経済産業省補助事業

平成１６年度情報基盤対策技術開発等推進事業

（電子商取引（ＥＣ）技術基盤の相互運用性に関する調査研究）

特恵電子原産地証明書パイロットシステムによる PKI 相互運用性評価報告書

平成１７年３月

（財）日本情報処理開発協会

― 目次 ―

1 はじめに

近年、世界の経済社会の幅広い分野において情報技術（デジタル技術）を高度に活用する動きが急速に進展しつつある。その中において、公開鍵認証基盤（Public Key Infrastructure:以下 PKI という）の整備は、各国で進められており、インターネット上で電子商取引を安全にかつ確実に実現する技術として、世界の経済社会に多大な影響をもたらすものである。

日本 PKI フォーラムでは、これまでアジアを中心とする PKI 技術の相互運用性の確保を図るために、日本、韓国、シンガポール、チャイニーズ台北、香港チャイナ、タイにおける認証局間相互接続実証実験を通して、相互接続のモデル、公開鍵証明書検証の記載方法、電子署名および公開鍵証明書の検証方法、PKI 技術を利用するためのインターフェースに関する標準化を推進してきた。今後は、これらの成果がビジネスで利用されていくことが期待されている。

日本と海外諸国との関係は、日本が自由貿易協定（FTA：Free Trade Agreement）の締結を進めていることにより、大きな変革期を迎え始めている。日本－シンガポール間においては、「新たな時代における経済上の連携に関する日本国とシンガポール共和国との間の協定」（平成 14 年 1 月）が締結された。この協定においては、貿易取引文書の電子化に関する両締約国間の協力が明示され、貿易取引文書の電子化に関する活動に従事する両締約国に関連する民間の団体間の協力を奨励することも謳われている。

今回、パイロットプロジェクトでは、このような PKI フォーラムの経緯と日本の海外との経済連携の進展を考慮し、シンガポール PKI フォーラムと連携し、日本－シンガポール間の貿易取引に利用される特恵原産地証明書を電子化し、それを運用するためのパイロットシステムを構築した。プロジェクトの主たる狙いは、その成果を広く日本国内および関係諸国において共有し、国際間の電子文書のビジネスにおける運用の実現を加速させることである。

本プロジェクトにおいては、PKI の実ビジネスにおける利用を促進するために、海外における電子署名の安全を評価するための認証局の公認制度調査、および米国を中心とする PKI の相互運用に関する海外事例調査を合わせて実施している。

2 プロジェクト概要

2.1　目的

PKI の国際間相互接続実験および PKI の実ビジネスへの展開へ向けたパイロットシステム構築・運用を通して、国際的な実ビジネスへの PKI 適用について検証する。

2.2　期間

平成 16 年 10 月 15 日～平成 17 年 3 月 7 日

2.3　推進体制

本パイロットプロジェクトの推進体制を「図 2.1　プロジェクト推進体制図」に示す。国内の推進体制は「経済産業省→日本 PKI フォーラム→パイロットプロジェクトコンソーシアム」といった構成となるが、商工会議所等関連団体にも協力を頂いてプロジェクトを推進した。また、「図 2.2　コンソーシアム体制図」にはコンソーシアム体制を示す。

海外の推進体制は「IDA→シンガポール PKI フォーラム→CrimsonLogic 社」といった構成となり、日本のパイロットプロジェクトコンソーシアムとシンガポール PKI フォーラムの会員である CrimsonLogic 社でプロジェクトの推進を図った。また、アジア PKI フォーラムおよび IWG へのプロジェクト報告を行った。

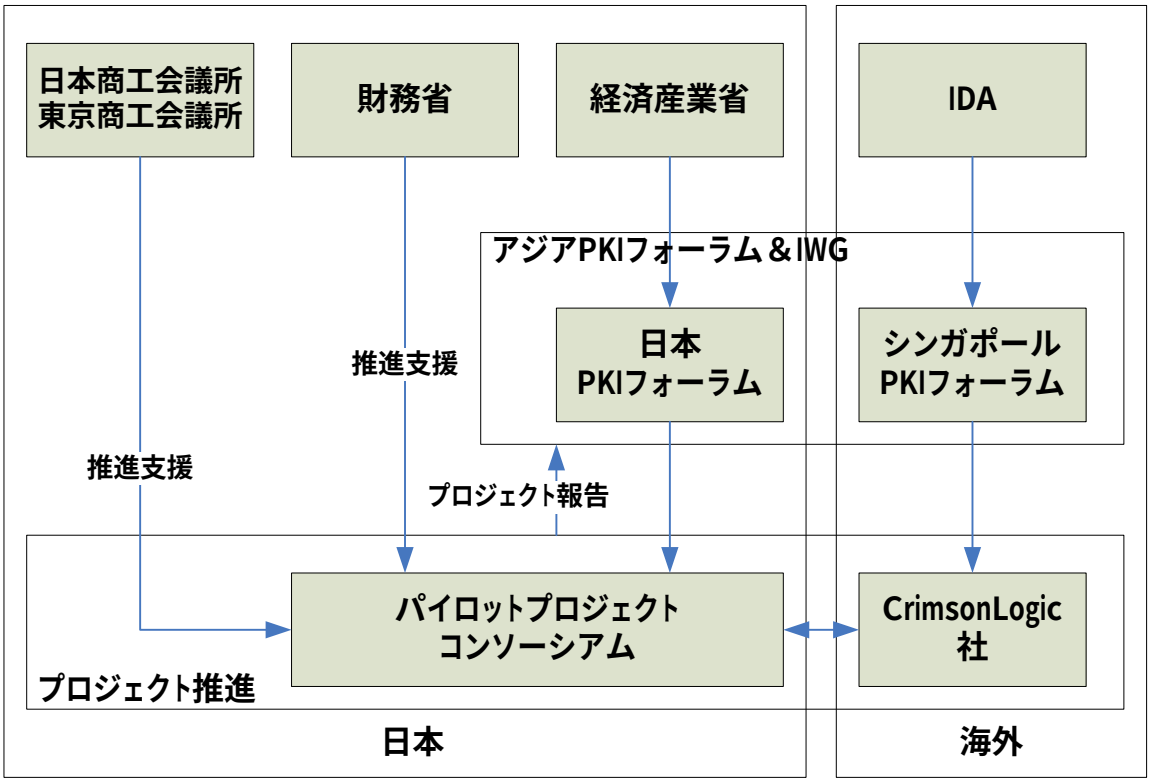

図 2.1　プロジェクト推進体制図

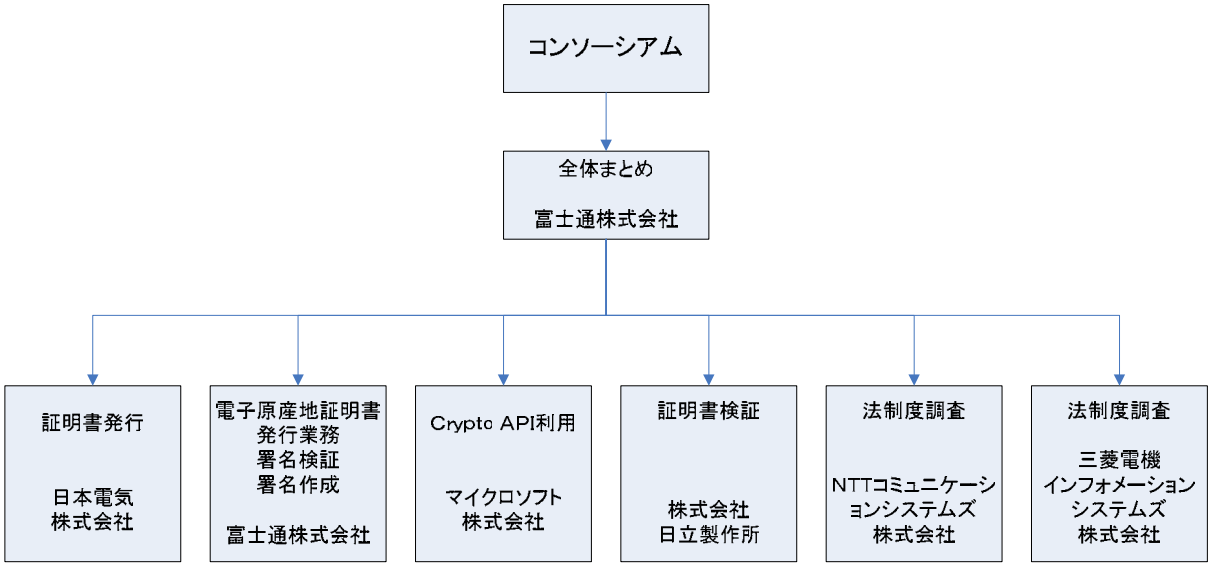

図 2.2　コンソーシアム体制図

※IWG（Interoperability Working Group）とは、本プロジェクト開始時点では日本 PKI フォーラム、韓国 PKI フォーラム、シンガポール PKI フォーラムおよびチャイニーズ台北 PKI フォーラムにそれぞれ参加している団体の担当者を含むメンバーから構成されるワーキンググループを指していた。その後、平成 16 年 11 月のアジア PKI フォーラム・韓国ミーティングにおいて、参加国を特に限定せずに活動していくことが合意された。

また、CrimsonLogic 社の CEO である V.Mathivanan 氏はシンガポール PKI フォーラムの会長を務めている。

2.4　活動概要

パイロットプロジェクトとして特恵原産地証明書の電子化モデルを例に取り、本年度は以下の活動を実施した。

(1) 認証局の公認制度調査

国際間における電子署名の有効性は、一般的には、両国間で取り決めを行う外国の認証局の認定制度に依存している。電子原産地証明書に利用される電子署名についてもその安全性を評価する必要があるため、認証局の公認制度について調査を実施した。

(2) PKI を利用したアプリケーションの実用化に向けての課題と方向性調査

現在のインターネットにおける認証の課題解決の糸口を見いだし、ユビキタスネットワーク社会で要求される個々のネットワークや組織を超えた広範囲なドメインにおける認証が実現可能となるよう、国内企業が抱える認証の問題点の把握と海外における先進事例について調査を実施した。

(3) PKI の国際的相互接続に関する手引作成

昨年度までの成果である Asia PKI Interoperability Guideline の有効性を検証するために本プロジェクトでは Asia PKI Interoperability Guideline に則った方式で行い、その利用に関して手引を作成した。

(4) PKI 実利用のためのガイドライン作成

特恵原産地証明書の電子化モデルを通じ、実ビジネスに PKI 技術を導入する際の検討事項等をまとめ、ガイドラインとして作成した。

(5) 特恵 ECO フォーマット検討

特恵原産地証明書を電子化するにあたり、各国で共通して利用し得るフォーマットを検討する必要があるため実施した。

(6) 特恵 ECO プロトコル検討

特恵 ECO の国際間の送受信に関して、真正性および安全性を確保した伝送方法を検討する必要があるため実施した。

(7) パイロットシステム構築

パイロットシステムによる実験を実施した。

(8) シンガポール PKI フォーラムとの調整

本パイロットプロジェクトの対象国であるシンガポール PKI フォーラムと特

恵 ECO フォーマットや特恵 ECO プロトコルについて協議を行った。また、PKI の国際的相互接続に関する手引作成や PKI 実利用のためのガイドライン作成についてもシンガポール PKI フォーラムの意向を取り入れる必要があるため調整作業を実施した。

3 調査作業

3.1　PKI 実利用のための背景となる認証局の公認制度調査

(1) 目的

国際間における電子署名の有効性は、一般的には、両国間で取り決めを行う外国の認証局の認定制度に依存している。電子原産地証明書に利用される電子署名についてもその安全性を評価する必要があるため、認証局の公認制度について調査を実施した。

このような背景を踏まえ、日本と以下の FTA 交渉国および FTA 締結国との認証局の公認制度の文献調査を行い、ギャップ分析を実施した。

報告は、電子取引法または電子署名法等の公布日または施行日の成立順とした。

詳細を「図 3.1　電子取引法または電子署名法等の公布日または施行日の成立順」に示す。

・マレーシア
・シンガポール
・韓国
・フィリピン
・タイ

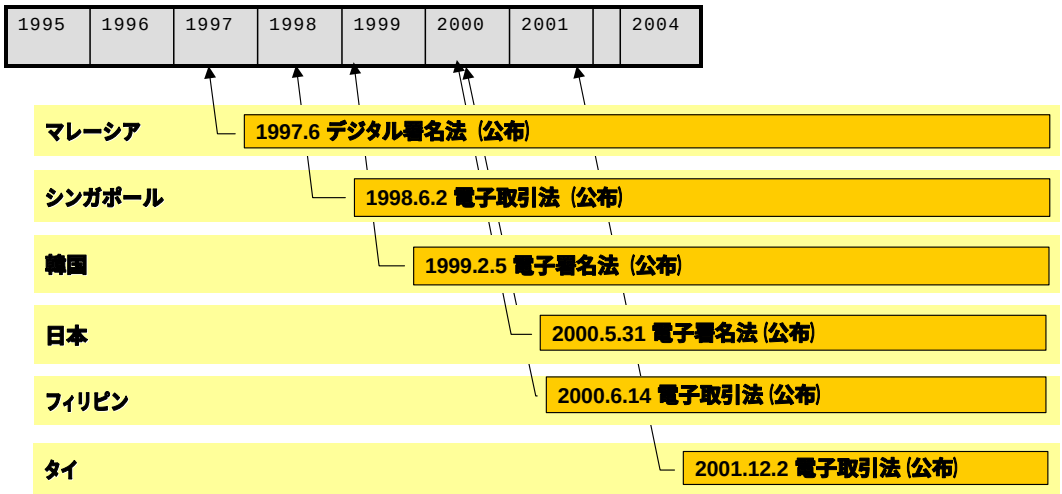

図 3.1　電子取引法または電子署名法等の公布日または施行日の成立順

(2) 調査対象／手順

(a) 調査対象

「表 3.1　調査文献一覧」に示す FTA 交渉国および FTA 締結国の認証局の公認制度に関する文献を調査対象にした。以下、文献は略語で示す。

表 3.1　調査文献一覧

国	文献	公布/施行
マレーシア	デジタル署名法[MY/L]	1997.6 公布
シンガポール	電子取引法[SG/L]	1998.6.2 公布 1999.12.30 改正
	電子取引法規則[SG/R]	1999.2.10 施行
	認証局セキュリティガイドライン[SG/CA]	2003.9 V2.0
韓国	電子署名法[KR/L]	1999.2.5 公布 2001.12.31 改正
	電子署名法施行令[KR/E]	1999.7.1 施行 2002.6.10 改正
	電子署名法施行規則[KR/R]	1999.8.12 施行 2002.7.11 改正
	実在性確認および本人確認に関する告示[KR/CP]	2002.12.17 施行
	CPS ガイドラインに関する告示[KR/CPS]	2003.11.27 施行
	認証局が採用する安全対策に関する告示[KR/PR]	2002.11.15 施行
	公認認証局の施設設備基準に関する告示[KR/F]	2002.11.15 施行
日本	電子署名および認証業務に関する法律[JP/L]	2000.5.31 公布 2001.4.1 施行
	電子署名および認証業務に関する法律施行令[JP/E]	2001.4.1 施行
	電子署名および認証業務に関する法律施行規則[JP/R]	2001.4.1 施行 2003.8.28 改正
	電子署名および認証業務に関する法律に基づく特定認証業務の認定に関する指針[JP/G]	2001.4.1 施行 2003.6.2 改正

	電子署名および認証業務に関する法律に基づく指定調査機関等に関する省令[JP/ASS]	2001.3.1 施行
	JIPDEC 特定認証業務の認定に関する調査票[JP/A]	2004.4.9 V2.2
フィリピン	電子取引法[PH/L]	2000.6.14 公布
	電子認証および電子署名に関する施行規則[PH/R]	2001.9.28 公布 2001.10.27 施行
タイ	電子取引法[TL/L]	2001.12.2 公布 2002.4.1 施行

(b) 調査手順

一般に、認証局の公認制度に関する法規は、次の事項を規定している。

・電子署名の効果
・公認基準
・認証サービス
・認証局運営の安全対策
・認証局設備および装置の安全対策

なお、法規の比較では、規定の違いを浮き彫りにすべく、「表 3.2　マッピングの構成」に示すキーワードで条項をマッピングし、その特徴を抽出して要旨とした。

表 3.2　マッピングの構成

構成	分類キーワード
電子署名の効果	電子文書の真正な成立に関する推定項等
公認基準	公認に関する推進体制、有効期間、申請および変更等手続き、公認基準、公認の取消、罰則等
認証サービス	加入者登録、証明書の発行と受領に関する義務等
認証局運営の安全対策	内部牽制を含むアクセス管理、記録保管等の安全対策
認証局設備および装置の安全対策	施設、設備、システム等の物理的および技術的管理策

(3) 調査結果

調査の結果、FTA 交渉国および FTA 締結国との制度間のギャップが以下に記述するように明確になった。なお、フィリピンおよびタイは現時点で公認制度が制度化されておらずここでは省略した。

(a) 全般

(i) 公認認証局の資本要件

シンガポール（SG/R-7.1）、韓国（KR/E-2.1.2）の公認制度では、公認認証局の資本要件を規定している。

FTA 相手国または地域の公認制度が資本要件を規定していない場合、あるいは規定していても金額が異なる場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(ii) 加入者証明書の停止処理

マレーシア（MY/L-46.1）、シンガポール（SG/L-31.1、SG/R21.4）、韓国（KR/L-17.1、KR/L-17.2）の公認制度では、加入者証明書の停止を規定している。

FTA 相手国または地域の公認制度が加入者証明書の停止処理を規定していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(iii) 事業の継承、廃止または取消に伴う業務の継承

マレーシア（MY/L-12.6）、シンガポール（SG/L-41.4）、韓国（KR/L-10.3、KR/L-10.4、KR/L-12.2、KR/L-12.3、KR/R8.1）の公認制度では、公認認証局事業の継承、廃止または取消に伴う業務の継承を規定している。

FTA 相手国または地域の公認制度が継承を規定していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(b) マレーシア

(i) タイムスタンプ

マレーシアは、TSA（Time-Stamping Authority タイムスタンプ局）の公認制度を有し、タイムスタンプの法的地位または法的効力を規定している（MY/L-70.1）。

マレーシアの在外認証局の公認規定（MY/L-19.2c）では上記規定を適用外としているが、紛争解決時の推定の要件としてデジタル署名が公認 TSA のタイムスタンプがなされる前に生成されていることを要求している（MY/L-67.1d）。

TSA の公認制度を持たない FTA 相手国または地域で発行されたタイムス

タンプが使われた場合、ギャップが生じ、そのタイムスタンプにマレーシアと同一の法的地位または法的効力が与えられるかについて、主管者間の調整が必要となる。

(c) シンガポール

(i) リポジトリ

シンガポールの公認制度では、リポジトリのダウン時間およびダウン率を規定している（SG/R-30）。

FTA 相手国または地域の公認制度がリポジトリのダウン時間およびダウン率を規定していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(ii) ネットワーク診断

シンガポールの公認制度では、半年毎に資格がある独立機関のネットワーク診断を受けることを規定している（SG/CA-2.5.5、SG/CA-5.4.4）。

ネットワーク診断機関の資格を制度化していない FTA 相手国または地域のネットワーク診断機関からネットワーク診断を受けた場合、ギャップが生じ、その診断の有効性について主管者間の調整が必要となる。

(iii) 準拠性監査

シンガポールの公認制度では、監督者に年 2 回の業務および財務に関する報告を提出することになっており、その中にはシステムの稼動時間/停止時間、障害を含むシステムの稼働率が含まれている（SG/R-34.1、SG/R-34.2）。

FTA 相手国または地域の公認制度が準拠性監査の報告回数を年 1 回と規定している場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

また、公認認証局が連続運転を必要としない場合、ギャップが生じ、システムの稼動時間/停止時間、障害を含むシステムの稼働率の報告について認証局の対応が必要となる。

(iv) システムの情報技術セキュリティ評価基準

シンガポールの公認制度では、システムおよびアプリケーションが EAL4 相当以上であることを規定している（SG/CA-5.2.3）。

FTA 相手国または地域の公認制度がシステムおよびアプリケーションの EAL を規定していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

また、EAL に対応していないシステムおよびアプリケーションしか入手できない場合、どう対応すべきか、主管者間の調整が必要となる。

(v) 署名鍵と暗号化鍵の分離

シンガポールの公認制度では、署名鍵と暗号化鍵を分離することを推奨している（SG/CA-4.1.3）。

FTA 相手国または地域の公認制度が署名鍵と暗号化鍵の分離を規定していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(d) 韓国

(i) 相互接続

韓国の公認制度では、全ての認証局が KISA（Korea Information Security Agency 韓国情報保護振興院）のルート認証局に相互接続されることが前提となっている（KR/CPS-29.3）。

FTA 相手国または地域の公認制度が公認認証局以外との相互接続を認めていない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(ii) タイムスタンプ有効性検証システム

韓国の公認制度では、タイムスタンプ有効性検証システムに対する仕様要件を規定している（KR/F-2.4.2.2 イ）。

FTA 相手国または地域の公認制度がタイムスタンプ有効性検証システムに対する仕様要件を規定していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(iii) システムの二重化

韓国の公認制度では、次のシステムの二重化を規定している。

・認証システム（KR/PR-t3.2.1.4、KR/F-2.3.1.5、KR/F-2.3.2.1 エ、KR/PR-t3.2.2.4）
・リポジトリ（KR/F-2.3.2.2 ウ）
・HSM（KR/F-2.2.2 カ）

FTA 相手国または地域の公認制度が当該システムの二重化を規定していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(iv) 要員の条件

韓国の公認制度では、公認認証局は 12 名以上の要員の確保および要員の韓国資格の保有かつ KISA の教育課程の履修を規定している（KR/E-2.1.1）。

FTA 相手国または地域の公認認証局の要員が 12 名未満である、あるいは当該資格および課程を履修した要員がいない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(v) 加入者ソフトウェア

韓国の公認制度では、加入者ソフトウェアの要件として監査記録の生成または更新機能を規定している（KR/F-2.2.3.1 ウ、KR/F-2.6.5 イ）。

FTA 相手国または地域の公認制度が加入者ソフトウェアの要件として監査記録の生成または更新機能を規定していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(e) 日本

(i) 公認認証局秘密鍵の利用制限

日本の公認制度では、認定認証業務以外のサービスで公認認証局秘密鍵を利用しないことを規定している（JP/G-10.1.1）。

FTA 相手国または地域の公認認証局が認定認証業務以外のサービスで公認認証局秘密鍵を利用している場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(ii) 団体用加入者証明書の扱い

日本の公認制度では、団体用加入者証明書の扱いが規定されていない。

FTA 相手国または地域の公認認証局が団体用加入者証明書を取り扱っている場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

(iii) 施設の建築基準

日本の公認制度では、施設の災害対策として建築基準法への準拠を規定している（JP/G-7.1.3.3）。

FTA 相手国または地域の公認制度が日本の建築基準法に準拠していない場合、ギャップが生じ、主管者間の調整または認証局の対応が必要となる。

3.2　PKI を利用したアプリケーションの実用化に向けての課題と方向性調査

PKI は、非対称鍵暗号を利用して、認証局が公開鍵証明書を発行することが基本となっている。公開鍵証明書は、印鑑証明書と比較してよく説明されるが、必ずしも電子署名法が想定しているネットワーク上の印鑑証明書だけの機能にとどまらず、ID やパスワードに代わるより安全な電子認証（電子情報を利用した本人確認）の用途にも利用できる。

電子認証は今後、より安全で安心なネットワーク社会を実現する上で必要となる技術であり、PKI の利用も含む電子認証の実用化に向けての課題と方向性について調査を実施した。

3.2.1 電子認証の課題

人、サービス、デバイスがシームレスに接続されていくユビキタスネットワーク社会において、安全・安心を提供するサービスを実現するためには、信頼関係を確立するための認証（Authentication）が重要になる。人の認証だけでなく、サービスやデバイス等の認証も重要な役割を果たし、また、時刻（いつ）や位置（どこ）等といった認証が必要な場面もある。認証は、安全、安心なユビキタスネットワーク社会を実現するための、最も重要な要素のひとつになると考えられるが、これらの認証に対して、これまでにない多様な要求が浮上している。人の認証ということだけをとっても、プライバシー保護のための仮名による認証、人の色々な属性に関する認証が挙げられる。これらの認証が、シームレスに接続されたユビキタスネットワークにおいて、より大規模に、更に色々な組織を超えて行われることが要求されている。

様々な認証技術が登場しているものの、ユビキタスネットワーク社会で要求される個々のネットワークや組織を超えた広範囲なドメインにおける認証を実現するには、まだ大きな壁がある。それは、閉じられたローカルな認証では大きく取り上げられることのなかった、下記のような問題があるためである。

- 相互運用性の問題
  これまでの多くの認証技術は、限られた環境で動作すればよかったが、広いドメインの認証ではそれらの相互運用性が重要な問題となる。
- 認証に対するセキュリティレベルの向上
  これまでのインターネットにおける認証は当たり前に利用されているにもかかわらず、認証に対して何の評価基準もなく、実際に利用されている認証も低いセキュリティレベルのものが主流であると思われる。
- プライバシーの問題
  ドメインを超えた認証を行う場合には、利用者のプライバシーを十分に考慮する必要がある。

こうした壁を取り除き、安全･安心なサービスの連携や協調を実現するためには、電子認証基盤の整備が重要である。「図 3.2　電子認証基盤」では電子認証基盤と、その基盤上で実現されるサービスとの関係を示す。電子認証基盤が広範なサービスの連携や協調のための信頼の礎となるためには、技術、ポリシ・運用、ビジネスルールを含めたフレームワークを提供することが必要である。例えば、下記に掲げた項目を提供することが必要であろう。また、このような電子認証基盤の整備は先行する海外の事例が参考となる。海外の事例や動向と日本の現状を踏まえ、日本で実現すべき電子認証基盤とはどうあるべきかを考えることが重要である。

[技術]

・ 認証に関わる要素技術や実装についての調査・検討
　セキュアな認証を実現するための技術（例えば PKI やバイオメトリクス等）や実装を調査・検討し、適用する技術や実装を選定するための指針を与える。例えば、NIST の電子認証ガイドラインが参考となる。

・ 連携フレームワーク
　連携フレームワークとは認証システムを相互に連携するための技術仕様である。電子認証基盤を利用するシステムの構築を容易にするための開発環境（ライブラリ等）や、相互運用性を確保するためのテストスイートの提供や、実装の評価も重要である。例えば、Shibboleth や Liberty の活動や技術仕様が参考となる。

[ポリシ＆運用]

・ 認証の評価基準
　認証に対する保証レベルの規定と、その保証レベルを決定するプロセス（認証に関わるリスクアセスメント等）や、保証レベルを実現するための要件（本人確認手段や認証技術等）を与える。

・ 認証に関わる事業者に対する評価方法と認定制度
　利用者の認証に関わる事業者（例えば公開鍵証明書を発行する認証局や、認証を必要とするサービスを実施する事業者等）に対する評価方法を定め、認定制度を設ける。
　事業者の認定は、上記の認証の保証レベルや利用者の個人情報の取り扱いに関するプライバシーポリシ等に基づいて評価をした結果に基づくものと考えられる。

　このような認証の評価基準を始めとする課題は、従来の企業内等閉じられたド

メインでの認証とは異なり、組織を超えた広範な連携を行なうためには特に重要である。

[ビジネス]

・ ビジネスルール

参加する事業者に対する責任や規約等を含むビジネスルールを策定する。ビジネスルールは一意ではなく、リスクやコスト等の関係から様々なレベルの契約が存在することも考えられる。このような契約レベルは認証の保証レベル等を含めた様々な評価基準によって考えられるものである。

・ ビジネスモデル

アプリケーションや基本的なビジネスモデルを提示することにより、広範で多数の参加者による連携を促進する。

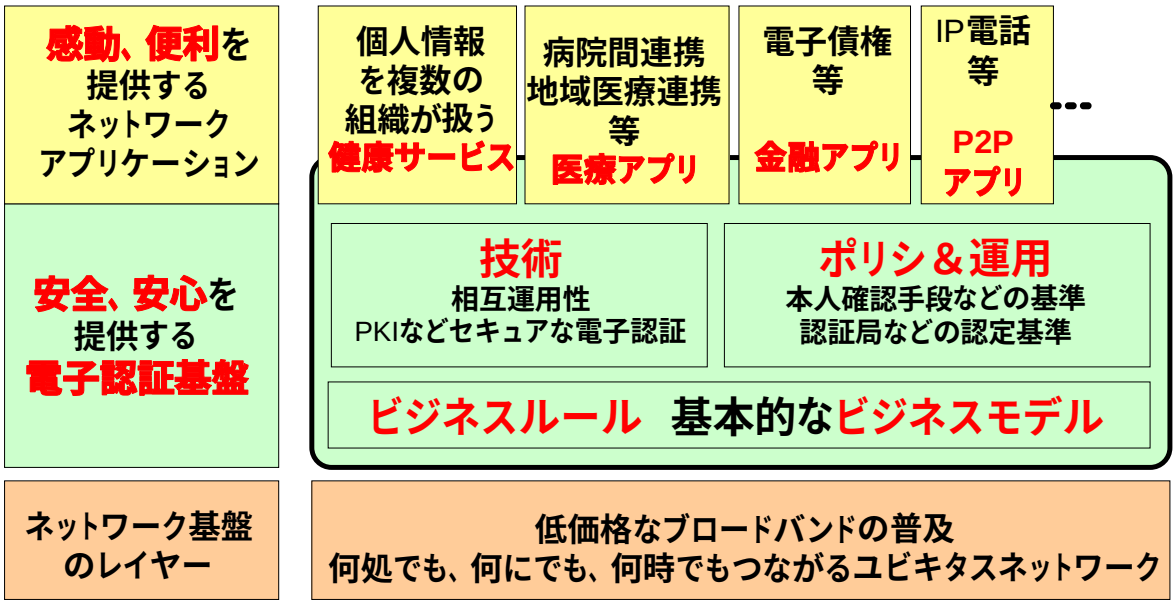

図 3.2　電子認証基盤

3.2.2 ID 連携（Identity federation）

これまでのインターネット上のサービスでは、利用者の認証が必要な場合に、それぞれのサービスで認証システムを構築し、自身で利用者の認証を行うものが一般的であった「図 3.3　従来型の認証モデル」。こうした認証システムはサービス毎に閉じられたものであり、サービス間で相互に認証システムを利用するための共通の仕組みを持たないため、利用者は利用するサービス毎に、それぞれの認証プロセスが必要であった。

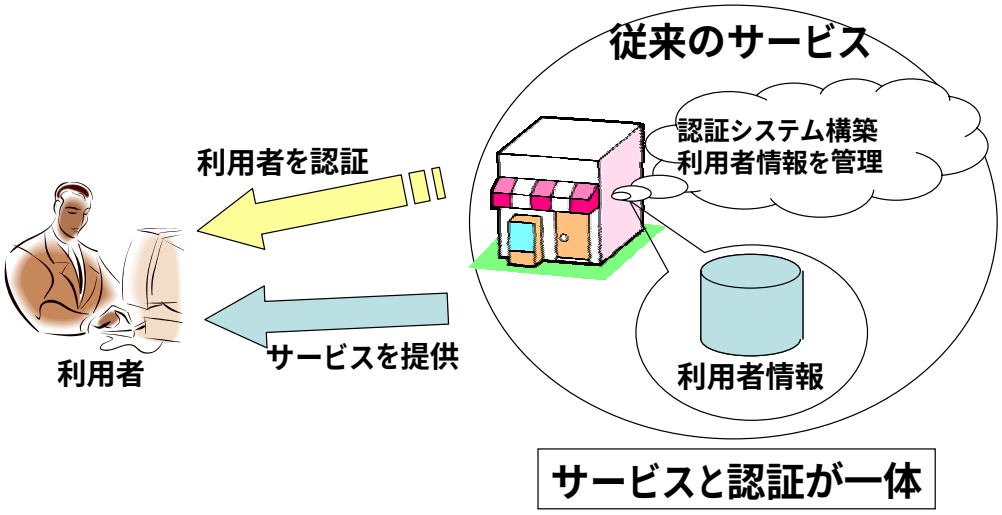

図 3.3　従来型の認証モデル

しかし、近年、OASIS により標準化された SAML（Security Assertion Markup Language）が登場し、さらに SAML の拡張として、Liberty Alliance の ID-FF 仕様や、Internet2/MACE プロジェクトの Shibboleth といったフレームワークが登場したことで、異なる認証システム間で利用者の認証情報を交換しシングルサインオン（SSO）を実現する ID 連携が実現可能になりつつある。

この ID 連携の仕組みにより､利用者の認証を行う役割を担う認証プロバイダと、その認証プロバイダから認証に関する情報を受けることでサービスを実施するサービスプロバイダのように、サービスと認証が分離した事業者モデルを考えることができるようになった。

例えば、「図 3.4　ID連携による事業者モデル」に示したモデルでは、認証プロバイダは利用者を認証し、認証情報（例えば、いつ、どのような方法で認証したか等）をサービスプロバイダに提供する。サービスプロバイダはその認証情報を得ることで利用者が認証済みであると判断し、サービスを実施する。サービスプロバイダはサービスの実施にあたり、認証情報だけでなく利用者に関する属性情報（例えば、年齢や性別等）を必要とするかもしれない。その場合には、サービスプロバイダ自身が管理する利用者の属性情報を用いるか、あるいは、他の事業者から利用者の属性情報の提供を受けることが考えられる。他の事業者との属性情報の連携のためには、さらに別の仕組み[1]が必要となるが、その仕組みはID連携を基礎として実施されるものである。

[1] 例えばLibertyのID-WSF,ID-SIS仕様で各事業者が持つ属性情報を連携するための仕組みを提供している。

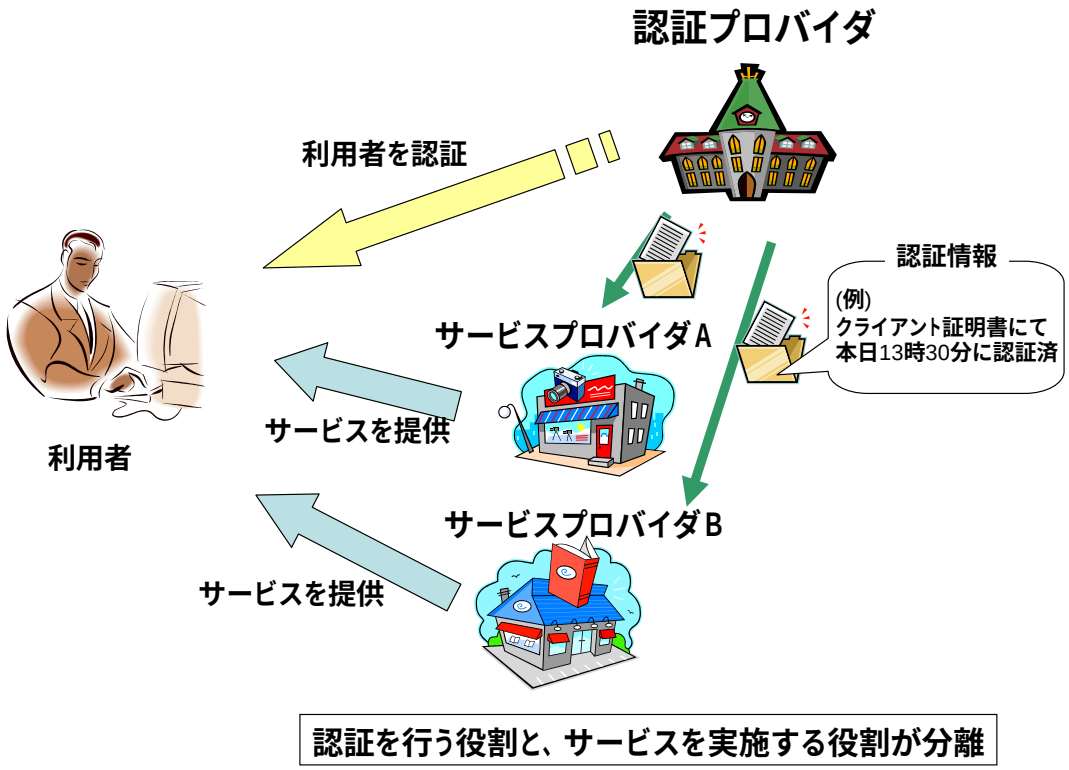

図 3.4　ID 連携による事業者モデル

SAML、Liberty、Shibboleth により実現可能となった ID 連携の仕組みは、単に利便性においてシングルサインオンを提供するという考えではなく、利用者に関する情報のセキュリティやプライバシー保護の観点にあることが重要である。利用者の情報が分散管理されることで情報漏えい時のリスクを抑えること、また、プライバシー保護の仕組みとして、利用者の同意のもとで ID 連携が行われることや、事業者間における利用者の追跡を防ぐためにグローバルな ID を用いずに、それぞれの事業者だけに有効な ID（仮名による認証）を用いること等が考えられる。

認証システムの連携に関する標準化とその実用化の機運は世界的に高まっている。そして、このような ID 連携のモデルは、電子政府等にも取り入れられるような動向がある。米国電子政府においては、認証の連携を推進する e-Authentication イニシアチブが活発な活動を行っており、米国連邦政府ポータルにおいて e-Authentication イニシアチブが推進する認証の連携基盤が取り込まれようしている。また、米国では民間および官民における認証の連携を図る EAP（Electronic Authentication Partnership）が設立され、その基盤構築において認証の評価基準をはじめとする e-Authentication の成果を利用している。

3.2.3 認証の評価基準

認証に対するセキュリティレベルや保証レベルを向上し、さらに、サービスの連携を推進するためには認証の評価基準を明確にすることが重要である。

認証を必要とするネットワーク上のサービスを実施するためには、認証の脅威に対するリスクを分析し、適切な認証方法を適用することが求められる。

例えば、医療における患者情報等は機密度の高い情報であり、それを扱うサービスには高度の認証が求められなければならない。高度な認証を行うためには高いコストも要求される「図 3.5　リスクと認証方法のバランス(1)」。日本の電子署名法特定認証業務認定制度のように、認証局の認定における本人の身元確認や認証局の運用といった観点からの高度な要求を考えた場合、証明書発行コストは当然高いものとなる。一方、機密性の低いファイルをメンバー内で共有するといったサービスを考えた場合、そのサービスのためだけに高いコストをかけ、先の場合と同様の高度な認証を採用する必要性は考えにくい「図 3.6　リスクと認証方法のバランス(2)」。高度な本人確認性を必要以上に求めたためにコスト高になるだけでなく、普及を阻害することにもなる。

