ＳＴ確認報告書

評価対象

申請受付年月日(受付番号)	平成14年 5 月 8日（ST確認2007）
ＳＴ確認申請者	日立ソフトウェアエンジニアリング株式会社
ＳＴの名称	Smart Folder 3 Security Target Version2.19
ＰＰ適合	なし
適合する保証要件	ASE（ST評価）クラス （TOEの保証パッケージはEAL4）
ＳＴ開発者	日立ソフトウェアエンジニアリング株式会社
評価実施機関の名称	電子商取引安全技術研究組合研究所

上記のSTについての評価は、以下のとおりであることを確認したので報告します。
平成16年2月26日

独立行政法人製品評価技術基盤機構
適合性評価センター管理課情報セキュリティ室
技術管理者　田渕　治樹

評価基準等：「セキュリティターゲットの確認業務実施規程」で定める下記の規格に基づいて評価された。

① ISO/IEC 15408:1999 Information technology － Security techniques － Evaluation criteria for IT security.
② JIS X 5070(2000) セキュリティ技術 － 情報技術セキュリティの評価基準。
③ Common Criteria for Information Technology Security Evaluation Version 2.1
④ JIS TR X 0049(2001) 情報技術セキュリティ評価のための共通方法
⑤ Common Methodology for Information Technology Security Evaluation
⑥ 認証機関が公開する③および⑤の翻訳文書

評価結果：合格

Smart Folder 3 Security Target Version 2.19 は、独立行政法人製品評価技術基盤機構が定めるセキュリティターゲットの確認業務実施規程に従い、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。

その他：なし

目次

1 全体要約

1.1 はじめに

このST確認報告書は、「Smart Folder 3 Security Target Version 2.19」（以下「本ST」という。）について電子商取引安全技術研究組合研究所（以下「評価実施機関」という。）が行ったセキュリティ評価に対し、その内容の確認結果を申請者である日立ソフトウェアエンジニアリング株式会社に報告するものである。

本ST確認報告書の読者は、本書とともに、対応する本ST［1］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、本STにおいて詳述されている。

本ST確認報告書は、本STに対する確認結果を示すものであり、対応するTOEのいかなる実装についても言及していないことに留意されたい。

1.2 評価製品

1.2.1 製品名称

本STが対象とする製品は、以下のとおりである。なお、TOEの正確な範囲は、1.2.3節で定義される。

- 名称: Smart Folder 3 MULTOS application
- バージョン: 03-06
- 開発者: 日立ソフトウェアエンジニアリング株式会社

1.2.2 製品概要

本製品は、ICカード用OSであるMULTOS上で動作するアプリケーションである。このアプリケーションは、PKI（公開鍵認証基盤）スマートカードアクセスソフトウェアのコンポーネントとして、MULTOSを搭載したICカード(MULTOS smart card)内においてPKIで用いられる鍵（公開鍵・秘密鍵）の生成・削除や格納、署名の生成、生成またはインポートしたPKI秘密鍵による復号、デジタル証明書のインポート/エクスポートを可能とする。

本製品はMULTOS smart cardのEEPROM上にロードされ、MULTOS アプリケーションのひとつとして実行される（図 1)。

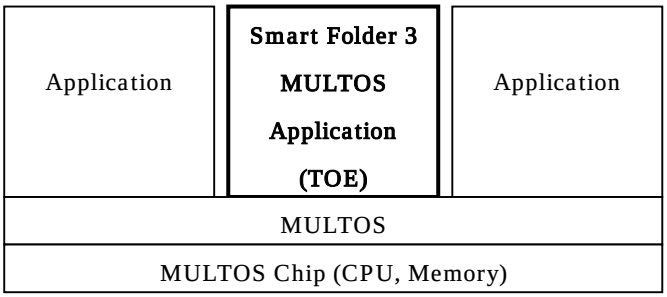

図 1 MULTOS smart card**における**TOE

1.2.3 TOEの範囲

本製品とTOEの範囲は完全に一致する。本TOEはMULTOS上で動作するアプリケーションソフトウェアである。

1.2.4 TOEの動作概要

TOEは、一般的利用者のPKI鍵とデジタル署名を格納し、これらの利用にあたってはユーザ認証によりアクセス制御を行う。TOEに関連する利用者は、PKIソフトウェアなどのサービス利用にあたりTOEをそのスマートカードアクセスソフトコンポーネントとして用いるnormal user（一般利用者)、TOEを含むMULTOS smart cardを発行するissuer（発行者)、normal userの利用に便宜を図るadministrator（管理者）を想定する。それぞれの利用者における運用形態を図 2に示し、それらのTOEの動作概要を以下に述べる。

