ECOM長期署名フォーマット相互運用性テスト結果報告

2005年　12月16日

セキュリティワーキンググループ

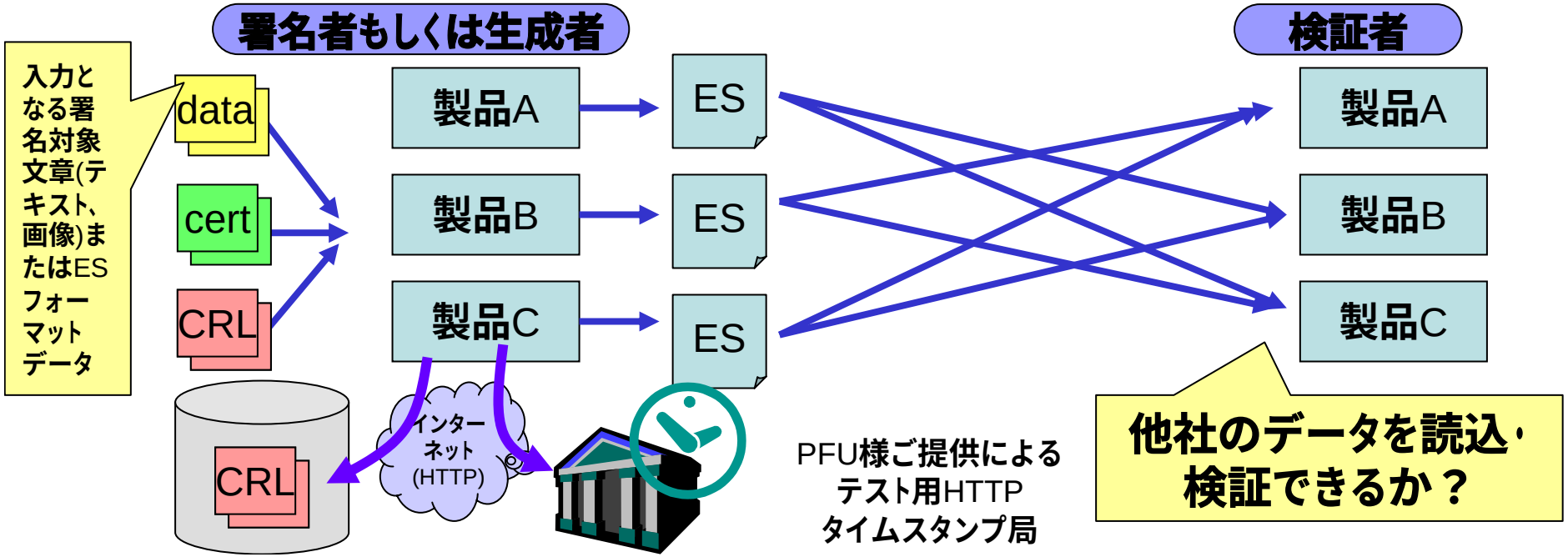
長期署名フォーマット普及サブワーキンググループ

次世代電子商取引推進協議会

試験項目	：	オンラインマトリックス生成･相互検証テスト オフライン共通データ検証テスト
試験期間	：	10月15日～12月14日
参加企業	：	13社
試験協力企業	：	2社（エントラストジャパン㈱、㈱PFU）

テスト1：オンラインマトリックス生成・相互検証テスト

目的	・他社製品が生成した有効なESフォーマットのデータが相互に読み取り、検証できることを確認
内容	指定した証明書、CRL、タイムスタンプサービスにより各製品により有効であるようなESフォーマット(ES-T, ES-X Long, ES-A)を生成する。各製品において読込み、他社の生成したデータが有効である事を検証する。CRL、TSAはオンライン、それ以外はオフラインとする。



