



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



評価対象

申請受付年月日(受付番号)	平成18年7月24日 (IT認証6093)
認証番号	C0076
認証申請者	ミラクル・リナックス株式会社
TOEの名称	MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One オペレーティングシステム
TOEのバージョン	V4.0
PP適合	なし
適合する保証要件	EAL1
TOE開発者	ミラクル・リナックス株式会社
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19年1月24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セキュリティ評価機関に対する要求事項」で定める下記の規格に基づいて評価された。

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

評価結果：合格

「MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One オペレーティングシステム」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
1.1	はじめに	1
1.2	評価製品	1
1.2.1	製品名称	1
1.2.2	製品概要	1
1.2.3	TOEの範囲と動作概要	2
1.2.4	TOEの機能	3
1.3	評価の実施	5
1.4	評価の認証	6
1.5	報告概要	6
1.5.1	PP適合	6
1.5.2	EAL	6
1.5.3	セキュリティ機能強度	6
1.5.4	セキュリティ機能	6
1.5.5	脅威	7
1.5.6	組織のセキュリティ方針	7
1.5.7	構成条件	7
1.5.8	操作環境の前提条件	7
1.5.9	製品添付ドキュメント	8
2	評価機関による評価実施及び結果	9
2.1	評価方法	9
2.2	評価実施概要	9
2.3	製品テスト	9
2.3.1	開発者テスト	9
2.3.2	評価者テスト	9
2.4	評価結果	11
3	認証実施	11
4	結論	12
4.1	認証結果	12
4.2	注意事項	15
5	用語	16
6	参照	17

1 全体要約

1.1 はじめに

この認証報告書は、「MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One オペレーティングシステム」（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ミラクル・リナックス株式会社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。

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: MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One /
MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One
オペレーティングシステム

バージョン:V4.0

開発者: ミラクル・リナックス株式会社

1.2.2 製品概要

本TOEは、Linuxオペレーティングシステムの商用ディストリビューションMIRACLE LINUX V4.0、MIRACLE LINUX V4.0 One、MIRACLE LINUX V4.0 x86-64、MIRACLE LINUX V4.0 x86-64 Oneの各製品の共通部分であるマルチユーザ、マルチタスクのオペレーティングシステムであり、Intel x86プラットフォーム上で動作する。

本TOEは、管理する情報の不正アクセス、改竄、漏洩を防ぐために、個々の利用者を識別/認証する機能、識別/認証された利用者のオブジェクトへのアクセスを制限するアクセス制御機能、各プロセス間の分離を保証するプロセス分離機能、および利用者を識別/認証する際の監査証跡を記録する監査機能を提供する。

1.2.3 TOEの範囲と動作概要

評価対象となるTOEは、MIRACLE LINUX V4.0、MIRACLE LINUX V4.0 One、MIRACLE LINUX V4.0 x86-64、MIRACLE LINUX V4.0 x86-64 Oneの各製品の共通部分であるオペレーティングシステム部分であり、図 1-1の点線で示す範囲のソフトウェア群である。

