認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤江　一正　原紙押印済

評価対象

申請受付日（受付番号）	平成21年11月6日 (IT認証9277)
認証番号	C0275
認証申請者	スカパーJSAT株式会社
TOEの名称	S*Plex3クラウドストレージサーバシステム
TOEのバージョン	Version 1.00
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	スカパーJSAT株式会社
評価機関の名称	みずほ情報総研株式会社　情報セキュリティ評価室

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成22年9月28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　山里　拓己

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 リリース３
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 リリース３

評価結果：合格

「S*Plex3クラウドストレージサーバシステム」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証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

この認証報告書は、スカパーJSAT株式会社が開発した「S*Plex3クラウドストレージサーバシステム、 バージョン Version 1.00」（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。）が平成22年9月7日に完了した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スカパーJSAT株式会社に報告するとともに、本TOEに関心を持つ消費者や調達者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本TOEのセキュリティ機能要件、保証要件及びその十分性の根拠は、STにおいて詳述されている。

本認証報告書は、本TOEの提供する機能を使用して一般消費者にサービスを提供する事業者、及びそのサービスを利用する一般消費者を読者と想定している。本認証報告書は、本TOEが適合する保証要件に基づいた認証結果を示すものであり、個別のIT製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本TOEの機能、運用条件の概要を以下に示す。詳細は2章以降を参照のこと。

1.1.1 保証パッケージ

本TOEの保証パッケージは、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。

1.1.2 TOEとセキュリティ機能性

本TOEは、ASP・SaaS事業者向けに、インターネットでストレージサービスを提供するシステムである。ASP・SaaS事業者は、本TOEがサービスとして提供する機能を利用して、各事業者個別のサービスを構築して一般利用者に提供する。

本TOEは、消失訂正符号を用いて格納するデータを符号分割し、符号分割したデータの断片を複数の拠点に設置されたストレージ装置に分散して格納する。読出し時には、分散して格納されたデータの断片を集めて復元する。その際、消失訂正符号を用いているため、障害や災害等でデータの断片の一部が失われても、元のデータを復元することができる。

本TOEは、セキュリティ機能として、所有者の異なるデータを不正に改ざんしたり暴露したりする脅威を防止するアクセス制御機能を提供する。それに加えて、利

用者データの保護に寄与する、データの分散復元機能、データの完全性検証機能、及び通信データの暗号化を行う高信頼チャネル機能もセキュリティ機能として提供している。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本TOEが想定する脅威及び前提については次項のとおり。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは、以下の脅威を想定しており、それに対抗するセキュリティ機能を提供する。

保護資産であるTOEに格納されるデータは、所有者以外の利用者によって、許可なく改ざんされたり暴露されたりする脅威がある。そのためTOEは、利用者がデータにアクセスする際に対象データのアクセス権限を確認することで、データのアクセスを許可された利用者に制限する。

上記の脅威への対抗に加えて、本TOEでは、データの分散復元、データの完全性検証、及び通信データの暗号化を行うセキュリティ機能を提供しているが、これらは組織のセキュリティ方針に基づいて提供している機能である。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定している。

本TOEは、iDCに設置され、ASP・SaaS事業者向けにストレージサービスを提供し、ASP・SaaS事業者が本TOEの提供する機能を使用して一般利用者向けのサービスを提供することを想定している。そのため、ASP・SaaS事業者側では、TOEの提供する機能を利用する各事業者固有のサービスの構築が必要である。

本TOEは、ASP・SaaS事業者側の機能で利用者の管理と識別認証を行い、識別認証の成功した利用者に、本TOEの提供する機能の利用が許可されることを想定している。

本TOEは、「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」[14]（以下「医療ガイドライン」という。）の要求を満たしたサービスを提供することを意図しており、ASP・SaaS事業者や本TOEが設置されているiDCの事業者には、医療ガイドラインが要求している各種管理対策を遵守することが求められている。

1.1.3 免責事項

(1) 本TOEは、以下のセキュリティ機能は提供していない。

・利用者の識別認証機能は、TOEの機能を利用するASP・SaaS事業者側で行われることを前提としており、TOEは識別認証機能を提供していない。
・監査ログ機能は、TOEの機能を利用するASP・SaaS事業者側で取得することが想定されており、TOEは監査ログ機能を提供していない。

