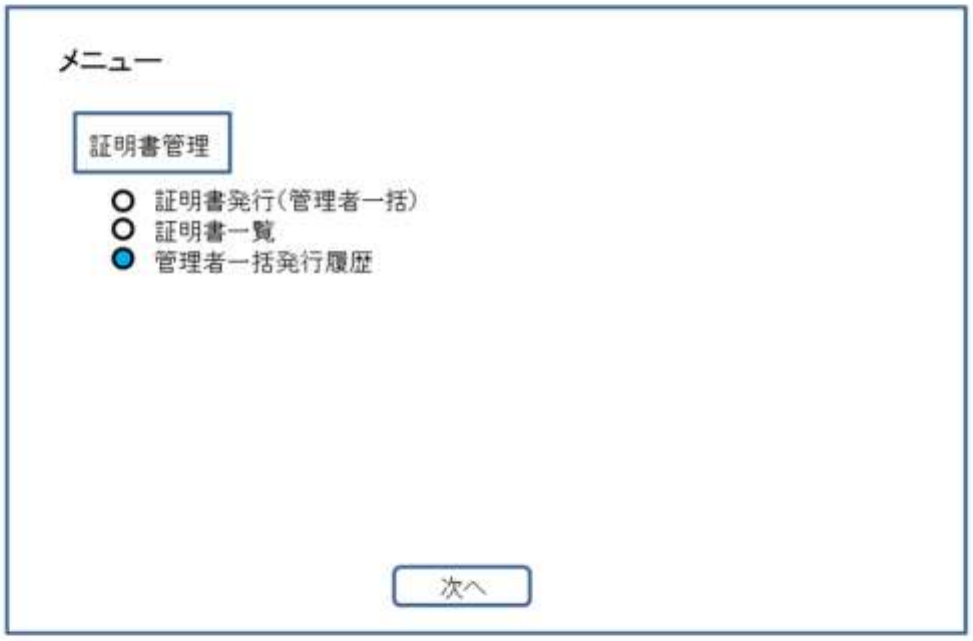
① 証明書発行が完了すると、LRA 操作責任者に通知メールが送られる。

② LRA 操作責任者は登録業務コントロールパネルにアクセスしアップロードした発行申請 CSV ファイル単位での証明書発行処理が完了したことを確認する。

(2) 登録業務コントロールパネルからの証明書（PKCS#12 型式）ダウンロード

① LRA 操作責任者は登録業務コントロールパネルから、発行が完了した証明書（PKCS#12 型式の集合体）ファイルを選択しダウンロードを行う。

② ダウンロードされるファイルは発行申請 CSV ファイル単位での申請件数分の証明書を一括して含む Zip 型式である。



PKCS#12　一覧画面

検索結果

3.4 証明書の配付

(1) 証明書割当状況の管理台帳への反映

① ダウンロードしたZipファイルを解凍する。

② 申請の際付与された個々の証明書申請を特定する情報を紐付情報として、管理台帳への証明書割当状況の反映を行う。

(2) EndEntityへの証明書配付

① LRA操作責任者は個々の証明書（PKCS#12型式）とPKCS#12パスワードを安全な方法で確実に当該EndEntityに配付する。

② JCANは、PCハードディスクやトークン等EE証明書の格納媒体及び配付型式について規定しない。

③ リカバリー目的で証明書をPKCS#12型式で保管する際には秘密鍵が危殆化しない様十分に配慮すること。

3.5 証明書情報の照会

(1) 検索・レポート表示

① LRA操作責任者は、登録業務コントロールパネルを通じて自組織証明書状況を照会することができる。

② 検索項目例

- 申請日
- 発行日
- 証明書有効期限
- CommonName
- E-mailアドレス
- 証明書ステイタス
- 証明書申請特定情報
- 証明書タイプ
- LRA操作責任者

3.6 証明書の失効

(1) 登録業務コントロールパネルからの失効申請

① EE 証明書の失効が必要となった場合、LRA 操作責任者は登録業務コントロールパネルを通じて当該証明書の失効申請を行う。

② メニューより証明書管理→証明書一覧を選択する。

③ 該当する証明書を検索・抽出し失効する。該当する証明書を検索・抽出し失効する。

④ 失効するに至った理由等と共に管理台帳に履歴を残す。

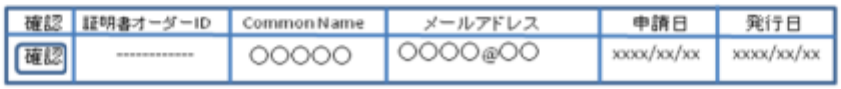
(2) CRL 及び証明書情報への反映

① CRL の更新は、指定 CSB が定める間隔で行われる。

② 証明書情報へも失効のステイタスが反映される。

証明書 一覧画面

検索結果



3-10

証明書詳細確認・失効申請

証明書情報

項目	記載情報
ローカル管理番号	----------
メールアドレス	----------
CommonName	----------
EE所属部門電話番号	----------
国名	----------
都道府県名	----------
申請事業者英文名	----------
JCAN認定番号	----------
LRA窓口URL	----------
LRA電話番号	----------

失効

証明書失効

失効完了

検索結果

3-11

3.7 指定CSBオプション(指定CSBのポリシーに基づき機能実装及び運用を行う事項)

(1) 証明書の再発行

① 再発行の定義と留意事項

- PCのクラッシュによりEndEntityの所有する秘密鍵が回復不能となった場合等に、従前と同じ証明書及び秘密鍵をリカバリー目的で提供することを再発行と定義する。
- 再発行を行う際はEndEntityに対し秘密鍵の取扱いについて再度喚起する等して秘密鍵の危殆化防止に留意する。

② 自組織に発行済証明書(PKCS#12)情報を保管している場合

- LRA操作責任者は、保管している情報から当該EE証明書(PKCS#12型式)とPKCS#12パスワードを安全な方法で確実に当該EndEntityに配付する。
- 再発行に至った理由等と共に管理台帳に履歴を残す。

③ 自組織に発行済証明書(PKCS#12)情報を保管していない場合

- LRA操作責任者は、当該EndEntity証明書を失効し、新規に証明書発行を行う。
- 再発行に至った理由等と共に管理台帳に履歴を残す。

(2) 証明書の更新

① 更新の定義

- EE証明書の有効期間が一ヶ月未満になった時点から有効期限までの間に、従前のSubject情報を変更すること無く当該EEに対し証明書を新規に発行することを更新と定義する。

② 更新についての対応

- 新規発行と同様の手続きにて証明書発行申請を行うことを基本とする。

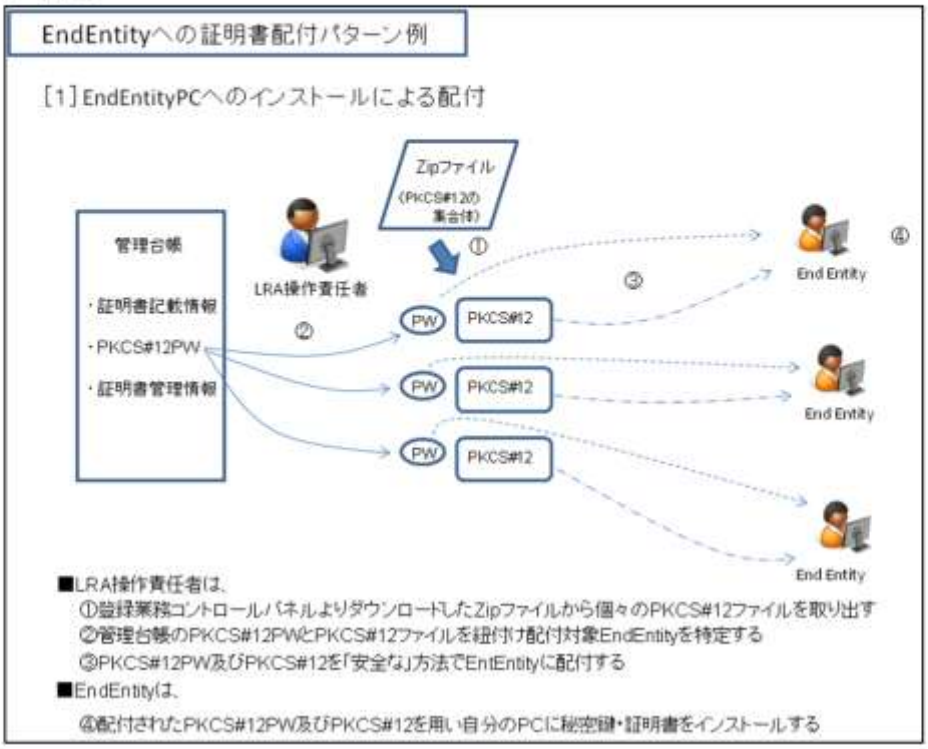
③ 新旧証明書の世代交代に際して考慮が必要と思われる事項

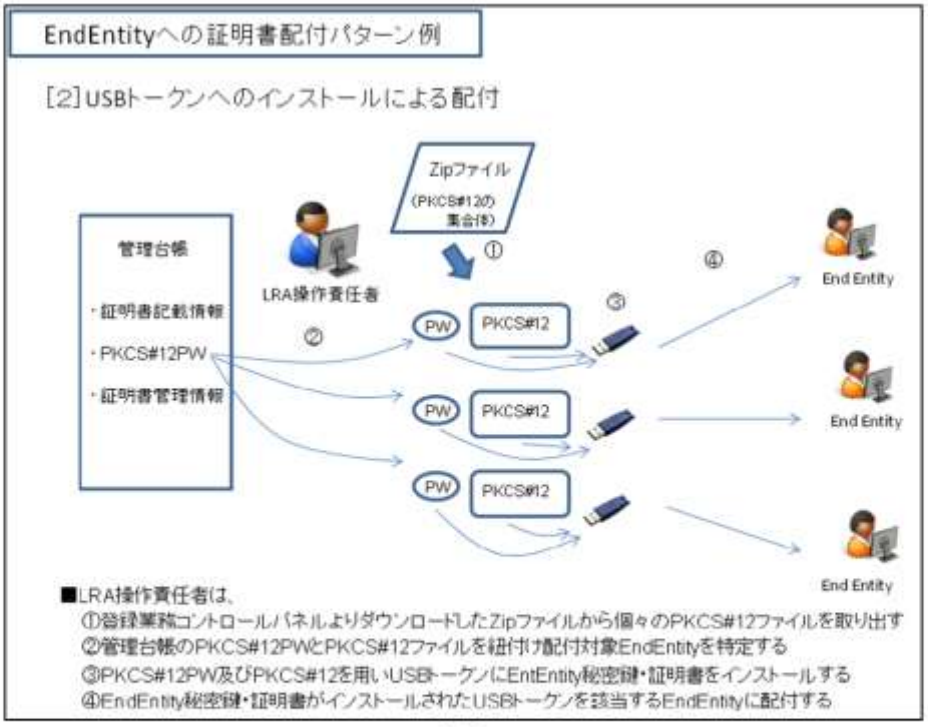
- 新世代証明書を発行後即時に当該EEへ配付するのが困難な状況も考えられるため、新世代証明書発行と同時での旧世代証明書失効を必須とはしないが、EEに対し新世代証明書の配付を受けて以降は旧世代証明書の使用を停止させることが望ましい。
- 特に、証明書を利用するアプリケーションが、証明書の世代交代により引き継がれない情報(シリアルNo.、鍵情報等)をキーとして処理し、当該証明書が一定期間有効であることが必須である場合には残存有効期間を考慮した証明書利用が必要となる。

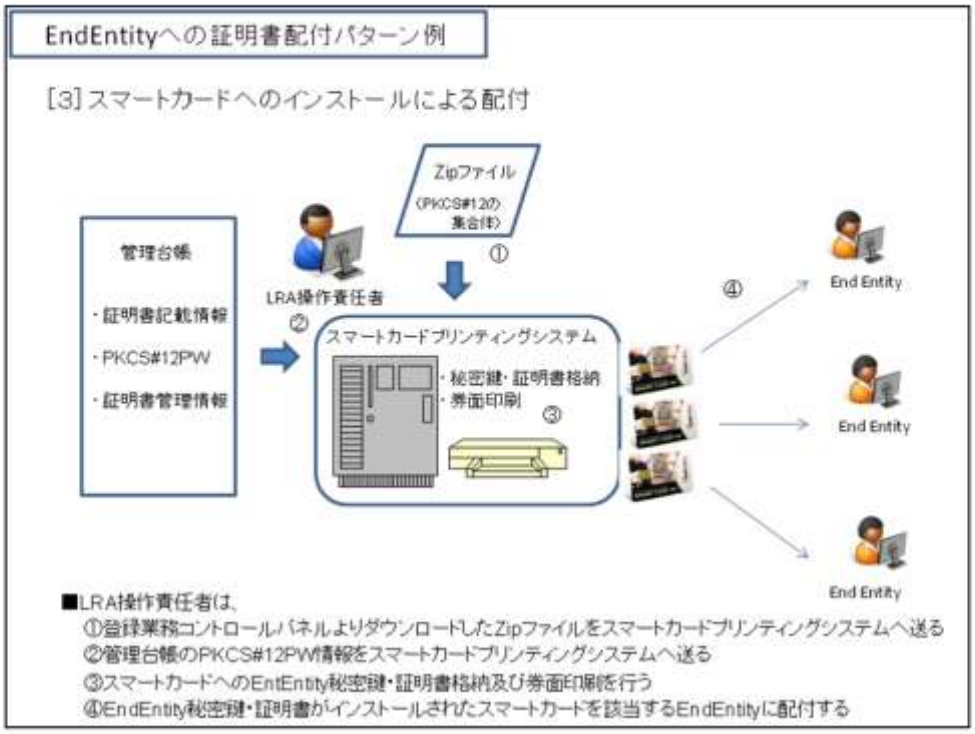
(3) Zipファイル(PKCS#12の集合体)の取扱い

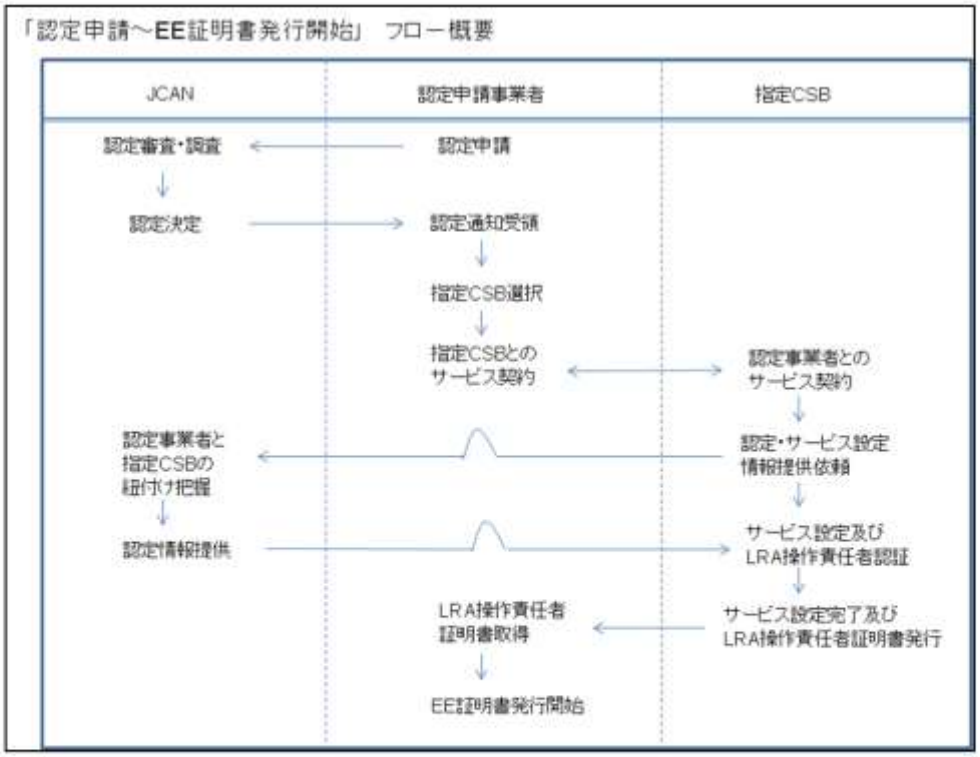
- EE証明書が発行され登録業務コントロールパネルからダウンロード可能になったZipファイル(PKCS#12の集合体)をLRA操作責任者がダウンロードするまでに許容する保持期間、同一ファイルの複数回ダウンロード可否、ダウンロード後の情報保管・廃棄等についての機能実装/運用ポリシーを指す。

［ 別紙：補足 ］


EndEntityへの証明書配付パターン例
[1]EndEntityPCへのインストールによる配付
Zipファイル
(PKCS#12の集合体)
①
管理台帳
・証明書記載情報
・PKCS#12PW
・証明書管理情報
LRA操作責任者
②
PW
PKCS#12
③
④
End Entity
■LRA操作責任者は、
①登録業務コントロールパネルよりダウンロードしたZipファイルから個々のPKCS#12ファイルを取り出す
②管理台帳のPKCS#12PWとPKCS#12ファイルを紐付け配付対象EndEntityを特定する
③PKCS#12PW及びPKCS#12を「安全な」方法でEntEntityに配付する
■EndEntityは、
④配付されたPKCS#12PW及びPKCS#12を用い自分のPCに秘密鍵・証明書をインストールする

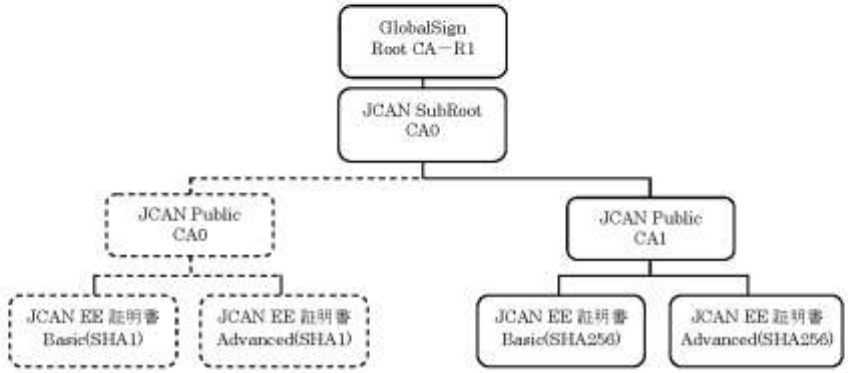

EndEntityへの証明書配付パターン例
[2]USBトークンへのインストールによる配付
Zipファイル
(PKCS#12の集合体)
①
管理台帳
・証明書記載情報
・PKCS#12PW
・証明書管理情報
LRA操作責任者
②
PW
PKCS#12
③
④
End Entity
■LRA操作責任者は、
①登録業務コントロールパネルよりダウンロードしたZipファイルから個々のPKCS#12ファイルを取り出す
②管理台帳のPKCS#12PWとPKCS#12ファイルを紐付け配付対象EndEntityを特定する
③PKCS#12PW及びPKCS#12を用いUSBトークンにEntEntity秘密鍵・証明書をインストールする
④EndEntity秘密鍵・証明書がインストールされたUSBトークンを該当するEndEntityに配付する


EndEntityへの証明書配付パターン例
[3] スマートカードへのインストールによる配付
Zipファイル
(PKCS#12の集合体)
①
管理台帳
・証明書記載情報
・PKCS#12PW
・証明書管理情報
LRA操作責任者
②
スマートカードプリンティングシステム
・秘密鍵・証明書格納
・券面印刷
③
④
End Entity
End Entity
End Entity
■LRA操作責任者は、
①登録業務コントロールパネルよりダウンロードしたZipファイルをスマートカードプリンティングシステムへ送る
②管理台帳のPKCS#12PW情報をスマートカードプリンティングシステムへ送る
③スマートカードへのEntEntity秘密鍵・証明書格納及び券面印刷を行う
④EndEntity秘密鍵・証明書がインストールされたスマートカードを該当するEndEntityに配付する


「認定申請～EE証明書発行開始」 フロー概要
JCAN
認定申請事業者
指定CSB
認定審査・調査
認定申請
認定決定
認定通知受領
指定CSB選択
指定CSBとの
サービス契約
認定事業者との
サービス契約
認定事業者と
指定CSBの
紐付け把握
認定・サービス設定
情報提供依頼
認定情報提供
サービス設定及び
LRA操作責任者認証
LRA操作責任者
証明書取得
サービス設定完了及び
LRA操作責任者証明書発行
EE証明書発行開始

7.4 JCAN の証明書チェーン階層図と証明書プロファイル

JCAN の証明書チェーン階層図



JCAN SubRoot CA0 Certificate

■Certificate Profile (Basic Certific

項目 Certificate Fields		Setting	Data type	Explanation	
				Value	Description
Version			INTEGER	2	V3
SerialNumber			INTEGER	<nnnn>	Unique No. allocated by CA
Signature			AlgorithmIdentifier	1.2.840.113549.1.1.5	SHA-1with RSA Encryption
Validity			Validity	<n>	Validity Period of Certificate
	NotBefore		UTCTime	YymmddhhmmssZ	YymmddhhmmssZ(YMDHMSZ)
	NotAfter		UTCTime	YymmddhhmmssZ	YymmddhhmmssZ(YMDHMSZ)
Issuer			Name		Name of Issuing Authority which issued this Cert
	CountryName		PrintableString	BE	Country Code (2-letter code)
	OrganizationName		Object Identifier (OID)	2.5.4.10	
			PrintableString	GlobalSign nv-sa	
	OrganizationUnitName		Object Identifier (OID)	2.5.4.11	
			PrintableString	Root_CA	
	CommonName		Object Identifier (OID)	2.5.4.3	
			PrintableString	GlobalSign Root CA	
Subject			Name		Name of the holder of the certificate
	CountryName		PrintableString	JP	JP
	OrganizationName		Object Identifier (OID)	2.5.4.10	
			PrintableString	JIPDEC	
	OrganizationUnitName		Object Identifier (OID)	2.5.4.11	
			PrintableString	JCAN Sub Root CA0	
	CommonName		Object Identifier (OID)	2.5.4.3	
			PrintableString	JCAN Sub Root CA0	
SubjectPublicKeyInfo			SubjectPublicKeyInfo	<CHAR>	Certificate Subject's Public Key Information
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1	Public Key Algorithm: rsaEncryption
	SubjectPublicKey		BIT STRING	<nnnn>	2048bit Public Key

■Certificate Profile (Standard Certificate Extensions)

Items			Setting criticality	Data Type	Explanation	
					Value	Description
authorityKeyIdentifier			FALSE	Object Identifier (OID)	2.5.29.35	
				OCTET STRING		SHA-1 Value according to RFC5280 4.2.1.2
subjectKeyIdentifier			FALSE	Object Identifier (OID)	2.5.29.14	
				OCTET STRING		SHA-1 Value according to RFC5280 4.2.1.2
KeyUsage			TRUE	Object Identifier (OID)	2.5.29.15	
	KeyCertSign			BIT STRING	1	
	CRLSign			BIT STRING	1	
Basic Constraints			TRUE	Object Identifier (OID)	2.5.29.19	
	CA			BOOLEAN	TRUE	
	PathLenConstraint			INTEGER	1	
cRLDistributionPoints			FALSE	Object Identifier (OID)	2.5.29.31	
	distributionPoint					CA Access information
	FullName					
		uniformResourceIdentifier		IA5String	http://crl.globalsign.net/root.crl	to Publish URL of the Certificate of CA that issued this certificate

JCAN Public CA 1 証明書プロファイル

JCAN_PublicCA1 Certificate

■Certificate Profile (Basic Certificate Fields)

項目 Certificate Fields			Setting	Data Type	Explanation	
					Value	Description
Version				INTEGER	2	V3
SerialNumber				INTEGER	<integer>	Unique No. allocated by CA
Signature				AlgorithmIdentifier	1.2.840.113549.1.1.11	SHA-256withRSAEncryption
Validity				Validity	<n>	Validity Period (10 years?) Considering CA Hierarchy
	NotBefore			UTCTime	YymmddhhmmssZ	YymmddhhmmssZ [YMDHMSZ]
	NotAfter			UTCTime	YymmddhhmmssZ	YymmddhhmmssZ [YMDHMSZ]
Issuer				Name	<CHAR>	Name of Issuing Authority which issued this Cert
	CountryName			PrintableString	JP	Country Code (2-letter code)
	OrganizationName			Object Identifier (OID)	2.5.4.10	
				PrintableString	JPDEBI	
	OrganizationUnitName			Object Identifier (OID)	2.5.4.11	
				PrintableString	JCAN Sub Root CA2	
	CommonName			Object Identifier (OID)	2.5.4.3	
				PrintableString	JCAN Sub Root CA2	
Subject				Name		Name of the holder of the certificate
	CountryName			PrintableString	JP	Country Code (2-letter code)
	OrganizationName			Object Identifier (OID)	2.5.4.10	
				PrintableString	JPDEBI	
	OrganizationUnitName			Object Identifier (OID)	2.5.4.11	
				PrintableString	JCAN Public CA1	
	CommonName			Object Identifier (OID)	2.5.4.3	
				PrintableString	JCAN Public CA1	
SubjectPublicKeyInfo				SubjectPublicKeyInfo	<CHAR>	Certificate Subscriber (Subject) ' s Public Key Information
	Algorithm			AlgorithmIdentifier	1.2.840.113549.1.1.1	Public Key Algorithm: rsaEncryption
	SubjectPublicKey			BIT STRING	<n>n>	2048bit Public Key

Items			Setting	Data Type	Explanation	
					Value	Description
authority Key Identifier			FALSE	Object Identifier (OID)	2.5.29.35	CA Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
subjectKeyIdentifier			FALSE	Object Identifier (OID)	2.5.29.14	Subscriber Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
KeyUsage			TRUE	Object Identifier (OID)	2.5.29.15	Purpose of Public Key contained in the Cert
	KeyCertSign			BIT STRING	1	for the purpose of Verifying electronic signature
	CRLSign			BIT STRING	1	for the purpose of enciphering the key of common key to distributing key
certificatePolicies			FALSE	Object Identifier (OID)	2.5.29.32	Certificate Policy
	policyIdentifier					
		certPolicyId		Object Identifier (OID)	1.2.392.200093.30.5300	OID of Certificate Policy
	policyQualifiers					
		policyQualifierID		Object Identifier (OID)	1.3.6.1.5.5.7.2.1(id-at-cps)	
		qualifier		IA5String	http://www.jpki.co.jp/repository/	Repository's URL where certificate policy and the like are published
		policyQualifierID		Object Identifier (OID)	1.3.6.1.5.5.7.2.2(id-at-unotice)	
		qualifier		Visible String	JCAN Business DP	Name of certificate Policy
Basic Constraints			TRUE	Object Identifier (OID)	2.5.29.19	2.5.29.19
	CA			BOOLEAN	TRUE	
	PathlenConstraint			INTEGER	0	
cRLDistributionPoints			FALSE	Object Identifier (OID)	2.5.29.31	Information to obtain certificate revocation list (CRL)
	distributionPoint					
		FullName				
		uniformResourceIdentifier		IA5String	http://crl.jpki.go.jp/jcapublic/ca1.crl	to set up a URL http:// **********
authorityInfoAccess			FALSE	Object Identifier (OID)	1.3.6.1.5.5.7.1.1	CA Access Information
	AccessMethod			Object Identifier (OID)	1.3.6.1.5.5.48.2	
	AccessLocation UniformResourceIdentifier			IA5String	http://www.jpki.go.jp/cert/jcapublic/ca1.der http://www.jpki.go.jp/cert/jcapublic/ca1.crt	to Publish URL of the Certificate of CA that issued this certificate

7.5 JCAN 認証局（クライアント証明書発行用）のプロファイル

JCAN Public CA 証明書のプロファイル

JCAN_PublicCA0 certificate

■Certificate Profile (Basic Certificate Fields)

項目 Certificate Fields		Setting	Data type	Explanation	
				Value	Description
Version			INTEGER	2	V2: due to taking V3
SerialNumber			INTEGER	(xxxxxx)	Unique No. allocated by CA
Signature			AlgorithmIdentifier	1.2.840.113549.1.1.5	SHA-1withRSAEncryption
Validity			Validity	<n>	Validity Period (10 years?) Considering CA lifetime?
	NotBefore		UTCTime	YymmddhhmmssZ	YymmddhhmmssZ (YMDHMSZ)
	NotAfter		UTCTime	YymmddhhmmssZ	YymmddhhmmssZ (YMDHMSZ)
Issuer			Name	(CHAR)	Name of Issuing Authority which issued this Cert.
	CountryName		PrintableString	JP	Country Code (2-letter code)
	OrganizationName		Object Identifier (OID)	2.5.4.10	
			PrintableString	JIPDEC	
	OrganizationUnitName		Object Identifier (OID)	2.5.4.11	
			PrintableString	JCAN Sub Root CA0	
	CommonName		Object Identifier (OID)	2.5.4.3	
			PrintableString	JCAN Sub Root CA0	
Subject			Name		Name of the holder of the certificate
	CountryName		PrintableString	JP	Country Code (2-letter code)
	OrganizationName		Object Identifier (OID)	2.5.4.10	
			PrintableString	JIPDEC	
	OrganizationUnitName		Object Identifier (OID)	2.5.4.11	
			PrintableString	JCAN Public CA0	
	CommonName		Object Identifier (OID)	2.5.4.3	
			PrintableString	JCAN Public CA0	
SubjectPublicKeyInfo			SubjectPublicKeyInfo	(CHAR)	Certificate Subscriber (Subject) 's Public Key Information
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1	Public Key Algorithm: rsaEncryption
	SubjectPublicKey		BIT STRING	(xxxxx)	2048bit Public Key

■Certificate Profile (Basic Certificate Fields)

Name				Setting	Data Type	Explanation	
						Value	Description
authority Key Identifier				FALSE	Object Identifier (OID)	2.5.29.35	CA Key Identifier
					OCTET STRING	(CHAR)	SHA-1 Value according to RFC5280 4.2.1.2
subjectKeyIdentifier				FALSE	Object Identifier (OID)	2.5.29.14	Subscriber Key Identifier
					OCTET STRING	(CHAR)	SHA-1 Value according to RFC5280 4.2.1.2
KeyUsage				TRUE	Object Identifier (OID)	2.5.29.15	Purpose of Public Key contained in the Cert
	keyCertSign				BIT STRING	1	for the purpose of 'verifying electronic signature
	CRLSign				BIT STRING	1	for the purpose of encrypting the key of common key to distributing key
certificatePolicies				FALSE	Object Identifier (OID)	2.5.29.32	Certificate Policy
	policyIdentifier						
		certPolicyId			Object Identifier (OID)	1.2.392.200091.201.5000	OID of Certificate Policy
	policyQualifiers						
		policyQualifierID			Object Identifier (OID)	1.3.6.1.5.5.7.2.1(id-qt-cps)	
		qualifier			IA5String	http://www.jipdec.or.jp/repository/	Repository's URL where certificate policy and the like are published
		policyQualifierID			Object Identifier (OID)	1.3.6.1.5.5.7.2.2(id-qt-unotice)	
		qualifier			VisibleString	JCAN Business CP	Name of certificate Policy
Basic Constraints				TRUE	Object Identifier (OID)	2.5.29.19	2.5.29.19
	CA				BOOLEAN	TRUE	
	PathLenConstraint				INTEGER	0	
cRLDistributionPoints				FALSE	Object Identifier (OID)	2.5.29.31	Information to obtain certificate revocation list (CRL)
	distributionPoint						
		FullName					
			uniformResourceIdentifier		IA5String	http://crl.jcanbetaca.net/jcansubrootca0.crl	to set up a URL http:// **********
authorityInfoAccess				FALSE	Object Identifier (OID)	1.3.6.1.5.5.7.1.1	CA Access Information
	AccessMethod				Object Identifier (OID)	1.3.6.1.5.5.48.2	
	AccessLocation UniformResourceIdentifier				IA5String	http://secure.jcanbetaca.net/cgi-crt/jcansubrootca0.crt	to Publish URL of the Certificate of CA that issued the certificate http:// *****

クライアント証明書（Basic）のプロファイル

EE Certificate Profile（1/2）

JDAN (Basic)

項目 Certificate Fields		Define	Data Type	Explanation	
				Value	Description
Version			INTEGER	2	"2" as it is V3
SerialNumber			INTEGER	<nnnnn>	Unique No. allocated by CA
Signature			AlgorithmIdentifier	SHA1 / SHA256 withRSAEncryption	Signature Algorism (SHA1 or SHA256)
Validity			Validity	<n>	1 year after issuance date
	NotBefore		UTCTime	YymmddhhmmssZ	YMDHMS
	NotAfter		UTCTime	YymmddhhmmssZ	YMDHMS
Issuer			Name	<CHAR>	Name of Issuing CA which issued this Cert State theSubject DN as contained in CA Certificate
	CountryName		PrintableString	JP	
	StateName		PrintableString	＊＊＊＊＊＊	
	LocalityName		PrintableString	＊＊＊＊＊＊	
	OrganizationName		Object Identifier（OID）	2.5.4.10	
			PrintableString		
	OrganizationUnitName		Object Identifier（OID）	2.5.4.11	
			PrintableString		
	CommonName		Object Identifier（OID）	2.5.4.3	
			PrintableString		
Subject			Name	<CHAR>	Name of the holder of the Cert State user name, server name, etc.
	CountryName		Object Identifier（OID）	2.5.4.6	
			PrintableString(2)		Country code
	StateName		Object Identifier（OID）	2.5.4.8	
			PrintableString(24)		Prefecture where organization is located
	LocalityName		Object Identifier（OID）	2.5.4.7	
			PrintableString(24)		Locality where organization is located
	OrganizationName		Object Identifier（OID）	2.5.4.10	
			PrintableString(64)		Organization name
	OrganizationUnitName1		Object Identifier（OID）	2.5.4.11	
			PrintableString(32)		"OU=1" +JDAN Accreditation No.
	OrganizationUnitName2		Object Identifier（OID）	2.5.4.11	
			PrintableString(16)		"OU=2" +LRA Organization's own management No.
	CommonName		Object Identifier（OID）	2.5.4.3	
			PrintableString(32)		English name of Object to which the cert is issued (acceptable for alphanumeric character)
SubjectPublicKeyInfo				<CHAR>	Certificate Subscriber (Subject) 's Public Key Info.
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1 (rsaEncryption)	Public Key Algorithm: rsaEncryption
	SubjectPublicKey		BIT STRING	<nnnn>	2048bit Public Key

EE Certificate Profile（2/2）

JDAN (Basic)

Items			Define criticality	Data Type	Explanation	
					Value	Description
authority Key Identifier			FALSE	Object Identifier（OID）	2.5.29.35	CA Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
subjectKeyIdentifier			FALSE	Object Identifier（OID）	2.5.29.14	Subscriber Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
KeyUsage			TRUE	Object Identifier（OID）	2.5.29.15	Purpose of Public Key contained in the Cert
	DigitalSignature			BIT STRING	1	for the purpose of Verifying electronic signature
	KeyEnciphermment			BIT STRING	1	for the purpose of encrypting the key of common key to distributing key
	DataEnciphermment			BIT STRING	1	for the purpose of data encription
extendedKeyUsage			FALSE	Object Identifier（OID）	2.5.29.37	Purpose of Extension key use
	clientAuth			Object Identifier（OID）	1.3.6.1.5.5.7.3.2	TLS Client Verification
	emailProtection			Object Identifier（OID）	1.3.6.1.5.5.7.3.4	used for S/MIME
	msEncryptionFileSystem			Object Identifier（OID）	1.3.6.1.4.1.311.10.3.4	used for Microsoft specification Encription File system
certificatePolicies			FALSE	Object Identifier（OID）	2.5.29.32	Certificate Policy
	policyIdentifier					
		certPolicyId		Object Identifier（OID）	1.2.392.200093.3.5.300	designate OID for Certificate Policy
	policyQualifiers					
		policyQualifierID		Object Identifier（OID）	1.3.6.1.5.5.7.2.1(id-qt-cps)	
		qualifier		IA5String	http://www.jipdec.or.jp/repository/	Repository's URL where certificate policy and the like are published
		policyQualifierID		Object Identifier（OID）	1.3.6.1.5.5.7.2.2(id-qt-unotice)	
		qualifier		VisibleString	JDAN (Basic)	Type of certificate
Basic Constraints			FALSE	Object Identifier（OID）	2.5.29.19	2.5.29.19
	CA			BOOLEAN	FALSE	
subjectAltName			FALSE	Object Identifier（OID）	2.5.29.17	Subscriber Identifier
	rfc822Name			IA5String		Subscriber's email address, which is required for S/MIME
cRLDistributionPoints			FALSE	Object Identifier（OID）	2.5.29.31	Information to obtain CRL
	distributionPoint					
		FullName				
		uniformResourceIdentifier		IA5String	http://crl.globalsign.net/jcanpublicca0.crl	URL of the CRL
authorityInfoAccess			FALSE	Object Identifier（OID）	1.3.6.1.5.5.7.1.1	CA Access Information
	AccessMethod			Object Identifier（OID）	1.3.6.1.5.5.7.48.2	
	AccessLocation UniformResourceIdentifier			IA5STRING	http://secure.globalsign.net/cacert/jcan/jcanpublica0.crt	URL of the Certificate of CA that issued this certificate

クライアント証明書（Advanced）のプロファイル

EE Certificate Profile (1/2)

JCAN (Advanced)

項目 Certificate Fields		Setting	Data Type	Explanation	
				Value	Description
Version			INTEGER	2	'2' as it is V3
SerialNumber			INTEGER	<nnnnn>	Unique No. allocated by CA
Signature			AlgorithmIdentifier	SHA1/SHA256 with RSAEncryption	Signature Algorism (SHA1 or SHA256)
Validity			Validity	<n>	1 year after issuance date
	NotBefore		UTCTime	Yymmddhhmmss	YMDHMS
	NotAfter		UTCTime	Yymmddhhmmss	YMDHMS
Issuer			Name	<CHAR>	Name of Issuing CA which issued this Cert. State theSubject DN as contained in CA Certificate
	CountryName		PrintableString	JP	
	StateName		PrintableString	＊＊＊＊＊＊	
	LocalityName		PrintableString	＊＊＊＊＊＊	
	OrganizationName		Object Identifier (OID)	2.5.4.10	
			PrintableString		
	OrganizationUnitName		Object Identifier (OID)	2.5.4.11	
			PrintableString		
	CommonName		Object Identifier (OID)	2.5.4.3	
			PrintableString		
Subject			Name	<CHAR>	Name of the holder of the Cert State user name, server name, etc.
	CountryName		Object Identifier (OID)	2.5.4.6	
			PrintableString(2)		Country code
	StateName		Object Identifier (OID)	2.5.4.8	
			PrintableString(24)		Prefecture where organization is located
	LocalityName		Object Identifier (OID)	2.5.4.7	
			PrintableString(24)		Locality where organization is located
	OrganizationName		Object Identifier (OID)	2.5.4.10	
			PrintableString(64)		Organization name
	OrganizationUnitName1		Object Identifier (OID)	2.5.4.11	
			PrintableString(32)		"OU=1"+JCAN Accreditation No.
	OrganizationUnitName2		Object Identifier (OID)	2.5.4.11	
			PrintableString(16)		"OU=2"+LRA Organization's own management No.
	CommonName		Object Identifier (OID)	2.5.4.3	
			PrintableString(32)		English name of Object to which the cert is issued (acceptable for alphanumeric character)
SubjectPublicKeyInfo				<CHAR>	Certificate Subscriber (Subject) 's Public Key Info.
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1 (rsaEncryption)	Public Key Algorithm: rsaEncryption
	SubjectPublicKey		BIT STRING	<nnnn>	2048bit Public Key

EE Certificate Profile (2/2)

JCAN (Advanced)

Items			Setting criticality	Data Type	Explanation	
					Value	Description
authority Key Identifier			FALSE	Object Identifier (OID)	2.5.29.35	CA Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
subjectKeyIdentifier			FALSE	Object Identifier (OID)	2.5.29.14	Subscriber Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
KeyUsage			TRUE	Object Identifier (OID)	2.5.29.15	Purpose of Public Key contained in the Cert
	DigitalSignature			BIT STRING	1	for the purpose of Verifying electronic signature
	KeyEnciphermant			BIT STRING	1	for the purpose of encripting the key of common key to distributing key
	DataEnciphermant			BIT STRING	1	for the purpose of data encription
extendedKeyUsage			FALSE	Object Identifier (OID)	2.5.29.37	Purpose of Extension key use
	clientAuth			Object Identifier (OID)	1.3.6.1.5.5.7.3.2	TLS Client Verification
	emailProtection			Object Identifier (OID)	1.3.6.1.5.5.7.3.4	used for S/MIME
	msEncryptionFileSystem			Object Identifier (OID)	1.3.6.1.4.1.311.10.3.4	used for Microsoft specification Encription File system
certificatePolicies			FALSE	Object Identifier (OID)	2.5.29.32	Certificate Policy
	policyIdentifier					
		certPolicyId		Object Identifier (OID)	1.2.392.200093.30.5300	designate OID for Certificate Policy
	policyQualifiers					
		policyQualifierID		Object Identifier (OID)	1.3.6.1.5.5.7.2.1(id-qt-cps)	
		qualifier		IA5String	http://www.jpdec.or.jp/repository/	Repository's URL where certificate policy and the like are published
		policyQualifierID		Object Identifier (OID)	1.3.6.1.5.5.7.2.2(id-qt-unotice)	
		qualifier		VisibleString	JCAN (Advanced)	Type of certificate
Basic Constraints			FALSE	Object Identifier (OID)	2.5.29.19	2.5.29.19
	CA			BOOLEAN	FALSE	
subjectAltName			FALSE	Object Identifier (OID)	2.5.29.17	Subscriber Identifier
	rfc822Name			IA5String		Subscriber's email address, which is required for S/MIME
cRLDistributionPoints			FALSE	Object Identifier (OID)	2.5.29.31	Information to obtain CRL
	distributionPoint					
		FullName				
		uniformResourceIdentifier		IA5String	"http://crl.globalsign.net/jcanpublicca0.crl"	URL of the CRL
authorityInfoAccess			FALSE	Object Identifier (OID)	1.3.6.1.5.5.7.1.1	CA Access information
	AccessMethod			Object Identifier (OID)	1.3.6.1.5.5.7.48.2	
	AccessLocation UniformResourceIdentifier			IA5STRING	http://secure.globalsign.net/cacert/jcan/jcanpublicca0.crt	URL of the Certificate of CA that issued this certificate

B　「団体向け認証基盤のプロトタイプ実証」

目次

1　背景

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。次の 10 年に向けたビジネス情報環境の変革を、企業のビジネススタイルに合った、発行しやすく使いやすい電子証明書の普及で実現していくことを目的に、電子認証の民間制度・基盤の確立に関する調査研究をスタートした。

2　事業の内容

1.1 調査の目的

「平成 21 年度情報化推進に関する調査研究等補助事業」（電子認証の民間制度・基盤の確立に関する調査研究）の成果を受けて、プロトタイプ実証として、民間の制度・基盤の中核となる認証局に係る領域における「団体向け認証基盤のプロトタイプ実証」を実施した。

1.2 事業の内容

(1) 規程類の作成・整備

下記の規定類を作成又は整備した。

- JCAN パブリック認証局（団体向け認証基盤）についての CPS

(2) プロトタイプ実証用認証局の構築

下記の認証局を構築した。

- JCAN パブリック認証局（団体向け認証基盤）認証局

(3) 発行システムの開発

上記認証局について JCAN が指定する証明書プロファイルで証明書を発行する仕組みを構築した。

(4) 認証局の保守・障害対応

上記認証局（１局）について実証期間中の運用と保守及び障害対応を行った。

3　期待される成果の利用・活用方法

- 証明書プロファイル共通化を軸とする JCAN 構想と、ワールドワイドで通用するルート認証局を活用することにより、新たな市場創出の加速化が期待できる。
- 証明書発行の確認に企業の人事情報等を用いることで、信頼感を保ちつつ発行フローを簡素化することがでる。
- 証明書の申請・取得を一括して行う仕組みにより、エンドユーザ負担が軽減され、且つ社員全員での導入を想定した価格体系によりビジネスシーンでの普及拡大が見込まれる。

・ 証明書に社員番号やシュードニウム名といった情報を記載することにより実ビジネスでの利用シーンに即した形での証明書利用推進が期待できる。

証明書の具体的な活用シーンとして下記が見込まれる。

(1) クライアント証明書を用いた認証強化(Web サーバー、Web アプリケーション)
-社員向け、パートナ向け

(2) 電子メールで S/MIME を用いた署名・暗号化、フィッシング対策
-配信メール、取引先とのやり取り

(3) 電子文書の署名を用いた保存
-保存文書の改竄検知

(4) 電子署名を用いた業務フロー(稟議書や決算書)
-電子文書の署名、確認フロー

(5) 模倣品対策
-模倣品対策の真贋判定とトレースのための模倣品対策システムに係るトレーサビリティのための電子認証

4 規定類の作成・整備

(1) JIPDEC 認証局の CPS の作成

JCAN 認証局（団体向け認証基盤）の認証業務運用規程を“JCAN Public CA CPS”として纏めた。本文は「8.1 JCAN パブリック CA CPS」を参照のこと。

5 認証局（１局）の構築・運用

(1) JIPDEC 認証局

グローバルサインルートの下、JCAN 認証局（団体向け認証基盤）を下記プロファイルにて構築（キーセレモニーの実施、オンライン発行局の設定）後、発行システムと接続した。

団体認証基盤の証明書階層と、証明書プロファイルは「8.2 団体認証基盤の証明書階層」を参照のこと。

6 発行システムの開発

JCAN ビジネス証明書を、発行、更新、失効するための「発行システム」を開発、上記団体向け認証基盤と接続した。

LRA の管理責任者は、管理台帳に基づき、証明書記載情報及び各証明書インストール用 PKCS#12 パスワード情報を発行申請シートに転記し、発行申請 CSV ファイルを作成、本システ

ムを用いて、当該 CSV ファイルをアップロードして発行申請を完了する。

7 認証局の保守・障害対応

本認証局構築後、2011 年 1 月よりプロトタイプ実証期間中、保守・障害対応を実施した。本認証局を大きな問題なく運用できた。

なお障害としては、プロトタイプ実証に入る前、認証局の構築段階で、オフライン認証局の構築時の検証で、証明書パス構築の検証チェックでエラーが発生した。調査の結果、ARL の発行及び公開漏れを発見、素早く対応解消された。

8　資料一覧

8.1 JCAN パブリック CA CPS

30-5401

JCAN Public CA CPS
(団体向け認証基盤)
(Certification Practice Statement)

JCAN パブリック CA CPS
(認証業務運用規程)

JIPDEC
財団法人日本情報処理開発協会

Date: February 8th, 2011
Version 1.2

Document Change Control
改訂履歴

Version	ReleaseDate	Status + Description	Author	Approver

Date: February 8th, 2011
Version 1.2

－Table of Contents－

Date: February 8th, 2011
Version 1.2

Date: February 8th, 2011
Version 1.2

1 Introduction （はじめに）

JCAN, Japan CA Network, is a private authorization project operated independently by JIPDEC (Address:3-5-8 Shibakouen, Minato-ku, Tokyo). JCAN Public CA is a CA (Certificate Authority) operated by JCAN.

JCAN（Japan CA Network）は、JIPDEC（所在地：東京都港区芝公園３丁目５番８号）が主体的に運用する民間認証プロジェクトであり、JCAN パブリック CA は JCAN が運営する認証局である。

1.1 Overview （概要）

JCAN Public CA JCAN Public CA CPS (Certification Practice Statement) is a document regulating various procedures having to do with operational maintenance of issuance, revocation of certificates JCAN Public CA conducts and operational maintenance of related Public Key Infrastructure (hereinafter, "PKI").

The policy of end-entity ("EE") Certificates issued by JCAN Public CA is prescribed in JCAN Business Certificate Policy.

In addition, GMO GlobalSign K.K. (Located : 20-1Sakuragaoka-cho, Setagaya-ku, Tokyo) operates this CA entrusted by JCAN.

JCAN パブリック CA CPS は、JCAN パブリック CA が行う証明書の発行、失効、及び関連する公開鍵基盤（Public Key Infrastructure:以下「PKI」という）の維持運用に関わる諸手続きとポリシを規定する文書である。JCAN パブリック CA が発行するエンドエンティティ証明書（以下「EE 証明書」という）のポリシは、JCAN ビジネス証明書ポリシに規定する。

なお、JCAN から委託をうけて、GMO グローバルサイン株式会社（所在地：東京都渋谷区桜丘町 20-1）が本 CA を運用する。

1.2 JCAN Certificate types （JCAN が取り扱う証明書タイプ）

The certificate types addressed in this CPS are the following:

本 CPS で取り扱う証明書タイプは、以下のとおりである。

1.2.1 JCAN Public CA Certificates （JCAN パブリック CA 証明書）

These are CA Certificates of JCAN Public CA. JCAN Public CA issues EE certificates, such as, JCAN Business Certificates.

これは "JCAN Public CA" の CA 証明書である。JCAN Public CA は JCAN ビジネス証明書等の EE 証明書を発行する。

Date: February 8th, 2011
Version 1.2

1.2.2LRA Operational Manager certificate　(LRA 操作責任者証明書)

Local Registration Authority ("LRA") is an organization to which the task of verifing the identity is delegated from the CA. LRA Operational Manager Certificate is an EE certificate issued by a designated CSB (Certificate Service Body) to an individual who is assigned by a JCAN-accredited LRA ("Accredited LRA").

ローカル登録局（"LRA"）とは、認証局から本人確認を委託された機関である。LRA 操作責任者証明書とは、JCAN により認定された LRA（以下、「認定 LRA」という）が指名する個人に、指定 CSB(認証機関)より発行される LRA 操作責任者用の EE 証明書である。

1.2.3JCAN Business Certificates　(JCAN ビジネス証明書)

JCAN provides EE Certificates to an organization which has established LRA （hereinafter, LRA Organization）, and offers EE Certificates for individual use within the organization. These EE Certificates are called "JCAN Business Certificates", and they are used to authenticate subscriber's identity within and between the organizations for non-monetary Internet transactions (eg. Secure Login, Digitally Signed Emails). The types of JCAN Business Certificates which JCAN manages are the following:

JCAN は、LRA を設置する組織（以下、「LRA 組織」という）及び組織内の個人が使用する幾つかのタイプの EE 証明書を提供する。これらの証明書は "JCAN ビジネス証明書" といい、組織内、或いは組織間での、インターネットでの金銭を伴わない取引で利用者を認証すること（例えば、Secure Login、や電子署名）
に利用できる。JCAN が取扱う JCAN ビジネス証明書のタイプを下記に示す。

(1)　JCAN (Qualified)　(JCAN クオリファイド)

A Digital Certificate of which "Certificate Profile" is in accordance with the regulations of "ETSI101862". And it shall be issued, ccorresponding to "Act on Electronic Signatures and Certification Business" of each country, and under the rules of JCAN common rules, with following of the procedures, confirmed and authorized by official documents.

However, "JCAN Qualified Certificate " is not prescribed in this CPS.

(2)　JCAN (Qualified)とは、証明書プロファイルは ETSI101862 に基づいて発行される電子証明書である。またその発行は、運用管理 ETSI101456 及び各国の電子署名法に係る認定認証業務に準じ、JCAN が定めた共通ルールによる公的な書類での認証によって行われる。但し、当該証明書は本 CPS では規定しない。

(3)　JCAN (Advanced)　(JCAN アドヴァンスト)

EE Certificates issued to the employees and staff of LRA Organisation. "JCAN Advanced Certificate" are administered by an LRA Organization. The LRA Organization carries out the authentication of employees and staff through database checks. The establishment and maintenance of staff database ("DB) is a prerequisite. The DB shall be based on the officially

issued documents.

組織が管理する社員・職員に対し発行する EE 証明書である。当該組織の LRA は、本人認証は社員・職員データベースの照合により実施する。なお、社員・職員データベースに対応する公的な根拠資料の保管が条件となる。

Subject Distinguished Name ("DN") includes the real name of the employee or a Pseudonym (PS[1]), and it is described based on:

- Employed contractor's name (Personnel DB is maintained by the Organization)

サブジェクト DN には実名又は PS 名を含み、以下に基づき記載される。

- 雇用契約対象者名（人事 DB を組織が管理している）

- JCAN (Basic)　　(JCAN ベーシック)

EE Certificates other than (1) and (2) above, that are issued when ;
LRA Organization validates that individuals or members and/or their roles or teams belong to the organization,
or the qualified organization authorized by the LRA Organization validates individuals or members and /or their roles or teams belong to an externally-related organization.
This EE issuing service is provided without official documents check. And it is also provided to validate existing email addresses. However, this "JCAN Basic EE Certificate" can be upgraded to "JCAN Advanced EE Certificate" when it is validated through official DB in (2) noted above.

上記(1)(2)以外で、以下の場合に発行される EE 証明である。

・LRA 組織が、個人や会員、またその職務、部署等がそこに所属するものであることを　認証する場合、

・或いはまた、LRA 組織より認定された組織が同様の対象に関しそれがある外部関連組織に所属するものであることを認証する場合であり、

これらの EE 発行サービスは公的な根拠資料は必要としない。また実在が確認されているメールアドレスも認証の対象とする。なお、公的な根拠資料を確認する場合には、当サービスを JCAN Advanced EE 証明ランクに格上げすることができる。

Subjejct DN of a Digital certificate is as follows:

- Employed contractor's name　(Real name or PS)
- Stakeholders outside the Organization (Real name or PS)
- Name of the Organization, Department, Role
- Name of the company or party associated to the Organization

[1] PS (Pseudonym) is an alias, or a false or a fictitious name based on a real name
PS 名 (Pseudonym：シュードニムと発音) とは、実名に裏付けされた擬名、仮名、別名をいう

・ID

・E-mail address

電子証明書に記載する発行対象（以下、「サブジェクト」という）の発行対象識別名（以下、「DN」という）には以下より記載される。

・組織外関係者（実名又はPS名）

・組織名、部門名、職務名

・関係会社名又は団体名

・ID

・メールアドレス

1.3 Document Name and Identification （文書名と識別）

Official name for this CPS is JCAN Public CA CPS.

Identification for referring to the document and the related Policy is the following.

本CPの正式名称はJCANビジネス証明書ポリシである。

本書及び関連するポリシを参照するための識別子は下記のとおりである。

1.2.392.200063.30.5100	JCAN ROOT CA CPS JCANルートCA CPS
1.2.392.200063.30.5150	JCAN ROOT CA Certificate Policy JCANルートCA 証明書ポリシ
1.2.392.200063.30.5300	JCAN Business Certificate Policy JCANビジネス証明書ポリシ
1.2.392.200063.30.5400	JCAN Accreditation CA Common CPS JCAN認定CA共通 CPS
1.2.392.200063.30.5401	JCAN Public CA CPS JCANパブリック CA CPS

1.4 PKI participants （PKIの関係者）

1.4.1 JCAN Root CA （JCANルートCA）

JCAN Root CA is a Root CA operated by JIPDEC. It is an Administration Authority which has the authority and responsibility to create and developf the policy of the certificates based on this CP.

JCANルートCAは、JIPDECが運営するルート認証局である。本CPに基づく証明書のポリシを起草する権限と責任を負うポリシ管理局である。

1.4.2 Designated CSB (Certificate Service Body) （指定CSB）

Designated CSB is a business entity which operates the Partner CA for the Organization, designated by JCAN. When an Organization applies, Designated CSB creates and operates the Partner CA after vetting and verification.

