DocumentBroker Server
セキュリティターゲット

2008/03/11

Version 1.02

(株)日立製作所

「DocumentBroker Server セキュリティターゲット」

－ 変更歴 －

項番	作成／変更年月日	ST バージョン	更新内容 （概要）
1	2008/01/21	1.00	新規作成
2	2008/01/25	1.01	キックオフ会議の結果を反映
3	2008/03/11	1.02	OR ASE-006-01，ASE-007-01，ASE-008-01，評価者コメント，設計内コメントを反映

■ 商標類

Active Directory は，米国 Microsoft Corporation の，米国およびその他の国における登録商標または商標です。
AIX は，米国における米国 International Business Machines Corp.の登録商標です。
IBM は, 米国およびその他の国における International Business Machines Corporation の商標です。
Microsoft は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。
Microsoft Word は，米国 Microsoft Corp.の商品名称です。
SecureWay は，米国における米国 International Business Machines Corp.の登録商標です。
Sun，Sun Microsystems，Java は，米国 Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。
Tivoli は，米国における米国 International Business Machines Corp.の登録商標です。
Windows は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。
Windows Server は，米国 Microsoft Corporation の米国およびその他の国における登録商標です。
その他記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■ 著作権

「DocumentBroker Server セキュリティターゲット」

－ 目次 －

1. ST 概説

本章では，ST 参照，TOE 参照，TOE 概要，および TOE 記述について記述する。

1.1. ST 参照

ST 名称	:	DocumentBroker Server セキュリティターゲット
バージョン	:	1.02
発行日	:	2008 年 3 月 11 日
作成者	:	株式会社　日立製作所　ソフトウェア事業部

1.2. TOE 参照

TOE	:	DocumentBroker Server Version 3
TOE バージョン	:	03
TOE リビジョン	:	11
キーワード	:	文書管理，電子文書管理，アクセス制御
開発者	:	株式会社　日立製作所

