



# 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

申請受付日（受付番号）	平成20年1月17日（IT認証8192）
認証番号	C0152
認証申請者	株式会社NEC情報システムズ
TOEの名称	機能特定（PROCENTER Web版）
TOEのバージョン	3.6
PP適合	なし
適合する保証パッケージ	EAL1（CC Ver3.1）
開発者	株式会社NEC情報システムズ
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20年3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 鈴木 秀二

**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。**

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 バージョン3.1 改訂第1版  
(翻訳第1.2版)

情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第1版 (翻訳第1.2版)

## 評価結果：合格

「PROCENTER Web版 3.6」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、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	4
1.4	評価の認証	5
1.5	報告概要	5
1.5.1	PP適合	5
1.5.2	EAL	5
1.5.3	セキュリティ機能	5
1.5.4	脅威	5
1.5.5	組織のセキュリティ方針	5
1.5.6	構成条件	5
1.5.7	製品添付ドキュメント	6
2	評価機関による評価実施及び結果	7
2.1	評価方法	7
2.2	評価実施概要	7
2.3	製品テスト	7
2.3.1	開発者テスト	7
2.3.2	評価者テスト	7
2.4	評価結果	10
3	認証実施	11
4	結論	12
4.1	認証結果	12
4.2	注意事項	14
5	用語	15
6	参照	17

## 1 全体要約

### 1.1 はじめに

この認証報告書は、「PROCENTER Web版 3.6」（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株式会社NEC情報システムズ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「1.5.7 製品添付ドキュメント」を参照のこと）を併読されたい。本TOEは低保証STのためセキュリティ課題定義などが記述されていないが、運用環境のセキュリティ対策方針、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： PROCENTER Web版  
バージョン： 3.6  
開発者： 株式会社NEC情報システムズ

#### 1.2.2 製品概要

本製品は文書・コンテンツ管理システムであり、実体ファイルや属性情報に関して登録、更新、参照、検索するための機能を提供する。本製品の主要なセキュリティ機能を以下に示す。