(2) 本評価において、以下は評価の範囲外である。

・本評価では、災害や障害時におけるTOE機能のサービス継続性は、評価の対象外である。
・本評価では、攻撃者が認証トークンを推測してASP・SaaS事業者に代わってTOEに直接アクセスする等の、認証トークンの悪用可能性は、評価の対象外である。
・TOEは、データを格納する際に暗号化する機能を有しているが、その暗号化機能は評価の対象外である。
・完全性検証機能は、分散して格納したデータの断片について、読み出したデータと元データのハッシュ値を比較する機能である。従って、完全性の検証精度は採用しているハッシュ関数(lookup3)のハッシュ値の衝突可能性に依存するが、それは評価の対象外である。

1.2 評価の実施

認証機関が運営するITセキュリティ評価・認証制度に基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[1]、「ITセキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本TOEに関わる機能要件及び保証要件に基づいてITセキュリティ評価が実施され、平成22年9月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本TOEの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。認証機関が指摘した問題点は、すべて解決され、かつ、本TOEの評価がCC（[4][5][6]または[7][8][9]）及びCEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本TOEは、以下のとおり識別される。

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

ASP・SaaS事業者は、使用しているTOEが評価･認証を受けた本TOEであることを、所定のURLにアクセスすることにより、画面に表示されるTOEの識別情報で確認することができる。識別されたTOEの構成は一意となることが保証されている。

また、ASP・SaaS事業者は、上記の確認手段を一般利用者に提供することが要求されている。そのため、ASP・SaaS事業者のサービスを使用する一般利用者は、ASP・SaaS事業者から提供される確認手段によって、ASP・SaaS事業者経由で使用しているTOEが、評価･認証を受けた本TOEであることを確認することができる。

3 セキュリティ方針

本章では、本TOEがセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

TOEは、ASP・SaaS事業者向けに、インターネットでストレージサービスを提供するシステムである。TOEは、TOEを利用したASP・SaaS事業者のサービスが、全体として医療ガイドラインを満足することを意図している。

TOEのセキュリティ機能は、格納された利用者データを、アクセス制御によって所有者以外の利用者による改ざんと暴露を防止することを実現している。

またTOEは、サービス提供方針から、データの分散復元、データの完全性検証、及び通信データの暗号化を行うセキュリティ機能を提供している。

3.1 セキュリティ機能方針

TOEは、3.1.1に示す脅威に対抗し、3.1.2に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本TOEは、表3-1に示す脅威を想定し、これに対抗する機能を備える。

表3-1 想定する脅威

識別子	脅 威
T.ILLEGAL_ACCESS	TOEの利用者が、所有者の異なるデータを、許可なく削除、改ざん、暴露するかもしれない。 （注）本脅威の対象は、ASP・SaaS事業者による識別認証が成功した正当な利用者によるTOEの操作である。 利用者の識別認証はTOE外のASP事業者で行われることを前提としており、利用者のなりすましは脅威として想定していない。

3.1.1.2 脅威に対するセキュリティ機能方針

本TOEは、表3-1に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.ILLEGAL_ACCESS」への対抗

TOEのアクセス制御機能は、TOEが格納するファイル及びディレクトリに対して、作成、削除、読み込み、書き込み等の操作を行う際に、操作を行う利用者情報と、操作対象データに設定されたアクセス権限によってアクセス制御を行う。これにより、所有者、及び所有者が共有を許可した利用者だけが、ファイル及びディレクトリの許可された操作を実行することができる。

なお、利用者情報は、ASP・SaaS事業者からTOEに渡される認証トークンから取り出す。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本TOEの利用に当たって要求される組織のセキュリティ方針を表3-2に示す。