Besides operating the Partner CA outsourced by the Organization, the Designated CSB itself may become the Partner CA.

指定 CSB とは、JCAN が指定するパートナ CA を運用する事業体をいう。パートナ CA の申込みがあった場合、指定 CSB は当該組織を審査・認証後、当該パートナ CA を構築・運用する。

指定 CSB は、当該組織からの委託を受けてパートナ CA を受託運用するほか、指定 CSB 自身がパートナ CA となり運営する場合がある。

1.4.3Partner CA （パートナ CA）

Following JCAN Business Certificate Policy, Partner CA is a CA which issues JCAN Business Certificates as stated in section 1.2.3. in accordance with its purpose of use, range of use, and procedures.

パートナ CA は、JCAN ビジネス証明書ポリシに従い、1.2.3 に記載の JCAN ビジネス証明書を、その利用目的、適用範囲、手続き等に準拠して発行する認証局である。

1.4.4JCAN Public CA （JCAN パブリック CA）

JCAN Public CA is a Partner CA operated by JCAN. Complying with policy set by this CPS, JCAN Public CA issues JCAN Business Certificates as stated in section 1.2.3 in accordance with its purpose of use, range of use, and procedures. JCAN Public CA contacts the subscribers through Accredited CA.

JCAN パブリック CA は、JCAN が運営するパートナ CA である。本 CPS が定めるポリシに従い、1.2.3 に記載の JCAN ビジネス証明書を、その利用目的、適用範囲、手続き等に準拠して発行する。利用者への連絡は認定 LRA を通じて行う。

1.4.5JCAN Accredited LRA （JCAN 認定 LRA）

JCAN Accredited Local Registration Authority (LRA) is an LRA which JCAN authorizes. An Accredited Local Registration Authority vets the authenticity of the DN (Distinguishing Name) and verifies the identity of the subscriber of JCAN Business Certificates. Furthermore, the JCAN Accredited Local Registration Authority operates the life-cycle management (issue, use, revoke,) of the certificate under this CP.

JCAN 認定 LRA とは JCAN が認定した LRA であり、JCAN ビジネス証明書に記載する DN の真正性の審査と利用者の本人認証を行う。 JCAN 認定 LRA は、JCAN ビジネス証明書ポリシの下、証明書のライフサイクルマネージメント（発行、使用、失効）を行う。

1.4.6Subscribers （利用者）

Subscribers who are issued the JCAN Business Certificates are subjects or the deputy of the subjects. If the subject to which the certificate is issued is an organization, the subscriber is an individual designated by the organization.

JCAN ビジネス証明書の発行を受ける利用者は、発行をうける主体又はその代理人である。

なお、証明書の発行をうける主体が組織の場合は、利用者は指定された組織内の個人である。

1.4.7Subjects　（サブジェクト・利用者識別情報）

The subjects of JCAN Business Certificates may be individuals, organizations, IDs or email addresses belonging to companies or parties.

JCAN ビジネス証明書のサブジェクトは、企業／団体に属する、個人、組織等、ID 及びメールアドレスである。

1.4.8Certificate Applicants　（証明書申請者）

A certificate applicant is a person who agrees to the Subscriber Agreement of the CA and applies for a certificate on behalf of the subject.

A certificate applicant is an individual, appointed from the organization to which the subject belongs. The subject may be an individual within the organization, the organization itself, or an ID.

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、サブジェクトが組織内個人、組織、ID 等のいずれの場合においても、サブジェクトが所属する組織から指定された個人である。

1.4.9Relying Parties　（検証者）

Relying Parties are persons that rely on a subscriber's certificate and/or a subscriber's digital signature. Relying Parties must refer to the revocation information of the CA in order to verify the validity of certificate.

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。

1.5　Certificate Usage　（証明書の用途）

1.5.1Usage　（用途）

The uses of JCAN Business Certificates are limited to section 1.2.3.

JCAN ビジネス証明書は、1.2.3 に記載される範囲で利用できる。

1.5.2Appropriate Certificate Usages　（適切な証明書の用途）

Appropriate use of JCAN Business certificates are limited in accordance with this CPS.

JCAN ビジネス証明書は、本 CPS に記載の範囲での適切な用途の利用に限る。

1.6　Policy Administration　（ポリシ管理）

The Policy Administration Authority manages this CPS. The Authority is comprised of members as mentioned below:

- One(1) entrusted member of JCAN

・ Two(2) entrusted member of GlobalSign

Any approval or change of the Policy regarding this CPS must be decided by the Policy Administration Authority. All members of the Policy Administration Authority have one vote.

本 CPS はポリシ管理局により管理され、以下のメンバーで構成される。

・JCAN から委任されるメンバ 1 名

・GlobalSign から委任されるメンバ 2 名

本 CPS を含むポリシの承認及び変更にはポリシ管理局の議決が必要である。全てのポリシ管理局メンバが 1 票の議決権をもつ。

2 Publication and Repository Responsibilities （公開とリポジトリの責任）

2.1 Repository （リポジトリ）

JCAN Public CA is to release the information about the certificates that it issues in its online site of Repository ("Repository"). And JCAN Public CA is to release the information in about its practices, procedures and the content of certain policies including this CPS, under certain rules

JCAN パブリック CA は、発行する証明書に関する情報を JCAN パブリック CA のリポジトリに公開する。また JCAN パブリック CA は、本 CPS を含む、その業務手続、特定のポリシの内容について、リポジトリに一定の開示を行う。

2.2 Publication of Certificate Information （証明書情報の公開）

JCAN、JCAN Public CA, and Accredited LRA are to release the following information in their respective online publicly accessible repositories to the certificate subscribers and relying parties:

JCAN、JCAN パブリック CA、及び認定 LRA は、次の内容を各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。

(1) JCAN Repository （JCAN リポジトリ）

・ Root CA Certificate, Sub Root CA Certificate

・ The two latest versions of the CP and CPS

・ 本 CA 証明書、Sub ルート CA 証明書

・ 最新 2 世代の CP、CPS

(2) JCAN Public CA Repository （JCAN パブリック CA リポジトリ）

・ CA Certificate

・ Certificate Revocation List ("CRL")

・ Other information regarding certificates which this CA issues

・ CA 証明書
・ 証明書失効リスト（CRL）
・ 本 CA が発行する証明書に関するその他の情報

(3) Accredited LRA Repository （認定 LRA）

・ Accredited LRA Attribute Information Table which includes contact information.
・ 認定 LRA 属性情報テーブル（コンタクト情報含む）

2.3 Time and Frequency ofrelease （公開の時期と頻度）

An updated CP or CPS is to be releassed after approval by the Policy Administration Authority. CRL's revocation informations are to be updated regularly. Update frequency is within the validity period of CRL.

本 CP 及び CPS は更新の都度、公開される。CRL の失効情報は、CRL の有効期限内で定期的に更新される。

3 Identification and Authentication （識別と認証）

Accredited LRA maintains business procedural controls and documents regarding the performance of identification and verification of the identity of applicants of a certificate, prior to the issuance of the certificate or before applicant receive a certificate.

認定 LRA は、証明書の発行の前、又は申請者が証明書を受理する前に実施する証明書申請者の本人識別と認証の業務手続文書を保持する。

3.1 Naming

JCAN follows the subscribers' specific names, including the type of names allocated by a Subject such as Distinguished Names defined in X.500, Names defined in RFC 822, and Names defined in X.400. And JCAN follows the regulation of personal identification in order to identify the subscriber.

When applying for the JCAN Business Certificates, the name of the subscriber must be structured as prescribed in this CPS.

Futhermore, the name of the issuer of JCAN Business Certificates must be an official name.

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。

JCAN ビジネス証明書を申請する場合、利用者の名前は、本 CP で規定された名称でなければならない。

なお、JCAN ビジネス証明書の発行者の名前は、正式な名称でなければならない。

3.2 Initial Identity Validation （初回の本人確認）

3.2.1 Validation of Organization （組織の認証）

(1) Accredited LRA Authentication （認定 LRA の認証）

JCAN authenticates the organization to which the Accredited LRA belongs. Authentication is carried out by whatever method JCAN deems reliable. This includes verification of the existence of the organization concerned, Standard Company Code, official documents issued by state and local governments, reliable database which the state and/or the local public body manages （hereinafter, QGIS） and Third party databases （hereinafter, QIIS） which JCAN relies on.

JCAN は、認定 LRA が設置された組織の認証を行う。JCAN はこれを、信頼性があると判断した方法によって実施する。この認証根拠には、当該組織の実在証拠、標準企業コード、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）等を用いる。

3.2.2 Accrediation of LRA Organization （LRA 組織の認定）

JCAN vets the qualification of the applying LRA organization after authentication of the Organization. The authentication is carried out by the method stated in Section 3.2.1.
JCAN is to validate the applying Organization as an Accredited LRA, if it conforms to the vetting qualifications.

JCAN は、認定 LRA が設置された組織の申請があった場合、「3.2.1 組織の認証」に記載の方法による組織の認証後、申請組織の資格審査を行う。

資格審査に適合する場合、申請組織を認定 LRA として認定する。.

3.2.3 Validation of an Individual within a JCAN Business Certificate issued by Partner CA （パートナ CA から発行する JCAN ビジネス証明書の本人確認）

When JCAN Business Certificates are issued, Accredited LRA authenticates the individual as below. Accredited LRA accepts all of the responsibilities regarding an Authentication of an individual.

JCAN ビジネス証明書の発行に際して、認定 LRA が下記の本人認証を行う。本人認証に関わる全ての責任は認定 LRA が負う。

(1) JCAN (Qualified)

Authentication of an individual and issuance of the certificate concerned are not prescribed in this CPS.

当該証明書の発行及び本人認証は、本 CPS では規定しない。

(2) JCAN (Advanced)

LRA authenticates the Individual using the Personnel Book managed by the Organization. In creating the Personnel Book, the existence of the Individual as an employee of the Organization is confirmed through such credible materials as : a copy of a resident's card or notice of local tax special levy determination, employment insurance, resident's tax, tax exemption, insurance premium deduction, or reliable documents with validity periods, such as Driver's licenses and Passports.

組織が管理する人事台帳等により、LRA が本人認証を行う。人事台帳等の作成にあたっては、住民票写し又は地方税特別徴収税額決定通知書、雇用保険被保険者、住民税／扶養控除／保険料控除情報により実在を確認されている、又は運転免許証、パスポート等の有効期間がある公的証明書を根拠資料として作成する。上記公的証明書の発行主体が、同じ手続きで本人認証を行い発行する。

(3) JCAN (Basic)

LRA confirms the existence of the subject belonging to the organization using methods belonging to the organization. When issuing the digital certificate to the external organization (applicant /business partner /student /patient etc), proof of identity is limited to official certificates or business cards and employee ID cards which are maintained and confirmed by the Organization.

JCAN Basic certificate might become JCAN Advanced when it is confirmed through official documents such as resident's cards, Driver's licenses, or Health Insurance Cards.

組織独自の方法によって実在が確認されている発行対象であることを LRA が確認する。外部の組織関係者（申請者、取引先、会員、学生、患者等）に電子証明書を発行する場合は、公的証明書または名刺、社員証等の確認・保管しているものに限る。なお、公的証明書を保管している場合は、当該電子証明書を Advanced にすることができる。

3.2.4 Required Information for Subscriber's Registration （利用者の登録に必要な情報）

Information required for subscriber's registration regarding certificates stated in section 1.2.3. include the following:

1.2.3 に記載される証明書について、利用者登録の際に使用される情報は下記のとおりである。

No.	Information used for registeration of subscribers	Types of Certificates applicable
(1)	An attribute of a Company/an individual within a Party（status）, Personnel Book which manages the official name of a company/ an individual within a party	・JCAN (Advanced) ・JCAN (Basic)

	企業／団体内個人及びそれに結びつく属性（肩書き等）、の正式名称を管理する人事台帳	
(2)	An Organizational Chart where official names of a company and party organization(Departments, roles) are managed 企業／団体の組織（部門名、役割）の正式名称を管理する体制表	・JCAN (Advanced) ・JCAN (Basic)
(3)	Official documents with validity periods, such as Driver's License or Passport 運転免許証、パスポート等、有効期限の記載がある公的証明書	・JCAN (Advanced)

3.2.5Records for subscriber registration （利用者の登録の記録）

Accredited LRA records all information used to verify the subscriber identity.

認定 LRA は、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管理台帳に記録する。

3.3 Identification of Subscribers for Re-Key Requests （鍵の再生成申請時の利用者の本人確認）

3.3.1General Identification and Validation upon Key Renewal （通常の鍵更新における本人性確認と認証）

Identification of the certificate subscribers upon key renewal is in accordance with "3.2 Initial Identity Validation"

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。

3.4 Identification and Authentication for Revocation Requests （失効申請時の本人性確認と認証）

For the identification and authentication procedures of revocation requests, Accredited LRA validates the revocation request by collating it with the logged earlier issuance request.

証明書の失効要求における本人識別と認証手続として、認定 LRA が、管理台帳による照合で失効申請の認証を行う。

4 Certificate Life-Cycle Operational Requirements （証明書のライ

フサイクルに対する運用上の要件）

All parties within the JCAN domain including authenticated LRAs and subscribers have a continuous duty to inform the JCAN Public CA of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or gets revoked.

The JCAN Public CA issues or revokes certificates following a request issued by an Accredited LRA.

認定 LRA、利用者、その他 JCAN 領域内の全ての当事者は、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、認定 LRA を介して JCAN パブリック CA に報告する継続的な義務を負う。

JCAN パブリック CA は、認定 LRA により提出される要求に従って、証明書を発行／失効する。

4.1 Enrollment Process （証明書申請手順）

Upon the request of a certificate, Accredited LRA verifies the individual as per point "3.2 Initial Identity Validation" and approves or rejects the application of the Certificate concerned.

認定 LRA は証明書の申請があった場合、3.2 に記載の初回の本人確認にもとづいた本人識別を行い、当該証明書申請を承認又は棄却する。

4.2 Certificate Issuance （証明書発行）

After verification of Certificate application, Accredited LRA registers the Certificate issuance request to the JCAN Public CA. If the request of Accredited LRA matches the requirements of JCAN Public CA, then the request shall be approved and issued. Issued Certificates are delivered through Accredited LRA and sent to the subscribers.

証明書申請の検証後、認定 LRA は、JCAN パブリック CA に証明書発行要求を登録する。

認定 LRA からの要求は、CA の仕様に合致していれば、承認され発行される。発行された証明書は、認定 LRA を介して利用者に配送される。

4.2.1Certificate generation （証明書生成）

For issuance and renewal of certificates, JCAN Public CA issues the certificates safely, based on the following conditions:

- JCAN Public CA guarantees the unique identification allotted to the subscribers within the domain of JCAN Public CA .
- The confidentiality and integrity of registration data is ensured at all times.
- The authentication of registrars is ensured through appropriate credentials issued to them.

証明書の発行及び更新に関して、JCAN パブリック CA は、以下に規定される条件に従って、

証明書を安全に発行する。

- JCAN パブリック CA は、JCAN パブリック CA 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。
- 認定 LRA の登録機関の認証は、JCAN が発行する認定証等、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。

4.3 Certificate Acceptance （証明書の受領）

An issued certificate is deemed accepted by the subscriber when the Accredited LRA confirms the acceptance of the issued certificate.

発行された証明書は、JCAN パブリック CA が発行する証明書の受領を認定 LRA 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。

4.4 Key Pair and Certificate Usage （鍵ペアと証明書の用途）

4.4.1 Usage of Private Key and Certificate by Subscriber （利用者による秘密鍵、及び証明書の使用）

(1) Subscriber Obligations （利用者の義務）

- Use of the certificate shall only be permitted once the Subscriber has agreed to the conditions within this CPS and to the Subscriber Agreement.
- Use the certificate under reasonable conditions, protect certificates from unauthorized use and discontinue use of the certificate upon expiration or revocation.
- Notify the Accredited LRA promptly of any changes in the information submitted that might affect the trustworthiness of that certificate.
- Should a crucial phenomenon occur which affects the integrity of the certificate, revocation of the certificate concerned shall be requested to Accredited LRA
- Secure private keys appropriately and protect from compromise, loss, unauthorized disclosure, modification, or other unauthorized use.

利用者の義務は以下の通りである。

- 本 CPS の諸条件を承諾し、本 CPS と利用規約に従って許可された用途にのみ証明書を使用すること
- 証明書を合理的な環境下で使用し、不正な操作から防御すること。また証明書が有効でなくなった場合は、使用をやめること。
- 証明書の信頼性に重大な影響を及ぼす情報の変更は、認定 LRA に、速やかに知らせること。
- 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認定 LRA に要求すること

・秘密鍵を適切に保護し、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

4.4.2Relying Party Public Key and Certificate Usage （検証者による公開鍵、及び証明書の使用）

(2) Relying Party Obligations （検証者の義務）

Obligations regarding reliance on a certificate are as follows:

- Certificates are verified by using the latest certificate status information published on the Repositories which are prescribed in this CPS. Certificates are trusted only when the certificate status information (CRL) is verified as the latest version.
- Rely on and trust the JCAN Business Certificates only under reasonable circumstances.

証明書検証者の義務は以下の通りである。

- 本CPSで規定したリポジトリで公開する最新の証明書ステータス情報を使用して証明書を検証し、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こと。
- JCANビジネス証明書を、合理的な環境下でのみ信頼すること。

(3) Conditions of respective Repositories and Websites （各リポジトリとウェブサイトの条件）

Subscribers and Relying Parties who access to Repositories and Websites must approve of the conditions of use published in this CPS.

Acceptable use of Repositories is as follows:

- Acquiring certificate information, verifying certificate status, and verifying corresponding digital signitures.
- Reviewing other information published on the Website.

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CPSの条項,及び リポジトリで公開された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。

- 証明書情報を取得し、証明書のステータスを検証すること、及び対応する電子署名を検証すること
- ウェブサイトに公開されるその他の情報を取得すること

4.5 Certificate Renewal （証明書の更新）

Certificates issued by JCAN will only be renewed if the private key is also renewed. The renewal of the certificates shall follow the same process as outlined in section 3.3 Identification of Subscribers for Re-Key Requests.

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、「3.3　鍵の再生成申請時の利用者の本人確認」と同じ方法による。

4.6　Certificate Revocation　（証明書の失効）

Upon request from Accredited LRA, JCAN Public CA revokes the JCAN Business certificate if :

- There has been loss, theft, unauthorized disclosure, or other compromise of the private key of the subscriber.
- The private key of the subscriber is damaged and can no longer be used.
- The Subscriber has breached a crucial obligation under this CPS.
- The execution of the obligations in the CPS is delayed or prevented by a natural disaster, computer or communications failure, or by other phenomenon out of their control, and as a result, other information is threatened or compromised.
- Information in the certificate has been modified or differs from the facts.
- The Subscriber no longer belongs to or is enrolled in the organization for reasons such as retirement or withdrawal.
- The organization which the subject belongs to decides that the Subscriber Certificate must be revoked.
- Accreditation of LRA is revoked by JCAN.
- There is a reasonable suspicion that the CA is terminated, or that CA private keys are compromised.
- JCAN Public CA decides to cancel the accreditation of the LRA for other reasons..

認定 LRA からの要請により、JCAN パブリック CA は、次のような場合に JCAN ビジネス証明書を失効する。

- 利用者の秘密鍵の紛失、盗難、不正開示、その他の危殆化があった場合
- 利用者の秘密鍵が破損し使用不能となった場合
- 利用者が、本 CPS の下の重大な義務に違反した場合
- 本 CPS 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さらされ危殆化した場合
- 証明書に含まれる情報に変更があった場合、もしくは事実と異なる場合
- 退職・脱退等の事由により利用者が所属組織に所属・在籍しなくなった場合
- その他、利用者所属組織が利用者証明書を失効させる必要があると判断した場合
- 当該 LRA が、JCAN の認定を取り消された場合
- 本 CA を終了する場合、及び CA 秘密鍵が危殆化もしくはその恐れがある場合
- その他、本 CA が必要と判断した場合

4.7　Certificate Status Services　（証明書のステータス確認サービス）

JCAN Public CA provides CRLs to the Subscribers as well as to the Relying Parties. JCAN Pubic CA offers certificate status confirmation services including Webinterfaces to Accredited

LRAs.

JCAN パブリック CA は、利用者及び検証者に対して、CRL を提供する。JCAN パブリック CA は認定 LRA に対して、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。

4.8 End of subscription （利用の終了）

Subscription of JCAN Business Certificate ends when the certificate is revoked, expired or the service is terminated.

JCAN ビジネス証明書の利用は、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に終了する。

5 Facility, Operational, And Management Controls （設備上、運営上、運用上の管理）

This section describes security controls used by JCAN Public CA to perform key generation, subject authentication, CA certificate issuance, CA certificate revocation, audit, and archival.

本章では、鍵生成、サブジェクトの認証、CA 証明書発行、CA 証明書失効、監査、及びアーカイブを実施するために JCAN パブリック CA が使用するセキュリティ管理について説明する。

5.1 Physical Security Controls （物理的管理）

JCAN Public CA implements high-security controls within the data center. These include restricting personnel and physical access using electronic security mechanisms. The Data Center implements measures which protect against waterdamage, earthquakes, fire, and other disasters and implements other structural measures to prevent physical damage to the facility.

JCAN パブリック CA は、認証局の設備の重要性に対応して、人的・物理的なアクセス制御と、電子的なセキュリティメカニズムをもつ高度なセキュリティコントロールを、データセンター内に設置する。データセンターは、水害、地震、火災、その他の災害を容易に受けない構造と防災措置を講じる。

5.2 Procedural Controls （手続的管理）

The JCAN Public CA follows personnel practices that provide reasonable assurance of the trustworthiness and ccompetence of the members of the staff and of the satisfactory performance of their duties.

JCAN パブリック CA は、要員の信頼性と適性及び技術的な業務遂行について、合理的な保証を提供できる人事を実施する。

5.3 Personnel Controls （人事的管理）

5.3.1Qualifications, Experience, Clearance Requirements （資格、経験及び身分の要件）

Employees employed under the employment standards of this CPS or contractor personnel equivalent are the personnel in trusted positions prescribed in Procedural Controls in section 5.2.

本 CPS の採用基準に基づき採用された従業員、或いは同等の契約者が 5.2.項の手続的管理事項に記載の信任された役職につく要員である。

5.3.2Training Requirements （研修要件）

JCAN Public CA provides training to their personnel to carry out the CA functions.

JCAN パブリック CA は、認証業務を実行するために、その要員に研修を実施する。

5.3.3Retraining Frequency and Requirements （再研修の頻度及び要件）

Personnel are regularly retrained for the purpose of renewing and maintaining the procedural knowledge.

手続についての知識の更新と維持を目的に、定期的な再研修をその要員に実施する。

5.3.4Sanctions for Unauthorized Actions （認められていない行動に対する懲戒）

JCAN Public CA will take disciplinary actions toward personnel who perform unauthorized actions, use unauthorized authority, or use unauthorized systems.

JCAN パブリック CA は、認められていない行動、認められていない権限の使用、認められていないシステムの使用をした要員に対し、適切でないと判断した時は懲戒を行うことがある。

5.3.5Documentation Supplied to Personnel （要員に提供する資料）

JCAN Public CA provides documents to personnel on the first day of training and between other training sessions.

パートナ CA は、初回の研修とその他の研修の期間、要員に対し資料を提供する。

5.4 Audit Logging Procedures （監査ログの手続）

JCAN Public CA implement Audit logging. These include logging of audit event, and audit systems implemented for the purpose of maintaining a secure environment. JCAN Public CA implements the following controls.

監査ログの手続には、安全な環境を維持する目的で実装されたイベントログと監査ツールのログを含む。JCAN パブリック CA は、以下の管理を実装する。

5.4.1Types of Logs to be Audited （監査するログの種類）

JCAN Public CA implements the following controls:

JCAN パブリック CA は、以下の記録を監査する。

(1) System Log （システムに関するログ）

- Issuance of a certificate
- Revocation of a certificate
- Publishing of a CRL
- Others (such as Record Log)
  - CA 証明書の発行
  - CA 証明書の失効
  - CRL の公開
  - その他（ログイン記録等）

(2) Records regarding entry/exit and operation of CA private key. （入退室と CA 秘密鍵の操作に関する記録）

- CA facility visitor entry/exit.
- Records regarding operation and life-cycle management of CA private key.
- CA を設置する室への入退室記録
- 秘密鍵の操作に関する記録

5.4.2Audit trail records contain: （監査ツールのログに含まれる項目）

- The identification of the operation
- The data and time of the operation
- The identification of the certificate involved in the operation
- The identification of the person that performed the operation
- A reference to the request for the operation
  - 操作の識別
  - 操作の日時、時刻
  - 操作に含まれる証明書の識別
  - 操作を実施した人の識別
  - 操作要求に関する参照情報

5.4.3Frequency of Processing Log （監査ログを処理する頻度）

Appointed personnel inspect the log file in regular interval and detect and reports when there is an abnormal event.

一定の間隔で、指命された要員がログファイルを点検し、異常事象を検知し、報告できるようにする。

5.4.4Storage and Protection of Records and Backup （記録の保存と保護、及びバックアップ）

The log files and auditing trails are recorded. These are appropriately protected using an Access Control Structure. These log files can only be accessed by an individual appointed to JCAN Public CA or for the purpose of inspection by the appointed auditor.

JCAN パブリック CA の任命された者、及び指定された監査人による検査のため、ログファイルと監査証跡は保存される。これらは、アクセス制御機構により適切に保護され、バックアップされる。

5.5 Records Archive （記録のアーカイブ）

5.5.1Types of Records Archived （アーカイブされる記録の種類）

JCAN Public CA maintains the details of all CA Certificates, auditing data of issuance and revocation of CA Certificates, application information of CA Certificates, CRLs, log files, and any other records which support the application of CA Certificates. These records are maintained through reliable methods.

JCAN パブリック CA は、CA 証明書、CA 証明書の発行・失効の監査データ、CRL、CA 証明書申請情報、ログファイル、及び CA 証明書申請の裏付け資料の記録を、信頼性のある方法で保持する

5.5.2Retention Period for Archive （アーカイブ保存期間）

JCAN Public CA retains records of CA Certificates in a reliable format for no more than seven years following the date the Certificate expires or is revoked.

JCAN パブリック CA は、CA 証明書の記録を、有効期限切れ後、又は失効後、最長 7 年間、信頼のある方法で保持する。

5.6 Compromise and Disaster Recovery （危殆化、及び災害からの復旧）

JCAN Public CA maintains records on reporting and handling procedures for incidents and compromises in a separate internal document. JCAN Public CA documents the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

JCAN パブリック CA は、インシデント及び危殆化が発生した場合の報告と取り扱い手続を、内部文書として文書化する。JCAN パブリック CA は、コンピュータ資源、ソフトウェア、又はデータが破損した場合に使用する復旧手続を文書化する。（災害復旧計画）

5.7 Termination of CA or RA （認証局又は登録局の終了）

Before terminating its CA or RA (Registrarion Authority) activities, the JCAN Public CA will take steps to transfer to a designated organization the following information at JCAN Public CA's own costs:

- All information , data, documents and repositories pertaining to the JCAN Public CA
- Archives and audit trails

認証局としての活動を終了する前に、JCAN パブリック CA は指定された組織に以下の情報を、段階を踏んで譲渡する。

- JCAN パブリック CA に関するすべての情報、データ、文書、リポジトリ

・アーカイブデータ、監査証跡

6 Technical Security Controls （技術的セキュリティ管理）

This section describes the security measures taken by JCAN Public CA to protect its cryptographic keys and activation data.

本章では、暗号鍵及び活性化データを保護するために採用するセキュリティ対策を説明する。

6.1 Key Pair Generation and Installation （鍵ペアの生成、及びインストール）

6.1.1 CA Key Generation Devices （CA 鍵生成のデバイス）

Hardware Security Module ("HSM"), Cryptographic Signing equipment for safely generating and managing private keys, is used for generating and managing private keys.

本 CA の秘密鍵の生成と管理には、秘密鍵を安全に保護する署名暗号装置であるハードウェアセキュリティモジュール（以下「HSM」という）を用いる。

6.1.2 CA Private Key Generation （CA 秘密鍵の生成）

The CA generates the CA private keys by following the documented procedures. The generation of the CA private key requires more than two authorized staff members serving in trustworthy positions. And this action requires "Mutual supervision". Private keys are managed on HSM and the shared secret system. The generation algorithm shall be the RSA (an algorithm for public-key encryption) in the way of SHA-1 or SHA-256 hashes, and the key length is to be 2048 bit minimum.

パートナ CA は、文書化された手続に従って CA 秘密鍵を生成する。CA の秘密鍵の生成は、信任された役職 2 名以上の要員による管理を必要とする。この行為は相互牽制を伴い、秘密鍵は、HSM で管理され、秘密分散方式で管理される。鍵生成アルゴリズムは RSA　SHA-1 又は SHA-256 を使用し、鍵長は最低 2048bit とする。

6.1.3 CA Private Key Usage （CA 秘密鍵の利用方法）

Private keys of the JCAN Public CA are used to sign Partner CA Certificates and CRLs. Other usage is prohibited.

本 CA の秘密鍵は、CA が発行する証明書と証明書失効リストの署名に使用される。その他の利用方法は禁止されている。

6.1.4 CA Private Key Types （CA 秘密鍵のタイプ）

The CA private key shall be 2048 bit in length and generated by RSA algorithm, with SHA-1 or SHA-256 hashes.

本 CA 秘密鍵は、鍵長 2048 ビットで、RSA アルゴリズムを使用する。

6.1.5 Generation of the Subscriber Private Keys　（利用者の秘密鍵の生成）

The Private Key of Subscribers are 2048 bit in length and uses RSA algorithm. For its generation, the following method is used:

利用者秘密鍵の生成は、鍵長 2048 ビットで RSA アルゴリズムを使用し、下記の何れかの方法で行う：

(1)　Generation of Private Keys by JCAN Public CA　（JCAN パブリック CA による秘密鍵の生成）

When JCAN Public CA generates the private key on behalf of subscribers or LRA, the key pair and CSR is generated according to a safe key generating procedure and by following the key generation policy referenced above.　The CA enforces to subscribers to use of a PIN code. The PIN protects the generated private key in PKSC#12 format. Once subscriber or LRA receives the PKSC#12, all instances of this PKSC#12 are destroyed by CA including the PIN code.　None of the generated private keys are archived.

JCAN パブリック CA が利用者又は LRA に代わって秘密鍵の生成を行う場合は、安全な鍵生成手順を用いて、上記鍵生成のポリシに準拠して PKI の鍵ペア及び CSR を生成する。本 CA は、申請者に強固な PIN の使用を義務付け、当該 PIN を用いて秘密鍵を含む pkcs#12 形式の暗号化証明書パッケージ（以下「pkcs#12 形式証明書」という）を生成する。当該 PIN 及び生成した秘密鍵はアーカイブせず、全てのインスタンスは pkcs#12 形式証明書の生成後に破棄される。

6.2　Key Pair re-generation and re-installation　（鍵ペアの再生成と再インストール）

The JCAN Public CA decommissions and destroys keys used in the past and zero-out cryptographic devices in a secure manner at the end of the life-cycle.　All backup or escrowed copies of its private keys are also destroyed at the end of the life-cycle.

パートナ CA はライフサイクルの終了時に、安全な方法で過去に使用された全ての鍵を廃棄し、暗号デバイスをゼロ設定する。同様に、すべてのバックアップ及びキーエスクローされた秘密鍵の複写はライフサイクルの終了時に破棄される。

6.2.1 CA Key Generation Controls　（CA 鍵生成の管理）

Please see section 6.1.2

6.1.2 に準じる。

6.2.2 CA Private Key Storage　（CA 秘密鍵の保管）

The private key of the CA is stored in an HSM. When outside the HSM, the private key is always strongly encrypted.

本 CA の秘密鍵は HSM に保管し、HSM の外では CA の秘密鍵は常に暗号化される。

6.2.3CA Public Key Distribution　(CA 公開鍵の交付)

Public key distribution of the CA's own public key takes place according to the CA's own practices.

本 CA 自身の公開鍵配付は、本 CA 自身の業務手続に従って実行される。

6.2.4CA Private Key Destruction　(CA 秘密鍵の破壊方法)

The CA private keys are destroyed at the end of their lifetimes by at least two trusted operatives. The Key destruction process is documented and associated records are archived.

本 CA の秘密鍵は、ライフタイムの最後に、信任された役職 2 名以上の要員の立会いの下に破棄される。鍵の破棄の処理は文書化し、関連する記録は保存する。

6.3　Private Key Protection and Cryptographic Module Engineering Controls (秘密鍵の保護、及び暗号モジュール技術の管理)

6.3.1CA Private Key Protection　(CA 秘密鍵の保護)

JCAN Public CA uses HSM which meets the standards of FIPS140-2 Level 3.

JCAN パブリック CA は、FIPS140-2 のレベル 3 相当の認定を取得した HSM を使用する。

6.3.2Subscriber's Private Key Protection　(利用者秘密鍵の保護)

(2)　Subscriber Obligations　(利用者の義務)

Subscribers must secure the private keys of the certificate on their own.

利用者は、証明書の秘密鍵を利用者自身の責任で安全に保護しなければならない。

(3)　LRA's Obligation　(LRA の義務)

LRA safely distributes pkcs#12 format certificate and corresponding PIN to the subscribers and securely protects them.

LRA は pkcs#12 形式証明書及び対応する PIN を安全に利用者に配布し、かつ安全に保管しなければならない。

(4)　CA Obligation　(本 CA の義務)

After generating the of pkcs#12 formatted certificate, the CA protects the private key through the use of a PIN. None of the corresponding PINs are retained: they are destroyed.

本 CA は、pkcs#12 形式証明書を生成したあとは、利用証明書の秘密鍵を PKCS#12 と PIN で保護し、対応する PIN は一切保存せず破棄する。

6.4　Activation Data　(活性化データ)

The JCAN Public CA securely stores activation data associated with its own private key and operations.

JCAN パブリック CA は、自己の秘密鍵と業務に関連する活性化データを安全に保管する。

6.5　Computer Security Controls　(コンピュータのセキュリティ管理)

The JCAN Public CA implements required computer security controls.

JCAN パブリック CA は、必要なコンピュータセキュリティ管理を実装する。

6.6 Life Cycle Security Controls （ライフサイクルの技術上の管理）

The JCAN Public CA reviews periodic security management controls.

JCAN パブリック CA は、定期的なセキュリティ管理レビューを実施する。

6.7 Network Security Controls ネットワークセキュリティ管理

The JCAN Public CA network is protected by firewall and intrusion detection system.

本 CA のネットワークは、ファイアウォールと不正検知システムにより保護される。

7 Certificate and CRL Profiles （証明書、及び CRL のプロファイル）

This section specifies Certificate and CRL Profiles

このセクションは、証明書フォーマット、及び CRL のプロファイルを規定する。

7.1 Certificate Profile （証明書プロファイル）

The JCAN Public CA issues certificates in the X.509 Version 3 Format.

JCAN パブリック CA が発行する証明書は、X.509 バージョン 3 フォーマットにより作成される。

Field（フィールド）	Value or Value constraint（値、又は値制約）
Serial Number シリアルナンバー	Unique value within the CA domain CA が割り当てる一意な番号
Signature Algorithm 署名アルゴリズム	Object identifier of the algorithm used to sign the certificate. SHA1 RSA or SHA256 RSA in accordance with RFC3279. 証明書に署名するために使用されたアルゴリズムのオブジェクト識別子 RFC3279 に従い、SHA1 RSA または SHA256 RSA
Issuer Certificate 証明書発行者	The name of the CA which issued the digital certificate - written in X.500 identifier (DN) format 電子証明書を発行した CA の名前、X.500 識別名(DN)で記述
Valid From 有効期間開始日	Start of the validity period of the certificate 証明書の有効期間開始日
Valid To 有効期間終了日	End of the validity period of the certificate 証明書の有効期間終了日
Subject DN サブジェクト DN	The name of the owner of the digital ceritificate and other pertinent information 電子証明書の所有者の名前

Subject Public Key サブジェクト公開鍵	The public key. 証明書所有者の公開鍵に関する情報

7.1.1 Authority Key Identifier　(Authority Key Identifier 拡張)

JCAN generally incorporates the Authority Key Identifier extension in the EE Certificates and Intermediate CA Certificates. The Authority Key Identifier is composed of the 160-bit SHA-1hash of the public key of the CA issuing the Certificate.

JCAN は、EE 証明書と中間 CA 証明書に対し、X.509 バージョン 3 の Authority Key Identifier 拡張を挿入する。証明書発行者が subjectKeyIdntifier 拡張を含む際、Authority 鍵識別子は、証明書を発行する認証局の公開鍵の 160 ビットの SHA-1 ハッシュから構成される。

7.1.2 Authority Information Access　(Authority Information Access 拡張)

JCAN generally incorporates the Authority Information Access ("AIA") extension of X.509 the appropriate EE Certificates and Intermediate CA Certificates.　AIA is incorporated through the URL of the location where a Relying Party can obtain the issuing CA certificate.

JCAN は、EE 証明書、及び適当であれば中間 CA 証明書に対し、X.509 バージョン 3 の Authority Information Access 拡張を、検証者がパブリック CA 証明書を取得できる URL と共に挿入する。

7.1.3 CRL Distribution Points　(CRL Distribution Points 拡張)

Most JCAN X.509 Version 3 EE user Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the certificate's status.

JCAN の EE ユーザ証明書と中間 CA 証明書は、検証者が CA 証明書のステータスを確認するための CRL を取得できる URL を含む、X.509 バージョン 3 の cRLDistributionPoints 拡張を含む。

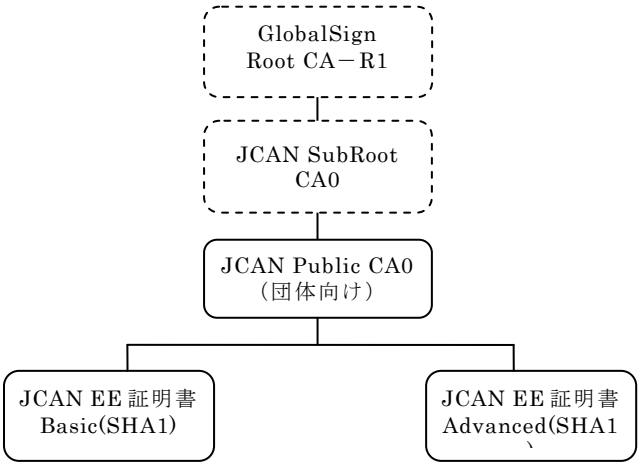
7.1.4 Subject Key Identifier　(Subject Key Identifier 拡張)

Where JCAN incorporates X.509 Version 3 certificates with a subjectKeyIdentifier extension, the keyIdentifier based on the public key of the Subject of the Certificate is composed of 160 bit SHA-1 hash.

JCAN が subjectKeyIdentifier 拡張を X.509 バージョン 3 証明書に挿入する場合、証明書のサブジェクトの公開鍵にもとづく keyIdentifier は、160 ビットの SHA-1 ハッシュ値から構成される。

8.2 団体認証基盤の証明書階層

団体認証基盤の証明書階層



JCAN Public CA0　CA 証明書プロファイル

■Certificate Profile (Basic Certificate Fields)

項目 Certificate Fields		Setting	Data type	Explanation	
				Value	Description
Version			INTEGER	2	「2」due to being V3
SerialNumber			INTEGER	<nnnnn>	Unique No. allocated by CA
Signature			AlgorithmIdentifier	1.2.840.113549.1.1.5	SHA-1withRSAEncryption
Validity			Validity	<n>	Validity Period (10 year?) Considering CA Hiarachy
	NotBefore		UTCTime	Yymmddhhmmss	YymmddhhmmssZ(YMDHMSZ)
	NotAfter		UTCTime	Yymmddhhmmss	YymmddhhmmssZ(YMDHMSZ)
Issuer			Name	<CHAR>	Name of Issuing Authority which issued this Cert
	CountryName		PrintableString	JP	Country Code(2-letter code)
	OrganizationName		Object Identifier (OID)	2.5.4.10	
			PrintableString	JIPDEC	
	OrganizationUnitName		Object Identifier (OID)	2.5.4.11	
			PrintableString	JCAN Sub Root CA0	
	CommonName		Object Identifier (OID)	2.5.4.3	
			PrintableString	JCAN Sub Root CA0	
Subject			Name		Name of the holder of the certificate
	CountryName		PrintableString	JP	Country Code(2-letter code)
	OrganizationName		Object Identifier (OID)	2.5.4.10	
			PrintableString	JIPDEC	
	OrganizationUnitName		Object Identifier (OID)	2.5.4.11	
			PrintableString	JCAN Public CA0	
	CommonName		Object Identifier (OID)	2.5.4.3	
			PrintableString	JCAN Public CA0	
SubjectPublicKeyInfo			SubjectPublicKeyInfo	<CHAR>	Certificate Subscriber (Subject) ' s Public Key Information
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1	Public Key Algorithm: rsaEncryption
	SubjectPublicKey		BIT STRING	<nnnn>	2048bit Public Key

■Certificate Profile (Basic Certificate Fields)

Items			Setting criticality	Data Type	Explanation	
					Value	Description
authority Key Identifier			FALSE	Object Identifier (OID)	2.5.29.35	CA Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
subjectKeyIdentifier			FALSE	Object Identifier (OID)	2.5.29.14	Subscriber Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
KeyUsage			TRUE	Object Identifier (OID)	2.5.29.15	Purpose of Public Key contained in the Cert
	KeyCertSign			BIT STRING	1	for the purpose of Verifying electronic signature
	CRLSign			BIT STRING	1	for the purpose of encripting the key of common key to distributing key
certificatePolicies			FALSE	Object Identifier (OID)	2.5.29.32	Certificate Policy
	policyIdentifier					
		certPolicyId		Object Identifier (OID)	1.2.392.200063.30.5300	OID of Certificate Policy
	policyQualifiers					
		policyQualifierID		Object Identifier (OID)	1.3.6.1.5.5.7.2.1(id-qt-cps)	
		qualifier		IA5String	http://www.jipdec.or.jp/repository/	Repository's URL where certificate policy and the like are published
		policyQualifierID		Object Identifier (OID)	1.3.6.1.5.5.7.2.2(id-qt-unotice)	
		qualifier		VIsible String	JCAN Business CP	Name of certificate Policy
Basic Constraints			TRUE	Object Identifier (OID)	2 5 29 19	2 5 29 19
	CA			BOOLEAN	TRUE	
	PathlenConstraint			INTEGER	0	
cRLDistriburionPoints			FALSE	Object Identifier (OID)	2.5.29.31	Information to obtain certificate revocation list (CRL)
	distributionPoint					
		FullName				
		uniformResourceIdentifier		IA5String	http://crl.globalsign.net/jcansubrootca0.crl	to set up a URL http:// *********
authorutyInfoAccess			FALSE	Object Identifier (OID)	1.3.6.1.5.5.7.1.1	CA Access information
	AccessMethod			Object Identifier (OID)	1.3.6.1.5.5.48.2	
	AccessLocation UniformResourceIdentifier			IA5String	http://secure.globalsign.net/cacert/jcan/jcansubrootca0.crt	to Publish URL of the Certificate of CA that issued this certificate http:// *****

JCAN EE 証明書プロファイル（Basic）

JCAN (Basic)

項目 Certificate Fields		Setting	Data Type	Explanation	
				Value	Description
Version			INTEGER	2	「2」as it is V3
SerialNumber			INTEGER	<nnnnn>	Unique No. allocated by CA
Signature			AlgorithmIdentifier	SHA1WithRSAEncryption (1.2.840.113549.1.1.5)	Signature Algorism (SHA1)
Validity			Validity	<n>	1 year after issuance date
	NotBefore		UTCTime	Yymmddhhmmss	YMDHMS
	NotAfter		UTCTime	Yymmddhhmmss	YMDHMS
Issuer			Name	<CHAR>	Name of Issuing CA which issued this Cert. State theSubject DN as contained in CA Certificate.
	CountryName		PrintableString	JP	
	StateName		PrintableString	＊＊＊＊＊＊	
	LocalityName		PrintableString	＊＊＊＊＊＊	
	OrganizationName		Object Identifier（OID）	2.5.4.10	
			PrintableString		
	OrganizationUnitName		Object Identifier（OID）	2.5.4.11	
			PrintableString		
	CommonName		Object Identifier（OID）	2.5.4.3	
			PrintableString		
Subject			Name	<CHAR>	Name of the holder of the Cert State user name, server name, etc.
	CountryName		Object Identifier（OID）	2.5.4.6	
			PrintableString(2)		Country code
	StateName		Object Identifier（OID）	2.5.4.8	
			PrintableString(24)		Prefecture where organization is located
	LocalityName		Object Identifier（OID）	2.5.4.7	
			PrintableString(24)		Locality where organization is located
	OrganizationName		Object Identifier（OID）	2.5.4.10	
			PrintableString(54)		Organization name
	OrganizationUnitName1		Object Identifier（OID）	2.5.4.11	
			PrintableString(32)		"OU-1"+JCAN Accreditation No.
	OrganizationUnitName2		Object Identifier（OID）	2.5.4.11	
			PrintableString(16)		"OU-2"+LRA Organization's own management No.
	CommonName		Object Identifier（OID）	2.5.4.3	
			PrintableString(32)		English name of Object to which the cert is issued (acceptable for alphanumeric charater)
SubjectPublicKeyInfo				<CHAR>	Certificate Subscriber (Subject) ' s Public Key Info.
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1(rsaEncryption)	Public Key Algorithm: rsaEncryption
	SubjectPublicKey		BIT STRING	<nnnn>	2048bit Public Key

JCAN (Basic)

Items			Setting criticality	Data Type	Explanation	
					Value	Description
authority Key Identifier			FALSE	Object Identifier（OID）	2.5.29.35	CA Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
subjectKeyIdentifier			FALSE	Object Identifier（OID）	2.5.29.14	Subscriber Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
KeyUsage			TRUE	Object Identifier（OID）	2.5.29.15	Purpose of Public Key contained in the Cert
	DigitalSignature			BIT STRING	1	for the purpose of Verifying electronic signature
	KeyEncipherment			BIT STRING	1	for the purpose of encripting the key of common key to distributing key
	DataEncipherment			BIT STRING	1	for the purpose of data encription
extendedKeyUsage			FALSE	Object Identifier（OID）	2.5.29.37	Purpose of Extension key use
	clientAuth			Object Identifier（OID）	1.3.6.1.5.5.7.3.2	TLS Client Verification
	emailProtection			Object Identifier（OID）	1.3.6.1.5.5.7.3.4	used for S/MIME
	msEncryptionFileSystem			Object Identifier（OID）	1.3.6.1.4.1.311.10.3.4	used for Microsoft specification Encription File system
certificatePolicies			FALSE	Object Identifier（OID）	2 .5 .29 .32	Certificate Policy
	policyIdentifier					
	certPolicyId			Object Identifier（OID）	1.2.392.200063.30.5300	desiganate OID for Certificate Policy
	policyQualifiers					
		policyQualifierID		Object Identifier（OID）	1.3.6.1.5.5.7.2.1(id-qt-cps)	
		qualifier		IA5String	http://www.jipdec.or.jp/repository/	Repository's URL where certificate policy and the like are published
		policyQualifierID		Object Identifier（OID）	1.3.6.1.5.5.7.2.2(id-qt-unotice)	
		qualifier		VisibleString	JCAN (Basic)	Type of certificate
Basic Constraints			FALSE	Object Identifier（OID）	2 5 29 19	2 5 29 19
	CA			BOOLEAN	FALSE	
subjectAltName			FALSE	Object Identifier（OID）	2.5.29.17	Subscriber Identifier
	rfc822Name			IA5String		Subscriber's email address, which is required for S/MIME
cRLDistriburionPoints			FALSE	Object Identifier（OID）	2.5.29.31	Information to obtain CRL
	distributionPoint					
		FullName				
			uniformResourceIdentifier	IA5String	"http://crl.globalsign.net/jcanpublicca0.crl"	URL of the CRL
authorutyInfoAccess			FALSE	Object Identifier（OID）	1.3.6.1.5.5.7.1.1	CA Access information
	AccessMethod			Object Identifier（OID）	1.3.6.1.5.5.7.48.2	
	AccessLocation UniformResourceIdentifier			IA5STRING	http://secure.globalsign.net/cacert/jcan/jcanpublicca0.crt	URL of the Certificate of CA that issued this certificate

JCAN EE 証明書プロファイル（Advanced）

JCAN (Advanced)

項目 Certificate Fields		Setting	Data Type	Explanation	
				Value	Description
Version			INTEGER	2	「2」as it is V3
SerialNumber			INTEGER	<nnnnn>	Unique No. allocated by CA
Signature			AlgorithmIdentifier	SHA1WithRSAEncryption (1.2.840.113549.1.1.5)	Signature Algorism (SHA1)
Validity			Validity	<n>	1 year after issuance date
	NotBefore		UTCTime	Yymmddhhmmss	YMDHMS
	NotAfter		UTCTime	Yymmddhhmmss	YMDHMS
Issuer			Name	<CHAR>	Name of Issuing CA which issued this Cert. State theSubject DN as contained in CA Certificate.
	CountryName		PrintableString	JP	
	StateName		PrintableString	＊＊＊＊＊＊	
	LocalityName		PrintableString	＊＊＊＊＊＊	
	OrganizationName		Object Identifier（OID）	2.5.4.10	
			PrintableString		
	OrganizationUnitName		Object Identifier（OID）	2.5.4.11	
			PrintableString		
	CommonName		Object Identifier（OID）	2.5.4.3	
			PrintableString		
Subject			Name	<CHAR>	Name of the holder of the Cert State user name, server name, etc.
	CountryName		Object Identifier（OID）	2.5.4.6	
			PrintableString(2)		Country code
	StateName		Object Identifier（OID）	2.5.4.8	
			PrintableString(24)		Prefecture where organization is located
	LocalityName		Object Identifier（OID）	2.5.4.7	
			PrintableString(24)		Locality where organization is located
	OrganizationName		Object Identifier（OID）	2.5.4.10	
			PrintableString(54)		Organization name
	OrganizationUnitName1		Object Identifier（OID）	2.5.4.11	
			PrintableString(32)		"OU-1"+JCAN Accreditation No.
	OrganizationUnitName2		Object Identifier（OID）	2.5.4.11	
			PrintableString(16)		"OU-2"+LRA Organization's own management No.
	CommonName		Object Identifier（OID）	2.5.4.3	
			PrintableString(32)		English name of Object to which the cert is issued (acceptable for alphanumeric charater)
SubjectPublicKeyInfo				<CHAR>	Certificate Subscriber (Subject) ' s Public Key Info.
	Algorithm		AlgorithmIdentifier	1.2.840.113549.1.1.1 (rsaEncryption)	Public Key Algorithm: rsaEncryption
	SubjectPublicKey		BIT STRING	<nnnn>	2048bit Public Key

JCAN (Advanced)

Items			Setting criticality	Data Type	Explanation	
					Value	Description
authority Key Identifier			FALSE	Object Identifier（OID）	2.5.29.35	CA Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
subjectKeyIdentifier			FALSE	Object Identifier（OID）	2.5.29.14	Subscriber Key Identifier
				OCTET STRING	<CHAR>	SHA-1 Value according to RFC5280 4.2.1.2
KeyUsage			TRUE	Object Identifier（OID）	2.5.29.15	Purpose of Public Key contained in the Cert
	DigitalSignature			BIT STRING	1	for the purpose of Verifying electronic signature
	KeyEncipherment			BIT STRING	1	for the purpose of encripting the key of common key to distributing key
	DataEncipherment			BIT STRING	1	for the purpose of data encription
extendedKeyUsage			FALSE	Object Identifier（OID）	2.5.29.37	Purpose of Extension key use
	clientAuth			Object Identifier（OID）	1.3.6.1.5.5.7.3.2	TLS Client Verification
	emailProtection			Object Identifier（OID）	1.3.6.1.5.5.7.3.4	used for S/MIME
	msEncryptionFileSystem			Object Identifier（OID）	1.3.6.1.4.1.311.10.3.4	used for Microsoft specification Encription File system
certificatePolicies			FALSE	Object Identifier（OID）	2 .5 .29 .32	Certificate Policy
	policyIdentifier					
		certPolicyId		Object Identifier（OID）	1.2.392.200063.30.5300	desiganate OID for Certificate Policy
	policyQualifiers					
		policyQualifierID		Object Identifier（OID）	1.3.6.1.5.5.7.2.1(id-qt-cps)	
		qualifier		IA5String	http://www.jipdec.or.jp/repository/	Repository's URL where certificate policy and the like are published
		policyQualifierID		Object Identifier（OID）	1.3.6.1.5.5.7.2.2(id-qt-unotice)	
		qualifier		VisibleString	JCAN (Advanced)	Type of certificate
Basic Constraints			FALSE	Object Identifier（OID）	2 5 29 19	2 5 29 19
	CA			BOOLEAN	FALSE	
subjectAltName			FALSE	Object Identifier（OID）	2.5.29.17	Subscriber Identifier
	rfc822Name			IA5String		Subscriber's email address, which is required for S/MIME
cRLDistriburionPoints			FALSE	Object Identifier（OID）	2.5.29.31	Information to obtain CRL
	distributionPoint					
		FullName				
			uniformResourceIdentifier	IA5String	"http://crl.globalsign.net/jcanpublicca0.crl"	URL of the CRL
authorutyInfoAccess			FALSE	Object Identifier（OID）	1.3.6.1.5.5.7.1.1	CA Access information
	AccessMethod			Object Identifier（OID）	1.3.6.1.5.5.7.48.2	
	AccessLocation UniformResourceIdentifier			IA5STRING	http://secure.globalsign.net/cacert/jcan/jcanpublicca0.crt	URL of the Certificate of CA that issued this certificate

C「マルチユース格納媒体のプロトタイプ実証調査」

目次

1 概要

1.1 目的

公開鍵基盤（PKI）は、信頼された電子証明書に基づく厳格な個人認証や、否認防止を確実にする電子署名など、高度なセキュリティを確保するソリューションとして知られている。公開鍵基盤（PKI）の信頼性を確保するために、電子証明書と署名鍵（プライベート鍵）は、本人以外の第三者が利用できないように安全に保管しておく必要がある。

電子証明書の導入の初期段階では、パソコンのハードディスク内の証明書ストアに電子証明書と署名鍵（プライベート鍵）を格納しておくところからスタートする事例が多く見られる。しかし、この方法では署名鍵（プライベート鍵）を利用して電子署名をしているユーザが電子証明書に記載された本人であることを保証できない。

そこで、公開鍵基盤（PKI）の信頼性を確実に担保するために、電子証明書と署名鍵（プライベート鍵）を安全に格納する媒体として IC カードが知られている。IC カードは、権限を持たない第三者に対して IC カード内部に格納された情報を漏えいさせない耐タンパー性を備えた媒体である。従来は、高度な公開鍵計算能力を備えた接触型 IC カードに、電子証明書と署名鍵（プライベート鍵）を格納しておき、IC カード内部で電子署名値を計算し、署名鍵（プライベート鍵）を IC カードの外へ出さないことにより、公開鍵基盤（PKI）の信頼性を確実にするという運用が行なわれてきた。この方法は、高度な信頼性を確保できる反面、公開鍵計算能力を備えた接触型 IC カードを必要とするため、コスト面からは電子証明書の普及を阻害する要因の一つとなっている。

