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

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。

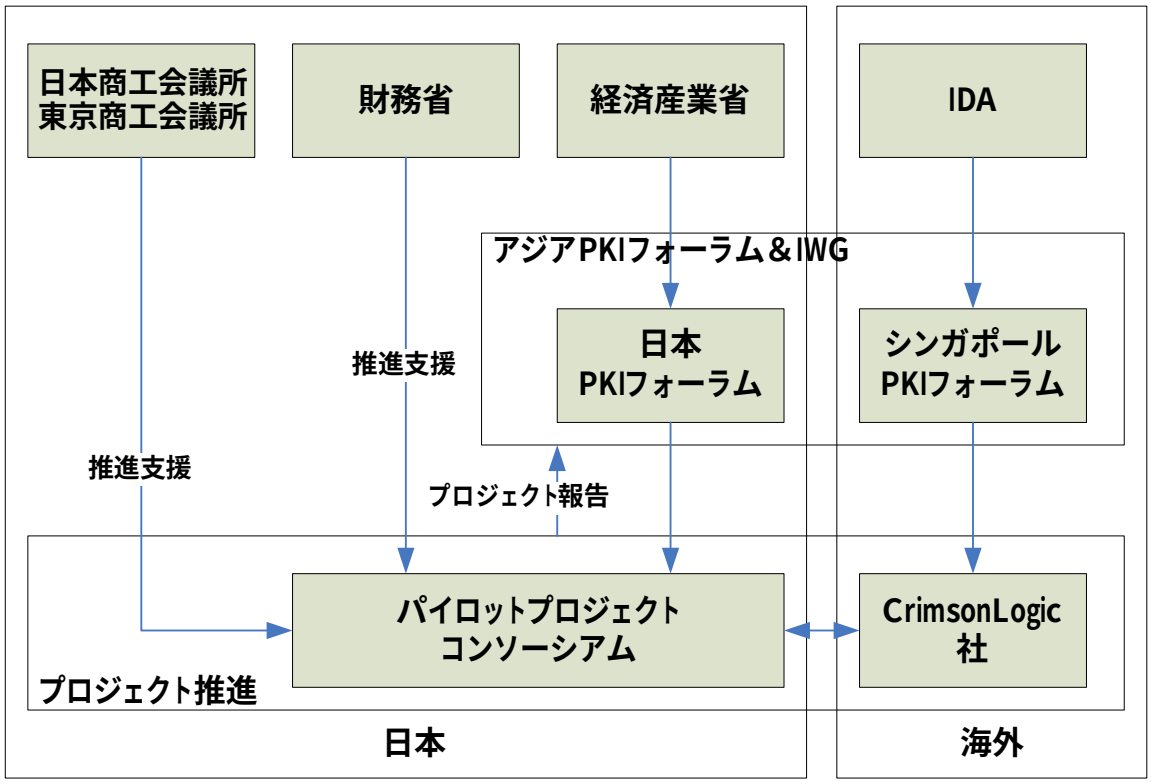

図 2.1　プロジェクト推進体制図

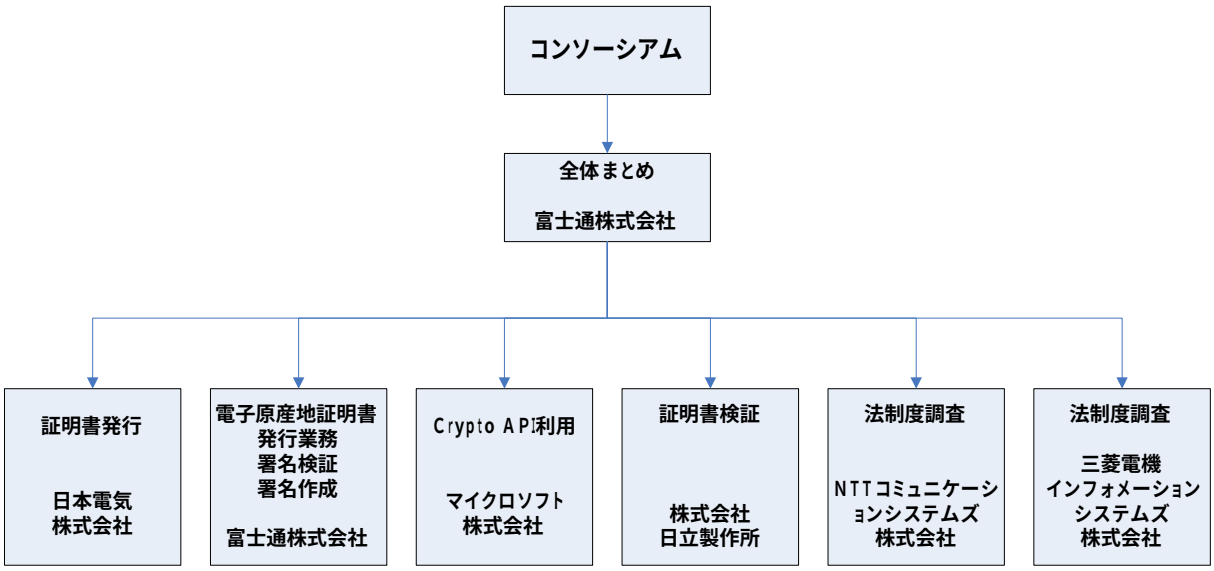

図 2.2　コンソーシアム体制図

※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

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。

- マレーシア
- シンガポール
- 韓国
- フィリピン
- タイ

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。

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。

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。

4.2 PKI 環境概要

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。

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

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。

4.3.2 仮想対象国との相互接続における検証

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。

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。

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。

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。

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

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。

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

「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。

6.2 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。