- ・ 識別認証機能
- ・ アクセス制御機能

### 1.2.3 TOEの範囲と動作概要

本TOEは、PROCENTERサーバ上で稼動する「PROCENTERサーバソフトウェア」及び「PROCENTER Webサーバソフトウェア」である。

本TOEの動作環境概要を図1-1に示す。

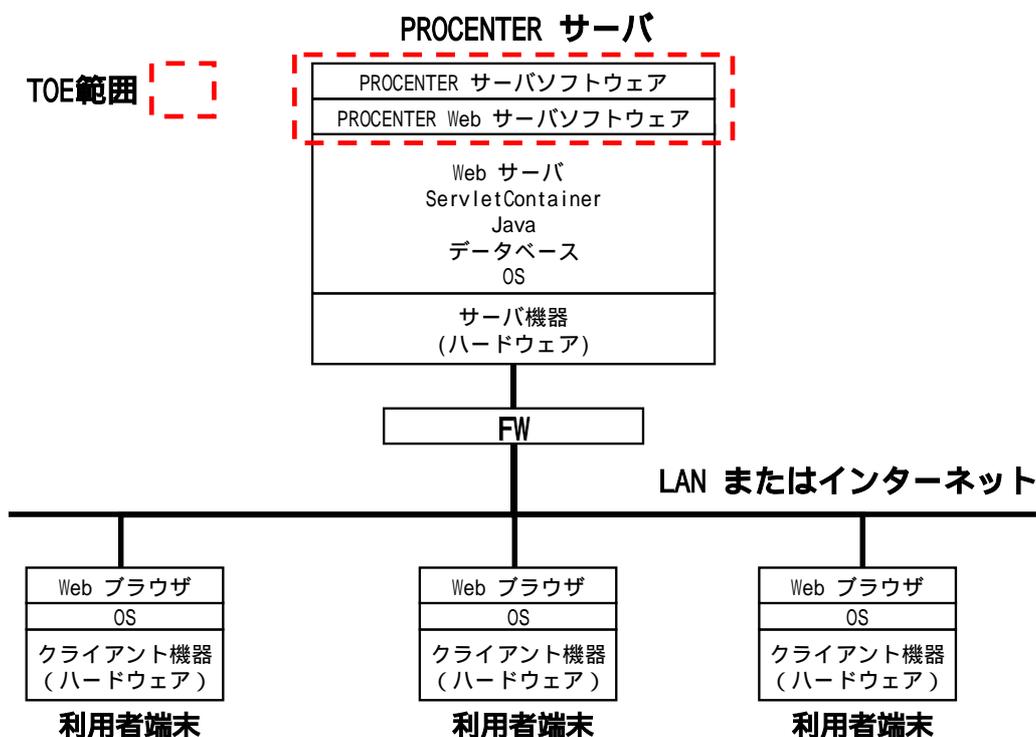


図1-1 TOEの動作環境概要

本TOEの動作概要について以下に示す。

TOEを使用するには、システム管理者が利用者を登録する。

サーバ内の文書・コンテンツは、論理的な階層構造を構築するためのフォルダノード、その配下に、ひとつあるいは複数の実際のファイルを保存するファイルノード、属性情報の1つとしてURLを登録できるURLノードからなるデータ構造で管理される。

すべてのノード（フォルダ、ファイル、URL）に対して、利用者毎の、表示、読み込み、書き込み、削除といったアクセス権レベル制御があり、ノードアクセス権リストとして管理される。

利用者は、LANまたはインターネット上の利用者端末からWebブラウザを使用し、指定されたURLよりPROCENTERサーバにHTTPSプロトコル通信によりアクセスし、ユーザIDとパスワードを入力する。

TOEは、入力されたユーザIDとパスワードにより利用者の識別と認証を行う。

利用者は、TOEにより識別認証された後、アクセス制御により、許可される範囲内で、各ノード（フォルダ、ファイル、URL）に対し、登録、更新、参照、削除、検索機能を利用する。

本TOE及び本TOEと連動する構成要素について以下に示す。

(1) PROCENTER サーバ（TOEを含む）

TOEである「PROCENTERサーバソフトウェア」及び「PROCENTER Webサーバソフトウェア」が動作するサーバ。

TOEを稼働させるために、PROCENTERサーバには、サーバ機器（ハードウェア）、OS、データベース、Java、ServletContainer、Webサーバが必要となる。

(2) 利用者端末（TOE範囲外）

利用者はLANまたはインターネット上の利用者端末からWebブラウザを使用し、指定されたURLよりPROCENTERサーバにアクセスする。利用者がTOEを利用するために、利用者端末には、クライアント機器（ハードウェア）、OS、Webブラウザが必要となる。