JCAN ビジネス証明書は、JCAN から認定された企業／団体の総務部門等が社員／職員に配付し、自社の職員であることを証明する証明書である。手軽に導入でき、リーズナブルなコストで運用できる方法が求められる。JCAN ビジネス証明書は電子認証にも署名にも利用されることから、証明書を配付された社員／職員本人だけが利用できる仕組みを手軽に構築する必要がある。そこで、パソコンのハードディスク内に電子証明書と署名鍵（プライベート鍵）を格納しておき、なおかつ、その利用時には本人だけが所持する利用者認証用媒体を使うことを検討した。そのため、非接触 IC カードを使った ID 証カード・フォーマットとして広く普及しているとして SSFC カードと FCF カードの双方のフォーマットを JCAN パスとして利用するための検討を行い、プロトタイプ実証用 JCAN パスを試作して実証実験を行なった。

1.2 JCAN パス・システムが備えるべき要件

JCAN パスの利用シーンを想定し、PKI 用途での妥当性、業務効率等の観点から、JCAN パス・システムが備えるべき要件を検討した。

JCAN パス・システムが備えるべき要件	要件の概要
(1) 1 枚の JCAN パスから複数の電子証明書へリンクできる	個人に対して発行される証明書と役職に対して発行される証明書がある。
(2) 電子証明書申請発行管理サーバ（仮称）へのアクセス情報	証明書利用時に電子証明書申請発行管理サーバ（仮称）へのアクセスが想定される。
(3) 取得した電子証明書（EE 証明書）の正当性検証	電子証明書申請発行管理サーバ（仮称）から取得した電子証明書の正当性を検証したいという要求に対応。
(4) ID 情報の読み出し効率が高いこと	個人が保持する現在有効な JCAN パスを特定するために必要な ID 情報項目を一度に読み取れることが望ましい。
(5) 1 枚の JCAN パスを物理的セキュリティ（入退室管理等）と PKI で連携利用できること	JCAN ビジネス証明書による電子署名が、どこで署名されたかを証明できる仕組みにより JCAN パスの付加価値を高める。
(6) 既存で流通し利用されている ID 証カード（SSFC カード、FCF カード）をそのまま JCAN パスとして利用できること	社員等に配付済み ID 証カードを回収して再発行する手間をかけずに、そのまま JCAN パスとして利用できることが望ましい。

1.3 JCAN パス・フォーマットの検討

SSFC カードと FCF カードの双方を JCAN パスとして利用できるようにするため、「JCAN パス・サービス（仮称）」を FeliCa プライベート領域に搭載する方式を検討した。

以下のいずれのケースでも JCAN パスとして発行できる。

- SSFC カードを JCAN パスとして発行するケース
- SSFC カード（共通領域版）を JCAN パスとして発行するケース
- FCF キャンパスカードを JCAN パスとして発行するケース

今年度のプロトタイプ実証では、上記の中から SSFC カードをプロトタイプ実証用 JCAN パスとして発行して試作した。

1.4 実証実験

試作したプロトタイプ実証用 JCAN パスを用いて、以下の 3 項目について実証実験を実施し、マルチユース格納媒体の有効性を確認した。

- 入退
- ネットワークログイン
- 電子署名

2　マルチユース格納媒体による実証用身分証明書試作に関する検討

プロトタイプ実証用 JCAN パスの試作に向けた検討では、平成 21 年度「電子認証の民間制度・基盤確立に関する調査研究」報告書（以下、「平成 21 年度報告書」）等を参考に、マルチユース格納媒体のあるべき姿を検討した。

2.1 JCAN パス・システムの要件

ここでは、JCAN パスのコンセプトを説明し、JCAN パスのあるべき姿についての検討結果について述べる。この章では、JCAN パス（非接触 IC カード）と JCAN パスを利用するためのドライバー・ソフトウェア（以下、「JCAN パス用ドライバー・ソフトウェア」）を総称して、「JCAN パス・システム」と呼ぶ。また、この報告書では、LRA からの申請に基づき発行された JCAN ビジネス証明書と署名鍵（プライベート鍵）の対を、配付用にパスワードにより暗号化保護された PKCS#12 形式のデータ・パッケージを「暗号化された電子証明書等」（PKCS#12）と呼ぶ。

2.1.1 JCAN パス

「安信簡」情報環境を実現するために、共通のルールと認定制度に基づきビジネスでの利用に適するように設計された安価で扱いやすく信頼性の高い電子証明書「JCAN ビジネス証明書」の普及促進が必要である。「JCAN パス」は「JCAN ビジネス証明書」の利用環境における業務効率化を支える格納媒体であり、機能としては以下を有するものである。

- ID 情報（社員番号、学籍番号など)、電子証明書を活性化するための情報を格納できる。
- 格納した情報に対して、必要に応じて暗号化及び読み書きへの PIN 認証等によるアクセス制御等のセキュリティ機能を備えている。
- 格納した情報は、必要に応じて、セキュリティ要件を満たせば、その一部を書き換えることができる。
- 必要に応じて、セキュリティ要件を満たせば、後から情報の追加、また一部の情報の削除が行える。
- 基本的なルールを守れば、誰でも実装情報を利用できる。

2.1.2 ベースとなる ID 証フォーマット

JCAN パスとして利用するマルチユース格納媒体のベースとなるフォーマット仕様を検討した。JCAN ビジネス証明書を早期に普及させるためには、社員証・学生証等の ID 証カードとして既に広く普及している ID 証カードフォーマットをベースに JCAN パスとして活用できることが望ましい。ID 証カードは、職場への入退室、出退勤管理等の用途で利用されることから、利便性やコストの面から非接触 IC カードが好まれている。なかでも、日本では交通系 IC カード、電子マネー等の用途で広く普及している FeliCa カードを ID 証として採用する動きが広がっている。そこで、本検討では FeliCa カードベースの ID 証フォーマットとして広く産業界に普及している SSFC カードと、FCF カードの双方を JCAN パスとして利用できることが望ましいと考えた。

2.1.3 JCAN パス・システムが備えるべき要件

JCAN パスの利用シーンを想定し、PKI(Public Key Infrastructure、公開鍵認証基盤)用途での妥当性、業務効率等の観点から、JCAN パス・システムが備えるべき要件を以下にまとめる。

(1) 1 枚の JCAN パスから複数の電子証明書へリンクできる

JCAN ビジネス証明書には、従業員個人に対して発行される証明書と、役職に対して発行される証明書がある。このため、役職者は 1 枚の JCAN パスで複数枚の JCAN ビジネス証明書をハンドリングする必要がある。また、一般に PKI では、電子証明書の有効期限が近づいてくると、新しい証明書が発行されるので、1 つの ID 番号に新旧複数の証明書が紐付けられる必要がある。

JCAN パス用ドライバー･ソフトウェアにて、1 つの ID 番号から複数の電子証明書を紐付けられる(1:n 対応)仕組みを、JCAN パス・フォーマットに持たせる必要がある。

(2) 電子証明書申請発行管理サーバ（仮称）へのアクセス情報

総務部門/教務部門等から JCAN パスを交付された職員が、メーラや業務アプリケーションから JCAN ビジネス証明書を認証や電子署名用途に利用するシーンを想定する。JCAN ビジネス証明書を利用するアプリケーションは、JCAN パス用ドライバー・ソフトウェアを経由して電子証明書申請発行管理サーバ（仮称）へアクセスし、JCAN パス保持者の「暗号化された電子証明書等」（PKCS#12）を取り出すことになる。

電子証明書申請発行サーバ（仮称）と JCAN パス利用者の PC 環境等のネットワーク構成とセキュリティポリシーは、JCAN ビジネス証明書を導入する企業/団体等によって様々な構成が考えられる。JCAN パス･システムは、JCAN パス利用者のアプリケーションから電子証明書申請発行管理サーバ(仮称)へアクセスできるように設計される必要がある。

(3) 取得した電子証明書（EE 証明書）の正当性検証

電子証明書申請発行管理サーバ（仮称）から取得した電子証明書（EE エンド・エンティティ証明書） をそのまま信用して利用することも考えられるが、その正当性を検証したいという要求がセキュリティ要求基準の厳しい利用者企業から求められる可能性もある。このための仕組みについて考慮しておく必要がある。一例として JCAN パス用ドライバー･ソフトウェアにて、JCAN 中間 CA またはルート CA の証明書を用いて、EE 証明書を検証する方法が考えられる。あるいは、JCAN パス・フォーマット内に電子証明書（EE 証明書）のハッシュ値等を格納しておき、JCAN パス用ドライバー・ソフトウェアにて、取得した EE 証明書の整合性を確認する方法も考えられる。

(4) ID 情報の読み出し効率

電子証明書を利用しない認証サービス（例：入退出）で、JCAN パス保持者個人を識別するために、JCAN パス内の ID 情報を利用する。個人が保持する現在有効な JCAN パスを特定するためには、次の 3 項目が必要になる：

- JCAN パスを導入した企業/団体を識別するコード
- 個人を識別する ID 番号
- （再）発行回数

JCAN パスを搭載する格納媒体（非接触 IC カード等）は、一度の読み取りで物理的に取得できるデータ・ブロックのサイズに制限がある。読み取り効率を考慮して、上記 3 項目を一度に読み取れるよう JCAN パス・フォーマットを設計することが望ましい。

(5) 1 枚の JCAN パスを物理的セキュリティ（入退出管理等）と PKI で連携利用

今年度のプロトタイプ実証では、試作したプロトタイプ実証用 JCAN パス 1 枚で、入退、ネットワークログイン、電子署名のマルチユースに活用できることを示した。これらの個々のユースケース場面で JCAN パスを用いるだけでなく、入退室管理の物理的セキュリティと電子証明書の利用(PKI)を有機的に連携させる利用シーンへの展開も考慮して JCAN パス･フォーマットを検討した。

JCAN パス用ドライバー・ソフトウェアがインストールされたノート PC を持っていれば、どこに居ても JCAN パス保持者の「暗号化された電子証明書等」（PKCS#12）を利用して電子署名つき e-mail を発信できる。このユースケースは、モバイル・ユースでの利便性を向上させるが、JCAN パスを用いた電子署名がどの場所でなされたかを証明することはできない。オフィスへの入退室時刻を JCAN パス内に記録しておき、JCAN パス用ドライバー・ソフトウェアが JCAN パス内の入退室記録を確認して、入室状態でなければ JCAN パス保持者の「暗号化された電子証明書等」（PKCS#12）を利用できないといったオプション機能を提供すれば、JCAN の電子署名が付されたデジタル文書について、誰が、どこで署名したかを証明することも可能となり、JCAN ビジネス証明書基盤の有効性、パフォーマンスを更に向上させることができる。JCAN パスに記録する入退室記録情報として、オフィスへの入室時刻を記録するようにしておけば、在社時間、サービス残業有無などの労務管理にも活用することができるのである。

(6) 既存で流通し利用されている ID 証カード（SSFC カード、FCF カード）をそのまま JCAN パスとして利用

JCAN パスのあるべき姿としては、社員等に配付済み ID 証カードを回収して再発行する手間をかけることなく、そのまま JCAN パスとして利用できることが望ましい。既に流通し利用されている（SSFC カードと FCF カードを合計すると）200 万枚を超える非接触 IC カード ID 証を仮想化して JCAN パスのサブセットとして認識させる「仮想 JCAN パス化ドライバ（仮称)」のあり方を検討した。(4.1.2 節参照)

2.2 JCAN パス・フォーマットの検討

2.1.3 節で挙げた JCAN パスが備えるべき要件を念頭に JCAN パスのフォーマットを検討した。

2.2.1 ID 情報と JCAN 認定番号

JCAN パスのフォーマット検討に際し、本調査研究では FeliCa カードベースの ID 証フォーマットとして広く普及している SSFC カードと FCF カードの双方を JCAN パスとして利用できることを要件としている。一般に ID 証カードに搭載される ID 情報には、個人が保持する現在有効な ID 証カードを特定するために、次の 3 項目が必要である：

① 当該 ID 証フォーマットを導入した企業/団体を識別するコード

② 個人を識別する ID 番号

③ （再）発行回数

社員番号/学籍番号等の ID 番号体系（上記②）は、個々の企業/学校で決めているため、同じ ID 証フォーマットを導入している企業/学校の中に、たまたま同じ ID 番号体系を採用しているところがあると、ID 番号の同じ ID 証カードが複数枚世の中に存在してしまう可能性がある。こうした事態を防ぐために、①の企業/団体を識別するコードが必要になるのである。③の（再）発行回数は、紛失した ID 証カードを他人に拾われた場合に、ID 証カード保持者本人へのなりすましを防ぐために、紛失した ID 証カードを無効化する際に必要となる。今回検討対象とした SSFC カードと FCF カードは、ともに標準フォーマットの中に上記 3 項目を規定し[1]、対応した入退室管理システム等で ID 情報として利用されている。

JCAN では LRA 認定を受けた企業/団体に対して「JCAN 認定番号」を付与する。「JCAN 認定番号」は JCAN ビジネス証明書の Subject の OrganizationUnitName1 に格納して配付する。JCAN ビジネス証明書に記載される JCAN 認定番号の構造は、

{1.2.392.200063(JIPDEC の OID)}.{3 桁(区分コード)}.{8 桁(団体識別番号)}.{3 桁(LRA 識別番号)}

で、グローバルに一意の番号となる。

JCAN パスには、JCAN ビジネス証明書導入企業を識別するコードとして「JCAN 認定番号」を格納することとした。SSFC カード、FCF カードの既定の標準フォーマットには「JCAN 認定番号」を格納する空き領域を確保できないため、次節の JCAN パス･サービス（仮称）内に「JCAN 認定番号」を格納することとする。

2.2.2 JCAN パス・サービス（仮称）

SSFC カードと FCF カードの双方を JCAN パスとして利用できるようにするため、JCAN パスとして発行する FeliCa カードには、ID 情報サービスとしての SSFC サービス、FCF サービスとは別に JCAN パス用のサービスとして「JCAN パス・サービス（仮称）」を搭載することとする。

JCAN パスを JCAN の本来の目的に沿って、リーズナブルで低コストの運用を可能とすること

[1] （再）発行回数は、<SSFC 仕様>と<FCF キャンパスカード仕様>では規定されているが、<FCF 一般仕様>では規定されていない。

を第一義に、「JCAN パス・サービス（仮称）」を FeliCa カード上に搭載する際の属性を検討した。「JCAN パス・サービス（仮称）」への FeliCa アクセス制御を「鍵あり」とした場合、JCAN パスをパソコンで利用する際に、FeliCa「鍵あり」アクセスに対応可能なリーダライターが必要となりコスト高となる。FeliCa 共通領域にサービスを追加する場合には、登録手続き、維持管理コストが必要となる。

以上の理由から、「JCAN パス・サービス(仮称)」は、FeliCa カードのプライベート領域に搭載し、このサービスへの FeliCa アクセス制御は Read/Write ともに「鍵なし」とした。「JCAN パス・サービス（仮称）」へ書込むデータは、引き続き検討していく JCAN パス・フォーマット仕様で規定する方法で暗号化して書込む。JCAN パス・フォーマット仕様では、「JCAN パス･サービス（仮称）」に使用するエリア情報、サービスコード、各データ項目の領域情報等を規定する。

JCAN パス導入企業/学校で、「JCAN パス・サービス（仮称）」の他に利用（または利用を予定）している FeliCa カード上のサービスと、JCAN パス・フォーマットで規定する「JCAN パス・サービス（仮称）」のサービスコードが競合する場合には、カード発行仕様を決める際に調整することになる。

「JCAN パス・サービス（仮称）」のデータは暗号化されているため、通常の FeliCa コマンドで読み出してもデータ内容を知ることができない。JCAN パス用ドライバー・ソフトウェア仕様で規定する仕様に準拠した JCAN パス用ドライバー・ソフトウェアを経由しなければデータを読み書きできない。

JCAN パス・サービス領域には JCAN 電子証明書を活性化するための情報として、以下のデータ領域を確保する：

- カード保持者認証用パスワード（PIN）
- 「暗号化された電子証明書等」（PKCS#12）にアクセスするためのパスワード
- JCAN 認定番号
- 電子証明書申請発行管理サーバ（仮称）へのアクセス情報
- オフィスへの入室時刻

カード保持者認証用パスワード（PIN）による PIN 認証に成功していなければ、「暗号化された電子証明書等」（PKCS#12）にアクセスするためのパスワードが格納された領域へアクセスできない仕様とする。

以降の節では、「JCAN パス・サービス（仮称）」を SSFC カード、FCF カードに搭載する場合のケースについて見ていく。

2.2.3 SSFC カードを JCAN パスとして発行するケース

SSFC（Shared Security Formats Cooperation）は、セキュリティ機器メーカー（入退室管理システム、監視カメラ等）や事務機器メーカー（什器、コピー機、シュレッダー等）、さらに PC セキュリティソフトウェア・ベンダー等 220 社以上が参加するアライアンスで、1 枚の SSFC カードを核にしてコストを抑えながら容易にオフィスのセキュリティレベルと利便性を向上させてきた。SSFC に対応した機器は SSFC カードの ID 情報フォーマットを共有しているので、入退室ゲートを正しく通過した SSFC カードを持っていない限り、室内の SSFC 対応機器を利用できないようにする、といった機器連携も可能である。

この節ではFeliCaカードのプライベート領域にSSFCサービスが搭載されたカードに、「JCANパス・サービス（仮称）」を搭載し、JCANパスとして利用するケースを検討する。

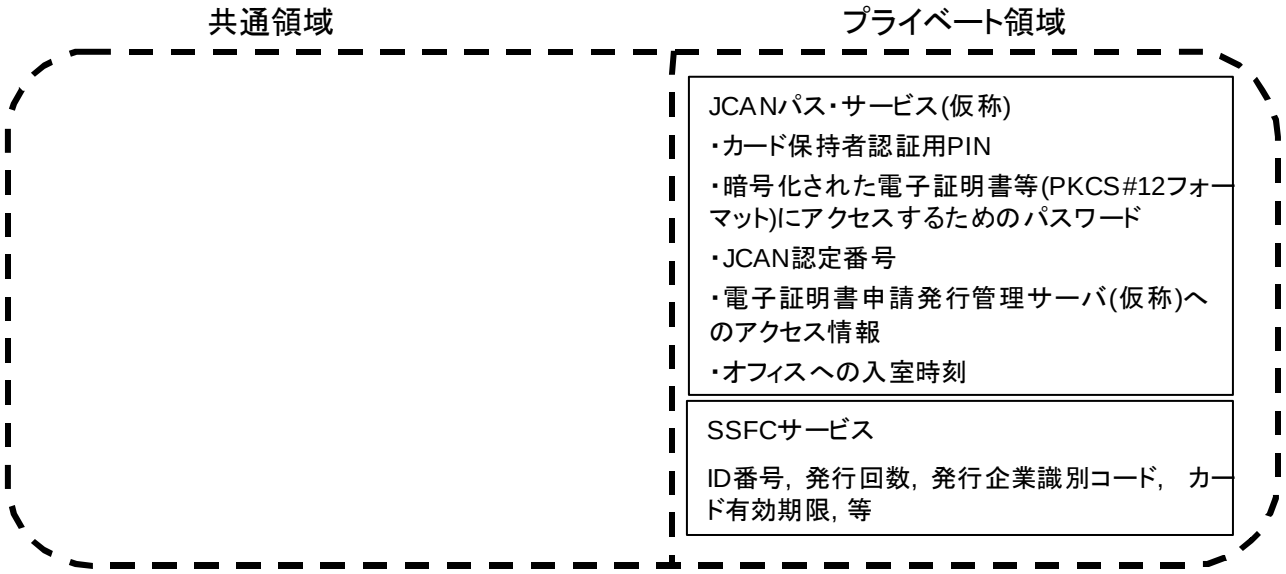


図 2-1

このケースでは、JCANパスのID情報を利用するアプリケーションは、FeliCaプライベート領域のSSFCサービスを1回読込むだけで
発行企業識別コード＋ID番号＋発行回数
が揃い、個人が保持する現在有効なJCANパスを特定することができる。

JCANビジネス証明書を利用するアプリケーション（電子メールソフト等）はJCANパス用ドライバー・ソフトウェアを介してJCANパス・サービス（仮称）にアクセスし、PKI用途でJCANビジネス証明書を活性化するキーとしてJCANパスを利用することができる。

今年度のプロトタイプ実証では、このフォーマットでプロトタイプ実証用JCANパスを試作した。

2.2.4 SSFC カード（共通領域版）を JCAN パスとして発行するケース

交通系 IC カード（Suica、ICOCA、PASMO 等）と SSFC を 1 枚の FeliCa カードに共存させる場合、SSFC サービスを FeliCa 共通領域に搭載することがある。このケースでも、「JCAN パス・サービス（仮称）」を FeliCa プライベート領域に搭載可能である。

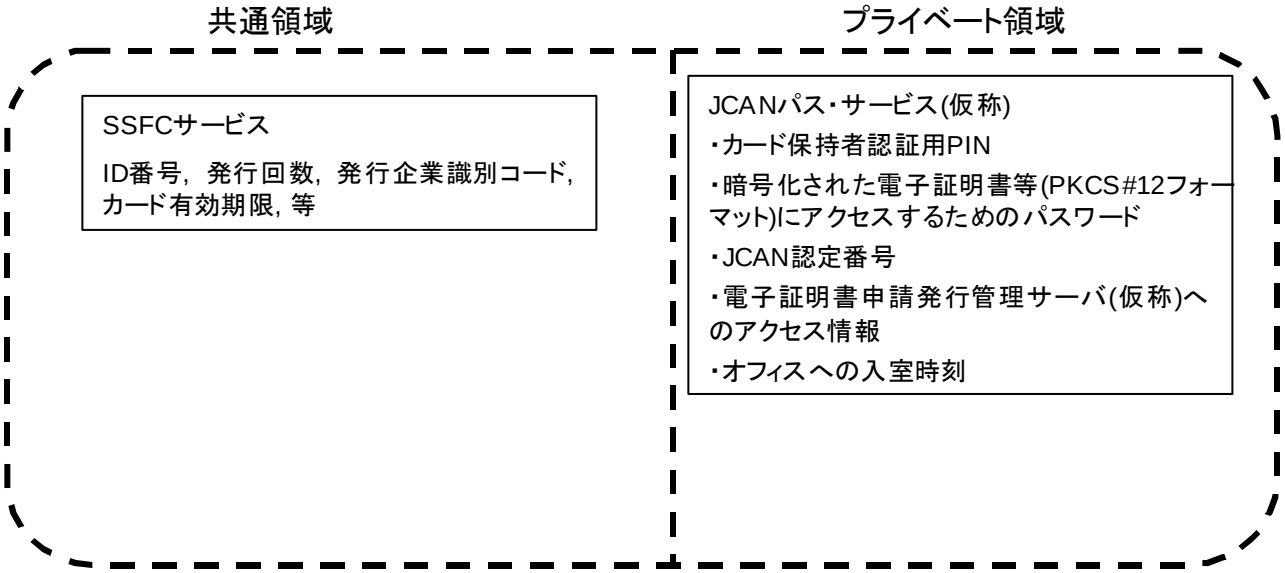


図 2-2

このケースでは、JCAN パスの ID 情報を利用するサービスは、FeliCa 共通領域の SSFC サービスを 1 回読込むだけで

発行企業識別コード＋ID 番号＋発行回数

が揃い、個人が保持する現在有効な JCAN パスを特定することができる。

JCAN ビジネス証明書を利用するアプリケーション（電子メールソフト等）は JCAN パス用ドライバー・ソフトウェアを介して JCAN パス･サービス（仮称）にアクセスし、PKI 用途で JCAN ビジネス証明書を活性化するキーとして JCAN パスを利用することができる。

2.2.5 FCF キャンパスカードを JCAN パスとして発行するケース

学生証用途で採用される事例が多い FCF キャンパスカード仕様の FeliCa カードを JCAN パスとして発行するケースでは、FeliCa 共通領域に FCF サービスの基本サービス（サービス A）を搭載し、プライベート領域に「JCAN パス・サービス（仮称)」を搭載する。

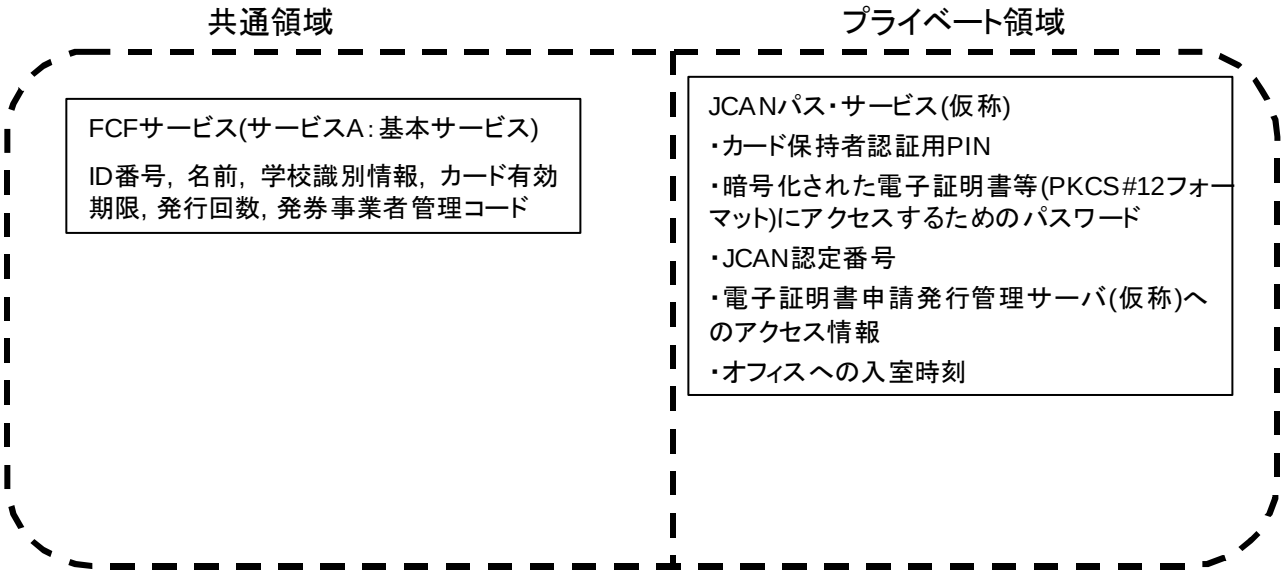


図 2-3

このケースでは､JCAN パスの ID 情報を利用するアプリケーションは､FeliCa 共通領域の FCF サービスの基本サービス（サービス A）を 1 回読込むだけで

学校識別情報＋ID 番号＋発行回数

が揃い、個人が保持する現在有効な JCAN パスを特定することができる。

JCAN ビジネス証明書を利用するアプリケーション（電子メールソフト等）は JCAN パス用ドライバー・ソフトウェアを介して JCAN パス･サービス（仮称）にアクセスし、PKI 用途で JCAN ビジネス証明書を活性化するキーとして JCAN パスを利用することができる。

3　実証用身分証明書によるプロトタイプ実証

JCAN パス・システムの要件、フォーマットの検討結果を踏まえ、今年度のプロトタイプ実証用 JCAN パスを試作した。この章では、プロトタイプ実証用 JCAN パスを用いた、「入退」「ネットワークログイン」「電子署名」の実証結果について述べる。

3.1　プロトタイプ実証用 JCAN パス

今年度のプロトタイプ実証用 JCAN パスとして、2.2 節で検討した JCAN パス・フォーマットの中から、現在 ID 証カードとして市場で広く使われている SSFC カードを JCAN パスとして発行するケースを採用し、プロトタイプ実証用 JCAN パスを試作した。具体的には FeliCa カード（RC-S962）のプライベート領域に「JCAN パス・サービス（仮称)」、「SSFC」、「入退出ゲート・サービス」を搭載した。

JCAN パス・サービス領域には JCAN 電子証明書を活性化するための情報として、以下のデータを搭載した：

- カード保持者認証用パスワード（PIN）
- 「暗号化された電子証明書等」（PKCS#12）にアクセスするためのパスワード

カード保持者認証用パスワード（PIN）による PIN 認証に成功していなければ、「暗号化された電子証明書等」（PKCS#12）にアクセスするためのパスワードが格納された領域へアクセスできない仕様で発行した。

3.2 入退

プロトタイプ実証用 JCAN パスを使って、財団法人日本情報処理開発協会（JIPDEC）のオフィスで入退室の実証を行なうため、JIPDEC オフィスの入退室ゲートベンダーと調整した。

JIPDEC オフィスの入退室管理用ゲートのファームウェア書換えにより、プロトタイプ実証用 JCAN パスの FeliCa プライベート領域に搭載した上記入退室ゲートベンダー固有の「入退出ゲート・サービス」を利用して入退室できることを確認した。

3.3 ネットワークログイン

プロトタイプ実証用 JCAN パスと、大日本印刷製 PC セキュリティソフトウェア「Endpoint Saver F」を使って、以下の環境でネットワークログインの実証を行なった。

テスト機の OS ： Microsoft Windows 7 Professional <日本語 OS>(32bit バージョン)
R/W ： RC-S330/S(ソニー製)、および、SCL010(SCM マイクロシステムズ製)

テスト機には、R/W ベンダー提供の R/W ドライバー･ソフトウェア、大日本印刷製「Endpoint Saver F」、プロトタイプ実証用に開発した JCAN パス用ドライバー・ソフトウェアの順にインストールした。

PC を起動すると「Endpoint Saver F」から IC カードの認証が要求され、プロトタイプ実証用 JCAN パスを R/W にかざすことにより PC へのログオンに成功した。今回の実証では、スタンドアロンの PC にログオンしたが、Windows ネットワークの一部を構成する PC へのログオンでも同様にログオンすることが可能である。

ログオン後、R/W からプロトタイプ実証用 JCAN パスを離すと、図 3-1 のようにスクリーンがロックされ、JCAN パスを R/W に戻すとスクリーンロックが解除された。

R/W は、市場に広く出回っている「PaSoRi」RC-S330/S（ソニー製）と、Windows 環境上でスマートカードを利用するための標準インタフェース「PC/SC 仕様」に準拠した SCL010（SCM マイクロシステムズ製）の 2 種類を使用し、どちらでも問題なく JCAN パスによるネットワークログインとスクリーンロックの制御が可能であることを実証した。

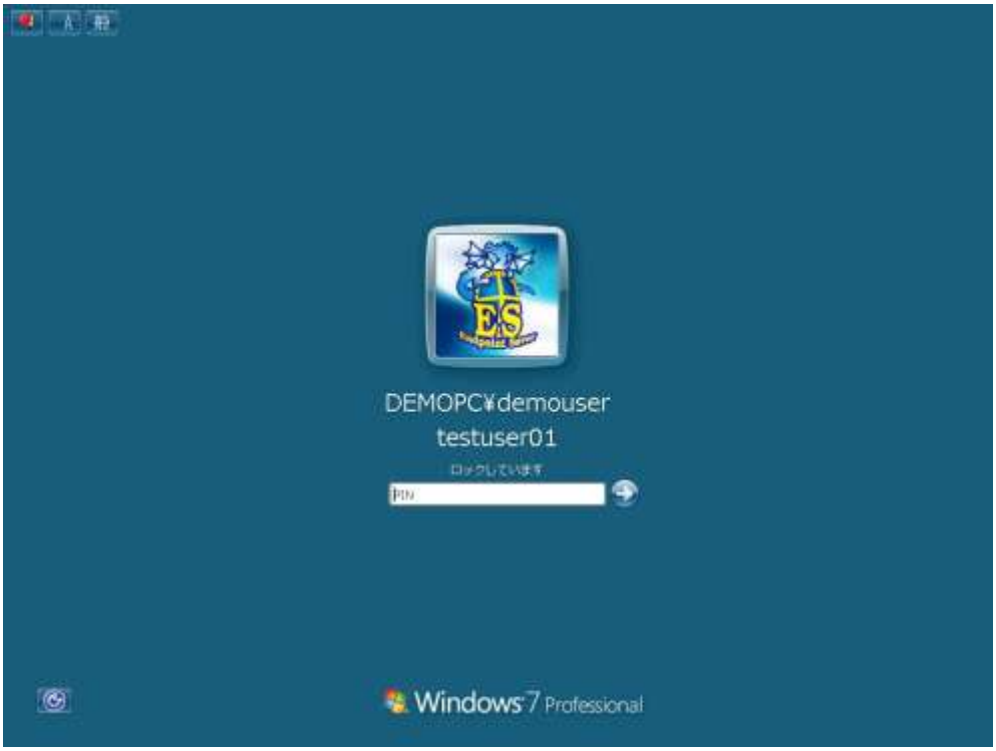


図 3-1 Endpoint Saver F によるスクリーンロック画面

3.4 電子署名

プロトタイプ実証用 JCAN パスを使って、JCAN ビジネス証明書による電子署名機能の実証を行なった。この節では、プロトタイプ実証用に開発した JCAN パス用ドライバー・ソフトウェア（以下、「プロトタイプ実証用 JCAN ドライバー」）について説明し、JCAN ビジネス証明書の申請から社員への配付までの実運用シーンを想定した電子署名機能デモについて説明する。

3.4.1 プロトタイプ実証用ドライバー･ソフトウェア

プロトタイプ実証用 JCAN ドライバーは、プロトタイプ実証用 JCAN パスの「JCAN パス・サービス（仮称）」と「SSFC サービス」にアクセスするライブラリである。

プロトタイプ実証用 JCAN ドライバーは、FeliCa 用 R/W ドライバーを呼び出して FeliCa カ

ードにアクセスする。今回開発したプロトタイプ実証用 JCAN ドライバーは FeliCa 用 R/W として広く普及している PaSoRi 及び、PC/SC 仕様に準拠した R/W をサポートしている。

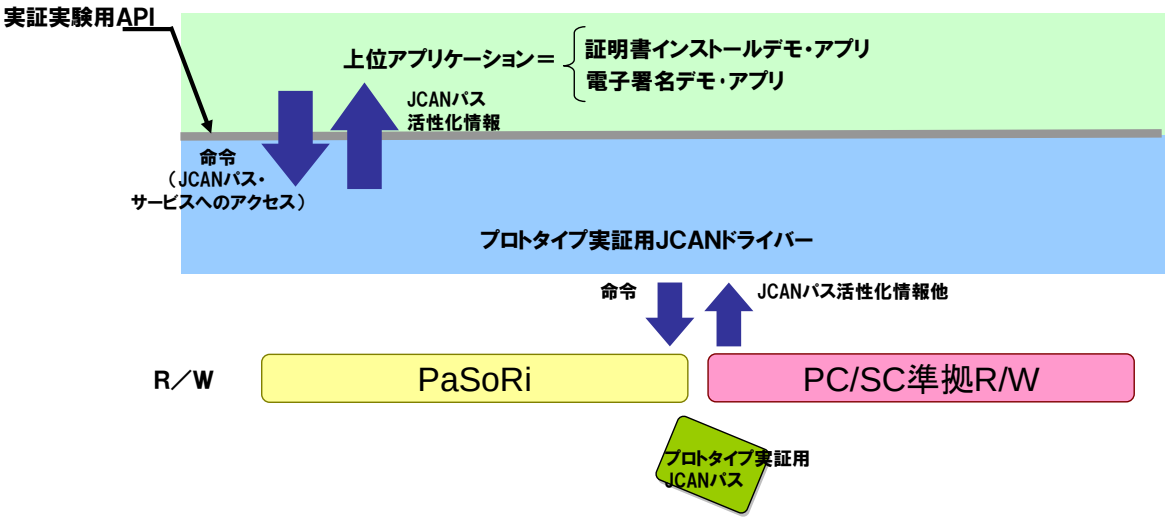


図 3-2

3.4.2 JCAN ビジネス証明書の申請から配付までの運用フロー

今年度の JCAN パス・プロトタイプ実証では、JCAN ビジネス証明書導入企業の総務部門（以下、「LRA オペレータ」）が JCAN パートナーCA へ JCAN ビジネス証明書を申請し、取得した JCAN ビジネス証明書を各社員へ配付するまでの運用フローを以下のように想定した。

(1) JCAN ビジネス証明書の発行申請

LRA オペレータは、JCAN への申請に基づき配付される「暗号化された電子証明書等」（PKCS#12）を保護するためのパスワード（以下「PW1」）を各社員ごと異なる値に設定し、JCAN に対して証明書の発行申請を行う。

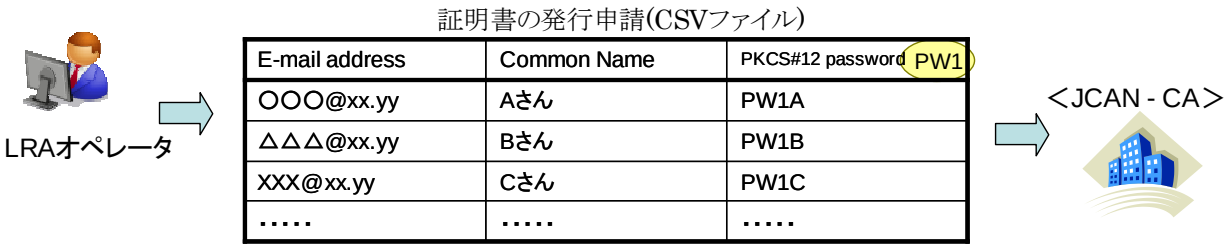


図 3-3

(2) JCAN パスのパーソナライズ

LRA オペレータは、各社員（End Entity）の「PW1」と ID 情報を JCAN パスに書き込んで JCAN パスをパーソナライズする。

JCAN パスの「PW1」が格納された領域にアクセスするためには、8 桁以上の PIN（以下、「PW2」）による PIN 認証に成功しなければアクセスできないように JCAN パスは設計されている。LRA オペレータは、社員ごとに異なる「PW2」の値を設定して各社員用 JCAN パスをパーソナライズする。

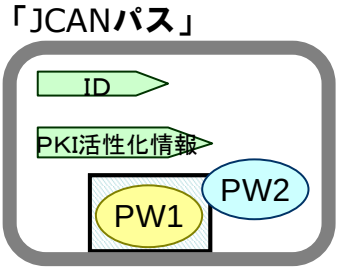


図 3-4

(3) JCAN ビジネス証明書と JCAN パスの配付

LRA オペレータは、JCAN から取得した「暗号化された電子証明書等」（PKCS#12）と JCAN パスを各社員へ「PW2」の値とともに配付する。ただし、「PW1」の値を各社員へは開示しない。

これにより、各社員は「PW1」を知らないので、配付された「暗号化された電子証明書等」（PKCS#12）を各自の PC のローカル証明書ストアに勝手にインストールして利用することはできなくなる。JCAN パスを持っている社員本人だけが、自分の JCAN ビジネス証明書を利用できるのである。

なお、LRA オペレータは「暗号化された電子証明書等」（PKCS#12）を各社員に配付する代わりに、サーバ等のフォルダに格納しておき、各社員には証明書格納フォルダの場所だけを知らせる、という運用も可能である。

3.4.3 JCAN ビジネス証明書のインストール

LRA オペレータから JCAN パスの交付を受け、「PW2」の値を知らされた各社員（End Entity）は、自分の PC への JCAN ビジネス証明書インストール作業を行なう。プロトタイプ実証用デモは、この証明書インストール段階から実施した。

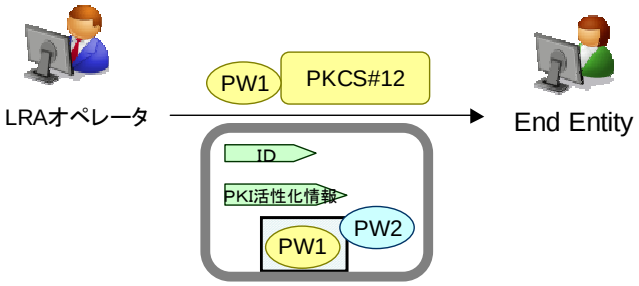


図 3-5

JCAN ビジネス証明書インストール手順は以下のとおり：

(1) 「PW2」を入力し、JCAN パス保持者認証を行なう。

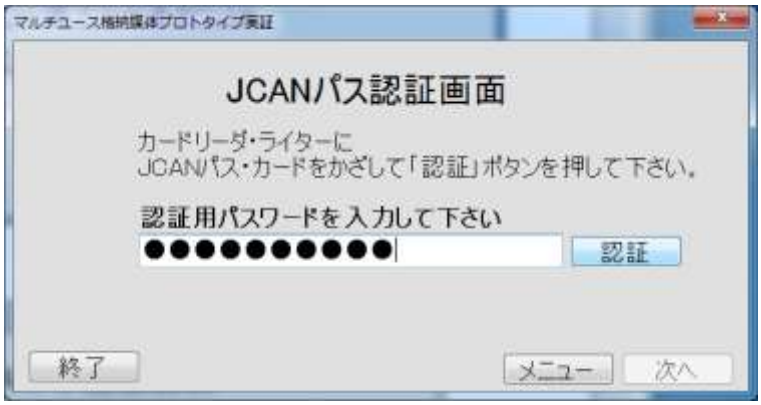


図 3-6 JCAN パス保持者認証画面

(2) LRA オペレータから配付された「暗号化された電子**証明書等**」(PKCS#12)**ファイルを指定して、各社員のパソコンに個人 ID と関連づけて格納する。**

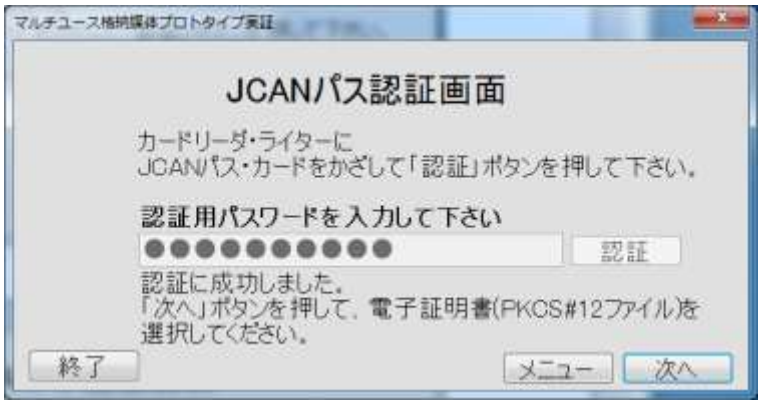


図 3-7 JCAN ビジネス証明書インストール

(3) JCAN パスの PIN 初期値「PW2」を、各社員が自身で設定した値「PW3」(8 桁以上)に変更する運用を推奨するが、必須とはしない。

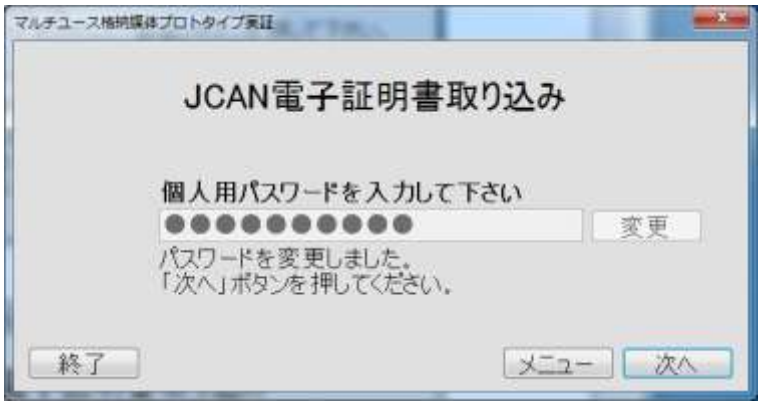


図 3-8 「PW2」から「PW3」への変更

JCAN パスの PIN 初期値「PW2」を、各社員が「PW3」に変更する運用では、社員が「PW3」を失念してしまった場合の対策をあらかじめ講じておく必要がある。たとえば、各社員は JCAN パスの保持者 PIN として設定した「PW3」の値を封筒に密封して LRA オペレータに預託しておくという運用が考えられる。遠隔地に事業所が散在し、この運用が現実的でないケースでは、LRA オペレータが遠隔地から、認証手続きを経て JCAN パスの保持者 PIN を解除できる管理者用プログラムの導入も考えられる。

3.4.4 JCAN ビジネス証明書を利用した電子署名

「暗号化された電子証明書等」（PKCS#12）は、各社員のパソコンに個人 ID と関連づけて格納されており、そのパスワードは JCAN パスの中に格納されているので、JCAN パス保持者本人だけが自分の「暗号化された電子証明書等」（PKCS#12）を利用することができる。

今年度のプロトタイプ実証デモでは、JCAN パス保持者が自身の「暗号化された電子証明書等」（PKCS#12）を利用して任意のファイルに電子署名を付すデモ・プログラムを作成して実証した。

(1) 「PW2」（「PW3」に変更されている場合は「PW3」）を入力し、JCAN パス保持者認証

(2) 電子署名対象ファイルと署名値の出力ファイルを指定し、「署名する」ボタンをクリックすることにより、電子署名デモ・プログラムは JCAN パスから「PW1」を読み出し、「暗号化された電子証明書等」（PKCS#12）から署名鍵（プライベート鍵）を取り出して、署名対象ファイルの電子署名値を計算することにより、電子署名機能を実証した。

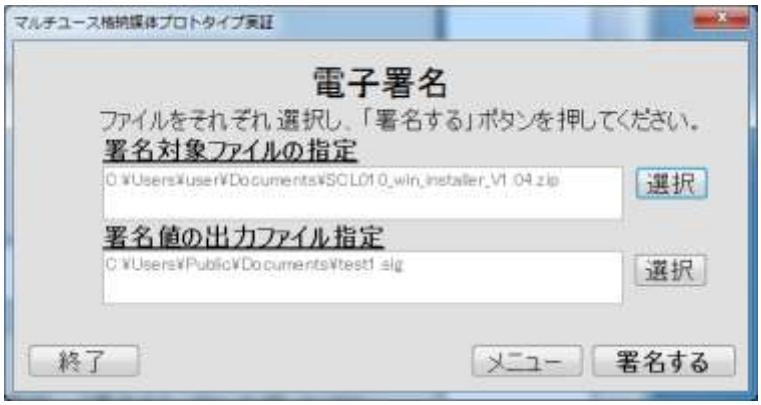


図 3-9 電子署名機能

3.5 プロトタイプ実証の結果考察

試作したプロトタイプ実証用 JCAN パスにより、1 枚のマルチユース格納媒体を、入退室管理、ネットワークログイン、電子署名（JCAN ビジネス証明書の活性化・利用）に利用できることを実証した。

4　課題

この章では、今年度のプロトタイプ実証を通じて浮き彫りにされた JCAN パス事業化に向けた課題と解決方針について記述する。

4.1 JCAN パス用ドライバー・ソフトウェア

今年度のプロトタイプ実証で開発したプロトタイプ実証用 JCAN ドライバーは、上位アプリケーション（JCAN 電子証明書インストールデモ・アプリ、電子署名デモ・アプリ）に対して、実証実験用の独自 API を提供した。この節では、JCAN パスを PKI 用途で広く普及させるために JCAN パス用ドライバー･ソフトウェアが対応すべき課題について整理する。これらの課題を踏まえて、JCAN パス用ドライバー・ソフトウェア仕様を引き続き検討していく。

4.1.1 PKI アプリケーション向け標準 API の提供

Outlook Express や Windows Live Mail、Mozilla Thunderbird などの Windows 環境で広く使われている電子メールソフトが電子証明書格納媒体にアクセスする際には、CSP や PKCS#11 といった、PKI アプリケーションで標準的に利用される API を利用する。このため、JCAN パス用ドライバー・ソフトウェアは CSP や PKCS#11 といった、PKI 標準 API を提供する必要がある。このための要求機能、ドライバーの構成を検討した。

JCAN パスの媒体としては、FeliCa カード以外にも TypeA など複数種類の非接触 IC カード媒体に展開していくことが考えられる。このため、複数の非接触 IC カード媒体に対応した PKI ドライバーを効率良く開発するため、以下の 2 階層構造を検討した。

(1) 下位層：Windows ライブラリ for JCAN パス（仮称）

TypeA と FeliCa の 2 種類の非接触 IC カード媒体を自動認識し、媒体の種類によらず同一の API で、JCAN パスの ID 情報および電子証明書の読み出しと、署名鍵（プライベート鍵）を用いた電子署名を行なうことができる。

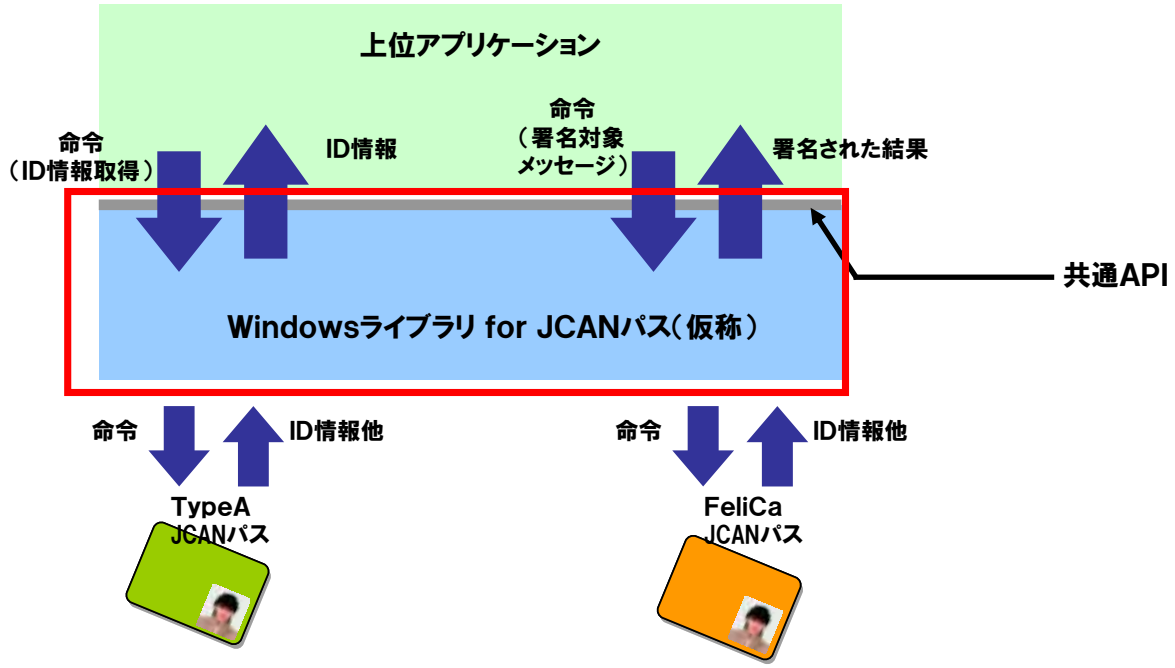


図 4-1 Windows ライブラリ for JCAN パス（仮称）

(2) 上位層：JCAN パス対応 Windows 用 PKI ドライバー

前項に記載の Windows ライブラリ for JCAN パス（仮称）を呼び出し、上位アプリケーション（電子メールソフト、ブラウザ等）に対して PKI 標準 API である CSP と PKCS#11 を提供する PKI ドライバーである。

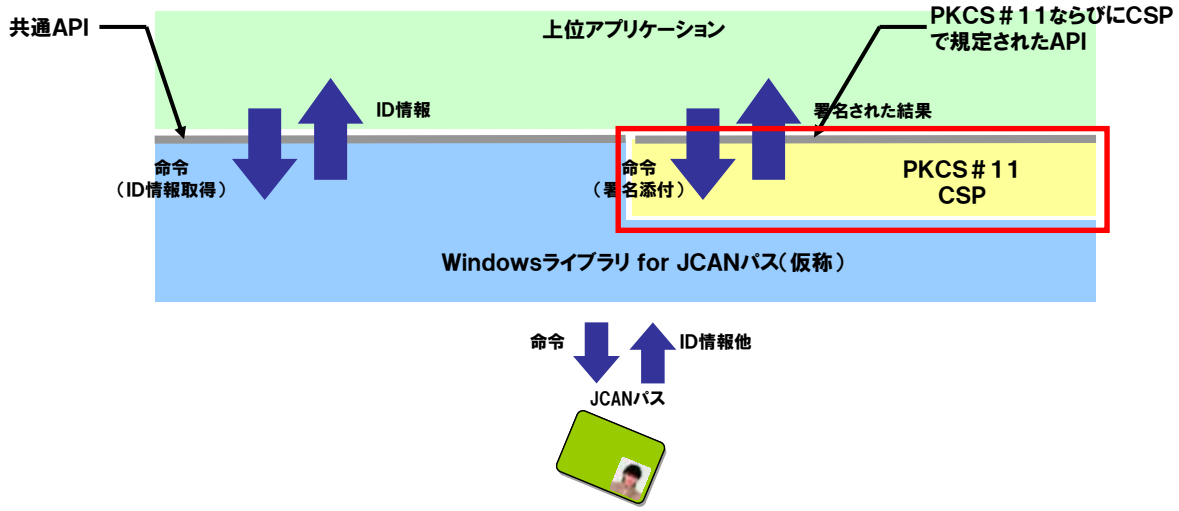


図 4-2 JCAN パス対応 Windows 用 PKI ドライバー

4.1.2 既に配付済の ID 証カードを JCAN パスとして利用

既に流通し利用されている 220 万枚以上の SSFC カード、FCF カードを、回収して JCAN パス・サービス（仮称）を書き込むことには、実運用上さまざまなハードルが考えられる。

この課題を解決するためには、配付済の SSFC カード、FCF カードに、追加書き込みすることなく、そのままで仮想化して JCAN パスの“サブセット”と認識させるドライバーとして『仮想 JCAN パス化ドライバー』（仮称）が望まれる。

JCAN ビジネス証明書の格納先、PKCS#12 パスワードなどをサーバ等で管理させ、署名鍵（プライベート鍵）演算を代替させることにより JCAN パス仮想化の実現可能性を検討した。仮想 JCAN パス化ドライバー自身の中に、アクセスするサーバ等を特定する情報を格納することになる。

仮想 JCAN パス化ドライバーがアクセスするサーバー・システムは、JCAN ビジネス証明書の交付を受けた組織の LRA（総務部門）の管理下にあることが望ましく、プリンタ複合機（MFP）の活用も検討していくべきである。

