



# JISEC

## 保証継続報告書

### 変更TOE

申請受付年月日（受付番号）	平成16年11月5日（IT継続4001）
認証番号	C0006
申請者	シャープ株式会社
TOEの名称	AR-FR10データセキュリティキット
TOEのバージョン	Version S.11
適合する保証要件	EAL3+ADV_SPM.1
TOE開発者	シャープ株式会社

上記の変更TOEについて、以下のとおり保証継続の結果を報告します。

平成16年11月17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 田淵 治樹

評価基準等：「ITセキュリティ認証申請者・登録者に対する要求事項」で定める下記の規格、及び「ITセキュリティ認証に係る保証継続の要件」に基づき、変更TOEに対して保証継続の検証がされた。

Common Criteria for Information Technology Security Evaluation Version 2.1  
Common Methodology for Information Technology Security Evaluation Version 1.0  
CCIMB Interpretations-0210

### 認証結果：合格

「AR-FR10データセキュリティキット Version S.11」（変更TOE）は、独立行政法人 情報処理推進機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、定められた規格に基づいて検証した結果、継続TOEとして、保証が継続されることを確認した。

## 目次

---

1	全体要約	1
1.1	はじめに	1
1.2	保証継続識別	1
1.2.1	変更TOE識別	1
1.2.2	認証TOE識別	1
1.2.3	認証TOEのST識別	2
1.2.4	認証TOEの認証報告書識別	2
1.3	保証継続の認証	2
1.4	報告概要	2
1.4.1	変更の記述	2
1.4.2	影響する開発者証拠	4
1.4.3	変更された開発者証拠	5
1.4.4	変更TOE添付ドキュメント	6
2	認証機関による保証継続実施及び結果	7
2.1	実施概要	7
2.2	認証実施	7
3	結論	8
3.1	認証結果	8
3.1.1	各変更による保証への影響	8
3.1.2	テスト	10
3.1.3	全体への影響	10
3.2	注意事項	10
4	用語	11
5	参照	13

# 1 全体要約

## 1.1 はじめに

この保証継続報告書は、認証済みのTOE「AR-FR10データセキュリティキット Version S.10」（以下「認証TOE」という。）を変更した「AR-FR10データセキュリティキット Version S.11」（以下「変更TOE」という。）の保証継続について、認証結果を申請者であるシャープ株式会社に報告するものである。

本保証継続報告書の読者は、本書と共に、対応する認証報告書、認証TOEのST[23]および変更TOEに添付されるマニュアル（詳細は「1.4.4 変更TOE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、認証TOEの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変更TOEに添付されるドキュメントに詳述されている。

本保証継続報告書は、変更TOEに対して、認証TOEと同じ保証レベルを与える保証継続についての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。

## 1.2 保証継続識別

### 1.2.1 変更TOE識別

本保証継続の対象とする変更TOEは以下である。

名称: AR-FR10データセキュリティキット  
バージョン: Version S.11  
開発者: シャープ株式会社

### 1.2.2 認証TOE識別

本保証継続の認証TOEは以下のとおりである

認証番号: C0006

名称: AR-FR10データセキュリティキット  
バージョン: Version S.10  
開発者: シャープ株式会社  
EAL: EAL3+ ADV\_SPM.1

### 1.2.3 認証TOEのST識別

本保証継続の認証TOEのSTは以下のとおりである

名称: デジタル複合機データセキュリティキットAR-FR10セキュリティター  
ゲット

バージョン: 0.21

作成者: シャープ株式会社

作成日: 2004年2月20日

### 1.2.4 認証TOEの認証報告書識別

本保証継続の認証TOEの認証報告書は以下のとおりである

TOEの名称: デジタル複合機データセキュリティキットAR-FR10 Version S.10

受付番号: IT認証4019

作成日: 2004年3月15日

作成者: 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

## 1.3 保証継続の認証

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」[1]、「ITセキュリティ認証申請等の手引き」[2]、「ITセキュリティ認証申請者・登録者に対する要求事項」[3]、「ITセキュリティ認証に係る保証継続の要件」[4]に規定された内容に従い、認証機関は、開発者が作成した「影響分析報告書」[5](以下「IAR」という。)を検証し、変更TOEに対し保証が継続されることを確認した。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。認証機関が指摘した問題点は、すべて解決された。認証機関はIARに基づき本保証継続報告書を作成し、認証作業を終了した。

