S*Plex3

クラウドストレージサーバシステム

セキュリティターゲット

バージョン：1.21

2010 年 8 月 27 日

《変更履歴》

バージョン	日付	作成者	確認者	承認者	内容
1.00	2009/11/05	中尾	堀越	福田	新規作成
1.01	2009/11/30	中尾	堀越	福田	誤植修正
1.02	2009/12/15	中尾	堀越	福田	誤植修正
1.03	2010/01/05	中尾	堀越	福田	誤植修正
1.04	2010/01/08	中尾	堀越	福田	誤植修正
1.05	2010/03/05	中尾	堀越	福田	誤植修正
1.06	2010/03/15	中尾	堀越	福田	誤植修正
1.07	2010/03/29	中尾	堀越	福田	誤植修正
1.08	2010/04/28	中尾	堀越	福田	誤植修正
1.09	2010/05/12	中尾	堀越	福田	誤植修正
1.10	2010/05/13	中尾	堀越	福田	誤植修正
1.11	2010/05/18	中尾	堀越	福田	誤植修正
1.12	2010/06/02	中尾	堀越	福田	誤植修正
1.13	2010/06/04	中尾	堀越	福田	誤植修正
1.14	2010/06/08	中尾	堀越	福田	誤植修正
1.15	2010/06/17	中尾	堀越	福田	誤植修正
1.16	2010/07/01	中尾	堀越	福田	誤植修正
1.17	2010/07/08	中尾	堀越	福田	誤植修正
1.18	2010/07/15	中尾	堀越	福田	誤植修正
1.19	2010/08/11	中尾	堀越	福田	誤植修正
1.20	2010/08/18	中尾	堀越	福田	誤植修正
1.21	2010/08/27	中尾	堀越	福田	誤植修正

目　次

略語

ASP	Application Service Provider
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
EAL	Evaluation Assurance Level
FW	FireWall（TCP/UDP のポートレベルで通信を制御する装置であり、フィルタリング機能をもつルータや L3 スイッチを含む）
iDC	Internet Data Center
IDS	Interusion Detection System
OS	Operating System
PC	Personal Computer
PP	Protection Profile
SaaS	Software as a Service
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement)
SSL	Secure Socket Layer（ネットワーク上の通信データを秘匿する技術）
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

用語

連携 ASP・SaaS 事業者	自らの ASP・SaaS サービスに他の ASP・SaaS サービスを組み込むことにより、アプリケーション間の統合・連携を実施する際に、他の ASP・SaaS サービスを提供する ASP・SaaS 事業者。
業務プロセス	ASP・SaaS サービスを提供するために行われる一連の活動。
情報処理施設	ASP・SaaS 事業者がサービスを提供するための設備が設置された建物。
物理的セキュリティ境界	情報処理施設の特定の領域を保護するために設置される壁、カード制御による出入口等の物理的な仕切り。
プラットフォーム	認証、決済等の付加的機能を提供する、ASP・SaaS サービスで提供されるアプリケーションの基盤。
通信機器	ルータ、スイッチ等、通信を制御するための装置。
情報セキュリティ対策機器	FW、IDS 等、コンピュータウイルスや不正アクセス等の情報セキュリティ事象から、ASP・SaaS 事業者の設備を防護するための機器。
外部ネットワーク	情報処理施設とその外部とを結ぶネットワークの総称で、ASP・SaaS 事業者間（ASP・SaaS 事業者と連携 ASP・SaaS 事業者間や事業者の保守管理用回線）、利用者と ASP・SaaS 事業者間及び ASP・SaaS 事業者と iDC 間

	の公開されたネットワーク（インターネット等）を示す。なお、利用者が契約する通信回線及びインターネット・サービスは外部ネットワークに含み、利用者環境内部のローカルネットワーク、ASP・SaaS 事業者内部のローカルネットワーク、連携 ASP・SaaS 事業者内部のローカルネットワークは外部ネットワークに含まない。
内部ネットワーク	iDC 内部のネットワーク及び iDC 間等の公開されないネットワーク（専用線等）、利用者環境内部のネットワーク。
消失訂正符号	符号誤りが発生した場合に検出・訂正が可能な誤り訂正符号の一種であり、消失を訂正できる訂正符号。
符号分割	分割とともに符号化する方式の総称。
冗長比率	符号分割前及び符号分割後におけるデータ量の比率。冗長度を持たせて符号分割する。
復元閾値	復元に必要な分散保管されたデータ量と符号分割後におけるデータ量の比率。
ASP サーバ	ASP・SaaS 事業者が ASP サービスを提供する際に利用するアプリケーション等を搭載する機器及び装置の総称。
医療ガイドライン	「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン、総務省、平成 21 年 7 月」
医療ガイドラインのうちシステムに関わる項目	医療ガイドラインのうち、技術的、物理環境的に担保すべき以下の項目。 ・物理的安全管理策の全ての項目（最低限） ・技術的安全管理策の全ての項目（最低限）
個人情報	法令上「個人情報」とは、生存する個人に関する情報であり、個人情報取扱事業者の義務等の対象となるのは、生存する個人に関する情報に限定されている。医療ガイドラインは、医療・介護関係事業者が保有する生存する個人に関する情報のうち、医療・介護関係の情報を対象とするものであり、また、診療録等の形態に整理されていない場合でも個人情報に該当する。 なお、当該患者・利用者が死亡した後においても、医療・介護関係事業者が当該患者・利用者の情報を保存している場合には、漏えい、滅失又はき損等の防止のため、個人情報と同等の安全管理措置を講ずるものとする。
利用者識別情報	利用者を識別する情報（利用者 ID、グループ ID）。
認証トークン	TOE が参照する情報（利用者識別情報が含まれる）。TOE 外で識別認証が成功した利用者に TOE 外の機能により発行される。
オーナー	利用者データの利用者 ID と一致する利用者 ID をもつ利用者。

1. ST 概説

1.1. ST 参照

・ST名称　：S*Plex3クラウドストレージサーバシステム　セキュリティターゲット
・STバージョン　：1.21
・作成日　：2010/8/27
・作成者　：スカパーJSAT株式会社

1.2. TOE 参照

・TOE名称　：S*Plex3クラウドストレージサーバシステム
・TOEバージョン　：Version 1.00
・TOEの種別　：クラウドストレージサーバシステム
・開発者　：スカパーJSAT株式会社

