e－MRP国際互換性試験について

2005．1．12

(財) ニューメディア開発協会

基本的な考え方

1. 本資料は、日本で開催する国際互換性検証イベントでの試験方法について、基本的な考え方を示すものである。
2. 互換性試験は、各国で開発されるIC旅券(e-MRP)とリーダ(PCD)について、NMDAで定める「バイオメトリクス旅券用近接型通信インタフェース実装規約書」への準拠性の確認（ISO/IEC14443タイプB）（タイプAに関してはエッセングループと連携）する互換性検証の他に、IC旅券固有機能であるPassive Authentication（SO_D構造検証試験）機能や、Basic Access Control（オプション）機能についても互換性検証試験の中であわせて動作確認し、処理時間等を把握する。
3. 検証方法としては、IC旅券とリーダの実機同士の組合せで行う互換性検証（クロス）試験と、開発中のe-MRP標準機、PCD標準機との組合せで行う互換性検証試験とで構成する。
4. 試験（シルバー）データは、事前準備し提示するものと、各国がICAO－TRを元に準備するケースの2通りを想定する。

本資料は、未調整の部分もあり、検討の進捗と共に変更があり得る。

開催場所：つくば国際会議場（エポカル・つくば）

〒305-0032茨城県つくば市竹園2丁目20番地3号

電話：029(861)0001

FAX：029(861)1209

URL：http://www.epochal.or.jp

開催日時：2005年3月8日（火）～10日（木）

主催：日本国政府（外務省、経済産業省）