TOEはissuerによりMULTOS smart card上にロードされる。Issuerは、認証に用いるnormal user PINとadministrator PINの初期値の設定、認証における方針を決定するポリシーデータの初期値の設定を行う。また、ユーザデータ（PKI鍵とデジタル証明書）の生成あるいはインポートがなされる。これらの操作はissuerのみが保持する

Issuer Tool Libraryによってのみ可能である。これらの操作の後、TOEとともにMULTOS smart cardがnormal userに配付される。

配付されたTOEは、normal user PINの初期値による認証の後、normal user PINを変更することで利用可能となる。TOEはPKI鍵の生成・削除・インポート、デジタル証明書のインポート/エクスポート、署名、生成またはインポートしたPKI秘密鍵による復号をuser toolを用いて行うことができる。これらの操作に先立ち、TOEは利用者に対しnormal user PINによる認証を求める。TOEはissuerが設定したポリシーデータに従い以下の認証方針を実施する。

- normal user PIN変更の際、最低長を下回る入力PINを拒否する。
- 認証の際のPIN入力の連続した誤り回数を検出し、設定回数に達した場合normal userの機能をロックする。
- 署名と復号操作時に再認証を要求する。

Administrator PINによる認証が成功すると、TOEにおいてadministrator PINの変更とnormal userの機能ロックの解除、そしてTOEの初期化（発行前の状態に戻す）がadministrator toolを用いて可能となる。

