認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

申請受付年月日(受付番号)	**平成18年7月10日（IT認証6089）**
認証番号	C0068
認証申請者	**株式会社 日立製作所**
TOEの名称	EUR Form Client
TOEのバージョン	05-07
PP適合	**なし**
適合する保証要件	EAL2+ALC_FLR.1
TOE開発者	**株式会社 日立製作所**
評価機関の名称	**みずほ情報総研株式会社　情報セキュリティ評価室**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成18年12月15日

独立行政法人 情報処理推進機構
セキュリティセンター 情報セキュリティ認証室
技術管理者　田渕　治樹

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「EUR Form Client 05-07」は、独立行政法人 情報処理推進機構が定める ITセキュリティ認証手続規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「EUR Form Client 05-07」（以下「本TOE」という。）について「みずほ情報総研株式会社　情報セキュリティ評価室」（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である株式会社 日立製作所に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称:	EUR Form Client
バージョン:	05-07
開発者:	株式会社 日立製作所

1.2.2 製品概要

本製品は、紙帳票と同じイメージでWeb画面に帳票を表示し、データの入力及びサーバへの送信を行うシステムである電子フォームシステムにおいて、電子的な帳票入力を行うためにクライアント実行環境で利用するソフトウェアである。また本製品は、入力する帳票データに対して予め設定されたセキュリティポリシーを実現するために、入力データに対するXML署名付与機能、XML署名検証機能、及び暗号通信開始機能を提供する。

