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

申請年月日（受付番号）	**平成18年8月30日（IT認証6096）**
認証番号	C0107
認証申請者	Stiftung Secure Information and Communication Technologies SIC
TOEの名称	IAIK-JCE CC Core
TOEのバージョン	3.15
PP適合	**なし**
適合する保証パッケージ	EAL3
開発者	Stiftung Secure Information and Communication Technologies SIC
評価機関の名称	TÜV Informationstechnik GmbH, Evaluation Body for IT-Security

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19年6月27日

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

「IAIK-JCE CC Core」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、「IAIK-JCE CC Core」（以下「本TOE」という。）についてTÜV Informationstechnik GmbH, Evaluation Body for IT-Security（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Stiftung Secure Information and Communication Technologies SIC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: IAIK-JCE CC Core

バージョン: 3.15

開発者: Stiftung Secure Information and Communication Technologies SIC

1.2.2 製品概要

本TOE、IAIK-JCE CC Core, version 3.15は、Java言語により開発され「IAIK-JCE toolkit」の一部として利用者に提供され、アプリケーションソフトウェアを開発する際に利用可能な各種機能（電子署名の生成・検証、データの暗号・復号化、乱数生成等）を提供するライブラリである。本TOEにより、以下の機能が提供される。

- hash functions
- signature schemes
- block ciphers
- stream ciphers

- asymmetric ciphers
- message authentication codes
- random number generators

1.2.3 TOEの範囲と動作概要

評価対象となるTOEは、JCA(Java Cryptography Architecture)/JCE(Java Cryptography Extension) frameworkに準拠するCryptographic Service Providerを実装するソフトウェアであり、そのTOE範囲は以下のFigure 1の“IAIK Cryptography Provider”とその直下の各種暗号機能（SHA-1、SHA-256、SHA-384、SHA-512、RIPEMD-160、HMAC、RSA Signature、RSA Cipher、AES、Triple-DES、RC2、ARCFOUR、Secure Random）で示されている。

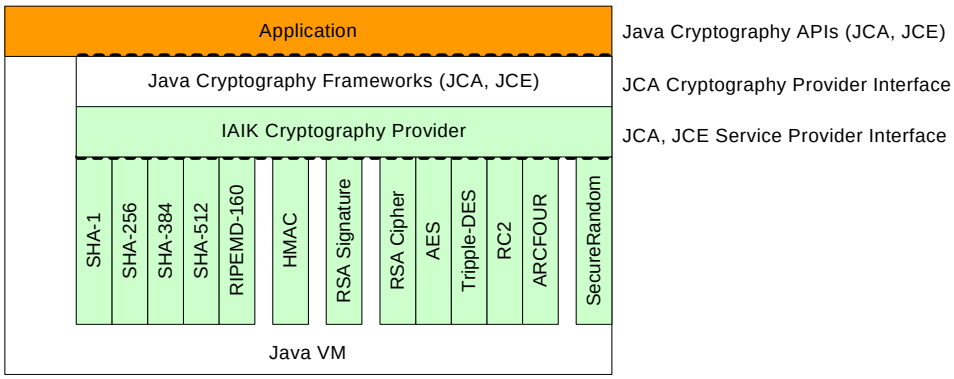

Figure 1: The TOE and its environment

TOEはJCA/JCE frameworkを介してApplicationよりアクセスされ、上図に示されているようなSHA-1やAES等の暗号化機能をApplicationに対し提供する。TOEが提供する機能に関しては、次節にて詳述する。

1.2.4 TOEの機能

TOEはFigure 1で示されている以下の機能群をApplicationに対して提供し、その全機能がTOEセキュリティ機能として定義されている。

a) Hash related functionality

TOEは以下のハッシュアルゴリズムを実装している。

・SHA-1 [FIPS PUB 180-1]
・Ripemd-160 [ISO/IEC 10118-3]
・SHA-256 [FIPS PUB 180-2]
・SHA-384 [FIPS PUB 180-2]
・SHA-512 [FIPS PUB 180-2]

b) MAC related functionality

TOEはHMACアルゴリズムに従いmessage authentication codeを生成する。HMACは以下のハッシュアルゴリズムを使用する。

・SHA-1 [FIPS PUB 180-1]