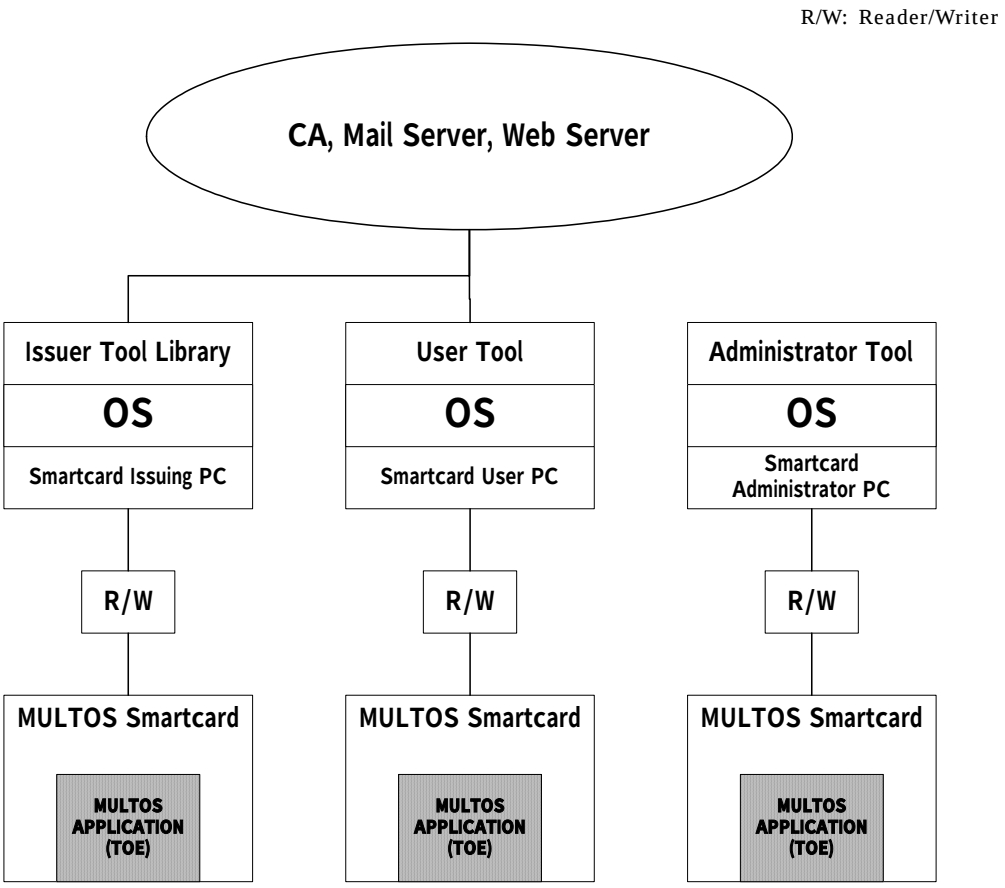

図 2　TOEの運用形態

1.3 評価実施

Smart Folder 3 Security Target Version 2.19のセキュリティ評価は、独立行政法人製品評価技術基盤機構が独立した認証機関として運営するITセキュリティ評価・認証プログラムに基づき、公表文書「セキュリティターゲットの評価・確認申請等の手引き（平成14年4月)」[2]、「セキュリティターゲット評価実施機関に対する要求事項(平成14年4月)」[3]、セキュリティターゲットの確認申請者・登録者に対する要求事項 (平成14年4月)」[4]に規定された内容に従い、評価実施機関によって実施された。

本評価の目的は、申請者から提出された本ST[1]が、CCパート1 ([5][8][11][14]のいずれか) 附属書C、CCパート2 ([6][9][12][15]のいずれか) の機能要件及びCCパート3 ([7][10][13][16]のいずれか) のASEクラスの規定を満たしており、セキュリティ機能設計の基本文書として技術的に妥当なものであるかどうかを評価することである。ただし、ASEクラスの規定の中で、TOE評価と関連する要求事項については、評価の項目に含まれていない。なお、評価方法は、CEMパート2 ([17][18][19]のいずれか) に準拠する。

認証機関は、評価実施機関である電子商取引安全技術研究組合研究所が実施するSTの評価を監督し、ST評価が所定の手続きに沿って行われたことを確認した。評価は、平成16年1月15日の評価実施機関による「ST評価報告書 5.0版 2004年1月15日 DEN-ETRST-0005-00」の提出をもって完了し、同報告書に基づき、認証機関は本ST確認報告書案を作成した。

1.4 報告概要

1.4.1 PP適合

適合するPPはない。

1.4.2 EAL

本STが規定するTOEの評価保証レベルは、EAL4である。

1.4.3 セキュリティ機能強度

本STは、最小機能強度として、”SOF-basic”を主張する。

SOF-basicは、低い攻撃力を持つ攻撃者に対抗できるレベルである。本製品は接続される外部装置が安全に管理されており、R/Wを経由しない直接的な資産へのアクセスも物理的攻撃には高度な攻撃力を要するため、最小機能強度はSOF-basicで適切とされた。

1.4.4 セキュリティ機能

本STで扱うTOEのセキュリティ機能は以下のとおりである。

- SF.ACCESSCONTROL（ユーザデータアクセス制御）
  TOEに格納されているPKI鍵及び証明書へのアクセスは、ユーザアクセス制御方針に従ったアクセス制御がなされ、それに違反するアクセスを制限することができる。

- SF.PINAUTHENTICATION（PINによる認証）
  TOEは、TOEの機能の利用に先立ち、利用者にPINによる認証を求める。認証後、利用者はそれぞれのPINを変更することが可能となる。

- SF.CARDLOCK（認証失敗によるカードのロック）
  TOEは、認証を連続してissuerにより予め設定された回数を超えて失敗した場合、その利用者の機能をロックすることができる。Normal userの機能ロックはadministratorにより解除することが可能である。Administrator機能がロックされるとTOEのセキュリティ機能は利用不可能となる。

- SF.INITIALIZE（TOEの初期化）
  Administratorは、TOEを発行前の状態に初期化することができる。

- SF.PINLENGTHMANGE（PIN長の検査）
  PINの変更に際しては、予め設定された最低長以下のPINの設定を拒否する。

- SF.PKIKEY（PKI鍵の生成・削除）
  TOEは暗号アルゴリズムを用いて1024ビット長のPKI鍵を作成することができる。また、PKI鍵をTOE外からインポートすることも可能であるが、この場合のPKI鍵の強度についてTOEは関与しない。PKI鍵を削除する場合、TOEはその再利用を防ぐため、不揮発性メモリのPKI鍵領域をゼロ化する。

