|  |
| --- |
| 戦略的イノベーション創造プログラム（ＳＩＰ）第２期／ビッグデータ・ＡＩを活用したサイバー空間基盤技術／分野間データ連携基盤技術／分野・組織を超えたデータ活用とサービス提供を実現する基盤の研究 |
| トラスト基盤連携 |
| リストモデルによる証明書有効性検証システム技術仕様書 |

セコムトラストシステムズ　株式会社

2023年3月

変更履歴

| # | 年月日 | 変更者 | 変更内容 |
| --- | --- | --- | --- |
| 1 | 2023年3月17日 |  | 初版作成 |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |

目次

[1 目的 5](#_Toc130911952)

[2 リストモデルによる証明書有効性検証システム技術仕様 6](#_Toc130911953)

[2.1 リストオブトラステッドリストの認証 7](#_Toc130911954)

[2.2 各国のトラステッドリストの認証 8](#_Toc130911955)

[2.3 証明書と一致するリストアップされたトラストサービスの取得 9](#_Toc130911956)

[2.4 適格証明書の判定 10](#_Toc130911957)

[2.5 適格署名/eシール生成デバイス(QCSD)の判定 12](#_Toc130911958)

[2.6 適格タイムスタンプの判定 13](#_Toc130911959)

[2.7 適格検証サービスの判定 14](#_Toc130911960)

[2.8 適格保存サービスの判定 15](#_Toc130911961)

[2.9 適格電子登録配送サービスの判定 17](#_Toc130911962)

[3 各国のトラストサービスを模擬する検証環境 19](#_Toc130911963)

[3.1 検証環境概要 19](#_Toc130911964)

[3.2 欧州（EU）のトラストサービスの模擬 21](#_Toc130911965)

[3.2.1 EU LoLT 21](#_Toc130911966)

[3.2.2 MS TL 21](#_Toc130911967)

[3.3 英国（UK）のトラストサービスの模擬 22](#_Toc130911968)

[3.3.1 UK LoLT 22](#_Toc130911969)

[3.3.2 UK TL 22](#_Toc130911970)

[3.4 米国（US）のトラストサービスの模擬 22](#_Toc130911971)

[3.5 日本（JP）のトラストサービスの模擬 23](#_Toc130911972)

[3.5.1 トラステッドリスト環境 23](#_Toc130911973)

[3.5.2 ブリッジ認証環境 24](#_Toc130911974)

[4 各国のトラストサービスの相互承認の模擬 25](#_Toc130911975)

[4.1 日本と欧州（JP-EU）の相互承認の模擬 25](#_Toc130911976)

[4.2 日本と英国（JP-UK）の相互承認の模擬 26](#_Toc130911977)

[4.3 日本と米国（JP-US）の相互承認の模擬 26](#_Toc130911978)

[4.4 欧州と英国（EU-UK）の相互承認の模擬 26](#_Toc130911979)

[4.5 欧州と米国（EU-US）の相互承認の模擬 26](#_Toc130911980)

[4.6 英国と米国（UK-US）の相互承認の模擬 27](#_Toc130911981)

[5 参考文献 28](#_Toc130911982)

用語集

BCA Bridge Certification Authority ブリッジ認証局

CA Certification Authority 認証局

CC Country Code 国コード

CP Certificate Policy 証明書ポリシー

CPS Certification Practices Statement 認証局運用規程

CRL Certificate Revocation List 証明書失効リスト

CSP Certification Service Provider 認証事業者

CSR Certificate Signing Request 証明書署名要求

DN Distinguished Name 識別名

DSS Digital Signature Services デジタル署名サービス

EC European Commission 欧州委員会

EDS Electronic Delivery Service 電子配信サービス

EEA European Economic Area 欧州経済領域

EU European Union 欧州連合

EUMS European Union Member States 欧州連合加盟国

FBCA Federal Bridge Certificate Authority アメリカ連邦政府ブリッジ認証局

FCP Federal Common Policy アメリカ連邦政府共通ポリシー

FTP File Transfer Protocol ファイル転送プロトコル

GPKI-BCA Government Public Key Infrastructure Bridge Certificate Authority

日本政府認証基盤相互認証局

HTML HyperText Markup Language ハイパーテキスト マークアップ ランゲージ

HTTP HyperText Transfer Protocol ハイパーテキスト トランスファー プロトコル

ISO International Organization for Standardization 国際標準化機構

JPKI Japanese Public Key Infrastructure 日本の公的個人認証基盤

LDAP Lightweight Directory Access Protocol 軽量なディレクトリ アクセス プロトコル

LOTL List Of Trusted Lists 各国のトラステッドリストの統合リスト

MRA Mutual recognition agreement 相互承認協定

MS Member State 加盟国

MS TL Member State Trusted Lists 加盟国のトラステッドリスト

OCSP Online Certificate Status Protocol オンライン証明書状態プロトコル

OID Object Identifier オブジェクト識別子

OJEU Official Journal of the European Union 欧州連合の公報

PIN Personal Identification Number 個人識別番号

PKC Public Key Certificate 公開鍵証明書

PKI Public Key Infrastructure 公開鍵基盤

PSES Preservation Service for Electronic Signatures 電子署名データ保存サービス

QC Qualified Certificate 適格証明書

QSCD Qualified Signature/Seal Creation Device 適格署名/eシール生成デバイス

RA Registration Authority 登録局

REM Registered Electronic Mail 書留電子メール

SHA Secure Hash Algorithm セキュアハッシュアルゴリズム

SSCD Secure Signature Creation Device セキュア署名生成デバイス

TDP TL Distribution Point トラステッドリスト配布点

TL Trusted List トラステッドリスト

TLSO Trusted List Scheme Operator トラステッドリストスキームオペレータ

TSA Time-Stamping Authority タイムスタンプ局

TSL Trust-service Status List トラストサービスステータスリスト

TSP Trust Service Provider トラストサービスプロバイダ

TST Time-Stamp Token タイムスタンプトークン

UCS Universal Character Set 国際符号化文字セット

URI Uniform Resource Identifier 統一資源識別子

UTC Coordinated Universal Time 協定世界時

UTF Unicode Transformation Format ユニコード変換フォーマット

WWW World Wide Web ワールドワイドウェブ

XAdES XML Advanced Electronic Signature XML先進電子署名

XHTML eXtended HTML 拡張マークアップ言語

XML eXtensible Markup Language エクステンシブル マークアップ ランゲージ

# 目的

国内外のトラストアンカーを相互に確認するために、機械可読なトラストアンカーの開示のしくみである「トラステッドリスト」に関する技術仕様を検討する必要がある。また、電子署名国内外で作成された電子データの相互連携を行うためには、電子データに付与されている電子署名、タイムスタンプ、電子証明書の有効性を検証が電子データの提供側、受領側で相互に行える必要がある。ここでは、電子データを取り扱うアプリケーションが電子署名、タイムスタンプ、電子証明書の技術仕様やトラストアンカーへの接続方法についての国内外の差異を意識することなく容易にデータの信頼性を確認することができる署名検証システムの技術的な検討を行う。

# リストモデルによる証明書有効性検証システム技術仕様

　本章では、トラステッドリストを利用した証明書有効性検証システムの仕様を述べる。証明書有効性検証システムとは、図2-1に示したようにトラストサービスの一つである署名検証サービス（VA）のシステムを指している。例えば2者間での電子取引では、互いに業務アプリケーションからリモート署名サービスを利用して作成した署名済み電子データの授受を行う。証明書有効性検証システムは取引相手から受領した電子データの有効性を検証する際に利用されるVAサービスのシステムである。また、証明書有効性検証システムは自らが信頼するトラステッドリスト（トラストアンカーの方式の一つ）を参照して証明書の有効性を検証する。トラストサービスの国際的な相互運用を可能にするためには、トラストアンカー間の相互連携が必要である。