協賛：（財）ニューメディア開発協会

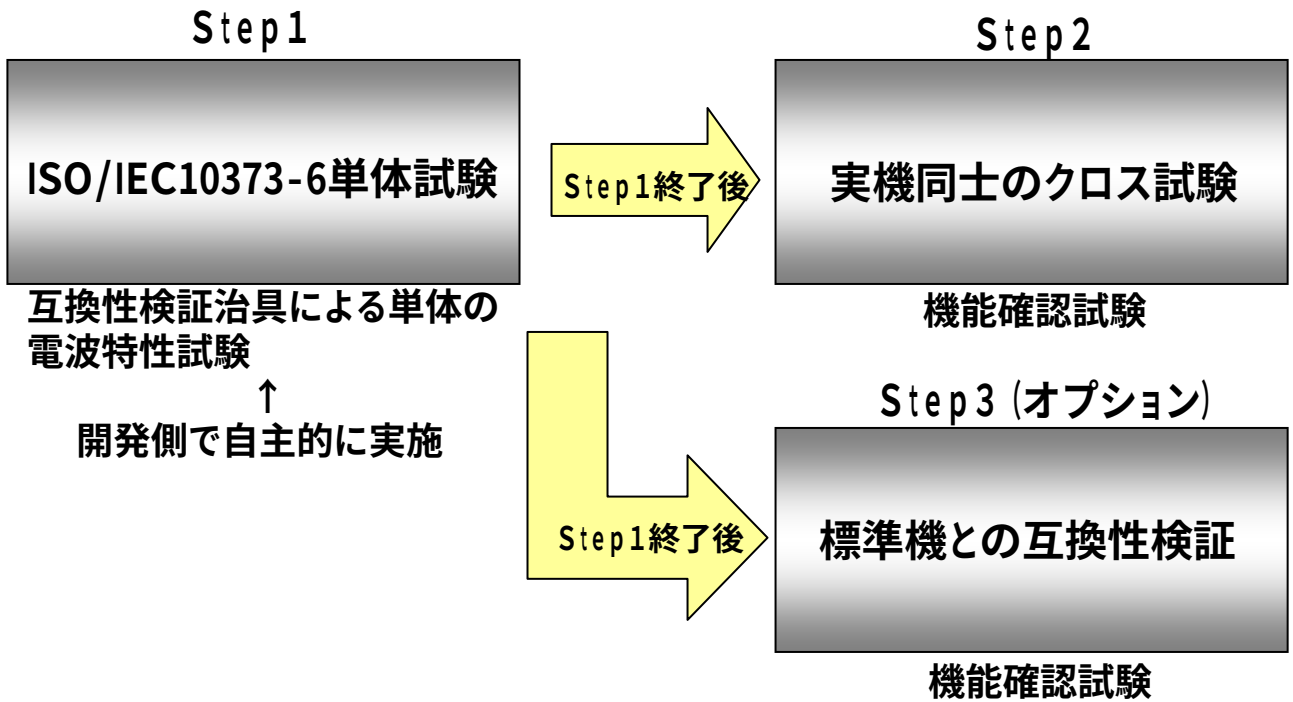
（社）ビジネス機械・情報システム産業協会

エッセングループ

試験実施スケジュール

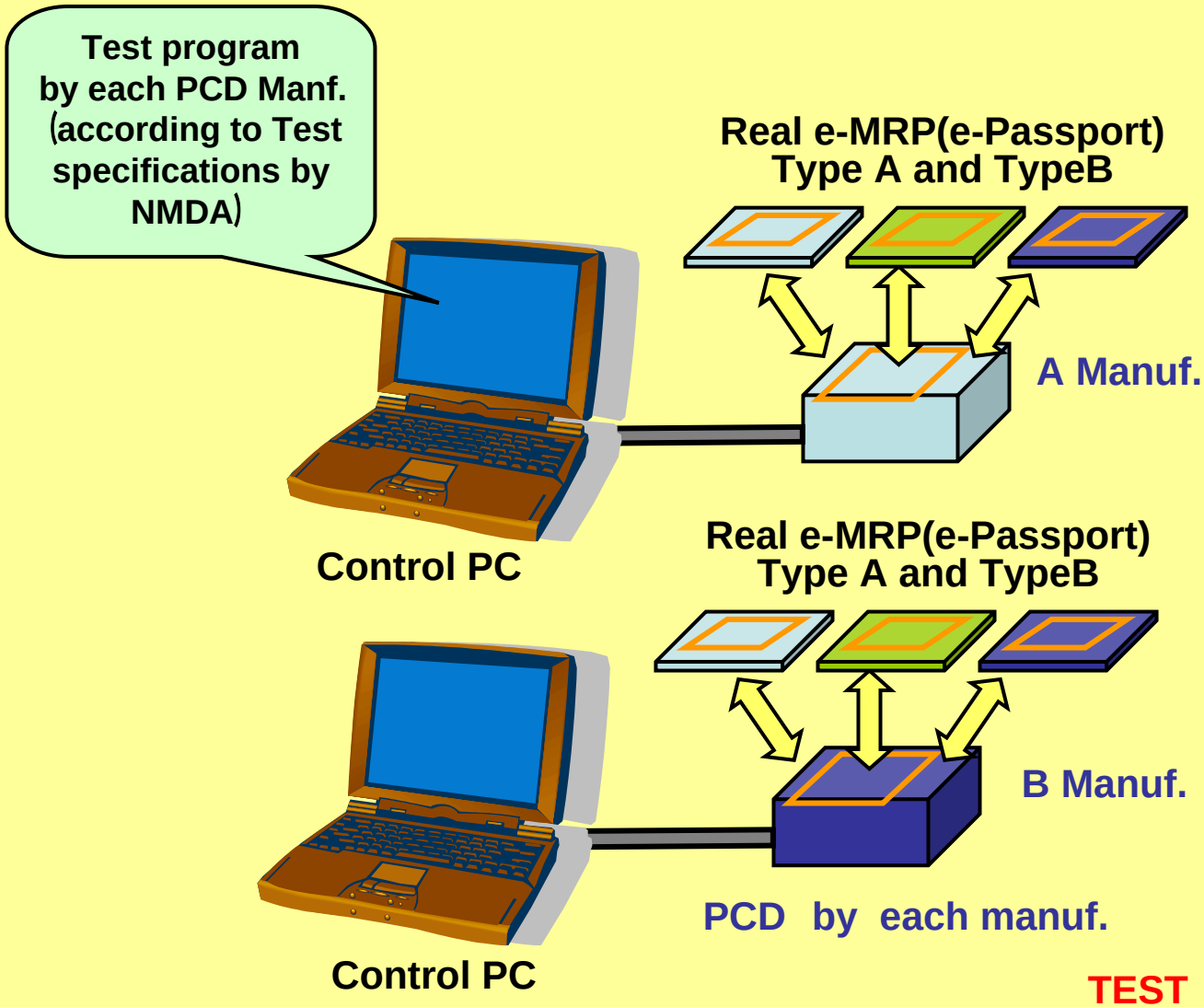
	3月8日 (火)	3月9日 (水)	3月10日 (木)
日　程	登録作業・予備試験	本試験	試験予備日・結果発表
9:00～12:00	参加者登録 試験機材登録 試験機材への登録シール貼付 ブリーフィング 予備試験開始	試験実施	試験実施
12:00～13:00	休　憩	休　憩	休　憩
13:00～17:00	参加者試験環境セットアップと任意確認試験の実施 標準機による試験開始 試験終了	試験実施 試験終了	試験結果 (概要) 閉会の挨拶 後片付け

ISO/IEC10373-6における単体試験と実機（クロス）試験 標準機による試験の関係



実機同士のクロス試験での互換性検証（Step2）が望ましいが、国際間では困難な場合も想定し、Step3で標準機を用いて検証する。

実機同士試験



TEST CONTENTS

- Activation test
- Command send/receive test
- SO_D Structure Verification Test
- Basic Access Control
  +
  SO_D Structure Verification test
- Processing time measurement

(refer to Test spec.by NMDA)