- SF.REAUTH（操作の再認証）
  TOEは、issuerが発行前にフラグを設定することで、TOEの署名と復号操作の際、利用者に再認証を求める。

1.4.5 脅威

TOEは、**表 1**に示す脅威を想定し、本製品は、これに対抗する機能を備える。

表 1　想定する脅威

識別子	脅威
T.ATTACK	An unauthorized person logs on the TOE. Then, the TOE is utilized to generate a signature and/or decrypt encrypted information by PKI private key.
T.GENKEY	An unauthorized person guesses PKI private key from PKI public key, when TOE generates vulnerable PKI keys.
T.SENDDATA	While normal user leaves the TOE without logging off after successful authentication, an unauthorized person uses PKI private key of the TOE.
T.IMPERSONATE	An unauthorized person tries the PIN-input thousands of times and eventually guesses the PIN, which is used for user authentication, and uses PKI private key of the TOE.
T.ATTACKSFDATA	A malicious user modifies TSF data, to which an access is not permitted for the person, after logging on to the TOE.
T.ATTACKUSERDATA	A malicious user modifies User data, to which an access is not permitted for the person, after logging on to the TOE.
T.MODIFYPIN	A malicious user modifies the PIN stored in the TOE. And the malicious user illegally logs on.
T.RESIDUAL	A malicious user steals residual data after a deletion of secret data (e.g. the PKI private key) to restore the secret data.
T.ABUSE	If the TOE includes PKI private key, an unauthorized person abuses PKI private key of the TOE while the TOE is being delivered from an issuer's site to a user's site
T.ADMIN	A malicious administrator of the TOE abuses a normal user's PKI private key of the TOE

1.4.6　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はない。

1.4.7　構成条件

本TOEは、MULTOS smart card上にのるMULTOS用アプリケーション製品である。本TOEの動作環境は図 1に示すものであり、個々の詳細は以下のとおりである。

MULTOS smart card	
OS	HITACHI MULTOS 4.06
Chip	AE45C

本TOEは、利用者が保持し必要に応じてPKIアプリケーションのコンポーネントとしてR/Wを通じ図 2のような使用形態で用いられる。本TOEと接続されるハードウェア及びソフトウェアの構成は以下のとおりである。

Cooperate PC (issuer tool library / administrator tool)	
Hardware	AT compatible
OS	Microsoft Windows 2000 / NT 4.0
Browser/Mailer	Netscape Navigator / Communicator 4.75 Microsoft Internet Explorer 5.0
Cooperate PC (user tool)	
Hardware	AT compatible
OS	Microsoft Windows 2000/ NT4.0/ 98/ 98SE
Browser/Mailer	Netscape Navigator / Communicator 4.75 Microsoft Internet Explorer 5.0
Smart Card Reader / Writer	
PC/SC compliant smart card Reader / Writer	

1.4.8 動作環境の前提条件

TOEを使用する環境において有する前提条件を**表 2**に示す。

これらの前提条件が満たされない場合、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 2 TOE使用の前提条件

識別子	前提条件
A.CARD	The TOE must run on MULTOS smart card. It is assumed that MULTOS chip implements countermeasures against hardware attacks (e.g. direct electrical modification or probing). The MULTOS OS also implements countermeasures against attacks from other applications loaded on a same MULTOS smart card by providing firewalls. Therefore MULTOS smart card is safe.
A.ISSUER	It is assumed that issuer is not malicious and does what issuer is supposed to do correctly. The issuers set Minimum length of administrator PIN and Minimum length of normal user PIN of 6 characters or longer. The issuers must set the Re-authentication flag for signing operation and the Re-authentication flag for decrypting operation “enable”. And the issuer must set the TOE lock function “ON”.

