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22年12月27日 (IT認証0331)
認証番号	C0305
認証申請者	Hewlett-Packard Company
TOEの名称	HP StorageWorks P9000 Command View Advanced Edition Software Common Component
TOEのバージョン	7.0.1-00
PP適合	なし
適合する保証パッケージ	EAL2 及び追加の保証コンポーネントALC_FLR.1
開発者	Hewlett-Packard Company
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23年8月15日

技術本部 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

「HP StorageWorks P9000 Command View Advanced Edition Software Common Component」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、Hewlett-Packard Companyが開発した「HP StorageWorks P9000 Command View Advanced Edition Software Common Component、バージョン 7.0.1-00」（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23年7月25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Hewlett-Packard Company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、TOE利用者（ストレージ管理者、アカウント管理者、システム構築者）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、EAL2及び追加の保証コンポーネントALC_FLR.1である。

1.1.2 TOEとセキュリティ機能性

本TOE HP StorageWorks P9000 Command View Advanced Edition Software Common Component（以降，CVAECCと略記）は、SAN環境に接続された複数のストレージデバイスを一元的に管理するHP StorageWorks P9000 Command View Advanced Edition Softwareシリーズのストレージ管理ソフトウェア対し、共通機能を実現する基盤モジュールを提供するソフトウェア製品である。ストレージ管理ソフトウェアにはHP StorageWorks P9000 Device Manager Software（以降，DevMgrと略記），HP StorageWorks P9000 Replication Manager Software（以降，RepMgrと略記），HP StorageWorks P9000 Tiered Storage Manager Software（以降，TSMgrと略記），HP StorageWorks P9000 Tuning Manager Software (以降，TunMgrと略記)等があ

り、これらの製品群とCVAECCを総称してHP StorageWorks P9000 Command View Advanced Edition Softwareと呼ぶ。

CVAECCはHP StorageWorks P9000 Command View Advanced Edition Softwareの基盤モジュール製品として，各製品パッケージに同梱されて提供される。

本TOEは、ストレージ管理者がクライアント端末からストレージ管理ソフトウェア群にアクセスし、コピー等の操作を要求する際の識別・認証や、認証結果に基づいた権限情報の提示、警告バナー表示など、ストレージ管理ソフトウェア群に共通のセキュリティ機能を提供する。

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である。

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。

保護資産であるアカウントの権限情報が、不正な利用者により、あるいは、認証されたストレージ管理者またはアカウント管理者が、クライアント端末から本来は許可されていない操作を実行することにより、削除、改ざん、暴露されること及び警告バナー機能で使用する文面情報が削除、改ざんされることを脅威と想定する。

TOEは、その脅威に対抗するため、利用者がクライアント端末からストレージ管理ソフトウェアにアクセスする際、利用者の識別・認証を行い、ストレージ管理ソフトウェアからの要求に応じて、ログイン中の利用者のセッションを管理し、ログインした利用者の識別・認証が維持されていることの確認を行う（識別・認証機能）。また、各利用者の認証方式、アカウント情報、ACLテーブル、バナー情報、セキュリティパラメタ等の管理を行い（セキュリティ情報管理機能）、ストレージ管理ソフトウェアにアクセスする際、不正な使用に対する警告メッセージ（設定されたバナー情報）を返信する（警告バナー機能）。

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する。

本TOEを設置する場所は、施錠され入退場が制限された業務サーバエリア／センタであり、入室を許可されるのは悪意を持たない、信頼できるハードウェア・

ソフトウェアの管理者のみである。外部ネットワークからはファイアウォールによって保護された業務サーバエリア/センタに、管理ネットワークとして、管理サーバ、ストレージ、周辺機器等とともに設置されることを想定している。

TOEの識別・認証機能を外部認証サーバ・認可サーバに代行させる場合、それらはストレージ管理ソフトウェアのサーバと同一の業務サーバエリアに設置する。両サーバを異なるサーバエリアに設置する場合は、両サーバ間の通信路は秘匿性と完全性が確保されているものとする。

TOEは、ストレージ管理ソフトウェア製品に同梱される製品であり、次の製品と組み合わせて利用されるものとする。

DevMgr v5.6.0以降
TSMgr v5.5.0以降
RepMgr v5.6.0以降
TunMgr v7.0.0以降

1.1.3 免責事項

・本TOEは、クライアント端末からWebのインタフェースを介してアクセスする運用環境を想定しており、本TOE が想定する攻撃者は、高度な専門知識を持たず､管理者が操作できるクライアント端末からWebのインタフェースを利用する攻撃者に限られる。

・外部認証機能､外部認証グループ連携機能を利用する場合の､外部認証サーバ・外部認可サーバが持つ識別・認証機能は本評価の対象外である。また、外部認証サーバ･認可サーバのなりすましは運用環境で防止されていることを前提とする。

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23年7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]、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。

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。

2 TOE識別

本TOEは、以下のとおり識別される。

TOE名称：	HP StorageWorks P9000 Command View Advanced Edition Software Common Component
バージョン：	7.0.1-00
開発者：	Hewlett-Packard Company

製品が評価･認証を受けた本TOEであることを、利用者は以下の方法によって確認することができる。

ガイダンスに記述されたバージョン確認手順に従い操作することで正しいバージョンであることを確認できる。また購入時のセキュリティガイドからも、識別が可能である。

3 セキュリティ方針

本章では、本TOEが脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本TOEは、識別・認証された正当なストレージ管理者が、認証に従った適切な権限情報を取得することで、ストレージ管理権限に基づく管理環境を得られるようにするため、ストレージ管理ソフトウェア群に以下のような共通のセキュリティ機能を提供する。

