認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	**平成19年12月27日** (IT**認証**7189)
認証番号	C0158
認証申請者	**株式会社日立製作所**
TOE**の名称**	DocumentBroker Server Version 3
TOE**のバージョン**	03-11
PP**適合**	**なし**
適合する保証パッケージ	EAL1**及び追加の保証コンポーネント**ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1
開発者	**株式会社日立製作所**
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4月25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。

① 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)
② 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

「DocumentBroker Server Version 3」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 はじめに

この認証報告書は、「DocumentBroker Server Version 3」（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日立製作所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「1.5.8 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：　DocumentBroker Server Version 3
バージョン：　03-11
開発者：　株式会社日立製作所

1.2.2 製品概要

本TOEは、リレーショナルデータベース（RDBMS）上に構築された文書管理システムを構成するソフトウェア製品である。文書管理システムのサーバとして機能し、クライアントからの要求に応じて、データベースに格納された情報にアクセスする。TOEはミドルウェアでありエンドユーザ（一般利用者）に対するインタフェースを提供していない。

TOEは、次に示す基本機能とセキュリティ機能を提供する。

【基本機能】

・文書の登録機能
・バージョン管理機能

・マルチレンディション管理機能
・コンテナ管理機能
・文書間リレーション管理機能
・文書の属性情報の管理機能
・検索機能
・ファイル転送機能
・複数の実行環境機能

【セキュリティ機能】
・アクセス制御機能
TOEが提供する文書空間において、オブジェクトの新規作成とTOEの管理下にある作成済みのオブジェクトに対する操作を、識別・認証されたセッションに対して、ユーザ識別子またはグループ識別子単位で許可する。また、このアクセス判定に使用されるアクセス制御情報を変更する権限を特定のユーザ識別子またはグループ識別子を持つセッションに制限する。

1.2.3 TOEの範囲と動作概要

（1）TOEの動作環境と検証環境

TOEを使用して構築される文書管理システムの構成を図 1-1に示す。

文書管理システムは、業務の内容に応じて作成されるユーザアプリケーションプログラム（UAP）を実行する文書管理クライアントと、そのUAPに文書の登録、バージョン管理、検索といった文書管理の基盤機能を提供する文書管理サーバから構成される。TOEは文書管理サーバに含まれる。

TOEはファイアウォールにより適切に保護されたネットワーク、または公衆ネットワークと直接接続されないネットワーク上に設置される。

【文書管理クライアント】

システム管理者により運用管理されたUAPが動作する端末である。UAPの実行により、DocumentBrokerクライアントの提供するAPIが発行される。発行されたAPIによる要求はTPBrokerを介して文書管理サーバのDocumentBroker Serverに送信され、文書空間への接続、文書オブジェクトの参照などの操作が行われる。文書管理クライアントはTOEの範囲外である。

【ディレクトリサーバ】

LDAP対応のディレクトリサービスが動作する端末である。DocumentBroker Serverから受信したユーザ識別子とパスワードに基づいて識別・認証を行い、ユーザ識別子に対応するグループ識別子を返信する。ディレクトリサーバはTOEの範囲

外である。

【文書管理サーバ】

DocumentBroker Server、DABroker、TPBroker、HiRDBサーバが動作する端末である。DocumentBroker ServerはTPBrokerを介して送られてきたリクエストに応じ、DABrokerを介してHiRDBサーバへのアクセスを行い、実行結果をUAPに返却する。TOEは文書管理サーバ上で動作する。