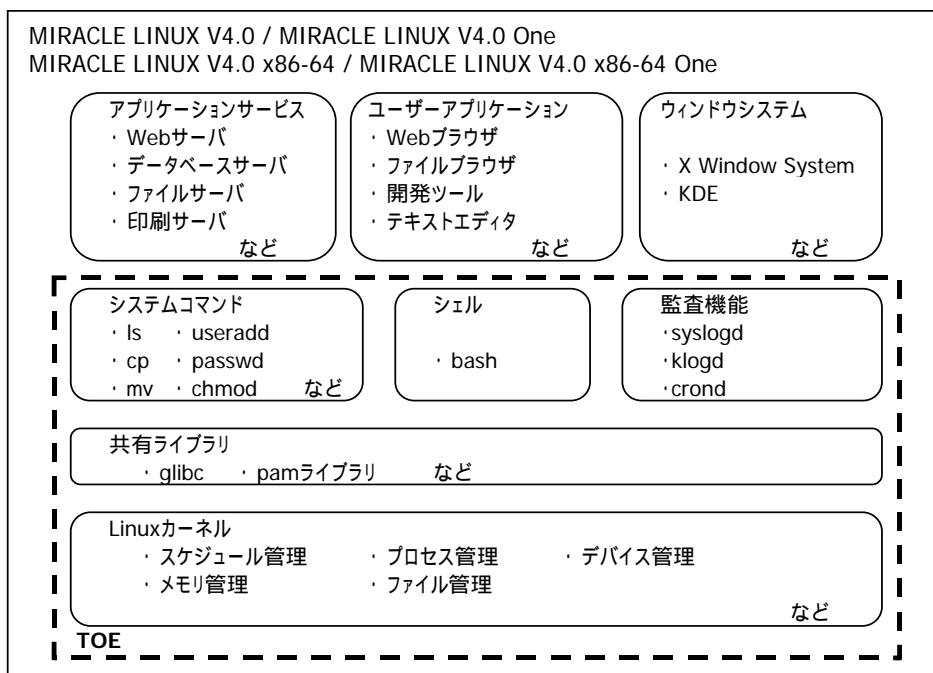


図 1-1 TOEの物理的範囲

TOEを構成するファイルとその動作概要は以下のとおり。

- Linuxカーネル

/boot下のvmlinuzで始まる名称のファイルが評価範囲に含まれる。

スケジュール管理、メモリ管理、プロセス管理、ファイル管理、デバイス管理、入出力制御などのオペレーティングシステム特有のサービスを提供する。
- 共有ライブラリ

最小インストール時の/lib、/usr/lib下のすべてのファイルが評価範囲に含まれる。

関数や定数の定義など部品化したソフトウェアの集合であり、単独のファイルとして実行される形式のプログラムとは異なる。各種アプリケーションプログラムが共通で利用する機能を提供する。
- システムコマンド

最小インストール時の/bin、/sbin、/usr/bin、/usr/sbin下のすべてのファイルが評価範囲に含まれる。

キャラクタユーザインタフェース上で利用されるコマンド群であり、MIRACLE LINUX V4.0、MIRACLE LINUX V4.0 One、MIRACLE LINUX V4.0 x86-64、

MIRACLE LINUX V4.0 x86-64 Oneの各製品を管理する上で必要となる基本機能を提供する。

- ・ シェル

製品に含まれる各種シェルのうちbashのみが評価範囲に含まれる。

利用者が対話的にシステムを操作するためのインタフェース及び機能を有し、システムコマンドを実行するためのプラットフォームを提供する。

- ・ 監査機能

監査機能の提供に関わるsyslogd、klogd、及びcrondが評価範囲に含まれる。

各利用者が識別/認証を試みた際に、その監査証跡を記録する。

1.2.4 TOEの機能

本TOEが提供する機能の概要は以下のとおり。

(1) Linuxカーネル

アプリケーションプログラムに命令セットを供給し、ハードウェアプラットフォームと対話する。このために、カーネルモードと呼ばれるプロセッサの特権モードで動作し、コンピュータのすべての資源へのフルアクセス権を持つ。

代表的なものとして、スケジュール管理、メモリ管理、プロセス管理、ファイル管理、デバイス管理、入出力管理の機能を提供する。

a) スケジュール管理

異なるタスクにCPU時間を割当てるためのスケジュールサービスを提供する。タスクにはユーザプロセスおよびカーネルプロセスの両方が含まれる。スケジュールサービスでは、プロセッサ時間の割当てを管理するだけでなく、カーネルタスクによる共有データへのアクセスが混乱しないことを保証するとともに、複数のプロセッサへのタスクの割当ても行う。

b) メモリ管理

物理メモリにページ、ページグループ、あるいは小さなブロックの割当てを行うために提供され、実行中のプロセスのアドレス空間のマッピングや仮想メモリの割当てを行う。仮想メモリシステムでは各プロセスから利用されるアドレス空間の管理を行う。

c) プロセス管理

プロセスとは独自の仮想アドレス空間で動作しているプログラムであり、動作中に新しいプロセスを作成したり新しいプログラムを既存のプロセス内で実行したりすることができる。

