平成20年度　地域情報プラットフォーム推進事業（地域活性化分野：子育て支援）

別冊：相互接続検証結果

平成21年3月27日

安川情報システム株式会社

目次

１　はじめに

１．１　相互接続検証の目的

１．１．１　目的

相互接続検証では、地域情報プラットフォーム標準仕様書 V2.0 で規定する仕様に準拠した分野横断基盤が、マルチベンダ環境で相互接続できることを検証した。また、平成 20 年度の地域情報プラットフォーム推進事業の「引越ワンストップサービス分野」事業で構築する基準分野横断基盤及び、他の「地域活性化分野」事業と連携して、各事業が個別に構築する分野横断基盤間の相互接続性を検証した。

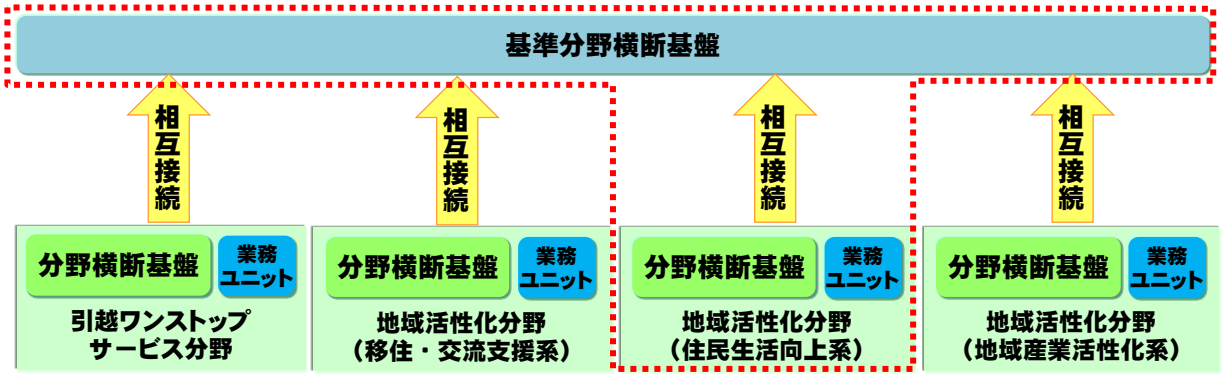

図　1-1　相互接続検証の実施概要図

１．１．２　範囲

検証の対象とする範囲を以下に示す。

- ライフイベントを実現するために必要となる分野横断基盤の接続確認の範囲を扱う。
- 業務シナリオそのものの疎通は対象外とする。

２　対象とする技術仕様及びテストモデル

２．１　対象とする技術仕様

基準分野横断基盤との相互接続検証では、以下の技術仕様を対象範囲とした。

表２-１　技術仕様と実施可否（地域活性化分野：住民生活向上系）

No	技術仕様名	相互接続検証実施可否
1	SOAP、XML、WSDL	○
2	SSL	○
3	MEP(Message Exchange Protocol)	○
4	共通ヘッダ処理	○
5	添付ファイル処理	○

２．２　テストモデル

基準分野横断基盤との相互接続検証では、以下のテストモデル（以下、TM）を実施範囲とし、相互にリクエスタとレスポンダの立場で確認を行なった。

表　２-２　テストモデルと実施可否（地域活性化分野：住民生活向上系）

No	テストモデル	相互接続検証実施可否
1	ＴＭ１（PF 通信 ＋PF 規定の XML パターン）	○
2	ＴＭ２（PF 通信の MEP 基本テスト(３種類)）	○
3	ＴＭ３（PF 通信＋ SSL（サーバ認証、クライアント認証)）	○
4	ＴＭ４（PF 通信＋PF 規定添付ファイル）	○