・Ripemd-160 [ISO/IEC 10118-3]

・SHA-256 [FIPS PUB 180-2]

・SHA-384 [FIPS PUB 180-2]

・SHA-512 [FIPS PUB 180-2]

アプリケーションは「(128 + k * 8) bit ≤ blocksize of the used hash function, with [k=0,1,2,...]」を満たす秘密鍵を提供しなければならない。TOEはより小さいサイズの鍵もサポートしているが、それらの鍵を本TOEが主張する「SOF-High」の環境で使用することは適切ではない。

c) Digital Signature related functionality

TOEは以下の電子署名スキームに従い電子署名の生成・検証を実施する。

・RSA with SHA-1, SHA-256, SHA-384, SHA-512 or RIPEMD-160 according to [PKCS#1v1.5], with key lengths of 1024 + k * 64 [k=0,1,2,...] bit. The maximum key size is 8192 bit.

・RSA-PSS with SHA-1, SHA-256, SHA-384, SHA-512 or RIPEMD-160 according to [PKCS#1v2.1], with key lengths of 1024 + k * 64 [k=0,1,2,...] bit. The maximum key size is 8192 bit.

TOEはより小さいサイズの鍵もサポートしているが、それらの鍵を本TOEが主張する「SOF-High」の環境で使用することは適切ではない。

d) Encryption functionality

TOEは以下のブロック暗号を実装する。

・AES 128, 192, 256 bit [FIPS PUB 197]

・Triple-DES 112, 168 bit [FIPS 46-3]

・RC2 128-1024 bit [RFC 2268]

これらのブロック暗号は、以下の操作モードで使用できる。

・ECB

・CBC

・OFB

・CFB

AESにおいては上記に加えCTRもサポートする。

TOEは以下のストリーム暗号を実装する。

・ARCFOUR 128 – 2048 bit according to [IETF-Draft-Kaukonen]. This algorithm

is assumed to be compatible with RC4TM from RSA Security Inc.

TOEは以下の非対称暗号を実装する。
・RSA 1024 + k * 64 [k=0,1,2,...] bit according to [PKCS#1v1.5]. The maximum key size is 8192 bit.
・RSA-OAEP 1024 + k * 64 [k=0,1,2,...] bit according to [PKCS#1v2.1]. The maximum key size is 8192 bit.

TOEはより小さいサイズの鍵もサポートしているが、それらの鍵を本TOEが主張する「SOF-High」の環境で使用することは適切ではない。

e) Random Number Generator related functionality
TOEは以下の何れかのハッシュ関数に基づき2つの乱数生成方法を実装する。
・SHA-1 [FIPS PUB 180-1]
・Ripemd-160 [ISO/IEC 10118-3]
・SHA-256 [FIPS PUB 180-2]
・SHA-384 [FIPS PUB 180-2]
・SHA-512 [FIPS PUB 180-2]
乱数生成の際には適切なエントロピーを有するseedにより初期化されなければならない。

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「IAIK-JCE CC Core Security Target」（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B、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、「EVALUATION TECHNICAL REPORT (ETR)」（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19年6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、EAL3適合である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-High”を主張する。

本TOEのセキュリティ対策方針においては安全な暗号化機能を提供することを目的としており、従って本TOEはSOF-Highを主張する必要がある。

1.5.4 セキュリティ機能

本TOEにより提供される機能は全てセキュリティ機能であり、「1.2.4 TOEの機能」に示されている通りである。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.SignatureForgery	S.Attacker could forge O.Signature or recover O.PrivateKey from O.Signature.
T.DeduceData	S.Attacker could deduce O.Data from O.CipherText.
T.DeduceKey	S.Attacker could deduce O.SecretKey from O.CipherText.
T.DeduceRandomSeed	S.Attacker could deduce O.RandomSeed.
T.PredictRandomNumber	S.Attacker could predict the next generated O.RandomNumber.
T.MACForgery	S.Attacker could forge O.MAC or recover O.SecretKey.
T.HashForgery	S.Attacker could find collisions to O.Hash.