1.3. TOE 概要

本節では TOE 種別、TOE の使用方法及び主要なセキュリティ機能、TOE の動作環境について説明する。

1.3.1. TOE の種別

TOE である S*Plex3 クラウドストレージサーバシステムとは、データ分散ネットワーク・ストレージサービスを提供するシステムである。

1.3.2. TOE の使用方法と主要なセキュリティ機能

TOE は、iDC 内に存在するシステムであり ASP と連携して医療機関などの利用者に様々なサービスを提供する。利用者は ASP・SaaS 事業者が提示する Web ブラウザをインタフェースとして、識別認証を経て TOE を利用することにより、データの保存・読み出し・管理を行う。TOE に保存されるデータは消失訂正符号により符号分割され、広域に展開された iDC 内のストレージ装置に分散[1]され配置される。この広域に分散配置されたデータ（符号分割されたデータの断片）を集め復元することによってデータの読出しが行われる。この際、消失訂正符号を用いることにより、符号分割されたデータ断片の内、30%程度の断片が欠損した場合でも復元が可能である。この分散／復元機能によって、大規模災害等により一部のストレージ装置の故障や、iDC 間の回線障害があったとしても、継続したデータの読出しが可能であり、ASP・SaaS 事業者が提供するサービスも継続して提供可能であ

[1] 本ドキュメントでは、特にことわりの無い場合、“分散”の対義語として“復元”を用いる。また、“暗号”の対義語として“復号”を用いて区別する。

る。TOE が提供する主要なセキュリティ機能は以下となる。

■ アクセス制御機能

アクセス権限に従って、権限の無いデータへのアクセスを制限する機能。

■ 完全性検証機能

TOE が一時的または長期的に保管するデータの完全性の検証を行う機能。

■ 分散／復元機能

TOE が保管するデータの可用性を担保するために、データを分散して保管・復元する機能。

なお、本 ST は、医療機関に所属する利用者への対応も想定している。このような利用の場合は、TOE を利用する ASP が、医療ガイドラインの要求を満たしたサービス[2] を提供するために、医療ガイドラインのうちシステムに関わる項目を満たすことを想定している。但し、TOE が提供するセキュリティ機能は上記で示した通り、データのアクセス制御及び分散保存や保存したデータの完全性検証機能であり、医療ガイドラインのうちシステムに関わる項目を満たすために期待される識別認証機能、監査機能及び、ストレージに格納されるデータの暗号化機能等は TOE 外の機能である。

1.3.3. TOE の動作環境

TOE の利用者に要求される環境は、利用する ASP・SaaS 事業者のサービスにより異なり、サービスを提供する ASP・SaaS 事業者から提示されるが、一般的には Web ブラウザが想定される。本 ST では 1.4.2.2 節にテストで用いた具体的な利用者のクライアント PC の動作環境を記載する。また、1.4.2.2 節に示す通り、TOE の利用については、認証トークン生成モジュール（スカパーJSAT 開発）が必要である。

1.4. TOE 記述

1.4.1. TOE の利用に関する人物の役割

TOE の利用に関連する人物の役割を以下に定義する。

利用者	TOE が提供する機能を ASP・SaaS サービスとして利用する個人。 TOE が管理するデータに対して、アクセス権限の範囲でデータの読み書き等の操作が可能。
利用管理者	TOE が提供する機能を ASP・SaaS サービスとして利用する組織の管理者であり、信頼できる人物であることが求められる。また、TOE の機能では無いが、IT 環境の機能を利用した、利用者及びグループの追加、変更、削除の管理も行う。

[2] 利用者と契約を結び、他の複数の事業者のサービスを組み込んでサービス提供する連携型提供形態により、利用者から送信されたデータを ASP・SaaS で処理を行うほか、送信されたデータの保存も行う外部保存型サービス。

ASP 管理者 （管理責任者） (※1)	TOE が提供する機能によるサービス提供 ASP の管理者であり、 TOE が提供する機能によるサービス提供 ASP の運用管理を行う。 ASP・SaaS 事業者が提供するサービスに使用する設備の運用管理を担当する現場責任者であり、信頼できる人物であることが求められる。なお、TOE は利用しない。
iDC 管理者	TOE が設置される iDC の管理者であり、iDC の各種設定、運用、管理を行う。なお、TOE は利用しない。
組織の責任者	各組織の長であり、各管理者の任命を行う。
グループ	利用管理者が設定する、複数の利用者を束ねた単位。

※1:連携 ASP・SaaS 事業者であり、自らの ASP・SaaS サービスに他の ASP・SaaS サービスを組み込むことにより、アプリケーション間の統合・連携を実施する際に、他の ASP・SaaS サービスを提供する ASP・SaaS 事業者。

1.4.2. TOE の物理的範囲

1.4.2.1. 利用環境

TOE の利用環境について説明する。TOE は、iDC 内に設置されたシステムであり、ASP サービスとしてクライアント PC にサービスを提供する。TOE は複数のサーバ及び機器で構成される既設のシステムであり、その物理的範囲は下記点線内である（各サーバ及び機器の役割は以下の通り）。

WebGW	セッション維持、アクセス権限制御を行うサーバ
IF Server	データの分散や復元を制御するサーバ
MIMS	利用者データ及び利用者管理情報をデータベース化するサーバ
SP3 ストレージノード	分散されたデータを保管するストレージ