上記で示した、テストモデル TM1 から TM4 の詳細を以下に示す。

（１）TM1（PF通信 ＋PF規定のXMLパターン）

リクエスト・レスポンス型同期型レスポンス（以降、同期 2Way）を検証する。下図にイメージを示す。

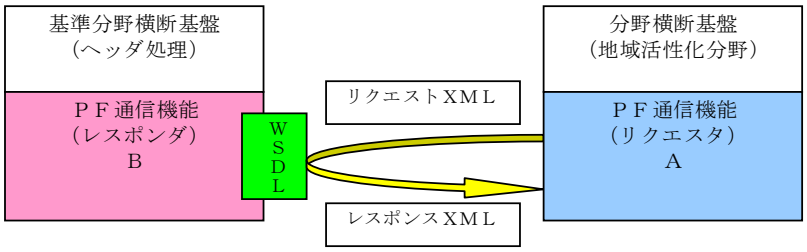

図　２-１　TM1（PF 通信＋PF 規定の XML パターン１）

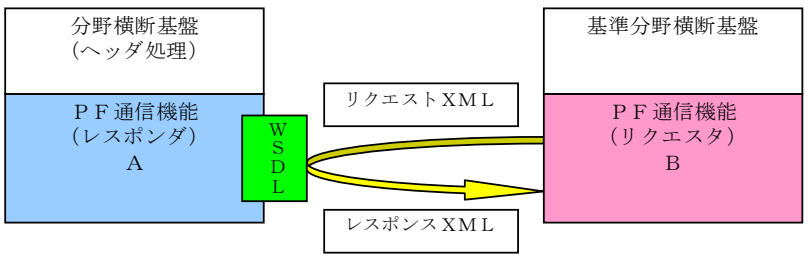

図　２-２　TM1（PF 通信＋PF 規定の XML パターン２）

（２）TM2（PF通信のMEP基本テスト(３種類））

ア）（TM2-1）リクエスト型受領Ackあり（以降、1Way(受領)）を検証する。

下図にイメージを示す。

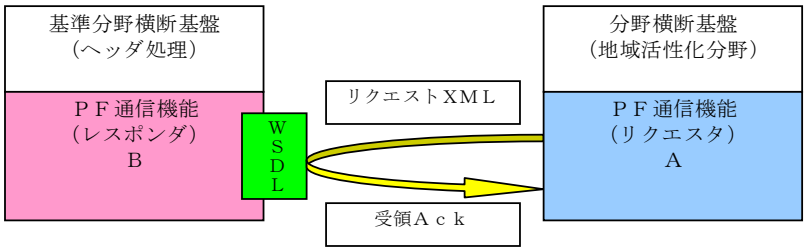

図　２-３　TM2-1（PF 通信＋MEP 基本テスト 1Way（受領）パターン１）

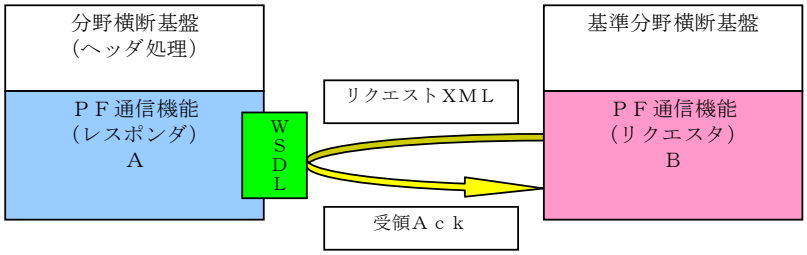

図　２-４　TM2-1（PF 通信＋MEP 基本テスト 1Way（受領）パターン２）

イ）（TM2-2）リクエスト・レスポンス型同期型レスポンス（以降、同期 2Way）を検証する。ただし、TM1 が実施済みなら、TM2-2 は実施済みとみなす。

イメージは TM１と同様のため、省略する。

ウ）（TM2-3）リクエスト･レスポンス型同期型受領Ack＋非同期型レスポンス（以降、非同期 2way）を検証する。

下図にイメージを示す。

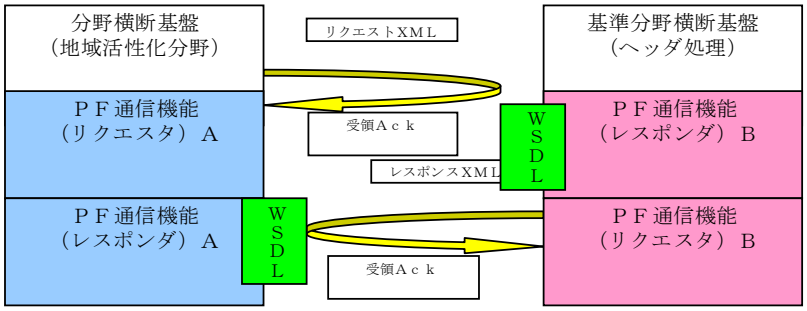

図　２-５　TM2-3（PF 通信＋MEP 基本テスト非同期 2Way パターン１）

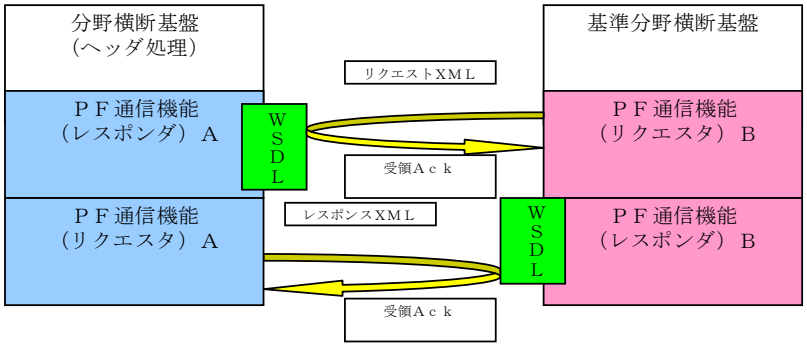

図　２-６　TM2-3（PF 通信＋MEP 基本テスト非同期 2Way パターン２）

（３）TM3（PF通信 ＋SSL（サーバ認証、クライアント認証）

ア）（TM3-1）同期 2Way+SSLサーバ認証を検証する。

下図にイメージを示す。

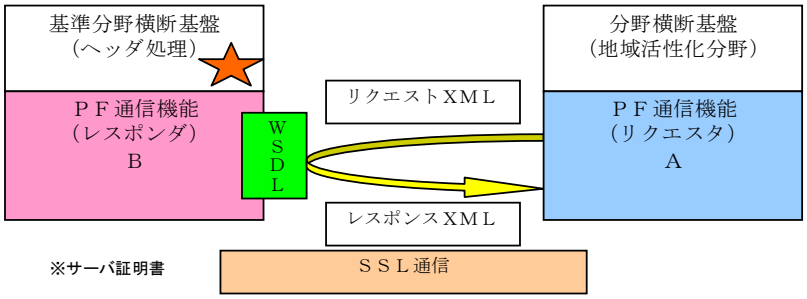

図　２-７　TM3-1（PF 通信＋SSL サーバ認証　同期 2Way パターン１）

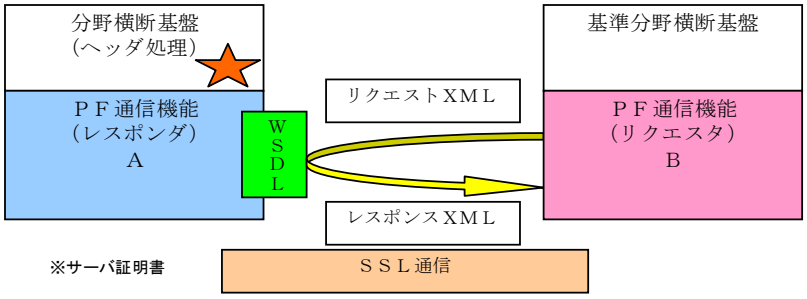

図　２-８　TM3-1（PF 通信＋SSL サーバ認証　同期 2Way パターン２）

イ）（TM3-2）同期 2Way+SSLサーバ認証＆クライアント認証を検証する。

下図にイメージを示す。

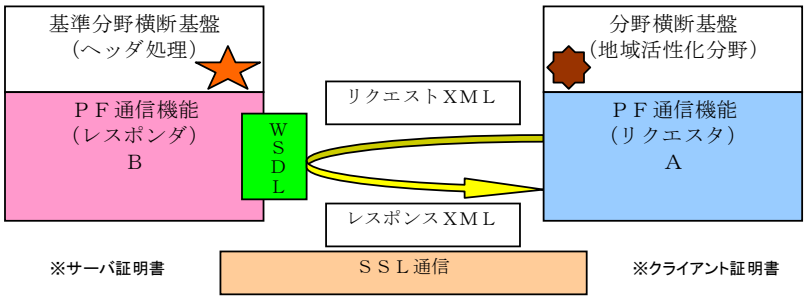

図　２-９　TM3-2（PF 通信＋SSL サーバ&クライアント認証 同期 2Way パターン１）

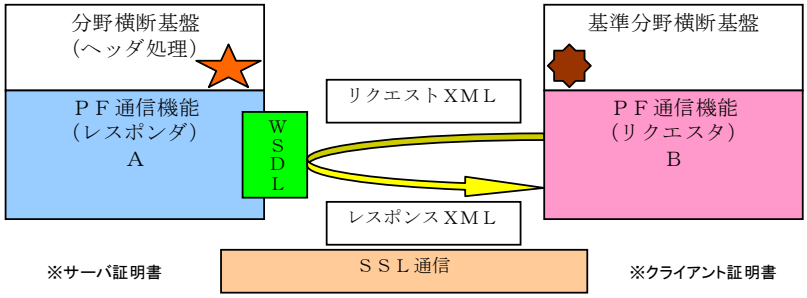

図　２-１０　TM3-2（PF 通信＋SSL サーバ&クライアント認証 同期 2Way パターン２）

（４）TM4（PF通信 ＋PF規定添付ファイル（内包型））

同期 2Way+PF 規定添付ファイル（内包型）を検証する。

下図にイメージを示す。

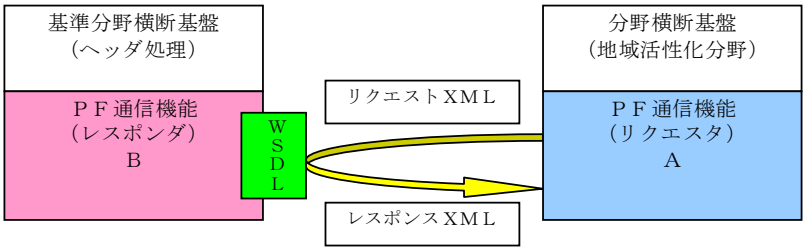

図　２-１１　TM4（PF 通信＋PF 規定添付ファイル（内包型） １）

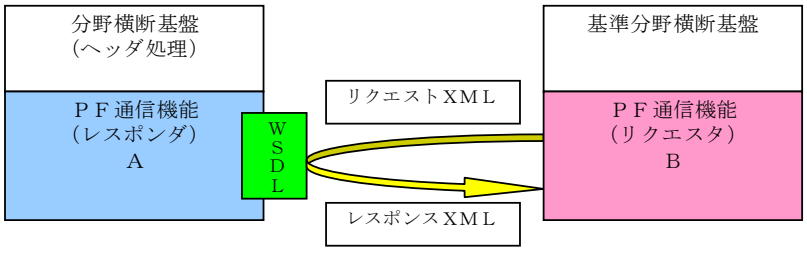

図　２-１２　TM4（PF 通信＋PF 規定添付ファイル（内包型） ２）

３　実施手順

３．１　相互接続検証の実施概要

相互接続検証では、基準分野横断基盤と分野横断基盤の間で地域情報プラットフォーム仕様に準拠したテストパターンで相互接続が問題なく行えることを検証した。
検証は、事前検証⇒総合テスト及び相互接続検証を同日に実施した。

作業フェーズの概要と検証内容を以下に示す。

表 3-1　作業フェーズの概要と検証内容

No.	作業フェーズ	作業概要	検証内容
1	事前検証（1/23）	基準分野横断基盤マシンと分野横断基盤（地域活性化分野）マシンの連携テストを実施し、各マシン間の疎通確認を行う	PING での接続確認 エンドポイント URL への接続確認 相互接続検証用に用意された XML 定義及び WSDL での接続確認（TM1 想定）
2	総合テスト及び相互接続検証（1/23）	基準分野横断基盤マシンと分野横断基盤（地域活性化分野）マシン間で、確認チェックリスト（詳細版）に従い、検証項目の確認を行う	相互接続検証用に用意された XML 定義及び WSDL での接続確認 ※2.2 テストモデルの内容を検証

３．２　検証項目および手順

３．２．１　事前検証

検証する項目と確認方法について以下に示す。

表 3-2　検証項目と確認方法

No.	検証項目	確認方法
1	PING での接続確認	基準分野横断基盤マシンと分野横断基盤マシンがネットワーク接続し、PING コマンドを入力し、互いが接続できていることを確認する
2	エンドポイント URL への接続確認	基準分野横断基盤マシンと分野横断基盤マシン間で各テスト用サービスのエンドポイント URL に接続できていることを確認する（HTTP としての ENDPOINT 接続確認（Web ブラウザ）から ENDPONT の呼出とその応答の確認）
3	相互接続検証用に用意された XML 定義及び WSDL での接続確認	確認チェックリスト（詳細版）に従い、分野横断基盤の送受信ログと基準分野横断基盤の送受信ログを採取し、「送信したデータと受信したデータが同じ内容であること」、「同期通信ができていること」、そして「日本語タグ/document/literal に対応していること」を確認する

（１）PINGでの接続確認

PING コマンドを入力し、互いが接続できていることを確認する。
IP アドレスについては、「ＩＰアドレス／ホスト名」に従う。

- 基準分野横断基盤マシン　→分野横断基盤マシン
- 分野横断基盤マシン　　→基準分野横断基盤マシン

（２）エンドポイントURLでの接続確認

Web ブラウザ（IE6.0 等）のアドレスバーにエンドポイント URL を入力し、要求及び応答を確認する。

エンドポイント URL については、「エンドポイントＵＲＬ」に従う。

・ 基準分野横断基盤マシン　→分野横断基盤マシン

・ 分野横断基盤マシン　　→基準分野横断基盤マシン

（３）相互接続検証用に用意されたXML定義及びWSDLでの接続確認（TM1）

リクエスト・レスポンス型同期型レスポンス（以降、同期 2Way）を検証する。

・XML 定義及び WSDL の接続確認は、下記に示す処理とメッセージで行う。

表 ３-３　検証項目と確認方法（TM1）

No.	処理	メッセージ
1	リクエスト（要求）	・TM1_IN
2	レスポンス（応答）	・TM1_OUT

・ 分野横断基盤マシン（リクエスト）→基準分野横断基盤マシン（レスポンス）

・ 基準分野横断基盤マシン（リクエスト）→分野横断基盤マシン（レスポンス）

３．２．２　総合テスト及び相互接続検証

総合テスト及び相互接続検証する内容と確認方法について以下に示す。

表　３-４　検証項目と確認方法

No.	検証項目	確認方法
1	相互接続検証用に用意された XML 定義及び WSDL での接続確認	確認チェックリスト（詳細版）に従い、分野横断基盤の送受信ログと基準分野横断基盤の送受信ログを採取し、「送信したデータと受信したデータが同じ内容であること」、「同期通信ができていること」、「非同期で応答メッセージを返すことができていること」、「https 通信ができること」、「添付ファイル（本文内へ埋め込み型）が送受信でき、当該データを取り出し、内容確認ができること」、そして「日本語タグ/document/literal に対応していること」を確認する

上記を確認するための確認シーケンスを以下に示す。なお、ログの採取により検証するため、実施前に必ず手作業による時刻同期をとることとする。

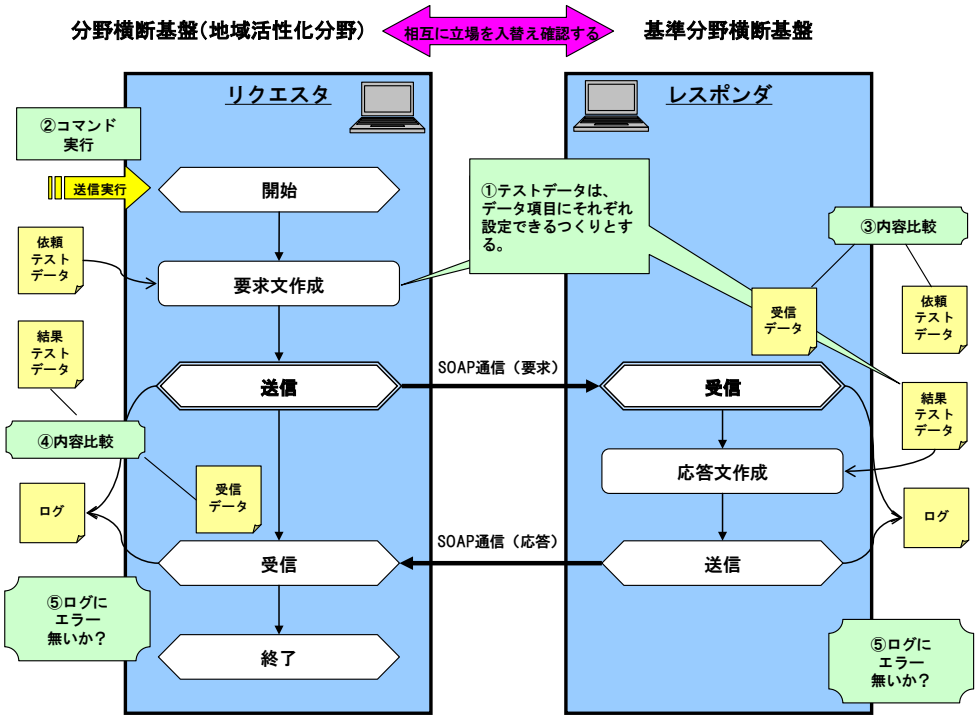

図　３-１　相互接続検証の確認シーケンス

（１）相互接続検証用に用意されたXML定義及びWSDLでの接続確認（TM1）

前述の 3.2.1 事前検証の記載内容と同様であるため、省略する。

（２）相互接続検証用に用意されたXML定義及びWSDLでの接続確認（TM2）

（TM2-1）リクエスト型受領 Ack あり（以降、1Way(受領)）を検証する。
（TM2-2）リクエスト・レスポンス型同期型レスポンス（以降、同期 2Way）を検証する。
（TM2-3）リクエスト・レスポンス型同期型受領 Ack＋非同期型レスポンス（以降、非同期 2way）を検証する。