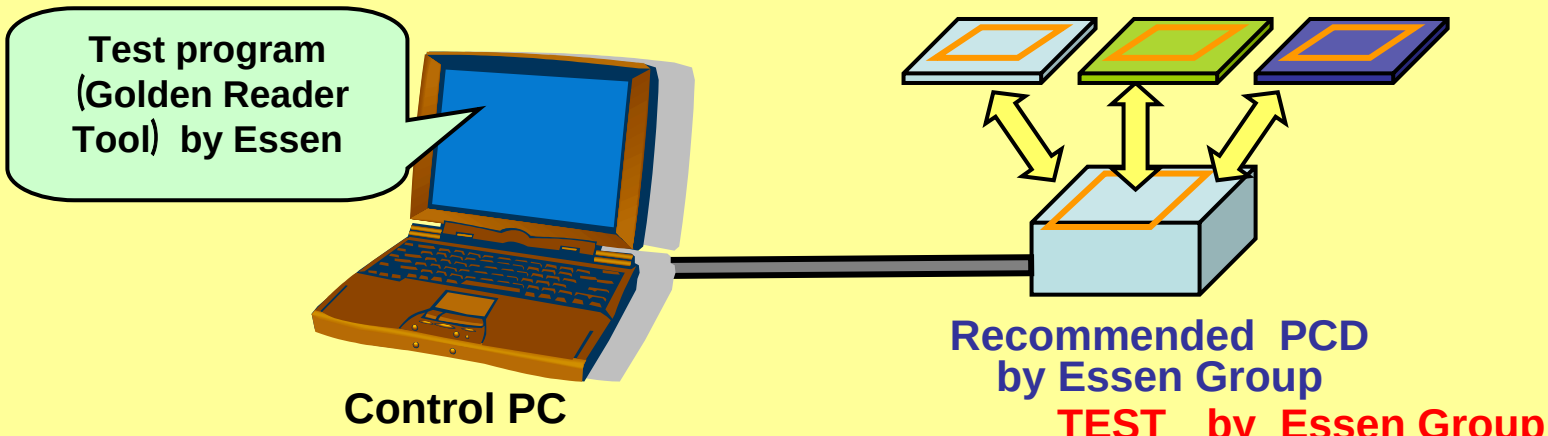
TEST PARAMERTER

- Distance(0,20[mm])
- Data Set etc

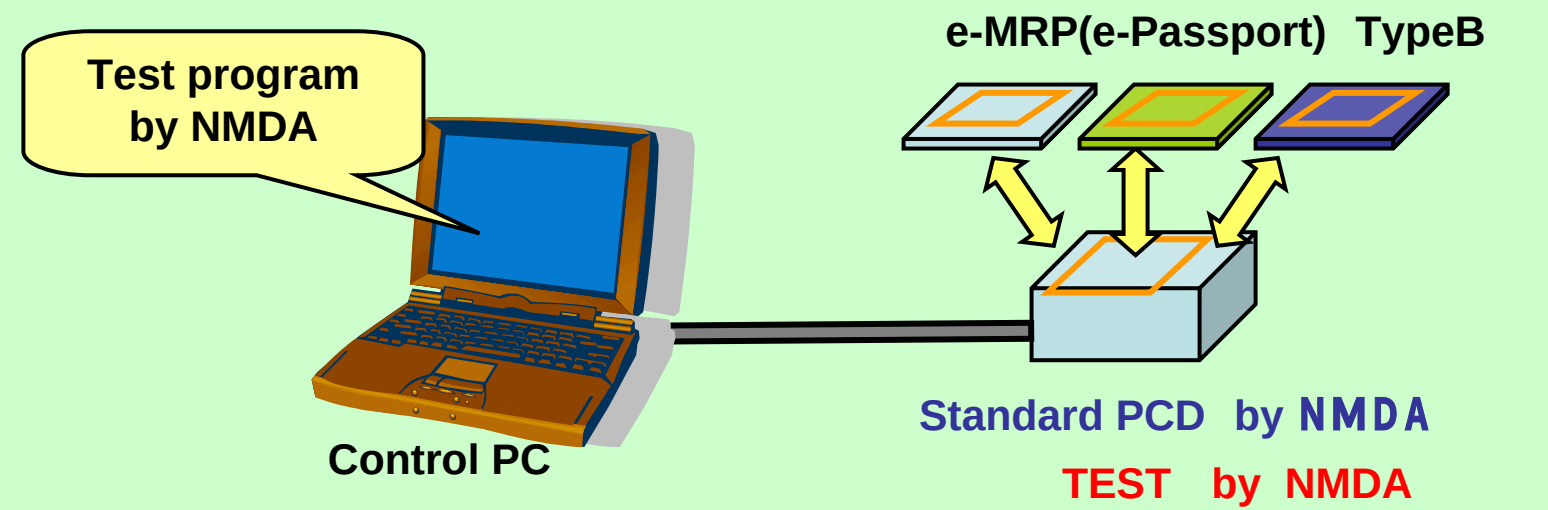
TEST by each PCD Manuf.