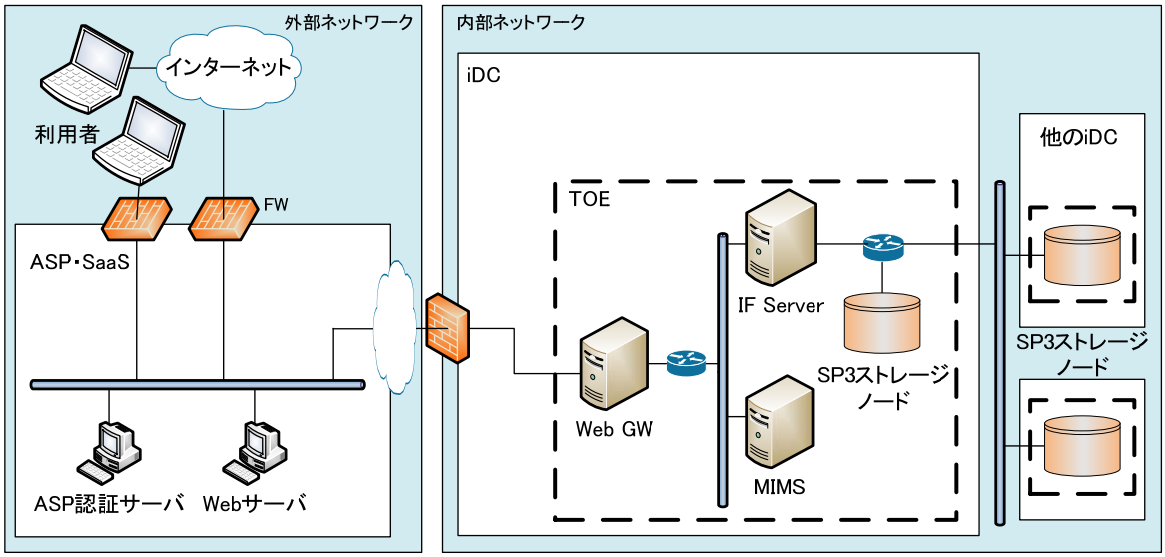

図 1　TOE システム構成図

TOE は、ASP・SaaS 事業者と連携してサービスを提供する。ASP・SaaS 事業者は、TOE の機能であるアクセス制御機能、分散保存機能、完全性検証機能を用いて個別のサービスを利用者に提供する。利用者が ASP・SaaS 事業者のサービスを受ける場合、ASP・SaaS 事業者との契約内容に基づき、TOE に対して ASP・SaaS 事業者が利用管理者登録を行う。利用管理者の登録時には、契約に基づき利用者の組織全体で利用できるディスク容量が定められる。また、登録された利用管理者が利用者登録を行うことで利用者がサービスを利用することができる。利用者の登録時には、利用者が利用できるディスク容量が定められ初期ディレクトリが設定される。TOE の利用については、ASP・SaaS 事業者が管理する Web サーバや ASP 認証サーバ等による識別認証機能が提供されることを想定しており、TOE はこれら TOE 外の識別認証が成功した際に ASP 認証サーバから発行される認証トークンに従いサービスを提供する。また、ASP・SaaS 事業者の Web サーバと TOE 間は SSL 等により保護されたインターネットを介してサービスの利用及び、管理行為が可能となる。

なお、TOE を構成するサーバは直接的な攻撃（サーバへのログインや破壊）から保護される iDC に設置されており、他の iDC とは専用のネットワーク（内部ネットワーク）網を介して接続される。

1.4.2.2. 動作環境

本 TOE は既設のシステムであり、セットアップを要する様なサーバモジュールでの提供は行わないため、TOE の動作環境は存在しない。また利用者に対する動作要件は、TOE を利用する ASP・SaaS 事業者のサービスにより異なり、サービスを提供する ASP・SaaS 事業者から提供されるものであり、TOE による制限はない。

なお、本 TOE のテストを実施した環境は以下に示す通りである。

表 1　テストで用いたサーバ及び利用者環境

サーバ・環境	分類	項目	要件
Web サーバ	ソフトウェア	OS	CentOS 5.2
		その他	Apache 2.2.11 OpenSSL 0.9.8l
	ハードウェア	CPU	Intel 64 (Pentium Dual Core E2160)
		メモリ	1GB
利用者	ソフトウェア	OS	Windows XP SP3
		その他	Internet Explorer 6
			Adobe Flash Player
	ハードウェア	CPU	Intel 64
		メモリ	2GB
ASP 認証サーバ	ソフトウェア	OS	CentOS 5.2
		認証トークン 生成モジュール	ASP バージョン 3.5.3
		その他	Apache 2.2.11 OpenSSL 0.9.8l
	ハードウェア	CPU	Intel 64 (Pentium Dual Core E2160)
		メモリ	1GB

CC の制度上、保証範囲外ではあるが、本 TOE が設置された iDC 及び TOE を用いたサービスを提供する ASP･SaaS 事業者が医療ガイドラインのうちシステムに関わる項目を満たす運用方針に従ったサービスを提供していることは､利用者がサービス選択時に開発者に問い合わせることにより確認することを想定している。また、上表に示した通り、TOE の利用については、認証トークン生成モジュール（スカパーJSAT 開発）が必要である。

1.4.2.3. ガイダンス

■ ASP・SaaS 事業者向け
- ・ 医療ガイドライン対策用利用者ガイダンス作成規定
- ・医療ガイドライン対策文書
- ・Web API 仕様詳細
- ・Web API 利用ガイド

■ iDC 向け
- ・医療ガイドライン対策文書

利用者向けのガイダンスは、ASP・SaaS 事業者が上記の「医療ガイドライン対策用利用者ガイダンス作成規定」を元に作成し配付することを想定している。開発者から利用者へ提供されるガイダンスは存在しない。

1.4.3. TOE の論理的範囲

1.4.3.1. セキュリティ機能

TOE が提供するセキュリティに関係する主な機能について説明する。

■ アクセス制御機能

TOE は、アクセス制御機能を提供する。アクセス制御機能を提供することで、セッション維持された利用者に対するアクセス権限に従って、権限の無いデータへのアクセスを制限する。これにより機密性を確保した状態で格納、編集することが可能となる。

■ 完全性検証機能

TOE は、完全性検証機能を提供する。TOE が一時的または長期的に保管するデータは、完全性の検証を行うために、分散化されたデータにハッシュ値を付加し、再度読み出す際に検証を行う。

■ 分散／復元機能

TOE は、分散／復元機能を提供する。TOE が一時的または長期的に保管するデータは、可用性を担保するために、データを保管する際に分散化し、複数の異なる SP3 ストレージノードに分散化して冗長的に保管される。これにより、例えば複数拠点の SP3 ストレージノードに格納された各分散化データは、通信障害及び災害によって各拠点に格納された分散化データの消失が発生した場合でも閾値を満たす分散化データを得れば復元可能である。

■ 暗号通信機能

TOEはWEBサーバとの間で送受信されるデータをSSL/TLSを利用して暗号化し、通信する。

2. 適合主張

2.1. CC 適合主張

本 ST は、以下の規格に適合する。

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 3 版 ［翻訳第 1.0 版］
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 3 版 ［翻訳第 1.0 版］
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 3 版 ［翻訳第 1.0 版］

- セキュリティ機能要件 : パート 2 適合。
- セキュリティ保証要件 : パート 3 適合。

2.2. PP 主張

本 ST が適合する PP はない。

2.3. パッケージ主張

本 ST は、パッケージ : EAL1 追加（追加コンポーネント : ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1）に適合する。
追加する保証コンポーネントはない。

2.4. 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model Version 3.1 Revision 3 CCMB-2009-07-001
- Common Criteria for Information Technology Security Evaluation Part 2:Security functional components Version 3.1 Revision 3 CCMB-2009-07-002
- Common Criteria for Information Technology Security Evaluation Part 3:Security assurance components Version 3.1 Revision 3 CCMB-2009-07-003
- Common Methodology for Information Technology Security Evaluation Evaluation methodology Version 3.1 Revision 3 CCMB-2009-07-004

3. セキュリティ課題定義

本章では、保護対象資産の考え方、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 保護対象資産

本節では、TOE の保護対象資産を識別し、説明する。TOE は、利用者が TOE 内のストレージ装置に格納したデータに対して大規模災害等も考慮した高い可用性を維持する。また、ストレージ装置内の格納データは、機密性と完全性についても担保された状態で一時的または長期的に保管する。更に保存されたデータは利用者の操作（削除、保存）のタイミングでストレージ装置内にバックアップされ、利用者の希望に応じてバックアップされたデータの参照が可能となっている。[3]

また、IT 環境である ASP・SaaS 事業者が提供するサービスにおいて、識別された利用者の情報を維持し、その権限に従い、ストレージ内のデータに対するアクセス制御機能を提供する。これらのことから、以下が TOE の保護対象資産である。