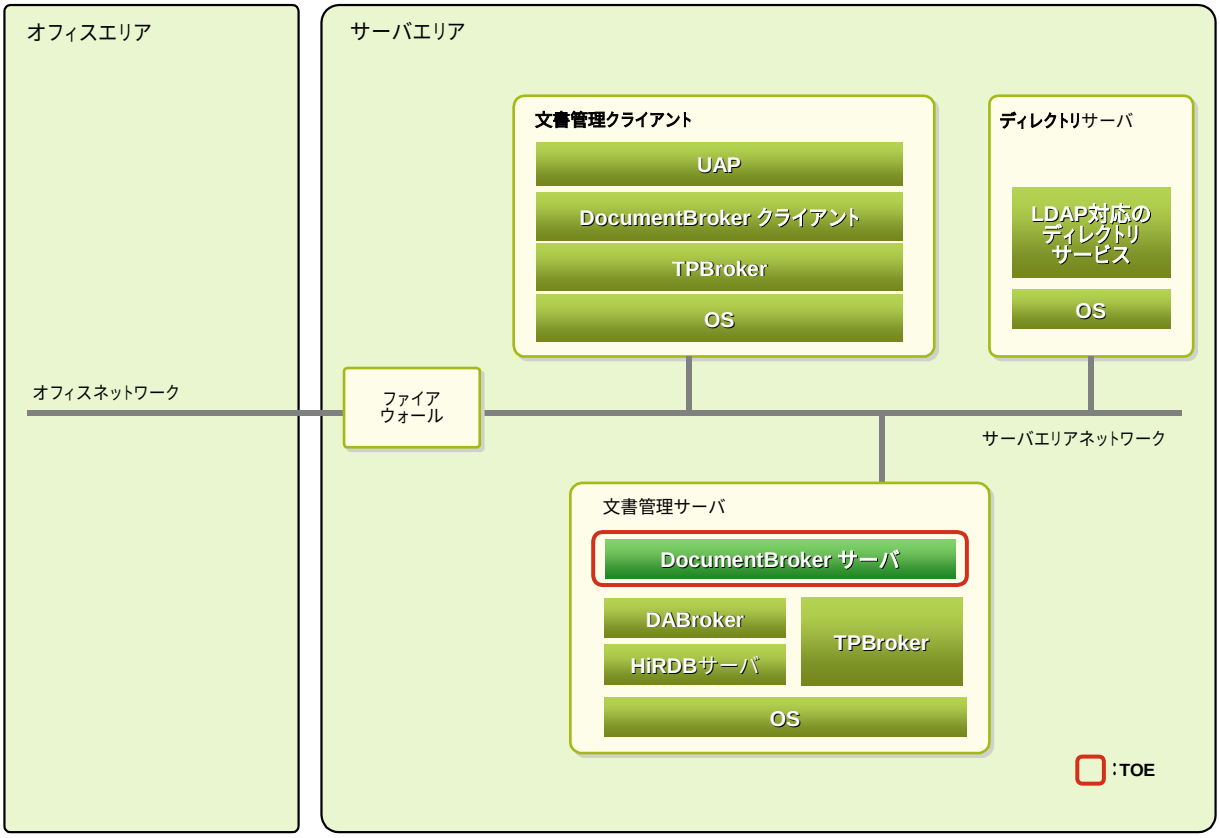

図 1-1　TOEを含む文書管理システムのシステム構成図

文書管理システムを構築するために必要な構成要素を表1-1に示す。

表 1-1　文書管理システムの構成

構成要素	概要説明
UAP	TOEによる文書管理機能を利用し、業務に応じて作成されるユーザアプリケーションプログラム。
DocumentBroker クライアント	TOEの機能を利用したユーザアプリケーションを実行するためのAPIを提供するランタイムモジュール。

DocumentBrokerサーバ	TOE：DocumentBroker Server Version 3
DABroker	データベースにアクセスするためのインタフェースを提供する。
LDAP対応の ディレクトリサービス	文書管理システムのユーザ管理とユーザ認証の機能を提供するサーバ。
HiRDB サーバ	文書管理システムが扱う文書データや文書プロパティを格納するデータベースサーバ。
TPBroker	分散システムの通信制御機能などを提供する開発環境兼実行環境。
OS	上記の各構成要素が動作するために必要なOS。

なお、文書管理システムを構成する要素であるUAP、TOE、LDAP対応のディレクトリサービス、HiRDBサーバの各ソフトウェアは、単一の端末上で構築することも、複数の端末に分散させて構築することもできる。

文書管理システムの構成要素(表 1-1)に要求されるソフトウェア条件を表1-2から表1-5に示す。なお、各構成要素につき、製品名欄に示された製品のいずれか一つを選択することになる。

表 1-2　文書管理サーバ環境のソフトウェア条件

構成要素	製品名	ベンダ名
DocumentBroker サーバ	・ DocumentBroker Server Version 3	(株)日立製作所
DABroker	・ DABroker 及び DABroker for C++	(株)日立製作所
HiRDB サーバ	・ HiRDB/Single Server Version 6 ・ HiRDB/Parallel Server Version 6 ・ HiRDB/Single Server Version 7 ・ HiRDB/Parallel Server Version 7 ・ HiRDB/Single Server Version 8 ・ HiRDB/Parallel Server Version 8	(株)日立製作所