1.3. TOE 概要

1.3.1. TOE の種別およびセキュリティ機能

(1) TOE 種別

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(2)に示すセキュリティ機能を提供する。

- 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

(2) セキュリティ機能

TOE が提供するセキュリティ機能の概要を以下に示す。

【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。

1.3.2. TOE の動作環境

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。

想定する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。

図 1-1及び表 1-1に記載される構成要素については，1.4.1項も参照のこと。

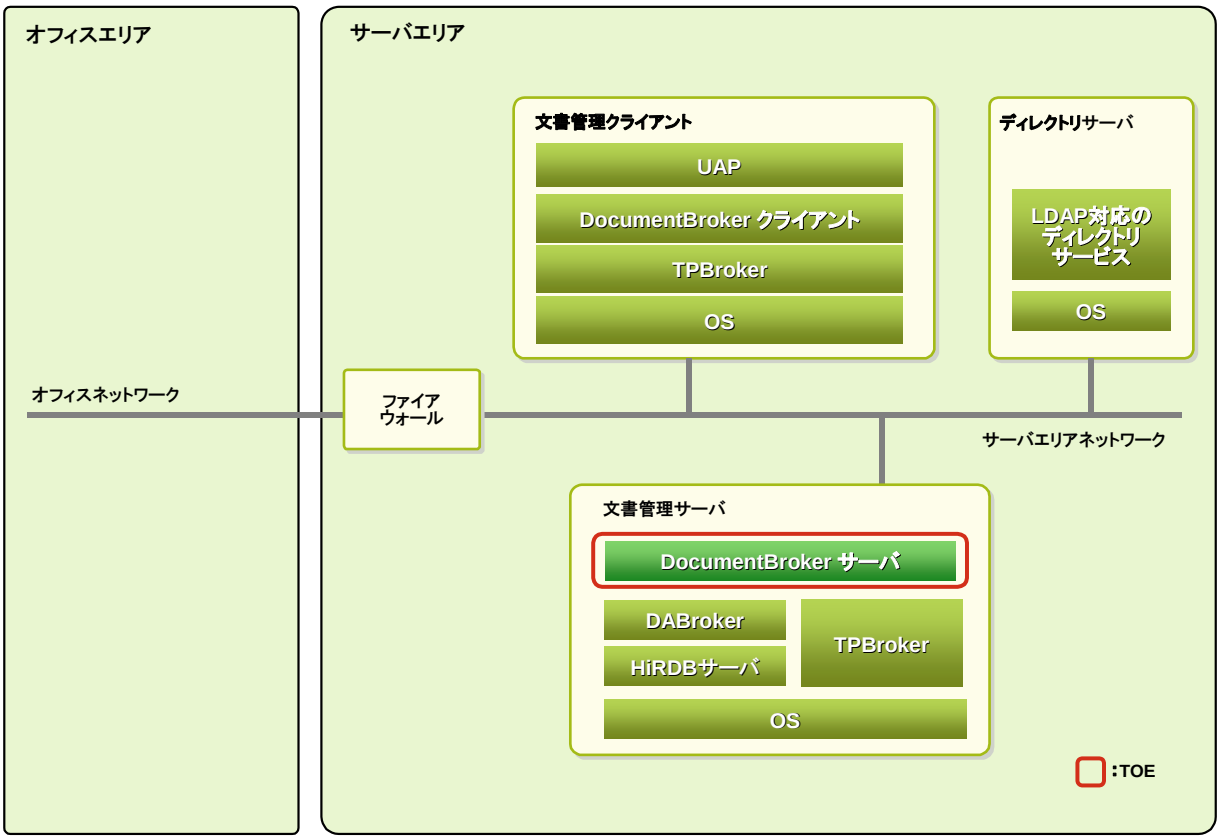

図 1-1　TOE を含む文書管理システムのシステム構成図

文書管理システムを構築するために必要な構成要素を以下に示す。

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以下に示す。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 および 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。）

1.4. TOE 記述

本章では，TOE の利用方法の概要を示し，TOE の構成要素，TOE が提供する機能，TOE が動作するために運用環境に必要な機能について記述する。また，TOE とその運用環境の関係者と保護対象資産について定義する。

1.4.1. TOE の利用方法

以下に，図 1-1を元にシステムを構成する各要素について説明する。

【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。

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は下記のとおりである。

表 1-6 検証した環境（TOE の IT 環境が Windows の場合）

端末	ソフトウェア名称およびバージョン・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/Singel 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	ソフトウェア名称およびバージョン・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/Singel Server Version 8 08-03

	AIX 5L V5.3

表 1-8 検証した環境（共通）

端末	ソフトウェア名称およびバージョン・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)

1.4.2. TOE の構成

TOEは表 1-1においてTOEとして示したソフトウェアと付属のガイダンス文書で構成される。TOEの構成要素を以下に示す。

表 1-9 TOE を構成するソフトウェア

ソフトウェア名称	バージョン番号ーリビジョン番号
DocumentBroker Server Version 3	03-11

表 1-10 TOE を構成するガイダンス文書

文書名
DocumentBroker Version 3　システム導入・運用ガイド 解説・手引書
DocumentBroker Version 3　統計解析ツール 文法書
DocumentBroker Version 3　メッセージ 操作書
DocumentBroker Server Version 3 03-11　リリースノート
取扱説明書　電子マニュアル
取扱説明書　セキュリティ構築適用

1.4.3. TOE が提供する機能

(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。

1.4.4. 運用環境が提供する機能

TOE が提供する機能が動作するために，運用環境によって提供される機能について以下に説明する。

【ディレクトリサービス（LDAP)】

LDAP は，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，その識別・認証の成功/失敗を応答する。識別・認証に成功した場合は，そのユーザ識別子に対応するグループ識別子を応答する。

LDAP に登録されているユーザ識別子，グループ識別子，パスワードは，システム管理者によって適切に管理・運用されており，識別・認証データは信頼できる。

1.4.5. TOE および運用環境の関係者の役割

TOE とその運用環境の関係者の役割を以下に説明する。

【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 および 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。以下のような作業を行う。

- 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。

1.4.6. 保護対象資産

本 TOE が保護対象とするデータは文書オブジェクトである。文書オブジェクトの詳細は以下のとおりである。

(1) 文書データ（文書オブジェクトのコンテント）

文書オブジェクトのコンテントとして，TOE の管理下にあるデータ。UAP からファイルがアップロードされることにより TOE の管理下に入り，ダウンロードされた複製は TOE の管理下から外れる。

(2) 文書プロパティ

文書オブジェクトを管理するための属性情報。以下の情報がある。

① DocumentBroker によってあらかじめ定義されているオブジェクト制御用のシステムプロパティ。オブジェクトを特定するための識別子がある。

② DocumentBroker によってあらかじめ定義されているアクセス制御用のシステムプロパティ。オブジェクトの所有者を示す識別子やパーミッションがある。

③ 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）。ユーザプロパティの例には，「文書名」や「作成日時」などの標準的な属性情報や「顧客名」や「競合他社名」などの業務に応じた属性情報がある。

2. 適合主張

2.1. CC 適合主張

本 ST が適合主張する CC は以下のとおり。

- ST が適合主張する CC のバージョン
  パート 1： 概説と一般モデル 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
  パート 2： セキュリティ機能コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
  パート 3： セキュリティ保証コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版