上記表1-1のSubject（S.Attacker等）、Object（O.Signature等）の定義は以下を参照の事。

表1-2① Subjectの定義

Subject	Definition
S.Admin	User who is in charge to perform the **TOE** installation and **TOE** configuration.
S.Developer	User who is in charge to use the **TOE** for developing his Application (S.Application).
S.Application	The surrounding application which is using the **TOE**.
S.JavaVM	Java™ Virtual Machine.
S.Attacker	A human or a process outside the **TOE** whose main goal is to access Application sensitive information. For functions with SOF-high claim the attacker has a high attack potential and no time limit. For all other functions the **TOE** has no obvious vulnerabilities that are exploitable by attackers possessing low attack potential.

表1-3② Objectの定義

Object	Definition
O.Data	Private data obtained from the S.Application (e.g. Data to be signed).
O.MAC	MAC generated by the **TOE**.
O.Hash	Hash generated by the **TOE**.
O.Signature	Signature generated by the **TOE**.
O.CipherText	The cipher text generated by the **TOE**.
O.PrivateKey	Private Key Data which the **TOE** uses to generate O.Signature (e.g. RSA Private key).
O.SecretKey	Secret Key Data which the **TOE** uses to encrypt O.Data and/or decrypt O.CipherText (e.g. AES key).
O.RandomSeed	The seed (initial state) used by the DRNG
O.RandomNumber	The random number generated by the **TOE**

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は存在しない。

1.5.7 構成条件

本TOEは以下の環境で動作する。

- JVM Specification 1.0.2 with the Java Platform 1.1 API and JCE 1.2.x
- JVM Specification 1.2 with one of the following APIs:
  - o J2SE 5.0
  - o J2SE 1.4.x
  - o J2SE 1.3.x and JCE 1.2.x
  - o J2SE 1.2.x and JCE 1.2.x

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1-3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.Protection	The TOE and its environment are protected in such a way that it is impossible for S.Attacker to read or modify any

	data managed by the TOE, i.e. objects defined in chapter 3.4.2.
A.Train	Administrators (S.Admin) are assumed to be suitably qualified to set up the system and to verify the TOE integrity.
A.Manual	S.Developer uses the TOE in the right way as described in the manual. In order to reach SOF high, the S.Developer must use the key sizes recommend in the manual.
A.SeedManagement	The IT-Environment must provide a suitable seed for the RandomNumberGenerator. Furthermore it must ensure that the seed is kept secret.
A.KeyManagement	The IT-Environment is responsible for key management. Key management is out of scope of the TOE. O.PrivateKey and O.SecretKey, needed for computation of O.CipherText, O.MAC and O.Signature, must be provided by S.Application. The TOE does not generate or destruct keys. Given key material won't be modified or stored by the TOE.
A.Java_Spec	The S.Admin or S.Developer has to install a Java™ VM that works according the JVM Specification V 1.0.2 [JVMSpec1] with the API of Java™ 1.1 [JavaAPI1.1] or JVM 1.2 [JVMSpec2] with one of the following APIs: • J2SE 5.x [JavaAPI5] • J2SE 1.4.x [JavaAPI1.4] • J2SE 1.3.x [JavaAPI1.3] • J2SE 1.2.x [JavaAPI1.2]
A.JCE_Spec	If the Java™ API in use is older than version 1.4 [JavaAPI1.4] (1.1.x [JavaAPI1.1], 1.2.x [JavaAPI1.2] or 1.3.x [JavaAPI1.3]) the S.Admin/S.Developer has to install a JCE framework that works according to the JCE 1.2 [JCE1.2-REF], JCE 1.2.1 [JCE1.2.1-REF] or JCE 1.2.2 [JCE1.2.2-REF] specification.