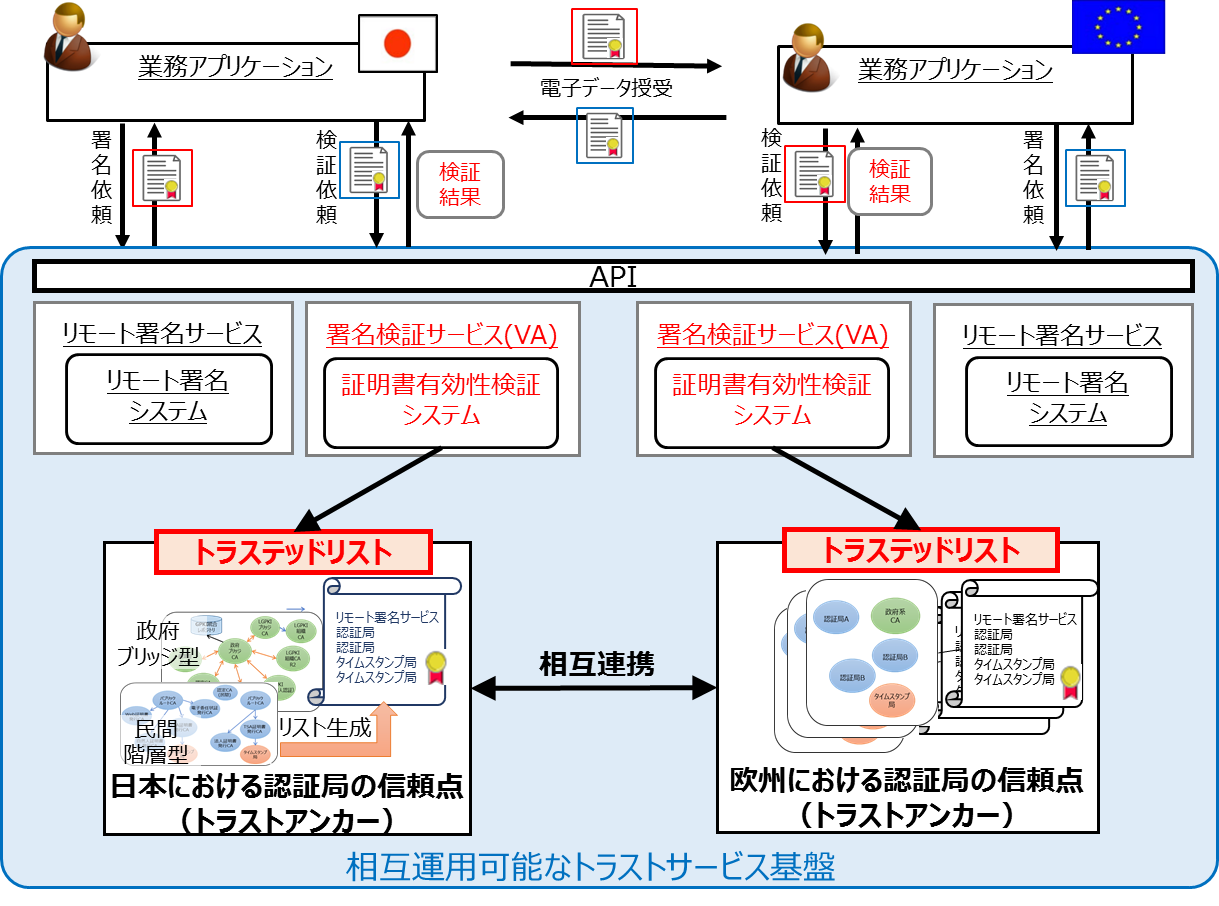


図 2‑1　トラステッドリストを用いた証明書有効性検証システム

表2-2はトラステッドリストを利用した証明書有効性検証システムの技術仕様の概要を示したものである。これはトラステッドリストを用いた証明書有効性検証の手続きを述べたETSI TS 119 615[2]を参考にしている。

表 2‑2　トラステッドリストを用いた証明書有効性検証システムの技術仕様の概要一覧

| # | 項目 | 説明 | 備考 |
| --- | --- | --- | --- |
| 1 | リストオブトラステッドリストの認証 | リストオブトラステッドリスト(XML)の真正性と完全性を確認する。 |  |
| 2 | 各国のトラステッドリストの認証 | トラステッドリスト(XML)の真正性と完全性を確認する。リストオブトラステッドリストに含まれる国の数だけ行う。 |  |
| 3 | 証明書と一致するリストアップされたトラストサービスの取得 | トラステッドリストを用いて、特定の日時において、証明書と一致するトラストサービスの情報を取得する。 |  |
| 4 | 適格証明書の判定 | トラステッドリストを用いて、特定の日時において、証明書がどのタイプの適格証明書に一致するかを判定する。 |  |
| 5 | 適格署名/eシール生成デバイス(QCSD)の判定 | トラステッドリストを用いて、特定の日時において、適格証明書に対応する秘密鍵がQCSDに存在することを判定する。 |  |
| 6 | 適格タイムスタンプの判定 | トラステッドリストを用いて、タイムスタンプトークンの生成時刻に適格タイムスタンプであったことを判定する。 |  |
| 7 | 適格検証サービスの判定 | トラステッドリストを用いて、特定の日時において証明書の署名者が、適格検証サービスプロバイダであったことを判定する。 |  |
| 8 | 適格保存サービスの判定 | トラステッドリストを用いて、特定の日時において証明書の署名者が、適格保存サービスプロバイダであったことを判定する。 |  |
| 9 | 適格電子登録配送サービスの判定 | トラステッドリストを用いて、特定の日時において証明書の署名者が、適格電子登録配送サービスプロバイダであったことを判定する。 |  |

## リストオブトラステッドリストの認証

リストオブトラステッドリストの認証は、アルゴリズムの形で、各国のトラステッドリストを使用し解釈するための手順を示すものである。本手順の入力を表 2‑3に示し、出力を表 2‑4に示す。おもな入力は、リストオブトラステッドリストを示すURIと、リストオブトラステッドリストを検証するための証明書である。おもな出力は、リストオブトラステッドリストのステータス表示である。

表 2‑3　リストオブトラステッドリストの認証の入力

| **名前** | **入力内容の説明** |
| --- | --- |
| OJEU-LOC | 欧州委員会の実施決定（EU）2015/1505に基づいて通知された、EUMS TLのデータに関連する欧州連合の官報（OJEU）の最新の発行物を参照するURI値。 |
| OJEU-LOTL-LOC | OJEU-LOCから入手可能なOJEU出版物で指定されている、LOTLのXMLファイルの現在のインスタンスが利用可能な場所を表すURI値。 |
| OJEU-LOTL-Certs-Set | OJEU-LOCから入手可能なOJEU出版物に記載されている、LOTLの真正性と完全性を確保するために使用される証明書のフルセット。 |

表 2‑4　リストオブトラステッドリストの認証の出力

| **名前** | **出力内容の説明** |
| --- | --- |
| Authenticated- LOTL | 現在のLOTLのインスタンスの認証されたXMLバージョン。 |
| LOTL-Status | 現在のLOTLのインスタンスを認証するプロセスのステータス表示。 |
| LOTL-Sub-Status | LOTLの現在のインスタンスを認証するプロセスのLOTL-Status表示を補足する表示のリスト。 |