1.2.3 TOEの範囲と動作概要

(1) TOE動作環境

TOEを利用したシステム概要及びTOEを利用した業務の流れを図1-1に示す。

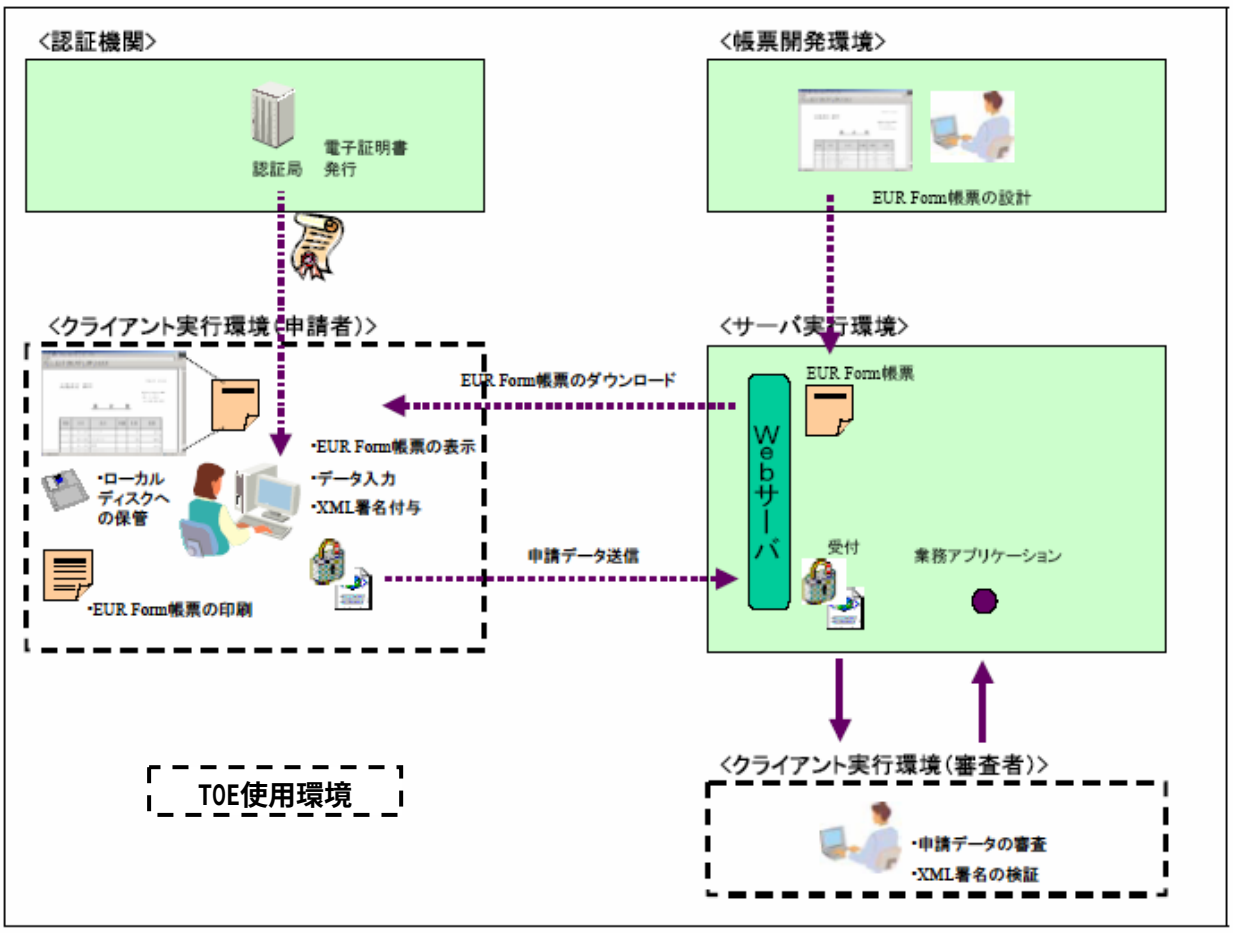

図1-1　TOEを利用したシステム概要

図1-1に示したシステムを構成する構成要素について説明する。

認証機関：

　当該電子フォームシステムで必要な電子証明書を発行する。

帳票開発環境：

　当該電子フォームシステムで利用するEUR Form帳票を設計する。

クライアント実行環境（申請者）：

　EUR Form帳票の表示, 申請データ入力、XML署名の付与及び入力した申請データをサーバへ送信する。クライアント実行環境（申請者）はTOEである。

クライアント実行環境（審査者）：

　申請者が付与したXML署名の検証を行う。クライアント実行環境（審査者）はTOEである。

サーバ実行環境：

Webサーバを介して、申請者に対するEUR Form帳票及びTOEのダウンロード、申請者からの申請データの受付、審査者に対する申請データのダウンロードなどを行う。

図1-1に示したシステムにおける申請業務の流れを以下に示す。

- 申請者は、あらかじめ当該電子フォームシステムで指定された認証機関から電子証明書を申請・取得する。
- 電子フォームシステム設計者は、当該電子フォームシステムで利用するEUR Form帳票を設計する。その際XML署名が必要かどうか、HTTPS通信が必要かどうかに関するセキュリティポリシーを決定し、EUR Form帳票に設定する。
- 電子フォームシステム設計者は、作成したEUR Form帳票及びTOEをサーバ実行環境に登録する。
- 申請者は、TOEをサーバ実行環境からダウンロードし、インストールする。
- 申請者は、当該電子フォームシステムのEUR Form帳票を、Webブラウザを用いてダウンロードする。
- TOEは、ダウンロードされたEUR Form帳票を表示し、EUR Form帳票に当該電子フォームシステムで指定された申請データを入力する。
- 申請者は、当該電子フォームシステムのセキュリティポリシーで指定されていた場合、XML署名を付与する。
- 申請者は、申請データの入力・XML署名付与の後、申請データをサーバに送信する。その際、当該電子フォームシステムのセキュリティポリシーで指定されていた場合、TOEは、送信する申請データに対してXML署名を付与し、またHTTPS通信の開始を指示する。
- 審査者は、サーバ実行環境からWebブラウザを用いて申請データをダウンロードし、申請データの確認及びXML署名の検証を行う。

(2) TOE範囲

本TOEは図1-1の動作環境において破線内に示される＜クライアント実行環境（申請者）＞及び＜クライアント実行環境（審査者）＞における端末上で動作するクライアントアプリケーションである。