プロセス管理では、それぞれのプロセスに固有の識別子(関連するユーザ識別子(ユーザID)及び1つ以上のグループ識別子(グループID))を付与し、これらの識別子に基づいてオブジェクトにアクセスするためのプロセスの権限を決定する。また、プロセスが

新しいプロセスを作成した場合には、作成されたプロセスに元のプロセスの持っている識別子などの特性を継承させる。

さらに、シグナル及びセマフォによって実装されるプロセス間通信において、仮想メモリ空間やオブジェクトを共有している場合に内容の不整合や破壊を防ぐ機能も提供する。

d) ファイル管理

データストリームの入出力を扱うことができるものはすべてファイルとしてファイルシステムの下で管理する。このファイルには、一般的にファイルと呼ばれるオブジェクトに加えて、ディレクトリ、デバイスドライバおよびネットワーク接続などが含まれる。本TOEではext2やext3などの複数のファイルシステムを提供するが、それぞれは仮想ファイルシステム(VFS)をベースに詳細に実装されている。

e) デバイス管理

ハードウェア装置(デバイス)などを通常のファイルとして管理する。デバイスファイルには、次の3つの種別が存在する。

- ・ ブロックデバイス
独立した固定サイズブロックのデータへのランダムなアクセスが可能な装置
- ・ キャラクタデバイス
文字のストリームによってされる装置
- ・ ネットワークデバイス
ネットワーク通信をサポートするためにカーネルのネットワークサブシステムによって使用される物理デバイス及びソフトウェアデバイス

(2) 共有ライブラリ

他のプログラムにカーネルサービスを提供するために使われるプログラムである。カーネルモードで動作する必要のない各種アプリケーションが共有ライブラリを呼び出すことにより、必要なオペレーティングシステムのサービスが提供される。なお、UNIXまたはPOSIXのアプリケーションをサポートするために必要な機能はすべて共有ライブラリによって実装されている。

(3) システムコマンド

シェル上で動作し、TOEを管理するために必要となるコマンド群である。オブジェクトの管理、セキュリティ属性の管理、利用者の管理などを行うために必要なコマンドが含まれ、それらは1つのプログラム、またはシェルの機能の一部として提供される。

(4) シェル

プロンプトを出力し、ユーザから入力されたコマンドライン解釈し、与えられた指示をカーネルに命令する。また、システムコマンドを実行するための環境を提供する。

(5) 監査機能

各利用者が識別/認証を試みた際に、その成功・失敗の監査証跡を記録する。監査証跡へのアクセスは管理者のみが行うことができる。

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「MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One オペレーティングシステム 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、「MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One オペレーティングシステム評価報告書」(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19年1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、EAL1適合である。

1.5.3 セキュリティ機能強度

STは、AVA_SOF.1を含まないため、最小機能強度を主張しない。

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) 識別/認証

すべての利用者にユニークな識別子を割当て、セキュリティ機能を介してTOEにアクセスするすべての利用者に対して、要求した利用者の身元を認証する。この認証はパスワード方式により行う。

(2) アクセス制御

プロセス（プロセス間通信データを含む）、ファイル、ディレクトリ等のオブジェクトに対するアクセスを制御する。プロセスのユーザID及びグループIDと、操作対象となるオブジェクトの所有ユーザID、所有グループID、各パーミッション、ext2/ext3ファイルシステムのアトリビュートに基づいて制御を行う。

(3) 監査

管理者及び利用者の認証/識別を逐次記録し、蓄積する。監査証跡は通常のテキストファイル形式で記録され、管理者のみが読み出し可能である。また、一定のサイズでローテーションされるように監査証跡を管理する。

(4) プロセス分離

オペレーティングシステムカーネルとユーザプロセス間、及び各ユーザプロセス間の分離を保証する機構を提供する。

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.AUTHORISED_USERS	許可された利用者のみがTOEにアクセス可能である。
P.NEED_TO_KNOW.1	ファイルおよびディレクトリの所有者は、セキュリティ属性を変更することで自身以外の利用者の該当ファイルおよびディレクトリへのアクセスを必要な利用者だけに制限する。
P.NEED_TO_KNOW.2	プロセスへのアクセスは、所有者および管理者のみに制限する。
P.ACCOUNTABILITY	利用者がTOEにアクセスする際の識別/認証を記録する。
P.LOG_SIZE	管理者は、データのおふれによる監査記録の消失を防ぐ設定を行う。