TPBroker	TPBrokerとしてTPBrokerのバージョン3を使用する場合 ・ TPBroker for C++ ・ TPBroker Developer for C++ TPBrokerとしてTPBrokerのバージョン5を使用する場合 ・ TPBroker ・ TPBroker Developer	(株)日立製作所
OS	・ Windows 2000 Professional ・ Windows 2000 Server ・ Windows 2000 Advanced Server ・ Windows 2000 Datacenter Server ・ Windows Server 2003, Standard Edition (32bit) ・ Windows Server 2003, Enterprise Edition (32bit) ・ Windows Server 2003 R2, Standard Edition (32bit) ・ Windows Server 2003 R2, Enterprise Edition (32bit)	Microsoft
	・ AIX 5L V5.1 ・ AIX 5L V5.2 ・ AIX 5L V5.3	IBM

表 1-3　文書管理クライアント環境のソフトウェア条件

構成要素	製品名	ベンダ名
DocumentBroker クライアント	・ DocumentBroker Runtime Version 3 ・ DocumentBroker Development Kit Version 3	(株)日立製作所
TPBroker	TPBrokerとしてTPBrokerのバージョン3を使用する場合 ・ TPBroker for C++ ・ TPBroker Developer for C++ TPBrokerとしてTPBrokerのバージョン5を使用する場合 ・ TPBroker ・ TPBroker Developer	(株)日立製作所

OS	・ Windows 2000 Professional ・ Windows 2000 Server ・ Windows 2000 Advanced Server ・ Windows 2000 Datacenter Server ・ Windows XP Professional ・ Windows Server 2003, Standard Edition (32bit) ・ Windows Server 2003, Enterprise Edition (32bit) ・ Windows Server 2003 R2, Standard Edition (32bit) ・ Windows Server 2003 R2, Enterprise Edition (32bit)	Microsoft
	・ AIX 5L V5.1 ・ AIX 5L V5.2 ・ AIX 5L V5.3	IBM

表 1-4　ディレクトリサーバ環境のソフトウェア条件（IT環境がWindowsの場合）

構成要素	製品名	ベンダ名
LDAP対応のディレクトリサービス	・ Active Directory	Microsoft
	・ Sun ONE Directory Server ・ Sun Java System Directory Server	Sun Microsystems
OS	・ Windows 2000 Server ・ Windows 2000 Advanced Server ・ Windows Server 2003, Standard Edition (32bit) ・ Windows Server 2003, Enterprise Edition (32bit) ・ Windows Server 2003 R2, Standard Edition (32bit) ・ Windows Server 2003 R2, Enterprise Edition (32bit)	Microsoft

表 1-5　ディレクトリサーバ環境のソフトウェア条件（IT環境がAIXの場合）

構成要素	製品名	ベンダ名
LDAP対応のディレクトリサービス	・ IBM SecureWay Directory ・ IBM Directory Server ・ IBM Tivoli Directory Server	IBM

OS	・ AIX 5L V5.1 ・ AIX 5L V5.2 ・ AIX 5L V5.3	IBM

（注：TOEのIT環境がWindowsの場合に表 1-5のディレクトリサーバと連携することは、TOE利用方法の対象外である。）

本評価が実施した検証環境を表1-6から表1-8に示す。

表 1-6 検証した環境（TOEのIT環境がWindowsの場合）

端末	ソフトウェア名称及びバージョン・リビジョン
文書管理サーバ	DocumentBroker Server Version 3 03-11
	DABroker 03-14
	DABroker for C++ 02-09
	TPBroker for C++ 03-08-/E
	HiRDB/Single Server Version 8 08-03
	Windows Server 2003, Standard Edition (32bit) (Service Pack 2)

表 1-7 検証した環境（TOEのIT環境がAIXの場合）

端末	ソフトウェア名称及びバージョン・リビジョン
文書管理サーバ	DocumentBroker Server Version 3 03-11
	DABroker 03-13-/B
	DABroker for C++ 02-07-/B
	TPBroker for C++ 03-06-/X
	HiRDB/Single Server Version 8 08-03
	AIX 5L V5.3