(3) ファイアウォール（TOE範囲外）

PROCENTERサーバとLANまたはインターネットの間にはFWを設置し、利用者からのリクエストによるHTTPSプロトコル通信だけを通すように制御する。

#### 1.2.4 TOEの機能

本TOEのセキュリティ機能の内容を以下に示す。

(1) 識別認証機能

利用者によって入力されたユーザIDとパスワードを使用し、利用者の識別と認証を行う機能。

(2) アクセス制御機能

利用者の役割及びアクセス権設定に基づいてノードに対するアクセス制御を行う機能。

TOEの論理的範囲を、図1-2に示す。

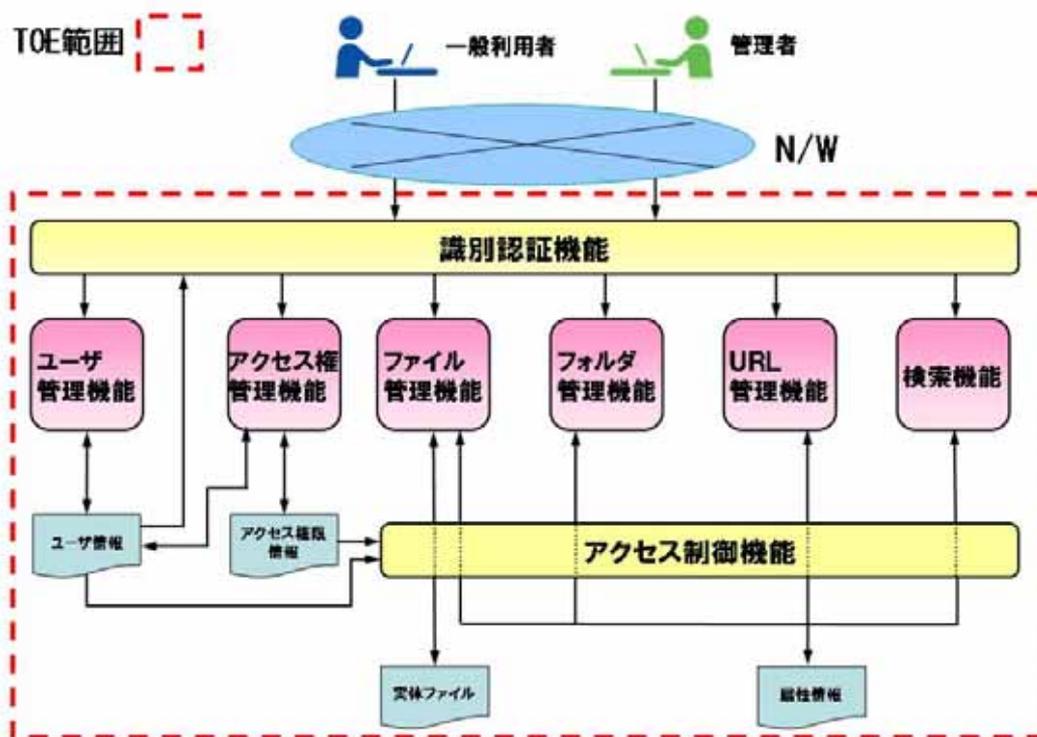


図1-2 TOEの論理的範囲

### 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セキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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「PROCENTER Web版 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]のいずれか) 附属書A、CCパート2 ([6][9]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]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、「PROCENTER Web版 評価報告書」(以下「評価報告書」という。)[13]に示されている。なお、評価方法は、CEM ([11][12]のいずれか)に準拠する。

## 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。 評価は、平成20年3月の評価機関による評価報告書の提出をもって完了し、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

本TOEのセキュリティ機能は、1.2.4を参照のこと。

本TOEのセキュリティ機能は、以下に示すセキュリティ機能要件を実現している。

- アクセス制御
- 識別・認証
- セキュリティ管理

### 1.5.4 脅威

本TOEでは、セキュリティ課題定義は評価対象外である。

### 1.5.5 組織のセキュリティ方針

本TOEでは、セキュリティ課題定義は評価対象外である。

### 1.5.6 構成条件

TOEが動作するために必要なIT製品の中で、本評価にて検証した環境を以下に示

す。

PROCENTER サーバの動作環境：

【ハードウェア】

- メモリ：1GB 以上
- ハードディスク：600MB 以上
- Microsoft Windows Server 2003 SP2 が動作するサーバ機器

【ソフトウェア】

- OS：Microsoft Windows Server 2003 SP2
- Web サーバ：IIS6.0
- ServletContainer：Adobe JRun4 Professional Edition  
(Updater6 適用必須)
- Java:1.4.2\_14
- データベース：Oracle Database 10g Release2

利用者端末の動作環境：

【ハードウェア】

- Microsoft Internet Explorer 6.0 SP2 が動作するクライアント機器

【ソフトウェア】

- OS：Microsoft Internet Explorer 6.0 SP2 が動作する OS
- Web ブラウザ：Microsoft Internet Explorer 6.0 SP2

### 1.5.7 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。

- PROCENTER AMIGO ユーザーズガイド Version1.3 (2008/3/17)
- PROCENTER AMIGO ユーザーズガイド 補足 Version1.3 (2008/3/17)
- PROCENTER サーバ Version 3.6 インストールガイド Version1.2 (2008/3/10)  
(PROCENTER サーバソフトウェアのインストールガイド)
- PROCENTER AMIGO インストールガイド JRun4 用 Version1.2 (2008/2/26)  
(PROCENTER Web サーバソフトウェアのインストールガイド)
- PROCENTER Web 版 はじめにお読みください Version1.4 (2008/3/24)

## 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20年1月に始まり、平成20年3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20年2月及び3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。