しかし、現状での様々なサービスにおいてはこのような認証にかかわるリスクを評価して適切な認証が行われているとは言いがたい。それは、認証の保証に関して明確な基準や指標が欠如していることがひとつの要因である。

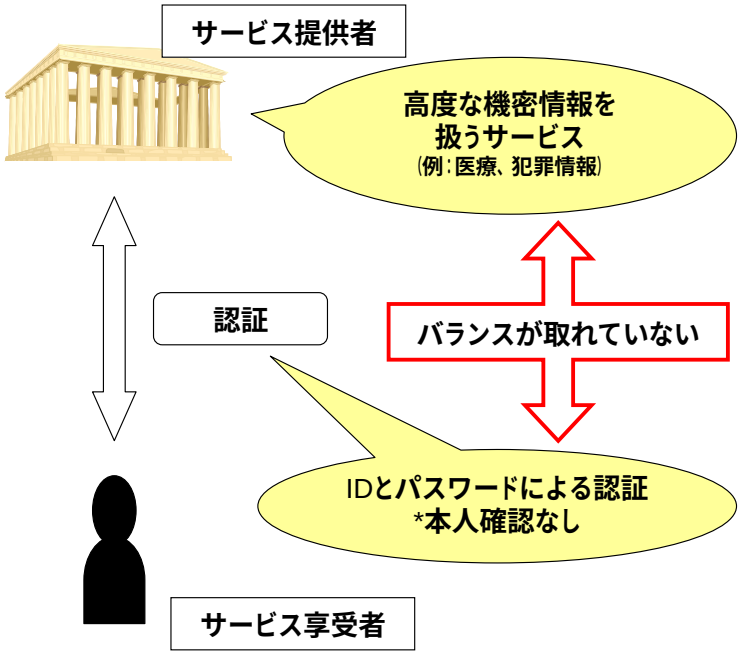

図 3.5　リスクと認証方法のバランス(1)

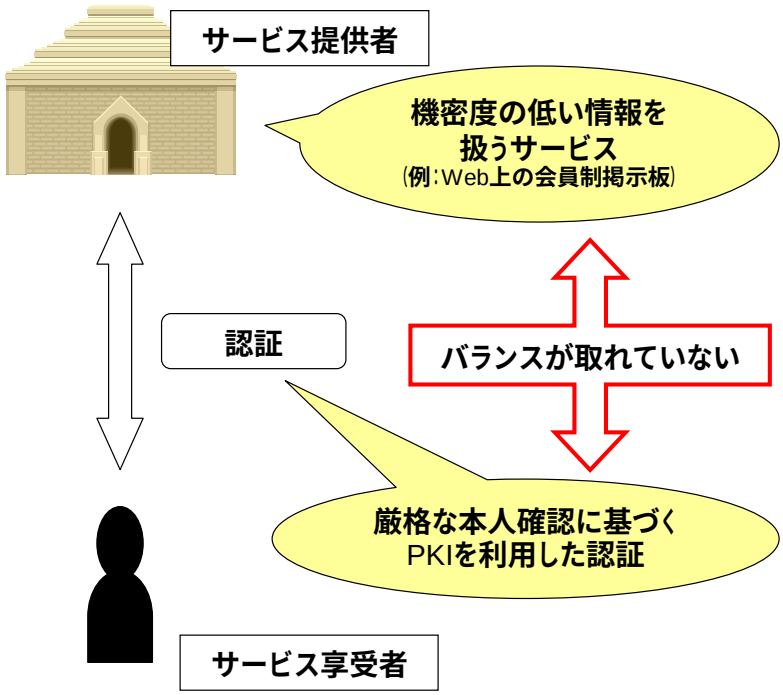

図 3.6　リスクと認証方法のバランス(2)

また、認証の評価基準の不備は、複数のサービスによる ID 連携を阻害する要因にもなりえる。これまでの認証が要求される多くのサービスは、サービス自身が認証を提供、つまりサービスと認証が一体化しており、そのため、サービスの数だけ認証システムが必要となっていた。こうした中、ID 連携によるシングルサインオンのモデルが注目されており、標準化等も急速に進展しており、電子政府等の認証基盤として取り入れようとする動きもある。

サービスと認証が一体化した従来型のモデルでは、認証の脅威に対するリスクは、一体化したサービスの主体者（サービスプロバイダ）自体が負えばよかった。一方、サービスプロバイダと、認証の主体者、すなわち認証プロバイダが個別に存在するモデルでは、サービスプロバイダと、認証プロバイダ間で何らかの契約が必要である。その契約においては、認証に対するリスクを分析し、サービスに対して認証の保証レベルを適切に決定する必要があるだろう。

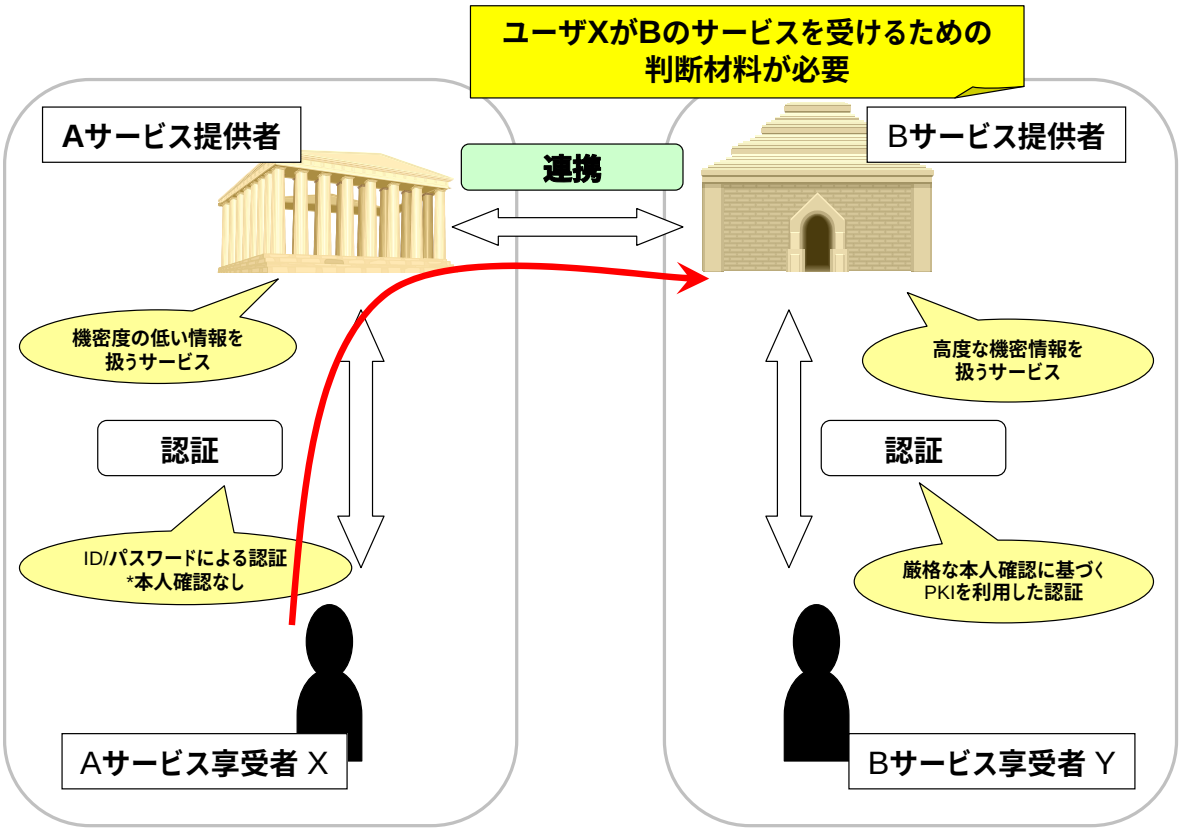

図 3.7　ID 連携と保証レベル

例えば、「図 3.7　ID 連携と保証レベル」に示すように、A サービス提供者と B サービス提供者が ID 連携を行う場合を考える。A サービス提供者は自身の管理するサービス享受者 X を認証し、B サービス提供者に対してサービス享受者 X の認証結果を含んだ情報（アサーション）を発行する。B サービス提供者は A サービス提供者から得たアサーションによってサービス享受者 X へのサービス提供の認可を行う。A サービス提供者は B サービス提供者に対し認証プロバイダとなる。このとき、A サービス提供者が認証するユーザの身元の保証と、B サービス提供者が認証するユーザの身元の保証は異なっているため、これらの認証におけるリスクを分析し、そのサービスで求められる認証の保証レベルを事前に決定する必要がある。

しかし、2 者間で多くの時間を費やし、認証に対するリスクを分析して設定したとしても、2 者間だけの連携で終わってしまう。また、もう少し範囲を広げ、業界内での規約や基準を作成したとしても、その業界内での連携に終わってしまう。

認証の評価基準が明確になっていれば、その評価基準を使うことにより、組織や業種を超えた認証の連携が推進されると考えられる。更に、認証プロバイダや、サービスプロバイダに対しての認定制度のようなものが確立すれば、異なった利害関係を持つ組織が、色々な場を共有するポータルが普及すると考えられる。

このような認証の評価基準について海外の動向を眺めると、米国の e-Authentication イニシアチブや EAP、連邦 PKI、また、オーストラリアの政府

電子認証フレームワークでは、複数の保証レベルという考えがある。これらは、アプリケーションのリスクに応じた保証レベルの認証や電子署名を使い分けている。ユーザはアプリケーションの要求に応じて、クレデンシャル発行に高いコストが掛かる高い保証レベルから、比較的低いコストとなる低い保証レベルまで、適切な保証レベルの認証を利用することができる。

米国 e-Authentication イニチアチブでは保証レベルを 4 つにわけ、OMB 電子認証ガイダンスと NIST 電子認証ガイドラインにおいて、リスクを分析し保証レベルおよびその保証レベルを実現するための技術的要素を決定するプロセスを示している。

4 PKI の国際的相互接続に関する手引の作成

アジア PKI フォーラムにて策定された「Asia PKI Interoperability Guideline」を利用するための参考情報となる以下の手引を作成した。

・Asia PKI Interoperability Guideline の利用に関する手引

作成した「Asia PKI Interoperability Guideline の利用に関する手引」を、特恵原産地証明書を電子化するパイロットシステムの PKI 環境を構築するにあたって使用し、有効性の検証を行った。

本章では、この一連の作業について記述する。

なお、手引詳細に関しては「付録 1 Asia PKI Interoperability Guideline の利用に関する手引」として収録。

4.1 Asia PKI Interoperability Guideline の利用に関する手引

各国の認証局設計者が国際的な実ビジネスに必要な PKI 環境の整備のために利用するものとして、「Asia PKI Interoperability Guideline の利用に関する手引」を作成した。

本手引は、特恵原産地証明書を電子化するパイロットシステムへの「Asia PKI Interoperability Guideline」の適用事例を解説したものである。「Asia PKI Interoperability Guideline」は、パート II でアジア諸国・地域において相互運用可能な PKI の枠組みを構築するための推奨技術仕様（PKI の信頼モデル、コンポーネント・インターフェース、証明書/CRL プロファイル、リポジトリ、証明書検証）の詳細を規定している。これらは過去の実証実験において国際間の認証ドメイン間の信頼関係構築に適用することが有効であることが実証されている。今回のパイロットシステムの PKI 環境の構築にあたってはこの「Asia PKI Interoperability Guideline」に準拠することで、シンガポールとの信頼関係構築を実績ある仕様に基づくものとしている。この作業を「Asia PKI Interoperability Guideline」利用のケーススタディとして解説した。

構成としては、以下の作業フェーズ毎に「Asia PKI Interoperability Guideline」の参照箇所とその際に留意すべき点を、補足情報を交えて記述する形をとっている。

(1) 認証局建局

(a) 準備作業

・構成検討／プロダクト選定

・環境設定

(b) 自己署名証明書の発行

・プロファイル設計

・データ記載／発行

・リポジトリ格納

(c) 失効リストの発行

・プロファイル／配布ポリシ設計

・データ記載／発行

・リポジトリ格納

(2) エンドエンティティへの証明書発行

(a) 準備作業

・申請・配布方法の設計

・プロファイル設計

・ECO 署名用証明書

・S/MIME 用証明書（暗号化用、および署名用）

・VA 証明書

(b) エンドエンティティ証明書の発行

・データ記載／発行

・リポジトリ格納（optional）

・エンドエンティティへの送付

(3) ドメイン間の信頼関係構築

(a) 信頼モデル選択

(b) 相互承認

・関係構築手順

4.2 PKI 環境概要

本パイロットプロジェクトにて構築した PKI 環境を「図 4.1 PKI 環境概略」、「図 4.2 PKI 環境（日本輸出→シンガポール輸入）」、「図 4.3 PKI 環境（シンガポール輸出→日本輸入）」に示す。

なお、本パイロットプロジェクトでは特恵 ECO の発行権限者および特恵 ECO の送信先である ASP の電子証明書を事前に外交ルート等により交換を行うという想定で行った。

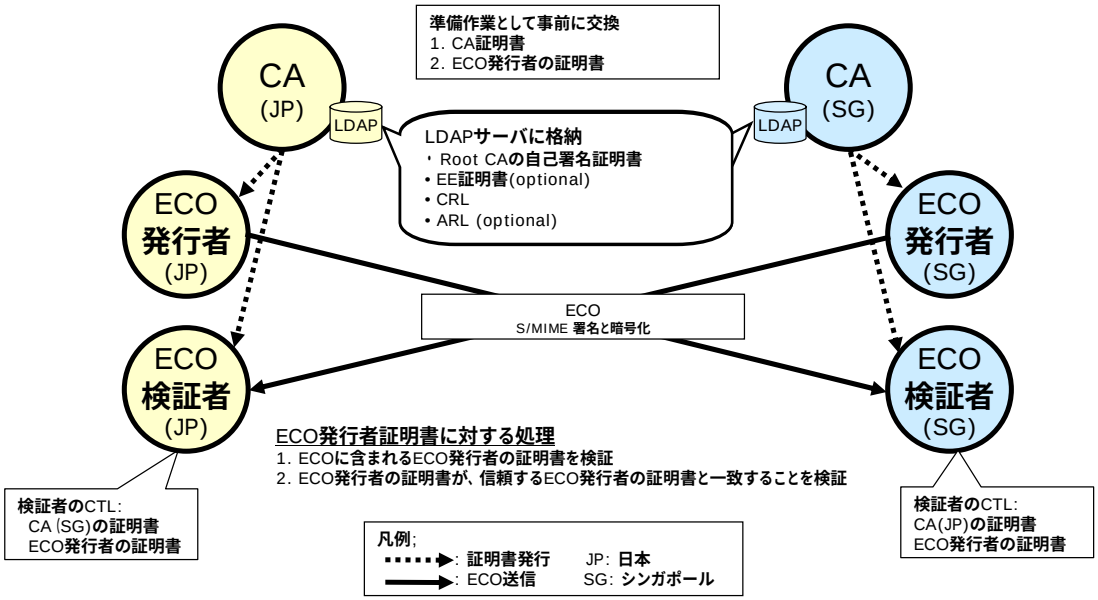

図 4.1　PKI 環境概略

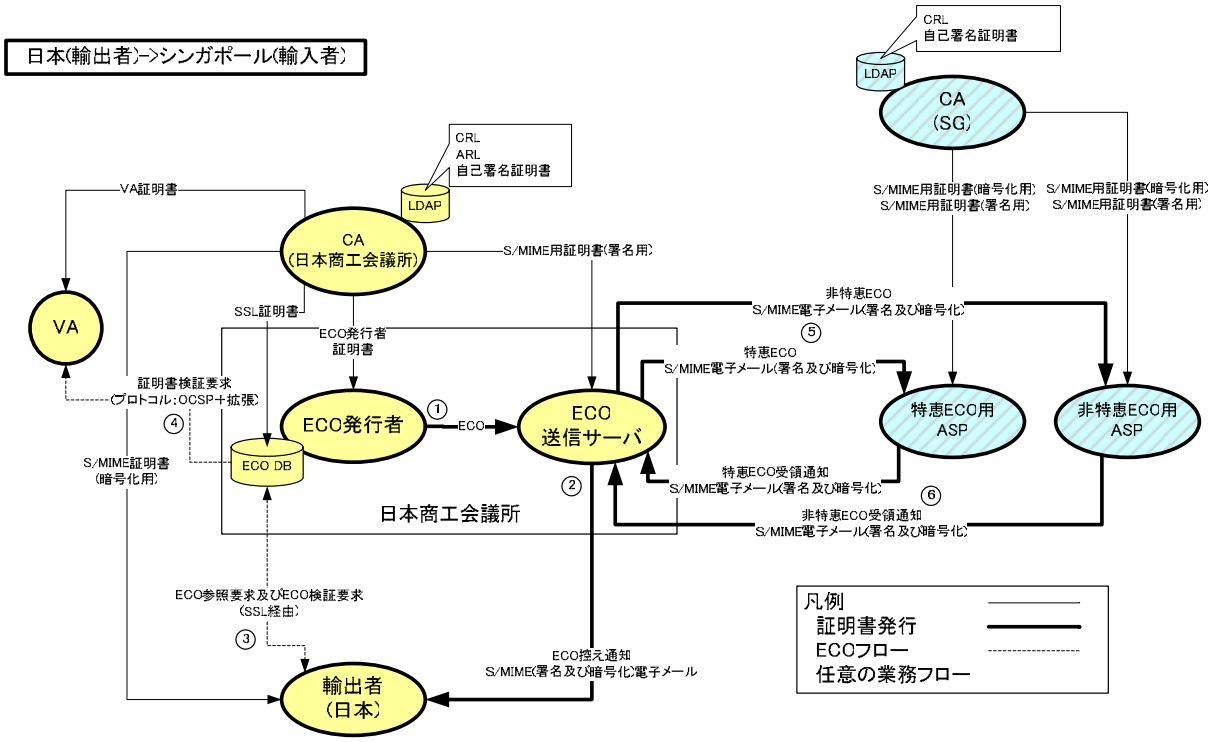

図 4.2　PKI 環境（日本輸出→シンガポール輸入）

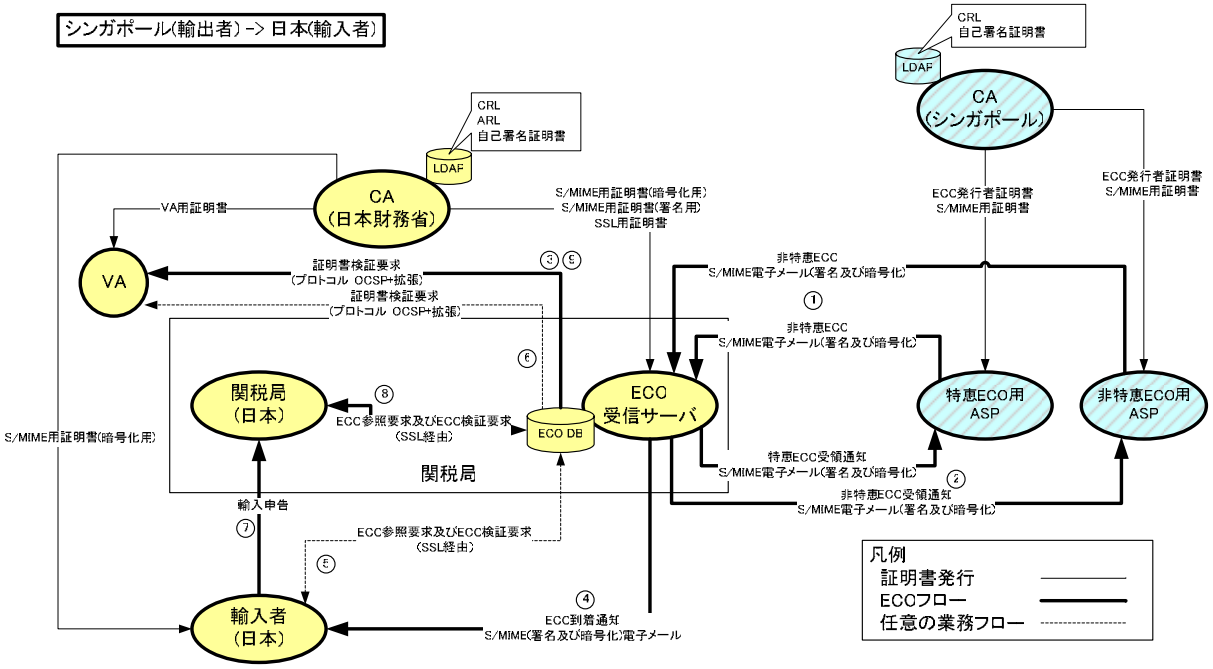

図 4.3　PKI 環境（シンガポール輸出→日本輸入）

4.3　PKI の国際的相互接続に関する手引の実証実験

4.3.1 シンガポールとの相互接続における検証

(1) 目的

本実験では、「Asia PKI Interoperability Guideline」の実ビジネスでの利用を助ける情報を提供するために作成した「Asia PKI Interoperability Guideline の利用に関する手引」の有効性を検証する。

シンガポールとのパイロットシステムの PKI 環境構築の作業を実施する。その作業にあたって「Asia PKI Interoperability Guideline の利用に関する手引」を利用し、「Asia PKI Interoperability Guideline」に正しく準拠した結果が得られることを確認する。さらにその環境を構築するために「Asia PKI Interoperability Guideline の利用に関する手引」が有効な情報を提供することを確認することで「Asia PKI Interoperability Guideline の利用に関する手引」の有効性を実証するものである。

(2) 方法

「Asia PKI Interoperability Guideline の利用に関する手引」を参照して、実験環境内にシンガポールの認証局と相互接続する日本国の認証局を設置し、パイロットシステムとして必要な PKI 環境を構築する。その環境で発行された証明書および証明書失効リストを実験結果データとして採取する。日本国の認証局としては、模擬日本商工会議所認証局および模擬財務省認証局を構築する。

表 4.1　日本国認証局が発行する証明書一覧

No	発行元認証局	証明書の種類
1	模擬日本商工会議所認証局	自己署名証明書
2		証明書失効リスト（CRL）
3		証明書失効リスト（ARL)
4		特恵 ECO 発行者証明書
5		ASP サーバ用 S/MIME 証明書（署名用）
6		ASP サーバ用 S/MIME 証明書(暗号化用)
7	模擬財務省認証局	自己署名証明書
8		証明書失効リスト（CRL）
9		証明書失効リスト（ARL）
10		特恵 ECO 検証者証明書
11		ASP サーバ用 S/MIME 証明書（署名用）
12		ASP サーバ用 S/MIME 証明書(暗号化用)

「表 4.1　日本国認証局が発行する証明書一覧」に示す証明書がすべて「Asia

PKI Interoperability Guideline」に正しく準拠していることを確認し、本実証実験の作業でアジア地域での PKI の相互接続性を保証する仕様に沿った PKI 環境が構築されることを示す。

さらに、構築した PKI 環境で証明書の検証を行い期待した検証結果が得られることを確認することで、PKI 環境の構築が正しく行われていることを示す。

「表 4.2　PKI 相互接続実験項目概略」に実験項目の概略を示す。

表 4.2　PKI相互接続実験項目概略

Step		ID	項目	対象
1	構成検討	1-1	認証局の PKI コンポーネント構成を決定する	模擬日本商工会議所認証局 模擬財務省認証局
		1-2	コンポーネント間インターフェースを設計する	
		1-3	プロダクトを選定する	
2	HW/SW 設定	2-1	認証局の機器を設定する	
		2-2	ネットワーク設定	
		2-3	認証局の PKI コンポーネントソフトウェアをインストール、設定する	
3	自己署名証明書発行	3-1	プロファイル設計	模擬日本商工会議所認証局 模擬財務省認証局
		3-2	データを入力し、署名して発行する	
		3-3	発行した自己署名証明書の内容をチェックする	
		3-4	発行した自己署名証明書を LDAP サーバに格納する	
		3-5	LDAP サーバ上の自己署名証明書の格納エントリの DN をチェックする	
		3-6	LDAP サーバ上の自己署名証明書の格納エントリのオブジェクトクラスをチェックする	
		3-7	LDAP サーバ上の自己署名証明書の属性をチェックする	

4	CRL/ARL 発行	4-1	CRL プロファイル設計	
		4-2	ARL プロファイル設計	
		4-3	データを入力し、署名して CRL を発行する	
		4-4	データを入力し、署名して CRL を発行する	
		4-5	発行した CRL の内容をチェックする	
		4-6	発行した ARL の内容をチェックする	
		4-7	発行した CRL を LDAP サーバに格納する	
		4-8	発行した ARL を LDAP サーバに格納する	
		4-9	LDAP サーバ上の CRL の格納エントリの DN をチェックする	
		4-10	LDAP サーバ上の CRL の格納エントリのオブジェクトクラスをチェックする	
		4-11	LDAP サーバ上の CRL の属性をチェックする	
		4-12	LDAP サーバ上の ARL の格納エントリの DN をチェックする	
		4-13	LDAP サーバ上の ARL の格納エントリのオブジェクトクラスをチェックする	
		4-14	LDAP サーバ上の ARL の属性をチェックする	
5	EE 証明書発行	5-1	利用者からの申請方法、利用者への配布方法を決定する	・特恵 ECO 発行者証明書 ・特恵 ECO 発行者 S/MIME 証明書（署名用）
		5-2	利用者からの申請を受取る（optional)	

		5-3	プロファイル設計	・特恵 ECO 発行者 S/MIME 証明書（暗号化用） ・特恵 ECO 検証者証明書 ・ASP サーバ用 S/MIME 証明書（署名用） ・ASP サーバ用 S/MIME 証明書（暗号化用）
		5-4	データを入力し、署名して発行する	
		5-5	発行した証明書の内容をチェックする	
		5-6	発行した証明書を LDAP サーバに格納する（optional）	
		5-7	LDAP サーバ上の証明書の格納エントリの DN をチェックする（optional）	
		5-8	LDAP サーバ上の証明書の納エントリのオブジェクトクラスをチェックする（optional）	
		5-9	LDAP サーバ上の証明書の属性をチェックする（optional）	
		5-10	利用者へ証明書を配布する	
6	EE 証明書検証	6-1	正常証明書の検証（期待する検証結果　有効）	「表 4.3　検証対象証明書一覧」参照
a	ドメイン間信頼関係構築	a-1	信頼モデルの選択	（CR モデルで実験実施）
		a-2	自己署名証明書を相手ドメインに渡す	
		a-3	証明書ポリシを相手ドメインに通知する	

これらの項目で「Asia PKI Interoperability Guideline の利用に関する手引」を参照して「Asia PKI Interoperability Guideline」を利用したものを記録し、分析する。

「表 4.3　検証対象証明書一覧」に証明書検証の対象となる証明書を示す。

表 4.3　検証対象証明書一覧

Test ID	検証対象公開鍵証明書	トラストアンカ	証明書検証者	実験結果期待値
1	シンガポール特恵 ECO 発行機関証明書	シンガポール認証局の自己署名証明書	仮想対象国税関ドメインの証明書検証者	有効（Valid）
2	シンガポール ASP サーバ用 S/MIME 証明書			有効（Valid）
3	模擬商工会議所認証局特恵 ECO 発行者証明書	模擬商工会議所認証局の自己署名証明書	仮想対象国税関ドメイン証明書検証者	有効（Valid）
4	模擬財務省認証局 ASP サーバ用 S/MIME 証明書	模擬財務省認証局の自己署名証明書		有効（Valid）

(3) 手順

本実証実験は、PKI 環境の構築作業自体が検証対象である。認証局を建局するための準備作業から証明書の発行や証明書失効リストの管理までの運用作業のすべて、さらに構築した PKI 環境での証明書検証による環境の確認までを実証実験の検証項目として実施する。

(a) 準備作業
- PKI コンポーネントの構成検討
- ハードウェアおよびソフトウェア設定
- ネットワーク設定

(b) 認証局建局
- 自己署名証明書発行
- 証明書失効リスト（CRL/ARL）発行

(c) EE 証明書発行

(d) EE 証明書検証

(e) ドメイン間の信頼関係構築

(a)から(c)の項目について作業を実施し、実験結果データとして発行した証明書類（「表 4.1　日本国認証局が発行する証明書一覧」参照）を採取し分析する。

さらに、(d)により構築した PKI 環境を確認し(c)までの作業が正しく行われたことを確認する。

(4) 実験結果データ

(a) 証明書チェック結果

「表 4.4　証明書類 APKI ガイドライン準拠チェック結果一覧（対シンガポ

ール)」に実験結果データとして採取した証明書と証明書失効リストの一覧を示す。結果欄は当該データが「Asia PKI Interoperability Guideline」に準拠しているかどうかのチェック結果を示す。

表 4.4　証明書類APKIガイドライン準拠チェック結果一覧（対シンガポール）

No	発行元認証局	証明書の種類	結果
1	模擬商工会議所認証局	自己署名証明書	○
2		証明書失効リスト（CRL）	○
3		証明書失効リスト（ARL）	○
4		特恵 ECO 発行者証明書	○
5		ASP サーバ用 S/MIME 証明書（署名用）	○
6		ASP サーバ用 S/MIME 証明書（暗号化用）	○
7	模擬財務省認証局	自己署名証明書	○
8		証明書失効リスト（CRL）	○
9		証明書失効リスト（ARL）	○
10		特恵 ECO 検証者証明書	○
11		ASP サーバ用 S/MIME 証明書（署名用）	○
12		ASP サーバ用 S/MIME 証明書（暗号化用）	○

(b) エンドエンティティ証明書検証結果

エンドエンティティ証明書の検証結果を「表 4.5　証明書検証結果」に示す。

表 4.5　証明書検証結果

Test ID	検証対象公開鍵証明書	トラストアンカ	証明書検証者	実験結果期待値	実験結果
1	シンガポール特恵 ECO 発行機関証明書	シンガポール認証局の自己署名証明書	仮想対象国税関ドメインの証明書検証者	有効（Valid）	有効（Valid）
2	シンガポール ASP サーバ用 S/MIME 証明書			有効（Valid）	有効（Valid）
3	模擬商工会議所認証局特恵 ECO 発行者証明書	模擬商工会議所認証局の自己署名証明書	仮想対象国税関ドメインの証明書検証者	有効（Valid）	有効（Valid）
4	模擬財務省認証局 ASP サーバ用 S/MIME 証明書	模擬財務省認証局の自己署名証明書		有効（Valid）	有効（Valid）

(c) 作業項目中の「Asia PKI Interoperability Guideline の利用に関する手引」参照の割合

作業の際に「Asia PKI Interoperability Guideline の利用に関する手引」を参照したか否か、参照によって有効な情報を得られたか否かを作業項目ごとに検証した。「表 4.6　手引利用頻度（対シンガポール)」にその結果を示す。

表 4.6　手引利用頻度（対シンガポール）

No	step	作業項目数	参照項目数	備考
1	構成検討	6	6	-
2	HW/SW 設定	12	12	-
3	自己署名証明書発行	14	9	「PKI の国際的相互接続に関する手引」に該当する項目がない作業項目が１つあり、追記すべき内容と判断したので手引を改訂した。
4	CRL/ARL 発行	28	20	-
5	EE 証明書発行	15	12	-
6	EE 証明書検証	-	-	「PKI の国際的相互接続に関する手引」対象外作業
7	ドメイン間信頼関係構築	3	3	-
-	計	78	62	-

(5) 評価

採取データである証明書、CRL/ARL の分析結果は問題なく、本実証実験では「Asia PKI Interoperability Guideline」に正しく準拠した PKI 環境を構築することができた。

エンドエンティティ証明書の検証結果でも、期待したとおりの結果が得られ、重ねて PKI 環境の正しさを確認することができた。

上記 2 点から、「Asia PKI Interoperability Guideline の利用に関する手引」を参照しての作業は正しく期待した結果が得られ、「Asia PKI Interoperability Guideline の利用に関する手引」が有効に機能することが実証されたと考える。

作業手順 78 項目中、62 項目で「Asia PKI Interoperability Guideline の利用に関する手引」を参照して「Asia PKI Interoperability Guideline」を利用した。

これらの項目は特に PKI の国際間の相互接続において「Asia PKI Interoperability Guideline」に準拠することが相互接続性を確保するための重要な要件である項目である。それらのポイントについて「Asia PKI Interoperability Guideline の利用に関する手引」が簡潔にして有効な「Asia PKI Interoperability Guideline」へのポインタを示していることは認証局を構築する利用者にとって大きな利便性を提供し、適切な PKI 環境の構築と利用に寄与するところである。

4.3.2 仮想対象国との相互接続における検証

(1) 目的

仮想対象国との間で実施するパイロットシステム実験の PKI 環境構築の作業を通して、シンガポールとの実験で洗い出した「Asia PKI Interoperability Guideline の利用に関する手引」の改善点についての再検証を重点目的とした PKI 環境構築に関する検証を実施する。

(2) 方法

「Asia PKI Interoperability Guideline の利用に関する手引」を参照して、実験環境内に日本国の認証局と相互接続する仮想対象国の認証局を設置し、パイロットシステムとして必要な PKI 環境を構築する。その環境で発行された証明書および証明書失効リストを実験結果データとして採取する。仮想対象国の認証局としては、模擬日本商工会議所認証局および模擬財務省認証局を構築する。

表 4.7　仮想対象国認証局が発行する証明書一覧

No	発行元認証局	証明書の種類
1	仮想対象国特恵 ECO 発行機関認証局	自己署名証明書
2		証明書失効リスト（CRL）
3		証明書失効リスト（ARL）
4		特恵 ECO 発行者証明書
5		ASP サーバ用 S/MIME 証明書（署名用）
6		ASP サーバ用 S/MIME 証明書(暗号化用)
7	仮想対象国税関認証局	自己署名証明書
8		証明書失効リスト（CRL）
9		証明書失効リスト（ARL）
10		特恵 ECO 検証者証明書
11		ASP サーバ用 S/MIME 証明書（署名用）
12		ASP サーバ用 S/MIME 証明書(暗号化用)

「表 4.7　仮想対象国認証局が発行する証明書一覧」に示す証明書がすべて「Asia PKI Interoperability Guideline」に正しく準拠していることを確認し、本実証実験の作業でアジア地域での PKI の相互接続性を保証する仕様に沿った PKI 環境が構築されることを示す。

さらに、構築した PKI 環境で証明書の検証を行い期待した検証結果が得られることを確認することで、PKI 環境の構築が正しく行われていることを示す。

「表 4.2　PKI 相互接続実験項目概略」に概略を示した実験項目を実施する。

これらの項目で「Asia PKI Interoperability Guideline の利用に関する手引」を参照して「Asia PKI Interoperability Guideline」を利用したものを記録し、分析する。

「表 4.8　検証対象証明書一覧（仮想対象国）」に証明書検証の対象とする証明書を示す。

表 4.8　検証対象証明書一覧（仮想対象国）

Test ID	検証対象公開鍵証明書	トラストアンカ	証明書検証者	実験結果期待値
5	仮想対象国特恵 ECO 発行機関証明書	仮想対象国特恵 ECO 発行機関認証局の自己署名証明書	模擬財務省認証局ドメイン証明書検証者	有効（Valid）
6	仮想対象国 ASP サーバ用 S/MIME 証明書			有効（Valid）
7	仮想対象国税関用 S/MIME 証明書	仮想対象国税関認証局の自己署名証明書	日本国輸入者	有効（Valid）

(3) 手順

本実証実験は、PKI 環境の構築作業自体が検証対象である。認証局を建局するための準備作業から証明書の発行や証明書失効リストの管理までの運用作業のすべて、さらに構築した PKI 環境での証明書検証による環境の確認までを実証実験の検証項目として実施する。

(a) 準備作業
- PKI コンポーネントの構成検討
- ハードウェアおよびソフトウェア設定
- ネットワーク設定

(b) 認証局建局
- 自己署名証明書発行
- 証明書失効リスト（CRL/ARL）発行

(c) EE 証明書発行

(d) EE 証明書検証

(e) ドメイン間の信頼関係構築

(a)から(c)の項目について作業を実施し、実験結果データとして発行した証明書類(「表 4.7　仮想対象国認証局が発行する証明書一覧」参照)を採取し分析する。

さらに、(d)により構築した PKI 環境を確認し(c)までの作業が正しく行われたことを確認する。

(4) 実験結果データ

(a) 証明書チェック結果

「表 4.9　証明書類 APKI ガイドライン準拠チェック結果一覧（仮想対象国）」に実験結果データとして採取した証明書と証明書失効リストの一覧を示す。結果欄は当該データが「Asia PKI Interoperability Guideline」に準拠しているかどうかのチェック結果を示す。

表 4.9　証明書類APKIガイドライン準拠チェック結果一覧（仮想対象国）

No	発行元認証局	証明書の種類	結果
1	仮想対象国特恵ECO発行機関認証局	自己署名証明書	○
2		証明書失効リスト（CRL）	○
3		証明書失効リスト（ARL）	○
4		特恵 ECO 発行者証明書	○
5		特恵 ECO 送信者 S/MIME 用証明書（署名用）	○
6		特恵 ECO 送信者 S/MIME 用証明書（暗号化用）	○
7	仮想対象国税関認証局	自己署名証明書	○
8		証明書失効リスト（CRL）	○
9		証明書失効リスト（ARL）	○
10		特恵 ECO 検証者証明書	○
11		特恵 ECO 受信者 S/MIME 証明書（署名用）	○
12		特恵 ECO 受信者 S/MIME 証明書（暗号化用）	○

(b) エンドエンティティ証明書検証結果

エンドエンティティ証明書の検証結果を「表 4.10　証明書検証結果（仮想対象国）」に示す。

表 4.10　証明書検証結果（仮想対象国）

Test ID	検証対象公開鍵証明書	トラストアンカ	証明書検証者	実験結果期待値	実験結果
5	仮想対象国特恵ECO発行機関証明書	仮想対象国特恵ECO 発行機関認証局の自己署名証明書	模擬財務省認証局ドメイン証明書検証者	有効（Valid）	有効（Valid）
6	仮想対象国ASP サーバ用 S/MIME 証明書			有効（Valid）	有効（Valid）
7	仮想対象国税関用 S/MIME 証明書	仮想対象国税関認証局の自己署名証明書	日本国輸入者	有効（Valid）	有効（Valid）

(c) 作業項目中の「Asia PKI Interoperability Guideline の利用に関する手引」参照の割合

作業の際に「Asia PKI Interoperability Guideline の利用に関する手引」を参照したか否か、参照によって有効な情報を得られたか否かを作業項目ごとに検証した。「表 4.11　手引利用頻度（仮想対象国）」にその結果を示す。