表 1-8 検証した環境（共通）

端末	ソフトウェア名称及びバージョン・リビジョン
文書管理クライアント兼ディレクトリサーバ	DocumentBroker Development Kit Version 3 03-11
	TPBroker for C++ 03-08-/E
	Sun Java System Directory Server 5.2 Patch 4
	Windows Server 2003, Standard Edition (32bit) (Service Pack 2)

（2）TOEの関係者

【システム管理者】

サーバエリア内のハードウェア、ソフトウェア、ネットワークに対して責任を持ち、TOE、データベース、LDAP、UAP及びOSの運用、管理、保守を担当する役割を持つOS上のユーザ。この役割を担うシステム管理者は担当業務に必要な知識・技術を備える。OSの管理者権限を持ち、システムの構成変更の権限を持つ。以下の作業を行う。

- TOE／データベース／LDAPの構築、起動、停止
- LDAPに登録されているユーザ識別子とパスワードの管理
- UAPの配置、起動、停止

【セキュリティ運用者】

TOEのアクセス制御機能の基本動作に関わる設定を保守する役割を持つOS上のユーザ。システム管理者と兼務することができる。セキュリティ運用者は、OS上の設定ファイル（セキュリティ定義ファイル）を編集することにより、以下の作業を行う。

- セキュリティ管理者（後述）の指定
- オブジェクトを新規に作成する権限（オブジェクト作成権限）とすべてのオブジェクトに対する操作範囲（オブジェクト操作権限）のユーザ/グループ単位での指定
- オブジェクト生成時に付与されるデフォルトのパーミッションの指定

【セキュリティ管理者】

TOEの文書空間において、すべてのオブジェクトのアクセスに対してフルコントロールの特権を持つ、LDAPに登録されているユーザ。セキュリティ管理者として識別されたセッションは、オブジェクトのプロパティやコンテントの参照・更新など、オブジェクトに対して提供されているすべての操作を実行できる。

【文書管理ユーザ】

UAPからTOEの文書空間への接続要求の際に指定するLDAPに登録されているユーザ。TOEにおけるユーザとは識別・認証されたセッションである。識別・認証されたセッションに対して、オブジェクトのプロパティやコンテントの参照・更新の際にアクセス可否の判定が行われる。

1.2.4 TOEの機能

（1） 文書管理基盤としての機能

文書管理基盤ソフトウェアとしてTOEが提供する機能について以下に説明する。

【文書の登録機能】

文書の実体であるコンテント（Wordやテキストエディタなどのアプリケーションプログラムで作成された文書データのファイル）をデータベースに登録して一元管理することができる。

【バージョン管理機能】

コンテントを登録する際には、必要に応じて「Version1」や「Version2」などの版（バージョン）を付けて、文書の履歴を管理することができる。

【マルチレンディション管理機能】

コンテントと、その形式を表すレンディションタイプ（MIME形式）の情報をあわせて、レンディションと定義する。

文書には1個または複数のレンディションを登録して管理することができる。一つの文書に対して同じ内容を表す複数のレンディションを登録して管理する機能のことをマルチレンディション管理機能という。マルチレンディション管理機能は、一つの文書の内容を、対応するアプリケーションごとの複数の形式に変換した場合などに使用できる。

【コンテナ管理機能】

文書をまとめて格納するフォルダや、文書を分類するフォルダを利用して文書を管理できる。文書をまとめたり、分類したりするフォルダに相当するオブジェクトを、コンテナという。

コンテナには、複数の文書またはコンテナを関連づけることができる。コンテナを使用すると、複数の文書を目的に応じて一つにまとめて管理したり、一つの文書を複数の観点から分類して管理したりできる。また、コンテナとコンテナを関連づけることで、フォルダや分類に階層を持たせることもできる。

【文書間リレーション管理機能】

文書と文書を関連づけて管理する機能を、文書間リレーションという。文書間リレーションは、次のような場合に使用できる。

- 参考文献のある論文などの文書を、参考文献とともに管理したい場合
- 別文書として登録しているテキストと図データを関連がわかるように管理したい場合

【文書の属性情報の管理機能】

文書やコンテナなどのオブジェクトにさまざまな属性を付けて管理できる。この属性をプロパティという。プロパティには、DocumentBrokerによってあらかじめ定義されているプロパティ（システムプロパティ）と、文書管理システムで行う業務とUAPの設計によりシステム管理者が任意に追加定義するプロパティ（ユーザプロパティ）がある。例えば、文書を管理する場合、ユーザプロパティとして、「文書名」や「作成日時」などの標準的な属性情報だけでなく、「顧客名」や「競合他社名」などの業務に応じた属性情報も一緒に管理できる。文書やコンテナにプロパティを定義すると、プロパティをキーにしてオブジェクトを検索したり、プロパティの値を参照してオブジェクトの状態を確認したりできる。