・XML 定義及び WSDL の接続確認は、下記に示す処理とメッセージで行う。

表　3-5　検証項目と確認方法（TM2-1）

No.	処理	メッセージ
1	リクエスト（要求）	・TM1_IN
2	レスポンス（応答）	・受領 Ack

表　3-6　検証項目と確認方法（TM2-2）

No.	処理	メッセージ
1	リクエスト（要求）	・TM1_IN
2	レスポンス（応答）	・TM1_OUT

表　3-7　検証項目と確認方法（TM2-3）

No.	処理	メッセージ
1	リクエスト（要求）	・TM1_IN
2	レスポンス（応答）	・受領 Ack
3	リクエスト（要求）	・TM1_OUT
4	レスポンス（応答）	・受領 Ack

・ 分野横断基盤マシン（リクエスト）→基準分野横断基盤マシン（レスポンス）
・ 基準分野横断基盤マシン（リクエスト）→分野横断基盤マシン（レスポンス）

（３）相互接続検証用に用意されたXML定義及びWSDLでの接続確認（TM3）

（TM３-1）同期 2Way+SSL サーバ認証を検証する。
（TM３-2）同期 2Way+SSL サーバ認証&クライアント認証を検証する。

・事前にサーバ証明書、クライアント証明書を準備しておく。
・XML 定義及び WSDL の接続確認は、下記に示す処理とメッセージで行う。

表　3-8　検証項目と確認方法（TM3）

No.	処理	メッセージ
1	リクエスト（要求）	・TM1_IN
2	レスポンス（応答）	・TM1_OUT

・ 分野横断基盤マシン（リクエスト）→基準分野横断基盤マシン（レスポンス）
・ 基準分野横断基盤マシン（リクエスト）→分野横断基盤マシン（レスポンス）

（４）相互接続検証用に用意されたXML定義及びWSDLでの接続確認（TM4）

（TM４-1）同期 2Way+PF 規定添付ファイル（内包型）を検証する。
・XML 定義及び WSDL の接続確認は、下記に示す処理とメッセージで行う。

表 ３-９　検証項目と確認方法（TM4）

No.	処理	メッセージ
1	リクエスト（要求）	・TM1_IN_attached
2	レスポンス（応答）	・TM1_OUT_attached

・ 分野横断基盤マシン（リクエスト）→基準分野横断基盤マシン（レスポンス）
・ 基準分野横断基盤マシン（リクエスト）→分野横断基盤マシン（レスポンス）

３．２．３　スケジュール

相互接続検証を実施した、スケジュールを以下に示す。

表 ３-１０　相互接続検証スケジュール

フェーズ	11 月	12 月	1 月
開発 （基準分野横断基盤）			
開発 （分野横断基盤）			
事前検証(TM1)、総合テスト及び相互接続検証(TM1～TM4)			1/23 ○

・ 事前検証（機器設置、環境確認、テストパターン TM1 検証）
1 月 23 日（金） AM 10:00～AM 12:00
・ 総合テスト及び相互接続検証(テストパターン TM1～4 検証、チェックリスト記入)
1 月 23 日（金） PM 1:00～PM 3:00

３．２．４　検証場所

〒107-0052　東京都港区赤坂２－１７－２８　NTT 赤坂ビル（会議室内）

４　システム構成

４．１　システム概要

相互接続検証ではテストドライバを用いて、対象とする技術仕様の相互接続性の確認を行う。テストドライバは、送信処理を行う「リクエスタ」、受信処理を行う「レスポンダ」から構成され、図 ４-１に示すような流れで、分野横断基盤、基準分野横断基盤間の処理を行う。また、テストドライバに実装される機能の概要を表 ４-１に示す。

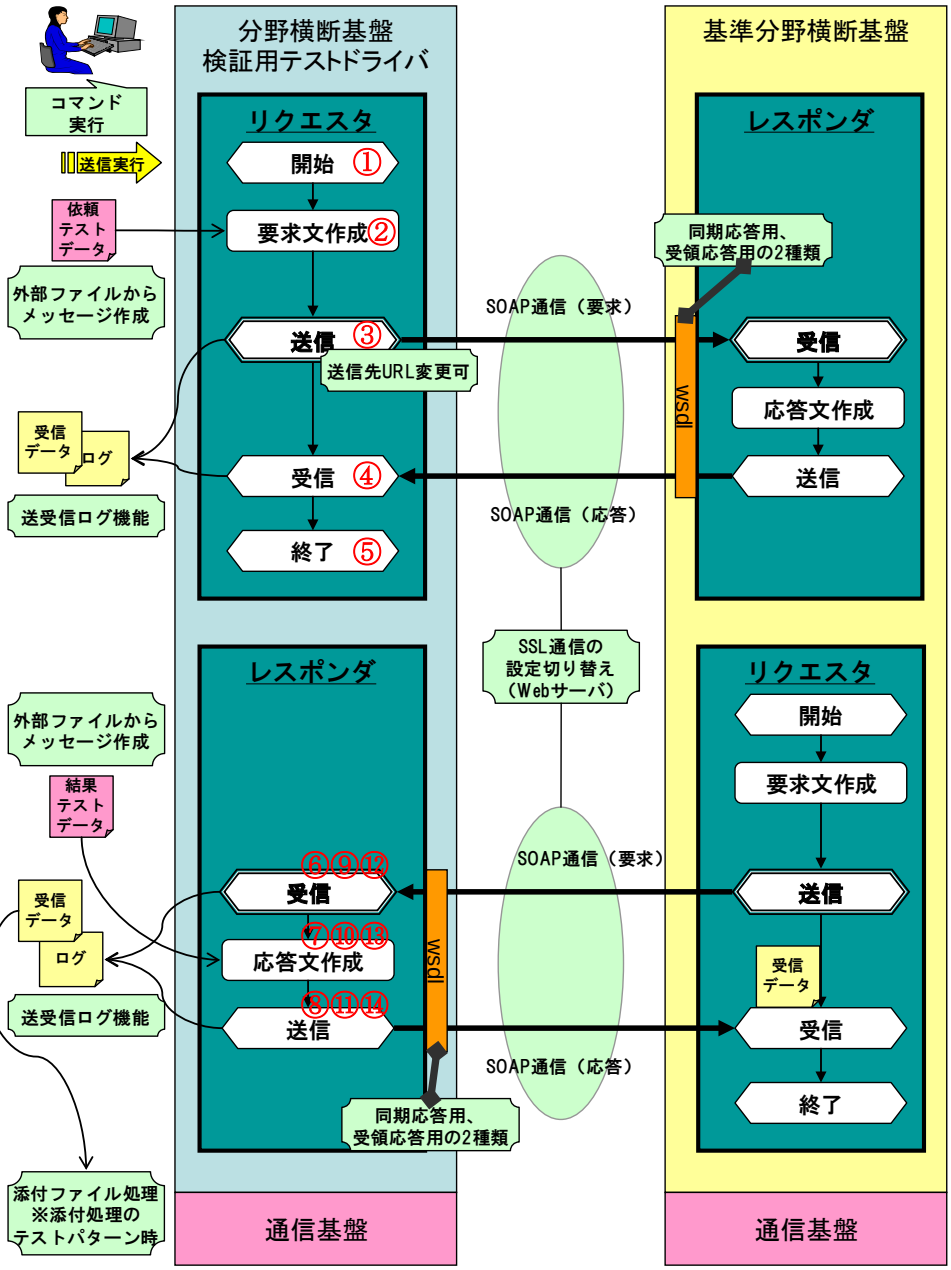

図　４-１　相互接続検証のシステム概要図

表 4-1　相互接続検証処理説明

No.	機能	詳細機能	処理概要
1	リクエスタ機能	開始	処理を開始する。
2		要求文作成	外部ファイルとして読み込んだ要求テストデータを元に SOAP 要求電文を作成する。
3		送信	外部設定ファイルより取得した送信先 URL に作成した SOAP 要求電文を送信する。 送信先 URL によってそれぞれ異なる通信手段を持つレスポンダ機能が動作する。 また、SSL 相互認証の場合、指定したクライアント証明書を用いて暗号化通信を行う。
4		受信	応答電文を解析しログ出力を行う。
5		終了	処理を終了する。
6	レスポンダ機能 (pf_suisin)	受信	要求電文を解析しログ出力を行う。 また、添付書類タグに値がセットされている場合、添付ファイル処理を行う。
7		応答文作成	外部ファイルとして読み込んだ応答テストデータを元に SOAP 応答電文を作成する。
8		送信	リクエスト元に作成した SOAP 応答電文を送信する。
9	レスポンダ機能 (pf_suisin_SSL_SVR)	受信	要求電文を解析しログ出力を行う。 リクエスト機能の送信処理との間で暗号化通信を行う。またその際にサーバ認証を行いサーバが正しい通信相手かどうかの確認を行う。
10		応答文作成	外部ファイルとして読み込んだ応答テストデータを元に SOAP 応答電文を作成する。
11		送信	リクエスト元に作成した SOAP 応答電文を送信する。
12	レスポンダ機能 (pf_suisin_SSL_CLI)	受信	要求電文を解析しログ出力を行う。 リクエスト機能の送信処理との間で暗号化通信を行う。またその際に相互認証を行いサーバ、クライアントがそれぞれ正しい通信相手かどうかの確認を行う。
13		応答文作成	外部ファイルとして読み込んだ応答テストデータを元に SOAP 応答電文を作成する。
14		送信	リクエスト元に作成した SOAP 応答電文を送信する。

４．２　インタフェース定義

４．２．１　WSDL定義

本検証では、2 種類の WSDL を定義し、相互接続検証を実施した。
以下に WSDL 定義を示す。

ア）PFサイト間電子封筒形式⇔PFサイト間電子封筒形式(Synchronous-2way.wsdl)