①「識別・認証機能」

TOE利用者がストレージ管理ソフトウェアにログインする際に、ユーザID及び対応するパスワードを用いて識別・認証を行い、その結果に基づいてセッションを生成・維持する機能。また、認証結果に基づいて、複数あるストレージ管理ソフトウェアが持つ操作権限情報を、要求元（ストレージ管理ソフトウェア）に応答する機能。

識別・認証に一定回数続けて失敗した場合には、アカウントをロックする。

TOEは、TOEが持つ内部認証機能に代えて、TOE外にある外部認証サーバの提供する外部認証機能、あるいは外部認証グループ連携機能を利用することもできるが、外部認証サーバ・外部認可サーバが持つ識別・認証機能はTOEに含まない。

②「セキュリティ管理機能」

TOEに登録され、識別・認証されたTOE利用者が、クライアント端末から本来は許可されていない操作を実行することによって、TOEで管理する権限情報を削除、改ざん、暴露し、バナー情報を削除、改ざんすることのないよう、TOE利用者のアカウント情報（ユーザID、パスワード、ロックステータス）を管理し、セキュリティパラメタ（「アカウント自動ロック」,「パスワード複雑性チェック」）を設定する機能。

③「警告バナー機能」

TOEの利用者の権限・役割に関係なく、ストレージ管理ソフトウェアにログイン時に、ログイン画面に警告用のバナー情報を表示する機能。また、システム構築者またはアカウント管理者が、そのメッセージデータを入力する機能。

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（不正な接続）	不正な利用者が、管理クライアントから、ストレージ管理ソフトウェアの機能のために必要な、TOEで管理する権限情報を削除、改ざん、暴露し、バナー情報を削除、改ざんするかもしれない。
T.UNAUTHORISED_ACCESS（権限外のアクセス）	認証されたストレージ管理者またはアカウント管理者が、管理クライアントから、本来は許可されていない操作を実行することによって、TOEで管理する権限情報を削除、改ざん、暴露し、バナー情報を削除、改ざんするかもしれない。

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

ストレージ管理クライアント端末の利用者がTOEおよびストレージ管理ソフトウェアにアクセスする際に、内部認証を指定された利用者の場合はTOEで、外部認証を指定された利用者の場合は外部認証サーバが、その利用者の識別・認証を行い、許可された利用者であるかどうかの確認を行う。

TOEおよび外部認証サーバは、推測されにくいパスワードが設定されるようパスワードの登録パターンを制限するとともに、利用者自身も、パスワードの長さ、パスワードに利用する文字種の組み合わせから、推測困難なパスワードを設定し、適切な頻度で変更する上、パスワードを漏えいさせないことで、安全なパスワード管理を実現する。さらに、TOEが所定の回数以上連続して認証に失敗した場合、利用者のアカウントを自動的にロックすることで、総当りによるパスワード攻撃にも対抗する。

(2) 脅威「**T.UNAUTHORISED_ACCESS**」への対抗

TOEは、ストレージ管理ソフトウェアおよびTOEの利用者に与えられた権限情報に従って、ストレージ管理クライアント端末の利用者による権限情報、バナー情報へのアクセスを制御する。

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.BANNER（警告バナー）	ストレージ管理ソフトウェアは、ストレージ管理ソフトウェアの不正な使用に関する勧告的な警告メッセージを表示する機能を持たなければならない。

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満たす機能を具備する。

(1) 組織のセキュリティ方針「**P.BANNER**」への対応

TOEは、ストレージ管理ソフトウェアの不正な使用に関する勧告的な警告メッセージを、ストレージ管理ソフトウェアに提供する。ストレージ管理ソフトウェアは、TOEより提供されたストレージ管理ソフトウェアの不正な使用に関する勧告的なメッセージを表示する機能をもつ。

4 前提条件と評価範囲の明確化

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運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

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.PHYSICAL（ハードウェア等の管理）	TOEおよびストレージ管理ソフトウェアが動作する管理サーバと周辺機器、TOEが利用する外部認証サーバ・外部認可サーバ、ストレージ装置、内部ネットワーク、および内部ネットワークの境界に位置するファイアウォールは、物理的に隔離された業務サーバエリアに設置されるものとする。そのエリアに入室を許可される人物はそのエリアに設置されたハードウェア・ソフトウェアの管理者のみであり、その管理者はエリア内に対し悪意を働かない信頼できる人物であるものとする。
A.ADMINISTRATORS（管理者）	システム構築者は信頼できる。アカウント管理者、ストレージ管理者、およびアプリケーションサーバを含めた他サーバの管理者は、それぞれに課せられたストレージ管理ソフトウェアの利用者のアカウントおよび権限情報の管理業務、ストレージ管理業務、他サーバの管理業務に関して、悪意のある操作を行わない。
A.PASSWORD（複雑なパスワード）	不正な利用者がパスワードを推測してログインしないように、パスワードは、パスワードの長さ、パスワードに利用する文字種の組み合わせから、推測困難なパスワードを設定するものとする。さらに、認証の試行回数を制限する機能を利用し、無制限に認証が試行されることを防止するものとする。
A.SECURE_CHANNEL（通信の秘匿性）	TOEおよびストレージ管理ソフトウェアが動作する管理サーバと管理クライアントとの間のネットワーク、TOEが利用する外部認証サーバ・外部認可サーバとTOEの間のネットワークは、通信の秘匿性と完全性が確保されているものとする。

A.NETWORKS （ネットワーク）	管理サーバが接続される管理ネットワークを含めた業務サーバエリアに設置される内部ネットワークは、ファイアウォールなどにより、ストレージ管理クライアント端末からの通信に制限する。
A.SRV_MGMT (サーバの管理)	管理クライアントから内部ネットワークに対してTOEを介さずに直接アクセスされることがないように、サーバで実行するサービスやサーバの設定、サーバに登録するアカウントを管理されているものとする。 （補足）SSHやtelnetによるリモートアクセスは、内部ネットワークへのアクセスとみなされるために禁止されていることを前提とする。
A.CLIENTS（ストレージ管理クライアントの管理）	ストレージ管理クライアントには、悪意のあるソフトウェアは存在しない。
A.VERSION（TOEと組み合わせて利用可能な製品バージョン）	TOEは、次の製品と組み合わせて利用されるものとする。 DevMgr v5.6.0以降 TSMgr v5.5.0以降 RepMgr v5.6.0以降 TunMgr v7.0.0以降