- CC パート 2 に対する適合
  CC パート 2 適合

- CC パート 3 に対する適合
  CC パート 3 適合

2.2. PP 主張，パッケージ主張

2.2.1. PP 主張

本 ST が適合主張する PP はない。

2.2.2. パッケージ主張

本 ST は EAL1 追加である。
追加されるセキュリティ保証要件は，ASE_SPD.1，ASE_OBJ.2，ASE_REQ.2 である。

3. セキュリティ課題定義

本章では、脅威，組織のセキュリティポリシー，および前提条件について記述する。

3.1. 脅威

本 TOE が想定する脅威を以下に示す。

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。

3.2. 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。

3.3. 前提条件

本 TOE が想定する前提条件を以下に示す。

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。

4. セキュリティ対策方針

本章では、TOE のセキュリティ対策方針および運用環境のセキュリティ対策方針について記述する。

4.1. TOE のセキュリティ対策方針

本 TOE が達成しなければならないセキュリティ対策方針を以下に示す。

O.ACCESS

TOE は，識別・認証されたセッションによる許可範囲外の操作を防ぐために、保護対象資産に対するアクセス制御を行う。

O.MANAGE

TOE は，権限を付与されたセッションのみが各文書に付与されるアクセス制御情報を登録・変更できるように制限する。

4.2. 運用環境のセキュリティ対策方針

本 TOE の運用環境が達成しなければならないセキュリティ対策方針を以下に示す。

OE.ADMIN

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と信頼できる人物をシステム管理者，セキュリティ運用者，及びセキュリティ管理者に選定する。

OE.PHYSICAL

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する。また，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ように管理する。

OE.NETWORK

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がサーバエリア外から UAP を介した通信のみが行えるように構築する。

OE.MANAGE

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，TOE が動作するために必要なソフトウェアを適切にインストールし，悪意のあるソフトウェアをインストールされないように管理する。

OE.USER_CONFIG

システム管理者は，LDAP 上で管理されているユーザ情報を登録・変更・削除する。また，セキュリティ運用者は，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を登録・変更・削除する。

4.3. セキュリティ対策方針根拠

セキュリティ対策方針と対応する脅威・前提条件の対応関係を表 4-1に示す。

表 4-1 セキュリティ対策方針と対応する脅威・前提条件

セキュリティ課題定義 / セキュリティ対策方針	T.UNAUTHORIZED_OPERATION	A.ADMIN	A.PHYSICAL	A.NETWORK	A.MANAGE	A.USER_CONFIG
O.ACCESS	○					
O.MANAGE	○					
OE.ADMIN		○				

OE.PHYSICAL			○			
OE.NETWORK				○		
OE.MANAGE					○	
OE.USER_CONFIG						○

表 4-1に示すとおり、各セキュリティ対策方針は１つ以上の脅威または前提条件に対応している。

次に、各脅威がセキュリティ対策方針により対抗され，各前提条件がセキュリティ対策方針により充足している根拠を示す。

＜脅威＞

T.UNAUTHORIZED_OPERATION

この脅威に対抗するためには，各文書データに対して許可されたセッションが許可された操作の範囲でしか，その文書データにアクセスできないように制御する必要がある。このため，TOE は，セッションによる文書データへの各種のアクセスを制御すること（**O.ACCESS**）が必要である。

さらに，このアクセス制御の対策（**O.ACCESS**）が効果を発揮するためには，セッションに割り付けられるユーザ情報及び権限情報と，各文書に付与するアクセス制御情報が不正に操作されないようにする必要がある。

前者については，LDAP 上に格納されるユーザ情報と文書管理サーバの OS 上に格納される設定ファイルが許可された信頼できる人物により運用管理されており（A.ADMIN，A.USER_CONFIG），許可されていない人物・機器によって不正に変更されない（A.PHYSICAL，A.NETWORK）という前提により満たされている。したがって，後者のために，権限を付与された人物のみに各文書のアクセス制御情報を操作できるように TOE が制限（**O.MANAGE**）すれば，その不正操作を防ぐことができる。

以上により，**T.UNAUTHORIZED_OPERATION** は **O.ACCESS** および **O.MANAGE** により適切に対抗できる。

＜前提条件＞

A.ADMIN

OE.ADMIN は **A.ADMIN** の表現を対策方針としての表現に修正しただけで，明らかに同じ内容を意味している。したがって，**A.ADMIN** は **OE.ADMIN** によって適切に充足できる。

A.PHYSICAL

OE.PHYSICAL は **A.PHYSICAL** の表現を対策方針としての表現に修正しただけで，明らかに同じ内容を意味している。したがって，**A.PHYSICAL** は **OE.PHYSICAL** によって適切に充足できる。

A.NETWORK

OE.NETWORK は **A.NETWORK** の表現を対策方針としての表現に修正しただけで, 明らかに同じ内容を意味している。したがって，**A.NETWORK** は **OE.NETWORK** によって適切に充足できる。

A.MANAGE

OE.MANAGE は **A.MANAGE** の表現を対策方針としての表現に修正しただけで，明らかに同じ内容を意味している。したがって，**A.MANAGE** は **OE.MANAGE** によって適切に充足できる。