## 各国のトラステッドリストの認証

　各国のトラステッドリストの認証は、国を示す国コードを入力として、当該国のトラステッドリストのステータス表示を出力する手順を示すものである。本手順の入力を表 2‑5に示し、出力を表 2‑6に示す。おもな入力は、国を示す国コードである。おもな出力は、当該国のトラステッドリストのステータス表示である。

表 2‑5　各国のトラステッドリストの認証の入力

| **名前** | **入力内容の説明** |
| --- | --- |
| CC | 信頼されたリストが認証されるEUMSの国コードで、その値はISO 3166-1 Alpha 2の国コードに準拠し、大文字で設定される。 |

表 2‑6　各国のトラステッドリストの認証の出力

| **名前** | **出力内容の説明** |
| --- | --- |
| Authenticated-EUTL | EUMS CCの要求されたTLの認証されたXMLバージョン。 |
| EUTL-Status | EUMS CCの要求されたTLを認証するプロセスのステータス表示。 |
| EUTL-Sub-Status | EUMS CCの要求されたTLを認証するプロセスのEUTL-Status表示を補足する表示のリスト。 |

## 証明書と一致するリストアップされたトラストサービスの取得

証明書と一致するリストアップされたトラストサービスの取得は、特定の国のトラステッドリストから、特定のサービスタイプ識別子と、特定の日時の証明書を入力として、リストアップされたサービスおよび関連するサービス情報を出力する手順を示すものである。本手順の入力を表 2‑7に示し、出力を表 2‑8に示す。おもな入力は、情報を取得するX.509証明書、サービスタイプ識別子、特定の日時、国コードである。おもな出力は、一致するリストアップされたサービス情報、TSP名、TSP商号である。

表 2‑7　証明書と一致するリストアップされたトラストサービスの入力

| **名前** | **入力内容の説明** |
| --- | --- |
| CERT | 情報を取得するX.509証明書(例：ds:Signatureのds:KeyInfoのds:X509Certificateの値) |
| TLS-Sti | ETSI TS 119 612の5.5.1.1項で規定されたサービスタイプ識別子URI値の一つ。 |
| Date-time | ETSI TS 119 612の5.1.3項で規定されている日付と時刻の表示。 |
| CC | ISO 3166-1 Alpha 2の国別コードに準拠した国別コードの値で、大文字で設定されている。 |

表 2‑8　証明書と一致するリストアップされたトラストサービスの出力

| **名前** | **出力内容の説明** |
| --- | --- |
| SI-Results | 要素のグループのセットで、各グループは以下のものでできる。   1. SI-full は、ETSI TS 119 612　の 5.5 項で規定された「サービス情報」要素に対応する XML セクションとして定義される。 2. SI-at-Date-timeは、5.5.10項を除いてETSI TS 119 612の5.5項で規定されているDate-time関連の「サービス（現行）情報」要素、またはETSI TS 119 612の5.6項で規定されているDate-time関連の「サービス履歴インスタンス」要素のいずれかに対応するXMLセクションとして定義される。 3. ETSI TS 119 612　の5.4.1項で定義された「TSP名」要素として定義されたTSP-Name 4. TSP-Trade-Name は、ETSI TS 119 612　の 5.4.2 節に定義されている「TSP商号」要素として定義されている。 |
| SI-Status | ETSI TS 119 612の 5.5.1.1 項に規定された特定のタイプの「サービスタイプ識別子」URI 値について、特定の日時に、一致するリストされたサービスとその関連サービス情報を証明書で取得することからなるプロセスの状態表示。 |
| SI-Sub-Status | プロセスのSI-Status表示を補足する表示のリスト。 |

## 適格証明書の判定

　適格証明書の判定は、ある証明書の特定の日時を入力として、該当する(各国の)トラステッドリストによって、どのタイプの適格証明書であったかを確認した結果を出力する手順を示すものである。本手順の入力を表 2‑9に示し、出力を表 2‑10に示す。おもな入力は、情報を取得するX.509証明書と、特定の日時である。おもな出力は、X.509証明書の適格状態を示す一連の情報である。

表 2‑9　適格証明書の判定の入力

| **名前** | **入力内容の説明** |
| --- | --- |
| CERT | 情報を取得するX.509証明書(例：ds:Signatureのds:KeyInfoのds:X509Certificateの値) |
| Date-time | ETSI TS 119 612 の5.1.3項で規定されている日付と時刻の表示。 |

表 2‑10　適格証明書の判定の出力

| **名前** | **出力内容の説明** |
| --- | --- |
| QC-Results | 以下の値の 1 つ以上を通じて、CERT の EU 適格状態を示す一連の表示。   1. 「Not\_Qualified」は、CERT がDate-time時点の CC の EUMS トラステッドリストに基づく EU 適格証明書ではないことを示す。 2. 「Not\_Qualified\_For\_eSig」は、CERT が、Date-timeに CC から発行された EUMS トラステッドリストに従った電子署名用の EU 適格証明書ではないことを示す。 3. 「Not\_Qualified\_For\_eSeal」は、CERT が、Date-timeに CC から発行された EUMS トラステッドリストに従ったeシールの EU 適格証明書ではないことを示す。 4. "Not\_QWAC "は、CERT がDate-time に CC から提供された EUMS トラステッドリストに従っ て、ウェブサイト認証用の EU 適格証明書ではないことを示す。 5. 「QC\_For\_eSig」は、CERT が、Date-timeに CC から提供される EUMS トラステッドリストに従い、電子 署名のための EU 適格証明書であることを示す。 6. 「QC\_For\_eSeal」は、CERT が、Date-timeに CC から提供される EUMS トラステッドリストに従ったeシールの EU 適格証明書であることを示す。 7. "QWAC "は、CERT がDate-timeの CC からの EUMS トラステッドリストに従って、Web サイト認証のための EU 適格証明書であることを示すものである。 8. 「INDET\_QC\_For\_eSig」は、CC からの EUMS トラステッドリストが、CERT がDate-timeにおける電子署名の適格証明書であることを確認するために使用できないことを示す。 9. 「INDET\_QC\_For\_eSeal」は、CC からの EUMS トラステッドリストが、CERT がDate-timeにおけるeシールの適格証明書であることを確認するために使用できないことを示す。 10. 「INDET\_QWAC」は、CC からの EUMS トラステッドリストを使用して、CERT がDate-timeにおけるウェブサイト認証用の適格な証明書であることを確認できないことを示す。 11. "indeterminate"(不確定) 12. Void |
| QC-Status | プロセスの状態表示。 |
| QC-Sub-Status | QC-Status表示を補足する表示のリスト。 |
| CHECK\_1\_SET-OF\_QE | 中間プロセスで定義される中間結果 |
| CHECK\_2\_SET- OF\_QE | 中間プロセスで定義される中間結果 |
| CHECK\_3\_SET-OF\_QE | 中間プロセスで定義される中間結果 |

## 適格署名/eシール生成デバイス(QCSD)の判定

　QCSDの判定は、ある適格証明書と特定の日時を入力として、該当する国のトラステッドリストにより、そのプライベート鍵が特定の日時にQCSDに存在していたことが確認されているかどうかを判断した結果を出力する手順を示すものである。本手順の入力を表 2‑11に示し、出力を表 2‑12に示す。おもな入力は、情報を取得するX.509証明書と、特定の日時である。おもな出力は、証明書がトラステッドリストに従って秘密鍵をQCSDに保有していることの判定結果である。