図1-2にTOEの物理的範囲（コンポーネント構成）を示す。

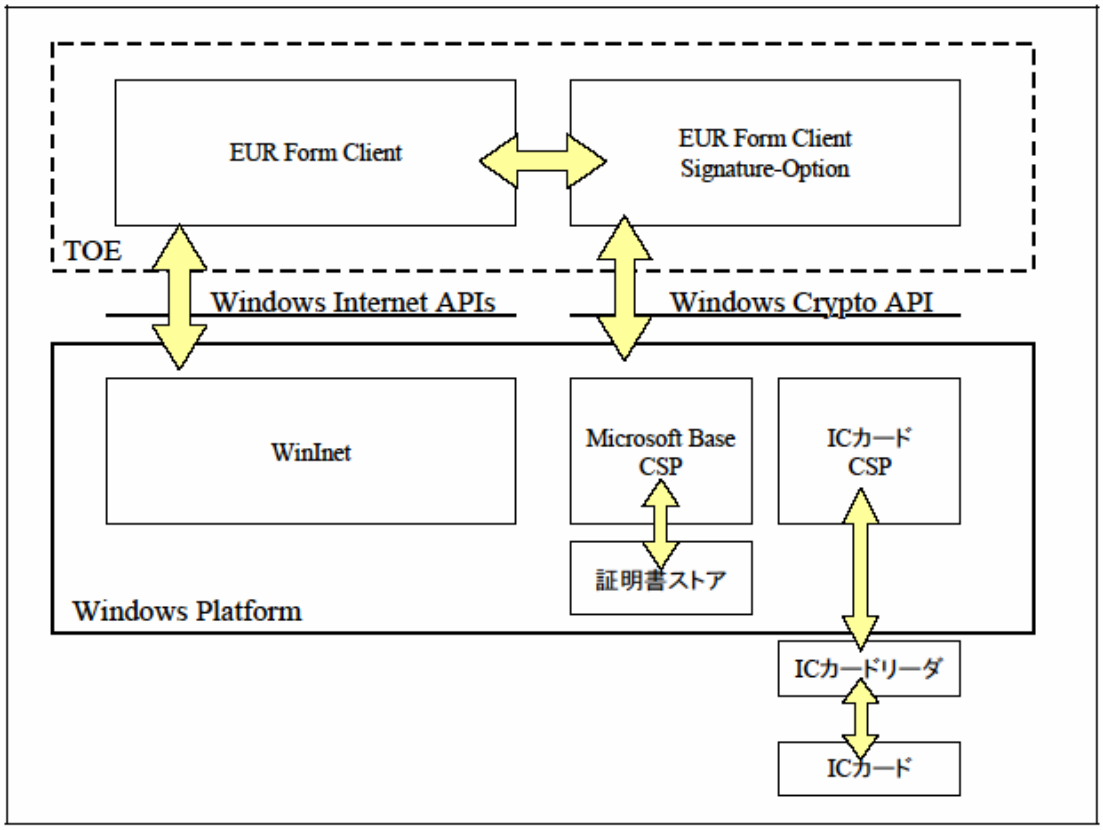

図1-2　TOEの物理的範囲（コンポーネント構成）

図1-2の破線内で示したコンポーネントであるEUR Form Client及びEUR Form Client – Signature Optionが、TOEの物理的範囲内である。 TOEは、Windows Platformが提供するWindows Crypto APIを介し Cryptographic Service Provider(CSP)を用いて、署名付与、署名検証を行う。Windows Platformの証明書ストアを使用する場合、Windows Platformが提供するMicrosoft Base CSPを利用する。ICカードを使用する場合、ICカードアクセスのための専用ソフトウェアが提供するICカードCSPを利用する。またTOEは、Windows Platformが提供する Windows Internet APIsを介し、WinInetに対してHTTPS通信の開始を指示する。

1.2.4　TOEの機能

TOEが提供する機能は、帳票データ入力クライアントとしてのメイン機能、及びセキュリティ機能である。以下に各提供機能に関する機能概要を示す。

(1)TOEメイン機能

・EUR Form帳票表示

申請者がWebブラウザを用いてダウンロードした、あるいはダウンロード後ローカルディスクへ保存したEUR Form帳票をWebブラウザ上に表示する。

・申請データ入力

申請者が入力する申請データを受け付ける。

・EUR Form帳票印刷

EUR Form帳票を申請者が入力した申請データと共に印刷する。

・EUR Form 帳票保存

申請者が申請データの入力途中の場合、あるいはサーバへ送信する申請データの控えとして、EUR Form帳票をローカルディスクへ保存する。

・申請データ送信

申請者による入力が完了した申請データを、電子フォームシステムによって指定されたサーバに送信する。

(2)TOEセキュリティ機能

・XML署名付与機能

(a) メッセージ署名機能

EUR Form帳票にメッセージ署名機能を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOEは、申請者がサーバに送信する申請データ全体を署名対象としてXML署名を付与する機能を提供する。