A.USER_CONFIG

OE.USER_CONFIG は，TOE が導入された文書管理システムのユーザ及び権限の管理について，その文書管理システムの方針にしたがって，システム管理者及びセキュリティ運用者が管理することを意味している。したがって，**A.USER_CONFIG** は **OE.USER_CONFIG** によって適切に充足できる。

5. 拡張コンポーネント定義

本 ST は，拡張コンポーネントを定義しない。

6. セキュリティ要件

本章では、セキュリティ要件について記述する。

6.1. セキュリティ機能要件

本節では，TOE が備えるべきセキュリティ機能要件を記述する。なお，すべてのセキュリティ機能要件に CC パート 2 のセキュリティ機能コンポーネントを使用する。

FDP_ACC.1　サブセットアクセス制御

下位階層:　なし
依存性:　**FDP_ACF.1** セキュリティ属性によるアクセス制御

FDP_ACC.1.1　TSF は、[割付: *サブジェクト、オブジェクト、および SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: サブジェクト、オブジェクト、およびSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]

サブジェクト	オブジェクト	操作
識別・認証されたセッション	文書	・ 文書の作成 ・ 文書の削除 ・ コンテントの参照 ・ コンテントの更新 ・ プロパティの参照 ・ プロパティの更新 ・ リンクに関する操作 ・ バージョンに関する操作

[割付: アクセス制御SFP]
DocumentBrokerアクセス制御方針

FDP_ACF.1　セキュリティ属性によるアクセス制御

下位階層:　なし
依存性:　**FDP_ACC.1** サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1.1　TSF は、以下の[割付: *示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御 SFP*]を実施しなければならない。

[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]

	サブジェクト	サブジェクト属性	オブジェクト	オブジェクト属性
1	識別・認証されたセッション	・ ユーザ ・ グループ ・ 特権 ・ ユーザ権限	文書	アクセス制御情報

[割付: アクセス制御SFP]
DocumentBrokerアクセス制御方針

FDP_ACF.1.2　TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: *制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

a) サブジェクトが特権をもつ場合，任意の文書に対して，すべての操作を許可する。
b) サブジェクトがユーザ権限をもつ場合，任意の文書に対して，そのユーザ権限の範囲の操作を許可する。
c) 文書に設定されたアクセス制御情報において，サブジェクトのユーザ識別子またはグループ識別子に対して，その文書に要求された操作のパーミッションを付与している場合，その文書に

要求された操作を許可する。

FDP_ACF.1.3 TSF は、次の追加規則、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]

なし

FDP_ACF.1.4 TSF は、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]

なし

FIA_ATD.1 利用者属性定義

下位階層: なし
依存性: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。: [割付: *セキュリティ属性のリスト*]

[割付：セキュリティ属性のリスト]

- ユーザ
- グループ
- 特権
- ユーザ権限

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし
依存性: **FIA_ATD.1** 利用者属性定義

FIA_USB.1.1 TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。: [割付: *利用者セキュリティ属性のリスト*]

[割付：利用者セキュリティ属性のリスト]
- ユーザ
- グループ
- 特権
- ユーザ権限

FIA_USB.1.2 TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しけなければならない。: [割付: *属性の最初の関連付けの規則*]

[割付：属性の最初の関連付けに関する規則]
- LDAPによる識別・認証に成功した「ユーザ識別子」をユーザ属性に設定する。
- 識別・認証成功時にLDAPから受信した「グループ識別子」をグループ属性に設定する。
- サブジェクトのユーザ識別子がセキュリティ管理者としてセキュリティ定義ファイルに定義されている場合は「セキュリティ管理者」を，定義されていない場合は「なし」を，特権属性として設定する。
- サブジェクトのユーザ識別子またはグループ識別子に対するパーミッションがユーザ権限定義ファイルに定義されている場合はその「パーミッション」を，定義されていない場合は「なし」を，ユーザ権限属性として設定する。

FIA_USB.1.3 TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *属性の変更の規則*]

[割付：属性の変更に関する規則]
なし

FMT_SMR.1 セキュリティ役割

下位階層: なし
依存性: **FIA_UID.1** 識別のタイミング

FMT_SMR.1.1 TSF は、役割[割付: *許可された識別された役割*]を維持しなければならない。

[割付: 許可された識別された役割]
- セキュリティ管理者
- 所有者
- アクセス制御情報変更権保持者

FMT_SMR.1.2 TSF は、利用者を役割に関連付けなければならない。

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし
依存性: [**FDP_ACC.1** サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

FMT_MSA.1.1 TSF は、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更, 問い合わせ, 改変, 削除,* [割付: *その他の操作*]]をする能力を[割付: *許可された識別された役割*]に制限する[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。