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="汎用同期型サービス WSDL" targetNamespace="urn:go.jp:xmlns:wsdl:1-01"
xmlns:oss1-wsdl="urn:go.jp:xmlns:wsdl:1-01" xmlns:oss1-xsd="urn:go.jp:xmlns:schema:1-01"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.xmlsoap.org/wsdl/">
    <documentation>作成日：2008/11/12</documentation>
    <types>
        <xsd:schema targetNamespace="urn:go.jp:xmlns:schema:1-01">
            <xsd:include schemaLocation="Envelope.xsd"/>
        </xsd:schema>
    </types>
    <message name="PF サイト間電子封筒形式">
        <part name="PF サイト間電子封筒形式" element="oss1-xsd:PF サイト間電子封筒形式"/>
    </message>
    <portType name="Synchronous-2wayPT">
        <operation name="Synchronous-2way">
            <input name="PF サイト間電子封筒形式 IN" message="oss1-wsdl:PF サイト間電子封筒形式"/>
            <output name="PF サイト間電子封筒形式 OUT" message="oss1-wsdl:PF サイト間電子封筒形式"/>
        </operation>
    </portType>
    <binding name="Synchronous-2waySOAPBinding" type="oss1-wsdl:Synchronous-2wayPT">
        <wsdlsoap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
        <operation name="Synchronous-2way">
            <wsdlsoap:operation soapAction="Synchronous-2way"/>
            <input name="PF サイト間電子封筒形式 IN">
                <wsdlsoap:body use="literal"/>
            </input>
            <output name="PF サイト間電子封筒形式 OUT">
                <wsdlsoap:body use="literal"/>
            </output>
        </operation>
    </binding>
    <service name="Synchronous-2wayService">
        <port name="Synchronous-2wayPT" binding="oss1-wsdl:Synchronous-2waySOAPBinding">
            <wsdlsoap:address location="http://somedomain/somelocation"/>
        </port>
    </service>
</definitions>
```

イ）PFサイト間電子封筒形式⇔受領Ack(Synchronous-1way.wsdl)

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="汎用非同期型サービス WSDL" targetNamespace="urn:go.jp:xmlns:wsdl:1-01"
xmlns:oss1-wsdl="urn:go.jp:xmlns:wsdl:1-01" xmlns:oss1-xsd="urn:go.jp:xmlns:schema:1-01"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://schemas.xmlsoap.org/wsdl/">
    <documentation>作成日：2008/11/12</documentation>
    <types>
        <xsd:schema targetNamespace="urn:go.jp:xmlns:schema:1-01">
            <xsd:include schemaLocation="Envelope.xsd"/>
            <xsd:include schemaLocation="AcceptAck.xsd"/>
        </xsd:schema>
    </types>
    <message name="PF サイト間電子封筒形式">
        <part name="PF サイト間電子封筒形式" element="oss1-xsd:PF サイト間電子封筒形式"/>
    </message>
    <message name="受領 Ack">
        <part name="受領 Ack" element="oss1-xsd:受領 Ack"/>
    </message>
    <portType name="Asynchronous-1wayPT">
        <operation name="Asynchronous-1way">
            <input name="PF サイト間電子封筒形式" message="oss1-wsdl:PF サイト間電子封筒形式"/>
            <output name="受領 Ack" message="oss1-wsdl:受領 Ack"/>
        </operation>
    </portType>
    <binding name="Asynchronous-1waySOAPBinding" type="oss1-wsdl:Asynchronous-1wayPT">
        <wsdlsoap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
        <operation name="Asynchronous-1way">
            <wsdlsoap:operation soapAction="Asynchronous-1way"/>
            <input name="PF サイト間電子封筒形式">
                <wsdlsoap:body use="literal"/>
            </input>
            <output name="受領 Ack">
                <wsdlsoap:body use="literal"/>
            </output>
        </operation>
    </binding>
    <service name="Asynchronous-1wayService">
        <port name="Asynchronous-1wayPT" binding="oss1-wsdl:Asynchronous-1waySOAPBinding">
            <wsdlsoap:address location="http://somedomain/somelocation"/>
        </port>
    </service>
</definitions>
```

４．２．２　サイト間電文定義

本検証では、SOAP 通信におけるメッセージ形式をサイト間電子封筒形式、受領 ACK 形式の 2 種類を定義し、相互接続検証を実施した。

ア）PFサイト間電子封筒形式

表 4-2　PF サイト間電子封筒形式

No.	ﾃﾞｰﾀ項目	ﾃﾞｰﾀ型	桁数	コード		出現回数		項目の説明
				ＣＤ	コード名	最小	最大	
1	PF サイト間 電子封筒形式					1	1	
2	共通ヘッダ					1	1	
3	TO	X	1024			0	1	非同期メッセージによる送信先 URI
4	MsgID	X	1024			0	1	メッセージ毎に固有となる ID
5	RelatesTo	X	1024			0	1	本メッセージの契機として関連するメッセージの MsgID
6	ReplyTo	X	1024			0	1	非同期メッセージによる返信先 URI（同期呼び出し時不要）（このメッセージの処理結果の返信先アドレス）
7	受付番号	X	256			1	1	一連の業務 1 つに割り振られる識別子
8	共通ｺﾘﾚｰｼｮﾝｾｯﾄ	X	256			0	1	BP インスタンス識別用（BPM 用）（本文の業務項目をコリレーションセットとする場合は不要）
9	ビジネスプロセス 制御情報	X	10			0	1	ビジネスプロセス呼び出し側からのフロー制御（本文（申請データ等）でフロー制御する場合は不要）
10	業務サービス 結果情報	X	10			0	1	呼び出した業務サービスの実行結果情報（ユニット呼び出し時や、本文の結果内容でフロー制御する場合は不要）
11	結果情報	X	1			0	1	システム的なサービスの呼び出し処理が正常(0)終了したか異常(1)かの結果情報
12	システムエラー 報告	X	1024			0	1	システム的なサービスの呼出処理がエラー時に、コード化されたエラー状態を戻す情報

No.	ﾃﾞｰﾀ項目	ﾃﾞｰﾀ型	桁数	コード		出現回数		項目の説明
				ＣＤ	コード名	最小	最大	
13	メッセージ属性					0	N	ライフイベントに関する属性とその値を入れる。例、引越しなら、転出元と先の自治体
14	属性名	X	256			1	1	
15	属性値	X	256			1	1	
16	添付書類					0	N	各サイトへ渡す XML を、添付データとして扱う
17	添付書類名称	X				1	1	内容がわかる名称をつける
18	添付書類 ファイル名称	X				1	1	内容の形式をファイル名としてあつかう。例、選出元自治体申請書.xml
19	添付書類内容	X				0	1	各サイトへ渡す XML を、添付データとして格納。CDATA 等で扱う。
20	添付書類参照情報	X				0	1	添付ファイル本体の外部参照を URL の形で記載する。

イ）受領Ack

表 4-3　受領 Ack

No.	ﾃﾞｰﾀ項目	ﾃﾞｰﾀ型	桁数	コード		出現回数		項目の説明
				ＣＤ	コード名	最小	最大	
1	受領 Ack					1	1	
2	共通ヘッダ					1	1	
3	TO	X	1024			0	1	非同期メッセージによる送信先 URI
4	MsgID	X	1024			0	1	メッセージ毎に固有となる ID
5	RelatesTo	X	1024			0	1	本メッセージの契機として関連するメッセージの MsgID
6	ReplyTo	X	1024			0	1	非同期メッセージによる返信先 URI（同期呼び出し時不要）（このメッセージの処理結果の返信先アドレス）
7	受付番号	X	256			1	1	一連の業務 1 つに割り振られる識別子
8	共通ｺﾘﾚｰｼｮﾝｾｯﾄ	X	256			0	1	BP インスタンス識別用（BPM 用）（本文の業務項目をコリレーションセットとする場合は不要）
9	ビジネスプロセス制御情報	X	10			0	1	ビジネスプロセス呼び出し側からのフロー制御（本文（申請データ等）でフロー制御する場合は不要）
10	業務サービス結果情報	X	10			0	1	呼び出した業務サービスの実行結果情報（ユニット呼び出し時や、本文の結果内容でフロー制御する場合は不要）
11	結果情報	X	1			0	1	システム的なサービスの呼び出し処理が正常(0)終了したか異常(1)かの結果情報

No.	ﾃﾞｰﾀ項目	ﾃﾞｰﾀ型	桁数	コード		出現回数		項目の説明
				ＣＤ	コード名	最小	最大	
12	システムエラー報告	X	1024			0	1	システム的なサービスの呼び出し処理がエラー時に、コード化されたエラー状態を戻す情報
13	受領ステータス	X	1			1	1	"0".. 成功／"1".. 異常有り
14	受領日時	日付時間情報(※)				1	1	受領日時を入れる
15	備考	X	1024			0	1	備考情報を入れる

表 4-4　日付時間情報

No.	データ項目	ﾃﾞｰﾀ型	桁数	コード		出現回数		項目の説明
				ＣＤ	ｺｰﾄﾞ名	最小	最大	
1	日付					1	1	日付情報
2	年	9	4			1	1	該当年を西暦にて指定
3	月	9	2			1	1	
4	日	9	2			1	1	
5	時	9	2			1	1	
6	分	9	2			1	1	
7	秒	9	2			1	1	

４．３　環境設定

各システムは、ネットワーク情報など接続に必要な情報を事前に設定するものとする。設定に必要な情報を以下に記す。

４．３．１　IPアドレス／ホスト名

表 4-5　IP アドレス／ホスト名一覧

No.	施設	機器	IP アドレス	ホスト名
1	NTT 赤坂ビル（会議室）	基準分野横断基盤	192.168.1.200	pf-kijyun1
2		地域活性化分野：住民生活向上（分野横断基盤）	192.168.1.11	pf-bunya1

※C:¥WINDOWS¥system32¥drivers¥etc¥hosts ファイルへ上記内容を追加しておくこととする。（OS を C ドライブへ標準インストールした場合のパス）

４．３．２　エンドポイントＵＲＬ

表 4-6　エンドポイント URL 一覧

No.	相互接続検証実施用の定義			
	テストケース		wsdl	エンドポイント
1	TM 1		Synchronous-2way.wsdl（Synchronous-2way）	（基準分野横断基盤） http://pf-kijyun1/pf_suisin/TM1.asmx （分野横断基盤） http://pf-bunya1/pf_suisin/services/TM1
2	TM 2	TM 2-1	Asynchronous-1way.wsdl（Asynchronous-1way）	（基準分野横断基盤） http://pf-kijyun1/pf_suisin/TM2-1.asmx （分野横断基盤） http://pf-bunya1/pf_suisin/services/TM2-1
3		TM 2-2	Synchronous-2way.wsdl（Synchronous-2way）	（基準分野横断基盤） http://pf-kijyun1/pf_suisin/TM2-2.asmx （分野横断基盤） http://pf-bunya1/pf_suisin/services/TM2-2
4		TM 2-3	Asynchronous-1way.wsdl（Asynchronous-1way）	（基準分野横断基盤） http://pf-kijyun1/pf_suisin/TM2-3.asmx （分野横断基盤） http://pf-bunya1/pf_suisin/services/TM2-3
5	TM 3	TM 3-1	Synchronous-2way.wsdl（Synchronous-2way）	（基準分野横断基盤） https://pf-kijyun1/pf_suisin_SSL_SVR/TM3-1.asmx （分野横断基盤） https://pf-bunya1/pf_suisin_SSL_SVR/services/TM3-1
6		TM 3-2	Synchronous-2way.wsdl（Synchronous-2way）	（基準分野横断基盤） https://pf-kijyun1/pf_suisin_SSL_CLI/TM3-2.asmx （分野横断基盤） https://pf-bunya1/pf_suisin_SSL_CLI/services/TM3-2

