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

序

公開鍵認証基盤（PKI：Public Key Infrastructure）は、インターネット上で電子商取引を安全かつ確実に実現する技術として、世界の経済社会に大きな貢献をもたらすものとして期待されている。しかしながら、各地で進められている PKI を利用したプロジェクトや実証実験では、各々が置かれた環境の要件に従って独自に行われているのが現状である。こうしたなかで、アメリカやヨーロッパでは PKI を地域で統一する動きが始まっており、日本でも政府認証基盤（GPKI）を中心とした PKI 相互接続の動きが開始されている。しかしこれまでのところアジア地域では PKI の統一に向けた動きが活発に行われているとは言い難く、PKI 普及の大きな阻害要因となっていた。日本情報処理開発協会では平成 12 年度事業として、韓国、シンガポールとともに PKI で使用される証明書を発行する認証局（CA：Certificate Authority）の国際的相互接続の実験をおこなってきたが、この動きを加速し内容を充実させながら継続してゆくことが、各国・地域の境を越えたアジア圏での共通な PKI の実現に向けた大きな原動力になるものと考える。

本事業は、このような目的のもと、経済産業省の補助金を受け、従来の韓国、シンガポールに加えてチャイニーズ台北、香港チャイナを実験の対象とし、実験内容についても従来の国際的な CA 間相互接続だけにとどまらず、証明書が実際に使用される際の処理に着目してテスト項目を拡大して行ったものである。

平成 15 年 3 月

財団法人 日本情報処理開発協会

— 目 次 —

— 表 目 次 —

— 図 目 次 —

― 付　録 ―

- 付録 1 PKI コンポーネント間接続に関する標準
  - 1-1 相互接続インターフェース仕様

- 付録 2 PKI アプリケーションに関する標準
  - 2-1 パス検証テストガイドライン
  - 2-2 署名用トークンインターフェース仕様

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)が構成される。

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

顕在化した技術的な課題の解決を含む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

本報告書では、活動の概要と実証実験の結果を記述する。策定した標準は付録として添付する。

3 標準作成

本実証実験では、以下に示す 2 つの標準を作成する。

- PKI コンポーネント間接続に関する標準
- PKI アプリケーションに関する標準

PKI コンポーネント間接続に関する標準には以下の標準を含む。

- 相互接続インターフェース仕様（「付録 1-1」として添付）

PKI アプリケーションに関する標準には以下の標準を含む。

- パス検証テストガイドライン（「付録 2-1」として添付）
- 署名用トークンインターフェース仕様（「付録 2-2」として添付）

3.1 PKI コンポーネント間接続に関する標準

3.1.1 相互接続インターフェース仕様

本標準は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である。

標準書の要約を以下に示す。詳細は「付録 1-1 相互接続インターフェース仕様」として本標準を添付するので参照のこと。

(1) 昨年度 IWG プロファイルとの違い

本標準は、相互接続を行う時に、より相互運用性を高めるために、昨年度プロファイルから以下に示す点について変更を行う。また、より適用性の高い標準とするために、実験を 2 つのフェーズに分けてパラメータを変更して実験を行う。

GPKI 相互運用性仕様に準拠する範囲内での変更を以下に示す。

表 3.1 昨年度プロファイルからの変更点(GPKI 相互運用性仕様範囲内)

ルート認証局証明書			
領域名	昨年度 プロファイル	今年度 プロファイル	理由
authorityKeyIdentifier	mandatory	optional	RFC3280 の記述に従い変更する。
keyUsage	mandatory	optional	RFC3280 において定義されている証明書検証では検証対象では無いため。詳細は 16.2.2(4)の考察に示す。
certificatePolicies	mandatory	optional	

cRLDistributionPoints	mandatory	optional	通常、ルート認証局証明書の失効情報の配布には失効リストを用いないため。

以下に関しては、各国／地域との相互接続における相互運用性を重視し、GPKI 相互運用性仕様の範囲外となる変更を行う。

表 3.2　昨年度プロファイルからの変更点(GPKI 相互運用性仕様範囲外)

相互認証証明書、中間認証局証明書、EE 証明書			
領域名	昨年度 プロファイル	今年度 プロファイル	理由
cRLDistributionPoints	mandatory	optional	多様な失効リスト配布ポリシに対応するため。詳細は16.2.1(3)を参照のこと。
issuingDistributionPoint	mandatory	optional	
certificatePolicies	critical	either critical or non-critical	既存アプリにおいて利用可能とするため。[1]

以下に関しては、GPKI 相互運用性仕様では曖昧な点である。アプリケーションの相互運用性を確保するために、以下の項目について明確にする。

- LDAPURI における attribute;binary の記載について

  昨年度プロファイルでは、attribute;binary は必須となっていたが、本年度は 16.2.1(5)の考察に従い、

  ldap://example.tld[:portnum]/dn?attribute[;binary]

  と定義する。本項目の実現性の確認のために、実証実験においては、実験をフェーズ 1 及びフェーズ 2 に分けて行うことで、attribute 及び binary の有無についてすべてのパターンを検証する。

(2) コンポーネント間インターフェース

本標準が想定する相互接続モデルにおいて現れる対象エンティティ、エンティティ間の通信インターフェース及びデータ形式について定義する。概要を「図 3.1 PKI コンポーネント」に示す。

[1] Microsoft Windows 2000 OS 以前の Windows OS では利用できないことが知られている

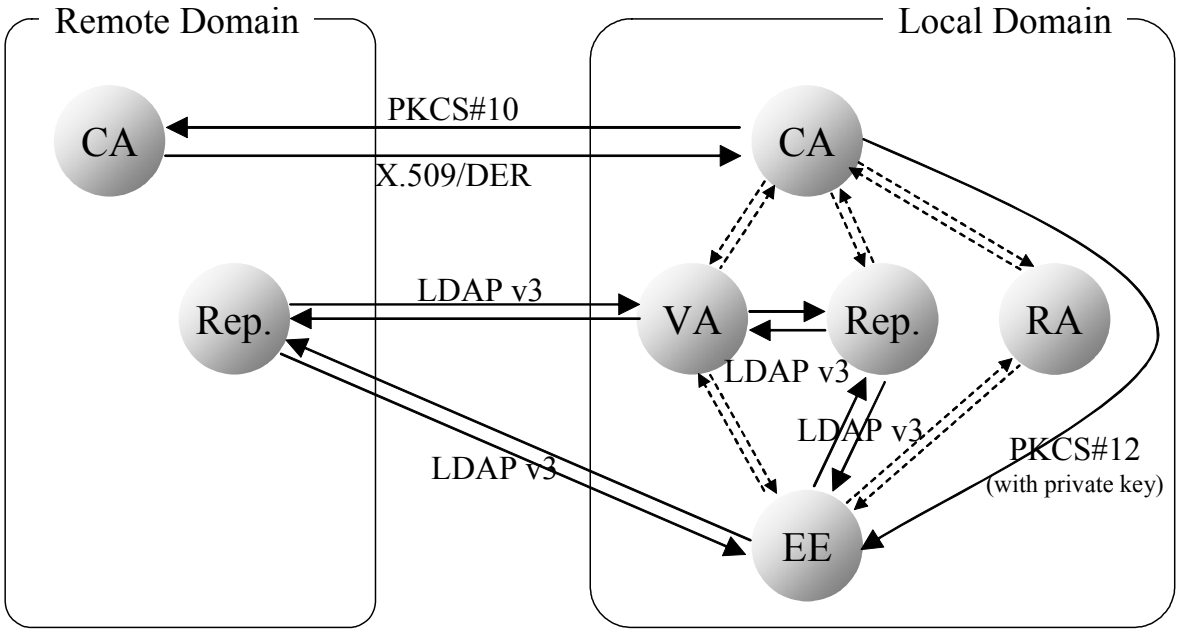


図 3.1　PKI コンポーネント[2]

(a) CA 間インターフェース

CA 間インターフェースを「表 3.3　CA 間インターフェース」に示す。

表 3.3　CA 間インターフェース

Content	Interface
Certificate profile	X.509(97) v3[x509], RFC3280[3280]
Certificate encoding format	DER[x690]
CRL profile	X.509(97) v3, RFC3280
CRL encoding format	DER
Cross-Cert request format	PKCS#10[p10]
Cross-Cert response format.	X.509/DER
The method, which sends the fingerprint.	E-Mail
POP (proof of possession)	Verification of digital signature on certificate request format

[2]破線部分は本標準の範囲外であり、本標準は実線部分のみを規定するものである。

(b) CA-EE 間インターフェース

CA-EE 間インターフェースを「表 3.4　CA-EE 間インターフェース」に示す[3]。

表 3.4　CA-EE 間インターフェース

Content	Interface
EE Certificate response format	PKCS#12[p12] (Private-key included)

(c) EE-リポジトリ間インターフェース及びVA-リポジトリ間インターフェース

EE-リポジトリ間インターフェース及び VA-リポジトリ間インターフェースを「表 3.5 EE-リポジトリ間インターフェース及び VA-リポジトリ間インターフェース」に示す。

表 3.5 EE-リポジトリ間インターフェース及び VA-リポジトリ間インターフェース

Content	Interface
Repository access protocol (e.g., LDAPv2, LDAPv3, DAP)	LDAPv3[2251]

(3) プロファイル

本標準が想定する相互接続モデルにおいて利用される証明書プロファイルについて定義する。

(a) 自己署名証明書

(i) 証明書基本領域

表 3.6　自己署名証明書　証明書基本領域

FIELD	NOTE
version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 2 (v3).
serialNumber (Mandatory)	unique integer. up to 20 octets.
signature (Mandatory)	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)

[3] 本標準においては、CA が EE の鍵ペアを生成することを前提とし、EE が CA に対して証明書リクエストを送付する場合は範囲外とする。

issuer (Mandatory)	X.500 DN. Although DN is generally encoded by UTF8STRING, according to description of the X.520(2001), Country attribute is encoded by PrintableString.
validity (Mandatory)	UTC TIME
subject (Mandatory)	X.500 DN. and see issure.
subjectPublicKeyInfo (Mandatory)	1.2.840.113549.1.1.1 (rsaEncryption) CA: 2,048bit
issureUniqueID (not used)	
subjectUniqueID (not used)	

(ii) 証明書標準拡張領域

表 3.7　自己署名証明書　証明書標準拡張領域

FIELD	NOTE
authorityKeyIdentifier (optional, non-critical)	**keyId(Mandatory):** The hash value of Issuer's public key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2. **authorityCertIssuer(optional):** DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
subjectKeyIdentifier (Mandatory, non-critical)	The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage (optional, critical)	When used, keyCertSign and cRLSign should be included at least.
extKeyUsage (not used)	
privateKeyUsagePeriod (not used)	
certificatePolicies (optional, critical)	When used, policyID MUST be present.

policyMappings (not used)	
subjectAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
issureAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
subjectDirectryAttributes (not used)	
basicConstraints (Mandatory, critical)	cA=TRUE pathLen=optional (INTEGER)
nameConstraints (not used)	
policyConstraints (not used)	
cRLDistributionPoints (optional, non-critical)	directoryName, URI
authorityInfoAccess (optional, non-critical)	If the PKI domain uses OCSP, this field will be used.
inhibitAnyPolicy (not used)	
freshestCRL (not used)	
subjectInfoAccessSyntax (not used)	

(b) 相互認証証明書

(i) 証明書基本領域

自己署名証明書を参照

(ii) 証明書標準拡張領域

表 3.8　相互認証証明書　証明書標準拡張領域

FIELD	NOTE
authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2 **authorityCertIssuer(optional):** DN

	authCertSerialNum(optional): INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
subjectKeyIdentifier (Mandatory, non-critical)	The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage (Mandatory, critical)	keyCertSign, cRLSign
extKeyUsage (not used)	
privateKeyUsagePeriod (not used)	
certificatePolicies (Mandatory, ether critical or non-critical[4])	policyID MUST be present.
policyMappings (Mandatory, non-critical)	
subjectAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
issureAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
subjectDirectryAttributes (not used)	
basicConstraints (Mandatory, critical)	cA=TRUE pathLen=optional (INTEGER)
nameConstraints (optional, critical)	
policyConstraints (optional, critical)	If the PKI domain wants to strictly validate certificate policies, this field will be set as requireExplicitPolicy=0.
cRLDistributionPoints (Mandatory, non-critical)	"distPoint.fullname" must contain URI (port number, attribute and binary option are optional[5])

[4] It must be verified of a policy by the case of non-critical as well as the case of critical.
[5] ldap://hostname[:portnumber]/dn[?attr[;binary]]

authorityInfoAccess (not used)	If the PKI domain uses OCSP, this field will be used.
inhibitAnyPolicy (not used)	
freshestCRL (not used)	
subjectInfoAccessSyntax (not used)	

(c) 中間認証局証明書

(i) 証明書基本領域

自己署名証明書を参照

(ii) 証明書標準拡張領域

表 3.9　中間認証局証明書　証明書標準拡張領域

FIELD	NOTE
authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2 **authorityCertIssuer(optional):** DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
subjectKeyIdentifier (Mandatory, non-critical)	The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage (Mandatory, critical)	keyCertSign, cRLSign
extKeyUsage (not used)	
privateKeyUsagePeriod (not used)	
certificatePolicies (Mandatory, ether critical or non-critical [6])	policyID MUST be present.
policyMappings	

[6] It must be verified of a policy by the case of non-critical as well as the case of critical.

(Mandatory, non-critical)	
subjectAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
issureAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
subjectDirectryAttributes (not used)	
basicConstraints (Mandatory, critical)	cA=TRUE pathLen=optional (INTEGER)
nameConstraints (optional, critical)	
policyConstraints (not used)	
cRLDistributionPoints (Mandatory, non-critical)	"distPoint.fullname" must contain URI (attribute: mandatory port number and binary option: optional[7])
authorityInfoAccess (not used)	If the PKI domain uses OCSP, this field will be used.
inhibitAnyPolicy (not used)	
freshestCRL (not used)	
subjectInfoAccessSyntax (not used)	

(d) エンドエンティティ証明書

(i) 証明書標準領域

自己署名証明書を参照

(ii) 証明書標準拡張領域

表 3.10　エンドエンティティ証明書　証明書標準拡張領域

FIELD	NOTE
authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's public key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2

[7] ldap://hostname[:portnumber]/dn?attr[;binary]

	authorityCertIssuer(optional): DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
subjectKeyIdentifier (Mandatory, non-critical)	The hash value of Issuer's public key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage (Mandatory, critical)	
extKeyUsage (not used)	
privateKeyUsagePeriod (not used)	
certificatePolicies (Mandatory, ether critical or non-critical [8])	policyID MUST be present.
policyMappings (not used)	
subjectAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
issureAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
subjectDirectryAttributes (not used)	
basicConstraints (not used)	
nameConstraints (not used)	
policyConstraints (not used)	
cRLDistributionPoints (Mandatory, non-critical)	"distPoint.fullname" must contain URI (attribute: mandatory port number and binary option: optional[9])
authorityInfoAccess (not used)	If the PKI domain uses OCSP, this fieldwill be used.
inhibitAnyPolicy (not used)	

[8] It must be verified of a policy by the case of non-critical as well as the case of critical.
[9] ldap://hostname[:portnumber]/dn?attr[;binary]

freshestCRL (not used)	
subjectInfoAccessSyntax (not used)	

(e) ＣＲＬ／ＡＲＬプロファイル

(i) 標準領域

表 3.11　ＣＲＬ／ＡＲＬ　標準領域

FIELD	NOTE
version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 1 (v2).
signature (Mandatory)	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
issure (Mandatory)	X.500 DN. Although DN is generally encoded by UTF8STRING, according to description of the X.520(2001), Country attribute is encoded by PrintableString.
thisUpdate (Mandatory)	UTCTIME
nextUpdate (Mandatory)	UTCTIME
revokedCertificates (Mandatory)	

(ii) エントリ拡張領域

表 3.12　ＣＲＬ／ＡＲＬ　エントリ拡張領域

FIELD	NOTE
reasonCode (Mandatory, non-critical)	
holdInstructionCode (not used)	
invalidityDate (optional, non-critical)	GeneralizedTime
CertificateIssuer (not used)	

(iii) 標準拡張領域

表 3.13　ＣＲＬ／ＡＲＬ　標準拡張領域

FIELD	NOTE
authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2 **authorityCertIssuer(optional):** DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
issureAltName (not-used)	
cRLNumber (Mandatory, non-critical)	unique integer. up to 20 octets.
deltaCRLIndicator (optional, critical)	If the PKI domain wants to use dCRL, this field will be used.
issuingDistributionPoint	
freshestCRL (optional, non-critical)	If the PKI domain wants to use dCRL, this field will be used.
crlScope (not-used)	

(f) リポジトリプロファイル

各ドメイン内におけるリポジトリの DIT 構造については、特に規定しない。但し、すべての DN が一意でなければならない。以下に例を示す。

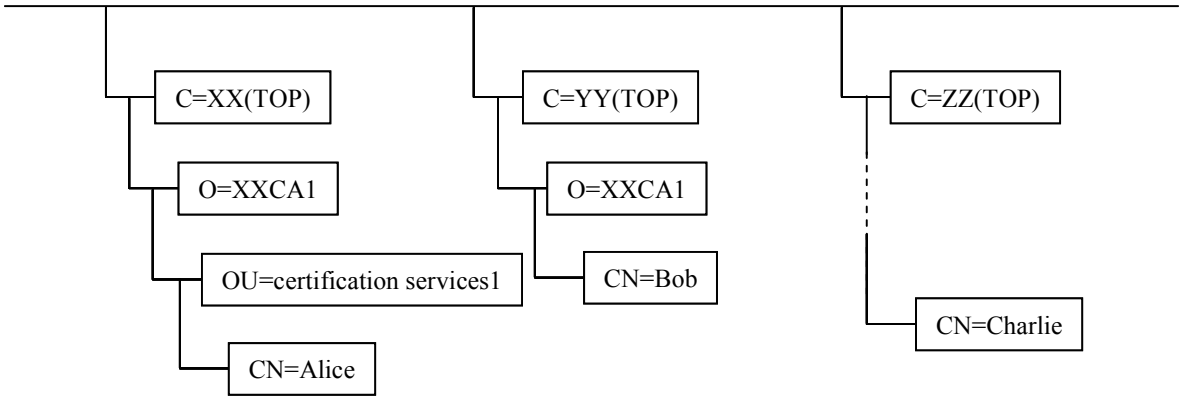


図 3.2　DIT の例

また、スキーマは以下を利用する。

(i) CA

pkiCA (2.5.6.21) or certificationAuthority (2.5.6.16)

(ii) End Entity

pkiUser (2.5.6.21) or inetOrgPerson (2.16.840.1.113730.3.2.2)

(iii) cRLDP

cRLDistributionPoint (2.5.6.19)

(iv) Referral

Referral (2.16.840.1.113730.3.2.6)

3.2 PKI アプリケーションに関する標準

3.2.1 パス検証テストガイドライン

本標準は、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である。

標準書の要約を以下に示す。詳細は「付録 2-1 パス検証テストガイドライン」として本標準を添付するので参照のこと。

(1) パス検証テストパターン

本標準は、汎用性を高めるために、なるべく様々な相互接続形態への適応を目指した。典型的な相互接続環境(モデル)を分析・定義し、個々のモデルに必要なテスト要件とテスト項目を定義することで、どのような相互接続環境にも適用しやすいガイドラインを設計した。

(a) テストモデルと要件

本標準が想定するテストモデルを明確化し、各テストモデルにおける認証局側テスト要件(CA.*nn*)と、署名検証者側テスト要件(RP.*nn*)をそれぞれ定義した。

nn: テスト番号

(i) 基本モデル

以下(ii)(iv)の全モデルに共通したテスト要件、テスト項目を定義したものを基本モデルとした。

表 3.14　基本モデルテスト要件

項番	要件および[出典]
CA.01	発行者識別名、主体者識別名について、country 属性を除き UTF8String でエンコードした証明書を発行できること。 **[PKI コンポーネント間接続に関する標準(H.12)]**
CA.02	発行する全ての証明書について、160bit SHA-1 の鍵識別子を生成すること。 **[PKI コンポーネント間接続に関する標準(H.12), RFC3280 4.2.1.1 & 4.2.1.2]**
CA.03	発行する全ての証明書について、一貫した鍵識別子を用いること。 **[PKI コンポーネント間接続に関する標準(H.12), RFC3280 4.2.1.1 & 4.2.1.2]**
CA.04	発行する全ての証明書について、一貫した書式の認証局鍵識別子拡張を用いること。 **[PKI コンポーネント間接続に関する標準(H.12), RFC3280 4.2.1.1]**
CA.05	クリティカルな基本制約拡張に cA フラグをセットした自己署名証明書を発行できること。 **[PKI コンポーネント間接続に関する標準(H.12)]**
CA.06	有効期間を UTCTime でエンコードした証明書を発行できること。 **[X.509 7]**
RP.07	正しい認証パスの検証に成功すること。
RP.08 ～ RP.11	認証パスに含まれる各証明書について、証明書の発行者識別名と、その発行者証明書の主体者識別名が一致していることを確認すること。 **[X.509 10.5.1]**
RP.12	認証パスに含まれる各証明書について、認証局鍵識別子と主体者鍵識別子による鍵チェーンを確認できること。 **[RFC3280 4.2.1.2]**
RP.13 ～ RP.16	認証パスに含まれる各証明書について、現在時刻がその有効期間内であることを確認できること。 **[X.509 10.5.1]**
RP.17 ～ RP.18	認証パスに含まれる各証明書について、UTCTime でエンコードされた有効期間の西暦年下 2 桁を正しく処理できること。 **[X.509 7]**

RP.19	認証パス中の各証明書を、その署名者証明書で検証できること。 [X.509 10.5.1]
RP.20	署名者証明書が失効してないかどうか確認できること。 [X.509 10.5.1]
RP.21	未知の拡張を持つ証明書を含む認証パスを処理できること。 [X.509 7]

(ii) 相互接続モデル

本標準では、下記の 7 つの相互接続モデルを定義した。このうちさらに、昨年度の実績として相互認証モデル、相互承認モデル、また典型例として知られる厳密階層モデルの 3 モデルについてのテスト要件を定義した。メッシュモデル、ブリッジ認証局モデル、公認証明書モデルについては、相互認証モデルの応用とみなせること、また証明書信用リストモデルについては、実装モデルがほとんどないことなどから、本年度は対象外とした。

- 厳密階層(Strict Hierarchy)
- 相互認証(Cross-Certification)
- 相互承認(Cross-Recognition)
- メッシュ(Mesh)
- ブリッジ認証局(Bridge CA)
- 公認証明書(Accreditation Certificate)
- 証明書信用リスト(Certificate Trust Lists)

本概要報告書では、一例として厳密階層(Strict Hierarchy)のテスト要件を以下に記す。

(ｲ) 厳密階層(Strict Hierarchy)

表 3.15　厳密階層モデルのテスト要件

項番	要件および[出典]
CA.01	基本制約拡張の cA フラグをセットした認証局証明書(自己署名証明書を除く)を発行できること。 [X.509 8.4.2.1]
CA.02	クリティカルな鍵用途拡張に keyCertSign をセットした認証局証明書(自己署名証明書を除く)を発行できること。 [X.509 8.2.2.3]
CA.03	クリティカルな鍵用途拡張に pathLenConstraint を含んだ認証局証明書(自己署名証明書を除く)を発行できること。

	[X.509 8.4.2.1]
CA.04 ～ CA.07	証明書ポリシ拡張に policyIdentifier を含んだ認証局証明書(自己署名証明書を除く)を発行できること。 [X.509 8.2.2.6]
RP.08	正しい認証パスの検証に成功すること。
RP.09 ～ RP.10	下位認証局証明書を含む認証パスを検証できること。 [X.509 10.5.1]
RP.11 ～ RP.13	認証パス中の全ての認証局証明書が、クリティカルな基本制約拡張に cA フラグをセットしているか確認できること。 [X.509 10.5.1]
RP.14	認証パスの長さが pathLenConstraint よりも短いか確認できること。 [X.509 10.5.1]
RP.15 ～ RP.17	認証パス中の全ての認証局証明書が、クリティカルな鍵用途拡張に keyCertSign をセットしているか確認できること。 [IWG profile]
RP.18 ～ RP.21	認証パス中の全ての証明書の検証するために証明書ポリシを処理できること。 [X.509 8.1.1]
RP.22	認証パス中の全ての認証局証明書が、失効してないかどうか確認できること。 [X.509 10.5.1]
RP.23	認証パス中の全ての認証局証明書を、その署名者証明書で検証できること。 [X.509 10.5.1]

(iii) サービスモデル

本標準では、下記の 4 つのサービスモデルを定義した。このうちさらに、昨年度の実績から電子署名モデルについてのテスト要件を定義した。他のモデルについては日本を含む諸国法制度の整備状況を考慮して、本年度は対象外とした。

- 電子署名(Signing)
- 電子公証・長期署名(Notary / Long term signing)
- 認証(Authentication)
- 暗号(Encryption)

(ｲ) 電子署名(Signing)

表 3.16　電子署名モデルのテスト要件

項番	要件および[出典]
CA.01	クリティカルな鍵用途拡張に digitalSignature をセットしたエンドエンティティ証明書を発行できること。
CA.02 ～ CA.05	証明書ポリシ拡張に policyIdentifier を含んだ認証局証明書(自己署名証明書を除く)を発行できること。 [X.509 8.2.2.6]
RP.06	正しい認証パスの検証に成功すること。
RP.07	署名者証明書の鍵用途拡張に適切な値がセットされているか確認できること。 [IWG consideration]
RP.08	認証パス中の全ての証明書の検証するために証明書ポリシを処理できること。 [X.509 8.1.1]

(iv) 失効・検証モデル

本標準では、下記の 3 つのサービスモデルを定義した。このうちさらに、昨年度の実績から CRL モデルについてのテスト要件を定義した。OCSP モデルについては韓国側の協力が困難であったこと、DPV/DPD モデルについては IETF/PKIX での検討がまだ十分でないことなどから、本年度は対象外とした。

- CRL (Certificate Revocation List)
- OCSP (Online Certificate Status Protocol)
- DPV/DPD (Delegated Path Validation and Discovery)

(ｲ) CRL (Certificate Revocation List)

表 3.17　CRL モデルのテスト要件

項番	要件および[出典]
CA.01	クリティカルな鍵用途拡張に cRLSign をセットした認証局証明書を発行できること。 [IWG profile]
CA.02	クリティカルな発行配布点拡張を含んだ失効リストを発行できること。 [IWG profile]

CA.03	クリティカルな発行配布点拡張に onlyContainsUserCerts フラグをセットした証明書失効リスト(CRL)を発行できること。 **[IWG profile]**
CA.04	クリティカルな発行配布点拡張に onlyContainsCACerts フラグをセットした認証局失効リスト(ARL)を発行できること。 **[IWG profile]**
CA.05	失効リスト配布点拡張の distributionPoint(CA エントリ以外の場合)を含んだ証明書を発行できること。 **[X.509 8.6.2.2, RFC3280 5.2.5]**
CA.06	発行した証明書の失効リスト配布点拡張と一致した distributionPoint を含む失効リストを発行できること。 **[RFC3280 5.2.5]**
CA.07	認証局鍵識別子拡張に keyIdentifier を含む失効リストを発行できること。 **[IWG profile]**
RP.08	正しい認証パスの検証に成功すること。
RP.09 ～ RP.10	検証する証明書に必要な CRL を関連づけられること。 **[X.509 10.5.1]**
RP.11	当該証明書の revocationDate が有効か確認できること。 **[IWG consideration]**
RP.12	失効リストを、失効リスト署名者証明書で検証できること。 **[RFC3280 6.3.3 (b)]**
RP.13	失効リスト署名者証明書が鍵用途拡張に cRLSign がセットされているか確認できること。 **[RFC3280 6.3.3 (f)]**
RP.14	失効リストが改竄されてないか確認できること。 **[X.509 10.5.1, RFC3280 6.3.3 (g)]**
RP.15 ～ RP.16	未知あるいは既知の CRL エントリ拡張を含む失効リストを正しく処理できること。 **[X.509 8]**
RP.17 ～ RP.18	未知あるいは既知の CRL 拡張を含む失効リストを正しく処理できること。 **[X.509 8]**
RP.19 ～	クリティカルな発行配布点拡張の onlyContainsCACerts フラグがセットされた失効リストを利用して、証明書の失効検証を適

RP.22	切に処理できること。 **[RFC3280 6.3.3 (b)]**
RP.23 ～ RP.26	クリティカルな発行配布点拡張の onlyContainsUserCerts フラグがセットされた失効リストを利用して、証明書の失効検証を適切に処理できること。 **[RFC3280 6.3.3 (b)]**
RP.27 ～ RP.31	証明書の失効リスト配布点拡張と、失効リストの発行配布点拡張の distributionPoint が一致しているか確認できること。 **[RFC3280 5.2.5]**

(b) テスト条件

テストモデル毎に、各テスト項目で前提とするテストパラメータについて明記した。

(ｲ) テストに必要なエンティティ

関係する認証局、署名者、署名検証者など、認証パスを把握するために必要な要素を定義している。

(ﾛ) 各エンティティの証明書プロファイル

認証パスを構成する各種証明書や失効情報などのプロファイルを定義している。

(ﾊ) 認証パスの検証パラメータ

認証パスを検証する際に用いる入力値を定義している。

(i) 基本モデル

- テストに必要なエンティティ

表 3.18　基本モデルのエンティティ

エンティティ名	説明
ルート認証局	自己署名証明書を持つ唯一の認証局
署名者	ルート認証局から発行された証明書を持つエンドエンティティ
署名検証者	署名者の署名データを検証するエンドエンティティ

- 各エンティティの証明書プロファイル

各エンティティの証明書プロファイルについては「付録 2-1 パス検証テストガイドライン」に示し、本概要報告書では割愛する。

- 認証パスの検証に用いられる入力値

表 3.19　基本モデルの入力値

パラメータ名	値
user-initial-policy-set	any-policy
trustAnchorInfo	ルート認証局
initial-explicit-policy	False

(ii) 相互接続モデル

前項(a)テストモデルと要件で定義した厳密階層モデル、相互認証モデル、相互承認モデルの 3 モデルについて、それぞれテストパラメータを定義した。

(ｲ) 厳密階層(Strict Hierarchy)

- テストに必要なエンティティ

表 3.20　厳密階層モデルのエンティティ

エンティティ名	説明
ルート認証局	自己署名証明書を持つ唯一の認証局
下位認証局 1	ルート認証局から発行された証明書を持つ認証局
署名者 1	下位認証局 1 から発行された証明書を持つエンドエンティティ
下位認証局 2	下位認証局 1 から発行された証明書を持つ認証局
署名者 2	下位認証局 2 から発行された証明書を持つエンドエンティティ

- 各エンティティの証明書プロファイル

各エンティティの証明書プロファイルについては「付録 2-1 パス検証テストガイドライン」に示し、本概要報告書では割愛する。

- 認証パスの検証に用いられる入力値

表 3.21　厳密階層モデルの入力値

パラメータ名	値
user-initial-policy-set	policy-A
trustAnchorInfo	Root CA
initial-explicit-policy	True

(ﾛ) 相互認証(Cross-Certification)

- テストに必要なエンティティ

表 3.22　相互認証モデルのエンティティ

エンティティ名	説明
ルート認証局 X	自己署名証明書を持つ認証局
ルート認証局 Y	ルート認証局 X と相互認証の関係にある認証局 Y
署名者 Y	ルート認証局 Y から発行された証明書を持つエンドエンティティ
ルート認証局 Z	ルート認証局 Y と相互認証している認証局 Z
署名者 Z	ルート認証局 Z から発行された証明書を持つエンドエンティティ

- 各エンティティの証明書プロファイル

各エンティティの証明書プロファイルについては「付録 2-1 パス検証テストガイドライン」に示し、本概要報告書では割愛する。

- 認証パスの検証に用いられる入力値

表 3.23　相互認証モデルの入力値

パラメータ名	値
user-initial-policy-set	policy-X
trustAnchorInfo	Root CA-X
initial-explicit-policy	False

(ﾊ) 相互承認(Cross-Recognition)

- テストに必要なエンティティ

表 3.24　相互承認モデルのエンティティ

エンティティ名	説明
ルート認証局 X	自己署名証明書を持つ認証局 X
ルート認証局 Y	ルート認証局 X と相互承認の関係にある認証局 Y
署名者 Y	ルート認証局 Y から発行された証明書を持つエンドエンティティ

- 各エンティティの証明書プロファイル

各エンティティの証明書プロファイルについては「付録 2-1 パス検証テ

ストガイドライン」に示し、本概要報告書では割愛する。

- 認証パスの検証に用いられる入力値

表 3.25　相互承認モデルの入力値

パラメータ名	値
user-initial-policy-set	policy-X, policy-Y
trustAnchorInfo	Root CA-X, RootCA-Y
initial-explicit-policy	True

(iii) サービスモデル

前項(a)テストモデルと要件で定義した電子署名モデルについて、テストパラメータを定義した。

(ｲ) 電子署名(Signing)

- テストに必要なエンティティ

表 3.26　電子署名モデルのエンティティ

エンティティ名	説明
ルート認証局	自己署名証明書を持つ唯一の認証局
署名者	ルート認証局から発行された証明書を持つエンドエンティティ
署名検証者	署名者の署名データを検証するエンドエンティティ

- 各エンティティの証明書プロファイル

各エンティティの証明書プロファイルについては「付録 2-1 パス検証テストガイドライン」に示し、本概要報告書では割愛する。

- 認証パスの検証に用いられる入力値

表 3.27　電子署名モデルの入力値

パラメータ名	値
user-initial-policy-set	policy-A
trustAnchorInfo	Root CA
initial-explicit-policy	True

(iv) 失効・検証モデル

前項(a)テストモデルと要件で定義した CRL モデルについて、テストパラメータを定義した。

(ｲ) CRL(Certificate Revocation List)

- テストに必要なエンティティ

表 3.28　CRL モデルのエンティティ

エンティティ名	説明
ルート認証局 A	自己署名証明書を持つ唯一の認証局
署名者 A	ルート認証局から発行された証明書を持つエンドエンティティ
下位認証局	ルート認証局から発行された証明書を持つ認証局
下位認証局署名者	下位認証局から発行された証明書を持つエンドエンティティ
署名検証者	署名者の署名データを検証するエンドエンティティ

- 各エンティティの証明書プロファイル

各エンティティの証明書プロファイルについては「付録 2-1 パス検証テストガイドライン」に示し、本報告書では割愛する。

- 認証パスの検証に用いられる入力値

表 3.29　CRL モデルの入力値

パラメータ名	値
user-initial-policy-set	unspecified
trustAnchorInfo	Root CA-A
initial-explicit-policy	unspecified

(c) 基本モデルにおけるテストアイテム

本項では、前項(a)(i)基本モデルで定義したテスト要件に対応する基本モデルのテストアイテムを定義した。

(d) 相互接続モデルにおけるテストアイテム

本項では、前項(a)(ii)相互接続モデルで定義したテスト要件のうち、厳密階層モデル、相互認証モデル、相互承認モデルに対応するテストアイテムをそれぞれ定義した。

- 厳密階層(Strict Hierarchy)
- 相互認証(Cross-Certification)
- 相互承認(Cross-Recognition)

- メッシュ(Mesh)
- ブリッジ認証局(Bridge CA)
- 公認証明書(Accreditation Certificate)
- 証明書信用リスト(Certificate Trust Lists)

(e) サービスモデルにおけるテストアイテム

本項では、前項(a)(iii)サービスモデルで定義したテスト要件のうち、電子署名モデルに対応するテストアイテムを定義した。

- 電子署名(Signing)
- 電子公証・長期署名(Notary / Long term signing)
- 認証(Authentication)
- 暗号(Encryption)

(f) 失効・検証モデルにおけるテストアイテム

本項では、前項(a)(iv)失効・検証モデルで定義したテスト要件のうち、CRLモデルに対応するテストアイテムを定義した。

- CRL (Certificate Revocation List)
- OCSP (Online Certificate Status Protocol)
- DPV/DPD (Delegated Path Validation and Discovery)

3.2.2 署名用トークンインターフェース仕様

本標準は、アプリケーション開発者が国際間で利用可能なアプリケーションを開発するにあたり、要件及び仕様を検討する際に使用する標準である。

標準書の要約を以下に示す。詳細は「付録 2-2 署名用トークンインターフェース仕様」として本標準を添付するので参照のこと。

本標準が想定するアプリケーションモデルでは PKCS#11 を使用する。PKCS#11 は広く世界的に普及している仕様であり、OS に関するオープンプラットフォーム、細部まで仕様が策定されているため異なる PKCS#11 ライブラリ間で連携が取りやすいといったメリットを備えているため採用した。

PKCS#11 の関数及びリターンコード、使用する関数で設定する必要がある各種パラメータについて定義する。アプリケーションモデルの概要を図 3.3 に示す。

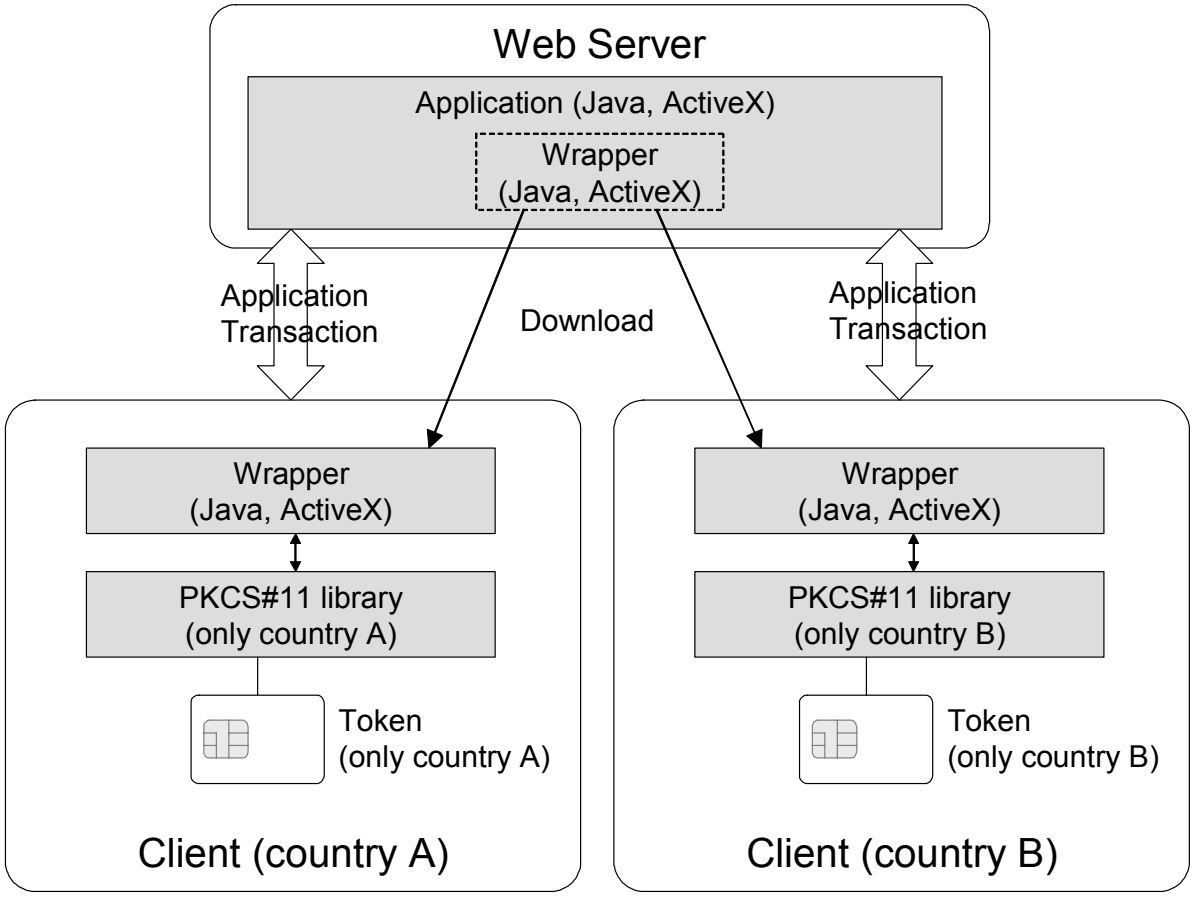


図 3.3　アプリケーションモデルの概要

このモデルの構成として、Web Server 上のアプリケーションとセットで Wrapper と呼ばれるモジュール（Java Applet or ActiveX）が置かれ、クライアントからの要求に応じてクライアントへダウンロードされる。

クライアントにおいては、PKCS#11 ライブラリが予めインストールされており、その PKCS#11 ライブラリが管理するトークンに秘密鍵と証明書が格納されている。クライアントは Web ブラウザを使用して Web Server 上のアプリケーションへアクセスし、必要に応じて Wrapper をダウンロードし、Wrapper を介してアプリケーションと PKCS#11 ライブラリが連携する。