## 1.4 報告概要

### 1.4.1 変更の記述

#### 1) 認証TOEに対する変更

##### a) 目的

デジタル複合機データセキュリティキットAR-FR10 Version S.11は、Version S.10に対し、動作状態復帰遅延時間の許容範囲を超えるハードディスク利用、鉛フリー半田に対応したIDE制御LSI利用を可能にすることを目的とする。

## b)変更内容

動作状態復帰遅延時間の許容範囲を超えるハードディスク利用、及び鉛フリー半田に対応したIDE制御LSI利用を可能とするため、必要となった変更内容を記述する。

- ・ TOE

TOEの構成要素であるソースコードの変更を行った。ソースコードへの変更内容は以下の2点。

- ハードディスク制御方法の変更

認証TOEの動作環境であるIDE制御LSI、及び鉛フリー半田に対応した新たなIDE制御LSI対応のため、IDE制御LSIの識別と新たなIDE制御LSI制御コードの追加

- ・ ガイダンス文書

取扱説明書データセキュリティキットAR-FR10及びAR-FR10設置手順書について、TOE版番号記述の変更

以下、変更TOEについて記述する。

認証TOEは、動作状態復帰遅延時間について、認証TOEの動作環境となっているハードディスクに特化したものである。このためハードディスクを変更する場合、動作状態復帰遅延時間が許容される範囲外であれば、TOEとして正常動作が保証されない。変更TOEは、この動作状態復帰遅延時間に係る制約を撤廃し、休止状態から動作状態に復帰した後、ハードディスクへの書き込み動作を開始するまでに要する時間が許容範囲を超えてもTOEとして正常動作を保証することを目的としたものである。(認証TOEにおける動作状態復帰遅延時間の許容範囲を超えるものを、以下「レスポンスの遅いハードディスク」という)

また、地球環境への配慮から、TOEを搭載するMFDのコントロール基板は、鉛フリー半田による電気・電子部品を実装することとなった。鉛フリー半田は融点が高く、認証TOEの動作環境としているIDE制御LSIは、鉛フリー半田の融点温度に対応できない。変更TOEは、鉛フリー半田の融点温度に対応した新たなIDE制御LSIを利用することも目的としている。鉛フリー半田対応のIDE制御LSIは、認証TOEの動作環境であるIDE制御LSIに比して、レジスタ構成、IDE制御LSIへ発行するコマンドが異なり、変更TOEはこのレジスタ構成、コマンドに対応可能なようにソースコードを追加したものである。

以上のように、変更TOEは、レスポンスの遅いハードディスク及び複数のIDE制御LSIの利用を可能とするためのソースコードの追加及び変更を実施したものであり、新たなセキュリティ機能や新たなMFDとしての機能を追加したのではない。

デジタル複合機データセキュリティキットAR-FR10セキュリティターゲット Version 0.21では、IDE制御LSIの存在を明示していないが、ハードディスクと同じくTOEの物理的、論理的範囲外にある。変更TOEは、ハードディスクに対する

書き込み、読み込み等の動作を実施するが、この動作はIDE制御LSIを制御することで実施され、変更TOEからみえるインタフェースは、認証TOEと同一となる。また、変更TOEを搭載したMFDは認証TOEを搭載したMFDと同一の動作をする。これは変更TOEのセキュリティ機能インタフェース（外部TSFI）が、認証TOEと同一であることを示すものである。このため保証パッケージEAL3が要求するADV\_FSP.1（非形式的機能仕様）に対し、影響を及ぼさない。

レスポンスの遅いハードディスク利用と複数のIDE制御LSI利用は、IDE制御LSIを制御しているサブシステムを構成するソースの変更だけで実施可能であり、IDE制御LSIを制御しているサブシステムのインタフェースの変更を必要としない。このため保証パッケージEAL3が要求するADV\_HLD.2（セキュリティ実施上位レベル設計）についても、影響を及ぼさない。