(b) 部分署名機能

EUR Form帳票に部分署名機能を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOEは、EUR Form帳票に設定されている署名対象データに対してXML署名を付与する機能を提供する。

XML署名の付与機能において、署名形式は、PKCS#1形式、署名アルゴリズムは、SHA-1 RSA を使用する。 また、サーバに申請データを送信する前に、記入内容の誤りに気付いた場合など、部分署名を付与した者であれば、当該部分署名を解除し、記入訂正を行うことができる。

・XML署名の検証機能

申請データに部分署名が付与されていた場合、TOEは審査者が、当該部分署名を検証する機能を提供する。本機能により、審査者は、当該部分署名が付与された以降に、当該部分署名の署名対象データに改ざんが行われたか否かを確認することができる。

ただし、上記XML署名付与及び検証機能を実現する上での以下の実装は、TOEが依存するWindows Platformあるいは専用ソフトウェアにより提供され、それらはTOEの範囲外である。

- 具体的な暗号アルゴリズムの実装
  （FIPS-186-2 RSA using PKCS-1、FIPS-180-2 SHA-1）
- 電子証明書のハンドリング機能
- ICカードへのアクセス関連機能

・HTTPS通信の開始機能

EUR Form帳票にHTTPS通信を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOEは、Windows Platformに対してHTTPS通信の開始を指示する機能を提供する。

但し、具体的なHTTPS通信の実装はWindows Platformにより提供され、TOEの範囲外である。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証手続規程」[3]、「評価機関承認手続規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。

(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

(3) 本TOEがセキュリティ設計に基づいて開発されていること。

(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「EUR Form セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1([5][8][11]のいずれか) 附属書C、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「EUR Form Client 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成

18年12月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL2追加である。

追加されるコンポーネントはALC_FLR.1である。

1.5.3 セキュリティ機能強度

本TOEにおいて、確率的または順列的メカニズムに基づくセキュリティ機能要件が無く、セキュリティ機能強度主張を実現すべきITセキュリティ機能が存在しないため、セキュリティ機能強度主張は行わない。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

(1)XML署名の付与機能

(a)メッセージ署名付与機能（SF.MESSAGE_SIGN）

EUR Form帳票にメッセージ署名機能を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOEは、申請者がサーバに送信する申請データ全体を署名対象としてXML署名を付与する機能を提供する。 申請者が、EUR Form帳票に設定された送信ボタンを押下することにより、本機能は起動する。EUR Form帳票には､電子フォームシステム設計者がセキュリティポリシーに従い設定した 電子証明書の格納先が設定されている。

(b)部分署名付与機能（SF.PARTIAL_SIGN）

EUR Form帳票に部分署名機能を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOEは、EUR Form帳票に設定されている署名対

象データに対してXML署名を付与する機能を提供する。 申請者が、EUR Form帳票に設定されたSign帳票コントロールを押下することにより、本機能は起動する。EUR Form帳票には、電子フォームシステム設計者がセキュリティポリシーに従い設定した 、署名対象データ、電子証明書の格納先が設定されている。 部分署名の付与に成功した場合、TOEは、EUR Form帳票に設定された定義に従い、部分署名を付与した旨を示すマークを申請者に提示する。

部分署名の付与に使用した電子証明書を保持している場合、申請者は、Sign帳票コントロールを操作することにより、一旦付与した部分署名を解除することができる。部分署名の解除に成功した場合、TOEは 部分署名を付与した旨を示すマークも解除する。

上述した２つのセキュリティ機能において、TOEはIT環境に格納された電子証明書、及びIT環境が提供する暗号操作機能(Microsoft Base CSP：図1-2参照）を利用してXML署名を付与する。

電子証明書の格納先として、Windows Platformの証明書ストアが指定されていた場合、TOEは、署名対象データを成形しMicrosoft Base CSPを利用して署名データを生成する。 証明書ストアに複数の電子証明書が格納されていた場合、TOEは電子証明書を識別する情報を申請者に提示し、申請者は適切な電子証明書を選択する。TOEは、選択された情報で示される電子証明書を用い、Microsoft Base CSPを利用して署名データを生成する。電子証明書の格納先として、ICカードが指定されていた場合、TOEは、署名対象データを成形しICカードCSPを利用して署名データを生成する。また、上記いずれの場合も署名生成の際にはSHA-1/RSAアルゴリズムが使用される。