テスト2：オフライン共通データ検証テスト

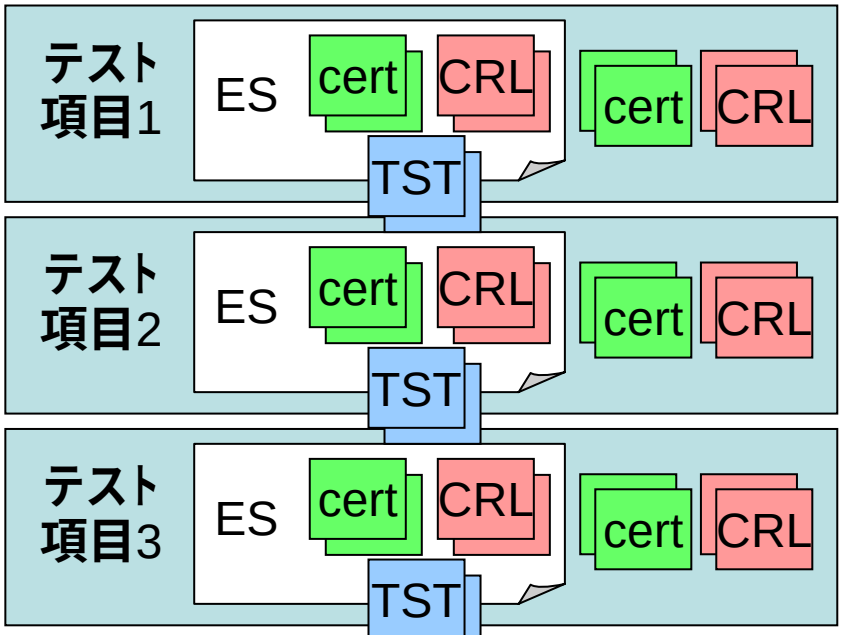
目的

・実装されている長期署名フォーマットの検証機能の確認
・ECOMプロファイルの準拠性の確認

内容

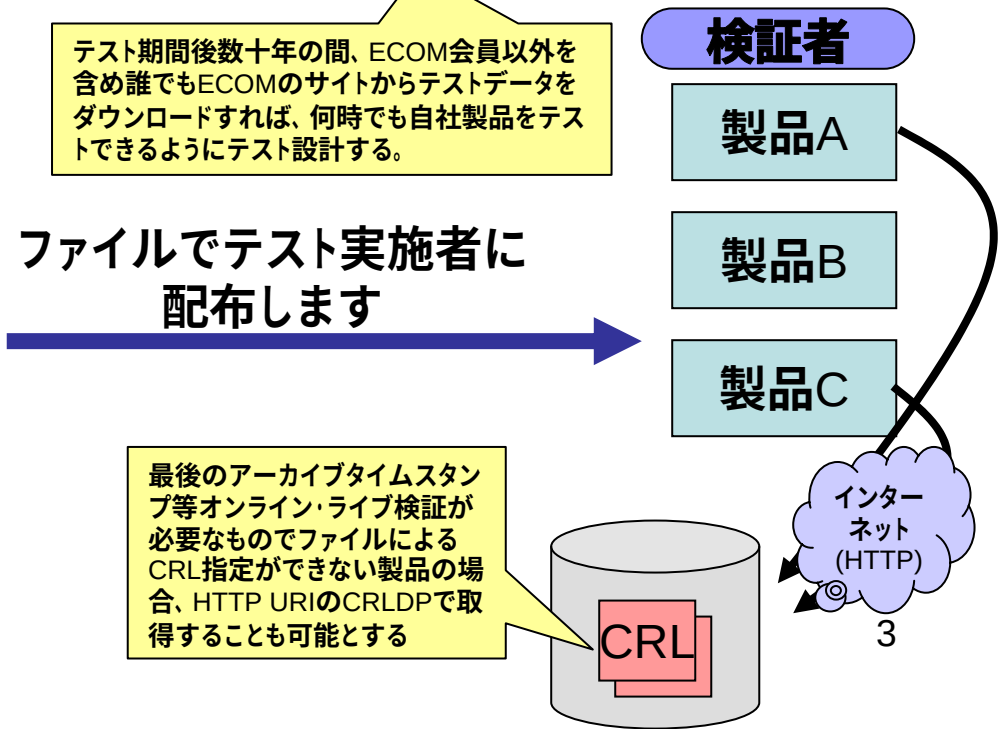
ツールにより生成されたESフォーマットのデータ(ES-T, ES-X Long, ES-A)、検証情報、設定情報のセットをテスト対象として、各社製品でオフラインにより有効性を検証する。結果は有効、無効の2種類のみ。無効の理由は問わないこととする。