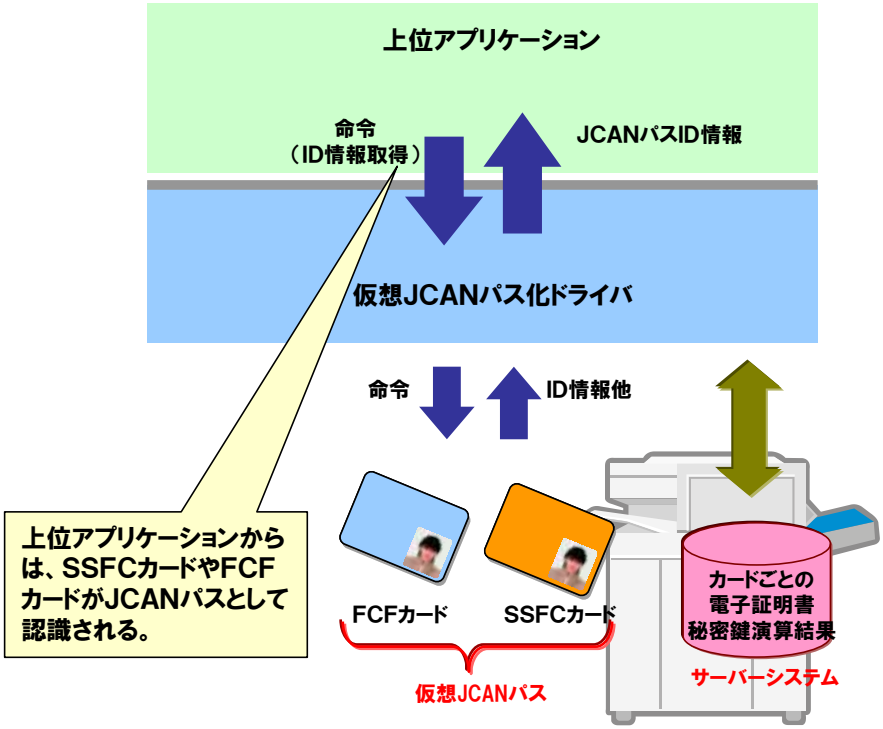


図 4-3 仮想 JCAN パス化ドライバ概念図

4.2 JCAN パスの国際展開へ向けて

JCAN ビジネス証明書の交付を受けた組織の LRA（総務部門）は、JCAN から交付された全社

員分の JCAN ビジネス証明書を電子証明書申請発行管理サーバ（仮称）の共有フォルダ等に置いて、各社員がそのフォルダにアクセスして JCAN ビジネス証明書を利用するケースが一般的と考えられる。また、4.1.2 節で述べた仮想 JCAN パス化ドライバーもサーバ･システムへアクセスすると考えられる。

これらのサーバ･システムは JCAN ビジネス証明書の交付を受けた組織の LRA（総務部門）の管理下にあることが望ましい。サーバー・システムの運用メンテナンスの負荷を考えると、プリンタ複合機（MFP）の活用も検討していくべきである。なぜならば、プリンタ複合機（MFP）は内部に大容量のハードディスクと制御用 CPU を備え、サーバー・システムとみなすことができるからである。幸い、プリンタ複合機（MFP）業界は世界シェアで見ても日本メーカーが大きなシェアを持っている。プリンタ複合機（MFP）を電子証明書申請発行管理サーバ（仮称）として活用していくための検討が次年度以降に望まれる。

4.3 電子マネーとの共存

今年度のプロトタイプ実証では、1 枚の JCAN パスを、入退室管理、ネットワークログイン、電子署名（JCAN ビジネス証明書の活性化・利用）に利用できることを実証した。JCAN パスに電子マネーも搭載することにより、福利厚生面でも JCAN パスを活用できるので、JCAN パスの更なる普及に資することができる。

国内外の各種電子マネーは、搭載される媒体が限定されていたり、バリュー発行者、電子マネーのスキームオーナーとの契約を要したりするなど、さまざまな技術的課題、ビジネス的な課題がある。

JCAN パスを発行する際には、カード製造会社と相談していただき、電子マネーを搭載するための申請手順、各種手続きなどを把握し、余裕を持った発行スケジュールで進める必要がある。

D「登録業務のプロトタイプ実証」

目次

1 はじめに

事業の背景および目的

日本の労働力人口が減少する一方で、出産・育児・介護などで思うような就業ができず本来発揮できる能力を発揮できていない方も多くなっている。またインターネット社会においても未だ大多数の社会人は都市圏への通勤のためストレスを蓄積すると同時に、交通手段の過密化による CO2 の排出拡大、大都市圏への資源偏重という問題も抱えている。

昨今、既にビジネスにおいて当然にインターネットを活用するようになった。今後はビジネスへの活用を更に発展させ、社会全体の最適化を促すことができる環境が整ってきたと言える。

そこで特に日本全国で約 5500 万人強の給与取得者及び約 380 万件弱の従業員を雇用する事業者の双方にとってより合理的で生産性の高い、安心・安全なビジネスインフラを広く活用できる基盤の構築を目指した。

事業の内容

株式会社スマイルワークスで企画・開発・運用を行っている ClearWorks（財務会計・給与計算・販売管理の SaaS 型統合業務システムサービス）の「給与ワークス」をカスタマイズ・拡張した上で従業員がネットワークまたはインターネットを介して電子認証を通じて、勤怠管理・給与計算などの実務に活用できる基盤の実証を行った。

事業の期待

本事業は次のような点を期待している。

(1) 従業員管理と ID 管理・認証管理の統一による合理化
(2) 従業員の勤怠管理の合理化
(3) 従業員が利用する各種システムなどへの SSO などの実現
(4) （電子証明書を FeliCa などに格納すれば）入退出管理と勤怠管理の統一管理
(5) （更にカスタマイズは必要ですが）給与明細書を安心・安全に個別に PDF 配信
(6) 外部とのコミュニケーションや取引においても従業員認証情報の参照を実現
(7) その他、社会保険や労働保険、源泉取得税などとの連動を実現

実証の方法と結果概要

SaaS 型統合業務システムサービスである「ClearWorks」から JCAN ビジネス証明書の登録業務で使われる「管理台帳」に必要なデータを生成する環境を試作し、実証する調査研究を行うため、以下の方法を用いて行った。

(1) 財務会計･給与計算･販売管理の SaaS 型統合業務システムサービスである「ClearWorks」の機能拡張を行い、従業員マスター情報に JCAN ビジネス証明書の発行申請に必要な情報を格納できる拡張を試作する。

(2) 拡張された従業員マスター情報の管理画面から、業務管理者が JCAN ビジネス証明書の発行に必要なデータを所定の形式で出力できる機能を試作する。

(3) 発行された電子証明書を使って「ClearWorks」にログイン認証することができるように ClearWorks の認証機能を試作する。

本研究により、実際の SaaS 型業務アプリーションより、JCAN ビジネス証明書発行に必要な情報の出力が可能となり、企業の従業員データと発行申請情報の連携による情報管理の一元化が可能であることが実証された。

1　概要

1.1　プロトタイプ実証の目的

企業の従業員と雇用する事業者の双方にとってより合理的で生産性の高い、安心・安全なビジネスインフラを広く活用頂ける基盤の構築を目指し、実際の業務システムに登録されている社員情報と JCAN ビジネス証明書申請情報を効率的に管理するシステムのプロトタイプ構築による実証実験を行った。

1.2　本実証研究のスコープ

本実証研究では、「電子認証の民間制度基盤調査報告書」の「登録業務のフロー」の一部（登録業務）をスコープとして実証研究を行った。

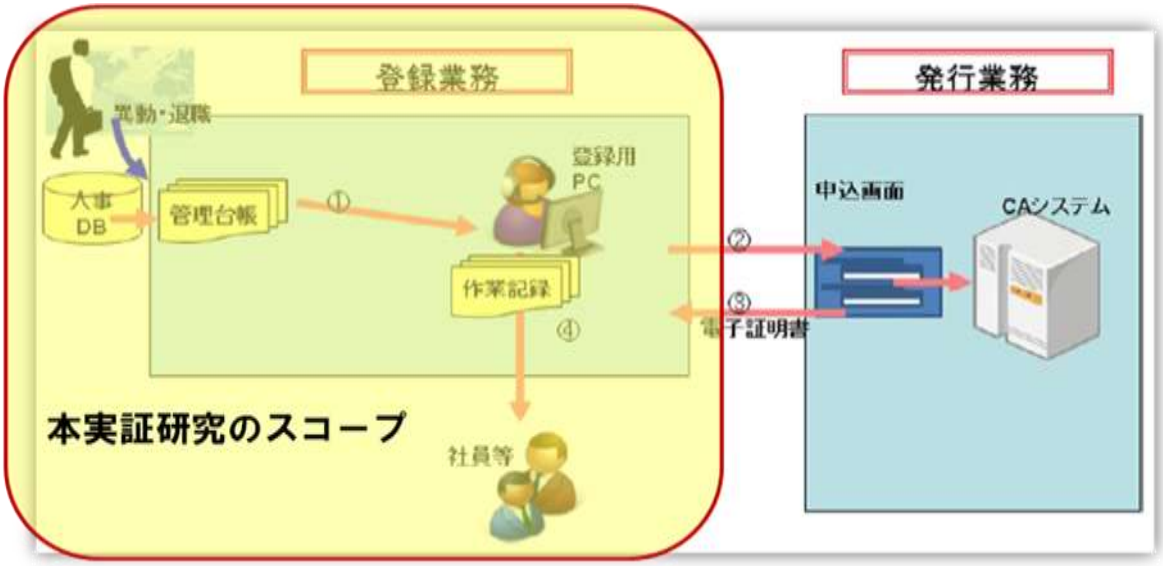


図 1-1　登録業務のフロー（電子認証の民間制度基盤調査報告書より）

1.3 プロトタイプ実証の方法

SaaS 型統合業務システムサービスである「ClearWorks」から、JCAN ビジネス証明書の登録業務で使われる「管理台帳」に必要なデータを生成する環境を試作し、実証する調査研究を行うため、以下の方法を用いて行った。

- 財務会計・給与計算・販売管理の SaaS 型統合業務システムサービスである「ClearWorks」の機能拡張を行い、従業員マスター情報に JCAN ビジネス証明書の発行申請に必要な情報を格納できる拡張を試作する。

- 拡張された従業員マスター情報の管理画面から、業務管理者が JCAN ビジネス証明書の発行に必要なデータを所定の形式で出力できる機能を試作する。

- 発行された電子証明書を使って「ClearWorks」にログイン認証することができるように ClearWorks の認証機能を試作する。

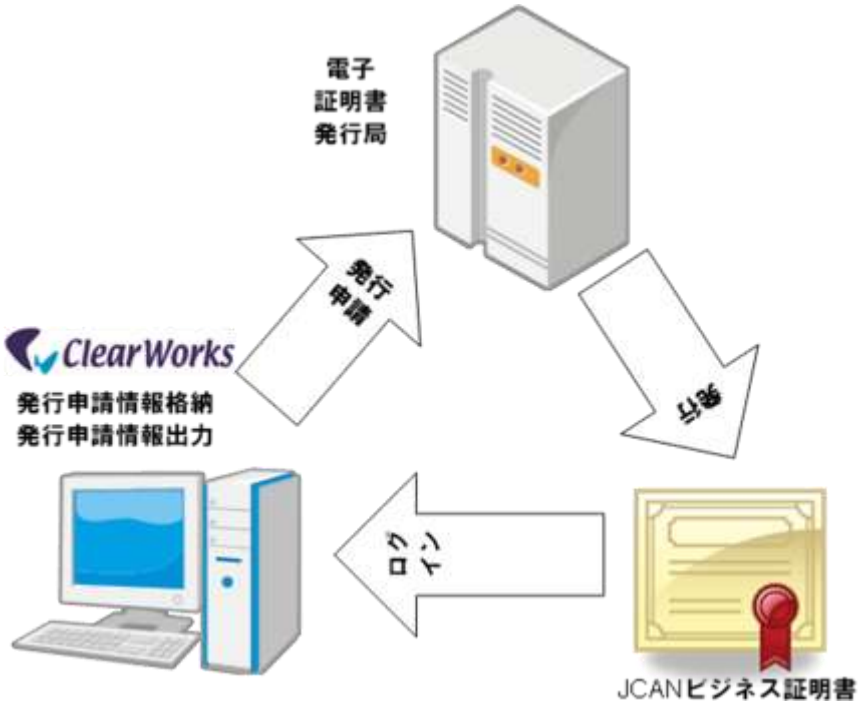


図 1-2　実証イメージ

1.4 実装方法の検討

登録業務では JCAN ビジネス証明書発行申請を行うための CSV ファイルを CSB（電子証明書発行局）の申込み画面よりアップロードすることを想定し、実証検収プロトタイプシステムより直接 CSV ファイルを出力する方法（A ルート）と、汎用的な管理台帳を介する方法（B ルート）で検討を行い、今回は汎用性を考慮し後者（B ルート）で実装を行うこととした。

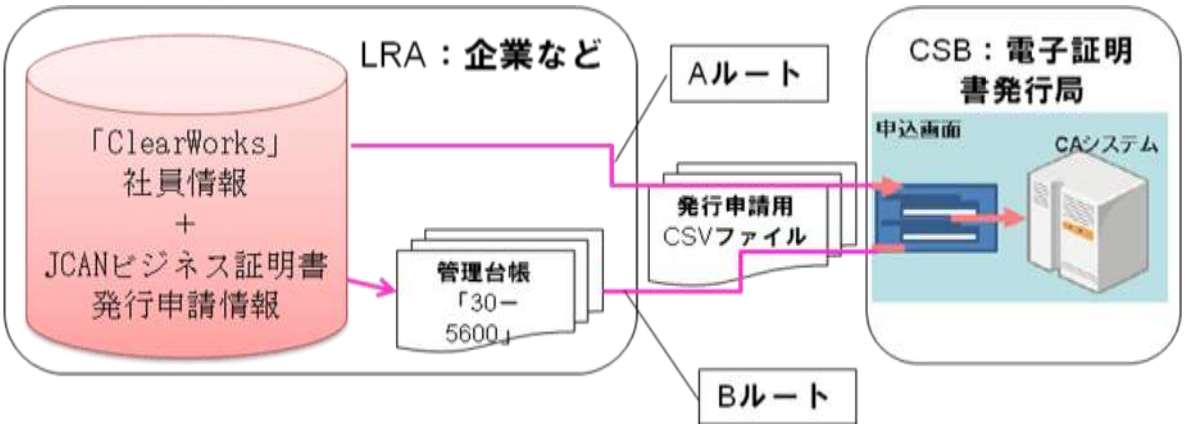


図 1-3　実装方法の検討ルート

1.5 実証結果

本プロトタイプシステムにより、EXCEL 上で社員台帳上の JCAN ビジネス証明書発行申請情報を「30-5600」管理台帳へペーストすることで発行申請が可能となり、社員情報と管理台帳情報の効率的な管理を実現することが実証された。

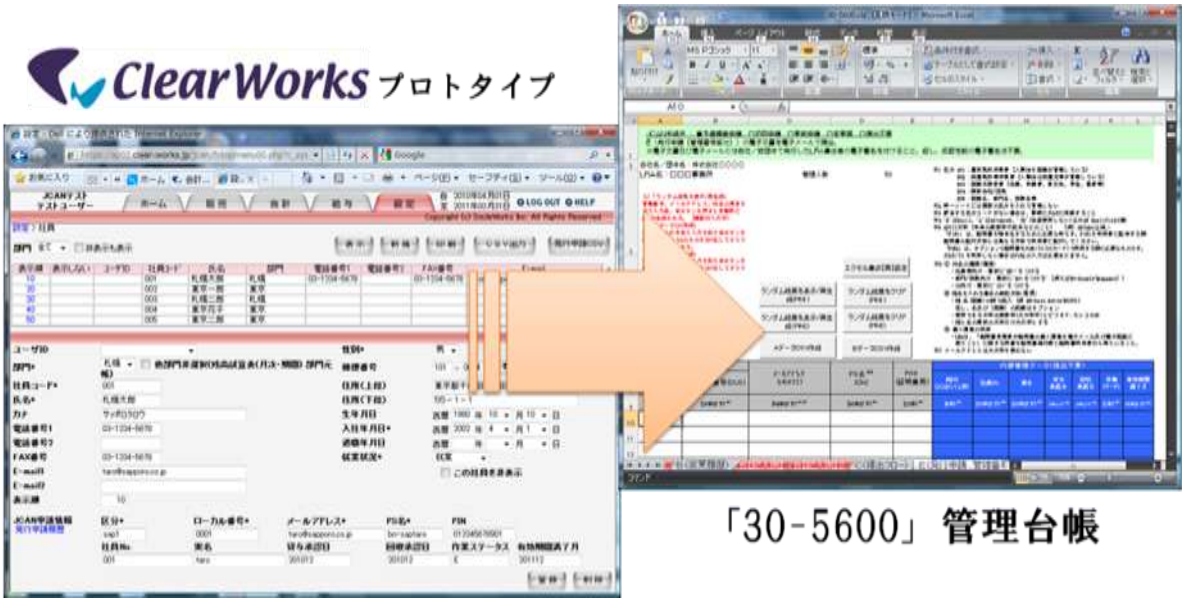


図 1-4　登録業務フローイメージ

1.6 実運用に向けての課題

本実証研究において、実運用されている業務システムの社員情報と電子証明書情報を紐づけて管理することが可能であることの実証を行ったが、実運用に向けては以下のような課題について更なる検討を要する。

① 実運用時には、より効率的な発行申請を実現するために、今回の実装方法（B ルート）以外にも直接 CSB にアップロード可能なフォーマット（A ルート）での出力機能実装の為の検討

② 発行申請情報の追加・削減等への対応検討

③ 発行申請情報をより効率的に登録するための機能強化（OCR 用紙からの入力、電子メールなど電子情報からの自動登録など）の検討

④ 紙印刷コストの削減のために、業務システムが出力する帳票（見積、受発注、請求書など）への電子証明書の添付機能の実装のための検討

⑤ JCAN パス使用者の為の、JCAN パスドライバ対応実装の検討

2　JCAN ビジネス証明書発行申請情報保持機能

SaaS 型統合業務システムサービス ClearWorks の社員台帳マスターを拡張し、JCAN ビジネス証明書発行申請に必要な情報を登録、格納する機能を追加する。これにより、既存の社員マスター情報に JCAN ビジネス証明書発行申請情報をリンクさせることで、一元的な管理が可能となる。

2.1　社員台帳画面構成

ClearWorks 社員台帳画面に対し、「JCAN 発行申請情報項目」の追加を行った。

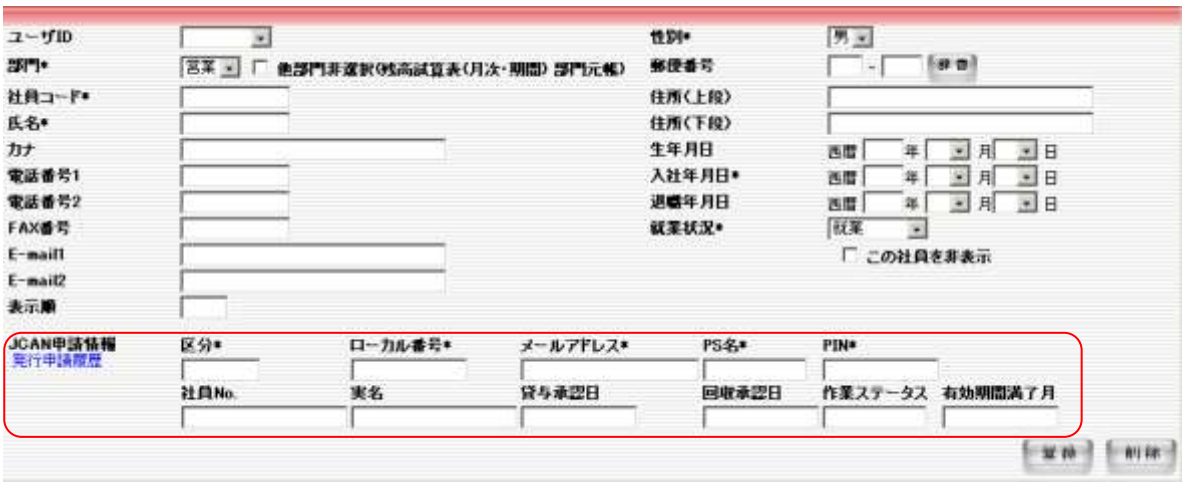
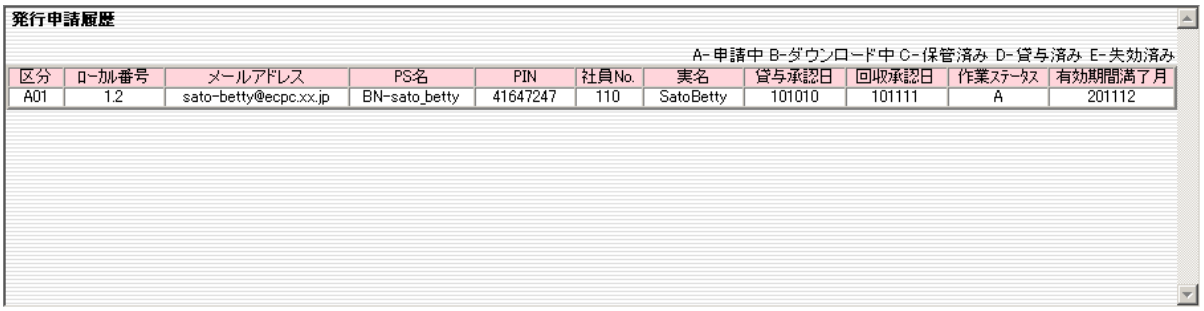


図 2-1　JCAN 申請情報項目

2.2　発行申請履歴

社員台帳明細項目の発行申請履歴リンクをクリックにより、発行申請履歴ページが別ウィンドウで表示する機能を追加した。



区分	ローカル番号	メールアドレス	PS名	PIN	社員No.	実名	貸与承認日	回収承認日	作業ステータス	有効期間満了月
A01	1.2	sato-betty@ecpc.xx.jp	BN-sato_betty	41647247	110	SatoBetty	101010	101111	A	201112

図 2-2　発行申請履歴ウィンドウ

2.2.1 発行申請履歴テーブル

```
--
-- JCAN登録申請情報履歴追加
-- PostgreSQL database
--
--  JCAN登録申請情報履歴(c_jcan_historyテーブル)作成
--
DROP TABLE IF EXISTS c_jcan_history;
DROP SEQUENCE IF EXISTS c_jcan_history_id_seq;

--
-- Name: c_jcan_history Type: TABLE Owner: fxsystem
--
CREATE TABLE c_jcan_history (
        id                      serial,                                 -- 登録申請情報履歴
ID
        emp_id                  integer NOT NULL,                       -- 社員ID
        jcan_segment            character varying(4) NOT NULL,                  -- 区分
        jcan_localnumber        character varying(16) NOT NULL,                 -- ローカ
ル番号
        jcan_email                      character varying(64) NOT NULL,
        -- メールアドレス
        jcan_ps                 character varying(32) NOT NULL,                 -- PS名
        jcan_pin                character varying(32),                  -- PIN
        jcan_number             character varying(20),                  -- 社員No.
        jcan_name               character varying(20),                  -- 実名
        jcan_rentdate           character varying(6),                           -- 貸与承
認日
        jcan_returndate         character varying(6),                           -- 回収承
認日
        jcan_status             character varying(1),                           -- 作業ス
テータス
        jcan_validmonth         character varying(6),                           -- 有効期
間満了月
        add_user                character varying(20),                  -- 新規登録者
        add_date                timestamp with time zone,               -- 新規登録日
        upd_user                character varying(20),                  -- 最新更新者
        upd_date                timestamp with time zone,               -- 最終更新日
        CONSTRAINT                      c_jcan_history_pkey Primary Key (id)
);
ALTER TABLE c_jcan_history OWNER TO fxsystem;

--
-- Name: c_jcan_history; Type: ACL; Schema: public; Owner: fxsystem
--
REVOKE ALL ON c_jcan_history FROM PUBLIC;
REVOKE ALL ON c_jcan_history FROM fxsystem;
GRANT ALL ON  c_jcan_history TO fxsystem;
GRANT ALL ON  c_jcan_history TO GROUP fxsystem;
GRANT SELECT,INSERT,DELETE,UPDATE ON c_jcan_history TO GROUP fxuser;

COMMENT ON COLUMN "c_jcan_history"."id"                                 IS '登録申請情報履歴
ID';
COMMENT ON COLUMN "c_jcan_history"."emp_id"                     IS '社員ID';
COMMENT ON COLUMN "c_jcan_history"."jcan_segment"                       IS '区分';
COMMENT ON COLUMN "c_jcan_history"."jcan_localnumber"                   IS 'ローカル番号';
COMMENT ON COLUMN "c_jcan_history"."jcan_email"                 IS 'メールアドレス';
COMMENT ON COLUMN "c_jcan_history"."jcan_ps"                    IS 'PS名';
COMMENT ON COLUMN "c_jcan_history"."jcan_pin"                   IS 'PIN';
COMMENT ON COLUMN "c_jcan_history"."jcan_number"                        IS '社員No.';
COMMENT ON COLUMN "c_jcan_history"."jcan_name"                  IS '実名';
```

2.3 登録、保持項目

JCAN ビジネス証明書発行申請情報保持機能で保持される項目は以下の通りである。

表 2-1 JCAN 発行申請情報項目

項目名	仕様	サンプル	備考
区分	ASCII 文字 4 文字以下	A01	追加
ローカル番号(OU2)	ASCII 文字 16 文字以下	1.2	追加
メールアドレス(rfc822)	ASCII 文字 64 文字以下	Sato-betty@ecpc.xx.jp	追加
PS 名(CN)	ASCII 文字 32 文字以下	BN-sato_betty	追加
PIN	ASCII 文字 12 文字以下	41647247	追加
以下管理情報			
社員 No.	ASCII 文字 20 文字以下	110	追加
実名	ASCII 文字 20 文字以下	SatoBetty	追加
貸与承認日	ASCII 文字 6 文字以下	101010	追加 YYMMDD 西暦
回収承認日	ASCII 文字 6 文字以下	101111	追加 YYMMDD 西暦
作業ステータス	ASCII 文字 1 文字(A-E)	A	追加 A 申請中 B ダウンロード中 C 保管済み D 貸与済み E 失効済み
有効期間満了	ASCII 文字 6 文字以下	201112	追加 YYYYMM

2.4 登録時検証項目

社員台帳画面で登録または更新される際、必須項目や文字数制限などのチェックを行い、規定外の場合はメッセージを表示し、正しい内容で登録する機能を追加した。

表 2-2 登録、更新時検証項目

項目名	検証条件	メッセージ
区分	必須	区分を入力してください。
	ASCII 文字のみ	区分に ASCII 文字のみ入力してください。
	4 文字以下	区分は ASCII 文字 4 桁以内で入力してください。
ローカル番号(OU2)	必須	ローカル番号を入力してください。
	ASCII 文字のみ	ローカル番号に ASCII 文字のみ入力してください。
	16 文字以下	ローカル番号は ASCII 文字 16 桁以内で入力してください。
メールアドレス (rfc822)	必須	メールアドレスを入力してください。
	メール形式	メールアドレスに正しいメールアドレスを入力してください。
	64 文字以下	メールアドレスは ASCII 文字 64 桁以内で入力してください。
PS 名(CN)	必須、ASCII 文字 32 文字以下	PS 名を入力してください。
	ASCII 文字のみ	PS 名に ASCII 文字のみ入力してください。
	32 文字以下	PS 名は ASCII 文字 32 桁以内で入力してください。
PIN	ASCII 文字のみ	PIN に ASCII 文字のみ入力してください。
	12 文字以下	PIN は ASCII 文字 12 桁以内で入力してください。
社員 No.	ASCII 文字	社員 No.に ASCII 文字のみ入力してください。
	20 文字以下	社員 No.は ASCII 文字 20 桁以内で入力してください。
実名	ASCII 文字	実名に ASCII 文字のみ入力してください。
	20 文字以下	実名は ASCII 文字 20 桁以内で入力してください。
貸与承認日	YYMMDD 形式	貸与承認日に日付を YYMMDD 形式で入力してください。
	不正な日付	貸与承認日に正しい日付を入力してください。
	6 文字以下	貸与承認日に日付を YYMMDD 形式で入力してください。
回収承認日	YYMMDD 形式	貸与承認日に日付を YYMMDD 形式で入力してください。
	不正な日付	貸与承認日に正しい日付を入力してください。
	6 文字以下	貸与承認日に日付を YYMMDD 形式で入力してください。
作業ステータス	A から E	作業ステータスには A から E を入力してください。
	1 文字	作業ステータスには A から E を入力してください。
有効期間満了	YYYYMM 形式	有効期間満了月に日付を YYYYMM 形式で入力してください。
	不正な日付	有効期間満了月に日付を YYYYMM 形式で入力してください。
	6 文字以下	貸与承認日に日付を YYMMDD 形式で入力してください。

3　JCAN ビジネス証明書発行申請出力機能

JCAN ビジネス証明書発行申請情報保持機能により格納された発行申請情報を CSV ファイルとして出力し、自動的に Microsoft EXCEL にて表示する。これにより、管理台帳へのコピー／ペーストを可能にする。

3.1　社員台帳画面構成

ClearWorks 社員台帳画面に対し、「発行申請情 CSV」ボタンの追加を行った。

図 3-1　発行申請 CSV ボタン

3.2　出力 CSV

発行申請 CSV ボタンクリックにより、以下の項目を JCAN 発行申請情報より抽出し CSV ファイルとして出力を行う。

区分,

ローカル番号,

メールアドレス,

PS 名,

PIN,

社員 No.,

実名,

貸与承認日,

回収承認日,

作業ステータス,

有効期間満了月

例：“A01”,”1.2”,”sato-bety@ecpc.xx.jp”,”BN-sato_betty”,””,”110”,”SatoBetty”,”101010”,”101111”,”A”,”201112”

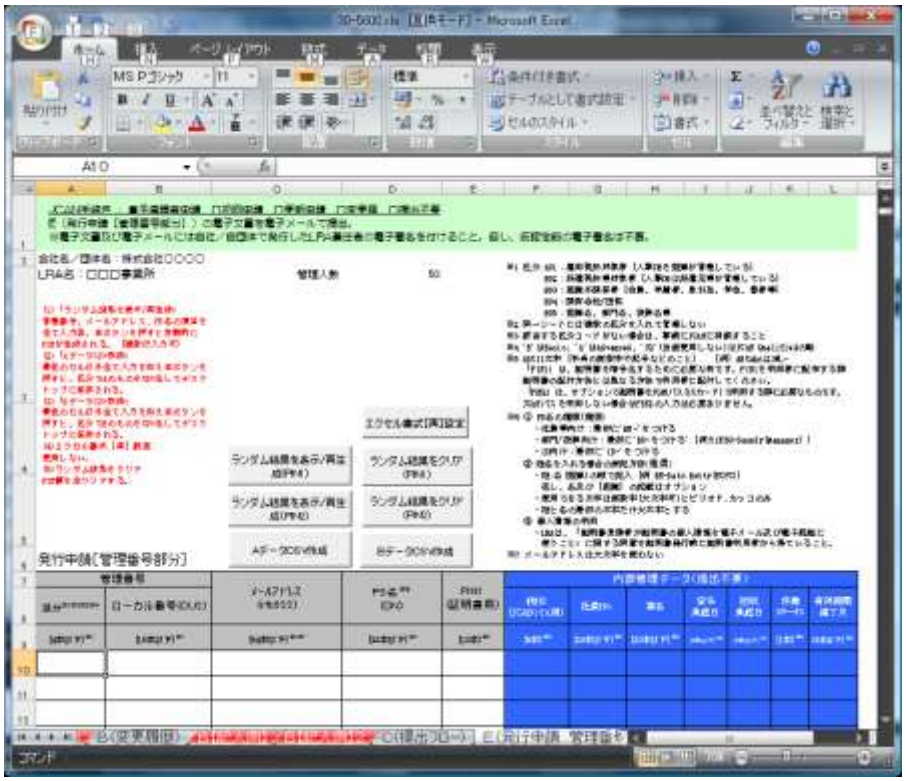
3.2.1 出力 CSV ファイルの EXCEL による表示

出力した CSV ファイルを、Microsoft EXCEL で表示し、操作を可能にする。

図 3-2　CSV ファイルを EXCEL で表示

3.3 運用フロー

出力された CSV ファイルの該当行をコピーして「30-5600」管理台帳にペーストすることにより、CSB；発行局システムへ取り込み可能なデータを作成することが可能となる。



4　JCAN ビジネス証明書による認証ログイン

本実証実験でのプロトタイプシステムとしての「ClearWorks」へのログイン時には、通常の ID およびパスワード認証に加え JCAN ビジネス証明書による認証によるログイン機能を実装した。

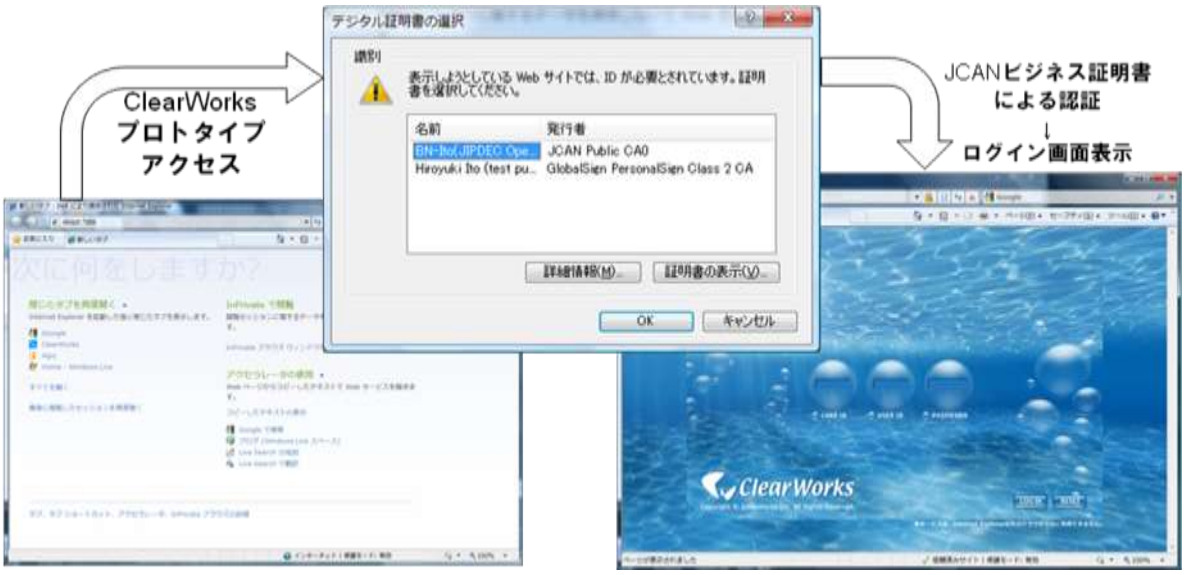


図 4-1　JCAN ビジネス証明書によるログイン認証

通常の ClearWorks では、ログイン画面での ID／パスワード入力後、再度 ID／パスワードによる二重の認証を行っているが、今回のプロトタイプシステムではログイン画面へのアクセス時にデジタル証明書による認証を行うことでセキュリティレベルを担保した。

5　プロトタイプ実証システム検証試験

本プロトタイプ実証システムの開発機能の検証を行い、機能が正常に動作することが確認された。

5.1 検証項目

以下の検証項目の動作検証を行った。

項番	テストタイプ	テスト内容	操作	動作	確認
1	正常	社員を新規登録時に発行申請情報も新規登録される。	新規ボタンをクリックし、社員を登録します。	社員情報とともに JCAN 申請情報が c_jcan_history に新規の emp_id とともに登録されます。	○
2	正常	社員が選択されると、該当する社員の最新の発行申請情報が表示される。	複数の発行申請情報が入力された社員を一覧から選択します。	社員明細の JCAN 申請情報に最新(登録日時がもっとも新しい)の申請情報が表示されます。	○
3	正常	社員を更新時に、区分またはローカル番号が変更されている場合、発行申請情報が新規に登録される。	区分またはローカル番号を変更して、社員を更新します。	c_jcan_history に emp_id とともに新しいレコードとして登録されます。	○
4	正常	社員を更新時に、区分またはローカル番号が変更されていない場合、発行申請情報が更新される。	区分とローカル番号以外の発行申請情報を変更し、[登録]をクリックします。	表示されている発行申請情報が更新されます。	○
5	正常	CSV が指定形式通り出力されます。ファイル名 jcan.csv	CSV 出力したい部門を選択し、[表示]をクリックし一覧を更新し、[発行申請 CSV]ボタンをクリックします。	jcan.csv というファイル名で csv ファイルがダウンロードされ内容は、表示されている社員の最新の登録申請情報が記載されている。	○

6	正常	指定した部門の社員の発行申請情報が出力されている。	2つ以上の部門があり、それぞれの部門に社員が登録されている状態で、CSV出力したい部門を選択し、[表示]をクリックし一覧を更新し、[発行申請 CSV]ボタンをクリックします。	CSVの内容は、指定した部門の社員の最新の登録申請情報が記載されている。	○
7	異常	発行申請情報がない社員が表示できる	c_jcan_historyの該当社員ID(emp_id)のレコードを削除して、該当社員を表示する。	JCAN申請情報が空白で表示される。	○
8	異常	発行申請情報がない社員を削除が表示できる	c_jcan_historyの該当社員ID(emp_id)のレコードを削除して、該当社員を削除する。	社員を正常に削除される。	○
9	正常	社員の新規入力画面には発行申請履歴リンクは表示されない。	新規ボタンをクリックします。	発行申請履歴のリンクが表示されない状態で、社員の詳細入力フォームが表示されます。	○
10	正常	社員情報入力フォームのタブオーダーが正しい	新規ボタンをクリックし、ユーザIDを選択し、タブでフォーカスを移動します。	この社員を非表示のチェックボックス以降発行申請履歴→区分→ローカル番号→メールアドレス→PS名→PIN→社員No.→実名→貸与承認日→回収承認日→作業ステータス→有効期間満了月→登録ボタン→削除ボタン順に移動する。	○
11	正常	区分フィールドのmaxlengthによる制限	区分フィールドに4文字以上入力する	4文字までしか入力できない	○
12	正常	区分が入力されていないチェックがされている	区分が入力されていない状態で、[登録]をクリックする	「区分を入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
13	正常	区分の入力文字列がチェックされている	区分にASCII文字以外が入力されている状態で、[登録]をクリックする	「区分にASCII文字のみ入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○

14	正常	ローカル番号フィールドの maxlength による制限	ローカル番号フィールドに 16 文字以上入力する	16 文字までしか入力できない	○
15	正常	ローカル番号が入力されていないチェックがされている	ローカル番号が入力されていない状態で、[登録]をクリックする	「ローカル番号を入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
16	正常	ローカル番号の入力文字列がチェックされている	ローカル番号に ASCII 文字以外が入力されている状態で、[登録]をクリックする	「ローカル番号に ASCII 文字のみ入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
17	正常	メールアドレスフィールドの maxlength による制限	メールアドレスフィールドに 64 文字以上入力する	64 文字までしか入力できない	○
18	正常	メールアドレスが入力されていないチェックがされている	メールアドレスが入力されていない状態で、[登録]をクリックする	「メールアドレスを入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
19	正常	メールアドレスの入力文字列がチェックされている	メールアドレスに不正なメールアドレス形式(mail)状態で、[登録]をクリックする	「メールアドレスに正しいメールアドレスを入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
20	正常	メールアドレスの入力文字列がチェックされている	メールアドレスに ASCII 文字以外が入力されている状態で、[登録]をクリックする	「メールアドレスに正しいメールアドレスを入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
21	正常	PS 名フィールドの maxlength による制限	PS 名フィールドに 32 文字以上入力する	32 文字までしか入力できない	○
22	正常	PS 名が入力されていないチェックがされている	PS 名が入力されていない状態で、[登録]をクリックする	「PS 名を入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○

23	正常	PS 名の入力文字列がチェックされている	PS 名に ASCII 文字以外が入力されている状態で、[登録]をクリックする	「PS 名に ASCII 文字のみ入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
24	正常	PIN フィールドの maxlength による制限	PINフィールドに12文字以上入力する	12 文字までしか入力できない	○
25	正常	PIN が入力されていないチェックがされている	PIN が入力されていない状態で、[登録]をクリックする	登録できる	○
26	正常	PIN の入力文字列がチェックされている	PIN に ASCII 文字以外が入力されている状態で、[登録]をクリックする	「PIN に ASCII 文字のみ入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
27	正常	社員 No.フィールドの maxlength による制限	社員 No.フィールドに 20 文字以上入力する	20 文字までしか入力できない	○
28	正常	社員 No.の入力文字列がチェックされている	社員 No.に ASCII 文字以外が入力されている状態で、[登録]をクリックする	「社員 No.に ASCII 文字のみ入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
29	正常	実名フィールドの maxlength による制限	実名フィールドに 20 文字以上入力する	20 文字までしか入力できない	○
30	正常	実名の入力文字列がチェックされている	実名に ASCII 文字以外が入力されている状態で、[登録]をクリックする	「実名に ASCII 文字のみ入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
31	正常	貸与承認日フィールドの maxlength による制限	貸与承認日フィールドに 6 字以上入力する	6 文字までしか入力できない	○

32	正常	貸与承認日の入力文字列がチェックされている	貸与承認日に YYMMDD 形式以外が入力されている状態で、[登録]をクリックする	「貸与承認日に日付を YYMMDD 形式で入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
33	正常	貸与承認日の入力文字列がチェックされている	貸与承認日に 110231 が入力されている状態で、[登録]をクリックする	「貸与承認日に正しい日付を入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
34	正常	回収承認日フィールドの maxlength による制限	回収承認日フィールドに 6 字以上入力する	6 文字までしか入力できない	○
35	正常	回収承認日の入力文字列がチェックされている	回収承認日に YYMMDD 形式以外が入力されている状態で、[登録]をクリックする	「回収承認日に日付を YYMMDD 形式で入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
36	正常	貸与承認日の入力文字列がチェックされている	回収承認日に 110231 が入力されている状態で、[登録]をクリックする	「回収承認日に正しい日付を入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
37	正常	作業ステータスフィールドの maxlength による制限	作業ステータスフィールドに 1 文字以上入力する	1 文字までしか入力できない	○
38	正常	作業ステータスの入力文字列がチェックされている	作業ステータスに A から E 以外が入力されている状態で、[登録]をクリックする	「作業ステータスには A から E を入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○
39	正常	有効期間満了付きフィールドの maxlength による制限	有効期間満了付きフィールドに 6 字以上入力する	6 文字までしか入力できない	○
40	正常	有効期間満了付きの入力文字列がチェックされている	有効期間満了付きに YYMMDD 形式以外が入力されている状態で、[登録]をクリックする	「有効期間満了月に日付を YYYYMM 形式で入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○

41	正常	有効期間満了付きの入力文字列がチェックされている	有効期間満了付きに000001が入力されている状態で、[登録]をクリックする	「有効期間満了月に正しい日付を入力してください。 前の画面に戻り、やり直してください。」と警告が表示される。登録はされない。	○

6　実運用に向けての課題

本実証研究において、実運用されている業務システムの社員情報と電子証明書情報を紐づけて管理することが可能であることの実証を行ったが、実運用に向けては以下のような課題について更なる検討を要する。

① 実運用時には、より効率的な発行申請を実現するために、今回の実装方法（B ルート）以外にも直接 CSB にアップロード可能なフォーマット（A ルート）での出力機能の実証

② 発行申請情報をより効率的に登録するための機能強化（OCR 用紙からの入力、電子メールなど電子情報からの自動登録など）の検討

③ 社員などの人事異動情報などと連動して、発行電子証明書の追加・変更・削減・失効・更新等の管理ができる機能の実証

④ 紙印刷コストの削減のために、業務システムが出力する帳票（見積書、請求書などの PDF）へ個人印の印影と合わせて電子証明書の添付機能の実装のための実証。また受発注に際して相手先認証による注文処理、注文請処理、受領確認、などインターネットを介した受発注ステータス管理機能の実証。

⑤ JCAN パス使用者の為の、JCAN パスドライバ対応実装の検討

7　ClearWorks 概要

本実証にてプロトタイプシステムのベースとなった ClearWorks は、「会計」「販売管理」「給与計算」の機能を備えた SaaS 型統合業務システムであり、 2009 年には当時経済産業省が主管していた「J-SaaS」事業採択アプリケーションとなった。

企業情報、社員情報等は全ての機能の共通データベースとして管理されているシステムであり、本実証実験ではこの社員情報部分の拡張などを行いプロトタイプシステムとした。

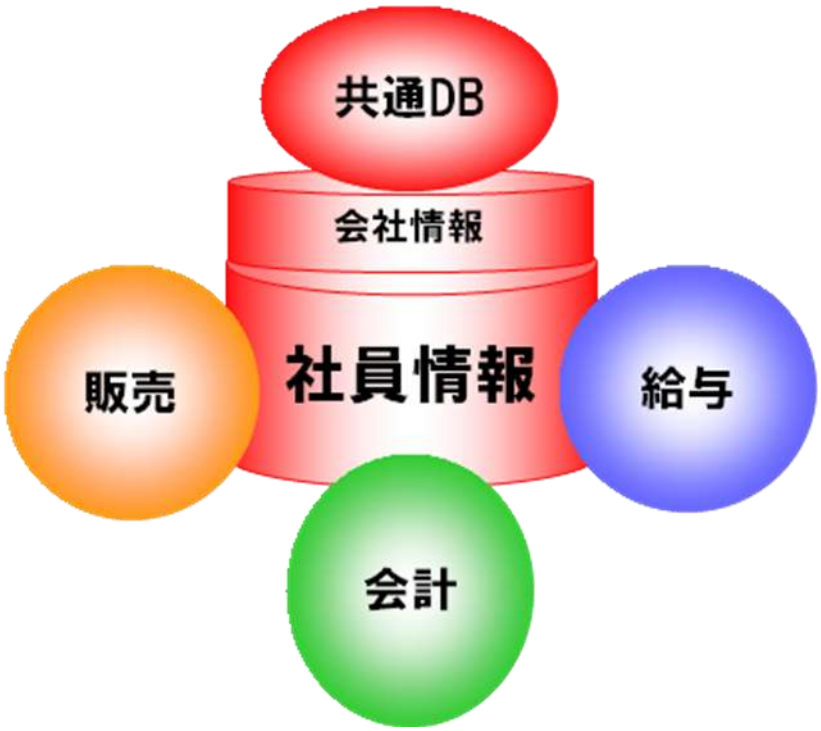


図 7-1　ClearWorks アーキテクチャ概念図

7.1 ClearWorks の特徴

SaaS 型統合業務システムサービスの ClearWorks は以下のような特徴を備える。

① 「財務会計」「給与計算」「販売管理」の統合型 SaaS アプリケーション
- 共有設定機能で各モジュールに共通の項目を一括で登録・設定・変更可能。
- 各種データを自動仕訳連動。販売や給与から会計へ自動仕訳が可能。

② 完全 Web アプリケーション
- 個別のプログラムのダウンロードやインストールは不要。Web ブラウザのみで全機能利用可能。
- 万が一 PC が壊れても紛失・盗難してもデータは安全にデータセンターに保管管理。

③ 自動法令対応・自動バージョンアップ
- 各種料率の法令改定などを自動的にメンテナンス。煩雑なバージョンアップ・データコンバート作業不要。
- 標準機能の追加や機能向上などのバージョンアップも月額利用料内で自動的にバージョンアップ。

④ 業務効率の高い複数拠点利用
- 複数の事業所や会社と自宅、或いは税理士とのデータ共有など ID 発行のみで利用可能。
- アクセス権限を設定した上で更に高度な暗号化技術で全て通信を暗号化。

⑤ 堅牢な大規模データセンターで 24 時間 365 日安心のセキュリティ。
- 耐震耐火構造など堅牢なデータセンターで 24H365D 運用監視。強固なセキュリティとバックアップ体制。
- 毎日自動的にバックアップを行い 32 世代のバックアップを管理。

図 7-2 ClearWorks 画面

E「電子認証応用領域のプロトタイプ実証」

目次

1　事業の概要

本章では、電子認証応用領域のプロトタイプ実証事業の概要について示す。1.1 節で本事業の背景と目的を示し、1.2 節で事業内容を、1.3 節で推進体制を、1.4 節で検討スケジュールを示す。

1.1 事業実施の背景と目的

本節では、電子認証応用領域のプロトタイプ実証事業実施に関する背景と目的について示す。半導体　認証、トレーサビリティでは、SEMI 標準化 T20(Structure of Authentication / Verification Capability)に向け、SEMI-J と JEITA の協力のもとで、日本からの提案として Doc4845(CSB：人と組織の認証)、Doc4847(SASB，ASB：物の認証)として、SEMI での標準化を行っている。また、半導体に限らない全業界にまたがる ISO TC247(Fraud countermeasures and Controls)に対しても、日本からの提案を進めている。ISO TC247 の詳細については附属 A を参照。

本調査では、日本からの認証、トレーサビリティの提案内容に沿った模倣品対策の真贋判定とトレースのための模倣品対策システムのプロトタイプを実証し、電子認証とトレーサビリティの仕組みを含めた実証・調査を行うことで、今後の本格的なシステム構築と運用に向けた課題から改善へとつなげる。さらに、電子証明書を活用したビジネスシーンにおいての応用領域で、その効果を明らかにすることを目的とする。

1.2 事業内容

本節では、電子認証応用領域のプロトタイプ実証事業の内容について示す。本事業では、電子認証応用領域として、模倣品対策システムのプトロタイプ実証を行う。模倣品対策システムは前節で示した TC247 の日本提案内容を基に、模倣品対策システムを実証した。

本事業では、模倣品対策システムに関する運用上の問題や課題を確認、整理することが目的であるため、模倣品対策システム実証は、模倣品対策システムに関する運用上の問題や課題を確認できる程度のシステム概要の仕様を示すことで、プロトタイプの課題や効果を確認する。

プロトタイプの確認については、運用上での問題を確認することを意義があるため、関係者への説明として、グラフィカルユーザインタフェースの一部を示した。また、説明時に行うデモンストレーションのために、一部の機能については、ダミーの処理を示した（各インタフェースから入力されたデータに対するダミー処理、及びダミー処理結果の表示、出力する処理等)。

以上の手法によって、実証するプロトタイプを用いて、関係者に対して、実運用に耐え得ること、または課題等を確認した。

1.3 推進体制

本節では、電子認証応用領域のプロトタイプ実証事業の推進体制について示す。

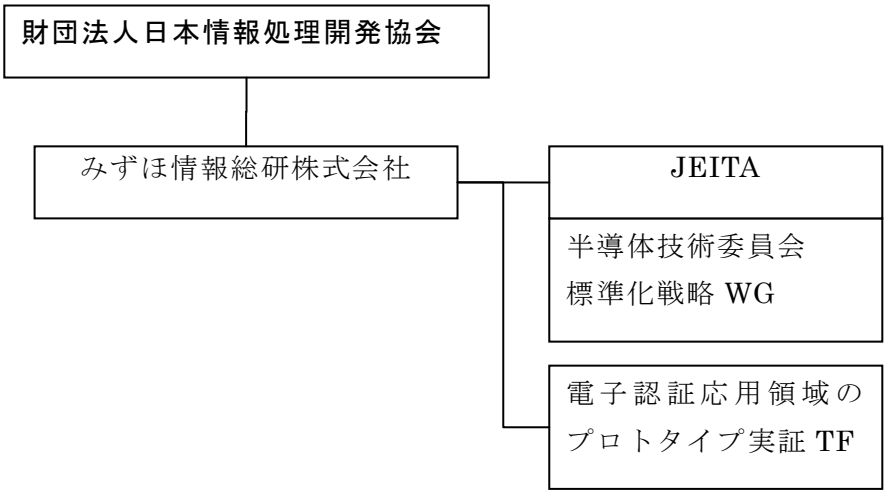


図 1-1 推進図

1.4 検討スケジュール

本節では、電子認証応用領域のプロトタイプ実証事業の検討スケジュールについて示す。

表 1-1 検討スケジュール

月 / 調査研究事業	平成 22 年						
	8 月	9 月	10 月	11 月	12 月	1 月	2 月
模倣品対策システムの検証結果の検討		→	→				
模倣品対策システムの課題の整理			→	→	→		
模倣品対策システムのまとめ						→	→

2 模倣品対策システムの概要

本章では、プロトタイプの基となる TC247 において日本が提案している模倣品対策システムの概要を示す。2.1 節で本システムに関連する役割とプレイヤを示し、2.2 節で本システムにおいて利用するコード体系を、2.3 節で想定するアプリケーションと認証コードのレベルを、2.4 節でモデル定義を、2.5 節にシステムの全体像、2.6 節で処理フローを示す。また、2.7 節で電子認証を含んだアクセス制御に関連する認証の種類と制御対象等を示す。

なお、本章で説明する模倣品対策システムは、TC247 において日本が提案しているシステムであり、本事業において実証したプロトタイプではない。本事業で実証したプロトタイプは、次章で説明する。

2.1 役割・プレイヤについて

本システムでは、3 種類の役割が存在する。これらの役割は、Doc4845(CSB：人と組織の認証)及び Doc4847(SASB、ASB：物の認証)として日本が提案している内容に則している。また、各役割で想定するプレイヤとその概要を以下に示す。

表 2-1 役割の定義

略称	名称	想定する団体	備考
SASB	Self Authentication Service Body	企業等を想定	
ASB	Authentication Service Body	任意の業界団体を想定	主に B to B に関連する
CSB	Certificate Service Body	認証機関(各国認証)を想定	主に B to C に関連する

SASB は、模倣品対策を実施したい団体や個人であり、一般的には製造業者を想定している。ASB は、信頼できる特定の業界団体ごとに設置・設定される業界団体である。例えば、半導体業界であれば JEITA などを想定している。CSB は、各国ごとに設置・設定された認証機関である。例えば、企業コードの管理及び電子証明書の発行等を含め JIPDEC などを想定している。

また、上記に設定した役割以外に、製造品の真贋判定を行う顧客(カスタマ)を想定している。

各役割の関係を下図に示す。模倣品対策を実施したい SASB は、自らが属している業界に設定されている ASB に対して各種コードの発行依頼や、コードに関連付ける製品・商品の情報登録等を行う。SASB と SAB でやり取りする情報は、機密情報も含むため、通信相手が意図した相手であることを確認するための認証や通信路の暗号化も必要となる。認証等によって、情報のやり取りを安心・安全に実施するために電子証明者の利用を想定している。この電子証明書の発行を CSB が行う。また、CSB は国ごとに設定される役割であり、コード体系において、国ごとに設定された CSB と、各国の業界ごとに設定された ASB が階層構造で、管理することによって取り扱うコードの一意性(ユニーク性)を担保しやすいスキームとして構成する。