【検索機能】

オブジェクトに設定されているプロパティの値を条件にした検索を実行できる、属性検索機能を提供する。プロパティの値を基に、文書、フォルダ、インデクスに相当するオブジェクトなどが検索できる。例えば、文書名と著者がプロパティとして設定されている場合に、「文書名が『報告書』であり、著者が『日立太郎』である文書を検索する」というような検索ができる。

【ファイル転送機能】

DocumentBroker Server（サーバ）とDocumentBroker Runtime（クライアント）を別のマシンで運用する場合、サーバとクライアント間のデータ転送に、このファイル転送機能を使用する。例えば、TOEで管理している文書のファイルをクライアントのマシンに取得したり、クライアントのマシン上にあるファイルをTOE管理下の文書として登録したりする場合に、ファイル転送が必要になる。

【複数の実行環境機能】

使用ユーザ数や単位時間当たりのトランザクション数の増加などによるシステム負荷を軽減するために、一つのデータベースに複数のDocumentBroker Serverの実行環境を配置したシステム構成を構築することができる。DocumentBroker Serverをスケールアウトするための機能である。これによって、システム負荷が複数のサーバ端末に分散されるため、システム全体の処理能力が向上する。なお、評価環境では、単一のサーバ端末で構成する。

（2） セキュリティ機能

TOEが提供するセキュリティ機能について以下に説明する。

【アクセス制御機能】

TOEが管理する文書空間に対してUAP下のDocumentBroker Runtimeから接続

が要求された場合、TOEは接続時に指定されたユーザ識別子とパスワードを使って、LDAP対応のディレクトリサービスへ識別･認証を要求する。これが成功するとTOEはUAPとのセッションを確立する。

TOEは、この識別・認証されたセッションに対して、文書空間上のオブジェクトに設定されたアクセス制御情報などから、セッションのアクセス権を判定してオブジェクトに対するアクセスを制御する。

識別・認証されたセッションは、オブジェクトの作成時にアクセス権を設定できる。例えば、文書に対してアクセス権を設定すると、アクセスを許可されていないセッションが誤って文書を更新してしまうようなことがなくなる。特定のユーザ識別子やグループ識別子を持つセッションだけに文書の参照や編集を許可する運用もできる。

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「DocumentBroker Server セキュリティターゲット バージョン1.02」（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、「DocumentBroker Server Version 3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。

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20年4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及び追加の保証コンポーネントASE_OBJ.2、ASE_REQ.2、ASE_SPD.1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 TOEの機能」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

1.5.4 脅威

本TOEは、表1-9に示す脅威を想定し、これに対抗する機能を備える。

表1-9　想定する脅威

識別子	脅　威
T.UNAUTHORIZED_OPERATION（許可されていない操作）	識別・認証されたセッションが、保護対象資産に対して許可されていない操作を行った結果、文書データ・文書プロパティの漏えいや改ざんが行われるかもしれない。

1.5.5 組織のセキュリティ方針

本TOEが想定する組織のセキュリティ方針はない。

1.5.6 構成条件

本TOEは、「1.2.3　TOEの範囲と動作概要」-「（１）TOEの動作環境と検証環境」

で示された、環境で動作する。

1.5.7 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1-10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1-10 TOE使用の前提条件