No.	相互接続検証実施用の定義			
	テストケース		wsdl	エンドポイント
7	TM4	TM4-1	Synchronous-2way.wsdl（Synchronous-2way）	（基準分野横断基盤） http://pf-kijyun1/pf_suisin/TM4-1.asmx （分野横断基盤） http://pf-bunya1/pf_suisin/services/TM4-1

４．３．３　サーバ証明書／クライアント証明書

テストモデル（TM3）において、各システムは SSL サーバ証明書／SSL クライアント証明書を事前にインストール設定するものとする。

（１）事前準備

ア）CSR（証明書発行要求）作成情報の提供

CSR（証明書発行要求）作成に必要な情報を基準分野横断基盤側から分野横断基盤側に送付する。

表 4-7　CSR に入力する情報

【CSR に入力する情報（ディスティングイッシュネーム）】

項目	説明	値
コモンネーム	SSL 接続サイトの URL(FQDN)　（例：sample.verisign.co.jp）	pf-bunya1
組織名	申請団体の正式な英語組織名　（例：VeriSign Japan K.K.）	pf-suisin
部門名	部署やサービスなど任意の判別文字列　（例：Web Sales）	hikkoshi
市区町村名	所在地情報　（例：Chuo-ku）	
都道府県名	所在地情報　（例：Tokyo）	
国名	日本の国別記号 JP　（例：JP）	JP

イ）CSR（証明書発行要求）の作成、送付

CSR に入力する情報をもとに、分野横断基盤側（自身のサーバ上）で作成を行い、準分野横断基盤側に送付する。

表 4-8　CSR フォーマット

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB4DCCAUkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTEV
MBMGA1UEBxMMWW9rb2hhbWEtc2hpMRIwEAYDVQQKEwlwZi1zdWlzaW4xETAPBgNV
BAsTCGhpa2tvc2hpMRIwEAYDVQQDEwlwZi1idW55YTExKzApBgkqhkiG9w0BCQEW
HHd3dy1hZG1pbkBzZXJ2ZXIuZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAK/aXrUpn95TDOE3UzGj2/xqXnJbzZAitHpEvHo7Qlpu0XTljYTT
G1WyBye7L+3yGwc3l/FTmMNedgAwpJm5WarDZIj4Ij6woEnyiY71MWsDi+piJdBt
+FnJ2Srz/eC0m0PkS0dQAqxVXkFKKiltlyK96iu7KLtBvGFCJB1FHDCDAgMBAAGg
ADANBgkqhkiG9w0BAQUFAAOBgQAWbrHFYewtmtAGwiQ4F8rPszUHas8Og2g9mh1u
UNmOPZDa1VBGdlUr8ZUAs6HrAlBrvw5jWLi/C/braf9iOoBiw3pd4Dtnhunjs1DR
lnF6mwP1ro75CzmerSfEXQdOK/B32Dx/tz44DmFr0X4uv04Wf0wRMWs4eTTCvXUA
008taQ==
-----END CERTIFICATE REQUEST-----
```

ウ）　証明書の発行、送付

送付された CSR をもとに、基準分野横断基盤側で各証明書を発行し、分野横断基盤側に送付する。

■CA 証明書（cacert.cer）

```
Certificate：
  DATA：
    Version：3
    SerialNumber：1
    Signature Algorithm: SHA1WithRSAEncryption
    Issuer　：
      C=JP, O=pfsuisin, OU=kijyun, CN=kijyun1, /Email=kijyun1@pfsuisin.com
    Validity：
      notBefore：Jan 20 01:45:52 2009 UTC
      notAfter　：Jan 27 01:45:52 2009 UTC
    Subject：
      C=JP, O=pfsuisin, OU=kijyun, CN=kijyun1, /Email=kijyun1@pfsuisin.com

    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (512 bit)
        Modulus (512 bit):
          d0:61:41:c9:dd:32:6d:2c:85:f8:f4:20:d3:1c:82:7d:78:53:60:e6:
          74:29:13:74:d7:d1:65:67:1f:fa:b4:4c:35:d5:9e:77:fa:4f:f8:73:
          46:d7:be:7d:69:c6:30:03:80:72:e8:49:0b:ac:a3:bc:07:9f:a3:ed:
          ca:38:f9:77:
        Exponent:
          00:01:00:01:

    X509v3 extensions:
      x509 Basic Constraints: [critical]
        CA:TRUE
        PathLenConstraint:NULL
      x509 Key Usage: [critical]
        digitalSignature, nonRepudiation, keyCertSign, cRLSign (0xc6)
      x509 Subject Key Identifier:
        5b:49:e4:96:23:06:47:2c:15:88:2d:cb:a7:86:89:ae:0a:d5:c6:f5:

  Signature Algorithm: SHA1WithRSAEncryption
    8e:24:b3:12:82:f3:48:02:aa:93:16:43:0c:fa:f7:f8:04:b3:
    89:24:5d:1f:2b:38:b9:ff:00:44:76:e3:30:b8:50:40:9f:c7:
    59:fc:d1:75:0a:4d:5d:7e:fb:11:b5:15:10:73:87:90:b5:9c:
    4b:d0:2a:8f:62:1b:f0:1f:52:39:
```

■サーバ証明書（sv.cer）

```
Certificate：
  DATA：
    Version：3
    SerialNumber：2001
    Signature Algorithm: SHA1WithRSAEncryption
    Issuer　：
      C=JP, O=pfsuisin, OU=kijyun, CN=kijyun1, /Email=kijyun1@pfsuisin.com
    Validity：
      notBefore：Jan 20 02:02:49 2009 UTC
      notAfter　：Jan 27 01:45:52 2009 UTC
    Subject：
      C=JP, ST=Kanagawa, L=Yokohama-shi, O=pf-suisin, OU=hikkoshi, CN=pf-bunya1,
/Email=www-admin@server.example.com

    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          af:da:5e:b5:29:9f:de:53:0c:e1:37:53:31:a3:db:fc:6a:5e:72:5b:
          cd:90:22:b4:7a:44:bc:7a:3b:42:5a:6e:d1:74:e5:8d:84:d3:1b:55:
          b2:07:27:bb:2f:ed:f2:1b:07:37:97:f1:53:98:c3:5e:76:00:30:a4:
          99:b9:59:aa:c3:64:88:f8:22:3e:b0:a0:49:f2:89:8e:f5:31:6b:03:
          8b:ea:62:25:d0:6d:f8:59:c9:d9:2a:f3:fd:e0:b4:9b:43:e4:4b:47:
          50:02:ac:55:5e:41:4a:2a:29:6d:97:22:bd:ea:2b:bb:28:bb:41:bc:
          61:42:24:1d:45:1c:30:83:
        Exponent:
          00:01:00:01:

    X509v3 extensions:
      x509 Basic Constraints:
        CA:FALSE
        PathLenConstraint:NULL
      x509 Key Usage:
        digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment,
keyAgreement, keyCertSign, cRLSign (0xfe)
      x509 Authority Key Identifier:
        5b:49:e4:96:23:06:47:2c:15:88:2d:cb:a7:86:89:ae:0a:d5:c6:f5:
      x509 Subject Key Identifier:
        5c:ed:21:10:91:bf:6a:9c:83:91:8a:05:f5:7e:48:13:da:13:b5:c7:

  Signature Algorithm: SHA1WithRSAEncryption
    25:27:60:4d:e4:ce:c0:53:6f:aa:a3:dd:a2:81:d4:26:79:4f:
    d0:d5:c1:54:75:bf:d2:fd:6c:33:a4:70:ba:03:b2:6c:0c:58:
    78:1c:6c:85:29:ca:50:79:b4:ab:20:e4:75:2d:92:aa:9e:7e:
    34:09:99:b5:75:f8:13:66:5d:5d:
```

■クライアント証明書（pfbunya1.p12）

```
PKCS#12 file version : 3

 ----- PKCS#12 v1 Private Key Bag -----
Friendly Name: pf-bunya1
Local Key ID: 01 00 00 00
RSA Private Key:
  modules:
    b0:7f:9b:38:f2:2b:93:3d:ef:b2:a9:11:5f:ec:01:1b:b6:79:03:9d:
    04:16:e0:bc:2e:52:ab:32:15:84:76:cf:c2:3a:c9:ae:74:eb:f6:92:
    99:26:29:fc:1a:28:83:ab:dd:95:1e:33:7c:69:d5:64:80:95:41:49:
    3f:9a:56:75:
  publicExponent:
    00:01:00:01:
  privateExponent:
    62:48:fd:18:4e:0b:23:f8:76:95:87:fe:8b:ea:f1:87:0c:2b:01:6f:
    1b:8a:dd:e5:0c:ea:ae:38:ba:b0:c4:33:ea:c2:c5:ec:37:ab:35:30:
    0f:20:d6:2c:89:d0:75:8b:43:ef:71:e9:67:b3:31:12:41:e7:70:50:
    41:75:ef:c1:
  prime1:
    da:52:fa:74:78:60:72:d2:bb:37:a1:21:b3:aa:ad:27:d7:18:82:11:
    e1:bf:83:75:41:43:b1:4a:eb:e8:da:91:
  prime2:
    ce:f4:df:7c:8e:f9:17:76:59:df:e0:fb:90:d5:01:b1:60:f6:c0:0d:
    ec:7a:e8:da:10:30:71:da:86:93:87:a5:
  exponent1:
    1c:47:8d:4b:92:e0:23:5f:6a:82:bd:2b:69:63:5d:44:80:d7:1a:da:
    08:1c:cf:81:5b:af:d2:02:3b:66:91:11:
  exponent2:
    bf:c1:2d:ed:a8:3f:6e:18:cf:af:5b:33:5b:ff:b1:00:dc:19:e4:db:
    41:d8:a4:35:a0:38:72:d5:8a:49:d9:ad:
  coefficient:
    53:fc:71:36:a8:a0:07:05:ef:bb:ef:cf:9c:e5:cd:66:b7:6e:b2:7c:
    16:6a:a7:bc:31:6f:6d:7d:c3:53:63:75:
 ------- END of Private Key Bag -------