4.2 運用環境と構成

本TOE（CVAECC）はHP StorageWorks P9000 Command View Advanced Edition Software シリーズのストレージ管理ソフトウェアに、共通機能を実現する基盤モジュールを提供するソフトウェアとして、ストレージ管理ソフトウェアと共に管理サーバにインストールされる。

管理サーバは、アプリケーションサーバ、ストレージ、周辺機器等とともに、オフィスの施錠された業務サーバエリア/センタ内に設置され、エリア内はファイアウォールによって外部のネットワークから保護されている。

利用者であるストレージ管理者及びアカウント管理者は、業務サーバエリア外のストレージ管理クライアント端末から、ファイウォールを介してエリア内のストレージ管理ソフトウェアにアクセスし、ストレージ管理業務に必要なコピー等の操作を行う。

ストレージは、業務アプリケーションを実行するアプリケーションサーバに接続され、ボリュームの中に業務アプリケーション実行に必要な情報を保持している。そのため、管理ネットワーク（内部ネットワーク）と業務ネットワーク（外部ネットワーク）の両方に属しているが、それぞれのネットワーク接続用に独立したネットワークカードを搭載しており、ふたつの管理ネットワークは分離され、相互に干渉しない。

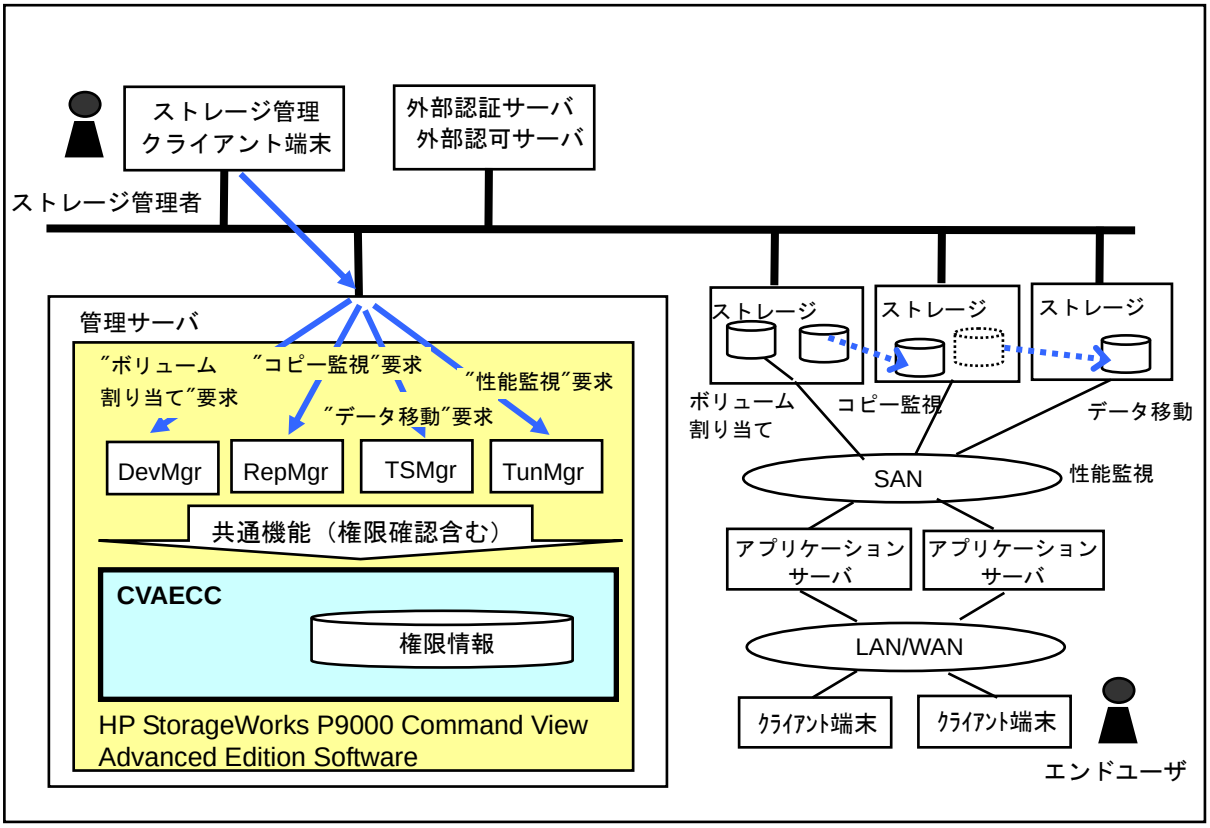

図 4-1　TOEの運用環境

構成条件

ストレージ管理ソフトウェア（TOEと組み合わせて利用可能な製品バージョン）

・HP StorageWorks P9000 Device Manager Software（DevMgrと略記、v5.6.0以降）
・HP StorageWorks P9000 Replication Manager Software（RepMgrと略記、v5.6.0以降）
・HP StorageWorks P9000 Tiered Storage Manager Software（TSMgrと略記、v5.5.0以降）
・HP StorageWorks P9000 Tuning Manager Software（TunMgrと略記、v7.0.0以降）

TOEは、以下のいずれかを満たすプラットフォームで動作する。

(1) 管理サーバ

・Windows 版の HP StorageWorks P9000 Command View Advanced Edition Software Common Component がインストールする Java™VM（Version 1.5.0_11 以降）が動作するプラットフォーム。
・Linux版のHP StorageWorks P9000 Command View Advanced Edition Software Common Componentがインストールする Java™VM（Version 1.5.0_05以降）が動