表3-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.BUSINESS_CONTINUANCE	利用者データを冗長的に分散して格納し、格納されたデータの一部が消失しても、元のデータが保護されるしくみを提供することを求めている。 （注）本方針は、障害や災害時のデータ保全のために、利用者組織から求められると想定される内容を、サービス提供の方針として規定したものである。
P.CRYPTO	インターネットを利用する通信データの暗号化を求めている。 （注）本方針は、重要データが通信経路上で盗聴や改ざんされることを防止するために、医療ガイドラインで規定されている内容である。
P.MANAGE_OFFICE	利用者が医療ガイドラインに沿ったサービス及び運用を希望する場合、利用者自身も医療ガイドラインの項目を遵守することを求めている。 （注）本方針は、医療ガイドラインで規定されている内容であり、利用者に個人情報保護等の環境やパスワード管理等を求めるものである。なお本TOEは、医療関連以外の利用も可能である。本方針は、利用者によってはあてはまらない場合もあり、本TOEをセキュアに運用するための必須項目ではない。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOEは、表3-2に示す組織のセキュリティ方針を、以下のように満足する。

(1) 組織のセキュリティ方針「P.BUSINESS_CONTINUANCE」への対応

TOEの分散復元機能は、スカパーJSAT株式会社独自の消失訂正符号を用いて、データを符合分割して分散して格納し、読出し時には分散したデータの断片を集めて元のデータを復元する。その際、完全性検証機能が適用され、正常なデータ断片だけが復元に使用される。

TOEの完全性検証機能は、ハッシュ関数（lookup3）を用いて、読み出したデータ断片のハッシュ値が、格納前のハッシュ値と一致するかどうかを検証する。検証結果は、分散復元機能で使用される。

それにより、ネットワークやストレージ装置の障害等で、一部のデータ断片が読み出せない場合や、一部のデータが破損してハッシュ値が異常になった場合でも、一定量以上の数のデータ断片が揃えば、消失訂正符号により元データを復元することができる。

(2) 組織のセキュリティ方針「P.CRYPTO」への対応

TOEの高信頼チャネル機能は、ASP・SaaS事業者とTOEの間の通信にSSL/TLSプロトコルを使用することにより、通信データを暗号化する。

また、ASP・SaaS事業者も、その利用者とASP・SaaS事業者との間の通信データを暗号化する必要がある。そのため、TOEは、ASP・SaaS事業者向けのガイダンスで、通信データの暗号化を要求する。

それにより、利用者がASP・SaaS事業者を介してTOEを利用する際に、インターネットを通過するすべてのデータが暗号化される。

(3) 組織のセキュリティ方針「P.MANAGE_OFFICE」への対応

TOEは、一般利用者が遵守すべき内容を、TOEのASP・SaaS事業者向けのガイダンスにおいて、利用者向けガイダンスの作成規定として提供する。

それにより、本方針が求める内容が、ASP・SaaS事業者からその利用者に周知される。

4 前提条件と使用環境

本章では、想定する読者が本TOEの利用の判断に有用な情報として、本TOEを運用するための前提条件及び使用環境について記述する。

4.1 使用及び環境に関する前提条件

TOEの提供する機能には、利用者以外の特別な役割は存在しない。しかし、TOEの使用環境においては、以下の役割を想定している。

・利用管理者
TOEを利用したASP・SaaS事業者のサービスを利用する組織の管理者。ASP・SaaS事業者から提供される機能を使用して、利用者の管理を行う。
・ASP管理者
ASP・SaaS事業者が提供するサービスの管理者。
・iDC管理者
TOEが設置されるiDCの管理者。

本TOEを運用する際の前提条件を表4-1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4-1 前提条件

識別子	前提条件
A.TRUSTED_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。 ・ASP管理者は、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。 （注）ASP・SaaS事業者側で、利用者の識別認証を行い、識別認証の成功した利用者だけにTOEの利用を許可することを意図している。認証トークンには識別認証の成功した利用者の識別情報が含まれており、利用者がASP・SaaS事業者のサービスを介してTOEを利用する際に、ASP・SaaS事業者側からTOEに渡す必要がある。

	「認証トークン生成モジュール」は、認証トークンを生成するためのTOE外のソフトウェアであり、開発者から提供される。
A.TRUSTED_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。
A.ADMIN_OFFICE	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。