機能については次のようになる。まず、Web Server がアプリケーションサービスを提供する。クライアントにおいては、Web Server へアクセスしている状態で、電子署名の付与及び検証を行う際に Web Server から Wrapper をダウンロードし、PKCS#11 ライブラリで作成された署名値又は検証結果をアプリケーションへ渡す。Wrapper とは、各国／地域の機能的な差異及び PKCS#11 ライブラリとアプリケーションの開発言語の差異を吸収するための機能として導入している。

PKCS#11 ライブラリとトークンは各国／地域が利用可能なものを使用するが、Wrapper はアプリケーションサービス提供者が共通なモジュールとして提供する。

(1) 使用する PKCS#11 関数

C_Initialize、C_GetSlotList、C_GetTokenInfo、C_OpenSession、
C_Login、C_Logout、C_CloseSession、C_Finalize
C_FindObjectsInit、C_FindObjects、C_FindObjectsFinal、
C_GetAttributeValue、C_CreateObject、
C_DestroyObject、C_GenerateKey (Optional)
C_SignInit、C_Sign、C_VerifyInit、C_Verify
C_EncryptInit (Optional)、C_Encrypt (Optional)、
C_DecryptInit (Optional)、C_Decrypt (Optional)

実際はこれらの関数を処理単位でシーケンスとし、シーケンス単位で実行する。シーケンスは次のとおりである。

(a) Initialize Sequence

C_Initialize
C_GetSlotList
C_GetTokenInfo
C_OpenSession
C_Login

(b) Logout Sequence

C_Logout
C_CloseSession
C_Finalize

(c) Get Certificate Sequence

C_FindObjectsInit
C_FindObjects
C_FindObjectsFinal
C_GetAttributeValue

(d) Sign Sequence

C_SignInit
C_Sign

(e) Verify Sequence

C_CreateObject
C_VerifyInit

C_Verify

(f) Delete Object Sequence
C_DestroyObject

(g) Common Key Generate Sequence (Optional)
C_GenerateKey
C_GetAttributeValue

(h) Encryption Sequence (Optional)
C_EncryptInit
C_Encrypt

(i) Decryption Sequence (Optional)
C_DecryptInit
C_Decrypt

(2) 使用する関数で必要となるパラメータ

(a) PKCS#11 ライブラリのファイル名

PKCS#11 ライブラリのファイル名は、Wrapper がクライアントに格納されている「PKCS11.ini」ファイルをロードすることで解決を図る。

(b) 署名メカニズム

署名メカニズムは CKM_RSA_PKCS 又は CKM_SHA1_RSA_PKCS とする。

(c) 署名アルゴリズム

署名アルゴリズムはメカニズムとして CKM_RSA_PKCS を使用する場合は RSA Encryption、メカニズムとして CKM_SHA1_RSA_PKCS を使用する場合は SHA1 とする。

(d) 鍵長

エンドエンティティの秘密鍵及び公開鍵の鍵長は RSA アルゴリズムの 1024 ビットとする。

4 検証項目

作成した標準案の実用性及び有効性を検証するため、「表 4.1　実験単位一覧」に示す実験単位で実証実験を実施する。

表 4.1　実験単位一覧

大項目	中項目	小項目
(1)シミュレーションセンタにおける認証局間の実証実験	(1-1)相互接続に係わる証明書発行	(1-1-1)自己署名証明書の発行
		(1-1-2)証明書要求の発行
		(1-1-3)相互認証証明書の発行
		(1-1-4)相互認証証明書ペアの発行
		(1-1-5)エンドエンティティ証明書の発行
		(1-1-6)証明書検証サーバ証明書の発行
	(1-2)相互接続に係わる証明書失効	(1-2-1)CRLの発行
		(1-2-2)ARLの発行
	(1-3)相互接続に係わる証明書更新	(1-3-1)相互認証証明書の更新
	(1-4)相互接続に係わる証明書再発行	(1-4-1)旧相互認証証明書の失効
		(1-4-2)新相互認証証明書の発行
(2)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	(2-1)認証パス検証	-
	(2-2)失効検証	-
	(2-3)有効期限検証	-
	(2-4)ポリシ検証	-
	(2-5)認証パス構築検証	-
(3)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	(3-1)正常系検証	-
	(3-2)失効系検証(1)	-
	(3-3)失効系検証(2)	-
(4)現地環境における認証局間の実証実験	(4-1)相互接続に係わる証明書発行	(4-1-1)自己署名証明書の発行
		(4-1-2)証明書要求の発行
		(4-1-3)相互認証証明書の発行
		(4-1-4)相互認証証明書ペアの発行

		(4-1-5)エンドエンティティ証明書の発行
		(4-1-6)証明書検証サーバ証明書の発行
	(4-2)相互接続に係わる証明書失効	(4-2-1)CRLの発行
		(4-2-2)ARLの発行
	(4-3)相互接続に係わる証明書更新	(4-3-1)相互認証証明書の更新
	(4-4)相互接続に係わる証明書再発行	(4-4-1)旧相互認証証明書の失効
		(4-4-2)新相互認証証明書の発行
(5)現地環境における証明書検証の実証実験	(5-1)認証パス検証	-
	(5-2)失効検証	-
	(5-3)有効期限検証	-
	(5-4)ポリシ検証	-
	(5-5)認証パス構築検証	-
(6)現地環境における国際間調達の実証実験	(6-1)正常系検証	-
	(6-2)失効系検証(1)	-
	(6-3)失効系検証(2)	-
(7)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	(7-1)基本モデル	-
	(7-2)相互接続モデル	(7-2-1)Strict Hierarchyモデル
		(7-2-2)Cross Certificationモデル
		(7-2-3)Cross Recognitionモデル
	(7-3)サービスモデル	-
	(7-4)失効モデル	-
(8)現地環境における署名用トークンインターフェース仕様の実証実験	(8-1)正常系検証	-
	(8-1)異常系検証	-

7 章以降で「表 4.1　実験単位一覧」に示した実験単位ごとに実証実験の詳細を記述する。

実験単位ごとの対象国／地域を「表 4.2　実証実験対象国／地域」に示す。

表 4.2　実証実験対象国／地域

実験単位大項目	対象国／地域
(1)シミュレーションセンタにおける認証局間の実証実験	日本
	チャイニーズ台北
	香港チャイナ
(2)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	日本
	チャイニーズ台北
	香港チャイナ
(3)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	日本
	チャイニーズ台北
	香港チャイナ
(4)現地環境における認証局間の実証実験	日本
	チャイニーズ台北
	香港チャイナ
(5)現地環境における証明書検証の実証実験	日本
	チャイニーズ台北
	香港チャイナ
(6)現地環境における国際間調達の実証実験	日本
	チャイニーズ台北
	香港チャイナ
(7)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	日本
	韓国
	チャイニーズ台北
(8)現地環境における署名用トークンインターフェース仕様の実証実験	日本
	韓国
	チャイニーズ台北

「表 4.3　参加認証局一覧」に本実証実験に参加した認証局を示す。

表 4.3　参加認証局一覧

参加国／地域	認証局
日本	模擬 JCSI（日本認証サービス株式会社）認証局として設立した実験用認証局[10]

[10] 日本の政府認証基盤（GPKI）相互運用性仕様に準拠して運営されている。

チャイニーズ台北	Chunghwa Telecom Co., Ltd(以降、中華電信と表記)の運営する実験用認証局[11]
チャイニーズ台北	TAIWAN-CA.COM.,INC（以降、TaiCA と表記）の運営する実験用認証局
香港チャイナ	Hongkong Post の運営する実験用認証局

シミュレーションセンタ実験環境では「表 4.3　参加認証局一覧」に示す日本、チャイニーズ台北及び香港チャイナの認証局を模擬的に再現した認証局を設置した。チャイニーズ台北については２つの認証局のうち、中華電信の模擬認証局とした。

「表 4.4　パス検証モジュール一覧」にパス検証テストガイドラインの実証実験で使用した検証モジュールを示す。

表 4.4　パス検証モジュール一覧

参加国／地域	認証局
日本	株式会社日立製作所の所有する検証モジュール
韓国	Korea Information Security Agency（以降、KISA と表記）の所有する検証モジュール
チャイニーズ台北	中華電信の所有する検証モジュール

「表 4.5　PKCS#11 ライブラリ一覧」に署名用トークンインターフェース仕様の実証実験で使用した PKCS#11 ライブラリを示す。

表 4.5　PKCS#11 ライブラリー覧

参加国／地域	認証局
日本	富士通株式会社製 PKCS#11 ライブラリ
韓国	KISA 製 PKCS#11 ライブラリ
チャイニーズ台北	TaiCA 製 PKCS#11 ライブラリ

[11] チャイニーズ台北の GPKI 仕様に準拠して運営されている。

5 実験環境

標準案の検証を行うために、実証実験環境を構築した。実証実験環境は、

- シミュレーションセンタ実験環境
- 現地実証実験環境

の２段階を用意した。

5.1　シミュレーションセンタ実験環境

シミュレーションセンタとして、日本国内に日本、チャイニーズ台北、香港チャイナ３国／地域の模擬環境を構築した。本環境は、現地実証実験環境より柔軟に設定の変更が可能であり、実運用の制約のない技術的な検証を可能とするものである。この環境での検証は、本実証実験で策定した標準の実用性、すなわち、策定された標準の技術的側面及び運用的側面の論理的実証、動作検証を目的とした。更に、現地環境で抽出した課題について検証を深め、解決策を試行する環境として機能した。

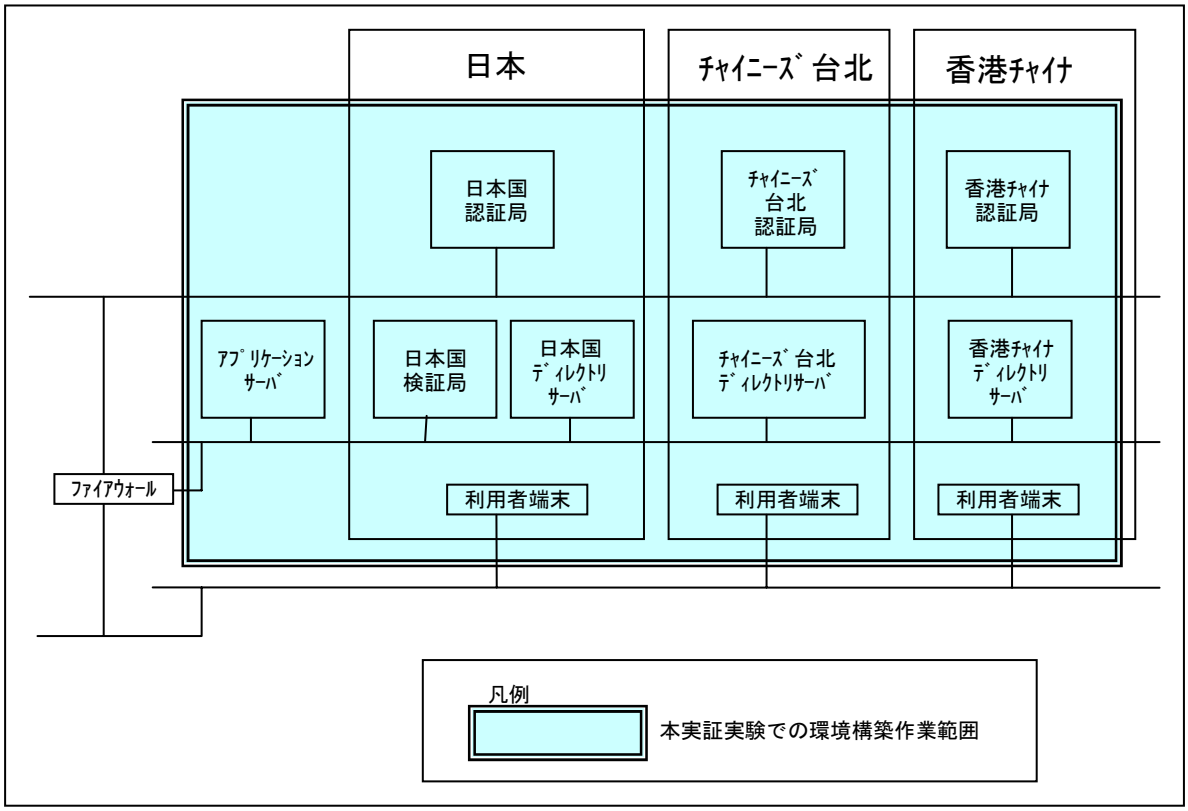


図 5.1　シミュレーションセンタ実証実験構成図

5.2　現地実証実験環境

現地実証実験環境として、現地に実際運用している場所を想定した模擬環境を設置した。この環境での検証は、実運用に近い環境を想定した環境を利用して、策定

された標準の現地環境への適応性及び有効性の検証、並びに課題抽出を目的とするものである。

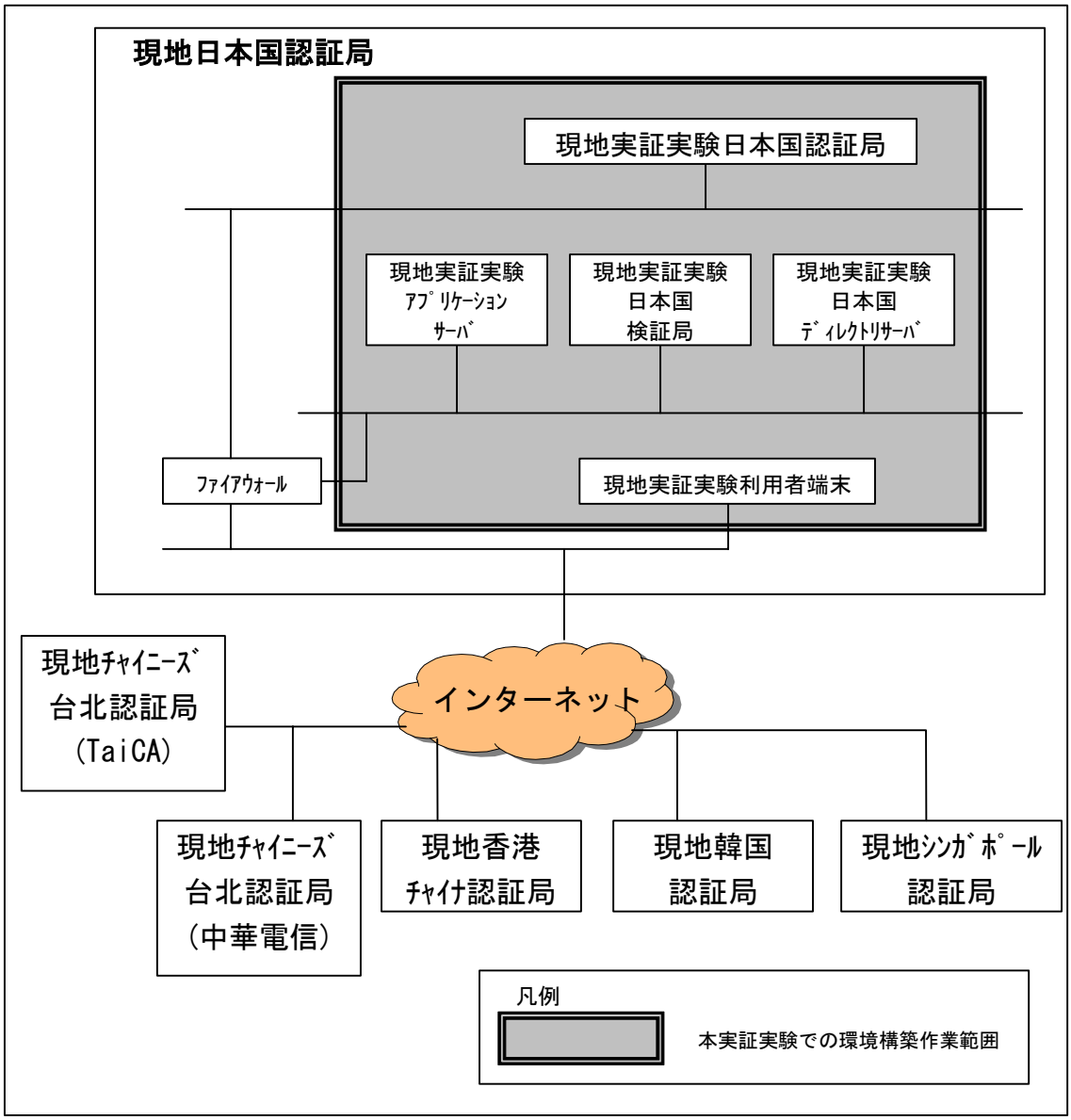


図 5.2　現地実証実験構成図

6 開発作業

「署名用トークンインターフェース仕様」を実証実験で検証できるように、日本における個別仕様を共通仕様へ変換する機能等を具備するソフトウェアの開発を行った。

本ソフトウェアは、以下の機能を有する。

- 署名用トークン確認機能
- 共通インターフェース機能

本ソフトウェアは、Java アプレット及び DLL（ダイナミックリンクライブラリ）として提供される。稼働環境として PKCS#11 ライブラリを使用する

利用者は、クライアントに JavaVM（Java Runtime Environment）をインストールし、WWW ブラウザ上から本機能を利用する。

以下の「図 6.1　ソフトウェアの全体構成」に本ソフトウェアの全体構成を示す。

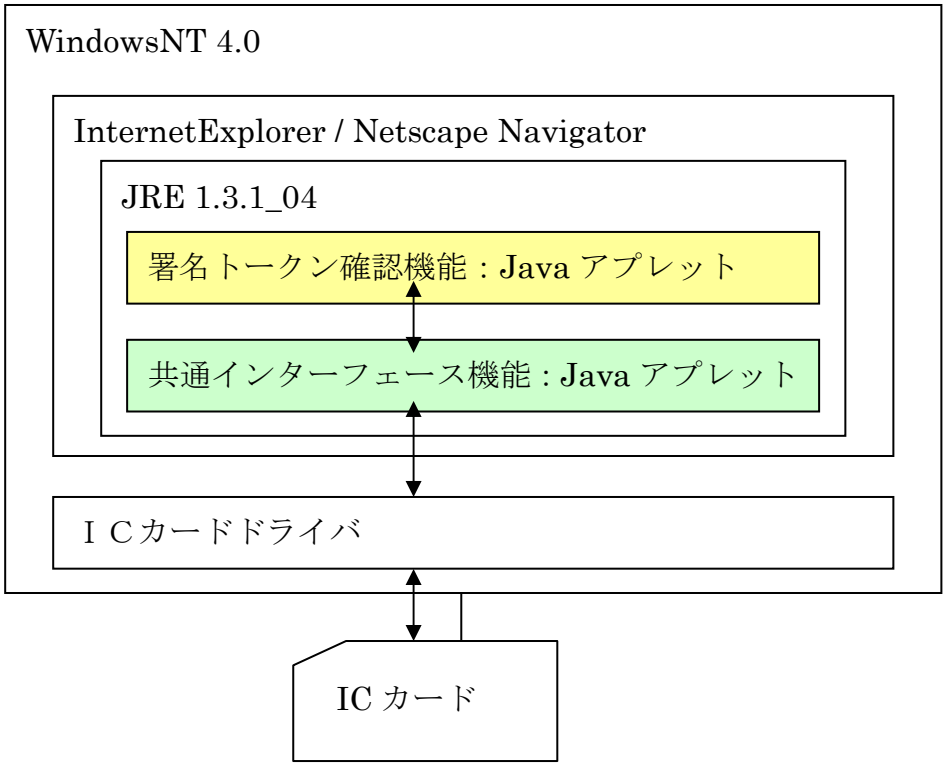


図 6.1　ソフトウェアの全体構成

「図 3.3　アプリケーションモデルの概要」との対比で説明すると、署名用トークン確認機能は Web Server 上に配置されるアプリケーション、共通インターフェース機能は Wrapper、IC カードドライバは PKCS#11 ライブラリとなる。

7 シミュレーションセンタにおける認証局間の実証実験

7.1　概要

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う。

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する。

7.2　相互接続に係わる証明書発行

(1) 実験内容

シミュレーションセンタにおいて、「相互接続インターフェース仕様」に従って相互接続に係わる証明書、及び証明書発行要求を発行し、その結果得られた実験データを収集して分析する。

本実験単位においては、日本国認証局とチャイニーズ台北認証局の間で「相互接続インターフェース仕様」に従い、下記「表 7.1　シミュレーションセンタ環境における 2 種類の証明書プロファイル」に示す 2 種類の異なった証明書プロファイルによる証明書発行を行う。Phase1 は、昨年度 IWG プロファイルに基づいたものである。Phase2 はチャイニーズ台北及び香港チャイナが Phase1 のプロファイルに対して異なる見解を持っていた点を吸収し、両国／地域の実際の運用に近づけたものである。

表 7.1　シミュレーションセンタ環境における2種類の証明書プロファイル

プロファイルの種類	プロファイルの相違	
	証明書種別	相違点
Phase1	自己署名証明書	cRLDP.distPoint.fullName の LDAPURI に属性値あり
	相互認証証明書	cRLDP.distPoint.fullName の LDAPURI に属性値あり

	CRL/ARL	iDP 有り
	エンドエンティティ証明書	keyUsage に digitalSignature を設定
		cRLDP.distPoint.fullName の LDAPURI に属性値あり
Phase2	自己署名証明書	cRLDP.distPoint.fullName の LDAPURI に属性値なし
	相互認証証明書	cRLDP.distPoint.fullName の LDAPURI に属性値なし
	CRL/ARL	iDP なし
	エンドエンティティ証明書	keyUsage ・ digitalSignature を設定 ・ keyEncipherment 及び dataEncipherment を設定
		cRLDP.distPoint.fullName の LDAPURI に属性値なし
		subjectAltName.rfc822Name を設定

認証局が発行する証明書の種類による実験単位の小項目を「表 7.2　シミュレーションセンタにおける証明書発行実験単位小項目一覧」に示す。

表 7.2　シミュレーションセンタにおける証明書発行実験単位小項目一覧

小項目番号	実験単位小項目
1-1-1	自己署名証明書の発行
1-1-2	証明書要求の発行
1-1-3	相互認証証明書の発行
1-1-4	相互認証証明書ペアの発行
1-1-5	エンドエンティティ証明書の発行
1-1-6	証明書検証サーバの証明書発行

各国認証局が発行する証明書は運用により異なる。本実証実験で対象とする 3 国／地域の認証局が発行する証明書は以下のとおりである。

(a) 日本国認証局が発行する証明書類

- 自己署名証明書
- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア

- エンドエンティティ証明書
- 証明書検証サーバ証明書

(b) チャイニーズ台北認証局が発行する証明書類

- 自己署名証明書
- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア
- エンドエンティティ証明書

(c) 香港チャイナ認証局

- 自己署名証明書
- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア
- エンドエンティティ証明書
- 証明書検証サーバ証明書

(2) 実験方法

シミュレーションセンタ内に設置した日本国認証局、チャイニーズ台北認証局及び香港チャイナ認証局で、相互接続に係わる証明書を発行する。

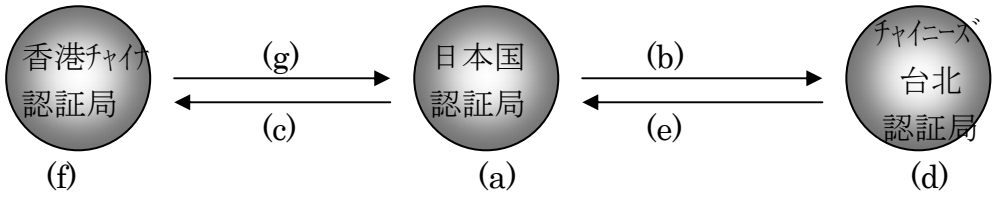


図 7.1　認証局間の証明書発行（Phase1）

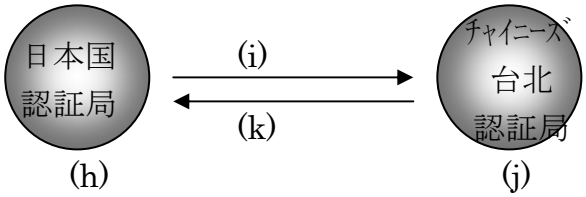


図 7.2　認証局間の証明書発行(Phase2)

各認証局のローカルドメイン内の証明書発行と、「図 7.1　認証局間の証明書発行」及び「図 7.2　認証局間の証明書発行(Phase2)」で実線で示した認証局間の証明書発行を実験対象とする。

(a) 日本国認証局のローカルドメイン内の証明書発行（Phase1）

「表 7.3　日本国認証局のローカルドメイン内の証明書発行チェック項目」にチェック項目を示す。

表 7.3　日本国認証局のローカルドメイン内の証明書発行チェック項目

小項目	ID	チェック項目
1-1-1 自己署名証明書の発行	J-1	自己署名証明書の内容が、「相互接続インターフェース仕様」に従っていることを確認。
1-1-5 エンドエンティティ証明書の発行	J-1	エンドエンティティに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
1-1-6 証明書検証サーバ証明書の発行	J-1	証明書検証サーバの証明書要求により証明書を発行し、ファイル出力できることを確認。
	J-2	証明書検証サーバに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

(b) 日本国認証局からチャイニーズ台北認証局への証明書発行（Phase1：相互認証）

「表 7.4　日本国認証局からチャイニーズ台北認証局への証明書発行チェック項目」にチェック項目を示す。

表 7.4　日本国認証局からチャイニーズ台北認証局への証明書発行チェック項目

小項目	ID	チェック項目
1-1-2 証明書要求の発行	JT-1	日本国認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。
	JT-2	証明書要求に対応する相互認証証明書がチャイニーズ台北認証局から発行されたことを確認。
1-1-3 相互認証証明書の発行	JT-1	チャイニーズ台北認証局から受け取った証明書要求により相互認証証明書を発行し、DER 形式でファイル出力できることを確認。
	JT-2	チャイニーズ台北認証局に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

1-1-4 相互認証証明書ペアの発行	JT-1	日本国認証局がチャイニーズ台北認証局に対して発行した相互認証証明書と、チャイニーズ台北認証局から日本国認証局に対して発行された相互認証証明書（DER 形式で受領）から相互認証証明書ペアが生成できることを確認。
	JT-2	チャイニーズ台北認証局が発行した相互認証証明書が相互認証証明書ペアの forward に格納されていることを確認。
	JT-3	チャイニーズ台北認証局に対して発行した相互認証証明書が相互認証証明書ペアの reverse に格納されていることを確認。

(c) 日本国認証局から香港チャイナ認証局への証明書発行（Phase1：相互認証）

「表 7.5　日本国認証局から香港チャイナ認証局への証明書発行チェック項目」にチェック項目を示す。

表 7.5　日本国認証局から香港チャイナ認証局への証明書発行チェック項目

小項目	ID	チェック項目
1-1-3 相互認証証明書の発行	JH-1	香港チャイナ認証局から受け取った証明書要求により相互認証証明書を発行し、DER 形式でファイル出力できることを確認。
	JH-2	香港チャイナ認証局に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
1-1-4 相互認証証明書ペアの発行	JH-1	日本国認証局が香港チャイナ認証局に対して発行した相互認証証明書と、香港チャイナ認証局から日本国認証局に対して発行された相互認証証明書（DER 形式で受領）から相互認証証明書ペアが生成できることを確認。
	JH-2	香港チャイナ台北認証局が発行した相互認証証明書が相互認証証明書ペアの forward に格納されていることを確認。
	JH-3	香港チャイナ認証局に対して発行した相互認証証明書が相互認証証明書ペアの reverse に格納されていることを確認。

(d) チャイニーズ台北認証局のローカルドメイン内の証明書発行（Phase1）

「表 7.6　チャイニーズ台北認証局のローカルドメイン内の証明書発行チェック項目」にチェック項目を示す。

表 7.6　チャイニーズ台北認証局のローカルドメイン内の証明書発行チェック項目

小項目	ID	チェック項目
1-1-1 自己署名証明書の発行	T-1	自己署名証明書の内容が、「相互接続インターフェース仕様」に従っていることを確認。
1-1-5 エンドエンティティ証明書の発行	T-1	エンドエンティティに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

(e) チャイニーズ台北認証局から日本国認証局への証明書発行

「表 7.7　チャイニーズ台北認証局から日本国認証局への証明書発行チェック項目」にチェック項目を示す。

表 7.7　チャイニーズ台北認証局から日本国認証局への証明書発行チェック項目

小項目	ID	チェック項目
1-1-2 証明書要求の発行	TJ-1	チャイニーズ台北認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。
	TJ-2	証明書要求に対応する相互認証証明書が日本国認証局から発行されたことを確認。
1-1-3 相互認証証明書の発行	TJ-1	日本国認証局から受け取った証明書要求により相互認証証明書を発行し、DER 形式でファイル出力できることを確認。
	TJ-2	日本国認証局に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
1-1-4 相互認証証明書ペアの発行	TJ-1	チャイニーズ台北認証局が日本国認証局に対して発行した相互認証証明書と、日本国認証局からチャイニーズ台北認証局に対して発行された相互認証証明書（DER 形式で受領）から相互認証証明書ペアが生成できることを確認。
	TJ-2	日本国認証局が発行した相互認証証明書が相互認証証明書ペアの forward に格納されていることを確認。
	TJ-3	日本国認証局に対して発行した相互認証証明書が相互認証証明書ペアの reverse に格納されていることを確認。

(f) 香港チャイナ認証局のローカルドメイン内の証明書発行（Phase1）

「表 7.8　香港チャイナ認証局のローカルドメイン内の証明書発行チェック項目」にチェック項目を示す。

表 7.8　香港チャイナ認証局のローカルドメイン内の証明書発行チェック項目

小項目	ID	チェック項目
1-1-1 自己署名証明書の発行	H-1	自己署名証明書の内容が、「相互接続インターフェース仕様」に従っていることを確認。
1-1-5 エンドエンティティ証明書の発行	H-1	エンドエンティティに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
1-1-6 証明書検証サーバ証明書の発行	H-1	証明書検証サーバの証明書要求により証明書を発行し、ファイル出力できることを確認。
	H-2	証明書検証サーバに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

(g) 香港チャイナ認証局から日本国認証局への証明書発行(Phase1:相互認証)

「表 7.9　香港チャイナ認証局から日本国認証局への証明書発行チェック項目」にチェック項目を示す。

表 7.9　香港チャイナ認証局から日本国認証局への証明書発行チェック項目

小項目	ID	チェック項目
1-1-2 証明書要求の発行	HJ-1	香港チャイナ認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。
	HJ-2	証明書要求に対応する相互認証証明書が日本国認証局から発行されたことを確認。
1-1-3 相互認証証明書の発行	HJ-1	日本国認証局から受け取った証明書要求により相互認証証明書を発行し、DER 形式でファイル出力できることを確認。
	HJ-2	日本国認証局に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

1-1-4 相互認証証明書ペアの発行	HJ-1	香港チャイナ認証局が日本国認証局に対して発行した相互認証証明書と、日本国認証局から香港チャイナ認証局に対して発行された相互認証証明書（DER形式で受領）から相互認証証明書ペアが生成できることを確認。
	HJ-2	日本国認証局が発行した相互認証証明書が相互認証証明書ペアのforwardに格納されていることを確認。
	HJ-3	日本国認証局に対して発行した相互認証証明書が相互認証証明書ペアの reverse に格納されていることを確認。

(h) 日本国認証局のローカルドメイン内の証明書発行（Phase2）

「表 7.10　日本国認証局のローカルドメイン内の証明書発行チェック項目」にチェック項目を示す。

表 7.10　日本国認証局のローカルドメイン内の証明書発行チェック項目

小項目	ID	チェック項目
1-1-1 自己署名証明書の発行	J-1	自己署名証明書の内容が、「相互接続インターフェース仕様」に従っていることを確認。
1-1-5 エンドエンティティ証明書の発行	J-1	エンドエンティティに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
1-1-6 証明書検証サーバ証明書の発行	J-1	証明書検証サーバの証明書要求により証明書を発行し、ファイル出力できることを確認。
	J-2	証明書検証サーバに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

(i) 日本国認証局からチャイニーズ台北認証局への証明書発行（Phase2:相互認証）

「表 7.11　日本国認証局からチャイニーズ台北認証局への証明書発行チェック項目」にチェック項目を示す。

表 7.11　日本国認証局からチャイニーズ台北認証局への証明書発行チェック項目

小項目	ID	チェック項目
1-1-2 証明書要求の発行	JT-1	日本国認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。

	JT-2	証明書要求に対応する相互認証証明書がチャイニーズ台北認証局から発行されたことを確認。
1-1-3 相互認証証明書の発行	JT-1	チャイニーズ台北認証局から受け取った証明書要求により相互認証証明書を発行し、DER 形式でファイル出力できることを確認。
	JT-2	チャイニーズ台北認証局に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
1-1-4 相互認証証明書ペアの発行	JT-1	日本国認証局がチャイニーズ台北認証局に対して発行した相互認証証明書と、チャイニーズ台北認証局から日本国認証局に対して発行された相互認証証明書（DER 形式で受領）から相互認証証明書ペアが生成できることを確認。
	JT-2	チャイニーズ台北認証局が発行した相互認証証明書が相互認証証明書ペアの forward に格納されていることを確認。
	JT-3	チャイニーズ台北認証局に対して発行した相互認証証明書が相互認証証明書ペアの reverse に格納されていることを確認。

(j) チャイニーズ台北認証局のローカルドメイン内の証明書発行（Phase2）

「表 7.12 チャイニーズ台北認証局のローカルドメイン内の証明書発行チェック項目」にチェック項目を示す。

表 7.12 チャイニーズ台北認証局のローカルドメイン内の証明書発行チェック項目

小項目	ID	チェック項目
1-1-1 自己署名証明書の発行	T-1	自己署名証明書の内容が、「相互接続インターフェース仕様」に従っていることを確認。
1-1-5 エンドエンティティ証明書の発行	T-1	エンドエンティティに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

(k) チャイニーズ台北認証局から日本国認証局への証明書発行（Phase2：相互認証）

「表 7.13　チャイニーズ台北認証局から日本国認証局への証明書発行チェック項目」にチェック項目を示す。

表 7.13　チャイニーズ台北認証局から日本国認証局への証明書発行チェック項目

小項目	ID	チェック項目
1-1-2 証明書要求の発行	TJ-1	チャイニーズ台北認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。
	TJ-2	証明書要求に対応する相互認証証明書が日本国認証局から発行されたことを確認。
1-1-3 相互認証証明書の発行	TJ-1	日本国認証局から受け取った証明書要求により相互認証証明書を発行し、DER 形式でファイル出力できることを確認。
	TJ-2	日本国認証局に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
1-1-4 相互認証証明書ペアの発行	TJ-1	チャイニーズ台北認証局が日本国認証局に対して発行した相互認証証明書と、日本国認証局からチャイニーズ台北認証局に対して発行された相互認証証明書（DER 形式で受領）から相互認証証明書ペアが生成できることを確認。
	TJ-2	日本国認証局が発行した相互認証証明書が相互認証証明書ペアの forward に格納されていることを確認。
	TJ-3	日本国認証局に対して発行した相互認証証明書が相互認証証明書ペアの reverse に格納されていることを確認。

(3) 実験結果

すべてのチェック項目の実施結果は「問題なし」である。

(4) 評価及び考察

本実験単位では、シミュレーションセンタという実運用の制約のない環境において「相互接続インターフェース仕様」の証明書プロファイルに関して「表 7.1 シミュレーションセンタ環境における 2 種類の証明書プロファイル」に示す 2 つの証明書プロファイルを用い証明書発行の実証実験を行った。

「相互接続インターフェース仕様」に従った証明書発行を行うことで、正しい実験結果を得ることができた。この結果は「相互接続インターフェース仕様」の認証局の証明書発行業務への適用が可能であり、標準が実用性を持つことを示している。

7.3　相互接続に係わる証明書失効

(1) 実験内容

シミュレーションセンタにおいて、「相互接続インターフェース仕様」に従って相互接続に係わる証明書の失効、CRL 及び ARL の発行を実施し、その結果得られた実験データを収集して分析する。

認証局が発行する失効情報の種類による実験単位の小項目を「表 7.14　シミュレーションセンタにおける証明書失効実験単位小項目一覧」に示す。

表 7.14　シミュレーションセンタにおける証明書失効実験単位小項目一覧

小項目番号	実験単位小項目
1-2-1	CRL の発行
1-2-2	ARL の発行

各国認証局が失効する証明書は運用により異なる。本実証実験で対象とする 3 国／地域の認証局が失効する証明書は以下のとおりである。

(a) 日本国認証局が失効する証明書

- 相互認証証明書
- エンドエンティティ証明書

(b) チャイニーズ台北認証局が失効する証明書

- 相互認証証明書
- エンドエンティティ証明書

(c) 香港チャイナ認証局が失効する証明書

- 相互認証証明書
- エンドエンティティ証明書

(2) 実験方法

シミュレーションセンタ内に設置した日本国認証局、チャイニーズ台北認証局及び香港チャイナ認証局が発行した相互接続に係わる証明書を失効する。

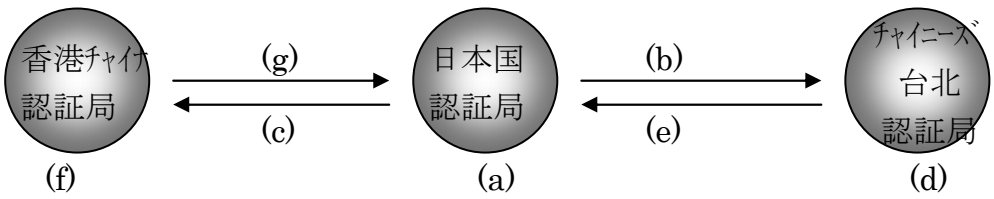


図 7.3　認証局間の証明書失効

各認証局のローカルドメイン内の証明書失効と、「図 7.3　認証局間の証明書失効」で実線で示した認証局間の証明書失効を実験対象とする。

(a) 日本国認証局内のローカルドメイン内の証明書失効

「表 7.15　日本国認証局内のローカルドメイン内の証明書失効チェック項目」にチェック項目を示す。

表 7.15　日本国認証局内のローカルドメイン内の証明書失効チェック項目

小項目	ID	チェック項目
1-2-1 CRL の発行	J-1	CRL が発行されることを確認。
	J-2	CRL の内容が「相互接続インターフェース仕様」に従っていることを確認。
	J-3	失効したエンドエンティティ証明書情報が、「相互接続インターフェース仕様」に従って格納されることを確認。

(b) 日本国認証局からチャイニーズ台北認証局への証明書失効

「表 7.16　日本国認証局からチャイニーズ台北認証局への証明書失効チェック項目」にチェック項目を示す。

表 7.16　日本国認証局からチャイニーズ台北認証局への証明書失効チェック項目

小項目	ID	チェック項目
1-2-2 ARL の発行	JT-1	ARL が発行されることを確認。
	JT-2	ARL の内容が「相互接続インターフェース仕様」に従っていることを確認。
	JT-3	失効した相互認証証明書情報が、「相互接続インターフェース仕様」に従って格納されることを確認。

(c) 日本国認証局から香港チャイナ認証局への証明書の失効

「表 7.17　日本国認証局から香港チャイナ認証局への証明書失効チェック項目」にチェック項目を示す。

表 7.17　日本国認証局から香港チャイナ認証局への証明書失効チェック項目

小項目	ID	チェック項目
1-2-2 ARL の発行	JH-1	ARL が発行されることを確認。
	JH-2	ARL の内容が「相互接続インターフェース仕様」に従っていることを確認。

	JH-3	失効した相互認証証明書情報が、「相互接続インターフェース仕様」に従って格納されることを確認。

(d) チャイニーズ台北認証局のローカルドメイン内証明書失効

「表 7.18　チャイニーズ台北認証局内ローカルドメイン内証明書失効チェック項目」にチェック項目を示す。

表 7.18　チャイニーズ台北認証局内ローカルドメイン内証明書失効チェック項目

小項目	ID	チェック項目
1-2-1 CRL の発行	T-1	CRL が発行されることを確認。
	T-2	CRL の内容が「相互接続インターフェース仕様」に従っていることを確認。
	T-3	失効したエンドエンティティ証明書情報が、「相互接続インターフェース仕様」に従って格納されることを確認。

(e) チャイニーズ台北認証局から日本国認証局への証明書の失効

「表 7.19　チャイニーズ台北認証局から日本国認証局への証明書失効チェック項目」にチェック項目を示す。

表 7.19　チャイニーズ台北認証局から日本国認証局への証明書失効チェック項目

小項目	ID	チェック項目
1-2-2 ARL の発行	TJ-1	ARL が発行されることを確認。
	TJ-2	ARL の内容が「相互接続インターフェース仕様」に従っていることを確認。
	TJ-3	失効した相互認証証明書情報が、「相互接続インターフェース仕様」に従って格納されることを確認。

(f) 香港チャイナ認証局のローカルドメイン内証明書失効

「表 7.20　香港チャイナ認証局のローカルドメイン内証明書失効チェック項目」にチェック項目を示す。

表 7.20　香港チャイナ認証局のローカルドメイン内証明書失効チェック項目

小項目	ID	チェック項目
1-2-1 CRL の発行	H-1	CRL が発行されることを確認。
	H-2	CRL の内容が「相互接続インターフェース仕様」に従っていることを確認。

