国際セキュリティ評価基準 ISO/IEC15408 EAL4 の取得

Validation of International Security System ISO/IEC15408 EAL4

岩 崎 章 彦*　　山 中 敏 弘*
Akihiko Iwasaki　　Toshihiro Yamanaka

要　旨

デジタル複合機内に残存するデジタルイメージデータから，情報漏洩を防止するデータセキュリティキットを他社に先駆けて商品化した。これらのうち，AR-FR4 及び AR-FR5 について，ISO/IEC15408 のセキュリティ評価基準に基づく評価を受け，評価保証レベル（Evaluation Assurance Level:）EAL 4 の認証を取得した。このセキュリティ評価基準，国内におけるセキュリティ認証制度，及び当社の対応について以下に概説する。

Sharp has been commercialized the Data Security Kit prior to the other company. This Data Security Kit prevents an information leak from the digital image data which remains in the digital multifunctional system. The AR-FR4 Data Security Kit and the AR-FR5 Data Security Kit obtained the certification of Common Criteria (Evaluation Assurance Level) EAL4 in response to the evaluation based on the security valuation basis of ISO/IEC15408. This paper outlines this security valuation basis, a domestic security certification system, and the response of our company.

まえがき

IT，ネットワークの技術の進展とともに，情報システム機器によって取り扱われるデジタルデータのセキュリティ性が問題となり，機器に対するセキュリティ評価が注目されている。

1980 年代，欧米各国では軍事上の観点からセキュリティ評価基準に関し様々な検討が行われ，各国毎にセキュリティ評価制度が存在していた。国際的な必要性から，1996 年 Common Criteria（CC）Version 1.0 と呼ばれるセキュリティ評価基準が誕生した。この評価基準に基づき評価された製品について，その評価結果を他国でも利用できるように国際的相互認証をするための枠組みが Common Criteria Recognition Arrangement（CCRA）である。1999年，Common Criteria Version 2.1 を ISO（International Standardization Organization）で IS（International Standard）化したものが，ISO/IEC15408 である。

日本では 2001 年，経済産業省の委託により，独立行政法人製品評価技術基盤機構（NITE）が IT セキュリティ評価・認証プログラム（JISEC: Japan Information Technology Security Evaluation and Certification Scheme）として，ISO/IEC15408 及び CC に基づくセキュリティ評価認証制度を運営していたが，2003 年 10 月，認証国として CCRA に加盟した[注]。これにより，国内でも CC 認証を取得できるようになった。2004 年 3 月現在，CCRA には 19ヵ国が加盟している。

注：2004 年 4 月より，認証機関としての役割は，独立行政法人製品評価技術基盤機構より，独立行政法人情報処理推進機構（IPA）に移管されている。

1．MFP/Printer のデータセキュリティキット AR-FR4/5 機能概要

デジタル複合機やプリンタでは，データの処理効率を高めるため，幾種類ものデータメモリが存在している。コピー，プリント，FAX，Scan のそれぞれのデータは，一旦，ページメモリの形で揮発性メモリ（DRAM 等），不揮発性メモリ（HDD，Flash メモリ等）に蓄えられる。コピー，プリント，FAX，Scan のそれぞれの処理が終了すると，データを蓄えていた領域は不要となり消去される。一般的には，この消去動作は実データ領域を消去するのではなく，データの管理領域を消去することにより実施されている。つまり，管理領域が消去されても，実データ領域は消去されない

* ドキュメントシステム事業本部　ドキュメントシステム事業部　第 6 技術部

ままの状態となっている。この実データ領域が存在している状態のまま不揮発性メモリが盗難に遭う，またデジタル複合機を廃棄するといった場合，実データから情報が漏洩する可能性がある。

当社が開発したデータセキュリティキットAR-FR4/5は以下のセキュリティ機能を持つ。

（1）コピー，プリント，FAX，Scanのそれぞれのデータは暗号化後，揮発性メモリ，不揮発性メモリに蓄える。この暗号化により，実データからの情報漏洩を不能としている。

（2）また，暗号化が万全ではないことから，Flashメモリについては，デバイスの特性上，実データ領域に値（0）を上書きすることにより消去し，DRAM，HDDのメモリに対しては，実データ領域をランダムなデータで上書きすることにより消去する。DRAM，HDDの上書きについては，上書き回数を1回から7回まで設定可能である。