なお、本システムにおける証明書プロファイルの共通フォームについては、付属 C を参照。

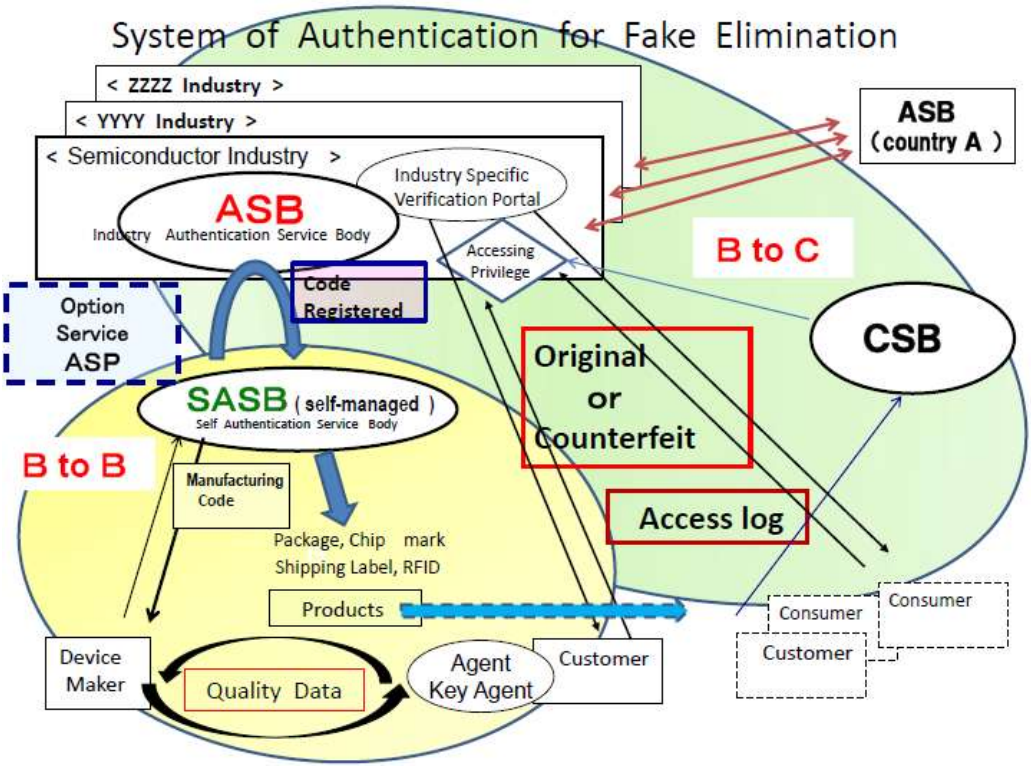


図 2-1 各役割の概要図

2.2 コード体系について

本システムでは、2 種類の認証コードが存在する。以下にその概要を示す。

- ライセンスプレート用認証コード(以下 LC)
  - 20 桁の英数字から構成されるコードである。
  - 一般的に製品の箱やトレーなどに貼付／印字されることを想定している。

  ex）薬品の箱に貼れている製品識別のラベル

- デバイス認証用コード(以下 DC)
  - 43 桁の英数字から構成されるコードである。
  - 一般的にデバイス自体に貼付／印字されることを想定している。

  ex）薬品のカプセル自体に印字されている製品識別情報

なお、本システムにおけるコードのデータマトリックスは ECC200 などを想定している。詳細な例示は、附属 B を参照。

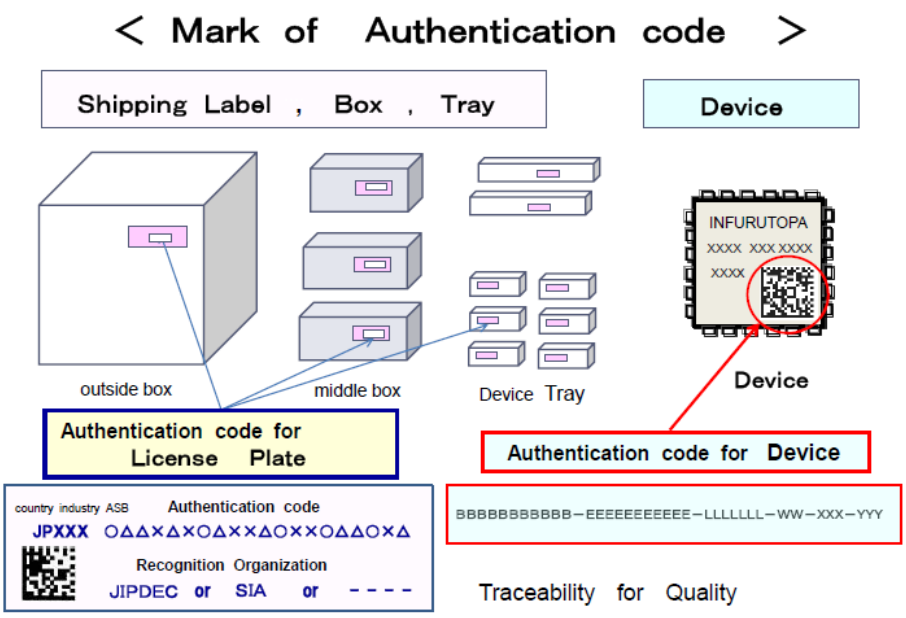


図 2-2 ライセンスプレート、デバイスコード概要

2.2.1 ライセンスプレート用認証コード(LC)

ライセンスプレート用の認証コードの概要を以下に示す。

表 2-2 ライセンスプレート用認証コード概要

発行・登録・管理	・ LC は、ASB が発行し、SASB が購入するコードである。 ・ SASB が購入時に登録した情報は、ASB が管理する。
必要な情報	・ SASB は、コードを購入する際に、以下の登録を行う。 ・ 登録企業名、品名、型名など標準フォーマットで定められた情報であり、テキストや画像データ等を ASB に送信する。
その他	・ LC の値は、ASB が生成するランダムな値である。 ・ LC には、ASB のコード(識別番号)が付加される。

図 2-3 デバイスコードのイメージ図

※ この LC 自体の改ざん発行などを防止したい企業は、別途、自らがホログラム等の別技術を採用して対応することを想定している。

2.2.2 デバイス認証用コード(DC)

デバイス認証用コードの概要を以下に示す。

表 2-3 デバイス認証用コード概要

発行・登録・管理	・ DC は、SASB が作成・発行し、ASB に登録するコードである。 ・ DC は、SASB が ASB に対して管理を依頼するコードである。 ・ SASB が購入時に登録した情報は、ASB が管理する。
必要な情報	・ DC の値自体は、規定の使用文字種及び桁数を除き、SASB が任意に設定できる。
その他	・ DC には、Non-Secret 部分と Secret 部分がある。 ・ Non-Secret 部分は、デバイスに印字されているコードなど目で見られる情報と同じであることを想定している。 ・ Secret 部分は、SASB が社外機密情報として使用、管理する情報を想定している。そのため、この部分は、全て任意である。

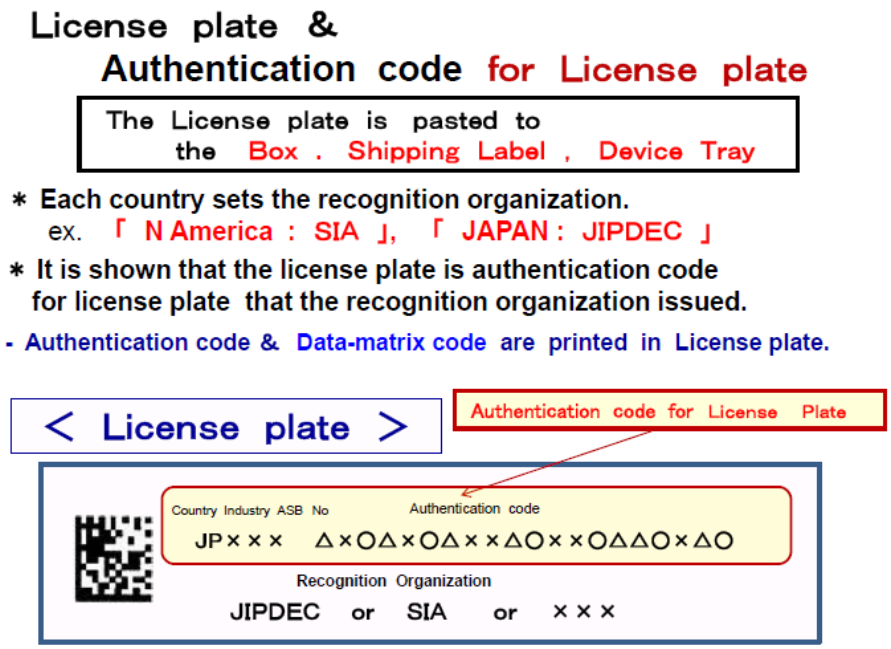


図 2-4 ライセンスコードのイメージ図

※ ASB は、LC、DC を関連付け、LC と DC を連結した状態で、他のコードと重複していないことをチェックし、コード発行を認め、発番、管理する。

2.3 想定アプリケーションと認証コードレベルについて

本システムは、想定するアプリケーションについて、関連分野と各認証コードの関係を示す。関連する分野によっては、認証コードに求められるセキュリティが異なることを想定している。そのため、この関係を 4 段階のレベルによって示す。レベル 4 が最も高いセキュリティであり、レベル 1 が最も低いセキュリティである。なお、下表で示したレベルは、認証コードの利用について想定するセキュリティのレベルを示したものであり、認証のレベル付けではなく、第三者による認証を強制するものではない。

表 2-4 想定アプリケーションのレベル

レベル	関連分野及び事項
レベル 4	Cyber Safety, Social impact, Critical infrastructure
レベル 3	Safety, High Damage, Health and safety
レベル 2	High quality, High Cost ・ Value,

	Security
レベル 1	Future business model ・ Risk, Traceability Effect

既に製品を提供している SASB では、製品単価や想定する被害やリスクに応じた対策を行うことを想定しているため、上記のレベルに応じて自らがコード自体の改ざん防止などを考慮して技術的対策を講じることとする。詳細については、TC247 WG1 等の資料を参照。

2.4 モデルの定義について

プロトタイプによる実証を行うにあたり、適用するモデルを以下に定義する。本モデル定義の基本的な考え方としては、各プレイヤと役割を説明するために、最もシンプルで理解し易いモデルとした。まず、各プレイヤが担当する役割は最小限であり、各プレイヤと役割が一対一で対応させる基本形であることを原則とした。

- 現実的なシステムでは、複数の物流(部品代理店管理外の配送業者や輸出入業者等)が関与し、その各々がトレースを管理することが考えられるが、最も単純で基本となるモデルは単独の物流業者が存在するモデルであるため、本モデルでは部品代理店が管理する単独の物流業者がトレースを管理することとする。
- 実際のモデルでは複数の部品を組み合わせることで製品を製造する場合も考えられる。その場合は、ひとつの製品に対して複数の SASB が関連するが、本モデルの定義では、最も基本的なモデルとして単独の SASB と物流企業が製品を顧客へ提供するモデルとする。

なお、上記で現実的な利用方法であり、複数のプレイヤや複数の役割に拡張可能である。

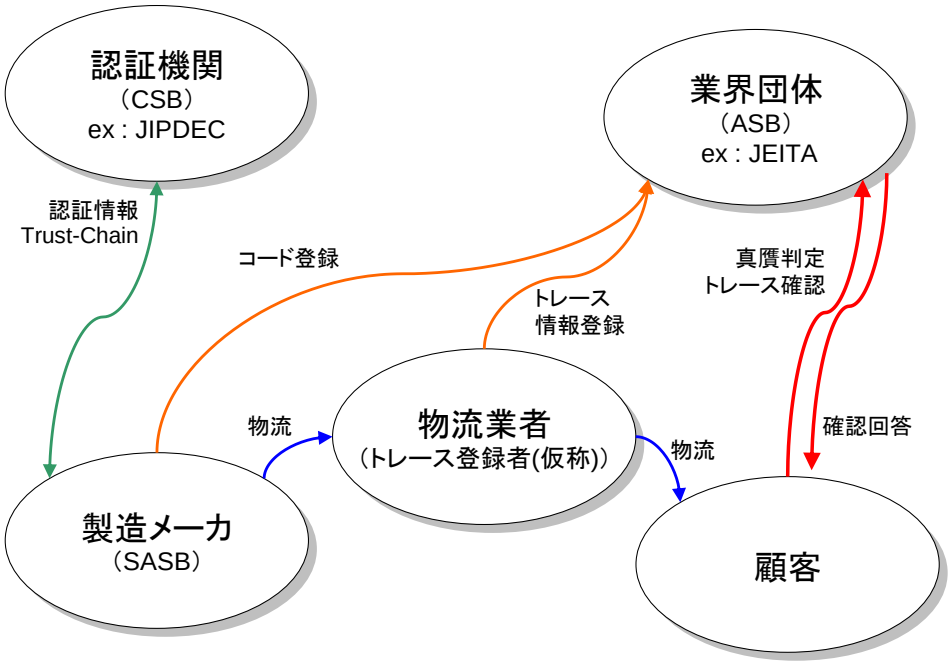


図 2-5 モデル概要図

2.5 システムの全体像について

本システムでは、SASB が各種認証コードや物流のトレース情報を ASB に登録する。SASB や ASB の登録情報及び存在の確かさについては CSB が発行する電子証明書によって確認する。また、顧客は ASB に登録された情報を確認することで、真贋判定やトレースを実施できる。

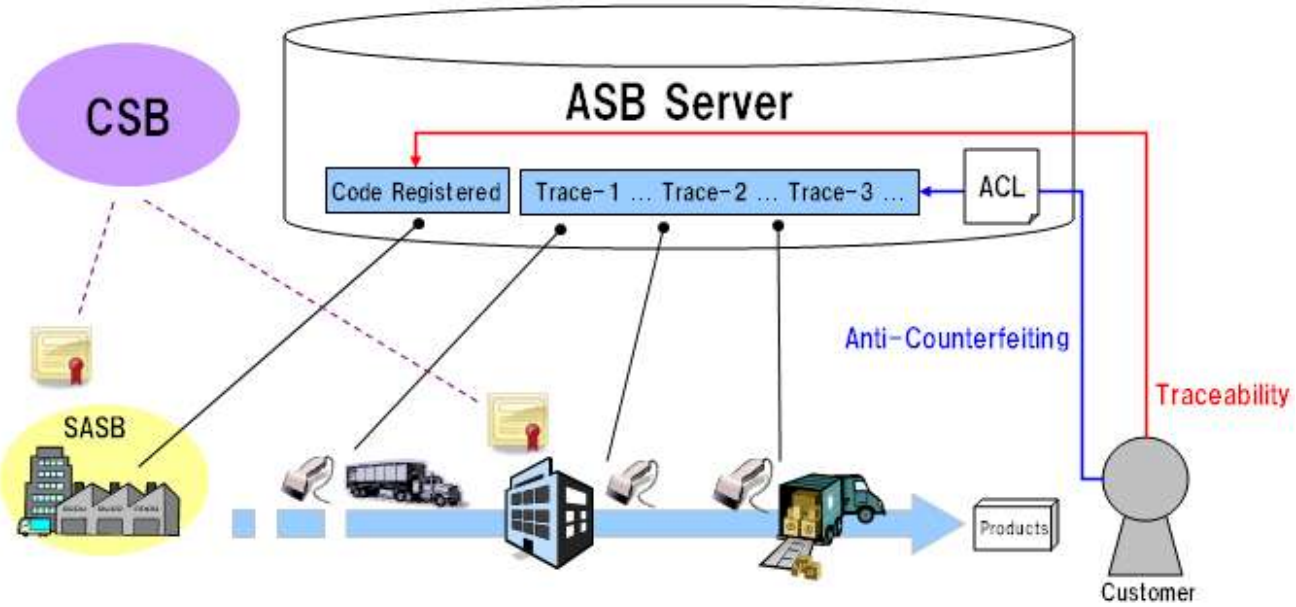


図 2-6 全体像

上記のシステムによって、ASB がユニーク性(一意性)を確認したコードに対する不正な関連付

けの検出が可能である(コードと製品・物の不正な関連付け、コードと製品情報・物情報の不正な関連付け、コードとトレース情報の不正な関連付け等)。また、不正な関連付けを検出した顧客は、購入先への問合せや返品等の事後対策によって解決することを想定している。

なお、本事業のテーマである電子認証の応用領域として電子証明書を用いた主な機能を明確にするために、以降に電子証明書を利用した模倣品確認の処理及び、物流トレース確認の処理を示す。

2.5.1 模倣品確認の処理

模倣品の確認については、製造メーカである SASB が業界団体である ASB に登録した認証コード(DC 及び LC)と認証コードに関連付けられた製品情報を顧客が確認することで、模倣品であるか否かを確認する。この確認情報は、SASB が登録する情報であるため、正しい SASB(属性)が登録した正しい情報である必要がある。この正しさの確認のために、CSB から SASB に発行した電子証明書を用いる。

下図の例示では、顧客が利用している製品をバーコードスキャナなどによって認証コードを読み取り、読み取った認証コードをもとに、(1)本物確認を ASB に依頼する。(2)ASB は登録されている製品固有のコードを確認し、(3)登録されていないコードであることが判明し、確認した製品が偽物であることを通知する処理である。

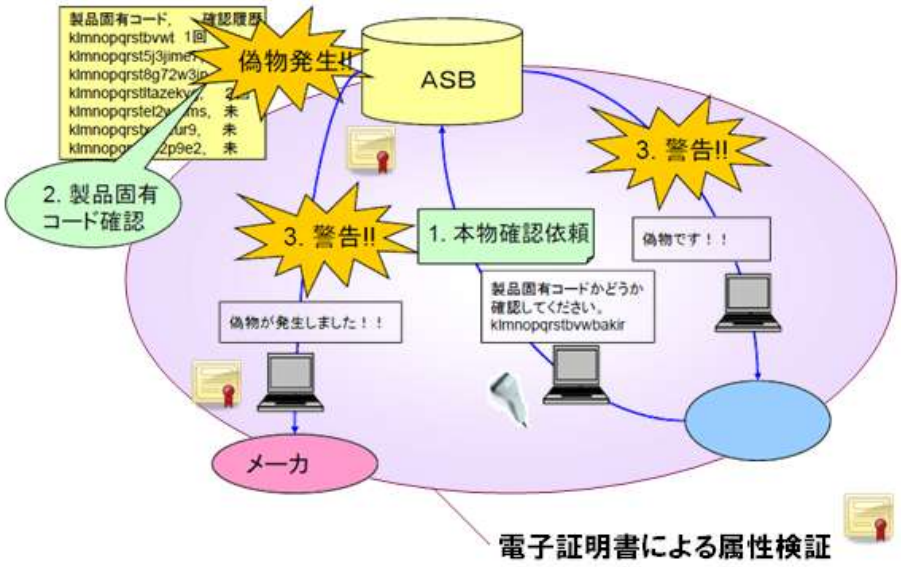


図 2-7 模倣品確認の処理概要

2.5.2 物流トレース確認の処理

物流トレースの確認については、物流業者など物流管理を行う関係者が業界団体である ASB に登録した認証コード(DC 及び LC)に対する物流トレース情報を顧客などが確認することで、正しく物流されていた製品であるか否かを確認する。この確認情報は、物流管理を行う関係者が登録する情報であるため、正しい関係者(属性)が登録した正しい情報である必要がある。この正し

さの確認のために、CSB から SASB 等の関係者に発行した電子証明書を用いる。

また、任意で電子証明書を用いた閲覧情報のアクセス制御を想定する。SASB が事前に閲覧者権限を設定し、トレース情報の開示粒度を制限する。この権限認証に電子証明書を用いる。

下図の例示では、代理店などが所持している製品をバーコードスキャナなどによって認証コードを読み取り、読み取った認証コードをもとに、(1)本物確認と同時に詳細情報(物流トレース情報)の開示を ASB に依頼する。(2)ASB は登録されている製品固有のコードを確認し、さらに(2-1)問合せの権限(アクセスレベル)の確認を行い、(2-2)権限(アクセスレベル)に見合った情報を抽出する。(3)問合せた代理店などに権限(アクセスレベル)に見合った情報を通知する処理である。

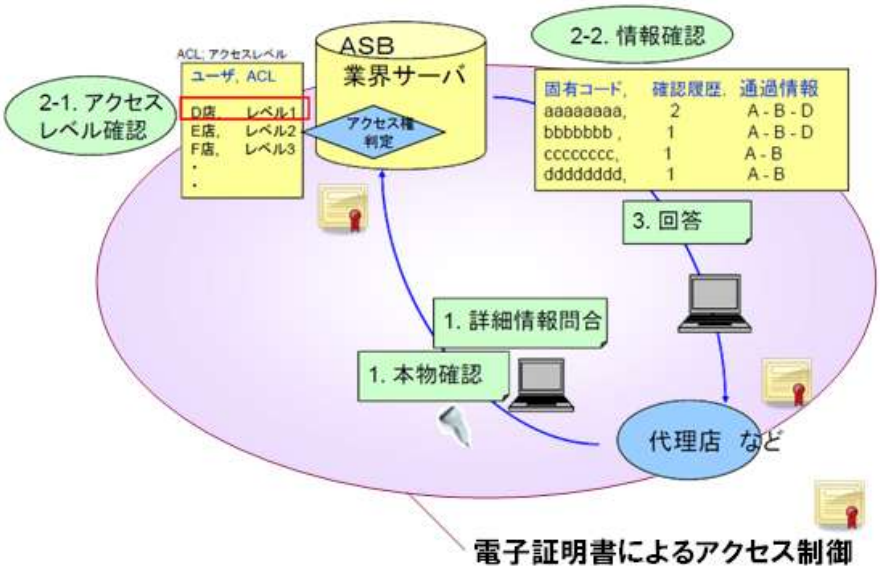


図 2-8 物流トレース確認の処理概要

2.6 処理フローについて

前節の全体像に基づく、模倣品対策システムの処理フローを以下に示す。

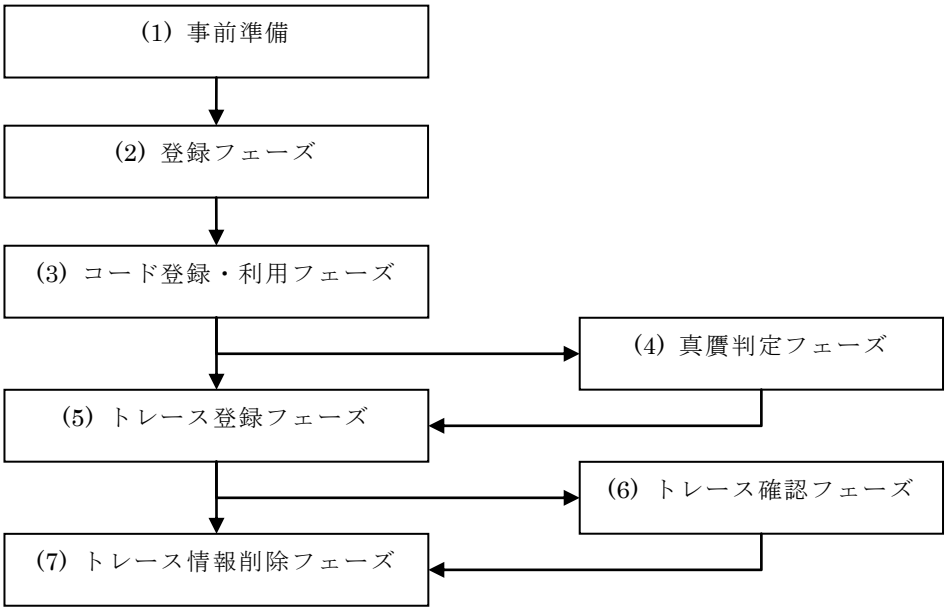


図 2-9 処理フロー概要図

2.6.1 事前準備

表 2-5 事前準備概要

(1)前提条件(事前準備)	前提条件として、以下が存在していることとする。 ・CSB(各国の認証機関：JIPDEC を想定) ・ASB(業界団体：JEITA を想定) また、任意に、ASB は、CSB から電子証明書を入手し、入手した電子証明書は、SASB や顧客がアクセスする Web サーバに対して、適切に設定されていることとする。

2.6.2 SASB 登録フェーズ

表 2-6 SASB 登録フェーズ概要

(2)SASB 登録フェーズ(仮称)	SASB 登録フェーズは、本システムに SASB として利用登録するフェーズである。SASB は、ASB と CSB に対して各種の情報を送り、登録を行う。この際、任意で ASB からシステム利用に関する ID/PWD を入手し、CSB から電子証明書を入手する。本システムでは、入手した電子証明書を用いて、SASB の認証を行う。 ■CSB に対する登録 ① SASB は CSB に、自身の電子証明書用の登録データを送信する。 登録データには担当者の連絡先であるメールアドレスや企業情報を含むデータであり、JCAN[1]の登録データと同様である。 ② CSB は SASB から受信した登録データを登録し、電子証明書の元データを SASB に送信する。CSB は登録前に、法人格の実在性を確認する。 ③ SASB は CSB から受信した電子証明書の元データを用いて電子証明書を生成し、安全に保管する。 ■ASB に対する登録 ① SASB は ASB に、本システム用の登録データを送信する。登録データには担当者の連絡先であるメールアドレスや企業情報を含むデータである。 ② ASB は SASB から受信した登録データを登録し、初回ログイン時に必要となるデータを SASB に送信する。 ③ SASB は ASB から受信したデータを用いて以降ログインして本システムを利用する。 CSB 向け登録：・企業登録し、電子証明書を入手する。(任意) ・企業の従業員(個人)ごとの登録が必要。(任意) ・トレース登録者の登録を行う。 ・トレース確認者の登録を行う。 ASB 向け登録：・企業登録し、ID/PWD を得る。(任意) ・企業の従業員(個人)ごとの登録が必要。(任意) ・トレース登録者の登録を行う。 ・トレース確認者の登録を行う。

[1] JIPDEC JCAN トップページ http://www.jipdec.or.jp/project/anshinkan/jcan/index.html

2.6.3 コード登録・利用フェーズ

表 2-7 コード登録・利用フェーズ概要

(3)コード登録・利用フェーズ(仮称)	コード登録・利用フェーズは、SASB が本システムを利用しコードを登録及び利用するフェーズである。SASB は、ASB に対して、コードの購入や登録を行い、利用する。なお、LC は ASB が発番するため、購入と呼び、DC は SASB が発番するため、登録と呼ぶ。また、購入及び登録したコードは SASB が管理する。 ■LC の発番 ① SASB は ASB に LC の発番・購入依頼を行う。 LC の発番は ASB が行うため、SASB が LC の数量などを申請し購入する。LC の購入依頼には、LC の情報を付帯することが必須である。 また、購入依頼とは別に任意のタイミングで一度登録した LC の情報の修正を行うことができる。なお、LC の利用形態(製品や部品に対する印字方法や保管等)は SASB が実施する。 ② SASB は ASB が発番した LC を受取る。 上記、情報の送受信については、重要な情報をやり取りするため、SASB 及び ASB は電子証明書による相互認証を行うことで通信相手を確認し、通信路の暗号化を行い傍受や改ざんに耐性のある通信によって安全性を満たす。(任意)

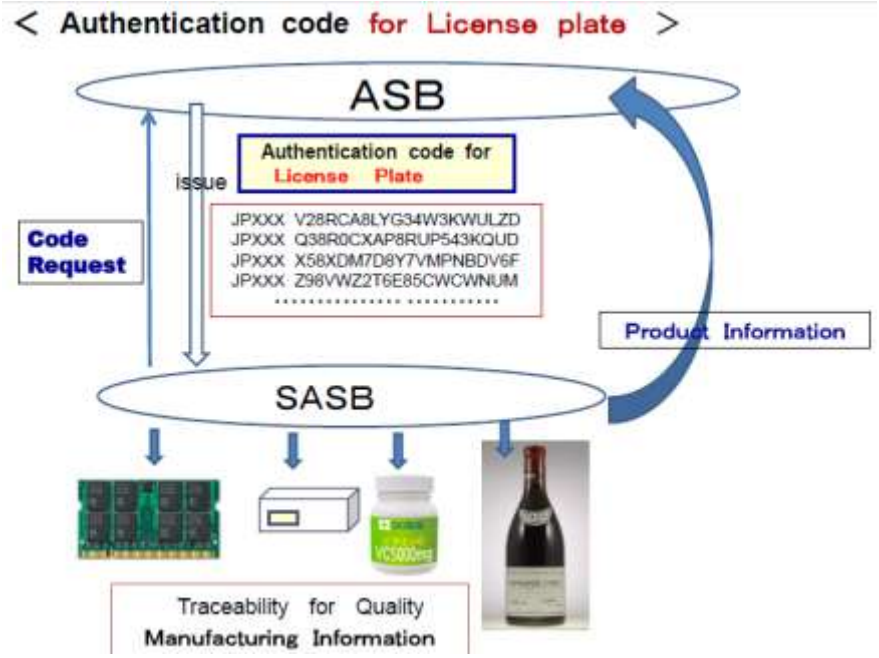


図 2-10 LC 発番処理フローの概要図

■DC の登録

① SASB は ASB に DC の登録を行う。

DC の発番は、SASB が行うため、SASB が発番した DC を ASB が確認し、重複をチェクした後に、登録する。登録依頼には、DC の情報を付帯することが必須である。

また、購入依頼とは別に任意のタイミングで一度登録した DC の情報の修正を行うことができる。なお、DC の利用形態(製品や部品に対する印字方法や保管等)は SASB が実施する。

② SASB は ASB が発番した DC を受取る。

上記、情報の送受信については、重要な情報をやり取りするため、SASB 及び ASB は電子証明書による相互認証を行うことで通信相手を確認し、通信路の暗号化を行い傍受や改ざんに耐性のある通信によって安全性を満たす。(任意)

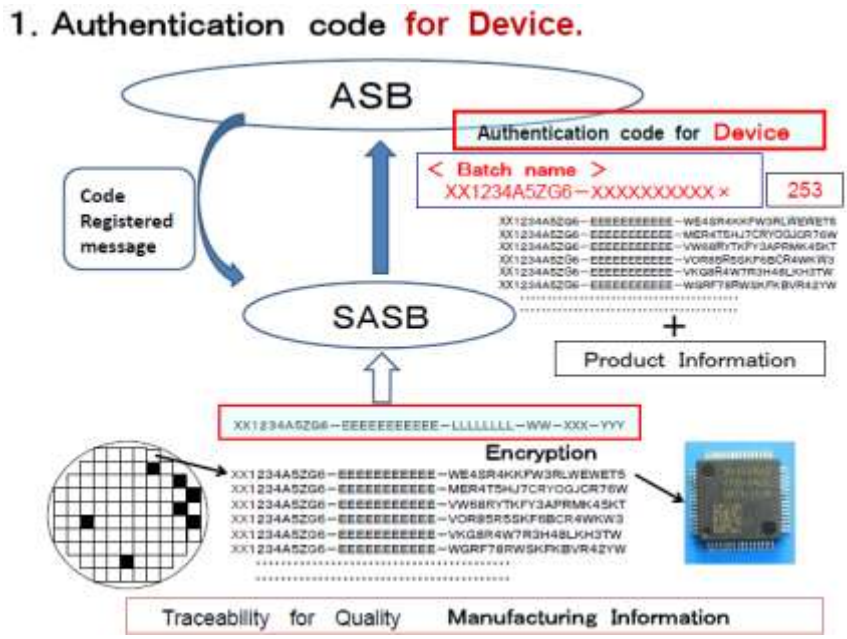


図 2-11 DC 登録処理フローの概要図

※コードの使い回しは許容する。

(異なる部品等にコードを付帯し、何度も同じコードを使い回してもよい。)

※コード重複チェック方式としては、DC のみと DC&LC の双方で重複チェックを行う。

2.6.4 真贋判定フェーズ

表 2-8 真贋判定フェーズ概要

(4)真贋判定フェーズ(仮称)	真贋判定フェーズは、顧客及びその他の関係者(SASB 登録者等)が、ASB に LC 及び DC が登録されている正規のコードであるかを確認するフェーズである。このフェーズではコード(LC 及び DC)が登録されていることを確認できる機能であり、各製品や部品の流通経路情報であるトレース情報は事前に定められた情報のみ確認できる。そのため真贋判定フェーズの説明ではトレース情報を確認するトレース機能確認については割愛する。(トレース機能確認については、後述(6)に示す。) ① 顧客は、自らが使用している製品及び部品に付帯しているコード(LC 及び DC)を ASB に問い合わせる。 ② ASB は、登録されているコードであれば、登録されている情報を返し、登録されていないコードであれば、登録されていないことを顧客に返す。 ※顧客及びその他の関係者の識別/認証及び確認などを行う。(任意)

2.6.5 トレース登録フェーズ

表 2-9 トレース登録フェーズ概要

(5)トレース登録フェーズ(仮称)	トレース登録フェーズは、本システムに登録したトレース登録者が、各製品や部品の流通経路情報をトレース情報として登録するフェーズである。 ①トレース登録者は、(2) SASB 登録フェーズでトレース登録している情報を用いて本システムのトレース登録者認証を行う。 ②トレース登録者は、ASB に LC 及び DC に関する流通経路情報をトレース情報として登録する。この登録情報には、任意で電子証明書を含む。(証明書プロファイルについては、附属 C を参照。) ※トレース登録者は、識別/認証などを行う。(任意)

2.6.6 トレース確認フェーズ

表 2-10 トレース確認フェーズ概要

(6) トレース確認フェーズ(仮称)	トレース確認フェーズは、顧客及びその他の関係者(SASB 登録者等)が、各製品や部品の流通経路情報をトレース情報として確認するフェーズである。 ① 顧客及びその他の関係者は、自らが使用・利用している製品及び部品に付帯しているコード(LC 及び DC)を ASB に問い合わせる。 ② ASB は、登録されているコードであれば、登録されているトレース情報を返し、登録されていないコードであれば、登録されていないことを顧客に返す。(SASB にリダイレクトする) ※トレース確認者は、識別/認証などを行う。(任意)

2.6.7 トレース情報削除フェーズ

表 2-11 トレース情報削除フェーズ概要

(7)トレース情報削除フェーズ(登録後一年を想定)	トレース情報削除フェーズは、ASB に登録されているトレース情報を削除するフェーズである。トレース情報は、蓄積する量が多く、ASB の資源を圧迫する可能性がある。そのため、登録後一年間を目処に蓄積したトレース情報を自動的に削除する。登録後一年に自動的に削除する際には、コード購入及び申請者である SASB はトレース情報を一括して ASB から得ることができる。 ① ASB から SASB に対して、登録一年後のトレース情報に関する受入確認が行われる。(また、(2) SASB 登録フェーズによって、登録一年後のトレース情報に関する受入設定を行っている) ② ASB から SASB に対して、登録一年後のトレース情報が送られ、SASB は受け付ける。 ※トレース情報削除の際は、トレース登録者は、識別/認証などを行う。(任意) ※トレース情報削除フェーズ(登録後一年)以降は、トレース確認を SASB が処理する。

2.7 アクセスコントロールについて

ASB で管理する情報に関するアクセス制御の手法及び、制御対象情報と操作者及び権限者のリストを示す。認証手段については、電子証明書(双方向の認証を含む)場合と、Basic 認証、認証を行わない場合が考えられる。一方、SASB が既に開始しているビジネス的な要素(製品単価に対する認証コードに求めるレベル及び想定する損害やそのリスク等)を考慮し、認証手段はすべて任意とし、求めるレベルによって SASB が任意に選択することを想定する。想定するアプリケーションと求めるレベルについては、2.3 節に示した通りである。

表 2-12 ASB のアクセスコントロールリスト

	権限	認証手段			LC			DC			トレース		
		署名	Basic	無	登録	修正	確認	登録	修正	確認	登録	修正	確認
SASB 内(組織内関係者)	LC 登録	任意		－	○	○	－	－	－	－	－	－	－
	LC 確認	任意		－	－	－	○	－	－	－	－	－	－
	DC 登録	任意		－	－	－	－	○	○	－	－	－	－
	DC 確認	任意		－	－	－	－	－	－	○	－	－	－
	トレース登録	任意		－	－	－	－	－	－	－	○	○	－
	トレース確認	任意		－	－	－	－	－	－	－	－	－	○
SASB 外(組織外部関係者)	LC 登録	任意		－	○	○	－	－	－	－	－	－	－
	LC 確認	任意		－	－	－	○	－	－	－	－	－	－
	DC 登録	任意		－	－	－	－	○	○	－	－	－	－
	DC 確認	任意		－	－	－	－	－	－	○	－	－	－
	トレース登録	任意		－	－	－	－	－	－	－	○	○	－
	トレース確認	任意		－	－	－	－	－	－	－	－	－	○
エンドユーザ	LC 確認	任意			－	－	○	－	－	－	－	－	－
	DC 確認	任意			－	－	－	－	－	○	－	－	－
	トレース確認	任意			－	－	－	－	－	－	－	－	○

3　プロトタイプ実証結果

本章では、プロトタイプによる実証の結果を報告する。3.1 節でプロトタイプの概要を示し、3.2 節でプロトタイプ実証の結果概要を報告し、3.3 節でプロトタイプ実証によって得られた課題と解決策を報告し、3.4 節でプロトタイプ実証によって確認できた電子証明書利用の効果を報告する。

3.1 プロトタイプの概要

本システムでは、3 種類の役割が存在する。これらの役割は、Doc4845(CSB：人と組織の認証)及び Doc4847(SASB，ASB：物の認証)として日本が提案している内容に則している。

また、各役割で想定するプレイヤとその概要を以下に示す。

3.1.1 プロトタイプに実装する機能

表 3-1 プロトタイプ実装機能

ASB に必要な(実装する)機能	・ LC 情報の登録／修正／検索／出力 ・ LC 通過ログの登録／削除／修正／取得／検索／出力 ・ DC 情報の登録／修正／検索／出力 ・ DC 通過ログの登録／削除／修正／取得／検索／出力
SASB に必要な(実装する)機能	・ LC 発番依頼 ・ DC の情報入力／修正 ・ DC の生成 ・ DC 内の Secret(暗号)部分の生成機能(暗号化)

3.1.2 プロトタイプに実装する画面

表 3-2 プロトタイプ実装画面

ASB のトップ画面(ログイン画面含む)	LC 関連の選択画面	・LC 登録情報入力画面 ・LC 登録情報修正画面 ・LC 検証画面 ・LC 通過ログ登録画面 ・LC 通過ログ取得画面
	DC 関連の選択画面	・DC 登録情報入力画面 ・DC 登録情報修正画面 ・LC 検証画面 ・DC 通過ログ登録画面

		・DC 通過ログ取得画面
SASB のトップ画面 (ログイン画面含む)	・LC 発番(依頼) ・DC 生成機能 ・DC 生成情報入力機能 ・DC 生成情報修正機能 ・Secret(暗号)部分の生成機能(暗号化)	

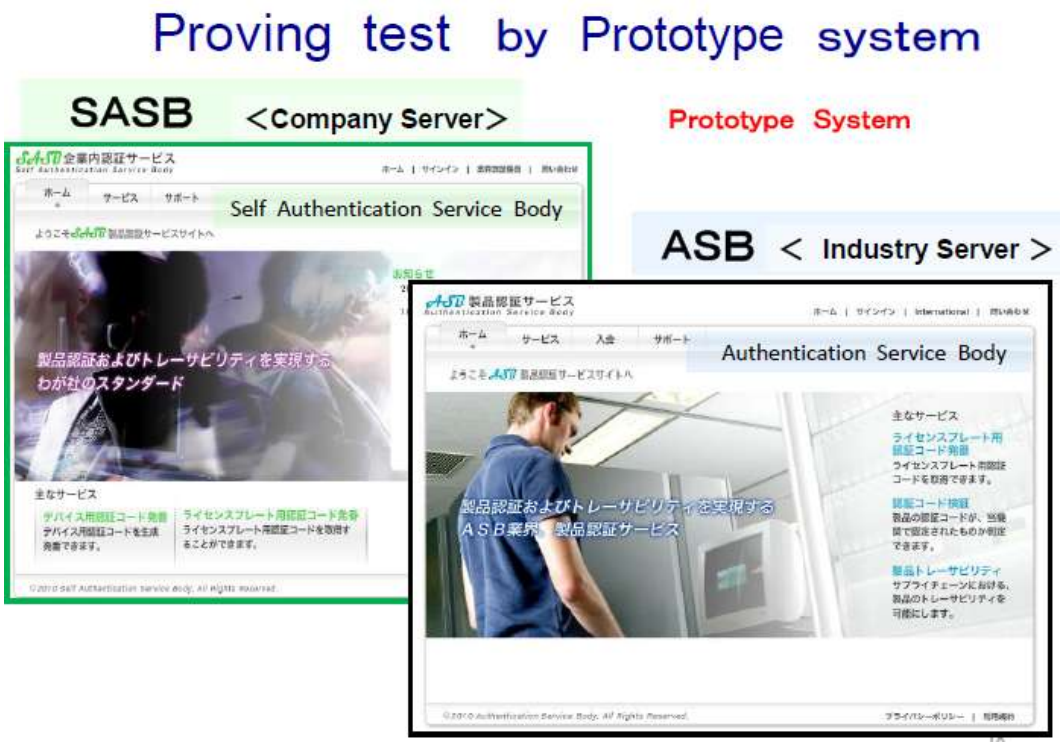


図 3-1 プトロタイプの画面イメージ図

3.2 プロトタイプ実証の結果概要

想定する関係者に対して、プロトタイプのデモを行い、処理フローや機能を説明し、実用性及び模倣品対策として期待する効果等を確認した。以下にその結果の概要を報告する。

表 3-3 プロトタイプ実証の結果概要

主なヒアリング先	・JEITA の各種委員会 ・ISO PC246/ TC247 の国内審議委員会 ・ISO PC246 ベルリン ・ISO TC247 フランス ・SEMI：Semicon Japan トレーサビリティ委員会 ・JIPDEC 主催の PC246/ TC247 セミナー (2010 年 12 月 1 日開催) ・その他、説明希望のあった印刷業界、試験関係、認証会社等に対して個別に説明を実施
主なコメント	・認証コードが強制でないことを賛同する。 ・プロトタイプの機能や処理フローは実用に耐える仕様である。 ・コストが問題である。(認証コード発番、システム登録、トレース取得、真贋判定等にかかるコストを抑える必要がある。)

3.3 プロトタイプ実証による課題の整理

本節では、電子認証応用領域のプロトタイプ実証の課題について示す。各課題について検討し、プロトタイプの改良や運用上の取り決めによって解決した内容については、課題と共にその解決方法も報告する。

3.3.1 ASB の運用に関する課題

表 3-4 ASB の運用に関する課題

	課題内容	解決策		
		システム対応	運用対応	内容
(1) トレース情報の管理コスト	真贋判定を求める者(主に顧客)には、トレース情報は不要であるが、トレース情報は重要であるため削除しない。また、ID情報やトレース情報は膨大に蓄積されるので、定期的に SASB が引き取る(不要であれが削除)する必要がある。		○	ASB が保管する情報は、1 年間とし、1 年以上経過した情報については、SASB に移管するし、ASB の管理工数を削減する。

3.3.2 SASB の運用に関する課題

表 3-5 SASB の運用に関する課題

	課題内容	解決策		
		システム対応	運用対応	内容
(2) 物と情報の接合時点での管理ミスの可能性	ＩＤが印字されたラベルという“物”と、購入した段階のＩＤという“情報”は、ラベルが物に貼られるまで、別々に管理されるため､管理ミス(貼り間違え)が発生する可能性がある。(箱に印字する物理ラベルと番号という情報は別に管理され、最終的には箱にラベルとして貼る又は、ラベル自体を印字される。このため、SASB の管理工数が増え、また管理ミスが発生する可能性がある。)		○	実運用を想定した管理策に対する取り決め等、ガイドラインの策定を検討する必要がある。
(3) 製品情報登録と管理工数の増大について	真贋判定(顧客視点)では、ＩＤの購入時点で製品情報が登録される方が望ましく、企業の管理コスト削減を考えるとＩＤの購入時点では製品情報を登録したくない。	○		ＩＤの購入時に製品情報の登録は必須であるが、品種などの概要名目などを認め、必要に応じてその登録情報を修正することで管理コストを削減する。
(4) ID の使い回しによる SASB の管理ミス	ＩＤの購入者によるＩＤの使い回し(再利用)は禁止しないが、使い回し(再利用)時の貼り間違い等、SASB の管理ミスが発生する可能性がある。		○	実運用を想定した管理策に対する取り決め等、ガイドラインの策定を検討する必要がある。
(5) SASB の罰則について	SASB は各コードや製品を正しく管理することを前提としているが、正しく管理しない場合の罰則等はない。(SASB が正しく管理しない場合の罰則等をどのように実施するかを検討しておく必要があると考えられる。)		○	上記同様。

3.3.3 システム全体に関わる課題

表 3-6 システム全体に関わる課題

	課題内容	解決策		
		システム対応	運用対応	内容
(6) コードに対する耐性の問題	真贋判定は、ＩＤの存在を第三者に確認する方法なので、ラベルや印字自体に判定技術が付加されているわけではない。(真贋判定ではコードの偽造防止が重要になるが、本システムでは SASB が個別に対応することを前提としている。このため、一カ所の信頼性の綻びがシステム全体の信頼性を低下させる可能性がある。)		○	本システムの真贋判定する方法に関して、適切に告知を行うことで、真贋判定顧客に理解を促す等、実運用時の告知手法を検討する必要がある。
(7) トレース情報の閲覧制御	製品及び部品供給者が管理する物流のトレース情報は、事業部間及び部門間を移動するトレース情報も含んでいるため、一般に公開したくない物流記録も含まれる。一方、顧客が真贋判定を行う場合は、上記の物流記録も含めた情報として確認できる場合も考えられる。以上のように一部の関係者には確認でき、他には確認できない情報開示方法が課題となっている。	○		電子証明書や ID/パスワードなど認証とアクセスコントロールを機能追加することを検討している。現時点ではコントロールすべき情報と閲覧者の関係など詳細については、さらに調査することが必要である。
(8) トレース情報の閲覧の多様性	上記の(7)とも関連するが、コンシューマ商品では、確認者(真贋判定者)がより顧客に近く、運用が異なる場合も考えられる。例えば、薬は処方する顧客が確認するが、ワイン等は顧客が確認する前にレストラン等の最終提供者が確認することも考えられる。	○		真贋判定の確認者は、SASB が任意に設定できることとし、トレース確認者を含め、閲覧者をシステム上で制限しないことで対応する。

3.4 電子証明書利用の効果について

プロトタイプ実証で確認できた電子証明書利用による効果について報告する。

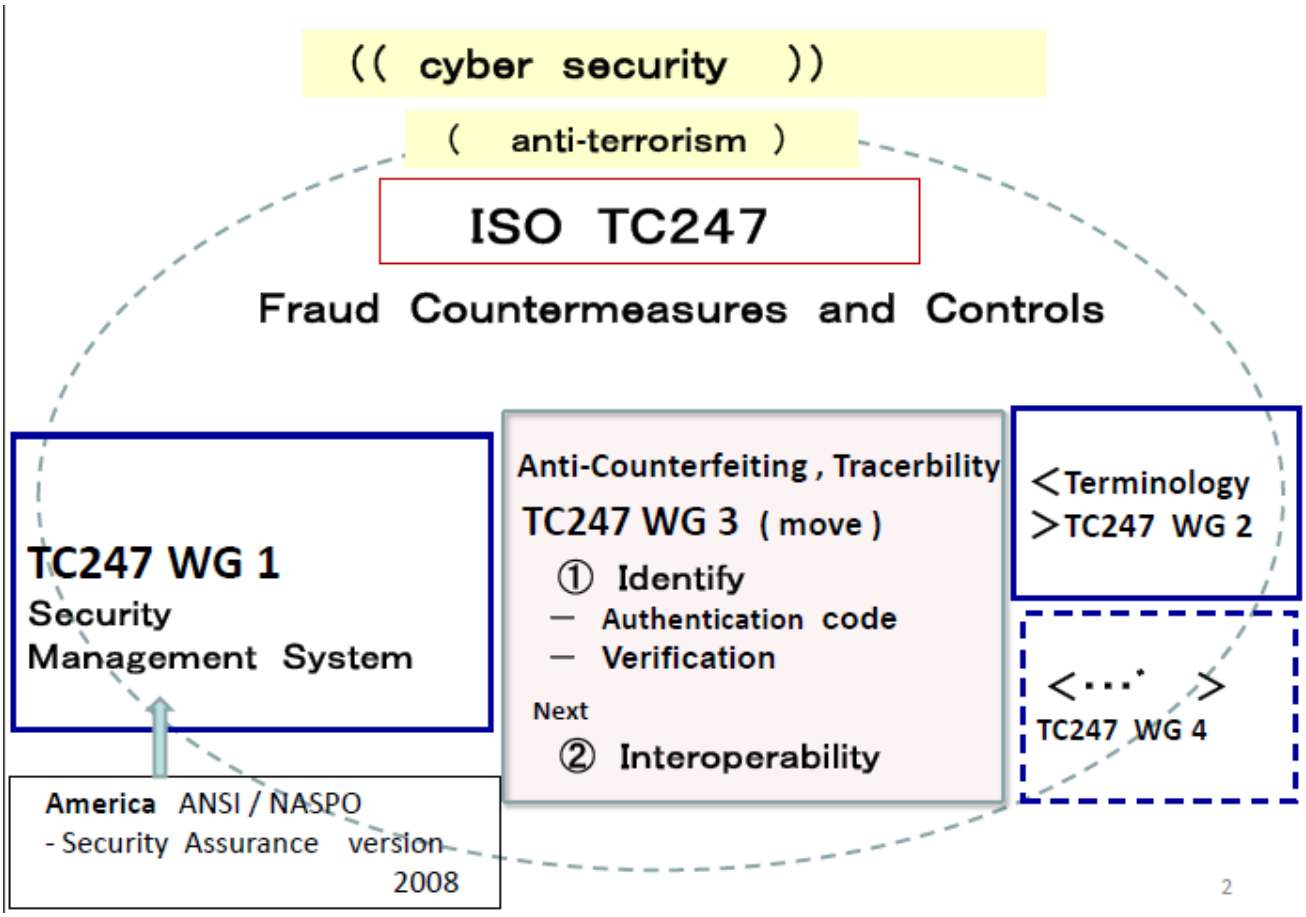
表 3-7 プロトタイプ実証による効果の確認結果

信頼性･セキュリティに関する効果	・ 電子証明書の組織情報は TTP で識別されているため信頼できる。 ・ 電子証明書を用いたアクセス制御が可能。
システム構築、運用に関する有効性	・ X.509 電子証明書は、OS や一般的なアプリケーションで既にサポートされているため、特別なソフトウェアを必要とせず、システムに利用できる。 ・ 電子証明書により、機械読取が可能であり、管理工数等の削減が期待できる。 ・ X.509 のプロファイルを共通書式にすることで、トレース時のログをコンパクトにすることが可能。 ・ 変更されやすい属性情報を記録しないことで期限満了まで証明

	書を利用することが可能(変更されやすい属性情報は、CSB のリポジトリで公開する等の運用が考えられる)。
国際相互運用で期待できる効果	・ 以下の要件を適用することで CSB の国際相互運用が可能となり海外製品の真贋判定にも利用可能。 ➢ 各国の法による CA 及び下位 CA の認可 ➢ ISO による CA 及び下位 CA の認定 ➢ ESTI-TS-102042 による CA 及び下位 CA の認定 ➢ Web Trust for CA による CA 及び下位 CA の認定

附属 A：ISO TC247 の概要

ISO TC247 では、真贋判定と物流トレースのための模倣品対策システムを検討している。WG1 ではセキュリティマネジメントシステムを検討し、WG2 では、技術的な検討が行われている。また、WG3 において、本事業に関連する識別性及び相互運用性が検討され、日本が提案している。ISO TC247 に関する詳細な情報は、国内審議団体である JIPDEC の公開情報(JIPDEC ISO/TC247、http://www.jipdec.or.jp/project/iso/tc247/index.html)を参照。



附属 B：データマトリックス ECC200(抜粋)

以下は、プロトタイプ実証時点において検討した証明書プロファイルの共通フォームである。

セル数	データセル		情報量			誤り訂正率
	セル数	ブロック数	数字	英数字	バイナリ	
10×10	8×8	1	6	3	1	62.50%
18×18	16×16	1	36	25	16	43.80%
22×22	20×20	1	60	43	28	40.00%
26×26	24×24	1	88	64	42	38.90%
32×32	14×14	4	124	91	60	36.70%
40×40	18×18	4	228	169	112	29.60%
52×52	24×24	4	408	304	202	29.20%
64×64	14×14	16	560	418	278	28.60%
80×80	18×18	16	912	682	454	29.60%
104×104	24×24	16	1632	1222	814	29.20%
120×120	18×18	36	2100	1573	1048	28.00%
132×132	20×20	36	2608	1954	1032	27.60%
144×144	22×22	36	3116	2335	1556	28.50%

附属 C: 証明書プロファイルの共通フォーム

以下は、プロトタイプ実証時点において検討した証明書プロファイルの共通フォームである。

Basic Certificate Fields

Certificate Fieids		Data type (The number of character)	Example for personnel certificate	Example for section/role certificate	備考
Subject					
	CountryName	PrintableString(2)	JP		Mandatoty ISO3166-1 alpha-2 国コード
	StateName	PrintableString(24)	Tokyo		Mandatoty 都道府県名
	LocalityName	PrintableString(24)	Chiyoda-ku		Mandatoty 市区町村名
	OrganizationName	PrintableString(56)	MHIR		Mandatoty LRA 所属団体名
	OrganizationUnitame1	PrintableString(32)	OU1-1.2.392.2000000.00.1.1000		Mandatoty JCAN 認定番号
	OrganizationUnitame2	PrintableString(16)	OU2-0800		Mandatoty LRA 所属団体が独自管理の管理番号
	CommonName	PrintableString(32)	BN-smith	BO-supply	Mandatoty 証明書発行対象の英字名(PS 名可)

Standard Certificate

Certificate Fieids		Data type (The number of character)	Example for personnel certificate	Example for section/role certificate	備考
Subject AltName					
	rfc822Name	IA5String(64)	derive@mhir.co.jp	supply@mhri.co.jp	証明書発行対象のメールアドレス

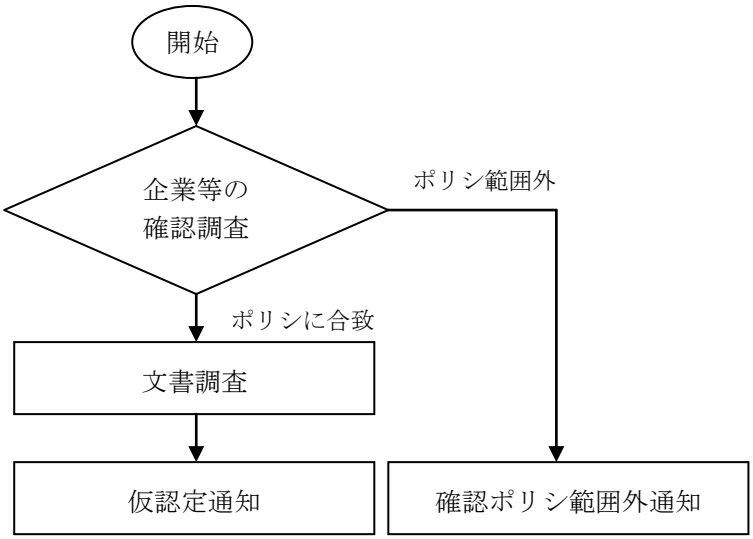
F「認定 LRA 運用マニュアル」

認定 LRA 運用マニュアルより、第 2 編のみ抜粋
全文閲覧は http://www.jipdec.or.jp/repository/を参照のこと

第 2 編 LRA 認定手続き

2.1 予備調査申請

(1) 手続き概略フロー



(2) 提出書類一覧

	文書名	記入例
企業等の確認調査	30-5020 LRA 認定調査申請書（A-1）	【No.1】
	30-5020 LRA 認定調査申請書（A-2）	【No.2】
	30-5020 LRA 認定調査申請書（A-3）	【No.3】
	30-5020 LRA 認定調査申請書（A-4）	【No.4】
文書調査	30-5510 認定 LRA 責任者体制表（A）	【No.5】
	30-5510 認定 LRA 責任者体制表（B）	【No.6】
	30-5600 管理台帳（A）	【No.7】
	30-5600 管理台帳（B）	【No.8】
	30-5600 管理台帳（E）	【No.9】