表 4.11　手引利用頻度（仮想対象国）

No	Step	作業項目数	参照項目数	備考
1	構成検討	6	6	-
2	HW/SW 設定	12	12	-
3	自己署名証明書発行	14	10	-
4	CRL/ARL 発行	28	20	-
5	EE 証明書発行	15	12	-
6	EE 証明書検証	-	-	「Asia PKI Interoperability Guideline の利用に関する手引」対象外作業
7	ドメイン間信頼関係構築	3	3	-
-	計	78	63	-

(5) 評価

シンガポールとの相互接続における検証を通して、「Asia PKI Interoperability Guideline の利用に関する手引」の改訂が行われた。本実験項目では改訂版を対象として検証を行った。

採取データである証明書、CRL/ARL の分析結果は問題なく、本実証実験では「Asia PKI Interoperability Guideline」に正しく準拠した PKI 環境を構築することができた。

エンドエンティティ証明書の検証結果でも、期待したとおりの結果が得られ、重ねて PKI 環境の正しさを確認することができた。

上記 2 点から、「Asia PKI Interoperability Guideline の利用に関する手引」を参照しての作業は正しく期待した結果が得られ、「Asia PKI Interoperability Guideline の利用に関する手引」が有効に機能することが実証されたと考える。

作業手順 78 項目中、63 項目で「Asia PKI Interoperability Guideline の利用に関する手引」を参照して「Asia PKI Interoperability Guideline」を利用した。対シンガポール実験より参照箇所が 1 項目増えているが、これは対シンガポール実験で「Asia PKI Interoperability Guideline の利用に関する手引」に不足のあった箇所が改訂されたためである。この他にも、項目数には表れないが、「Asia PKI Interoperability Guideline の利用に関する手引」の記述内容の改訂が行われた上で参照されており、実証実験を通して内容の充実が図られている。これにより「Asia PKI Interoperability Guideline の利用に関する手引」はさらに有効性を増したと評価する。

4.3.3 考察

本実証実験項目は「Asia PKI Interoperability Guideline の利用に関する手引」の有効性検証と合わせて「Asia PKI Interoperability Guideline」の再検証の性格も併せ持つ作業であった。PKI 環境構築は問題なく実施され「Asia PKI Interoperability Guideline」が国際的な認証ドメイン間の信頼関係構築において有効であることは実証された。ただし、現在「Asia PKI Interoperability Guideline」で規定する証明書プロファイルでは指定を必須としている intermediate CA の PolicyMappings を任意とするのが妥当ではないかという点が検討課題として浮上した。本件については「6.1.1PKI の国際的相互接続に関する手引の評価および考察」で詳細を記述する。

5 PKI 実利用のためのガイドライン作成

PKI 実利用のためのガイドラインとして「特恵原産地証明書の電子化に係るガイドライン」を作成した。

本章では、「特恵原産地証明書の電子化に係るガイドライン」の作成について、書面運用時の課題および要件の洗い出し、書面運用から電子文書運用への移行に際し考慮すべき点、パイロットシステムを用いた運用例、検証結果等を示す。

なお、ガイドラインの記載事項についてはシンガポールと協議し、改版を行った。ガイドライン詳細に関しては「付録２　特恵原産地証明書の電子化に係るガイドライン」として収録。

5.1　ガイドラインの目的および想定する読者

(1) ガイドラインの目的

PKI 実利用のためのガイドラインとして、FTA 等により 2 カ国間で有効な特恵原産地証明書を電子的に発行し、交換する場合に必要となる下記の 8 つの項目について、考慮すべき事項およびパイロット事例を記述する。それにより、今後実用が期待されている特恵原産地証明書の電子化を促進すること、および、国際的な取引環境で電子文書を交換する際の電子文書の真正性、秘匿性を確保するために利用されることを想定している。事例として電子原産地証明書を取り上げることにより、その他の取引においても PKI を利用した安全性の高い取引環境を促進する狙いがある。

- 基本的なシステムの仕組み
- 信頼の構築方法
- データ交換の方法
- データのフォーマット
- 電子署名の実施
- 電子署名の検証
- 公開鍵証明書の内容
- 電子原産地証明書の検証方法

(2) 想定する読者

本ガイドラインの読者は、以下のいずれかの項目に当てはまる者を想定し、電子原産地証明書およびその他の国際間での電子文書交換の企画、実装、運用を行う場合の参考資料として利用されることを期待している。

・ 電子原産地証明書の発行を企画する者
・ 商工会議所等、原産地証明書の発行者
・ 税関等、原産地証明書の最終受領者
・ 国際間における書面を電子的に交換する業務の計画や実施に携わる者
・ PKI 技術を実ビジネスへ実装することに携わる者、等

5.2　特恵原産地証明書の法的な要件と課題

5.2.1 特恵原産地証明書（GSP）における要件

特恵原産地証明書（GSP）の認定基準については、政令において、輸入物が特恵の処遇を得られるためには、

(1) 特恵受益国において完全に生産された物品であること。
(2) 特恵受益国において完全に生産された物品以外の物品は、その原料又は材料の全部又は一部としてこれに実質的な変更を加える加工又は製造により生産された物品であること。

が要件とされ、特恵関税の適用には、そのことを証明する特恵原産地証明書が必要とされている。

輸入者は輸出者よりこの特恵原産地証明書を取得することになる。税関は特恵原産地証明書が正規に発行されたものかを次の基準に基づいて検査を実施している。

(1) Form A 様式の証明書であること。
(2) 輸出前に発行されていること。
(3) 特恵原産地証明書が輸出国税関、商工会議所、または然るべき機関によって発行されたものであること。
(4) 各項目が正確に記載されて、日本の税関に登録されたスタンプおよび署名があること。
(5) インボイスの輸入品目が、証明書と同一であること。
(6) 修正のある場合はその発給機関の修正印が押してあること。

5.2.2 日本－シンガポール間の協定における要件

「新たな時代における経済上の連携に関する日本国とシンガポール共和国との間の協定」の内、その第 31 条において、

(1) 特恵原産地証明書は、輸出締約国が特定する機関又は団体によって発行されたものでなければならない。
(2) 特恵原産地証明書には、附属書ⅡB に定める事項についての記載を必ず含めるものとする。
(3) 特恵原産地証明書は、証明の日付の日から 12 箇月間有効なものとする。

と定められている。

また、附属書ⅡB においては、下記が特恵原産地証明書の必要記載事項として定められている。

(1) 輸出者
- 輸出者の氏名および住所

(2) 輸入者
- 輸入者の氏名および住所

(3) 輸送手段
- 出発日
- 船舶又は航空機の出港日（判明している場合）
- 船舶名又は便名
- 船舶の名称又は航空機の便名（判明している場合）
- 荷揚港
- 産品の最終的な荷揚港（判明している場合）
- 輸出国から輸入国に直接輸送されない場合の経路

(4) 最終仕向国

(5) 産品の原産国

(6) 記号および番号
- 貨物の記号および番号（必要な場合には、別紙に記載）

(7) 包装の個数および種類並びに品名（統一システム番号を併記）

(8) 数量
- 産品の数量およびその計量単位（個数、キログラム等）

(9) 仕入書の番号および日付
- 貨物の仕入書の番号および日付

(10) 輸出者による申告

(11) 機関又は団体による証明
- 輸出締約国内の機関又は団体の署名および印章

(12) 証明番号
- 証明書ごとの個別番号

第 33 条には、特恵原産地証明書の確認のための援助とて、産品の輸入から 3 年の間は、輸出締約国に対して特恵原産地証明書の真正性や正確性について確認することができることを規定している。

また、第 40 条から第 43 条において、貿易取引文書の電子化についての展望が規定されている。

第 40 条　貿易取引文書の電子化に関する両締約国間の協力

貿易取引情報及び船荷証券、送り状、信用状、保険証明書その他の文書上の内容を電子的方式により入力したものを書面によらず電子的に保管し及び移転することが、費用及び時間の削減を通じて貿易の効率を著しく高めることを認識して、両締約国間の貿易取引文書の電子化を実現及び促進

するために協力する。

第 41 条　意見及び情報の交換

貿易取引文書の電子化の実現、促進及び発展に関する意見及び情報を交換する。

第 42 条　貿易取引文書の電子化に関する民間の団体間の協力

貿易取引文書の電子化に関する活動に従事する両締約国の関連する民間の団体間の協力を奨励する。

第 43 条　貿易取引文書の電子化の実現に関する検討

電子的な貿易取引情報及び関係文書上の内容を電子的方式により入力したものが貿易規制当局により補助的なものとして使用されることを可能とする方策について、できる限り速やかに、いかなる場合にも 2004 年以前に検討を行う。

5.2.3 日本－メキシコ間における要件

「経済上の連携強化に関する日本国とメキシコ合衆国との間の協定」では次のような取り決めがなされている。

第 39 条：協定に基づく特恵原産地証明書に関して、以下の事項が定められている。

(1) 特恵原産地証明書は、輸出者又は代理人による書面による申請に基づき、輸出締約国の権限のある政府当局が発給する。
(2) 特恵原産地証明書は、輸出締約国の権限のある政府当局又はその指定する団体により押印され、かつ、署名されなければならない。
(3) 輸出締約国の権限のある政府当局は、自国の関係法令により与えられた権限に基づき、特恵原産地証明書の発給について責任を負う政府以外の団体を指定することができる。
(4) 輸出締約国の権限のある政府当局が政府以外の団体について特恵原産地証明書を発給するものとして指定する場合には、当該輸出締約国は、輸入締約国に対し書面により当該政府以外の団体を通報する。
(5) 特恵原産地証明書の様式は、協議のうえ統一規則において定める。
(6) 産品が輸出された後であっても特恵原産地証明書を発給できる。遡及して発給された特恵原産地証明書は、統一規則に定める文言を明示しなければならない。
(7) 特恵原産地証明書が盗まれ、亡失し、又は著しく損傷した場合には、当該特恵原産地証明書を発給した権限のある政府当局又は指定団体は、申請に基づき、

特恵原産地証明書を再発給することができる。この場合、特恵原産地証明書は、統一規則に定める再発行を示す文言を記さなければならない。

(8) 特恵原産地証明書は、産品の 1 回限りの輸入に適用され、かつ、当該特恵原産地証明書が発給された日の後 1 年間又は両締約国が合意するその他の期間、税関当局において受理される。

(9) 輸出締約国の権限のある政府当局は、輸入締約国の要請に応じ、関税上の特恵待遇を要求された産品が原産品であるか否かに関する情報を提供する。

(10) 権限のある政府当局又は指定団体が特恵原産地証明書の発給のために使用する印章の図案を、輸入締約国に提供する。

第 40 条：特恵原産地証明書に係る輸入に関する以下の義務が規定されている。

(1) 輸入者は、当該産品が原産品であることについて書面による申告を行うこと。

(2) 申告を行う際に特恵原産地証明書を所持すること。

(3) 税関当局の要請に応じ、特恵原産地証明書を提出すること。

(4) 輸入者が輸入の際に特恵原産地証明書を所持していない場合には、国内法令に従い、輸入の後 1 年を超えない期間内に提出することができる。

第 43 条：特恵原産地証明書に係る記録の保管について、以下が規定されている。

(1) 権限のある政府当局又は指定団体は、特恵原産地証明書についての記録を発給の日の後、5 年間以上保管すること。当該記録には、原産品であることを証明するために提示されたすべての文書等を含める。

(2) 輸出者または生産者は、特恵原産性を証明する記録を特恵原産地証明書の発給の日の後 5 年間又は当該締約国が指定するこれよりも長い期間保存すること。

(3) 輸入者は、当該産品の輸入の日の後 5 年間又は当該締約国が指定するこれよりも長い期間、保管すること。

5.2.4 特恵原産地証明書の電子化にあたっての協定上の留意点

(1) 書面要求

日本－シンガポール間の協定では、特恵原産地証明書が明示的に書面でなくてはならないとは規定していないが、特恵原産地証明書の記載事項において、発行機関の署名および印章が必要であることが明記されており、書面を前提とした運用を想定している。また、特恵原産地証明書とは明示されていないが、貿易取引文書の電子化を実現し、これを促進するために協力することが合意されている。

日本－メキシコ間の協定では、特恵原産地証明書は、発行者により押印され、かつ、署名されなければならないことが規定されている。

(2) 特恵原産地証明書発行者

日本－シンガポール間の協定では、輸出国が特定する機関または団体を指定できることが定められている。

日本－メキシコ間の協定では、特恵原産地証明書は、政府により発行されることを原則とするが、政府は、政府以外の団体を発行者として指定できる。

(3) 特恵原産地証明書の真偽性判定の資料

日本－メキシコ間の協定では、権限のある政府当局または指定団体が特恵原産地証明書の発給のために使用する印章の図案を、輸入締約国に外交ルートを通して提供することが規定されている。

(4) 輸入申告方法

日本－メキシコ間の協定では、輸入者は、当該産品が原産品であることについて書面による申告を行うことが規定されている。また、特恵原産地証明書の原本の提示については、国内法に規定があれば、輸入後、1 年以内の提示を許容している。

(5) 記録保管

日本－シンガポール間の協定では、発行から 1 年以内の利用、利用から 3 年以内の輸入国側からの問い合わせ対応が必要となるので、協定上は、発行から 4 年間の保存が必要である。

日本－メキシコ間の協定では、発行から 5 年間以上の保存を明示的に要求している。

5.3　書面による特恵原産地証明書に係る課題

(1) 発行機関にとっての改善期待項目

(a) 書面データの入力項目確認作業

(i) 特恵原産地証明書の申請書に記載された輸出者に関する内容と登録されている内容とに差異がないことの確認が、目視作業となっている。機械化による自動チェックが期待される。

(ii) 特恵原産地証明書の申請書に記載された商品の内容と提出されたインボイス（商業送り状）の内容とに差異がないことの確認が、目視作業となっている。インボイスは必ずしも電子データ化されているとは限らず、また、インボイスにおける表記方法と特恵原産地証明書における表記方法の違いもあるので、単純な機械化は困難と思われるが、ある程度の自動化が期待される。

(iii) インボイスおよび特恵原産地証明書用紙にある署名と貿易登録情報に登録された肉筆署名との整合確認作業は、イメージの照合処理であり、高度な情報処理技術を要するため、現状では完全自動化の技術には至っていない。た

だし、毎回、署名を要求するのではなく、商工会議所側に登録した署名をイメージデータとして書面に印字することは可能なので、特恵原産地証明書における署名作成手続きの方法を変更することにより大幅な自動化が可能となる。

(b) 人手による受け渡し事務

(i) 来訪者が正当な申請者・受領者であることの確認は、人が来る限り必要であり、自動的な受け渡し装置の導入となると大掛かりなものとなるので、簡単な改善は難しい。

(ii) 書面に依存している限り、手作業による分類業務は必須である。文書の電子化により改善されることが期待される。

(iii) 書面に依存している限り、人手による書類の受け渡し事務が発生する。文書の電子化により、受け渡しおよびその管理が改善されることが期待される。

(c) 原産性の確認

申請情報とあらかじめ登録されてある貿易登録情報との整合性確認作業は、登録データと申請データの照合機能によりある程度の自動化が可能となるが、最終的には人による判断が必要である。

(d) 人手による発行作業

スタンプ押印作業およびパンチ式エンボッサーによる刻印作業は、特恵原産地証明書の偽造を防ぎ、信頼性を高めるものである。より一層の自動的な機械化も可能ではあるが、投資に見合うだけの効率化はあまり期待できない。特恵原産地証明書の電子化データによる改善が期待される。

(e) 保存面での課題

特恵原産地証明書は 5 年以上の保存が必要なため、保存スペースの確保が必要となり、また、輸入国からの問い合わせに対して答えられるよう容易な検索が行えなければならない。電子的な媒体への保存により、スペースの問題と検索の問題が改善されることが期待される。

(2) 利用者にとっての改善期待項目

(a) 移動

申請書および特恵原産地証明書の受け取りに、商工会議所まで赴く必要があり、また、商工会議所において待ち時間が発生する。移動コストおよび人的コストの削減が期待される。

(b) 営業時間の制限

現行では商工会議所の申請受付時間は 9:00～16:30 に限定されている。そのため、午前中に申請を受け付けた場合は、当日の午後に受け取りが可能であるが、午後に申請を受け付けた場合は、翌日の午前中に受け取りとなる。インターネットを利用した電子受付が可能となれば、利用者の利便性は向上する。

(3) 輸入国側の税関にとっての改善期待項目

(a) 安全性

締約国からの原産品として認定されれば関税が免除されるので、輸入者にとって特恵原産地証明書の入手については、不正を行う動機を誘発する。また、輸出者が、不正な特恵原産地証明書を添付する動機も否定しきれない。高度なコピー技術が容易に入手可能な時代となっているので、書面だけによる真偽性の判定には限界がある。

現状では、特恵原産地証明書に記載されている内容の通りに実際に発行されたかどうかは、輸入国税関職員から輸出国発行機関に対して電話で不明点を確認するという手段に頼っている。

電子的なデータ交換による改善が期待されている。

5.4　特恵原産地証明書の電子化について

5.4.1 信頼の連鎖の形成

(1) 書面による特恵原産地証明書における信頼の連鎖の形成

現在の日本－シンガポール間、あるいは、日本－メキシコ間で交換される情報の信頼の原点は外交ルートにある。両国は、信頼できるコンタクト先およびその情報交換の方法を限定することにより、信頼できる情報を交換している。

特恵原産地証明書に関しては、外交ルートを通して、輸出者側が発行する特恵原産地証明書の書面様式、特恵原産地証明書の発行機関、発行機関の印章、特恵原産地証明書を発行する権限者の氏名、署名サンプルが交換され、輸入国側の税関に手渡される。また、発行機関へのコンタクト情報も交換される。

輸入国側の税関は、これらの情報を安全なルートから入手することにより、特恵原産地証明書の真偽性をはじめて判定できるようになり、必要に応じて、発行機関に直接問い合わせることが可能となる。

(2) 特恵 ECO における信頼の連鎖の形成

特恵 ECO においても、基本的な信頼の連鎖の形成の考え方に相違はないが、電子的な仕組みを取り入れるので、少し複雑になるパターンも存在する。

特恵 ECO は、電子データであるので、書面における原本性の概念はもはや通用しない。電子データにおいては、原本とコピーとの区別をつけることはできな

い。ただし、電子データにおいては、電子署名を利用することにより、データの改ざんを防止することができ、また、その内容が誰によって署名されたかを検証することが可能となる。特恵 ECO の場合には、署名サンプルの代わりに、発行者が電子署名を検証するときに必要となる公開鍵証明書を交換する必要がある。この場合、輸入国の税関にとっての信頼の原点は、外交ルートより入手した発行者の公開鍵証明書である。

上記は、一番シンプルな特恵 ECO における信頼の連鎖の形成である。
公開鍵証明書は、認証局によって電子的に署名され、発行されるので、認証局の公開鍵証明書を信頼の原点として交換することも考えられる。この場合、外交ルートを通して交換されるのは、認証局の公開鍵証明書である。輸入国の税関は、「認証局の公開鍵証明書」→「発行者の公開鍵証明書」→「特恵原産地証明書」という連鎖を辿り、特恵原産地証明書の真正性を判定する。

以上は、特恵 ECO を発行して、データとして交換するという考え方に基づいているが、発行者が特恵 ECO を特定のデータベースに格納して、輸入国側の税関がこのデータベースを見ることにより、特恵原産地証明書の真偽性を検証することも可能である。この場合、輸出国側では、特恵原産地証明書を従来どおり書面で発行すると同時に、発行データをデータベースに登録する。輸入国側の税関は提出された特恵原産地証明書とデータベースの内容を比較し、その真偽性を検証する。

5.4.2 特恵 ECO の実装パターン

(1) 特恵 ECO のみの発行

発行者は、書面に代わり、電子書名付きの電子データからなる特恵 ECO を発行する。特恵 ECO は、インターネットを経由して、申請者である輸出者に送付される。輸出者は、輸入者に特恵 ECO を送付し、輸入者は、税関に輸入申告の添付データとして、特恵 ECO を送付する。税関は、電子署名を検証し、特恵 ECO の真正性を確認する。

(2) 書面による特恵原産地証明書と特恵原産地証明書データベースの併用

発行者は、従来どおり、書面による特恵原産地証明書を発行する。これと並行して、発行された特恵原産地証明書の内容が、輸入国側の税関から参照可能なデータとして登録される。特恵原産地証明書は、輸出者から輸入者に送付される。輸入者は、税関に輸入申告の添付データとして、特恵原産地証明書の原本または特恵原産地証明書をスキャンしたデータ、または特恵原産地証明書の発行番号を送付する。

税関は、送られてきた特恵原産地証明書に関するデータを利用して、特恵原産

地証明書データベースを検索し、該当データと申告された内容を比較し、真偽性の判定を行う。

5.4.3 特恵原産地証明書の電子化における留意点

国際間において貿易に用いられる書面を電子文書に代えて利用する場合に、留意しなければならない点に以下のものがある。

(1) システムの設計において必要とされる留意事項

(a) データのフォーマット共通化

2 カ国間の経済協定においては、特恵原産地証明書（EPA：Economic Partnership Agreement）のフォーマットを事前に協議して決定している。協定においては、締約国は、基本的に同じ経済領域にあるという考え方をとるので、フォーマットも共通のものが使われる。

データフォーマットとしては、EDIFACT フォーマットが既に普及しているが、そのフォーマットの考え方は、XML が開発される前のもので、利用するためには特別のソフトウェアを用意しなければならず、開発コストもかさむ。現状の利用者環境を考慮すると、XML フォーマットの採用が望ましい。

(b) 電子署名の検証方法

特恵原産地証明書に利用される電子署名の検証方法については、どこを信頼の原点とし、どのような連鎖を経由して、また、どのようなプロセスで検証するのかを事前に取り決めておく必要がある。

(c) 電子文書の送受信方法

作成された電子文書を安全にかつ確実に送付するシステムの仕様を決定し、相互に接続の確認をしておく必要がある。

(d) 公開鍵証明書の利用方法

誰がどの認証局が発行した公開鍵証明書を利用するのかを明確にした上で、公開鍵証明書の必要なデータが利用できることを確認しておく必要がある。

(e) 失効情報の利用方法

公開鍵証明書の失効情報が実際に入手できることを確認しておく必要がある。

(2) 電子原産地証明書サービスを開始するにあたっての付加的な留意事項

(a) 電子申請

特恵原産地証明書の電子化とその発行に関わる申請の電子化は、制度上、必ずしも同期して行う必要はないが、紙と電子データの混在は、管理が複雑とな

り、総合的な観点からはそれほどの効率化は期待できない。

特恵原産地証明書の電子化を実施する場合は、電子申請も合わせて計画することにより、利用者および発行者における事務手続きの簡素化・自動化を達成することが期待できる。

(b) インボイス情報との情報連携

特恵原産地証明書の発行にあたり、申請依頼内容の正当性を確認するため、当該取引に関するインボイスとの照合が必要である。

電子申請を実施するにあたっては輸出者からの信頼できる電子的なインボイス情報の取得方法についても検討する必要がある。電子的なインボイスが標準化されていない場合は、書面をスキャンしたイメージファイルの提出での運用となり、自動的な照合作業を行うことはできない。

5.4.4 特恵原産地証明書を電子化するにあたっての技術上の要件

特恵原産地証明書を電子化するにあたっての要件を以下に記述する。

(1) 真正性確保

書面による運用では、輸入国側の税関が輸出側の特恵原産地証明書の発行者の署名サンプルを事前に入手し、特恵原産地証明書に記載されている署名と署名サンプル等を比較することにより特恵原産地証明書の真正性を検証している。特恵 ECO の真正性を確保するためには、受信したデータが特恵 ECO の発行者により発行されていることを検証できる仕組みが必要である。

(2) 完全性確保

電子データは、書面の場合よりも容易に変更することが可能であり、そのままでは、変更の形跡が残らない。電子データが変更されていないという完全性を確保するためには、電子データを変更した場合にその形跡が必ず残り、その事実を容易に検証できる仕組みが必要である。

(3) 秘匿性確保

電子文書をそのままインターネット経由で送付することは、第三者にその内容が漏えいするリスクが存在する。インターネット上で情報の漏えいを防止するためには、想定している受信者のみが暗号化された電子文書を復号でき、解読できる暗号技術を採用する必要がある。

(4) 通信性確保

国際間で容易にデータを交換する場合には、アクセスの容易性およびコストの面からインターネットを利用することが考えられる。インターネットを利用したデータ交換には、電子メール、ファイル交換プロトコル（FTP）、Web で利用されているプロトコル（HTTP）等の種々の方法がある。利用者間での容易な通信が可能となるためには、輸出側、輸入側の両者において容易に利用できる仕組みを採用する必要がある。

5.4.5 特恵 ECO フォーマット

本章は特恵 ECO のフォーマットについて、書面フォーマットから電子フォーマットへの対応を考える際に考慮すべき点を示す。

(1) 特恵 ECO フォーマット作成要件

特恵 ECO のフォーマットを作成する際に以下の考慮が必要である。

(a) 特恵 ECO には、2 カ国間の協定で定められている特恵原産地証明書に記載されるべき項目が網羅されていること。
(b) ただし、書面運用時を想定した項目がある場合、その記載目的を考慮し、同等の目的を達成するための項目としての変更を行うこと。
(c) フォーマットの作成が容易にできること。
(d) フォーマットの解読が容易にできること。
(e) 特定の 2 カ国間での利用のみに限定せず、どの国家間でも利用できるよう共通性をもたせること。

パイロットプロジェクトのシステムにおいては、ソフトウェアの利用環境の整備が整ってきており、また、ビジネスにおいても利用が広がっている XML を用いたフォーマットを採用することとした。

パイロットプロジェクトの相手国シンガポールで特恵 ECO および非特恵の電子原産地証明書について XML 形式にてデータフォーマットのひな型を作成しており、世界税関機構（WCO：World Customs Organization）に対して、その評価を依頼している。

今回のパイロットプロジェクトではシンガポールと協議の上、シンガポールが作成した XML フォーマットをベースとして、日本－シンガポール間の協定および実務要件に基づき、改良を加え、日本－シンガポール間およびその他の国々でも利用可能な汎用性の高い特恵 ECO フォーマットとなっている。

(2) 特恵 ECO フォーマット

本ガイドラインでは、現在、シンガポールが電子データとして流通させる原産地証明書のフォーマットとして WCO に提案している XML を利用したフォーマットをベースに検討した。

現在、シンガポールが利用している XML フォーマットは、特恵原産地証明書に必要な情報以外に、発行するまでの手続きに必要な情報や書類間の連携を自動化するための情報が含まれている。これらの情報を取り除き、日本－シンガポール間および、日本－メキシコ間の協定において規定されている特恵原産地証明書の必須記載事項を考慮し、特恵 ECO フォーマットを作成した。

(3) 署名方式に関する考察

署名に関わる特恵原産地証明書は、以下の構造となっている。

(a) 輸出者が輸出および貨物の情報について記述し、輸出者が記述内容に間違いが無いことを宣誓する。

(b) 発行機関が輸出者の申請内容を規定された範囲で検査し、宣誓内容に間違いが無い場合、対象となっている商品について、原産性があることを発行機関としての署名を添えて証明する。

(c) さらに、特定の国に対して、輸出国に設置している領事館等が特恵原産地証明書に対して、有効な発行機関が発行したものであることを本国に対する証明の裏書として、領事館等のスタンプを押印する。

このような構造を忠実に再現するならば、以下のことを実現しなければならない。

(a) 輸出者が輸出、貨物の情報およびに宣誓文に対して電子署名を付与し、申請データとして、発行機関に送付する。

(b) 発行機関が、受領した申請データに証明宣言を付けたものに対して、電子署名を付与し、特恵 ECO として発行する。

(c) 輸出国にある輸入国の領事館が、特恵 ECO に対して、電子署名を付与する。

上記(a)〜(c)が必要になるので、電子署名には、輸出者の電子署名、発行者の電子署名、輸入国領事館の電子署名の 3 種類が必要となる。

これを実現するために、「図 5.1　署名方式（包括方式）」「図 5.2　署名方式（追記方式）」に示す署名方式について検討した。

・ 階層化して署名を行い、後から署名した署名範囲はそれまでに署名されたものを包括する。

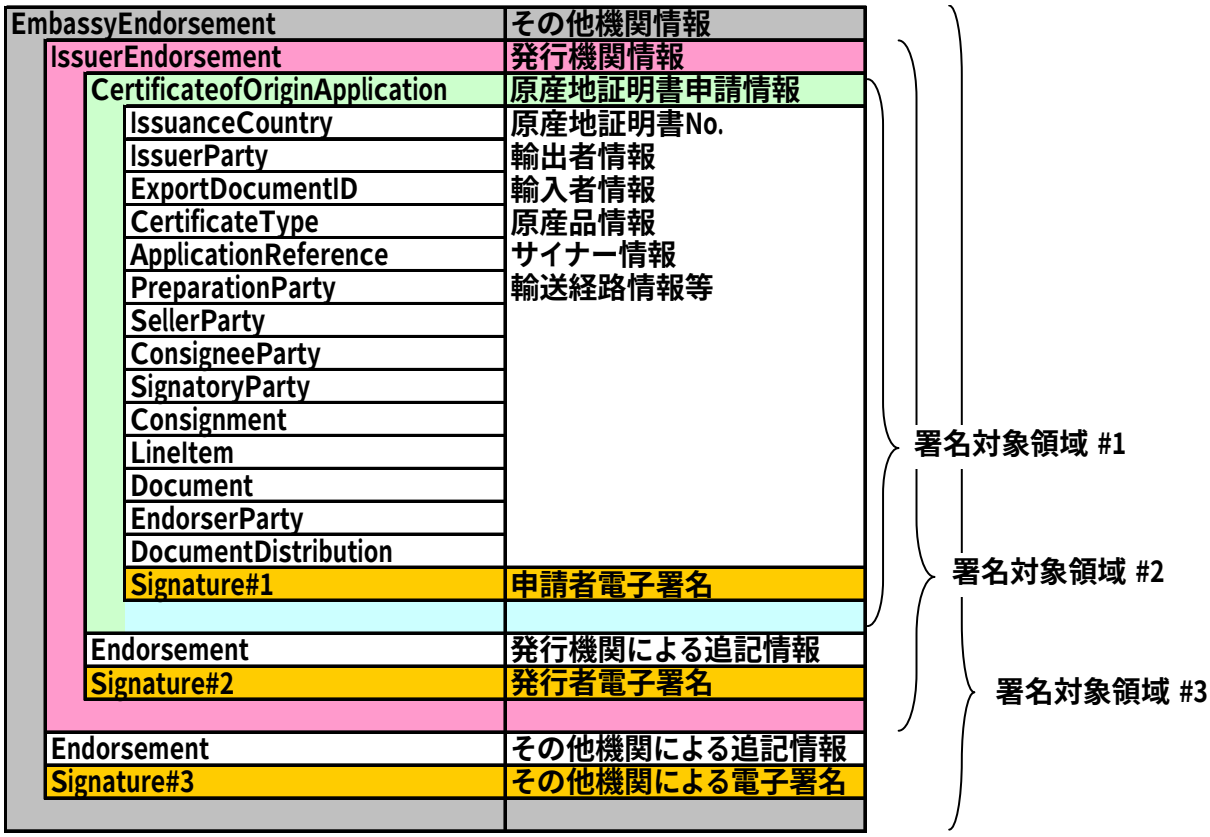

図 5.1　署名方式（包括方式）

・ 署名を追記し、それぞれの署名の署名範囲を明記する

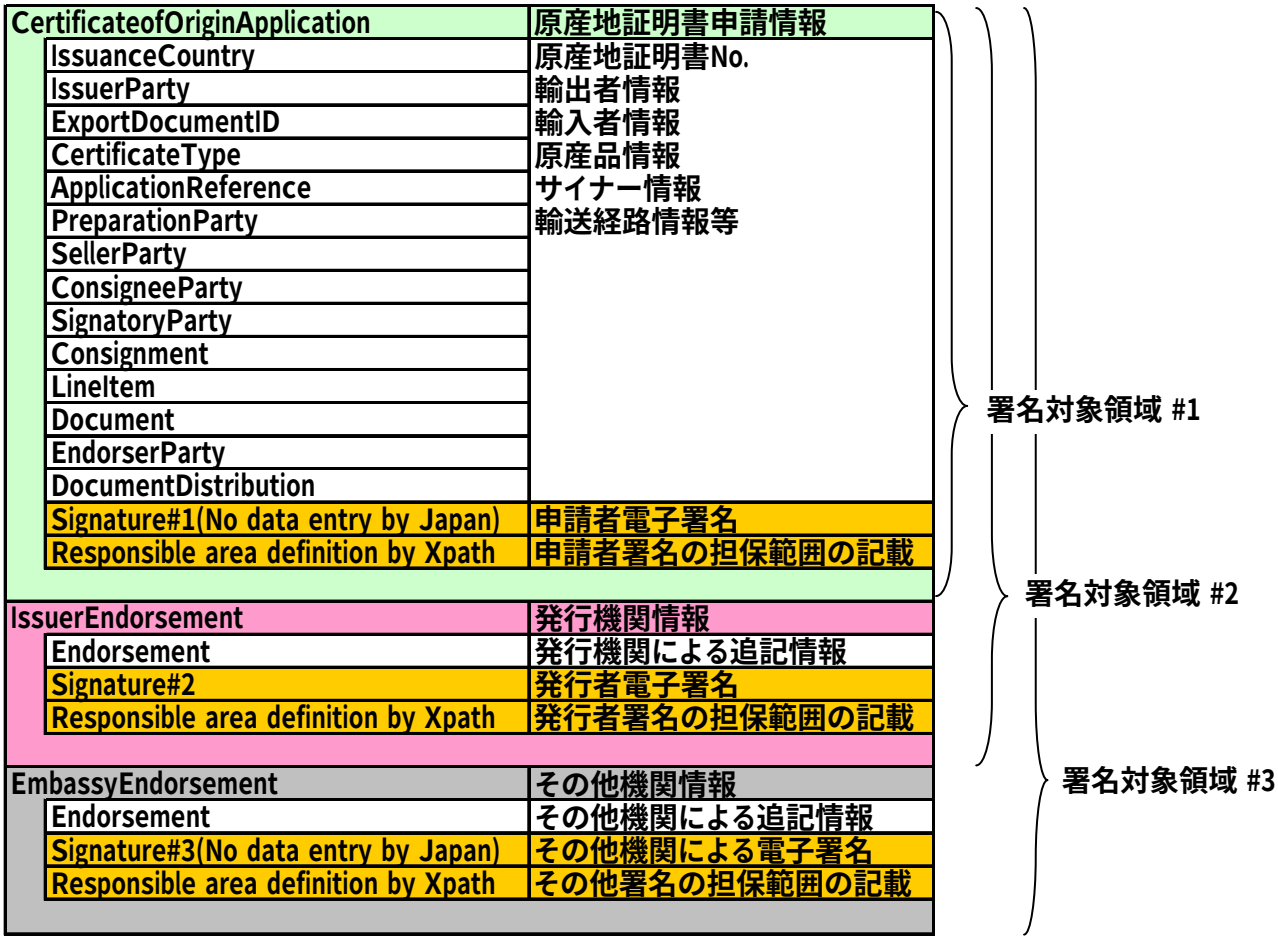

図 5.2　署名方式（追記方式）

書面の運用においては、輸入国側の税関は、発行機関の署名サンプルを事前に入手しているので、これを特恵原産地証明書の真正性の検査に利用することが可能である。しかし、輸出者の署名サンプルは、輸出国側の発行機関には存在していても、輸入国側の税関には存在しないので、輸入者の署名の真正性を検査することができない。

また、日本－シンガポール間および日本－メキシコ間の運用においては、輸入国領事館による裏書スタンプは制度上不要である。

上記を考慮して、今回取り扱う特恵 ECO に関しては、発行者の署名のみを必須としている。

今回は必須となる署名が異なっても取り交わされる特恵 ECO 自体の署名の階層が変わらないように「図 5.2　署名方式（追記方式）」のような方式を採用し、署名者を追記していく。

この例では 1 番内側の署名（#1）は申請者の署名、2 番目の署名（#2）は特恵 ECO 発行者の署名、3 番目の署名（#3）は輸出国側にある輸入国の領事館による

署名である。

以下に追記方式の XML イメージの例を示す。

〜〜

```
<?xml version="1.0" encoding="UTF-8" ?>
- <!--
 edited with XMLSPY v2004 rel. 4 U (http://www.xmlspy.com) by suresh (ORiON)
  -->
- <!--
Sample XML file generated by XMLSPY v2004 rel. 3 U (http://www.xmlspy.com)
  -->
-<CertificateofOrigin xmlns="urn:oasis:names:tc:ubl:COML:1:0-beta"
xmlns:cat="urn:oasis:names:tc:ubl:CommonAggregateTypes:1:0-beta"
xmlns:ccts="urn:oasis:names:tc:ubl:CoreComponentParameters:1:0-beta"
xmlns:cur="urn:oasis:names:tc:ubl:codelist:CurrencyCode:1:0-beta"
xmlns:res="urn:oasis:names:tc:ubl:codelist:OrderAcknowledgementCode:1:0-beta"
xmlns:rt="urn:oasis:names:tc:ubl:RepresentationTerms:1:0-beta"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:ubl:COML:1:0-
beta ..¥XMLSchemas¥mainubldoc¥COApplicationv0.8.xsd">
==================================================================
- <CertificateofOriginApplication>
+ <cat:IssuanceCountry>
+ <cat:IssuerParty Qualifier="CHAMBERS">
  <cat:ExportDocumentID>SICC-04-000001</cat:ExportDocumentID>
  <cat:CertificateType>CERTIFICATE OF ORIGIN</cat:CertificateType>
+ <cat:ApplicationReference>
+ <cat:PreparationParty Qualifier="AGENT">
+ <cat:SellerParty>
+ <cat:ConsigneeParty>
+ <cat:SignatoryParty>
+ <cat:Consignment>
+ <cat:LineItem>
+ <cat:LineItem>
+ <cat:Document>
+ <cat:Document>
+ <cat:EndorserParty Qualifier="ISSUER">
+ <cat:EndorserParty Qualifier="EMBASSY">
+ <cat:DocumentDistribution>
  <cat:Signature Id="EXPORTER" xmlns="http://www.w3.org/2000/09/xmldsig#" />
  </CertificateofOriginApplication>
==================================================================
- <cat:IssuerEndorsement>
+ <cat:Endorsement Qualifier="CHAMBERS">
   <cat:Signature Id="ISSUER" xmlns="http://www.w3.org/2000/09/xmldsig#" />
  </cat:IssuerEndorsement>
==================================================================
- <cat:EmbassyEndorsement>
+ <cat:Endorsement>
   <cat:Signature Id="EMBASSY" xmlns="http://www.w3.org/2000/09/xmldsig#" />
  </cat:EmbassyEndorsement>
==================================================================
</CertificateofOrigin>
```

optional

MUST

optional

〜〜

(4) 文字コードに関する考察

日本－シンガポール間で特恵 ECO の伝送を行うにあたり、英語が標準的にビジネスに使用されるシンガポールと原則的に英語表記による特恵原産地証明書を発行し、それを税関で受領する日本との間で行われる特恵 ECO の表記は英語に限定している。