テスト用の鍵、証明書、CRLの発行にはIPA/JNSA Challenge PKIテストスイートを用いる。



テスト期間後数十年の間、ECOM会員以外を含め誰でもECOMのサイトからテストデータをダウンロードすれば、何時でも自社製品をテストできるようにテスト設計する。

ファイルでテスト実施者に配布します



最後のアーカイブタイムスタンプ等オンライン・ライブ検証が必要なものでファイルによるCRL指定ができない製品の場合、HTTP URIのCRLDPで取得することも可能とする

実験参加製品名またはプロトタイプ名一覧 (カテゴリ内企業名五十音順)

	企業名(略称)	種別	製品名	Ver	リリース予定
CAdES	RSAセキュリティ	既存製品	RSA BSAFE e文書法対応ライブラリ	V1.1(β1)	‘06.02
	NTTデータ	試作品	長期署名対応プラットフォーム(プロトタイプ)	0.1	–
	セコム	既存製品	セコム長期署名ライブラリ	1.3	‘06.01
	日本電子公証機構	既存製品	JN++ 電子署名タイムスタンプSDKキット	2.0	2006
	NTT	試作品	CYNOS-L(プロトタイプ)	1	–
	ハイパーギア	既存製品	HG/PscanServ Pro	4.0	‘06.02
	PFU	試作品	PFU長期署名ライブラリ(プロトタイプ)	0.1	–
	日立製作所	試作品	長期署名フォーマットライブラリ(プロトタイプ)	0.1	–
	三菱電機	試作品	–	–	–
	MDIS	既存製品	三菱署名有効性延長システム MistyGuard<EVERSIGN>	2.0	‘06春
XAdES	関電システム	新規製品	XAdES長期署名ライブラリ for .NET	1.3	‘06.01
	NEC	試作品	PKIサーバ/Carassuite原本保管サーバ	3.0プロトタイプ	–
	富士ゼロックス	新規製品	ArcSuite e-文書法対応	1.0	‘ 06.01

オンライン生成･相互検証テスト結果
実験参加他社製品との相互運用性

(カテゴリ内企業名五十音順)

	データ生成企業名(略称)	種別	ES-T	ES-XL	ES-A	備考
CAdES	RSAセキュリティ	既存製品	○	○	○	
	NTTデータ	試作品	○	○	○	
	セコム	既存製品	○	○	○	
	日本電子公証機構	既存製品	○	○	○	
	NTT	試作品	○	○	○	
	ハイパーギア	既存製品	○	○	○	
	PFU	試作品	○	○	○	
	日立製作所	試作品	○	○	○	
	三菱電機	試作品	○	○	○	
	MDIS	既存製品	○	ー	○	
XAdES	関電システム	新規製品	○	ー	○	
	NEC	試作品	○	ー	○	
	富士ゼロックス	新規製品	○	ー	○	

凡例：
○：サポート(合格)
×：不合格
ー：製品非サポート

オフライン共通データ検証テスト結果 (カテゴリ内企業名五十音順)

	データ生成企業名(略称)	種別	ES-T	ES-XL	ES-A	備考
CAdES	RSAセキュリティ	既存製品	○	○	○	
	NTTデータ	試作品	○	○	○	
	セコム	既存製品	○	○	○	
	日本電子公証機構	既存製品	○	○	○	
	NTT	試作品	○	○	○	
	ハイパーギア	既存製品	○	○	○	
	PFU	試作品	ー	ー	ー	
	日立製作所	試作品	○	○	○	
	三菱電機	試作品	○	○	○	
	MDIS	既存製品	○	ー	○	
XAdES	関電システム	新規製品	○	ー	○	
	NEC	試作品	○	ー	○	
	富士ゼロックス	新規製品	○	ー	○	

凡例：
○：サポート(合格)
×：不合格
ー：製品非サポート