作するプラットフォーム。

(2) ストレージ管理クライアント端末

[クライアントのOSがWindowsの場合]

・Microsoft Internet Explorer 6.0, 7.0, 8.0

[クライアントのOSがLinuxの場合]

・Firefox 3.6.0 以降

(3) 外部認証サーバ／外部認可サーバ

Microsoft Active Directory (Windows Server 2003 シリーズまたは Windows Server 2008 シリーズ付属のもの)

4.3 運用環境におけるTOE範囲

業務サーバエリア内に、外部認証サーバ・外部認可サーバを設置し、TOEの識別・認証機能を代行させる「外部認証機能」、「外部認証グループ連携機能」も使用することが可能であるが、外部認証サーバ・外部認可サーバの持つ識別・認証機能自体はTOEの範囲ではなく、セキュリティ対策方針に則りセキュアに運用されることは、運用者の責任となる。

TOEは汎用のOS上で稼動（OSの機能に（プロセス管理/プロセス分離等）に依存）するサーバプログラムであるが、前提条件からTOEへのアクセスは管理クライアント端末からのアクセスに限定されており、さらに管理クライアント端末に悪意のあるソフトウェアは存在せず、OSのコマンド等が悪用されることもない。

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（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

TOEの構成を図 5-1 に示す。破線で囲われたライブラリ及びプログラムから構成される範囲である。動作するオペレーティングシステムはTOEの範囲ではない。

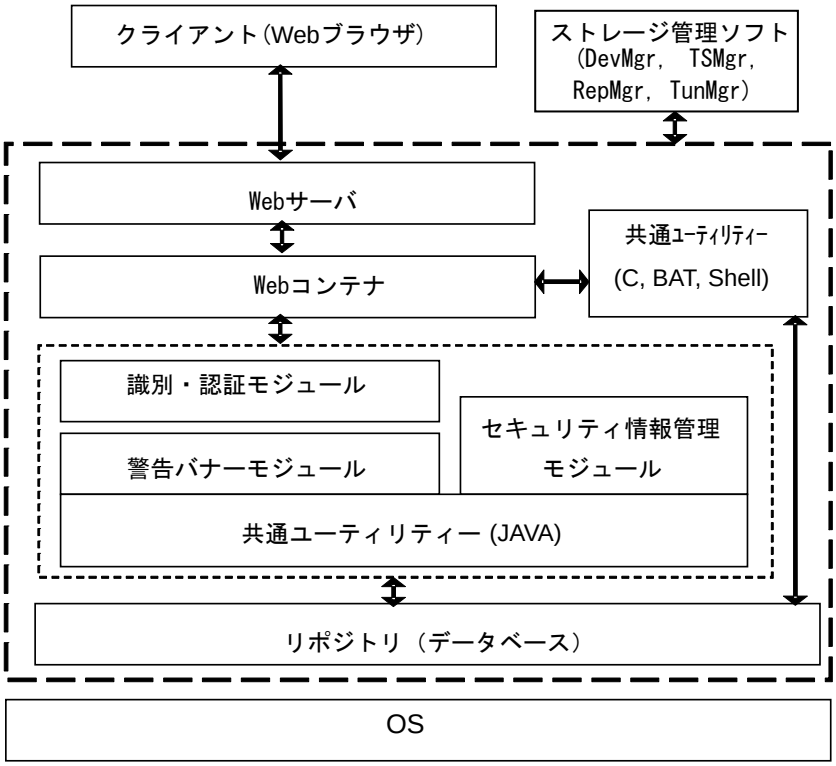

図 5-1 TOE境界

・識別・認証モジュールは、TOEの識別・認証機能を実現しているモジュールである。
・セキュリティ情報管理モジュールは、TOEのセキュリティ情報管理機能を実現しているモジュールである。
・警告バナーモジュールは、TOEの警告バナー機能を実現しているモジュールである。
・共通ユーティリティは、TOEの共通ユーティリティを実現しているモジュールである。
・webサービスモジュールは、TOEのwebサービスを実現しているモジュールである。
・GUIフレームワークは、TOEのGUIフレームワークを実現しているモジュールである。
・リポジトリは、TOEが有するデータを保持しているDBである。

5.2 IT環境

本TOEは、SAN環境に接続された複数のストレージデバイスを一元的に管理するストレージ管理ソフトウェアに対して、共通機能を提供する基盤モジュールとして、ストレージ管理ソフトウェアとともに、動作プラットフォームとして、Windows (Java™VM(Version 1.5.0_11以降)が動作する)、Linux (Java™VM（Version 1.5.0_05以降）が動作する）のいずれかをOSとする管理サーバ上にインストールされる。

TOE利用者は、クライアント端末から、ブラウザとしてMicrosoft Internet Explorer 6.0, 7.0, 8.0 (クライアントのOSがWindowsの場合)、Firefox 3.6.0以降（クライアントのOSがLinuxの場合)を介して操作を行う。

認証サーバでは、Microsoft Active Directory (Windows Server 2003シリーズまたは Windows Server 2008シリーズ付属のもの)を利用する。

外部認証では、LDAPディレクトリサーバ、RADIUSサーバ、Kerberosサーバの認証機能を利用する。

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の利用者は、前提条件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。

HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Guide	TB581-96059

および上記セキュリティガイドの構成要素である下記ガイダンス。

- HP StorageWorks P9000 Command View Advanced Edition Suite Software Administrator Guide	TB581-96037
- HP StorageWorks P9000 Command View Advanced Edition Suite Software User Guide	TB581-96041
- HP StorageWorks P9000 Command View Advanced Edition Suite Software Installation and Configuration Guide	TB581-96036
- HP StorageWorks P9000 Replication Manager Software Configuration Guide	TB584-96016
- HP StorageWorks P9000 Replication Manager Software User Guide	TB584-96017
- HP StorageWorks P9000 Tuning Manager Software Server Administration Guide	TB588-96020
- HP StorageWorks P9000 Tuning Manager Software User Guide	TB588-96022
- HP StorageWorks P9000 Tuning Manager Software Installation Guide	TB588-96019