2．ITセキュリティ評価及び認証制度

ITセキュリティ評価及び認証制度とは，独立行政法人製品評価技術基盤機構法（平成11年12月22日法律第204号）第11条第1項第2号（工業製品等に関する技術上の評価を行うこと）に基づき経済産業省の監督のもと，独立行政法人製品評価技術基盤機構がCCRA（コモンクライテリア承認アレンジメント）及び関連する国際基準に適合させたITセキュリティの評価及び認証を行う制度である。本制度は，認証プログラムの運営に関わる事項を審議する運営委員会，認証プログラムの技術に関わる事項を審議する技術委員会，認証の授与，資格付与等に関わる事項を審議する評定委員会で運営されている。

本制度のいう評価及び認証とは，**図1**に示すように，開発者（認証申請者）が開発したIT製品及びシステムについて，セキュリティ規格に基づいていることを第三者評価機関が評価し，その評価が本制度の定めに従って実施されたこと及び当該評価結果が正しいことを，認証プログラムが検証することである。

3．評価のためのドキュメントと評価保証レベル

ITセキュリティ評価及び認証制度に基づき，AR-FR4/5が取得した保証パッケージEAL4で必要としたドキュメントを**表1**に示す。なお，表中のTOEとは，評価対象（Target of Evaluation）のことである。

表1の評価項目に記載しているクラス，ファミリ，及びコンポーネントの関係について**図2**に示す。

クラスとは，“共通の対象を共有するファミリのグループ”のことであり，ファミリとは，“セキュリティ対策方針を共有するが，重点または厳密さが異なるコンポーネントのグループ”である。ファミリのメンバは，コンポーネントと呼ばれ，特定のセキュリティ要件の集合を表すもので，CCに定義されている構造に含めることができる最小の選択可能なセキュリティ要件セットである。ファミリ内のコンポーネントセットは，共通の目的を持つセキュリティ要件の強度，または能力の増加を表現するように順序付けされている。また，関連する非階層セットを表現するように部分的に順序付けされている。場合によっては，ファミリ内に1つのコンポーネントしか含まれていないこともあり，その場合には順序付けは適用されない。

評価機関に提出したドキュメントについて，Common Criteriaセキュリティ評価基準と対比させながら，

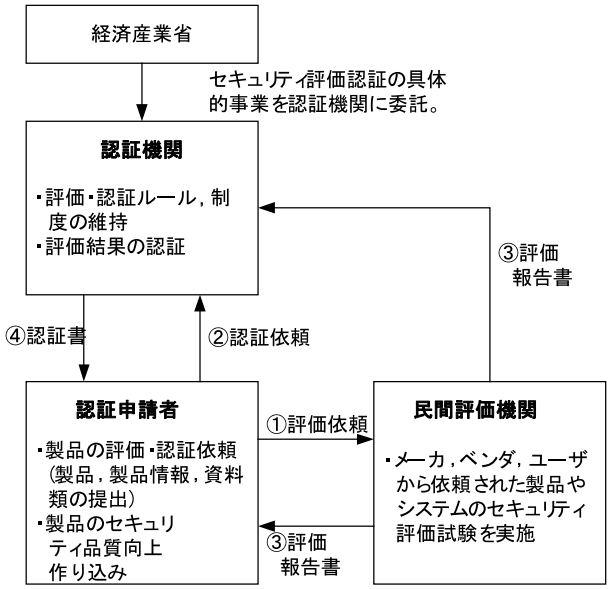

図1　評価・認証の手順
Fig. 1　Procedure of evaluation and certification.

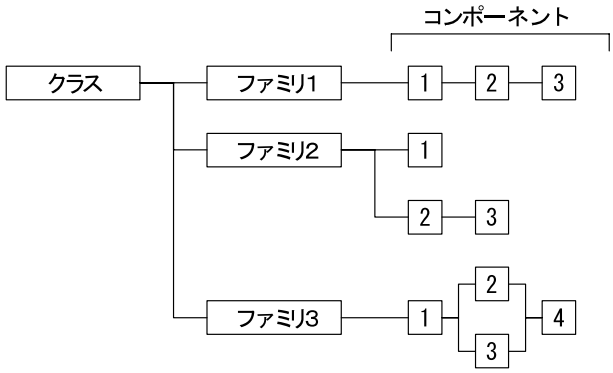

図2　クラスのコンポーネント構成
Fig. 2　Class decomposition diagram.