## 2) 認証TOEの開発環境に対する変更

開発環境に対する変更はない。

### 1.4.2 影響する開発者証拠

認証TOEの変更により、影響される開発者証拠を表 1-1に示す。

表 1-1 影響する開発者証拠

保証 コンポーネント	保証手段		開発者証拠への 影響
	証拠名称	バージョン	
ASE_INT.1	・ デジタル複合機データセキュリティキット AR-FR10セキュリティターゲット	0.21	・ 影響あり
ASE_DES.1			
ASE_ENV.1			
ASE_OBJ.1			
ASE_REQ.1			
ASE_SRE.1			
ASE_TSS.1			
ASE_PPC.1			
ACM_CAP.3	・ デジタル複合機データセキュリティキット AR-FR10構成管理説明書	0.05	・ 構成管理証拠資料 (TOEの 構成要素のリスト) について 影響あり
	・ デジタル複合機データセキュリティキット AR-FR10 Version S.10構成リスト	0.23	
ACM_SCP.1	・ デジタル複合機データセキュリティキット AR-FR10構成管理範囲説明書	0.04	・ 影響あり
ADO_DEL.1	・ デジタル複合機データセキュリティキット AR-FR10配付手順説明書	0.04	・ 影響なし
ADO_IGS.1	・ デジタル複合機データセキュリティキット AR-FR10配付手順説明書	0.07	・ 影響なし
	・ AR-FR10設置手順書	TCADZ1614 FCZZ	・ 影響あり
ADV_FSP.1	・ デジタル複合機データセキュリティキット AR-FR10セキュリティ機能仕様書	0.07	・ 影響なし
ADV_HLD.2	・ デジタル複合機データセキュリティキット AR-FR10上位レベル設計書	0.09	・ 影響なし

保証 コンポーネント	保証手段		開発者証拠への 影響
	証拠名称	バージョン	
ADV_RCR.1	・ デジタル複合機データセキュリティキット AR-FR10表現対応分析書	0.07	・ 影響なし
ADV_SPM.1	・ デジタル複合機データセキュリティキット AR-FR10セキュリティ方針モデル仕様書	0.04	・ 影響なし
AGD_ADM.1	・ 取扱説明書データセキュリティキット AR-FR10	CINSJ2569 FC51	・ 影響あり
	・ 取扱説明書デジタル複合機 キーオペレータープログラム編	0.03	・ 影響なし
	・ 取扱説明書デジタル複合機 共通編 / コピー編	0.03	・ 影響なし
	・ 取扱説明書デジタル複合機ファクス編	0.03	・ 影響なし
AGD_USR.1	・ 取扱説明書デジタル複合機 共通編 / コピー編	0.03	・ 影響なし
	・ 取扱説明書デジタル複合機ファクス編	0.03	・ 影響なし
ALC_DVS.1	・ デジタル複合機データセキュリティキット AR-FR10開発セキュリティ仕様書	0.03	・ 影響なし
ATE_COV.2	・ デジタル複合機データセキュリティキット AR-FR10カバレッジ分析書	0.04	・ 影響なし
ATE_DPT.1	・ デジタル複合機データセキュリティキット AR-FR10上位レベル設計テスト分析書	0.03	・ 影響なし
ATE_FUN.1	・ デジタル複合機データセキュリティキット AR-FR10機能テスト仕様書	0.03	・ 影響あり
ATE_IND.2	・ デジタル複合機データセキュリティキット AR-FR10独立テスト環境・ツール説明書 (評価者作成)	0.02	・ 評価者作成のため対象外
AVA_MSU.1	・ 取扱説明書データセキュリティキット AR-FR10	CINSJ2569 FC51	・ 影響あり
	・ 取扱説明書デジタル複合機 キーオペレータープログラム編	0.03	・ 影響なし
	・ 取扱説明書デジタル複合機 共通編 / コピー編	0.03	・ 影響なし
	・ 取扱説明書デジタル複合機ファクス編	0.03	・ 影響なし
AVA_SOF.1	・ デジタル複合機データセキュリティキット AR-FR10セキュリティ機能強度分析書	0.06	・ 影響なし
AVA_VLA.1	・ デジタル複合機データセキュリティキット AR-FR10脆弱性分析書	0.04	・ 影響あり

### 1.4.3 変更された開発者証拠

表 1-2に変更された開発者証拠を示す。

表 1-2 変更された開発者証拠

証拠資料名	バージョン	発効日
デジタル複合機データセキュリティキット AR-FR10セキュリティターゲット	0.22	2004年9月6日
デジタル複合機データセキュリティキット AR-FR10 Version S.11構成リスト	0.09	2004年8月19日
デジタル複合機データセキュリティキット AR-FR10 構成管理範囲説明書	0.05	2004年8月19日