表 2‑11　QCSDの判定の入力

| **名前** | **入力内容の説明** |
| --- | --- |
| CERT | 情報を取得するX.509証明書(例：ds:Signatureのds:KeyInfoのds:X509Certificateの値) |
| Date-time | ETSI TS 119 612 の5.1.3項で規定されている日付と時刻の表示。 |

表 2‑12　 QCSDの判定の出力

| **名前** | **出力内容の説明** |
| --- | --- |
| QSCD-Result | CERT が、トラステッドリストに従って QSCD に存在するその秘密鍵を保有しているかどうかを、 以下の値のいずれかで示す。   1. 「QSCD\_YES」は、CERT が、EUMS トラステッドリストに従い、日付時刻にその秘密鍵を QSCD に保有していたことを示す。 2. 「QSCD\_NO」は、CERT が、EUMS トラステッドリストに従い、日付時刻に QSCD 内にその秘密鍵を保有していないことを示す。 3. 「QSCD\_INDETERMINATE」は、日付時刻に CERT がその秘密鍵を QSCD に存在させていたかどうかを確認するために、 EUMS トラステッドリストを使用できないことを示すためのものである。 4. void |
| QSCD-Status | プロセスの状態表示。 |
| QSCD-Sub-Status | QSCD-Status表示を補足する表示のリスト。 |

## 適格タイムスタンプの判定

適格タイムスタンプの判定は、タイムスタンプトークンを入力として、タイムスタンプが有効であることを条件に、その生成時刻に適格タイムスタンプであったことが、(各国の)トラステッドリストにより確認されているかどうかを判断した結果を出力する手順を示すものである。本手順の入力を表 2‑13に示し、出力を表 2‑14に示す。おもな入力は、情報を取得するためのタイムスタンプトークンである。おもな出力は、タイムスタンプトークンの適格ステータスである。

表 2‑13　適格タイムスタンプの判定の入力

| **名前** | **入力内容の説明** |
| --- | --- |
| TST | 情報を取得するためのタイムスタンプトークンである。 |

表 2‑14　適格タイムスタンプの判定の出力

| **名前** | **出力内容の説明** |
| --- | --- |
| QTST-Results | 以下のいずれかの値により、TSTのEU適格ステータスを示す。   1. 「Not\_Qualified 」は、TSTがDate-timeにCCから送られてきたEUMSのトラステッドリストに従って、EUの適格なタイムスタンプではないことを示す。 2. 「Qualified」は、TSTがDate-timeのCCからEUMSのトラステッドリストに従って、EUの適格なタイムスタンプであることを示す。 3. 「Indeterminate」は、TSTがDate-timeのEU Qualified Time Stampであることを確認するために、CCからのEUMSトラステッドリストを使用できないことを示す。 |
| QTST-Status | プロセスの状態表示。 |
| QTST-Sub-Status | QTST-Statusの表示を補完する表示のリスト。 |
| CC | 上記の他の3つの出力を得るために使用されるEUMSトラステッドリストの国コード。 |

## 適格検証サービスの判定

　適格検証サービスの判定は、トラストサービス出力の電子署名の検証サポートする証明書に識別される署名者が、特定の日時に、適格電子署名の適格検証サービスの提供者および適格eシールの適格検証サービスの提供者として、適格トラストサービスプロバイダであったことが、該当するトラステッドリストにより確認されているかどうかを判定する手順を示すものである。本手順の入力を表 2‑15に示し、出力を表 2‑16に示す。おもな入力は、情報を取得するX.509証明書、特定の日時である。おもな出力は、適格検証サービスプロバイダであることをトラステッドリストにより確認した結果である。

表 2‑15　適格検証サービスの判定の入力

| **名前** | **入力内容の説明** |
| --- | --- |
| CERT | 情報を取得するX.509証明書(例：対応するトラストサービスの出力からのds:Signatureのds:KeyInfoのds:X509Certificate値) |
| Date-time | ETSI TS 119 612 の5.1.3項で規定されている日付と時刻の表示。 |

表 2‑16　適格検証サービスの判定の出力

| **名前** | **出力内容の説明** |
| --- | --- |
| QVSO-Result | CERT の subjectName 属性を通じて特定される QTSP/QTS の EU 適格ステータスを示す一連の表示で、 以下の値のうち 1 つ以上を含む。   1. 「Not\_Qualified\_For\_eSig」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストにより、Date-timeにおいて、適格電子署名のための適格検証サービスを提供する EU 適格トラストサービスプロバイダではなかったことが確認されたことを示す。 2. 「Not\_Qualified\_For\_eSeal」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストによって、Date-timeにおいて、適格eシールの適格検証サービスを提供する EU 適格トラストサービスプロバイダではなかったことが確認されたことを示す。 3. 「Qualified\_For\_eSig」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストにより、Date-timeにおいて、適格な電子署名のための適格な検証サービスを提供する EU の適格なトラストサービス・ プロバイダであったことが確認されていることを示すために使用される。 4. 「Qualified\_For\_eSeal」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストにより、Date-timeにおいて、適格eシールの適格検証サービスを提供する EU 適格トラストサービス提供者であったことが確認されていることを示すためのものである。 5. 「不確定（Indeterminate）」とは、CC からの EUMS トラステッドリストを使用して、CERT で特定された署名者が、 Date-timeにおいて、適格電子署名の適格検証サービスまたは適格eシールの適格検証サービスを提供する EU の適格トラストサービスプロバイダであったことを確認できないことを示すものである。 |
| QVSO-Status | プロセスの状態表示。 |
| QVSO-Sub-Status | QVSO-Statusの表示を補足する表示のリスト。 |
| CC | 上記の他の3つの出力を得るために使用されるEUMSトラステッドリストの国コード。 |

## 適格保存サービスの判定

　適格保存サービスの判定は、トラストサービス出力の電子署名の検証をサポートする証明書で識別される署名者が、特定の日時に、適格電子署名の適格保存サービスまたは適格eシールの適格保存サービスの提供を行う、適格トラストサービス提供者であったことを、トラステッドリストで確認するための手順を示すものである。本手順の入力を表 2‑17に示し、出力を表 2‑18に示す。本手順の入力を表 2‑17に示し、出力を表 2‑18に示す。おもな入力は、情報を取得するX.509証明書、特定の日時である。おもな出力は、適格保存サービスプロバイダであることをトラステッドリストにより確認した結果である。

表 2‑17　適格保存サービスの判定の入力

| **名前** | **入力内容の説明** |
| --- | --- |
| CERT | 情報を取得するX.509証明書(例：対応するトラストサービスの出力からのds:Signatureのds:KeyInfoのds:X509Certificate値) |
| Date-time | ETSI TS 119 612の5.1.3項で規定されている日付と時刻の表示。 |

表 2‑18　適格保存サービスの判定の出力

| **名前** | **出力内容の説明** |
| --- | --- |
| QPSO-Result | CERT の subjectName 属性を通じて特定される QTSP/QTS の EU 適格ステータスを示す一連の表示で、 以下の値のうち 1 つ以上を含む。   1. 「Not\_Qualified\_For\_eSig」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストによ り、Date-timeにおいて、適格電子署名のための適格保存サービスを提供する EU の適格トラストサービス・プロバイ ダではなかったことが確認されたことを示す。 2. 「Not\_Qualified\_For\_eSeal」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストにより、Date-timeにおいて、適格eシールの適格保存サービスを提供する EU 適格トラストサービス提供者ではなかったこと が確認されたことを示す。 3. 「Qualified\_For\_eSig」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストにより、Date-timeにおいて、適格電子署名のための適格保存サービスを提供する EU 適格トラストサービス提供者であった ことが確認されていることを示すためのものである。 4. 「Qualified\_For\_eSeal」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストによって、Date-timeにおいて、適格eシールの適格保存サービスを提供する EU 適格トラストサービス提供者であったことが確認されていることを示す。 5. 「不確定（Indeterminate）」は、CC からの EUMS トラステッドリストが、CERT で特定された署名者が、 Date-timeにおいて、適格電子署名の適格保存サービスまたは適格eシールの適格保存サービスを提供する EU の適格トラストサービスプロバイダであったことを確認するために使用できないことを示す。 |
| QPSO-Status | プロセスの状態表示。 |
| QPSO-Sub-Status | QPSO-Status表示を補足する表示のリスト。 |
| CC | 上記の他の3つの出力を得るために使用されるEUMSトラステッドリストの国コード。 |