(2)XML署名検証機能（ SF.PARTIAL_VERIFY）

申請者から送信されたEUR Form 帳票に部分署名が付与されていた場合、TOEは審査者が当該部分署名を検証する機能を提供する。 審査者が当該Sign帳票コントロールを操作することにより本機能は起動する。 当該Sign帳票コントロールの署名対象データに対する改ざんが検出された場合、TOEは、当該署名対象データが改ざんされた可能性がある旨、審査者に対して提示する。 当該Sign帳票コントロールの署名対象データに対する改ざんが検出されなかった場合、TOEは、当該署名対象データが署名付与後変更されていない旨、審査者に対して提示する。 本機能により、審査者は、当該部分署名が付与された以降に、当該部分署名の署名対象データに改ざんが行われたか否かを確認することができる。

TOEは、EUR Form 帳票に付与された部分署名の署名対象データを成形し、IT環境であるWindows Platformが提供するMicrosoft Base CSPを利用して署名の検証を行う。

(3) HTTPS通信の開始機能（SF.INITIATE_HTTPS）

Form帳票にHTTPS通信を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOEは、申請データを送信するサーバとの間でHTTPS通信を開始する機能を提供する。

TOEは、Windows Platformに対してHTTPS通信の開始を指示し、実際のHTTPS通信はWindows Platformが提供される機能により実施される。

1.5.5 脅威

本TOEが想定する脅威は存在しない。

1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-1に示す。

表1-1 組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.SIGN	当該電子フォームシステムにおいては、申請データに対して署名を付与すること。
P.VERIFY	当該電子フォームシステムにおいては、電子証明書に格納されている公開鍵を用いて、申請データに付与された署名を検証し、申請データの改ざんチェックを行なうこと。
P.SECURE_CHANNEL	当該電子フォームシステムにおいて、申請データの送信を行なう場合、HTTPSを使用し、通信経路の暗号化を行なうこと。

1.5.7 構成条件

本TOEはソフトウェアアプリケーションであり、必要とするハードウェア構成及びソフトウェア構成は表1-2、表1-3に示す通りである。

表1-2　ハードウェア構成

端末名	種別	説明
クライアント実行環境（申請者）及び（審査者）		
本体		
	本体マシン	表1-3に示すOSが動作するPC/AT互換機
	CPU	Intel ®Celeronプロセッサ1GHz以上
	メモリ	512MB以上
	HDD	20GB以上
クライアント実行環境（申請者）		
ICカードリーダ	※電子証明書がICカードに格納されている場合に使用	
	「公的個人認証に対応するICカードリーダライタ」	

「公的個人認証に対応するICカードリーダライタ」は、財団法人 自治体衛星通信機構 公的個人認証サービスセンターが仕様公開及び適合性検証を実施している。

表1-3　ソフトウェア構成

ベンダ名	製品名	説明
クライアント実行環境		
Microsoft	Windows XP Professional SP2 以降	OS
Microsoft	Internet Explorer Version 6.0 以降	Webブラウザ
(株)日立製作所	EUR Form Client 05-07	TOE
(株)日立製作所	EUR Form Client – Signature Option 05-04	TOE
公的個人認証サービス 指定認証機関 財団法人 自治体衛星通信機構	公的個人認証サービス 利用者クライアントソフト平成17年10月版	ICカードに格納された電子証明書を利用する場合に使用する。

公的個人認証サービス 利用者クライアントソフト は、ICカードに格納された公的個人認証サービスの電子証明書を利用するためのソフトウェアであり、公的個人認証サービスを利用した電子申請を行うために必要となるソフトウェアである。 ICカードに格納された公的個人認証サービスの電子証明書の発行を受けた際に、市区町村の窓口にてCD-ROM形式で渡される。 図1-2のICカードCSPと示したコンポーネントは、本ソフトウェアに格納されている。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-4に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-4　TOE使用の前提条件