セキュリティ機能実施ソース (MAIN部)	0.03	2004年8月19日
セキュリティ機能実施ソース (BSP部)	0.03	2004年8月19日
AR-FR10 設置手順書	TCADZ1614FCZ1	2004年10月26日
取扱説明書データセキュリティキット AR-FR10	CINSJ2569FC52	2004年10月26日
デジタル複合機データセキュリティキット AR-FR10 機能テスト仕様書	0.04	2004年8月19日
デジタル複合機データセキュリティキット AR-FR10 脆弱性分析書	0.05	2004年9月24日

#### 1.4.4 変更TOE添付ドキュメント

変更TOEに添付されるドキュメントを以下に示す。

1) 取扱説明書 データセキュリティキット AR-FR10

バージョン : CINSJ2569FC52

対象者 : キーオペレータ

内容 : 本TOEを利用するガイドとして提供され、TOEのセキュアな管理運用に必要な事項が述べられている

2) AR-FR10 設置手順書

バージョン : TCADZ1614FCZ1

対象者 : キーオペレータ、サービスマン

内容 : 本TOEの設置に伴い、サービスマン及びキーオペレータが行うべきTOEのセキュアな管理・運用に必要な事項が述べられている



## 2 認証機関による保証継続実施及び結果

### 2.1 実施概要

保証継続は、平成16年8月に開始し、平成16年11月にIARの完成をもって完了した。認証機関は、開発者から保証継続に要するIARの提供を受け、変更TOEに対する影響を調査した。

また、調査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開発者へ渡された。これらは開発者による検討ののち、IARに反映されている。

### 2.2 認証実施

認証の過程で開発者より提出されるIARについて以下の検証を実施した。

認証TOEに対する変更について、正しく記述されていること。

変更によって、変更する開発者証拠は妥当であること。

開発者証拠の変更が、変更TOEに対する影響分析の結果について、開発者の判断の根拠が妥当であること。

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、開発者に送付した。

認証機関は、IAR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。

### 3 結論

#### 3.1 認証結果

提出されたIARを検証した結果、認証機関は、認証TOEに対する変更が本変更TOEにおいても認証TOEのEAL3+ADV\_SPM.1保証要件を満たしており、変更TOEに対する保証への影響が無いことを確認した。

##### 3.1.1 各変更による保証への影響

変更TOEの保証要件に対する影響について、検証結果を表3-1にまとめる。

表3-1 保証継続の検証結果

保証要件	検証結果
<b>セキュリティターゲット</b>	<b>影響が無いことを確認した。</b>
ASE_DES	認証TOEに対する変更は、TOE識別情報のみの変更であり、変更TOEの評価に影響が無いことを確認した。
ASE_ENV	
ASE_INT	
ASE_OBJ	
ASE_PPC	
ASE_REQ	
ASE_SRE	
ASE_TSS.	
<b>構成管理</b>	
ACM_CAP.3	構成リストは、TOEバージョンアップによる変更が必要となった開発者証拠の版数の変更のみであり、変更TOEの評価に影響が無いことを確認した。
ACM_SCP.1	ソースファイルのバージョンの版数変更のみであり、変更TOEの評価に影響が無いことを確認した。
<b>配付と運用</b>	<b>影響が無いことを確認した。</b>
ADO_DEL.1	開発者証拠資料に変更が無いことを確認した。
ADO_IGS.1	認証TOEのバージョンアップによる、TOE識別情報の変更のみであり、変更TOEの評価に影響が無いことを確認した。