※文書調査の書類は、企業等の確認調査後提出すること。

(3) 予備調査の流れを次に示す。

(a) 仮認定までの流れ

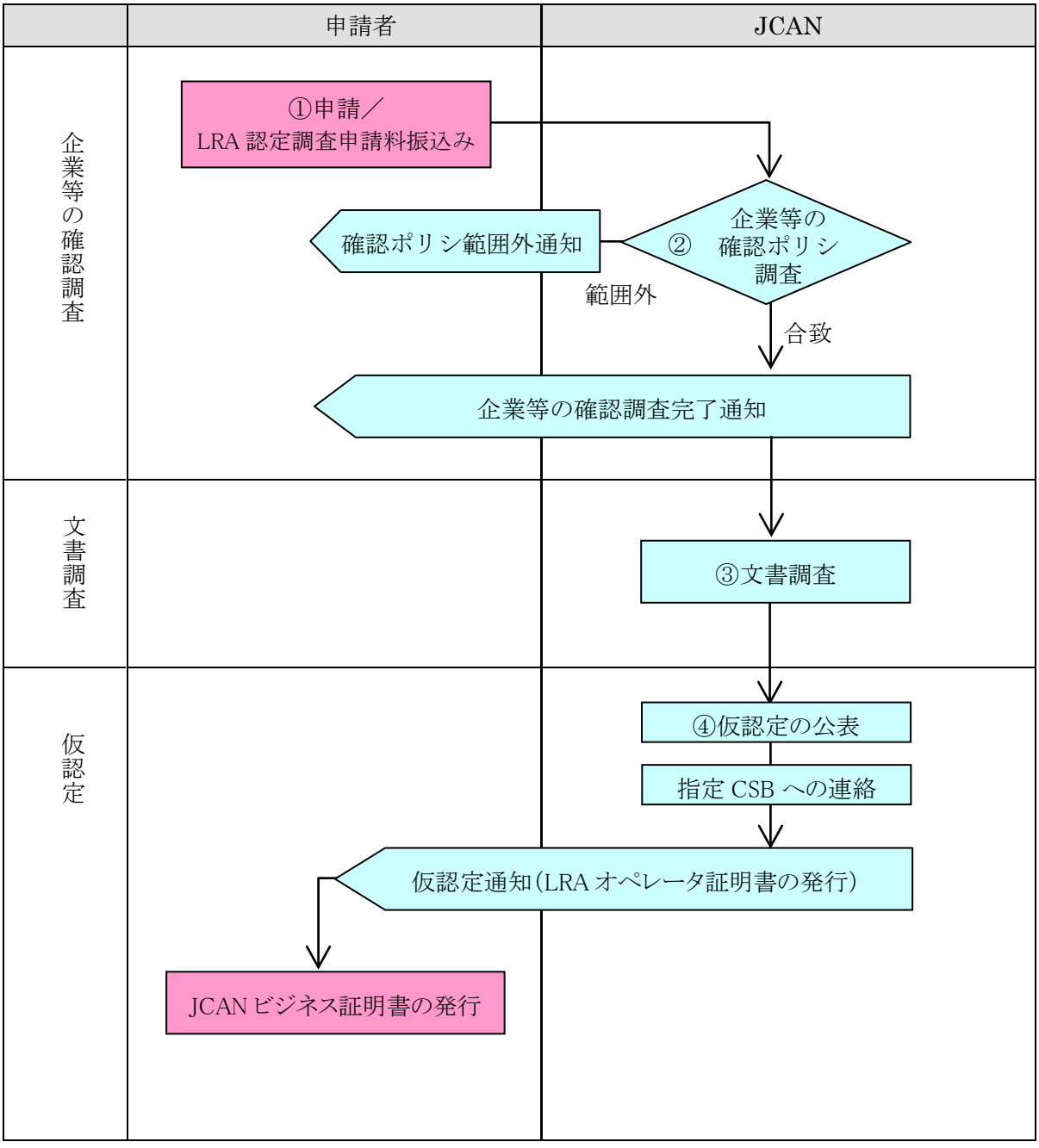


図２－１．予備調査の流れ（１）

(b) 仮認定から 3 ヶ月以内に初回申請を行わない場合の流れ

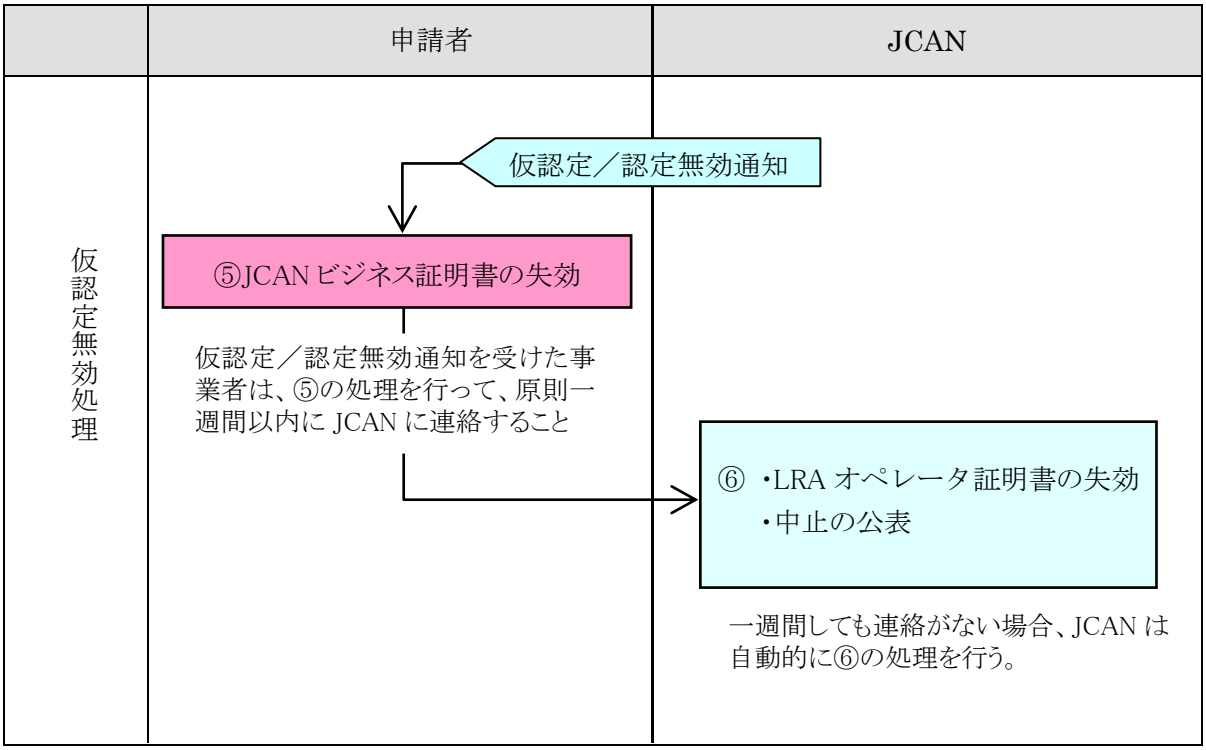


図 2－2．予備調査の流れ（2）

① 予備調査申請

申請窓口は、http://www.jipdec.or.jp/project/anshinkan/jcan/。
申請料は上記申請窓口を参照。料金は登録業務を行う LRA 単位。
但し、当面初回の申請料は無料。

② 企業等の確認ポリシ調査

企業等の確認ポリシに基づく調査を行い、合致していれば「企業等の確認調査完了通知」を行う。

■確認ポリシ
JIPDEC が指定するサイトにある DUNS 企業情報、TDB 企業情報のいずれかで企業等の実在を確認する。
上記で確認できない場合は、ROBINS(2011 年 4 月サービス開始予定)で実在を確認する。

③ 文書調査

文書調査に不備が無ければ次のステップに進む。

④ 仮認定の公表

文書調査が完了すると、仮認定の公表、指定 CSB への連絡及び「LRA オペレータ証明書」の発行が行われ、「JCAN ビジネス証明書の発行」ができるようになる。

⑤ 仮認定から 3 ヶ月以内に初回申請を行わない場合

仮認定／認定無効通知が行われる。
仮認定／認定無効通知が行われたら、発行した全「JCAN ビジネス証明書の失効」を行って、原則一週間以内に JCAN 連絡すること。

⑥ 中止の公表等

JCAN に連絡が来たら、「LRA オペレータ証明書」が失効され、中止の公表が行われる。
なお、一週間しても連絡がない場合、JCAN は自動的にこの処理を行う。

(4) 記入例

以下の記入例は、次のような仮想の組織（例）及び日程（例）を前提としています。

組織（例）

事業者名称 英字名 英字名略称	電子証明書推進センター株式会社 Electronic Certificate Promotion Center ECPC	
住所	東京都港区芝公園 3－5－8	
代表者(役職)	(代表取締役社長)高橋 三郎	
申請担当者(所属)	(本社 情報システム部)山田 太郎	
事業所	本社(東京)	大阪支社
LRA 責任者(役職)	(総務部長)佐藤 ベティ	(総務部長)木村 四郎
LRA 操作責任者	(情報システム部主任)山田 太郎	(情報システム部主任)後藤 二郎
LRA 内部監査責任者	(監査部)田中 一	

申請日程（例）

日程	イベント	備考
2010 年 1 月 10 日	予備調査申請	
4 月 2 日	仮認定取得	
4 月 20～21 日	教育実施	
5 月 1 日	電子証明書発行	
6 月 1 日	内部監査実施	エビデンス不要
6 月 20 日	LRA 内部監査責任者見直し確認	エビデンス不要
7 月 1 日	初回申請	仮認定取得後、3 ヶ月以内であること
8 月 1 日	認定取得	
10 月 1 日	教育実施	
10 月 5～6 日	内部監査実施	
10 月 20 日	LRA 内部監査責任者見直し確認	
11 月 1 日	更新申請	認定取得後、2～8 ヶ月であること
2011 年 2 月 1 日	認定取得	
3 月 15 日	LRA 操作責任者の異動	山田太郎→加藤五郎

【No.1】30-5020 A-1 『LRA 認定調査申請書　表紙』

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。
（LRA責任者が複数の場合は代表者1名で可。）但し、仮認定前の電子署名は不要。

LRA認定調査申請書　■予備調査　□初回　□更新

財団法人日本情報処理開発協会
JCAN事務局 行

西暦　2010年　1月　10日

フリガナ　デンシショウメイショ スイシンセンター カブシキガイシャ
申請事業者名称　電子証明書推進センター株式会社

フリガナ　タカハシ　サブロウ
代表責任者氏名　高橋 三郎

当社は、JCANの認定制度の趣旨に賛同し、下記の事項を承認し、JCANビジネス認定（登録業務）を申請します。

記

1. 「30-5250 JCAN運営要領」、「30-5270 JCAN検証者規約」、「30-5300 JCANビジネス証明書ポリシ」及び「30-5210　認定LRA共通事務取扱要領」を遵守すること
2. 「30-5250 JCAN運営要領」第10条の2に定める確認ポリシの範囲外となった場合は、仮認定できないこと
3. 認定の調査のために必要なすべての情報を開示すること
4. 開示する情報の一切は、事実であること
5. 「30-5250 JCAN運営要領」第8条に定める欠格事項に該当しないこと
6. 証明書の利用等による損害については「30-5300 JCANビジネス証明書ポリシ」に基づくこと
7. 認定後も含め現地調査を行う場合は対応すること

申請責任者
フリガナ　ﾔﾏﾀﾞ ﾀﾛｳ
氏　名　山田 太郎
フリガナ　ﾎﾝｼｬ ｼﾞｮｳﾎｳｼｽﾃﾑﾌﾞ
所　属　本社 情報システム部
郵便番号　105-0011
住　所　東京都港区芝公園3－5－8
電話番号　03-3436-xxxx
FAX番号　03-3436-xxxx
メールアドレス　BO-ra-honsha@ecpc.xx.jp
※申請責任者は、以後JCANとの連絡窓口となること。

□指定CSB未定
■指定CSB名　株式会社データセンター
※指定CSBは、http://www.jipdec.or.jp/project/anshinkan/jcan/を参照のこと

漢字変換できない文字は、カナで入力すること

【No.2】30-5020 A-2 『企業等属性情報』

JCAN手続き ： ■予備調査申請 ■初回申請 ■更新申請 ■変更届 □提出不要 本シートの電子文書を電子メールで提出。 ※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。 但し、仮認定前の電子署名は不要。			
事業者情報の入力			
事業者名（日本語）[必須]	正式名称で入力してください。 電子証明書推進センター株式会社	（全角文字）	
事業者名（カナ）[必須]	正式名称で入力してください。 デンシショウメイショスイシンセンターカブシキカイシャ	（全角カナ文字）	
事業者名（英字名）[必須]	ASCII文字（半角の英数字と記号）で56文字以下で入力してください Electronic Certificate Promotion Center 電子証明書のOrganizationNameに記載されます。	（半角文字）	
事業者の主たる事業所の所在地[必須]	東京都港区芝公園３－５－８	（全角文字）	
事業者の登記住所[必須]	東京都港区芝公園３－５－８	（全角文字）	
事業者を代表するウェブサイトのトップページURL	http://www.ecpc.xx.jp	（半角文字）	
企業コードの入力 ※「ROBINS」、「DUNSコード」、「帝国データバンク企業コード」いずれかの入力が必要です。 ご入力がない場合はJCANビジネス証明書が発行できない可能性がございます。			
ROBINS※	□登録済み □未登録 （2011年4月からサービス開始予定）		
DUNSコード※		（例）123456789（半角文字）	
	DUNSコードが複数ある場合は主たる事業所の所在地が登録されているコードの１つとします。		
帝国データバンク企業コード※		（例）123456789（半角文字）	
会社法人等番号		（例）1234-56-789012（半角文字）	
標準企業コード(CII)		（例）123456（半角文字）	
JAN企業コード		（例）123456789（半角文字）	
OID(取得年)	OID：	（例）1.2.392.200063（半角文字）	
	取得年： 年 月 日	（例）1995 04 08（半角文字）	
Pマーク認定番号(取得年)	認定番号：	（例）12345678(01)（半角文字）	
	取得年： 年 月 日	（例）1995 04 08（半角文字）	

【No.3】30-5020 A-3 『企業等概要表』

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。
　但し、仮認定前の電子署名は不要。

企業等名	電子証明書推進センター株式会社	代表電話	03-3436-xxxx
本社住所	〒105-0011　東京都港区芝公園3－5－8		
設立年月	1967年12月	主取引銀行（店/口座番号）	○○銀行（xxx-xxxxxxx）
資本金等	3,999百万円	資本系列	該当なし

企業等の沿革：

1967年12月20日「電子証明書推進センター株式会社」として設立。情報通信業を始める。
1970年4月1日　大阪支社開設。
1986年4月1日　ソフトウェア開発事業を開始。
1995年7月1日　サーバホスティング事業を開始。
2009年10月1日　Saas・クラウド事業を開始。

主要役員（非常勤は氏名の前に○印を記す）

氏名	役職名	担当部門
高橋　三郎	代表取締役社長	全社
佐藤 ベティ	常務取締役／総務部長	総務部門

事業規模

従業者数（単位：人）			事業規模（売上）（単位：百万円）		
前々期末 2008年	前期末 2009年	今期末（見込み） 2010年	前々期末 2008年	前期末 2009年	今期末（見込み） 2010年
90	95	100	4,500	5,000	6,000

関連企業（主なもの）	主要な取引先
なし	○○商事株式会社
団体の場合は、設立の根拠となる法律又は登録されている行政機関名	

漢字変換できない文字は、カナで入力すること

【No.4】30-5020 A-4『アンケート』

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　■変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。
　但し、仮認定前の電子署名は不要。

①LRAの業種

□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

②今後1年間の発行予定数

従業者数

	A01	A02
代表者・役員	5	
管理職	15	
担当	25	15

a)合計　60　名

区分
A01:雇用契約対象者
（人事DBを組織が管理）
A02:派遣契約等対象者
（人事DBは派遣元等が管理）
B03:組織外関係者
（会員、申請者、取引先、学生、患者等）
B04:関係会社/団体
B05:組織名、部門名、役割名等

今後1年間の発行予定数

	A01	A02	B03-05
代表者・役員	5		
管理職	15		
担当	25	15	15

b)合計　75　枚

(b÷a)×100＝　125%

③利用目的（全て）

■1. S/MIMEを利用した電子メール
■2. 署名付きPDF文書
■3. 署名付き文書(PDF以外)
■4. SSLによるクライアント認証
□5. SSLによる機器認証
□6. SSL以外の認証
□7. 長期署名
□8. ﾀﾞｳﾝﾛｰﾄﾞ元の署名
□9.電子商取引(企業間取引)
□10.電子商取引(企業対消費者)
□11.ログイン認証
□12.その他
(　　)

漢字変換できない文字は、カナで入力すること

【No.5】30-5510 A『一覧』

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　■変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

*1 電子証明書のCountryNameに転記される。日本はJPとする。
*2 電子証明書のStateNameに転記される。都道府県は-To,-Do,-Fu,-Kenとする。
*3 電子証明書のLocalityNameに転記される。 市区郡町村は-Shi,-Ku,-Gun,-Choまたは-Machi,-Muraまたは-Son
*4 ASCII文字(半角の英数字や記号などのこと)　(例)ABCabc123@_-

	LRA情報						LRA操作責任者			
	LRA名	所在地	国名*1 (2字以下*4)	都道府県名*2 (24字以下*4)	市区町村名*3 (24字以下*4)	窓口URL	氏名	フリガナ	窓口電話番号	窓口メールｱﾄﾞﾚｽ
1	本社	東京都港区芝公園3－5－8	JP	Tokyo-To	Minato-ku	http://www.ecpc.xx.jp/lra	山田 太郎	ヤマダ タロウ	03-3436-xxxx	BO-ra-honsha@ecpc.xx.jp
2	大阪支社	大阪府大阪市北区○○	JP	Osaka-Fu	Osaka-Shi	http://www.ecpc.xx.jp/lra	後藤 二郎	ゴトウ ジロウ	06-6313-xxxx	BN-goto2@ecpc.xx.jp
3										
4										
5										

漢字変換できない文字は、カナで入力すること

【No.6】30-5510 B『認定 LRA 責任者体制表』

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　■変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。
　但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：本社

認定LRA 責任者体制表

2010年1月10日

役割・担当	所属	氏名	フリガナ
LRA責任者※	本社 総務部	佐藤ベティ	サトウ ベティ
LRA操作責任者※	本社 情報システム部	山田太郎	ヤマダ タロウ
LRA内部監査責任者※	本社 監査部	田中一	タナカ ハジメ

※ 正社員又は正職員であること
※ 上記責任者は兼務不可
※ LRA責任者は人事担当の経営責任者または委任された者であること

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　■変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。
　但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：大阪支社

認定LRA 責任者体制表

2010年1月10日

役割・担当	所属	氏名	フリガナ
LRA責任者※	大阪支社 総務部	木村四郎	キムラ シロウ
LRA操作責任者※	大阪支社 情報システム部	後藤二郎	ゴトウ ジロウ
LRA内部監査責任者※	本社 監査部	田中一	タナカ ハジメ

※ 正社員又は正職員であること
※ 上記責任者は兼務不可
※ LRA責任者は人事担当の経営責任者または委任された者であること

【No.7】30-5600 A『管理台帳　A(表紙)』

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
A（表紙）の電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社　1.1版
LRA名：本社

管理台帳

2010年度（4月～翌年3月）

昨年度実績　本年度途中経過（ 6月 1日）

総有効枚数	0	45
総失効枚数	0	0

	承認日	LRA責任者	LRA内部監査責任者
上期点検	2010.6.1	佐藤	田中
下期点検			

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
A（表紙）の電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社　1.1版
LRA名：大阪支社

管理台帳

2010年度（4月～翌年3月）

昨年度実績　本年度途中経過（ 6月 1日）

総有効枚数	0	40
総失効枚数	0	0

	承認日	LRA責任者	LRA内部監査責任者
上期点検	2010.6.1	木村	田中
下期点検			

【No.8】30-5600 B『管理台帳　B(変更履歴)』

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
B（改訂履歴）の電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：本社

変更履歴

変更履歴No.	承認日	変更理由	LRA責任者	LRA操作責任者
1	2010.5.1	管理番号 10001～10045追加(45枚)	佐藤	山田
2				
3				

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
B（改訂履歴）の電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：大阪事業所

変更履歴

変更履歴No.	承認日	変更理由	LRA責任者	LRA操作責任者
1	2010.5.1	管理番号 11001～11040追加(40枚)	木村	後藤
2				
3				

【No.9】30-5600 E『管理台帳　E(発行申請 管理番号部分)』

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
E（発行申請［管理番号部分］）の電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：本社

※1 区分 A01：雇用契約対象者（人事DBを組織が管理している）
B02：派遣契約等対象者（人事DBは派遣元等が管理している）
B03：組織外関係者（会員、申請者、取引先、学生、患者等）
B04：関係会社/団体
B05：組織名、部門名、役割名等
※2 同一シートには複数の区分を入れて管理しない
※3 該当する区分コードがない場合は、事前にJCANに相談すること
※4 'B'はBasic、'A'はAdvanced、'JQ'(当面使用しない)はJCAN Qualifiedの略
※5 ASCII文字（半角の英数字や記号などのこと）　（例）ABCabc123@_-
※6 ① PS名の種類(推奨)
・社員等向け：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)）
・ID向け：最初に'ID-'をつける
② 姓名を入れる場合の表記方法(推奨)
・姓.名(組織)の順で記入（例 BN-Sato.Betty(ECPC)）
但し、名及び（組織）の記載はオプション
・使用できる文字は英数字(大文字可)とピリオド,カッコのみ
・姓と名の最初の文字だけ大文字とする
③ 個人情報の利用
・LRAは、「証明書受信者が証明書の個人情報を電子メール及び電子認証に使うこと」に関する同意を証明書発行前に証明書利用者から得ていること。
※7 メールアドレスは大文字を使わない

発行申請[管理番号部分]

管理番号		メールｱﾄﾞﾚｽ (rfc822)	PS名※6 (CN)	PIN1 (証明書用)	内部管理データ(提出不要)						
区分※1※2※3※4	ローカル番号(OU2)				PIN2 (JCANﾊﾟｽ用)	社員No.	実名	貸与承認日	回収承認日	作業ステータス	有効期間満了月
(4字以下)※5	(16字以下)※5	(64字以下)※5※7	(32字以下)※5	(12字)※5	(8字)※5	(20字以下)※5	(20字以下)※5	(6字以下)※5	(6字以下)※5	(1字)※5	(6字以下)※5
A01	1.2	sato-betty@ecpc.xx.jp	BN-Sato.Betty	3782493							
A01	1.3	yamada-taro@ecpc.xx.jp	BN-Yamada.Taro	12506846							

JCAN手続き ： ■予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
E（発行申請［管理番号部分］）の電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

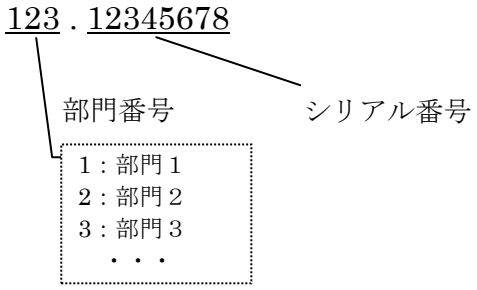
会社名／団体名：電子証明書推進センター株式会社
LRA名：大阪支社

※1 区分 A01：雇用契約対象者（人事DBを組織が管理している）
B02：派遣契約等対象者（人事DBは派遣元等が管理している）
B03：組織外関係者（会員、申請者、取引先、学生、患者等）
B04：関係会社/団体
B05：組織名、部門名、役割名等
※2 同一シートには複数の区分を入れて管理しない
※3 該当する区分コードがない場合は、事前にJCANに相談すること
※4 'B'はBasic、'A'はAdvanced、'JQ'(当面使用しない)はJCAN Qualifiedの略
※5 ASCII文字（半角の英数字や記号などのこと）　（例）ABCabc123@_-
※6 ① PS名の種類(推奨)
・社員等向け：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)）
・ID向け：最初に'ID-'をつける
② 姓名を入れる場合の表記方法(推奨)
・姓.名(組織)の順で記入（例 BN-Sato.Betty(ECPC)）
但し、名及び（組織）の記載はオプション
・使用できる文字は英数字(大文字可)とピリオド,カッコのみ
・姓と名の最初の文字だけ大文字とする
③ 個人情報の利用
・LRAは、「証明書受信者が証明書の個人情報を電子メール及び電子認証に使うこと」に関する同意を証明書発行前に証明書利用者から得ていること。
※7 メールアドレスは大文字を使わない

発行申請[管理番号部分]

管理番号		メールｱﾄﾞﾚｽ (rfc822)	PS名※6 (CN)	PIN1 (証明書用)	内部管理データ(提出不要)						
区分※1※2※3※4	ローカル番号(OU2)				PIN2 (JCANﾊﾟｽ用)	社員No.	実名	貸与承認日	回収承認日	作業ステータス	有効期間満了月
(4字以下)※5	(16字以下)※5	(64字以下)※5※7	(32字以下)※5	(12字)※5	(8字)※5	(20字以下)※5	(20字以下)※5	(6字以下)※5	(6字以下)※5	(1字)※5	(6字以下)※5
A01	2.1	kimura-shiro@ecpc.xx.jp	BN-Kimura.Shiro	29372248							
A01	2.2	goto2@ecpc.xx.jp	BN-Goto2	6993102							

ローカル番号の例（認定 LRA 所属団体が発番する番号）



電子証明書の発行手順

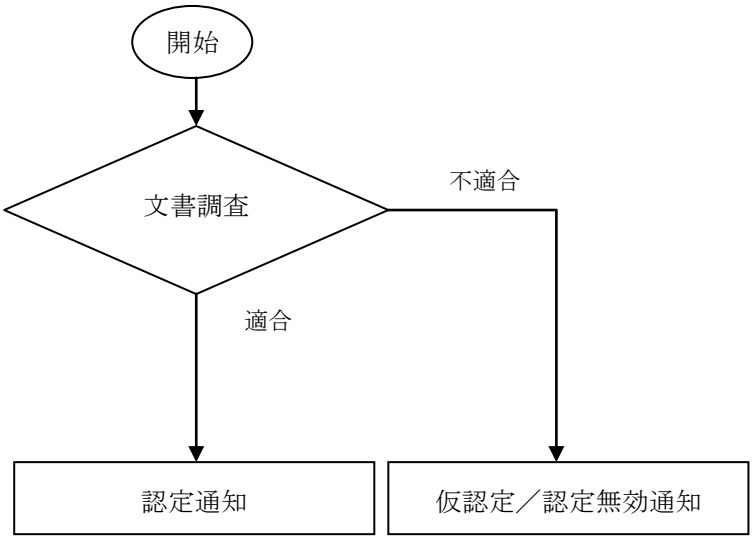
電子証明書の発行に際しては、指定 CSB から配布される発行要求シートに、管理台帳の必要部分をコピーして発行要求を行う。

作業ステータスの例

A 申請中
B ダウンロード中
C 保管済み
D 貸与済み
E 失効済み

2.2 初回申請

(1) 手続き概略フロー



(2) 提出書類一覧

	文書名	記入例
文書調査	30-5020 LRA 認定調査申請書（A-1）	【No.1】
	30-5020 LRA 認定調査申請書（A-2）	【No.2】
	30-5020 LRA 認定調査申請書（A-3）	【No.3】
	30-5020 LRA 認定調査申請書（A-4）	【No.4】
	30-5510 認定 LRA 責任者体制表（A）	【No.5】
	30-5510 認定 LRA 責任者体制表（B）	【No.6】
	30-5600 管理台帳（A）	【No.7】
	30-5600 管理台帳（B）	【No.8】
	30-5600 管理台帳（E）	【No.9】
	30-5700 認定 LRA 作業記録（A）	【No.10】
	30-5700 認定 LRA 作業記録（B）	【No.11】
	30-5800 教育記録 (A)	【No.12】
	30-5800 教育記録 (B)	【No.13】
	30-5900 内部監査実施記録（A）	第 4 編【No.16】
	30-5900 内部監査実施記録（B）	第 4 編【No.17】
	30-5900 内部監査実施記録（C）	第 4 編【No.18】

(3) 初回申請の流れを次に示す。

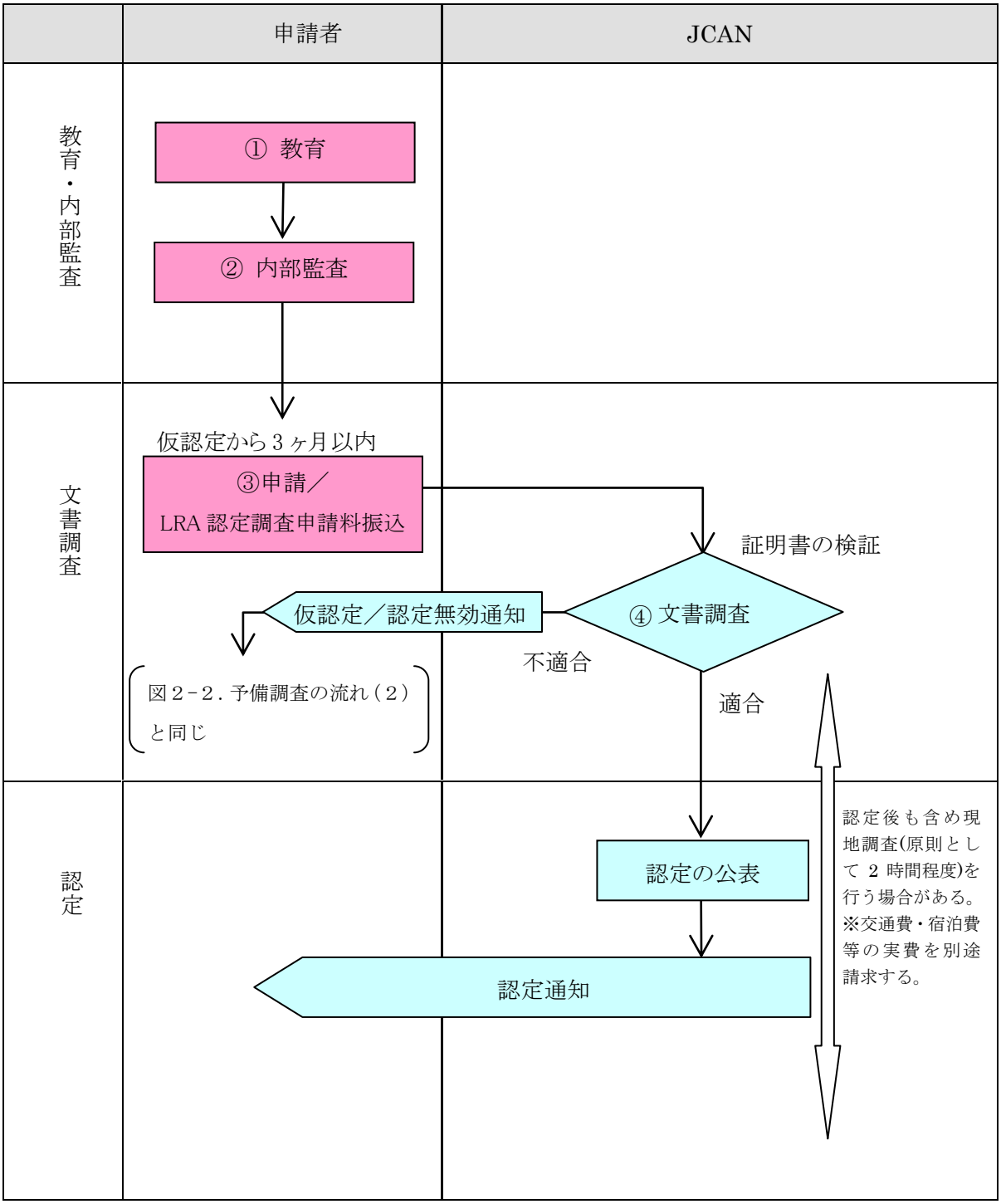


図３． 初回申請の流れ

① 教育

・申請に先立ち、定期的な教育を実施する。
ただし、以下の場合は遅滞なく臨時の教育を実施するものとする。
- 規程の改定
- 要員の変更

・教育は「30-5210 認定 LRA 共通事務取扱要領」、「30-5300 JCAN ビジネス証明書ポリシ」等規程の周知を目的とする。

・教育を実施した場合は、教育結果を記録する。

② 内部監査

第 4 編による。

③ 申請

申請窓口は、http://www.jipdec.or.jp/project/anshinkan/jcan/。
申請料は上記申請窓口を参照。料金は登録業務を行う LRA 単位。

④ 文書調査

仮認定から 3 ケ月以内に「初回申請」行われると文書調査が行われる。
文書調査に不備が無ければ認定の公表が行われる。
※文書審査で不適合になると「仮認定／認定無効通知」が行われる。

(4) 記入例

（No.1～9 は予備調査申請と同じ）

【No.10】30-5700A 『認定 LRA 作業記録 A（表紙）』

JCAN手続き ： □予備調査申請 ■初回申請 ■更新申請 □変更届 □提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：本社

認定LRA
作業記録

2010年度

	承認日	LRA責任者	点検実施者
上期点検	2010.4.20	佐藤	田上
下期点検			

JCAN手続き ： □予備調査申請 ■初回申請 ■更新申請 □変更届 □提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：大阪支社

認定LRA
作業記録

2010年度

	承認日	LRA責任者	点検実施者
上期点検	2010.4.20	木村	高坂
下期点検			

【No.11】30-5700B 『認定 LRA 作業記録 B（作業記録）』

JCAN手続き ： □予備調査申請 ■初回申請 ■更新申請 □変更届 □提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：本社

作業記録（保管・廃棄等）

日付	区分	作業者氏名	管理番号	備考
2010.5.2	■保管 □廃棄 □持出 □返却	山田	1.0001	PKCS#12アーカイブ
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			

JCAN手続き ： □予備調査申請 ■初回申請 ■更新申請 □変更届 □提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：大阪支社

作業記録（保管・廃棄等）

日付	区分	作業者氏名	管理番号	備考
2010.5.2	■保管 □廃棄 □持出 □返却	後藤	2.0001	PKCS#12アーカイブ
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			
	□保管 □廃棄 □持出 □返却			

【No.12】30-5800A『教育記録 A(表紙)』

JCAN手続き ： □予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：本社

教育記録

2010年度

定期的な教育	実施日(年1回以上)	参加率(60%以上)
初回	2010.4.20	40名(90%)
最終回	2010.4.21	計45名(100%)

	承認日	LRA責任者	点検実施者
上期点検	2010.4.20	佐藤	青田
下期点検			

JCAN手続き ： □予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：大阪支社

教育記録

2010年度

定期的な教育	実施日(年1回以上)	参加率(60%以上)
初回	2010.4.20	32名(80%)
最終回	2010.4.21	計40名(100%)

	承認日	LRA責任者	点検実施者
上期点検	2010.4.20	木村	笹木
下期点検			

【No.13】30-5800B『教育記録 B(教育記録)』

JCAN手続き ： □予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：本社

教育記録

実施日	講師	受講者	教育テーマ	備考
2010.4.20	佐藤　ベティ	40名	以下規程の周知 ・30-5210 JCAN認定LRA共通事務取扱要領 ・30-5300 JCANビジネス証明書ポリシ	
2010.4.21	佐藤　ベティ	5名	以下規程の周知 ・30-5210 JCAN認定LRA共通事務取扱要領 ・30-5300 JCANビジネス証明書ポリシ	4/20欠席者対応

JCAN手続き ： □予備調査申請　■初回申請　■更新申請　□変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行したLRA責任者の電子署名を付けること。但し、仮認定前の電子署名は不要。

会社名／団体名：電子証明書推進センター株式会社
LRA名：大阪支社

教育記録

実施日	講師	受講者	教育テーマ	備考
2010.4.20	木村　四郎	32名	以下規程の周知 ・30-5210 JCAN認定LRA共通事務取扱要領 ・30-5300 JCANビジネス証明書ポリシ	
2010.4.21	木村　四郎	8名	以下規程の周知 ・30-5210 JCAN認定LRA共通事務取扱要領 ・30-5300 JCANビジネス証明書ポリシ	4/20欠席者対応

2.3 更新申請

(1) 手続き概略フロー

初回申請と同じ。

(2) 提出書類一覧

初回申請と同じ。

(3) 更新申請の流れを次に示す。

初回申請と同じ。

(4) 記入例

初回申請と同じ。

2.4 変更届

(1) 変更届は、以下の場合に提出すること。

・30-5510 の内容に変更があった場合。

・30-5020 A-1、A-2、A-4（発行予定数）の内容に変更があった場合。

(2) 変更届の流れを次に示す。

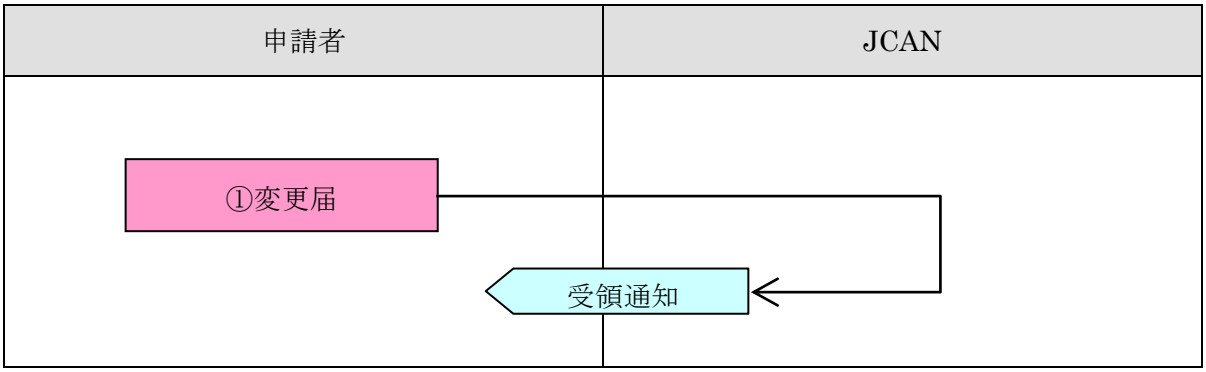


図５．変更届けの流れ

① 「変更届」が提出されると、「受領通知」が行われる。

(3) 提出書類一覧

	文書名	記入例
変更届	30-5020 LRA 認定調査申請書（A-2）	【No.2】
	30-5020 LRA 認定調査申請書（A-4）	【No.4】
	30-5510 認定 LRA 責任者体制表（A）	【No.5】
	30-5510 認定 LRA 責任者体制表（B）	【No.6】
	30-5020 LRA 認定調査申請書（D）	【No.14】

(4) 記入例

（No.2,4,5 は予備調査申請と同じ）

【No.14】30-5020 D『変更届』

JCAN手続き ： □予備調査申請　□初回申請　□更新申請　■変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行した登録業務責任者の電子署名を付けること。
　但し、仮認定前の電子署名は不要。

変更届

財団法人日本情報処理開発協会
JCAN事務局 行

西暦　2011年　3月　15日

JCAN認定番号　xxxxxxxx

フリガナ　デンシショウメイショ スイシンセンター カブシキガイシャ
申請事業者名称　電子証明書推進センター株式会社

フリガナ　タカハシ サブロウ
代表責任者氏名　高橋 三郎

変更項目	変更内容
□30-5510の内容変更	添付資料 30-5510（A、B）参照
□30-5020 A-2の内容変更	添付資料 30-5020（A-2）参照
□30-5020 A-4（発行予定数）の内容変更	添付資料 30-5020（A-4）参照
■30-5020 A-1の内容変更	本紙参照

申請責任者
フリガナ　カトウ ゴロウ
氏　名　加藤 五郎
フリガナ　ホンシャ ジョウホウシステムブ
所　属　本社 情報システム部
住　所　東京都港区芝公園3－5－8
電話番号　03-3436-xxxx
FAX番号　03-3436-xxxx
メールアドレス　ra-honsha@ecpc.xx.jp

※申請責任者は、以後JCANとの連絡窓口となること。

漢字変換できない文字は、カナで入力すること

2.5 終了届

(1) 終了届の流れを次に示す。

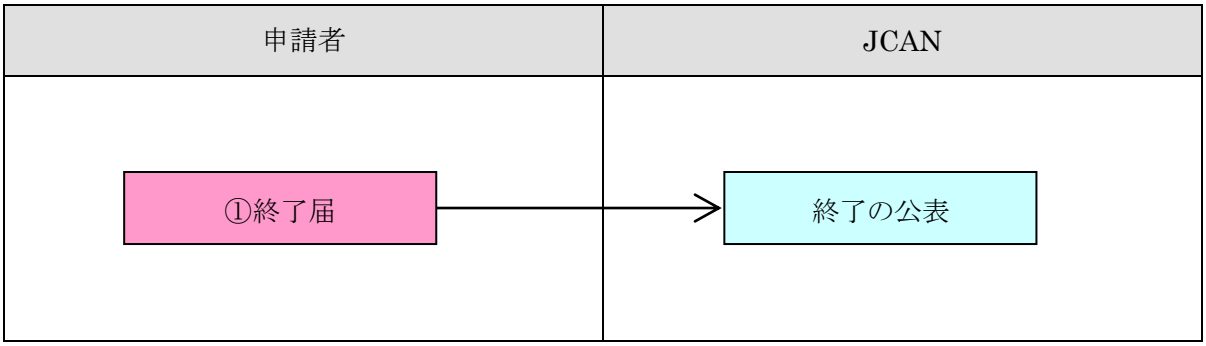


図６．中止届の流れ

① 「終了届」が提出されると、「終了の公表」が行われる。

(2) 提出書類一覧

	文書名	記入例
終了届	30-5020 LRA 認定調査申請書（E）	【No.15】

(3) 記入例

【No.15】30-5020 E『終了届』

JCAN手続き ： □予備調査申請　□初回申請　□更新申請　□変更届　□提出不要
本シートの電子文書を電子メールで提出。
※電子文書及び電子メールには自社／自団体で発行した登録業務責任者の電子署名を付けること。
　但し、仮認定前の電子署名は不要。

終了届

財団法人日本情報処理開発協会
JCAN事務局 行

西暦○○○年○○月○○日

JCAN認定番号 xxxxxxxx

フリガナ デンシショウメイショ スイシンセンター カブシキガイシャ
申請事業者名称 電子証明書推進センター株式会社

フリガナ タカハシ サブロウ
代表責任者氏名 高橋 三郎

当社は、JCANビジネス認定（登録業務）を終了します。

終了の理由 ㈱港区商事との合併のため。

申請責任者
フリガナ ﾔﾏﾀﾞ ﾀﾛｳ
氏　名 山田 太郎
フリガナ ﾎﾝｼｬ ｼﾞｮｳﾎｳｼｽﾃﾑﾌﾞ
所　属 本社 情報システム部
住　所 東京都港区芝公園3－5－8
電話番号 03-3436-xxxx
FAX番号 03-3436-xxxx
メールアドレス ra-honsha@ecpc.xx.jp

※申請責任者は、以後JCANとの連絡窓口となること。

漢字変換できない文字は、カナで入力すること

G「電子証明書インストールガイド」

30-5010 別冊

電子証明書インストールガイド

電子メール/Microsoft Office/Acrobat

本ガイドは平成 23 年 1 月 27 日に発行したものです。
最新版は　http://www.jipdec.or.jp/repository/　でダウンロードしてください。

平成 23 年 1 月
JIPDEC
財団法人 日本情報処理開発協会

本事業は、競輪の補助金を受けて実施しています。
http://ringring-keirin.jp

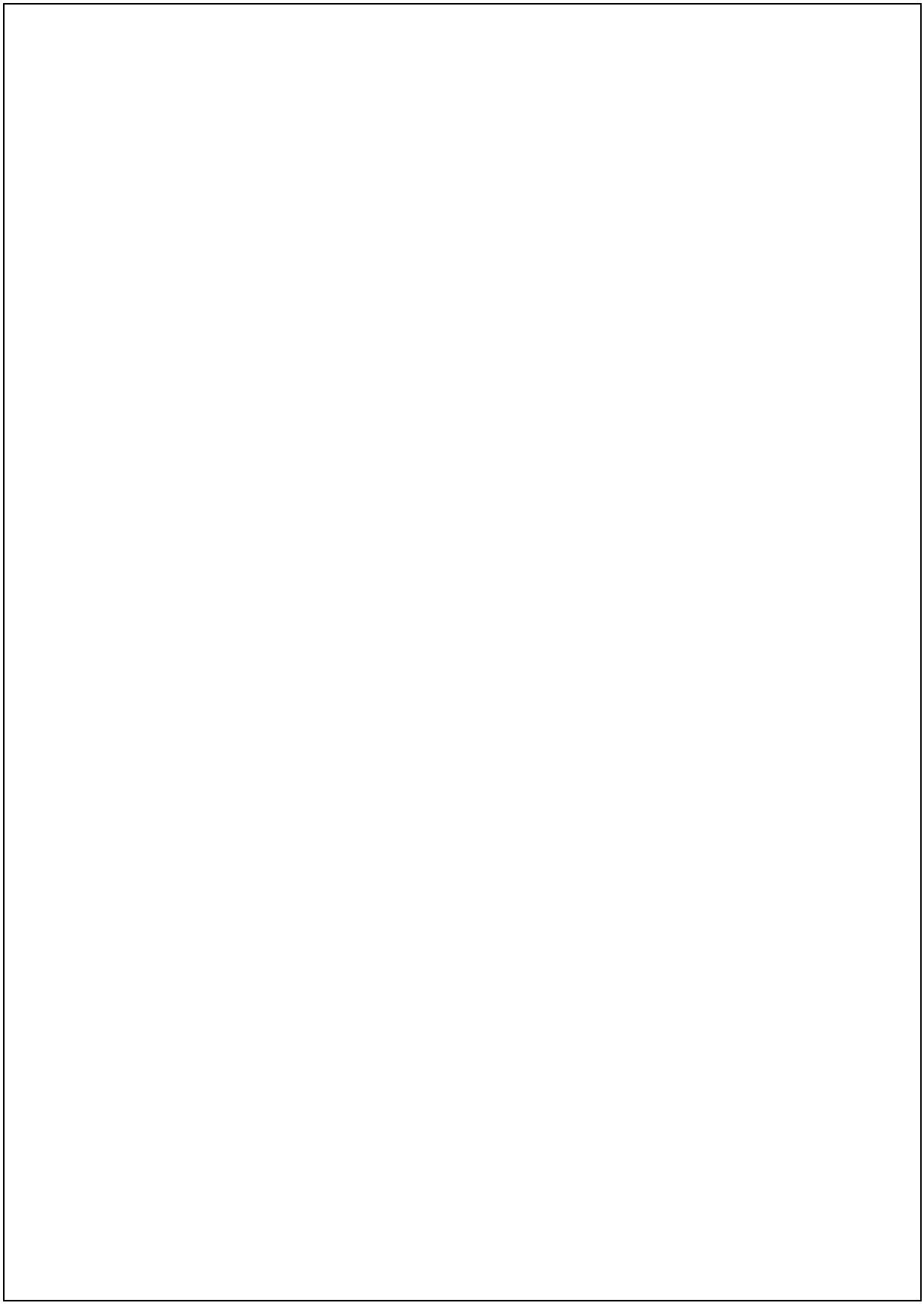
電子証明書インストールガイド

電子メール/Microsoft Office/Acrobat

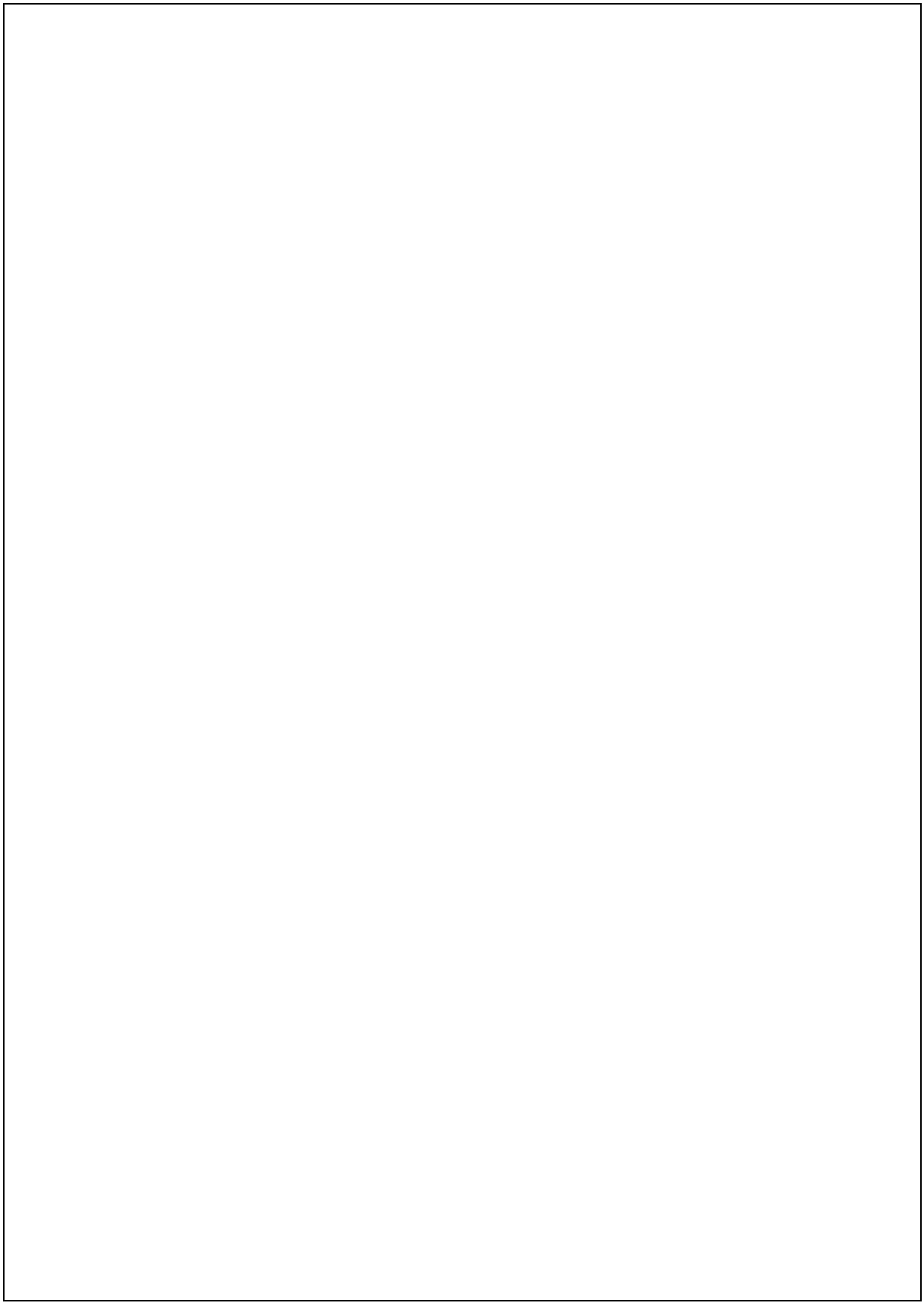
平成 23 年 1 月

JIPDEC

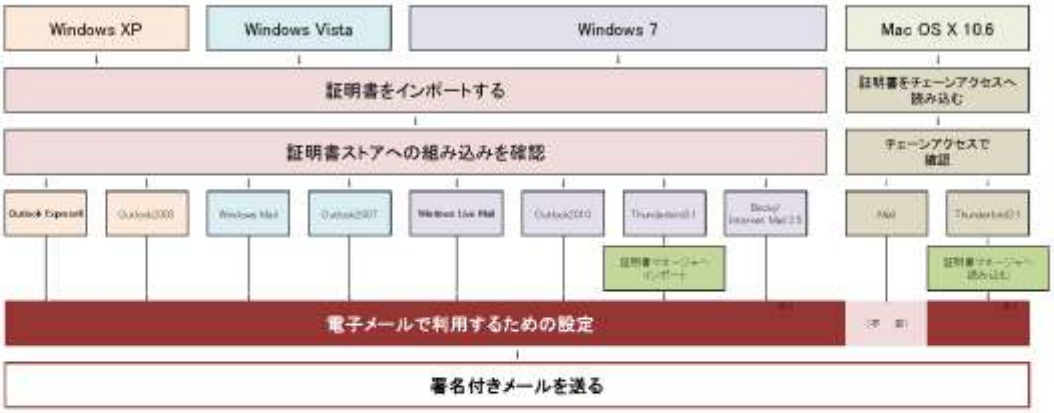
財団法人 日本情報処理開発協会



CONTENTS



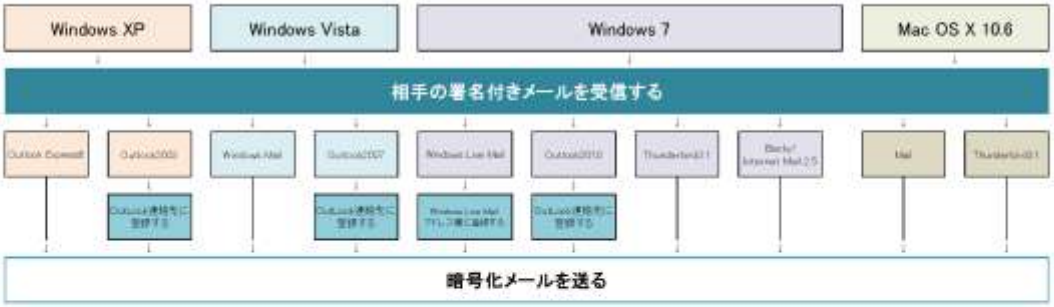
1. 署名付きメールを送るまでの手順



署名付きメールは，メッセージの内容が送信者により署名されていること，および転送中に改ざんされていないことを受信者に証明します。

※1 ここでは Thunderbird へ証明書を読み込みます。
Firefox に証明書を読み込む場合は，Windows，Mac ともに P41 の『1.証明書を「証明書マネージャ」にインポートします。』を参考にしてください。
その際，Windows の場合，①は「Firefox メイン画面」，Mac の場合，「Firefox メイン画面」の<Firefox>メニューの<環境設定>に読み替え，②の「証明書」タブは「暗号化」タブに読み替えてください。

2. 暗号化メールを送るまでの手順



暗号化メールは，メッセージのプライバシーを保護できます。暗号化に使用された公開キーと対になる秘密キーを持つ受信者だけが，このメッセージを読むことができます。

署名付き暗号化メールを送る
上記の 1.と 2.ができる環境が整えば，署名付き暗号化メールを送ったり，受信して読むことができます。

証明書を Windows OS へインポートする方法

Windows XP（Internet Explorer 6）の場合

インポートウィザードを起動して証明書をインポートします。 インポート

① 管理者から配布された証明書ファイル（xxxxx.p12 ファイル）をダブルクリックします。

② 「証明書のインポートウィザード」が起動します。
次へ ボタンをクリックします。

③ 変更する必要はありません。次へ ボタンをクリックします。

④ 管理者から証明書ファイルと一緒に配布されたパスワードを入力し、「このキーをエクスポート可能にする、キーのバックアップやトランスポートを可能にします。」を✓して、次へ ボタンをクリックします。

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」のオプションが選択されていることを確認し、次へ ボタンをクリックします。

⑥ 証明書のインポートウィザードの完了画面が表示されます。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、OK ボタンをクリックします。