### 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図2-1に、TOEの動作に関する各構成要素の要件を表2-1及び表2-2示す。

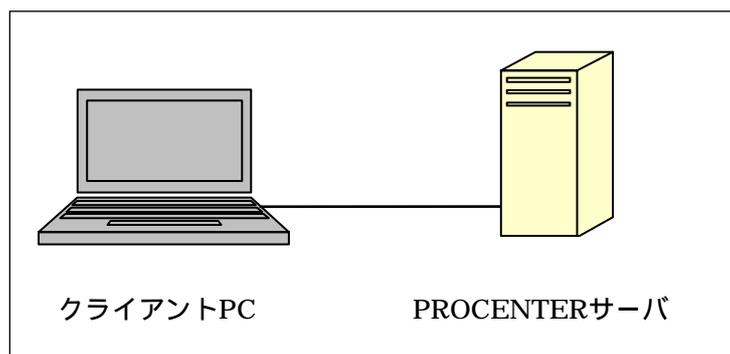


図2-1 評価者テストの環境

表2-1 評価者テストの環境におけるTOEの動作に関する各構成要素の要件

名称	製品
PROCENTERサーバ	<p><u>ハードウェア</u>： DELL POWER EDG SC-1420</p> <p><u>OS</u>： Microsoft Windows Server 2003 Standard Edition Service Pack2</p> <p><u>PROCENTERサーバソフトウェア</u>：(TOE) PROCENTER SERVER VERSION 3.6.4.8 PANDA Version 6.3.3.33</p> <p><u>PROCENTER Webサーバソフトウェア</u>：(TOE) PROCENTER Web版 Version 3.6</p> <p><u>Webサーバ</u>： IIS6.0</p> <p><u>ServletContainer</u>： Adobe JRun4 Professional Edition (Updater6 適用) JRun/4 [SERVLET 2.3, JSP 1.2]</p> <p><u>Java</u>： Java1.4.2_14 Java1.4.2_14-b05 JVM[Java HotSpot(TM) Client VM:mixed mode] Sun Microsystems</p> <p><u>データベース</u>： Oracle Database 10g Release 10.2.0.3.0 – Production</p>
クライアントPC	<p>OS : Windows XP SP2</p> <ul style="list-style-type: none"> <li>・2008年2月29日現在、Microsoft update 対応済</li> </ul>
ブラウザ (クライアントPC)	<p>ブラウザ : Internet Explorer 6 SP2、Firefox 2.0.0.12</p> <ul style="list-style-type: none"> <li>・通常のHTTPのGETリクエスト、HTML内のPOSTリクエストを送信するために利用。なお、Firefoxは侵入検査(AVAクラス)のテストで使用。</li> </ul>
Fiddler2.1.4.2	<p>HTTPデバッグツール</p> <ul style="list-style-type: none"> <li>・IE6の送信情報を記録すると共に、記録情報をベースとして任意</li> </ul>

名称	製品
(クライアントPC)	<p>のリクエストを構成することができる。</p> <ul style="list-style-type: none"> <li>任意のリクエストの送信が可能であり、そのレスポンスと含めてモニタリングすることが可能。</li> </ul> <p>HTTP デバッギングツールは、テスト結果を確認するために使用するのではなく、TOE の動作で予期しない現象が発生した時のエビデンス取得ツールとして使用する。</p>
WebView Inspector	<p>Fiddler 2 のアドオン</p> <ul style="list-style-type: none"> <li>任意のリクエストに対するレスポンスを IE 的に表示することが可能。</li> </ul>
Stunnel 4.21 (with Openssl 0.9.8g)	<p>SSL 通信ツール</p> <ul style="list-style-type: none"> <li>任意の TCP 通信データを SSL 化するためのツール。</li> <li>SSL に対応していないソフトでも、本ソフトを経由させることによって通信を SSL 化することが可能。</li> </ul>
Tamper Data 10.0.3	<p>Firefox のアドオン</p> <ul style="list-style-type: none"> <li>リクエストを任意に書き換えることが可能。</li> <li>代表的な不正なパラメタバリューが準備済みである。</li> </ul>
Ollydbg 1.10	<p>ユーザモードデバッガ</p> <ul style="list-style-type: none"> <li>Windows 上のプログラムを実行状態でデバッグする。</li> <li>CPU、スタック、利用メモリ領域、実行コードを解析する。</li> </ul>

## 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図2-1、TOEの動作に関する各構成要素の要件を表2-1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。

Webブラウザ、HTTPデバッギングツール、SSL通信ツールを用いて、外部インターフェースからセキュリティ機能に刺激（パラメタ）を与え、外部インターフェースや送受信されるパケットの情報を参照してセキュリティ機能のふるまいを目視確認する。

