経済産業省補助事業

平成１４年度情報セキュリティ対策推進事業

「電子商取引（ＥＣ）技術基盤の相互運用性に関する調査研究」

PKI の国際的相互接続実証実験報告書

平成 15 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、各国で加速的に進められており、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貢献をもたらすものと期待されている。

しかしながら、PKI を使用した国際間相互認証に関する分野において、特にアジア地域においては現在 PKI が構築されつつあるが、PKI の構築方法は各国の事情に応じて構築されることから、統一されていないのが現状である。

そこで、平成 12 年度事業としてアジア圏の中で PKI の整備が進んでいる韓国、シンガポール及び日本の間で、PKI の相互接続の実証実験を実施した。1 つの PKI ドメインの中に相互認証と相互承認のモデルが併存するハイブリッドモデルを採用し、ここで得た成果を現在、3 国の推奨仕様として PKI 国際組織等に提案しているところである。

しかしながら、実験で顕在化した技術的な課題が残されたままであり、国際的な認証基盤としてはまだ実験対象国が少ないこと、アプリケーションで PKI を活用するにはアプリケーションとのインターフェースについて検証する必要がある等の課題が残されている。

国際間での本格的な電子商取引を実現するためには、上記課題を解決し、PKI 技術に関する国際間相互接続の基盤整備を行うことが、必須かつ急務である。

本実証実験は、5 国／地域における相互認証基盤の確立を目的とし、今後アジア圏における相互認証基盤の普及並びにグローバルな電子商取引市場の創出を目指すものである。

2 プロジェクト概要

2.1 期間

2002 年 8 月 9 日～2003 年 3 月 7 日

2.2 体制

本実証実験の参加国／地域と推進組織を「表 2.1 体制」に示す。これら組織により IWG(Interoperability Working Group)が構成された。

表 2.1 体制

参加国／地域	組織
日本	日本 PKI フォーラム
韓国	Korea PKI Forum
シンガポール	PKI Forum Singapore
チャイニーズ台北	Chinese Taipei PKI Forum
香港チャイナ	Hong Kong PKI Forum

2.3 活動概要

相互接続基盤の整備にあたり、以下の活動を実施した。

- シンガポール、韓国、チャイニーズ台北、香港チャイナ、日本における PKI コンポーネント間接続に関する標準案、及び、PKI アプリケーションに関する標準案を作成
- PKI コンポーネント間接続に関する標準案について PKI Forum Singapore、Korea PKI Forum、Chinese Taipei PKI Forum、Hong Kong PKI Forum、及び日本 PKI フォーラムの参加団体のメンバを含む各国／地域技術者と調整
- PKI アプリケーションに関する標準案について PKI Forum Singapore、Korea PKI Forum、Chinese Taipei PKI Forum、及び日本 PKI フォーラムの参加団体のメンバを含む各国／地域技術者と調整
- 標準案の実用性及び有効性を、国内シミュレーションセンタ並びに現地実証実験環境にて検証
- 実証実験の成果を標準案にフィードバックし、標準を作成

3 標準作成

3.1. PKI コンポーネント間接続に関する標準（相互接続インターフェース仕様）

認証局の設計担当者が、相互接続の設計作業における PKI コンポーネント間の接続インターフェースの要件を検討する際に使用する標準の策定を行った。

3.2. PKI アプリケーションに関する標準（パス検証テストガイドライン）

認証局の設計担当者及びソフトウェア開発者がアプリケーションにおける証明書検証方法の設計作業において必要となる検証要件、及び評価作業におけるテスト項目を検討する際に使用する標準の策定を行った。

4 シミュレーションセンタにおける認証局間の実証実験

相互接続のために認証局間で交換する証明書発行要求と相互認証証明書は、相手認証局が受け入れることができるものでなければならず、また相手認証局が発行した情報を受け入れることができなければならない。また、相互接続を行った認証局ドメイン間ではエンドエンティティ証明書が相互に利用可能であり有効性検証が可能でなければならない。これを保証するために、認証局の運用者は「(相互接続インターフェース仕様」に従って証明書の発行、失効、更新及び再発行を行う。認証局が発行した証明書、相互認証証明書ペア、CRL及びARLは、認証局のポリシに応じてリポジトリにより公開される情報である。PKI を利用するアプリケーション等の利用者が必要な証明書や証明書の失効情報を取得できるようにリポジトリに情報を格納する必要がある。これを保証するために、認証局の運用者は「(相互接続インターフェース仕様」に従ってディレクトリサーバの運営を行った。

認証局が「(相互接続インターフェース仕様」に従って証明書のライフサイクル管理を行うことにより相互接続の関係を構築できることを確認することで、認証局の運用者にとっての標準の実用性を検証した。