以上で OS へのインポートは終了です。

次に証明書ストアに組み込まれたことを確認します。 推奨

① Internet Explorer を開き、≪ツール≫メニューから≪インターネットオプション≫をクリックします。

② ［インターネットオプション］ダイアログボックスの「コンテンツ」タブをクリックし、証明書 ボタンをクリックします。

③ 「個人」タブに新しい証明書が組み込まれていることを確認します。
確認する証明書を選択し、表示 ボタンをクリックします。

■「全般」タブ
証明書の有効性などを確認できます。

■「詳細」タブ
証明書の各項目名（フィールド）とその値を確認できます。
E = 署名者のメールアドレス
CN = 署名者の氏名（英語表記）
OU = 証明書所有組織の連絡先
O = 署名者の所属組織・団体名（英語表記）
S = 都道府県
C = 国名

■「証明のパス」タブ
証明書の階層構造が確認できます。

確認後は、OK ボタンをクリックして［証明書］ダイアログボックスおよび［インターネットオプション］ダイアログボックスを閉じます。

以上で確認は終了です。Windows を再起動してください。

Windows Vista（Internet Explorer 7）の場合

インポートウィザードを起動して証明書をインポートします。 インポート

① 管理者から配布された証明書ファイル（xxxxx.p12 ファイル）をダブルクリックします。

② 「証明書のインポートウィザード」が起動します。
次へ ボタンをクリックします。

③ 変更する必要はありません。次へ ボタンをクリックします。

④ 管理者から証明書ファイルと一緒に配布されたパスワードを入力し、「このキーをエクスポート可能にする、キーのバックアップやトランスポートを可能にします。」と「すべての拡張プロパティを含める」を✔して、次へ ボタンをクリックします。

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」のオプションが選択されていることを確認し、次へ ボタンをクリックします。

⑥ 証明書のインポートウィザードの完了画面が表示されます。完了 ボタンをクリックします。

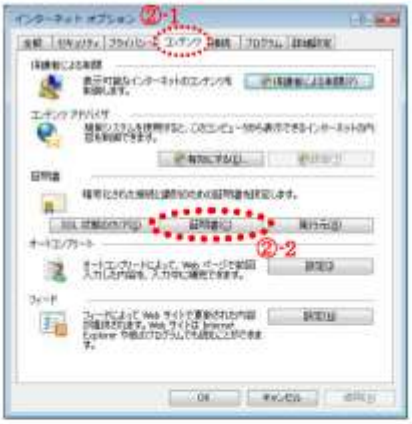
⑦ 「正しくインポートされました。」というメッセージが表示されたことを確認し、OK をクリックします。

以上で OS へのインポートは終了です。

次に証明書ストアに組み込まれたことを確認します。 省略

① Internet Explorer を開き、≪ツール≫メニューから≪インターネットオプション≫をクリックします。

② ［インターネットオプション］ダイアログボックスの「コンテンツ」タブをクリックし、証明書 ボタンをクリックします。



③　「個人」タブに新しい証明書が組み込まれていることを確認します。
確認する証明書を選択し、表示 ボタンをクリックします。

表示された［証明書］ダイアログボックスで確認できる内容は、P5 と同様です。

■「全般」タブ

■「詳細」タブ

■「証明のパス」タブ

確認後は、OK ボタンをクリックして［証明書］ダイアログボックスおよび［インターネットオプション］ダイアログボックスを閉じます。

以上で確認は終了です。Windows を再起動してください。

Windows 7（Internet Explorer 8）の場合

インポートウィザードを起動して証明書をインポートします。 インポート

① 管理者から配布された証明書ファイル（xxxxx.p12 ファイル）をダブルクリックします。

② 「証明書のインポートウィザード」が起動します。次へ ボタンをクリックします。

③ 変更する必要はありません。次へ ボタンをクリックします。

④ 管理者から証明書ファイルと一緒に配布されたパスワードを入力し、「このキーをエクスポート可能にする、キーのバックアップやトランスポートを可能にします。」と「すべての拡張プロパティを含める」を✓して、次へ ボタンをクリックします。

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」のオプションが選択されていることを確認し、次へ ボタンをクリックします。

⑥ 証明書のインポートウィザードの完了画面が表示されます。完了 ボタンをクリックします。

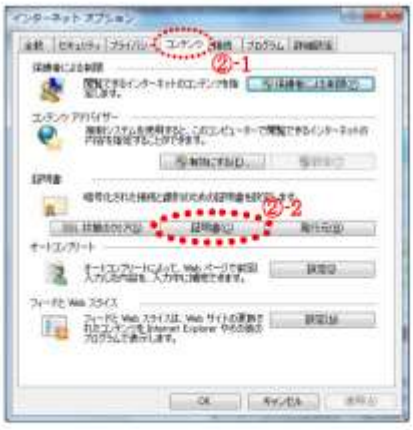
⑦ 「正しくインポートされました」というメッセージが表示されたことを確認し、OK ボタンをクリックします。

以上で OS へのインポートは終了です。

次に証明書ストアに組み込まれたことを確認します。 確認

① Internet Explorer を開き、≪ツール≫メニューから≪インターネットオプション≫をクリックします。

② ［インターネットオプション］ダイアログボックスの「コンテンツ」タブをクリックし、証明書 ボタンをクリックします。



③　「個人」タブに新しい証明書が組み込まれていることを確認します。
確認する証明書を選択し、表示 ボタンをクリックします。

表示された［証明書］ダイアログボックスで確認できる内容は、P5 と同様です。

■「全般」タブ

■「詳細」タブ

■「証明のパス」タブ

確認後は、OK ボタンをクリックして［証明書］ダイアログボックスおよび［インターネットオプション］ダイアログボックスを閉じます。

以上で確認は終了です。Windows を再起動してください。

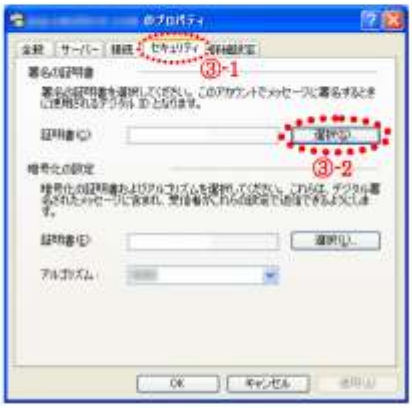
Outlook Express 6

1　電子メールで利用するための設定

① ≪ツール≫メニューから≪アカウント≫をクリックします。

② ［インターネットアカウント］ダイアログボックスの「メール」タブをクリックし、証明書を利用するメールアカウントを選択し、プロパティ ボタンをクリックします。

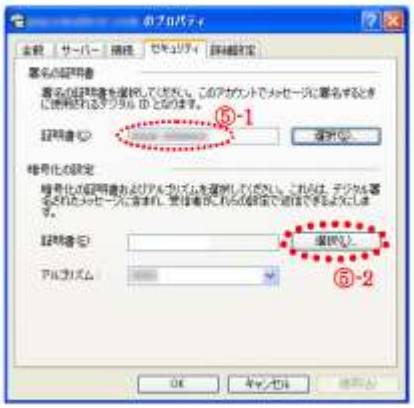
③ プロパティダイアログボックスの「セキュリティ」タブをクリックし、「署名の証明書」グループの「証明書」欄右の 選択 ボタンをクリックします。



④ ［既定のアカウントデジタル ID の選択］ダイアログボックスで、該当する証明書を選択し、OK ボタンをクリックします。

※ 複数の証明書が表示された場合は、証明書の表示 ボタンをクリックして内容を確認してください。

⑤ 「署名の証明書」グループの「証明書」欄に名前が表示されたことを確認し、「暗号化の設定」グループの「証明書」欄右側の 選択 ボタンをクリックします。



⑥ ［既定のアカウントデジタル ID の選択］ダイアログボックスで、該当する証明書を選択し、OK ボタンをクリックします。

※1 複数の証明書が表示された場合は、証明書の表示 ボタンをクリックして内容を確認してください。

⑦ 「暗号化の設定」グループの「証明書」欄に名前が表示されたことを確認し、OK ボタンをクリックします。

⑧ ［インターネットアカウント］ダイアログボックスの 閉じる ボタンをクリックして、インターネットアカウントダイアログボックスを閉じます。

2　署名付きメール

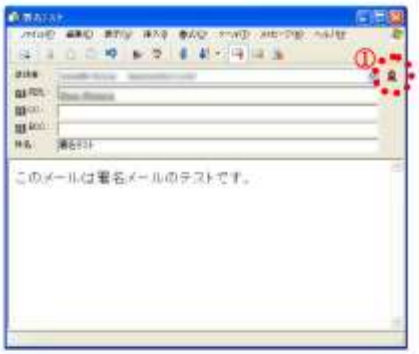
2.1　署名付きメールの送信

署名付きのメールの設定は、メール作成画面で以下のいずれかの方法で行います。

【メニューを利用する方法】
≪ツール≫メニューの≪デジタル署名≫をクリックします。（署名されている場合は、メニュー項目の前に✓が付きます。

【ツールバーを利用する方法】※ツールバーをカスタマイズしている場合，ボタンの形状が違う場合があります。
ツールバーの 署名 （メッセージにデジタル署名）をクリックします。

① 作成中のメール画面の右側に署名アイコンが表示されます。



② メールを送信します。

2.2　署名付きメールの受信

署名付きメールには「このメッセージは送信者によってデジタル署名されています。」と表示されます。
受信したメールは 続行 ボタンをクリックすると読むことができます。

※ 署名アイコンをクリックしてメッセージの作成者から正常に送信されていることやメッセージが改ざんされていないことを確認できます。

参考

前ページ2.2で表示したダイアログボックス内の「セキュリティ」タブの 証明書の表示 ボタンをクリックし、[証明書の表示] ダイアログボックス内の 署名の証明書 ボタンをクリックすると証明書の内容を確認できます。

※ 表示したダイアログボックスで確認できる内容

■「全般」タブ

■「詳細」タブ

■「証明のパス」タブ

■「信頼」タブ

3　暗号化メール

3.1　暗号化メールの送信

暗号化メールの設定は、メール作成画面で以下のいずれかの方法で行います。

【メニューを利用する方法】
≪ツール≫メニューの≪暗号化≫をクリックします。（暗号化されている場合は、メニュー項目の前に✓が付きます。

【ツールバーを利用する方法】※ツールバーをカスタマイズしている場合，ボタンの形状が違う場合があります。
ツールバーの 暗号化 （メッセージの暗号化）をクリックします。

① 作成中のメール画面の右側に鍵前のアイコンが表示されたことを確認して、メールを送信します。

3.2　暗号化メールの受信

暗号化メールには「このメッセージは送信者によって暗号化されています。」と表示されます。
受信したメールは、続行 ボタンをクリックすると読むことができます。

※　鍵前アイコンをクリックして改ざんされていないことや証明書を表示して確認できます。

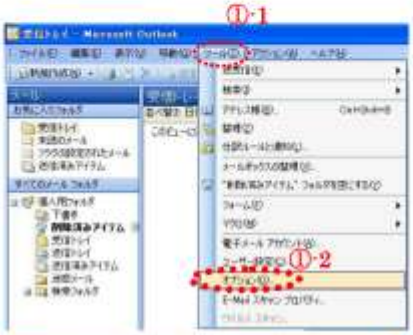
証明書の表示 ボタンをクリックし、暗号の証明書 ボタンをクリックすると暗号化に使われた証明書を確認できます。確認できる内容は、P15 と同じです。

4　署名付き暗号化メール

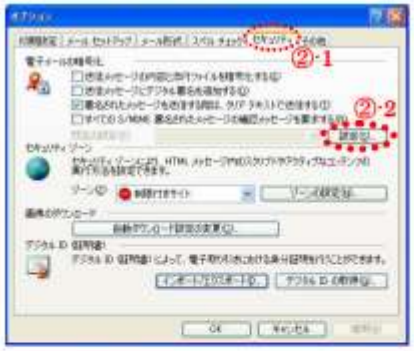
署名することにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

1. 電子メールで利用するための設定

① ≪ツール≫メニューから≪オプション≫をクリックします。



② ［オプション］ダイアログボックスの「セキュリティ」タブをクリックし、「電子メールの暗号化」グループの 設定 ボタンをクリックします。



③ ［セキュリティ設定の変更］ダイアログボックスの「保護されたメッセージの形式」グループの「セキュリティ設定名」と「証明書とアルゴリズム」グループの「署名証明書」および「暗号証明書」欄が証明書を利用するメールアドレスになっていることを確認します。

④ 「保護されたメッセージの形式」グループの「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」と「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」に✓マークが入っていることを確認します。

⑤ OK ボタンをクリックします。

⑥ ［オプション］ダイアログボックスの OK ボタンをクリックします。

※1「証明書とアルゴリズム」グループ内右側の 選択 ボタンをクリックし、証明書を確認することができます。

2　署名付きメール

2.1　署名付きメールの送信

① 作成中のメール画面でツールバーの（デジタル署名）ボタンをクリックします。

② メールを送信します。

2.2　署名付きメールの受信

① 受信したメールをアイテム一覧で選択すると、正しく署名されたメールは閲覧ウィンドウに本文の内容と署名アイコンが表示されます。署名アイコンにマウスを近付けると「デジタル署名は信頼されています。詳細を表示するにはここをクリックしてください。」と表示されます。

② 署名アイコンをクリックし、デジタル署名が有効であることを確認し、詳細 ボタンをクリックします。

③ ［メッセージセキュリティのプロパティ］ダイアログボックスが表示されます。
「署名者」に表示されているメールアドレスが送信者と同じであることを確認して、詳細の表示 ボタンをクリックします。

④　［署名］ダイアログボックスの「全般」タブの
証明書の表示 ボタンをクリックします。

⑤　［証明書の表示］ダイアログボックスの「全般」「詳細」「証明書のパス」「信頼」タブで各内容を確認し、OK ボタンをクリックします。
各タブの内容は、P15 を参照してください。

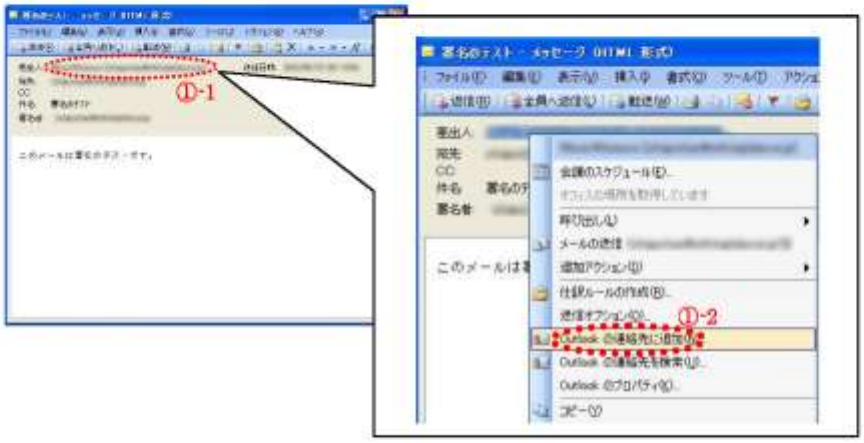
⑥　［署名］ダイアログボックスの 閉じる ボタンをクリックします。

⑦　［メッセージセキュリティのプロパティ］ダイアログボックスの 閉じる ボタンをクリックします。

⑧　［デジタル署名］ダイアログボックスの 閉じる ボタンをクリックします。

2.3　署名付きメールを受信したら、送信者の電子証明書を Outlook の連絡先に登録します。

① アイテム一覧ウィンドウから受信した署名付きメールをダブルクリックして開き、差出人を右クリックし、「Outlook の連絡先に追加」をクリックします。



② 連絡先の登録画面が表示されますので、「証明書」タブをクリックします。
「証明書（デジタル ID）」の一覧に証明書が登録されていることを確認し、ツールバーの 保存して閉じる ボタンをクリックします。

③ 開いていたメールを閉じて、ナビゲーションウィンドウの 連絡先 ボタンをクリックし、Outlook 連絡先に送信者の情報および証明書情報が登録されたことを確認します。

3　暗号化メール

3.1　暗号化メールの送信

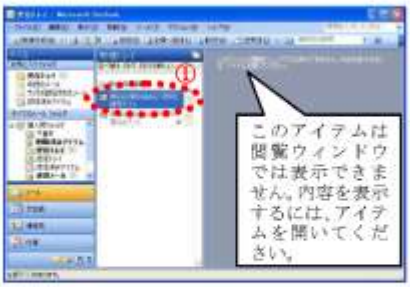
① 作成中のメール画面で、ツールバーの （暗号化）ボタンをクリックします。

② メールを送信します。

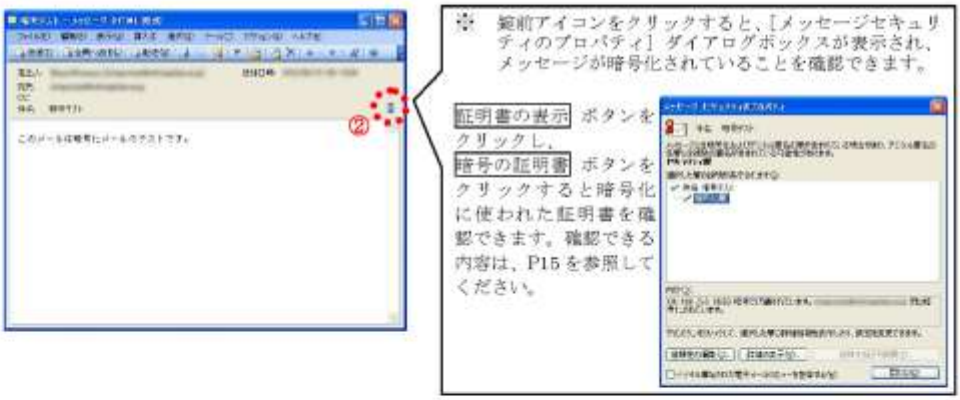
3.2　暗号化メールの受信

暗号化されたメールを受信しても閲覧ウィンドウに内容は表示されません。

① アイテム一覧ウィンドウの件名をダブルクリックして開きます。



② 本文と情報表示領域に錠前アイコンが表示されます。



4　署名付き暗号化メール

署名することにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

1. 電子メールで利用するための設定

① ≪ツール≫メニューから≪アカウント≫をクリックします。

② ［インターネットアカウント］ダイアログボックスの「メール」グループから証明書を設定するメールアドレスを選択し、プロパティ ボタンをクリックします。

③ 選択したメールアドレスのプロパティダイアログボックスの「セキュリティ」タブをクリックし、「署名の証明書」グループの「証明書」の 選択 ボタンをクリックします。

④ ［既定のアカウントデジタル ID の選択］ダイアログボックスの証明書の一覧から証明書を選択し、OK ボタンをクリックします。

※1 複数の証明書が表示された場合は、証明書の表示 ボタンをクリックして詳細情報を確認してください。

⑤ 「署名の証明書」グループの「証明書」欄に選択したアドレスが表示されていることを確認して、「暗号化の設定」グループの 選択 ボタンをクリックします。

⑥ ［既定のアカウントデジタル ID の選択］ダイアログボックスの証明書の一覧から証明書を選択し、OK ボタンをクリックします。

※1 複数の証明書が表示された場合は、証明書の表示 ボタンをクリックして詳細情報を確認してください。

⑦ 選択したメールアドレスのプロパティダイアログボックスの「暗号化の設定」グループの証明書欄に選択したアドレスが表示されていることを確認して、OK ボタンをクリックします。

⑧ ［インターネットアカウント］ダイアログボックスに戻りますので、閉じる ボタンをクリックします。

2　署名付きメール

2.1　署名付きメールを送信する

署名付きメールの設定は、メール作成画面で以下のいずれかの方法で行います。

【メニューバーを利用する方法】
≪ツール≫メニューの≪デジタル署名≫をクリックします。（署名されている場合は、メニュー項目の前に✓が付きます。）

【ツールバーを利用する方法】※ボタンは、大きいアイコンで文字列を表示しています。
ツールバーの  （メッセージにデジタル署名）をクリックします。

① 作成中のメール画面の右側に署名アイコンが表示されます。

② メールを送信します。

2.2　署名付きメールの受信

署名付きメールには「このメッセージは送信者によってデジタル署名されています。」と表示されます。
受信したメールは 続行 ボタンをクリックすると読むことができます。

この画面はメールを開いた状態です。

※　署名アイコンをクリックしてメッセージの作成者から正常に送信されていることやメッセージが改ざんされていないことを確認できます。

証明書の表示 ボタンをクリックして内容を確認することができます。
これ以降の確認は，P15 を参照してください。

受信したメールを開かずにプレビュー画面で確認した場合は，署名アイコンにマウスを近付けると「このメッセージはデジタル署名付きです。」というメッセージを確認することができます。

3　暗号化メール

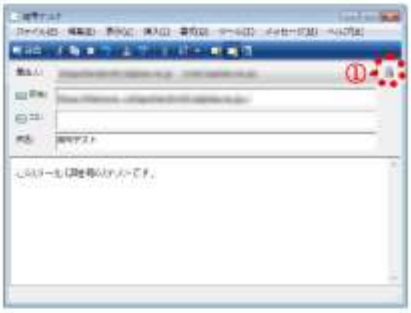
3.1　暗号化メールの送信

暗号化メールの設定は、メール作成画面で以下のいずれかの方法で行います。

【メニューを利用する方法】
≪ツール≫メニューの≪暗号化≫をクリックします。(暗号化されている場合は、メニュー項目の前に✓が付きます。

【ツールバーを利用する方法】※ボタンは、大きいアイコンで文字列を表示しています。
ツールバーの  (メッセージの暗号化) をクリックします。

① 作成中のメール画面の右側に錠前のアイコンが表示されたことを確認して、メールを送信します。

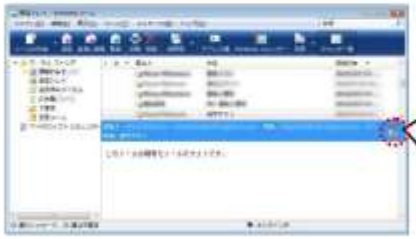


3.2　暗号化メールの受信

暗号化メールには「このメッセージは送信者によって暗号化されています。」と表示され、続行 ボタンをクリックすると読むことができます。

※　錠前アイコンをクリックすると、メッセージが暗号化されていることを確認できます。

証明書の表示 ボタンをクリックし、暗号の証明書 ボタンをクリックすると暗号化に使われた証明書を確認できます。確認できる内容は、P15 を参照してください。

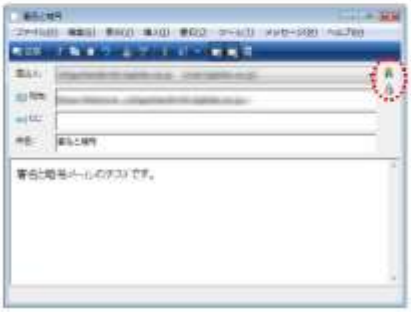


受信したメールを開かずにプレビュー画面で確認した場合は、錠前アイコンにマウスを近付けると「このメッセージは暗号化されています。」というメッセージを確認することができます。

4　署名付き暗号化メール

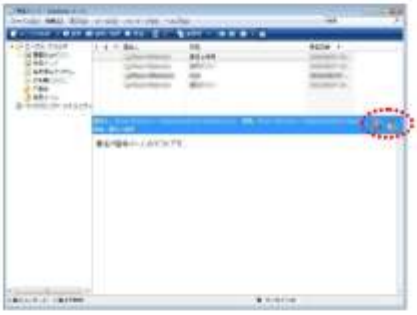
署名する事により、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

【署名付き暗号化メールの作成例】



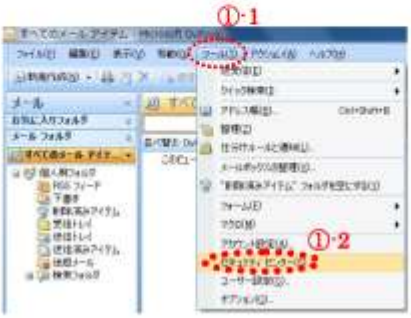
【署名付き暗号化メールの受信例】

【署名付き暗号化メールをプレビュー画面で確認した場合の例】



1　電子メールで利用するための設定

① ≪ツール≫メニューから≪セキュリティセンター≫をクリックします。

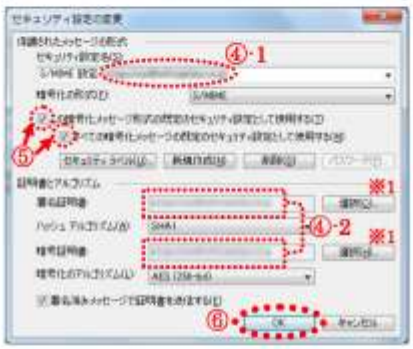


② 左側のメニューから「電子メールのセキュリティ」をクリックします。

③ 「電子メールの暗号化」グループの「既定の設定」項目の右側の 設定 ボタンをクリックします。

④ ［セキュリティ設定の変更］ダイアログボックスの「保護されたメッセージの形式」グループの「セキュリティ設定名」と「証明書とアルゴリズム」グループの「署名証明書」および「暗号証明書」欄が証明書を利用するメールアドレスになっていることを確認します。

⑤ 「保護されたメッセージの形式」グループの「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」と「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」に✓マークが入っていることを確認します。



⑥ OK ボタンをクリックします。

※1「証明書とアルゴリズム」グループ内右側の 選択 ボタンをクリックし、証明書を確認することができます。

Windows XP および Vista で Outlook2007 を利用している場合

Windows 7 で Outlook2007 を利用している場合

⑦　［セキュリティセンター］ダイアログボックスの「電子メールの暗号化」グループの「既定の設定」が設定されたことを確認して、OK ボタンをクリックします。

2　署名付きメール

2.1　署名付きメールを送信する

①　作成中のメール画面のリボンの≪メッセージ≫タブから「メッセージにデジタル署名を追加」ボタンをクリックします。署名ボタンはウィンドウのサイズによって 署名 や に変わります。

②　メールを送信します。

2.2　署名付きメールの受信

①　受信したメールをアイテム一覧で選択すると、正しく署名されたメールは閲覧ウィンドウに本文の内容と署名アイコンが表示されます。署名アイコンにマウスを近付けると、「デジタル署名は信頼されています。詳細を表示するにはここをクリックしてください。」と表示されます。

②　署名アイコンをクリックし、デジタル署名が有効であることを確認し、詳細 ボタンをクリックします。

③　［メッセージセキュリティのプロパティ］ダイアログボックスが表示されます。
「署名者」に表示されているメールアドレスが送信者と同じであることを確認して、詳細の表示 ボタンをクリックします。

④　「全般」タブの 証明書の表示 ボタンをクリックします。

⑤　［証明書の表示］ダイアログボックスの「全般」「詳細」「証明書のパス」「信頼」タブで各内容を確認し、OK ボタンをクリックします。
各タブの内容は、P15 を参照してください。

⑥　［署名］ダイアログボックスの 閉じる ボタンをクリックします。

⑦　［メッセージセキュリティのプロパティ］ダイアログボックスの 閉じる ボタンをクリックします。

⑧　［デジタル署名］ダイアログボックスの 閉じる ボタンをクリックします。

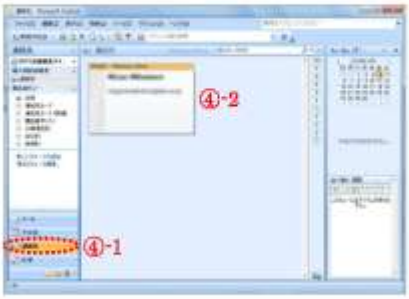
2.3　署名付きメールを受信したら、送信者の電子証明書を Outlook の連絡先に登録します。

① アイテム一覧ウィンドウから受信した署名付きのメールをダブルクリックして開き、差出人を右クリックし、「Outlook の連絡先に追加」をクリックします。

② 登録画面が表示されますので、証明書（証明書）ボタンをクリックします。

③ 「証明書（デジタル ID）」の一覧に電子証明書が登録されていることを確認し、リボンの「連絡先」タブ内の 保存して閉じる ボタンをクリックします。

④ 開いたメールを閉じて、ナビゲーションウィンドウの 連絡先 ボタンをクリックし、Outlook 連絡先に送信者の情報および証明書情報が登録されたことを確認します。（この画面の現在のビューは「名刺」です。）



3　暗号化メール

3.1　暗号化メールの送信

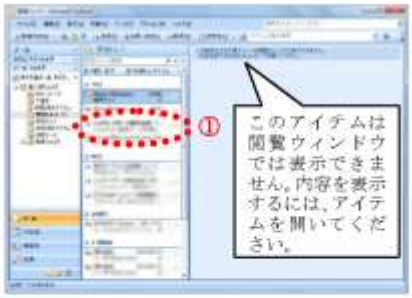
① 作成中のメール画面でリボンの≪メッセージ≫タブから 暗号化 ボタンをクリックします。暗号化ボタンはウィンドウのサイズによって 暗号化 や に変わります。

② メールを送信します。

3.2　暗号化メールの受信

暗号化されたメールを受信しても閲覧ウィンドウに内容は表示されません。

① アイテム一覧ウィンドウの件名をダブルクリックして開きます。



② 本文と情報表示領域に鍵前アイコンが表示されます。

※　鍵前アイコンをクリックすると、[メッセージセキュリティプロパティ] のダイアログボックスが表示され、メッセージが暗号化されていることを確認できます。

証明書の表示 ボタンをクリックし、暗号の証明書 ボタンをクリックすると暗号化に使われた証明書を確認できます。確認できる内容は、P15 を参照してください。

4　署名付き暗号化メール

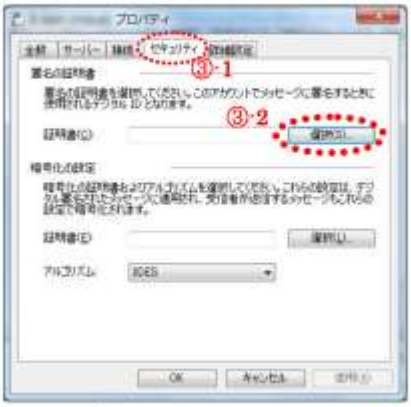
署名することにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

1　電子メールで利用するための設定

① ≪ツール≫メニューから≪アカウント≫をクリックします。

② ［アカウント］ダイアログボックスの「メール」グループから証明書を設定するメールアドレスを選択し、プロパティ ボタンをクリックします。

③ 選択したメールアドレスのプロパティダイアログボックスの「セキュリティ」タブをクリックし、「署名の証明書」グループの 選択 ボタンをクリックします。



④ 選択したメールアドレスに紐付いた「既定のアカウントデジタル ID の選択」画面が表示されますので、内容を確認して、OK ボタンをクリックします。

⑤ 選択したメールアドレスのプロパティダイアログボックスの「署名の証明書」グループの「証明書」欄に選択したアドレスが表示されていることを確認して、「暗号化の設定」グループの 選択 ボタンをクリックします。

⑥ 「既定のアカウントデジタル ID の選択」画面が表示されますので、内容を確認して OK ボタンをクリックします。

⑦ 選択したメールアドレスのプロパティダイアログボックスの「暗号化の証明書」グループの「証明書」欄に選択したアドレスが表示されていることを確認して、OK ボタンをクリックします。

⑧ ［アカウント］ダイアログボックスに戻りますので、閉じる ボタンをクリックします。

2 署名付きメール

2.1 署名付きメールを送信する

署名付きメールの設定は、メール作成画面で以下のいずれかの方法で行います。

【メニューを利用する方法】

≪ツール≫メニューの≪デジタル署名≫をクリックします。作成中のメール画面の右側に署名アイコンが表示されます。（署名されている場合は、メニュー項目の前に✓が付きます。）

【ツールバーを利用する方法】

ツールバーに デジタル署名 ボタンを表示させておきクリックします。

※ツールバーへのボタンの表示方法は、Windows Live Mail のヘルプ機能をご確認ください。

① 作成中のメール画面の右側に署名アイコンが表示されたことを確認して、メールを送信します。

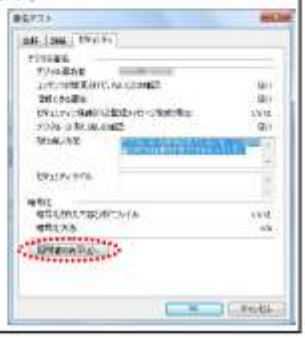
2.2　署名付きメールの受信

署名付きメールには「このメッセージは送信者によってデジタル署名されています。」と表示されます。
受信したメールは 続行 ボタンをクリックすると読むことができます。

この画面はメールをダブルクリックで開いた状態です。

※　署名アイコンをクリックしてメッセージの作成者から正常に送信されていることやメッセージが改ざんされていないことを確認できます。

証明書の表示 ボタンをクリックして内容を確認することができます。
これ以降の確認は、P15 をご参照ください。



※　Windows Live Mail の場合は、メールを開いていない場合でも、閲覧ウィンドウで署名を確認することができます。

2.3　署名付きのメールを受信したら、送信者の電子証明書を Windows Live Mail のアドレス帳に登録します。

署名付きメールを選択し、閲覧ウィンドウの上部に表示された「アドレス帳に追加」をクリックします。以下のダイアログボックスが表示されたら、OK ボタンをクリックしてください。

3　暗号化メール

3.1　暗号化メールの送信

暗号化メールの設定は、メール作成画面で以下のいずれかの方法で行います。

【メニューを利用する方法】
≪ツール≫メニューの≪暗号化≫をクリックします。（暗号化されている場合は、メニュー項目の前に✔が付きます。）

【ツールバーを利用する方法】
ツールバーに 暗号化 ボタンを表示させておきクリックします。
※ツールバーへのボタンの表示方法は、Windows Live Mail のヘルプ機能をご確認ください。

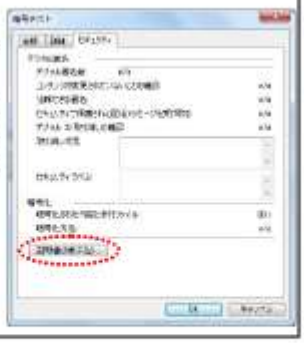
① 作成中のメール画面の右側に錠前のアイコンが表示されたことを確認して、メールを送信します。

3.2 暗号化メールの受信

暗号化メールには「このメッセージは差出人によって暗号化されています。」と表示されます。暗号化されたメッセージは、続行 ボタンをクリックすると読むことができます。

※ 錠前アイコンをクリックすると、メッセージが暗号化されていることを確認できます。

証明書の表示 ボタンをクリックし、暗号の証明書 ボタンをクリックすると暗号化に使われた証明書を確認できます。確認できる内容は、P15 をご参照ください。



4 署名付き暗号化メール

署名することにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

1　電子メールで利用するための設定

① ≪ファイル≫タブをクリックして Backstage ビューを開き、［オプション］をクリックします。

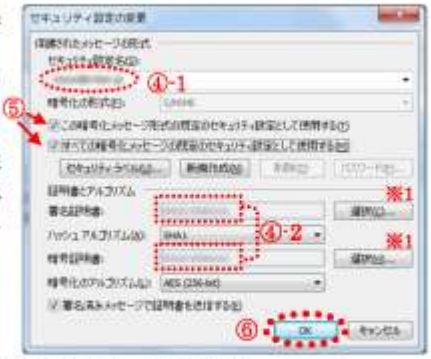
② 左側のメニューの「セキュリティセンター」をクリックし、セキュリティセンターの設定 ボタンをクリックします。

③ 左側のメニューの「電子メールのセキュリティ」をクリックし、「電子メールの暗号化」グループの 設定 ボタンをクリックします。

④ ［セキュリティ設定の変更］ダイアログボックスの「保護されたメッセージの形式」グループの「セキュリティ設定名」と「証明書とアルゴリズム」グループの「署名証明書」および「暗号証明書」を確認します。

⑤ 「暗号化の形式」グループの「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」と「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」を✓します。

⑥ OK ボタンをクリックします。



※1　選択 ボタンをクリックして証明書を確認することができます。（P27 参照）

⑦　［セキュリティセンター］ダイアログボックスの OK ボタンをクリックします。

⑧　Outlook オプション画面の、OK ボタンをクリックします。

2　署名付きメール

2.1　署名付きメールを送信する

①　作成中のメール画面のリボンの≪オプション≫タブからアクセス許可グループの 署名（メッセージにデジタル署名を追加）ボタンをクリックします。

②　メールを送信します。

2.2　署名付きメールの受信

①　受信したメールをアイテム一覧で選択すると、正しく署名されたメールは閲覧ウィンドウに本文の内容と署名アイコンが表示されます。署名アイコンにマウスを近付けると「デジタル署名は信頼されています。詳細を表示するにはここをクリックしてください。」と表示されます。

②　署名アイコンをクリックし、デジタル署名が有効であることを確認し、詳細 ボタンをクリックします。

③　［メッセージセキュリティのプロパティ］ダイアログボックスが表示されます。
「署名者」に表示されているメールアドレスが送信者と同じであることを確認して、詳細の表示 ボタンをクリックします。

④　「全般」タブの 証明書の表示 ボタンをクリックします。

⑤　［証明書の表示］ダイアログボックスの「全般」「詳細」「証明書のパス」「信頼」タブで各内容を確認し、OK ボタンをクリックします。
各タブでの内容は、P15 を参照してください。

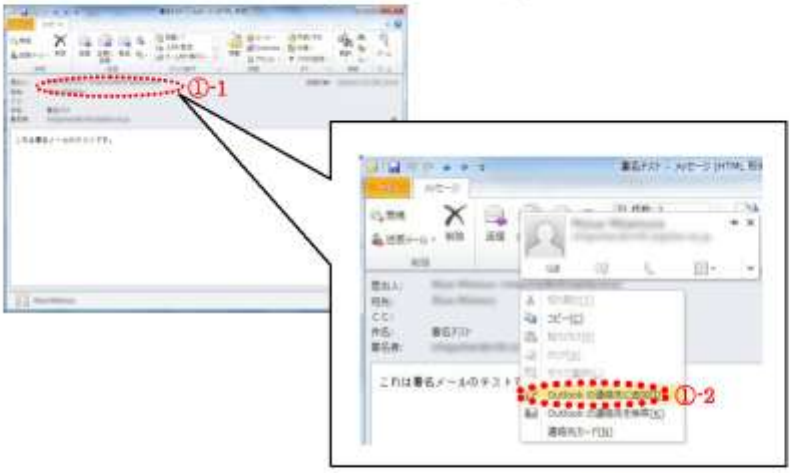
⑥　［署名］ダイアログボックスの OK ボタンをクリックします。

⑦　［メッセージセキュリティのプロパティ］ダイアログボックスの 閉じる ボタンをクリックします。

⑧　［デジタル署名］ダイアログボックスの 閉じる ボタンをクリックします。

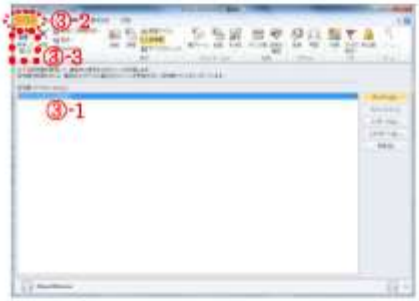
2.3　署名付きメールを受信したら、送信者の電子証明書を Outlook の連絡先に登録します。

① アイテム一覧ウィンドウから受信した署名付きメールをダブルクリックして開き、差出人を右クリックし、「Outlook の連絡先に追加」をクリックします。



② 登録画面が表示されますので、 証明書 ボタンをクリックします。

③ 「証明書（デジタル ID）」の一覧に証明書が登録されていることを確認し、リボンの「連絡先」タブ内の 保存して閉じる ボタンをクリックします。



③ 開いたメールを閉じて、ナビゲーションウィンドウの 連絡先 をクリックし、Outlook 連絡先に送信者の情報および証明書情報が登録されたことを確認します。（この画面の現在のビューは「名刺」です。）

3　暗号化メール

3.1　暗号化メールの送信

① 作成中のメール画面でリボンの≪オプション≫タブから、暗号化 ボタンをクリックします。

② 送信します。

3.2　暗号化メールの受信

送信者が暗号化する際に使用した公開鍵と対になる秘密鍵を持っている場合は、受信した暗号化メールを選択すると閲覧ウィンドウ内容が表示されます。

① 情報表示領域の錠前アイコンをクリックします。

② ［メッセージセキュリティプロパティ］ダイアログボックスが表示され、メッセージが暗号化されていることを確認します。

詳細の表示 ボタンをクリックすると暗号化ダイアログボックスで暗号化情報を確認することができます。

さらに 証明書の表示 ボタンをクリックして［証明書］ダイアログボックスを表示し、証明書の内容を確認することができます。

証明書の内容の確認は P15 をご参照ください。

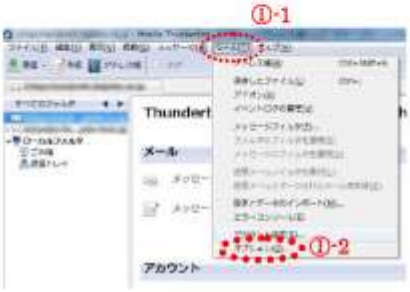
4　署名付き暗号化メール

署名することにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

1　証明書を「証明書マネージャ」へインポートします。

証明書を Thunderbird の証明書マネージャにインポートします。

① Thunderbird メイン画面の≪ツール≫メニューから≪オプション≫をクリックします。



② 「詳細」カテゴリの「証明書」タブをクリックし、証明書を表示 ボタンをクリックします。

③ ［証明書マネージャ］ダイアログボックスが表示されます。
「あなたの証明書」タブを選択し、インポート ボタンをクリックします。

④ ［復元するファイル名］ダイアログボックスが表示されますので、管理者から配布された証明書ファイル（xxxxx.p12 ファイル）を選択し、開く ボタンをクリックします。

マスターパスワードを設定している場合は、Software Security Device のマスターパスワードを入力し、OK ボタンをクリックします。
マスターパスワードを設定していない場合は、マスターパスワードを設定する画面が表示されますので、適宜設定してください。

「マスターパスワード」とは、Thunderbird の証明書マネージャへアクセスするためのパスワードです。このパスワードを忘れると、Thunderbird の証明書マネージャにアクセスすることができません。設定したマスターパスワードは絶対に忘れないように注意してください。

⑤ ［パスワードの入力］ダイアログボックスが表示されますので、管理者から証明書ファイルと一緒に配布されたパスワードを入力し、OK ボタンをクリックします。

⑥ 正常に復元ができたメッセージが表示されます。
OK ボタンをクリックします。

⑦ ［証明書マネージャ］ダイアログボックスにインポートした証明書を選択して、表示 ボタンをクリックします。

⑧ ［証明書ビューア］ダイアログボックスに表示された「一般」タブと「詳細」タブを切り替え、各内容を確認します

「一般」タブ、「詳細」タブに表示される内容は、P15 と変わりありません。

⑨ ［証明書ビューア］ダイアログボックスの 閉じる ボタンをクリックします。

⑩ ［証明書マネージャ］ダイアログボックスの OK ボタンをクリックします。

⑪ ［オプション］ダイアログボックスの OK ボタンをクリックします。

2　電子メールで利用するための設定

① Thunderbird メイン画面の≪ツール≫メニューから≪アカウント設定≫をクリックします。

② 左側のメニューから「セキュリティ」をクリックし、デジタル署名グループの「メッセージのデジタル署名に使用する証明書」欄の 選択 ボタンをクリックします。

③ 選択可能な証明書が表示されます。
設定する証明書を選択して、OK ボタンをクリックします。

④ 暗号化グループの「あなたへのメッセージの暗号化と復号に使用する証明書」欄も同時に設定します。はい をクリックします。

⑤ デジタル署名グループの「メッセージのデジタル署名に使用する証明書」と暗号化グループの「あなたへのメッセージの暗号化と復号に使用する証明書」が設定されたことを確認し、OK をクリックします。

3　署名付きメール

3.1　署名付きメールを送信する

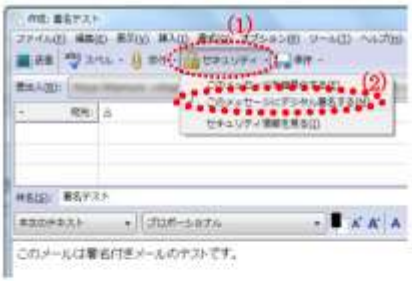
署名付きメールの設定は、メール作成画面で以下のいずれかの方法で行います。

【メニューを使う方法】

≪オプション≫メニューから「このメッセージにデジタル署名する」をクリックします。（署名されている場合は、メニュー項目の前に✔が付きます。）

【ツールバーのボタンを使う方法】

セキュリティ ボタンの ▼ をクリックして「このメッセージにデジタル署名する」をクリックします。（署名されている場合は、メニュー項目の前に✔が付きます。）



① メール作成画面の右下に ●（赤丸で封をした封筒）アイコンが表示されます。

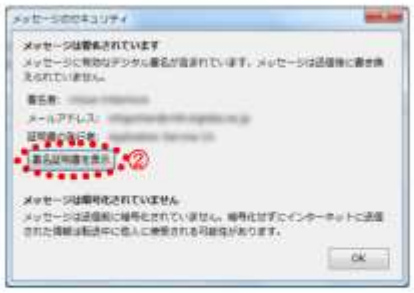
② 送信します。マスターパスワードの入力を要求するダイアログボックスが表示された場合は、マスターパスワードを入力し、OK ボタンをクリックします。

3.2　署名付きメールの受信

受信した署名付きメールをスレッドペインから選択すると、正しく署名されたメールは、メッセージペインの上部（メッセージヘッダ）に ● アイコンが表示されます。

① ● アイコンをクリックします。

② ［メッセージのセキュリティ］ダイアログボックスが表示されます。署名証明書を表示 をクリックすると証明書ビューアが開き、証明書を確認することができます。証明書の内容は、P42 の⑧と同じです。



③ 証明書の内容を確認したら、証明書ビューアの 閉じる ボタンをクリックします。

④ ［メッセージのセキュリティ］ダイアログボックスの OK ボタンをクリックします。

4.1 暗号化メールの送信

Thunderbird は、署名付きメールを受信すると、相手の証明書とメールアドレスの情報を自動的に証明書マネージャに登録します。
一度署名付きでメールを送信してもらった相手に対しては、特別な設定をしなくても暗号化メールを送信することができます。

暗号化メールの設定は、メール作成画面で以下のいずれかの方法で行います。

【メニューを使う方法】

≪オプション≫メニューから「このメッセージを暗号化する」をクリックします。作成中のメール画面の右側に錠前アイコンが表示されます。（暗号化されている場合は、メニュー項目の前に✓が付きます。）
メールを送信します。

【ツールバーのボタンを使う方法】

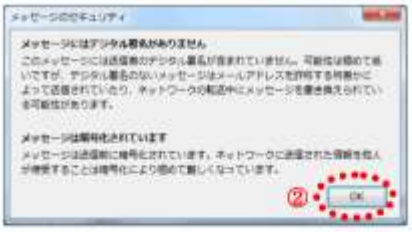
セキュリティ ボタンの ▼ をクリックして「このメッセージを暗号化する」をクリックします。（暗号化されている場合は、メニュー項目の前に✓が付きます。）作成中のメール画面の右下に錠前のアイコンが表示されたことを確認して、メールを送信します。

4.2　暗号化メールの受信

受信した暗号化メールをスレッドペインから選択すると、メッセージペインの上部（メッセージヘッダ）に錠前アイコンが表示されます。

① アイコンクリックします。

② ［メッセージセキュリティ］ダイアログボックスが表示され、メッセージは暗号化されていることを確認することができます。
OK ボタンをクリックして、［メッセージのセキュリティ］ダイアログボックスを閉じます



5　署名付き暗号化メール

署名することにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

【署名付きと暗号化メールの作成例】

【署名と暗号化を組み合わせたメールの受信例】

【 アイコンもしくは アイコンをクリックしたときの表示】

1　Becky! に S/MIME による暗号化、署名の機能を追加します。
※Becky! を起動している場合は、終了して作業を進めてください。

① Becky! の公式サイトから必要なプラグインをダウンロードします。
【URL】http://www.rimarts.co.jp/beckyj.htm

画面をスクロールすると、「ダウンロード」の項目が現れます。

② さらにスクロールして「プラグイン」の項目から「Becky! S/MIME plug-in Ver.1.10」のリンクをクリックします。

③ ［ファイルのダウンロード］ダイアログボックスが表示されますので、保存 ボタンをクリックします。

④ ［名前を付けて保存］ダイアログボックスが表示されますので、任意の場所を選択して、保存 ボタンをクリックします。

⑤ ［ダウンロードの完了］ダイアログボックスが表示されたら、ファイルを開く ボタンをクリックします。

⑥ ［BkSMIME110.zip］ウィンドウが開きますので、中の BkSMIME フォルダをダブルクリックします。
※この図では見やすくするため「大きいアイコン」で表示しています。

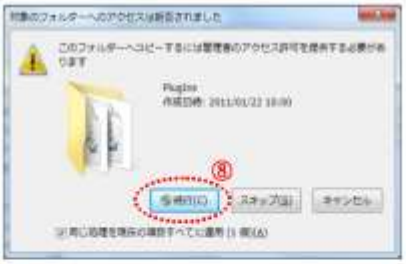
⑦ 「BkSMIME.dll」と「BkSMIME-j.txt」ファイルがあることを確認してください。
※「BkSMIME-j.txt」と「BkSMIME-e.txt」を間違えないようご注意ください。

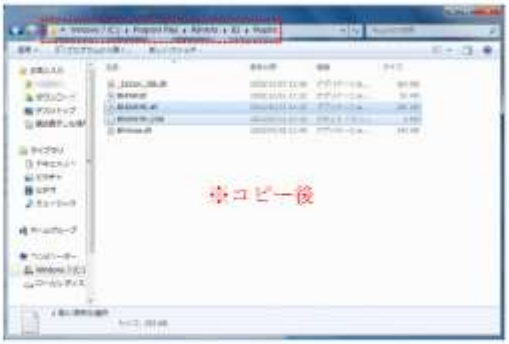
⑧ 2 つのファイルを以下のフォルダにコピーします。

[Becky! のプログラムがインストールされているフォルダ]¥PlugIns¥
（例：C:¥Program Files¥RimArts¥B2!¥PlugIns¥）

この場所にコピーすると、同じパソコンで Becky! を利用するすべてのユーザーがプラグインを利用することができるようになります。詳細は、BkSMIME-e.txt をお読みください。

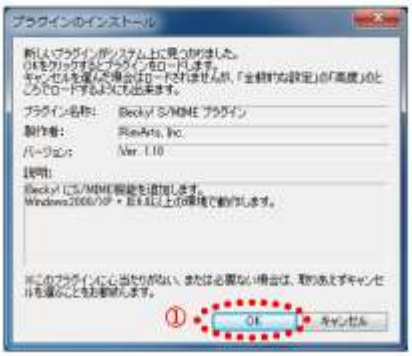
対象フォルダへのアクセスが拒否された場合は、続行してください。



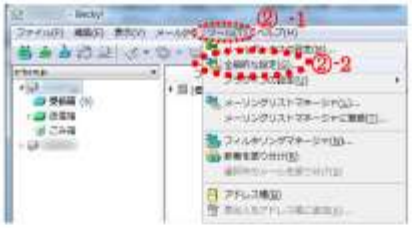


2　電子メールで利用するための設定

① Becky! を起動します。［プラグインのインストール］ダイアログボックスが表示されますので、OK ボタンをクリックします。
※ダイアログボックスが表示されない場合は、正しくインストールされていない可能性があります。



② ≪ツール≫メニューから「全般的な設定」をクリックします。



③ 「高度」タブをクリックし、プラグイン ボタンをクリックします。

④ ［プラグインの選択］ダイアログボックスが表示されますので、「BKSMIME.DLL/Becky! S/MIME プラグイン Ver.1.10」に✓があることを確認します。

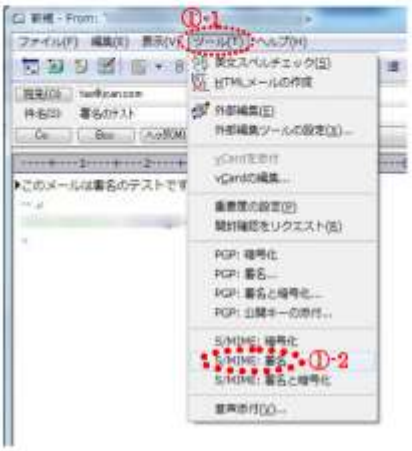
⑤ OK ボタンをクリックしてダイアログボックスを閉じます。

⑥ ［全般的な設定］ダイアログボックスの OK ボタンをクリックして閉じます。

3　署名付きメール

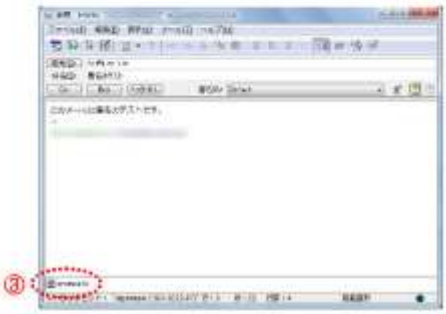
3.1　署名付きメールを送信する

① メッセージ作成画面の≪ツール≫メニューから「S/MIME：署名」をクリックします。



② ［S/MIME message］ダイアログボックスが表示され署名したことを確認し、OK ボタンをクリックします。

③ 署名情報が追加されたことを確認して、送信します。

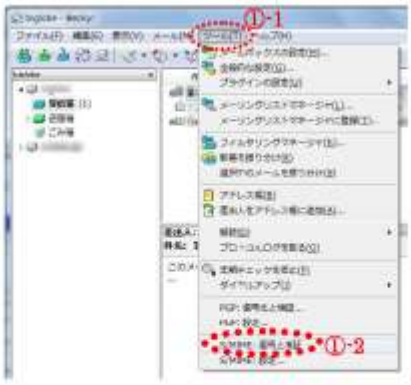


※エラーメッセージが表示された場合は、OS に証明書がインストールされているか確認してください。

3.2　署名付きメールの受信

正しく署名されたメールを受信すると、アイコンにクリップが付きます。（ ）
Becky!では、MIME タイプが指定されているメールを一律、添付ありと判断しているためです。
また、署名付きメールの本文領域の下側に署名情報（smime.p7s）が表示されます。

① ≪ツール≫メニューから「S/MIME：復号と検証」をクリックします。



② ［S/MIME message］ダイアログボックスで表示されます。検証結果を確認し、OK ボタンをクリックします。

※証明書は、証明書ストアの「他の人」タブ登録されたことを確認できます。（P11 の③「個人」タブを「他の人」タブに読み替えて確認してください。）

4　暗号化メール

4.1　暗号化メールの送信

Becky! は、署名付きメールを受信し、検証すると、自動的に証明書ストアに登録します。
一度署名付きでメールを送信してもらった相手に対しては、特別な設定をしなくても暗号化メールを送信することができます。

① メッセージ作成画面の≪ツール≫メニューから「S/MIME 暗号化」をクリックします。

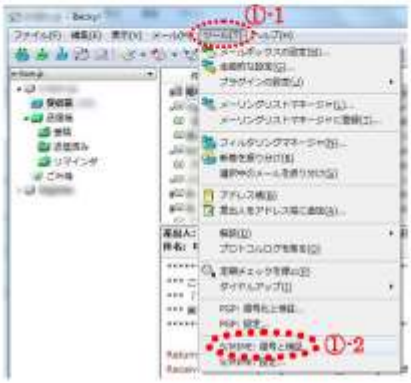
② ［S/MIME message］ダイアログボックスが表示されますので、メッセージが暗号化されたことを確認し、OK ボタンをクリックします。