日本－メキシコ間の協定においても、特恵原産地証明書は、英語で記述することを原則としている。ただし、英語以外の場合も許容しており、その場合には、輸入国の言語に合わせた翻訳文を添付することとしている。すなわち、輸入国が日本である場合には日本語、輸入国がメキシコの場合にはスペイン語である。

日本が特恵原産地証明書の対象国としてシンガポール、メキシコを想定した場合、英語のみを考慮すれば、実運用にも十分であるので、本ガイドラインでは、特恵原産地証明書を記載する文字コードは、1 バイトコードを利用することとした。

(5) 申請者の宣誓文に関する考察

日本－シンガポール間の協定において、特恵原産地証明書の必須記載事項として「申告者による申告（Declaration by the Exporter）が必須とされている。また、本項目は書面においては、特恵原産地証明書に定型文言として事前に印刷されている。

申請者の宣誓文は、交換されるデータの文脈を示すものであり、特恵原産地証明書が単独の文書として、転々流通する場合には必須である。なぜなら、文脈が設定されていないまま、電子署名だけが付与されていても、その電子署名が何についてを署名対象としているかが判断できないからである。具体的には、記述されている輸出や産品の内容について、「宣誓しているのか」、「聞いたことを記述しているのか」、あるいは、「否定しているのか」、といった判断材料を記載する必要がある。

ただし、特恵 ECO においては、交換されるデータの大きな文脈は、2 カ国間の協定で決められており、さらに、それに基づき実務レベルで協議され、同意書として取り留められることが想定されるので、この実務レベルの同意書において、「申請者が署名対象となっているデータに対して電子署名を付与した場合は、署名者が署名対象となっているデータが正しいことを宣誓しているものとみなす」等の条項が必要になる。

今回の特恵 ECO のフォーマットにおいては、申請者の宣誓文については、交換されるデータには含めないこととした。

(6) 署名者名

シンガポールが WCO に提示したフォーマットには、署名を行った特定個人の名前を示す入力フィールドは存在していなかった。署名を行う者の証明書には、

個人の特定が可能な氏名の入力フィールドが存在するが、署名を行う者の属性が使用される場合には（例えば商工会議所の所長という属性等）、個人を特定する氏名は用いられない。このためシンガポールとの会議にて、署名を行った特定個人名の入力フィールドを設ける旨の協議を行い、特恵 ECO に特定個人名の入力フィールドを設けることとした。

(7) 有効期限

書面の特恵原産地証明書には有効期限が記載されていないが、規約により日本の特恵原産地証明書の有効期限は発行日から 1 年間である。このため電子化された特恵 ECO についても有効期限の概念が必要とされる。

シンガポールと特恵 ECO のフォーマットを策定するにあたり、当初有効期限の項目は存在していなかったが、特恵 ECO に付与される署名・証明書には付与された日付情報が格納されており、この日付を特恵 ECO の発行日付と考え、システム側で有効期限を算出して運用することが協議された。

しかしながら、有効期限は特恵 ECO 発行国の発行機関がいつまでその発行責任を負うかが国によって違う可能性があること、および将来的に有効期限の期間が変更されても発行側システムが責任をもってその有効期限を格納することで受信国側に大きなシステム改変を発生させないという観点から、特恵 ECO のデータフォーマットに有効期限の項目を追加した。

(8) ORIGINAL フラグに関する考察

書面による特恵原産地証明書の場合には、使用される用紙、署名に使われるインクや筆跡により、原本とそのコピー機による複写を区別することが可能である。原本に”ORIGINAL”表示をすれば、複写にも “ ORIGINAL"と表記はされるものの、それがコピーであることは一目瞭然である。

しかしながら、電子データをコピーした場合、複写元のデータと複写先のデータには、まったく区別はなく、書面を前提とした場合のような “ ORIGINAL”の使い方は不可能である。

しかしながら、ビジネスにおいては、特恵原産地証明書のコピーを税関以外にも提出することがあるので、原本ではなく、「コピーとして流通している」ことを明示的に示すことに意味がある場合もある。

このような状況を想定して、データの項目として ORIGINAL や COPY についてのフラグを設けている。

(9) 添付ファイル

特恵原産地証明書を、税関に提出する場合、特恵原産地証明書は輸入申告書の添付書類として提出し、通常はインボイスのコピーも同時に要求される。このような状況を考慮すると、特恵原産地証明書と他の書類を関係付け、それらを１つのパッケージとして送付できる仕組みが必要になる。

特恵 ECO を相手国に送付する際に、特恵 ECO 以外の貿易文書情報が添付される場合の送付方法について３種類の案を検討した。

(a) XML データの中に格納する方式

XML データの中に添付ファイルを示すタグを作成し、そのタグの範囲に添付ファイルの内容をテキストデータのみに変換して格納する。特恵 ECO の XML と添付ファイルの送付イメージを「図 5.3　添付ファイルデータ格納方式」に示す。添付ファイルのデータも電子署名の対象となる。

(i) メリット

- 複数のファイルを 1 つのメッセージとして、送受信できるため管理が容易である

(ii) デメリット

- 複数のファイルが特恵 ECO を形成するため、本体のサイズが肥大する

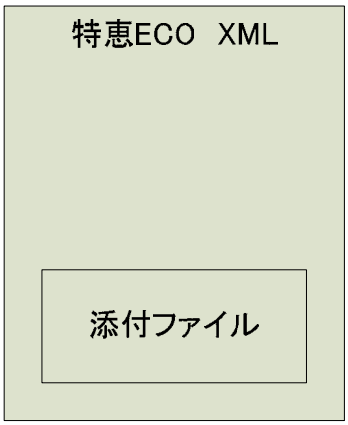

図 5.3　添付ファイルデータ格納方式

(b) XML データとは別の添付ファイルとする方式

特恵 ECO の XML とは別ファイルにて送信を行う方式である。

ただし、一般的な電子メールソフトウェアでは XML データとの関連付けができない。また、署名が付けられないため内容の保証もできない。

特恵 ECO の XML と添付ファイルの送付イメージを「図 5.4　添付ファイル別送付方式」に示す。

(i) メリット

・特恵 ECO 本体のサイズは肥大しない

(ii) デメリット

・特恵 ECO との関連付けができない

・添付ファイルに対して特恵 ECO と同レベルで保証ができない

図 5.4　添付ファイル別送付方式

(c) 添付ファイルのファイル名および添付ファイルのハッシュ値を特恵 ECO の XML 内部に格納し、ファイル本体との関連付けを行う方式

添付ファイルのハッシュ値を含むものが署名の対象となっており、添付ファイルも実質的に特恵 ECO の電子署名対象に含まれる。

特恵 ECO の XML と添付ファイルの送付イメージを「図 5.5　添付ファイル関連付け方式」に示す。

(i) メリット

・(a)と比較してファイルは分割されてしまうが、添付ファイルにも特恵 ECO の電子署名が有効でかつ特恵 ECO 本体のサイズは肥大しない

・(b)と比較して特恵 ECO との関連付けが可能となる

(ii) デメリット

・特に大きな問題は発生しない

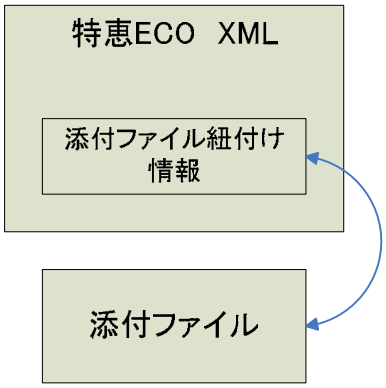

図 5.5　添付ファイル関連付け方式

本プロジェクトでは(c)の方式を採用した。

5.4.6 特恵 ECO プロトコル

本章では特恵 ECO を送受信する手段として必要となる通信プロトコルについて示す。

(1) 特恵 ECO プロトコルの要件

特恵 ECO は特定の貿易関係者間で取り交わされる機密情報であることから、特恵 ECO プロトコルに求められる要件は「真正性」「秘匿性」であり具体的には以下の内容を考慮する必要がある。

(a) 署名

なりすまし、改ざん等を防ぐために伝送時には電子署名を付与する。

(b) 暗号化

権限の無い第三者が参照できないように伝送時には暗号化する。

なお、特恵 ECO の記載情報は、関係者以外に知りえない機密情報である。

(2) 採用した通信プロトコル

本パイロットプロジェクトでは、S/MIME が通信プロトコルとして採用された。以下がその選択理由である。

(a) 広く普及しており、利用者人口が大きいことから利用者の使用に抵抗感が少ないと推測されること

(b) 暗号化が実装されており比較的簡単に利用できること

(c) 署名が簡単に付与できること

ただし、通信プロトコルについては「真正性」「秘匿性」が確保できるならば、他のプロトコルの採用でも問題ない。

また、電子メールソフトの仕様等により、送受信された特恵 ECO の XML に不要な改行が入る場合が考えられる。その際は正規化についての考慮、もしくは正規化が不要な状態での送受信を考慮する必要がある。

(3) メッセージフォーマット

(a) メッセージフォーマットについて検討した項目とその結果

(i) S/MIME におけるタイトル情報の利用

S/MIME は、メールの本文は暗号の対象となるが、タイトル等のヘッダ部分は暗号化の対象とはならない。

メール本文の内容を解読できなくても、ヘッダ部分に処理が必要な情報や機密度の低い情報を記述することにより、送受信管理の効率化を達成できる。

ヘッダのタイトルに設定する情報として、発行機関名、特恵 ECO 発行番号等を組み合わせる方式を採用した。

(ii) 配送先（輸入者）の電子メールアドレスの取得方法

特恵 ECO 内部に記述してある XML のデータ項目より取得するか、もしくは、タイトル等暗号化の対象とならない部分に記述する方法がある。

本パイロットプロジェクトでは、情報の漏えいを防ぐため、特恵 ECO の内部に記述してある輸入者のデータから送付先の電子メールアドレスを取得する方式を採用した。そのため、特恵 ECO フォーマットの輸入者情報において電子メールアドレスの記述は必須とした。

(iii) 複数アドレス同時配送について

到達確認を容易に行えるよう、本パイロットプロジェクトでは複数同時配送を行わない方式を採用。

(b) 採用されたメッセージフォーマット

検討の結果本パイロットプロジェクトにて採用されたメッセージフォーマットを以下に示す。

【Format：電子メール送信に関する規約】

・送信者（From）

送信者の電子メールアドレス

・受信者（To）

受信者の電子メールアドレス

複数アドレス同時配送は不可とする

・Cc

未使用

・Bcc

未使用

・Title

ヘッダのタイトルで ECO の内容が推測されないこと、および ECO の送信

であることを識別するために、以下のようにヘッダのタイトルのルールを作成する。

例）ヘッダのタイトルのルール

「国コード」+「送信先機関コード」+「特恵原産地証明書番号」

5.5　パイロットシステムの概要

本章では特恵 ECO の運用モデルについての検討内容、およびパイロットシステムの概要について示す。

5.5.1 運用モデル

特恵 ECO の運用モデルについて以下の 4 つのモデルについて検討を行った。

- 特恵 ECO データベース参照　2 カ国間利用者認証モデル
- 特恵 ECO データベース参照　第三者利用者認証モデル
- 特恵 ECO 持ち回りモデル（利用者間持ち回り）
- 特恵 ECO 持ち回りモデル（リポジトリ利用）

(1) 検討された運用モデル

(a) 特恵 ECO データベース参照　2 カ国間利用者認証モデル

電子文書による交換・検証モデルと書面運用が残ることを想定した、書面による輸入国への手続きの真正性向上のために輸入国から輸出国の特恵 ECO データベースを参照させるモデルを検討した。フロー図を「図 5.6　Case1：特恵原産地証明書フロー（書面運用モデル）」に示す。本運用では利用者認証に PKI 技術を活用することを想定した。

併せて Case2 として特恵 ECO を持ち回り、検証する方式についても検討を行った。フロー図を「図 5.7　Case2：特恵原産地証明書フロー（電子化モデル）」に示す。

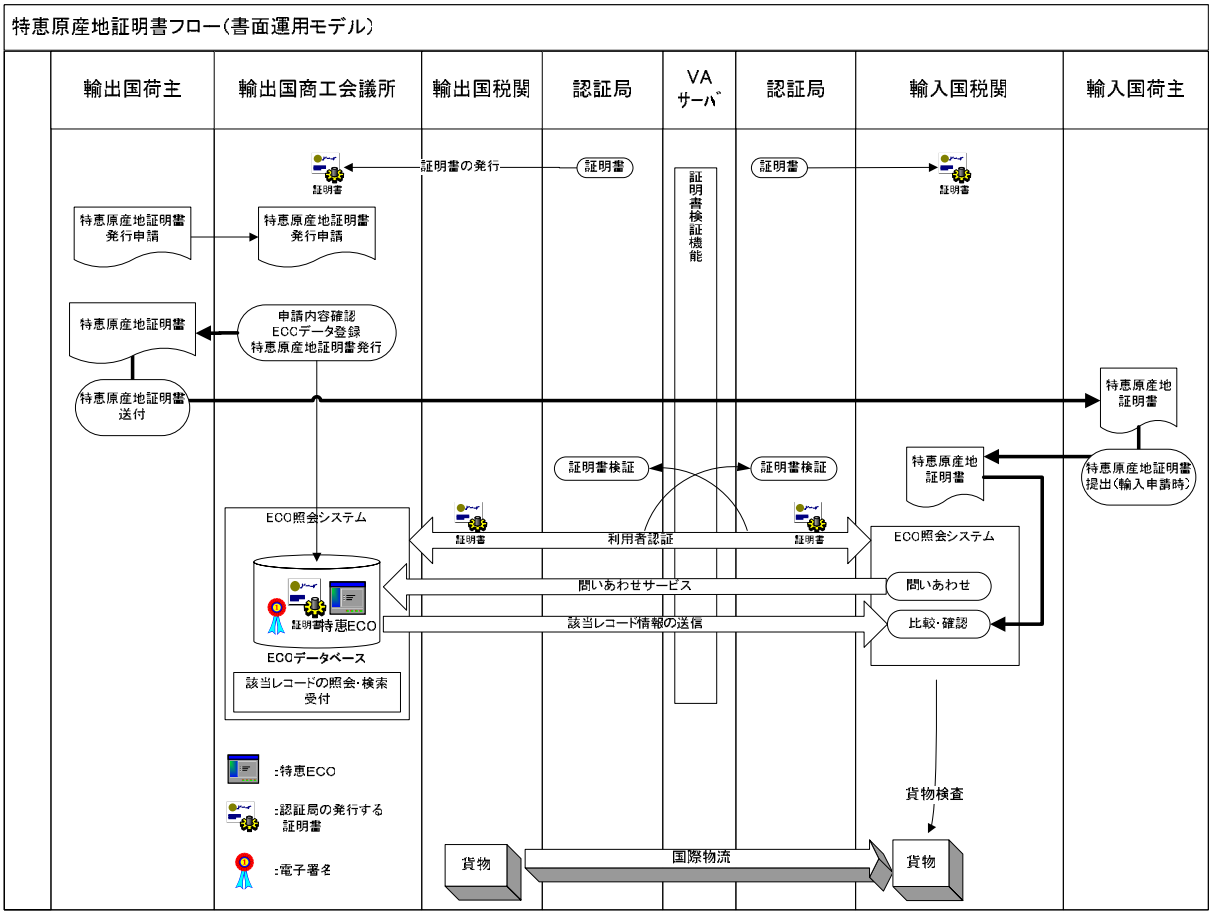

図 5.6　Case1：特恵原産地証明書フロー（書面運用モデル）

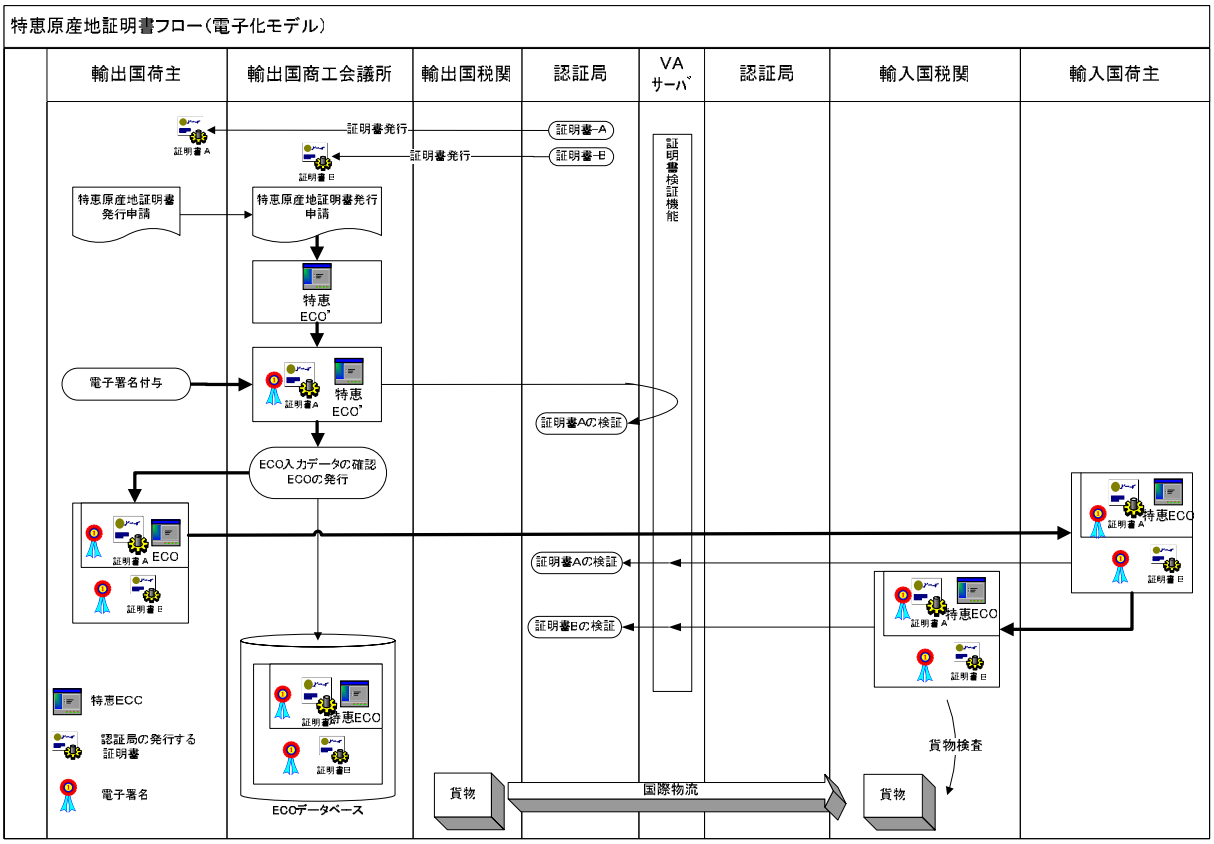

図 5.7　Case2：特恵原産地証明書フロー（電子化モデル）

輸出国側参照システムの利用者認証において PKI 技術を利用する。利用者認証時の証明書検証については次の３つのケースについて検討を行った。

- 輸出国の認証局が輸入国の利用者に証明書を発行するケース
- 輸入国で発行した証明書の真正性を利用者認証時に検証するケース
- 各国間でルールを決め、ルールに則った証明書であれば発行国に依存しないケース

(i) 利用者認証の仕組みについての検討

電子文書による交換･検証のケースについて利用者認証部分に PKI 技術を取り入れることを検討した。ここで、国際間の PKI 技術を用いた利用者認証方式について検討するにあたり、PKI に必要な証明書等を国際間の外交ルート等の場を用いて交換する方式が現実的な案であると想定し、検討を行った。

(ii) 認証方式についての検討

認証方式ついてセキュアチャネルの利用用途および利用頻度について複数のパターンについて考察を行った。

「表 5.1　認証方式一覧」に認証方式と特徴をまとめた一覧を示す。

表 5.1　認証方式一覧

	特徴	セキュアチャネルの利用用途	セキュアチャネルの利用頻度	備考
パターン 1	利用者登録 ･輸出国から輸入国利用者に証明書を発行	利用者ﾘｽﾄ 利用者の秘密鍵証明書	利用者の変更の度に証明書の交換が必要	
パターン 2	利用者登録 ･輸入国で発行した証明書を輸出国で利用	利用者の公開鍵証明書	利用者の変更の度に証明書の交換が必要	
パターン 3	利用する証明書のロール情報の取決め	認証局毎のロール情報	初回のみ	属性の取決めに調整が必要
パターン 4	利用者の登録権限者の取決め	利用者登録者の公開鍵証明書	頻度は少ないが登録者の変更の度に証明書の交換が必要	利用者に対する責任を認証局ではなく登録者が持つ
パターン 5	専用の認証局の取決め	認証局のセルフサイン証明書	初回のみ	新規認証局の構築のための調整が必要

パターン 1：輸入国より利用者のリストを入手し、輸出国側で証明書を発行する。利用者を輸出国側で容易に管理できるので、仕組みとしては国内向けの作りと同等となる。輸入国側の利用者は変更があるたびにそのリストを輸出国へ通知し、その後証明書を発行してもらうために、利用者の更新頻度が高い場合運用が回らない可能性がある。運用フローを「図 5.8　利用者認証方式パターン 1」に示す。

パターン 2：輸入国の利用者に輸入国で証明書を発行し、その証明書を輸出国へ通知する方式。このパターンの場合、入手した証明書を検証可能なシステムの構築が必要であることと、パターン 1 程ではないが、利用者の

更新頻度が高いケースでは運用の負荷が高くなる。運用フローを「図 5.9　利用者認証方式パターン 2」に示す。

パターン 3：利用する証明書のロール情報を取り決めることにより、その取決めに従った証明書であれば、利用者認証を可能とする方式。取決めの調整とシステムへの対応が必要であるが、ルールが決まれば利用者の更新があった場合でも特別な運用が不要となる。運用フローを「図 5.10 利用者認証方式パターン 3」に示す。

パターン 4：パターン 2 では利用者を保証するものは利用者の証明書を発行した認証局であるが、パターン 4 は、利用者の責任を登録者が負うという方式である。認証局ではなく登録を行う関係者が責任を持つという点に違いがある。責任範囲の他に、更新頻度も利用者の更新単位から登録者の更新単位となることから運用負荷は軽減される。運用フローを「図 5.11　利用者認証方式パターン 4」に示す。

パターン 5：それぞれの国で専用の認証局を取り決める方式。特定の認証局であれば信頼するため、仕組みはシンプルであるが、新規の認証局を構築する必要があり、初期の準備作業の負荷が大きくなる。運用フローを「図 5.12　利用者認証方式パターン 5」に示す。

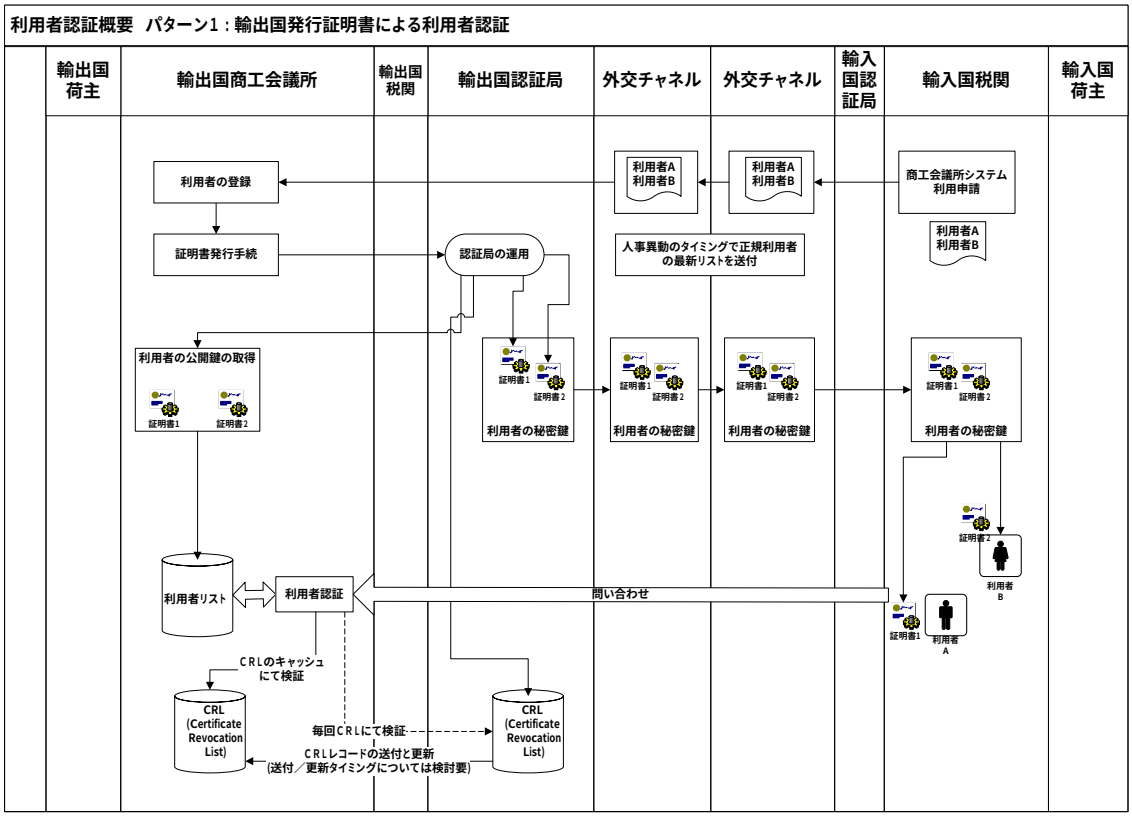

図 5.8　利用者認証方式パターン 1

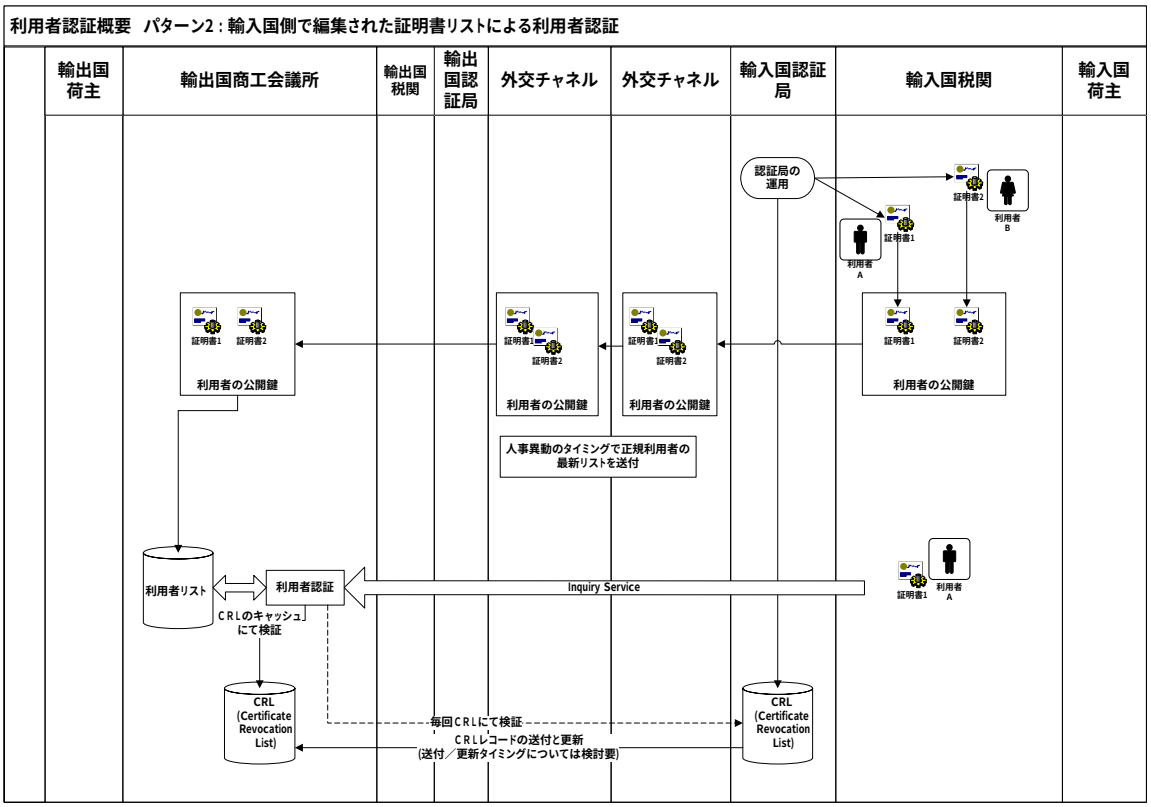

図 5.9　利用者認証方式パターン 2

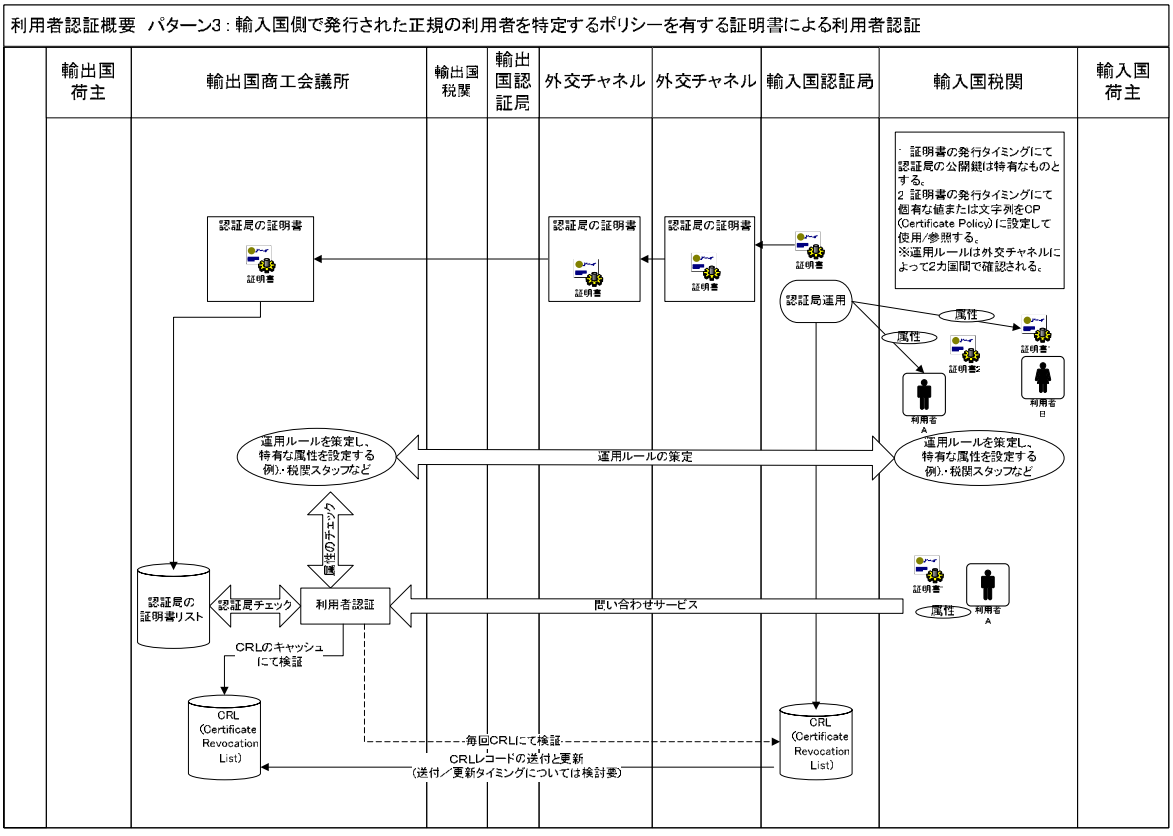

図 5.10　利用者認証方式パターン 3

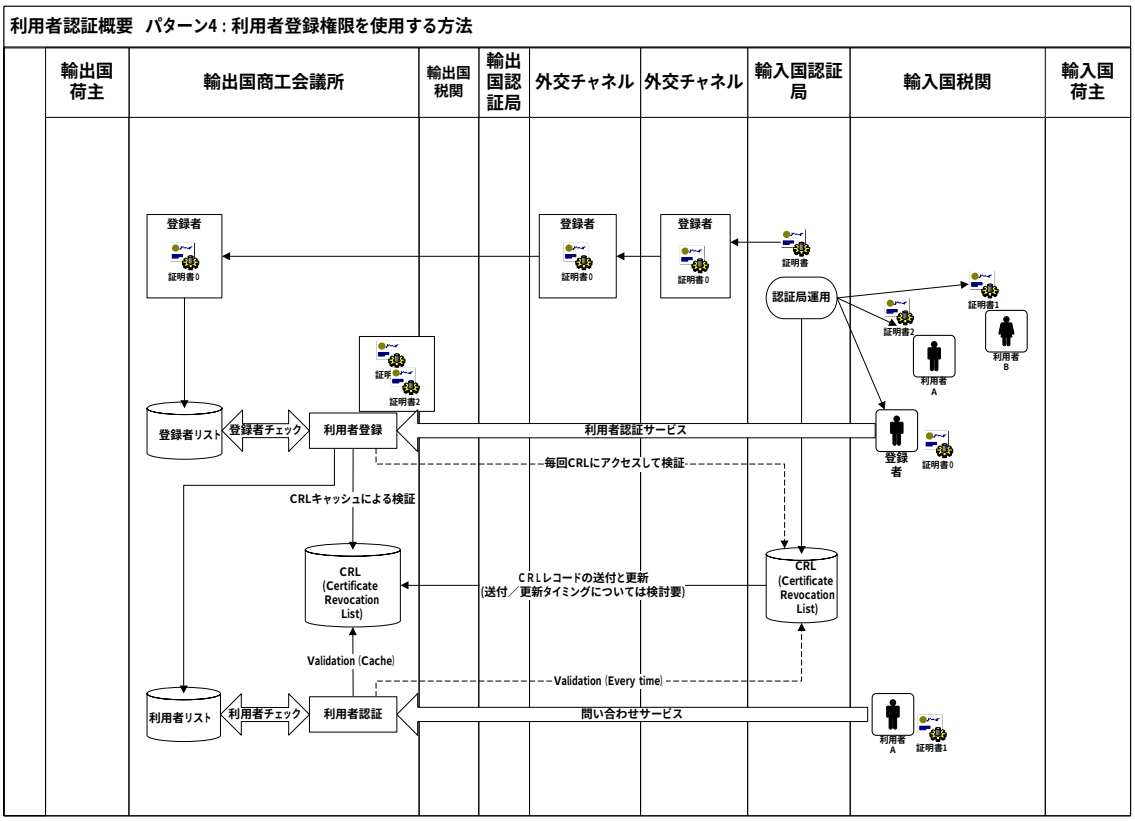

図 5.11　利用者認証方式パターン 4

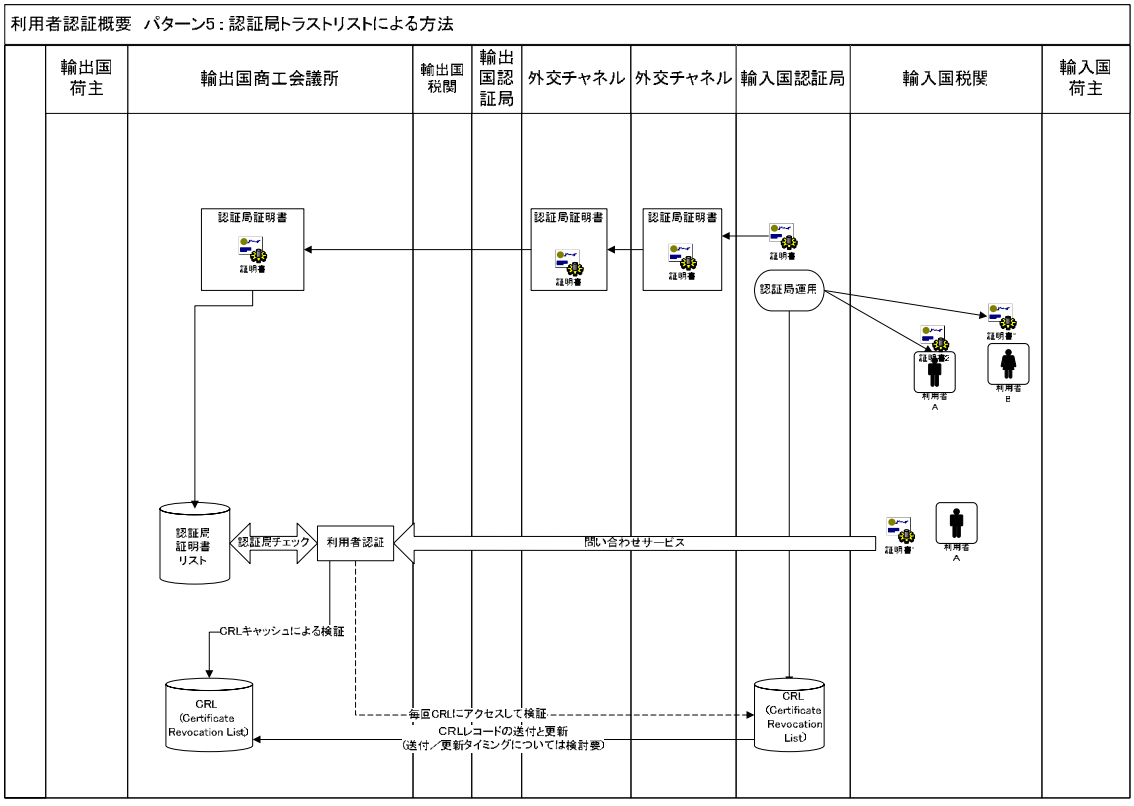

図 5.12　利用者認証方式パターン 5

(b) 特恵 ECO データベース参照　第三者利用者認証モデル

利用者認証の仕組みを第三者の機関が運営する方式。

「図 5.13　利用者の証明書を交換」には特恵 ECO の発行に係る利用者の証明書を予め登録する方式を示す。

このケースでは、利用者に変更が生じる毎に第三者機関に利用者情報の更新を行う必要がある。

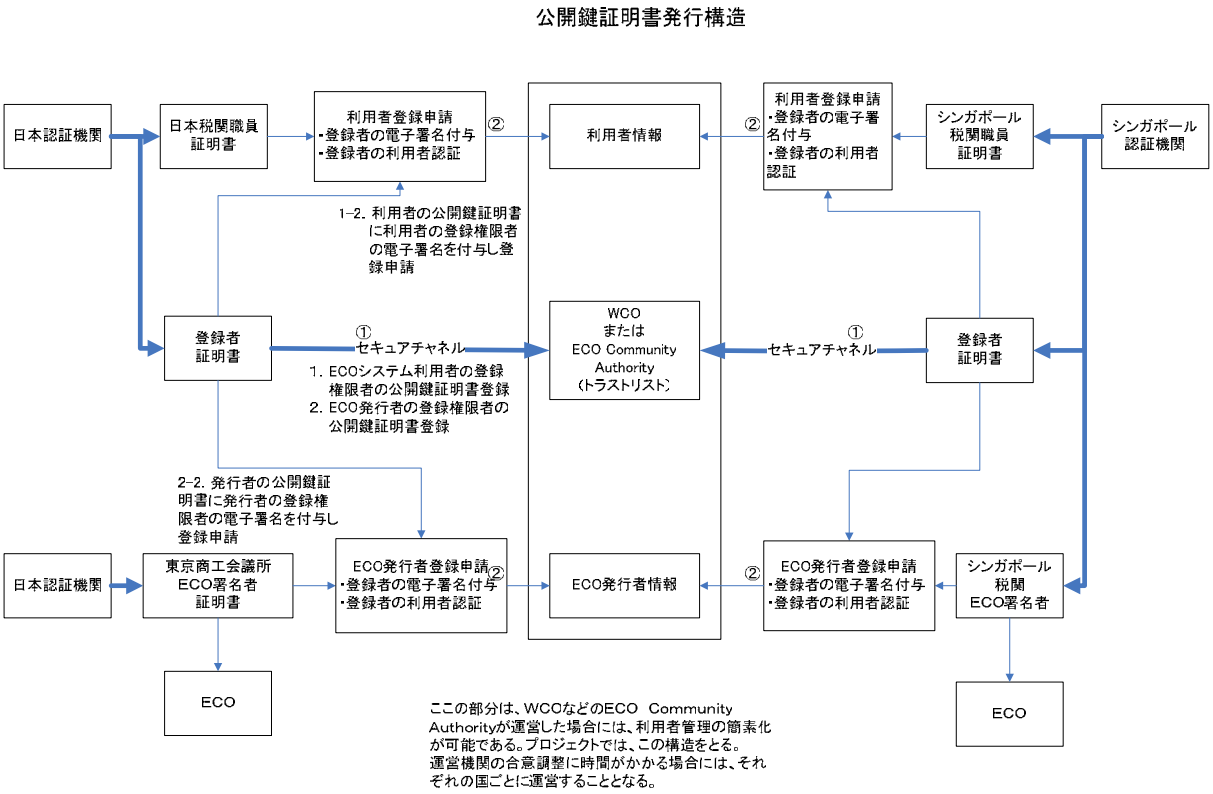

図 5.13　利用者の証明書を交換

「図 5.14　利用者の証明書の属性を交換」は利用者の証明書そのものではなく、利用者として認められる属性の登録を第三者機関へ行うものである。

本ケースでは、利用者として認められる証明書のルールを決めることで、基本的に第三者機関への登録は初回の１回のみとなり、利用者自体の更新の際はそれぞれの国内で証明書を管理すればよいため、前述のケースよりも利用者更新に係る運用が簡易になる。