	H-3	失効したエンドエンティティ証明書情報が、「相互接続インターフェース仕様」に従って格納されることを確認。

(g) 香港チャイナ認証局から日本国認証局への証明書失効

「表 7.21　香港チャイナ認証局から日本国認証局への証明書失効チェック項目」にチェック項目を示す。

表 7.21　香港チャイナ認証局から日本国認証局への証明書失効チェック項目

小項目	ID	チェック項目
1-2-2 ARL の発行	HJ-1	ARL が発行されることを確認。
	HJ-2	ARL の内容が「相互接続インターフェース仕様」に従っていることを確認。
	HJ-3	失効した相互認証証明書情報が、「相互接続インターフェース仕様」に従って格納されることを確認。

(3) 実験結果

すべてのチェック項目の実施結果は「問題なし」である。

(4) 評価及び考察

シミュレーションセンタという実運用の制約のない環境において「相互接続インターフェース仕様」に従った証明書失効を行うことで、正しい実験結果を得ることができた。この結果は「相互接続インターフェース仕様」の認証局の証明書失効業務への適用が可能であり、標準が実用性を持つことを示している。

7.4　相互接続に係わる証明書更新

(1) 実験内容

シミュレーションセンタにおいて、「相互接続インターフェース仕様」に従って相互接続に係わる証明書を更新し、その結果得られた実験データを収集して分析する。

実験単位の小項目を「表 7.22　証明書更新に関する実験単位小項目一覧」に示す。

表 7.22　証明書更新に関する実験単位小項目一覧

項目番号	実験単位の小項目
1-3-1	相互認証証明書の更新

各国認証局が更新する証明書は相互接続モデルにより異なる。本実証実験で対象とする 3 国／地域の認証局が更新する証明書は以下のとおりである。

(a) 日本国認証局が更新する証明書

- 相互認証証明書

(b) チャイニーズ台北認証局が更新する証明書

- 相互認証証明書

(c) 香港チャイナ認証局が更新する証明書

- 相互認証証明書

(2) 実験方法

シミュレーションセンタ内に設置した日本国認証局、チャイニーズ台北認証局及び香港チャイナ認証局で、相互認証証明書を更新する。

図 7.4　認証局間の証明書更新

「図 7.4　認証局間の証明書更新」で実線で示した認証局間の相互証明書再発行を実験対象とする。

(a) 日本国認証局からチャイニーズ台北認証局への証明書更新チェック項目

「表 7.23　日本国認証局からチャイニーズ台北認証局への証明書更新チェック項目」にチェック項目を示す。

表 7.23　日本国認証局からチャイニーズ台北認証局への証明書更新チェック項目

小項目	ID	チェック項目
1-3-1 相互認証証明書の更新	JT-1	相互認証証明書更新ができることを確認。
	JT-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(b) 日本国認証局から香港チャイナ認証局への証明書更新チェック項目

「表 7.24　日本国認証局から香港チャイナ認証局への証明書更新チェック項目」にチェック項目を示す。

表 7.24　日本国認証局から香港チャイナ認証局への証明書更新チェック項目

小項目	ID	チェック項目
1-3-1 相互認証証明書の更新	JH-1	相互認証証明書更新ができることを確認。
	JH-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(c) チャイニーズ台北認証局から日本国認証局への証明書更新チェック項目

「表 7.25　チャイニーズ台北認証局から日本国認証局への証明書更新チェック項目」にチェック項目を示す。

表 7.25　チャイニーズ台北認証局から日本国認証局への証明書更新チェック項目

小項目	ID	チェック項目
1-3-1 相互認証証明書の更新	TJ-1	相互認証証明書更新ができることを確認。
	TJ-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(d) 香港チャイナ認証局から日本国認証局への証明書更新チェック項目

「表 7.26　香港チャイナ認証局から日本国認証局への証明書更新チェック項目」にチェック項目を示す。

表 7.26　香港チャイナ認証局から日本国認証局への証明書更新チェック項目

小項目	ID	チェック項目
1-3-1 相互認証証明書の更新	HJ-1	相互認証証明書更新ができることを確認。
	HJ-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(3) 実験結果

すべてのチェック項目の実施結果は「問題なし」である。

(4) 評価及び考察

シミュレーションセンタという実運用の制約のない環境において、正しい実験結果を得ることができた。この結果は「相互接続インターフェース仕様」の認証局の証明書更新業務への適用が可能であり、標準が実用性を持つことを示している。

7.5　相互接続に係わる証明書再発行

(1) 実験内容

シミュレーションセンタにおいて、「相互接続インターフェース仕様」に従って相互接続に係わる証明書を再発行し、その結果得られた実験データを収集して分析する。

実験単位の小項目を「表 7.27　証明書再発行に関する実験単位小項目一覧」に示す。

表 7.27　証明書再発行に関する実験単位小項目一覧

項目番号	実験単位小項目
1-4-1	旧相互認証証明書の失効
1-4-2	新相互認証証明書の発行

各国認証局が再発行する証明書は相互接続モデルにより異なる。本実証実験で対象とする 3 国／地域の認証局が再発行する証明書は以下のとおりである。

(a) 日本国認証局が更新する証明書

- 相互認証証明書

(b) チャイニーズ台北認証局が更新する証明書

- 相互認証証明書

(c) 香港チャイナ認証局が更新する証明書

- 相互認証証明書

(2) 実験方法

シミュレーションセンタ内に設置した日本国認証局、チャイニーズ台北認証局および香港チャイナ認証局で、相互認証証明書を再発行する。

図 7.5　認証局間の証明書再発行

「図 7.5　認証局間の証明書再発行」で実線で示した認証局間の相互証明書再発行を実験対象とする。

(a) 日本国認証局からチャイニーズ台北認証局への証明書再発行チェック項目

「表 7.28 日本国認証局からチャイニーズ台北認証局への証明書再発行チェック項目」にチェック項目を示す。

表 7.28 日本国認証局からチャイニーズ台北認証局への証明書再発行チェック項目

小項目	ID	チェック項目
1-4-1 旧相互認証証明書の失効	JT-1	旧相互認証証明書を失効できることを確認。
	JT-2	失効した相互認証証明書の情報がARLに格納されることを確認。
1-4-2 相互認証証明書の再発行	JT-1	相互認証証明書の再発行ができることを確認。
	JT-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(b) 日本国認証局から香港チャイナ認証局への証明書再発行チェック項目

「表 7.29　日本国認証局から香港チャイナ認証局への証明書再発行チェック項目」にチェック項目を示す。

表 7.29　日本国認証局から香港チャイナ認証局への証明書再発行チェック項目

小項目	ID	チェック項目
1-4-1 旧相互認証証明書の失効	JH-1	旧相互認証証明書を失効できることを確認。
	JH-2	失効した相互認証証明書の情報がARLに格納されることを確認。
1-4-2 相互認証証明書の再発行	JH-1	相互認証証明書の再発行ができることを確認。
	JH-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(c) チャイニーズ台北認証局から日本国認証局への証明書再発行チェック項目

「表 7.30 チャイニーズ台北認証局から日本国認証局への証明書再発行チェック項目」にチェック項目を示す。

表 7.30 チャイニーズ台北認証局から日本国認証局への証明書再発行チェック項目

小項目	ID	チェック項目
1-4-1 旧相互認証証明書の失効	TJ-1	旧相互認証証明書を失効できることを確認。
	TJ-2	失効した相互認証証明書の情報がARLに格納されることを確認。
1-4-2	TJ-1	相互認証証明書の再発行ができることを確認。

相互認証証明書の再発行	TJ-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(d) 香港チャイナ認証局から日本国認証局への証明書再発行チェック項目

「表 7.31　香港チャイナ認証局から日本国認証局への証明書再発行チェック項目」にチェック項目を示す。

表 7.31　香港チャイナ認証局から日本国認証局への証明書再発行チェック項目

小項目	ID	チェック項目
1-4-1 旧相互認証証明書の失効	HJ-1	旧相互認証証明書を失効できることを確認。
	HJ-2	失効した相互認証証明書の情報がARLに格納されることを確認。
1-4-2 相互認証証明書の再発行	HJ-1	相互認証証明書の再発行ができることを確認。
	HJ-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(3) 実験結果

すべてのチェック項目の実施結果は「問題なし」である。

(4) 評価及び考察

シミュレーションセンタという実運用の制約のない環境において、「相互接続インターフェース仕様」に従った証明書の再発行を行うことで、正しい実験結果を得ることができた。この結果は「相互接続インターフェース仕様」の認証局の証明書再発行業務への適用が可能であり、標準が実用性を持つことを示している。

8 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

8.1　概要

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する。証明書の検証には検証局を使用する。また、実験にはシミュレーション環境を利用する。

(1) 実験データ

実験データとしては「表 8.1　実験データ」のものを収集する。

表 8.1　実験データ

No	実験データ	補足
1	日本国認証局、チャイニーズ台北認証局及び香港チャイナ認証局の発行する証明書、CRL、証明書発行要求、及び証明書配付データを含む出力データ	「7 シミュレーションセンタにおける認証局間の実証実験」で発行した証明書を使用する。
2	日本国ディレクトリサーバ、チャイニーズ台北ディレクトリサーバ及び香港チャイナディレクトリサーバのエントリ情報を含む LDIF(LDAP Data Interchange Format)データ	「7 シミュレーションセンタにおける認証局間の実証実験」において発行した証明書及びディレクトリサーバを使用する。
3	日本国検証局のログ情報による検証結果情報	ログを解析し、証明書検証結果の評価を行う。

(2) 実験内容

本実験で実施する検証内容と対応する実験単位中項目を「表 8.2　シミュレーションセンタにおける証明書検証実験単位中項目一覧」に示す。

表 8.2　シミュレーションセンタにおける証明書検証実験単位中項目一覧

実験単位中項目	検証項目	検証内容
2-1	認証パス検証	利用者が有効な証明書を受け取った場合の証

		明書検証を行う。
2-2	失効検証	利用者が失効されている証明書を受け取った場合の証明書検証を行う。
2-3	有効期限検証	利用者が有効期限の切れた証明書を受け取った場合の証明書検証を行う。
2-4	ポリシ検証	利用者が受け入れられないポリシがセットされた証明書を受け取った場合の証明書検証を行う。
2-5	認証パス構築検証	認証パス構築を完成することができない場合の証明書検証を行う。

(3) 実験方法

(a) 実験環境

シミュレーションセンタ内に、日本国認証局、チャイニーズ台北認証局及び香港チャイナ認証局を模擬的に設置する。

本実験における、各国/地域の認証局、日本国検証局、利用者、証明書検証の関係を表したものを「図 8.1　シミュレーションセンタにおける証明書検証の実験環境」に示す。

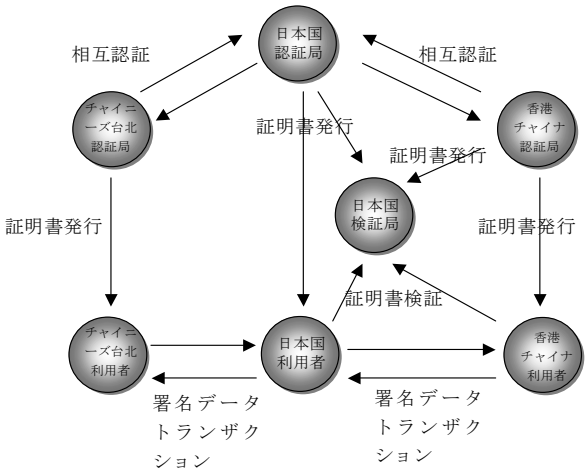


図 8.1　シミュレーションセンタにおける証明書検証の実験環境

本実験では、日本－香港チャイナ間で相互認証がなされ、かつ、それぞれの認証局より日本国検証局へ VA 証明書の発行を行うことを想定した。従って日本国検証局は、日本国利用者からの証明書検証要求を受け付けるとともに、香港チャイナ利用者からの証明書検証要求も受け付ける。つまり、日本国検証局は、日本および香港チャイナの両ドメインで共用されている。

(b) 実験手順

本実験を実施するにあたっての実験手順を「表 8.3　実験手順」に示す。

表 8.3　実験手順

実験項目	担当		項番	内容
	日本	相手		
事前準備	○		1	相互認証証明書ペアがリポジトリに格納されていることを確認する
	○		2	自己署名証明書がリポジトリに格納されていることを確認する
	○		3	検証局の VA 証明書を発行する
	○		4	検証局に VA 証明書を格納する
	○		5	エンドエンティティ証明書を発行する
	○		6	エンドエンティティ証明書を渡す
		○	7	エンドエンティティ証明書を受け取る
		○	8	相互認証証明書ペアがリポジトリに格納されていることを確認する
		○	9	自己署名証明書がリポジトリに格納されていることを確認する
		○	10	検証局の VA 証明書を発行する（香港チャイナのみ）
	○		11	検証局に VA 証明書を格納する（香港チャイナのみ）
		○	12	エンドエンティティ証明書を発行する
		○	13	エンドエンティティ証明書を渡す
	○		14	エンドエンティティ証明書を受け取る
証明書検証	○		1	相手国/地域のエンドエンティティ証明書の検証を実施する
	○		2	日本国検証局のログを取得する
	○		3	日本国利用者端末のログを取得する
		○	4	日本のエンドエンティティ証明書の検証を実施する（香港チャイナのみ）
	○		5	検証局のログを取得する（香港チャイナのみ）
		○	6	相手国/地域利用者端末のログを取得する（香港チャイナのみ）
結果評価	○		1	日本国検証局のログを解析し、証明書検証結果の評価を行う

8.2　認証パス検証

(1) 実験内容

「7 シミュレーションセンタにおける認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に、「利用者が有効な証明書を受け取ったときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 8.4　認証パス検証における実験項目」に示す。

表 8.4　認証パス検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	VAモデル	チャイニーズ台北利用者の証明書は有効
S-HJ-JVA	日本国利用者	香港チャイナ利用者	VAモデル	香港チャイナ利用者の証明書は有効
S-HJ-OVA	香港チャイナ利用者	日本国利用者	VAモデル	日本国利用者の証明書は有効

本実験における期待値を「表 8.5　認証パス検証における期待値」に示す。

表 8.5　認証パス検証における期待値

実験単位 中項目	検証項目	EE 証明書	期待値		意味
			結果	Return Code[12]	
2-1	認証パス検証	EE01	Valid	0	証明書は有効である

(2) 実験結果データ

本実験における検証結果を「表 8.6　認証パス検証における検証結果」に示す。

表 8.6　認証パス検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	Valid	0	○

[12] ReturnCode については、政府認証基盤(GPKI)相互運用性仕様書を参照。URL: http://www.gpki.go.jp/

S-HJ-JVA	日本国利用者	香港チャイナ利用者	Valid	0	○
S-HJ-OVA	香港チャイナ利用者	日本国利用者	Valid	0	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 8.6　認証パス検証における検証結果」よりわかるとおり、全ての ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書が有効であることから、証明書の検証を行った結果は、有効である旨の結果が返らなければならない。

証明書検証ログを解析したところ、各検証項目に対して「0」という結果が出力された。これは正常に証明書検証が実施され、問題がなかったことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

8.3　失効検証

(1) 実験内容

「7 シミュレーションセンタにおける認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に、「利用者が失効している証明書を受け取ったときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 8.7　失効検証における実験項目」に示す。

表 8.7　失効検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	VA モデル	チャイニーズ台北利用者の証明書は失効されている
S-HJ-JVA	日本国利用者	香港チャイナ利用者	VA モデル	香港チャイナ利用者の証明書は失効されている
S-HJ-OVA	香港チャイナ利用者	日本国利用者	VA モデル	日本国利用者の証明書は失効されている

本実験における期待値を「表 8.8　失効検証における期待値」に示す。

表 8.8　失効検証における期待値

中項目番号	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
2-2	失効検証	EE02	Invalid	203	証明書は失効されている

(2) 実験結果データ

本実験における検証結果を「表 8.9　失効検証における検証結果」に示す。

表 8.9　失効検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	Invalid	203	○
S-HJ-JVA	日本国利用者	香港チャイナ利用者	Invalid	203	○
S-HJ-OVA	香港チャイナ利用者	日本国利用者	Invalid	203	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 8.9　失効検証における検証結果」よりわかるとおり、全の ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書が失効されていることから、証明書の検証を行った結果は、有効でない旨の結果が返らなければならない。

証明書検証ログを解析したところ、「203」という結果が出力された。これは認証パス中に失効されている証明書が含まれていたことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

8.4　有効期限検証

(1) 実験内容

「7 シミュレーションセンタにおける認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に､｢利用者が有効期限の切れた証明書を受け取ったときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 8.10　有効期限検証における実験項目」に示す。

表 8.10　有効期限検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	VAモデル	チャイニーズ台北利用者の証明書の有効期限が切れている
S-HJ-JVA	日本国利用者	香港チャイナ利用者	VAモデル	香港チャイナ利用者の証明書の有効期限が切れている
S-HJ-OVA	香港チャイナ利用者	日本国利用者	VAモデル	日本国利用者の証明書の有効期限が切れている

本実験における期待値を「表 8.11　有効期限検証における期待値」に示す。

表 8.11　有効期限検証における期待値

実験単位 中項目	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
2-3	有効期限検証	EE03	Invalid	203	証明書が有効期間の範囲外である

(2) 実験結果データ

本実験における検証結果を｢表 8.12　有効期限検証における検証結果｣に示す。

表 8.12　有効期限検証における検証結果

ID	検証者	検証対象者	検証結果		期待値 との比較
			結果	Return Code	

S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	Invalid	203	○
S-HJ-JVA	日本国利用者	香港チャイナ利用者	Invalid	203	○
S-HJ-OVA	香港チャイナ利用者	日本国利用者	Invalid	203	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 8.12　有効期限検証における検証結果」よりわかるとおり、全ての ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書の有効期限が切れていることから、証明書の検証を行った結果は、有効でない旨の結果が返らなければならない。

証明書検証ログを解析したところ、「203」という結果が出力された。これは認証パス中に失効されている証明書（有効期限が切れている証明書）が含まれていたことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

8.5　ポリシ検証

(1) 実験内容

「7 シミュレーションセンタにおける認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に、「利用者が受け入れられないポリシがセットされた証明書を受け取ったときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 8.13　ポリシ検証における実験項目」に示す。

表 8.13　ポリシ検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	VAモデル	チャイニーズ台北利用者の証明書には受け入れられないポリシがセットされている
S-HJ-JVA	日本国利用者	香港チャイナ利用者	VAモデル	香港チャイナ利用者の証明書には受け入れられないポリシがセットされている
S-HJ-OVA	香港チャイナ利用者	日本国利用者	VAモデル	日本国利用者の証明書には受け入れられないポリシがセットされている

本実験における期待値を「表 8.14　ポリシ検証における期待値」に示す。

表 8.14　ポリシ検証における期待値

実験単位 中項目	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
2-4	ポリシ検証	EE04	Invalid	205	証明書がポリシ制約の条件を満たさない

(2) 実験結果データ

本実験における検証結果を「表 8.15　ポリシ検証における検証結果」に示す。

表 8.15　ポリシ検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	Invalid	205	○
S-HJ-JVA	日本国利用者	香港チャイナ利用者	Invalid	205	○
S-HJ-OVA	香港チャイナ利用者	日本国利用者	Invalid	205	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 8.15　ポリシ検証における検証結果」よりわかるとおり、全てのIDにおいて期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書のポリシが受け入れられないため、証明書の検証を行った結果は、有効でない旨の結果が返らなければならない。

証明書検証ログを解析したところ、「205」という結果が出力された。これは認証パス中に含まれる証明書のポリシが受け入れられないことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

8.6　認証パス構築検証

(1) 実験内容

「7 シミュレーションセンタにおける認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に、「認証パス構築を完成することができないときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 8.16　認証パス構築検証における実験項目」に示す。

表 8.16　認証パス構築検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
S-TCJ-JVA	日本国 利用者	チャイニーズ 台北利用者	VAモデル	チャイニーズ台北利用者の証明書とトラストアンカ間で、認証パスの構築ができない
S-HJ-JVA	日本国 利用者	香港チャイナ 利用者	VAモデル	香港チャイナ利用者の証明書とトラストアンカ間で、認証パスの構築ができない
S-HJ-OVA	香港チャイナ 利用者	日本国利用者	VAモデル	日本国利用者の証明書とトラストアンカ間で、認証パスの構築ができない

本実験における期待値を「表 8.17　認証パス構築検証における期待値」に示す。

表 8.17　認証パス構築検証における期待値

実験単位 中項目	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
2-5	認証パス検証	EE05	Invalid	101	認証パスの構築ができないい

(2) 実験結果データ

本実験における検証結果を「表 8.18　認証パス構築検証における検証結果」に示す。

表 8.18　認証パス構築検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
S-TCJ-JVA	日本国利用者	チャイニーズ台北利用者	Invalid	101	○
S-HJ-JVA	日本国利用者	香港チャイナ利用者	Invalid	101	○
S-HJ-OVA	香港チャイナ利用者	日本国利用者	Invalid	101	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 8.18　認証パス構築検証における検証結果」よりわかるとおり、全ての ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書とトラストアンカ間で認証パスの構築ができないため、証明書の検証を行った結果は有効でない旨の結果が返らなければならない。

証明書検証ログを解析したところ、「101」という結果が出力された。これは認証パスの構築ができなかったことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

9 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

9.1　概要

「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する。

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う。

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」の実用性を検証する。

(1) 実験方法

業務シナリオに従った「表 9.1　シミュレーションセンタにおける国際間調達の実験手順」に示す手順を実施する。

表 9.1　シミュレーションセンタにおける国際間調達の実験手順

手順番号	手順
1	エンドエンティティ証明書を発行する。
	エンドエンティティ証明書を格納する。
2	失効用エンドエンティティ証明書のCRLを発行する。
3	認証局自己署名証明書を格納する。
4	利用者登録を行う。
5	見積依頼書を作成する。
	見積依頼書に署名を付与し、結果を確認する。
	結果表示画面のハードコピーを採取する。
	見積依頼書をサーバへアップロードする。
6	見積依頼書を参照する。
	見積依頼書の署名を検証し、結果を確認する。
	結果表示画面のハードコピーを採取する。
7	見積回答書を作成する。
	見積回答書に署名を付与し、結果を確認する。
	結果表示画面のハードコピーを採取する。

	見積回答書をサーバへアップロードする。
8	見積回答書を参照する。
	見積回答書の署名を検証し、結果を確認する。
	結果表示画面のハードコピーを採取する。

9.2 正常系検証

(1) 目的

本実験単位は、売り手と買い手の双方が正常証明書を使用して「相互接続インターフェース仕様」の実用性の検証を目的とする。

(2) 実験内容

各国認証局より発行された正常証明書を売り手と買い手が使用する。売り手側利用者と買い手側利用者は業務シナリオに沿ってチェックリストに従い署名付与及び署名結果を確認する。

使用するエンドエンティティ証明書を以下の「表 9.2　使用するエンドエンティティ証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 9.2　使用するエンドエンティティ証明書

	証明書名	発行元	種別
1	EE01jp	日本国認証局	正常証明書
2	EE01chtssc	チャイニーズ台北認証局	正常証明書
3	EE01hkssc	香港チャイナ認証局	正常証明書

使用する自己署名証明書を以下の「表 9.3　使用する自己署名証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 9.3　使用する自己署名証明書

	証明書名	発行元
1	CAjp-SSC	日本国認証局
2	CAcht-SSC	チャイニーズ台北認証局
3	CAhk-SSC	香港チャイナ認証局

(3) 実験結果データ

署名付与や署名検証の結果が表示される画面のコピーやアプリケーションのログといった、実験データを取得した。その実験データを分析した結果得られた、本実験単位における実験結果を以下の「表 9.4　正常系検証実験結果データ」に示す。

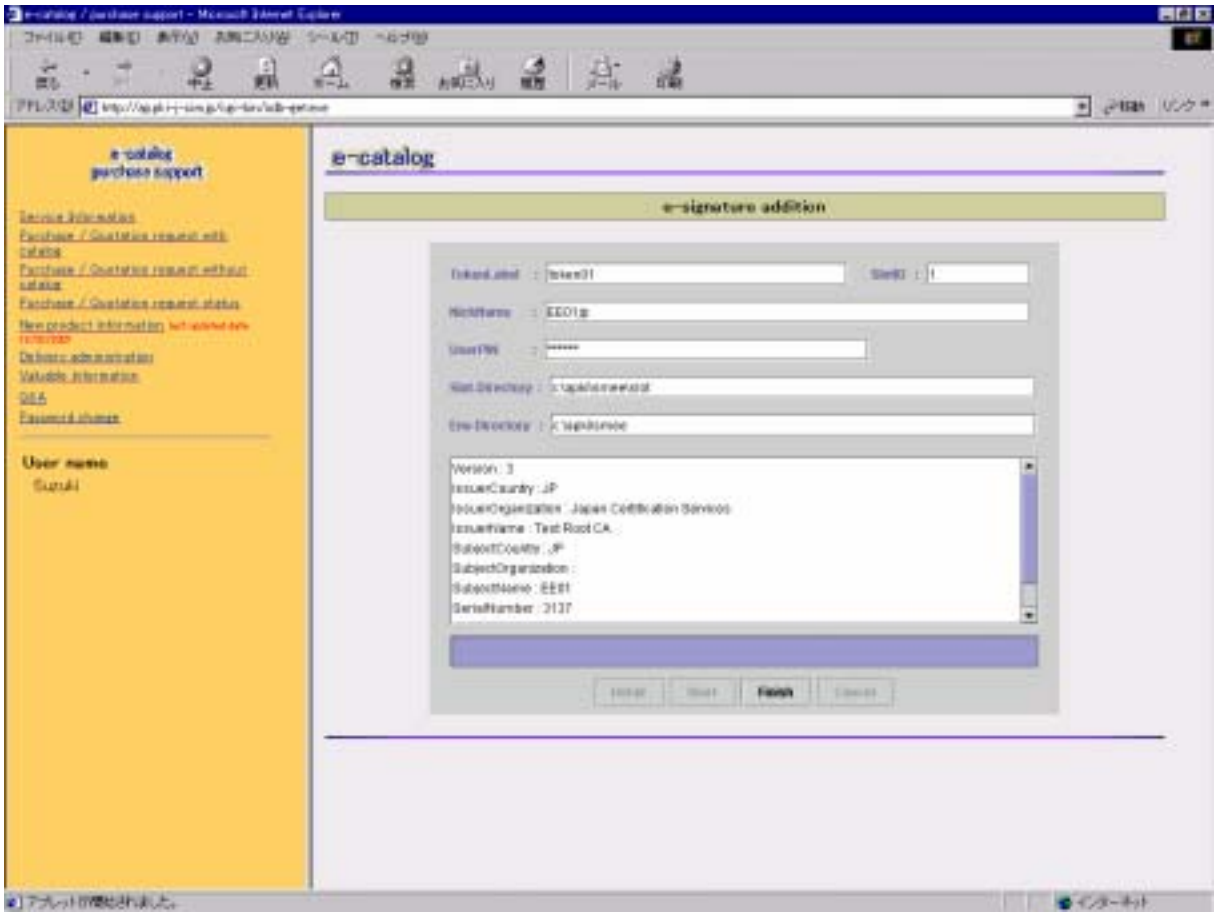
表 9.4　正常系検証実験結果データ

no	パターン	買い手	売り手	期待値	結果	判定
1	正常系(1)	日本・正常証明書	チャイニーズ台北・正常証明書	○	○	○
2	正常系(2)	チャイニーズ台北・正常証明書	日本・正常証明書	○	○	○
3	正常系(3)	日本・正常証明書	香港チャイナ・正常証明書	○	○	○
4	正常系(4)	香港チャイナ・正常証明書	日本・正常証明書	○	○	○

(4) 評価・考察

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正常系検証では、すべてのパターンにおいて、期待どおりの結果を得ることができた。

日本・チャイニーズ台北、日本・香港チャイナそしてチャイニーズ台北・香港チャイナの間における正常系の検証では、すべての署名付与を行うと正しく署名を付与できた旨伝える以下の「図 9.1　署名付与（例）日本・チャイニーズ台北」のような画面が表示された。



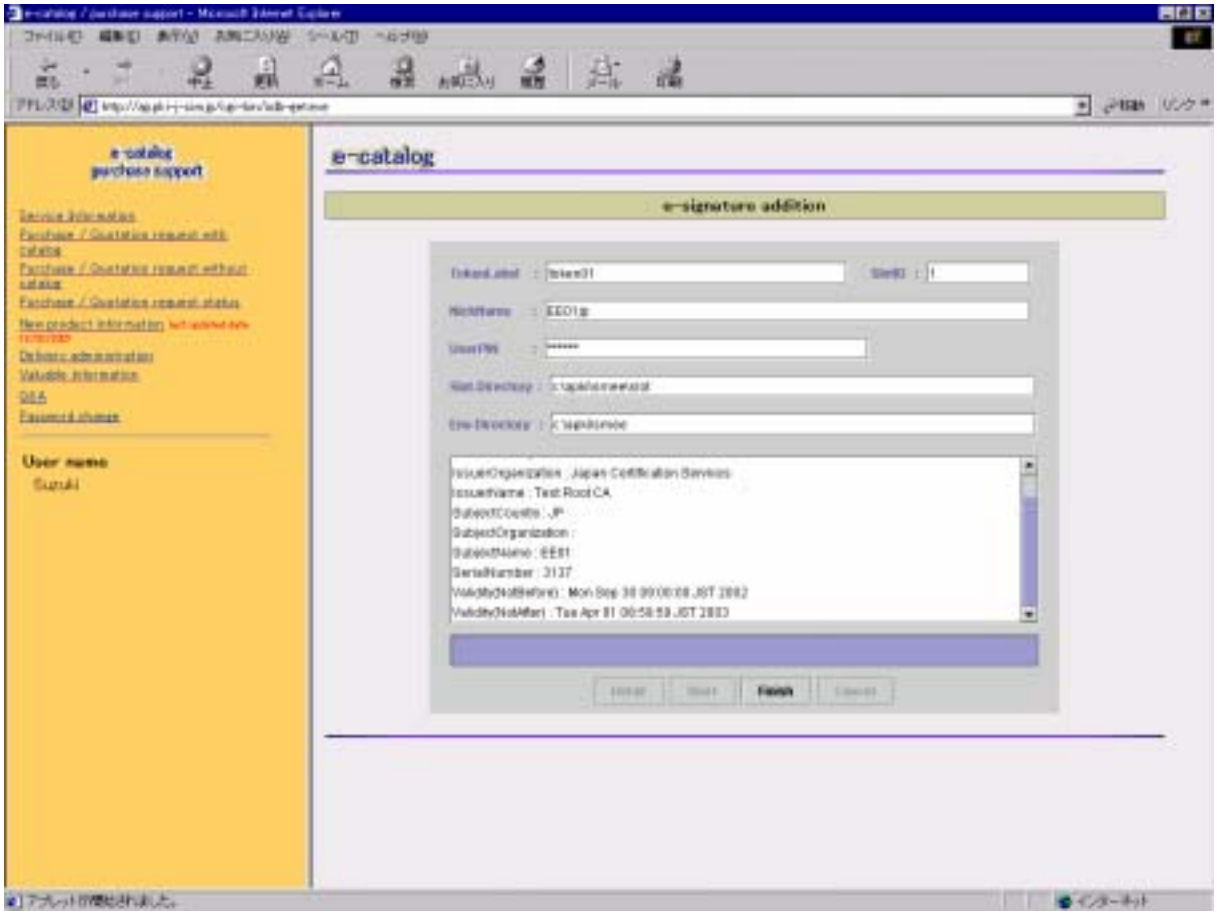


図 9.1　署名付与（例）日本・チャイニーズ台北

また、本正常系検証で証明書を検証する時すべてにおいて、証明書を正しく検証した結果を表示する以下の「図 9.2　有効性検証（例）日本・チャイニーズ台北」のような画面を得ることができた。

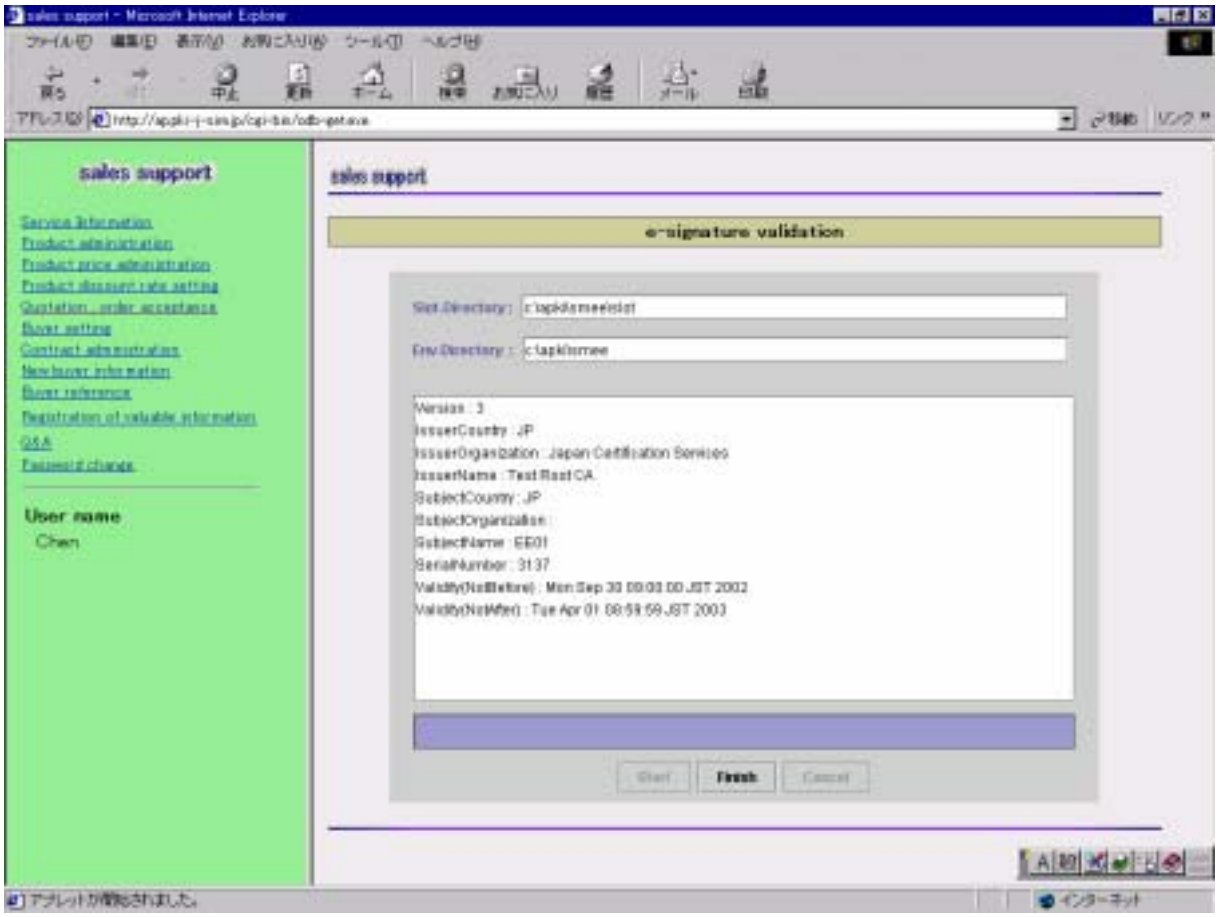


図 9.2　有効性検証（例）日本・チャイニーズ台北

以上より、「相互接続インターフェース仕様」は、国際間調達に支障をきたすものではなく、その実用性が評価されたと考える。

9.3　失効系 1 検証

(1) 目的

本実験単位は、売り手が失効証明書そして買い手が正常証明書を使用して PKI コンポーネント間接続に関する標準の実用性の検証を目的とする。

(2) 実験内容

各国認証局より発行された失効証明書を売り手が使用し、正常証明書を買い手が使用する。売り手側利用者と買い手側利用者は業務シナリオに沿ってチェックリストに従い署名付与及び署名結果を確認する。

使用するエンドエンティティ証明書を以下の「表 9.5　使用するエンドエンティティ証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 9.5　使用するエンドエンティティ証明書

	証明書名	発行元	種別
1	EE01jp	日本国認証局	正常証明書
2	EE02jp	日本国認証局	失効証明書
3	EE01chtssc	チャイニーズ台北認証局	正常証明書
4	EE02chtssc	チャイニーズ台北認証局	失効証明書
5	EE01hkssc	香港チャイナ認証局	正常証明書
6	EE02hkssc	香港チャイナ認証局	失効証明書

使用する自己署名証明書は以下を「表 9.6　使用する自己署名証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 9.6　使用する自己署名証明書

	証明書名	発行元
1	CAjp	日本国認証局
2	CAcht-SSC	チャイニーズ台北認証局
3	CAhk-SSC	香港チャイナ認証局

(3) 実験結果データ

署名付与や署名検証の結果が表示される画面のコピーとアプリケーションのログから実験データを取得した。その実験データを分析した結果得られた、本実験単位における実験結果を以下の「表 9.7　失効系 1 検証実験結果データ」に示す。

表 9.7　失効系 1 検証実験結果データ

no	パターン	買い手	売り手	期待値	結果	判定
1	失効系1(1)	日本・正常証明書	チャイニーズ台北・失効証明書	×	×	○
2	失効系1(2)	チャイニーズ台北・正常証明書	日本・失効証明書	×	×	○
3	失効系1(3)	日本・正常証明書	香港チャイナ・失効証明書	×	×	○
4	失効系1(4)	香港チャイナ・正常証明書	日本・失効証明書	×	×	○

(4) 評価・考察

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失効系 1 検証では、すべてのパターンにおいて、期待どおりの結果を得ることができた。

失効している証明書を使用して署名を行おうとすると、「図 9.3　署名付与　失敗（例）」のようなエラーが表示されることを確認した。

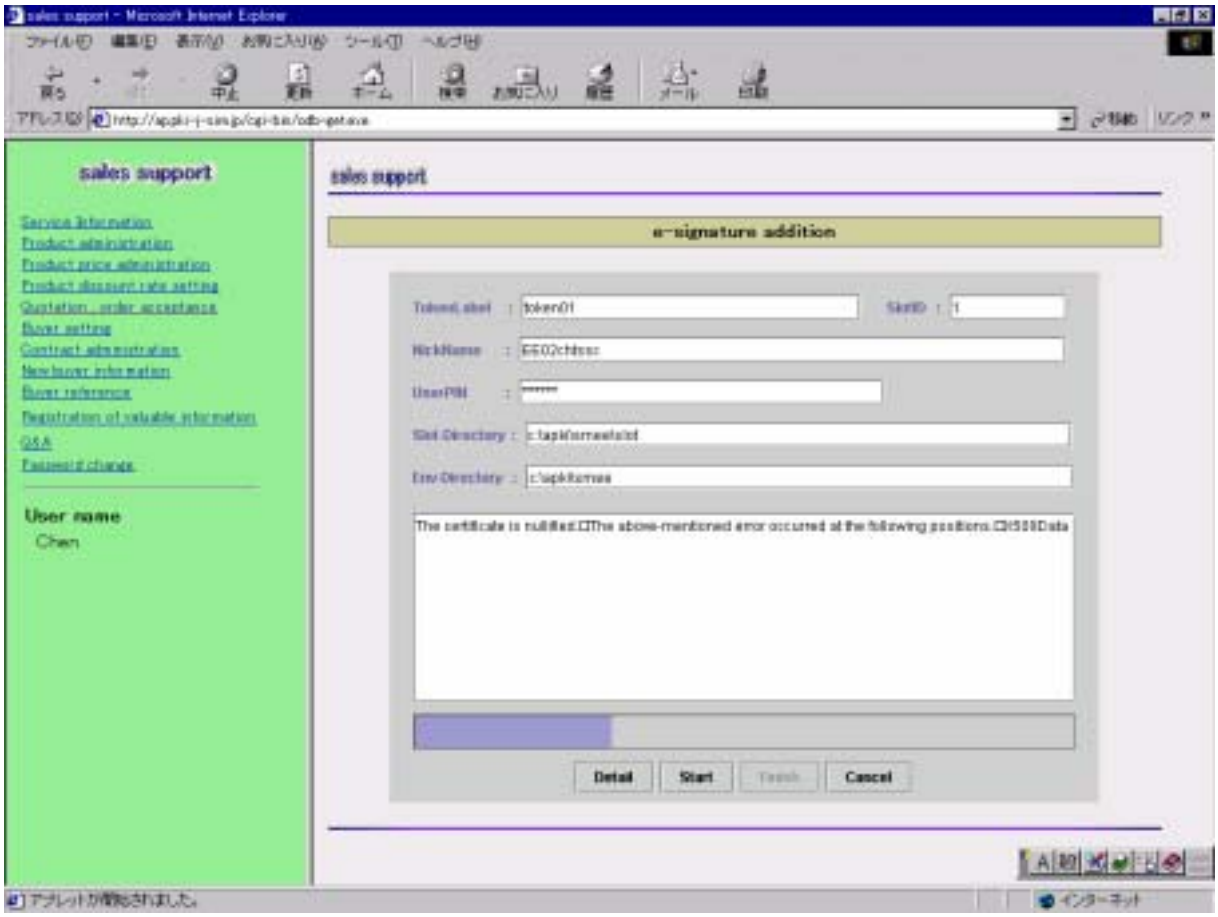


図 9.3　署名付与　失敗（例）

以上より、「相互接続インターフェース仕様」は、売り手の証明書が失効されている場合でも国際間調達に支障をきたすものではなく、その実用性が評価されたと考える。

9.4　失効系 2 検証

(1) 目的

本実験単位は、買い手が失効証明書そして売り手が正常証明書を使用して PKI コンポーネント間接続に関する標準の実用性の検証を目的とする。

(2) 実験内容

各国認証局より発行された失効証明書を買い手が使用し、正常証明書を売り手が使用する。売り手側利用者と買い手側利用者は業務シナリオに沿ってチェックリストに従い署名付与及び署名結果を確認する。