表 1　提供物件
Table 1　Evaluation document list.

評価項目		提供文書
クラス	ファミリ/コンポーネント	
ASE		デジタル複合機データセキュリティキット　セキュリティターゲット
ACM（構成管理）	AUT.1（部分的なCM自動化）	デジタル複合機データセキュリティキット　構成管理自動化ツール説明書
	CAP.4（生成の支援と受入手続き）	デジタル複合機データセキュリティキット　構成管理システム説明書
	SCP.2（問題追跡のCM 範囲）	デジタル複合機データセキュリティキット　CM範囲説明書
ADO（配付と運用）	DEL.2（改変の検出）	デジタル複合機データセキュリティキット　配付手順説明書
	IGS.1（設置,生成,及び立上げ手順）	デジタル複合機データセキュリティキット　設置手順適合確認資料
ADV（開発）	FSP.2（完全に定義された外部インタフェース）	デジタル複合機データセキュリティキット　セキュリティ機能仕様書
	HLD.2（セキュリティ実施上位レベル設計）	デジタル複合機データセキュリティキット　上位レベル設計書
	IMP.1（TSF の実装のサブセット）	デジタル複合機データセキュリティキット　ソースコード説明書
	LLD.1（記述的下位レベル設計）	デジタル複合機データセキュリティキット　下位レベル設計書
	RCR.1（非形式的対応の実証）	デジタル複合機データセキュリティキット　表現対応分析書
	SPM.1（非形式的なTOE セキュリティ方針モデル）	デジタル複合機データセキュリティキット　セキュリティ方針モデル仕様書
AGD（ガイダンス）	ADM.1（管理者ガイダンス）	デジタル複合機データセキュリティキット　ガイダンス文書クラス適合確認資料, 取扱説明書データセキュリティキットAR-FR4, AR-FR4 Data Security Kit Operation Manual, AR-FR5 Data Security Kit Operation Manual, 設置チェックリスト･取扱説明書追補版, Installation Checklist･Supplemental Sheet, レーザープリンタ 取扱説明書（共通編）, レーザープリンタ 取扱説明書（コピー編）, レーザープリンタ デジタル複合機取扱説明書（ネットワークスキャナ編）, レーザープリンタ デジタル複合機取扱説明書（ファクス編）, LASER PRINTER Operation manual (for printer operation and general information)
	USR.1（利用者ガイダンス）	
ALC（ライフサイクルサポート）	DVS.1（セキュリティ手段の識別）	デジタル複合機データセキュリティキット　開発セキュリティ仕様書
	LCD.1（開発者によるライフサイクルモデルの定義）	デジタル複合機データセキュリティキット　ライフサイクル管理手順書
	TAT.1（明確に定義された開発ツール）	デジタル複合機データセキュリティキット　開発ツール資料
ATE（テスト）	COV.2（カバレージの分析）	デジタル複合機データセキュリティキット　カバレージ分析書
	DPT.1（テスト:上位レベル設計）	デジタル複合機データセキュリティキット　上位レベル設計･テスト分析書
	FUN.1（機能テスト）	デジタル複合機データセキュリティキット　機能テスト仕様書
	IND.2（独立テスト-サンプル）	デジタル複合機データセキュリティキット　独立テスト環境･ツール説明書
AVA（脆弱性評定）	MSU.2（分析の確認）	デジタル複合機データセキュリティキット　TOEの誤使用分析説明書, 取扱説明書データセキュリティキットAR-FR4, AR-FR4 Data Security Kit Operation Manual, AR-FR5 Data Security Kit Operation Manual, 設置チェックリスト･取扱説明書追補版, Installation Checklist･Supplemental Sheet, レーザープリンタ 取扱説明書（共通編）, レーザープリンタ 取扱説明書（コピー編）, レーザープリンタ デジタル複合機取扱説明書（ネットワークスキャナ編）, レーザープリンタ デジタル複合機取扱説明書（ファクス編）, LASER PRINTER Operation manual (for printer operation and general information)
	SOF.1（TOE セキュリティ機能強度評価）	デジタル複合機データセキュリティキット　TOEセキュリティ機能強度評価
	VLA.2（独立脆弱性テスト）	デジタル複合機データセキュリティキット　脆弱性分析書