識別子	前提条件
A.ADMIN （管理者の適性）	システム管理者、セキュリティ運用者、及びセキュリティ管理者は、担当範囲の運用管理に関する知識・技術を備え、悪意のある行為を行わない。
A.PHYSICAL（サーバ機器の設置場所）	サーバエリア内の文書管理クライアント、文書管理サーバ、ディレクトリサーバの各端末、ファイアウォールとサーバエリアネットワークは、外部から物理的に隔離されたサーバエリアに設置され、システム管理者、セキュリティ運用者以外はそのエリアに入場できない。
A.NETWORK（サーバエリア外からのネットワークアクセス）	サーバエリア内の文書管理クライアント、文書管理サーバ、ディレクトリサーバの各端末とサーバエリアネットワークは、サーバエリア外からUAPを介した通信のみが行われるように構築される。
A.MANAGE （サーバ機器の管理）	サーバエリア内の文書管理クライアント、文書管理サーバ、ディレクトリサーバの各端末には、悪意のあるソフトウェアは存在しない。
A.USER_CONFIG（ユーザ情報と設定ファイルの管理）	LDAP 上で管理されているユーザ情報は、システム管理者により登録・変更・削除されている。文書管理サーバの OS 上で管理されているセキュリティ定義ファイルとユーザ権限定義ファイルの内容は、セキュリティ運用者により登録・変更・削除されている。

1.5.8 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表1-11に示す。

表1-11 TOEのガイダンス文書

文書名
DocumentBroker Version 3 システム導入・運用ガイド 3020-3-J14-10
DocumentBroker Version 3 メッセージ 3000-3-D07-10

DocumentBroker Version 3 統計解析ツール 3000-3-D06
DocumentBroker Version 3 システム導入・運用ガイド 3000-3-D01
DocumentBroker Version 3 メッセージ 3000-3-D07-20
DocumentBroker Version 3 統計解析ツール 3000-3-D06-10
取扱説明書 038413 R-15958-13 DocumentBroker Server Version 3 03-11 セキュリティ構築適用
取扱説明書 038414 R-1M958-13 DocumentBroker Server Version 3 03-11 セキュリティ構築適用
リリースノート　R-15958-13 03-11 DocumentBroker Server Version 3
リリースノート　R-1M958-13 03-11 DocumentBroker Server Version 3
梱包明細書
ソフトウェア製品別構成明細書
取扱説明書 037926 R-15958-13 DocumentBroker Server Version 3 03-11 電子マニュアル
取扱説明書 038141 R-1M958-13 DocumentBroker Server Version 3 03-11 電子マニュアル

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19年12月に始まり、平成20年4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～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（独立テストと侵入テスト）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

評価者の実施した評価者テストの概要を以下に示す。

2.3.1 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を図2-1に示す。

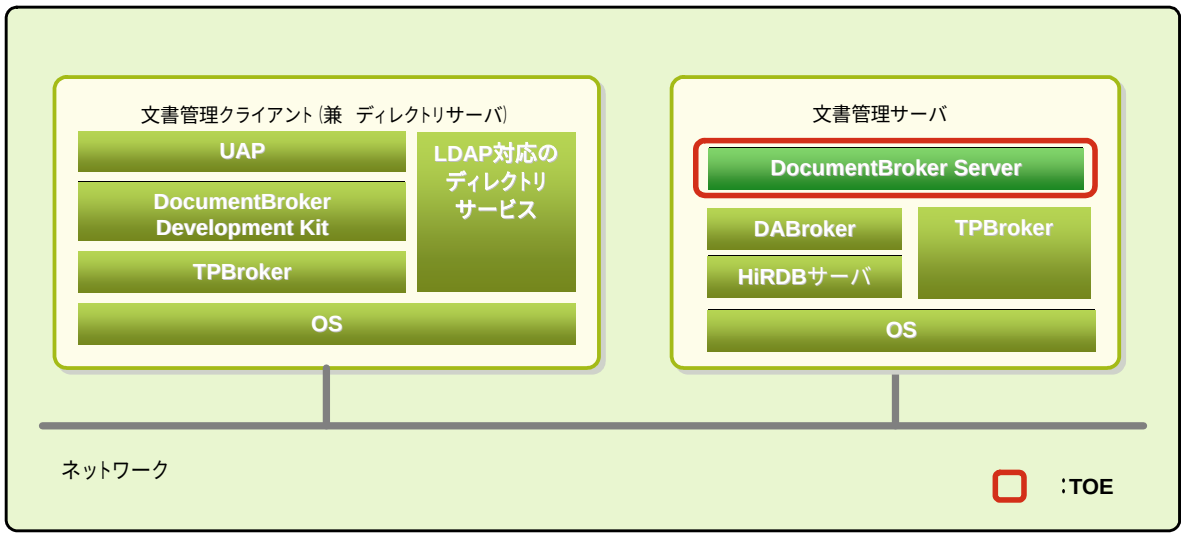

図2-1　評価者テストの構成

ハードウェア構成を表2-1から表2-3に示す。

表 2-1　文書管理サーバのハードウェア情報（TOEのIT環境がWindowsの場合）

項目	詳細
モデル名	FLORA 270W(MF2)
型名	PC8MF2-XNJJ5DAC0
CPU	Intel Core 2 Duo T7200 2.0GHz
HDD	80GB
メモリ	2GB