使用するエンドエンティティ証明書を以下の「表 9.8　使用するエンドエンテ

ィティ証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 9.8　使用するエンドエンティティ証明書

	証明書名	発行元	種別
1	EE01jp	日本国認証局	正常証明書
2	EE02jp	日本国認証局	失効証明書
3	EE01chtssc	チャイニーズ台北認証局	正常証明書
4	EE02chtssc	チャイニーズ台北認証局	失効証明書
5	EE01hkssc	香港チャイナ認証局	正常証明書
6	EE02hkssc	香港チャイナ認証局	失効証明書

使用する自己署名証明書は以下の「表 9.9　使用する自己署名証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 9.9　使用する自己署名証明書

	証明書名	発行元
1	CAjp	日本国認証局
2	CAcht-SSC	チャイニーズ台北認証局
3	CAhk-SSC	香港チャイナ認証局

(3) 実験結果データ

署名付与や署名検証の結果が表示される画面のコピーとアプリケーションのログから実験データを取得した。その実験データを分析した結果得られた、本実験単位における実験結果を以下の「表 9.10　失効系 2 検証実験結果データ」に示す。

表 9.10　失効系 2 検証実験結果データ

no	パターン	買い手	売り手	期待値	結果	判定
1	失効系2(1)	日本・失効証明書	チャイニーズ台北・正常証明書	×	×	○
2	失効系2(2)	チャイニーズ台北・失効証明書	日本・正常証明書	×	×	○
3	失効系2(3)	日本・失効証明書	香港チャイナ・正常証明書	×	×	○
4	失効系2(4)	香港チャイナ・失効証明書	日本・正常証明書	×	×	○

(4) 評価・考察

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失効系 2 検証では、すべてのパターンにおいて、期待どおりの結果を得ることができた。

失効している証明書を使用して署名を行おうとすると、署名の付与に失敗して

いることを確認した。

以上より、「相互接続インターフェース仕様」は、買い手の証明書が失効されている場合でも国際間調達に支障をきたすものではなく、その実用性が評価されたと考える。

10 現地環境における認証局間の実証実験

10.1　概要

本実験単位は、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」の有効性の検証を目的とする。

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する。

10.2　相互接続に係わる証明書発行

(1) 実験内容

現地実証実験環境において、「相互接続インターフェース仕様」に従って相互接続に係わる証明書、及び証明書発行要求を発行し、その結果得られた実験データを収集して分析する。

本実験単位においては「表 10.1　現地実証実験環境における 2 種類の証明書プロファイル」に示す 2 種類の異なった証明書プロファイルによる証明書発行を行う。Phase1 は、昨年度 IWG プロファイルに基づいたものである。Phase2 はチャイニーズ台北及び香港チャイナが Phase1 のプロファイルに対して異なる見解を持っていた点を吸収し、両国／地域の実際の運用に近づけたものである。

表 10.1　現地実証実験環境における2種類の証明書プロファイル

プロファイルの種類	プロファイルの相違	
	証明書種別	相違点
Phase1	自己署名証明書	cRLDP.distPoint.fullName の LDAPURI に属性値あり
	相互認証証明書	cRLDP.distPoint.fullName の LDAPURI に属性値あり
	CRL/ARL	iDP 指定必須
	エンドエンティティ証明書	keyUsage に digitalSignature を設定
		cRLDP.distPoint.fullName の LDAPURI に属性値あり
		CertificatePolicies は critical
Phase2	自己署名証明書	cRLDP.distPoint.fullName の LDAPURI は以下の 2 通り ・属性値なし ・属性値あり、binary オプションなし

	相互認証証明書	cRLDP.distPoint.fullName の LDAPURI は以下の 2 通り ・属性値なし ・属性値あり、binary オプションなし
	CRL/ARL	IssuingDistributionPoint 指定任意
	エンドエンティティ証明書	keyUsage は以下の 2 通り ・digitalSignature ・keyEncipherment 及び dataEncipherment
		CRLDistributionPoints は以下の 2 通り ・属性値なし ・属性値あり、binary オプションなし
		subjectAltName.rfc822Name を設定
		certificatePolicies は以下の 2 通り ・critical ・non critical

認証局が発行する証明書の種類による実験単位の小項目を「表 10.2　現地実証実験環境における証明書発行実験単位小項目一覧」に示す。

表 10.2　現地実証実験環境における証明書発行実験単位小項目一覧

小項目番号	実験単位小項目
4-1-1	自己署名証明書の発行
4-1-2	証明書要求の発行
4-1-3	相互認証証明書の発行
4-1-4	相互認証証明書ペアの発行
4-1-5	エンドエンティティ証明書の発行
4-1-6	証明書検証サーバの証明書発行

各国認証局が発行する証明書は運用により異なる。本実証実験で対象とする認証局が発行する証明書は以下のとおりである。

(a) 現地実証実験日本国認証局が発行する証明書類　(Phase1：相互認証、相互承認)

- 自己署名証明書
- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア

- エンドエンティティ証明書
- 証明書検証サーバ証明書

(b) 現地チャイニーズ台北認証局（中華電信）が発行する証明書類 （Phase1：相互認証）
- 自己署名証明書
- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア
- エンドエンティティ証明書

(c) 現地チャイニーズ台北認証局（TaiCA）が発行する証明書類（Phase1：相互承認）
- 自己署名証明書
- エンドエンティティ証明書

(d) 現地香港チャイナ認証局が発行する証明書類 （Phase1：相互承認）
- 自己署名証明書
- エンドエンティティ証明書

(e) 現地香港チャイナ認証局が発行する証明書類 （Phase1：相互認証）
- 自己署名証明書（(d)と同一）
- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア
- エンドエンティティ証明書（(d)と同一）

(f) 現地実証実験日本国認証局が発行する証明書類 （Phase2：相互認証）
- 自己署名証明書
- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア
- エンドエンティティ証明書
- 証明書検証サーバ証明書

(g) 現地チャイニーズ台北認証局（中華電信）が発行する証明書類 （Phase2：相互認証）
- 自己署名証明書

- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア
- エンドエンティティ証明書

(h) 現地チャイニーズ台北認証局（TaiCA）が発行する証明書類 （Phase2:相互認証）

- 自己署名証明書
- 証明書要求
- 相互認証証明書
- 相互認証証明書ペア
- エンドエンティティ証明書

(2) 実験方法

現地実証実験環境の現地実証実験日本国認証局、現地チャイニーズ台北認証局（中華電信)、現地チャイニーズ台北認証局（TaiCA）及び現地香港チャイナ認証局で、相互接続に係わる証明書を発行する。

各認証局間の相互接続時の信頼モデルとして、相互承認モデルと相互認証モデルの 2 通りを採用する。認証局間の信頼モデルと証明書プロファイルの関係を「表 10.3　現地環境における認証局間の信頼モデル」に示す。

表 10.3　現地環境における認証局間の信頼モデル

実験対象	信頼モデル	
	証明書プロファイル Phase1	証明書プロファイル Phase2
現地チャイニーズ台北認証局（中華電信）	相互認証	相互認証
現地チャイニーズ台北認証局（TaiCA）	相互承認	相互認証（証明書発行のみ）
現地香港チャイナ認証局	相互承認	―
現地香港チャイナ認証局	相互認証（証明書発行のみ）	―

また現地香港チャイナ認証局と現地実証実験日本国認証局との間は、香港チャイナの下位認証局と日本国のルート認証局の間で相互接続を行う。

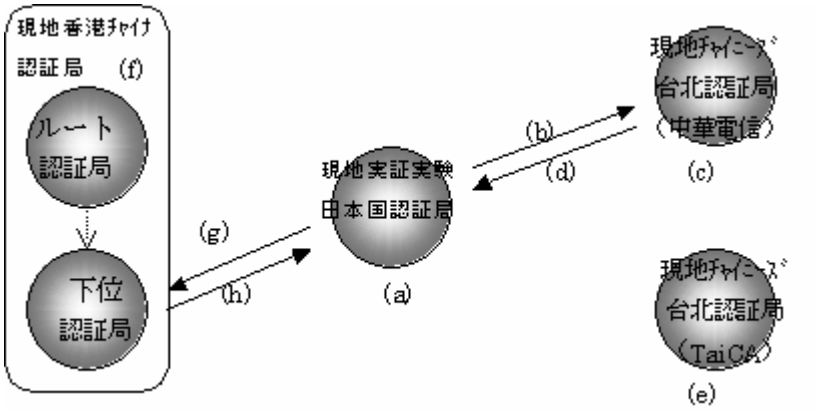


図 10.1　現地実証実験環境における認証局間の証明書発行(Phase1)

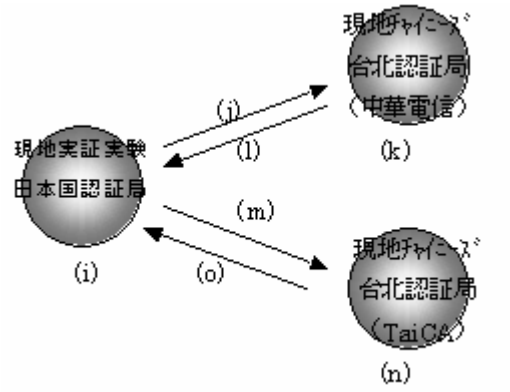


図 10.2　現地実証実験環境における認証局間の証明書発行(Phase2)

各認証局のローカルドメイン内の証明書発行と、「図 10.1　現地実証実験環境における認証局間の証明書発行(Phase1)」及び「図 10.2　現地実証実験環境における認証局間の証明書発行(Phase2)」に実線で示した認証局間の証明書発行を実験対象とする。

(a) 現地日本国認証局のローカルドメイン内の証明書発行(Phase1)

「表 10.4　現地実証実験日本国認証局のローカルドメイン内の証明書発行チェック項目」にチェック項目を示す。

表 10.4　現地実証実験日本国認証局のローカルドメイン内の証明書発行チェック項目

小項目	ID	チェック項目
4-1-1 自己署名証明書の発行	J-1	自己署名証明書の内容が、「相互接続インターフェース仕様」に従っていることを確認。

4-1-5 エンドエンティティ証明書の発行	J-1	エンドエンティティに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
4-1-6 証明書検証サーバ証明書の発行	J-1	証明書検証サーバの証明書要求により証明書を発行し、PKCS#7形式(自己署名証明書含む)でファイル出力できることを確認。
	J-2	証明書検証サーバに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

(b) 現地日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書発行(Phase1:相互認証)

「表 10.5　現地実証実験日本国認証局から現地チャイニーズ台北認証局(中華電信）への証明書発行チェック項目」にチェック項目を示す。

表 10.5　現地実証実験日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書発行チェック項目

小項目	ID	チェック項目
4-1-2 証明書要求の発行	T-1	現地実証実験日本国認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。
	T-2	証明書要求に対応する相互認証証明書が現地チャイニーズ台北認証局（中華電信）から発行されたことを確認。
4-1-3 相互認証証明書の発行	T-1	現地チャイニーズ台北認証局（中華電信）から受け取った証明書要求により相互認証証明書を発行し、DER形式でファイル出力できることを確認。
	T-2	現地チャイニーズ台北認証局（中華電信）に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
4-1-4 相互認証証明書ペアの発行	T-1	現地実証実験日本国認証局が現地チャイニーズ台北認証局（中華電信）に対して発行した相互認証証明書と、現地チャイニーズ台北認証局（中華電信）から現地日本国認証局に対して発行された相互認証証明書（DER形式で受領）から相互認証証明書ペアが生成できることを確認。
	T-2	現地チャイニーズ台北認証局（中華電信）が発行した相互認証証明書が相互認証証明書ペアのforwardに格納されていることを確認。

	T-3	現地チャイニーズ台北認証局（中華電信）に対して発行した相互認証証明書が相互認証証明書ペアのreverseに格納されていることを確認。

(c) 現地チャイニーズ台北認証局（中華電信）のローカルドメイン内の証明書発行（Phase1）

現地チャイニーズ台北認証局（中華電信）運用者により実施。

(d) 現地チャイニーズ台北認証局（中華電信）から現地日本国認証局への証明書発行(Phase1:相互認証)

現地チャイニーズ台北認証局（中華電信）運用者により実施。

(e) 現地チャイニーズ台北認証局（TaiCA）のローカルドメイン内の証明書発行（Phase1:相互承認）

現地チャイニーズ台北認証局（TaiCA）運用者により実施。

(f) 現地香港チャイナ認証局のローカルドメイン内の証明書発行（Phase1）

現地香港チャイナ認証局運用者により実施。

(g) 現地日本国認証局から現地香港チャイナ認証局への証明書発行（Phase1:相互認証）

「表 10.6　現地実証実験日本国認証局から現地香港チャイナ認証局への証明書発行チェック項目」にチェック項目を示す。

表 10.6　現地実証実験日本国認証局から現地香港チャイナ認証局への証明書発行チェック項目

小項目	ID	チェック項目
4-1-2 証明書要求の発行	T-1	現地実証実験日本国認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。
	T-2	証明書要求に対応する相互認証証明書が現地香港チャイナ認証局から発行されたことを確認。
4-1-3 相互認証証明書の発行	T-1	現地香港チャイナ認証局から受け取った証明書要求により相互認証証明書を発行し、DER形式でファイル出力できることを確認。

	T-2	現地香港チャイナ認証局に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
4-1-4 相互認証証明書ペアの発行	T-1	現地実証実験日本国認証局が現地香港チャイナ認証局に対して発行した相互認証証明書と、現地香港チャイナ認証局から現地日本国認証局に対して発行された相互認証証明書（DER形式で受領）から相互認証証明書ペアが生成できることを確認。
	T-2	現地香港チャイナ認証局が発行した相互認証証明書が相互認証証明書ペアのforwardに格納されていることを確認。
	T-3	現地香港チャイナ認証局に対して発行した相互認証証明書が相互認証証明書ペアのreverseに格納されていることを確認。

(h) 現地香港チャイナ認証局から現地日本国認証局への証明書発行(Phase1:相互認証)

現地香港チャイナ認証局運用者により実施。

(i) 現地日本国認証局のローカルドメイン内の証明書発行(Phase2)

「表 10.7　現地実証実験日本国認証局のローカルドメイン内の証明書発行チェック項目」にチェック項目を示す。

表 10.7　現地実証実験日本国認証局のローカルドメイン内の証明書発行チェック項目

小項目	ID	チェック項目
4-1-1 自己署名証明書の発行	J-1	自己署名証明書の内容が、「相互接続インターフェース仕様」に従っていることを確認。
4-1-5 エンドエンティティ証明書の発行	J-1	エンドエンティティに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
4-1-6 証明書検証サーバ証明書の発行	J-1	証明書検証サーバの証明書要求により証明書を発行し、PKCS#7形式(自己署名証明書含む)でファイル出力できることを確認。
	J-2	証明書検証サーバに発行した証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。

(j) 現地日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書

発行(Phase2:相互認証)

「表 10.8　現地実証実験日本国認証局から現地チャイニーズ台北認証局(中華電信）への証明書発行チェック項目」にチェック項目を示す。

表 10.8　現地実証実験日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書発行チェック項目

小項目	ID	チェック項目
4-1-2 証明書要求の発行	T-1	現地実証実験日本国認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。
	T-2	証明書要求に対応する相互認証証明書が現地チャイニーズ台北認証局（中華電信）から発行されたことを確認。
4-1-3 相互認証証明書の発行	T-1	現地チャイニーズ台北認証局（中華電信）から受け取った証明書要求により相互認証証明書を発行し、DER形式でファイル出力できることを確認。
	T-2	現地チャイニーズ台北認証局（中華電信）に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
4-1-4 相互認証証明書ペアの発行	T-1	現地実証実験日本国認証局が現地チャイニーズ台北認証局（中華電信）に対して発行した相互認証証明書と、現地チャイニーズ台北認証局（中華電信）から現地日本国認証局に対して発行された相互認証証明書（DER形式で受領）から相互認証証明書ペアが生成できることを確認。
	T-2	現地チャイニーズ台北認証局（中華電信）が発行した相互認証証明書が相互認証証明書ペアのforwardに格納されていることを確認。
	T-3	現地チャイニーズ台北認証局（中華電信）に対して発行した相互認証証明書が相互認証証明書ペアのreverseに格納されていることを確認。

(k) 現地チャイニーズ台北認証局（中華電信）のローカルドメイン内の証明書発行（Phase2）

現地チャイニーズ台北認証局（中華電信）運用者により実施。

(l) 現地チャイニーズ台北認証局（中華電信）から現地日本国認証局への証明書発行（Phase2:相互認証）

現地チャイニーズ台北認証局（中華電信）運用者により実施。

(m) 現地日本国認証局から現地チャイニーズ台北認証局（TaiCA）への証明書発行(Phase2:相互認証)

「表 10.9　現地実証実験日本国認証局から現地チャイニーズ台北認証局（TaiCA）への証明書発行チェック項目」にチェック項目を示す。

表 10.9　現地実証実験日本国認証局から現地チャイニーズ台北認証局（TaiCA）への証明書発行チェック項目

小項目	ID	チェック項目
4-1-2 証明書要求の発行	T-1	現地実証実験日本国認証局が発行した証明書要求の内容が「相互接続インターフェース仕様」に従っていることを確認。
	T-2	証明書要求に対応する相互認証証明書が現地チャイニーズ台北認証局（TaiCA）から発行されたことを確認。
4-1-3 相互認証証明書の発行	T-1	現地チャイニーズ台北認証局（TaiCA）から受け取った証明書要求により相互認証証明書を発行し、DER形式でファイル出力できることを確認。
	T-2	現地チャイニーズ台北認証局（TaiCA）に発行した相互認証証明書の内容が「相互接続インターフェース仕様」に従っていることを確認。
4-1-4 相互認証証明書ペアの発行	T-1	現地実証実験日本国認証局が現地チャイニーズ台北認証局（TaiCA）に対して発行した相互認証証明書と、現地チャイニーズ台北認証局（TaiCA）から現地日本国認証局に対して発行された相互認証証明書（DER形式で受領）から相互認証証明書ペアが生成できることを確認。
	T-2	現地チャイニーズ台北認証局（TaiCA）が発行した相互認証証明書が相互認証証明書ペアのforwardに格納されていることを確認。
	T-3	現地チャイニーズ台北認証局（TaiCA）に対して発行した相互認証証明書が相互認証証明書ペアのreverseに格納されていることを確認。

(n) 現地チャイニーズ台北認証局（TaiCA）のローカルドメイン内の証明書発行（Phase2）

現地チャイニーズ台北認証局（TaiCA）運用者により実施。

(o) 現地チャイニーズ台北認証局（TaiCA）から現地日本国認証局への証明書発

行（Phase2：相互認証）
現地チャイニーズ台北認証局（TaiCA）運用者により実施。

(3) 実験結果
すべてのチェック項目の実施結果は「問題なし」である。

(4) 評価及び考察
本実験単位では、3 国／地域による現地実証実験環境において「相互接続インターフェース仕様」の証明書プロファイルに関して「表 10.1　現地実証実験環境における 2 種類の証明書プロファイル」に示す 2 つの異なった証明書プロファイルを用い証明書発行の実証実験を行った。

現地実証実験日本国認証局が本実験単位で発行した全ての証明書に対してチェックを行った結果、「相互接続インターフェース仕様」に従った正しい結果を得ることができた。しかし、現地実証実験日本国認証局が発行した証明書要求を現地香港チャイナ認証局が証明書要求データとして取り扱えないことが判明した。これは証明書要求の subject の OrganizationName 及び commonName に UTF8String が入った証明書要求を現地香港チャイナ認証局のシステムが取り扱えない実装であることが原因であった。subject に UTF8String を使用することは、「相互接続インターフェース仕様」に従っており正しい証明書要求データである。本実験においては香港チャイナ向けに subject に PrintableString を使用するように現地日本国認証局の設定を変更し、証明書要求を再発行し実験を継続した。これは UTF8String に対応した PKI コンポーネントが全世界的に完全には普及していない実状をものがたっており、今後国際間の相互認証を行う上で考慮すべき課題である。

また、現地香港チャイナ認証局と現地実証実験日本国認証局との間は、当初想定していたルート認証局同士ではなく香港チャイナの下位認証局と日本のルート認証局の間での相互認証関係及び相互承認関係の構築とした。「相互接続インターフェース仕様」に違反するものではなく技術的な問題はないが、認証局の運用ポリシの面からは考慮すべき問題を含んだ認証モデルである。ここで、認証ドメイン間の相互接続を行う場合の認証局の階層構造について検討すべき課題が摘出された。

実験の結果、上記課題以外の問題点は摘出されず、本実験単位においては「相互接続インターフェース仕様」に従った正しい結果を得ることができた。

本実験単位で摘出された 2 つの課題に関しては「16 全体考察（まとめ）」で考察する。

10.3　相互接続に係わる証明書失効

(1) 実験内容

現地実証実験環境において、「相互接続インターフェース仕様」に従って相互接続に係わる証明書の失効、CRL 及び ARL の発行を実施し、その結果得られた実験データを収集して分析する。

認証局が発行する失効情報の種類による実験単位の小項目を「表 10.10　現地実証実験環境における証明書失効実験単位小項目一覧」に示す。

表 10.10　現地実証実験環境における証明書失効実験単位小項目一覧

小項目番号	実験単位小項目
4-2-1	CRL の発行
4-2-2	ARL の発行

本実証実験で対象とする 3 国／地域の認証局が失効する証明書は以下のとおりである。

(a) 現地実証実験日本国認証局が失効する証明書

- 相互認証証明書
- エンドエンティティ証明書

(b) 現地チャイニーズ台北認証局（中華電信）が失効する証明書

- 相互認証証明書
- エンドエンティティ証明書

(c) 現地チャイニーズ台北認証局（TaiCA）が失効する証明書

- エンドエンティティ証明書

(d) 現地香港チャイナ認証局が失効する証明書

- エンドエンティティ証明書

(2) 実験方法

現地実証実験日本国認証局、現地チャイニーズ台北認証局（中華電信）、現地チャイニーズ台北認証局（TaiCA）及び現地香港チャイナ認証局が発行した相互接続に係わる証明書を失効する。

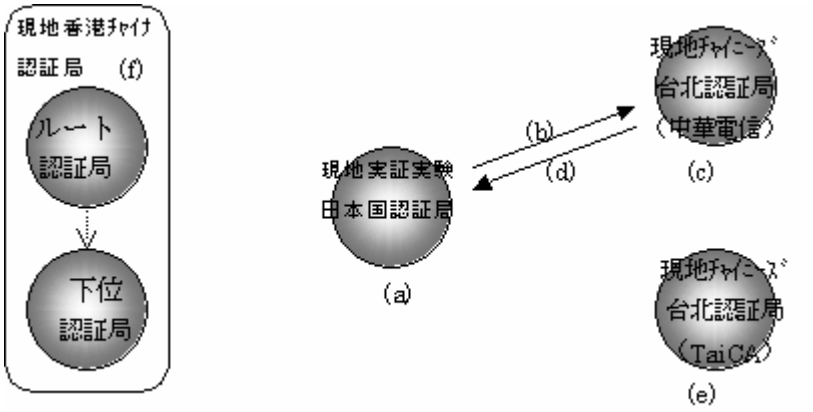


図 10.3　現地実証実験環境における証明書失効

各認証局のローカルドメイン内の証明書失効と、「図 10.3　現地実証実験環境における証明書失効」で実線で示した認証局間の証明書失効を実験対象とする。

(a) 現地実証実験日本国認証局内のローカルドメイン内の証明書失効

「表 10.11　現地実証実験日本国認証局内のローカルドメイン内の証明書失効チェック項目」にチェック項目を示す。

表 10.11　現地実証実験日本国認証局内のローカルドメイン内の証明書失効チェック項目

小項目	ID	チェック項目
4-2-1 CRLの発行	J-1	CRLが発行されることを確認。
	J-2	CRLの内容が規定に従っていることを確認。
	J-3	失効した相互認証証明書情報が、相互接続インターフェース仕様に従って格納されることを確認。

(b) 現地実証実験日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書失効

「表 10.12　現地実証実験日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書失効チェック項目」にチェック項目を示す。

表 10.12　現地実証実験日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書失効チェック項目

小項目	ID	チェック項目
4-2-2 ARLの発行	JT-1	ARLが発行されることを確認。

	JT-2	ARLの内容が規定に従っていることを確認。
	JT-3	失効した相互認証証明書情報が、相互接続インターフェース仕様に従って格納されることを確認。

(c) 現地チャイニーズ台北認証局（中華電信）のローカルドメイン内証明書失効
現地チャイニーズ台北認証局（中華電信）運用者により実施。

(d) 現地チャイニーズ台北認証局（中華電信）から現地実証実験日本国認証局への証明書の失効
現地チャイニーズ台北認証局（中華電信）運用者により実施。

(e) 現地チャイニーズ台北認証局（TaiCA）のローカルドメイン内証明書失効
現地チャイニーズ台北認証局（TaiCA）運用者により実施。

(f) 現地香港チャイナ認証局のローカルドメイン内証明書失効
現地香港チャイナ認証局運用者により実施。

(3) 実験結果
すべてのチェック項目の実施結果は「問題なし」である。

(4) 評価及び考察
現地実証実験日本国認証局及び現地実証実験チャイニーズ台北認証局（中華電信）の発行した CRL 及び ARL の内容を確認し、「相互接続インターフェース仕様」に従った証明書失効が正しく行われている事を確認した。
「相互接続インターフェース仕様」に従って証明書の失効を行うことで、正しい実験結果を得ることができた。このことは「相互接続インターフェース仕様」を認証局の証明書失効業務に適用することが可能であり、標準が有効性を持つことを示している。

10.4 相互接続に係わる証明書更新

(1) 実験内容
現地実証実験環境において、「相互接続インターフェース仕様」に従って相互接続に係わる証明書を更新し、その結果得られた実験データを収集して分析する。
実験単位の小項目を「表 10.13 証明書更新に関する実験単位小項目一覧」に示す。

表 10.13　証明書更新に関する実験単位小項目一覧

項目番号	実験単位の小項目
4-3-1	相互認証証明書の更新

各国認証局が更新する証明書は相互接続モデルにより異なる。本実証実験で対象とする 3 国／地域の認証局が更新する証明書は以下のとおりである。

(a) 現地実証実験日本国認証局が更新する証明書
- 相互認証証明書

(b) 現地チャイニーズ台北認証局（中華電信）が更新する証明書
- 相互認証証明書

(c) 現地チャイニーズ台北認証局（TaiCA）が更新する証明書
- なし（相互承認モデルとして運用）

(d) 現地香港チャイナ認証局が更新する証明書
- なし（相互承認モデルとして運用）

(2) 実験方法

現地実証実験日本国認証局、現地チャイニーズ台北認証局（中華電信）で、相互認証証明書を更新する。

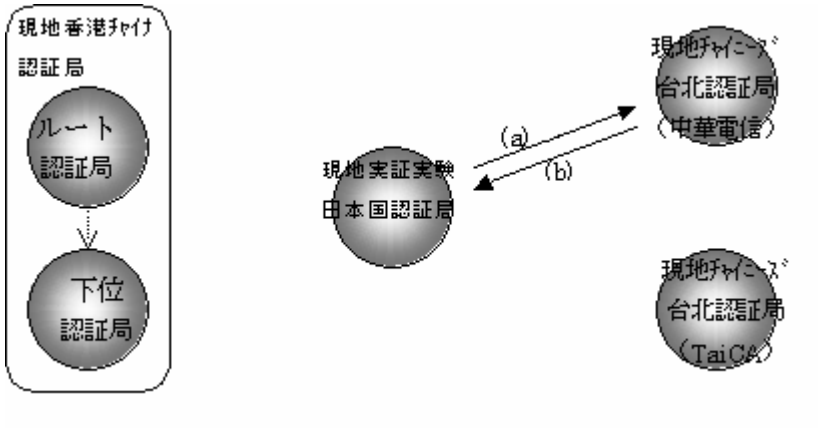


図 10.4　現地実証実験環境における証明書更新

(a) 現地実証実験日本国認証局から現地チャイニーズ台北認証局への証明書更新チェック項目

「表 10.14　現地日本国認証局から現地チャイニーズ台北認証局への証明書更新チェック項目」にチェック項目を示す。

表 10.14　現地日本国認証局から現地チャイニーズ台北認証局への証明書更新チェック項目

小項目	ID	チェック項目
4-3-1 相互認証証明書の更新	JT-1	相互認証証明書更新ができることを確認。
	JT-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(b) チャイニーズ台北認証局（中華電信）から日本国認証局への証明書更新チェック項目

現地チャイニーズ台北認証局（中華電信）運用者により実施。

(3) 実験結果

すべてのチェック項目の実施結果は「問題なし」である。

(4) 評価及び考察

「相互接続インターフェース仕様」に従って証明書の更新を行うことで、正しい実験結果を得ることができた。このことは「相互接続インターフェース仕様」を認証局の証明書更新業務に適用することが可能であり、標準が有効性を持つことを示している。

10.5　相互接続に係わる証明書再発行

(1) 実験内容

現地実証実験環境において、「相互接続インターフェース仕様」に従って相互接続に係わる証明書を再発行し、その結果得られた実験データを収集して分析する。

実験単位の小項目を「表 10.15　証明書再発行に関する実験単位小項目一覧」に示す。

表 10.15　証明書再発行に関する実験単位小項目一覧

項目番号	実験単位小項目
4-4-1	旧相互認証証明書の失効
4-4-2	新相互認証証明書の発行

各国認証局が再発行する証明書は相互接続モデルにより異なる。本実証実験で対象とする 3 国／地域の認証局が再発行する証明書は以下のとおりである。

(a) 現地実証実験日本国認証局が更新する証明書

- 相互認証証明書

(b) 現地チャイニーズ台北認証局（中華電信）が更新する証明書
- 相互認証証明書

(c) 現地チャイニーズ台北認証局（TaiCA）が更新する証明書
- なし（相互承認モデルとして運用）

(d) 現地香港チャイナ認証局が更新する証明書
- なし（相互承認モデルとして運用）

(2) 実験方法

現地実証実験日本国認証局、現地チャイニーズ台北認証局で相互認証証明書を再発行する。

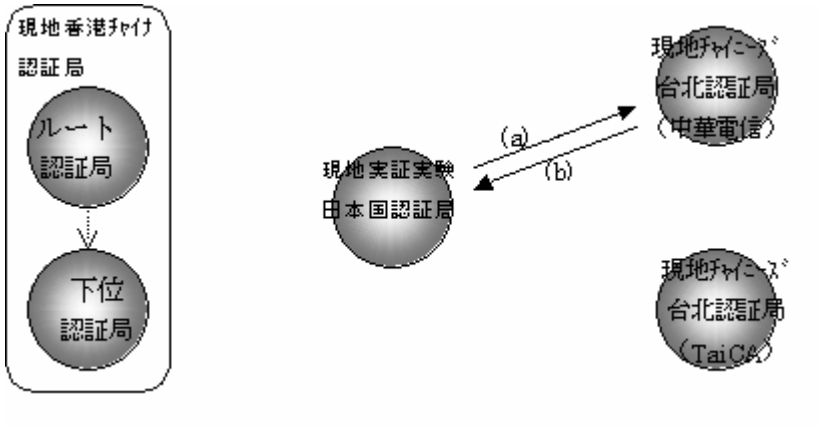


図 10.5　現地実証実験環境における証明書再発行

(a) 現地日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書再発行チェック項目

「表 10.16　現地実証実験日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書再発行チェック項目」にチェック項目を示す。

表 10.16　現地実証実験日本国認証局から現地チャイニーズ台北認証局（中華電信）への証明書再発行チェック項目

小項目	ID	チェック項目
4-4-1 旧相互認証証明書の失効	JT-1	旧相互認証証明書を失効できることを確認。
	JT-2	失効した相互認証証明書の情報がARLに格納されることを確認。

4-4-2 相互認証証明書の再発行	JT-1	相互認証証明書の再発行ができることを確認。
	JT-2	更新した相互認証証明書がディレクトリサーバのcrossCertificatePairのreverseに格納されることを確認。

(b) 現地チャイニーズ台北認証局から日本国認証局への証明書再発行チェック項目

・ 現地チャイニーズ台北認証局（中華電信）運用者により実施。

(3) 実験結果

すべてのチェック項目の実施結果は「問題なし」である。

(4) 評価及び考察

「相互接続インターフェース仕様」に従って証明書の再発行を行うことで、正しい実験結果を得ることができた。このことは「相互接続インターフェース仕様」を認証局の証明書再発行業務に適用することが可能であり、標準が有効性を持つことを示している。

11 現地環境における証明書検証の実証実験

11.1　概要

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する。証明書の検証には検証局を使用する。

(1) 実験データ

実験データとしては「表 11.1　実験データ」のものを収集する。

表 11.1　実験データ

No	実験データ	補足
1	現地チャイニーズ台北認証局（中華電信・TaiCA）及び現地香港チャイナ認証局の間で受け渡しされる証明書発行要求および証明書配布データ	「10 現地環境における認証局間の実証実験」で発行した証明書を使用する。
2	日本国検証局のログ情報による検証結果情報	ログを解析し、証明書検証結果の評価を行う。

(2) 実験内容

本実験で実施する検証内容と対応する実験単位中項目を「表 11.2　現地環境における証明書検証実験単位中項目一覧」に示す。

表 11.2　現地環境における証明書検証実験単位中項目一覧

実験単位中項目	検証項目	検証内容
5-1	認証パス検証	利用者が有効な証明書を受け取った場合の証明書検証を行う。
5-2	失効検証	利用者が失効されている証明書を受け取った場合の証明書検証を行う。
5-3	有効期限検証	利用者が有効期限の切れた証明書を受け取った場合の証明書検証を行う。
5-4	ポリシ検証	利用者が受け入れられないポリシがセットさ

		れた証明書を受け取った場合の証明書検証を行う。
5-5	認証パス構築検証	認証パス構築を完成することができない場合の証明書検証を行う。

(3) 実験方法

(a) 実験環境

現地実証実験環境に、現地実証実験日本国認証局、現地チャイニーズ台北（中華電信）・現地チャイニーズ台北（TaiCA）・現地香港チャイナ認証局を設置する。

本実験における各国/地域の認証局、日本国検証局、利用者、証明書検証の関係を表したものを「図 11.1　現地環境における証明書検証の実験環境」に示す。

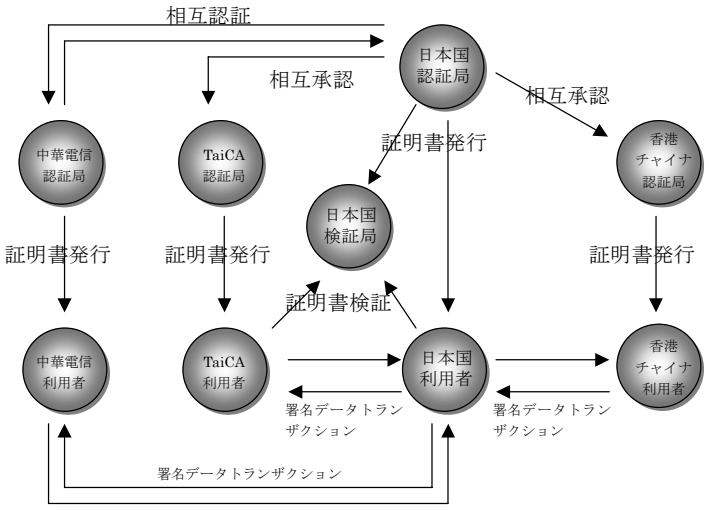


図 11.1　現地環境における証明書検証の実験環境

本実験では、日本ーチャイニーズ台北（TaiCA）間は相互承認であり、かつチャイニーズ台北（TaiCA）利用者は日本国認証局を信頼している事を想定した。これは、チャイニーズ台北（TaiCA）利用者が日本国検証局の VA 証明書を信頼することができることを意味する。従って、日本国検証局は日本国利用者からの証明書検証要求を受け付けるとともに、チャイニーズ台北（TaiCA）利用者からの証明書検証要求も受け付ける。つまり、日本国検証局は、日本およびチャイニーズ台北（TaiCA）の両ドメインで共用されている。

(b) 実験手順

本実験を実施するにあたっての実験手順を「表 11.3　実験手順」に示す。

表 11.3　実験手順

実験項目	担当		項番	内容
	日本	相手		
事前準備	○		1	相互認証証明書ペアがリポジトリに格納されていることを確認する
	○		2	自己署名証明書がリポジトリに格納されていることを確認する
	○		3	検証局の VA 証明書を発行する
	○		4	検証局に VA 証明書を格納する
	○		5	エンドエンティティ証明書を発行する
	○		6	エンドエンティティ証明書を渡す
		○	7	エンドエンティティ証明書を受け取る
		○	8	相互認証証明書ペアがリポジトリに格納されていることを確認する
		○	9	自己署名証明書がリポジトリに格納されていることを確認する
		○	10	エンドエンティティ証明書を発行する
		○	11	エンドエンティティ証明書を渡す
	○		12	エンドエンティティ証明書を受け取る
証明書検証	○		1	相手国/地域のエンドエンティティ証明書の検証を実施する
	○		2	日本国検証局のログを取得する
	○		3	日本国利用者端末のログを取得する
		○	4	日本のエンドエンティティ証明書の検証を実施する（チャイニーズ台北（TaiCA）のみ）
	○		5	日本国検証局のログを取得する（チャイニーズ台北（TaiCA）のみ）
結果評価	○		1	日本国検証局のログを解析し、証明書検証結果の評価を行う

11.2　認証パス検証

(1) 実験内容

「10 現地環境における認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた

実験データを収集・分析する。

本実験では特に、「利用者が有効な証明書を受け取ったときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 11.4　認証パス検証における実験項目」に示す。

表 11.4　認証パス検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
L-TCJ-JVA	日本国 利用者	チャイニーズ台北（中華電信）利用者	VAモデル	チャイニーズ台北（中華電信）利用者の証明書は有効
L-TTJ-JVA	日本国 利用者	チャイニーズ台北（TaiCA）利用者	VAモデル	チャイニーズ台北（TaiCA)利用者の証明書は有効
L-TTJ-OVA	チャイニーズ台北（TaiCA）利用者	日本国 利用者	VAモデル	日本国利用者の証明書は有効
L-HJ-JVA	日本国 利用者	香港チャイナ利用者	VAモデル	香港チャイナ利用者の証明書は有効

本実験における期待値を「表 11.5　認証パス検証における期待値」に示す。

表 11.5　認証パス検証における期待値

実験単位 中項目	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
5-1	認証パス検証	EE01	Valid	0	証明書は有効である

(2) 実験結果データ

本実験における検証結果を「表 11.6　認証パス検証における検証結果」に示す。

表 11.6　認証パス検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
L-TCJ-JVA	日本国利用者	チャイニーズ台北（中華電信）利用者	Valid	0	○

L-TTJ-JVA	日本国利用者	チャイニーズ台北（TaiCA）利用者	Valid	0	○
L-TTJ-OVA	チャイニーズ台北（TaiCA）利用者	日本国利用者	Valid	0	○
L-HJ-JVA	日本国利用者	香港チャイナ利用者	Valid	0	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 11.6　認証パス検証における検証結果」よりわかるとおり、全ての ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書が有効であることから、証明書の検証を行った結果は、有効である旨の結果が返らなければならない。

証明書検証ログを解析したところ、「0」という結果が出力された。これは正常に証明書検証が実施され、問題がなかったことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

11.3　失効検証

(1) 実験内容

「10 現地環境における認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に、「利用者が失効している証明書を受け取ったときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 11.7　失効検証における実験項目」に示す。

表 11.7　失効検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
L-TCJ-JVA	日本国利用者	チャイニーズ台北（中華電信）利用者	VAモデル	チャイニーズ台北（中華電信）利用者の証明書は失効されている