表 1 のドキュメントを解説する。

（1）セキュリティターゲット

Common Criteria で必要とするドキュメントは，トップダウンで作成しなければならない。この最上位に相当するものが，セキュリティターゲット（ST：Security Target）である。セキュリティターゲットは，TOEの開発設計書であり，セキュリティ脅威分析，装備すべき機能，品質対策などを記述したものである。

（2）構成管理クラス

構成管理は，TOE の実装において，機能要件と仕様が実装されることを確立する方法，手段である。TOEを構成する要素（ソースコード，取扱説明書，証拠書類等の評価機関に提供する全ての物件）について，統制と管理が実施されていることを保証することを目的としている。

（3）配付と運用クラス

開発サイトから利用者サイトまでの正しいTOE配付経路，及びTOE設置方法を保証することを目的としている。

（4）開発クラス

開発は，セキュリティ機能インタフェースから実装表現に至る種々の抽象レベルでのTSF（TOE Security Functions，TOEセキュリティ機能）を表現するTOE設計書である。

（5）ガイダンスクラス

利用者と管理者のガイダンス証拠資料（取扱説明書）に対し，TOEをセキュアに管理し使用するため，全ての側面が記述されていなければならない。

（6）ライフサイクルサポートクラス

ライフサイクルサポートは，TOEの開発及び保守中に，TOEを改良するプロセスに統制と管理を保証することを目的としている。

（7）テストクラス

テストクラスは，TSFがその仕様どおりに動作することの確認を目的としている。開発クラスとの対応を示す開発者分析，テストツール，テスト結果の提供も必要となる。

（8）脆弱性評定クラス

脆弱性評定クラスは，TOEの脆弱性を扱う。TOEの誤使用や設定誤りの可能性，確率的または順列的メカニズムが破られる可能性，悪用されうる隠れチャネルの存在に関し，開発者分析を行う。

4．今後の課題

図1に示す手続きによりISO/IEC15408，もしくはCommon Criteriaの認証取得が可能であるが，**表1**に示すドキュメント類は，一度で了承されることはなく，何度となく修正を必要とする。単に，ドキュメントの追加，修正だけであれば良いが，時には商品そのものの仕様を変更しなければならないこともある。このため認証取得スケジュールの確定は，非常に困難な状況となっている。AR-FR4/5については，仕様の変更こそなかったものの，作成着手から，認証取得完了まで約14ヶ月を要している。

このようなことから，いかに短期間でセキュリティ認証を取得するのか，ということが今後の課題となる。このためには，より的確なドキュメントを作成することによる評価機関及び認証機関からの指摘事項を最小限に止めるため，セキュリティ認証に関する開発者のレベルアップを行うことだけでなく，セキュリティ認証取得のための社内ルールの整備が必要となると考えている。

むすび

デジタル複合機のセキュリティ認証について概要を紹介した。“セキュリティ”をソリューションビジネス展開の柱として位置付け，今後開発する商品は全てセキュリティ機能を搭載する方針であり，セキュリティ認証についても取得する。また，デジタル複合機／プリンタのセキュリティ機能については，AR-FR4/5のような単純なものから，より複雑な機能のもの，またネットワーク機能を持つものへと拡大を行いながら取り組んでいく。

参考文献

1）情報処理推進機構，“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”，（オンライン），〈http://www.ipa.go.jp/security/jisec/evalbs.html〉（2004.6）.

2）情報処理推進機構，“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”，（オンライン），〈http://www.ipa.go.jp/security/jisec/evalbs.html〉（2004.6）.

3）情報処理推進機構，“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”，（オンライン），〈http://www.ipa.go.jp/security/jisec/evalbs.html〉（2004.6）.

4）情報処理推進機構，“ITセキュリティ評価及び認証セミナー 資料集”，（オンライン），〈http://www.ipa.go.jp/security/ccj/event/20030926/docs/papers.html〉（2004.6）.

（2004年6月1日受理）