## 適格電子登録配送サービスの判定

　適格電子登録配送サービスの判定は、トラストサービス出力の電子署名の検証をサポートする証明書で識別される署名者が、特定の日時に、適格な電子登録配送サービスを提供する適格なトラストサービス事業者であったことをトラステッドリストで確認するための手順を示すものである。本手順の入力を表 2‑19に示し、出力を表 2‑20に示す。おもな入力は、情報を取得するX.509証明書、特定の日時である。おもな出力は、適格電子登録配送サービスプロバイダであることをトラステッドリストにより確認した結果である。

表 2‑19　適格電子登録配送サービスの判定の入力

| **名前** | **入力内容の説明** |
| --- | --- |
| CERT | 情報を取得するX.509証明書(例：対応するトラストサービスの出力からのds:Signatureのds:KeyInfoのds:X509Certificate値) |
| Date-time | ETSI TS 119 612 の5.1.3項で規定されている日付と時刻の表示。 |

表 2‑20　適格電子登録配送サービスの判定の出力

| **名前** | **出力内容の説明** |
| --- | --- |
| QERDSO-Result | CERT の subjectName 属性を通じて特定される QTSP/QTS の EU 適格ステータスの表示であり、以下の値のいずれかである。   1. 「Not\_Qualified」は、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストにより、Date-timeにおいて、適格な電子登録配送サービスを提供する EU の適格なトラストサービス提供者ではなかったことが確認されたことを示す。 2. 「適格」とは、CERT で特定された署名者が、CC からの該当する EUMS トラステッドリストにより、 Date-timeにおいて、適格電子登録配送サービスを提供する EU 適格トラストサービス提供者であったことが確 認されていることを示す。 3. 「不確定（Indeterminate）」は、CC からの EUMS トラステッドリストが、CERT で特定された署名者が、 Date-timeにおいて、適格電子登録配送サービスを提供する EU 適格トラストサービス提供者であったことを確認するために使用できないことを示す。 |
| QERDSO-Status | プロセスの状態表示。 |
| QERDSO-Sub-Status | QERDSO-Statusの表示を補足する表示のリスト。 |
| CC | 上記の他の3つの出力を得るために使用されるEUMSトラステッドリストの国コード。 |

# 各国のトラストサービスを模擬する検証環境

## 検証環境概要

日欧英米それぞれでの国・地域の電子署名の相互認証を想定した相互認証環境（図 3‑1）をVMware vCenter上に構築した。日欧英相互認証環境（トラステッドリストによる相互認証）の構成を図 3‑2に、日米相互認証環境（ブリッジ認証）の構成を図 3‑3に示す。また、各認証方式で使用したアプリを表 3‑1に示す。