4.2 使用環境と構成

本TOEは、iDCに設置され、インターネットを介してASP・SaaS事業者から利用される。本TOEの一般的な使用環境を図4-1に示す。

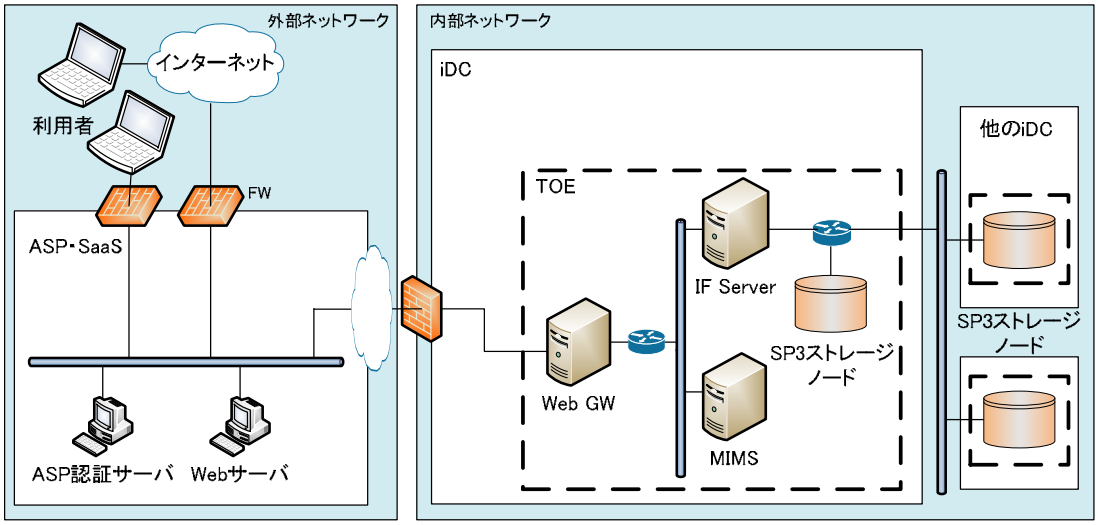

図4-1　TOEの使用環境

TOEの内部には、WebGW、IF Server、MIMS、SP3ストレージノードがあり、TOEの範囲は、それらのハードウェア及びソフトウェアの全体である。WebGW、IF Server、MIMS、SP3ストレージノードの用語説明については、11章を参照。

なお、TOE内部でデータを格納するSP3ストレージノードは、複数のiDCに設置されている。図4-1では、3つのiDCに3つのストレージノードが図示されているが、実際にはもっと多くのiDCとストレージノードが使われている。

4.3 使用環境におけるTOE範囲

本TOEでは、以下の脅威については想定していない。

・利用者の識別認証や、識別認証の成功した利用者に対する認証トークン生成は、TOE外のASP・SaaS事業者で行われることを前提としており、本評価では、利用者のなりすましや認証トークンの悪用は脅威として想定していない。

・本評価の構成では、ASP・SaaS事業者とTOEの接続は一ヶ所のiDCである。本評価では、災害や障害等により、接続箇所が使用不能になる場合は想定していない。

5 アーキテクチャに関する情報

本章では、本TOEの範囲と主要な構成について、目的と関連を説明する。

5.1 TOE境界とコンポーネント構成

TOEは、図4-1 TOEの使用環境において、点線で示された範囲のシステム全体である。TOEは、ASP・SaaS事業者に対して、HTTPSプロトコルを使用したAPIを提供する。

TOEは、APIによる指示に従って、ファイル及びディレクトリの作成、削除、読み込み、書き込み等の操作を実行し、結果を返却する。その際、アクセス制御機能、データの分散復元機能、データの完全性検証機能が適用される。

5.2 IT環境

ASP・SaaS事業者は、利用者の管理と識別認証を行い、識別認証の成功した利用者に認証トークンを発行し、TOEの利用を許可する。ASP・SaaS事業者からTOEの提供するAPIを使用する際には、その認証トークンが必要となる。