＜ 利用者データ＞

○ 利用者データ

利用者が TOE のストレージ装置に対して格納するファイルやディレクトリ及び、それらのバックアップデータであるファイルやディレクトリ。

＜ TSF データ ＞

○ 管理情報

TOE の利用者（管理者役割、利用者役割）のアクセス制御用データであり、TOE のストレージ装置内に格納される。

管理情報は、以下の通り分類される。

・利用者識別情報

・権限情報（アクセス権限情報）

3.2. 前提条件

本節では、TOE の利用環境に関する前提条件を識別し、説明する。

A.ADMIN_OFFICE （利用管理者の人的条件）	利用管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。
A.TRUSTED_ASP （信頼できる ASP）	・ASP 管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。 ・ASP 管理者は、医療ガイドラインのうちシステムに関わる項目のなかで、ASP・SaaS 事業者に対する項目を全て満たした環境を利用者に提供する。

[3] なお、バックアップする機能はセキュリティ機能としていないため、評価対象ではない。

	・ASP 管理者は、ASP 認証サーバにおいて識別認証機能を提供する。 ・ASP 管理者は、認証トークン生成モジュールをインストールし、ガイダンスにしたがって、認証トークン生成の機能を実装する。
A.TRUSTED_IDC （信頼できる iDC）	・iDC 管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。 ・iDC 管理者は、医療ガイドラインのうちシステムに関わる項目のなかで、iDC に対する項目を全て満たした環境を TOE に提供する。

3.3. 脅威

本節では、TOE の利用及び TOE 利用環境において想定される脅威を識別し、説明する。

T.ILLEGAL_ACCESS （不正利用者の操作）	TOE の利用者が、利用者識別情報の異なる利用者に権限のあるストレージ装置内の利用者データ及び管理情報を削除、改ざん、暴露するかもしれない。

3.4. 組織のセキュリティ方針

本節では、組織のセキュリティ方針を識別し、説明する。

P.BUSINESS_CONTINUANCE （事業継続）	情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するために、利用者のデータを格納するシステムは当該データを冗長的に保管し、保管されたデーター部の消失等から元のデータを保護する仕組みを提供しなければならない。
P.CRYPTO （重要情報の暗号化）	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信等から保護するため、通信を暗号化しなければならない。
P.MANAGE_OFFICE （利用環境の管理）	利用者の組織が希望する場合、利用管理者は、医療ガイドラインのうちシステムに関わる項目のなかで、医療機関に対する項目を厳守しなければならない。

4. セキュリティ対策方針

本章では、3 章で識別された前提条件、脅威、組織のセキュリティ方針を受けて、TOE 及び TOE の利用環境で必要なセキュリティ対策方針について記述する。以下、TOE のセキュリティ対策方針及び、運用環境のセキュリティ対策方針に分類して記述する。

4.1. TOE セキュリティ対策方針

本節では、TOE のセキュリティ対策方針について識別し、説明する。

O.ACCESS_CONTROL （アクセス制御）	TOE は、利用者識別情報と利用者データの権限情報に基づいて、利用者による利用者データへのアクセスを制御する。また、権限情報の改変は当該利用者データの作成者のみに許可する。
O.INTEGRITY （完全性検証）	TOE は保管する分散された利用者データ及び管理情報のハッシュ値を比較することにより、完全性を検証する。
O.SPLIT （分散復元）	TOE は保管する利用者データ及び管理情報を分散化して冗長的に格納し、格納されたデータの一定の比率以下の消失等に関わらず復元を行う。
O.TRUSTED-PASS （高信頼チャネルの利用）	TOE は、WEB サーバと TOE の間の保護対象資産が含まれる全ての通信を、高信頼チャネルを介して行う機能を提供する。

4.2. 運用環境のセキュリティ対策方針

本節では、運用環境のセキュリティ対策方針について識別し、説明する。

OE.ADMIN_OFFICE （利用管理者の人的条件）	利用管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わないことを保証するために、組織の責任者は適切な人選を行う。
OE.TRUSTED_ASP （信頼できる ASP）	・ASP 管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わないことを保証するために、組織の責任者は適切な人選を行う。 ・ASP 管理者は、開発者から提供されるガイダンスに従い、医療ガイドラインのうちシステムに関わる項目のなかで、ASP・SaaS 事業者に対する項目を全て満たす環境を構築し運用する。 ・ASP 管理者は、ASP 認証サーバにおいて識別認証機能を提供する。 ・ASP 管理者は、認証トークン生成モジュールをインストールし、ガイダンスにしたがって、認証トークン生成の機能を実装

	する。
OE.TRUSTED_IDC （信頼できる IDC）	・iDC 管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わないことを保証するために、組織の責任者は適切な人選を行う。 ・iDC 管理者は、開発者から提供されるガイダンスに従い、医療ガイドラインのうちシステムに関わる項目のなかで、iDC に対する項目を全て満たす環境を構築し運用する。
OE.MANAGE_OFFICE （利用環境の管理）	利用管理者は以下の対策を講じる。 ・ 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠する。 ・ 個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可した利用者以外立ち入ることが出来ない対策を講じる。 ・ 個人情報の物理的保存を行っている区画への入退管理を実施する。 ・ 個人情報が存在する PC 等の機器に盗難防止用チェーンを設置する。 ・ 個人情報を入力、参照できる端末は物理的に遮蔽する等、窃視防止の対策を実施する。 ・ TOE を用いる情報システムへのアクセスにおける利用者の識別と認証を行う。 ・ 利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、利用者本人しか知り得ない状態に保つよう教育等対策を行う。 ・ TOE を用いる情報システムの入力者が端末から離席する際に、クリアスクリーン等の防止策を講じるよう教育する。 ・ TOE を用いる情報システムの動作確認等で個人情報を含むデータを使用するときは、利用を制限し、漏えい等に十分留意する。 ・ 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行う。また、アクセス権限の見直しは、運用管理規程で定める。 ・ アクセスの記録及び定期的なログの確認を行う。 ・ アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じる。 ・ アクセスの記録に用いる時刻情報は信頼できるものを利用する。（医療機関等の内部で利用する時刻情報を定め、標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ。）

	・ システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認する。 ・ パスワードを利用者識別に使用する場合には、パスワードは必ず暗号化され適切な手法で管理及び運用し、パスワードを変更する場合には利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載し、本人以外が知りえない方法で再登録を実施し、利用管理者であっても利用者のパスワードを推定できる手段を防止する。また、利用者は、パスワードは定期的に変更し、極端に短い文字列を使用せず、英数字、記号を混在させた 8 文字以上の文字列に設定し、類推しやすいパスワードを使用しないこと。 ・ 無線 LAN を利用する場合は、ステルスモード及び ANY 接続拒否等の対策､SSID 及び MAC アドレスによるアクセス制限、WPA2/AES 等により、通信を暗号化し情報保護を講じる。
OE.CRYPTO （暗号化）	・ ASP 管理者は、WEB サーバを構築し、ガイダンスにしたがって設定をおこなうことで、利用者との通信を暗号化する。 ・ 利用管理者は、利用者が TOE を利用したサービスを利用する際は、ASP・SaaS 事業者が提供する通信を暗号化するための手段のみを利用した運用を行う。 ・ 利用者は、ASP・SaaS 事業者が提供する通信を暗号化するための手段が正しく設定されていることを確認する。