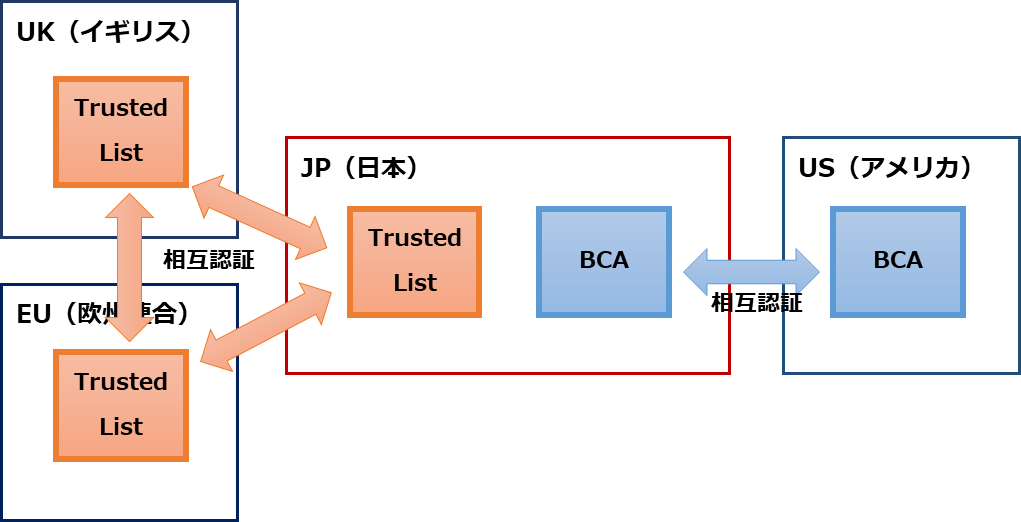


図 3‑1 検証環境で想定する日欧英米相互認証

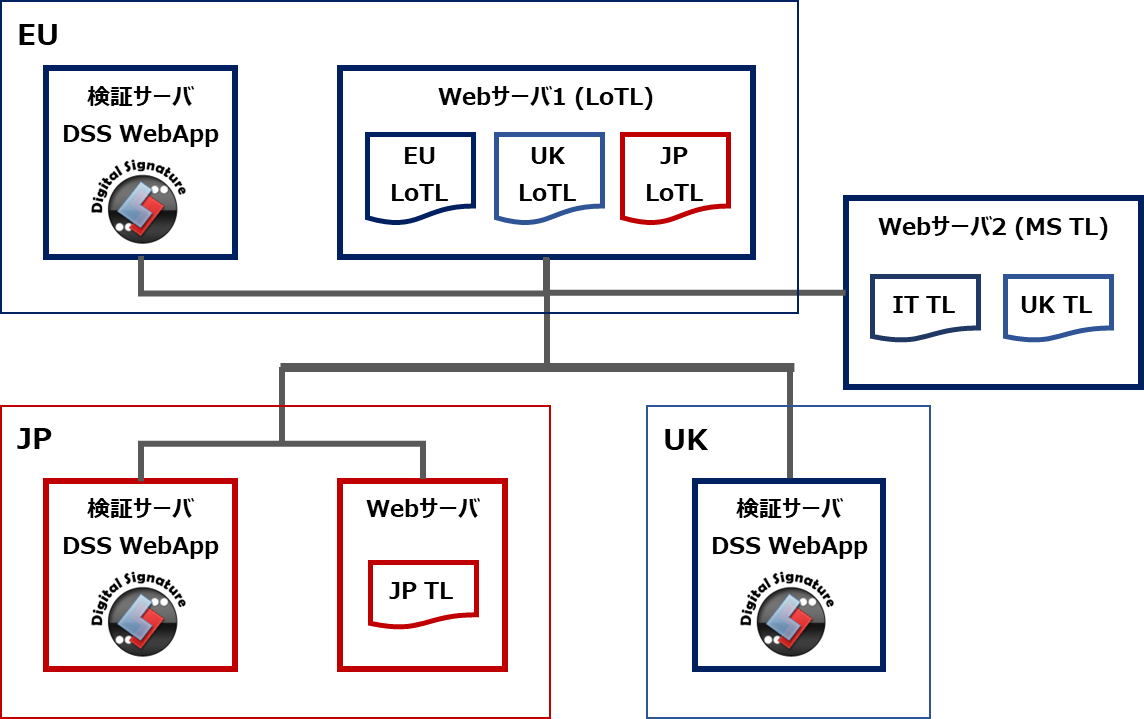


図 3‑2 日欧英トラステッドリスト相互認証環境 構成図

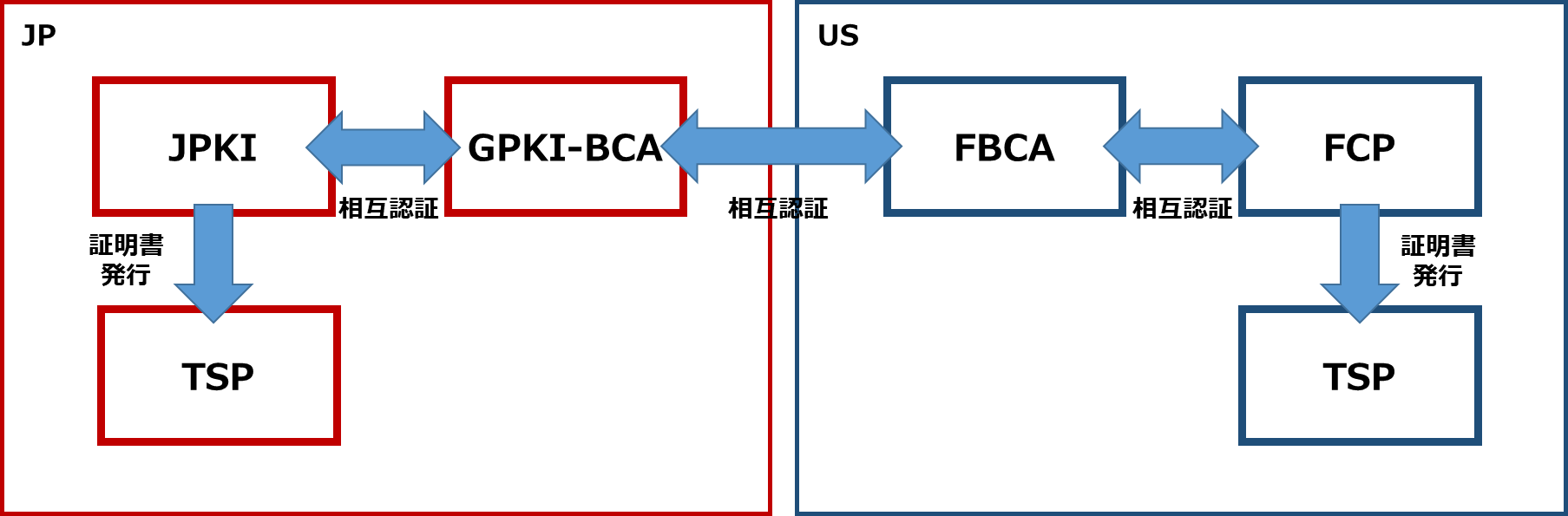


図 3‑3 日米ブリッジ認証環境 構成図

表 3‑1 検証環境導入アプリ一覧

| # | 認証方式 | 使用アプリ | 説明 |
| --- | --- | --- | --- |
| 1 | Trusted List | DSS Webアプリ | 証明書の検証と、JSON、PDF、XMLファイルへの署名および署名検証を行うツール。EUで公開しているソースコードにMRA対応の変更を行い、セルフビルドした。 |
| 2 | TL Manager | TLの作成・編集ツールで、EU加盟国以外の第3国向けアプリ（TL Manager NonEU）を使用した。 |
| 3 | OpenSSL | TLの署名証明書、および、検証で使用するTSP証明書の作成で使用する。 |
| 4 | Bridge認証 | OpenSSL | ブリッジ認証局の構築、および、検証で使用するTSP証明書の作成で使用する。 |

## 欧州（EU）のトラストサービスの模擬

### EU LoLT

検証環境では、表 3‑2に示す検証環境用のEU LoTLを作成し、検証環境のWebサーバで参照できるようにした。

表 3‑2 検証環境 EU LoTL

| # | 項目 | 内容 |
| --- | --- | --- |
| 1 | 第3国対応EU LoTL URL | <https://esignature.ec.europa.eu/efda/intl-pilot/api/v1/intl-pilot/mra_lotl.xml> |
| 2 | 検証環境での変更点 | ・Third Countryの登録を削除  ・イタリアTLの参照先を公式のURLから検証環境のWebサーバに変更（署名検証テスト用TSP登録のため） |

### MS TL

　署名検証を行うためにはJSONやPDF、XMLファイルに署名する必要があり、署名にはTSPの秘密鍵が必要となるため、署名検証テスト用のTSPが必要になる。検証環境では表 3‑3に示す証明書を作成し、イタリアの公式TLに署名検証用のTSPを追加した検証環境用イタリアTLを作成し、検証環境のWebサーバで参照できるようにした。

　なお、検証環境のMS TLを参照するのはイタリアTLのみで、その他のEU加盟国については公式のTLを参照する。

表 3‑3 署名検証用TSP証明書（EU）

| # | 項目 | 内容 |
| --- | --- | --- |
| 1 | TSP名 | Roma |
| 2 | 証明書入力項目 | CN = Roma  O = Roma  S = Roma  C = IT |

* 署名検証用TSPのTL登録項目、および、証明書の入力項目は架空の設定値としたが、トラステッドリストの仕様上、TSP英語名と証明書のO（組織名）の値は一致するように設定した。

また、TSP証明書にはqcStatementを設定した自己証明書を作成した。

## 英国（UK）のトラストサービスの模擬

### UK LoLT

　DSSライブラリバージョン5.11からサポートされたMRA機能を使用するためにはEU LoTLとは別に第3国用のLoTLを作成し、第3国LoTLから該当国のTLを参照する必要がある。このため、検証環境では、表 3‑4で示すUK LoTLを作成し、UK LoTLからUK TLを参照する構成とした。

表 3‑4 検証環境 UK LoTL

| # | 項目 | 内容 |
| --- | --- | --- |
| 1 | 第3国対応EU LoTL URL | https://esignature.ec.europa.eu/efda/intl-pilot/api/v1/intl-pilot/mra\_lotl.xml |
| 2 | 第3国EU LoTL⇒UK LoTLの変更内容 | ・全EU加盟国の登録を削除  ・Third Countryの登録内容をUK TLに変更 |

### UK TL

　UK TLは、EU MS TL同様、署名検証用TSPを追加した。このため、公式のUK TL（https://tl.ico.org.uk/uktrustedlist/UKTL.xml）に署名検証テスト用TSP（証明書の内容は表 3‑5参照）を追加した検証環境用UK TLを作成し、検証環境のWebサーバで参照できるようにした。

表 3‑5 署名検証用TSP証明書（UK）

| # | 項目 | 内容 |
| --- | --- | --- |
| 1 | TSP名 | London |
| 2 | 証明書入力項目 | CN = London  O = London  S = London  C = UK |

## 米国（US）のトラストサービスの模擬

　アメリカでは公開鍵基盤としてトラステッドリストではなくブリッジ認証を採用している。このため、日米相互認証を想定した米国環境では、図 3‑4のようにFCP、FBCAを想定した認証局でそれぞれCSRを作成し、相互に署名することで証明書チェーンを作成した。また、日米の相互認証用テスト用のTSPをFCPの配下に作成した。