認証トークンの発行には、スカパーJSAT株式会社が提供する「認証トークン生成モジュール（ASP バージョン3.5.3）」を使用する。

6 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。TOEを使ったサービスを提供するASP・SaaS事業者、及びTOEの運用管理を行うiDC事業者は、前提条件及び組織のセキュリティ方針を満たすため、下記ドキュメントの十分な理解と遵守が要求される。

■ 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　バージョン 1.03
・医療ガイドライン対策文書　バージョン 1.01
・WebAPI仕様詳細　バージョン 1.05
・WebAPI利用ガイド　バージョン 2.05

■ iDC事業者向け

・医療ガイドライン対策文書　バージョン 1.01

7 評価機関による評価実施及び結果

7.1 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。

7.2 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21年11月に始まり、平成22年9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22年6月に開発者サイトで開発者のテスト環境を使用し、評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

7.3 製品テスト

評価者は、評価の過程で示された証拠を検証した結果から、必要と判断されたテスト及び脆弱性評定に基づく侵入テストを実行した。

7.3.1 開発者テスト

本評価において、開発者テストは保証要件に含まれていない。

7.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成を、図7-1　評価者テストの構成図に示す。

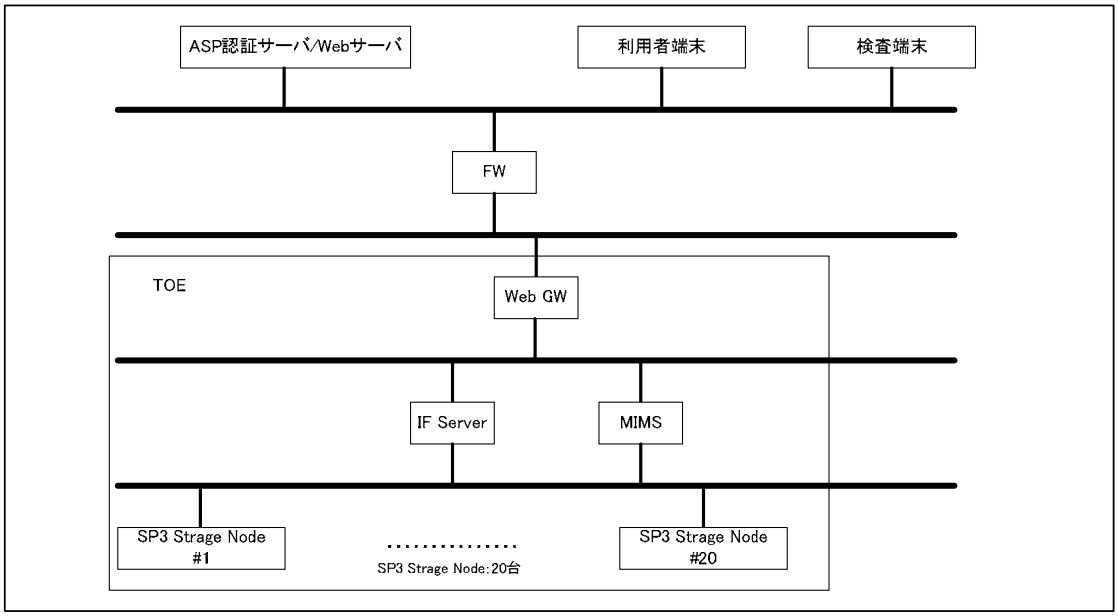

図7-1　評価者テストの構成図

対象としたTOEは、TOEテスト環境、及びTOE商用環境である。図7-1はTOEテスト環境の場合の構成図である。TOE商用環境の場合は、図7-1のTOEの部分が、インターネットを経由して商用環境のTOE部分に接続される。

評価者テストは本STにおいて識別されているTOEと同一のTOE商用環境、及び同等のTOEテスト環境で実施されている。

また、TOEのテストを行うためには、認証トークン生成モジュールを組み込んだASP・SaaS事業者の環境が必要となる。図7-1では、「ASP認証サーバ/Webサーバ」がASP・SaaS事業者の環境に相当する。テストに用いたASP認証サーバ/Webサーバの具体的構成は「7.4 評価構成について」に示す。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a.　独立テストの観点