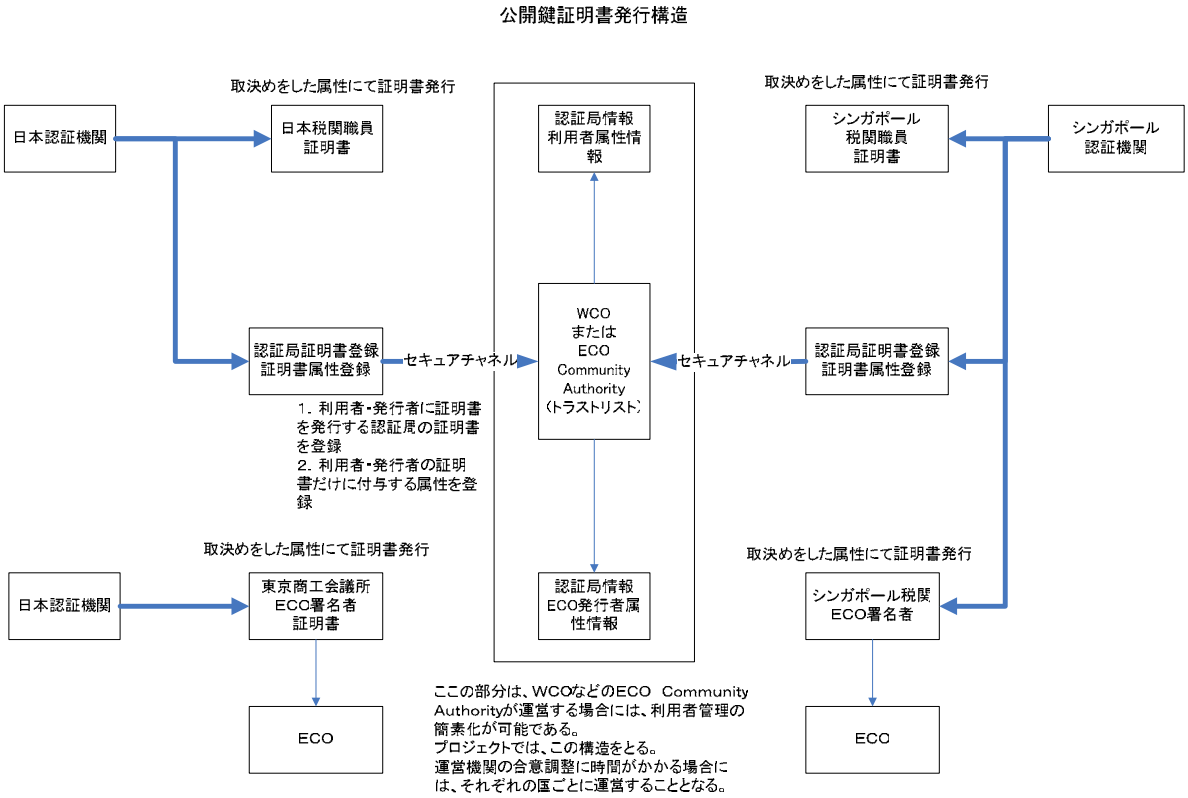

図 5.14　利用者の証明書の属性を交換

「図 5.15　利用者検証」に正規の利用者であることを検証する流れを示す。

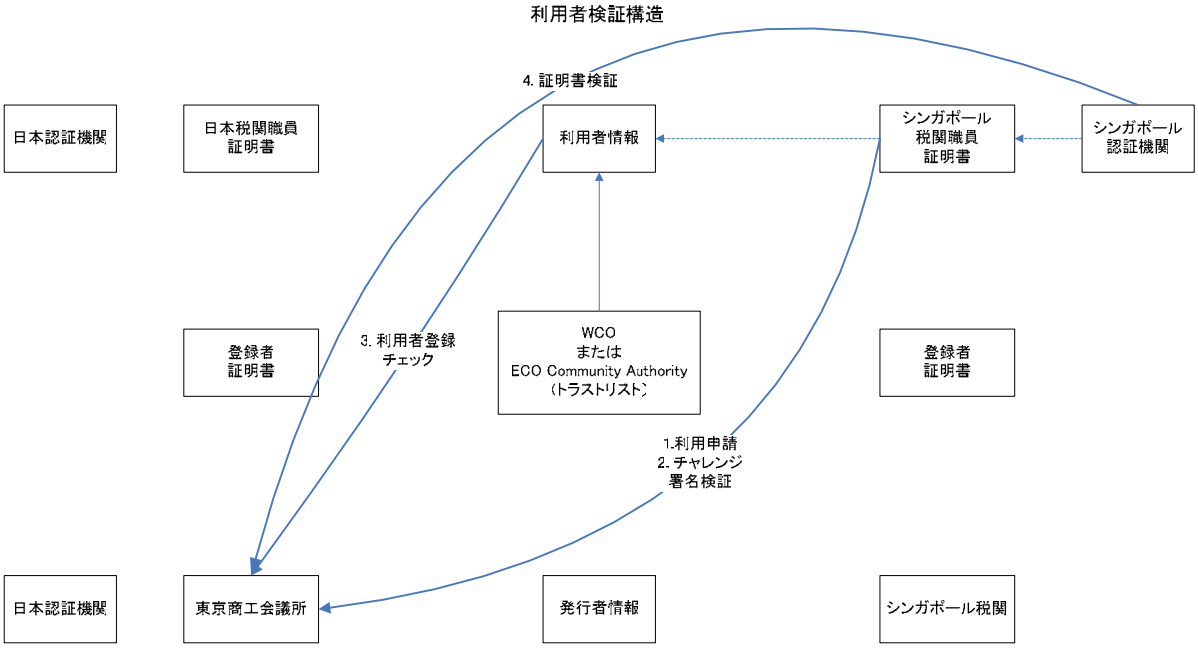

図 5.15　利用者検証

「図 5.16　特恵 ECO 検証」に特恵 ECO 自体を検証する流れを示す。

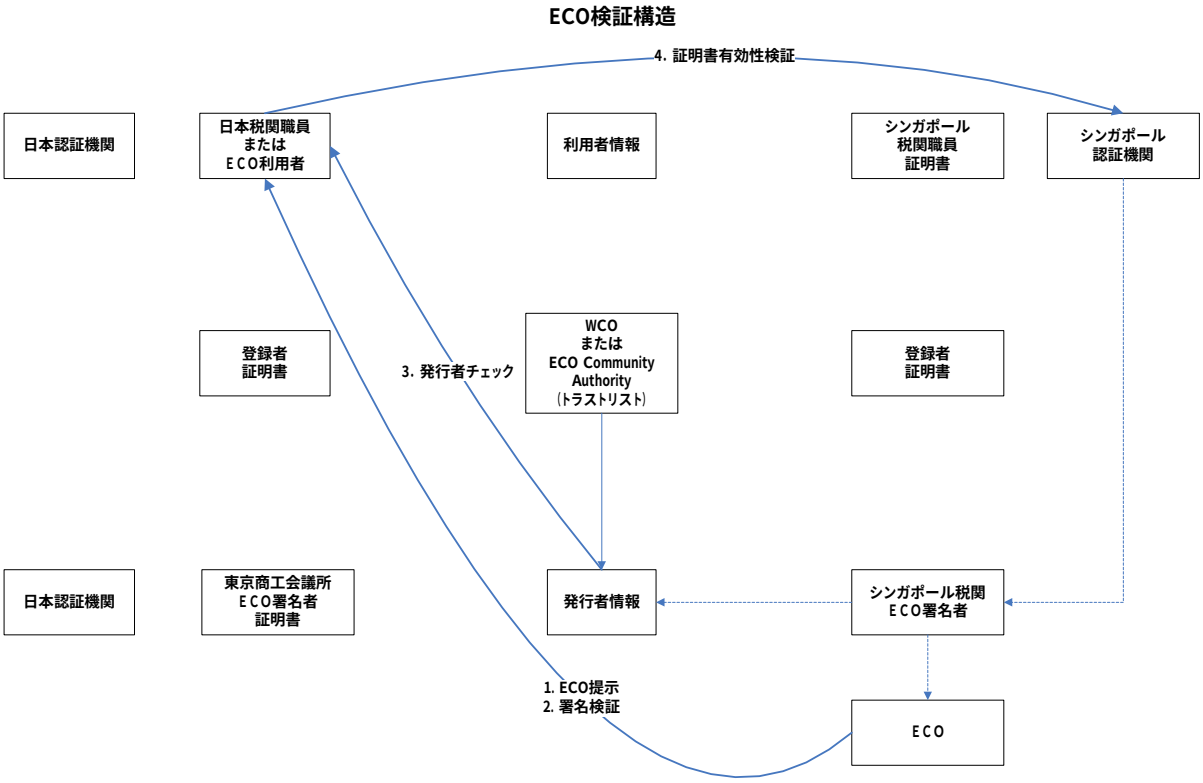

図 5.16　特恵 ECO 検証

「図 5.11　利用者認証方式パターン 4」で示した運用フローに第三者機関による利用者認証の仕組みを取り入れると「図 5.17　利用者認証方式パターン 4'」のように運用が簡略化される。国際間にまたがる第三者機関の調整が課題であるが、実現すれば運用は簡略化されると考えられる。

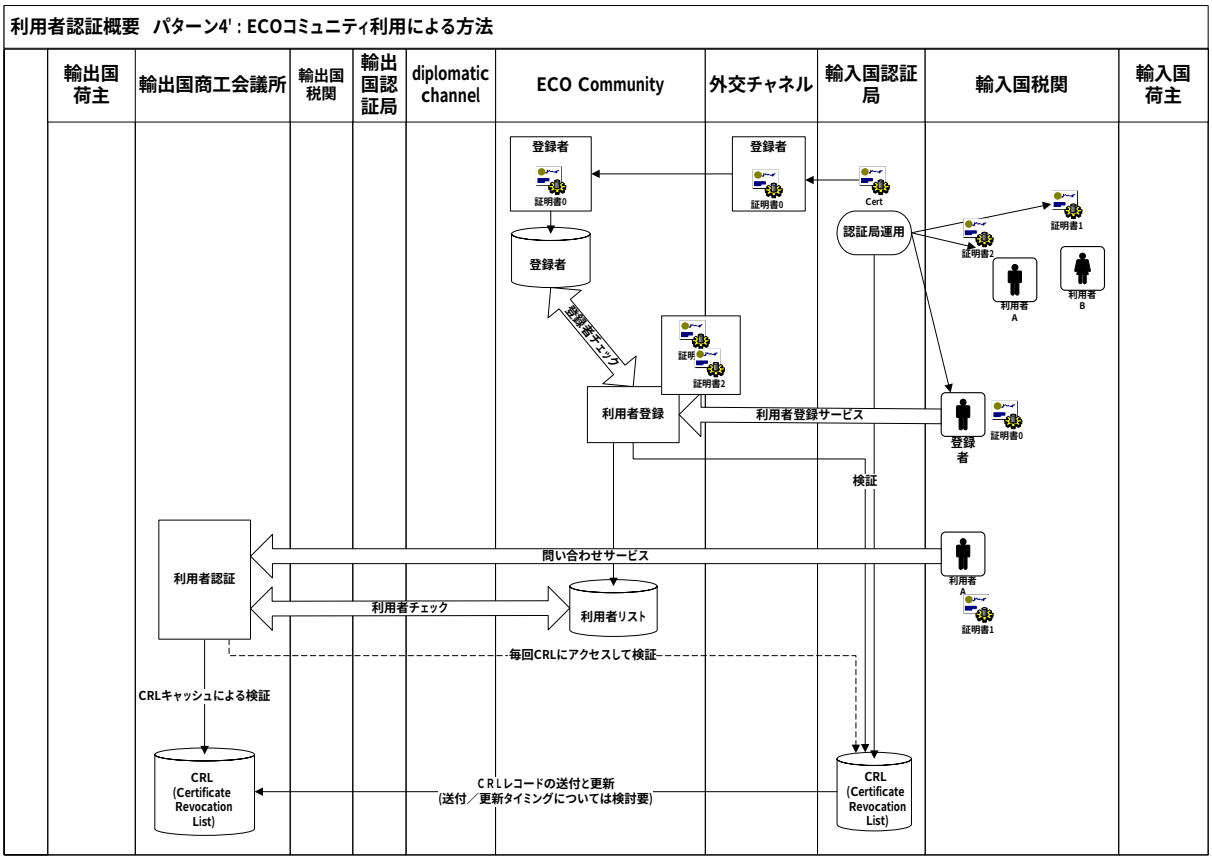

図 5.17　利用者認証方式パターン 4'

(c) 特恵 ECO 持ち回りモデル（利用者間持ち回り）

特恵 ECO の運用と書面による運用時の書面の真正性を確保するための方法（利用者認証を使用）について検討された運用フローを示す。

「図 5.18　特恵 ECO 発行」に本プロジェクトにおける日本側の特恵原産地証明書の発行までの仕組みを示す。

「図 5.19　書面特恵原産地証明書持ち回りモデル：日本→シンガポール」に日本からシンガポールへ書面による特恵原産地証明書を持ち回る運用フローを示す。

「図 5.20　特恵 ECO 持ち回りモデル」は特恵 ECO 自体を持ち回る将来的な実装モデルとして検討を行った運用モデルである。

「図 5.21　書面特恵原産地証明書持ち回りモデル：シンガポール→日本」はシンガポールから日本へ書面による特恵原産地証明書を持ち回る運用フローを示す。

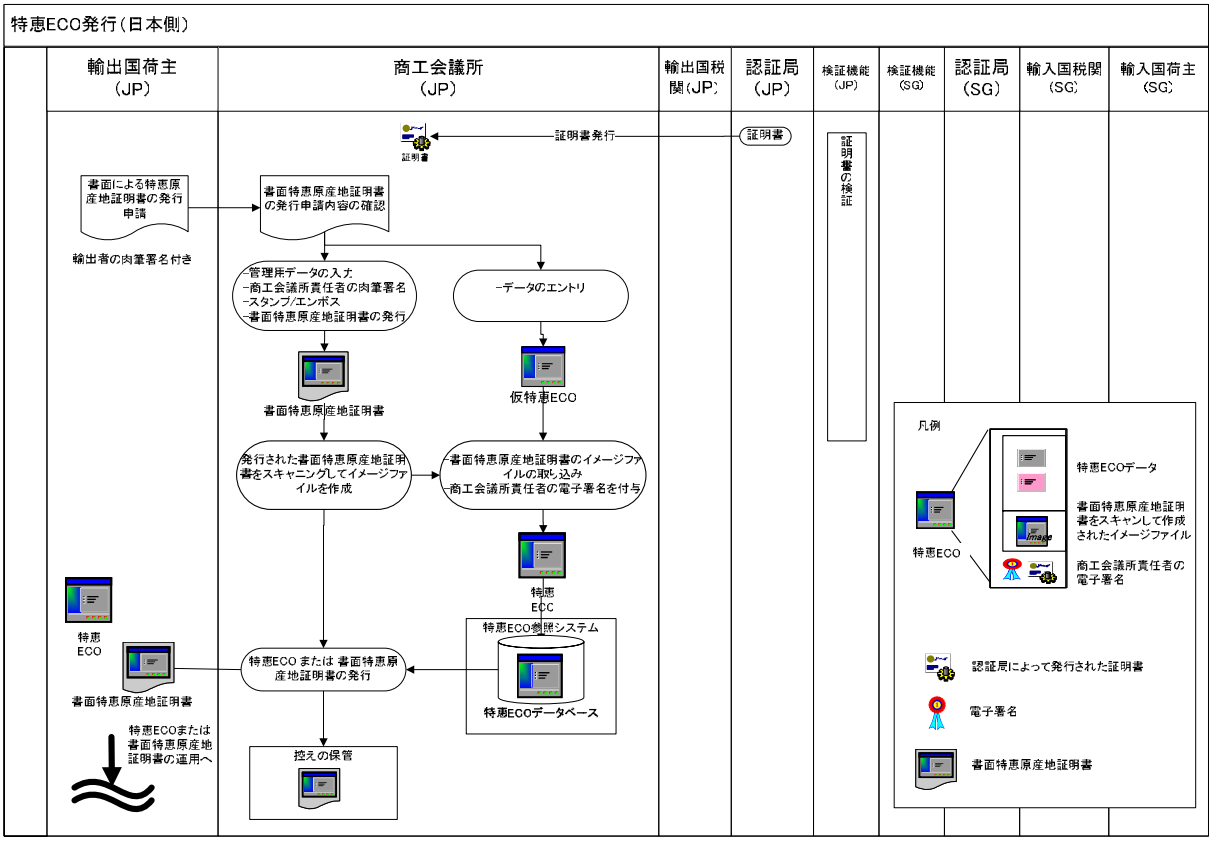

図 5.18　特恵 ECO 発行

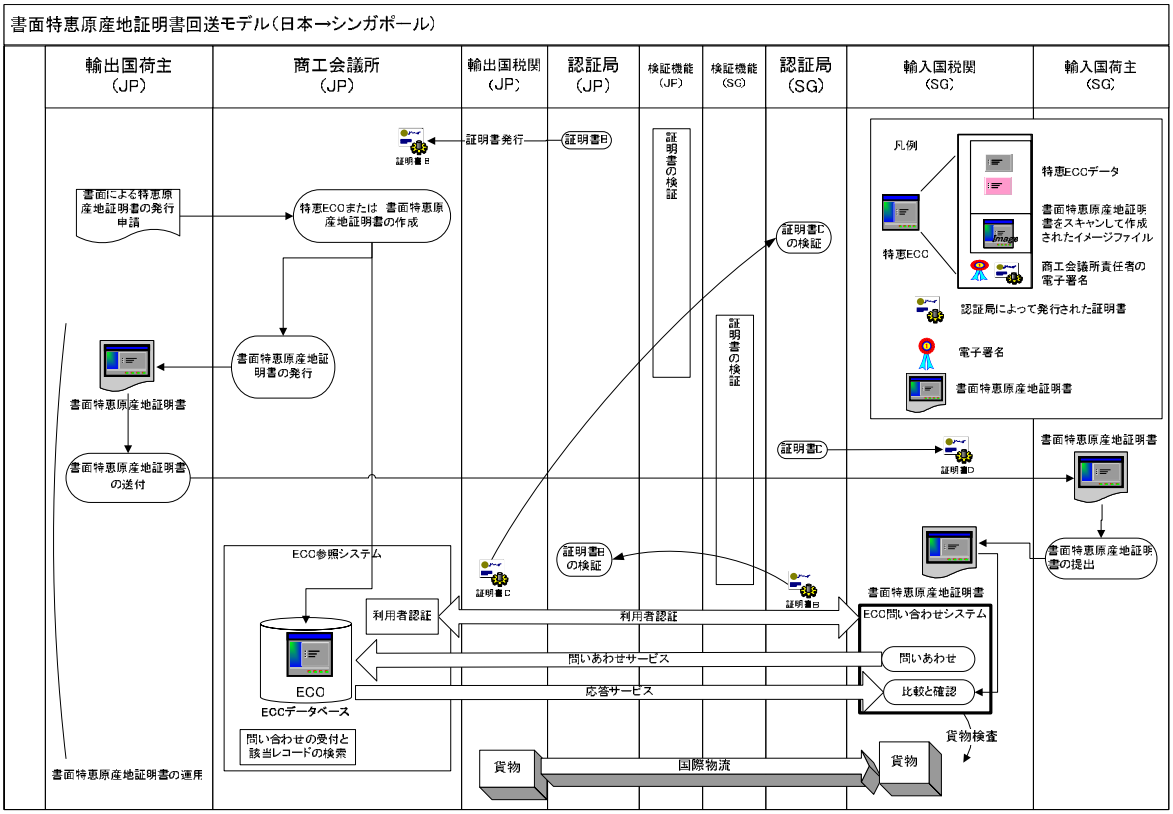

図 5.19　書面特恵原産地証明書持ち回りモデル：日本→シンガポール

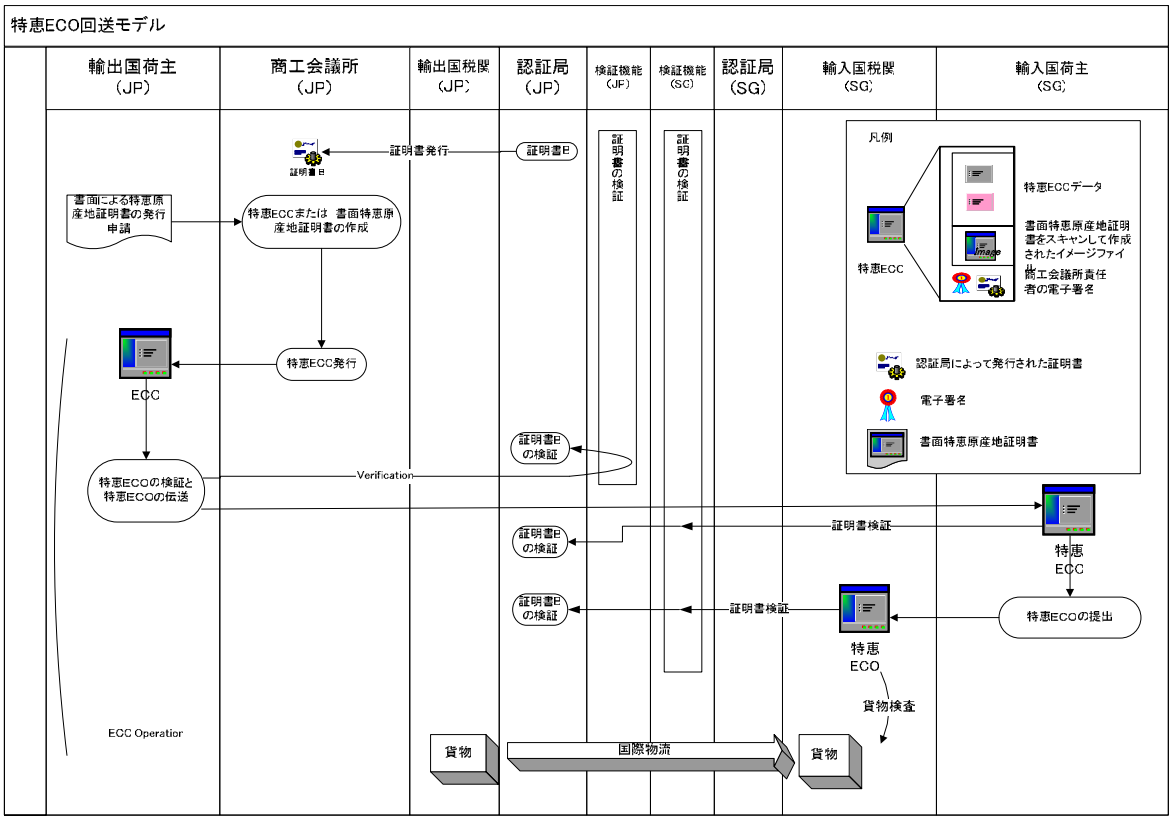

図 5.20　特恵 ECO 持ち回りモデル

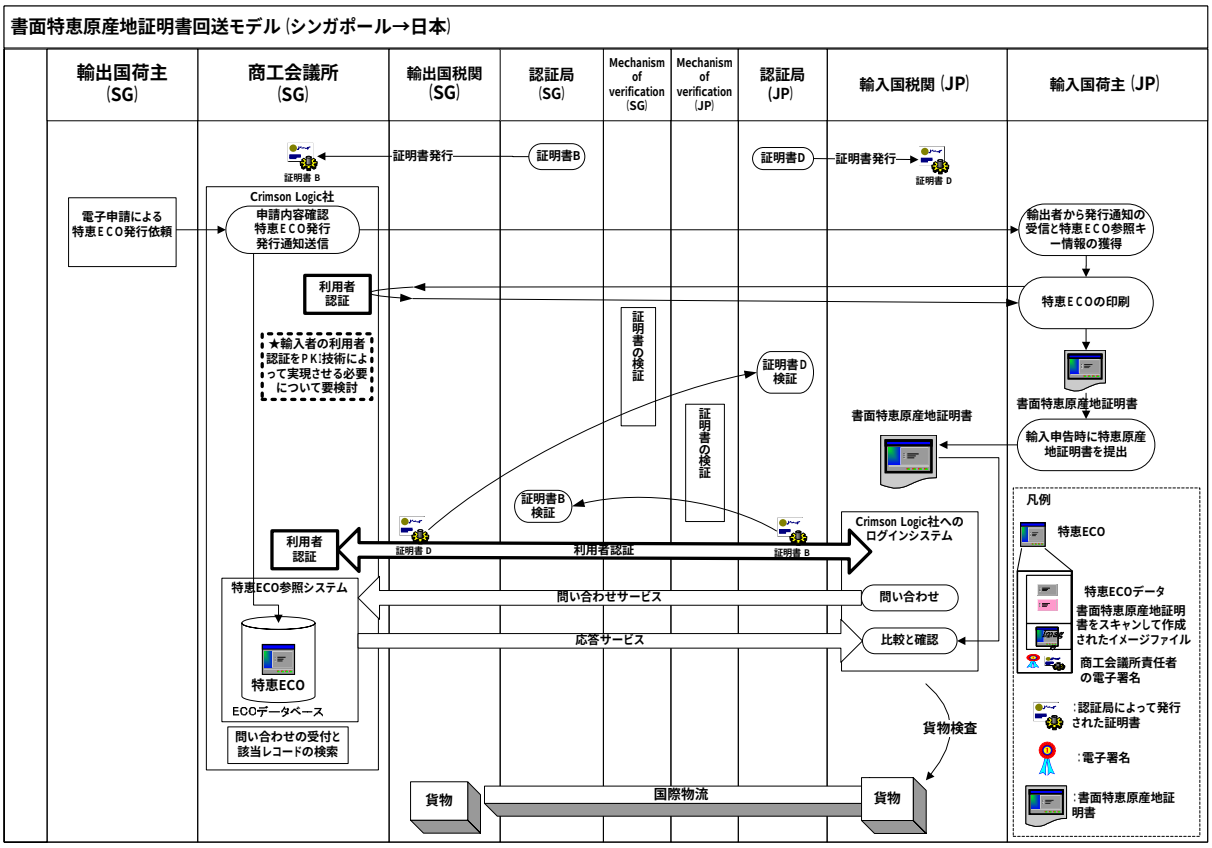

図 5.21　書面特恵原産地証明書持ち回りモデル：シンガポール→日本

(i) 署名運用について

特恵 ECO の署名モデルについて「図 5.22　特恵 ECO の署名運用」に示す。

本パイロットプロジェクトで検討した特恵 ECO フォーマットでは輸出者、特恵 ECO 発行機関、輸出国大使館等の署名を付与する可能性を考慮し、輸入者および輸入国の税関にてそれらの署名を検証可能なモデルとした。

本パイロット実験では特恵 ECO 発行機関の署名のみを必須とし、国際間のやり取りに重きを置いた実験としている。なお、輸出者の署名に関しては、電子署名は付与しないが、特恵 ECO の中に輸出者の情報が記載され、それを ECO 発行機関が保証し署名をすることで、運用上特に問題は発生しないと考えられる。大使館の署名に関しては、各国の運用ケースにより発行機関以外の署名が必要になる場合を想定したものであり、任意の項目としている。

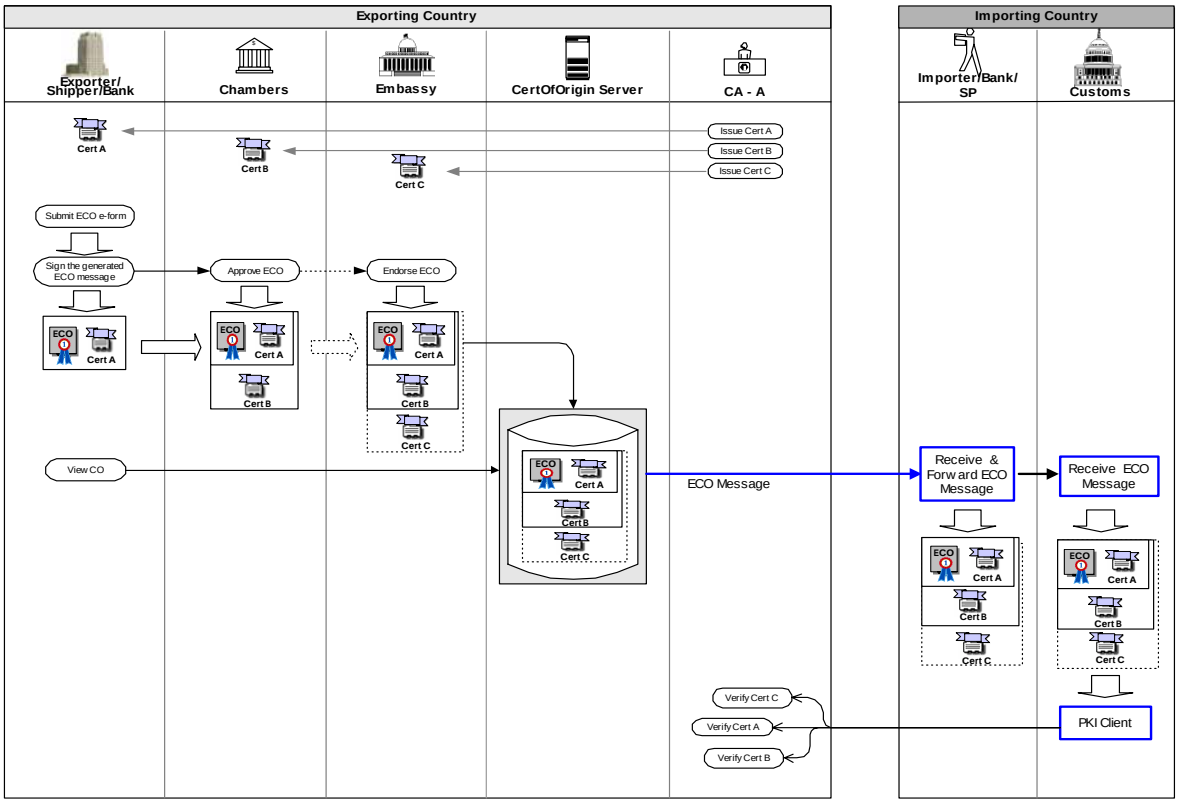

図 5.22　特恵 ECO の署名運用

(d) 特恵 ECO 持ち回りモデル（リポジトリ利用）

ECO を相手国側リポジトリ（このリポジトリという言葉は正規の受信者という意味で使用：日本国での CrimsonLogic 社のようなサービスプロバイダや税関輸入者を指す）に対して送付するケース。

案１、2 の利用者認証モデルのように仕組みが煩雑でないこと、輸入国から DB を参照させることのセキュリティ上の不安感からこのモデルを検討した。

本パイロットプロジェクトでは本モデルを採用し、対シンガポールとの実験において特恵 ECO のみの運用を検証。対仮想対象国との実験において書面による運用についての検証を行った。

(i) 特恵 ECO 運用（シンガポール→日本）

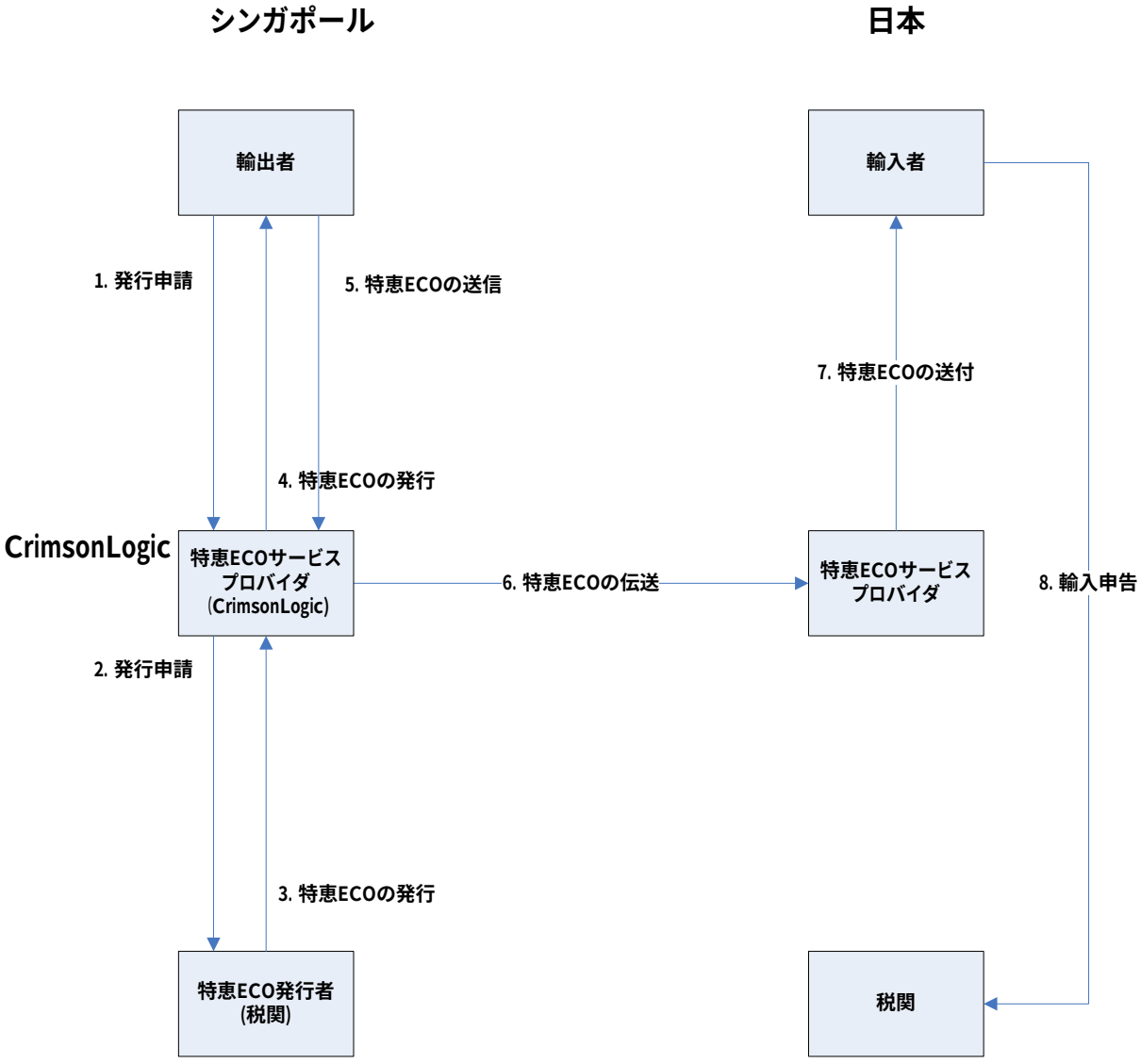

図 5.23　特恵 ECO 運用図（シンガポール→日本）

「図 5.23　特恵 ECO 運用図（シンガポール→日本）」のモデルは輸出者が ECO サービスプロバイダで特恵 ECO の申請を行い特恵 ECO が特恵 ECO

発行機関によって発行される。発行された特恵 ECO はサービスプロバイダの 1 機能として輸入国のサービスプロバイダへ送信され、輸入国のサービスプロバイダにより輸入者へ配送される。本モデルの運用フローを「図 5.24 特恵 ECO 運用フロー（シンガポール→日本)」に示す。