### c. 実施テストの範囲

評価者が独自に考案した評価者テスト（TSFIの47のインターフェースに対して）を20項目、侵入テストを12項目、計32項目を実施した。評価者テスト項目の選択基準として、下記を考慮している。

外部インターフェースを対象とし、限界値分析によるブラックボックステストを実施する。

テストするインタフェースは、重要性、複雑さ、テスト効率、インタフェースの種別、新規性を踏まえて決定する。

テストするインタフェースに関わるセキュリティ機能を網羅的にテストする。

侵入テストに関してはEAL1の証拠資料レベルから、インタフェースを単位として、公知の脆弱性の探索確認結果を踏まえて悪用可能性を分析し、疑いがもたれる内容についてテスト方法を考案し、想定する攻撃能力を持つ攻撃者が利用し得るインターネット上に公開されているフリーツールを使用し確認した。

#### d.結果

実施したすべての評価者テスト及び侵入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

認証機関は、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。

認証機関は、ST及び評価報告書において、所見報告書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に対する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
<b>セキュリティターゲット評価</b>	<b>適切な評価が実施された。</b>
ASE_INT.1.1E	評価はワークユニットに沿って行われ、TOE参照、TOE概要、及びTOE記述が正しく記述さ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、TOE参照、TOE概要、及びTOE記述が相互に一貫していることを確認している。
ASE_CCL.1.1E	評価はワークユニットに沿って行われ、CCの適合主張の有効性を確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、運用環境のセキュリティ対策方針が明確に定義されていることを確認している。
ASE_ECD.1.1E	評価はワークユニットに沿って行われ、拡張セキュリティ要件が含まれていないため非適用であることを確認している。
ASE_ECD.1.2E	評価はワークユニットに沿って行われ、拡張セキュリティ要件が含ま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、SFR、SARは明確に、曖昧さなく十分に定義され、また内部的に一貫し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要約仕様の記述がどのように各SFRを満たすかを示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TOE概要及びTOE記述と一貫していることを確認している。
<b>ライフサイクルサポート</b>	<b>適切な評価が実施された</b>
ALC_CMC.1.1E	評価はワークユニットに沿って行われ、TOEは一意の参照でラベル付けされていることを確認している。
ALC_CMS.1.1E	評価はワークユニットに沿って行われ、TOEの構成リストが管理され、構成要素が一意に識別可能なことを確認している。
<b>開発</b>	<b>適切な評価が実施された</b>
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。
<b>ガイダンス文書</b>	<b>適切な評価が実施された</b>
AGD_OPE.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_PRE.1.1E	評価はワークユニットに沿って行われ、準備手続きがTOEのセキュアな準備を記述し、STの運用環境のITセキュリティ方針に従った環境が構築可能であることを確認している。
AGD_PRE.1.2E	評価はワークユニットに沿って行われ、準備手続きを元に評価者がセキュアにTOEと準備環境を構築可能なことを実行し確認している。
<b>テスト</b>	<b>適切な評価が実施された</b>
ATE_IND.1.1E	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、提供されていることを確認している。
ATE_IND.1.2E	評価はワークユニットに沿って行われ、独立テストを実施し、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、本評価のテスト実施方法も適切と判断される。
<b>脆弱性評価</b>	<b>適切な評価が実施された</b>
AVA_VAN.1.1E	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、提供されていることを確認している。
AVA_VAN.1.2E	評価はワークユニットに沿って行われ、潜在的な脆弱性検出のために公知の資料を検査していることを確認している。
AVA_VAN.1.3E	評価はワークユニットに沿って行われ、識別された潜在的脆弱性が基本的な攻撃能力を持つ攻撃者からの攻撃に耐えられることを根拠とともに記述していることを確認している。