上述の割付および選択を下表に示す。

[割付: セキュリティ属性のリスト]	[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]	[割付: 許可された識別された役割]	[割付: アクセス制御SFP、情報フロー制御SFP]
アクセス制御情報（アクセス制御情報変更権）	改変	・ セキュリティ管理者 ・ 所有者	DocumentBroker アクセス制御方針
アクセス制御情報（上記以外）	改変	・ セキュリティ管理者 ・ 所有者 ・ アクセス制御情報変更権保持者	

FMT_MSA.3　静的属性初期化

下位階層:　なし
依存性:　**FMT_MSA.1** セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

FMT_MSA.3.1　TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択(以下の中から一つのみ): *制限的, 許可的, [割付: その他の特性]*]デフォルト値を与える[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]を実施しなければならない。

[選択(以下の中から一つのみ): 制限的, 許可的, [割付: その他の特性]]
[割付: その他の特性]: セキュリティ定義ファイルに定義される

[割付: アクセス制御SFP、情報フロー制御SFP]
DocumentBrokerアクセス制御方針

FMT_MSA.3.2　TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

[割付: 許可された識別された役割]
- 所有者

FMT_SMF.1　管理機能の特定

下位階層：　なし
依存性：　なし

FMT_SMF.1.1　TSF は、以下の管理機能を実行することができなければならない。: [割付: *TSF によって提供される管理機能のリスト*]

[割付： TSF によって提供されるセキュリティ管理機能のリスト]

表 6-1 TSF によって提供されるセキュリティ管理機能のリスト

機能要件	管理要件	管理項目
FDP_ACC.1	－	－
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	文書に付与されたアクセス制御情報の改変
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし（利用者に対する追加のセキュリティ属性はない）
FIA_USB.1	・ 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 ・ 許可管理者は、サブジェクトのセキュリティ属性を変更できる。	・ なし（サブジェクトのセキュリティ属性にデフォルト値はない） ・ なし（サブジェクトの所有者属性は文書へのアクセス時に決定され変更されず，その他のセキュリティ属性はTOE外の機能を使用して変更される）
FMT_SMR.1	役割の一部をなす利用者のグループの管理。	アクセス制御情報変更権保持者の登録・変更
FMT_MSA.1	セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	アクセス制御情報変更権保持者の登録・変更
FMT_MSA.3	・ 初期値を特定できる役割のグループを管理すること。 ・ 所定のアクセス制御SFPに対するデフォルト値の許可的あるいは制限的設定を管理すること。	・ なし（代替の初期値を特定できる役割は固定である） ・ なし（デフォルト値はTOE外の機能を使用して管理される）

6.2. セキュリティ保証要件

本節では，TOE が保証するセキュリティ保証要件を記述する。

本 TOE の評価保証レベルは EAL1 であり、追加する保証要件は ASE_SPD.1，ASE_OBJ.2，ASE_REQ.2 である。すべてのセキュリティ保証要件に CC パート 3 のセキュリティ保証コンポーネントを使用する。セキュリティ保証要件の一覧を以下に示す。

表 6-2 セキュリティ保証要件一覧

保証クラス	セキュリティ保証要件	
開発（ADV クラス）	**ADV_FSP.1**	基本機能仕様
ガイダンス文書（AGD クラス）	**AGD_OPE.1**	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ライフサイクルサポート（ALC クラス）	**ALC_CMC.1**	TOE のラベル付け
	ALC_CMS.1	TOE の CM 範囲
セキュリティターゲット評価（ASE クラス）	**ASE_CCL.1**	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	導き出されたセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE 要約仕様
テスト（ATE クラス）	**ATE_IND.1**	独立テスト － 準拠
脆弱性評定（AVA クラス）	**AVA_VAN.1**	脆弱性調査

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

本 ST で選択した TOE および IT 環境のセキュリティ機能要件とセキュリティ対策方針の対応関係を表 8-2 に示す。

表 6-3 セキュリティ機能要件とセキュリティ対策方針の対応関係

TOE のセキュリティ対策方針 ＼ セキュリティ機能要件	**O.ACCESS**	**O.MANAGE**
FDP_ACC.1	○	
FDP_ACF.1	○	
FIA_ATD.1	○	
FIA_USB.1	○	

FMT_SMR.1		○
FMT_MSA.1		○
FMT_MSA.3		○
FMT_SMF.1		○

表 6-3により、TOEの各セキュリティ機能要件は、1 つ以上のTOEセキュリティ対策方針に対応している。また、IT環境の各セキュリティ機能要件は、1 つ以上のIT環境のセキュリティ対策方針に対応している。

次に、TOE の各セキュリティ対策方針が、TOE のセキュリティ機能要件で実現できることを説明する。

O.ACCESS

このセキュリティ対策方針を実現するためには，識別・認証されたセッションから文書に対して要求された操作について，そのセッションに固有のセキュリティ属性と各文書に付与されたセキュリティ属性とを使用して，許可範囲外の操作を防ぐアクセス制御を行うことが必要である。