上記表1-4のSubject（S.Attacker等）、Object（O.PrivateKey等）の定義は「1.5.5 脅威」の表1-1①、表1-1②を参照の事。

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。

（1）HTML guidance documentation included in the ZIP file iaikjce315cc.zip.

（2）API documentation included in the ZIP file iaikjce315cc.zip.

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9月に始まり、平成19年6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19年2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・ライフサイクル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19年1月及び2月に評価者・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検出されなかったため、所見報告書は発行されていない。

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以下に示す。

·SUN JRE 1.1.8_010 serves as Java version 1.1.8,

·SUN JRE 1.2.2_017 serves as Java version 1.2.2,

·SUN JRE 1.3.1_19 serves as Java version 1.3.1,

・SUN JRE 1.4.0_04 serves as Java version 1.4.0,

・SUN JRE 1.4.1_06 serves as Java version 1.4.1,

・SUN JRE 1.4.2_12 serves as Java version 1.4.2,

・SUN JRE 1.5.0_09 (32-bit) serves as Java version 1.5.0

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は上記1）開発者テスト環境に示されたとおりである。開発者テストは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。

b.テスト手法

テストには、以下の手法が使用された。

①Type1:Known-answer-tests

乱数生成以外においては、NIST等により提供されているtest vectorや開発者独自に作成したtest vector(その正当性はthird party製品を使用し検証）を使用・拡張（暗号操作モード等のパラメタの変更や鍵長（最大・最小を含む）の変更）し、TOEを検証する。乱数生成に関しては [AIS20]等に示されているtest suiteに従いテストを実施し、TOEを検証する。

②Type2:API tests

TOEが、JCA/JCEのAPI仕様に示されている通りに振舞うことを検証する。

c.実施テストの範囲

テストは開発者によって56項目実施されている。

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。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステム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。

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の構成は、開発者テストと同様の構成である。

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は、開発者テストにおける構成と同一である。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。

b.テスト手法

テストには、以下の手法が使用された。

①Augmentation of developer testing for the TSF

評価者独自に開発者とは内容・サイズが異なるtest vectorを生成し、TOEを検証する。

②Supplementation of developer testing strategy

開発者が実施していないテスト（ストレステスト等）を評価者独自に考案し、TOEを検証する。

c.実施テストの範囲

評価者が独自に考案したテストを24項目、開発者テストのサンプリングによるテストをcode coverage と[AIS20]テストを除く全てのテスト項目を実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストからは時間的な制約から実行できないテスト以外の全てのテストを実施

② 開発者とは異なるtest vectorを使用し独立テストを実施

③ ストレステスト等開発者と異なる観点での追加テストを実施

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 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。

② 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。

③ 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、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EAL3保証要件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識別、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。

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。
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。
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、STに定義された拡張機能要件が曖昧なく定義されてい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、STに定義された拡張機能要件の依存性が全て識別されてい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。
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.3.1E	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。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んで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。
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.2.1E	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.2.2E	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。

ライフサイクルサポート	適切な評価が実施された
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	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かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.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上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであ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_MSU.1.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされてい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、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しい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。

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

6 参照

[1] IAIK-JCE CC Core Security Target Version 1.8 16 March 2007

[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] EVALUATION TECHNICAL REPORT (ETR) Version 3 2007年06月25日

[AIS20] Application Notes and Interpretation of the Scheme (AIS) AIS 20, Version 1, Date: 2 December,1999, Status: Mandatory, Subject: Functionality classes and evaluation methodology for, deterministic random number generators, Publisher: Certification body of the BSI, Section II 2, as part of the certification scheme