4.3. セキュリティ方針根拠

本節では、前提条件、脅威及び、組織のセキュリティ方針に対して、TOE のセキュリティ対策方針、または環境のセキュリティ対策方針が少なくとも１つ以上対応していることを表 2 に示す。さらに、前提条件、脅威及び、組織のセキュリティ方針に対して、それぞれ十分なセキュリティ対策方針が取れていること及び、そのセキュリティ対策方針が必要であることを記述する。

表 2　対応表

	A.ADMIN_OFFICE	A.TRUSTED_ASP	A.TRUSTED_IDC	T.ILLEGAL_ACCESS	P.BUSINESS_CONTINUANCE	P.CRYPTO	P.MANAGE_OFFICE
O.ACCESS_CONTROL				○			
O.INTEGRITY					○		
O.SPLIT					○		
O.TRUSTED-PASS						○	
OE.ADMIN_OFFICE	○						
OE.TRUSTED_ASP		○					
OE.TRUSTED_IDC			○				
OE.MANAGE_OFFICE							○
OE.CRYPTO						○	

4.3.1. 前提条件に対するセキュリティ対策方針

前提条件に対するセキュリティ対策方針について以下に説明する。

A.ADMIN_OFFICE （利用管理者の人的条件）	本条件は、利用管理者が、悪意を持ったある行為を行わないことを想定している。 OE.ADMIN_OFFICE は、TOE を利用する組織が TOE を利用する組織において、信頼のおける人物を利用管理者に指定するため、利用管理者の信頼性が実現される。
A.TRUSTED_ASP （信頼できる ASP）	本条件は、ASP 管理者が、課せられた役割として許可される一連の作業において、悪意を持った行為は行わないこと及び、医療ガイドラインのうちシステムに関わる項目のなかで、ASP・SaaS 事業者に対する項目を全て満たした環境を利用者に提供すること、ASP 認証サーバにおいて識別認証機能を提供することを想定している。 OE.TRUSTED_ASP は、TOE を利用する ASP・SaaS において、信頼のおける人物を ASP 管理者に指定し、ASP 管理者は開発者から提供されるガイダンスに従い、医療ガイドラインのうちシステムに関わる項目を満たした環境を構築して運用をおこない、認証トークン生成モジュールをインストールし、ガイダンスにしたがって、認証トークン生成の機能を実装することから、この前提条件は実現される。
A.TRUSTED_IDC （信頼できる IDC）	本条件は、iDC 管理者が、課せられた役割として許可される一連の作業において、悪意を持った行為は行わないこと及び、医療ガイドラインのうちシステムに関わる項目のなかで、iDC に対する項目を全て満たした環境を利用者に提供することを想定している。 OE.TRUSTED_ASP は、TOE を設置する iDC において、信頼のおける人物を iDC 管理者に指定し、iDC 管理者は開発者から提供されるガイダンスに従い、医療ガイドラインのうちシステムに関わる項目を満たした環境を構築し運用するため、iDC の信頼性は実現される。

4.3.2. 脅威に対するセキュリティ対策方針

脅威に対するセキュリティ対策方針について以下に説明する。

T.ILLEGAL_ACCESS （不正利用者の操作）	本脅威は、TOE の利用者が、利用者識別情報の異なる利用者に権限のある利用者データ及び、管理情報を削除、改ざん、暴露する

	可能性を想定している。 これに対して、O.ACCESS_CONTROL は、TOE が利用者識別情報と利用者データの権限情報に基づいて、利用者による利用者データへのアクセスを制御し、また権限情報の改変は当該利用者データの作成者のみに許可するため、脅威の可能性は除去される。 よって本組織のセキュリティ方針は達成される。

4.3.3. 組織のセキュリティ対策に対するセキュリティ対策方針

組織のセキュリティ対策に対するセキュリティ対策方針について以下に説明する。

P.BUSINESS_CONTINUANCE （事業継続）	本組織のセキュリティ方針は、事業活動の中断に対処するために、利用者のデータを格納するシステムは当該データを冗長的に保管し、更に完全性を保護する仕組みを提供しなければならないことを想定している。 これに対して、O.SPLIT は、TOE が保管する利用者データ及び管理情報を分散して冗長的に格納し、一定の比率以下の消失等に関わらず復元を行う機能を提供している。O.INTEGRITY は、格納したデータを復元する際、保管する分散された利用者データ及び管理情報のハッシュ値を比較することにより、元のデータを検証している。 よって本組織のセキュリティ方針は達成される。
P.CRYPTO （重要情報の暗号化）	本組織のセキュリティ方針は、外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信等から保護するため、通信を暗号化しなければならないことを想定している。 これに対して、OE.CRYPTO は ASP 管理者が利用者との通信を暗号化することを規定し、さらに、利用管理者が ASP・SaaS 事業者が提供する通信を暗号化するための手段のみを利用した運用を行うことを既定し、利用者が通信を暗号化するための手段が正しく設定されていることを確認するを規定している。また、O.TRUSTED-PASS は ASP・SaaS 事業者と TOE 間の通信を暗号化することから、本組織のセキュリティ方針は達成される。
P.MANAGE_OFFICE （利用環境の管理）	本組織のセキュリティ方針は、TOE を利用した ASP サービスを利用者する組織において、医療ガイドラインのうちシステムに関わる項目のなかで、医療機関に対する項目を厳守することを想定している。 これに対して、OE.MANAGE_OFFICE は、TOE を利用する組織において、利用管理者が以下の対策を講じることが規定されている。

	・ 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠する。 ・ 個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可した利用者以外立ち入ることが出来ない対策を講じる。 ・ 個人情報の物理的保存を行っている区画への入退管理を実施する。 ・ 個人情報が存在する PC 等の機器に盗難防止用チェーンを設置する。 ・ 個人情報を入力、参照できる端末は物理的に遮蔽する等、窃視防止の対策を実施する。 ・ TOE を用いる情報システムへのアクセスにおける利用者の識別と認証を行う。 ・ 利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、利用者本人しか知り得ない状態に保つよう教育等対策を行う。 ・ TOE を用いる情報システムの入力者が端末から離席する際に、クリアスクリーン等の防止策を講じるよう教育する。 ・ TOE を用いる情報システムの動作確認等で個人情報を含むデータを使用するときは、利用を制限し、漏えい等に十分留意する。 ・ 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行う。また、アクセス権限の見直しは、運用管理規程で定める。 ・ アクセスの記録及び定期的なログの確認を行う。 ・ アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じる。 ・ アクセスの記録に用いる時刻情報は信頼できるものを利用する。（医療機関等の内部で利用する時刻情報を定め、標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ。） ・ システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認する。 ・ パスワードを利用者識別に使用する場合には、パスワードは必ず暗号化され適切な手法で管理及び運用し、パスワードを変更する場合には利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載し、本人以外が知りえない方法で再登録を実施し、利用管理者であっても利用者の