このためにまず，TOE は識別・認証されたセッションに対してそのセッション固有のサブジェクト属性を関連付ける（**FIA_ATD.1**，**FIA_USB.1**）。

次に，TOE は識別・認証されたセッションと文書との間の許可範囲外の操作を防ぐために，前述のとおりセッションに関連付けられたセキュリティ属性と操作対象の文書に関連付けられたセキュリティ属性を使用したアクセス制御規則に基づいてアクセス制御を行う（**FDP_ACC.1**，**FDP_ACF.1**）。

したがって，**O.ACCESS** は，**FIA_ATD.1**，**FIA_USB.1**，**FDP_ACC.1** および **FDP_ACF.1** により適切に実現できる。

O.MANAGE

TOE は，権限を付与されたセッションのみが各文書に付与されるアクセス制御情報を登録・変更できるように制限する。

このセキュリティ対策方針を実現するためには，アクセス制御情報を変更する権限をもつセッション以外はアクセス制御情報を変更できないように制限する。

このために，文書に付与されるアクセス制御情報の変更は，特権であるセキュリティ管理者，その文書の所有者，及びその文書のアクセス制御情報変更権のいずれかの役割を付与されたセッションに対してのみ許可する（**FMT_SMR.1**，**FMT_MSA.1**，**FMT_MSA.3**，**FMT_SMF.1**）。

したがって，**O.MANAGE** は，**FMT_SMR.1**，**FMT_MSA.1**，**FMT_MSA.3** および **FMT_SMF.1** により適切に実現できる。

6.3.2. セキュリティ機能要件依存性

セキュリティ機能要件のコンポーネントの依存性を表 6-4に示す。

表 6-4 セキュリティ要件のコンポーネントの依存性

セキュリティ機能要件	CC Part2 で規定されている依存コンポーネント	本 ST で選択したコンポーネント	依存性の充足
FDP_ACC.1	**FDP_ACF.1**	**FDP_ACF.1**	○
FDP_ACF.1	**FDP_ACC.1**	**FDP_ACC.1**	○
	FMT_MSA.3	**FMT_MSA.3**	○
FIA_ATD.1	なし	－	○
FIA_USB.1	**FIA_ATD.1**	**FIA_ATD.1**	○
FMT_SMR.1	**FIA_UID.1**	－	※
FMT_MSA.1	**FDP_ACC.1** または **FDP_IFC.1**	**FDP_ACC.1**	○
	FMT_SMF.1	**FMT_SMF.1**	○
	FMT_SMR.1	**FDP_SMR.1**	○
FMT_MSA.3	**FMT_MSA.1**	**FMT_MSA.1**	○
	FMT_SMR.1	**FMT_SMR.1**	○
FMT_SMF.1	なし	－	○

※TSF の制御対象は LDAP により識別・認証されたセッションであり，FMT_SMR.1 に必要な識別は既に行われているため，TOE 自体がこの依存関係を満たす必要はない。

以上により，各セキュリティ機能要件は必要な依存関係をすべて満たしている。

6.3.3. セキュリティ保証要件根拠

本TOEは，第 2 章および「3.3前提条件」の記述のとおり，物理的に保護されたエリアに設置され，ファイアウォールなどにより保護されたネットワーク上に接続され，信頼できる人物により適切に運用管理されている運用環境の下で，通常のオフィスエリアにいる一般的な従業員などの行為に起因する脅威にさらされている状況を想定している。

このように保護された運用環境下での低レベルな攻撃を想定しているため，本 TOE のセキュリティ保証要件 EAL1＋ASE_SPD.1＋ASE_OBJ.2+ASE_REQ.2 は妥当である。

7. TOE 要約仕様

本章では，TOE が提供するセキュリティ機能の仕様を概説する。

7.1. TOE のセキュリティ機能と SFR の対応関係

TOE の各セキュリティ機能要件とそれぞれを実現するセキュリティ機能との関係を以下に示す。なお，各セキュリティ機能の要約仕様は以降の節に記述する。

表 7-1 TOE セキュリティ機能とセキュリティ機能要件の対応関係

セキュリティ機能要件 / TOE セキュリティ機能	FDP_ACC.1	FDP_ACF.1	FIA_ATD.1	FIA_USB.1	FMT_SMR.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1
SF.ACCESS	○	○	○	○				
SF.MANAGE					○	○	○	○

7.2. アクセス制御機能 (SF.ACCESS，SF.MANAGE)

【アクセスコントロール】 （FIA_ATD.1，FIA_USB.1，FDP_ACC.1，FDP_ACF.1）

TOE が提供する文書空間において，文書オブジェクトの作成や管理されている文書オブジェクトに対する操作を，設定されたアクセス制御情報にしたがい，識別・認証されたセッションに対して，ユーザ識別子やグループ識別子単位で許可または制限する。