PCD標準機試験

PCD標準機TypeA試験



PCD標準機TypeB試験

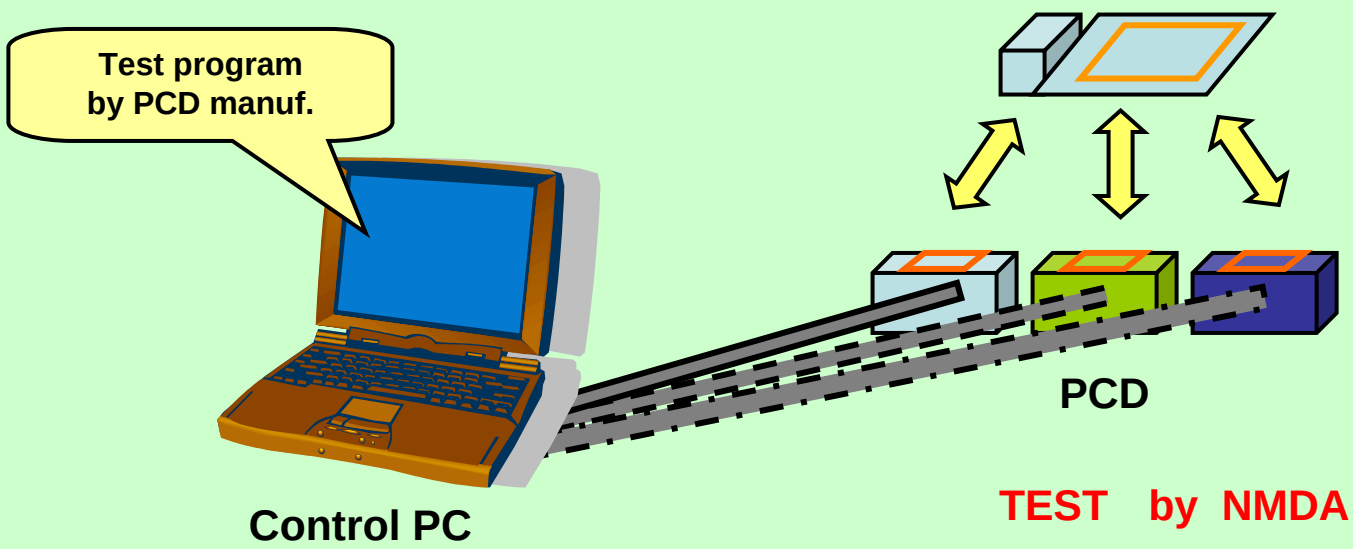


e-MRP標準機試験

e-MRP標準機TypeA試験

実施しない。

e-MRP標準機TypeB試験



IC旅券互換性試験方針

試験の組合せの考え方

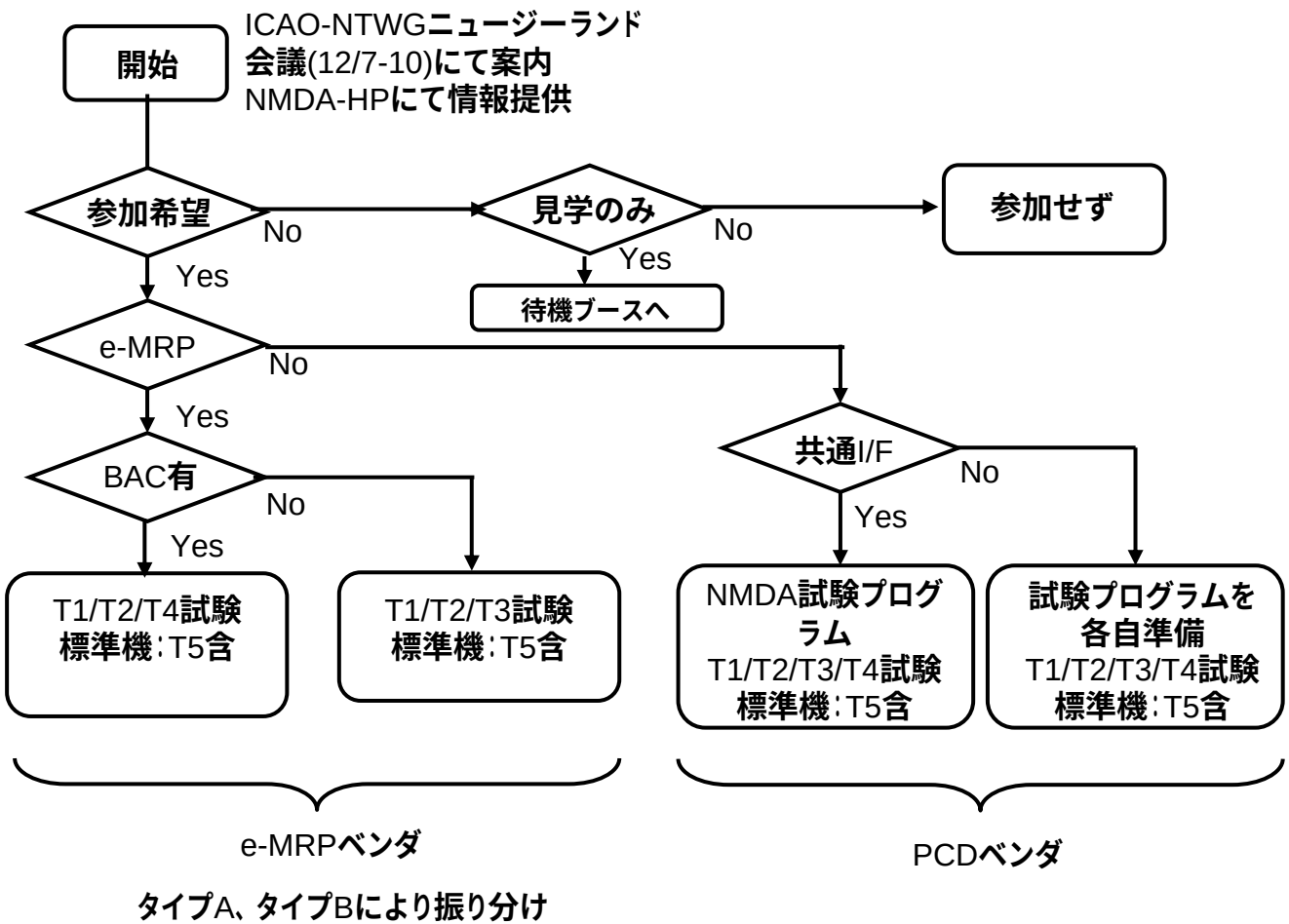
<table>
<tr><th colspan="4">e-MRP</th><th>上位I/F</th><th>単体試験
ISO10373</th><th>クロス（実機同士）試験</th><th>e-MRP × PCD標準機</th><th>PCD × e-MRP標準機</th></tr>
<tr><td rowspan="8">ICAO-TR</td><td rowspan="4">ISO/IEC 14443 Type A</td><td rowspan="2">BAC無</td><td>NMDA 非準拠</td><td rowspan="8">事前にﾍﾞﾝﾀﾞ各自で試験実施</td><td>各ベンダ作成の試験プログラムで試験</td><td rowspan="2">T1/T2/T3/T5試験（N）
ゴールデンリーダ
（ｴｯｾﾝｸﾞﾙｰﾌﾟ）</td><td rowspan="4">実施せず</td></tr>
<tr><td>NMDA 準拠 共通I/F</td><td>T1/T2/T3 試験（N）</td></tr>
<tr><td rowspan="2">BAC有</td><td>NMDA 非準拠</td><td>各ベンダ作成の試験プログラムで試験</td><td rowspan="2">T1/T2/T4/T5 試験（N）
ゴールンリーダ
（ｴｯｾﾝｸﾞﾙｰﾌﾟ）</td></tr>
<tr><td>NMDA 準拠 共通I/F</td><td>T1/T2/T4 試験（N）</td></tr>
<tr><td rowspan="4">ISO/IEC 14443 Type B</td><td rowspan="2">BAC無</td><td>NMDA 非準拠</td><td>各ベンダ独自の試験プログラムで試験</td><td rowspan="2">T1/T2/T3/T5 試験（N） NMDA-PCD標準機</td><td>実施せず</td></tr>
<tr><td>NMDA 準拠 共通I/F</td><td>T1/T2/T3 試験（N）</td><td>T1/T2/T3/T5 試験（N） NMDA-eMRP標準機</td></tr>
<tr><td rowspan="2">BAC有</td><td>NMDA 非準拠</td><td>各ベンダ作成の試験プログラムで試験</td><td rowspan="2">T1/T2/T4/T5試験（N）
NMDA-PCD標準機</td><td>実施せず</td></tr>
<tr><td>NMDA 準拠 共通I/F</td><td>T1/T2/T4 試験（N）</td><td>T1/T2/T4/T5 試験（N）
NMDA-eMRP標準機</td></tr>
</table>