評価者は、提供された評価証拠資料から、以下の観点での独立テストを考案した。

TOEの特性から評価者は、すべてのインタフェースとセキュリティ機能をテストするという方針のもと以下の観点で独立テストを実施した。

＜独立テストの観点＞

① TOEテスト環境において、アクセス制御を含め、TOEが提供しているすべての操作をテストする。

② TOEテスト環境において、データの分散復元、ハッシュ関数、及びSSL通信について､仕様どおりのメカニズムが実装されていることをテストする。

③ TOE商用環境において、典型的なファイル操作をテストする。

b. 独立テスト概要

評価者が実施した独立テストの概要は以下のとおり。

＜独立テスト手法＞

- TOEのAPIについて、利用者端末からTOEテスト環境に対して直接、様々な入力パラメタを設定した要求を送信し、その応答を観測した。その際、認証トークンは、ASP認証サーバ/Webサーバで生成したものを取り出して使用する。
- TOE内部のストレージノード上のファイルの状態の確認や、ファイルを消失する刺激を与えるために、TOEテスト環境のSP3ストレージノードにログインしてコマンドを実行した。
- TOEとASP認証サーバ/Webサーバとの間の通信プロトコルについて、専用ツールを用いてデータを取得し､通信プロトコルの種別とパラメタの確認を行った。
- TOE商用環境については、利用者端末のブラウザからASP認証サーバ/Webサーバ上に構築された模擬的なASP・SaaS環境を使用することによって、TOE商用環境の動作の確認を行った。

＜独立テストツール＞

独立テストにおいて利用したツールを表7-1に示す。

表7-1　独立テストツール

名称	概要・利用目的
利用者端末 （TOEテスト環境）	CentOS 5.5を搭載したPCであり、独立テストのため以下のツールを動作させる。
①curl 7.20.1	curlは、HTTTP形式でデータを送受信するためのコマンドラインツールである。端末からTOEのAPIを直接呼び出すために使用する。
利用者端末 （TOE商用環境）	Windows XP SP3を搭載したPC（ブラウザはInternet Explorer 6.0）。ブラウザを使用して、

		ASP認証サーバ/Webサーバにアクセスする。
検査端末		Windows XP SP3を搭載したPC（ブラウザはInternet Explorer 6.0）であり、独立テストのため以下のツールを動作させる。
	①Wireshark Version 1.2.8	パケットデータを解析するツール。SSL通信の確認のために使用する。
ASP認証サーバ/Webサーバ		模擬的なASP・SaaS環境。「7.4 評価構成について」の構成で、以下のツールを動作させる。
	①S*Plex3クラウドストレージサービス2010/6/30版	TOEの機能をデモするために、開発者が作成したWebアプリケーション。

＜独立テストの実施＞

独立テストの観点とその対応したテスト内容を表7-2に示す。

表7-2 実施した独立テスト

独立テストの観点	テスト概要
①	利用者端末からcurlを使用してTOEに要求を発行し、その返却値やダウンロードしたファイル内容を観測することにより、TOEが提供しているすべての操作が、仕様どおりに動作することを確認する。 また、所有者以外の利用者について、共有設定されている場合と共有設定されていない場合について、仕様どおりにアクセス制御されることを確認する。
②	TOE内のSP3ストレージノードにログインして、利用者データの断片、及び管理用データが格納されているファイル名を表示し、仕様どおりにハッシュ値の情報が含まれていることを確認する。
②	TOE内のSP3ストレージノードにログインして、分散格納されたデータの断片が消失した状況を作成し、その後、利用者端末からファイルをダウンロードして元どおりのファイルが得られるかどうかを確認する。 データ断片の消失は、データの一部を改ざんすることでハッシュ値がエラーとなりそのデータ断片が採用されない場合と、データの格納されているSP3ストレージノード上でTOEの動作を実現しているプロセスを停止することによりデータ断片が読み出せない場合の２種類をテストする。 いずれの場合も、消失断片数が、復元可能な閾値を越えた場合と超えない場合について、仕様どおりに復元可能かどうかを確認する。