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た。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

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、2011年1月に始まり、2011年7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、2011年2月に開発者サイトへ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付の各ワークユニットに関するプロセスの施行状況の調査、および、開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。

7.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加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

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1に示す。

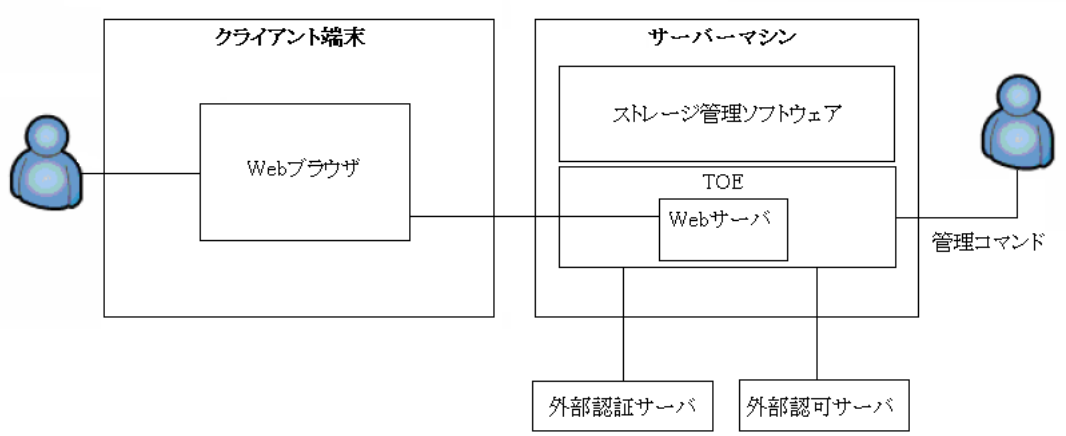

図 7-1 開発者テストの構成図

開発者テストは本 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。ST に TOE を同梱する製品のバージョンとして記述されているすべてのストレージ管理製品を使用したテストが実施されている。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

Web インタフェース、Java インタフェースおよびコマンドインタフェースについてはそれぞれブラウザとコンソールを介してアクセス

し動作を観察することにより行っている。一部の Java インタフェースについては、[ST]の前提条件を満たすストレージ管理製品は該当インタフェースを利用しないため、テストモジュールによりメソッドを起動してその動作を観察することにより行った。

＜開発者テストツール＞

開発者テストにおいて利用したツールを表 7-1に示す。

表 7-1　開発テストツール

	No	ハードウェア・ソフトウェア名称	詳細
構成機器	1	PCサーバ （クライアント端末、サーバマシン、外部認証サーバ）	・モデル名：dc7900SF/CT ・CPU：Core2Quad ・メモリ：4GB ・HDD容量：1000GB
ソフトウェア	1	TOE	・バージョン：7.0.1-00
	2	Windows（PCサーバのOS）	・Windows： Windows 2008 R2 Server Enterprise Edition
	3	Linux（PCサーバのOS）	・RedHat Enterprise Linux Advanced Edition 5 update 4 ・SuSE Linux Enterprise Server 11
	4	Active Directory	・Windows Server 2008附属
	5	Internet Explorer	・バージョン：7
	6	Firefox	・バージョン：3.6.9
	7	HP StorageWorks P9000 Device Manager Software 7.0.1-00	・バージョン：7.0.1-00
	8	HP StorageWorks P9000 Replication Manager Software 7.0.1-00	・バージョン：7.0.1-00
	9	HP StorageWorks P9000 Tiered Storage Manager Software 7.0.1-00	・バージョン：7.0.1-00
	10	HP StorageWorks P9000 Tuning Manager Software 7.0.0-01	・バージョン：7.0.0-01
	11	Eclipse	・バージョン：3.1.1

Eclipseは、STに記載される構成には含まれない、TOEの特定のJavaインタフェースをテストするために使用する開発用ソフトウェアであるが、テスト対象のインタフェースにのみアクセスしているため、TOEの他の部分に影響することがないと判断している。

b)　開発者テストの実施範囲

表 7-1 に列挙したストレージ管理製品と OS、ブラウザ毎に 422 件のテストが実施された。実施されたテストは、全ての TSFI を対象として

いる。

カバレージ分析によって、セキュリティ機能とテストIDの対応と、開発者が提示した [テスト項目とセキュリティ機能との関係] が一致していることを確認した。
テスト証拠資料におけるテストと機能仕様におけるTSFIとの間の対応が正確であり、セキュリティ機能に対して問題となるような点がないことが検証された。

c）結果

評価者は､開発者テストのテスト構成､テスト方法の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

なお、テスト結果において、ストレージ管理製品による違いはみられなかった。ストレージ管理製品はTOEのインタフェースを呼び出すために使用するものであり、開発証拠資料においてストレージ管理製品がセキュリティ機能のふるまいに影響をおよぼすと思われるような内容は確認されていない。

7.3.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプリングテストを実施するとともに、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をより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成を表 7-2 に示す。評価者が実施した独立テストの構成は、開発者テストと同様の構成である。