<b>開発</b>	<b>影響が無いことを確認した。</b>
ADV_FSP.1	開発者証拠資料に変更が無いことを確認した。
ADV_HLD.2	開発者証拠資料に変更が無いことを確認した。
ADV_RCR.1	開発者証拠資料に変更が無いことを確認した。
ADV_FSP.1	開発者証拠資料に変更が無いことを確認した。
<b>ガイダンス文書</b>	<b>影響が無いことを確認した。</b>
AGD_ADM.1	管理者ガイダンスで識別しているTOE識別情報のみの変更であり、変更TOEの評価に影響が無いことを確認した。
AGD_USR.1	開発者証拠資料に変更が無いことを確認した。
<b>ライフサイクルサポート</b>	<b>影響が無いことを確認した。</b>
ALC_DVS.1	開発者証拠資料に変更が無いことを確認した。
<b>テスト</b>	<b>影響が無いことを確認した。</b>
ATE_COV.2	開発者証拠資料に変更が無いことを確認した。
ATE_DPT.1	開発者証拠資料に変更が無いことを確認した。
ATE_FUN.1	ハードディスクおよびIDE制御LSIの変更によるテスト構成の追加であり、インターフェースの変更が無いため、テスト実施項目は認証TOEと同一となる。そのため、変更TOEの評価に影響が無いことを確認した。
ATE_IND.1	認証TOEに対して実施した評価者テストで考慮したテスト項目と同一になり、実施したテスト結果についても同一となったため、変更TOEの評価に影響が無いことを確認した。
<b>脆弱性評価</b>	<b>影響が無いことを確認した。</b>
AVA_MSU.1	管理者ガイダンスで識別している、TOE識別情報のみの変更であり、変更TOEの評価に影響が無いことを確認した。
AVA_SOF.1	開発者証拠資料に変更が無いことを確認した。
AVA_VLA.1	認証TOEの脆弱性と同一となり、新たに明らかな脆弱性は無い。そのため、変更TOEの評価に影響が無いことを確認した。

### 3.1.2 テスト

認証TOEに対する変更において、レグレッションテストの実施により、変更TOEの動作に影響が無いことを確認した。

### 3.1.3 全体への影響

各変更による影響が無いことから、変更TOEの検証において全体への影響が無いことを確認した。

## 3.2 注意事項

特になし。

## 4 用語

本保証継続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
IAR	Impact Analysis Report
IDE	Integrated Drive Electronics

本報告書で使用された用語を以下に示す。

IAR	影響分析報告書
認証TOE	評価され認証書が発行されたTOEのバージョンのことをいう。
変更TOE	認証TOEに対して、変更が加えられた異なるバージョンをいう。
継続TOE	認証TOEに対して継続プロセスを経て以前の認証の適用が認められた変更TOEをいう。認証TOEに対して与えられた同じ保証が、継続TOEにも適用される。
IDE	Personal Computer用のハードディスクインターフェイスの1つであり、ANSI (American National Standards Institute、米国規格協会) にて認定され、X3T92グループで管理されている。
IDE制御LSI	IDEインタフェースのハードディスクドライブを制御するためのLSI (大規模集積回路)。デジタル複合機のコントローラ基板に搭載されており、TOEがIDE制御LSIを制御することにより、ハードディスクへの書き込み及び読み込み動作を実施する。
MFD	認証TOE及び変更TOEを搭載可能なシャープのデジタル複合機AR-555S、AR-625S、及びAR-705S。

動作状態復帰遅延時間 休止状態からリード/ライト等のコマンド発行による実動作が可能な動作状態に復帰するまでに要する時間。

## 5 参照

- [1] ITセキュリティ評価及び認証制度 平成16年4月 独立行政法人 情報処理推進機構 ITQM-24 (平成16年11月5日改定)
- [2] ITセキュリティ認証申請等の手引き 平成16年4月 独立行政法人 情報処理推進機構 ITQM-23 (平成16年11月5日改定)
- [3] ITセキュリティ認証申請者・登録者に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-08 (平成16年11月5日改定)
- [4] ITセキュリティ認証に係る保証継続の要件 平成16年11月5日 独立行政法人 情報処理推進機構 ITQM-31
- [5] SHARP デジタル複合機 データセキュリティキット AR-FR10 影響分析報告書 Version 0.09 2004年11月12日 シャープ株式会社
- [6] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031
- [7] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- [8] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
- [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1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031
- [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
- [11] 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
- [12] ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)
- [13] ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)
- [14] ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)
- [15] 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
- [16] 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
- [17] 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

- [18] Common Methodology for Information Technology Security Evaluation  
CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999
- [19] 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
- [20] 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
- [21] CCIMB Interpretations-0210
- [22] 補足-0210
- [23] デジタル複合機データセキュリティキット AR-FR10 セキュリティターゲット  
Version 0.21 平成16年2月20日 シャープ株式会社
- [24] デジタル複合機 データセキュリティキット AR-FR10 評価報告書 第1.4版 2004年  
2月27日 社団法人電子情報技術産業協会 ITセキュリティセンター