 -------- PKCS#12 v1 Cert Bag ---------
Friendly Name: kijyun1
Local Key ID: 00 00 00 00
Certificate :
  DATA :
    Version : 3
    SerialNumber : 1
    Signature Algorithm: SHA1WithRSAEncryption
    Issuer   :
      C=JP, O=pfsuisin, OU=kijyun, CN=kijyun1, /Email=kijyun1@pfsuisin.com
    Validity :
      notBefore : Jan 20 01:45:52 2009 UTC
      notAfter   : Jan 27 01:45:52 2009 UTC
    Subject :
      C=JP, O=pfsuisin, OU=kijyun, CN=kijyun1, /Email=kijyun1@pfsuisin.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (512 bit)
        Modulus (512 bit):
          d0:61:41:c9:dd:32:6d:2c:85:f8:f4:20:d3:1c:82:7d:78:53:60:e6:
          74:29:13:74:d7:d1:65:67:1f:fa:b4:4c:35:d5:9e:77:fa:4f:f8:73:
          46:d7:be:7d:69:c6:30:03:80:72:e8:49:0b:ac:a3:bc:07:9f:a3:ed:
          ca:38:f9:77:
        Exponent:
          00:01:00:01:
```

※次ページに続く

■クライアント証明書（pfbunya1.p12）　前ページ続き

```
        X509v3 extensions:
          x509 Basic Constraints: [critical]
            CA:TRUE
            PathLenConstraint:NULL
          x509 Key Usage: [critical]
            digitalSignature, nonRepudiation, keyCertSign, cRLSign (0xc6)
          x509 Subject Key Identifier:
            5b:49:e4:96:23:06:47:2c:15:88:2d:cb:a7:86:89:ae:0a:d5:c6:f5:

      Signature Algorithm: SHA1WithRSAEncryption
        8e:24:b3:12:82:f3:48:02:aa:93:16:43:0c:fa:f7:f8:04:b3:
        89:24:5d:1f:2b:38:b9:ff:00:44:76:e3:30:b8:50:40:9f:c7:
        59:fc:d1:75:0a:4d:5d:7e:fb:11:b5:15:10:73:87:90:b5:9c:
        4b:d0:2a:8f:62:1b:f0:1f:52:39:
    ---------- END of Cert Bag ----------

    -------- PKCS#12 v1 Cert Bag ---------
  Friendly Name: pf-bunya1
  Local Key ID: 01 00 00 00
  Certificate :
    DATA :
      Version : 3
      SerialNumber : 8
      Signature Algorithm: SHA1WithRSAEncryption
      Issuer  :
        C=JP, O=pfsuisin, OU=kijyun, CN=kijyun1, /Email=kijyun1@pfsuisin.com
      Validity :
        notBefore : Jan 20 05:17:32 2009 UTC
        notAfter  : Jan 27 01:45:52 2009 UTC
      Subject :
        C=JP, O=pfsuisin, OU=kijyun, CN=pf-bunya1,

      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (512 bit)
          Modulus (512 bit):
            b0:7f:9b:38:f2:2b:93:3d:ef:b2:a9:11:5f:ec:01:1b:b6:79:03:9d:
            04:16:e0:bc:2e:52:ab:32:15:84:76:cf:c2:3a:c9:ae:74:eb:f6:92:
            99:26:29:fc:1a:28:83:ab:dd:95:1e:33:7c:69:d5:64:80:95:41:49:
            3f:9a:56:75:
          Exponent:
            00:01:00:01:

      X509v3 extensions:
        x509 Basic Constraints: [critical]
          CA:TRUE
          PathLenConstraint:00
        x509 Key Usage: [critical]
          digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment,
  keyAgreement, keyCertSign, cRLSign (0xfe)
        x509 Authority Key Identifier:
          5b:49:e4:96:23:06:47:2c:15:88:2d:cb:a7:86:89:ae:0a:d5:c6:f5:
        x509 Subject Key Identifier:
          c6:a7:e3:52:f7:af:a7:47:93:29:01:87:88:4c:42:fb:a2:b1:5c:63:

      Signature Algorithm: SHA1WithRSAEncryption
        b6:e9:60:42:95:a7:7f:bd:fb:00:35:99:f0:43:f5:33:40:2b:
        ec:2a:db:59:fa:e0:5e:f9:cd:78:4a:25:d2:42:e7:bc:e4:fa:
        d3:bb:ba:dc:d2:91:3e:19:b8:06:ce:6b:2b:ac:d6:84:7a:64:
        cc:8f:34:4b:9b:b2:ea:1d:6a:2c:
    ---------- END of Cert Bag ----------
```

（２）証明書の取込

基準分野横断基盤側が用意した各証明書を分野横断基盤マシンへインストールする。今回使用する証明書はテスト用となっているため、信頼された証明書として、ブラウザやテストドライバ側で処理するものとする。

■サーバ側取り込み(CA 証明書,サーバ証明書)
用意されたサーバ証明書を任意の位置(今回は"C:/Program Files/Hitachi/Cosminexus/httpsd/conf/ssl/server/sv.pem")に格納する。
サーバ証明書作成時に使用したサーバ秘密キーを任意の位置(今回は"C:/Program Files/Hitachi/Cosminexus/httpsd/conf/ssl/server/pkey.pem")に格納する。
用意された CA 証明書を任意の位置(今回は"C:/Program Files/Hitachi/Cosminexus/httpsd/conf/ssl/cacert/cacert.pem")に格納する。
<Cosminexus インストールディレクトリ>¥httpsd¥servers¥<Web サーバ>¥conf¥httpsd.conf に格納した証明書を含む SSL の設定を追記する。
指定は以下のとおり

```
ServerName 192.168.1.11
Listen 443
<VirtualHost 192.168.1.11:443>
SSLEnable
#提供を受けたサーバ証明書※３
SSLCertificateFile "C:/Program Files/Hitachi/Cosminexus/httpsd/conf/ssl/server/sv.pem"
#作成したサーバ秘密キー※１
SSLCertificateKeyFile "C:/Program Files/Hitachi/Cosminexus/httpsd/conf/ssl/server/pkey.pem"
#提供を受けた CA ルート証明書※４
SSLCACertificateFile "C:/Program Files/Hitachi/Cosminexus/httpsd/conf/ssl/cacert/cacert.pem"
#相互認証試験時設定　※１
SSLVerifyClient 2
#サーバ認証試験時設定　※１
#SSLVerifyClient 0
SSLVerifyDepth 2
SSLExportClientCertificates
SSLExportCertChainDepth 2
</VirtualHost>
```

※１　サーバ認証、クライアント認証時にそれぞれ設定が異なるため設定を変更しサーバの再起動を行う。

■クライアント側取り込み(CA 証明書,クライアント証明書)
「証明書インポートウィザード」を使用し、ブラウザへ信頼されたルート証明機関として登録する。
JAVA JDK を使用し、CA 証明書をキーストアに登録する。コマンドは以下のとおり

```
keytool -import -keystore "C:/soapclient/SSL/ks" -file "C:/Program Files/Hitachi/Cosminexus/httpsd/conf/ssl/cacert/cacert.pem"
```

※"C:/soapclient/SSL/ks"は任意に作成するキーストアファイル
※"C:/Program Files/Hitachi/Cosminexus/httpsd/conf/ssl/cacert/cacert.pem"は任意位置に格納された CA 証明書
リクエスタ機能にて使用するプロパティとして以下を指定する。

```
#CA ルート証明書を格納したキーストア※１
javax.net.ssl.trustStore=C:/soapclient/SSL/ks
#CA ルート証明書を格納したキーストアパスワード※２
javax.net.ssl.trustStorePassword=pfsuisin
#クライアント証明書※３
javax.net.ssl.keyStore=C:/soapclient/SSL/pfbunya1.p12
javax.net.ssl.keyStorePassword=pfsuisin
javax.net.ssl.keyStoreType=pkcs12
```

※１前述したキーストアファイル
※２(※１)にて設定したキーストアパスワード
※３"C:/soapclient/SSL/pfbunya1.p12"は任意位置に格納されたクライアント証明書、指定されたパスワード、ファイル形式

４．３．４　その他

検証機器にはシステム保護のためウィルス対策ソフト「Antivirus」のインストールを行う。

４．４　テストデータ

基準分野横断基盤との相互接続検証に用いた、テストデータを以下に示す。

（１）TM1_IN.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<PF サイト間電子封筒形式>
<共通ヘッダ>
<受付番号>20090123BB@0001</受付番号>
</共通ヘッダ>
<メッセージ属性>
<属性名>userID</属性名>
<属性値>pf0001</属性値>
</メッセージ属性>
<メッセージ属性>
<属性名>地域情報プラットフォーム相互接続検証用メッセージ</属性名>
<属性値>子育て支援　情報提供</属性値>
</メッセージ属性>
</PF サイト間電子封筒形式>
```

（２）TM1_OUT.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<PF サイト間電子封筒形式>
<共通ヘッダ>
<受付番号>20090123BB@0001</受付番号>
<業務サービス結果情報>100</業務サービス結果情報>
<結果情報>0</結果情報>
</共通ヘッダ>
<メッセージ属性>
<属性名>userID</属性名>
<属性値>pf0001</属性値>
</メッセージ属性>
<メッセージ属性>
<属性名>地域情報プラットフォーム相互接続検証用メッセージ</属性名>
<属性値>子育て支援　情報提供</属性値>
</メッセージ属性>
</PF サイト間電子封筒形式>
```

（３）受領Ack.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<受領 Ack>
<共通ヘッダ>
<受付番号>20090123BB@0001</受付番号>
<業務サービス結果情報>100</業務サービス結果情報>
<結果情報>0</結果情報>
</共通ヘッダ>
<受領ステータス>0</受領ステータス>
<受領日時>
<日付>
<年>2009</年>
<月>01</月>
<日>23</日>
</日付>
<時>13</時>
<分>30</分>
<秒>30</秒>
</受領日時>
</受領 Ack>
```