	パスワードを推定できる手段を防止する。また、利用者は、パスワードは定期的に変更し、極端に短い文字列を使用せず、英数字、記号を混在させた 8 文字以上の文字列に設定し、類推しやすいパスワードを使用しないこと。 ・ 無線 LAN を利用する場合は、ステルスモード及び ANY 接続拒否等の対策、SSID 及び MAC アドレスによるアクセス制限、WPA2/AES 等により、通信を暗号化し情報保護を講じる。 よって本組織のセキュリティ方針は達成される。

5. 拡張コンポーネント定義

このST では、拡張コンポーネントを使用しない。

6. セキュリティ要件

本章では、TOE セキュリティ要件について記述する。

6.1. TOE セキュリティ要件

6.1.1. TOE セキュリティ機能要件

6.1.1.1. 利用者データ保護

FDP_ACC.1　　サブセットアクセス制御
FDP_ACC.1.1
TSF は、[割付: *サブジェクト、オブジェクト、及び 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、及び 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*]: ***「表 3　アクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]: ***アクセス制御***
下位階層　　:　なし 依存性　　:　FDP_ACF.1（FDP_ACF.1）

表 3　アクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	*・ファイル* *・ディレクトリ*	*・作成* *・削除* *・移動（名前変更を含む）* *・読み込み* *・書き込み* *・コピー* *・ディレクトリ内エントリ[4]取得*

[4] ディレクトリ内のファイル及びディレクトリの一覧

FDP_ACF.1	**セキュリティ属性によるアクセス制御**
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、及び各々に対応する、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、及び各々に対応する、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＞*** ***・利用者を代行するタスク*** ⇒ ***・利用者 ID*** ***・グループ ID*** --- ***＜オブジェクト＞*** ***＜オブジェクト属性＞*** ***・ファイル*** ⇒ ***・利用者 ID*** ***・ディレクトリ*** ***・共有設定対象の利用者 ID と R または RW*** ***・共有設定対象のグループ ID と R または RW***	
[割付: *アクセス制御 SFP*]: ***アクセス制御***	
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*]: ***・「表 4　操作可能なサブジェクト属性とオブジェクト属性の関係（オーナーの操作）」に記載した操作*** ***・「表 5　操作可能なサブジェクト属性とオブジェクト属性の関係（共有）」に記載した操作***	
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***	
下位階層　:　なし 依存性　:　FDP_ACC.1（FDP_ACC.1）、FMT_MSA.3（FMT_MSA.3）	

表 4　操作可能なサブジェクト属性とオブジェクト属性の関係（オーナーの操作）

可能な操作		各属性の関係	
		サブジェクト属性	オブジェクト属性
ファイル・ディレクトリ共通の操作	作成、削除、移動（名前変更含む）、コピー	利用者 ID	左記と一致する利用者 ID
ファイル固有の操作	読み込み（R）	利用者 ID	左記と一致する利用者 ID
	読み込み/書き込み（RW）		
ディレクトリ固有の操作	ディレクトリ内エントリ取得	利用者 ID	左記と一致する利用者 ID

表 5　操作可能なサブジェクト属性とオブジェクト属性の関係（共有）

可能な操作		各属性の関係	
		サブジェクト属性	オブジェクト属性
ファイル・ディレクトリ共通の操作	作成、削除、移動（名前変更含む）	―	
ファイル固有の操作	読み込み（R）	利用者 ID	左記と一致する利用者 ID、R
		グループ ID	左記と一致するグループ ID、R
	読み込み、書き込み（RW）	利用者 ID	左記と一致する利用者 ID、RW
		グループ ID	左記と一致するグループ ID､RW
	コピー※	利用者 ID	左記と一致する利用者 ID、R
		グループ ID	左記と一致するグループ ID、R
ディレクトリ固有の操作	ディレクトリ内エントリ取得	―	

※共有（読み込み）設定されたファイルに対して自分のディレクトリ内へのコピーが可能。

FDP_DAU.1　　基本データ認証
FDP_DAU.1.1
TSF は、[割付: *オブジェクトまたは情報種別のリスト*]の有効性の保証として使用できる証拠（***完全性検証のためのハッシュ値***）を生成する能力を提供しなければならない。
[割付: *オブジェクトまたは情報種別のリスト*]： **・ファイル及びディレクトリが分散化されたデータ**
FDP_DAU.1.2
TSF は、示された情報の有効性の証拠（***完全性検証のためのハッシュ値***）を検証する（***利用者データの復元のタイミングで検証する***）能力を[割付: *サブジェクトのリスト*]に提供しなければならない。
[割付: *サブジェクトのリスト*]： **・利用者を代行するタスク**
下位階層　：　なし 依存性　：　なし

6.1.1.2. 識別と認証

FIA_ATD.1　　利用者属性定義
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*]： ***・利用者 ID*** ***・グループ ID***
下位階層　：　なし
依存性　：　なし

FIA_USB.1　　利用者・サブジェクト結合
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*]： ***・利用者 ID*** ***・グループ ID***

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の規則*] : ***利用者を代行するタスクに当該利用者の利用者 ID 及び、グループ ID を関連付ける。***
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: *属性の変更の規則*] : ***なし***
下位階層 : なし
依存性 : FIA_ATD.1（FIA_ATD.1）

6.1.1.3. セキュリティ管理

FMT_MSA.1 セキュリティ属性の管理
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。
[割付: *セキュリティ属性のリスト*] : ***・利用者データの共有設定（「表 5」に記載した対象（利用者 ID、グループ ID）、R、RW）***
[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]*] : ***・改変***
[割付: *許可された識別された役割*] : ***・オーナー***
[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*] : ***アクセス制御***
下位階層 : なし
依存性 : FDP_ACC.1 or FDP_IFC.1（FDP_ACC.1）、FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1）

FMT_MSA.3　　静的属性初期化
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（***利用者データの利用者 ID、利用者 ID に対応する操作、利用者データの共有設定（対象（利用者 ID、グループ ID）、R、RW)***）に対して*[選択: 制限的、許可的、[割付: その他の特性]*: から 1 つのみ選択]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: 制限的、許可的、[割付: その他の特性] : ***[割付: その他の特性] :*** ***利用者データを保存する利用者の利用者 ID*** ***利用者データの共有設定（対象無し）***
[割付: *アクセス制御 SFP、情報フロー制御 SFP*] : ***アクセス制御***
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指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*] ***なし***
下位階層　　:　　なし
依存性　　:　　FMT_MSA.1（なし）、FMT_SMR.1（なし）