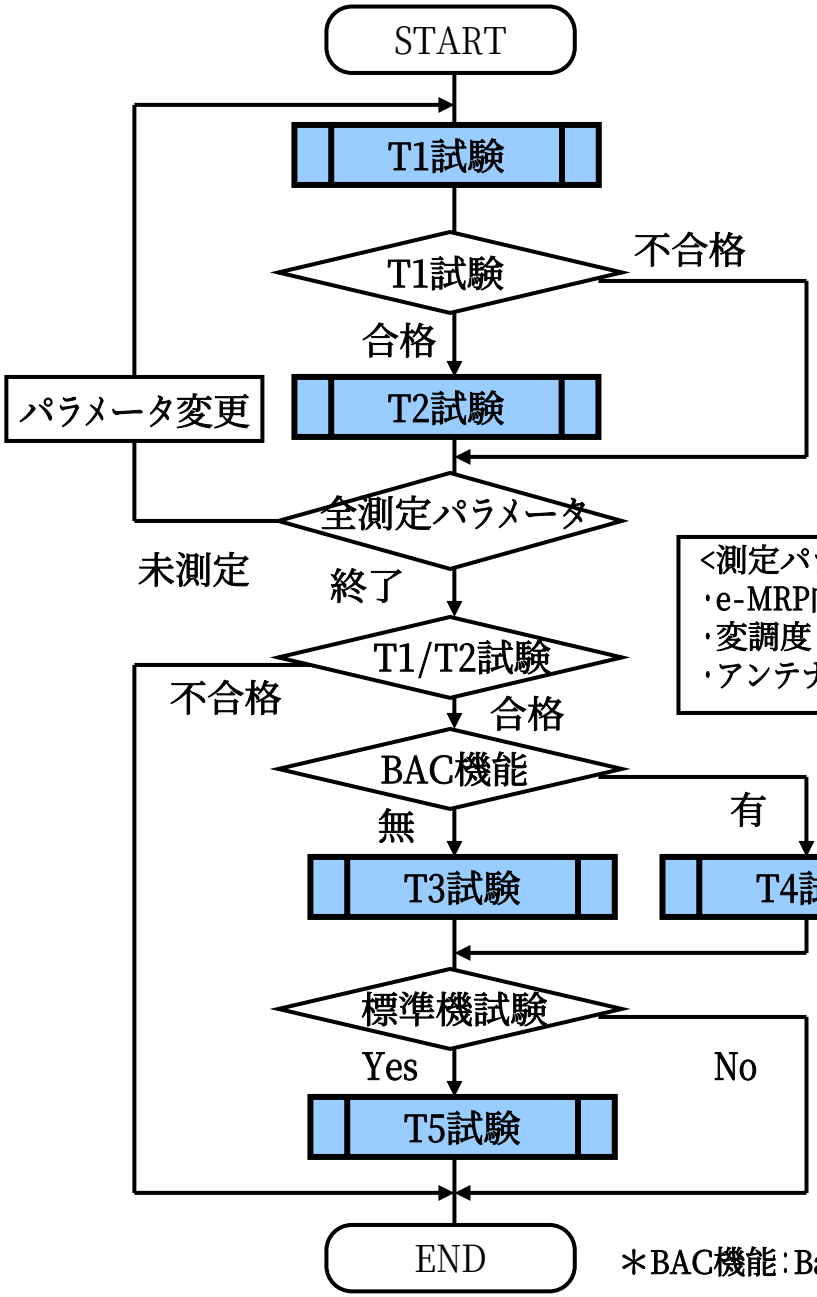
BAC：Basic Access Control
(N)：NMDA試験仕様準拠互換性試験プログラムを使用した試験
共通I/F：バイオメトリクス旅券用近接型通信インタフェース実装規約書第1.0版参照
タイプAについてはｴｯｾﾝｸﾞﾙｰﾌﾟと調整する