## 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
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

本報告書で使用された用語を以下に示す。

利用者	TOEが提供するサービスを利用する人。利用者はその役割により、管理者と一般利用者に分かれる。利用者のことをユーザとも呼ぶ。
ユーザID	利用者を識別するためのID。利用者のユーザ情報における「社員番号」が利用者を識別するためのIDとなる。
システム管理者	システム管理権限を有する管理者。
システム管理権限	ノードアクセス権リストやロック状態にかかわらず、すべてのノードに対して参照・更新・削除が行える権限。システム管理権限は、ユーザ管理権限、グループ管理権限を包括する。
ノード	TOEが保持する論理的なデータ構造の構成要素。利用者はノードに対して実体ファイルと属性情報を登録することができる。ノードはその役割により、フォルダノード、ファイルノード、URLノードに分かれる。実体ファイルが登録できるのはファイルノードだけである。
フォルダノード	階層構造を構築するためのノード。階層構造上、あるノードを基準として直上のノードを親ノード、直下のノードを子ノード、配下のノードを配下ノードと呼ぶ。フォルダノードは子ノードとして複数のノードを保持することができる。最上位のノードを除き、すべてのノードには必ず親ノードが1つ存在する。
ファイルノード	実体ファイルを登録できるノード。1つのファイルノードに対し、複数の実体ファイルを登録することができる。
URLノード	属性情報の1つとしてURLを登録できるノード。

ノードアクセス権リスト	あるノードに対して設定されたアクセス権の集合。
アクセス権	利用者もしくはグループに対するアクセス権レベル（操作権限）。
アクセス権レベル	<p>アクセス権レベルには [表示(V)] [読み込み(VR)] [書き込み(VRW)] [削除(VRWD)] があり、それぞれ後者の権限は、前者の権限を包括する。付与されたアクセス権レベルにより、利用者にはノードに対する下記の操作が許可される。</p> <ul style="list-style-type: none"> <li>・ [表示(V)] ... 属性参照</li> <li>・ [読み込み(VR)] ... 実体参照（ファイルノードの場合）</li> <li>・ [書き込み(VRW)]... 属性情報の更新 実体ファイルの登録・更新（ファイルノードの場合） 子ノードの新規作成（フォルダノードの場合）</li> <li>・ [削除(VRWD)] ... ノードの削除（ファイルノードの場合は登録されている実体ファイルも削除される。 フォルダノードの場合は配下ノードも削除される）</li> </ul>
実体ファイル	OS上ファイルとして管理されるデータ単位（いわゆるファイルのこと）。ファイルノードとの違いを明確化するため、TOEに登録するファイルのことを実体ファイルと呼ぶ。
属性情報	ノードの性質を表す文字列または数値による情報。「名前」、「ステータス」、備考」、「URL」等がある。
PROCENTERサーバ	TOEを稼動するために必要なハードウェアと、そのハードウェア上で動作するTOEを稼動するために必要なソフトウェア。
PROCENTERサーバソフトウェア	TOEの各機能を提供するためのソフトウェア。
PROCENTER Webサーバソフトウェア	TOEの各機能をWebブラウザから利用するための機能・インタフェースを提供するためのソフトウェア。
FW	Firewall(ファイアウォール)の略。
Firewall	ネットワーク上で特定のIPアドレス及びポートからのアクセスをフィルタリングするアプリケーション。
N/W	Network（ネットワーク）の略。

## 6 参照

- [1] PROCENTER Web版 セキュリティターゲット バージョン 1.8(2008年3月24日)  
株式会社NEC情報システムズ
- [2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報  
処理推進機構 CCS-01
- [3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報  
処理推進機構 CCM-02
- [4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政  
法人 情報処理推進機構 CCM-03
- [5] Common Criteria for Information Technology Security Evaluation Part1:  
Introduction and general model Version 3.1 Revision 1 September 2006  
CCMB-2006-09-001
- [6] Common Criteria for Information Technology Security Evaluation Part2:  
Security functional components Version 3.1 Revision 1 September 2006  
CCMB-2006-09-002
- [7] Common Criteria for Information Technology Security Evaluation Part3:  
Security assurance components Version 3.1 Revision 1 September 2006  
CCMB-2006-09-003
- [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3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2  
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  
コンポーネント バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-002 (平成  
19年3月翻訳第1.2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  
コンポーネント バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-003 (平成  
19年3月翻訳第1.2版))
- [11] Common Methodology for Information Technology Security Evaluation :  
Evaluation Methodology Version 3.1 Revision 1 September 2006  
CCMB-2006-09-004
- [12] 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3.1 改訂第1版  
2006年9月 CCMB-2006-09-004 (平成19年3月翻訳第1.2版)
- [13] PROCENTER Web版 評価報告書 第2版 2008年3月26日  
みずほ情報総研株式会社 情報セキュリティ評価室