FMT_SMF.1　　管理機能の特定
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管理機能のリスト*] : ***・　オーナーによる利用者データの共有設定改変***
下位階層　　:　　なし
依存性　　:　　なし

FMT_SMR.1　　セキュリティ役割
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*] : ***・オーナー***
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。
下位階層　　:　　なし
依存性　　:　　FIA_UID.1（なし）

6.1.1.4. TSF の保護

FPT_FLS.1　　セキュアな状態を保持する障害
FPT_FLS.1.1
TSF は、以下の種別の障害が生じたときはセキュアな状態を保持しなくてはならない: [割付: *TSF における障害の種別のリスト*]。
[割付: *TSF における障害の種別のリスト*]: ***SP3 ストレージノード上の分散された管理情報及び、利用者データの「表 6　冗長化方式（冗長比率と復元閾値）」に示した復元閾値を維持する範囲以下の消失***
下位階層　:　なし 依存性　:　なし

表 6　冗長化方式（冗長比率と復元閾値）

方式種別		冗長比率	復元閾値
管理情報		11:31	21:31
利用者データ	*冗長比率 1*	78:127	104:127
	冗長比率 2	64:127	86:127

※なお、利用者データの冗長比率（冗長比率１、もしくは２）は、利用者が利用者データを保存する際に任意に選択できる。

6.1.1.5. 資源利用

FRU_FLT.1　　機能削除された耐障害性
FRU_FLT.1.1
TSF は、以下の障害[割付: *障害の種別のリスト*]が生じたとき、[割付: *TOE 機能(capabilities)のリスト*]の動作を保証しなければならない。
[割付: *障害の種別のリスト*]: ***SP3 ストレージノード上の分散された利用者データ及び、管理情報の「表 6　冗長化方式（冗長比率と復元閾値）」に示した復元閾値を維持する範囲以下の消失***
[割付: *TOE 機能(capabilities)のリスト*]: ***・分散復元機能（利用者データ及び、管理情報に対する分散・冗長化及び、復元）***
下位階層　:　なし 依存性　:　FPT_FLS.1(FPT_FLS.1)

6.1.1.6. 高信頼パス/チャネル

FTP_ITC.1　　TSF 間高信頼チャネル
FTP_ITC.1.1
TSF は、それ自身と他の高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。
FTP_ITC.1.2
TSF は、[選択: *TSF、他の高信頼 IT 製品*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。
[選択: *TSF、他の高信頼 IT 製品*]: ***他の高信頼 IT 製品（WEB サーバ）***
FTP_ITC.1.3
TSF は、[割付: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始

しなければならない。
[割付: *高信頼チャネルが要求される機能のリスト*]: ***利用者データ、管理情報の LAN 経由通信***
下位階層　　:　なし
依存性　　:　なし

6.1.2. TOE のセキュリティ保証要件

本 TOE の評価保証レベルは EAL1 追加（追加するコンポーネントは ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1）であり、TOE セキュリティ保証要件は以下のとおりである。

表 7　TOE のセキュリティ保証要件

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

6.2. IT セキュリティ要件根拠

6.2.1. IT セキュリティ機能要件根拠

6.2.1.1. 必要性

セキュリティ対策方針と IT セキュリティ機能要件の対応関係を表 8　セキュリティ対策方針に対するセキュリティ機能要件の適合性に示す。表 8 の通り、全ての TOE セキュリティ機能要件は少なくとも一つの TOE セキュリティ対策方針と対応している。従って、全ての TOE セキュリティ機能要件の必要性は満たされている。

表 8　セキュリティ対策方針に対するセキュリティ機能要件の適合性

セキュリティ対策方針 / セキュリティ機能要件	O.ACCESS-CONTROL	O.INTEGRITY	O.SPLIT	O.TRUSTED-PASS
FDP_ACC.1	●			
FDP_ACF.1	●			
FDP_DAU.1		●		
FRU_FLT.1			●	
FIA_ATD.1	●			
FIA_USB.1	●			
FPT_FLS.1			●	
FMT_MSA.1	●			
FMT_MSA.3	●			
FMT_SMF.1	●			
FMT_SMR.1	●			
FTP_ITC.1				●

6.2.1.2. 十分性

各セキュリティ対策方針に対して適用される IT セキュリティ機能要件について以下に説明する。

■ O.ACCESS-CONTROL

本セキュリティ対策方針は、利用者に対しアクセス権限のある利用者データへのみアクセスを制限しており、アクセス権限に基づいたアクセス制御に関して諸要件が必要である。

＜アクセス制御＞

FIA_USB.1 により、利用者からの操作に対して、TOE 外の機能による識別認証の成功結果である認証トークンを用いて利用者 ID、グループ ID の属性を割り当てる。また、FIA_ATD.1 によってその属性を維持する。さらに、FDP_ACC.1、FDP_ACF.1 により、所属 ID をもつ利用者を代行するタスクは、利用者データに対して「表 4　操作可能なサブジェクト属性とオブジェクト属性の関係（オーナーの操作）」及び「表 5　操作可能なサブジェクト属性とオブジェクト属性の関係（共有）」に従った以下の操作が許可される。

・作成
・削除
・移動（名前変更含む）
・属性取得
・共有設定
・読み込み
・書き込み
・コピー
・ディレクトリ内エントリ取得

＜セキュリティ管理＞

FMT_MSA.3 により､利用者データには利用者データを保存する利用者の利用者 ID が付与され、FMT_SMF.1 及び、FMT_MSA.1 により、オーナーにのみ、以下の属性の改変が許可される。
FMT_SMR.1 によりオーナーであることが維持される。

・利用者データの共有設定（対象（利用者 ID、グループ ID）、R、RW）

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

■ O.INTEGRITY

本セキュリティ対策方針は、利用者の分散データに対し、完全性検証を行う諸要件が必要である。

＜完全性検証＞

FDP_DAU.1 により TOE に保存された分散データに対し、利用者の読出し、書込といった操作のタイミングで完全性検証を行う。

この機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

■ O.SPLIT

本セキュリティ対策方針は、利用者の読出し、書込といった操作のタイミングで、冗長化され分散保存される利用者データに対し、一定の比率以下の消失等に関わらず復元を行う耐障害性の諸要件が必要である。

＜復元に関する耐障害性＞

FRU_FLT.1、FPT_FLS.1 により、SP3 ストレージノード上の分散された利用者データは、一定の比率以下の消失等に関わらず、復元され、セキュアな状態は保持される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

■ O.TRUSTED-PASS（高信頼チャネルの利用）

本セキュリティ対策方針は、WEB サーバとの間の保護対象資産を含む通信において高信頼チャネルを生成するとしており、高信頼チャネルに関係する要件が必要である。

FTP_ITC.1 は、他の WEB サーバからのファイル及びディレクトリに対する以下の要求に応じて高信頼チャネルを生成するとしており、WEB サーバとの間の全ての通信に適用される。