試験内容

試験分類	試験名	試験内容	備考
T1	活性化試験	e-MRP（標準機）をPCD（標準機）に設置後、活性化まで遷移出来るか確認する。	全機種対象
T2	コマンド送受信試験	簡単なコマンドが正しく動作するか確認する。（Select DF）	全機種対象
T3	SO_D構造検証試験	Passive Authentication処理の一部である、パスポート格納情報のSO_Dを読み出すことが出来ることを確認する。各処理時間も測定する。	BAC処理機能を有していないe-MRP、もしくはe-MRP標準機のみ試験対象とする。
T4	Basic Access Control + SO_D構造検証試験	Basic Access Control（以下BAC）処理を行い、セッション鍵を作成、共有化する。本セッション鍵を用いてセキュアメッセージング処理下で、パスポート格納情報のSO_Dを読み出すことが出来ることを確認する。各処理時間も測定する。	BAC処理機能を有するe-MRP（標準機）のみ試験対象とする。
T5	通信距離測定試験	e-MRP及びPCDの組合せにおいて、両者の最大通信可能距離（Z軸上）を測定する。	全機種対象 標準機試験のみ実施

試験参加ベンダの分類


開始
ICAO-NTWGニュージーランド
会議(12/7-10)にて案内
NMDA-HPにて情報提供
参加希望
No
見学のみ
No
参加せず
Yes
Yes
待機ブースへ
e-MRP
No
Yes
共通I/F
No
BAC有
No
Yes
Yes
T1/T2/T4試験
標準機：T5含
T1/T2/T3試験
標準機：T5含
NMDA試験プログラム
T1/T2/T3/T4試験
標準機：T5含
試験プログラムを
各自準備
T1/T2/T3/T4試験
標準機：T5含
e-MRPベンダ
PCDベンダ
タイプA、タイプBにより振り分け