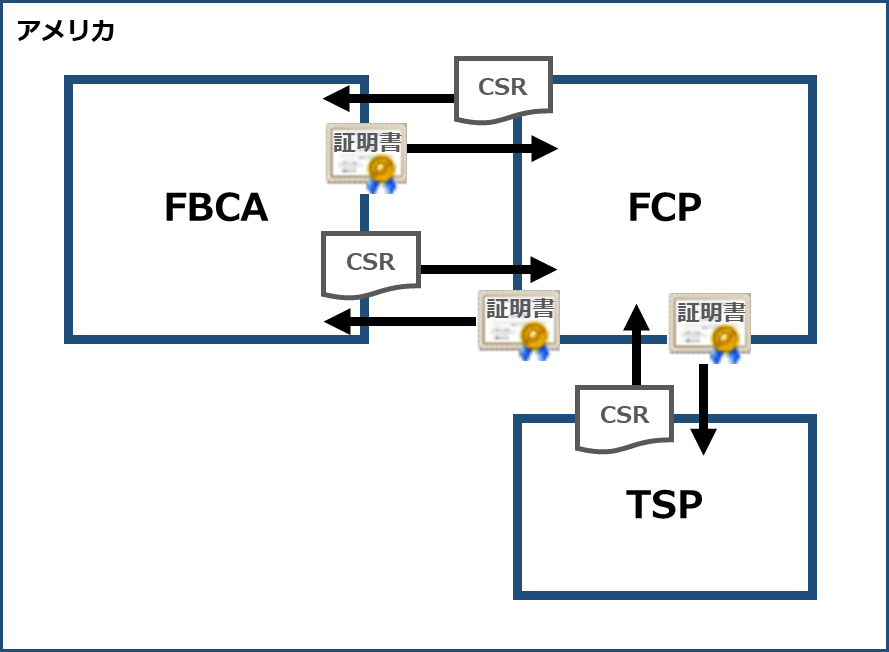


図 3‑4 ブリッジ認証環境（米国）

なお、日本でも図 3‑4と同様のブリッジ認証環境を作成し、日米間の証明書チェーンを作成した。

## 日本（JP）のトラストサービスの模擬

### トラステッドリスト環境

#### JP LoTL

　日本を想定したトラステッドリスト環境は、EU加盟国では無いため、イギリスを想定した環境と同様、表 3‑6で示すJP LoTLを作成し、JP LoTLからJP TLを参照する構成とした。

表 3‑6 検証環境 JP LoTL

| # | 項目 | 内容 |
| --- | --- | --- |
| 1 | 第3国対応EU LoTL URL | <https://esignature.ec.europa.eu/efda/intl-pilot/api/v1/intl-pilot/mra_lotl.xml> |
| 2 | 第3国EU LoTL⇒JP LoTLの変更内容 | ・全EU加盟国の登録を削除  ・Third Countryの登録をJP TLに変更 |

#### JP TL

　JP TLについてはEU加盟国、UK TLのように公式のTLが存在しないため、署名検証テスト用TSP（証明書の内容は表 3‑7参照）を追加したJP TLを作成し、検証環境のWebサーバで参照できるようにした。

表 3‑7 署名検証用TSP証明書（JP）

| # | 項目 | 内容 |
| --- | --- | --- |
| 1 | TSP名 | Tokyo |
| 2 | 証明書入力項目 | CN = Tokyo  O = Tokyo  S = Tokyo  C = JP |

### ブリッジ認証環境

　アメリカ環境のFCP、FBCA間のブリッジ認証を元に、図 3‑5で示すJPKI=GPKI-BCAを想定したブリッジ認証を作成した後、FBCA=GPKI-BCAでそれぞれのCSRに相互署名を行うことで、日米間のブリッジ認証環境を作成した。

なお、図 3‑5で示すTSP証明書を、3.5.1.2のJP TLの署名検証用TSPの証明書として登録することで、日欧英間ではトラステッドリストで認証し、日米間ではブリッジ認証で認証が可能なTSPを構成した。