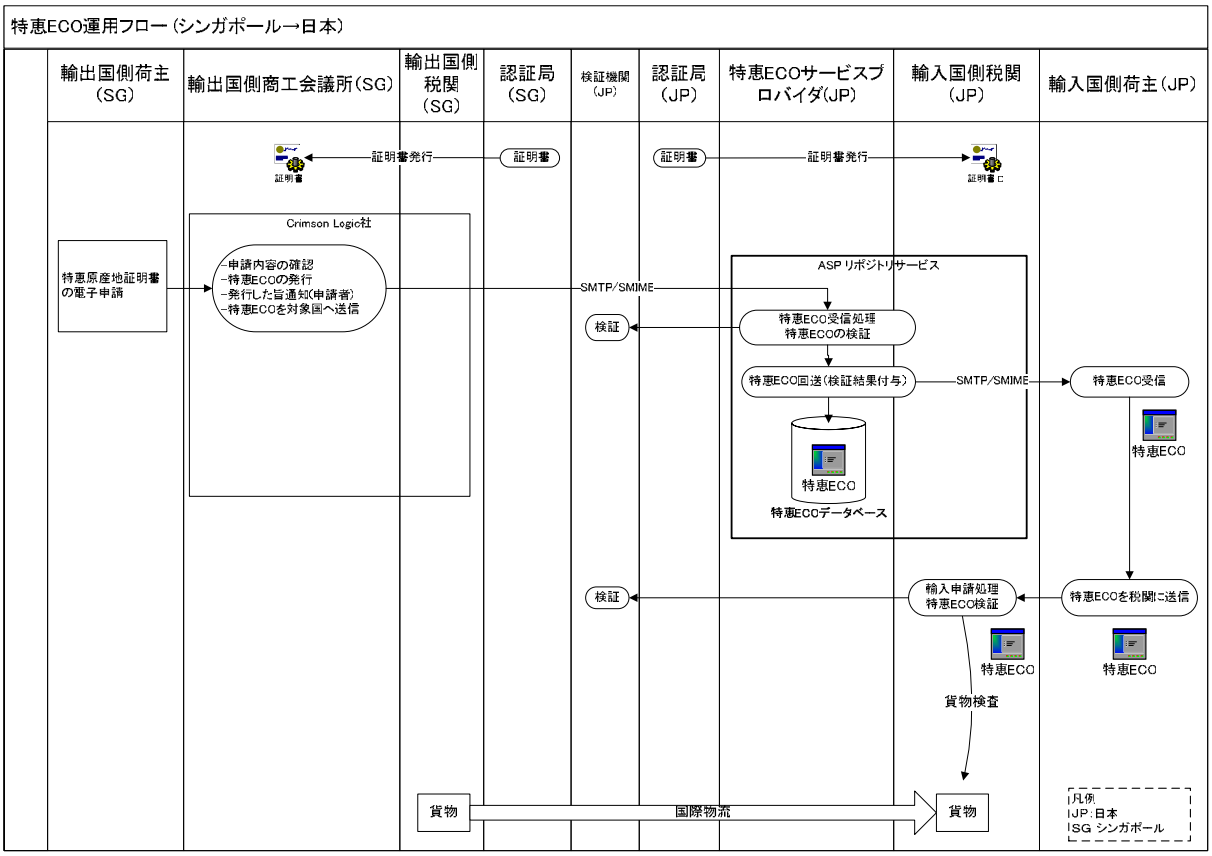

図 5.24　特恵 ECO 運用フロー（シンガポール→日本）

(ii) 書面特恵原産地証明書運用（シンガポール→日本）

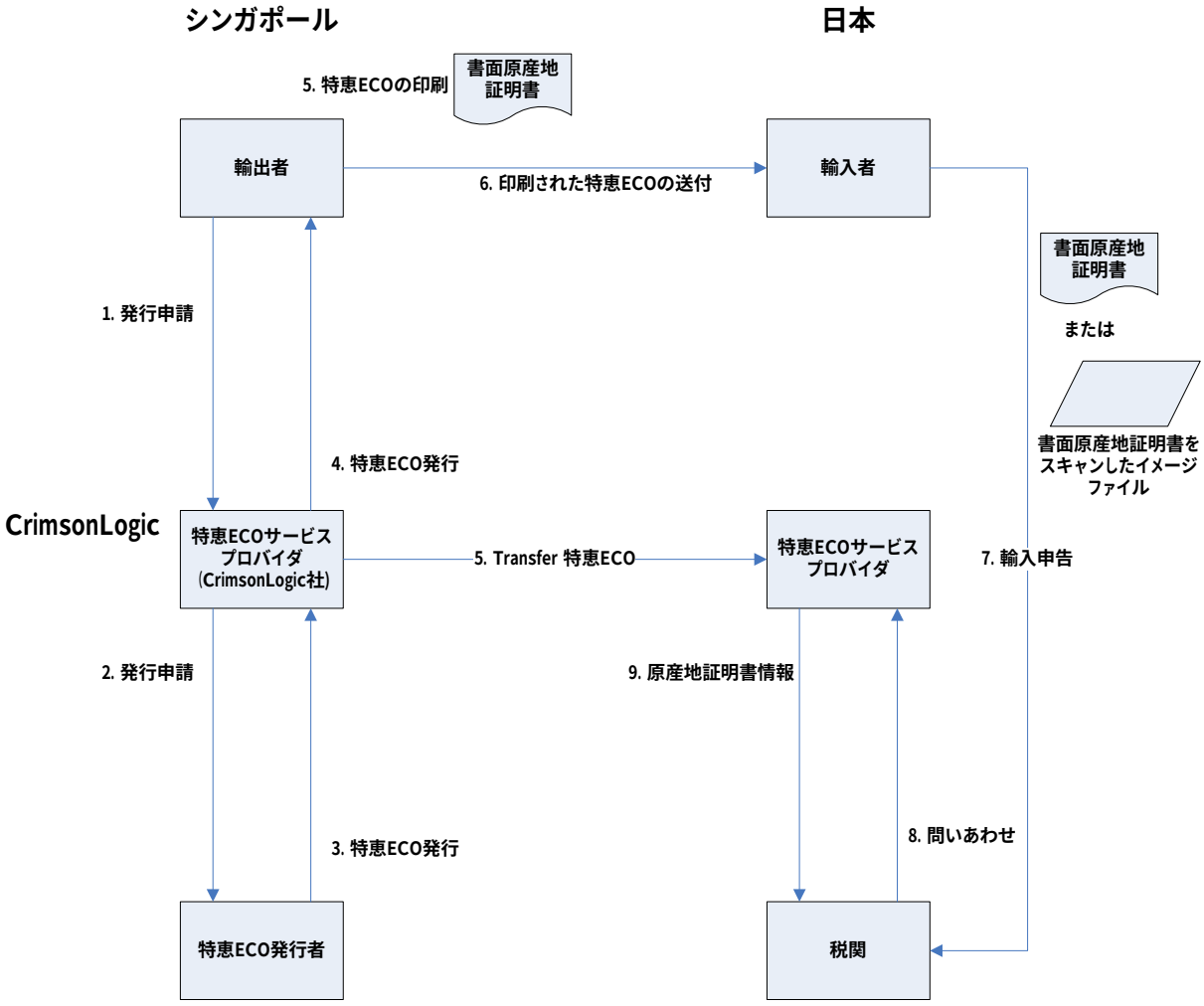

図 5.25　書面特恵原産地証明書運用図（シンガポール→日本）

「図 5.25　書面特恵原産地証明書運用図（シンガポール→日本）」のモデルは発行された特恵 ECO の書面出力を行い、輸出者から輸入者への持ち回りは書面にて行うモデルとなる。これは、輸入者に ECO サービスプロバイダとアクセスする環境が無い場合等を想定している。運用は現行の書面運用に近いものであるが、輸入国にも ECO サービスプロバイダを構築し、税関向けに実際に発行された特恵 ECO を公開することで、扱われた特恵原産地証明書が本物であることを確認できる仕組みとなる。本モデルの運用フローを「図 5.26　書面特恵原産地証明書運用フロー（シンガポール→日本）」に示す。

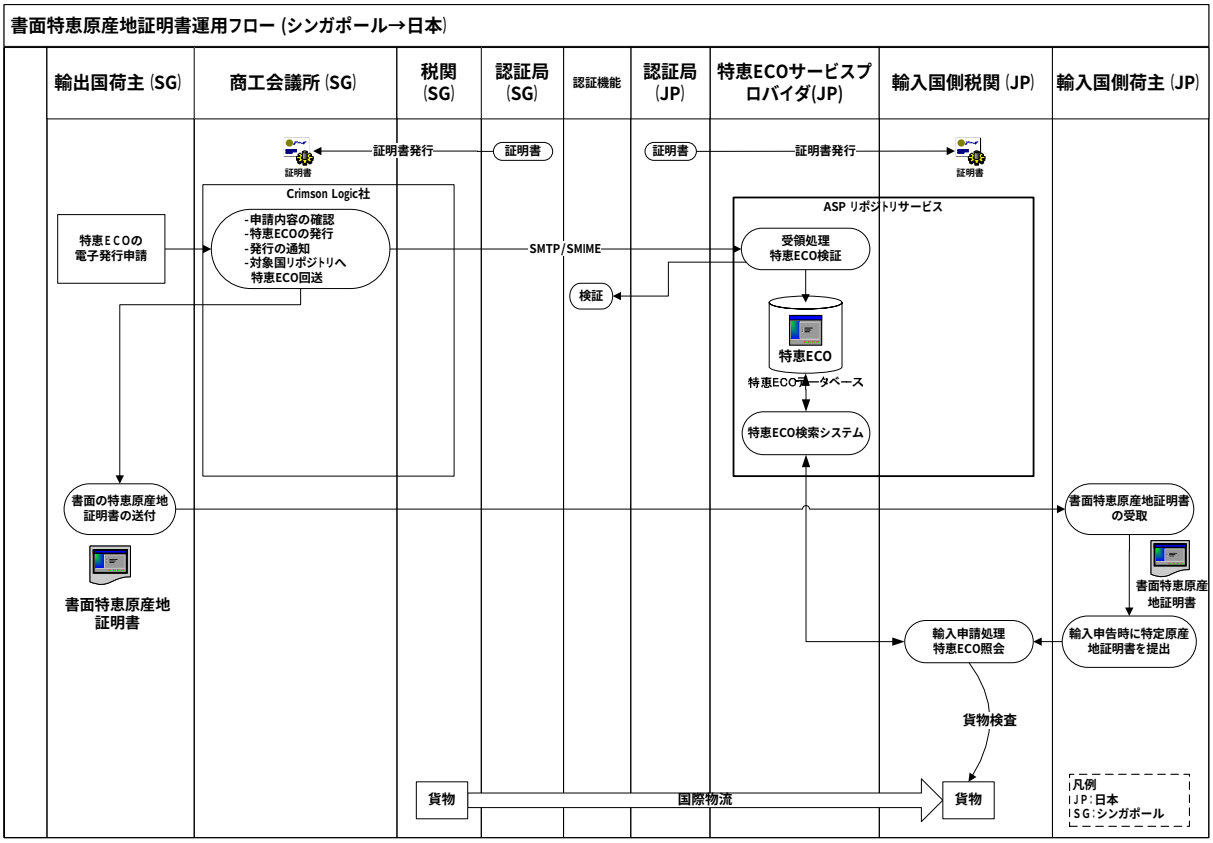

図 5.26　書面特恵原産地証明書運用フロー（シンガポール→日本）

(iii) 特恵 ECO 運用（日本→シンガポール）

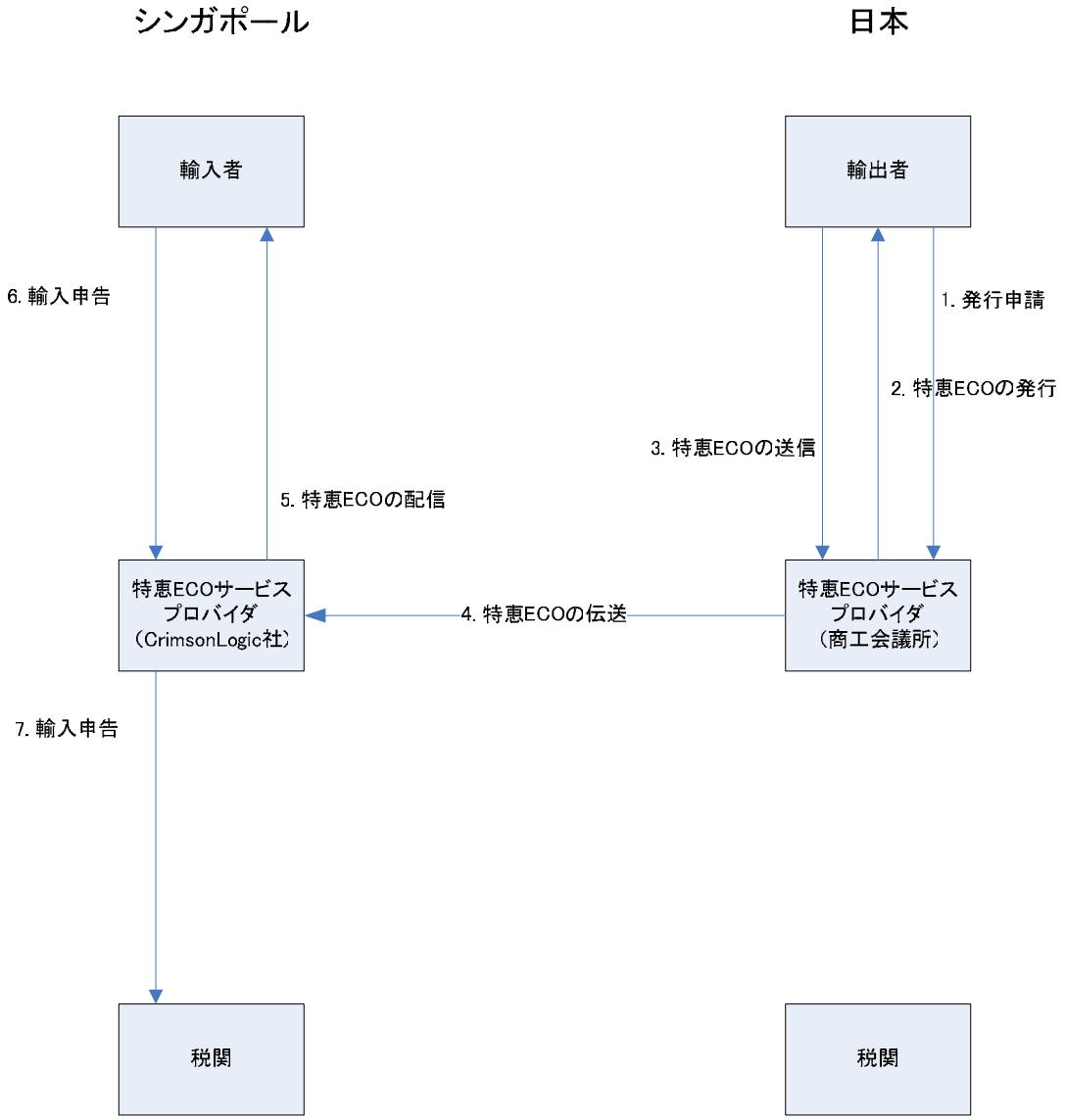

図 5.27　特恵 ECO 運用図（日本→シンガポール）

「図 5.27　特恵 ECO 運用図(日本→シンガポール)」のモデルは特恵 ECO を持ち回る「図 5.23　特恵 ECO 運用図（シンガポール→日本)」パターンとほぼ同様であり、日本からシンガポールへ輸出するケースである。異なる点は、シンガポールの特恵 ECO 発行機関が税関であり、日本が商工会議所であることから税関との関連が異なっている。また、日本が輸入の場合は輸入者が税関に特恵 ECO を持ち込むとしているが、シンガポール側は輸入者および税関職員が同一のサービスプロバイダを想定していることから、システム内での受け渡しモデルとしている箇所が異なる点である。本モデルの運用フローを「図 5.28　特恵 ECO 運用フロー（日本→シンガポール)」に示す。

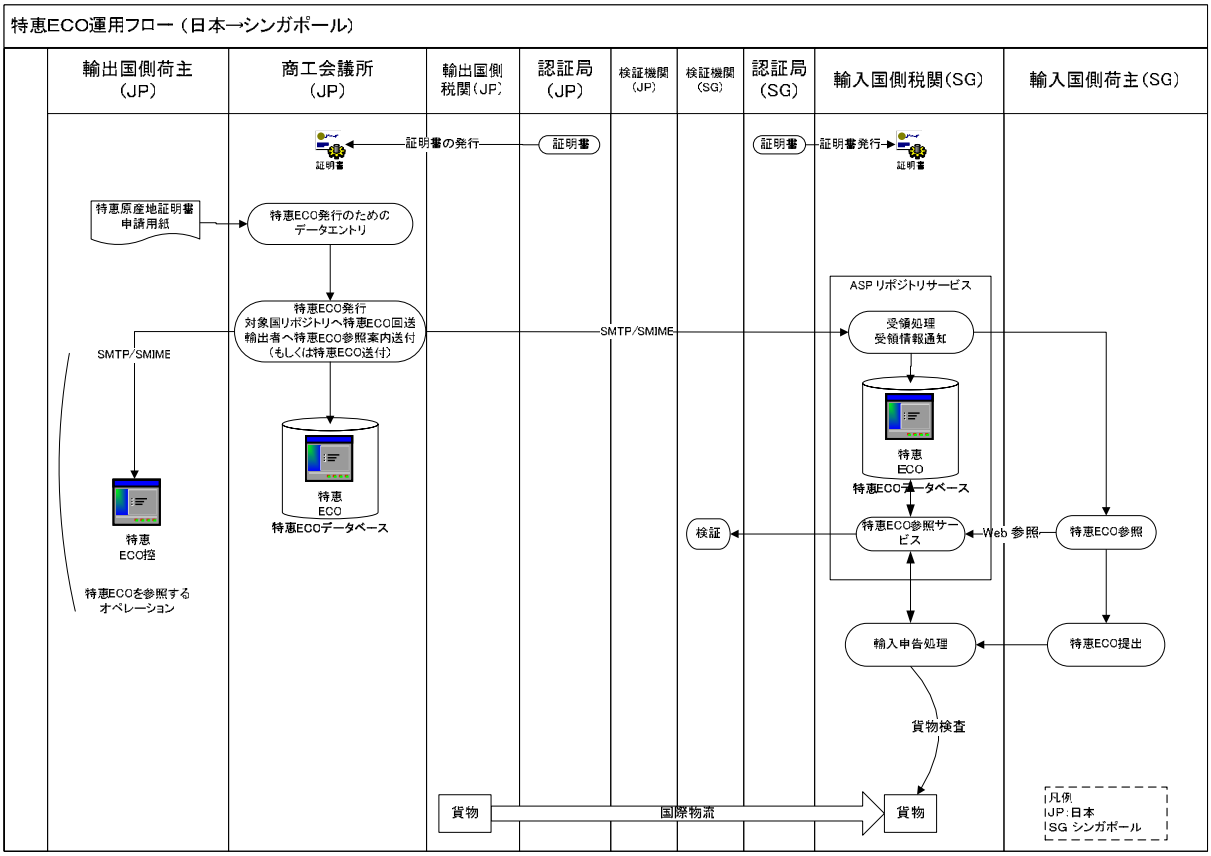

図 5.28　特恵 ECO 運用フロー（日本→シンガポール）

(iv) 書面特恵原産地証明書運用（仮想対象国→日本）

「図 5.29　書面特恵原産地証明書運用図(仮想対象国→日本)」～「図 5.32 書面特恵原産地証明書運用フロー（日本→仮想対象国)」は仮想対象国を想定した書面運用ベースの特恵原産地証明書の真正性を確保する方式である。この方法は現行の書面運用は基本的にそのまま残し、書面にて完成された特恵原産地証明書をシステムにイメージ取込を行い、そのイメージ情報を輸入国税関へ公開する方式である。これにより、電子化への移行期間や、書面運用を継続する必要がある場合の真正性の確保が可能となる。

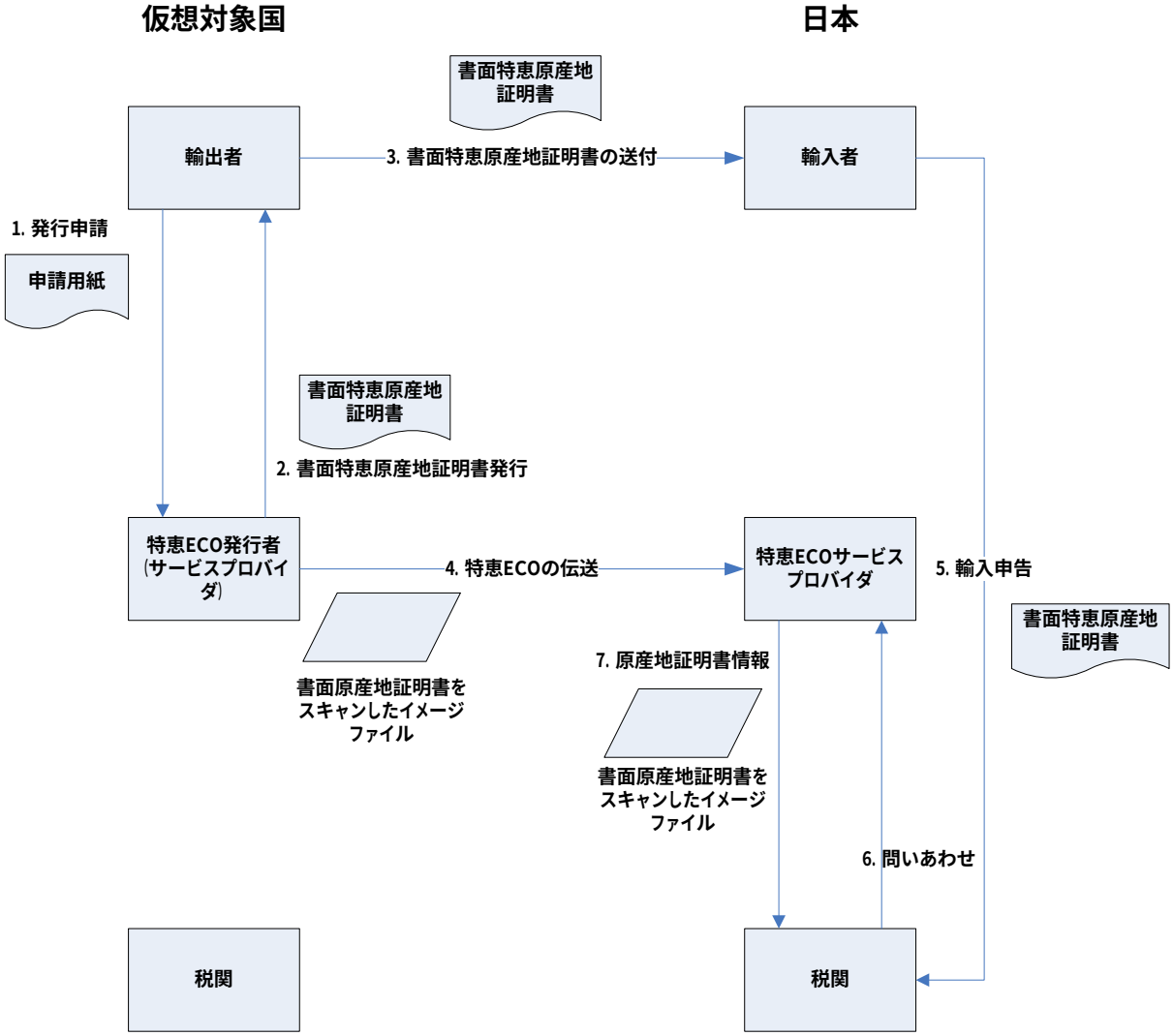

図 5.29　書面特恵原産地証明書運用図（仮想対象国→日本）

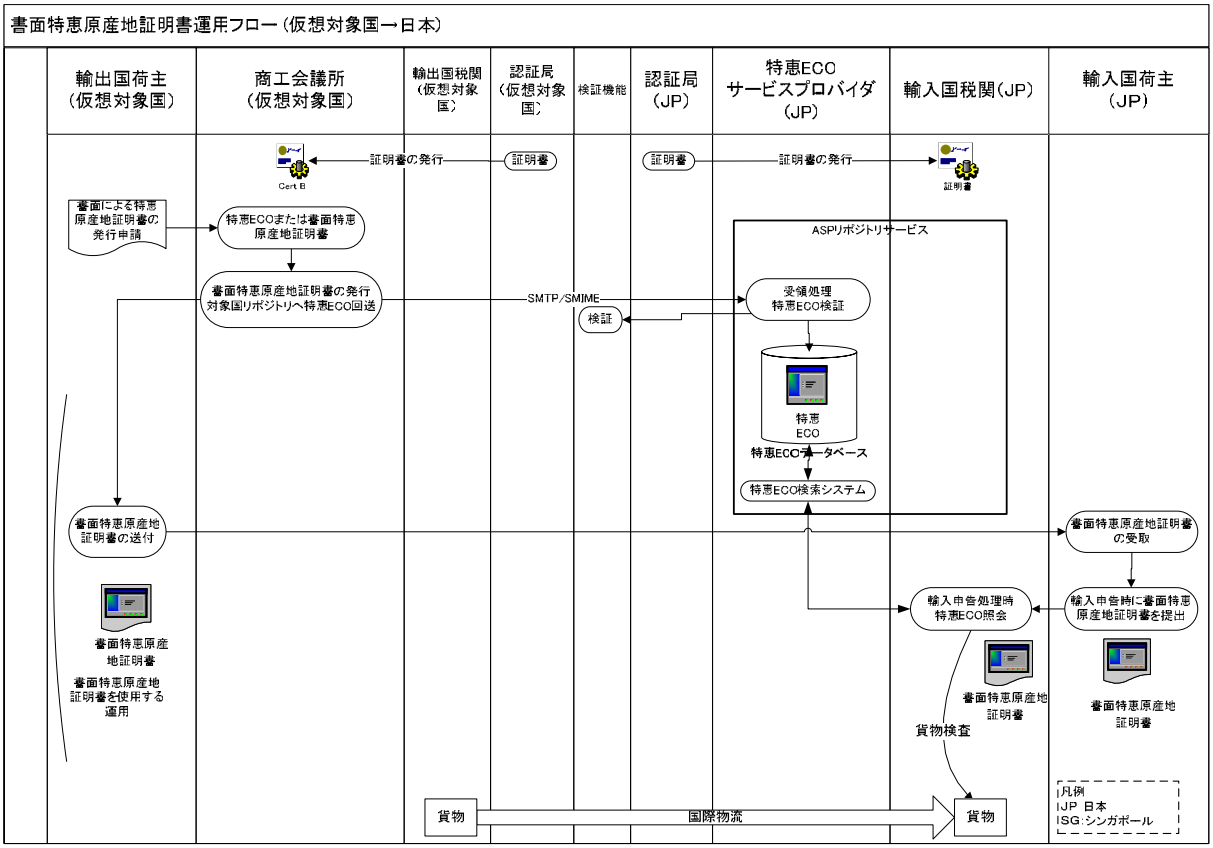

図 5.30　書面特恵原産地証明書運用フロー（仮想対象国→日本）

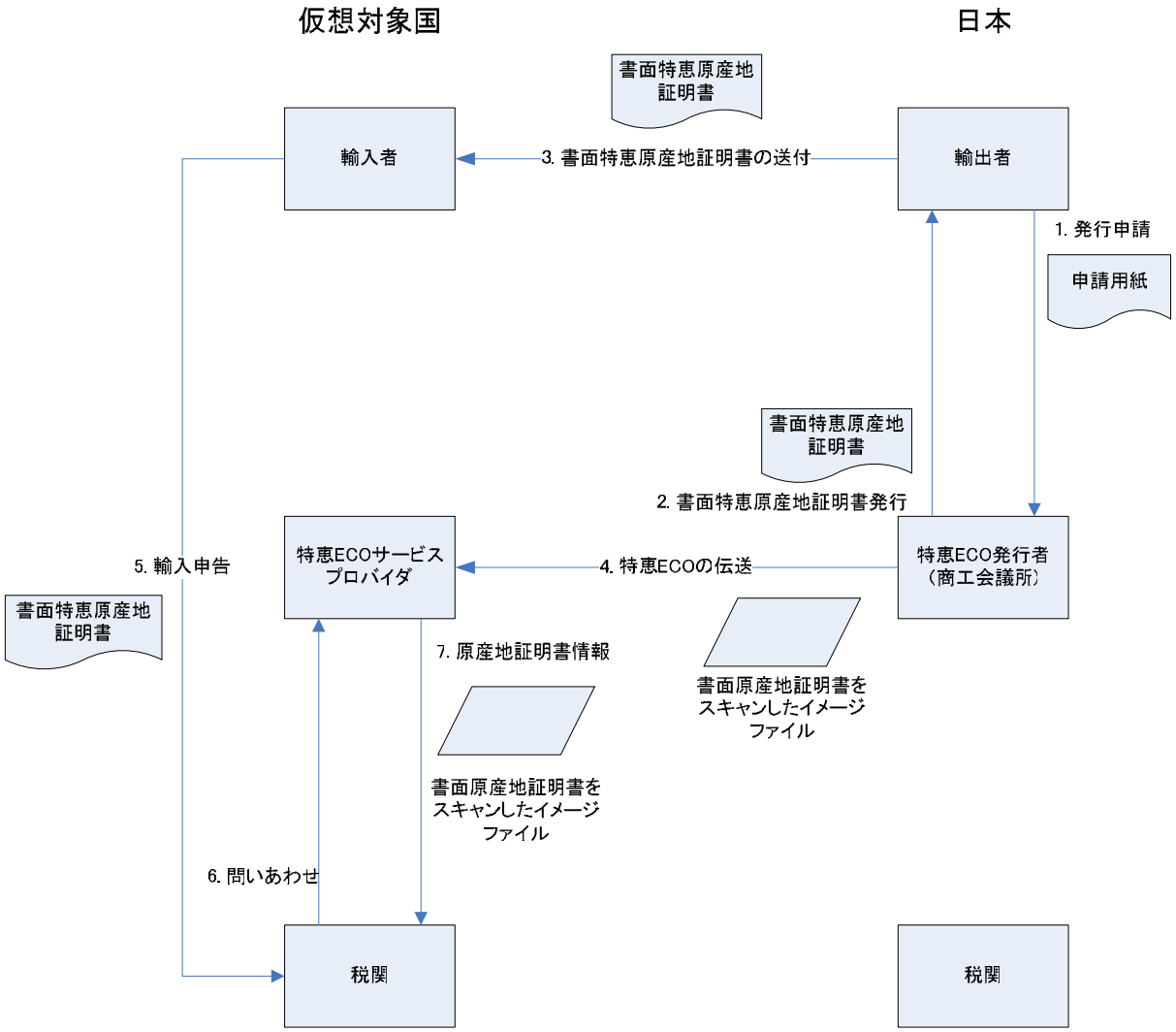

図 5.31　書面特恵原産地証明書運用図（日本→仮想対象国）

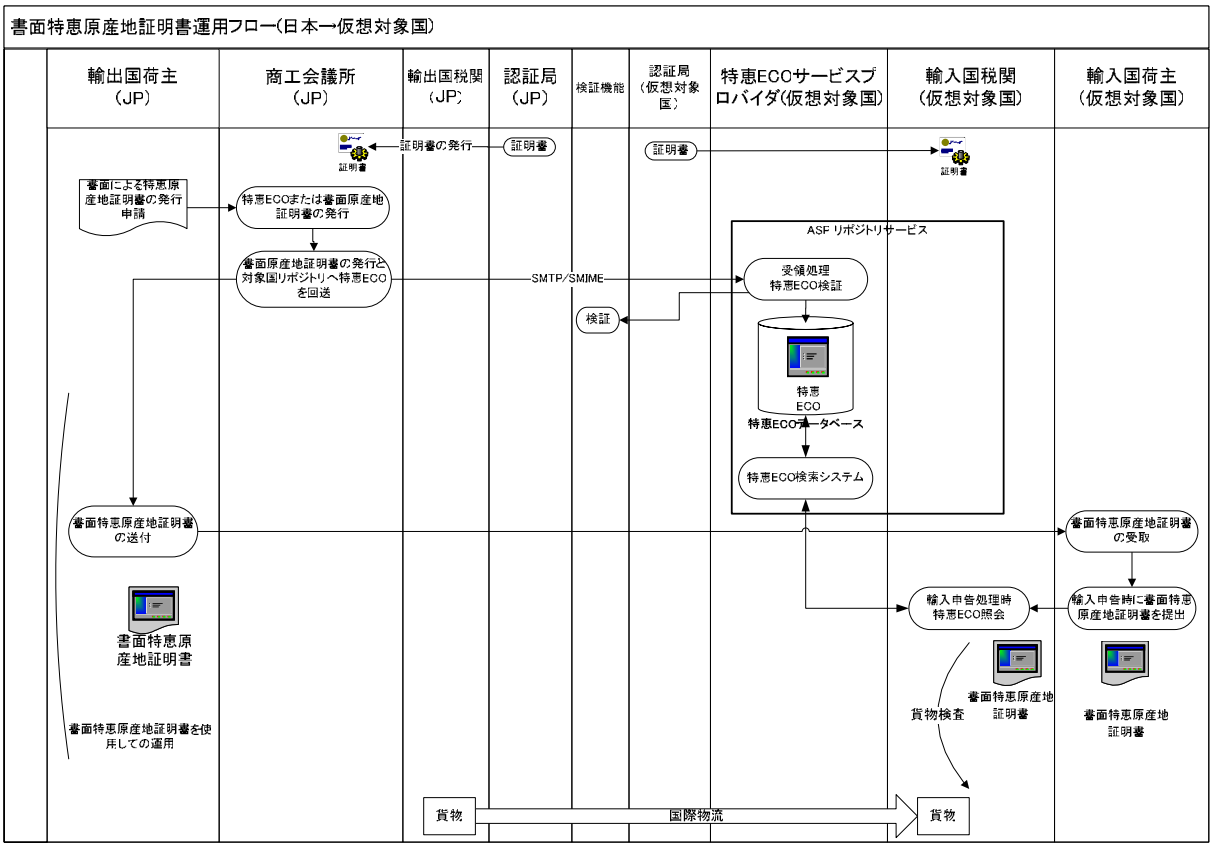

図 5.32　書面特恵原産地証明書運用フロー（日本→仮想対象国）

(2) パイロットシステムで採用された運用モデル

本パイロットシステムでは各国で 1 つのサービスプロバイダを構築するリポジトリモデルを採用した。このケースでは国際間の信頼関係はそれぞれのサービスプロバイダ間のみとなるため、信頼連鎖の形成がシンプルなケースとなる。