5 シミュレーションセンタにおける証明書検証の実証実験

国際間の電子商取引等を行うアプリケーションを利用するにあたって、利用者は相手方

から受け取った証明書が有効なものであるかどうか、受け取った証明書が信頼できる認証局から発行されたものであるかどうかについて検証しなければならない。この証明書検証に、PKI コンポーネントのひとつである検証局へ問合せを行い検証する方式（以下、VA モデルという）を適用するケースがある。

本実験単位では、「相互接続インターフェース仕様」に則って、実際に証明書の検証を実施することで、「相互接続インターフェース仕様」が利用者にとって実用的であるか否かを検証した。証明書の検証には検証局を使用した。また、実験にはシミュレーション環境を利用した。

6 シミュレーションセンタにおける国際間調達の実証実験

「相互接続インターフェース仕様」をシミュレーションセンタにおける国際間調達の実証実験の観点から、利用者にとって実用的か否かについて検証した。

国際間調達業務における業務シナリオを設定し、日本のシミュレーションセンタ内で、利用者端末を使用し、日本国認証局が発行したエンドエンティティ証明書を保有するエンドエンティティ、日本のシミュレーションセンタ内のチャイニーズ台北認証局が発行したエンドエンティティ証明書を保有するエンドエンティティ、日本のシミュレーションセンタ内の香港チャイナ認証局が発行したエンドエンティティ証明書を保有するエンドエンティティの間で買い手、売り手の立場を入れ替えて実証実験を行った。

各国／地域利用者端末と業務サーバで採取されるログ情報より検証内容を含むデータを収集し解析することで、「相互接続インターフェース仕様」の実用性を検証した。

7 現地環境における認証局間の実証実験

相互接続に係わる証明書のライフサイクル管理を通しての「相互接続インターフェース仕様」の有効性を検証した。

認証局が「相互接続インターフェース仕様」に従って相互接続に関する証明書の発行等を行うことにより相互接続の関係を構築できることを確認することで、認証局の運用者にとっての標準の有効性を検証した。

8 現地環境における証明書検証の実証実験

国際間の電子商取引等を行うアプリケーションを利用するにあたって、利用者は相手方から受け取った証明書が有効なものであるかどうか、受け取った証明書が信頼できる認証局から発行されたものであるかどうかについて検証しなければならない。この証明書検証に、PKI コンポーネントのひとつである検証局へ問合せを行い検証する方式（以下、VA モデルという）を適用するケースがある。

本実験単位では、「相互接続インターフェース仕様」に則って、実際に証明書の検証を実施することで、「相互接続インターフェース仕様」が利用者にとって有効であるか否かを検証した。証明書の検証には検証局を使用した。

9 現地環境における国際間調達の実証実験

「相互接続インターフェース仕様」を現地環境における国際間調達の実証実験の観点か

ら、利用者にとって有効か否かについて検証した。

国際間調達業務における業務シナリオを設定し、現地環境で、日本製アプリケーションをベースとした利用者端末を使用し、現地実証実験日本国認証局が発行したエンドエンティティ証明書を保有するエンドエンティティと、現地チャイニーズ台北認証局（中華電信及び TaiCA）が発行したエンドエンティティ証明書を保有するエンドエンティティ、現地香港チャイナ認証局が発行したエンドエンティティ証明書を保有するエンドエンティティの間で買い手、売り手の立場を入れ替えて実証実験を行った。

各国利用者端末で採取されるログ情報より検証内容を含むデータを収集し解析することで、「相互接続インターフェース仕様」の有効性を検証した。

10 現地環境におけるパス検証テストガイドラインの実証実験

現地実証実験環境において、利用者に「パス検証テストガイドライン」を利用してもらい、パス検証テストを実施した。これにより、「パス検証テストガイドライン」の有効性の確認を行った。

11 成果

11.1 PKI コンポーネント間接続に関する成果

(1) CC 及び CR ハイブリッドモデルの適用地域の拡大

昨年の実証実験で規定した Cross Certification(CC)と Cross Recognition(CR)のハイブリッドモデルを本年度実証実験の接続モデルとし、地域拡大に対するモデルの有効性検証を行った。本実証実験を通じてモデルの核である認証スキームや検証形態を崩すことなく、接続相手の拡大に適用できることを実証した。

(2) 相互接続における重点テスト項目の特定と共有

相互接続相手国の数を増やすことによって、相互接続を行う場合必ず陥るポイントやパターンを絞ることが可能となり、テストを行わなければならない範囲を明確にすることができた。そして、その対策として仕様への反映やテスト項目への盛り込み等を行った。

(3) 他国の政府認証基盤との親和性確保

今回採択した IWG モデルは、相互認証技術に関して実績のある日本の GPKI 相互運用性仕様を参照している。その IWG モデルは、今回チャイニーズ台北側の GPKI との親和性を確保することができた。