識別子	前提条件
A.CERT_USE	申請者は、署名の付与に使用する電子証明書として、当該電子フォームシステムで既定されたTOE外の信頼できる認証機関によって発行された電子証明書を利用する。発行された電子証明書は信頼できるものとする。また、申請者は、この電子証明書を適切に管理し、申請データへの署名に使用する電子証明書を正しく選択するものとする。
A.EUR_FORM	電子フォームシステム設計者は、当該電子フォームシステムのセキュリティを考慮し、適切なセキュリティポリシーを EUR Form帳票に設定するものとする。また、電子フォームシステム設計者は、適切なセキュリティポリシーが設定されたEUR Form帳票を当該電子フォームシステムのWebサーバに登録し、TOEの利用者に対してセキュアにダウンロードさせる。
A.IT_ENV	TOEが稼動するために使用するソフトウェアは、正しく動作するものとする。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

- 電子フォームシステムEUR Form　EUR Formサーバシステム構築

  識別子：3020-7-442-A0

- 電子フォームシステムEUR Form　EUR Form Client 操作

  識別子：3020-7-443-A0

- EUR Form セキュア取扱説明書

  識別子：036169

- EUR Formクライアントダウンロードサイト

  識別子：http://www.hitachi.co.jp/Prod/comp/soft1/eur/DL/index.html

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成18年7月に始まり、平成18年12月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成18年9月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成18年9月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1に示す。

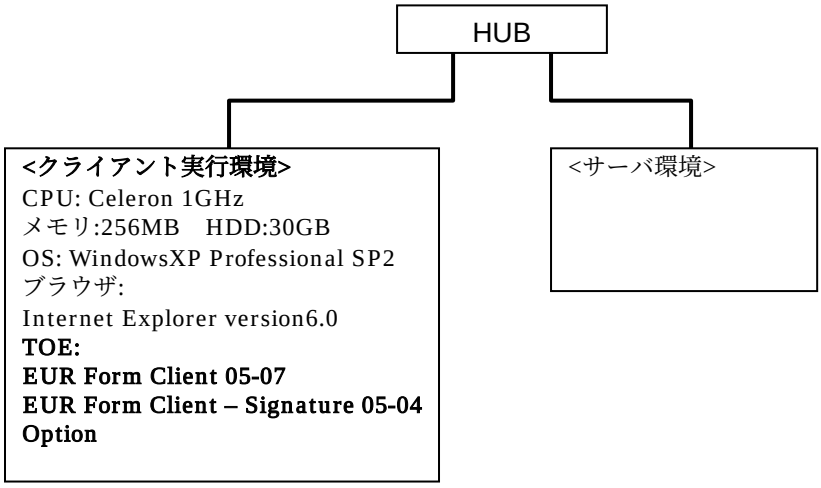

図2-1　開発者テストの構成

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストはSTにおいて識別されているTOE構成と同等のTOEテスト環境で実施されている。以下はSTで識別されるハードウェア構成とは完全に一致しない点に関して、同等とみなすことが出来る理由である。

STに識別されるハードウェア構成における本体のメモリについては、512MB以上が要求されているのに対し、テスト構成では256MBとなっている。しかしTOEが動作するために必要なメモリサイズとしては256MBで十分である事と、テストに使用する帳票データのサイズも小さいものであるため256MBのメモリ構成でもSTに識別されるハードウェア構成と同等であるとみなすことができる。

b.テスト手法

テストには、以下の手法が使用された。

①STで識別された各セキュリティ機能に対して、その機能のふるまいに影響を与える全ての操作、処理フローを分析し、その全てに対して網羅的にテストを実施する。

②抽出されたテスト項目に従ってTOEのGUI操作を行い、TOE自身のふるまいについて、表示されるメッセージダイアログ等の確認をする。

③TOEにネットワーク接続されたサーバマシン上で、TOEから送信された帳票データの検証を行いサーバマシン上でその検証結果を確認すると共に、TOEに対して返信された検証結果メッセージをTOE上で確認する。