A.ISSUERTOOL	It is assumed that only issuers can possess and use an issuer tool library. Only the issuer tool library can perform issuer operations. An attacker with low attack potential, which is expected for the TOE, can not develop a pseudo issuer tool library by guessing the TOE command and data structures.
A.PIN	It is assumed that users will keep their PIN secret and key inputs are not monitored by any means. And users select a PIN composed of at least one special character and one digit out of available special characters, digits and alphabets.
A.RW	It is assumed that the MULTOS smart card reader/writer used with the TOE works correctly and does not have any malicious functionality (e.g. stealing or modifying data going through it).
A.PC	It is assumed that the PC used with the TOE, operating system, other hardware, drivers and the cooperating PC software are properly managed and not infected with malicious codes or functionalities. Especially, cables connecting PC and peripherals must not be monitored.
A.IMPORTKEY	It is assumed that the TOE imports only not vulnerable PKI keys. The not vulnerable PKI keys can be utilized to generate a signature and/or decrypt encrypted information. And PKI private keys cannot be easily guessed from corresponding PKI public keys.

1.5 ST確認に関わる注意事項

ST確認は、CCで規定された評価の全過程から、ST評価の部分だけを抜き出した評価に基づいて行われるものである。したがって、ST評価を規定したASEクラスの要件の中で、TOE評価と関連する事項についてはST評価の対象になっていない。また、ASEクラス以外の保証クラスに属する事項、例えば、STの記載事項がそのとおりに設計されTOEに実装されているかどうか、TOEに悪用可能な脆弱性が残っていないかどうか、あるいはTOEの製造・配付が安全な手続きに基づいて行われているかなども評価の範囲外である。これら評価対象外の事項については確認も行われていないことに、本報告書の読者は留意すべきである。

ST確認は、TOEに対する、潜在的なものを含めたあらゆるセキュリティ上の脅威が完全に対策されていることを保証するものではない。評価完了後にTOEやそのIT環境にあらたな脅威が発見される可能性は常に考慮されるべきであり、TOE利用者は、TOEに関わる最新のセキュリティ関連情報に継続的な注意を払うことが必要である。

STの中で前提条件として記述されたものは、TOEを安全に使用する上での必須事項である。これらの条件が満たされないと、TOEのセキュリティ機能は、期待される効果を発揮することができない。前提条件を満たすためのTOEの安全な運用管理は、TOE利用者の責務である。

本ST確認報告書は、認証機関が該当するTOEを保証し、その使用を推奨することを意図したものではない。

2 TOE構成

TOEはMULTOS smart cardに搭載されるアプリケーションプログラムである。MULTOS smart cardにはCPU、RAM、ROM(MULTOSが格納されている)、EEPROMから構成され、TOEはこのEEPROM上にロードされる（図 3)。TOEとその他のアプリケーションプログラムはお互いに干渉できない構造になっている。

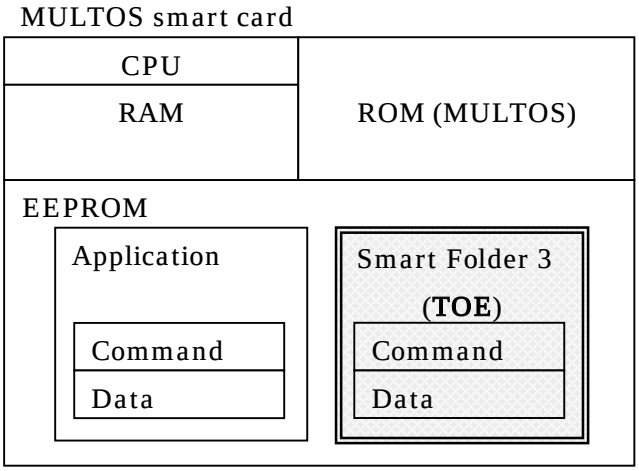

図 3 MULTOS smart card**における**TOE

TOEはコマンドライブラリとデータから構成される。TOEの保持する主なデータは表 3のとおりである。

表 3　TOE**のデータ**

TOE**のデータ**			**説明**
TSF Data	Policy Data	Minimum length of normal user PIN	Normal userが変更可能なPINの最低長。
		Minimum length of administrator PIN	Administratorが変更可能なPINの最低長。
		Maximum number of consecutive wrong normal user PIN inputs	Normal userが許されるPINの誤入力の連続回数。
		Maximum number of consecutive wrong administrator PIN inputs	Administratorが許されるPINの誤入力の連続回数。
		Re-authentication flag for signing operation	署名操作時に再認証を要求するためのフラグ。
		Re-authentication flag for decrypting operation	復号操作時に再認証を要求するためのフラグ。
	Card issue state flag		Issuerにより発行されたかを示すフラグ。ユーザデータのアクセス制御に用いる。