L-TTJ-JVA	日本国 利用者	チャイニーズ台北（TaiCA） 利用者	VAモデル	チャイニーズ台北（TaiCA)利用者の証明書は失効されている
L-TTJ-OVA	チャイニーズ台北（TaiCA） 利用者	日本国 利用者	VAモデル	日本国利用者の証明書は失効されている
L-HJ-JVA	日本国 利用者	香港チャイナ 利用者	VAモデル	香港チャイナ利用者の証明書は失効されている

本実験における期待値を「表 11.8　失効検証における期待値」に示す。

表 11.8　失効検証における期待値

中項目番号	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
5-2	失効検証	EE02	Invalid	203	証明書は失効されている

(2) 実験結果データ

本実験における検証結果を「表 11.9　失効検証における検証結果」に示す。

表 11.9　失効検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
L-TCJ-JVA	日本国利用者	チャイニーズ台北（中華電信）利用者	Invalid	203	○
L-TTJ-JVA	日本国利用者	チャイニーズ台北（TaiCA） 利用者	Invalid	203	○
L-TTJ-OVA	チャイニーズ台北（TaiCA） 利用者	日本国利用者	Invalid	203	○
L-HJ-JVA	日本国利用者	香港チャイナ 利用者	Invalid	203	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 11.9　失効検証における検証結果」よりわかるとおり、全の ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書が失効されていることから、証明書の検証を行った結果は、有効でない旨の結果が返らなければならない。

証明書検証ログを解析したところ、「203」という結果が出力された。これは認証パス中に失効されている証明書が含まれていたことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

11.4　有効期限検証

(1) 実験内容

「10 現地環境における認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に、「利用者が有効期限の切れた証明書を受け取ったときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 11.10　有効期限検証における実験項目」に示す。

表 11.10　有効期限検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
L-TCJ-JVA	日本国 利用者	チャイニーズ台北（中華電信）利用者	VAモデル	チャイニーズ台北（中華電信）利用者の証明書の有効期限が切れている
L-TTJ-JVA	日本国 利用者	チャイニーズ台北（TaiCA）利用者	VAモデル	チャイニーズ台北（TaiCA)利用者の証明書の有効期限が切れている
L-TTJ-OVA	チャイニーズ台北（TaiCA）利用者	日本国 利用者	VAモデル	日本国利用者の証明書の有効期限が切れている
L-HJ-JVA	日本国 利用者	香港チャイナ利用者	VAモデル	香港チャイナ利用者の証明書の有効期限が切

				れている

本実験における期待値を「表 11.11　有効期限検証における期待値」に示す。

表 11.11　有効期限検証における期待値

実験単位 中項目	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
5-3	有効期限検証	EE03	Invalid	203	証明書が有効期間の範囲外である

(2) 実験結果データ

本実験における検証結果を「表 11.12　有効期限検証における検証結果」に示す。

表 11.12　有効期限検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
L-TCJ-JVA	日本国利用者	チャイニーズ台北（中華電信）利用者	Invalid	203	○
L-TTJ-JVA	日本国利用者	チャイニーズ台北（TaiCA）利用者	Invalid	203	○
L-TTJ-OVA	チャイニーズ台北（TaiCA）利用者	日本国利用者	Invalid	203	○
L-HJ-JVA	日本国利用者	香港チャイナ利用者	Invalid	203	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 11.12　有効期限検証における検証結果」よりわかるとおり、全ての ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書の有効期限が切れていることから、証明書の検証を行った結果は、有効でない旨の結果が返らなければならない。

証明書検証ログを解析したところ、「203」という結果が出力された。これは認証パス中に失効されている証明書（有効期限が切れている証明書）が含まれていたことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

11.5　ポリシ検証

(1) 実験内容

「10 現地環境における認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に、「利用者が受け入れられないポリシがセットされた証明書を受け取ったときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 11.13　ポリシ検証における実験項目」に示す。

表 11.13　ポリシ検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
L-TCJ-JVA	日本国 利用者	チャイニーズ台北（中華電信）利用者	VAモデル	チャイニーズ台北（中華電信）利用者の証明書には受け入れられないポリシがセットされている
L-TTJ-JVA	日本国 利用者	チャイニーズ台北（TaiCA）利用者	VAモデル	チャイニーズ台北（TaiCA)利用者の証明書には受け入れられないポリシがセットされている
L-TTJ-JVA	チャイニーズ台北（TaiCA）利用者	日本国 利用者	VAモデル	日本国利用者の証明書には受け入れられないポリシがセットされている
L-HJ-JVA	日本国 利用者	香港チャイナ利用者	VAモデル	香港チャイナ利用者の証明書には受け入れられないポリシがセットされている

本実験における期待値を「表 11.14　ポリシ検証における期待値」に示す。

表 11.14　ポリシ検証における期待値

実験単位 中項目	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
5-4	ポリシ検証	EE04	Invalid	205	証明書がポリシ制約の条件を満たさない

(2) 実験結果データ

本実験における検証結果を「表 11.15　ポリシ検証における検証結果」に示す。

表 11.15　ポリシ検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
L-TCJ-JVA	日本国利用者	チャイニーズ台北（中華電信）利用者	Invalid	205	○
L-TTJ-JVA	日本国利用者	チャイニーズ台北（TaiCA）利用者	Invalid	205	○
L-TTJ-OVA	チャイニーズ台北（TaiCA）利用者	日本国利用者	Invalid	205	○
L-HJ-JVA	日本国利用者	香港チャイナ利用者	Invalid	205	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 11.15　ポリシ検証における検証結果」よりわかるとおり、全ての ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書のポリシが受け入れられないため、証明書の検証を行った結果は、有効でない旨の結果が返らなければならない。

証明書検証ログを解析したところ、「205」という結果が出力された。これは認証パス中に含まれる証明書のポリシが受け入れられないことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、「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ことがわかった。

11.6　認証パス構築検証

(1) 実験内容

「10 現地環境における認証局間の実証実験」で発行した証明書及びディレクトリサーバを使用し、検証局にて証明書の検証を行う。検証を行うたびに得られた実験データを収集・分析する。

本実験では特に、「認証パス構築を完成することができないときの証明書検証」についての検証を行うものとする。

本実験で実施する証明書検証を「表 11.16　認証パス構築検証における実験項目」に示す。

表 11.16　認証パス構築検証における実験項目

ID	検証者	検証対象者	モデル	確認内容
L-TCJ-JVA	日本国 利用者	チャイニーズ台北（中華電信）利用者	VAモデル	チャイニーズ台北（中華電信）利用者の証明書とトラストアンカ間で、認証パスの構築ができない
L-TTJ-JVA	日本国 利用者	チャイニーズ台北（TaiCA）利用者	VAモデル	チャイニーズ台北（TaiCA）利用者の証明書とトラストアンカ間で、認証パスの構築ができない
L-TTJ-JVA	チャイニーズ台北（TaiCA）利用者	日本国 利用者	VAモデル	日本国利用者の証明書とトラストアンカ間で、認証パスの構築ができない
L-HJ-JVA	日本国 利用者	香港チャイナ利用者	VAモデル	香港チャイナ利用者の証明書とトラストアンカ間で、認証パスの構築ができない

本実験における期待値を「表 11.17　認証パス構築検証における期待値」に示す。

表 11.17　認証パス構築検証における期待値

実験単位 中項目	検証項目	EE 証明書	期待値		意味
			結果	Return Code	
5-5	認証パス構築検証	EE05	Invalid	101	認証パスの構築ができない

(2) 実験結果データ

本実験における検証結果を「表 11.18　認証パス構築検証における検証結果」に示す。

表 11.18　認証パス構築検証における検証結果

ID	検証者	検証対象者	検証結果		期待値との比較
			結果	Return Code	
L-TCJ-JVA	日本国利用者	チャイニーズ台北（中華電信）利用者	Invalid	101	○
L-TTJ-JVA	日本国利用者	チャイニーズ台北（TaiCA）利用者	Invalid	101	○
L-TTJ-OVA	チャイニーズ台北（TaiCA）利用者	日本国利用者	Invalid	101	○
L-HJ-JVA	日本国利用者	香港チャイナ利用者	Invalid	101	○

凡例　「期待値との比較」○：期待値と同じ。×：期待値と異なる。

「表 11.18　認証パス構築検証における検証結果」よりわかるとおり、全ての ID において期待値通りの結果を得た。

(3) 評価及び考察

本実験では、検証する対象の証明書とトラストアンカ間で認証パスの構築ができないため、証明書の検証を行った結果は有効でない旨の結果が返らなければならない。

証明書検証ログを解析したところ、「101」という結果が出力された。これは認証パスの構築ができなかったことを意味する。従って、実験前に予測していた通りの結果を得ることができたといえる。

「相互接続インターフェース仕様」に則った検証が正しくできたことにより、

「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ことがわかった。

12 現地環境における国際間調達の実証実験

12.1　概要

「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する。

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う。

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」の有効性を検証する。

(1) 実験方法

業務シナリオに従った「表 12.1　現地実証実験環境における国際間調達の実験手順」に示す手順を実施する。

表 12.1　現地実証実験環境における国際間調達の実験手順

手順番号	手順
1	エンドエンティティ証明書を発行する。
	エンドエンティティ証明書を格納する。
2	失効用エンドエンティティ証明書のCRLを発行する。
3	認証局自己署名証明書を格納する。
4	利用者登録を行う。
5	見積依頼書を作成する。
	見積依頼書に署名を付与し、結果を確認する。
	結果表示画面のハードコピーを採取する。
	見積依頼書をサーバへアップロードする。
6	見積依頼書を参照する。
	見積依頼書の署名を検証し、結果を確認する。
	結果表示画面のハードコピーを採取する。
7	見積回答書を作成する。
	見積回答書に署名を付与し、結果を確認する。
	結果表示画面のハードコピーを採取する。
	見積回答書をサーバへアップロードする。

8	見積回答書を参照する。
	見積回答書の署名を検証し、結果を確認する。
	結果表示画面のハードコピーを採取する。

12.2　正常系検証

(1) 目的

本実験単位は、売り手と買い手の双方が正常証明書を使用して「相互接続インターフェース仕様」の有効性の検証を目的とする。

(2) 実験内容

各国認証局より発行された正常証明書を売り手と買い手が使用する。売り手側利用者と買い手側利用者は業務シナリオに沿ってチェックリストに従い署名付与及び署名結果を確認する。

使用するエンドエンティティ証明書を以下の「表 12.2　使用するエンドエンティティ証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 12.2　使用するエンドエンティティ証明書

	証明書名	発行元	種別
1	EE01jp	現地実証実験日本国認証局	正常証明書
2	EE01cht	現地チャイニーズ台北認証局（中華電信）	正常証明書
3	EE01taica	現地チャイニーズ台北認証局（TaiCA）	正常証明書
4	EE01hk	現地香港チャイナ認証局	正常証明書

使用する自己署名証明書を以下の「表 12.3　使用する自己署名証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 12.3　使用する自己署名証明書

	証明書名	発行元
1	CAjp	現地実証実験日本国認証局
2	CAcht	現地チャイニーズ台北認証局（中華電信）
3	CAtaica	現地チャイニーズ台北認証局（TaiCA）
4	CAhk	現地香港チャイナ認証局

(3) 実験結果データ

署名付与及び署名検証の結果が表示される画面のコピーとアプリケーションのログから実験データを取得した。その実験データを分析した結果得られた、本実

験単位における実験結果を以下の「表 12.4　正常系検証実験結果データ」に示す。

表 12.4　正常系検証実験結果データ

No	買い手	売り手	期待値	結果	判定
1	日本・正常証明書	チャイニーズ台北（中華電信）・正常証明書	○	○	○
2	チャイニーズ台北（中華電信）・正常証明書	日本・正常証明書	○	○	○
3	日本・正常証明書	チャイニーズ台北(TaiCA)・正常証明書	○	○	○
4	チャイニーズ台北(TaiCA)・正常証明書	日本・正常証明書	○	○	○
5	日本・正常証明書	香港チャイナ・正常証明書	○	○	○
6	香港チャイナ・正常証明書	日本・正常証明書	○	○	○

(4) 評価・考察

現地環境における国際間調達の実証実験を一通り成功させることができたが、実験を始める前に下記のとおりの幾多の問題点を解決しなければならなかった。

現地チャイニーズ台北認証局（中華電信）発行の証明書における CRL Number が 7 オクテットあり、当初は 4 オクテットまでしか対応していなかった日本側のアプリケーションでは検証できないことがわかったので、RFC3280 に従い日本側のアプリケーションにおいて、20 オクテットまでの CRL Number に対応させるよう改造した。RFC3280 によれば、CRL Number は 20 オクテットまで対応しなければならないが、日本側のアプリが準拠している GPKI ではこの CRl Number に関する規定が存在しない。チャイニーズ台北（中華電信）との実験で RFC と GPKI の違いの一部が明らかになった。

また、現地チャイニーズ台北（中華電信）証明書を検証するにあたり、証明書中の LDAPURI のフィールドにおける「,」（カンマ）の解釈に関する問題が発覚し、日本側アプリケーションを修正することにより解決させ、実験を開始させることができた。現地チャイニーズ台北認証局（中華電信）の証明書では発行元の正式名称が「Chunghwa Telecom Co.,Ltd.」である。プログラム上「,」は予約語であり、「,」の持つ特定の意味を解釈させないため、「,」をエスケープさせる必要がある。よって、証明書内の表記上では次のような表記となる。

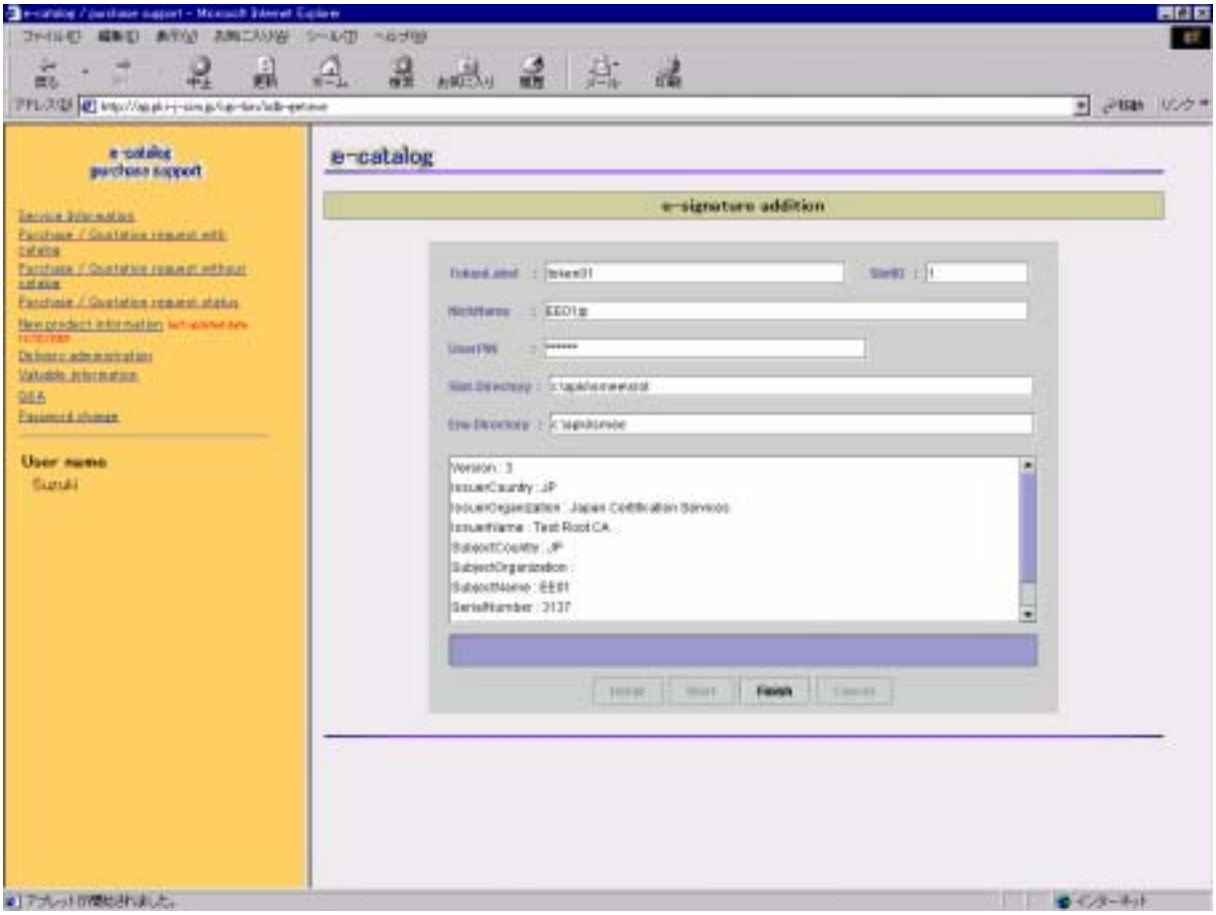
「Chunghwa%20Telecom%20Co.%5C,%20Ltd.」

しかし、日本側アプリケーションで「%5C」を現地チャイニーズ台北認証局（中

華電信）が意図したように解釈せず、検証エラーとなることがわかった。したがって、日本側で改造を施すことにより実験を成功させることができた。

日本のアプリケーションにおいては日本の GPKI の仕様に従い、CRL の iDP と証明書内の cRLDP の比較を行い完全一致していなければ証明書検証エラーを起こすようになっている。しかし、香港チャイナは iDP と cRLDP の一致はセキュリティ要件上厳しすぎると考えており、現地香港チャイナ認証局発行の証明書では両者は完全に一致しない。よって、香港チャイナとの実験に際し、日本側のアプリケーションを iDP と cRLDP の比較チェックを行わないよう改造を施すことにより実験を成功させることができた。

シミュレーションセンタでの実験と同様に、すべてのケースにおいて署名付与後は正しく署名付与ができたことを示す以下の「図 12.1　有効性検証　(例)チャイニーズ台北・香港チャイナ(正常系)」のようなメッセージを得た。



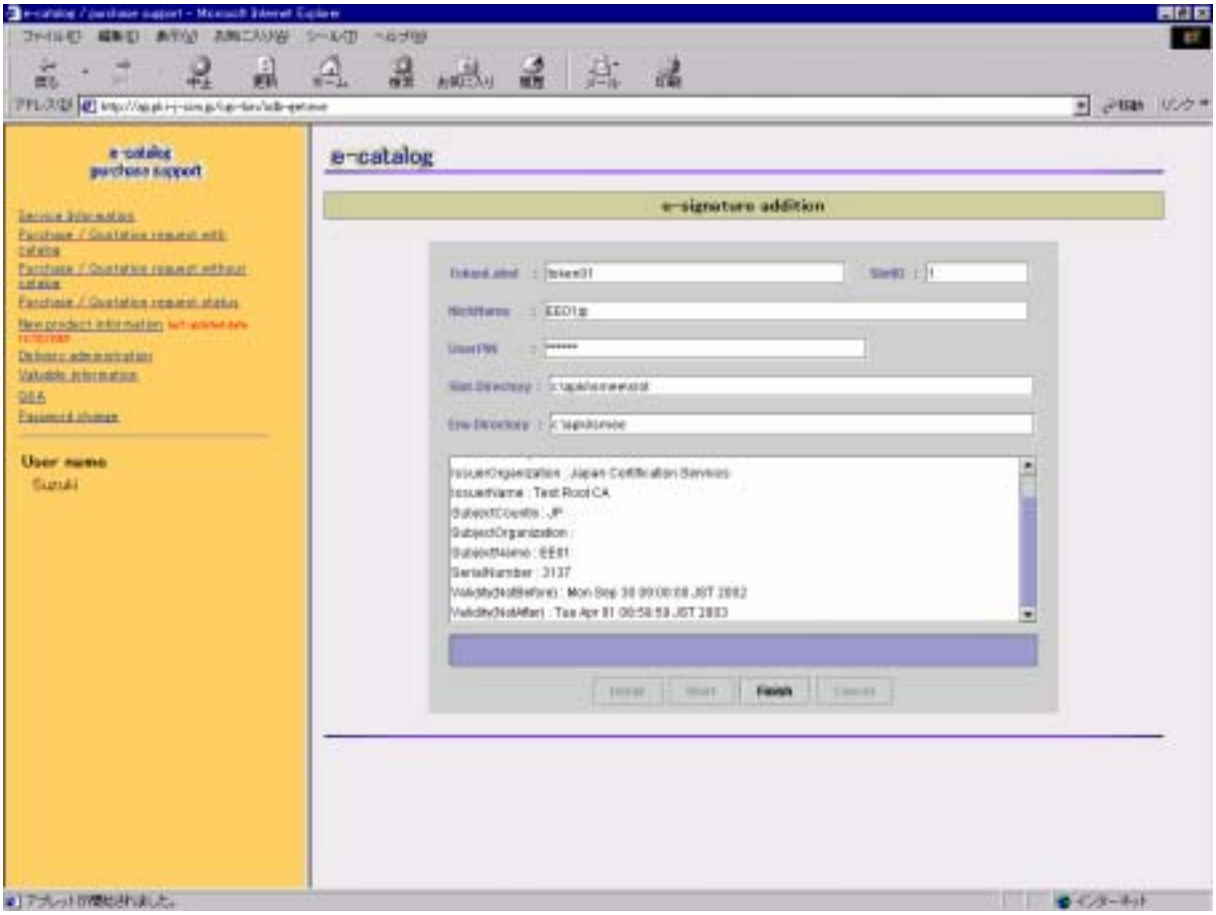


図 12.1　有効性検証　(例)チャイニーズ台北・香港チャイナ(正常系)

また、すべてのケースにおいて、署名を検証した後には正しく証明書を検証できたことを伝える、以下の「図 12.2　有効性検証（例）日本・チャイニーズ台北（正常系)」のような結果画面が表示された。

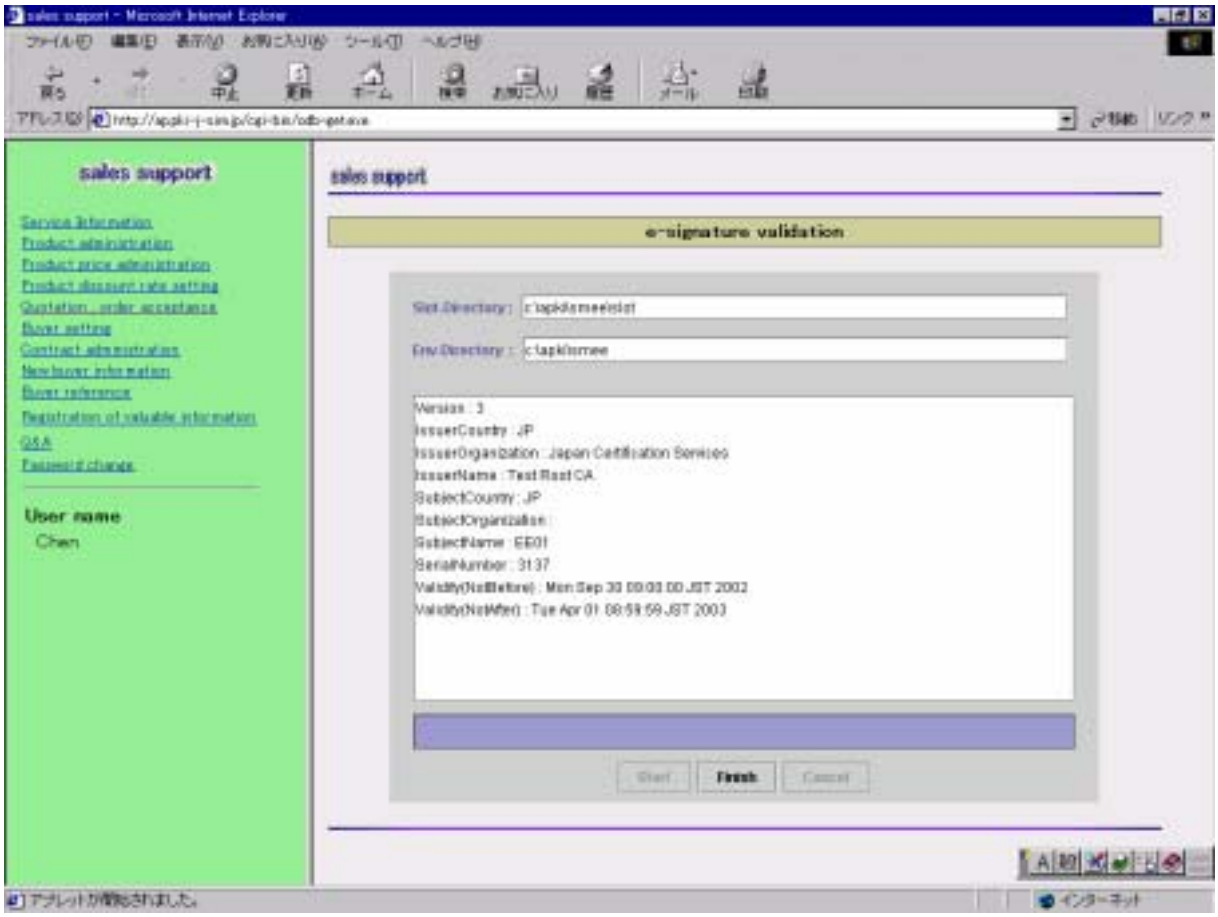


図 12.2　有効性検証（例）日本・チャイニーズ台北（正常系）

以上により、CRL Number の問題、LDAPURI 中のカンマの扱いに関する問題、iDP と cRLDP の一致問題が存在するが、「相互接続インターフェース仕様」は有効であると考えられる。

12.3　失効系 1 検証

(1) 目的

本実験単位は、売り手が失効した証明書そして買い手が正常の証明書を使用して PKI コンポーネント間接続に関する標準の有効性の検証を目的とする。

(2) 実験内容

各国認証局より発行された失効証明書を売り手が使用し、正常証明書を買い手が使用する。売り手側利用者と買い手側利用者は業務シナリオに沿ってチェックリストに従い署名付与及び署名結果を確認する。

使用するエンドエンティティ証明書を以下の「表 12.5　使用するエンドエンティティ証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 12.5　使用するエンドエンティティ証明書

	証明書名	発行元	種別
1	EE01jp	日本国認証局	正常証明書
2	EE02jp	日本国認証局	失効証明書
3	EE01cht	チャイニーズ台北認証局（中華電信）	正常証明書
4	EE02cht	チャイニーズ台北認証局（中華電信）	失効証明書
5	EE01taica	チャイニーズ台北認証局(TaiCA)	正常証明書
6	EE02taica	チャイニーズ台北認証局(TaiCA)	失効証明書
7	EE01hk	香港チャイナ認証局	正常証明書
8	EE02hk	香港チャイナ認証局	失効証明書

使用する自己署名証明書は以下を「表 12.6　使用する自己署名証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 12.6　使用する自己署名証明書

	証明書名	発行元
1	CAjp	日本国認証局
2	CAcht	チャイニーズ台北認証局（中華電信）
3	CAtaica	現地チャイニーズ台北認証局（TaiCA）
4	CAhk	香港チャイナ認証局

(3) 実験結果データ

本実験単位における実験結果を以下の「表 12.7　失効系 1 検証実験結果データ」に示す。

表 12.7　失効系 1 検証実験結果データ

No	買い手	売り手	期待値	結果	判定
1	日本・正常証明書	チャイニーズ台北（中華電信）・失効証明書	×	×	○
2	チャイニーズ台北（中華電信）・正常証明書	日本・失効証明書	×	×	○
3	日本・正常証明書	チャイニーズ台北(TaiCA)・失効証明書	×	×	○

4	チャイニーズ台北(TaiCA)・正常証明書	日本・失効証明書	×	×	○
5	日本・正常証明書	香港チャイナ・失効証明書	×	×	○
6	香港チャイナ・正常証明書	日本・失効証明書	×	×	○

以上の「表 12.7　失効系 1 検証実験結果データ」で見られるように、すべてのケースにおいて期待値どおりに実験が終了した。

(4) 評価・考察

日本・チャイニーズ台北間及び日本・香港チャイナ間において、署名付与時に失効した証明書を検知した時点で、以下の「図 12.3　署名付与　(例)日本・チャイニーズ台北（失効系 1)」のようなエラーメッセージを返した。証明書の失効を正しく検証した。

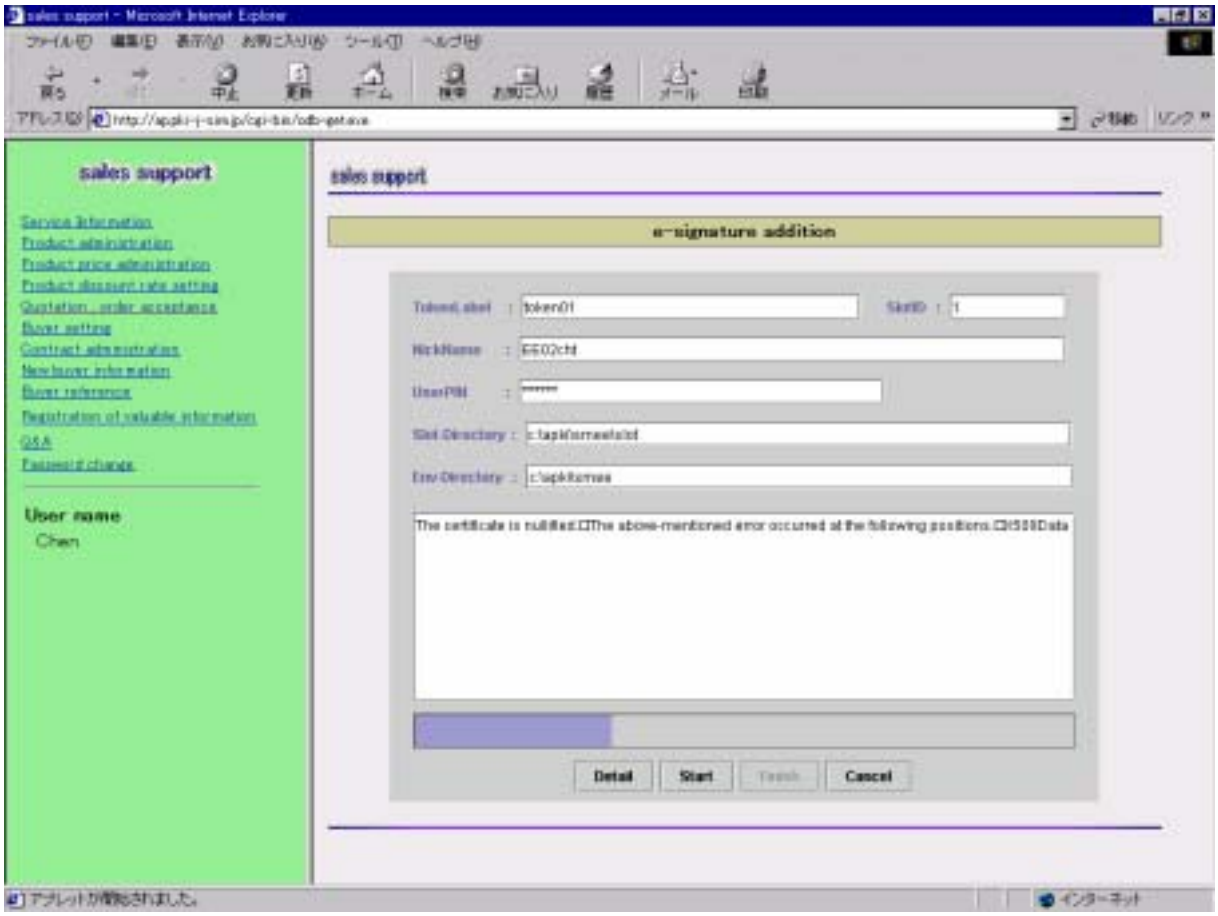


図 12.3　署名付与　(例)日本・チャイニーズ台北（失効系1)

「12.2　(4) 評価・考察」で述べられているとおり、実験前に CRL Number の問題・LDAPURI 中のカンマの扱いに関する問題・iDP と cRLDP の一致問題を解決するために日本側のアプリケーションに改造を施すことで実験を成功させ

ることができた。

これら問題を解決できれば、「相互接続インターフェース仕様」は有効であると考えられる。

12.4　失効系 2 検証

(1) 目的

本実験単位は、買い手が失効証明書そして売り手が正常証明書を使用して「相互接続インターフェース仕様」の有効性の検証を目的とする。

(2) 実験内容

各国認証局より発行された失効証明書を買い手が使用し、正常証明書を売り手が使用する。売り手側利用者と買い手側利用者は業務シナリオに沿ってチェックリストに従い署名付与及び署名結果を確認する。

使用するエンドエンティティ証明書を以下の「表 12.8　使用するエンドエンティティ証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 12.8　使用するエンドエンティティ証明書

	証明書名	発行元	種別
1	EE01jp	日本国認証局	正常証明書
2	EE02jp	日本国認証局	失効証明書
3	EE01cht	チャイニーズ台北認証局（中華電信）	正常証明書
4	EE02cht	チャイニーズ台北認証局（中華電信）	失効証明書
5	EE01taica	チャイニーズ台北認証局(TaiCA)	正常証明書
6	EE02taica	チャイニーズ台北認証局(TaiCA)	失効証明書
7	EE01hk	香港チャイナ認証局	正常証明書
8	EE02hk	香港チャイナ認証局	失効証明書

使用する自己署名証明書は以下を「表 12.9　使用する自己署名証明書」に示す。各証明書は、証明書発行元のリポジトリに格納される。

表 12.9　使用する自己署名証明書

	証明書名	発行元
1	CAjp	現地実証実験日本国認証局
2	CAcht	現地チャイニーズ台北認証局（中華電信）
3	CAtaica	現地チャイニーズ台北認証局（TaiCA）
4	CAhk	現地香港チャイナ認証局

(3) 実験結果データ

署名付与及び署名検証の結果が表示される画面のコピーとアプリケーションのログから実験データを取得した。その実験データを分析した結果得られた、本実験単位における実験結果は以下の「表 12.10　失効系 2 検証実験結果データ」のようにまとめられる。

表 12.10　失効系 2 検証実験結果データ

No	買い手	売り手	期待値	結果	判定
1	日本・失効証明書	チャイニーズ台北（中華電信）・正常証明書	×	×	○
2	チャイニーズ台北（中華電信）・失効証明書	日本・正常証明書	×	×	○
3	日本・失効証明書	チャイニーズ台北(TaiCA)・正常証明書	×	×	○
4	チャイニーズ台北(TaiCA)・失効証明書	日本・正常証明書	×	×	○
5	日本・失効証明書	香港チャイナ・正常証明書	×	×	○
6	香港チャイナ・失効証明書	日本・正常証明書	×	×	○

以上の「表 12.10　失効系 2 検証実験結果データ」に見られるとおり、すべてのケースにおいて期待値どおりに実験が終了した。

(4) 評価・考察

失効系 2 検証において、日本とチャイニーズ台北の間と日本と香港チャイナの間では、失効した証明書を使用して署名付与を行おうとすると、証明書の失効を正しく検知した。

「12.2　(4) 評価・考察」で述べられているとおり、実験前に CRL Number の問題、LDAPURI 中のカンマの扱いに関する問題、iDP と cRLDP の一致問題を解決するために日本側のアプリケーションに改造を施すことで実験を成功させ

ることができた。
　これら問題を解決できれば、「相互接続インターフェース仕様」は有効であると考えられる。

13 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

13.1　概要

本実験では、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する。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うことを目的とする。

本実験の対象国を「表 13.1　実験対象国/地域一覧」に示す。

表 13.1　実験対象国/地域一覧

No	対象国/地域	テスト範囲
1	日本	基本モデル、相互接続モデル(Strict Hierarcy、Cross Certification、Cross Recognition)、 サービスモデル、失効モデル
2	韓国	相互接続モデルのCross Certificationモデルのみ
3	チャイニーズ台北	相互接続モデルのCross Certificationモデルのみ

本実験の実施環境を「図 13.1　テスト実施環境」に示す。

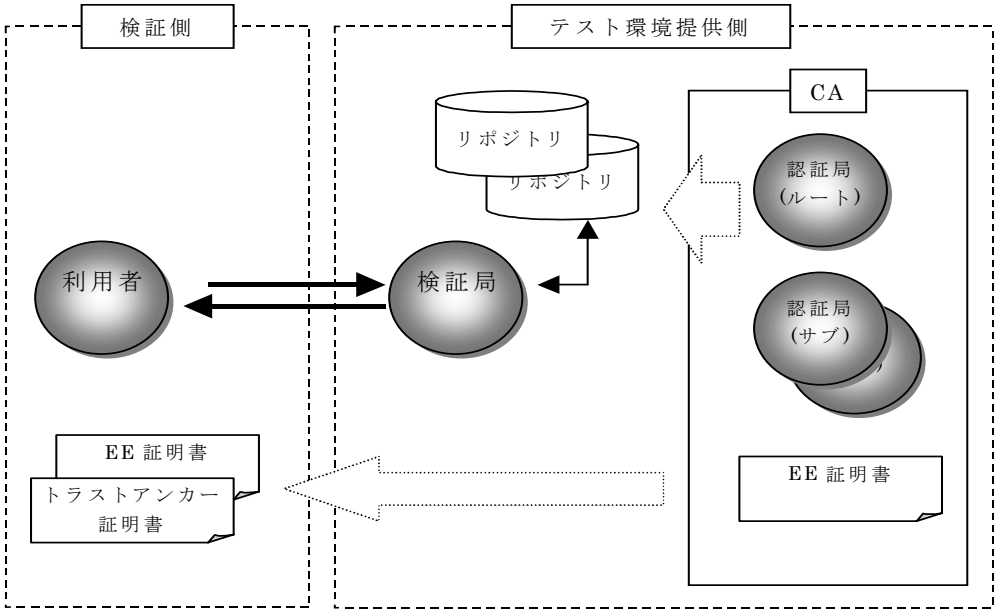


図 13.1　テスト実施環境

実験で作成した日本環境における CA 構造を「図 13.2　日本環境 CA 構造」に示す。

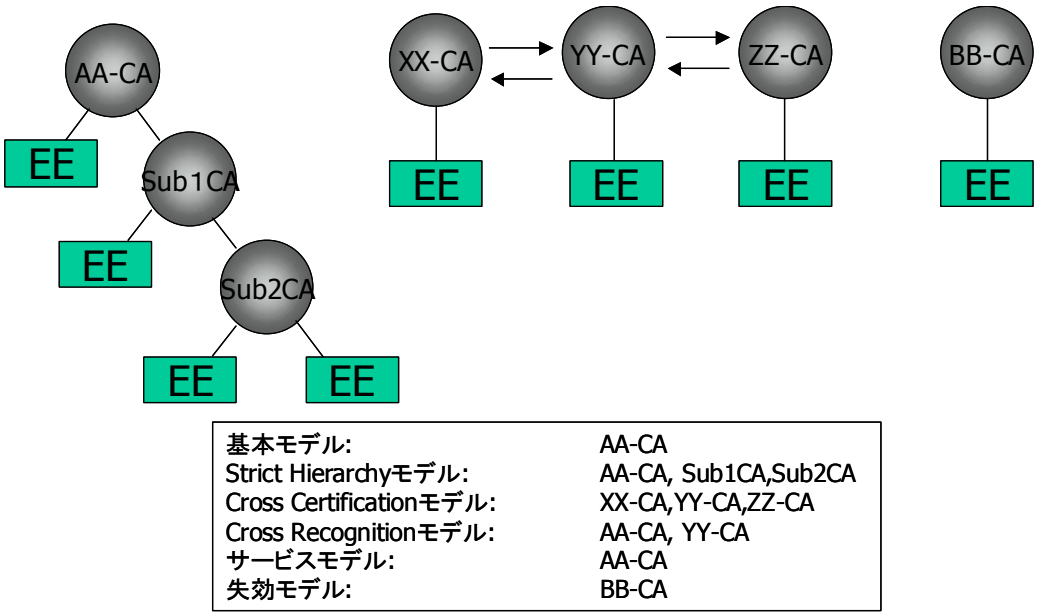


図 13.2　日本環境 CA 構造

韓国とチャイニーズ台北とで構築したテスト環境について「図 13.3　韓国/チャイニーズ台北とのテスト環境」に示す。

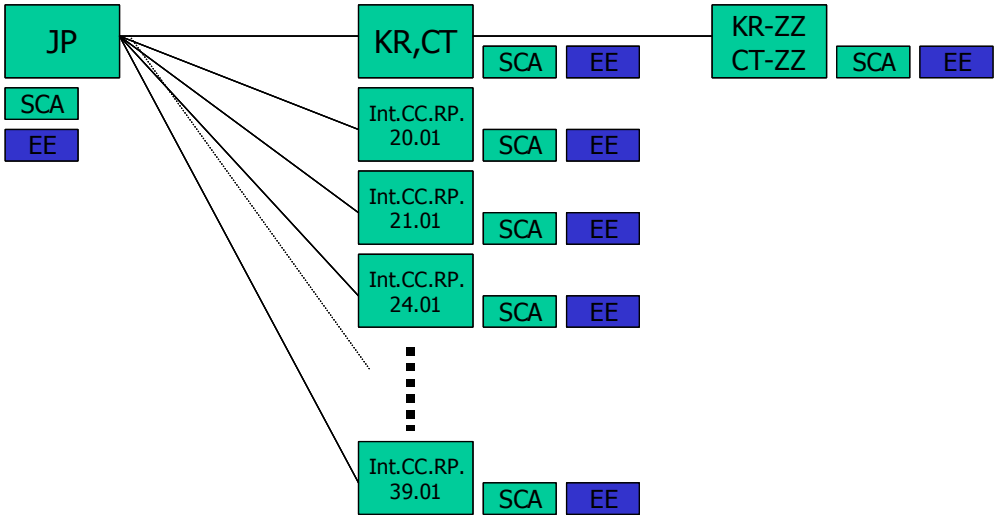


図 13.3　韓国/チャイニーズ台北とのテスト環境

本実験では、パス検証テストガイドラインの利用者に対して、ガイドラインの網羅性、テストパターンに関する妥当性、及びテスト期待値の適確さについてヒアリ

ングを行った。ヒアリング対象者を「表 13.2　ヒアリング対象者」に示す。

表 13.2　ヒアリング対象者

No	国/地域	所属
1	日本国	日本認証サービス株式会社
2	日本国	株式会社日立製作所
3	韓国	Korea Information Security Agency
4	チャイニーズ台北	Chunghwa Telecom Co., Ltd. (中華電信)
5	チャイニーズ台北	TAIWAN-CA.COM.,INC (TaiCA)