（４）TM1_IN_attached.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<PF サイト間電子封筒形式>
<共通ヘッダ>
<受付番号>20090123BB@0001</受付番号>
</共通ヘッダ>
<メッセージ属性>
<属性名>userID</属性名>
<属性値>pf0001</属性値>
</メッセージ属性>
<メッセージ属性>
<属性名>地域情報プラットフォーム相互接続検証用メッセージ</属性名>
<属性値>子育て支援　情報提供</属性値>
</メッセージ属性>
<添付書類>
<添付書類名称>子育て支援情報提供その１</添付書類名称>
<添付書類ファイル名称>attached.txt</添付書類ファイル名称>
<添付書類内容>
gZqCu4LmlZeOc4K+guaC6IGaDQoNCg0KgUCBeZXpgueCtYLMj+6V8YF6DQoNCoFAgUCCUYJPgk+
CWJROglGMjoJQk/qCyY5zlq+J74rZgsWXv5edi7OOuoLwikqNw4Kigr2CtYLcgreBQg0KgUANCoFAgU
CNoYnxgs2BQYK7guaVl45zgsyTwY5ZgsWCoILpk6SVhYLwjmeCwYK9gqiXv5edgvCCooKtgsKCqYKyj
9CJ7oKzgrmCxIKigr2CvoKrgtyCt4FCDQqBQIFADQqBQIFAk6SVhYLwioiXcIK1gr2DZoNVgVuDZ43s
guiCyYLgkqeQ7YK1gsSCooK9gr6Cq4LcgreBQiANCg0KgUCBQIKyicaRsIK7guuCwYLEgrKOUYnBgq
2CvoKzgqKBQg0KDQoNCoFAgUCBn5BcgrWNnoLdivqK1IFGgUCCUYJPgk+CV5ROglCCUYyOglGC
U5P6gWCCUYJPgk+CWJROglCMjoJRgk+T+g0KDQqBQIFAgZ+S6Ij1gUCBQIFAgUCBRoFAglWCT5a
8gWmS6Ij1gvCStIKmgr2P6o2Hgs2BQZKKkUmCyYLmguiMiJLogrWC3IK3gWoNCg0KgUCBQIGfkFy
CtY2egt2Ri4z7gUaBQIK7guaVl45zgUCPWpavg1SBW4Nyg1iJ2w0KDQo=</添付書類内容>
</添付書類>
<添付書類>
<添付書類名称>子育て支援情報提供その２</添付書類名称>
<添付書類ファイル名称>attached.pdf</添付書類ファイル名称>
<添付書類内容>※ＰＤＦファイルを BASE64 エンコーディングした値をセット</添付書類内容>
</添付書類>
</PF サイト間電子封筒形式>
```

（５）TM1_OUT_attached.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<PF サイト間電子封筒形式>
<共通ヘッダ>
<受付番号>20090123BB@0001</受付番号>
<業務サービス結果情報>100</業務サービス結果情報>
<結果情報>0</結果情報>
</共通ヘッダ>
<メッセージ属性>
<属性名>userID</属性名>
<属性値>pf0001</属性値>
</メッセージ属性>
<メッセージ属性>
<属性名>地域情報プラットフォーム相互接続検証用メッセージ</属性名>
<属性値>子育て支援　情報提供</属性値>
</メッセージ属性>
<添付書類>
<添付書類名称>子育て支援情報提供その１</添付書類名称>
<添付書類ファイル名称>attached.txt</添付書類ファイル名称>
<添付書類内容>
gZqCu4LmlZeOc4K+guaC6IGaDQoNCg0KgUCBeZXpgueCtYLMj+6V8YF6DQoNCoFAgUCCUYJPgk+
CWJROglGMjoJQk/qCyY5zlq+J74rZgsWXv5edi7OOuoLwikqNw4Kigr2CtYLcgreBQg0KgUANCoFAgU
CNoYnxgs2BQYK7guaVl45zgsyTwY5ZgsWCoILpk6SVhYLwjmeCwYK9gqiXv5edgvCCooKtgsKCqYKyj
9CJ7oKzgrmCxIKigr2CvoKrgtyCt4FCDQqBQIFADQqBQIFAk6SVhYLwioiXcIK1gr2DZoNVgVuDZ43s
guiCyYLgkqeQ7YK1gsSCooK9gr6Cq4LcgreBQiANCg0KgUCBQIKyicaRsIK7guuCwYLEgrKOUYnBgq
2CvoKzgqKBQg0KDQoNCoFAgUCBn5BcgrWNnoLdivqK1IFGgUCCUYJPgk+CV5ROglCCUYyOglGC
U5P6gWCCUYJPgk+CWJROglCMjoJRgk+T+g0KDQqBQIFAgZ+S6Ij1gUCBQIFAgUCBRoFAglWCT5a
8gWmS6Ij1gvCStIKmgr2P6o2Hgs2BQZKKkUmCyYLmguiMiJLogrWC3IK3gWoNCg0KgUCBQIGfkFy
CtY2egt2Ri4z7gUaBQIK7guaVl45zgUCPWpavg1SBW4Nyg1iJ2w0KDQo=</添付書類内容>
</添付書類>
<添付書類>
<添付書類名称>子育て支援情報提供その２</添付書類名称>
<添付書類ファイル名称>attached.pdf</添付書類ファイル名称>
<添付書類内容>※ＰＤＦファイルを BASE64 エンコーディングした値をセット</添付書類内容>
</添付書類>
</PF サイト間電子封筒形式>
```

５　基準分野横断基盤との相互接続検証結果

５．１　検証全体

「３　実施手順」に示した手順に従い、TM1～4 の検証を実施した。
検証全体の確認結果まとめたものを以下に示す。

５．１．１　正常動作の観点

表 ５-１　正常動作時の確認項目と結果

No	確認項目	確認結果
1	基準分野横断基盤マシンと地域活性化分野基盤マシンがネットワーク接続し、基準分野横断基盤マシンから地域活性化分野基盤マシンへ、PING で接続できたか？	○
2	基準分野横断基盤マシンと地域活性化分野基盤マシンがネットワーク接続し、地域活性化分野基盤マシンから基準分野横断基盤マシンへ、PING で接続できたか？	○
3	地域活性化分野基盤マシン上から、基準分野横断基盤マシン上のテスト用サービスのエンドポイント URL に接続できたか（HTTP としての ENDPOINT 接続確認（Web ブラウザから ENDPONT の呼出とその応答の確認）	○
4	基準分野横断基盤マシン上から、地域活性化分野基盤マシン上のテスト用サービスのエンドポイント URL に接続できたか（HTTP としての ENDPOINT 接続確認（Web ブラウザから ENDPONT の呼出とその応答の確認）	○
5	基準分野横断基盤マシンと地域活性化分野基盤マシン間で、双方向に、PF 通信による、「(TM1) : PF 通信 MEP 基本テスト」が成功したか？	○
6	基準分野横断基盤マシンと地域活性化分野基盤マシン間で、双方向に、「(TM2)： TM1-1 + PF 規定の XML パターン」が成功したか？	○
7	基準分野横断基盤マシンと地域活性化分野基盤マシン間で、双方向に、「(TM3)： TM1-1 + SSL（サーバ認証、クライアント認証)」が成功したか？	○
8	基準分野横断基盤マシンと地域活性化分野基盤マシン間で、双方向に、「(TM4)： TM1-1 + PF 規定の内包形添付」が成功したか？（オプション）？	○
9	テスト実施後、ログ等にエラーが発生していないか？	○
10	基準分野横断基盤サービス（テストドライバ）が停止はできたか	○
11	上記すべての確認が終了したか？	○

５．１．２　異常動作の観点

表 5-2　異常動作時の確認項目と結果

No	確認項目	確認結果
1	基準分野横断基盤マシンと地域活性化分野基盤マシンの各サーバは正常に動作しているか、また、ネットワークは正常か（PING 確認：PING のポートオープンが前提） 基準分野横断基盤マシンから地域活性化分野基盤マシン	○
2	基準分野横断基盤マシンと地域活性化分野基盤マシンの各サーバは正常に動作しているか、また、ネットワークは正常か（PING 確認：PING のポートオープンが前提） 地域活性化分野基盤マシンから基準分野横断基盤マシン	○
3	基準分野横断基盤のテストドライバは、正常に起動しているか？ GUI やコマンド、プロセスモニタで確認	○
4	地域活性化分野基盤のテストドライバは、正常に起動しているか？ GUI やコマンド、プロセスモニタで確認	○
5	基準分野横断基盤のテストドライバから、地域活性化分野基盤のテストドライバのサービスを呼び出す、エンドポイント URL ミスはないか？	○
6	地域活性化分野基盤のテストドライバから、基準分野横断基盤のテストドライバのサービスを呼び出す、エンドポイント URL ミスはないか？	○
7	双方で準備した､確認用の XML データと受信した XML データに齟齬がないか？	○
8	地域活性化分野基盤のテストドライバの通信ログに、エラーやワーニングはないか？ 例、コネクションが確立できない。HTTP タイムアウト、HTTP エラーレスポンス、SOAP フォルト、SOAP レベルの検定エラーが出ていないか？	○
9	基準分野横断基盤のテストドライバの通信ログに、エラーやワーニングはないか？ 例、コネクションが確立できない。HTTP タイムアウト、HTTP エラーレスポンス、SOAP フォルト、SOAP レベルの検定エラーが出ていないか？	－
10	SSL クライアント側において、SSL において、信頼されたサーバサイトではないとのエラーがでていないか？	○
11	SSL サーバ側において、SSL において、クライアント認証が失敗していないか？	○
12	上記のエラーが発生していないか？	○

５．２　相互接続検証

相互接続検証で実施した TM1～TM4 の結果の詳細を以下に示す。

５．２．１　TM1

（１）チェックリスト

表 ５-３　TM１の結果

No.	項　目	確　認	実施日	確認	確認データ項目
1	(TM1) ： PF通信 + PF規定のXMLパターン				
	同期通信に相当するメッセージ	同期通信に相当するメッセージが実行できたこと			
1-1	リクエスト　【送信メッセージ】	指定したエンドポイントに送信していること。	2009/1/23	OK	
1-2	XML	送信したメッセージがXML（TM1-IN用テストデータXML）の内容と同じであること。	2009/1/23	OK	TM1_IN.xml
1-3	ドキュメント／リテラル	ドキュメント／リテラル形式のXMLをリクエストメッセージとして送受信して問題が無いこと。	2009/1/23	OK	
1-4	日本語タグ	日本語タグを含むXMLをリクエストメッセージとして送受信して問題が無いこと。	2009/1/23	OK	
1-5	規定されたかたかなを含む	値が正しく送信できること。	2009/1/23	OK	共通ヘッダ、メッセージ属性、添付ファイル名称
1-6	規定された漢字を含む	値が正しく送信できること。	2009/1/23	OK	受付番号、属性名/属性値(2ﾊﾞｲﾄ系)、添付書類、添付書類名称、添付書類内容
1-7	タグ内の値	日本語タグ値を含むXMLを送受信して問題が無いこと。	2009/1/23	OK	
1-8	表示可能１バイトコードのみ	値が正しく送信できること。	2009/1/23	OK	受付番号、属性名/属性値(1ﾊﾞｲﾄ系)、添付ファイル名称
1-9	表示可能２バイトコードのみ	値が正しく送信できること。	2009/1/23	OK	属性名/属性値(2ﾊﾞｲﾄ系)、添付書類名称
1-10	空白（全角）を含む	値が正しく送信できること。	2009/1/23	OK	ﾒｯｾｰｼﾞ属性2ﾊﾞｲﾄｴﾘｱ(属性値)
1-11	レスポンス　【受信メッセージ】	同期通信のレスポンスメッセージとして送受信して問題がないこと。	2009/1/23	OK	
1-12	XML	同期応答したメッセージがXML（TM1-OUT用テストデータXML）の内容と同じであること。	2009/1/23	OK	TM1_OUT.xml
1-13	ドキュメント／リテラル	ドキュメント／リテラル形式のレスポンスメッセージとして送受信して問題がないこと。	2009/1/23	OK	
1-14	日本語タグ	日本語タグを含むXMLを受信して問題が無いこと。	2009/1/23	OK	
1-15	規定されたかたかなを含む	値が正しく送信できること。	2009/1/23	OK	共通ヘッダ、メッセージ属性、添付ファイル名称、業務サービス結果情報
1-16	規定された漢字を含む	値が正しく送信できること。	2009/1/23	OK	受付番号、結果情報、属性名/属性値(2ﾊﾞｲﾄ系)、添付書類、添付書類名称、添付書類内容
1-17	タグ内の値	日本語タグ値を含むXMLを送受信して問題が無いこと。	2009/1/23	OK	
1-18	表示可能１バイトコードのみ	値が正しく送信できること。	2009/1/23	OK	受付番号、属性名/属性値(1ﾊﾞｲﾄ系)、添付ファイル名称
1-19	表示可能２バイトコードのみ	値が正しく送信できること。	2009/1/23	OK	属性名/属性値(2ﾊﾞｲﾄ系)、添付書類名称
1-20	空白（全角）を含む	値が正しく送信できること。	2009/1/23	OK	ﾒｯｾｰｼﾞ属性2ﾊﾞｲﾄｴﾘｱ(属性値)