・作成
・削除
・移動（名前変更含む）
・属性取得
・共有設定
・読み込み
・書き込み
・コピー
・ディレクトリ内エントリ 取得

この機能要件によって本セキュリティ対策方針は満たされる。

6.2.1.3. IT セキュリティ機能要件の依存性

IT セキュリティ機能要件コンポーネントの依存関係を下表に示す。CC パート 2 で規定される依存

性を満たさない場合、「本 ST における依存関係」の欄にその理由を記述する。

表 9　IT セキュリティ機能要件コンポーネントの依存関係

N/A：Not Applicable

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1、 FMT_MSA.3
FDP_DAU.1	なし	N/A
FIA_ATD.1	なし	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1、 FMT_SMF.1、 FMT_SMR.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1、 FMT_SMR.1	＜FIA_MSA.1 を適用しない理由＞ デフォルト値を上書きする代替の初期値を特定する役割は存在しないため、本要件を適用する必要はない。 ＜FMT_SMR.1 を適用しない理由＞ 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する役割は存在しないため、本要件を適用する必要はない。
FMT_SMF.1	なし	N/A
FMT_SMR.1	FIA_UID.1	＜FIA_UID.1 を適用しない理由＞ 利用者の識別は OE.TRUSTED_ASP により運用環境でおこなわれる。
FPT_FLS.1	なし	N/A
FRU_FLT.1	FPT_FLS.1	FPT_FLS.1
FTP_ITC.1	なし	N/A

6.2.2. IT セキュリティ保証要件根拠

本 TOE は、TOE と ASP・SaaS 事業者及び、一部の ASP・SaaS 事業者と利用者の接続にインターネットを介した接続を想定している。但し、インターネットを介した接続における不特定多数の第三者による接続に関しては、運用環境により攻撃の可能性を排除している。また、TOE が搭載されたサーバは物理的に保護された iDC に設置され、TOE を利用したサービスを展開する ASP・SaaS 事業者にも同等の物理的環境への設置を規定している。さらに TOE の一部が搭載されるサーバへの OS 等を介したアクセスも運用環境により保護されることを想定している。以上のことから、本 TOE で想定する攻撃者は、サービスのために開放しているポートへの接続のみ可能な利用者及び、TOE に利用者として登録されていない利用者である組織内の従業員であり、基本レベルの攻撃能力をもつ攻撃者と想定する。また、上記を保証するうえで完全なセキュリティターゲット及びその ST 内の SFR を分析することが必要となる場合も想定でき、その場合は、セキュリティ対策方針及び、派生したセキュリティ要件や、セキュリティ課題定義を追加する必要がある。よって EAL1 追加（追加する保証要件は ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1）の選択は妥当である。

なお、選択した全てのセキュリティ保証要件は依存性を満たしている。

7. TOE 要約仕様

TOE のセキュリティ機能要件より導かれる TOE のセキュリティ機能を以下の表 10 にて一覧を示す。仕様詳細は、後述の項にて説明する。

表 10　TOE のセキュリティ機能名称と識別子の一覧

節番号	TOE のセキュリティ機能
7.1	F. ACC-CONTROL（アクセス制御機能）
7.2	F.INTEGRITY（完全性検証機能）
7.3	F.INFO-SHARING（分散復元機能）
7.4	F. TRUSTED-PASS（高信頼チャネル機能）

7.1. F. ACC-CONTROL（アクセス制御機能）

利用者を代行するタスクは、属性として利用者 ID、グループ ID を持つ。利用者データを操作しようとした際、TOE は TOE 外の機能により識別認証に成功した結果である認証トークンを用いて利用者 ID、グループ ID の情報を得る。また、TOE はこの利用者 ID、グループ ID を利用者を代行するタスクに関連付ける。TOE は利用者 ID、グループ ID を変更する機能を提供しない。この属性と利用者データに付加された利用者 ID、利用者 ID に対応する操作及び、グループ ID を比較し、「表 4　操作可能なサブジェクト属性とオブジェクト属性の関係（オーナーの操作）」及び「表 5　操作可能なサブジェクト属性とオブジェクト属性の関係（共有）」に記載された操作を許可する。

利用者データが作成された際は、利用者データに対して、作成した利用者を代行するタスクと同一の利用者 ID が設定され、ファイル及びディレクトリに対する操作が許可される。

また、オーナーには共有設定の改変を許可する。共有設定は利用者データが作成された際は何も割り当てず、共有設定によって許可される操作は、読出し及び、書込みのみである。

なお、オーナーという役割はサブジェクトのセキュリティ属性である利用者 ID とオブジェクトのセキュリティ属性である利用者 ID を比較し、両者が一致した場合にそのサブジェクトをオブジェクトのオーナーとするものであり、このセキュリティ属性は変更されることがないため、この役割が維持される。

以上により FDP_ACC.1、FDP_ACF.1、FIA_ATD.1、FIA_USB.1、FMT_MSA.1、FMT_MSA.3、FMT_SMF.1、FMT_SMR.1 がが実現される。

7.2. F.INTEGRITY（完全性検証機能）

TOE は利用者データの書込み要求があった際、利用者データを分散復元機能により分散して SP3 ストレージノードに格納すると同時に、分散された利用者データに対しハッシュ関数（lookup3 32bit x2 = 64bit）によるハッシュ値を取得し TOE 内に保存する。利用者データを読み出す際には、保存し

たハッシュ値と、分散された利用者データから計算したハッシュ値を比較する。

以上により FDP_DAU.1 が実現される。

7.3. F.INFO-SHARING（分散復元機能）

TOE は利用者からの利用者データの書込み要求があった際、暗号化された利用者データを分散・冗長化して複数の SP3 ストレージノードに保存する。SPTVJSAT 独自の分散アルゴリズムにより複数 SP3 ストレージノードへの保管時に、分散、符号化及び、冗長化（最小 1.6 割～最大 2.8 割）を施すことで、一部の利用者データが消失された場合でも、利用者からの利用者データの復元要求に対して利用者データを復元することができる機能を提供する。（利用者データに関しては利用者が選択した冗長比率 78：127 もしくは 64：127 で分散されたデータから復元が可能、管理情報に関して冗長比率 11：31 で分散されたデータから復元が可能）なお分散、もしくは復元に失敗した際は利用者からの要求に対してエラーを返す。

以上により FRU_FLT.1、FPT_FLS.1 が実現される。

7.4. F.TRUSTED-PASS（高信頼チャネル機能）

F.TRUSTED-PASS とは、WEB サーバと TOE 間でファイルやディレクトリの操作等の保護対象資産を含むデータを送受信する際に、SSL または TLS プロトコルを使用して、高信頼チャネルを生成、実現する機能である。

以上により FTP_ITC.1 が実現される。

- 以上 -