表 2-2　文書管理サーバのハードウェア情報（TOEのIT環境がAIXの場合）

項目	詳細
モデル名	EP8000/615
型名	THE-7029-6E32122
CPU	Power4 1.2GHz 2Way
HDD	140GB(外付け)
メモリ	4GB

表 2-3　文書管理クライアント兼ディレクトリサーバのハードウェア情報

項目	詳細
モデル名	FLORA 270W(MF2)

型名	PC8MF2-XNJJ5DAC0
CPU	Intel Core 2 Duo T7200 2.0GHz
HDD	80GB
メモリ	2GB

ソフトウェア構成は、「1.2.3 TOEの範囲と動作概要」の「表 1-6　検証した環境（TOEのIT環境がWindowsの場合)」、「表 1-7　検証した環境（TOEのIT環境がAIXの場合)」、「表-1 8　検証した環境（共通)」を使用した。

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。

①TOEが提供するインタフェース（TSFI）を利用しての機能テスト

具体的には以下の手法でテストを実施した。

- オブジェクト操作ツールを使用したテスト
- UAPを利用したテスト

c.実施テストの範囲

評価者が独自に考案した独立テストを71項目、侵入テストを5項目、計76項目のテストを実施した。(Windows版、AIX版それぞれで同一項目を実施)

テスト項目の選択基準として、下記を考慮している。

【独立テスト】

① インタフェースの重要性

オブジェクトに対する操作を許可するアクセス制御が、オブジェクトに対して設定された９つのパーミッションの値の組み合わせに基づいて行われていることを踏まえ､各パーミッションに関連する操作が網羅されるようにTSFIの選定を行う。

② インタフェースの利用頻度

UAP開発でよく利用されるメソッド、ほとんど利用されないメソッドを開発者にヒアリングし、これらをテストに含める。

【侵入テスト】

① 製品分類、関連製品等の公知の脆弱性情報の探索結果より分析し考案

② IPA公開情報（脆弱性チェックリスト）より分析し考案

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

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。

① 当該所見報告書でなされた指摘内容が妥当であること。
② 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。
③ 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。
④ 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。
⑤ 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及び追加の保証コンポーネントASE_OBJ.2、ASE_REQ.2、ASE_SPD.1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
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_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_SPD.1.1E	評価はワークユニットに沿って行われ、セキュリティ課題が明確に定義されていることを確認している。
ASE_OBJ.2.1E	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.2.1E	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、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。
ライフサイクルサポート	**適切な評価が実施された**
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。
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、SFR実施・SFR支援TSFIの目的と使用方法、パラメタが記載されて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。
ガイダンス文書	**適切な評価が実施された**
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。

テスト	適切な評価が実施された
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。
脆弱性評定	**適切な評価が実施された**
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
IT	Information Technology
PP	Protection Profile
SAR	Security assurance requirement
ST	Security Target
SFR	Security functional requirement
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functionality interface

本報告書で使用されたTOE特有の略語を以下に示す。

LDAP	Lightweight Directory Access Protocol(ディレクトリ・サービスに接続するために使用されるプロトコル)
UAP	User Application Program(ユーザアプリケーションプログラム)

本報告書で使用された用語を以下に示す。

アクセス権	オブジェクトを新規作成する権利と、既に作成されているオブジェクトを操作（オブジェクトのプロパティ参照、オブジェクトのコンテント更新など）する権利の総称。
アクセス制御情報	識別・認証されたセッションが文書オブジェクトを新規作成したり、既に作成されている文書オブジェクトにアクセスしたりするときに、アクセス可否の判定に使用される情報。アクセス権を付与するセッションの属性（ユーザ、グループ、など）とパーミッションの組として定義される。