表 7-2　評価者テストの使用機器

用途	ハードウェア	ソフトウェア
サーバマシン	モデル名：HP Compaq dc7900SF/CT CPU：Intel Core2 Quad メモリ：4GB HDD：1000GB （Windows/Linux共通）	・Windows Server 2008 R2 Enterprise Edition ・HP StorageWorks P9000 Device Manager 7.0.1-00 ・HP StorageWorks P9000 Replication Manager 7.0.1-00 （Windows版のHP StorageWorks P9000 Command View Advanced Edition Software Common ComponentがインストールするjavaVM Version 1.5.0_11）
		・RedHat Enterprise Linux Advanced Editon5 update4 ・HP StorageWorks P9000 Device Manager 7.0.1-00 ・HP StorageWorks P9000 Replication Manager 7.0.1-00 （Linux版のHP StorageWorks P9000 Command View Advanced Edition Software Common ComponentがインストールするjavaVM Version 1.5.0_05） ・Firefox 3.6.9
		・SuSE Linux Enterprise Server 11 ・HP StorageWorks P9000 Device Manager 7.0.1-00 ・HP StorageWorks P9000 Replication Manager 7.0.1-00 （Linux版のHP StorageWorks P9000 Command View Advanced Edition Software Common ComponentがインストールするjavaVM Version 1.5.0_05） ・Firefox 3.6.9
外部認証サーバ、外部認可サーバ	モデル名：HP Compaq dc7900SF/CT CPU：Intel Core2 Quad メモリ：4GB HDD：1000GB	・Windows Server 2008 Enterprise Edition ・Active Directory（上記OSに同梱されるもの）
クライアント端末	モデル名：HP Compaq dc7900SF/CT CPU：Intel Core2 Quad メモリ：4GB HDD：1000GB （Windows/Linux共通）	・Windows Server 2008 Enterprise Edition ・Internet Explorer 7
		・RedHat Enterprise Linux Advanced Editon5 update4 ・Firefox 3.6.9
		・SuSE Linux Enterprise Server 11 ・Firefox 3.6.9

独立テストは、本STにおいて識別されているTOE構成、評価者テスト環境と同一の環境で実施された。

(2) 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である。

a) 独立テストの観点

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

以下の観点により、開発者のテスト仕様書からテスト項目を抽出した。

①セキュリティ機能の観点

セキュリティ機能に偏りなくテストを行うために、セキュリティ機能（SF.I&A、SF.MGMT、SF.BANNER）それぞれからサンプリングする。

②インタフェースの観点

Webインタフェース、Javaインタフェース、コマンドインタフェースのふるまいを確認するために、それぞれのインタフェースタイプからサンプリングすると共に、全てのSFRを網羅するようサンプリングする。Javaインタフェースについ てはWebインタフェースから呼び出されることを考慮する。

テストのサブセットは以下の観点から考案した。

ｉ）開発者テストのバリエーション

開発者テストで実施されていない操作ケース、および開発者テストで実施されているがパラメタのバリエーションが限られているケースを補足する。

ⅱ）インタフェースの観点

Webインタフェース、Javaインタフェース、コマンドインタフェースのふるまいを確認するために、全てのTSFIをテストの対象とする。また、JavaインタフェースはWebインタフェースから呼び出されることを考慮する。

b) 独立テスト概要

開発者テストのサンプリングテストとして、OS とブラウザの組み合わせ毎に 54 件のテストを実施した。サンプルの選択にあたっては、上記の「a) 独立テストの観点」①および②で示したように、セキュリティ機能、インタフェースを考慮した。

評価者テストとして、12 件のテストを実施した。テストの考案に当たっては、上記の「a) 独立テストの観点」ｉ）およびⅱ）で示したように、

開発者テストで考慮されていないパラメタ､役割を考慮することにより、開発者テストを補足した。

インタフェースについては､SFR に関連しないインタフェースとログアウトのインタフェース以外を全てカバーした。カバーしていないインタフェースは、開発者が実施したテスト手法で十分にふるまいを確認できることから評価者テストを行う必要がないと判断した。

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テストの実施内容＞

独立テストの観点とそれに対応したテスト内容を表 7-3に示す。

表 7-3 実施した独立テスト

独立テストの観点	テスト概要
① ユーザ追加機能テスト	アカウント管理者によるユーザ登録のふるまいを確認する。 開発者はシステム構築者によるユーザ登録をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
② パスワード変更機能テスト	アカウント管理者による自分のパスワード変更のふるまいを確認する。 開発者はシステム構築者による自身のパスワード変更をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
③ パスワード複雑性設定の変更機能テスト	パスワード複雑性設定のふるまいを確認する。 開発者はパスワード複雑性設定として「0」や負の数を含む場合を確認していない。「0」や負の数を含む規則に関するふるまいを確認する。
④ Webインタフェースにおける警告バナーの変更機能テスト	警告バナーの設定時のふるまいを確認する。 開発者は単独のHTMLタグについてテストしているが、タグを構成する文字や属性を含む場合を確認していない。タグを構成する文字や属性を含む文字列を設定する場合のふるまいを確認する。
⑤ コマンドインタフェースにおける警告バナーの変更機能テスト	コマンドインタフェースでの警告バナー設定のふるまいを確認する。 開発者は新規にバナーを設定する場合についてテスト