③ メッセージビューのメール本文は見えなくなり、左下に「smime.p7m」と表示されたことを確認し、メールを送信します。

4.2　暗号化メールの受信

受信した暗号化メールは件名の先頭に アイコンが付き、メール一覧で選択しても、メッセージビューで内容を見ることはできません。（メッセージ選択時のアイコンは、 になります。）

① ≪ツール≫メニューから「S/MIME：複合と検証」をクリックします。



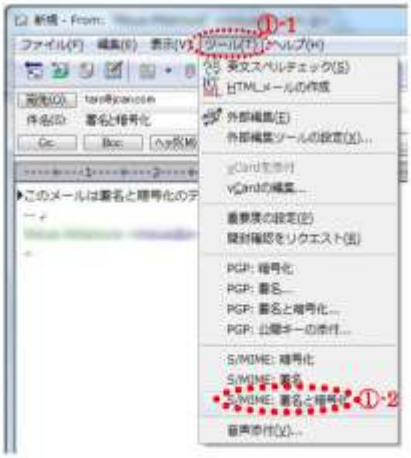
② ［S/MIME message］ダイアログボックスが表示され、復号された確認することができます。
OK ボタンをクリックして、［S/MIME message］ダイアログボックスを閉じて、メッセージの内容を確認します。

5　署名付き暗号化メール

署名することにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

【送信側】

① メッセージ作成画面の≪ツール≫メニューから「S/MIME：署名と暗号化」をクリックします。



② ［S/MIME message］ダイアログボックスが表示されますので，メッセージに署名したこととメッセージが暗号化されたことを確認し、OK ボタンをクリックします。

③ メッセージビューのメール本文は見えなくなり、左下に「smime.p7m」と表示されたことを確認し、メールを送信します。

【受信側】

① 受信したメールのメッセージビューには、以下のように表示されます。

```
**********************************************************
*** これは S/MIME メッセージです。
*** 「ツール」メニューの「S/MIME: 復号と検証」を
*** 実行して下さい。
**********************************************************
```

② 「3.2 署名付きメールの受信」もしくは「4.2 暗号化メールの受信」と同様に操作してください。

③ ［S/MIME message］ダイアログボックスが表示され、復号されたことと署名を確認することができます。
OK ボタンをクリックして、［S/MIME message］ダイアログボックスを閉じて、メッセージの内容を確認します。

証明書を Mac OS のキーチェーンアクセスへ読み込む方法

Mac OS X 10.6 （Snow Leopard）の場合

証明書をチェーンアクセスへ読み込みます。 読み込み

① 管理者から配布された証明書ファイル（xxxxx.p12 ファイル）をダブルクリックします。

② ［キーチェーンアクセス］が開き、パスワード入力のダイアログボックスが表示されます。管理者からこのファイルと一緒に渡されたパスタードを入力し、OK ボタンをクリックします。

③ 分類の「自分の証明書」カテゴリに証明書が表示されたことを確認します。

以上でチェーンアクセスへの読み込みは終了です。

※ 「チェーンアクセス」が開かない場合は、p12 ファイルを直接「チェーンアクセス」のアイコンにドラッグアンドドロップしてください。
※ 「チェーンアクセス」を開いていない場合は、［アプリケーション］フォルダの［ユーティリティ］から開きます。

内容を確認します。 確認

① メニューバーの［ファイル］から［情報を見る］をクリックします。
内容は P5 を参考にしてください。

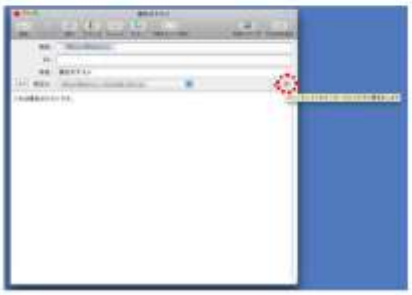
以上で終了です。Mac OS を再起動してください。

Mac Mail

1. 署名付きメール

1.1 署名付きメールを送信する

① 新規メッセージの作成画面を開くと、既定で署名付きメールを作成することができます。
署名をしない場合は、 マークをクリックします。

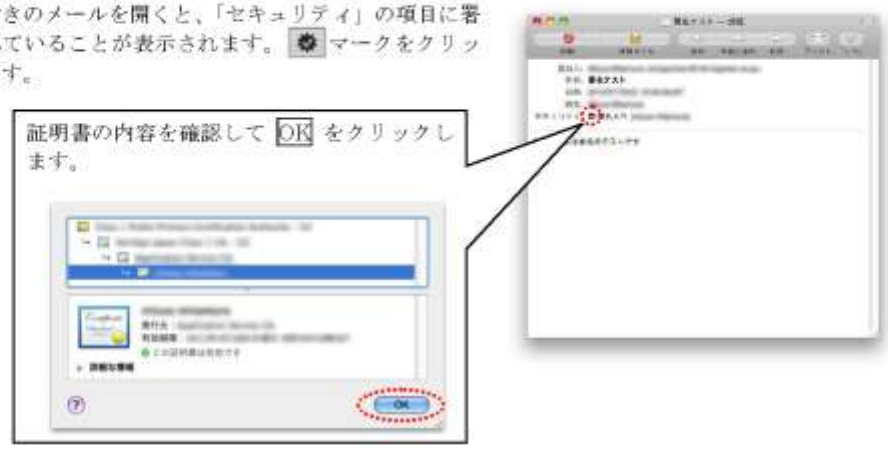


※ 送信者の証明書が正しく登録されていない場合は、マークは になり、操作することはできません。

1.2 署名付きメールの受信

① 署名付きのメールを開くと、「セキュリティ」の項目に署名されていることが表示されます。 マークをクリックします。

証明書の内容を確認して OK をクリックします。



2 暗号化メール

2.1 暗号化メールの送信

① 暗号化メールを送りたい相手のアドレスを入力すると、Mail は自動的に暗号します。
暗号化しない場合は、 をクリックします。

※ 送信者の電子証明書を入手していない場合は、マークは になり、操作することはできません。

2.2　暗号化メールの受信

暗号化メールを開くとセキュリティの項目で暗号化されていることを確認できます。

3　署名付き暗号化メール

署名するにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

【署名付き暗号化メールの作成例】

【署名と暗号化を組み合わせたメールの受信例】

【 アイコンもしくは アイコンをクリックしたときの表示】

1　証明書を「証明書マネージャ」へインポートします。

証明書を Thunderbird の証明書マネージャにインポートします。

① Thunderbird メイン画面の≪ツール≫メニューから≪アカウント設定≫をクリックします。

② 左側のメニューから「セキュリティ」をクリックし、「証明書」グループの 証明書を表示 ボタンをクリックします。

③ 「証明書マネージャ」ダイアログボックスが表示されます。
「あなたの証明書」タブが選択されていることを確認し、読み込む ボタンをクリックします。

④ 管理者から配布された証明書ファイル（xxxxx.p12 ファイル）を選択し、開く ボタンをクリックします。

⑤ このファイルと一緒に渡されたパスワードを入力し、OK ボタンをクリックします。

⑥ 正常に復元ができたメッセージが表示されます。
OK ボタンをクリックします。

⑦ インポートした証明書を選択して、表示 ボタンをクリックします。

⑧ 「一般」タブと「詳細」タブの内容を確認します。

「一般」タブ、「詳細」タブに表示する内容は、P15の内容と変わりありません。

⑨ 閉じる ボタンをクリックします。

⑩ 「証明書マネージャ」の OK ボタンをクリックします。

引き続き、電子メールで利用するための設定を行います。

2 電子メールで利用するための設定

① デジタル署名グループの「メッセージのデジタル署名に使用する証明書」欄の 選択 ボタンをクリックします。

② 選択可能な証明書が表示されます。
設定する証明書を選択して、OK ボタンをクリックします。

③ 「あなたへのメッセージの暗号化と復号に使用する証明書」欄も同時に設定します。
はい をクリックします。

④ デジタル署名グループの「メッセージのデジタル署名に使用する証明書」と暗号化グループの「あなたへのメッセージの暗号化と復号に使用する証明書」が設定されたことを確認し、OK をクリックします。

3. 署名付きメール

3.1 署名付きメールを送信する

① メール作成画面の セキュリティ ボタンの ▼ をクリックし、「このメッセージにデジタル署名する」をクリックします。（署名されている場合は、メニュー項目の前に✔が付きます。）
なお、アプリケーションメニューの≪オプション≫から「このメッセージにデジタル署名する」をクリックしても同じです。

② メール作成画面の右下に （赤丸付き封筒）アイコンが表示されます。

③ 送信します。

※ブラウザに Firefox を利用し、マスターパスワードを設定している場合は、送信する際にマスターパスワードを入力するボックスが表示されます。

3.2　署名付きメールの受信

受信した署名付きメールをスレッドペインから選択すると、メッセージペインの上部（メッセージヘッダ）に アイコンが表示されます。

① アイコンをクリックします。

② 「メッセージは署名されています」と表示されます。
署名証明書を表示 をクリックすると証明書を確認することができます。

③ 証明書の内容を確認し、表示しているウィンドウは OK ボタンをクリックして閉じます。

4.　暗号化メール

4.1　暗号化メールの送信

Thunderbird は、署名付きメールを受信すると、相手の電子証明書とメールアドレスの情報を自動的に証明書マネージャに登録します。
一度署名付きでメールを送信してもらった相手に対しては、特別な設定をしなくても暗号化メールを送信することができます。

① セキュリティ ボタンの ▼ をクリックして≪このメッセージを暗号化する≫をクリックします。（暗号化されている場合は、メニュー項目の前に✓が付きます。）
作成中のメール画面の右下に （錠前アイコン）が表示されたことを確認して、メールを送信します。

4.2　暗号化メールの受信

受信した暗号化メールをスレッドペインから選択すると、メッセージペインの上部（メッセージヘッダ）に （錠前アイコン）が表示されます。

① 錠前アイコンをクリックします。

② メッセージは暗号化されていることを確認して、OK ボタンをクリックします。

5　署名付き暗号化メール

署名することにより、メールの内容がなりすました人物ではなく送信者本人により署名されていること、および転送中に改ざんされていないことが受信者に証明されます。さらに、メールを暗号化して安全性を高めることができます。

【署名付き暗号化メールの作成例】

【署名付き暗号化メールの受信例】

【 アイコンもしくは アイコンをクリックしたときの表示】

Office ソフトでの利用

Office ドキュメントにデジタル署名を追加して、ドキュメントが署名した本人のものであること、デジタル署名された後に内容が変更または改ざんされていないことを証明することができます。

Microsoft Office2003 ドキュメントにデジタル署名する

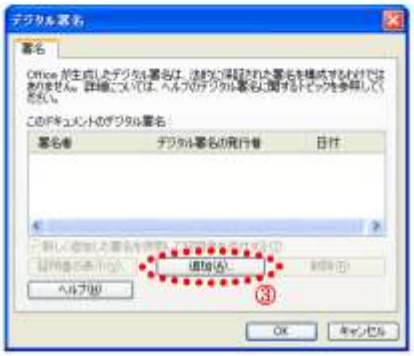
Word2003 にデジタル署名する

① ≪ツール≫メニューの≪オプション≫をクリックします。

② ［オプション］ダイアログボックスの「セキュリティ」タブをクリックし、「この文書のファイル共有オプション」グループの デジタル署名 ボタンをクリックします。

③ 追加 ボタンをクリックします。

保存のメッセージが表示された場合は、はい をクリックしてください。



④ 使用する証明書を選択し、OK ボタンをクリックします。

⑤　［デジタル署名］ダイアログボックスに戻りますので、OK ボタンをクリックします。

※証明書の表示 ボタンをクリックすると［証明書］ダイアログボックスが開き、証明書の内容を確認することができます。
表示される内容は５ページと同様です。

⑥　［オプション］ダイアログボックスの OK ボタンをクリックします。

⑦　ステータスバーに （署名アイコン）が表示されます。

以上でデジタル署名の追加は終了です。

署名付きドキュメントを確認する

署名付きの文書を開くと、ステータスバーに「(この文書にはデジタル署名が含まれています)」と表示されます。(文書を完全に開いた時点で消えます。)

タイトルバーに（署名済み、未確認）と表示されます。

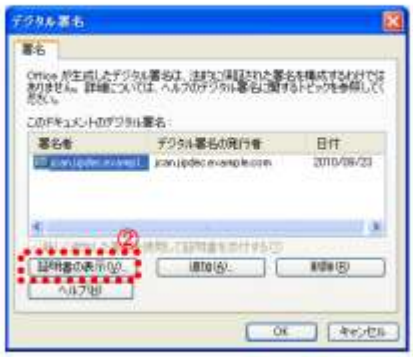
また、ステータスバーの署名アイコンにマウスを近付けると「この文書はデジタル署名がされています」と表示されます。

① 署名アイコンをダブルクリックします。

② 証明書の表示 ボタンをクリックして証明書の内容を確認します。
表示される内容は５ページと同様です。

③ 確認ができたら［証明書］ダイアログボックスの OK ボタンをクリックします。

④ ［デジタル署名］ダイアログボックスの OK ボタンをクリックします。



以上で確認は終了です。

Excel2003 および PowerPoint2003 にデジタル署名する/確認する

デジタル署名を付す手順は Word2003 と同様です。(①～⑦)
ただし、Word2003 のようにステータスバーで署名アイコンを確認することはできません。
署名していることを確認するには、保存したブックまたはスライドを開きます。
署名付きのドキュメントを開いたら、タイトルバーに（署名済み、未確認）と表示されます。

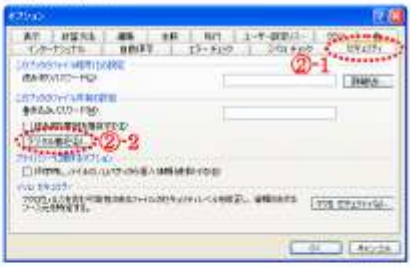
Excel2003 の場合 

PowerPoint2003 の場合 

① ≪ツール≫メニューの≪オプション≫をクリックします。

② ［オプション］ダイアログボックスの「セキュリティ」タブをクリックし、「この文書のファイル共有オプション」グループの デジタル署名 ボタンをクリックします

■Excel2003



■PowerPoint2003

③ ［デジタル署名］ダイアログボックスの「署名」タブの「このドキュメントのデジタル署名」の一覧に署名者の名前があることを確認します。

④ 確認ができたら、OK ボタンをクリックします。

⑤ ［オプション］ダイアログボックスの OK ボタンをクリックします。

※上位バージョン（2007 および 2010）で作成された署名付きドキュメントについて

上位バージョンの署名付きドキュメントを開くと、署名は削除されます。なお、Office 互換パックをインストールして開いても署名は削除されますのでご注意ください。

■互換パックをインストールしている場合

Microsoft Office2007 ドキュメントにデジタル署名する

Office2007 アプリケーションでは、署名欄を作成する方法（Word と Excel）とステータスバーに署名アイコンを表示するだけの非表示のデジタル署名（Word、Excel、PowerPoint）があります。ここでは、非表示のデジタル署名を扱います。

Word2007 にデジタル署名する

① （Office ボタン）をクリックし、≪配布準備≫の≪デジタル署名の追加≫をクリックします。

② 以下のダイアログボックスが表示されますので、OK ボタンをクリックします。

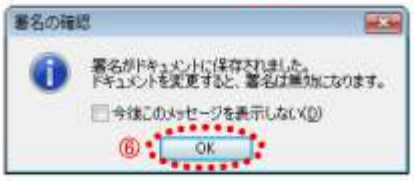
保存のダイアログボックスが表示された場合は、はい をクリックし、文書を保存します。

③ ［署名］ダイアログボックスの 変更 ボタンをクリックします。
※既に署名者欄に使用する署名者名が表示されている場合は、変更する必要はありません。

④ 使用する証明書を選択し、OK ボタンをクリックします。

⑤ 署名者の欄に署名者名が表示されたことを確認し、署名 ボタンをクリックします。
※必要に応じて「このドキュメントに署名する目的」を入力してください。

⑥ ［署名の確認］ダイアログボックスが表示されたら、OK ボタンをクリックします。



⑦ 署名作業ウィンドウが開き、ステータスバーに （署名アイコン）が表示されます。

以上でデジタル署名の追加は終了です。

署名付きドキュメントを確認する

① 署名付きの文書を開くとタスクバーに（署名アイコン）が付きます。署名アイコンにマウスを近付けてポップヒントを確認します。（「このドキュメントには署名が含まれています。」）

② （署名アイコン）をクリックし、［署名］作業ウィンドウに「有効な署名」と表示されていることを確認し、署名者の▼をクリックし、「署名の詳細」をクリックします。

③ ［署名の詳細］ダイアログボックスで署名者の名前を確認し、表示 ボタンをクリックして［証明書］ダイアログボックスを表示します。
表示される内容は 8 ページの「全般」タブ、「詳細」タブと同様です。
内容を確認したら、OK ボタンをクリックして［証明書］ダイアログボックスを閉じます。

④ ［署名の証明］ダイアログボックスの「収集された追加署名情報表示」のリンクをクリックします。

追加情報として、署名された日時や OS のバージョン、Office のバージョンなどを確認できます。日時が証明書の［有効期限］の期間内であることを確認します。

⑤ OK ボタンをクリックして［署名の証明］ダイアログボックスを閉じ、［署名の詳細］ダイアログボックスも閉じます。

以上で確認は終了です。

Excel2007 および PowerPoint2007 にデジタル署名する/確認する

デジタル署名を付する手順は Word2007 と同様です。(①～⑦)

■Excel2007

■PowerPoint2007

デジタル署名を確認する手順も Word2007 と同様です。(①～⑤)
ただし、署名付きの Excel ブックのみ、タイトルバーに［読み取り専用］と表示されます。

Microsoft Office2010 ドキュメントにデジタル署名する

Office2010 アプリケーションでは、署名欄を作成する方法（Word と Excel）とステータスバーに署名アイコンを表示するだけの非表示のデジタル署名（Word、Excel、PowerPoint）があります。ここでは、非表示のデジタル署名を扱います。

Word2010 にデジタル署名する

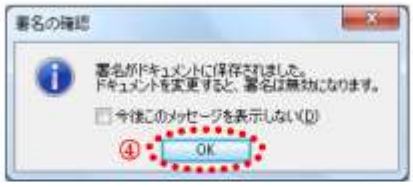
① ≪ファイル≫タブの≪情報≫から「情報の保護」ボタンをクリックし、「デジタル署名の追加」をクリックします。

② 以下のダイアログボックスが表示されますので、OK ボタンをクリックします。

以下のダイアログボックスが表示された場合は、はい をクリックし、文書を保存します。

③ 署名者の欄に名前が表示されたことを確認し、署名 ボタンをクリックします。
※必要に応じて「このドキュメントに署名する目的」を入力してください。

④ ［署名の確認］ダイアログボックスが表示されたら、OK ボタンをクリックします。



⑤ BackStage ビューに「署名された文書」「アクセス許可」の項目が表示されます。

⑥ 「署名の表示」ボタンをクリックすると、編集画面が表示され、署名ウィンドウが開きステータスバーに（署名アイコン）が表示されます。また、画面上部に最終版であることを示すメッセージが表示されます。

以上でデジタル署名の追加は終了です。

署名付きドキュメントを確認する

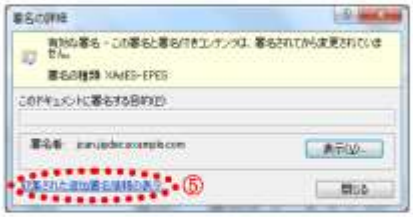
① 署名付きの文書を開くと、画面上部に最終版である表示と、ステータスバーに（署名アイコン）が表示されます。

② 署名アイコンにマウスを近付けてポップヒントを確認します。（「このドキュメントには署名が含まれています。」）

③ （署名アイコン）をクリックし、［署名］作業ウィンドウに「有効な署名」と表示されていることを確認し、署名者の▼をクリックし、「署名の詳細」をクリックします。

④ ［署名の詳細］ダイアログボックスで署名者の名前を確認し、表示 ボタンをクリックして［証明書］ダイアログボックスを表示します。
表示される内容は 11 ページの「全般」タブ、「詳細」タブと同様です。
内容を確認したら、OK ボタンをクリックして［証明書］ダイアログボックスを閉じます。

⑤ ［署名の詳細］ダイアログボックスの「収集された追加署名情報表示」のリンクをクリックし、追加情報の署名された日時や OS のバージョン、Office のバージョンなどを確認できます。表示される内容は 61 ページと同様です。日時が証明書の［有効期限］の期間内であることを確認します。



⑥ OK ボタンをクリックして［署名の証明］ダイアログボックスを閉じ、［署名の詳細］ダイアログボックスも閉じます。

以上で確認は終了です。

Excel2010 および PowerPoint2010 にデジタル署名する/確認する

デジタル署名を付す手順は Word2010 と同様です。（①～⑥）

■Excel2010

■PowerPoint2010

デジタル署名を確認する手順も Word2010 と同様です。（①～⑥）

1. 文書プレビューモード

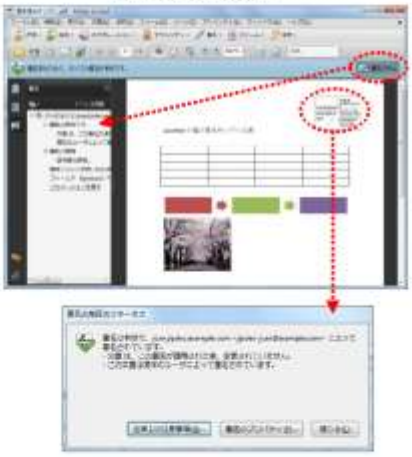
電子署名を行う際の環境を文書プレビューモードにします。文書プレビュー機能は、文書にダイナミックコンテンツや外部の依存関係が含まれていないかどうかを確認できます。文書の表示方法に影響する可能性があるフォームフィールド、マルチメディア、JavaScript などの要素が含まれていないか確認し、JavaScript、アクション、埋め込みメディアなど、文書を変更したり、文書の整合性を損なう可能性がある内容を無効にするか削除します。

1. ≪編集≫メニューの≪環境設定≫をクリックし、[環境設定]ダイアログボックスの分類から「セキュリティ」をクリックします。
2. 「署名時に文書を文書プレビューモードで表示する」を✔し、OK ボタンをクリックします。

2. 電子署名する

① ツールバーの 署名 から「文書に署名」をクリックします。
② 「マウスボタンを押しながらドラッグして…」のダイアログボックスが表示されたら OK をクリックし、署名フィールドを作成します。
③ 「署名に使用する ID」を確認し、署名 をクリックします。
④ 保存します。

Windows の場合



Mac の場合

補足 1：署名の表示方法を変更するには？

［文書に署名］ダイアログボックスの「表示方法」の▼をクリックし、「表示方法を新規作成」を選択します。

補足 2：署名の環境設定について

≪編集≫メニュー ⇒ ［環境設定］ダイアログボックス ⇒ 分類「セキュリティ」 ⇒「電子署名」グループ ⇒ 詳細環境設定 ボタン

【署名時に署名の失効ステータスを含める】（既定）
証明書が有効であるか、失効しているかに関する情報を埋め込みます（署名の検証が必要）。このオプションでは、オンラインで証明書が失効したかどうかを判定する必要がないので、検証処理が高速になります。

【署名時に理由を表示する】
署名フィールドに署名の理由を追加します。

【署名時に署名地と連絡先の情報を表示する】
署名フィールドに署名地情報を追加します。

署名付きメール/暗号化メールの送信時のエラー

Windows	Outlook Express 6	署名付きメール		送信者（自分）の証明書が正しく登録されていません。証明書を登録してください。
		暗号化メール		受信者の証明書が正しくアドレス帳に登録されていません。送信相手に電子署名付きのメールを送信してもらいます。
	Outlook2003	署名付きメール		送信者（自分）の証明書が正しく登録されていません。証明書を登録してください。
		暗号化メール		受信者の証明書が正しくアドレス帳に登録されていません。送信相手に電子署名付きのメールを送信してもらい、Outlook 連絡先に登録します。
	Outlook2007	署名付きメール		送信者（自分）の証明書が正しく登録されていません。証明書を登録してください。
		暗号化メール		受信者の証明書が正しくアドレス帳に登録されていません。送信相手に電子署名付きのメールを送信してもらい、Outlook 連絡先に登録します。
	Windows Mail Windows Live Mail	署名付きメール		送信者（自分）の証明書が正しく登録されていません。証明書を登録してください。
		暗号化メール		受信者の証明書が正しくアドレス帳に登録されていません。送信相手に電子署名付きのメールを送信してもらいます。
	Outlook2010	署名付きメール		送信者（自分）の証明書が正しく登録されていません。証明書を登録してください。
		暗号化メール		受信者の証明書が正しくアドレス帳に登録されていません。送信相手に電子署名付きのメールを送信してもらい、Outlook 連絡先に登録します。

Windows	Becky! Internet Mail 2.5	署名付きメール		送信者（自分）の証明書が正しく登録されていません。証明書を登録してください。
		暗号化メール		証明書マネージャに相手の証明書が登録されていません。相手から署名つきメールを送ってもらいます。
	Thunderbird3.1	署名付きメール		送信者（自分）の証明書が正しく登録されていません。証明書を登録してください。
		暗号化メール		証明書マネージャに相手の証明書が登録されていません。相手から署名つきメールを送ってもらいます。
Mac	Thunderbird3.1	署名付きメール		送信者（自分）の証明書が正しく登録されていません。証明書を登録してください。
		暗号化メール		証明書マネージャに相手の証明書が登録されていません。相手から署名つきメールを送ってもらいます。

※　署名付きメールで表示されるエラーは、証明書が失効している場合もあります。

※　署名付きメールで表示されるエラーは、複数のメールアドレスを所有している場合に現在の「送信者」欄のアドレスと証明書が合っていない場合もあります。証明書のあるメールアドレスで送信してください

署名付きメール、暗号化メール、署名付き・暗号化メールに必要な証明書とできること

	自分の証明書	相手の証明書		できること
署名付きメール	○	－	－	改ざん検知 なりすまし防止
暗号化メール	○	○	相手のアドレスを登録する必要があります。Outlook および Windows Live Mail 以外は、既定で自動的に登録されます。各メールソフトの設定を変更している場合は手動で登録してください。	盗聴防止
署名付き・暗号化	○	○		改ざん検知 なりすまし防止 盗聴防止

よくある質問

Q1. 署名付きメールを受信後、署名アイコンをクリックしてメッセージの作成者から正常に送信されていることを確認しましたが、「取り消し状態」に「デジタル ID の確認が無効になっています。」と表示されました。(Outlook Express6、Windows Mail)

初期設定では、証明書失効状態の確認は「実行しない」になっています。
［ツール］メニューの［オプション］をクリックし、オプションダイアログボックスの「セキュリティ」タブをクリックします。
次に 詳細設定 をクリックし、セキュリティの詳細設定ダイアログボックスの「デジタル ID の確認」グループで「オンラインのときのみ」をクリックしてください。

Q2. 署名付きのメールを送ってもらいましたが、自動的に相手の証明書がアドレス帳に登録されません。

Outlook Express6、Windows Mail の場合
初期設定では、送信者の証明書とメールアドレスを自動的にアドレス帳に登録するようになっています。自動的に登録されない場合は、［ツール］メニューの［オプション］をクリックし、オプションダイアログボックスの「セキュリティ」タブをクリックします。
次に 詳細設定 をクリックし、セキュリティの詳細設定ダイアログボックスの「デジタル署名されたメッセージ」グループで「送信者の証明書をアドレス帳に追加する」をクリックしてください。
なお、Outlook および Windows Live Mail の場合は、署名付きのメールを受信したら、アドレス帳に登録をしてください。
〔Outlook2003：P20、Outlook2007：P30、Windows Live Mail：P34、Outlook2010：P39 参照〕

Thunderbird の場合
初期設定では、送信者の証明書とメールアドレスを自動的にアドレス帳に登録するようになっています。自動的に登録されない場合は、［ファイル］メニューの［オプション］をクリックし、編集 ボタンをクリックし、「アドレス入力」タブの「メール送信時に受信者を次のアドレス帳に自動で追加する」をクリックしてください。(Mac 版の場合は、［Thunderbird］メニューの［環境設定］をクリックします。)

Q3. 署名付きのメールを送りましたが、送信相手に証明書の情報が届きませんでした。(Outlook Express6、Windows Mail)

初期設定では、署名付きメールに証明書の情報を追加した状態で送信されます。正しく送信できない場合は、［ツール］メニューの［オプション］をクリックし、オプションダイアログボックスの「セキュリティ」タブをクリックします。
次に 詳細設定 をクリックし、「デジタル署名されたメッセージ」グループの「署名付きメッセージにデジタル ID を追加する」をクリックしてください。

Q4. 署名付きのメールを送りましたが、送信相手に証明書の情報が届きませんでした。(Outlook2003、2007、2010)

電子メールの暗号化グループの「このメッセージにデジタル署名を追加する」に✓が付いていることを確認してください。

2003 の場合　≪ツール≫⇒≪オプション≫⇒≪セキュリティ≫タブ
2007 の場合　≪ツール≫⇒≪セキュリティセンター≫⇒≪電子メールのセキュリティ≫
2010 の場合　≪オプション≫タブ⇒≪その他のオプション≫ダイアログボックスを表示⇒≪セキュリティ設定≫

Q5.　証明書のバックアップはどのようにすればよいですか？（エクスポート）

バックアップは、メールソフトから行うこともできますが、ここではブラウザの証明書ストア（証明書マネージャ）から行う方法を紹介します。

Internet Explorer 6、7、8 の場合

① ≪ツール≫メニューから≪インターネットオプション≫をクリックします。
② ［インターネットオプション］ダイアログボックスの「コンテンツ」タブをクリックします。
③ 証明書 をクリックします。
④ ［証明書］ダイアログボックスの「個人」タブをクリックし、バックアップをする証明書を選択し、エクスポート をクリックします。
⑤ ［証明書のエクスポートウィザード］が起動します。
⑥ 次へ をクリックします。

⑦ 「証明書と一緒に秘密キーをエクスポートしますか？」の項目で「はい、秘密キーをエクスポートします」をクリックし、次へ をクリックします。

⑧ （IE6）Personal Information Exchange – PKCS#12 (PFX) が選択されていることを確認し、「証明のパスにある証明書を可能であればすべて含む」「強力な保護を有効にする」を✔して、次へ をクリックします。

（IE 7、IE8）Personal Information Exchange - PKCS#12 (PFX) が選択されていることを確認し、「証明のパスにある証明書を可能であればすべて含む」「すべての拡張プロパティをエクスポートする」を✔して、次へ をクリックします。

⑨ パスワードを入力して、次へ をクリックします。（ここで入力するパスワードは任意です。）
⑩ わかりやすいファイル名と保存先設定してくださいし、次へ をクリックします。
⑪ 「証明書のエクスポートウィザードの完了」画面が表示されますので、完了 をクリックします。
⑫ 「正しくエクスポートされました。」と表示されますので、OK をクリックします。

⑬ 表示しているウィンドウを閉じます。

拡張子は「.pfx」となりますが、p12 ファイルと同様に取り扱うことができます。

Windows 環境の Firefox

① ≪ツール≫メニューの≪オプション≫をクリックします。
② ［オプション］ダイアログボックスの「詳細」をクリックし、証明書を表示 をクリックします。
③ ［証明書マネージャ］ダイアログボックスの「あなたの証明書」タブをクリックし、バックアップをする証明書を選択し、すべてバックアップ をクリックします。
④ ファイル名と保存先はわかりやすい箇所を選択してください。選択後、保存 をクリックします。
⑤ ［証明書のバックアップ用パスワードの設定］ダイアログボックスが表示されますので、パスワードを入力して、OK をクリックしてください。（ここで入力するパスワードは任意です。）
⑥ 「証明書と秘密鍵が正常にバックアップされました。」と表示されます。OK をクリックします。
⑦ 表示しているウィンドウを閉じます。

Mac 環境の Firefox

① メニューバーの≪Firefox≫から≪環境設定≫をクリックします。
② 「詳細」の「暗号化」をクリックし、証明書を表示 をクリックします。
③ ［証明書マネージャ］ダイアログボックスの「あなたの証明書」タブをクリックし、バックアップをする証明書を選択し、すべてバックアップ をクリックします。
④ 名前と場所はわかりやすい箇所を選択してください。選択後、保存 をクリックします。
⑤ パスワード入力画面でパスワードを入力して、OK をクリックしてください。（ここで入力するパスワードは任意です。）

⑥ 「証明書と秘密鍵が正常にバックアップされました。」と表示されます。OK をクリックします。
⑦ 表示しているウィンドウを閉じます。

Q6. 複数のパソコンに証明書をインポートできますか？

電子証明書は、複数のパソコンにインポートすることが可能です。
管理者から配布された証明書ファイルをほかの PC へインポートして利用してください。なお、証明書ファイルのインポートには、管理者からファイルを配布された際に伝えられたパスワードが必要になります。パスワードを忘れるとインポートすることができません。

証明書ファイルがない場合は、証明書が入っているパソコンから証明書のバックアップを取り、バックアップした証明書を他のパソコンにインポートします。
インポートの方法は、Windows OS の場合は P3～P11、Mac OS の場合は P55 を参考にしてください。

Q7. パスワードを忘れてしまいました。

パスワードを忘れてしまった場合や秘密鍵を紛失した場合は、すみやかに管理者へ連絡してください。

Q8.　電子証明書の有効期限が切れました。暗号メールを送信できますか？

電子証明書の有効期限が切れた状態でも設定によって暗号メールは使えます。しかし、あくまでも一時的な対処です。新しい証明書をお使いください。

Q9.　失効した証明書を削除していいですか？

失効手続きを行うと、失効リストに登録されるため、二度と同じ電子証明書を利用することはできません。ただし、無効になったからといっても、暗号化された過去のデータを復合するには秘密鍵が必要ですので、必ず秘密鍵のバックアップを取り、安全な場所に保管してください。
削除してしまうと復号できなくなります。

Q10. 署名付きメールを送信すると「変な文字が表示されて読めない」、「文字化けが起きている」と受信者から言われました。

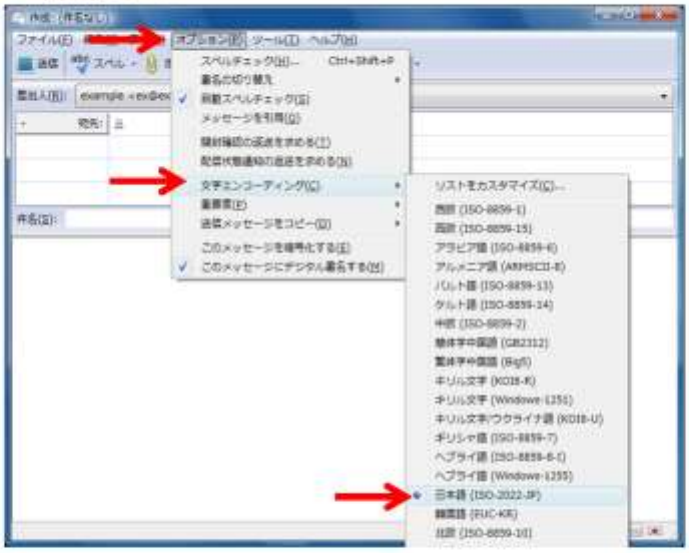
「文字化け」が起こる原因は、「電子署名付きメールの文字コード」と「受信者のメーラー」によると考えられます。「文字化け」の現象は、主に、受信者が一部のメーラー（Outlook Express、Windows Mail、Windows Live Mail）を利用しており、文字コードが JIS 以外（例えば UTF-8）の添付なしの電子署名付きメールを受信した場合に起こります。メーラーはそのメールの文字コードを判別して自動で正しい文字を表示されるようになっていますが、前述のメーラーは、添付なしの電子署名付きのメールについて文字コードの判別ができず、全てデフォルトの文字コード（日本語環境の場合は JIS）で画面に表示する仕様になっているようです。この問題を解決するには 3 つの方法が考えられます。(1) 送信者側で電子署名付きメールを送る際に文字コードを JIS に指定する方法、(2) 受信者側で文字コードをあわせる方法、(3) 電子署名を外す方法、です。それぞれの対処方法は以下の通りです。

(1) 送信者側で電子署名付きメールを送る際に文字コードを JIS に指定する方法。
電子署名付きメールを送る際に文字コードを JIS に指定して送信してください。以下に具体的なメーラー（Windows Mail、Thunderbird）について指定方法を記述しておきますのでご参考下さい。

Windows メールの場合
メール作成画面の「書式(O)」→「エンコード(N)」→「日本語(JIS)」を選択後、メールを送信します。

Thunderbird の場合

メール作成画面の「オプション(P)」→「文字エンコーディング(C)」→「日本語(ISO-2022-JP)」を選択後、メールを送信します。

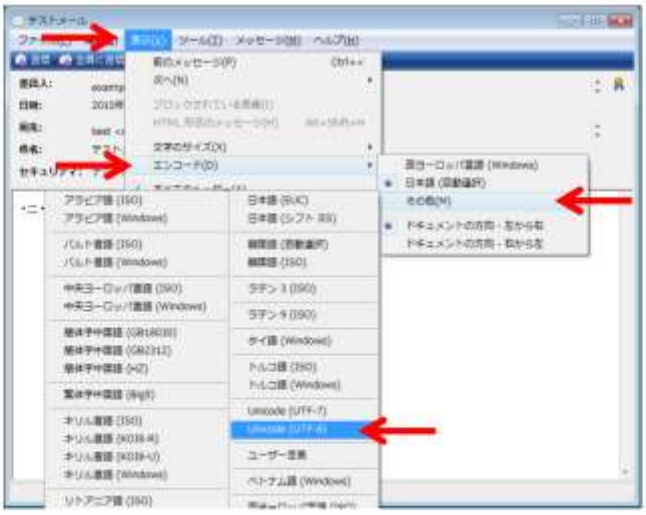


(2) 受信者側で文字コードをあわせる方法

文字化けが起きている受信者側で文字コードをあわせて、正しい文字を表示させる方法です。具体的なメーラー（Windows Mail）についての指定方法は以下の通りです。

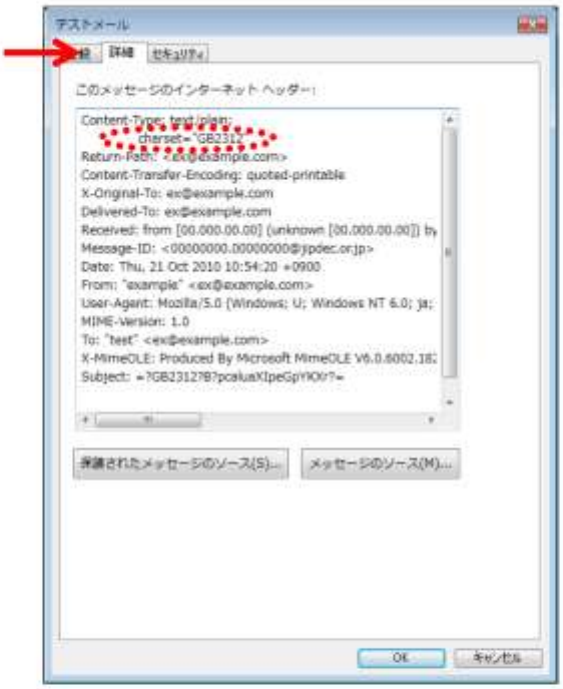
Windows Mail の場合

受信メールを開き、「表示(V)」→「エンコード(D)」→（適当な文字コード）を選択します。（適当な文字コード）ですが、日本語でやり取りをしている場合、「Unicode(UTF-8)」を選択すれば、たいていは正しく表示されます。それでも表示されない場合は、メールの（適当な文字コード）を調べて選択することになります。

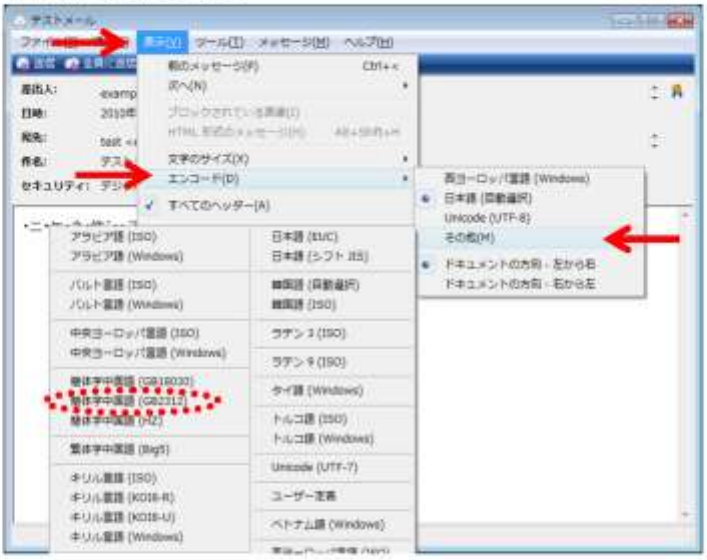


（適当な文字コード）を調べる方法　（UTF-8 でも正しく表示されない場合）
受信メールを開き、「ファイル(F)」→「プロパティ(R)」を選択します。

「詳細」タブを選択し、「このメッセージのインターネット ヘッダー」の「charset」を探して文字コードを特定します。（画像例では、GB2312）



文字コードが特定されたら、「表示(V)」→「エンコード(D)」を選び、特定された文字コードを選択します。(下の画像例では、GB2312)

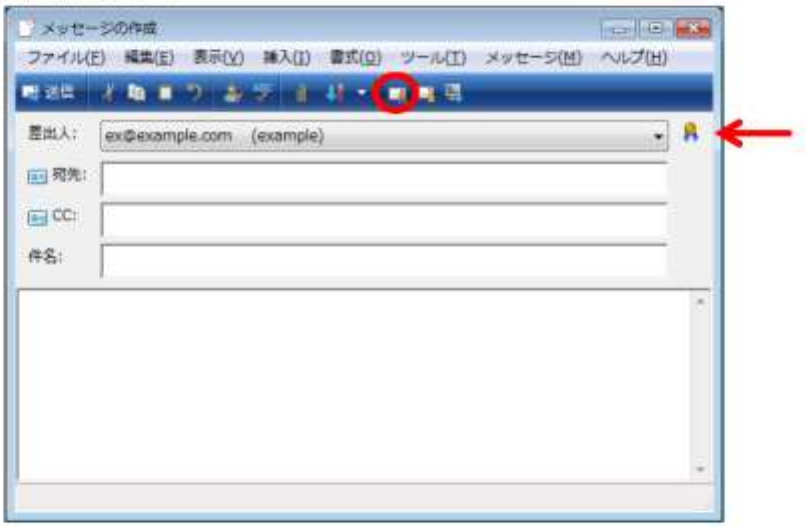


(3) 電子署名を外す

電子署名を外して送信します。

Windows Mail の場合

電子署名のチェックボタンを押すことで電子署名が外せます。右上にある電子署名のマークが消えれば電子署名が外れています。



Q11. 「Microsoft Office Outlook」を使用しているのですが、電子署名付きのメールの場合、添付のないメールなのに「添付マーク（クリップ）」がついています。同じメッセージでも他のメーラーでは「添付マーク（クリップ）」付いていません。

電子署名付きのメールは「電子証明書」をメールに添付した形でやり取りされます。「Microsoft Office Outlook」で電子署名付きメールを見ると、通常の添付ファイル欄に何も表示されず、一見添付ファイルがないように思えますが、実際は署名マークとして「電子証明書」が添付されています。署名マークをクリックすれば「電子証明書」の内容を見ることができます。そのため「Microsoft Office Outlook」の場合、「電子証明書」を添付ファイルとし、「添付マーク（クリップ）」を表示させているようです。しかし、メーラーによっては「電子証明書」を添付とみなさず「添付マーク（クリップ）」を付けない場合もあるようなので、同じメッセージでも他のメーラーでは「添付マーク（クリップ）」付かない時があります。

Q12. 「Microsoft Office Outlook」を使用しているのですが、電子署名付きメールはすべて「添付マーク（クリップ）」が付されるため、「その他の添付ファイル（ワード、エクセル等）」があるメールだけを区別してソートすることができません。

Q11 に関係しますが「Microsoft Office Outlook」の場合、電子署名付きメールは「電子証明書」が添付されるため、全て「添付マーク（クリップ）」が付されます。「その他の添付ファイル（ワード、エクセル等）」のメールだけを区別しソートすることは「Microsoft Office Outlook」の標準仕様ではできません。

Q13. メーリングリストに電子署名付きメールを投稿すると「セキュリティの問題 があります」、「メッセージが改ざんされています」等の「セキュリティ警告」が表示されると、メーリングリスト登録者から言われました。

メーリングリストと電子署名の併用は一般的に相性が悪いと言われています。メーリングリストの多くは投稿されたメール内容を変更してからメーリングリスト登録者に送信します。例えば、Subject に通し番号を加える、添付ファイルを削除する、本文に広告文を追記するなどの変更がされます。それらが「メッセージの改ざん」とみなされセキュリティ警告が出されます。もちろん特定のメーリングリストやメーラーでは問題なく使える場合もありますが、メーリングリストに投稿する際は、信頼性は劣ってしまいますが、電子署名を外して利用するとセキュリティ警告は回避できます。メーリングリストでの電子署名利用の課題については、現在検討中です。

Q14. 電子署名付きのメールを送ったところ、相手から「返信できない」と言われました。その際「署名されたメッセージや暗号化されたメッセージを送信するには、このアカウント用のデジタル ID を取得する必要があります」と表示されるそうです。

電子署名付きメールが返信できないのは、返信者である相手方が電子証明書を持っていない場合に生じます。特定のメーラー（Outlook Express、Windows Mail、Windows Live Mail）では電子署名付きメールに返信する際は、電子署名を付けて返信するようにデフォルトで設定されています。電子署名のチェックボタンを外すことで返信できるようになりますので、電子署名のチェックボタンを外して返信するようにお伝えください。電子署名の外し方は Q10 の(3)を参照ください。

Q15. 送信用のメールに必ず電子署名が付いてしまいます。

オプションに用意されている「送信メッセージにデジタル署名を付ける」の項目に✓している可能性があります。✓を外してください。

Outlook Express6、Outlook2003、Windows Mail の場合

≪ツール≫メニュー ⇒ 「オプション」 ⇒ 「セキュリティ」タブ

【Outlook Express6】

【Outlook2003】

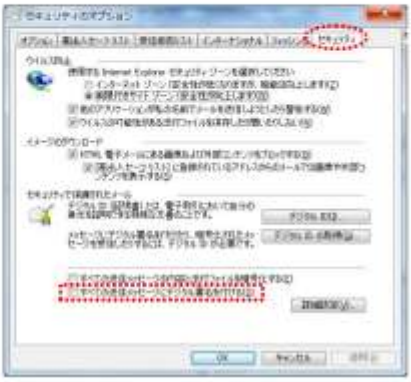
【Windows Mail】

Outlook2007 の場合

≪ツール≫メニュー ⇒ 「セキュリティセンター」 ⇒ 「電子メールのセキュリティ」

Windows Live Mail の場合

≪ツール≫メニュー ⇒ 「セキュリティオプション」 ⇒ 「セキュリティ」タブ



Outlook2010 の場合

≪ファイル≫タブ ⇒ 「オプション」 ⇒ 「セキュリティセンター」 ⇒ 「セキュリティセンターの設定」 ⇒ 「電子メールのセキュリティ」

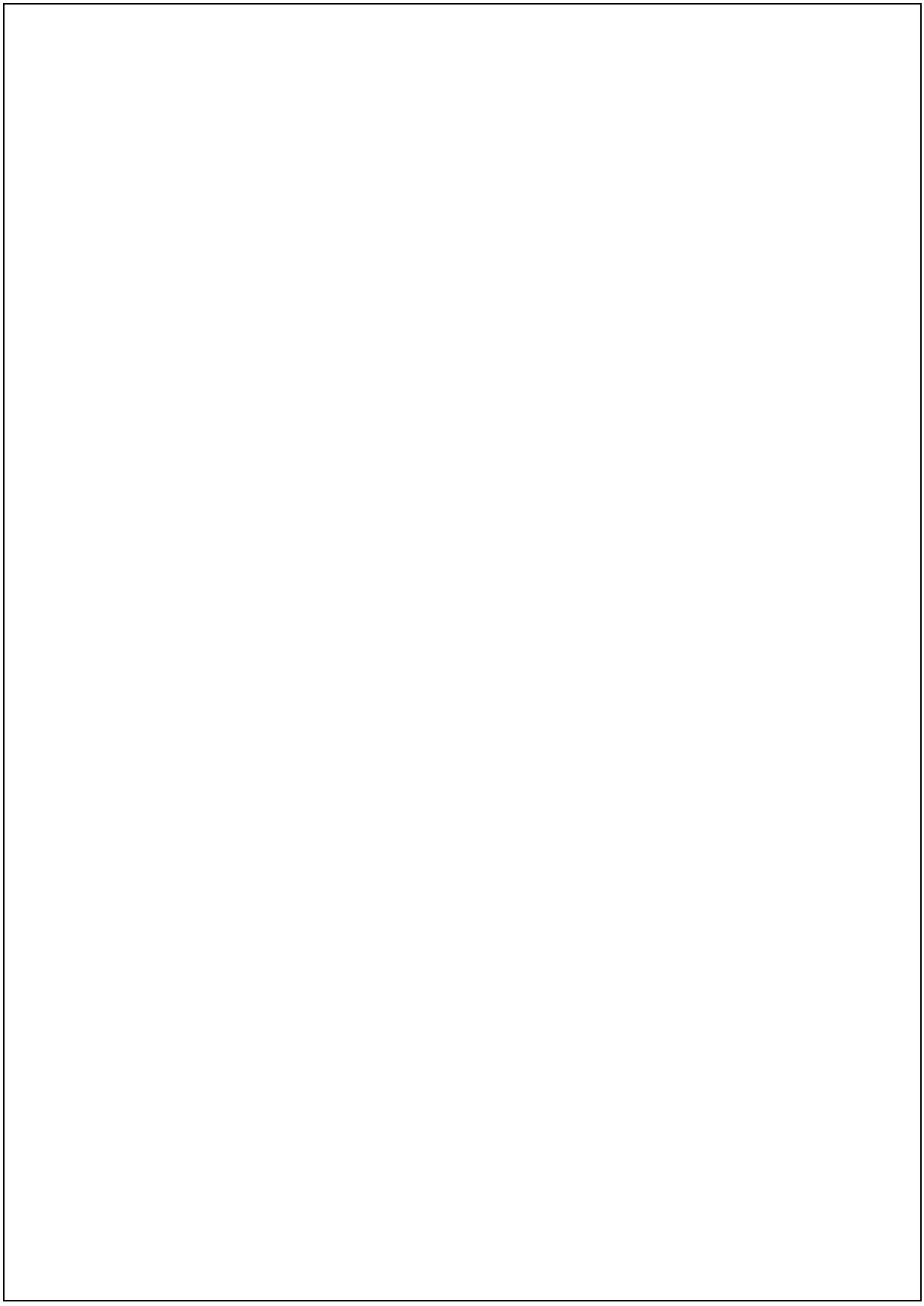
TunderBird3.1 の場合（Windows 版、Mac 版）

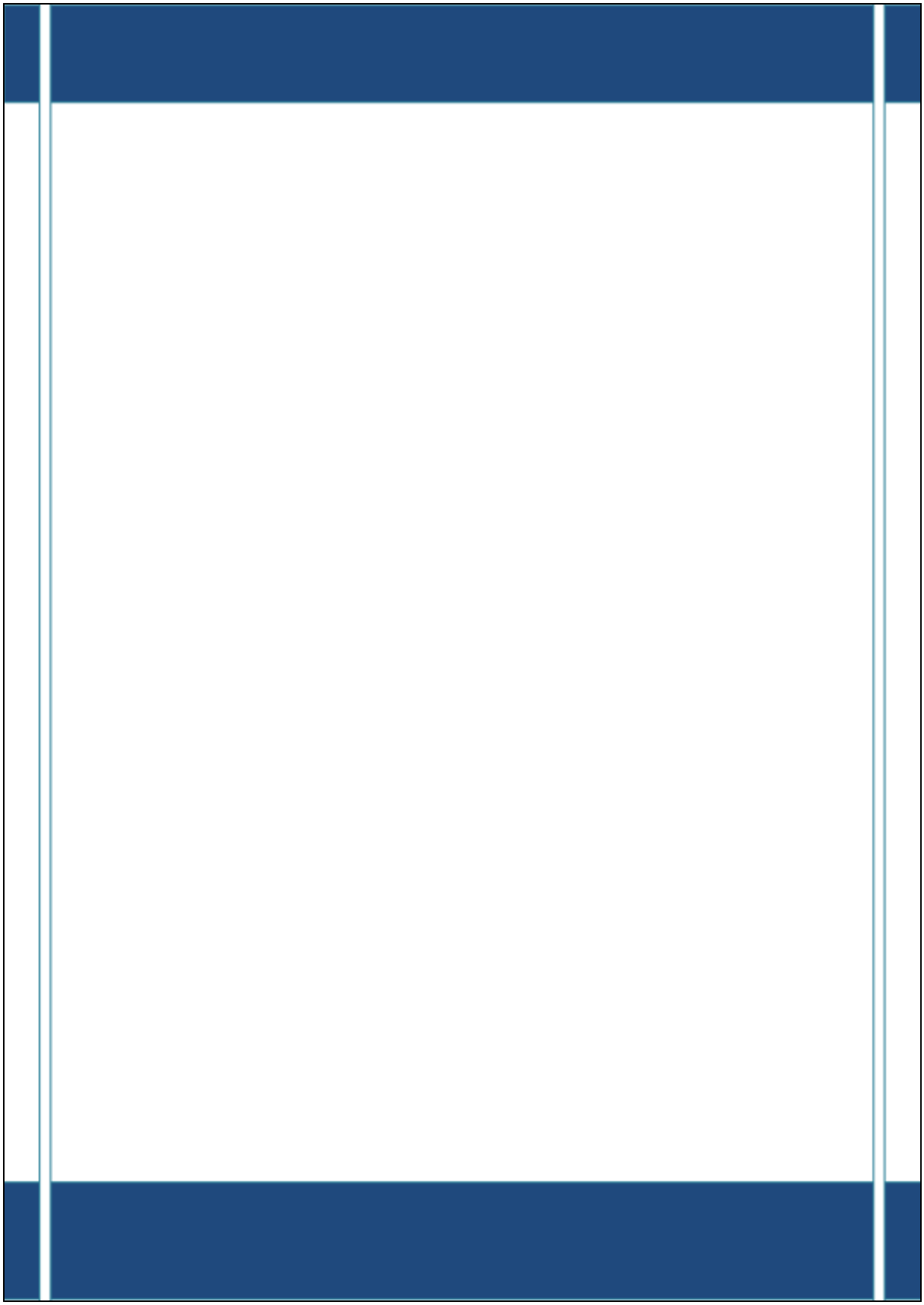
≪ツール≫メニュー ⇒ 「アカウント設定」 ⇒ 「セキュリティ」

第１版　平成　22　年　11　月発行
第２版　平成　22　年　12　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
機械振興会館内
ＴＥＬ（３４３６）７５１３





平成２３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
機械振興会館内
ＴＥＬ（３４３６）７５１３

印刷所　有限会社アクロスネットワーク

東京都千代田区三崎町３－３－６
工晋ビル
ＴＥＬ（５２１１）１７３０

２２－Ｈ００３