TM1-IN用テストデータですべて確認するようにする

TM1-OUT用テストデータですべて確認するようにする

５．２．２　TM2

（１）チェックリスト

表 ５-４　TM2 の結果

No.	項　目		確　認	実施日	確認	確認データ項目
2	(TM2) ： PF通信のMEP基本テスト(３種類)					
	リクエスト型同期受領Ackあり					
	正常系					
	リクエストに対して受領処理を実施し同期で受領アックを返す					
2-1-1	要求メッセージ	TM2-1 IN用テストデータは、TM1-INと同じとする。	正常に要求メッセージが送信できること。	2009/1/23	OK	TM1_IN.xml
2-1-2	受付番号		受付番号の値が設定されていること。	2009/1/23	OK	20090123BB@0001
2-1-3	リクエストXMLが正しくリクエスト		リクエストXMLが正しくリクエストされること。	2009/1/23	OK	
2-1-4	受領Ack		正常に受領Ackを受信できること。	2009/1/23	OK	受領Ack.xml
2-1-5	受付番号		要求元で設定された値が引き継がれていること。	2009/1/23	OK	20090123BB@0001
2-1-6	結果情報		正常（0）終了が設定されていること。	2009/1/23	OK	0
2-1-7	受領Ackの各項目		受領Ackの各項目が正しく設計されていること。	2009/1/23	OK	受領Ack.xml内の項目
	リクエスト・レスポンス型同期型レスポンス	TM2-2 IN用テストデータは、TM1-INと同じとする。				
	正常系					
	リクエストに対して同期でレスポンスを返す。					
2-2-1	要求メッセージ		正常に要求メッセージが送信できること。	2009/1/23	OK	TM1_IN.xml
2-2-2	受付番号		受付番号の値が設定されていること。	2009/1/23	OK	20090123BB@0001
2-2-3	リクエストXMLが正しくリクエスト		リクエストXMLが正しくリクエストされること。	2009/1/23	OK	
2-2-4	応答メッセージ	TM2-2 OUT用テストデータは、TM1-OUTと同じとする。	正常に応答メッセージを受信できること。	2009/1/23	OK	TM1_OUT.xml
2-2-5	受付番号		要求元で設定された値がそのまま引き継ぎ返されていること。	2009/1/23	OK	20090123BB@0001
2-2-6	結果情報		正常（0）終了が設定されていること。	2009/1/23	OK	0
2-2-7	業務サービス結果情報		業務的な処理結果が入っていること。	2009/1/23	OK	100
2-2-8	レスポンスXMLが正しくレスポンス		レスポンスXMLが正しくレスポンスされていること。	2009/1/23	OK	
	リクエスト・レスポンス型同期型受領Ack＋非同期型レスポンス					
	正常系					
	リクエストに対して受領処理を実施し、同期で受領アックを返し、その後、非同期で応答メッセージを返す。					
2-3-1	要求メッセージ	TM2-3 IN用テストデータは、TM1-INと同じとする。	正常に要求メッセージが送信できること。	2009/1/23	OK	TM1_IN.xml
2-3-2	受付番号		受付番号の値が設定されていること。	2009/1/23	OK	20090123BB@0001
2-3-3	リクエストXMLが正しくリクエスト		リクエストXMLが正しくリクエストされること。	2009/1/23	OK	
2-3-4	要求の受領Ack		正常に受領Ackを受信できること。	2009/1/23	OK	受領Ack.xml
2-3-5	受付番号		要求元で設定された値が引き継がれていること。	2009/1/23	OK	20090123BB@0001
2-3-6	結果情報		正常（0）終了が設定されていること。	2009/1/23	OK	0
2-3-7	受領Ackの各項目		受領Ackの各項目が正しく設計されていること。	2009/1/23	OK	受領Ack.xml内の項目
2-3-8	応答メッセージ		正常に要求メッセージが送信できること。	2009/1/23	OK	TM1_OUT.xml
2-3-9	受付番号	TM2-3 IN用テストデータは、TM1-OUTと同じとする。	要求元が採番した受付番号の値が引き継がれ設定されていること。	2009/1/23	OK	20090123BB@0001
2-3-10	業務サービス結果情報		業務的な処理結果が設定されていること。	2009/1/23	OK	100
2-3-11	リクエストXMLが正しくリクエスト		リクエストXMLが正しくリクエストされること。	2009/1/23	OK	
2-3-12	応答の受領Ack		正常に受領Ackを受信できること。	2009/1/23	OK	受領Ack.xml
2-3-13	受付番号		要求元が採番した受付番号の値が引き継がれ設定されていること。	2009/1/23	OK	20090123BB@0001
2-3-14	結果情報		正常（0）終了が設定されていること。	2009/1/23	OK	0
2-3-15	受領Ackの各項目		受領Ackの各項目が正しく設計されていること。	2009/1/23	OK	受領Ack.xml内の項目

ア）障害内容

TM2-3 分野横断基盤→基準分野横断基盤への送信テスト時に発生。基準分野基盤への応答メッセージを返す際に応答メッセージ(TM1_OUT.xml)ではなく要求メッセージ(TM1_IN.xml)を送信した。

イ）原因・対処

分野横断基盤→基準分野横断基盤に応答する際のテストデータの設定を間違えて指定していたため、要求メッセージ(TM1_IN.xml)が送信されていた。設定を変更し正しく応答メッセージ(TM1_OUT.xml)を送信するように修正した。

５．２．３　TM3

（１）チェックリスト

表 ５-５　TM3 の結果

No.	項　目	確　認	実施日	確認	確認データ項目
3	（TM3）：PF通信＋ SSL（サーバ認証、クライアント認証）				
	サーバ認証				
	サーバ認証書がサーバ側にインストールされて				
3-1-1	HTTPSで通信する	正常に通信できると共に電文が暗号化されていること。	1月23日	OK	エンドポイントURLに対して、https://～でアクセスでき、http でエラーとなる
	サーバ認証＋クライアント認証				
	サーバ認証書がサーバ側にインストールされている				
	クライアント認証書がクライアント側にインストールされている				
3-2-1	HTTPSで通信する	正常に通信がＳＳＬクライアントとして認証されできると共に電文が暗号化されていること。	1月23日	OK	エンドポイントURLに対して、https://～でアクセスでき、http でエラーとなる

TM3のテストデータは、TM1と同じとする。

※「暗号化されていること」の確認方法としては、"Wireshark"等のツールを使用して、パケットモニタリングを実施する。

ア）障害内容

TM3-2 SSL のサーバ認証＋クライアント認証テスト時に発生。クライアント認証を行えずエラーが発生した。

イ）原因・対処

分野横断基盤クライアント側にて指定するクライアント証明書のファイルパス名が間違っており正しく認証が行えなかった。ファイルパスを修正し、クライアント認証を介して正しく通信できることを確認した。

５．２．４　TM4

（１）チェックリスト

表 ５-６　TM4 の結果

No.	項　目	確　認	実施日	確認	確認データ項目
4	(TM4)： PF通信＋PF規定添付ファイル				
	[Type1] 本文と添付（本文内に埋め込み）				
	添付ファイルの種類				
4-1-1	テキストデータ	送信でき、受信側で当該データを取り出せるこ	1月23日	OK	TM1_IN_ attached.xml又はTM1_OUT.xml内添付書類ファイル名称タグ（attached.txt）
4-1-2	画像データ（PDF）	送信でき、受信側で当該データを取り出せるこ	1月23日	OK	TM1_IN_ attached.xml又はTM1_OUT.xml内添付書類ファイル名称タグ（attached.pdf）
	Base64エンコーディング				
4-1-3	エンコーディングされている	送信でき、エンコーディングされている情報で	1月23日	OK	TM1_IN_ attached.xml又はTM1_OUT.xml内添付書類内容タグ
	添付ファイルのファイル名称				
4-1-4	付与されている	付与されたファイル名称で、受信側にファイル	1月23日	OK	attached.txt、attached.pdf

TM4のテストデータは、TM1と同じで、最後に添付のタグが2つあるとする。

ア）障害内容

TM4-1 分野横断基盤→基準分野横断基盤への送信テスト時に、分野横断基盤からの要求メッセージが空で送信されていた。

イ）原因・対処

要求メッセージのもととなるテストデータのタグ構造が間違っており、テストデータが読み込めない状態であったため空メッセージを送信していた。テストデータを正しいデータに修正し、正しいメッセージが送信されていることを確認した。

６　まとめ

本検証では、地域活性化分野：住民生活向上系（子育て支援）で採用する技術仕様を選択し、各技術仕様にもとづく相互接続性を確認するための TM1～TM4 の各テストモデルの検証を実施した。

検証の結果、各テストモデルにおいて規定した検証項目全てにおいて正しく動作したことが確認でき、分野横断基盤(地域活性化分野：住民生活向上系)が地域情報プラットフォーム V2.0 仕様に準拠した相互接続性をもつことが確認できた。

また、本検証では、各技術仕様の相互接続性を確認するために、テストモデルを規定し、検証手順、チェックリストの整備を行った。これら一連の手順は、システム間の相互接続性を確認するための基本的な手順、検証項目として活用でき、地域情報プラットフォーム仕様にもとづいたシステム間の検証仕様として利用できるといえる。

表　6-1　相互接続検証の検証結果

No.	相互接続検証の目的	結果
1	基準分野横断基盤と分野横断基盤の間で、地域情報プラットフォーム仕様に準拠した相互接続性を検証できること	地域情報プラットフォーム仕様にもとづいたシステムである基準分野横断基盤と分野横断基盤間の相互接続性を確認することができた。
2	地域情報プラットフォーム標準仕様書に準拠した実装同士がマルチベンダ環境で接続可能な相互接続実用仕様案を策定できること	検証にいたる過程の中で事前準備に必要な情報、手順を整理することができ、実用仕様案策定に向けた検証が実施できた。