	しているが、Webインタフェースでの設定後について確認していない。Webインタフェースでの設定後にコマンドを実行した場合のふるまいを確認する。
⑥ hcmdslinkコマンドのロックステータス機能テスト	hcmdslinkコマンドのふるまいを確認する。 開発者はインタフェースでの連続認証失敗回数が、事象を発生させたインタフェースに影響することをテストしているが、別のインタフェースの失敗回数も関連することを確認していない。別のインタフェースの連続認証失敗回数も関連することを確認する。
⑦ hcmdsrepコマンドのロックステータス機能テスト	hcmdsrepコマンドのふるまいを確認する。 開発者はインタフェースでの連続認証失敗回数が、事象を発生させたインタフェースに影響することをテストしているが、別のインタフェースの失敗回数も関連することを確認していない。別のインタフェースの連続認証失敗回数も関連することを確認する。
⑧ hcmdsxrepコマンドのロックステータス機能テスト	hcmdsxrepコマンドのふるまいを確認する。 開発者はインタフェースでの連続認証失敗回数が、事象を発生させたインタフェースに影響することをテストしているが、別のインタフェースの失敗回数も関連することを確認していない。別のインタフェースの連続認証失敗回数も関連することを確認する。
⑨ hcmdsunlockaccountコマンドのロック解除機能テスト	hcmdsunlockaccountコマンドのロック解除のふるまいを確認する。 開発者は所定のパスワード長以上のパスワードを入力した場合について確認していない。設定されている以上のパスワード長を入力した場合のふるまいを確認する。
⑩ 外部認証の認証機能テスト（LDAP）	外部認証としてLDAPを指定している場合の外部認証機能のふるまいを確認する。 開発者はストレージ管理者による外部認証機能をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
⑪ 外部認証の認証機能テスト（RADIUS）	外部認証としてRADIUSを指定している場合の外部認証機能のふるまいを確認する。 開発者はストレージ管理者による外部認証機能をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
⑫ 外部認証の認証機能テスト	外部認証としてKerberosを指定している場合の外部

（Kerberos）	認証機能のふるまいを確認する。 開発者はストレージ管理者による外部認証機能をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者はTOEのふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが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となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a. 懸念される脆弱性

評価者は、提供された証拠資料（セキュリティアーキテクチャ仕様書、構造設計書、機能仕様書）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はデータベースを使用していることから、SQLインジェクションをひきおこす可能性が考えられる。
② TOEはOS上で動作するソフトウェアであることから、OSコマンドインジェクションをひきおこす可能性が考えられる。
③ ウェブアプリケーションで一般に懸念される問題として、パス名パラメタの未チェック/ディレクトリトラバーサルをひきおこす可能性が考えられる。
④ 直接攻撃の観点から、トークンのランダム性が不十分である可能性および不正なトークンにより攻撃される可能性が考えられる。
⑤ ウェブアプリケーションで一般に懸念される問題として、クロスサイトスクリプティングの可能性が考えられる。
⑥ 監視の観点から、TOEは、上位製品が提供するログイン画面で入力されたパスワードを受け取り、TOE自身はログイン画面を提供していな

いため認証フィードバックのSFRが選択されていないが、ログイン時のパスワード入力時に、画面にパスワードが表示されるなどして、盗み見られる危険が考えられる。

⑦ TOEは警告メッセージの文字数や最大数に制限がある機能が存在するため、その制限を超える大きさのデータを入力することにより、予期しない動作をするかもしれない。また、サニタイズ等がクライアント上で行われていた場合、TOEに直接サニタイズ等が必要な文字を入力することで予期しない動作をするかもしれない。

⑧ その他の公知の脆弱性

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を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは独立テストを実施した環境に検査 PC を追加した環境で実施した。

侵入テストで使用したツールの詳細を表 7-4 に示す。検査 PC 以外の部分については独立テストを実施した環境と同一である。侵入テストは独立テストを実施した環境に設置されているすべてのサーバを対象に実施した。

表 7-4　侵入テストで使用したソフトウェア

ソフトウェア名称	概　要
OS	WindowsXP SP3
Webブラウザ	Microsoft Internet Explorer Version 6.0
	Microsoft Internet Explorer Version 8.0
スキャンツール	Nessus 4.4.0 ・セキュリティスキャナ ・脆弱性データベースは2011年2月9日現在最新のものを使用
Webサーバスキャナ	Nikto 2.1.3 ・フリーウェア ・Webサーバを対象とするセキュリティ・スキャナ ・脆弱性データベースは2011年2月9日現在最新のものを使用
Tamper IE	TamperIE 1.2 ・フリーウェア ・IEからの送信データをキャプチャし、任意のデータに改ざんすることができる。

＜侵入テスト手法＞

独立テストを実施した環境に設置されているすべてのサーバを対象に、

上位製品を用いてTOEのインタフェースを刺激した。

・TSFI から刺激をあたえて振る舞いを確認する
・管理クライアントから TOE に対して送信されるパケットをツールを使ってキャプチャし内容を確認する
・キャプチャした内容を改ざんして TOE に送信する
・脆弱性検査ツールによるスキャンを実施する

バイナリ検査においては､｢バイナリファイル中に秘密のパラメタが抽出可能な形で存在していないか」という観点で、バイナリファイルをバイナリエディタ(Stirling)で開き、文字列として認識できる部分を確認した。

＜侵入テストの実施項目＞

侵入テストはバイパス、直接攻撃、監視、ウェブアプリケーションで一般に懸念される問題の観点から実施した。これらのテストは具体的には以下の 8 種類のテストに分類された。

懸念される脆弱性と対応する侵入テスト内容を表 7-5に示す。

表 7-5　侵入テスト概要

脆弱性	テスト概要
① SQLインジェクションのテスト	SQLインジェクションにつながる可能性のあるパラメタをPOSTパラメタに設定しTOEに入力して動作を確認する。
② OSコマンドインジェクションのテスト	OSコマンドインジェクションにつながる可能性のあるパラメタをPOSTパラメタに設定しTOEに入力して動作を確認する。
③ ディレクトリトラバーサルのテスト	ディレクトリを直接指定して動作を確認する。
④トークンのランダム性の確認と不正なトークンによる実行性の確認	トークンを取得し規則性がないことを確認する。パラメタに不正なトークンを入力して、TOE の動作を確認する。
⑤ クロスクサイトスクリプティングのテスト	クロスクサイトスクリプティングにつながる可能性のあるパラメタを POST パラメタに設定し TOE に入力し、動作を確認する。
⑥ パスワード入力時の入力値保護のテスト	パスワード入力時に、画面にパスワードが表示されるなどして、盗み見られる危険が無いかどうか