1.5.7 構成条件

本TOEは、IA32及びx86-64アーキテクチャーのCPUを搭載したIntel x86互換のコンピュータ上で動作する。

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1-2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1-2 TOE使用の前提条件

識別子	前提条件
A.LOCATE	TOEは、物理的な攻撃から保護されるものとする。

A.MANAGE	TOEの管理者は悪意のある行為を行わず、与えられた権限に対する責務を果たすものとする。
A.PASSWORD	TOEの利用者および管理者のパスワードは推測可能な文字列ではなく、かつ、各利用者および管理者は自身のパスワードを秘匿しなければならない。

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。

- MIRACLE LINUX インストレーションガイド (2005年10月1日)
- MIRACLE LINUX V4.0 セキュリティガイダンス (2006年12月20日)

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19年1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10月、11月に開発者サイトで開発者のテスト環境を使用し、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

本TOEでは、開発者テストは評価対象外である。

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環境を以下に示す。TOEは、下表の各PCにインストールされた状態でテストされた。

表 2-1 MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One

IBM THINK PAD A22M	
CPU	Pentium III.600 MHz
メモリ	384MB
ハードディスク	20GB

表 2-2 MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One

自作PC	
CPU	Intel Xeon.3.4GHz
メモリ	2048MB
ハードディスク	80GB

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表 2-1及び表 2-2に示す。評価者テストはSTにおいて識別されているTOE構成を満たす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。

TSFIとしてシェルコマンドをテストする場合、シェル上でコマンドを手入力するかコマンドを含むシェルスクリプトを実行し、その実行結果（ログイン画面の遷移、シェル上の出力内容、ファイル属性、ログファイルの内容、など）を観察する。

TSFIとしてシステムコールをテストする場合、gccを使用して対象となるシステムコールを含むテストプログラムを作成し、その実行結果（シェル上の出力内容、ファイル属性、ログファイルの内容、など）を観察する。

c. 実施テストの範囲

評価者が独自に考案した計27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。

すべてのセキュリティ機能要件（FPT_SEP.1を除く）をカバーするように、テスト対象のセキュリティ機能(TSF)とその外部セキュリティ機能インタフェース(TSFI)を選択する。

機能仕様に記載されているTSFIへの入力によって確認可能なTSFのふるまいをテスト対象とする。

テスト対象のTSFIとしてシェルコマンドをより多く選択する（シェルコマンドはシェルを介してシステムコール・ライブラリコールを呼び出すため、結果的に、入力に使用したTSFIよりも多くのTSFIが呼び出される。ただし、テスト項目の選択では、シェルコマンドとシステムコール・ライブラリコールの相関関係は考慮していない）。

TSF間の関係を考慮した組み合わせテストやTOEの状態別のテストは対象外とする。

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。

当該所見報告書でなされた指摘内容が妥当であること。

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。

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。

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。

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EAL1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種別、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_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。
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.1.2E	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.1.1E	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_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。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。
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_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	<p>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。</p>
AGD_USR.1.1E	<p>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。</p>
テスト	適切な評価が実施された
ATE_IND.1.1E	<p>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、TOEと同等の資源が提供されていることを確認している。</p>
ATE_IND.1.2E	<p>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。</p>

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
TSFI	TOE Security Functions Interface
VFS	Virtual File System

6 参照

- [1] MIRACLE LINUX V4.0 / MIRACLE LINUX V4.0 One / MIRACLE LINUX V4.0 x86-64 / MIRACLE LINUX V4.0 x86-64 One オペレーティングシステム セキュリティターゲット バージョン 1.0 (2007年1月11日) ミラクル・リナックス株式会社
- [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] MIRACLE LINUX v4.0 / MIRACLE LINUX v4.0 One / MIRACLE LINUX v4.0 x86-64 / MIRACLE LINUX v4.0 x86-64 One オペレーティングシステム 評価報告書 初版 2007年1月12日 みずほ情報総研株式会社 情報セキュリティ評価室