13.2　基本モデル

(1) 実験内容

現地日本国認証局において、本実験に必要となる証明書の発行を行い、その証明書を用いて証明書の検証を行う。検証を行うたびに得られた実験データを収集、分析する。検証内容の詳細については、パス検証テストガイドラインを参照のこと。

(2) 実験結果

本実験における検証結果を「表 13.3　基本モデル　テスト結果」に示す。

表 13.3　基本モデル　テスト結果

No	テスト項目	テスト期待値	検証結果	期待値の比較判定
1	Base.RP.07.01	成功	成功	○
2	Base.RP.08.01	失敗	失敗	○
3	Base.RP.09.01	失敗	成功	×
4	Base.RP.10.01	失敗	失敗	○
5	Base.RP.11.01	失敗	失敗	○
6	Base.RP.12.01	失敗	失敗	○
7	Base.RP.13.01	失敗	失敗	○
8	Base.RP.14.01	失敗	失敗	○
9	Base.RP.15.01	失敗	失敗	○
10	Base.RP.16.01	失敗	失敗	○
11	Base.RP.17.01	失敗	失敗	○
12	Base.RP.18.01	失敗	失敗	○

13	Base.RP.19.01	失敗	失敗	○
14	Base.RP.20.01	失敗	失敗	○

(3) ヒアリング結果

ヒアリング結果を、「表 13.4　基本モデル　ヒアリング結果」に示す。

表 13.4　基本モデル　ヒアリング結果

ヒアリング項目	ヒアリング結果	備考
ガイドラインの網羅性	・　十分に網羅性がある	-
テストパターンに関する妥当性	・　十分に妥当性がある	-
テスト期待値の的確さ	1) テスト項目「Base.RP.09.01」のテスト期待値に関しては、検証成功で良いのではないか。	1) Base.RP.09.01

(4) 考察

「Base.RP.09.01」以外のテスト項目では、パス検証テストガイドラインのテスト期待値と検証結果が一致した。また、ヒアリングにおいても課題が挙げられなかった。よって、パス検証テストガイドラインの有効性が確認できた。

一方、「Base.RP.09.01」のテスト項目では、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。また、ヒアリングから、「Base.RP.09.01」のテスト期待値を再確認するべきであるとの指摘が得られた。テスト結果とヒアリング結果から、「Base.RP.09.01」については、パス検証テストガイドラインのテスト期待値の再検討が必要であることが確認された。本件は、課題項目として、パス検証テストガイドライン作成作業へフィードバックを行った。

13.3　相互接続モデル

相互接続モデルとして次の 3 つのモデルについて、パス検証テストガイドラインに従って実験を行った。

- Strict Hierarchy モデル
- Cross Certification モデル
- Cross Recognition モデル

13.3.1 Strict Hierarchy モデル

(1) 実験内容

現地日本国認証局において、本実験に必要となる証明書の発行を行い、その証明書を用いて証明書の検証を行う。検証を行うたびに得られた実験データを収集、分析する。検証内容の詳細については、パス検証テストガイドラインを参照のこと。

(2) 実験結果

本実験における検証結果を「表 13.5　Strict Hierarchy モデル　テスト結果」に示す。

表 13.5　Strict Hierarchy モデル　テスト結果

No	テスト項目	テスト期待値	検証結果	期待値の比較判定
1	Int.SH.RP.08.01	成功	成功	○
2	Int.SH.RP.09.01	失敗	失敗	○
3	Int.SH.RP.10.01	失敗	失敗	○
4	Int.SH.RP.11.01	失敗	失敗	○
5	Int.SH.RP.12.01	失敗	失敗	○
6	Int.SH.RP.13.01	失敗	成功	×
7	Int.SH.RP.14.01	成功	成功	○
8	Int.SH.RP.14.02	失敗	失敗	○
9	Int.SH.RP.15.01	失敗	成功	×
10	Int.SH.RP.16.01	失敗	失敗	○
11	Int.SH.RP.17.01	失敗	成功	×
12	Int.SH.RP.18.01	失敗	失敗	○
13	Int.SH.RP.19.01	成功	成功	○
14	Int.SH.RP.19.02	失敗	失敗	○
15	Int.SH.RP.20.01	成功	成功	○
16	Int.SH.RP.20.02	失敗	失敗	○
17	Int.SH.RP.21.01	成功	成功	○
18	Int.SH.RP.21.02	失敗	失敗	○
19	Int.SH.RP.22.01	失敗	失敗	○
20	Int.SH.RP.23.01	失敗	失敗	○

(3) ヒアリング結果

ヒアリング結果を、「表 13.6　Strict Hierarchy モデル　ヒアリング結果」に

示す。

表 13.6　Strict Hierarchy モデル　ヒアリング結果

ヒアリング項目	ヒアリング結果	備考
ガイドラインの網羅性	・　十分に網羅性がある	-
テストパターンに関する妥当性	・　十分に妥当性がある	-
テスト期待値の的確さ	1）criticality の検証を署名検証者が行う必要が無いのではないか。本テスト項目のテスト期待値は検証失敗であるが、検証成功でも良いのではないか。	1）Int.SH.RP.13.01 Int.SH.RP.17.01

(4) 考察

「Int.SH.RP.13.01」、「Int.SH.RP.15.01」及び「Int.SH.RP.17.01」以外のテスト項目では、パス検証テストガイドラインのテスト期待値と検証結果が一致した。また、ヒアリングにおいて課題が挙げられなかった。よって、パス検証テストガイドラインの有効性が確認できた。

「Int.SH.RP.13.01」及び「Int.SH.RP.17.01」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。また、ヒアリングから、「Int.SH.RP.13.01」及び「Int.SH.RP.17.01」のテスト期待値を再検討するべきであるとの指摘が得られた。critical フラグは署名検証者が検証すべき X.509 証明書内の領域を示すインジケータであり、critical フラグ自身を検証する必要は必ずしもないといえる。本件は、課題項目として、パス検証テストガイドライン作成作業へフィードバックを行った。

「Int.SH.RP.15.01」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。これは、今回実験に使用した検証局が keyUsage が無い場合は、この領域を検証しないためである。ただし、検証局は、PKI ドメイン内における keyUsage の使用方法等により、keyUsage の検証方法をカスタマイズできる。このテスト項目におけるパス検証テストガイドラインのテスト期待値と検証結果の不一致は、検証局の実装方式によるものであり、パス検証テストガイドラインの有効性を損なわせるものではない。

「Int.SH.RP.13.01」及び「Int.SH.RP.17.01」については、テスト結果とヒアリング結果からパス検証テストガイドラインのテスト期待値の再検討が必要であることが確認された。本件は、課題項目として、パス検証テストガイドライン作成作業へフィードバックを行った。

13.3.2 Cross Certification モデル

(1) 実験内容

現地実証実験環境の各国/地域の認証局において、本実験に必要となる証明書の発行を行い、その証明書を用いて証明書の検証を行う。検証を行うたびに得られた実験データを収集、分析する。検証内容の詳細については、パス検証テストガイドラインを参照のこと。

(2) 実験結果

日本国内における異なる 2 つの認証局間の Cross Certification モデルの実証実験による検証結果を「表 13.7　Cross Certification モデル(日本国<->日本国)　テスト結果」に示す。

表 13.7　Cross Certification モデル(日本国<->日本国)　テスト結果

No	テスト項目	テスト期待値	日本国現地実験	
			検証結果	期待値の比較判定
1	Int.CC.RP.19.01	成功	成功	○
2	Int.CC.RP.20.01	失敗	失敗	○
3	Int.CC.RP.21.01	失敗	失敗	○
4	Int.CC.RP.22.01	失敗	失敗	○
5	Int.CC.RP.23.01	成功	成功	○
6	Int.CC.RP.23.02	失敗	失敗	○
7	Int.CC.RP.24.01	成功	成功	○
8	Int.CC.RP.24.02	失敗	失敗	○
9	Int.CC.RP.25.01	成功	成功	○
10	Int.CC.RP.25.02	失敗	失敗	○
11	Int.CC.RP.26.01	失敗	失敗	○
12	Int.CC.RP.27.01	失敗	失敗	○
13	Int.CC.RP.28.01	失敗	成功	×
14	Int.CC.RP.29.01	成功	成功	○
15	Int.CC.RP.29.02	失敗	失敗	○
16	Int.CC.RP.30.01	失敗	成功	×
17	Int.CC.RP.31.01	失敗	失敗	○
18	Int.CC.RP.32.01	失敗	成功	×
19	Int.CC.RP.33.01	成功	成功	○
20	Int.CC.RP.33.02	失敗	失敗	○

21	Int.CC.RP.34.01	成功	成功	○
22	Int.CC.RP.34.02	失敗	失敗	○
23	Int.CC.RP.35.01	成功	成功	○
24	Int.CC.RP.35.02	失敗	失敗	○
25	Int.CC.RP.36.01	成功	成功	○
26	Int.CC.RP.36.02	失敗	失敗	○
27	Int.CC.RP.37.01	失敗	失敗	○
28	Int.CC.RP.38.01	失敗	失敗	○
29	Int.CC.RP.39.01	失敗	失敗	○

日本国と韓国の Cross Certification モデルの実証実験による検証結果を「表 13.8　Cross Certification モデル(日本国<->韓国)　テスト結果」に示す。

表 13.8　Cross Certification モデル(日本国<->韓国)　テスト結果

No	テスト項目	テスト期待値	韓国現地実験	
			検証結果	期待値の比較判定
1	Int.CC.RP.19.01	成功	成功	○
2	Int.CC.RP.20.01	失敗	-	対象外
3	Int.CC.RP.21.01	失敗	-	対象外
4	Int.CC.RP.22.01	失敗	失敗	○
5	Int.CC.RP.23.01	成功	成功	○
6	Int.CC.RP.23.02	失敗	-	対象外
7	Int.CC.RP.24.01	成功	成功	○
8	Int.CC.RP.24.02	失敗	失敗	○
9	Int.CC.RP.25.01	成功	成功	○
10	Int.CC.RP.25.02	失敗	失敗	○
11	Int.CC.RP.26.01	失敗	失敗	○
12	Int.CC.RP.27.01	失敗	失敗	○
13	Int.CC.RP.28.01	失敗	成功	×
14	Int.CC.RP.29.01	成功	成功	○
15	Int.CC.RP.29.02	失敗	-	対象外
16	Int.CC.RP.30.01	失敗	成功	×
17	Int.CC.RP.31.01	失敗	失敗	○
18	Int.CC.RP.32.01	失敗	成功	×

19	Int.CC.RP.33.01	成功	成功	○
20	Int.CC.RP.33.02	失敗	失敗	○
21	Int.CC.RP.34.01	成功	-	対象外
22	Int.CC.RP.34.02	失敗	-	対象外
23	Int.CC.RP.35.01	成功	成功	○
24	Int.CC.RP.35.02	失敗	失敗	○
25	Int.CC.RP.36.01	成功	成功	○
26	Int.CC.RP.36.02	失敗	-	対象外
27	Int.CC.RP.37.01	失敗	失敗	○
28	Int.CC.RP.38.01	失敗	失敗	○
29	Int.CC.RP.39.01	失敗	失敗	○

日本国とチャイニーズ台北の Cross Certification モデルの実証実験による検証結果を「表 13.9　Cross Certification モデル(日本国<->チャイニーズ台北)　テスト結果」に示す。

表 13.9　Cross Certification モデル(日本国<->チャイニーズ台北)　テスト結果

No	テスト項目	テスト期待値	チャイニーズ台北現地実験	
			検証結果	期待値の比較判定
1	Int.CC.RP.19.01	成功	成功	○
2	Int.CC.RP.20.01	失敗	失敗	○
3	Int.CC.RP.21.01	失敗	-	対象外
4	Int.CC.RP.22.01	失敗	失敗	○
5	Int.CC.RP.23.01	成功	成功	○
6	Int.CC.RP.23.02	失敗	失敗	○
7	Int.CC.RP.24.01	成功	成功	○
8	Int.CC.RP.24.02	失敗	失敗	○
9	Int.CC.RP.25.01	成功	成功	○
10	Int.CC.RP.25.02	失敗	失敗	○
11	Int.CC.RP.26.01	失敗	失敗	○
12	Int.CC.RP.27.01	失敗	失敗	○
13	Int.CC.RP.28.01	失敗	成功	×
14	Int.CC.RP.29.01	成功	成功	○

15	Int.CC.RP.29.02	失敗	失敗	○
16	Int.CC.RP.30.01	失敗	成功	×
17	Int.CC.RP.31.01	失敗	失敗	○
18	Int.CC.RP.32.01	失敗	成功	×
19	Int.CC.RP.33.01	成功	成功	○
20	Int.CC.RP.33.02	失敗	失敗	○
21	Int.CC.RP.34.01	成功	成功	○
22	Int.CC.RP.34.02	失敗	失敗	○
23	Int.CC.RP.35.01	成功	成功	○
24	Int.CC.RP.35.02	失敗	失敗	○
25	Int.CC.RP.36.01	成功	成功	○
26	Int.CC.RP.36.02	失敗	失敗	○
27	Int.CC.RP.37.01	失敗	失敗	○
28	Int.CC.RP.38.01	失敗	失敗	○
29	Int.CC.RP.39.01	失敗	失敗	○

(3) ヒアリング結果

ヒアリング結果を、「表 13.10　Cross Certification モデル　ヒアリング結果」に示す。

表 13.10　Cross Certification モデル　ヒアリング結果

ヒアリング項目	ヒアリング結果	備考
ガイドラインの網羅性	・　十分に網羅性がある	-
テストパターンに関する妥当性	・　十分に妥当性がある	-
テスト期待値の的確さ	1) criticality の検証を署名検証者が行う必要が無いのではないか。本テスト項目のテスト期待値は検証失敗であるが、検証成功でも良いのではないか。	1) Int.CC.RP.28.01 Int.CC.RP.30.01

(4) 考察

「Int.CC.RP.28.01」、「Int.CC.RP.30.01」及び「Int.CC.RP.32.01」以外のテスト項目では、パス検証テストガイドラインのテスト期待値と検証結果が一致した。また、ヒアリングにおいて課題が挙げられなかった。よって、パス検証テストガイドラインの有効性が確認できた。

「Int.CC.RP.28.01」及び「Int.CC.RP.30.01」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。また、ヒアリングから、「Int.CC.RP.28.01」及び「Int.CC.RP.30.01」のテスト期待値を再検討するべきであるとの指摘が得られた。critical フラグは署名検証者が検証すべき X.509 証明書内の領域を示すインジケータであり、critical フラグ自身を検証する必要は必ずしもないといえる。本件は、課題項目として、パス検証テストガイドライン作成作業へフィードバックを行った。

「Int.CC.RP.32.01」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。これは、今回実験に使用した検証局が keyUsage が無い場合は、この領域を検証しないためである。ただし、検証局は、PKI ドメイン内における keyUsage の使用方法等により、keyUsage の検証方法をカスタマイズできる。このテスト項目におけるパス検証テストガイドラインのテスト期待値と検証結果の不一致は、検証局の実装方式によるものであり、パス検証テストガイドラインの有効性を損なわせるものではない。

「Int.CC.RP.28.01」及び「Int.CC.RP.30.01」については、テスト結果とヒアリング結果からパス検証テストガイドラインのテスト期待値の再検討が必要であることが確認された。本件は、課題項目として、パス検証テストガイドライン作成作業へフィードバックを行った。

13.3.3 Cross Recognition モデル

(1) 実験内容

現地日本国認証局において、本実験に必要となる証明書の発行を行い、その証明書を用いて証明書の検証を行う。検証を行うたびに得られた実験データを収集、分析する。検証内容の詳細については、パス検証テストガイドラインを参照のこと。

(2) 実験結果

本実験における検証結果を「表 13.11　Cross Recognition モデル　テスト結果」に示す。

表 13.11　Cross Recognition モデル　テスト結果

No	テスト項目	テスト期待値	検証結果	期待値の比較判定
1	Int.CR.RP.05.01	成功	成功	○
2	Int.CR.RP.06.01	失敗	-	対象外
3	Int.CR.RP.07.01	失敗	失敗	○
4	Int.CR.RP.08.01	失敗	失敗	○

5	Int.CR.RP.09.01	失敗	失敗	○
6	Int.CR.RP.10.01	失敗	失敗	○
7	Int.CR.RP.11.01	成功	成功	○
8	Int.CR.RP.11.02	失敗	失敗	○
9	Int.CR.RP.12.01	成功	成功	○
10	Int.CR.RP.12.02	失敗	失敗	○
11	Int.CR.RP.13.01	成功	成功	○
12	Int.CR.RP.13.02	失敗	失敗	○

(3) ヒアリング結果

ヒアリング結果を、「表 13.12　Cross Recognition モデル　ヒアリング結果」に示す。

表 13.12　Cross Recognition モデル　ヒアリング結果

ヒアリング項目	ヒアリング結果	備考
ガイドラインの網羅性	・　十分に網羅性がある	-
テストパターンに関する妥当性	・　十分に妥当性がある	-
テスト期待値の的確さ	・　十分に的確である	-

(4) 考察

本実験では､パス検証テストガイドラインのテスト要求と検証結果が一致した。また、ヒアリングにおいても課題が挙げられなかった。よって、パス検証テストガイドラインの有効性が確認できた。

13.4　サービスモデル

(1) 実験内容

現地日本国認証局において、本実験に必要となる証明書の発行を行い、その証明書を用いて証明書の検証を行う｡検証を行うたびに得られた実験データを収集、分析する。検証内容の詳細については、パス検証テストガイドラインを参照のこと。

(2) 実験結果

本実験における検証結果を｢表 13.13　サービスモデル　テスト結果｣に示す。

表 13.13　サービスモデル　テスト結果

No	テスト項目	テスト期待値	検証結果	期待値の比較判定
1	Svc.DS.RP.06.01	成功	成功	○
2	Svc.DS.RP.07.01	失敗	成功	×
3	Svc.DS.RP.07.02	失敗	成功	×
4	Svc.DS.RP.07.03	失敗	成功	×
5	Svc.DS.RP.07.04	成功	成功	○
6	Svc.DS.RP.08.01	失敗	失敗	○
7	Svc.DS.RP.09.01	成功	成功	○
8	Svc.DS.RP.09.02	失敗	失敗	○
9	Svc.DS.RP.10.01	成功	成功	○
10	Svc.DS.RP.10.02	失敗	失敗	○
11	Svc.DS.RP.11.01	成功	成功	○
12	Svc.DS.RP.11.02	失敗	失敗	○

(3) ヒアリング結果

ヒアリング結果を、「表 13.14　サービスモデル　ヒアリング結果」に示す。

表 13.14　サービスモデル　ヒアリング結果

ヒアリング項目	ヒアリング結果	備考
ガイドラインの網羅性	・　十分に網羅性がある	-
テストパターンに関する妥当性	1) 検証対象者のための一般的な keyUsage の検証は、パス検証テストとして実施する必要性は低いのではないか	1) Svc.DS.RP.07.02
テスト期待値の的確さ	1) criticality の検証を署名検証者が行う必要が無いのではないか。本テスト項目のテスト期待値は検証失敗であるが、検証成功でも良いのではないか。	1) Svc.DS.RP.07.03

(4) 考察

「Svc.DS.RP.07.01」、「Svc.DS.RP.07.02」及び「Svc.DS.RP.07.03」以外のテスト項目では、パス検証テストガイドラインのテスト期待値と検証結果が一致し

た。また、ヒアリングにおいて課題が挙げられなかった。よって、パス検証テストガイドラインの有効性が確認できた。

「Svc.DS.RP.07.01」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。これは、今回実験に使用した検証局が keyUsage が無い場合は、この領域を検証しないためである。ただし、検証局は、PKI ドメイン内における keyUsage の使用方法等により、keyUsage の検証方法をカスタマイズできる。このテスト項目におけるパス検証テストガイドラインのテスト期待値と検証結果の不一致は、検証局の実装方式によるものであり、パス検証テストガイドラインの有効性を損なわせるものではない。

「Svc.DS.RP.07.02」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。またヒアリング結果から「Svc.DS.RP.07.02」のテストパターンの妥当性を再検討するべきであるとの指摘が得られた。本件は、課題項目として、パス検証テストガイドライン作成作業へフィードバックを行った。

「Svc.DS.RP.07.03」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。また、ヒアリングから、「Svc.DS.RP.07.03」のテスト期待値を再検討するべきであるとの指摘が得られた。critical フラグは署名検証者が検証すべき X.509 証明書内の領域を示すインジケータであり、critical フラグ自身を検証する必要は必ずしもないといえる。本件は、課題項目として、パス検証テストガイドライン作成作業へフィードバックを行った。

13.5 失効モデル

(1) 実験内容

現地日本国認証局において、本実験に必要となる証明書の発行を行い、その証明書を用いて証明書の検証を行う。検証を行うたびに得られた実験データを収集、分析する。検証内容の詳細については、パス検証テストガイドラインを参照のこと。

(2) 実験結果

本実験における検証結果を「表 13.15　失効モデル　テスト結果」に示す。

表 13.15　失効モデル　テスト結果

No	テスト項目	テスト期待値	検証結果	期待値の比較判定
1	Rvk.CRL.RP.08.01	成功	成功	○
2	Rvk.CRL.RP.09.01	失敗	失敗	○
3	Rvk.CRL.RP.10.01	失敗	失敗	○

4	Rvk.CRL.RP.11.01	失敗	失敗	○
5	Rvk.CRL.RP.11.02	失敗	失敗	○
6	Rvk.CRL.RP.12.01	成功	成功	○
7	Rvk.CRL.RP.12.02	失敗	失敗	○
8	Rvk.CRL.RP.13.01	成功	成功	○
9	Rvk.CRL.RP.13.02	失敗	成功	×
10	Rvk.CRL.RP.13.03	失敗	失敗	○
11	Rvk.CRL.RP.13.04	失敗	失敗	○
12	Rvk.CRL.RP.13.05	失敗	成功	×
13	Rvk.CRL.RP.14.01	失敗	失敗	○
14	Rvk.CRL.RP.15.01	失敗	-	対象外
15	Rvk.CRL.RP.15.02	失敗	-	対象外
16	Rvk.CRL.RP.16.01	失敗	-	対象外
17	Rvk.CRL.RP.17.01	失敗	失敗	○
18	Rvk.CRL.RP.17.02	成功	成功	○
19	Rvk.CRL.RP.18.01	成功	成功	○
20	Rvk.CRL.RP.19.01	失敗	失敗	○
21	Rvk.CRL.RP.20.01	失敗	失敗	○
22	Rvk.CRL.RP.21.01	失敗	失敗	○
23	Rvk.CRL.RP.22.01	成功	成功	○
24	Rvk.CRL.RP.23.01	失敗	失敗	○
25	Rvk.CRL.RP.24.01	成功	成功	○
26	Rvk.CRL.RP.25.01	失敗	失敗	○
27	Rvk.CRL.RP.26.01	失敗	失敗	○
28	Rvk.CRL.RP.27.01	成功	成功	○
29	Rvk.CRL.RP.28.01	失敗	失敗	○
30	Rvk.CRL.RP.29.01	失敗	成功	×
31	Rvk.CRL.RP.30.01	成功	成功	○
32	Rvk.CRL.RP.31.01	失敗	失敗	○

(3) ヒアリング結果

ヒアリング結果を、「表 13.16　失効モデル　ヒアリング結果」に示す。

表 13.16　失効モデル　ヒアリング結果

ヒアリング項目	ヒアリング結果	備考
ガイドラインの網羅性	・　十分に網羅性がある	-

テストパターンに関する妥当性	・　十分に妥当性がある	-
テスト期待値の的確さ	1）criticality の検証を署名検証者が行う必要が無いのではないか。本テスト項目のテスト期待値は検証失敗であるが、検証成功でも良いのではないか。	1）Rvk.CRL.RP.13.02

(4) 考察

「Rvk.CRL.RP.13.02」、「Rvk.CRL.RP.13.05」及び「Rvk.CRL.RP.29.01」以外のテスト項目では、パス検証テストガイドラインのテスト期待値と検証結果が一致した。また、ヒアリングにおいて課題が挙げられなかった。よって、パス検証テストガイドラインの有効性が確認できた。

「Rvk.CRL.RP.13.02」ついては、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。また、ヒアリングから、「Rvk.CRL.RP.13.02」のテスト期待値を再検討するべきであるとの指摘が得られた。critical フラグは署名検証者が検証すべき X.509 証明書内の領域を示すインジケータであり、critical フラグ自身を検証する必要は必ずしもないといえる。本件は、課題項目として、パス検証テストガイドライン作成作業へフィードバックを行った。

「Rvk.CRL.RP.13.05」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。これは、今回実験に使用した検証局が keyUsage が無い場合は、この領域を検証しないためである。ただし、検証局は、PKI ドメイン内における keyUsage の使用方法等により、keyUsage の検証方法をカスタマイズできる。このテスト項目におけるパス検証テストガイドラインのテスト期待値と検証結果の不一致は、検証局の実装方式によるものであり、パス検証テストガイドラインの有効性を損なわせるものではない。

「Rvk.CRL.RP.29.01」については、パス検証テストガイドラインのテスト期待値と検証結果が一致しなかった。これは、今回使用した検証局は、失効リストに issuingDistributionPoint が無い場合、issuingDistributionPoint と crlDistributionPoint の一致性を検証しないためである。このテスト項目におけるパス検証テストガイドラインのテスト期待値と検証結果の不一致は、検証局の実装方式によるものであり、パス検証テストガイドラインの有効性を損なわせるものではない。

14 現地環境における署名用トークンインターフェース仕様の実証実験

14.1　概要

「署名用トークンインターフェース仕様」を現地環境における署名付与・検証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する。

共通のアプリケーションを各国の利用者端末から使用し、各国それぞれのエンドエンティティ証明書を使用して署名付与及び検証を行う。

利用者端末ログ情報による検証内容データを収集、解析することで利用者にとっての有効性を検証する。

14.2　正常系検証

(1) 実験内容

各国の正常なエンドエンティティ証明書を格納した利用端末を使用し、日本、韓国が構築するアプリケーションをアクセスし、署名の付与と検証を行う。

なお、本実験における署名検証においては、パス検証に関する実験を別に行っていることから証明書の有効性の検証は含まないものとする。

本実験で実施する項目を「表 14.1　正常系署名付与･検証の実験項目」に示す。

表 14.1　正常系署名付与･検証の実験項目

検証者	検証対象	確認内容
日本国	日本アプリケーション	・署名付与 ・署名検証
韓国	日本アプリケーション	・署名付与 ・署名検証
日本国	韓国アプリケーション	・署名付与 ・署名検証
チャイニーズ台北	日本アプリケーション	・署名付与 ・署名検証
日本国	チャイニーズ台北アプリケーション	・署名付与 ・署名検証

(2) 実験結果データ

本実験における検証結果を「表 14.2　正常系署名付与･検証における検証結果」に示す。

表 14.2　正常系署名付与･検証における検証結果

検証者	検証対象者	結果		判定
		期待値	検証結果	
日本国	日本アプリケーション	OK	OK	○
韓国	日本アプリケーション	OK	OK	○
日本国	韓国アプリケーション	OK	OK	○
チャイニーズ台北	日本アプリケーション	OK	OK	○
日本国	チャイニーズ台北アプリケーション	OK	OK	○

「表 14.2　正常系署名付与･検証における検証結果」よりわかるとおり、全ての項目において期待値通りの結果を得た。

(3) 評価・考察

本実験における署名の付与及び検証について、すべて期待どおりの結果を得ることができた。共通のアプリケーションを異なる PKCS#11 ライブラリを用いて署名の付与及び検証が行えたことから、署名用トークンインターフェース仕様の有効性を検証することができたと言える。

当実験においては、署名メカニズムとして CKM_RSA_PKCS を使用している。署名メカニズムとは、PKCS#11 で定められている署名の処理方式に関する設定値であり、CKM_RSA_PKCS とは、ハッシュ値は作成せず、平文を秘密鍵を使用して RSA 暗号化するメカニズムとなっている。署名メカニズムとしてもう一つ代表的なものに CKM_SHA1_RSA_PKCS があり、どちらを使用するかについては、アプリケーションにとっての署名がどうあるべきかの考察を交えて「18 全体考察（まとめ)」で述べる。

14.3　異常系検証

(1) 実験内容

各国の正常なエンドエンティティ証明書を格納した利用端末を使用し、日本、韓国が構築するアプリケーションをアクセスし、署名の付与と検証を行う。

署名の付与は「14.2　正常系検証」と同様であるが、署名を検証する前に署名データを故意に改竄することで改竄を検出可能かどうかを検証する。

なお、本実験における署名検証においては、証明書の有効性の検証は含まないものとする。

本実験で実施する項目を「表 14.3　異常系署名付与･検証の実験項目」に示す。

表 14.3　異常系署名付与･検証の実験項目

検証者	検証対象	確認内容
日本国	日本アプリケーション	・署名付与 ・署名検証
韓国	日本アプリケーション	・署名付与 ・署名検証
日本国	韓国アプリケーション	・署名付与 ・署名検証
チャイニーズ台北	日本アプリケーション	・署名付与 ・署名検証
日本国	チャイニーズ台北アプリケーション	・署名付与 ・署名検証

(2) 実験結果データ

本実験における検証結果を「表 14.4　異常系署名付与･検証における検証結果」に示す。

表 14.4　異常系署名付与･検証における検証結果

検証者	検証対象者	結果		判定
		期待値	検証結果	
日本国	日本アプリケーション	NG	NG	○
韓国	日本アプリケーション	NG	NG	○
日本国	韓国アプリケーション	NG	NG	○
チャイニーズ台北	日本アプリケーション	NG	NG	○
日本国	チャイニーズ台北アプリケーション	NG	NG	○

「表 14.4　異常系署名付与･検証における検証結果」よりわかるとおり、全ての項目において期待値通りの結果を得た。

(3) 評価・考察

本実験において、署名値の改竄の検証について、すべての実験項目で期待どおりの結果を得ることができた。

このことから、共通のアプリケーションを各国／地域の異なる PKCS#11 ライブラリを用いて署名値の改竄の検出について検証することができた。また、署名用トークンインターフェース仕様の改竄検出に関する有効性を検証することができた。

今後、シンガポールアプリケーションとの追加実験、或いは参加国同士での署名メカニズムに関する議論を重ね､より相互運用性の高い仕様とする必要がある。

また、今後の課題を明確にすることができたという点では、有意義な実験であったといえる。

15 検証結果

本章では、7 章から 14 章までで実験単位ごとに記述した検証結果について、収集したヒアリング結果の分析を加えながら考察する。

15.1　シミュレーションセンタにおける PKI コンポーネント間接続に関する標準の実用性の検証

本項目では、シミュレーションセンタにおいて「相互接続インターフェース仕様」の実用性を、証明書を発行する側である認証局の運用者の立場から検証する。

15.1.1　相互接続インターフェース仕様の実用性の検証

本項目では、「5　シミュレーションセンタにおける認証局間の実証実験」として検証した検証結果とヒアリングの結果を分析する。

「5　シミュレーションセンタにおける認証局間の実証実験」で行った検証作業を通じて、「相互接続インターフェース仕様」を業務に適用した場合に標準の不備に起因する障害の発生はない。実験結果としては、期待された結果が得られている。昨年度及び本年度の実証実験結果を経て、標準が十分な実用性を持った結果であると評価できる。

以下に、シミュレーションセンタの日本国認証局、チャイニーズ台北認証局及び香港チャイナ認証局の運用者から採取したヒアリング結果を示しながら考察を行う。

標準書の構成の妥当性、記述の明確性および内容の網羅性について問うたところ、回答者全員が適当であると回答しており、評価は高い。

内容の網羅性に関する問いには１名が「各種証明書の発行に必要な情報が十分に記載されている」と高く評価している。また「各種証明書の発行の際に、相互接続に必要な必須項目が明記されており、相互接続を行う際に円滑な接続が行えた」とのコメントが寄せられている。構成の妥当性に関する問いには、「RFC などへの参照の表記において章番号項番号まで記載されており、他の標準への参照が容易になっており評価できる」とのコメントが寄せられており、高い評価を得ていると言える。また、記述の明確性に関する問いには、「プロファイル仕様に Excel を使用しているが、実際に標準を配布・公開するという意味においては、pdf 等を利用したほうが良いのではないか」との意見が寄せられた。

以上、ヒアリングにより現状の標準の実用性に対して十分な評価を得られた。

15.2　現地実証実験環境における PKI コンポーネント間接続に関する標準の有効性の検証

本項目では、日本、チャイニーズ台北および香港チャイナの３国／地域による実証実験環境において「相互接続インターフェース仕様」の有効性を、証明書を発行する側である認証局の運用者の立場から検証する。

15.2.1　相互接続インターフェース仕様の有効性の検証

本項目では、「8　現地環境における認証局間の実証実験」として検証した検証結果とアンケートの結果を分析する。

検証作業を通じて、「相互接続インターフェース仕様」を業務に適用した場合に標準の不備に起因する障害の発生はない。運用上の制限などで標準を適用できない点で問題が発生しており、標準で定義された内容と現実の実装との差異を埋めることが課題であることを示す検証結果であると言える。

以下に、現地実証実験日本国認証局、現地チャイニーズ台北認証局及び現地香港チャイナ認証局の運用者から採取したアンケート結果を示しながら考察を行う。

まず、構成の妥当性に関する質問に対しては、回答者全員から妥当であるとの回答が得られている。コメントとして、「略語集に cRLDP /iDP を追記すべき」「CRL の置き換えによる脅威等、セキュリティ上の考慮点に関するセクションもあると良い」などのコメントが寄せられており、標準をさらに実用的にするための提言が行われた。

また、内容の網羅性に関する質問に対しても、回答者全員から十分であるのと回答が得られている。コメントとして「ビジネス環境においては実証実験環境より複雑な環境になる可能性がある。たとえばエンドエンティティの鍵及び証明書はスマートカードで配布する場合もあると思われる。標準としては、証明書及び CRL プロファイルのみとすることが望ましい」というコメントが寄せられた。これは、将来的な相互認証関係の拡大とより広範囲での相互接続に対応する汎用性の高い標準策定への前向きな提言である。

以上、ヒアリングにより現状の標準の有効性に対して十分な評価を得られ、かつ国際間の相互接続において標準がより高い有効性を持つための提言を得た。

15.3　現地実証実験環境における PKI アプリケーションに関する標準の有効性の検証

15.3.1 パス検証テストガイドラインの有効性の検証

本項目では、「13 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」として検証した検証結果とアンケート結果を分析する。

実証実験では、ほとんどのテスト項目において、テスト期待値と検証結果が一致し、パス検証テストガイドラインのテスト期待値の的確性に高い評価が得られた。また、テスト期待値と検証結果が不一致であったテスト項目については、ヒアリングにおいても指摘された点と共に、実証実験結果をパス検証テストガイドライン作成作業にフィードバックすることによって、パス検証テストガイドラインに改訂が加えられ、より評価が高められた。

以下に、PKI サービス担当者(シミュレーションセンタの日本国認証局、韓国認証局、チャイニーズ台北認証局及び日本国において実運用をしている認証局の運用者)並びに日本国で証明書検証サーバを開発している担当者へヒアリング及びアンケー

トを実施し、収集した評価データを分析することにより、パス検証テストガイドラインの有効性検証の評価を行う。

ガイドラインの網羅性に関する問いには、「ほぼ全てのパターンが考慮されており、高い網羅性を備えている」との総意を得ることができた。特に相互接続モデルに関しては、「実際の相互接続モデルを考慮し、利用者の安全なアプリケーション利用の場を促進するために有効である」とのコメントを得ており、これは、異なる PKI ドメイン間の相互接続を実現する上の一助としてパス検証テストガイドラインが非常に有意義であることを示す。

テストパターンに関する妥当性への問いには、「十分なテストパターンが考慮されている」との総意を得ることができた。また、「現状においては十分である」とした上で、「今後の展開として、IETF で議論されている検証モデル(OCSP、SCVP、CVP 及び DVCS 等)をパス検証テストガイドラインに組み込んでいくべきである」との積極的なコメントも得られた。

テスト期待値の適確さに関する問いには、「DistinguishedName のマッチングに関するテスト期待値、criticality のチェックに関するテスト期待値に関して、検討するべきである」とのコメントを得たが、このコメントを検討して、テスト期待値に見直しをかけることで、パス検証テストガイドラインのテスト期待値の適確さを高めることができた。また、その他のテスト期待値に関しては、総じて的確であるとの評価を得られた。

このように「13 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」とアンケートの結果からパス検証テストガイドラインの利用者にとっての有効性が明らかになった。また、実証実験結果及びアンケートの結果を踏まえ、パス検証テストガイドラインの改訂を行ったことで、より有効性が向上したと評価できる。

15.3.2 署名用トークンインターフェース仕様の有効性の検証

本項目では、「14 現地環境における署名用トークンインターフェース仕様の実証実験」における実験結果とヒアリングの結果を分析し、検証を行う。

今回の実験において、すべて期待とおりの結果を得ることができた。このことから、本標準はアプリケーション利用者にとっての有効性が高いと評価することができる。以下に、韓国、チャイニーズ台北の PKI 技術者及びアプリケーション開発経験者へ行ったヒアリングの結果を示しながら考察を行う。

まず、アプリケーションモデルとして PKCS#11 を選定したことについては、OS に関してオープンプラットフォームであることから全員より妥当であるとの評価を得た。また、署名付与・検証の機能に特化した点については、今後の電子商取引において電子署名が重要となってくると思われることから、全員より問題は無く妥当であるとの評価を得た。ただし、1 名が PKCS#11 における署名メカニズムに関して定義を行う必要性を述べており、今後の課題点として明確にすることができた。更に、アプリケーション開発者にとっての開発の容易性及び有効性については、全

員より有効であり、かつ実用的であるとの評価を得た。

以上のことから、本標準に対する有効性について十分に高い評価を得られたと分析することができる。

今回導入した Wrapper 機能についてもヒアリングを行ったところ、1 名より「機能としては非常に有効なものであるが、アプリケーションでも実現可能な機能であり、アプリケーションと独立した機能とする必要はない」との意見があった。

従って、本標準では、Wrapper 機能は実現する必要があるが、Wrapper を必ずしも独立したモジュールとする必要は無いことを記述し整理した。このことにより、本標準の有効性をより高めることができた。

16 全体考察（まとめ）

16.1　成果

以下に本実証実験の成果を示す。

16.1.1 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。

実証実験では、各国の認証スキームや検証形態を維持し、ユーザの負担を最低限にとどめ、いかに各国間の相互接続をスムーズに進めるかが大きな課題となる。地域拡大となると、構成が複雑になりやすく、意図しないトラブルを招くために、PKI 体系の広がりを考慮しながら、設計を行わなければならない。本実証実験で採用した CC と CR のハイブリッドモデルは、地域拡大の要求に対しても、各国間における相互認証証明書の発行、相互認証証明書の制限フィールドの利用、証明書/CRL やリポジトリプロファイルの変更することなしで稼動することを実証した。また、必須とされていた幾つかのフィールドを任意とし、より多くの相手が参加し接続しやすいアーキテクチャにすることも可能にした。

(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。

本実証実験で作成した標準は、X.509(2000)や RFC3280 の標準に基づき汎用性の高いプロファイルとして規定されている。しかしながら汎用性を高めると任意の設定項目が増え、相互接続時に問題になることが多く、また同じ個所で問題が検出される場合がほとんどである。本実証実験においても以下の問題が繰り返し検出された。