<測定パラメータ>
・e-MRP向き
・変調度（PCD標準機）
・アンテナサイズ（標準機）

＊BAC機能：Basic Access Control 機能

図　PCD標準機試験及び実機同士試験のフロー

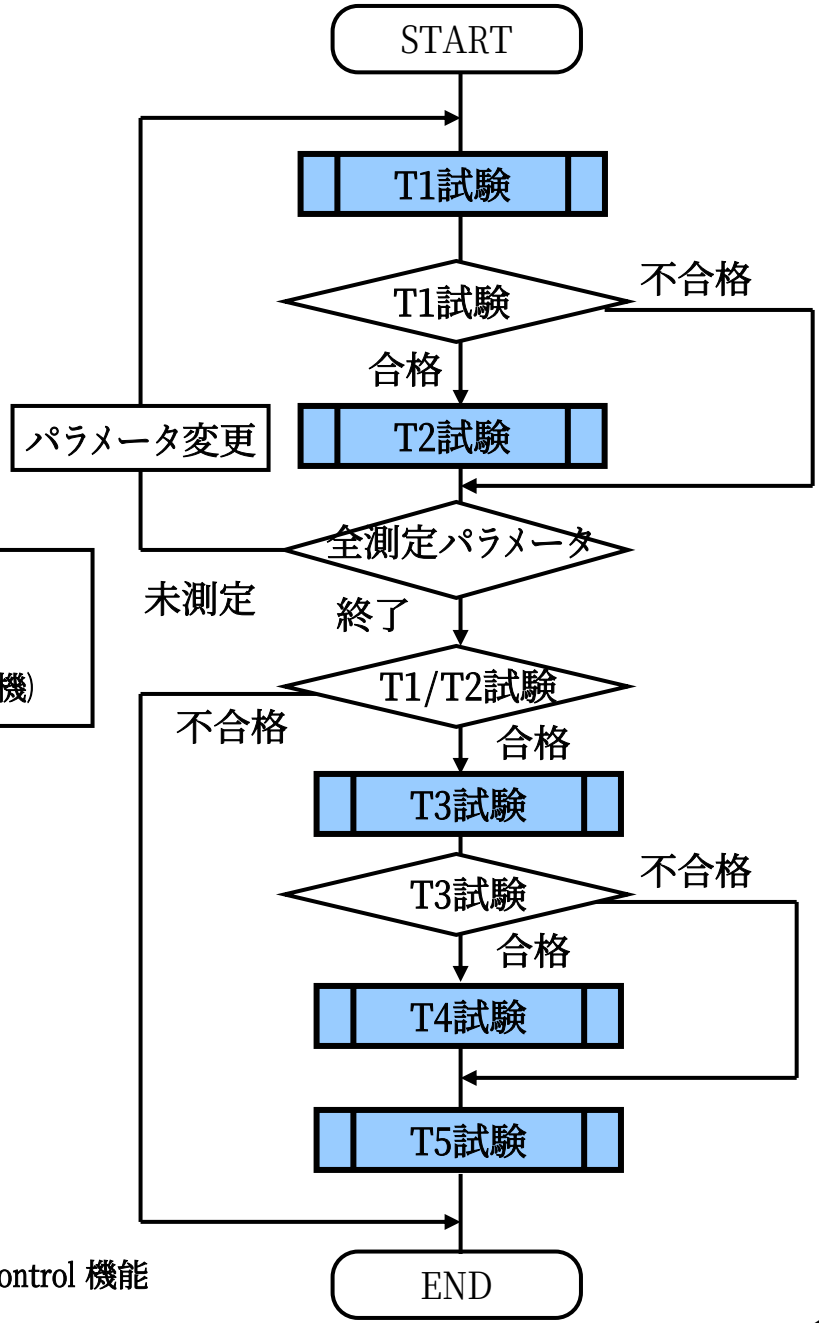
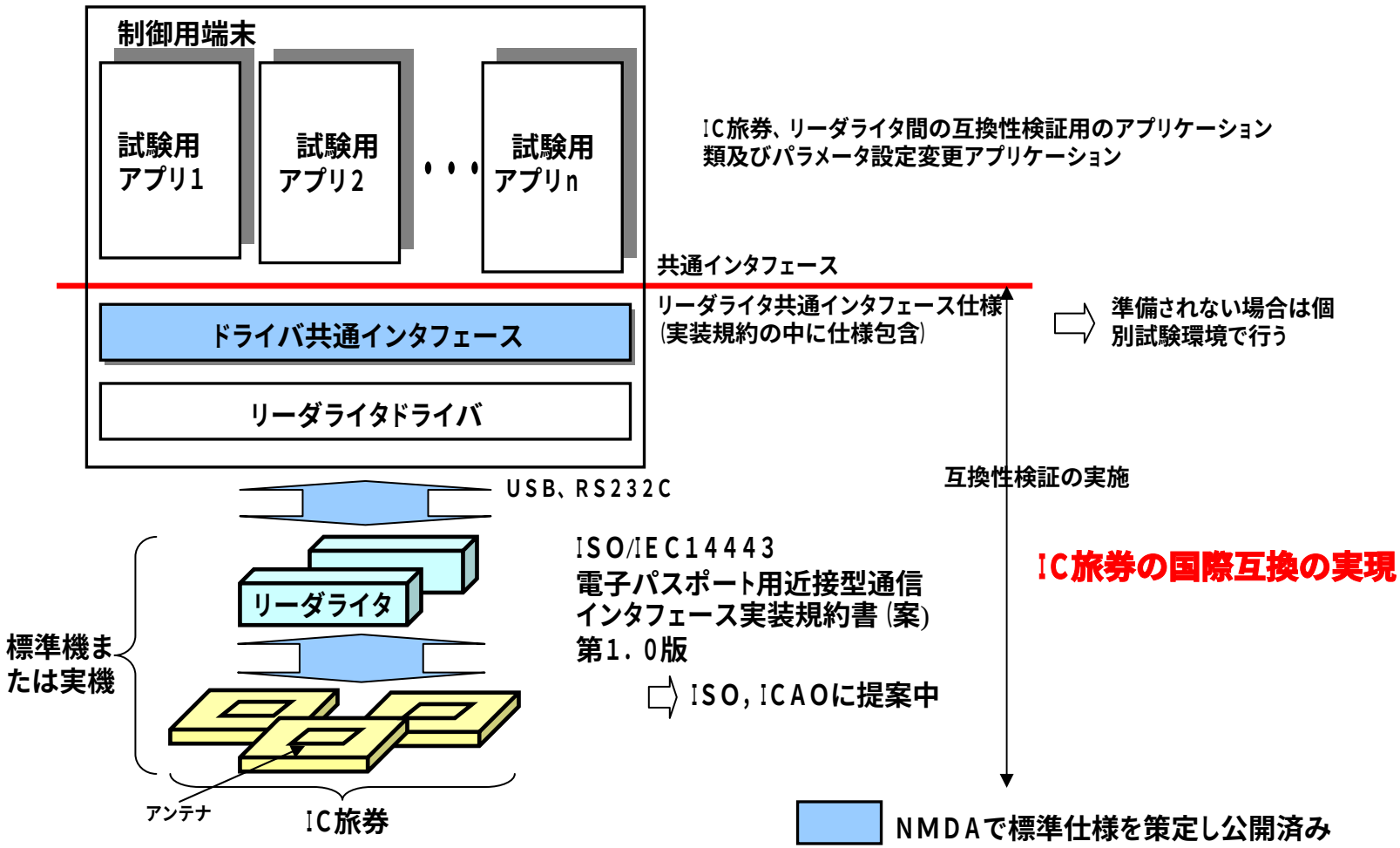