	を確認する。
⑦ バッファオーバフローのテスト	サイズに制限があるパラメタについて、制限を越える大きさの値を設定し、動作を確認する。
⑧ ツールによる検査	その他の公知の脆弱性を検査するためツールによる検査を行う。

c) 結果

評価者が実施した侵入テストでは、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

侵入テストは独立テストを実施した環境に検査PCを追加した環境で実施した。検査PC以外の部分については独立テストを実施した環境と同一である。侵入テストは独立テストを実施した環境に設置されているすべてのサーバを対象に実施した。

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。

- 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。

- EAL2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 ALC_FLR.1

評価の結果は、第2章に記述された識別に一致するTOEによって構成されたもののみに適用される。

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 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。
② 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。
③ 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。

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EAL2及び保証コンポーネントALC_FLR.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

一部は 1.1.3にも示したとおり、以下の点に注意する必要がある。

・本TOEは、クライアント端末からWebのインタフェースを介してアクセスする運用環境を想定しており、管理クライアントから内部ネットワークに対してTOEを介さずに直接アクセスされることがないように、SSHやtelnetによるリモートアクセスは禁止されていることを前提とする。攻撃者がローカルアクセスを行う環境は対象に含まれない。

・本TOEは、アプリケーションの実行環境を提供するものではないため、DoS攻撃は本評価の対象としていない。

・外部認証機能、外部認証グループ連携機能を利用する場合、外部認証サーバ・外部認可サーバが持つ識別・認証機能はTOEには含まれない。その場合のセキュリティ対策は、IT環境のセキュリティ対策方針、運用により実現するセキュリティ対策方針でカバーされるものとする。

・外部認証サーバ・認可サーバのなりすまし防止は運用環境で対策されていることを前提とする。

・TOEおよびデータは、OSが管理するファイルとして存在する。TOEのインストールはOSの管理者権限で行う必要があり、インストール後、TOEを構成するモジュールなどのファイルの変更／削除にはOSの管理者権限が必要である。また、データについてもOSの管理者権限でしか変更や削除ができないことを前提とする。

・製品のオンラインヘルプは、保証対象ガイダンスには含まれない。保証対象ガイダンスについては、6. 製品添付ドキュメントを参照のこと。

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。

HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Target バージョン 1.03　2011 年 4 月 8 日 Hewlett-Packard Company

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。

SAN	Storage Area Network
ACL	Access Control List
CVAECC	HP StorageWorks P9000 Command View Advanced Edition Software Common Component
DevMgr	HP StorageWorks P9000 Device Manager Software
RepMgr	HP StorageWorks P9000 Replication Manager Software
TSMgr	HP StorageWorks P9000 Tiered Storage Manager Software
TunMgr	HP StorageWorks P9000 Tuning Manager Software

本報告書で使用された用語の定義を以下に示す。

権限 (権限情報)	TOEがストレージ管理ソフトに許可する操作の種類を表す。ユーザ情報を管理するUser Management権限、ストレージの参照、改変、タスクを実行するためのView, Modify, Execute権限などがある。各利用者には、これらの各権限または各権限の組み合わせが権限情報として付与される。
ACLテーブル	アカウントとストレージ管理のための権限情報を管理するテーブル
CVAECC	HP StorageWorks P9000 Command View Advanced Edition Software Common Component。 HP StorageWorks P9000 Command View Advanced Edition Softwareの１つであり，HP StorageWorks P9000 Command View Advanced Edition Softwareに属するストレージ管理ソフ

	トウェアに対して共通機能を提供する基盤モジュール。
DevMgr	HP StorageWorks P9000 Device Manager Software。 HP StorageWorks P9000 Command View Advanced Edition Softwareの１つであるストレージ管理ソフトウェア。ストレージのボリューム管理機能を提供する。
RepMgr	HP StorageWorks P9000 Replication Manager Software。 HP StorageWorks P9000 Command View Advanced Edition Softwareの１つであるストレージ管理ソフトウェア。ストレージのボリューム間で行われるコピーの管理機能を提供する。
TSMgr	HP StorageWorks P9000 Tiered Storage Manager Software。 HP StorageWorks P9000 Command View Advanced Edition Softwareの１つであるストレージ管理ソフトウェア。ストレージのボリューム間でのデータ移動を制御する。
TunMgr	HP StorageWorks P9000 Tuning Manager Software。 HP StorageWorks P9000 Command View Advanced Edition Softwareの１つであるストレージ管理ソフトウェア。ストレージのリソース利用効率の管理機能を提供する。
セキュリティパラメタ	CVAECCのセキュリティ機能に関連するパラメタ情報。パスワードの文字数やパスワードに使用する文字種別、ログインの連続失敗回数とその閾値、閾値を超えた(アカウントがロックされたか)などの情報。
警告バナー	ストレージ管理ソフトウェアの利用者に対する、利用前の警告文面表示。主に不正利用に対する注意喚起に用いられる。
内部認証	TOEの内部認証機能のみを利用する認証。CVAECC 6.0.0-01と同じ認証方式。
外部認証	TOE内部から、TOE外部の外部認証サーバ（LDAPディレクトリサーバ、RADIUSサーバ、Kerberosサーバ）の認証機能を利用する認証方式。
外部認証グループ連携	外部認可サーバに登録された、グループとそのグループに属するアカウントの情報をTOEが取得し、TOE内部で権限情報を付与する機能。TOE外部の認証機能を前提とし、アカウントはグループに属していることから、「外部認証グループ連携」と呼ぶ。

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23年2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23年2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23年2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] HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Target、バージョン1.03、2011年4月8日、Hewlett-Packard Company

[13] HP StorageWorks P9000 Command View Advanced Edition Software Common Component 評価報告書、第2版、2011年7月25日、みずほ情報総研株式会社 情報セキュリティ評価室

[14] HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Guide、TB581-96059、Hewlett-Packard Company