- CRL 分割ポリシの差異と失効リストのリスク対策
- cRLDP の記載
- LDAP における属性設定

この課題を解消するために、アプリケーション実験を行う前にお互いの実装を確認するためテスト項目化を行い、実験し、その有効性を確認することができた。このことはより安全なアプリケーション通信を確立するためのテスト項目として提示することの有効性を示すことができ、今後の相互接続テストのリファレンスとなる実績を残すことができたことは大きいであろう。

(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。ただし鍵長及び cRLDP/iDP チェックについては、今後、日本の GPKI システムがチャイニーズ台北側の GPKI システムとトランザクションを行うためには､解決しなければならない課題である。

(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。

アジア圏における多種多様な認証基盤がある中、インターネット取引のディフォルト製品であるウェブベースの機能を使い、お互い合意した証明書プロファイルで相互接続が可能であることの実績を残せたことには大きいと考える。

16.1.2 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

本ガイドラインは、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 3 章において、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。

ガイドライン利用者は、評価対象となる相互接続環境をこれらのいずれかにあ

てはめることによって、テスト要件の抽出を容易にしている。

実験対象各国は、特に一点目「CA-CA 間の相互接続形態」の観点からの分類について強い興味を示した。これは本ガイドラインの「CA-CA 間の相互接続形態」に関する分類が、各国が今後様々な相互接続形態を持つ際のリファレンスとして有益である、と言うことができる。

他の二つの観点についても、今後さらに拡充することで、同様に価値を高めることができると考えられる。

(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。

また各テストケースでは、IWG recommendation profile のサブセット証明書を使用することにより、IWG recommendation profile のもとでは、標準のパス検証機能を正しく処理されることが確認できた。

本ガイドラインでは各テストケースは相互接続環境(モデル)ごとに定義してあり、PKI アプリケーションなどのパス検証機能を評価する際には、そのアプリケーションが動作する相互接続環境を明確にすることで、そこで満たすべきテスト要件とテスト期待値を抽出し、評価の指標に用いることができる。

このように本ガイドラインは、PKI アプリケーション等が各相互接続環境において必要なパス検証機能を実装しているかどうかを評価するためのフレームワークとして利用することができる。

(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。

今回、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。

16.2　考察及び今後の展開

16.2.1 相互接続インターフェース仕様

(1) 下位認証局との相互認証について

階層構造を持ったあるドメイン X が、他のドメイン Y と相互接続する際には、各ドメインの主要認証局(PrincipalCA)同士が信頼関係を築くのが一般的なケースと考えられる。

例えば相互接続モデルとして相互認証モデルを選択する場合、ドメイン X のルート認証局 X とドメイン Y のルート認証局 Y が相互認証することが典型例と考えられる。

が、何かしらの理由によりルート認証局-X が、相互認証証明書を発行できない(ポリシ上の問題であったり、技術的な問題であるかも知れない)場合、その下位認証局(SubCA-X)がドメイン X の主要認証局として、代わりに他のドメイン Y と相互認証するケースも考えられる。

ドメイン X のような階層モデルでは主要認証局もトラストアンカもルート認証局 X であるのが一般的だが、このように主要認証局が下位認証局 X であり、トラストアンカがルート認証局 X(あるいはこれも下位認証局 X とする場合があるかもしれない)である場合について、認証パスの構築又は検証の観点から検討・考察を行い、実際に相互認証を行うにあたっての注意点を明確にする。

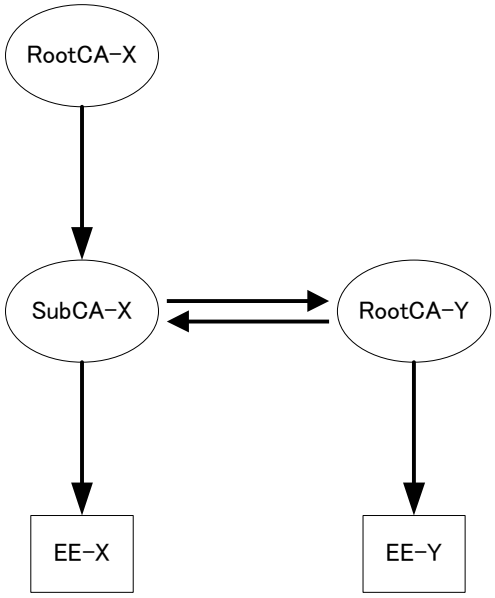


図 16.1　下位認証局との相互認証例

(a) エンドエンティティ X がエンドエンティティ Y の証明書を検証する場合

このケースでは、認証パスを構築する際に、以下のような条件が満たされている必要がある。

表 16.1　パス構築方法による違い

	トラストアンカに RootCA-X を指定した場合	トラストアンカに SubCA-X を指定した場合
順方向 **パス構築**[13]	RootCA-X エントリの crossCertificatePair.issuedByThisCA	特になし

[13]検証対象証明書から署名検証者トラストアンカへ向かって、主に crossCertificatePair.issuedToThisCA の issuer を辿っていくパス構築手法

	に SubCA-X の下位 CA 証明書が必要	
逆方向パス構築[14]	SubCA-X エントリの crossCertificatePair.issuedToThisCA に SubCA-X の下位 CA 証明書が必要	特になし
ハイブリッドパス構築[15]	特になし	特になし

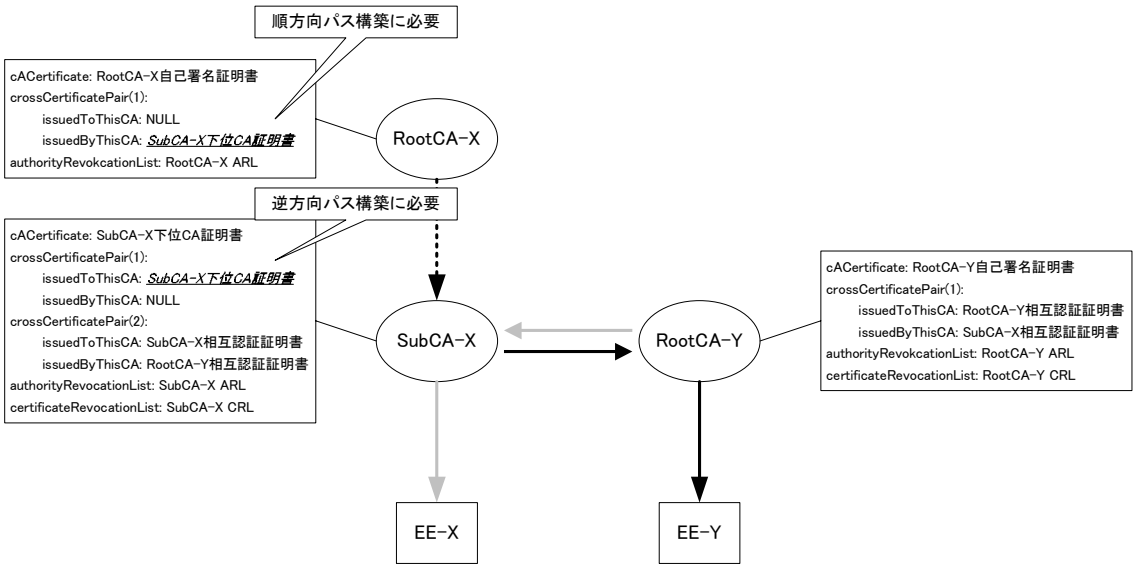


図 16.2　下位認証局 EE からのパス検証

16.2.2(5)下位認証局証明書の格納エントリと属性で後述するように、下位認証局証明書を crossCertificatePair へ格納することは、好ましいことではない。つまりエンドエンティティ Y 証明書を検証するにあたって、ルート認証局 X を指定することは難しいと言える。このためエンドエンティティ X は他ドメインへの認証パスを検証するためには下位認証局 X をトラストアンカとしなければならない。

一方でローカルドメイン X における認証パス検証時には、エンドエンティティ X は一般的にはルート認証局 X をトラストアンカとして指定すべきである。ここにドメイン内外での検証方法に差異が生じてしまう。これを解消するには、下位認証局 X が、ローカルドメイン X の実質的なトラストアンカとして利用で

[14]署名検証者トラストアンカから検証対象証明書へ向かって、主に crossCertificatePair.issuedByThisCA の subject を辿っていくパス構築手法

[15] 署名検証者トラストアンカから検証対象トラストアンカまでを順方向パス構築で、署名者証明書から検証対象トラストアンカまでを逆方向パス構築する手法

きるようにするなどの工夫が必要である。これは例えば技術的には下位認証局 X が同じ鍵ペアを用い自己署名証明書を発行するか、運用的には、下位認証局 X がルート認証局 X の唯一の下位認証局とすることで、実質的にルート認証局 X と同じ立場/権限を与えることである。

(b) エンドエンティティ Y がエンドエンティティ X の証明書を検証する場合

このケースでは、パス構築よりもパス検証において本質的な問題が潜在している。具体的には、認証パスに含まれている下位認証局 X の下位認証局証明書を検証しようとする場合に、認証パスに含まれないルート認証局 X が発行した ARL を必要とする問題である。

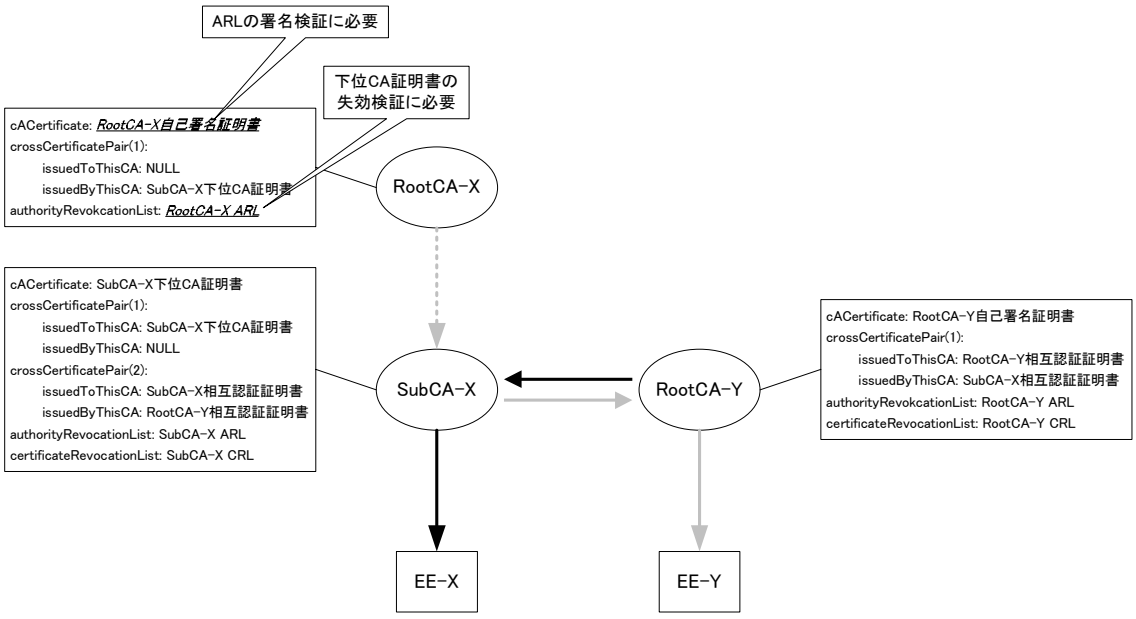


図 16.3　下位認証局 EE のパス検証

ルート認証局 Y からエンドエンティティ-X までに認証パスを検証する際、エンドエンティティ-X 証明書を検証するためには下位認証局 X の公開鍵が必要だが、これを下位認証局 X エントリの cACertificate に格納された下位認証局証明書から取得するか、ルート認証局 Y エントリ又は下位認証局 X エントリの crossCertificatePair に格納された下位認証局 X 相互認証証明書から取得するかは、X.509 や RFC3280 でも明確には定められていないようである。

下位認証局 X 相互認証証明書を用いた場合には、これを失効検証するのに必要なのは、ルート認証局 Y が発行する ARL なので、特に問題はない。

しかし下位認証局証明書を用いた場合には、下位認証局 X が失効していないことを確認するために、ルート認証局 X の発行する ARL を使わなければならない。これはルート認証局 Y がルート認証局 X を信頼しなければならないこと

を意味する。ルート認証局 X は図 16.3 を見ても明らかなように、ルート認証局 Y からエンドエンティティ-X への認証パスには含まれていない。つまり、検証者によっては、エンドエンティティ-X を信頼できない場合があり得るということになる。

これを解決するには、下位認証局 X の失効検証するために認証パス外の認証局を必要としないモデルを維持することだが、最も典型的な方法は、下位認証局 X が下位認証局証明書だけでなく、同じ鍵ペアによる自己署名証明書をも併せ持つことである。これは言い換えれば、他ドメインと相互接続する主要認証局は、自己署名証明書を持つ認証局であるべきだと考えることができる。

(c) まとめ

以上のように、他ドメインの下位認証局と相互認証する際の本質的な問題は、下位認証局 X が自己署名証明書を併せ持つことによって解決できるが、本質的に「自己署名証明書を持たない他ドメインの認証局を信頼することは、大きなリスクを背負うことになる」と言ってよいだろう。

他ドメインと相互接続する際には、(第三者に依存しない信頼関係を構築できる)自己署名証明書を持った主要認証局と信頼関係を結ぶべきである。

(2) 相互接続時における VA の在り方について

(a) 相互接続時における Validation Authority[16](VA)利用の問題点

VA は、VA 証明書を発行した認証局をトラストアンカとする PKI ドメイン内で利用することが前提となっている。そのため相互接続時においても、利用される VA は自ドメインのトラストアンカ認証局はもちろんのこと、VA が共有される場合においては、利用されるすべてのドメインのトラストアンカ認証局から証明書の発行を受けなければならない。相互接続時における VA の利用には、以下の問題が発生する。

(i) VA の審査

VA に対し認証局が証明書を発行する際、明確な審査対象物が存在しないという問題点がある。これは、何をもって認証局が VA を審査するかを意味している。

例えば、一個人に対して証明書を発行する際は、写真付きの証明書（例えば運転免許書）などが審査の対象物となり、証明書の発行を行う。また、SSL サーバ証明書を発行する際は、ドメインへの登録情報等が審査の対象物として用いられる場合がある。しかし、VA においては明確な審査対象物が存在しないのが現状である。

[16] Validation Authority (VA)は、証明書の信頼性や有効性を検証する。

(ii) VA の設置場所

国間で相互接続を行う場合には、VA の設置場所も問題と成り得る。例えば VA の利用者にとって、自国に設置された VA に比べ、他国に設置された VA を信頼するのは容易なことではない。

以上の問題点は、VA の運用規定を策定し、公開することにより回避できるかもしれない。また、VA 製品自身の評価には、例えば ISO/IEC15408 等の第三者による評価が有効に成り得る。これらの運用規定や評価結果は、証明書発行時の審査対象物として扱うことができると共に、VA の利用者にとっても他国の VA を信頼するための評価基準となる。

しかしながらこの運用規定の詳細については今後の検討課題となる。

(b) 相互接続時における VA モデル

先述したが、VA は VA 証明書を発行した認証局をトラストアンカとし、その PKI ドメイン内で利用することが前提となっている。それはつまり、他ドメインの検証依頼者による利用は考慮されていないものと考える事ができる。例えば GPKI の場合においても、互いのドメインは相互接続されているものの、ドメイン毎に VA が設置されており、他ドメインの検証依頼を処理する事ができないのが現状である。

相互接続時における VA の有効利用を考慮すると、以下のモデルが考えられる。

(i) 単一の VA を共有するモデル

異なるドメインの認証局間で相互認証がなされ、それぞれの認証局より VA 証明書の発行がなされている場合、1 つの VA を異なるドメインで共有することが可能となる。それは、異なるドメインのトラストアンカ認証局によって発行された VA 証明書が、各ドメインの検証依頼者にとって有効なものになるからである。

また、これとは別に CC モデルと CTL モデルの組合せが VA の共有を可能とさせる。例えば検証依頼者が、他ドメインの認証局によって発行された VA 証明書を受信した場合においても、クライアントの CTL にその認証局情報が含まれていれば、結果的にその VA 証明書を信頼することができる。またこのことは、相互認証を行っていないドメイン間の相互接続も成し得るのである（例えば CC モデルと CR モデルのハイブリッド型モデル)。

(ii) 複数の VA が共存するモデル（VA Relaying[17]）

VA の Relaying ロジックを用いれば、異なるドメインの証明書検証が可能と成り得る。例えば、ドメイン A の検証依頼者がドメイン A の VA（A-VA）にドメイン B 証明書の検証依頼を行う場合を考える。もし、A-VA がドメイン B におけるパス構築が行えない場合、A-VA はドメイン B の VA（B-VA）へその証明書の検証依頼を行う。B-VA はパス構築・検証を行い、その結果を A-VA へ返却する。A-VA は返却された結果を基に、残りのパス構築・検証（ドメイン A の証明書パス構築・検証が必要な場合）を行い、検証依頼者へ結果を返却する。これら一連の流れ（Relaying と呼ばれている）で最も重要な点は、A-VA と B-VA がどのようにしてお互いを信頼するかである。

この信頼の絆は VA 間の通信プロトコルに、OID で示されたポリシを共有することにより築く事ができると考えられる。例えば検証依頼をする A-VA が、A-VA のポリシである P を通信プロトコルに示し、B-VA が P を受け入れる事ができなければ、A-VA と B-VA 間には信頼関係が存在しないとみなすことができる。尚、この VA のポリシには、運用規定も示されているべきである。

国際間の相互運用において、どの VA モデルが適しているかは、今後の検討課題となる。

(3) 証明書/CRL プロファイルにおける cRLDP と iDP の扱いについて

cRLDP と iDP に関しては昨年度にも同様の議論が行われている。今年度は昨年度の議論に加え様々な認証局の失効リスト発行パターンなどを考慮して改めて考察する。

現在の IWG 仕様では、相互接続相手に対して以下の要求を行っている[18] 。

GPKI 要件 a)：cRLDP.distPoint を設定する場合には必ず iDP.distPoint を設定する

GPKI 要件 b)：これら 2 つの distPoint の名前を比較する

しかし、これらの要求は相互接続相手にスムーズに受け入れられていない。異なる PKI ドメインでは失効リスト発行及び配布ポリシに違いがある。その違いがスムーズに受け入れられない主な原因である。接続相手の経験や知識不足、又は単なる製品上の制限から起因すると考えてしまうのは軽率である。相互接続時には、失効リスト発行及び配布ポリシの差異をできるだけ吸収し、X509(2000)や RFC3280 で定義されている範囲で解決策を模索しなければならない。

以下に、現時点における問題点を明確化し、問題点に対する解決策を提言する。

---

17 Relaying については RFC3379 Delegated Path Validation and Delegated Path Discovery Protocol Requirements にて述べられている。http://www.ietf.org/rfc/rfc3379.txt?number=3379

18 この要件は相互接続に関して実績のある日本の政府認証基盤（GPKI）相互運用性仕様による。

(a) 現時点での要求項目の妥当性

上記、**GPKI 要件 a)**及び**GPKI 要件 b)**の目的は、失効リスト分割時に起きると想定される置換攻撃を防ぐのが目的である。証明書の発行量が増加するに従い失効される証明書の数も増える可能性があり、証明書の失効量に比例して失効リストのサイズも大きくなる。失効リストのサイズが肥大化することが予想される場合には、認証局運営者は失効リストを分割し配布したいと望むであろう[19]。

分割された失効リストはクラッカーなどが途中で意図しない別の失効リストにすり替え配布した場合にも、検証者側では識別できず、検証者は正しい検証結果を得られない事態が発生する[20]。この事態を防ぐため認証局が意図した場所から取得した失効リストと検証者が取得した場所の失効リストを比較して、失効リストがすり返られていないかどうかチェックする必要がある。

これが現時点での要求項目である。想定される脅威が提示され対策が施されている。ここまでの議論は何も問題ないものに見える。しかし複数間ドメインにおいて相互接続を行う場合、この要求はすんなりと受け入れられていない。

(b) 問題の所在 1：CRL 配布形態の想定範囲と対応策のオーバースペック

失効リスト置換攻撃への有効な対策を明確化するには、失効リストの発行ポリシについて現実的なパターンを明確にする必要がある。現在、実績のある失効リストの分割方法として、CRL と ARL に分割する方法、及び、CRL 自身を分割する方法がある[21]。これを整理すると失効リストの主な分割方法は以下の通りとなる。

(i) 分割しない場合
(ii) CRL と ARL に分割する場合
(iii)失効リストを CRL/ARL 以外の方法で分割する場合
(iv)失効リストを CRL と ARL を分割し、かつ CRL/ARL を分割する場合

失効リストを分割する場合､失効リスト置換攻撃 のリスクを負うことが良く知られている。失効リスト置換攻撃に対するプロファイルによる対策として、前述したように分割された失効リスト自身に、その識別情報をセットする方法が有効である。前述の(1)～(4)の場合において、それぞれの分割方法と対処方法について明確化する。

---

[19] 例えば、シリアル番号の範囲で失効リストを分割する場合などがあげられる。
[20] 別の失効リストを取得してしまった場合でも認証局の正しい署名が付与されており､有効期限内であるため､当該証明書が失効していても正常に検証が終了してしまう。
[21] ここではデルタ CRL や IndirectCRL は考慮しない

(i) 分割しない場合

失効リストを分割しないため失効リスト置換攻撃は発生しない。証明書 cRLDP 領域は、当該証明書の issuer エントリ以外で失効リストを配布する場合必要となる。CRL の iDP 領域は設定不要。

(ii) CRL と ARL に分割する場合

失効リストを分割するため失効リスト置換攻撃が発生する可能性がある。証明書 cRLDP 領域は、当該証明書の issuer エントリ以外で失効リストを配布する場合のみ必要となる。それぞれの失効リストの iDP 領域は、該当する onlyXXCerts を設定しなければならない。

(iii) 失効リストを CRL/ARL 以外の方法で分割する場合

失効リストを分割するため､失効リスト置換攻撃が発生する可能性がある。CRL を複数配布するため、証明書の cRLDP 領域は必須となる。それぞれの失効リストの iDP 領域は、iDP.distPoint に、当該証明書の cRLDP.distPoint における記載と同じ値を記載しなければならない。また、iDP.distPoint.fullname の値を検証しなければならない。

(iv) 失効リストを CRL と ARL を分割し、かつ CRL を分割する場合

失効リストを分割するため､失効リスト置換攻撃が発生する可能性がある。

CRL を複数配布するため、証明書の cRLDP 領域は、必須となる。CRL の iDP 領域は、該当する onlyXXCerts を設定しなければならない。また、それぞれの失効リストの iDP 領域は、iDP.distPoint.fullName に、当該証明書の cRLDP.distPoint.fullName における記載と同じ値を記載しなければならない。また、iDP.distPoint.fullName 値の検証をしなければならない。

これらをまとめると表 16.2 のようになる。

表 16.2　失効リスト分割によるリスクとその対策

	置換攻撃の可能性	cRLDP の設定	iDP.distPoint の設定	検証
分割しない場合	無し	設定してもよい	設定不要	
CRL と ARL に分割する場合	あり		onlyXXCerts	onlyXXCerts の確認

失効リストを CRL/ARL 以外の方法で分割する場合		必須	iDP.distPoint.fullName	iDP.distPoint.fullName の値を検証する。
失効リストを CRL と ARL を分割し、かつ CRL を分割する場合			必要に応じて onlyXXCerts, fullName を設定する。	必要に応じて、onlyXXCerts の確認又は、iDP.distPoint.fullName の値を検証する。

表 16.2 に示される通り、現在は置換攻撃が発生しないパターンがあるにも係わらずすべてのパターンに置換攻撃に対する対策を行っている。また iDP.distPoint.fullName に値を記載する必要もないパターンに対しても値の設定を要求している。

複数ドメイン間の相互接続を行う場合、この要求は、失効リストを CRL/ARL 以外で分割を想定するドメイン側にとっては、意図しない置換攻撃のためにこの対策は残しておきたいという懸案事項になり、失効リストを分割しないドメインにとっては、置換攻撃に対する対応はオーバースペックになってしまう。

(c) 問題の所在 2：RFC3280 や X.509(2000)の範囲外の対応要求

上記、GPKI 要件 a)及び GPKI 要件 b)は、RFC3280 や X.509(2000)にその記述は見当たらない。RFC 3280 では以下のように記述されている。

> (2) If the complete CRL includes an issuing distribution point (IDP) CRL extension check the following:
>
> (i) If the distribution point name is present in the IDP CRL extension and the distribution field is present in the DP, then verify that one of the names in the IDP matches one of the names in the DP. If the distribution point name is present in the IDP CRL extension and the distribution field is omitted from the DP, then verify that one of the names in the IDP matches one of the names in the cRLIssuer field of the DP.

iDP.distPoint.fullName が設定されていれば、証明書の cRLDP.distPoint.fullName と比較することのみが規定されている。

また X.509 (2000)においては、分割しない失効リスト、CRL/ARL に分割した失効リストについては、iDP.distPoint の記述は推奨されていない(むしろ禁止されている)。

B.5.1.1 Complete CRL

In order to determine that a CRL is a complete CRL for end-entity and CA-certificates, for all reason codes of interest, the following shall be true:

- Delta CRL indicator extension shall be absent; and
- Issuing distribution point extension may be present; and
- Issuing distribution point extension shall not contain distribution point field; and
- Issuing distribution point extension shall not contain onlyContainsUserCerts field set to TRUE; and
- Issuing distribution point extension shall not contain onlyContainsAuthorityCerts field set to TRUE; and
- Issuing distribution point extension shall not contain onlyContainsAttributeCerts field set to TRUE; and
- If the reasonCodes field is present in the issuing distribution point extension, the reasons code field shall include all the reasons of interest to the application; and
- Issuing distribution point extension may or may not contain indirectCRL field (hence, this field need not be checked).

上記から、RFC3280 や X.509(2000)等の標準を参照し、自ドメインの失効リストが置換攻撃への対策を必要と感じていない相手にとって、GPKI 要件 a)及び GPKI 要件 b)は、他国のローカルな要件を採用しなければならないとの印象を与える。

(d) 問題の所在 3：分割方法の不透明性への不安

分割される失効リストのスコープ(範囲)を明確にする必要がある。現在では CRL/ARL に分割される以外のスコープが不明である[22]。このようにスコープが明確でない分割に対する置換攻撃の対策は、接続相手にとって置換攻撃の対策自身よりもスコープの不透明さが目立ってしまい、そちらの方の不安を助長している。以下に分割される失効リストのスコープに関する考察を行う。

失効リストは分割されているに係わらずどのような範囲で発行されているかを示すスコープをもっている。RFC3280 では以下のように記述されている。

[22] 理由コードでの分割は明確には規定されている

> Each CRL has a particular scope. The CRL scope is the set of certificates that could appear on a given CRL. For example, the scope could be "all certificates issued by CA X", "all CA certificates issued by CA X", "all certificates issued by CA X that have been revoked for reasons of key compromise and CA compromise", or could be a set of certificates based on arbitrary local information, such as "all certificates issued to the NIST employees located in Boulder". (p48)

失効リストのスコープには全証明書の失効リスト、CA のみの失効リスト、ある特定の理由による失効リスト、又はローカル情報に基づく失効リストなどが含まれる。失効リストを分割しなければそれがスコープであり、すべての理由コードによるすべての証明書の失効リストが含まれると仮定される。失効リストを分割するのであれば、iDP 拡張を使いスコープを明示する。CRL/ARL に分割する場合は、onlyContainsUserCerts 又は onlyContainsCACerts に値を入れることで、スコープを end-entity 又は CA に限定することができる。また、失効理由によって分割する場合は、onlySomeReasons に理由コードを入れることで対応できる。しかしながらその他の分割方法は RFC3280 では標準化されていないため、各 PKI ドメインにおいてそれぞれ定義される。相互接続時において、一方の PKI ドメインがその他の分割方法を用いている場合、他方のドメインにはどのようなスコープで失効リストの分割を行っているのかわからず、その結果、検証者に対して大きな不安や負担をしいることになってしまう可能性もある。

(e) 問題の所在 4：現在の認証局ソフトウェアの対応状況

日本を除く実証実験参加国／地域のほとんどの認証局は、認証局ソフトウェアに何らかの改造を行なければ iDP 拡張を含めた CRL の発行に対応できなかった。シンガポール及び香港は未だに対応していない。日本製の主要な認証局ソフトウェアも GPKI の仕様となっていなければ、他国と同じ状況であったと考えられる。このことは、失効リストの分割の要求がなく、分割による置換攻撃の対策も必要なかったケースや特定サービスを前提とした認証局ソフトウェアの製品開発が影響を及ぼしているのだと考えられる。したがって、国際的な複数間ドメイン相互接続を考慮した場合、iDP を必須としたプロファイルは実現性が低いと考えられる。

(f) 提言

失効リスト置換攻撃への対策の要求がある一方で、その必要がない場合も存

在する。以下に相互接続時における注意点を明確化する。

(i) 失効リスト分割形態の明確化

失効リスト分割に対する置換攻撃への対策を議論するためには、失効リスト発行及び分割形態の明確化が必要である。この時、X.509(2000)の分類方法が参考になる。X.509(2000)では、CRL を分割しない場合、CRL/ARL を分割した場合、CRL/ARL 以外で分割した場合の CRL のフィールド設定/検証要件を定義している。これに従って分割形態を明確化することが推奨される。

(ii) 条件付処理

現在、GPKI 要件 a)及び GPKI 要件 b)の要件が混在する。

RFC3280 及び X.509(2000)では、GPKI 要件 a) 及び GPKI 要件 b)は必須ではない。必須とされている要件は“もし iDP.distPoint の名前が設定されていれば、cRLDP.distPoint と比較する”であり、これは CRL/ARL 以外で分割し cRLDP を記載する場合である。複数間ドメイン相互接続を考慮した場合、この定義では、CRL を分割せず iDP.distPoint の設定を行わなくてもよいドメイン、並びに CRL/ARL に分割する失効リスト配布ポリシをもち onlyContainsUserCerts 又は onlyContainsCACerts に値を入れるドメインの相互接続を許可している一方で、特別な分割形態をもつドメインに対しては、cRLDP.distPoint と iDP.distPoint の記載と検証を要請し置換攻撃を防いでいる。したがって、上記の要求に対する現在の有効なアクションとしては、GPKI 要件 a)及び GPKI 要件 b)を、「もし iDP.distPoint の名前が設定されていれば、cRLDP.distPoint と比較する」という条件付処理に変更すべきである。

iDP.distPoint を使用しない場合は、失効リストを分割しない失効リストポリシである。CRL/ARL に分割する失効リストポリシは必ず iDP 拡張の onlyContainsUserCerts 又は onlyContainsCACerts を入れることを義務付けるべきである。そしてその失効リストは、必ず失効リストの署名検証を行う必要がある。CA エントリに格納されることが推奨されることを明記する必要があるであろう。

しかしながら、CRL/ARL による分割や理由コード以外に失効リストを分割する場合には、そのようなローカル情報に基づく分割を許可するかどうかの議論を必ず相互接続ドメイン間で行う必要がある。もし合意が取れるのであれば、必ず iDP.distPoint に配布点を明記し、cRLDP.distPoint の配布点との比較を行うべきであろう。

(g) 結論

上記より、国際間相互接続における相互運用性や実用性を考えた場合、失効リストを分割することは慎重な議論を必要とする。認証局運営ポリシとセキュリティ要件に基づく失効リスト発行/分割ポリシを明確にし、合意することが必要である。ITU-T/X.509(2000)では、CRL/ARL 以外の失効リストの分割方法をサポートするために、crlScope 拡張を新たに定義するなどの、多種多様な分割方法が議論され、標準化されようとしている。このことからも、失効リスト発行ポリシの多様化は避けられない。したがって、認証局運営者が失効リスト配布ポリシを決定する際には、適切にリスク分析及び対策を行うことが求められる。また、失効リストの配布に頼らない失効検証方法や失効検証しないアーキテクチャの検討も今後の課題となる。更に、現在は範囲外となっている OCSP の活用や、IETF での標準化が間近となっている SCVP などがポイントとなるだろう。上記提言を含め、日本 GPKI にフィードバックする必要があると考える。

(4) 既存の CA を用いて相互認証を考える場合のルート CA 証明書のプロファイル

相互接続を行う場合、お互いの接続先認証局への要件を明確にする必要がある。この要件の一部はプロファイルの形で表される。

認証局間の実証実験では、既存の民間向け認証局を相互接続することを前提条件としている。Internet Explorer や Netscape Navigator などに含まれる著名なルート認証局は V1 の自己署名証明書で運営されていることが多い。しかし、昨年度 IWG プロファイルでは V3 を要求している。

Internet Explorer や Netscape Navigator にバンドルされている証明書は古いものが多い。これらの認証局が構築された時には、V3 を必要とするサービスを認証局が行っていなかったり、V3 証明書が成熟した技術として認められていなかったりしたため、主に V1 が用いられたと考えられる。

CC を行う時に keyRollOver を考えると V3 であることが必要となる。keyRollOver 時には、新旧の証明書の DN は同じで鍵ペアだけを更新するために、KeyID による証明書の区別が必要となるからである。keyRollOver は高度なセキュリティを保つには必要な運用である。

認証局間の実証実験では keyRollOver を前提として、ルート CA 証明書のプロファイルを V3 と規定している。ただし、セキュリティ要件が低い場合、V3 の証明書を持ったルート認証局を新たに構築するコスト、及び、既存の認証局の相互接続を考慮すると、ルート認証局証明書が V1 でも対応できるアーキテクチャが必要となるだろう。このことは今後の検討課題である。

(5) cRLDP(iDP)内の LDAPURI における attribute、及び binary オプションの有無

証明書検証アプリケーションの相互運用性を保つために、プロファイルにおいて、cRLDP(iDP).distPoint.fullName に LDAPURI を記載する場合の Attribute 及び binary オプションの有無について明確にする必要がある。

RFC2255 によると、LDAPURI における attribute 及び binary は記載してもしなくてもよい。そこで、cRLDP(iDP)内の LDAPURI における attribute 及び binary の有無について、標準仕様を検討し、既存アプリケーションの実装を検証することにより、実用的なプロファイルについて考察する。

(a) binary オプションの記載について

データを LDAP サーバに格納する際、及びデータを LDAP サーバから取り出す際にそのデータがバイナリであることを示す binary オプションが LDAPv3 より定義された。また、RFC2256 の記述に従うと、失効リストをサーバへ格納する時には binary を指定しなければならない。

5.40. certificateRevocationList
This attribute is to be stored and requested in the binary form, as 'certificateRevocationList;binary'.
(2.5.4.39 NAME 'certificateRevocationList'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.9)
5.41. crossCertificatePair
This attribute is to be stored and requested in the binary form, as 'crossCertificatePair;binary'.
(2.5.4.40 NAME 'crossCertificatePair'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.10)

しかし、各ベンダーのサーバ及びクライアントソフトウェアの実装がまちまちになっているために、binary オプションの有無によってデータの取得ができない場合がある。また、バージョン 2 準拠の LDAP サーバで運用されている場合には、binary オプションを理解できずに、データの取得ができなくなる。以下に各ベンダーによる実装状況について調査し、サーバの仕様及びクライアントの仕様について考察する。

(b) データ格納時及びデータ取得の際の binary オプションの有無によるサーバ及びクライアントの振るまい

サーバへの登録時の binary 指定の有無、サーバへのリクエスト時の binary 指定の有無による、レスポンス時のサーバによる binary 指定の付与、クライ

アントにおけるハンドリングについて、実際に利用されている製品を使用し、以下のような結果を得た。

表 16.3　サーバ及びクライアントの振るまい

サーバ製品名	サーバへの格納時の指定	リクエスト	レスポンス	CRL の扱い
サーバ A	binary 指定あり	binary 指定あり	binary あり	OK
		binary 指定無し	binary あり	OK
	binary 指定無し	binary 指定あり	取得不可	
		binary 指定無し	binary 無し	OK
サーバ B	binary 指定あり	binary 指定あり	binary あり	OK
		binary 指定無し	binary 無し	OK
	binary 指定無し	binary 指定あり	binary あり	OK
		binary 指定無し	binary 無し	OK
サーバ C[23]	binary 指定あり	binary 指定あり	binary あり	OK
		binary 指定無し	binary あり	OK

サーバへの格納時の指定、リクエストにおいて binary 指定を行った場合には、レスポンスも binary 指定されており、すべて正しくデータが取得されている。これは仕様どおりである。サーバへの格納時に binary 指定を行うが、リクエスト時に binary 指定を行わなかった場合には、サーバ側のレスポンスは一意ではなかった。サーバへの格納時に binary 指定を行わなかった場合には、データの格納ができない場合や、データの取得ができない場合もあった。

LDAP の次世代の仕様策定を行っている ldap-bis メーリングリスト[24]では、binary 指定が相互運用性を低下させるとの意見も出され、binary 指定の必要性に関して活発に議論されている。

以上より、失効リストをサーバへ格納する時の binary 指定は推奨されるが必須とはしない。また、実験結果では、binary の指定の有無によってデータの取得には変化が見られなかったものの、クライアントがサーバへリクエストを行う時には binary 指定を行うことが推奨される。

(c) attribute の記載について

attribute は LDAP サーバ上におけるデータの TYPE（種別：証明書、CRL、相互証明書ペアなど）を表す。CRL の在処を示す cRLDP 及び iDP においては

[23] サーバ C では binary 無しでのデータの格納はできなかった。

[24] http://www.openldap.org/lists/ietf-ldapbis/

データ種別が自明であるために attribute は記載しなくてもよいはず[25]であるが、アプリケーションの実装によっては attribute を明示する必要がある。また、attribute を明示するとアプリケーションの負荷軽減につながる。実際に利用されているクライアント製品を使用し、attribute の指定の有無によるクライアントソフトウェアの動作について、以下のような結果を得た。

表 16.4　クライアントソフトウェアの動作

クライアント製品名	cRLDP における attribute の指定	リクエスト	CRL の取得
クライアント A	あり	attribute あり	OK
	無し	attribute 無し	OK
クライアント B	あり	attribute あり	OK
	無し	attribute 無し	NG[26]

attribute の指定をした場合には、双方ともに失効リストを取得できたが、指定をしなかった場合には、失効リストを取得できなかった。

したがって、attribute は記載することが推奨される。

(d) 結論

前節の結果から考察すると、すべてのクライアントでの動作を保証するために、cRLDP(iDP)に LDAPURI を記載する場合には、attribute は必須、binary は任意に記載することが推奨される[27]。ただし、証明書検証ソフトウェアは、attribute;binary の記載にかかわらず、必要な失効リストを取得し失効検証できなければならない。

また、binary の付与については IETF の PKIX-ML において議論の最中であり、この議論の行方も注意深くウォッチしていく必要がある。

(6) serialNumber、cRLNumer の数字の範囲について

証明書検証アプリケーションの相互運用性を保つために、証明書プロファイルにおいて INTEGER と指定している場合の値域について明確にする必要がある。ここでは、特に serialNumber,cRLNumer について考察する。

今年度の実証実験において、チャイニーズ台北側の cRLNumber の値を、日本側アプリは正しく扱うことができなかった。一般的に ASN.1 の型として

[25] 当該証明書の basicConstraint 領域を参照して、認証局証明書であれば ARL を、EE 証明書であれば CRL を取得することが可能である（ARL がなかった場合には CRL を取得する）。ただし、この処理を行うかどうかは標準化されておらず、アプリケーションの実装による。

[26] 該当するエントリに失効リスト以外の値が多数入っていた場合

[27] ldap://example.tld[:portnumber]/?dn?attribute[;binary]

INTEGER を指定されると、実装時に言語の仕様としての整数型を指定されてしまうことが多く、相互運用性を低下させる要因となっている。今回の実験においてもそれが原因と考えられる。

また、昨年度の IWG 仕様策定時における標準仕様であった RFC2459 では、特に値域に関する指定はなく、昨年度実験参加各国における認証局ソフトウェアの実装状況から 16 オクテットまでとしていた。しかし、2002 年 4 月に策定された RFC3280 では 20 オクテットまでは扱えるべきであるとしている。また、現在、複数のメジャーな認証局が 20 オクテット長の serialNumber を利用している。

以上より、IWG プロファイルとして、serialNumber 及び cRLNumer は 20 オクテットを扱えるようにすることを推奨する。

(7) DN 中の″,″の扱いについて

証明書検証アプリケーションの相互運用性を保つために、LDAPURI 中における正しい「,」の扱いについて、明確にする必要がある。

今年度の実験において、チャイニーズ台北側は cRLDP に「,」を含む Distinguished Name を LDAPURI を用いて指定[28]したが、アプリケーションテストにおいて、日本のアプリケーションはこれを正しく認識できなかった。以下に、標準仕様から導き出される正しい「,」の扱い方及び相互運用性について考察する。

(a) 標準仕様における LDAPURI 中の「,」の扱いについて

LDAPURI の仕様は、RFC2255 によると以下の通りである。

> The dn is an LDAP Distinguished Name using the string format described in [1]. It identifies the base object of the LDAP search.
>
> ldapurl = scheme "://" [hostport] ["/"
> [dn ["?" [attributes] ["?" [scope]
> ["?" [filter] ["?" extensions]]]]]]
>
> [1] Wahl, M., Kille, S., and T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC 2253, December 1997.