	アクセス制御情報には、アクセス制御フラグ、アクセス制御リスト（ローカルACL、パブリックACL、セキュリティACL）がある。
オブジェクト作成権限	文書空間にオブジェクト（文書を含む）を作成する権利。ユーザ識別子単位またはグループ識別子単位で付与される。
オブジェクト操作権限	文書空間内の任意のオブジェクト（文書を含む）を操作する権利。操作種別には、オブジェクトのプロパティ参照、オブジェクトのコンテント更新、オブジェクトの削除などがあり、ユーザ識別子単位またはグループ識別子単位で付与される。
オブジェクト操作ツール	UAPの一例であり、DocumentBroker Development Kitに同梱される。
グループ識別子	ユーザ識別子に対応するグループ識別子を一意に識別するための文字列。LDAPに登録されている。
識別・認証されたセッション	TOEが提供する文書空間に対してUAPから接続が要求された場合、TOEは接続時に指定されたユーザ識別子とパスワードを使用して、LDAP対応のディレクトリサービスへ識別・認証を要求する。これが成功するとTOEはUAPとのセッションを確立する。この確立されたセッションのことを識別・認証されたセッションという。
セキュリティ定義ファイル	次に示すアクセス制御機能の運用に関する情報を定義するファイル。 ・ セキュリティ管理者 DocumentBroker Server に登録されたオブジェクトに対してフルコントロールアクセス権を付与するユーザ識別子を指定して登録 ・ ユーザ権限定義ファイル名 文書空間にオブジェクトを作成する権限や文書空間内のオブジェクトに対する操作の範囲を定義するために作成するファイルの名称 ・ デフォルトで設定されるパーミッション 新規にオブジェクトを作成した場合に、ACFlagに設定するパーミッション
パーミッション	許可される（実行可能な）操作の範囲を表す値であり、識別・認証されたセッションのユーザ権限または各文書のアクセス制御情報の中で定義される。パーミッションには、以下の基本となる操作権限とその組み合わせの操作権限がある。 ・ オブジェクト（文書を含む）の作成（オブジェクト作成権） ・ オブジェクト（文書を含む）の削除（基本削除権） ・ コンテントの更新（基本コンテント更新権）

- コンテントの参照（基本コンテント参照権）
- プロパティの更新（基本プロパティ更新権）
- プロパティの参照（基本プロパティ参照権）
- リンクに関する操作（基本リンク権）
- バージョンに関する操作（基本バージョン管理権）
- アクセス制御情報の変更（アクセス制御情報変更権）

文書オブジェクト	DocumentBroker上で文書を管理するための単位であり、文書データ（文書オブジェクトのコンテント）と文書プロパティ（文書オブジェクトのプロパティ）で構成される。文書オブジェクトに対するアクセスは、文書データと文書プロパティのそれぞれに対して制御できる。文書オブジェクトのことを単に文書と略すこともある。また、文書オブジェクトにはバージョンを管理できるバージョン付き文書オブジェクトと、バージョンを管理しないバージョンなし文書オブジェクトがある。バージョン付き文書オブジェクトの個々のバージョンは、バージョンなし文書オブジェクトとして扱うこともできる。
文書管理システム	組織や企業内に存在するマニュアルや仕様書といった、ワープロや表計算ソフトなどで作成された文書データを一元管理するためのシステム。
文書空間	一般的に１つの業務システム単位で使用される独立した空間。文書空間をまたがって共有される文書オブジェクトはない。
ユーザ権限	文書空間にオブジェクト（文書を含む）を作成する権利（オブジェクト作成権限）と、文書空間内の任意のオブジェクトに対する操作の範囲（オブジェクト操作権限）をユーザ識別子単位またはグループ識別子単位で定めるアクセス制御情報の一つで、ユーザ権限定義ファイルにより定義される。 セキュリティ運用者のみが、ユーザ権限定義ファイルを更新することでユーザ権限を変更できる。
ユーザ権限定義ファイル	ユーザ権限を定義するためのファイル。 セキュリティ定義ファイルに指定したユーザ権限定義ファイルにユーザ権限を定義する。
ユーザ識別子	セッションを一意に識別するための文字列。LDAPに登録されている。
ユーザ情報	LDAPで管理されているユーザ識別子、パスワード、グループ識別子。

6 参照

[1] DocumentBroker Server セキュリティターゲット バージョン 1.02（2008年3月11日）株式会社日立製作所

[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 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version　3.1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version　3.1 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 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] DocumentBroker Server Version 3 評価報告書 07004200-01-R003-02　2008年4月11日 みずほ情報総研株式会社　情報セキュリティ評価室