[FIPS 46-3] U.S. Department Of Commerce, Federal Information Processing Standards Publication: Data Encryption Standard (DES), FIPS PUB 46-3, U.S. Department Of Commerce, 199925 October 251999
(http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf).
[FIPS PUB 180-1] U.S. Department Of Commerce, Federal Information Processing Standards Publication: Secure Hash Standard, FIPS PUB 180-1, U.S. Department Of Commerce, 171995 April 1995 17
(http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).
[FIPS PUB 180-2] U.S. Department Of Commerce, Federal Information Processing Standards Publication: Secure Hash Standard, FIPS PUB 180-2, U.S. Department Of Commerce, 262001 November 2001 26
(http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf).
[FIPS PUB 197] U.S. Department Of Commerce, Federal Information Processing Standards Publication: Advanced Encryption Standard, FIPS PUB 197, U.S. Department Of Commerce, 26 November 2001
(http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf).
[IETF-Draft-Kaukonen] K.Kaukonen, R.Thayer: A Stream Cipher Encryption Algorithm "Arcfour", IETF draft (Internet Draft: draft-kaukonen-cipher-arcfour-03.txt), 14 July 1999.
[ISO/IEC 10118-3]
ISO/IEC 10118-3:2003, Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions, ISO/IEC, JTC 1/SC27, 14 November 2003.
[JavaAPI1.1] Java™ Platform 1.1 Core API Specification, SUN Microsystems, Inc., Palo Alto, California, 1995-1999, (http://java.sun.com/products/archive/jdk/1.1/index.html)
[JavaAPI1.2] Java™ 2 Platform, Standard Edition, v1.2.2 API Specification, SUN Microsystems, Inc., 1999, (http://java.sun.com/products/jdk/1.2/docs/api/index.html)
[JavaAPI1.3] Java™ 2 Platform, Standard Edition, v 1.3.1 API Specification, SUN Microsystems, Inc., 2001, (http://java.sun.com/j2se/1.3/docs/api/index.html)
[JavaAPI1.4] Java™ 2 Platform, Standard Edition, v 1.4.2 API Specification, SUN Microsystems, Inc., 2003, (http://java.sun.com/j2se/1.4.2/docs/api/)
[JavaAPI5] Java™ 2 Platform, Standard Edition, v 5.0 API Specification, SUN Microsystems, Inc., 2004, (http://java.sun.com/j2se/1.5.0/docs/api/)
[JCE1.2-REF] Java™ Cryptography Extension (JCE) API Specification & Reference, version 1.2, SUN Microsystems, Inc. (http://java.sun.com/products/jce/).
[JCE1.2.1-REF] Java™ Cryptography Extension (JCE) API Specification & Reference, version 1.2.1, SUN Microsystems, Inc. (http://java.sun.com/products/jce/).
[JCE1.2.2-REF] Java™ Cryptography Extension (JCE) API Specification & Reference, version 1.2.2, SUN Microsystems, Inc. (http://java.sun.com/products/jce/).
[JVMSpec1] Tim Lindholm, Frank Yellin: Tim Lindholm, Frank Yellin: The JavaTM

Virtual Machine Specification, Addison-Wesley Pub Co, September 1996, ASIN: 020163452X (http://java.sun.com/docs/books/vmspec/index.html).

[JVMSpec2] Tim Lindholm, Frank Yellin: Tim Lindholm, Frank Yellin: The JavaTM Virtual Machine Specification (2nd Edition), Addison-Wesley Pub Co, 2nd edition, April 1999, ISBN: 0201432943 (http://java.sun.com/docs/books/vmspec/index.html).

[PKCS#1v1.5] PKCS#1 v1.5: RSA Encryption Standard RSA Laboratories; 1 November 1, 1993 (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/).

[PKCS#1v2.1] PKCS#1 v2.1: RSA Cryptography Standard RSA Laboratories; June 14, 2002 (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/).

[RFC 2268] R. Rivest: A Description of the RC2(r) Encryption Algorithm, Network Working Group, March 1998 (http://www.ietf.org/rfc/rfc2268.txt).