文書オブジェクトのプロパティを参照する場合，次の順序でアクセス許可の判定を行う。なお，アクセス許可の判定前に，サブジェクト属性を取得する。

(1) 識別･認証されたセッションがセキュリティ管理者属性を持っていれば，アクセスを許可する。
(2) 識別・認証されたセッションにオブジェクト操作権限として基本プロパティ参照権が許可されていれば，アクセスを許可する。
(3) 文書オブジェクトに設定されている，所有者／プライマリグループ／全てのユーザに対するアクセス権限を判定し，基本プロパティ参照権が許可されていれば，アクセスを許可する。
(4) 文書オブジェクトと関連付けられているパブリック ACL オブジェクトを取得し，パブリック ACL オブジェクトに設定されているアクセス権を判定して，基本プロパティ参照権が許可され

ていれば，アクセスを許可する。

(5) 文書オブジェクトのローカル ACL を取得し，ローカル ACL に設定されているアクセス権を判定して，基本プロパティ参照権が許可されていれば，アクセスを許可する。

(6) (1)～(5)までの判定に全て失敗した場合，識別・認証されたセッション対してエラーを返信する。

文書オブジェクトのコンテントのダウンロード（基本コンテント参照権）・アップロード（基本コンテント更新権），ユーザプロパティなど各種プロパティの更新（基本プロパティ更新権），コンテナや文書間の関連付けの設定・解除（基本リンク権），チェックアウト・チェックインなどのバージョン操作（基本バージョン管理権），オブジェクトの削除（基本オブジェクト削除権）ついても，上記の判定方法に従う。

【パーミッション】 （FDP_ACC.1，FDP_ACF.1，FMT_MSA.1）

個々のオブジェクトに対する操作を許可するアクセス権限は表 7-2に示す基本パーミッションを用いる。オブジェクトに設定されるアクセス権限はこのパーミッションの論理和である。

表 7-2 基本パーミッションの種類

パーミッションの名称	説明
基本プロパティ参照権	プロパティの参照を許可する
基本プロパティ更新権	プロパティの更新を許可する
基本コンテント参照権	文書のコンテントの参照を許可する
基本コンテント更新権	文書のコンテントの更新を許可する
基本リンク権	リンクに関する操作を許可する
基本バージョン管理権	バージョンに関する操作を許可する
基本オブジェクト削除権	オブジェクトの削除を許可する

基本プロパティ参照権は，そのほかの基本パーミッションにも含まれる。したがって，基本プロパティ参照権以外の基本パーミッションを指定すると，各基本パーミッションで許可される操作に加えて，オブジェクトのプロパティの参照が許可される。

また，これらのほかに，オブジェクトのセキュリティ ACL に設定される「アクセス制御情報変更権」，ユーザ権限定義ファイルに記述される「オブジェクト作成権」がある。

【アクセス制御情報の保護】 （FMT_SMR.1，FMT_MSA.1，FMT_MSA.3，FMT_SMF.1）

オブジェクトに設定されたアクセス制御情報を示すプロパティの変更は，オブジェクトの所有者，セキュリティ管理者，またはセキュリティ ACL でアクセス制御情報変更権を与えられた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。なお，オブジェクト生成時のデフォルトのアクセス制御情報はセキュリティ定義ファイルに設定されており，オブジェクト生成時にあわせて指定すること

もできる。

また，オブジェクトのセキュリティ ACL に設定された「アクセス制御情報変更権」の変更は，オブジェクトの所有者属性またはセキュリティ管理者属性と一致するセッションに制限する。

8. 参考資料・用語

8.1. 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2006 Version3.1 Revision1 CCMB-2006-09-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2006 Version3.1 Revision1 CCMB-2006-09-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2006 Version3.1 Revision1 CCMB-2006-09-003
- Common Methodology for Information Technology Security Evaluation Evaluation Methodology September 2006 Version3.1 Revision1 CCMB-2006-09-04
- 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 2006 年 9 月 バージョン 3.1 改訂第 1 版 CCMB-2006-09-001 平成 19 年 3 月翻訳第 1.2 版 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
- 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 : パート 2 : セキュリティ機能コンポーネント 2006 年 9 月 バージョン 3.1 改訂第 1 版 CCMB-2006-09-002 平成 19 年 3 月翻訳第 1.2 版 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
- 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 2006 年 9 月 バージョン 3.1 改訂第 1 版 CCMB-2006-09-003 平成 19 年 3 月翻訳第 1.2 版 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
- 情報技術セキュリティ評価のための共通方法 評価方法 2006 年 9 月 バージョン 3.1 改訂第 1 版 CCMB-2006-09-004 平成 19 年 3 月翻訳第 1.2 版 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