ここで、上記引用によると dn は RFC2253 の記述に従って記述される。

したがって、ディレクトリ上のデータを URI で指定するには、指定したいデ

[28] ldap://pkiiwg.chttl.com.tw/cn=CRLforPhase2,ou=Test%20Root%20CA,ou=PKI%20IWG,o=Chunghwa%20Telecom%20Co.%5C,%20Ltd.,c=TW?certificateRevocationList

ータの Distinguished Name を RFC2253 の記述に従って LDAP String 表記とし、それを URI に変換するという２段階のステップを踏む必要がある。それぞれのステップについて、以下の例を用いて検証する。

例：

Country Name = JP

Organization name = ABC Co., Ltd.

この例を RFC2253 に従って記述すると、「,」をデリミタ(区切り文字)と区別するために、エスケープしなければならない。したがって、以下の通りとなる。

1. o=ABC Co.¥2c Ltd., c=JP
2. o=ABC Co.¥, Ltd., c=JP
3. o=”ABC Co., Ltd.”, c=JP

これをさらに RFC2255 に従って URI に変換すると空白文字及び「＼」、「”」は予約文字であるためにエスケープしなければならない。したがって、以下の通りとなる。

1'. ldap://example.tld/o=ABC%20Co.%5c2c%20Ltd., c=JP
2'. ldap://example.tld/o=ABC%20Co.%5c, %20Ltd., c=JP
3'. ldap://example.tld/o=%22ABC%20Co.,%20Ltd.%22, c=JP

ここで、注意すべきは、2’及び 3’中に現れるエスケープされていない、RDN の区切りでない「,」の扱いについてである。RFC2396 によると、区切り文字でない「,」は%2c とエスケープしなければならないとある。この部分のみを読むと%2c とエスケープしなければならないと誤解しがちである。しかし、この「,」は RDN の区切り文字であり、URI のコンポーネントの区切り文字ではないので、エスケープする必要はない[29]。

(b) アプリケーションにおける LDAPURI 中の「,」の扱いについて

実用性の面から「,」の扱いについて、明確にする必要がある。LDAPURI における「,」の正しい表記方法が明確になっても、それを既存のアプリケーションが扱えなければ意味がないからである。そこで、以下に示すリクエストに対して実際利用されている製品がどのように振る舞うのかを検証した。LDAP クライアントは Netscape Navigator 及び検証局を用い、いずれの場合も同じ結果を得た。

[29] する必要はないだけで、エスケープしてもよい。

表 16.5　サーバへのリクエスト

(a)	ldap://example.tld/o=Chunghwa%20Telecom%20Co.%5C2c%20Ltd.,c=TW
(b)	ldap://example.tld/o=Chunghwa%20Telecom%20Co.%5C,%20Ltd.,c=TW
(c)	ldap://example.tld/o=%22Chunghwa%20Telecom%20Co.,%20Ltd.%22,c=TW

表 16.6　サーバからのレスポンス

	サーバ A	サーバ B	サーバ C
(a)	OK	NG (0x20 no such object)	OK
(b)	OK	OK	OK
(c)	OK	OK	OK

以上より、利用するディレクトリサーバによっては、期待通りに「,」を扱えない可能性があることがわかる。

(c) 結論

「,」を LDAPURI 中に含めなければならない場合には、事前に注意深く動作確認をすることが必須となる。これらの「,」に代表される予約文字として利用される頻度の高い文字については仕様の理解が難しいが、LDAPURI 中に「,」を利用しなければならない頻度は非常に高い[30]。したがって、サーバ及びクライアントはこれらのすべてに対して対応できているべきである。また、仕様書においてもよりわかりやすい記述が求められる。

実際に利用する場合には、現在の標準仕様に従った(a)又は(b)の利用が望ましい。アプリケーションの実装によっては利用できない場合もあるので、その場合には(c)の利用も検討する必要がある。

(8) distinguishedName のエンコード方法について

RFC3280 においては、2003 年 12 月 31 日以降に発行する証明書については、UTF8String を用いることとしている。RFC3280 は以下のように記述する。

The UTF8String encoding [RFC 2279] is the preferred encoding, and all certificates issued after December 31, 2003 MUST use the UTF8String encoding of DirectoryString (except as noted below).

この期限が迫る現在、プロファイルとしてどうすべきかを考察する。

本年度実証実験において、香港チャイナ側は UTF8String を利用できなかったため、日本－香港チャイナ間においてはすべての属性について PrintableString を利用した。このことは、country 属性以外は UTF8String を用いることとして

[30] 本文中の例にも取り上げたが、企業名など、名称に「,」を用いる場合が多いため。

いるIWGプロファイルの推奨値に違反している。

しかし、現在、実際に運営されている認証局において利用されている認証局ソフトウェアのいくらかは、UTF8String が推奨される以前から稼動しておりUTF8Stringを利用できないことは事実である。 また、現在一般に広く利用されているOSやクライアントアプリケーションの一部においても同様である。上記の様なアプリケーションをすべてUTF8String対応とするには、大変な費用と労力がかかることは明白である。また、仕様を策定する場合、様々なレガシーアプリケーションに対する配慮は重要である。

ここで、PrintableStringと UTF8Stringが混在した場合のDNのマッチングルールについて注意しなければならない。PrintableString と UTF8Stringが混在した場合、すべてのアプリケーションにおいて正しく期待された通りにマッチングするとは限らない。DN のマッチングルールについては、非常に様々な仕様が絡み合っており、すべてのアプリケーションの実装者が正しく理解しているとは限らないからである。マッチングルールの詳細については、16.2.2(1)DN のMatchingRuleに考察されている通りである。

したがって、IWGプロファイルとしては、UTF8Stringを推奨するものの、レガシーアプリケーションに対する配慮としてやむを得ない場合にはPrintableStringを許可することが望ましい。ただし、DNのcountry属性以外にPrintableString を用いる認証局と相互接続を行う場合には、事前にアプリケーションの動作について注意深く検証することが必要となる。

そもそも、DN は、氏名や組織名などを含むため多言語表記が望まれるフィールドである。そのため DN には ASCII を維持し、多言語をサポートするキャラクターセットをサポートするエンコーディング方法を採用するのが望ましい。UTF8は、現行のASCIIキャラクターセットを維持し既存のレガシーシステムとの互換性を保ちながら、国際化にも対応できるため、RFC2277 において IETFで広く推奨されている。したがってPKIの世界においてもRFC3280においてもDNのエンコーディング方式にはUTF8Stringが推奨されている。

しかしながら、上記にもあるが PrintableString からの移行は、クライアントアプリケーションや CA アプリケーション対応状況及びアプリケーション修正/再発行/再配布の費用対効果などの経営判断から移行が進まないことが予想される。特にブラウザ等のUTF8String対応状況などは民間CAの意思決定に大きく影響を与える。

典型的なPKI(SSL)クライアントであるWebブラウザなどでは、必ずしもすべてのユーザが最新版を使っているわけではなく、そのためUTF8Stringを処理できない問題は当分続くと思われる。

プロファイルの設計を行うためには、PKIシステム稼動環境下において、あるべき理想と予想される問題を想定しながら対応していかなければならない。IWGプロファイルの場合、UTF8String をサポートし多言語表記の可能性を確保する

べきであるが、民間の CA 製品やアプリケーションなどレガシーシステムが UTF8String への移行を妨げる可能性が高い。また、複数国の取引において有効なキャラクターセットは ASCII 表記と判断されることが多いと考えられるため PrintableString が使用される場合があるであろう。したがって、現在は PKI アプリケーションにおいて PrintableString 及び UTF8String が混在する状況を想定した DN マッチングルールを明確にする必要がある。

16.2.2 パス検証テストガイドライン

(1) DN の MatchingRule

本ガイドラインでは、認証パスの name chain (ある証明書の issuer と、その証明書を発行した CA 証明書の subject が一致していること)を確認する際の DN の一致規則として、次の 2 つの要件を含んでいた。

- The RP should determine that the names are different when they differ by whitespace in values other than countryName.
- The RP should determine that the names are different when they differ by capitalization in values other than countryName.

これは、RFC3280 4.1.2.4 にある以下の記述から判断したものである。

> This specification requires only a subset of the name comparison functionality specified in the X.500 series of specifications. Conforming implementations are REQUIRED to implement the following name comparison rules:
>
> (a) attribute values encoded in different types (e.g., PrintableString and BMPString) MAY be assumed to represent different strings;
>
> (b) attribute values in types other than PrintableString are case sensitive (this permits matching of attribute values as binary objects);
>
> (c) attribute values in PrintableString are not case sensitive (e.g., "Marianne Swanson" is the same as "MARIANNE SWANSON"); and
>
> (d) attribute values in PrintableString are compared after removing leading and trailing white space and converting internal substrings of one or more consecutive white space characters to a single space.

つまり、DirectoryString 型の属性値のエンコードに UTF8 を使用している IWG のプロファイルでは、属性値を比較する際にはアルファベットの大文字小文字を同じ文字として扱ったり、文字列の先頭や後尾の空白や連続する空白の処理を行わないものとしている。

しかし、RFC3280 4.1.2.4 にはまた、次のような記述がある。

> Note that the comparison rules defined in the X.500 series of specifications indicate that the character sets used to encode data in distinguished names are irrelevant. The characters themselves are compared without regard to encoding. Implementations of this profile are permitted to use the comparison algorithm defined in the X.500 series. Such an implementation will recognize a superset of name matches recognized by the algorithm specified above.

これは、X.500 シリーズに規定された一致規則を実装した場合、RFC3280 で規定された一致規則のスーパーセットを実装しているとみなし、RFC3280 準拠としてもよい、と読むことができる。では、X.500 シリーズで定義されている DN の一致規則とはどのようなものなのか。

ITU-T X.501 (1993 E)の 12.5.2 には、DN と、それと同様の SYNTAX をもつ属性に使用できる distinguishedNameMatch という一致規則が定義されている。

> The **distinguishedNameMatch** is defined as follows:
>
> **distinguishedNameMatch MATCHING-RULE ::= {**
> **SYNTAX DistinguishedName**
> **ID id-mr-distinguishedNameMatch }**
>
> A presented distinguished name value matches a target distinguished name value if and only if all of the following are true:
>
> a) the number of RDNs in each is the same;
>
> b) corresponding RDNs have the same number of AVAs;
>
> c) corresponding AVAs (i.e. those in corresponding RDNs and with identical attribute types) have attribute values which match for equality (in such a match, the attribute values take the same roles – i.e. as presented or target value – as the distinguished name which contains them in the overall match).

つまり、2 つの DN が一致しているための条件は、

- 2 つの DN が持つ RDN の数が同じであること
- 2 つの DN 中の、対応する RDN が同じ数の AVA を持つこと
- 対応する AVA が同じ属性値を持つこと

の 3 つである。対応する RDN とは、それぞれの DN 中の順番が同じ RDN のことであり、対応する AVA とは、対応する RDN 中の同じ属性型を持つ AVA のことである。

ITU-T X.501 (1993 E)にある属性の定義によれば、AVA 中の属性値の比較には属性毎に定められている一致規則を使用する。つまり、属性値が PrintableString であろうと UTF8String であろうと、属性によって定められた一致規則を使用するのである。

RFC3280 に挙げられている扱うことができなければならない属性、扱うことができるべき属性を例に考えてみると、それらの属性はすべて caseIgnoreMatch という一致規則を使用するものである。

caseIgnoreMatch は、ITU-T X.520 (1993 E)に以下のように定義されている。

6.1.1 Case Ignore Match

The *Case Ignore Match* rule compares for equality a presented string with an attribute value of type **DirectoryString**, without regard to the case (upper or lower) of the strings (e.g., “Dundee” and “DUNDEE” match).

caseIgnoreMatch MATCHING-RULE ::= {
SYNTAX DirectoryString {ub-match}
ID id-mr-caseIgnoreMatch }

The rule returns TRUE if the strings are the same length and corresponding characters are identical except possibly with regard to case.

Where the strings being matched are of different ASN.1 syntax, the comparison proceeds as normal so long as the corresponding characters are in both character sets. Otherwise matching fails.

これによれば、大文字小文字の区別は行わない。さらに、ASN.1 の SYNTAX によらずどちらの文字セット内でも使用できる文字を使っている限り、比較は正常に行われる。

さらに、空白に関する記述が以下のようにされている。

6.1 String matching rules

In the matching rules specified in 7.1.1 through 7.1.11, the following spaces are regarded as not significant:

- leading spaces (i.e., those preceding the first printing character);
- trailing spaces (i.e., those following the last printing character);
- multiple consecutive internal spaces (these are taken as equivalent to a single space character).

In the matching rules to which these apply, the strings to be matched shall be matched as if the insignificant spaces were not present in either string.

これによれば、属性値の比較をする際は先頭と後尾の空白を無視し、文字列中の 2 つ以上連続する空白は単一の空白とみなさなければならない。

以上のことから、例えば commonName の属性値"IWG"と"iwg"と" IWG"があった場合、X.500 シリーズ準拠の一致規則では文字列のエンコードタイプによらずすべて一致することになるが、RFC3280 に挙げられている一致規則を使用すると、すべて PrintableString でない限り、同じものとしては扱われない。

RFC3280 にある X.500 シリーズに規定されている一致規則とは、各属性の定義を知っていて、DirectoryString の採りうる文字列のエンコードと文字セットを正しく処理できなくては実装できない。

この敷居を下げるという意味では、RFC3280 に定義されている一致規則は有用であると言えるが、一方でディレクトリや他のアプリケーションとの連携という点で問題になる可能性があったり、単純なオペレーションミスで大文字を小文字にしてしまっただけでも認証パスの検証に失敗してしまうこともありうる。

RFC3280 で規定されている一致規則は、確かに RFC3280 という標準準拠であるパス検証アプリケーションの実装を容易にするが、文字列の一致条件としては厳しすぎるものであると言える。

(2) AKID と SKID のチェーン

本ガイドラインには、証明書の AuthorityKeyIdentifier 拡張の中の keyIdentifier と、その証明書を発行した CA 証明書に含まれる SubjectKeyIdentifier が一致していなくてはならない、という要件がある。これは、セキュリティ的な問題によるものではなく、主にパス構築の効率に係わるものである。

簡単な例として、図 16.4 のような場合について考えてみる。

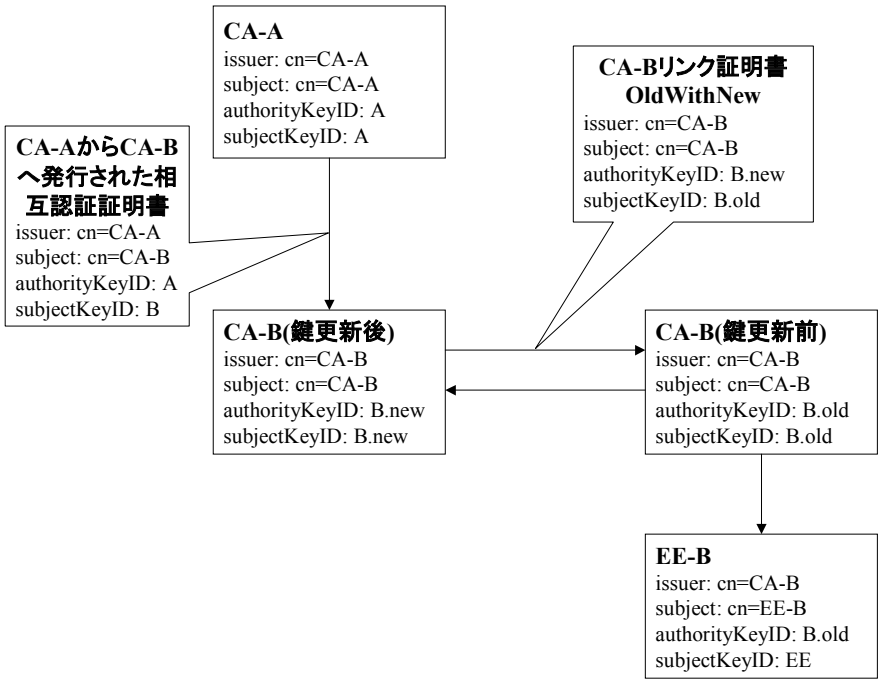


図 16.4　鍵更新時の keyID のチェーン

CA-A をトラストアンカとするドメインの RP が EE-B の証明書を検証しようとして、順方向にパスを構築していく場合、name chain のみをチェックしてパスを構築すると、余計なパスの検証が発生してしまう可能性がある。正しいパスは CA-A、CA-A から CA-B へ発行された相互認証証明書、CA-B リンク証明書(OldWithNew)、EE-B であるが、CA-A、CA-A から CA-B へ発行された相互認証証明書、EE-B というパスでも name chain はたどれてしまう。

パス検証アプリケーションが正しいパスを見つけるまで、パス構築が繰り返される、という実装がなされている場合には、単に効率が悪くなるだけで済む。しかし、誤ったパスを検証し、検証に失敗した時点で EE-B の証明書が信用できないものとしてしまう実装もあるかもしれない。

keyIdentifier のチェーンのチェックは、例のようにパス構築に失敗することを避け、効率よくパスの検証を行うための要件であるが、この要件をパス検証の必須要件とする場合には十分注意しなくてはならない。というのも RFC3280 には、keyIdentifier の求め方について 2 つの方法を推奨してはいるものの強制はしておらず、CA 証明書中の subjectKeyID とその CA が発行した証明書の authorityKeyID 中の keyID が一致していなくてはならない、とだけ記述されている。単一ドメインでの運用を考える場合には、確かに問題が無いかもしれないが、既存の PKI ドメイン間の相互運用という観点から考えると問題がある。

例えば図 16.4 の場合に、CA-A のドメインと CA-B のドメインで keyID の求

め方が異なっていたとする。CA-A、CA-B のそれぞれのドメイン内では問題なく“CA 証明書中の subjectKeyID とその CA が発行した証明書の authorityKeyID 中の keyID が一致していなくてはならない”という条件を満たしている。しかし、CA-A が CA-B に発行した相互認証証明書の中の subjectKeyID と、CA-B が発行したリンク証明書 OldWithNew の中の authorityKeyID の値は一致しなくなってしまう。このような場合に keyID の一致をパス検証の必須要件としていた場合には、当然パスの検証に失敗する。

このような状況を避け、keyID の一致をパス検証の要件とするには、

- keyID の求め方の標準を規定する
- 少なくとも異なるドメインと相互認証を行う際には、相互認証証明書発行要求に keyID を含め、keyID を含んだ相互認証証明書発行要求に対して証明書を発行する際には、含まれている keyID を subjectKeyID に設定して証明書を発行できる、という仕様を標準とする

以上 2 つのうちどちらかが必須であると考えられる。

ただし後者の場合では、subjectKeyID の一意性が保障できなくなってしまう可能性があり、前者がより好ましいといえるだろう。

⑶ iDP.fullname と cRLDP.fullname について

iDP を解釈できないパス検証アプリケーションは、iDP がセットされている CRL からしか失効情報を取得できない場合には、その証明書を含むパスの検証に失敗しなくてはいけない。

というのは、iDP はその CRL がどの証明書に関する失効情報を持っているかを示すものであり、ある証明書の有効性を確認するためには、その証明書に関する失効情報を取得し失効しているかいないのかを確認する必要があるからである。

CA 側の観点から見れば、iDP をサポートするかしないかは発行する CRL の形態に依存する決め事の問題であるが、パス検証という観点から見れば、特に異なるドメイン間の相互運用を視野に入れれば iDP を正しく処理できないというのは致命的な問題になるだろう。

あるドメインでは完全 CRL を発行しているが、異なるドメインでは CRL を分割して発行し完全 CRL を発行していない、という場合も考えられる。この場合、前者のドメインのみで使用されるパス検証アプリケーションについては iDP の解釈は必須ではないが、後者のドメインでは iDP.distPoint の解釈が必須要件になる。この例の場合、iDP.distPoint は、その CRL がどこで公開されているものかを単純に示すだけのものではなく、その値を cRLDP に持つ証明書についての失効情報を確かに持っている CRL、ということを示すことのできる重要な情報であるためである。

本ガイドラインでは失効モデルとして、大きく CRL モデルのみを定義してい

るため iDP.distPoint に関するテスト項目をレベル 2 としているが、今後 CRL の発行ポリシに応じて CRL モデルをさらに細分化し、それぞれについてテストケースを作成する必要があるだろう。

(4) 自己署名証明書の検証

パス検証において自己署名証明書の検証の必要性については、その方法等において X.509(2000)[31]及び RFC3280[32]に明確な記述がない。このことは、異なる PKI ドメイン間における証明書検証アルゴリズムの実装において相違を生じさせる要因となる。この現状を踏まえ、技術面及びポリシ面等を含め、相互運用性を高める観点からも自己署名証明書の検証の必要性について共通の認識が必要であると考える。ここでは、自己署名証明書の検証の必要性について考察する。

(a) 検証の必要性

自己署名証明書が認証パスに含まれるかどうかを確認するために、X.509(2000)及び RFC3280 を参照する。

X.509(2000)における、自己署名証明書に関する記述を以下に示す。

> 8.1.5 Self-issued certificates
> There are three circumstances under which a certification authority may issue a certificate to itself:
> a) as a convenient way of encoding its public key for communication to, and storage by, its certificate users;
> b) for certifying key usages other than certificate and CRL signing (such as time-stamping); and
> c) for replacing its own expired certificates.
> These types of certificate are called self-issued certificates, and they can be recognized by the fact that the issuer and subject names present in them are identical. For purposes of path validation, self-issued certificates of type a) are verified with the public key contained in them, and if they are encountered in the path, they shall be ignored.

(X.509(2000)「8.1.5 Self-issued certificates」より抜粋)

自己署名証明書は自己発行証明書(Self-issued certificates)に包含される。X.509(2000)においては、自己署名証明書は、上記 a)、b)、c)の中の a)にあたり認証パスに含まれた場合、検証する必要性は明記されていない。

---

[31] ITU-T Recommendation X.509 - Information technology - Open Systems Interconnection - The Directory: Authentication Framework, 03/2000

[32] Internet Request For Comments (RFC) 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

次に、RFC3280 における認証パスを構築する証明書に関する記述を以下に示す。

When the trust anchor is provided in the form of a self-signed certificate, this self-signed certificate is not included as part of the prospective certification path. Information about trust anchors are provided as inputs to the certification path validation algorithm (section 6.1.1).

(RFC3280「6.1 Basic Path Validation」より抜粋)

このように、RFC3280 においては、トラストアンカが自己署名証明書の場合、認証パスに含まれず、自己署名証明書を検証する必要性が明記されていない。

しかしながら、この事実から自己署名証明書をトラストアンカとして無条件に受け付けると結論付けることはできない。 なぜならば、自己署名証明書の記載事項は、適切な認証パスの検証の前提となる初期の入力情報となるからである。この入力情報の信頼性を保証しないと適切な認証パスの検証ができない恐れがあり、根本的に検証結果の過ちを引き起こす可能性がある。

X.509(2000)における、認証パス検証処理の入力情報に関する記述を以下に示す。

The inputs to the certification path processing procedure are:

a) a set of certificates comprising a certification path;

NOTE – Each certificate in a certification path is unique. A path that contains the same certificate two or more times is not a valid certification path.

b) a trusted public key value or key identifier (if the key is stored internally to the certification path processing module), for use in verifying the first certificate in the certification path;

c) an initial-policy-set comprising one or more certificate policy identifiers, indicating that any one of these policies would be acceptable to the certificate user for the purposes of certification path processing; this input can also take the special value any-policy;

d) an initial-explicit-policy indicator value, which indicates if an acceptable policy identifier needs to explicitly appear in the certificate policies extension field of all certificates in the path;

e) an initial-policy-mapping-inhibit indicator value, which indicates if policy mapping is forbidden in the certification path;

f) an initial-inhibit-policy indicator value, which indicates if the special value anyPolicy, if present in a certificate policies extension, is considered a match for

any specific certificate policy value in a constrained set; and

g) the current date/time (if not available internally to the certification path processing module).

(X.509(2000)「10.1　Path processing inputs」より抜粋)

このように X.509(2000)では、パス構築及び検証処理に必要な入力情報として上記の a)～g)の 7 つを規定している。

次に、RFC3280 における、認証パス検証処理の入力情報に関する記述を以下に示す。

(d) trust anchor information, describing a CA that serves as a trust anchor for the certification path. The trust anchor information includes:

(1) the trusted issuer name,

(2) the trusted public key algorithm,

(3) the trusted public key, and

(4) optionally, the trusted public key parameters associated with the public key.

The trust anchor information may be provided to the path processing procedure in the form of a self-signed certificate. The trusted anchor information is trusted because it was delivered to the path processing procedure by some trustworthy out-of-band procedure. If the trusted public key algorithm requires parameters, then the parameters are provided along with the trusted public key.

(RFC3280「6.1.1　Inputs」より抜粋)

このように RFC3280 では、パス構築及び検証処理に必要な入力情報として上記の(1)～(4)の 4 つを規定している。そして、これらの入力情報は、トラストアンカとして指定される証明書によって提供される。

パス検証処理を適切に行うために、X.509(2000)及び RFC3280 で規定されているこれらの入力情報は信頼されている必要がある。パス検証における入力情

報の信頼性は、最低限自己署名証明書を受け入れる時に適切なトラストアンカとして登録され、常に管理されていることから得られる。またユーザが検証毎にトラストアンカをチェックしたいという要件も存在するかもしれない。そのときには、パス検証処理を実行する時のトラストアンカチェックが必要であろう。

(b) 検証すべき項目

検証すべき項目とその理由を以下に示す。

(i) issureDN と subjectDN の一致性の検証

自己署名証明書であることを確認するためにこの事項を検証してもよい。むしろここでの本質は、入力情報である証明書を「信用される発行者(トラストアンカ)」として扱ってよいかのチェックである。それが満たされるのであれば、issuerDN と subjectDN のチェックを行ってもよい。両者のトラストアンカが自己署名証明書のみの場合このチェックは有効かもしれない。ただし RFC3280 においてもトラストアンカは自己署名証明書であることは明言されていない。したがって本チェックは行われる必要であるかどうかは議論の余地がある。ここでは最低限自己署名証明書をトラストアンカであると受け付けた場合、又は再確認を必要とする場合、ユーザによる DN の確認は必要になるであろう。

(ii) 有効期間の検証

最低限自己署名証明書をトラストアンカであると受け付けた場合、又は再確認を必要とする場合、その証明書が有効であることを確認しなければいけない。パス検証に関して、そもそも自己署名証明書が有効でない期限というのは、自己署名証明書が発行したすべての証明書が有効でないと考えるのが本質である。しかしながら誤ってリポジトリの中に失効した証明書がある場合に、パス構築してしまう可能性もあるが、最終的にはパス検証中にエラーになる。従って、自己署名証明書の有効期限の検証は必ずしも行わなくてもよい。

(iii) 署名検証

最低限自己署名証明書をトラストアンカとして受け付ける時、又は再確認を必要とする場合、自己署名証明書の公開鍵と秘密鍵の結びつきを確認するために必要である。これは、入力情報である「信用される公開鍵アルゴリズム」「信用される公開鍵」として扱ってよいかの検証でもある。これは上記 RFC3280 の引用にも記述されている。

(c) 結論

自己署名証明書の検証をトラストアンカの初期入力情報の確認と考えると、その入力情報が信頼されるかどうかを決定するための必要な要素となり得る。しかしながら現在では、入力情報の信頼性の確保は理解されているが、自己署名証明書の検証までパス検証処理として行う事は記述されていない。むしろそれは個々の PKI ドメインのポリシに依存すると思われる。複数間ドメイン相互接続を考える時には、最低限トラストアンカとして受け入れた時点での検証、及びトラストアンカとしての自己署名証明書の安全な配布方法に関して明確にする必要がある。

(5) 下位認証局証明書の格納エントリと属性

本実験では、相互認証を行う PKI ドメインが階層モデルを取っている場合がテストケースとして存在した。実際に PKI ドメイン間で相互認証を行う場合にも、個々の PKI ドメインが階層モデルとなることは多い。このような際に考慮すべき点の一つとして、同じ PKI ドメイン内の上位認証局から証明書の発行を受けた下位認証局証明書のリポジトリへの格納場所が挙げられる。

証明書の格納場所が問題なのは、認証パス構築に必要な証明書の取得先としてリポジトリを機能させるためである。以下、認証パス構築の観点から下位認証局証明書のリポジトリへの格納について考察を行う。

(a) 標準の規定

X.509[33]では認証局証明書が格納されるべき属性として、認証局のディレクトリエントリの cACertificate と crossCertificatePair の issuedToThisCA 及び issuedByThisCA の 3 つが以下のそれぞれの用途で規定されている。

1. caCertificate 属性
   自己発行証明書、あるいは同じ認証ドメインの認証局から当該認証局に対して発行された証明書
2. crossCertificatePair 属性の issuedToThisCA
   自己発行証明書を除いて当該認証局に対して発行されたすべての証明書
3. crossCertificatePair 属性の issuedByThisCA
   当該認証局から他の認証局へ発行された証明書のサブセット。

X.509 の記述は以下の通りである。

[33] ITU-T Recommendation X.509 “Information Technology—Open Systems Interconnection—The Directory: Public Key and Attribute Certificate Frameworks, March 2000 (equivalent to ISO/IEC 9594-8, 2000).

11.2.2 CA certificate attribute

The cACertificate attribute of a CA's directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA. In the case of v3 certificates, these certificates shall include a basicConstraints extension with the cA value set to TRUE. The definition of realm is purely a matter of local policy.
[snip]

11.2.3 Cross certificate pair attribute

The issuedToThisCA elements of the crossCertificatePair attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the issuedByThisCA elements of the crossCertificatePair attribute, of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs. If a CA issues a certificate to another CA, and the subject CA is not a subordinate to the issuer CA in a hierarchy, then the issuer CA shall place that certificate in the issuedByThisCA element of the crossCertificatePair attribute of its own directory entry.
[snip]

ここで下位認証局証明書を cACertificate 属性に格納すべきことは明記されている。さらに検討すべきは crossCertificatePair 属性に格納すべきか否かであるが、crossCertificatePair 属性の issuedByThisCA については下位認証局証明書を除く旨の記述がある。issuedToThisCA については明示的な記述はなく、格納対象として想定されていると解釈される。

“Understanding Certification Path Construction"[34] では cACertificate 属性、crossCertificatePair 属性の用途について X.509 とほぼ同様の記述をした上で、特に下位認証局については cACertificate と crossCertificatePair 属性の issuedToThisCA の両方への格納を以下のように提案している。これは、realm の定義が X.509 でなされておらず認証局のポリシ依存であり cACertificate に格納される範囲が明確でないことの安全策としてである。

[34] PKI Forum white paper “Understanding Certification Path Construction” September 2002

we would expect to see the issuedToThisCA element of the cross-certificate pair attribute to be populated with certificates that have been issued to this CA by other CAs. (This suggests that both the cACertificate and issuedToThisCA might be populated when the issuing CA is in the same realm as the issued to CA.)

(b) 認証パス構築のための証明書の取得

リポジトリをパス構築時の証明書の取得先とした場合の要件について、以下に検証する。

認証パス構築は、順方向パス構築、逆方向パス構築の 2 通りに大別される。順方向パス構築とは、検証者のトラストアンカを基点として署名者証明書へ向かって証明書チェーンを構築するものであり、逆方向パス構築とは、この逆に署名者証明書から検証者のトラストアンカへ向かうものである。

順方向パス検証、逆方向パス検証それぞれの場合で、必要な証明書を格納する属性の要件は異なる。順方向パス構築の場合、当該認証局が他の認証局へ発行した証明書によってチェーンを辿るため、リポジトリ中の当該認証局エントリの crossCertificatePair 属性の issuedByThisCA を参照し、この issuedByThisCA の主体者エントリをチェーンの次の証明書の格納先として求めていく。順方向パス構築ではどのような認証モデルであっても発行者エントリの issuedByThisCA が必須である。階層モデルで下位認証局証明書を主体者エントリの cACertificate 属性のみに登録した場合、順方向でのバス構築は非常に困難となる。逆方向パス構築の場合、署名者証明書の発行者エントリの crossCertificatePair 属性の issuedToThisCA を参照し、その証明書の発行者エントリを求めていく。階層モデルでは、issuedToThisCA の代わりに cACertificate 属性によって上位認証局証明書へのチェーンを求めていくことができる。よって階層モデルでの下位認証局エントリの issuedToThisCA への格納は必須でない。

(c) 順方向パス構築の必要性

前段落までで述べた通り、下位認証局証明書を crossCertificatePair 属性の issuedByThisCA に格納しなければ階層モデルでの順方向パス構築ができないが、処理効率の観点から判断すると階層モデルでの順方向パス構築は重要性が高くない。

順方向パス構築、逆方向パス構築は、処理効率の観点で適する認証モデルに違いがあり、階層モデルでは逆方向パス構築、他の信頼モデルでは順方向パス構築を効率的とする議論が "Building Certification Paths: Forward vs.

Revers"[35]に見られる。更に、階層、相互認証等が混在した複雑な認証モデルでは効率的なパス構築には順方向､逆方向を組み合わせて行うことが必要である。本実験のテーマである PKI ドメイン間の相互認証に対応するクライアントアプリケーションとしては、複雑な認証モデルに効率的に対応する双方向の認証パス構築ができる実装が望まれるところである。このようなクライアントアプリケーションにとっては、階層モデルの順方向パス構築は非効率な望ましくない処理であり、運用上の要件ではない。この場合、下位認証局証明書を crossCertificatePair 属性の issuedByThisCA へ格納することの必要性も高くない。しかし単純に順方向パス構築しか実装していないクライアントアプリケーションにとっては、下位認証局証明書が issuedByThisCA へ格納されていることは必須要件である。

本実験においては、階層モデル内のリポジトリ構造として下位認証局証明書を issuedToThisCA へ格納することは行わず、パス構築は cACertificate 属性を参照しての逆方向で支障なく機能した。

(d) crossCertificatePair へ格納した場合

下位認証局証明書を crossCertificatePair 属性に格納した場合、相互認証証明書と下位認証局証明書の区別がつかず、試行すべき検証パスの数をいたずらに増やし検索効率を落とす可能性がある。

(e) 結論

下位認証局証明書を crossCertificatePair 属性へ格納することのメリット、デメリットは以下である。

メリット: 順方向パス構築のみの実装にも対応できる。 デメリット: 相互認証証明書と下位認証局証明書の区別がつかず、探索効率が落ちる。

PKI ドメインはそのポリシにより、上記メリット、デメリットを勘案して証明書の格納属性を慎重に決定すべきである。特に、PKI ドメイン間の相互接続ではデメリットである検索効率の低下は影響が大きい。よって下位認証局証明書は cACertificate 属性にのみ格納することを、本報告書では推奨する。

[35] Building Certification Paths: Forward vs. Reverse, Yassir Elley, Anne Anderson, Steve Hanna, Sean Mullen, Radia Perlman, Seth Proctor (See http://www.isoc.org/isoc/conferences/ndss/01/2001/papers/elley.pdf).

16.2.3 署名用トークンインターフェース仕様

(1) Wrapper 開発によるアプリケーション機能の切り出し

今回、次の理由により Wrapper 機能をアプリケーションとは別機能として提供している。

- 各国／地域の PKCS#11 ライブラリが C 言語ベースのライブラリであり、Web アプリケーションを構築する Java 或いは ActiveX との間に言語変換インターフェースが必要である。
- 各国の PKCS#11 ライブラリは、ファイル名がそれぞれ異なるため、アプリケーションから呼び出す場合にファイル名をアプリケーションへ渡す必要がある。

(a) Wrapper 機能の検証

今回は個別の機能として設定した Wrapper について機能の検証を行った。

結果としては、差異の吸収を行うことができ、相互運用性として有効であるとの結論を導くことができ、Wrapper の機能としての有効性を検証することができた。ただし、この Wrapper 機能をアプリケーションと独立したモジュールとする必然性はない。

(b) アプリケーションの一部としての位置づけ

Wrapper は Java アプレット或いは ActiveX の形式で提供され、クライアントへ必要に応じてダウンロードされる。また、アプリケーションも同様に Java アプレット或いは ActiveX の形式で提供される。このことから、モジュールの形式としてはアプリケーションと Wrapper を同一のものとすることは可能である。また、ヒアリングの結果でも Wrapper 機能をアプリケーションの一部の機能として位置づけた方が自然であるとの意見が出ている。

機能としては、Wrapper は差異の吸収を行ってはいるものの、アプリケーションと PKCS#11 ライブラリの仲介をしているにすぎず、Wrapper 機能をアプリケーションで実現することは困難ではなく煩雑になることも無いと思われる。

(c) 結論

署名用トークンインターフェース仕様として Wrapper 機能を独立した機能とすることを必須としない方針とし、アプリケーション開発者の判断に委ねるべきである。本標準は、これまで Wrapper 機能に重点を置いて策定してきたが、アプリケーションに関する標準と見方を変え、再度整理することでより有効性の高い標準としていく必要がある。

(2) 署名メカニズムについて

今回の標準において、Function の選択としては相互運用性としての有効性を確

保することができたが、Function へ渡すパラメータとして「署名メカニズム」についての課題が顕在化したのでここで触れておく。

署名メカニズムとは、PKCS#11 の署名機能及び検証機能を使用する際に、どのような仕組みのデータであるかを指定するための PKCS#11 での型指定である。この署名メカニズムには、主に CKM_SHA1_RSA_PKCS というものと、CKM_RSA_PKCS というものの 2 つがある。それぞれの特徴を見てみる。

(a) 署名メカニズムの内容

CKM_RSA_PKCS は平文そのものを秘密鍵を使用して RSA アルゴリズムで暗号化し、PKCS#1 形式のデータを作成する。

一方、CKM_SHA1_RSA_PKCS は SHA1 アルゴリズムにより平文からハッシュ値を作成し、そのハッシュ値を秘密鍵を使用して RSA アルゴリズムで暗号化し、PKCS#1 形式のデータを作成する。

(b) PKI アプリケーションからの要件

PKI アプリケーションにおいて、電子署名に求められる 3 つの要件として改竄検出、本人性確認、否認防止がある。

CKM_RSA_PKCS を使用した場合は、改竄検出を厳密な意味で行うことができない。ただし、改竄された場合は暗号化されたデータを復号できないという点で間接的に改竄を検出することは可能である。また、暗号化する際に使用する鍵は送信相手の公開鍵となり、文書送信者の秘密鍵を使用しないことから本人性確認、否認防止を行うことができないというデメリットがある。

一方、CKM_SHA1_RSA_PKCS を使用した場合は、ハッシュ値を作成することにより改竄検出に対応しており、ハッシュ値を本人の秘密鍵で暗号化することから、本人性確認及び否認防止にも対応している。

(c) 署名に関する環境整備

署名付与・検証を行うハードウェアについて見た場合、CKM_RSA_PKCS では必要メモリ、CPU パワーに関するハードウェアリソースを CKM_SHA1_RSA_PKCS よりも少なくすることができる。その分レスポンスを良くすることが可能であるというメリットがある。

(d) 結論

今後アジア圏で PKI アプリケーションを普及させていくにあたり、CKM_RSA_PKCS を使用するのか CKM_SHA1_RSA_PKCS を使用するのかについて明確な定義を行う必要がある。その際、次の 3 つの点を明確にする必要がある。

1）PKI アプリケーションが電子署名に求める要件
2）レスポンスに関するクライアントが満たすべきハードウェア要件
3）アジア圏における PKCS#11 機能のサポート状況

(i) PKI アプリケーションが電子署名に求める要件

すべてのアプリケーションが CKM_SHA1_RSA_PKCS を適用しなければいけないと一律に決めることはできない。CKM_RSA_PKCS で済むケースもあると思われる。様々なアプリケーションの適用ケースにおいて、どのレベルまでを満たせば十分であるかを明確にしていく必要がある。

(ii) レスポンスに関するクライアントが満たすべきハードウェア要件

CKM_SHA1_RSA_PKCS と CKM_RSA_PKCS でどれだけレスポンスが異なるのか、様々なハードウェア環境及びトークンを使用し、実測を行う等の方法により、レスポンス時間の目安を明確にしていく必要がある。

(iii) アジア圏における PKCS#11 機能のサポート状況

CKM_SHA1_RSA_PKCS と CKM_RSA_PKCS でどれだけの国／地域で対応可能であるのかを明確にしていく必要がある。

(3) トークンにおける複数個の鍵管理について

今回の実験では、PKCS#11 ライブラリが管理するトークンに格納される鍵の数は 1 個であった。そのため、今回策定した PKCS#11 関数のシーケンスのみで対応することが可能であったが、トークンに格納される鍵の数が複数個となった場合、本標準の機能では不十分となってくることが予想される。

今後、本仕様の普及を高めるために、トークンで複数個の鍵を格納している場合を想定した仕様を提示していくことが必要である。