c.実施テストの範囲

テストは開発者によって表2-1に示す16項目が実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。

表2-1 開発者テスト項目概要

TOEセキュリティ機能	項目数
部分署名付与機能	8
部分署名解除機能	1
メッセージ署名付与機能	2
署名検証機能	3
HTTPS通信開始機能	2

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテスト構成を図2-2に示す。

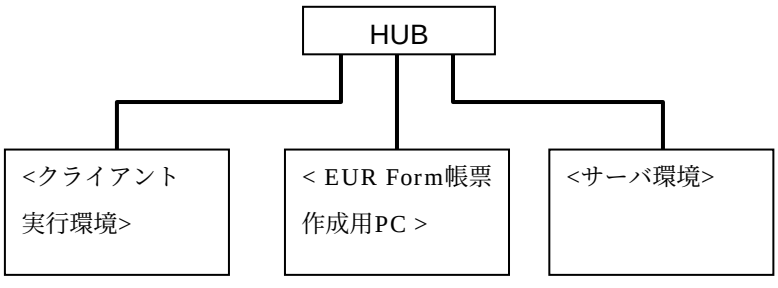

図2-2 評価者テストの構成

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-2に示す。図2-2のテスト構成は、開発者テスト環境と同様の構成に＜EUR Form帳票作成用PC＞が追加されているが、これはテスト用帳票をテスト中に作成する可能性があったため追加されたもので、テスト結果に影響を与えるものではない。従って、評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されているとみなすことができる。

b.テスト手法

評価者は、開発者が行ったテスト手法がセキュリティ機能の期待されたふるまいを検証するのに適していると判断し、開発者テストと同様の手法でテストを実施している。

c.実施テストの範囲

評価者が独自に考案したテストを7項目、開発者テストのサンプリングによるテストを16項目、計23項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① STで識別されたすべてのセキュリティ機能をカバーするためのテスト項目抽出
② セキュリティ機能のふるまいに影響を与えるすべての要因をカバーするためのテスト項目抽出
③ 利用者が入力したデータの影響を受けるセキュリティ機能に関するテスト項目

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。

② 当該所見報告書でなされた指摘内容が正しく反映されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL2及び保証コンポーネントALC_FLR.1を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るま

	でになされた所見報告書による指摘も適切と判断される。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別､概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示されたすべてのTOE及びIT環境のセキュリティ要件の記述が、正当であること、客観的に、明確に、曖昧さなく表現されていること、及び保証要件でサポートされるのに適切で妥当であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示されたあらゆるITセキュリティ要件の依存性のすべてが識別されていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_CAP.2.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。

ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.1.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのソフトウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.1.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**

AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確に対応していることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。

ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、確率的または順列的メカニズムが存在しないため非適用であることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、確率的または順列的メカニズムが存在しないため非適用であることを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。
ライフサイクルサポート	**適切な評価が実施された**
ALC_FLR.1.1E	評価はワークユニットに沿って行われ、欠陥修正手続き証拠資料がすべてのセキュリティ欠陥を追跡するために使用される手続き、及びTOE利用者に必要な情報を提供するための手段を含み、この手続きの適用により、欠陥訂正方法の調査状況と同時に各々のセキュリティ欠陥の性質と影響に関する記述が提供されることを確認している。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

CSP (Cryptographic Service Provider)	Microsoft(R)社は、暗号エンジンをOSに組み込む際に、柔軟性と拡張性を重視して、暗号化ベンダがそれぞれプラグインできるオープンAPIを提供している。これらのプラグイン暗号エンジンをCSPという。
EUR Form帳票	電子フォームシステム設計者が設計する帳票ファイル。記入すべき項目、Sign帳票コントロール、送信ボタンなどの各種コントロールが設定されている。当該電子フォームシステムで使用する。
Sign帳票コントロール	XML部分署名を付与する際に設定する署名用コントロール。
審査者	TOEであるEUR Form Clientを利用して申請者の申請情報を検証する者。
申請者	TOEであるEUR Form Clientを使用し、当該電子フォームシステムを利用して申請を行う者。
電子フォームシステム	紙帳票と同じイメージでWeb画面に帳票を表示し、データの入力及びサーバへの送信ができるシステム。

電子フォームシステム設計者	当該電子フォームシステムのセキュリティポリシーの設計を行う者。

6 参照

[1] EUR Formセキュリティターゲット Version 1.06（2006年11月10日）(株)日立製作所

[2] ITセキュリティ評価及び認証制度の基本規程　平成17年7月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月 (平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] EUR Form Client 評価報告書 (06000529-01-R003-02) 2006年12月6日 みずほ情報総研株式会社　情報セキュリティ評価室