8.2. 用語

8.2.1. 本 ST における用語

用語	定義内容
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。
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。
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。
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。
アクセス制御フラグ（ACFlag）	オブジェクトのプロパティとして設定される。以下のそれぞれに該当するセッションのアクセス権をオブジェクトに対して設定可能。 ・ オブジェクトの所有者 ・ プライマリグループ ・ すべてのユーザ
アクセス制御リスト（ACL）	ユーザ識別子またはグループ識別子ごとにパーミッションを設定してアクセス権を与えるためのリスト。アクセス制御対象オブジェクトに付与

	されるアクセス制御情報の一部として使用される。ACL は，設定されるオブジェクトや用途によって，次の 3 種類に分けられる。 ・ローカル ACL ・パブリック ACL ・セキュリティ ACL ACL は，アクセス制御エレメント（ACE）のリストで構成される。
アクセス制御エレメント（ACE）	一つのサブジェクトと一つのパーミッションの組で構成され，指定されたサブジェクトに対して指定されたパーミッションの範囲のアクセス権を与えることを示す情報。アクセス制御リスト（ACL）の構成要素。
ローカル ACL	アクセス制御対象オブジェクトごとのアクセス権を設定するためのアクセス制御リスト（ACL)。ローカル ACL は，アクセス制御対象オブジェクトのプロパティとして，アクセス制御対象オブジェクトに一つだけ設定される。アクセス制御エレメント（ACE）の形式で，指定したユーザ識別子またはグループ識別子に対してオブジェクト作成権とアクセス制御情報変更権を除いたパーミッションを設定できる。
パブリック ACL	複数のオブジェクトに対して同じアクセス制御情報を設定したい場合に使用するアクセス制御リスト（ACL)。ローカル ACL とセキュリティ ACL をプロパティとして持ち，独立したオブジェクトとして文書空間に作成し，複数のオブジェクトに適用したい ACL をローカル ACL に設定しておく。複数の文書やコンテナからパブリック ACL を参照することで，そのパブリック ACL に設定された ACL を適用できる。 ローカル ACL の変更は，パブリック ACL の所有者，セキュリティ管理者，またはセキュリティ ACL でアクセス制御情報変更権を与えられた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。また，セキュリティ ACL の変更は，パブリック ACL の所有者，セキュリティ管理者と一致するセッションに制限する。
セキュリティ ACL	オブジェクトに設定されたアクセス制御情報の変更権限（アクセス制御情報変更権）を制御するためのアクセス制御リスト（ACL)。セキュリティ ACL は，アクセス制御対象オブジェクトのプロパティとして，アクセス制御対象オブジェクトに一つだけ設定される。アクセス制御エレメント（ACE）の形式で，指定したユーザ識別子またはグループ識別子に対してアクセス制御情報変更権を設定できる。
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。
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。
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。
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）
リンクに関する操作	コンテナや文書間のリンク（関連付け）に関する以下の操作のこと。 ・ リンクの設定 ・ リンクの解除 ・ リンクに対するプロパティの設定
バージョンに関する操作	バージョン付き文書に関する以下の操作のこと。 ・ チェックアウト ・ チェックイン ・ チェックアウトの取り消し ・ バージョンの削除
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。
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
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，この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。
所有者	文書が DocumentBroker に登録された時にその所有者属性に設定されているユーザ識別子と一致するユーザ識別子を持つセッション。このユーザ識別子をもつセッションは，セキュリティ ACL を変更して，文書のアクセス制御情報を変更する権限をユーザやグループに付与することができる。 セッションが文書へアクセスする時にセッションのユーザ識別子が文書の所有者属性と一致するかどうかによって判定される。
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。
サブジェクト	識別・認証されたセッション。識別・認証されたユーザ識別子とユーザ識別子と関連付けて登録されているグループ識別子により識別される。
アクセス制御情報変更権保持者	セキュリティ ACL によってアクセス制御情報変更権を付与されたユーザ識別子またはグループ識別子と一致するこれらの識別子を持つセッション。

8.2.2. 略語

<CC 関連略語>

CC（Common Criteria）：コモンクライテリア

EAL（Evaluation Assurance Level）：評価保証レベル

IT（Information Technology）：情報技術

PP（Protection Profile）：プロテクションプロファイル

SAR（Security Assurance Requirement）

SFR（Security Functional Requirement）

SF（Security Function）：セキュリティ機能

SFP（Security Function Policy）：セキュリティ機能ポリシー

SOF（Strength Of Function）：機能強度

ST（Security Target）：セキュリティターゲット

TOE（Target Of Evaluation）：評価対象

TSF（TOE Security Functions）：TOE セキュリティ機能

<TOE 関連略語>

OS（Operating System）：基本ソフト

UAP（User Application Program）：ユーザアプリケーションプログラム

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

API（Application Programming Interface）：アプリケーションプログラミングインタフェース

MIME（Multipurpose Internet Mail Extensions）：データの種類を表現する規定