(4) ブラウザベースのサービスへの拡張

今回使用した証明書プロファイルは、ウェブブラウザベースの製品にも対応できるよう設計されている。本実証実験において、ウェブブラウザベースの制限された PKI 機能の環境下においても、証明書プロファイルが適用できることを確認した。実際にはウェブブラウザに標準実装されているメーラーの S/MIME 機能を使い、そのサービスの有効性を確認することができた。

11.2　PKI アプリケーションに関する成果

(1) テストパターン最適化のための相互接続環境の体系化

パス検証テストガイドラインは、典型的な相互接続環境をモデルとして定義し、そのモデル毎に必要なテスト要件及び関連したテスト項目を定義したものである。

適切なテスト項目を抽出するには、適切な相互接続環境の選択/分析が重要となる。

X.509 や RFC3280 などの標準に記述されたパス検証ロジックは、そもそもどのような環境でも均一な検証結果を得られるように、非常に汎用的に記述されている。これは実装するベンダーにとっては大きな負担であり、多くの実装がサブセットにしかすぎないという現状がある。これは評価する側にとっても同じことであり、ある環境において評価すべきテスト要件を抽出することは非常に高度なスキルを要求される。

そのため本ガイドラインでは典型的な相互接続環境(モデル)を定義している。これらのモデルは、

- CA-CA 間の相互接続形態
- 失効・検証情報の提供方法
- 証明書を用いたサービス内容

といった 3 つの観点から体系化されている。複数の観点から体系化することで適用範囲を広げ、汎用的なガイドラインとすることができた。

(2) パス検証機能に対する評価指標の確立

パス検証ガイドラインは、X.509 や RFC3280 などの標準に記述されたパス検証ロジックに基づいたテストケースの集合として設計した。

本実験では、今まで CA-CA 接続実験で使用してきた Cross Certification や Cross Recognition などについてガイドラインからテストケースを抽出し、CA-CA 接続実験で使用してきた各アプリケーションや検証局でそれぞれのテストケースを実行し、各アプリケーションや検証局が標準に忠実なパス検証機能を実装していることが確認できた。

(3) 署名・検証処理 API のインターオペラビリティ確保

昨今の PKI 推進活動は国の内外を問わず盛んであり、具体的な活動としてはアメリカにおける OASIS（旧 PKI フォーラム）、EU 圏における EESSI、国内における GPKI、LGPKI、JACIC、公的個人認証などが挙げられる。これらの状況において、PKI を活用する PKI アプリケーションの観点で見た場合、特定の仕様或いは特定の製品に依存した PKI アプリケーションとなることも多々見受けられる。このような場合、ある PKI アプリケーションサービスを利用するには利用者が PKI アプリケーションの要求を満たす署名・暗号機能をインストールする等の作業が必要となり、PKI アプリケーションごとにクライアント環境を構築する必要があるなどの煩雑さを増す要因となる。

1 国内で使用する場合にはこのような問題がある。また国際間で１つの PKI アプリケーションサービスを利用しようとした場合、クライアントで準備する必要がある署名・暗号機能は輸出規制の対象となり、特定の製品に依存する PKI アプリケーションを構築することは実用的ではない。また、PKI アプリケーションが各国で使用可能な署名・暗号機能を使用するには、署名・暗号機能の仕様が統一されていないことから、PKI アプリケーションの構築が不可能となるという問題がある。

これらの問題は、国際間における PKI アプリケーションの普及を妨げる要因であり、

国際間における PKI アプリケーションを普及させるにはこれらの問題解決を行うことが最大の課題であると言っても過言ではない。国際的な標準に基づいた上で、最低限の共通ルールを設定する必要がある。これらの課題を解決する目的で署名用トークンインターフェース仕様を策定した。

署名用トークンインターフェース仕様は、OS に関してオープンプラットフォームである PKCS#11 に基づいた機能仕様として設計した。具体的には、PKCS#11 で使用する機能の定義、各国の環境面の差異及び開発言語の差異を吸収する機能の定義、アプリケーション開発の容易性を高めるインターフェースの定義を行った。

本標準の有効性を確認するための実験では、テストアプリケーションを作成し、各国の PKCS#11 ライブラリを使用してテストアプリケーションへアクセスすることで本標準のすべての機能についての検証を行い、本標準の有効性を確認することができた。このことは、本標準が国際間のインターオペラビリティを確保していることを証明していると言うことができる。

本標準を使用することで、国際間の PKI アプリケーションを利用する上で各国の既存の PKCS#11 ライブラリをそのまま使用することができ、電子署名を有効的に活用することが可能となる。

以上より、本標準は、PKI アプリケーションの国際間での流動性を高め普及を推進するための 1 つの突破口を開いたという点で高く評価することができると考える。