	PIN state flag	Normal user PINが初期値か否かを示すフラグ。
	Normal user PIN	Normal user認証のためのPIN。
	Administrator PIN	Administrator認証のためのPIN。
	Wrong normal user PIN input counter	Normal user認証の誤入力連続回数カウンター。
	Wrong administrator PIN input counter	Administrator認証の誤入力連続回数カウンター。
	Logon state	TOEの状態を示すフラグ。ユーザデータのアクセス制御に用いる。
	User type	利用者がnormal userかadministratorかを示すフラグ。ユーザデータのアクセス制御に用いる。
	Lock state	機能のロック状態を示すフラグ。ユーザデータのアクセス制御に用いる。
User Data	PKI Keys(private and public keys)	利用者の使用するPKI鍵。
	Digital certificates	利用者の使用するデジタル証明書。

3 評価実施機関による評価結果

評価は、CCパート3のASEクラスの規定に基づき、CEMパート2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、ST評価報告書[20]において報告されている。ST評価報告書には、TOEの概要説明、CEMパート2のワークユニットごとの評価内容及び判断が記載されている。各ワークユニットの評価作業において発見された問題点及びその対処の経過・結果も記載されている。

評価実施機関が評価中に発見した問題点は、すべて、開発者による見直しが行われ、最終的に、全ての問題点が解決されている。

総合判定は、「合格」である。

4 結論

4.1 ST確認実施

確認は、評価の過程で評価機関より提出される各資料をもとに、以下の確認を実施した。

① 評価実施機関が評価作業中に指摘した所見報告書の内容が妥当であること。

② 所見報告書でなされた指摘内容が正しくSTに反映されていること。

③ 提出されたSTの内容を確認し、関連する評価者アクションエレメントが本評価報告書で示されたように評価されていること。

④ 本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 本評価報告書に示された評価者の評価方法がCEMに準拠していること。

これらの確認において発見された問題事項を認証レビューとして記載し、評価実施機関に送付した。

認証機関は、本STにおいて、所見報告書およ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。

4.2 ST確認結果

提出されたST評価報告書及び所見報告書を調査した結果、認証機関は、本STがCCパート3に規定されたASEクラスの保証要件を満たしていることを確認した。

評価実施機関の実施した各評価者アクションエレメントについての確認結果を**表 4**にまとめる。

表 4 評価者アクションエレメント確認結果

評価者アクションエレメント	確認結果
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識別、境界の記述が明瞭であることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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、当評価に至るまでなされた指摘(所見報告書)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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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明記され、それらが脅威、組織のセキュリティ、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、当評価に至るまでなされた指摘(所見報告書)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理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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、当評価に至るまでなされた指摘(所見報告書)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理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

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要件はないため非適用であることを確認している。
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要件はないため非適用であることを確認している。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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結しており、理路整然とし、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

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
CA	Certificate Authority
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PKI	Public Key Infrastructure
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の定義を以下に示す。

MULTOS	Multi Application OS。マルチアプリケーションに対応したICカード用オペレーティングシステム。
PC/SC	Personal Computer/Smart Card。Personal ComputerからSmart Cardアクセスのための標準規格。

6 参照

[1] Smart Folder 3 Security Target Version 2.19 Hitachi Software Engineering Co., Ltd. January 6, 2004

[2] セキュリティターゲットの評価・確認申請等の手引き 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター

[3] セキュリティターゲット 評価実施機関に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－ST評価要求－02

[4] セキュリティターゲットの確認申請者・登録者に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－ST申請要求－02

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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2.1 1999年8月 CCIMB-99-032

[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2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999
[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月
[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法
[20] ST評価報告書 5.0版 2004年1月15日 DEN-ETRST-0005-00 電子商取引安全技術研究組合研究所