本パイロットプロジェクトでは「図 5.33　実験フロー（対シンガポール）」「図 5.34　実験フロー（対仮想対象国）」のような運用フローを想定し実験を行った。

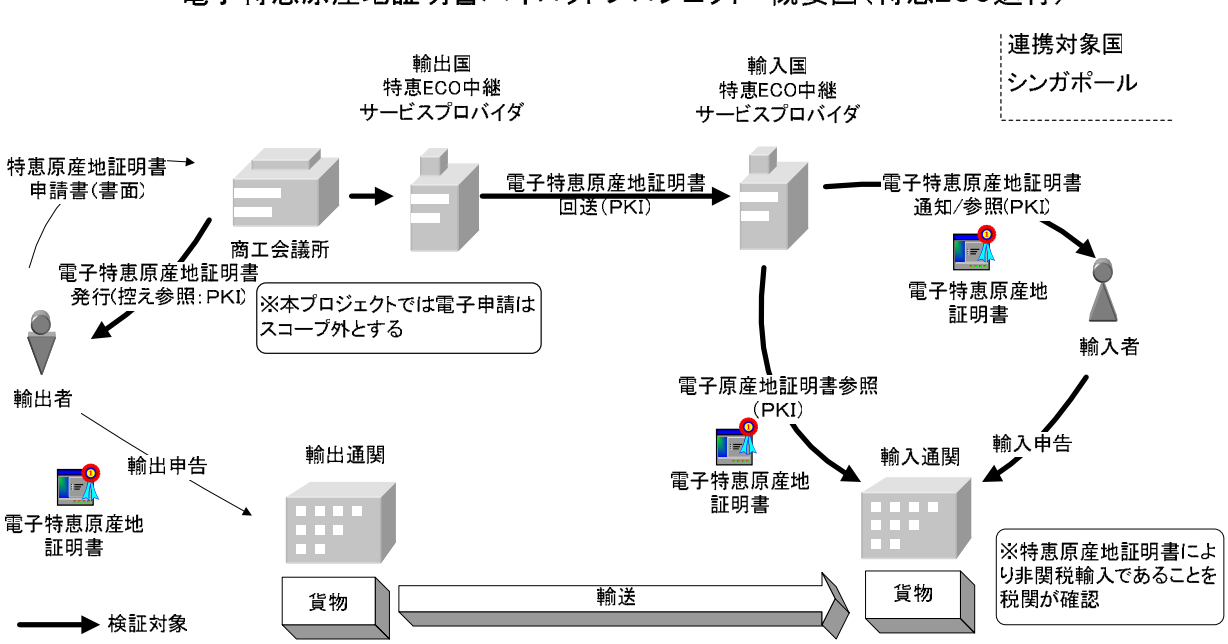

図 5.33　実験フロー（対シンガポール）

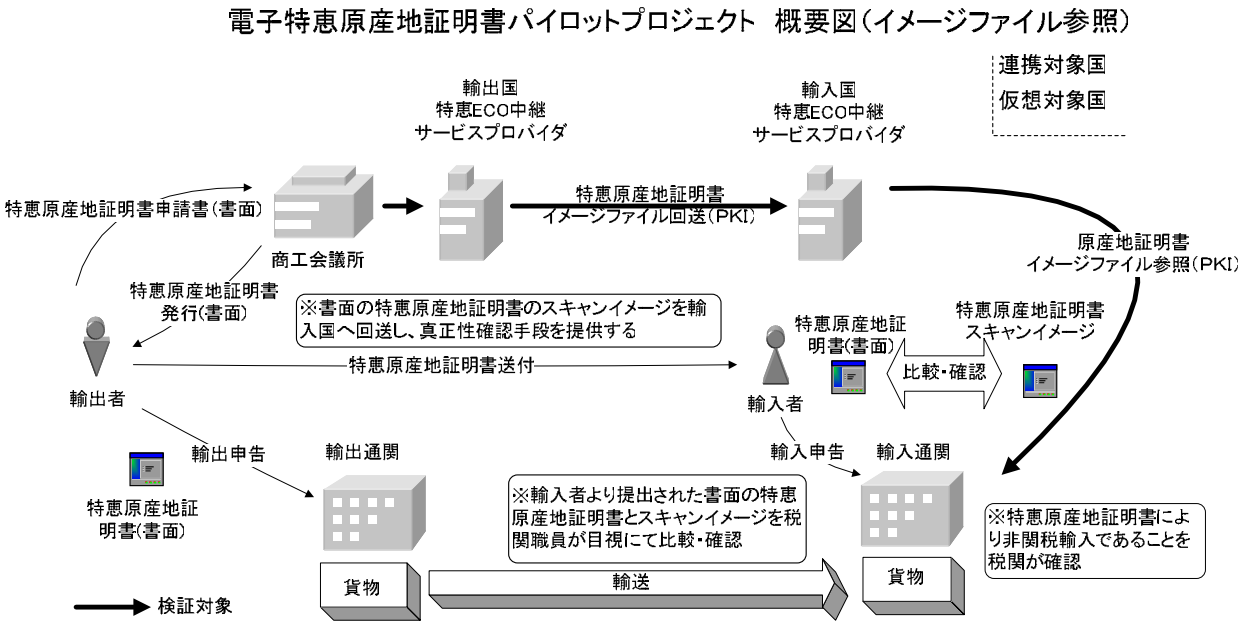

図 5.34　実験フロー（対仮想対象国）

5.5.2 システム概要

特恵 ECO 利用機能には大きく 4 つの機能があり、各機能は「図 5.35　特恵 ECO 利用機能概要」のような関わりを持っている。

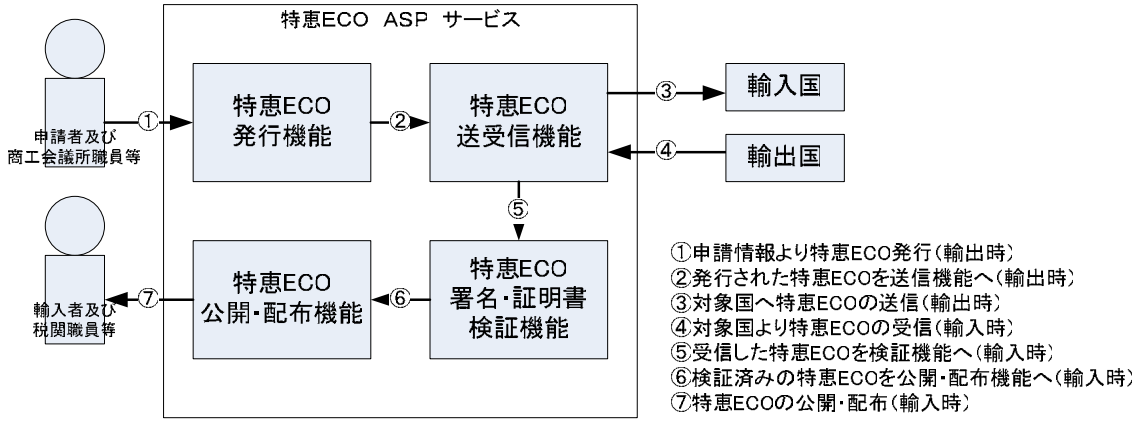

図 5.35　特恵 ECO 利用機能概要

(1) 特恵 ECO 発行機能

輸出入申請手続において、書面の特恵原産地証明書の代わりとなる特恵 ECO を発行する機能である。

入力画面より特恵原産地証明書の必要事項を入力し、その後承認者の署名を付与して特恵 ECO を発行する。

(a) 特恵原産地証明書情報検索機能

本機能はシステム内に格納された特恵原産地証明書情報を特定の条件により絞り込み、一覧表示させる機能である。

(b) 特恵原産地証明書情報入力機能

本機能は特恵原産地証明書情報をシステムに入力する機能である。

(c) イメージ取り込み機能

本機能は書面の特恵原産地証明書による申請時にイメージ情報として特恵 ECO にその情報を取り込むための機能である。

(d) 特恵原産地証明書情報承認機能

本機能は作成された特恵原産地証明書情報について承認処理を行い、特恵 ECO としての情報を最終確認させる機能である。承認処理により承認者の電子署名を付与することができる。

(e) ログ採取機能

本機能は特恵原産地証明書情報が作成、承認され、特恵 ECO が発行される過程の状態変化を追跡可能なログとして記録する機能である。

(2) 特恵 ECO 送受信機能

輸出国から輸入国へ特恵 ECO の送受信を行うための機能である。両国間の通信は安全かつ確実な伝送を可能とする。

(a) 特恵 ECO 送信機能

本機能は輸出国で発行した特恵 ECO を該当する輸入国へ送信する機能である。

特恵 ECO の伝送については第三者への情報漏えいや改ざん等の問題に対応し得る伝送方法とする。

(b) 特恵 ECO 受信機能

本機能は輸出国から送信された自己宛の特恵 ECO を輸入国にて受信する機能である。特恵 ECO の伝送については第三者への情報漏えいや改ざん等の問題に対応し得る伝送方法とする。

(c) ログ採取機能

本機能は特恵 ECO が送受信される過程の状態変化を追跡可能なログとして記録する機能である。

(3) 特恵 ECO 署名・証明書検証機能

特恵 ECO の手続時における特恵 ECO の電子署名および電子証明書について、その真正性を検証するための機能である。

(a) 署名検証機能

本機能は、特恵 ECO に対となる電子署名の検証を行うものである。

(b) 証明書検証機能

本機能は、特恵ECOの電子署名と対となる電子証明書の証明書検証を検証局へ依頼し、その返答を受信し分析するものである。

(c) ログ採取機能

本機能は署名・証明書検証の過程における状況を追跡可能なログとして記録する機能である。

(4) 特恵 ECO 公開・配布機能

輸出国から送信されてきた特恵 ECO を輸入国内にて輸入者、税関担当者等に情報提供をする機能である。輸入者への配布は「(3)特恵 ECO 署名・証明書検証機能」により得られた結果と共に、安全かつ確実な方法で伝送を行う。

税関への公開については、輸出者から輸入者への手続が書面の特恵原産地証明書で行われた場合に、輸入申請時に税関に持ち込まれた書面の特恵原産地証明書の真正性を確認するために行われる。税関は特恵 ECO 公開システムにアクセスし、該当する特恵 ECO の情報を参照できる機能を有する。

(a) 特恵 ECO を関係者に配布可能なこと

本機能は特恵 ECO を輸入者へ配布する機能である。

(b) 特恵 ECO を、閲覧を許可された者に公開可能なこと

本機能は輸入国にて特恵 ECO を閲覧するための機能である。輸出者から輸入者の手続が書面により行われた場合に、税関において書面の特恵原産地証明書の内容を確認するために用いられる。

(c) ログ採取機能

本機能は特恵 ECO が配布、閲覧される状況を追跡可能なログとして記録する機能である。

5.6　パイロットシステム環境

本パイロットシステムにおいてシンガポール側はシンガポール内で稼動している原産地証明書の申請／発行システムをベースにした環境を用意した。日本側については実験室を設け、各関連プレーヤーの環境を構築した。日本側のパイロットシステム環境について次に示す。

5.6.1 ハードウェア役割一覧

(1) 日本国検証局

本サーバは、以下の機能を提供するものとし、本サーバを実験環境で稼動させるために必要となる作業を実施する。

・ 証明書パス構築および証明書パス検証を支援する機能

(2) 日本国アプリケーションサーバ

本サーバは、以下の機能を提供する。

・特恵 ECO の発行を実現する機能

・特恵 ECO の送信を実現する機能

(3) 日本国 ASP サーバ

本サーバは、以下の機能を提供する。

・特恵 ECO の受信を実現する機能

・特恵 ECO の公開・配布を実現する機能

(4) 日本国認証局 1/日本国ディレクトリサーバ 1

本サーバは、以下の機能を提供するものとし、本サーバを実験環境で稼動させるために必要となる作業を実施する。

・ 相互接続に係わる証明書の発行、失効の機能

・ 証明書発行要求の受付をサポートする機能

・ 日本国認証局が発行する証明書および CRL 情報の格納を支援する機能

(5) 日本国認証局 2/日本国ディレクトリサーバ 2

本サーバは、以下の機能を提供するものとし、本サーバを実験環境で稼動させるために必要となる作業を実施する。

・ 相互接続に係わる証明書の発行、失効の機能

・ 証明書発行要求の受付をサポートする機能

・ 日本国認証局が発行する証明書および CRL 情報の格納を支援する機能

(6) 仮想対象国検証局（日本国検証局と兼用）

本サーバは、以下の機能を提供するものとし、本サーバを実験環境で稼動させ

るために必要となる作業を実施する。
・ 証明書パス構築および証明書パス検証を支援する機能

(7) 仮想対象国アプリケーションサーバ（日本国アプリケーションサーバと兼用）
本サーバは、以下の機能を提供する。
・特恵 ECO の発行を実現する機能
・特恵 ECO の送信を実現する機能

(8) 仮想対象国 ASP サーバ
本サーバは、以下の機能を提供する。
・特恵 ECO の受信を実現する機能
・特恵 ECO の公開・配布を実現する機能

(9) 仮想対象国認証局 1（日本国認証局 1/日本国ディレクトリサーバ 1 と兼用）
本サーバは、以下の機能を提供するものとし、本サーバを実験環境で稼動させるために必要となる作業を実施する。
・ 相互接続に係わる証明書の発行、失効を支援する機能

(10) 仮想対象国認証局 2（日本国認証局 2/日本国ディレクトリサーバ 2 と兼用）
本サーバは、以下の機能を提供するものとし、本サーバを実験環境で稼動させるために必要となる作業を実施する。
・ 相互接続に係わる証明書の発行、失効を支援する機能

(11) 仮想対象国ディレクトリサーバ 1
本サーバは、以下の機能を提供するものとし、本サーバを実験環境で稼動させるために必要となる作業を実施する。
・ 仮想対象国認証局が発行する証明書および CRL 情報の格納を支援する機能

(12) 仮想対象国ディレクトリサーバ 2
本サーバは、以下の機能を提供するものとし、本サーバを実験環境で稼動させるために必要となる作業を実施する。
・ 仮想対象国認証局が発行する証明書および CRL 情報の格納を支援する機能

(13) 税関端末
以下の機能を実現する。
・ WWW ブラウザを実現する機能

(14) 業者端末

以下の機能を実現する。

・ WWW ブラウザを実現する機能

5.6.2 ネットワーク構成

各機器を「図 5.36　ネットワーク構成図」のように構成し、パイロットシステム環境を構築した。

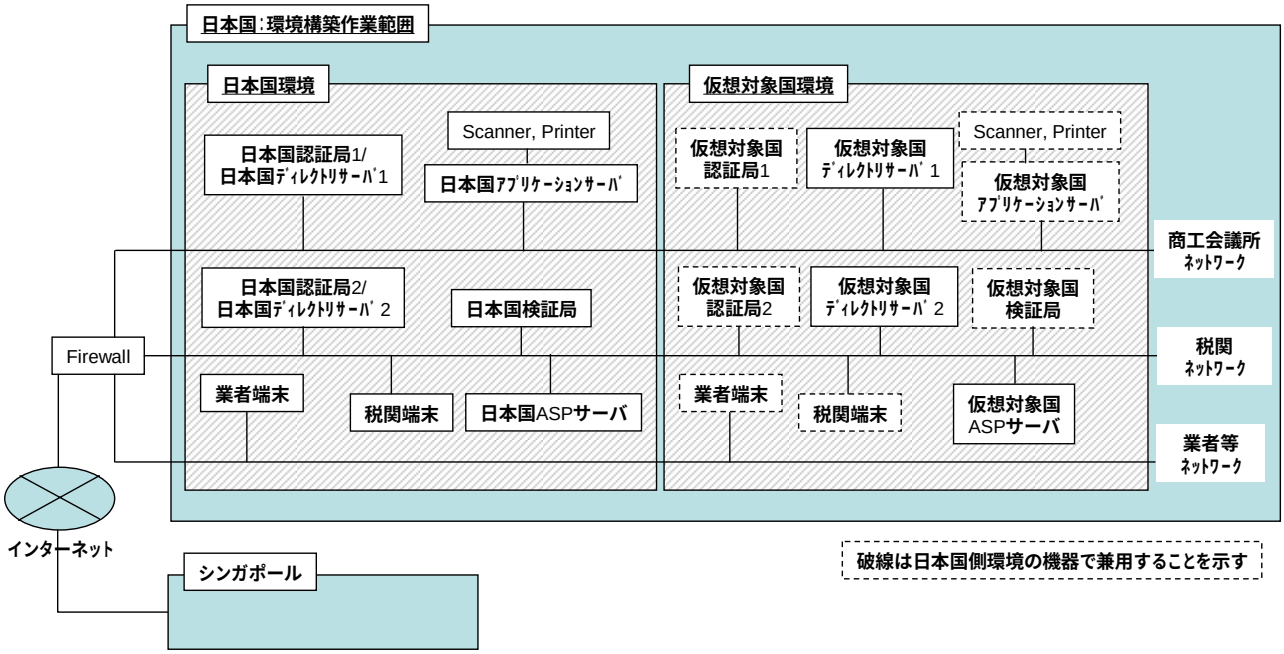

図 5.36　ネットワーク構成図

5.7　PKI 実利用のためのガイドラインの実証実験

5.7.1 実験概要

特恵原産地証明書の電子化モデルとしては、各国の電子化の事情を考慮して、書面の運用を継続することを前提とするモデルと完全に電子化した特恵原産地証明書を採用するモデルの 2 つのモデルを採用している。

なお、各国の国内で行われる特恵原産地証明書の発行申請については、国内に閉じた問題であり、本実証実験では、開発・検証の対象とはしていない。

(1) 書面の運用を前提とするモデル

本モデルは、書面による特恵原産地証明書を発行することを前提とし、発行される特恵原産地証明書の真偽性の検証を PKI 技術を利用して容易にするモデルである。このモデルは、日本－メキシコ間の協定が、書面を前提とする特恵原産地証明書を発行することを考慮して、構築したものである。本モデルにおいては、日本－メキシコ間等を対象経済領域としている。

仮想対象国との接続を想定した実験環境を「図 5.37　書面運用を前提とするモデル用パイロットシステム実証実験環境構成図」に示す。

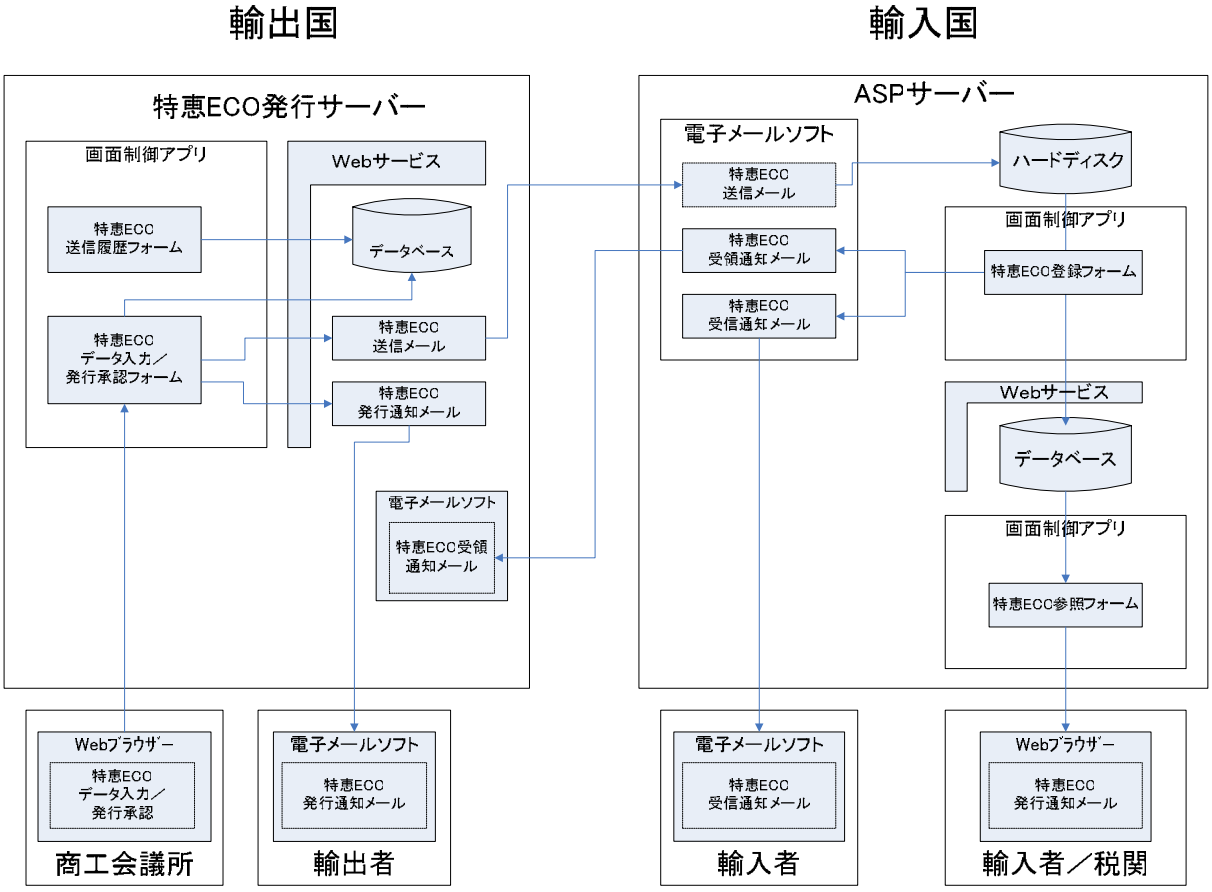

図 5.37　書面運用を前提とするモデル用パイロットシステム実証実験環境構成図

(2) 特恵原産地証明書を電子的に発行するモデル

本モデルは、電子的な特恵原産地証明書（特恵 ECO）を発行することを前提とし、特恵 ECO は、インターネットを利用して、商工会議所から輸出者へ、輸出者から輸入者へ、輸入者から税関へと転送されるモデルである。

本モデルは、日本－シンガポール間等の文書の電子化が進んでいる国との関係を想定している。

本モデルを前提とする実験の構成図を「図 5.38　日本からの輸出を想定したパイロットシステム実験環境構成」「図 5.39　シンガポールからの輸出を想定したパイロットシステム実験環境構成」に示す。

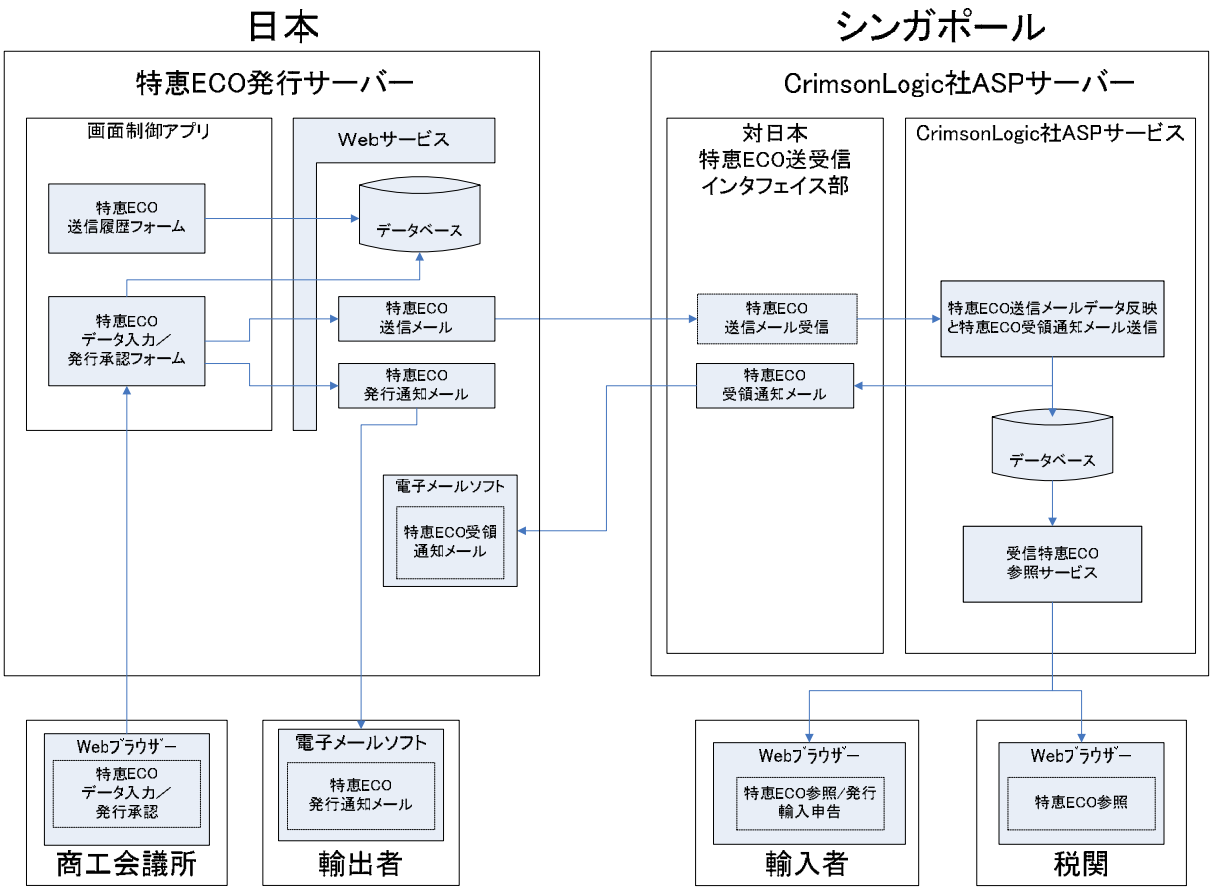

図 5.38　日本からの輸出を想定したパイロットシステム実験環境構成

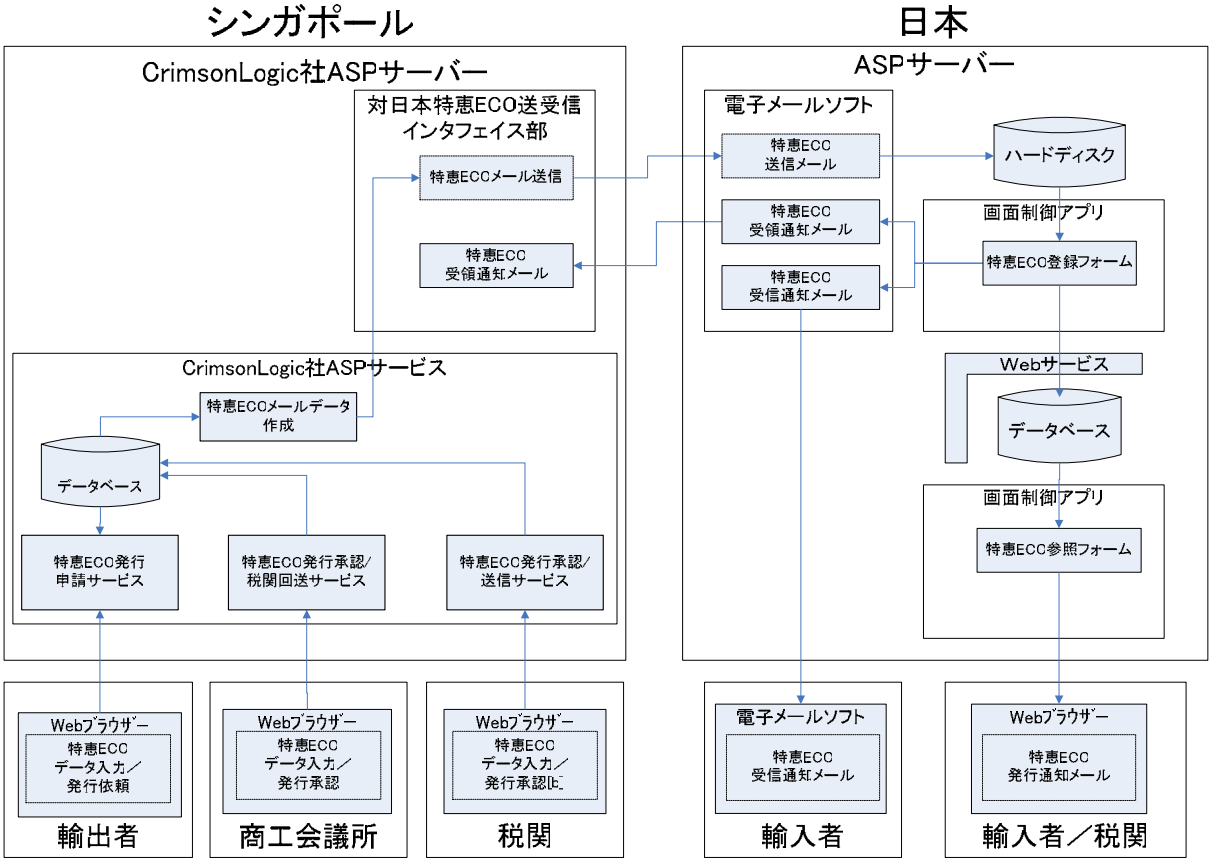

図 5.39　シンガポールからの輸出を想定したパイロットシステム実験環境構成

5.7.2 実験手順

(1) 日本と仮想対象国間実験手順

仮想対象国とのテストのための操作の流れを「表 5.2　日本から仮想対象国へ特恵 ECO を送信する実験の際の操作手順」「表 5.3　仮想対象国から日本へ特恵 ECO を送信する実験の際の操作手順」に示す。

表 5.2　日本から仮想対象国へ特恵 ECO を送信する実験の際の操作手順

No.	操作手順の内容
1	日本の商工会議所の担当者は輸出者からの申請情報を元に特恵原産地証明書を発行する。その後、発行した特恵原産地証明書をスキャンしたイメージファイルを格納した XML に署名・証明書を付与して特恵 ECO を作成する。
2	作成された特恵 ECO は ECO サーバのデータベースに格納されたのち、仮想対象国に S/MIME を使用して送信される。

3	特恵 ECO を受信した仮想対象国 ASP サーバは受信した特恵 ECO の署名・証明書検証を行い、真正性を確認する。真正性が確認できた場合は特恵 ECO をデータベースに格納し、輸入者に特恵 ECO が伝送された旨を電子メールにて通知する。通知される電子メールの内容は ASP への照会番号である。
4	電子メールにて特恵 ECO が通知された輸入者は Web ブラウザを利用して ASP にアクセスし、照会番号を用いることにより、その内容を確認することができる。輸入者は輸入申告の際に輸出者から送付された書面の特恵原産地証明書の提出と同時に ASP から通知された特恵 ECO の照会番号を税関に通知する。
5	税関では輸入申告を受け付けると、輸入者から通知された照会番号を元に ASP にアクセスし、日本から送付された特恵 ECO に包含されている書面の特恵原産地証明書のイメージファイルと提出された書面の特恵原産地証明書を見比べることによって、提出された書面の特恵原産地証明書の真正性を確認する。

表 5.3　仮想対象国から日本へ特恵 ECO を送信する実験の際の操作手順

No.	操作手順の内容
1	仮想対象国特恵 ECO 発行機関の担当者は輸出者からの申請情報を元に特恵原産地証明書を発行する。その後、発行した特恵原産地証明書をスキャンしたイメージファイルを格納した XML に署名･証明書を付与して特恵 ECO を作成する。
2	作成された特恵 ECO は ECO サーバのデータベースに格納されたのち、日本に S/MIME を使用して送信される。
3	特恵 ECO を受信した日本の ASP サーバは受信した特恵 ECO の署名・証明書検証を行い、真正性を確認する。真正性が確認できた場合は特恵 ECO をデータベースに格納し、輸入者に特恵 ECO が伝送された旨を電子メールにて通知する。通知される電子メールの内容は ASP への照会番号である。
4	電子メールにて特恵 ECO が通知された輸入者は Web ブラウザを利用して ASP にアクセスし、照会番号を用いることにより、その内容を確認することができる。輸入者は輸入申告の際に輸出者から送付された書面の特恵原産地証明書の提出と同時に ASP から通知された特恵 ECO の照会番号を税関に通知する。

5	税関では輸入申告を受け付けると、輸入者から通知された照会番号を元にASP にアクセスし、仮想対象国から送付された特恵 ECO に包含されている書面の特恵原産地証明書のイメージファイルと提出された書面の特恵原産地証明書を見比べることによって、提出された書面の特恵原産地証明書の真正性を確認する。

(2) 日本－シンガポール間実験手順

シンガポールとのテストのための操作の流れを「表 5.4　日本からシンガポールへ特恵 ECO を送信する実験の際の操作手順」に示す。

表 5.4　日本からシンガポールへ特恵 ECO を送信する実験の際の操作手順

No.	操作手順の内容
1	日本の商工会議所の担当者は輸出者から申請されたデータを用いて特恵 ECO 用の XML データに署名・証明書を付与して特恵 ECO を作成する。
2	作成された特恵 ECO は ECO サーバのデータベースに格納されたのち、シンガポールに S/MIME を使用して送信される。
3	特恵 ECO を受信したシンガポール ASP サーバは受信した特恵 ECO の署名・証明書検証を行い、真正性を確認する。真正性が確認できた場合は特恵 ECO をデータベースに格納し、輸入者に特恵 ECO が伝送された旨を電子メールにて通知する。通知される電子メールの内容は ASP への照会番号である。
4	電子メールにて特恵 ECO が通知された輸入者は Web ブラウザを利用して ASP にアクセスし、照会番号を用いることにより、その内容を確認することができる。輸入者は輸入申告の際に輸出者から送付された書面の特恵原産地証明書の提出と同時に ASP から通知された特恵 ECO の照会番号を税関に通知する。
5	税関では輸入申告を受け付けると、輸入者から通知された照会番号を元にASP にアクセスし、日本から送付された特恵 ECO のデータ内容を画面で確認し輸入申告の審査を行う。

5.7.3 検証要件および実験項目

特恵 ECO に係る運用を想定した際に必要となる要件と、実験項目の抽出を実施した。抽出された要件と実験項目を以下に示す。

(1) 特恵 ECO 発行について

表 5.5　特恵 ECO 発行要件

項番	要件	枝番	項目詳細
1	審査要件：署名前の確認事項	1	特恵 ECO の申請時の記載内容が他の関連書類と矛盾がないことを確認する
		2	特恵 ECO 申請者の署名を確認する
2	発行要件：特恵 ECO 発行時（後）の要件	1	特恵 ECO 発行者として登録されている特恵 ECO 発行者によって発行されること
		2	特恵 ECO に特恵 ECO 申請者の署名を確認できること
		3	特恵 ECO 発行時には電子署名したことを署名者が明確に理解できる方法であること
		4	特恵 ECO 発行後は１年間原本性が保証される形で控えを保管すること（保存年数は運用による取決めが必要）
		5	特恵 ECO は特恵 ECO フォーマットに従っていることを確認する
3	特恵 ECO の再発行	1	特恵 ECO の再発行については本パイロットプロジェクトではスコープ外とした
4	特恵 ECO の失効	1	特恵 ECO の失効については本パイロットプロジェクトではスコープ外とした

表 5.6　特恵 ECO 発行に係る実験項目

項番	大項目	枝番	詳細項目
1	審査	1	特恵 ECO の申請時の記載内容を貿易関係者が容易に参照をできるかどうか確認する
		2	特恵 ECO の申請時の申請者の署名を容易に参照できるかどうか確認する（本プロジェクトでは申請者の電子署名はスコープ外とした）
2	発行	1	特恵 ECO 発行時の電子署名付与方式について貿易関係者に評価を依頼する

		2	特恵 ECO 発行時に特恵 ECO の内容が容易に確認できるかどうか貿易関係者に評価を依頼する
		3	特恵 ECO 発行者として登録されていない人物による特恵 ECO の発行を行う

(2) 特恵 ECO の有効期限について

表 5.7　特恵 ECO の有効期限要件

項番	要件	枝番	項目詳細
1	特恵 ECO の有効期限内に特恵 ECO 発行者公開鍵証明書の有効期限が切れないような設計が必要	1	・運用によって実現する方法 ・特恵 ECO 発行者公開鍵証明書の有効期限がすべての発行した特恵 ECO の有効期限を含む様に設計する方法（本パイロットプロジェクトでは特恵 ECO の有効期限内は PKI による検証を可能とするため、こちらの方法を採用）
2	有効期限設定	1	特恵 ECO 発行者公開鍵証明書 GPKI 官職証明書や公的個人認証の証明書にならい３年とする
		2	特恵 ECO 本体 特恵 ECO 発行～税関による検証は長くても１年で実行可能と考えるので１年とする （現行の書面による運用では有効期限は１年）

表 5.8　特恵 ECO の有効期限に係る実験項目

項番	大項目	枝番	詳細項目
1	特恵 ECO 有効期限異常	1	特恵 ECO の有効期限切れ
		2	特恵 ECO 発行時証明書失効
		3	特恵 ECO 発行時証明書期限切れ
		4	特恵 ECO の有効期限よりも証明書の有効期限が短い（検証時公開鍵証明書有効）
		5	特恵 ECO の有効期限よりも証明書の有効期限が短い（検証時に公開鍵証明書期限切れ）
		6	証明書の有効開始前に特恵 ECO の有効開始が設定されている（検証時公開鍵証明書期限切れ）
		7	証明書の有効開始前に特恵 ECO の有効開始が設定されている（検証時公開鍵証明書有効）

(3) 特恵 ECO 発行者証明書更新について

表 5.9　特恵 ECO 発行者証明書更新要件

項番	要件	枝番	項目詳細
1	いつ、誰が、どのような方法で更新するのかを規定する	1	-特恵 ECO 発行者公開鍵証明書更新に関する要件 -いつ更新するのか -誰が誰宛に更新するのか -何のために更新するのか -失効したらどうするのか
		2	特恵 ECO 発行者証明書更新方法に関する要件 -機密性に関する要件 -完全性に関する要件 等
		3	上記要件を満たす実現手段の検討 -S/MIME, SSL 等の通信手段 -手渡し（外交ルート等） -国際郵便等

表 5.10　特恵 ECO 発行者証明書更新に係る実験項目

項番	大項目	枝番	詳細項目
1	特恵 ECO 発行者証明書交換	1	特恵 ECO 発行者が特恵 ECO 検証者の持っているリストに載っていない
		2	特恵 ECO 発行者リストの更新
2	特恵 ECO 発行者リストの更新後の検証	1	新しい特恵 ECO 発行者による発行および検証
		2	特恵 ECO 発行者証明書の失効に対する検証

(4) 特恵 ECO 検証について

表 5.11　特恵 ECO 検証要件

項番	要件	枝番	項目詳細
1	特恵 ECO の正常署名検証	1	検証エンティティ -輸入国 ASP -輸入者 -輸入国税関
2	特恵 ECO の正常証明書検証	1	検証エンティティ -輸入国 ASP -輸入者 -輸入国税関
3	特恵 ECO の署名検証に失敗する場合	1	検証エンティティ -輸入国 ASP -輸入者 -輸入国税関
4	特恵 ECO 発行者証明書の検証に失敗する場合	1	検証エンティティ -輸入国 ASP -輸入者 -輸入国税関

表 5.12　特恵 ECO 検証に係る実験項目

項番	大項目	枝番	詳細項目
1	正常検証	1	特恵 ECO の正常署名検証
		2	特恵 ECO の正常証明書検証
2	検証エラー	1	特恵 ECO の署名エラー
		2	特恵 ECO の証明書検証エラー

(5) 各エンティティでの特恵 ECO 検証失敗について

表 5.13　特恵 ECO フォーマット要件

項番	要件	枝番	項目詳細
1	特恵 ECO のフォーマット	1	特恵 ECO のフォーマット（国際標準になり得るか）
		2	特恵 ECO における必須項目・任意項目とそれぞれの理由（なぜ必須なのか、なぜ任意でよいのか）
		3	特恵 ECO の項目 -形式（任意のテキスト、数字、ある集合からの選択等） -制限（文字数や桁数の制限、文字および文字列に対する制限等） -説明（何に利用される項目で、なぜその項目が必要なのか）

表 5.14　特恵 ECO フォーマットに係る実験項目

項番	大項目	枝番	詳細項目
1	特恵 ECO フォーマット（システムのサービスレベルに依存し、システムテストの範囲とするため実験としてはスコープ外とした）	1	・フォーマットが妥当かどうか ・フォーマットの妥当性を判別できるかどうか
		2	・必須項目に抜け漏れがないか ・必須項目の有無を判別できるかどうか
		3	データの型が間違っていることを検知できるかどうか
		4	データの制限事項に準拠していないことを検知できるかどうか
		5	あり得ないデータが記載されていることを検知できるかどうか
		6	他の書類との矛盾を検知できるかどうか
		7	特恵対象品目かどうかを判断できるかどうか
		8	特恵対象国かどうかの判断ができるかどうか

(6) 特恵 ECO プロトコル（送受信）について

表 5.15　特恵 ECO プロトコル（送受信）要件

項番	要件	枝番	項目詳細
1	特恵 ECO プロトコル送付	1	要件 -確実に届くこと -安全に送付されること（送付中に改ざんされないこと）
		2	上記を満たす仕様の採用 （本パイロットプロジェクトでは S/MIME を利用して送付する）

表 5.16　特恵 ECO プロトコル（送受信）に係る実験項目

項番	大項目	枝番	詳細項目
1	S/MIME による送信	1	S/MIME による伝送が行われていることを確認（盗聴、改ざん等の問題に対応している）
		2	送信情報が暗号化されていることを確認
		3	送信情報に S/MIME の署名がなされていることを確認
		4	正常送信ができることを確認
		5	正常受信ができることを確認
2	S/MIME による応答受信	1	受信応答の正常送信を確認
		2	受信応答の正常受信を確認

(7) 仮想対象国仕様について

表 5.17　仮想対象国仕様要件

項番	要件	枝番	項目詳細
1	特恵 ECO フォーマット（仮想対象国用）	1	要件 -基本的に書面による特恵原産地証明書が原本となり、書面の特恵原産地証明書が作成されたのち、特恵 ECO データが手入力にて生成されるため、イメージと特恵 ECO のデータに差異が生じる可能性がある -電子的に送信される特恵 ECO およびイメージテータは参考資料の扱いとなる -発行国側からスキャンしたイメージデータを送信し、書面とイメージデータを見比べて真正性を確認する
2	特恵 ECO プロトコル仕様（仮想対象国用）	1	仕様 -送受信に関しては基本的にシンガポールと同様とする
3	特恵 ECO 運用（仮想対象国用）	1	仕様 （考えられる仕様） イメージデータと輸入国に送付された書面の特恵原産地証明書との比較が基本運用となる