図　e-MRP標準機試験のフロー

IC旅券の互換性の確保と試験環境のイメージ



互換性(クロス)試験プログラムの構成

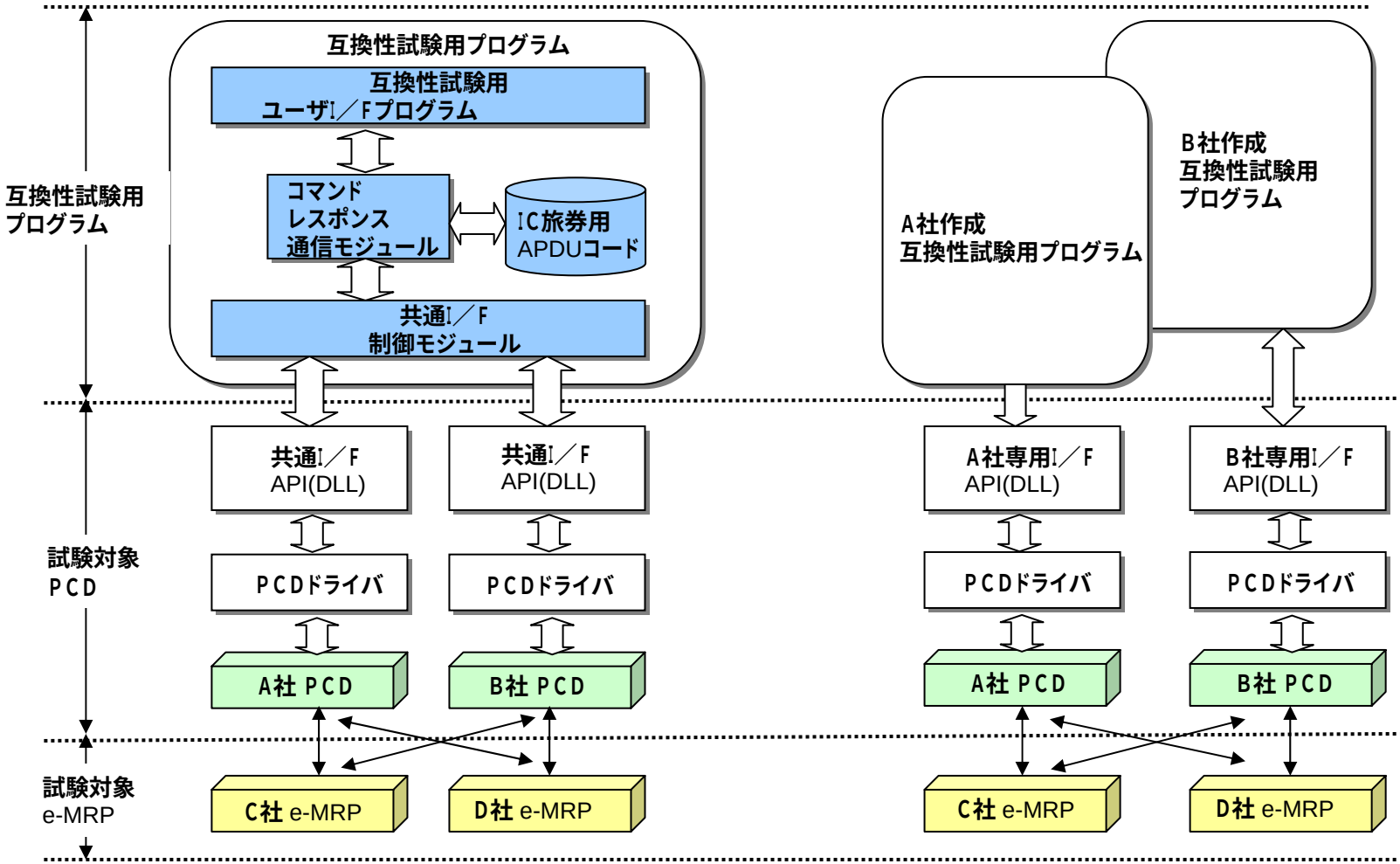


図　実機同士での組合せでの試験の構成

試験データの考え方

試験方法 / シルバーデータ	日本版シルバーデータ試験	各国準拠のデータを持ち寄って試験
EFCOM	指定データ	任意データ
DG1 (MRZ Data)	指定データ	任意データ
DG2 (顔画像 Data)	指定データ	任意データ
SO_D (Document Security Object settings)	指定データ ・証明書検証 (Document Signer Certificate) は行わない。	一部指定 (以下のデータのみ指定) ・ダイジェストアルゴリズム：指定 ・署名アルゴリズム：指定 ・証明書検証 (Document Signer Certificate) は行わない。
署名検証用鍵 (Document Signer Public Key)	指定データ ・同一鍵データを使用	指定データ ・同一鍵データを使用
K_{ENC}/K_{MAC} (Basic Access Key)	指定データ ・同一鍵データを使用	任意データ

＊ ICAO PKIVer1.1 / LDSVer1.7　準拠