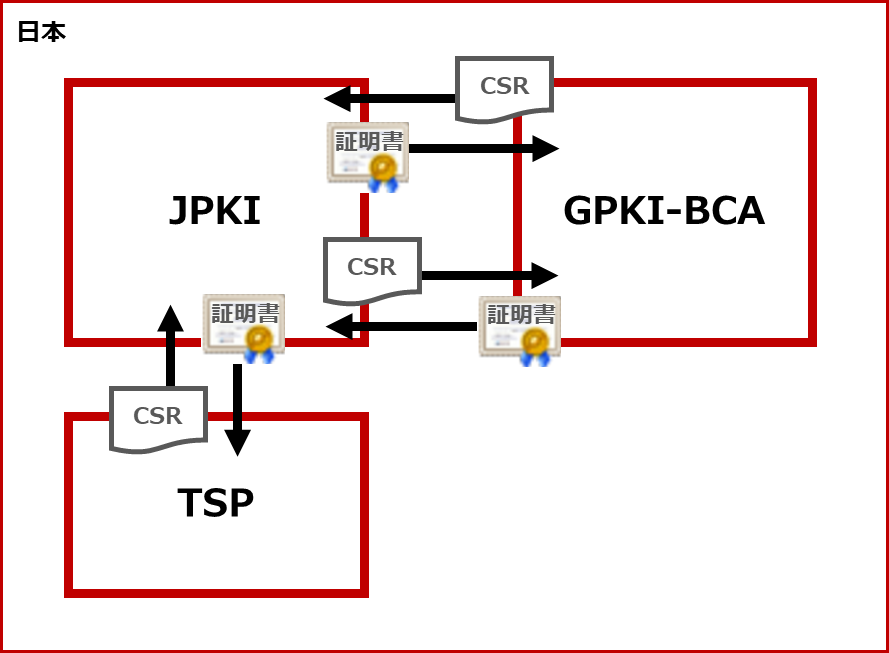


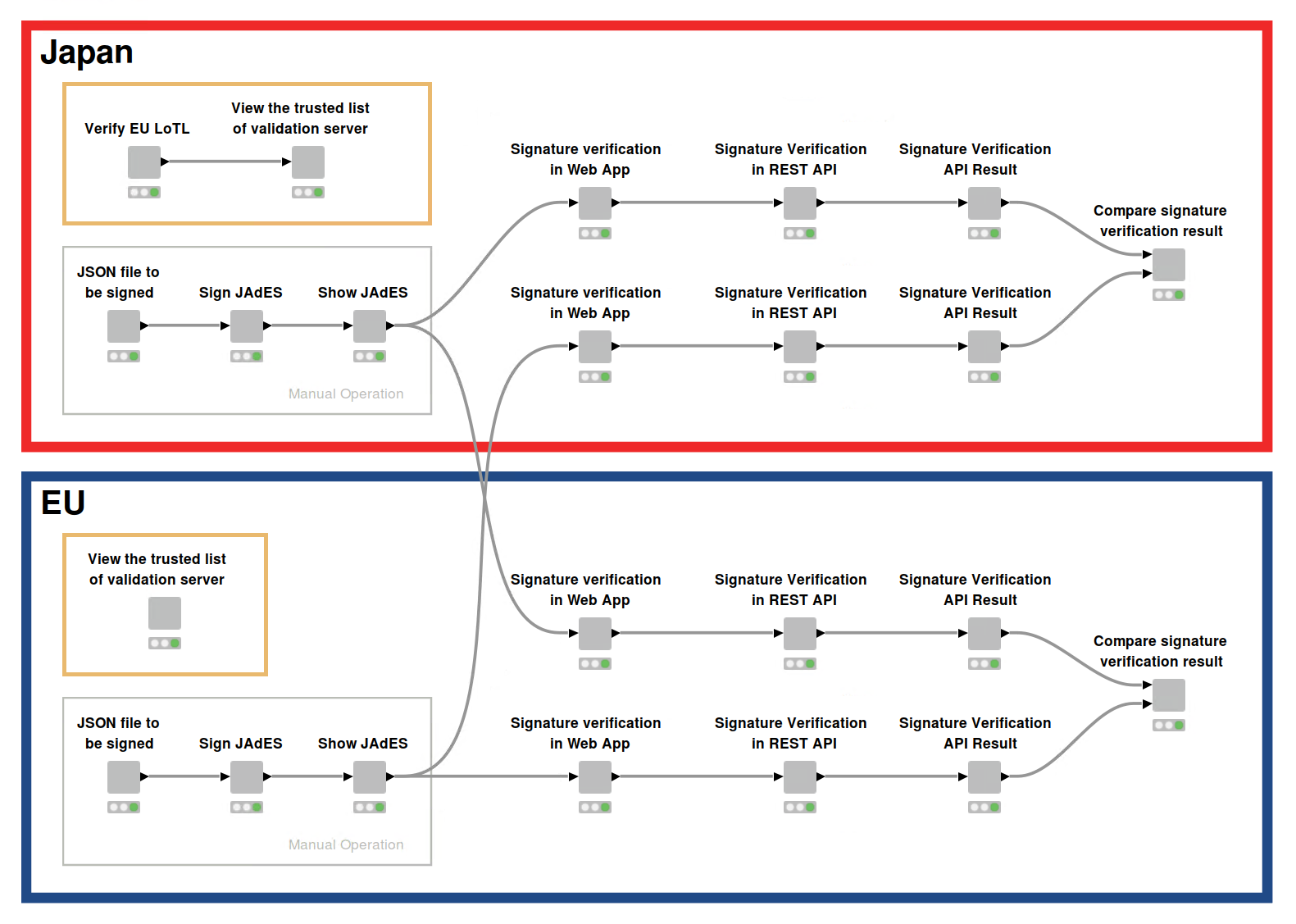
図 3‑5 ブリッジ認証環境（日本）

# 各国のトラストサービスの相互承認の模擬

## 日本と欧州（JP-EU）の相互承認の模擬

日本とEUそれぞれで署名したJSONファイルの署名検証を行うため、図 4‑1のようなワークフローを作成し、下記①②の検証を行った。

1. 日本のTSPで署名したJSONファイルをEUで検証する。
2. EUのTSPで署名したJSONファイルを日本で検証する。



**署名検証結果比較**

**署名検証(REST API)**

**署名検証(Webアプリ)**

**署名**

**署名**

図 4‑1 日欧署名相互検証ワークフロー

　日欧それぞれの署名検証結果の比較を行ったが、TSPにたどり着くまでに参照したTL以外に重要な差分は確認できなかった。ただし、署名検証APIの応答データには、MRAに関するデータ項目は存在したが、値が設定されていなかったため、今後のバージョンアップで比較結果が変わる可能性がある。

## 日本と英国（JP-UK）の相互承認の模擬

　UK⇔日本の署名・検証は、4.1節と同様の手順で実施し、検証結果については、4.1節と比べ参照するTLが異なるだけであった。

## 日本と米国（JP-US）の相互承認の模擬

　ブリッジ認証ではDSSライブラリのような署名・検証アプリが無い。このため、図 4‑2に示す証明書チェーンを作成した後、OpenSSLに実装されている検証機能を使用して下記①②の証明書検証が行えることを確認した。

1. FCPをトラストアンカーにして日本のTSPの証明書を検証する
2. JPLIをトラストアンカーにしてアメリカのTSPの証明書を検証する

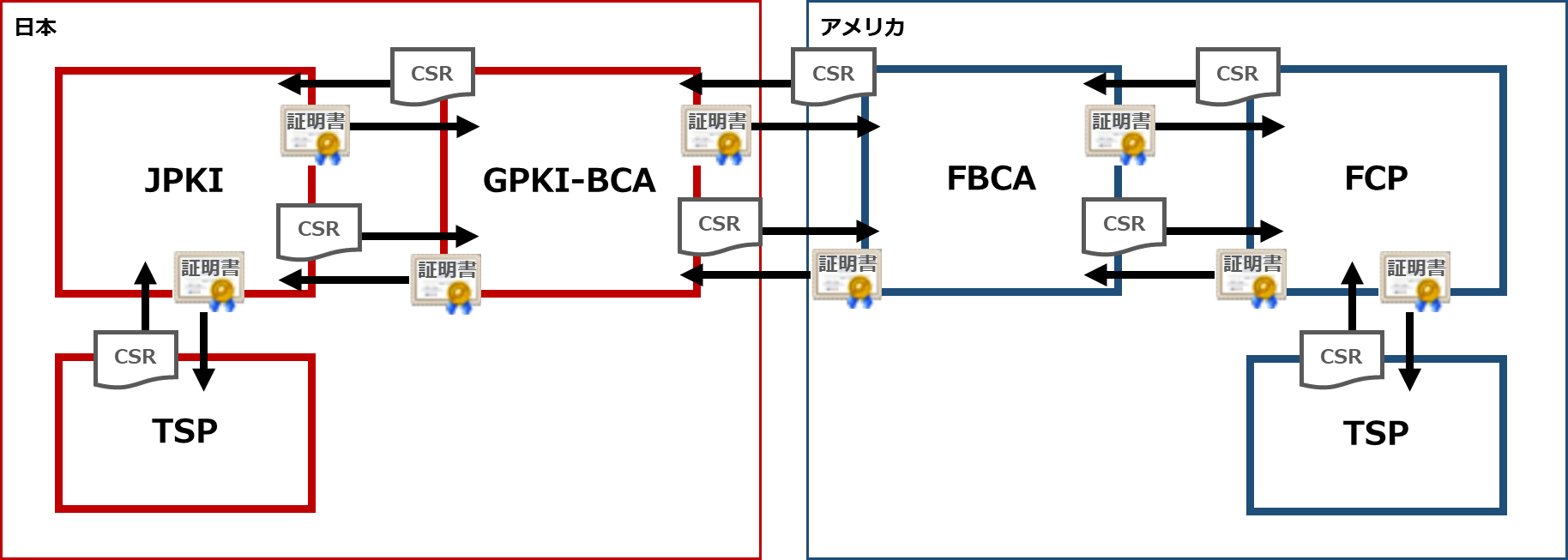


図 4‑2 JP-US間ブリッジ認証環境

## 欧州と英国（EU-UK）の相互承認の模擬

　EU⇔UKの署名・検証は、4.1節と同様の手順で実施し、検証結果については、4.1節と比べ参照するTLが異なるだけであった。

## 欧州と米国（EU-US）の相互承認の模擬

　EU⇔US間の相互承認は4.3節と同様の手順で実施可能であるが、証明書チェーンを構成する認証局を変更するだけであるため、検証環境の作成・検証の実施は省略した。

## 英国と米国（UK-US）の相互承認の模擬

　UK⇔US間の相互承認は4.3節と同様の手順で実施可能であるが、証明書チェーンを構成する認証局を変更するだけであるため、検証環境の作成・検証の実施は省略した。

# 参考文献

1. ETSI TS 119 612 v2.1.1 (2016-04), Electronic Signatures and Infrastructures (ESI);　Trusted Lists
2. ETSI TS 119 615 v0.0.13 (2021-03), Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists
3. CEF eSignature TLManager Version 0.01 TLManager "Non-EU" Installation and Utilisation guide
4. Digital Signature Service Documentation

(https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.pdf)

以上