②	検査端末のWiresharkで、Webサーバ（SSLクライアント）とTOE（SSLサーバ）の間の通信データを取得し、通信プロトコルがSSL/TLSであり、使用される暗号方式等が仕様どおりであることを確認する。
③	利用者端末のブラウザから、ASP認証サーバ/Webサーバの画面を操作して、ファイルの所有者の役割でログインし、アップロードしたファイルの共有設定と共有解除を行い、それらの操作が正常に動作することを確認する。また、共有を許可された利用者の役割でログインし、共有設定されているときにはファイルが参照でき、共有解除されたときにはファイルが参照できないことを確認する。

c. 結果

実施したすべての評価者独立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。

7.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① TOEに対して不正なパラメタを入力すると、TOEの入力パラメタ処理が適切でない場合、TOEが予期しない動作をする可能性がある。
② TOEに対して複数の操作を同時に実行すると、TOEの排他制御が適切でない場合、不完全なファイルが読み書きされる可能性がある。
③ 入力された文字列を解釈してコマンドを実行する処理では、公知の脆弱性として、文字列処理の誤りにより任意のプログラムが実行されることが知られており、TOEにもあてはまる可能性がある。
④ ネットワークを扱うプログラムには、多くの公知の脆弱性が知られており、TOEにもあてはまる可能性がある。

b. 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テスト環境は、検査端末を除き、評価者独立テストの環境と同じである。検査端末の詳細を表7-3に示す。

表7-3　侵入テストに用いた検査ツール

名称		概要・利用目的
検査端末		Windows XP SP2を搭載したPC（ブラウザはInternet Explorer 6.0）であり、侵入テストのため以下のツールを動作させる。
	①Nessus 4.2.2	ネットワーク上のサービスポートについて、既知の脆弱性の存在可能性を検出するツール。
	②Nikto 2.03	Webサーバについて、既知の脆弱性の存在可能性を検出するツール。

＜侵入テスト手法＞

- 評価者独立テストと同じテスト手法を用い、入力パラメタの変更や、処理を同時に実行した場合をテストする。
- 検査端末を用いて、公知の脆弱性が存在しないことを確認する。

＜脆弱性テストの実施＞

懸念される脆弱性と対応する侵入テスト内容を表7-4に示す。

表7-4　侵入テスト概要

脆弱性	テスト概要
①	利用者端末のcurlを使用して、APIの各種入力パラメタ（認証トークン、ディレクトリID、ファイルID、操作種別、取得データ数等）に不正な値を指定して処理を実行し、TOEのふるまい（エラーコード及びその後のTOE動作）が期待どおりであることを確認した。 テストした入力パラメタには、バッファオーバフローを引き起こす可能性のある文字列も含まれている。
②	利用者端末のcurlを使用して、ファイルの読み込みと削除をほぼ同時に実行し、その時のエラーコード、読み込まれたファイル、実行後の

	ディレクトリ一覧を検査して、不完全なファイル読み込みや削除漏れがないことを確認した。
③	利用者端末のブラウザから、ASP認証サーバ/WebサーバのWeb画面に、作成するディレクトリ名として特殊文字とOSコマンド等を含む文字列を指定しても、文字列全体がディレクトリ名と解釈されてエラーが返却されることを確認した。
④	検査端末を使用してNessusとNiktoをTOEに対して実行し、想定外のポートがオープンされていないこと、及びオープンされているポートに公知の脆弱性が存在しないことを確認した。

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.4 評価構成について

本TOEの範囲には、特別な設定や構成条件は存在しない。

なお、本TOEを使用するためには、認証トークン生成モジュールを組み込んだASP・SaaS事業者の環境が必要である。本評価では、ASP・SaaS事業者の環境として、以下のシステム構成を用いている。これらは、STに記述されているテストの構成と同じである。

表7-5 評価に用いたASP・SaaS事業者のシステム構成

サーバ	分類	項目	名称
ASP認証サーバ/Webサーバ	ハードウェア	CPU	Intel 64 (Pentium Dual Core E2160)
		メモリ	1GB
	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

7.5 評価結果

評価者は、評価報告書をもって本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。

評価では以下について確認された。

- PP適合：なし
- セキュリティ機能要件：　コモンクライテリア　パート２適合
- セキュリティ保証要件：　コモンクライテリア　パート３適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- EAL1パッケージのすべての保証コンポーネント
- 追加の保証コンポーネント　ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1