表 5.18　仮想対象国仕様に係る実験項目

項番	大項目	枝番	詳細項目
1	仮想対象国に特化した実験項目	1	イメージデータが参照可能なこと -画像フォーマットが異なる -イメージデータが添付されていない
		2	イメージデータと特恵 ECO の内容が異なる -イメージ選択ミス -イメージと特恵 ECO のデータ内容が異なる

5.7.4 検証項目

5.7.3 で検討した要件と実験項目を元に、パイロットプロジェクトで実施する検証項目について選定を行い、必要となる証明書のパターンと実施すべき検証項目について、対シンガポールおよび対仮想対象国を想定し検討を行った。以下は検討結果である。

(1) 対シンガポール

特恵 ECO の有効期間と特恵 ECO に付与される電子証明書の有効期間との関連を「図 5.40　特恵 ECO 有効期間と電子証明書有効期間」に示す。

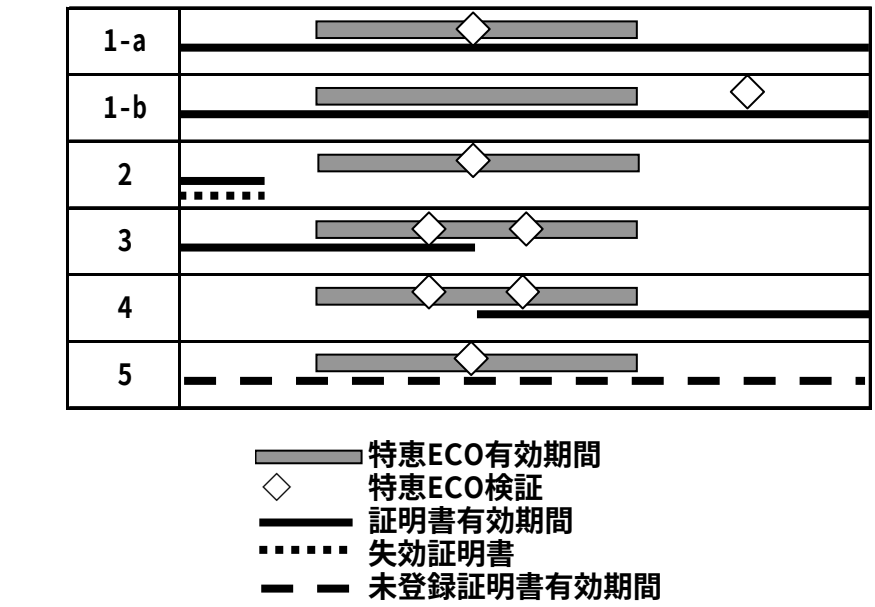

図 5.40　特恵 ECO 有効期間と電子証明書有効期間

「図 5.40　特恵 ECO 有効期間と電子証明書有効期間」のパターン 2、3、4 に関しては、特恵 ECO の有効期間が電子証明書の有効期間内に含まれないケースである。そのため、シンガポールとの協議の結果、基本的に特恵 ECO 自体を発行できないパターンとした。これらのパターンについては、発行前のシステムでチェックを行うため、該当する特恵 ECO は存在しないものとする。

パターン 5 に関しては、本来発行者とされていない署名が付与されたケースであるが、この場合は本来有効であるべき特恵 ECO にもかかわらず、特恵 ECO の発行者情報の更新タイミングのタイムラグ等により無効と判定されるケースも想定されるので注意が必要である。

パターン 1-a は正常運用時、特恵 ECO が有効な期間に検証を行うケース。

パターン 1-b は正常に発行された特恵 ECO を特恵 ECO の有効期間を過ぎて検証

を行ったケース。

対シンガポールの検証項目を「表 5.19　対シンガポール検証項目」に示す。ここで証明書パターンは「図 5.40　特恵 ECO 有効期間と電子証明書有効期間」と対応している。

なお、検証項目の中の証明書パターン 1-a'は証明書としては正常運用時の証明書を用いるが、意図的に特恵 ECO の改ざん等を行い検証エラーの確認を行うものである。

表 5.19　対シンガポール検証項目

実験分類	ﾃｽﾄ種別	実験項目	証明書パターン
異常系	ｼｽﾃﾑﾃｽﾄ	特恵 ECO 発行時証明書失効	2
		特恵 ECO 発行時証明書期限切れ	2
		証明書の有効開始前に特恵 ECO の有効開始が設定されている（検証時公開鍵証明書期限切れ）	4
		証明書の有効開始前に特恵 ECO の有効開始が設定されている（検証時公開鍵証明書有効）	4
日本からシンガポールへの特恵 ECO 送付	実証実験正常系	特恵 ECO を日本から送信	1-a
		特恵 ECO をシンガポールが受信	1-a
		受信応答をシンガポールから送信	1-a
		受信応答を日本が受信	1-a
		S/MIME 送受信	1-a
		日本の署名・証明書検証（正常系）	1-a
		特恵 ECO データ内容の確認	1-a
		証明書の交換（更新）	-
		署名・証明書検証（証明書更新の検証）	1-a
シンガポールから日本への特恵 ECO 送付	実証実験正常系	特恵 ECO をシンガポールから送信	1-a
		特恵 ECO を日本が受信	1-a
		受信応答を日本から送信	1-a
		受信応答をシンガポールが受信	1-a
		S/MIME 送受信	1-a
		シンガポールの署名・証明書検証（正常系）	1-a
		特恵 ECO データ内容の確認	1-a
		証明書の交換（更新）	-
		署名・証明書検証（証明書更新の検証）	1-a

日本からシンガポールへの特恵ECO送付	実証実験異常系	特恵 ECO の有効期限切れ	1-b
		登録されていない証明書で署名	5
		特恵 ECO の署名検証エラー	1-a'
		特恵 ECO の証明書検証エラー	1-a'
シンガポールから日本への特恵ECO送付	実証実験異常系	特恵 ECO の有効期限切れ	1-b
		特恵 ECO の有効期限よりも証明書の有効期限が短い（検証時公開鍵証明書有効）	3
		特恵 ECO の署名検証エラー	1-a'
		特恵 ECO の証明書検証エラー	1-a'

(2) 対仮想対象国

本パイロットプロジェクトでは特恵原産地証明書を全て電子化した特恵 ECO モデルの他に、書面による運用を残したケースでの特恵原産地証明書の真正性確保のための仕組みを検証した。

基本的な仕組みは対シンガポールとの仕組みを利用するが、対仮想対象国との場合には輸入国税関のために輸出国から発行した書面のイメージファイルを提供し、改ざん等の検証に活用するものである。

実験項目としては対シンガポールと同等の検証項目に加え、スキャンイメージの伝送、および閲覧についての検証を行う。対仮想対象国の検証項目を「表 5.20 対仮想対象国検証項目」に示す。

表 5.20　対仮想対象国検証項目

実験分類	ﾃｽﾄ種別	実験項目	証明書パターン
異常系	ｼｽﾃﾑﾃｽﾄ	特恵 ECO 発行時証明書失効	2
		特恵 ECO 発行時証明書期限切れ	2
		証明書の有効開始前に特恵 ECO の有効開始が設定されている（検証時公開鍵証明書期限切れ）	4
		証明書の有効開始前に特恵 ECO の有効開始が設定されている（検証時公開鍵証明書有効）	4
日本から仮想対象国への特恵 ECO 送付	実証実験正常系	特恵 ECO を日本から送信	1-a
		特恵 ECO を仮想対象国が受信	1-a
		受信応答を仮想対象国から送信	1-a
		受信応答を日本が受信	1-a
		S/MIME 送受信	1-a
		日本の署名・証明書検証（正常系）	1-a
		特恵 ECO データ内容の確認	1-a
		添付イメージデータファイルの確認	1-a
		証明書の交換（更新）	-
		署名・証明書検証（証明書更新の検証）	1-a
仮想対象国から日本への特恵 ECO 送付	実証実験正常系	特恵 ECO を仮想対象国から送信	1-a
		特恵 ECO を日本が受信	1-a
		受信応答を日本から送信	1-a
		受信応答を仮想対象国が受信	1-a
		S/MIME 送受信	1-a

		仮想対象国の署名・証明書検証（正常系）	1-a
		特恵 ECO データ内容の確認	1-a
		添付イメージデータファイルの確認	1-a
		証明書の交換（更新）	-
		署名・証明書検証（証明書更新の検証）	1-a
日本から仮想対象国への特恵 ECO 送付	実証実験異常系	特恵 ECO の有効期限切れ	1-b
		登録されていない証明書で署名	5
		特恵 ECO の署名検証エラー	1-a'
		特恵 ECO の証明書検証エラー	1-a'
仮想対象国から日本への特恵 ECO 送付	実証実験異常系	特恵 ECO の有効期限切れ	1-b
		特恵 ECO の有効期限よりも証明書の有効期限が短い（検証時公開鍵証明書有効）	3
		特恵 ECO の署名検証エラー	1-a'
		特恵 ECO の証明書検証エラー	1-a'

5.7.5 実験結果

(1) 日本と仮想対象国間実験結果

日本と仮想対象国間実験の実験結果を「表 5.21　日本と仮想対象国間の特恵 ECO 伝送実験結果」に示す。

表 5.21　日本と仮想対象国間の特恵 ECO 伝送実験結果

No.	実験項目	期待される実験結果	実施結果
1	日本から仮想対象国へ特恵 ECO を S/MIME を使用して送信	正常に送信	問題なし
2	日本から S/MIME を使用して送信された特恵 ECO を仮想対象国で受信	正常に受信	問題なし
3	特恵 ECO 受信応答を仮想対象国から日本へ S/MIME を使用して送信	正常に送信	問題なし
4	仮想対象国から S/MIME を使用して送信された受信応答を日本が受信	正常に受信	問題なし
5	仮想対象国にて日本から送信された特恵 ECO の署名・証明書検証（正常系）	正しく署名・証明書検証ができる	問題なし
6	証明書の交換（更新）	正しく署名・証明書検証ができる	問題なし
7	署名・証明書検証（証明書更新の検証）	正しく署名・証明書検証ができる	問題なし
8	特恵 ECO の有効期限切れ（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
9	登録されていない証明書で署名（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
10	特恵 ECO の署名検証エラー（異常系)	特恵 ECO 受信後の登録時にエラー発生	問題なし
11	特恵 ECO の証明書検証エラー（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
12	仮想対象国にて特恵 ECO データ内容の確認	策定した特恵 ECO データフォーマットに準拠している	問題なし

13	対象想定国にて特恵 ECO に添付されるイメージデータファイルの確認	スキャンした書面特恵原産地証明書が正しく参照できる	問題なし
14	仮想対象国から日本へ特恵 ECO を S/MIME を使用して送信	正常に送信	問題なし
15	仮想対象国から送信された特恵 ECO を日本で受信	正常に受信	問題なし
16	特恵 ECO 受信応答を日本から仮想対象国へ送信	正常に送信	問題なし
17	日本から送信された受信応答を仮想対象国が受信	正常に受信	問題なし
18	日本にて仮想対象国から送信された特恵 ECO の署名・証明書検証（正常系）	正しく署名・証明書検証	問題なし
19	証明書の交換（更新）	正しく署名・証明書検証	問題なし
20	署名・証明書検証（証明書更新の検証）	正しく署名・証明書検証	問題なし
21	特恵 ECO の有効期限切れ（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
22	登録されていない証明書で署名（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
23	特恵 ECO の署名検証エラー（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
24	特恵 ECO の証明書検証エラー（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
25	日本にて特恵 ECO データ内容の確認	策定した特恵 ECO データフォーマットに準拠している	問題なし
26	特恵 ECO に添付されるイメージデータファイルの確認	スキャンした書面特恵原産地証明書が正しく参照できる	問題なし

(2) 日本－シンガポール間実験結果

日本－シンガポール間の実験の実験結果を「表 5.22　日本－シンガポール間の特恵 ECO 伝送実験結果」に示す。

表 5.22　日本－シンガポール間の特恵 ECO 伝送実験結果

No.	実験項目	期待される実験結果	実施結果
27	日本からシンガポールへ特恵 ECO を S/MIME を使用して送信	正常に送信	問題なし
28	日本から送信された特恵 ECO をシンガポールで受信	正常に受信	問題なし
29	特恵 ECO 受信応答をシンガポールから日本へ送信	正常に送信	問題なし
30	シンガポールから送信された受信応答を日本が受信	正常に受信	問題なし
31	シンガポールにて日本から送信された特恵 ECO の署名・証明書検証（正常系）	正しく署名・証明書検証ができる	問題なし
32	証明書の交換（更新）	正しく署名・証明書検証ができる	問題なし
33	署名・証明書検証（証明書更新の検証）	正しく署名・証明書検証ができる	問題なし
34	特恵 ECO の有効期限切れ（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
35	登録されていない証明書で署名（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
36	特恵 ECO の署名検証エラー（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
37	特恵 ECO の証明書検証エラー（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
38	シンガポールにて特恵 ECO データ内容の確認	策定した特恵 ECO データフォーマットに準拠している	問題なし
39	シンガポールから日本へ特恵 ECO を S/MIME を使用して送信	正常に送信	問題なし
40	シンガポールから送信された特恵 ECO を日本で受信	正常に受信	問題なし
41	特恵 ECO 受信応答を日本からシンガポールへ送信	正常に送信	問題なし
42	日本から送信された受信応答をシンガポールが受信	正常に受信	問題なし

43	日本にてシンガポールから送信された特恵 ECO の署名・証明書検証（正常系）	正しく署名・証明書検証	問題なし
44	証明書の交換（更新）	正しく署名・証明書検証	問題なし
45	署名・証明書検証（証明書更新の検証）	正しく署名・証明書検証	問題なし
46	特恵 ECO の有効期限切れ（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
47	登録されていない証明書で署名（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
48	特恵 ECO の署名検証エラー（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
49	特恵 ECO の証明書検証エラー（異常系）	特恵 ECO 受信後の登録時にエラー発生	問題なし
50	日本にて特恵 ECO データ内容の確認	策定した特恵 ECO データフォーマットに準拠している	問題なし

(3) 考察

想定した実験項目を実施し、期待される結果を得ることができた。考察の詳細については 6.1 評価および考察を参照。

6 全体考察

6.1　評価および考察

6.1.1 PKI の国際的相互接続に関する手引の評価および考察

(1) 特恵 ECO パイロットシステムにおける PKI 適用の評価

特恵 ECO パイロットシステムにおける PKI の役割は、「特恵 ECO の完全性・真正性の確保」である。これには２つの要素が存在する。

・ 特恵 ECO が改ざんされないこと

・ 各エンティティ（特恵 ECO 申請者・発行者等）が信頼できること

これらについての詳細を以下に述べる。

(a) PKI を用いて特恵 ECO が改ざんされていないことを保証するには

特恵 ECO が改ざんされていないことを保証するためには電子署名を用いることがもっとも効果的である。

厳密に言うと、PKIを利用した電子署名の署名検証者にとっての有効性は、署名鍵に対応する公開鍵証明書の有効性に依存する。つまり、文書に付いている電子署名を検証する際、対応する公開鍵証明書が有効期限外であったり、何らかの理由で失効していた場合には、検証時点において電子署名された文書の完全性を保証できない。※2

このことを特恵 ECO システムに当てはめてみると大きく、以下のような２つの問題があることがわかる。

(i) 特恵 ECO を検証する時点において特恵 ECO 発行者公開鍵証明書が有効期限切れになっている場合がある

(ii) 特恵 ECO を検証する時点において特恵 ECO 発行者公開鍵証明書が失効している場合がある

このうち(ii)については、特恵 ECO 発行者公開鍵証明書の失効は技術的に回避することは不可能であり、特恵 ECO 発行者公開鍵証明書が失効してしまった場合には、当該発行者が発行した特恵 ECO をすべて再発行する等の、運用ルールによるサポートが必要となる。

以下に(i)の問題を回避する方法について述べる。

特恵 ECO を検証する時点において特恵 ECO 発行者公開鍵証明書が有効期限切れにならないようにするには、以下の「図 6.1　有効期間関連図」に示すように、特恵 ECO 発行者の公開鍵有効期間内に特恵 ECO 有効期間が含まれ、特恵 ECO 有効期間内に特恵 ECO 検証時点が存在しなければならない。

※2 このことを防ぐ仕組みとして、電子文書の長期保管に係る技術がある。

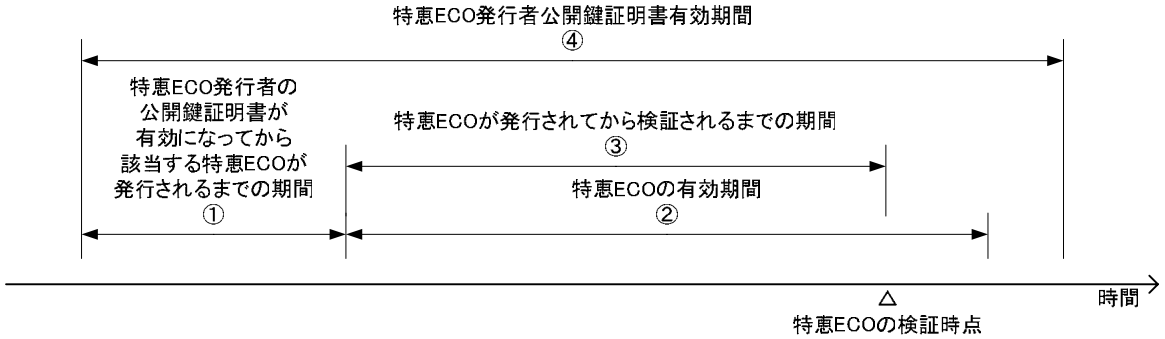

図 6.1　有効期間関連図

このことを満たすためには以下の条件を同時に満たすことが必要となる。

- ①＋②＜④
- ③＜②

これらのうち、②、④は固定値である。従って期間を考慮すべきは①と③のみである。ここで、③については技術的に制御することは不可能であるため、①の長さについて適切な設計を行えばよいこととなる。つまり、①の長さについて以下を常に満たすように制限すればよいこととなる。

- ①＜④－②－C　※3

上記の通りに①の長さを制限する方法には下記の２種類が存在する。

(ア)　公開鍵証明書の privateKeyUsagePeriod を利用し、ある一定期間以降は署名鍵を利用できなくする

(イ)　特恵 ECO 発行アプリケーションにおいて特恵 ECO 発行時に上記の制限を確認する

このうち、(ア)による方法は、RFC3280 等において privateKeyUsagePeriod を利用しないことを推奨していることや、privateKeyUsagePeriod を利用できない認証局ソフトウェアが存在することから、推奨できない。そこで、特恵 ECO パイロットシステムにおいては(イ)による方法を選択することにより、(a)に示す問題点を解決した。

以上により、いくつかの点については運用によるルールが必要になるものの、PKI を用いて、特恵 ECO が改ざんされていないことを保証することができる。

(b) 各エンティティ（特恵 ECO 申請者・発行者等）が信頼できること

自ドメイン以外の他 PKI ドメインの各エンティティを信頼するためには、他 PKI ドメインを信頼する仕組みとして認証局間相互接続が必要である。

アジアPKIフォーラムにおける認証局間相互接続の仕組みとしては、Cross-Certificateを発行する方式（以下、CC方式）と、相手のPKIドメインの

※3 Cは安全のためのバッファであり、特恵ECO発行者が次の公開鍵証明書と署名鍵のペアに切り替えるための移行期間である。混乱を避けるため、図には特に示していない。

ルート認証局を信頼して信頼の起点として相手ドメインのルート認証局公開鍵証明書を受け入れる方式（以下、CR方式）が存在する。CC方式とCR方式のいずれを選択するかは、技術的な比較による検討よりも、環境的な要因※4によって決定する事が多い。今回の特恵ECOパイロットシステムにおいては、CR方式を採用することとなった。ただしこれはあくまでパイロットシステムとして問題がないとの判断により採用したため、運用の際には再度検討を行う必要がある。

ここで、認証局間相互接続は、相手の PKI ドメインを信頼する仕組みであり、特定のエンティティを信頼する仕組みではない。相手国側 PKI ドメインに属しているエンティティが特恵 ECO を発行したとしても、PKI 上は有効な特恵 ECO となってしまう。つまり、認証局間相互接続を行っただけでは、相手側 PKI ドメインに所属しているすべてのエンティティが特恵 ECO 発行者になりすます事ができるため、別途、特恵 ECO 発行者を特定するための仕組みが必要となる。そのための仕組みとして以下の方法が考えられる。

- 特恵 ECO 発行者リストの交換を行い該当する特恵 ECO の署名者がその特恵 ECO 発行者リストに記載されていることを確認する
- 属性証明書を利用し特恵 ECO 発行者の権限を保証する
- 特恵ECO発行者であることを特恵ECO発行者公開鍵証明書のどこかに明記する※5
- 特恵 ECO 発行者用認証局を設立しその認証局と認証局間相互接続することでこの問題を回避する

上記の方法を用いる場合は、実現するためのコスト、複雑さの相違や、各国の技術的・法制度的な相違を考慮する必要がある。特恵 ECO パイロットシステムにおいては、上記のどの方法でも特に問題が無かったが、もっともシンプルな「特恵 ECO 発行者リストの交換」方式を採用した。

(c) まとめ

以上をまとめると、特恵 ECO システムにおける完全性の確保には、PKI の適用および以下のようなビジネスルールが必要である事がわかる。

- 特恵 ECO 発行者の公開鍵証明書が何らかの理由で失効した場合の特恵 ECO の扱いについて（当該特恵 ECO 発行者が発行した特恵 ECO をすべて失効させて、新たに再発行する等）。
- 特恵 ECO 発行者公開鍵証明書の有効期間内に特恵 ECO 有効期間があり、特恵 ECO の有効期間内に特恵 ECO を検証すること。
- 特恵 ECO 発行者を特定する仕組みを導入すること。

※4 例えばCC方式でないと法制度上有効でない場合や、CC方式を利用するための証明書発行要求を発行できない場合等。

※5 certificatePoliciesに特別な値を入れることや、Subject やsubjectAltNameに属性を記載すること等を含む。

また、それぞれの要件に沿って見てみると、「表 6.1　要件対応表」のようになる。

表 6.1　要件対応表

	PKI によって実現	ビジネスルールによって実現
改ざんされないこと	署名者公開鍵証明書の有効期間内であれば、PKI を利用した電子署名にて実現する	署名者公開鍵証明書の有効期間内に当該文書を検証することを実現する
各エンティティが信頼できること	認証局間相互接続により相手ドメインのエンティティであれば信頼できる	特定のエンティティの証明書情報を交換することにより、相手ドメインの特定のエンティティを特定できる

以上の様なビジネスルールのもとで、特恵 ECO システムにおける完全性は確保可能になる。

(2) 「Asia PKI Interoperability Guideline」の再検証と提言

特恵 ECO パイロットシステムの PKI 環境構築において「Asia PKI Interoperability Guideline」に準拠して作業を行い、その過程で下記 1 点を課題として抽出した。これを「Asia PKI Interoperability Guideline version 1.0」への改善案として提示する。

(a) intermediate CA の証明書プロファイルの PolicyMappings

「Asia PKI Interoperability Guideline」の推奨する証明書プロファイルでは intermediate CA の PolicyMappings は指定必須となっているが、これを指定任意とするよう提案する。

本実証実験において、シンガポール認証局は中間認証局を持つ階層構造を取り、エンドエンティティ証明書は中間認証局から発行している。そのシンガポールの中間認証局の証明書は PolicyMappings を設定していない。

検証要件から見れば、階層構造の認証局間でポリシマッピングが必要なのは上下それぞれの認証局が異なるポリシを持ち、それらをマッピングして認証パスを構築しなければならない場合である。しかし現状の階層構造の認証ドメインの多くは今回のシンガポールのように厳密なポリシ運用を行っておらず、上下階層のポリシをマッピングする必要がない。これは当該認証ドメインが保証すべきセキュリティ要件を確保するためになんら問題があるものではない。その中で PolicyMappings を必須として設定を強制する仕様は十分な説得力を持つものではない。

よって、「Asia PKI Interoperability Guideline」を現実の運用に親和性のあるより広く受け入れられる推奨仕様とするために、すべての場合に一律にintermediate CA の PolicyMappings を指定必須とするのではなく、指定任意とするのが妥当であると考えるものである。

6.1.2 PKI 実利用のためのガイドラインの評価および考察

(1) 特恵 ECO フォーマットについて

今回のパイロットシステムにて策定した特恵 ECO は、シンガポール CrimsonLogic 社がすでに WCO に提案していたフォーマットをベースにして以下の観点からデータ項目の確認、必要となる項目の追加を実施した。

(a) 日本の書面特恵原産地証明書の記載項目との確認を行い、不足していた項目を追加

(b) 従来の書面文書を電子化することに対応するための管理項目を追加

(c) 安全で確実な国際間電子文書伝送を実現するための PKI 技術適用に必要となる項目を追加

今回検討された特恵 ECO フォーマットについて、日本およびシンガポールの 2 カ国間のみならず、アジア標準となるべき項目は網羅したと評価することができる。

ただし、今回検討した特恵 ECO フォーマットの項目については、すべての項目が必須項目というわけではない。実運用への導入の際には、実際にその特恵 ECO を取り交わす 2 カ国間において必須項目の調整が必要である。

(2) 特恵 ECO 運用について

(a) 発行（署名）の方式

本パイロットプロジェクトでは、承認行為（承認ボタン押下時）に使用する証明書を確認させた上で電子署名を実現している。

特恵原産地証明書の署名の意味合いからすると、署名者が知らない内に電子署名がなされるのではなく、意思を持って署名を付与する行為をすることが、重要であることが確認された。

(b) 本人確認

本パイロットプロジェクトでは本人確認についてスコープ外とし、言及していない。しかし、今回の仕組みを実現するためには IC カード等を用いた秘密鍵の利用が想定される。

(c) オリジナル／コピーの考え方

書面による特恵原産地証明書の場合には、使用される用紙、署名に使われるインクや筆跡により、原本とそのコピー機による複写は、区別することが可能である。原本に”ORIGINAL”表示をすれば、複写にも “ ORIGINAL"と表記はされるものの、それがコピーであることは一目瞭然である。

しかしながら、電子データをコピーした場合、複写元のデータと複写先のデータには、まったく区別はなく、書面を前提とした場合のような“ ORIGINAL”

の使い方は不可能である。

しかしながら、ビジネスにおいては、特恵原産地証明書のコピーを税関以外にも提出することがあるので、原本ではなく、「コピーとして流通している」ことを明示的に示すことに意味がある場合もある。

このような状況を想定して、データの項目として ORIGINAL や COPY についてのフラグを設けている。

(d) ライフサイクル（発行から保管/廃棄、無効となるまで）

特恵 ECO のライフサイクルについては、一般的な電子文書と同様に発行された後、特恵 ECO の有効期間、保存期間がある。長期保存に関しては本プロジェクトではスコープ外としたが、特恵 ECO の有効期限、特恵 ECO に付与する証明書の有効期限に関して評価を行った。詳細は「6.1.2(4)適用された技術について」を参照。

(e) 従来からの改善点および新たな問題点

(i) 手続きのスピード

書面による特恵原産地証明書の運用と特恵 ECO による運用を比較すると申請から発行までの手続きのスピード感は増すと考えられる。また、電子申請についても実現すれば、申請者の発行に係る負荷はさらに軽減される。

しかし、発行業務を行う機関に関しては、現実的に電子的な運用を実現する際、従来の書面運用を残さざるを得ないケースも多く、一概に業務の負荷は低くなるとは言いがたい。また、書面運用を残すケースの場合、情報を一元管理する面から発行機関にて代理入力を行うことも想定され、負荷が上がる要因となる。電子的な申請の割合が多くなれば全体的な負荷は書面運用よりも軽減するため、書面による運用を電子化する場合には、その普及が課題となる。

(ii) コスト削減

コストの削減の可能性として「保存コストの削減」「運用コストの削減」が考えられる。

書面運用による場合は書面の原本を物理的に保存する必要があるため、保管倉庫の管理費が必要となる。電子文書による運用が行われ、電子媒体による保存が可能になると、格段に少ない保管スペースで保存が可能となる。

運用コストについては、主に保存された書面を管理する人件費等が削減可能である。逆に電子文書の管理に係る人件費等については新たに発生するが、管理や輸送コスト等、書面と比較すると軽微な量である。

また、統計データ等、申請情報や発行情報についてデータの再利用を行う際には、電子データを元に作成する方が圧倒的に容易である。

ただし、書面運用と電子文書運用を併用する場合、状況によっては書面運用のみの時よりもコストが増加する場合もあるため、「(i)手続きのスピード」と同様、電子文書運用の普及が不可欠である。

(iii) 確実性、安全性

PKI 技術を用いた伝送を行うことは、書面による運用と比較して、確実性、安全性両面から有益であると考えられる。書面による脆弱性であった改ざんの容易性や、第三者に参照される恐れがある点を電子署名および暗号化により防ぐことが可能である。

また、サービスにおける信頼性の向上につながり、情報漏えい等の原因となり得る外部からの脅威に対しても、効果があると言える。

(3) パイロットシステムについて

(a) ASP モデルの妥当性

本パイロットプロジェクトで採用した特恵 ECO 持ち回り ASP モデルは、今回のような国際間の電子文書交換において重要かつ困難である国際間の調整範囲が、それぞれの国の ASP 間に集約できる点が利点と言える。現状ではこの ASP モデルは有効であると評価できる。

(b) 証明書交換方式

国際間の伝送に用いられる PKI に必要な証明書等を国際間の外交ルート等の場を用いて交換する方式が現実的な案であると想定し本パイロットプロジェクトを行った。国際間で取り交わされる証明書は信頼できる機関より入手することが必要であるが、国対国の取引の場合、外交ルートを用いることが比較的容易に実現可能であると考えられる。

(c) 特恵 ECO 持ち回り方式

電子署名を付与した特恵 ECO を持ち回り、利用者が検証を行い、その真正性を確認する仕組みは PKI 技術を存分に活用した方式であり、かつ信頼のおける方式であると考えられる。ただし、全てのプレーヤーがこの環境を整えるには課題もあり、(a)のような ASP モデルと組み合わせ、ASP にて検証サービスも提供する等すれば、この問題も軽減されると考えられる。

(d) 書面イメージ公開方式

書面における運用時の真正性を高めるために有効であると考えられる。現在の書面による運用を残さざるを得ない場合や、電子化への途中の段階にて有効と考えられる。導入に際しては基幹となる機関のみとなるため比較的容易に実現が可能である。

(4) 適用された技術について

(a) 特恵 ECO の有効期限の考察

書面の特恵原産地証明書には有効期限が記載されていないが、規約により日本の特恵原産地証明書の有効期限は発行日から 1 年間である。このため電子化された特恵 ECO についても有効期限の概念が必要とされる。

シンガポールと特恵 ECO のフォーマットを策定するにあたり、当初有効期限の項目は存在していなかったが、特恵 ECO に付与される署名・証明書には付与された日付情報が格納されており、この日付を特恵 ECO の発行日付と考え、システム側で有効期限を算出して運用することが協議された。

しかしながら、有効期限は特恵 ECO 発行国の発行機関がいつまでその発行責任を負うかが国によって違う可能性があること、および将来的に有効期限の期間が変更されても発行側システムが責任をもってその有効期限を格納することで受信国側に大きなシステム改変を発生させないという観点から、特恵 ECO のデータフォーマットに有効期限の項目を追加した。

(b) 証明書の有効期限についての考察

本パイロットプロジェクトでは特恵 ECO の有効期限と証明書の有効期限が明らかな矛盾を起こすケースについては、特恵 ECO の発行自体をできないように設計を行った。つまり、特恵 ECO の有効な期間を十分に包括する期間を持つ証明書にて署名を行うものとした。この問題は長期保存も含めた運用ルールに依存する部分も多いが、特恵 ECO を保証する上で、特恵 ECO の有効な期間を十分に包括する期間を持つ証明書を用いることが有効であることを確認した。

(c) 保存期間の問題

特恵 ECO の有効期限を超えて保存を行う必要があると想定されるが、長期保存に関する検討は本パイロットプロジェクトではスコープ外とした。ただし、実装時には他の電子文書と同様に長期保存の仕組みを検討・構築しなければならない。

(d) S/MIME 伝送方式

(i) 広く普及しており、利用者人口が大きいことから利用者の使用に抵抗感が少ないと推測されること

(ii) 暗号化が実装されており比較的簡単に利用できること

(iii) 署名が簡単に付与できること

以上の観点より、S/MIME 伝送方式が本プロジェクトにて採用された。

ただし、通信プロトコルについては「真正性」「秘匿性」が確保できるならば、

他のプロトコルの採用でも問題ない。

(e) 検証方式

本パイロットプロジェクトでは、特恵 ECO の利用者が個別に検証を行うのではなく、特恵 ECO の検証は ASP が行い、各利用者へは ASP が検証サービスとして提供するモデルとした。このため、利用者の全てに検証を可能とする環境が必要ではなく、利用に対しての敷居を低くする効果が得られると考えられる。

6.2　成果および今後の展開

6.2.1 PKIの国際的相互接続に関する手引の実証実験における成果

平成 15 年度までの実証実験では、IWG プロファイルおよびコンポーネント間インターフェース、認証局間相互接続テスト手法が確立された。これらはすべて実証実験において確認されており、その有効性は確認されている。その中で、電子調達アプリケーションを用いた実験を行ってきたものの、あくまで仮想的な実験であった。

そこで、本年度は国際的な電子文書交換業務において、様々な業務に係る要件がある中で、今までの成果を適用することにより、その有効性を再確認するとともに、「Asia PKI Interoperability Guideline の利用に関する手引」を作成し、Asia PKI Interoperability Guideline の実ビジネスでの利用を助ける情報をまとめた。Asia PKI Interoperability Guideline の実ビジネスへの適用による主な成果を以下に述べる。

(1) 実ビジネスにおけるPKIの適用により実現可能な範囲の明確化

実ビジネスに PKI を適用する時に求められるのは主に情報の機密性と完全性である。特に完全性保証では当該情報が下記条件を同時に満たしていることが求められる。

- 信頼し得るエンティティによって当該情報が作成されていること
- 当該情報が改ざんされていないこと

これらの条件は PKI 技術のみでは実現不可能であり、付随する適切なビジネスルールがあって初めて実現できる。様々な業務要件の存在する国際的電子文書交換業務において、PKI 技術によって実現できる部分とビジネスルールによって実現できる部分の棲み分けが明確化されたと言える。

(2) Asia PKI Interoperability Guidelineの再検証

仮想的な電子商取引の実験とは異なり、国際的な電子文書交換業務において、様々な業務に係る要件がある中で、今までの成果を適用することにより、具体的には以下の項目について、その有効性を再確認できた。

- APKI 公開鍵証明書プロファイルの有効性
- コンポーネント間インターフェースの有効性
- 認証局間相互接続方式の有効性
- 認証局間相互接続テスト手法の有効性

再検証により「6.1.1PKI の国際的相互接続に関する手引の評価および考察」に示すように１点改善できる箇所を抽出し、改訂案として提示した。

(3) Asia PKI Interoperability Guidelineの利用促進

これまでの活動を通して技術仕様として確立した Asia PKI Interoperability Guideline の次の課題は、広く利用してもらうことである。その一助となる副読本として「Asia PKI Interoperability Guideline の利用に関する手引」を作成した。パイロットシステムのための PKI 構築の作業フローごとに、国際的な電子文書交換の業務要件を勘案しながら Asia PKI Interoperability Guideline を参照するケーススタディというアプローチを取っている。これにより Asia PKI Interoperability Guideline を目的に応じて参照する具体例を示した。また作業フローに合わせて参照すべき関連箇所を明示することで、情報の見落としなく Asia PKI Interoperability Guideline の情報が活かされる。

「Asia PKI Interoperability Guideline の利用に関する手引」は、Asia PKI Interoperability Guideline の有効性をより高め、利用者の便宜を図るものである。

6.2.2 PKI 実利用のためのガイドラインの実証実験における成果

貿易手続きの簡素化や電子化が APEC をはじめ、ASEAN においても推進されているが、国際間で流通可能な特恵原産地証明書の電子化は実現していない。

現在の日本を取り巻く貿易情勢としては、FTA または EPA の締結が推進されており、特恵原産地証明書の役割が重要になる。電子化された特恵原産地証明書の輸出国による発行から輸入国税関での受理およびその安全な搬送経路の確保に対する必要性は今後高まることが予想される。

今回のパイロットプロジェクトは 2 カ国間で授受される貿易文書の中で特恵原産地証明書を対象にして電子文書化を行うべく、パイロットプロジェクトの協力国であるシンガポールと共同で特恵 ECO のデータ形式に XML フォーマットを使用して策定、また安全に、確実に、かつシンプルな形での伝送をインターネット利用と PKI 技術の適用により可能とすべく、パイロットシステムを構築して、その有効性検証を行った。

(1) 国際間での電子文書交換

今回のパイロットプロジェクトで得られた第 1 の成果は国際間実ビジネスを想定した環境で、実ビジネスに携わる関係者の意見を踏まえた上で、国際間の PKI 技術の適用を実施したことである。

今回のパイロットシステムはいまだ実現していない電子文書交換の領域を、小規模ながら PKI 技術を用いて実現したことにより、国際間で有効な貿易手続きのコンセプトを確立することができたと評価できる。

なお、今回は、国際間の電子文書の交換に重点を置いているため、国内における特恵 ECO の電子申請については対象としていないが、実ビジネスにおける運用にあたっては、この分野も当然電子化の対象となるものである。

(2) PKI 普及のための情報発信

第 2 の成果は「特恵原産地証明書の電子化に係るガイドライン」の作成により、PKI 普及のための情報発信が可能となったことである。今回上記ガイドラインでは電子文書の交換方法および PKI 技術の適用範囲の策定にいたるまでの経緯についても記述している。これを記述しておくことにより、同様の課題を持つ者に対して十分な情報提供ができるようになった。

本プロジェクトにおいて得られた情報は以下の活動を通じて PKI 技術の普及の観点から情報共有活動を行う必要がある。

(a) アジア PKI フォーラムに対して本プロジェクトを通じて得た知識、ノウハウの情報発信・共有を行う。
(b) eASEAN および APEC のワーキンググループ等に対して本プロジェクトを通じて得た知識、ノウハウの情報発信・共有を行う。

(3) 特恵 ECO の有用性

第 3 の成果は、本パイロットプロジェクトで策定した特恵 ECO のフォーマットおよびシステムの実装については、汎用的なモデルとなっており、今後、各国の商工会議所や税関に対して、有用な情報と資源を提供することが可能となったことである。アジア各国やメキシコに対して、本パイロットプロジェクトの成果を活かし、実システムの効率的な開発の推進を行うことが期待される。

以上