評価の結果は、第2章で識別されたTOEについて、本章の評価された構成のみに適用される。

7.6 評価者コメント/勧告

消費者に喚起すべき評価者勧告は特にない。

8 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 所見報告書でなされた指摘内容が妥当であること。
② 所見報告書でなされた指摘内容が解決されていること。
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、本ST及び評価報告書において、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、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、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すものと判断する。

8.2 注意事項

本TOEは、障害や災害時のデータ保護のために、消失訂正符号によるデータの分散復元機能やハッシュ値によるデータの完全性検証機能を備えており、本評価では、それらの機能が仕様どおりに実装され動作することが評価されている。しかし、ハッシュ値の衝突可能性は評価されていないため、どのような条件の場合に利用者データの完全性が保証されるかが明確でない。

また、本TOEには監査ログ機能を備えていないため、利用者によってはニーズに合致しない場合も考えられる。

本TOEに興味のある消費者は、TOEを提供しているスカパーJSAT株式会社から詳細な情報を入手し、TOEの提供する機能やサービス保証レベルが、各自のニーズに合致するかどうか確認することを推奨する。

9 附属書

特になし。

10 セキュリティターゲット

本TOEのセキュリティターゲット[12]は、本報告書とは別文書として、以下のとおり本認証報告書とともに提供される。

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　スカパーJSAT株式会社

11 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
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 Functionality（TOEセキュリティ機能）

本報告書で使用されたTOEに関する略語を以下に示す。

ASP	Application Service Provider
SaaS	Software as a Service
iDC	Internet Data Center

本報告書で使用された用語の定義を以下に示す。

ASP・SaaS事業者	ネットワークを通じてアプリケーションサービスを提供する事業者。本書ではASPとSaaSを区別せずASP・SaaSと呼ぶ。
ASP管理者	ASP・SaaS事業者が提供するサービスの管理者。
ASP認証サーバ	ASP・SaaS事業者において、ASP・SaaS事業者のサービスを提供するWebサーバと連携して、利用者の識別認証を行うサーバ。
IF Server	TOEを構成する装置の１つで、データの分散や復元を制御するサーバ。
MIMS	TOEを構成する装置の１つで、利用者データ及びその管理情報をTOEの扱うデータ形式に変換するサーバ。
SP3 ストレージノード	TOEを構成する装置の１つで、分散されたデータを格納するストレージ。
WebGW	TOEを構成する装置の１つで、セッション維持やアクセス制御を行うサーバ。
iDC管理者	TOEが設置されるiDCの管理者。
lookup3	ハッシュテーブルによる検索用途に開発されたハッシュ関数。インターネットでソースコードが入手できる。
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」の略称。

消失訂正符号	データに冗長性を付加して符号分割することにより、符号分割したデータ断片の一部が消失した場合に検出・訂正が可能な符号化方式。ただし、データ断片の中の誤りの検出・訂正はできない。
認証トークン	ASP・SaaS事業者で、識別認証が成功した利用者に発行される情報。利用者の識別情報等が含まれており、TOEを使用する際に必要とされる。
符号分割	データを分割するとともに符号化すること。
利用管理者	TOEを利用したASP・SaaS事業者のサービスを利用する組織の管理者。ASP・SaaS事業者から提供される機能を使用して、利用者の管理を行う。

12 参照

[1] 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

[2] 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

[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　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[7] 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 2009年7月 CCMB-2009-07-001 (平成21年12月翻訳第1.0版)

[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 2009年7月 CCMB-2009-07-002 (平成21年12月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート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 2009年7月 CCMB-2009-07-003 (平成21年12月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 3 July 2009 CCMB-2009-07-004

[11] 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3版 2009年7月 CCMB-2009-07-004 (平成21年12月翻訳第1.0版)

[12] 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　スカパーJSAT株式会社

[13] S*Plex3クラウドストレージサーバシステム 評価報告書 第3版 2010年9月7日 みずほ情報総研株式会社　情報セキュリティ評価室

[14] 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 平成21年7月 総務省